# Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Πληροφορική»

**Μεταπτυχιακή Διατριβή**

| | |
|---|---|
| Τίτλος Διατριβής | **"ΗΛΕΚΤΡΟΝΙΚΟ ΈΓΚΛΗΜΑ"** |
| Ονοματεπώνυμο Φοιτητή | **ΛΑΜΠΡΙΝΗ ΧΑΛΙΜΟΥΡΔΑ** |
| Πατρώνυμο | **ΧΡΗΣΤΟΣ** |
| Αριθμός Μητρώου | **ΜΠΠΛ/ 07056** |
| Επιβλέπων | **ΣΙΝΑΝΙΩΤΗ ΑΡΙΣΤΕΑ** |

Ημερομηνία Παράδοσης **23/11/2010**



**Τριμελής Εξεταστική Επιτροπή**

| (υπογραφή) | (υπογραφή) | (υπογραφή) |
|---|---|---|
| ΜΑΡΙΑ ΒΙΡΒΟΥ<br>Καθηγήτρια | ΔΕΣΠΟΙΝΑ ΠΟΛΕΜΗ<br>Επίκουρος Καθηγήτρια | ΑΡΙΣΤΕΑ ΣΙΝΑΝΙΩΤΗ<br>Τακτική καθηγήτρια |

Περιεχόμενα

## Περίληψη

Με αφορμή την ραγδαία αύξηση μιας νέας μορφής εγκληματικότητας ,της ηλεκτρονικής, επιτεύχθηκε η συγγραφή αυτής της εργασίας. Κατά την συγγραφή της καταβάλλεται προσπάθεια να γίνει μια προσέγγιση και ανάλυση της ειδικότερης αυτής έννοιας .

Συγκεκριμένα, κατά κύριο λόγο, η εργασία ξεκινά με μια ιστορική αναδρομή για το έγκλημα και τις βασικές διαφορές του με το ηλεκτρονικό .Έπειτα, ορίζεται ο νέος αυτός όρος αλλά και αναφέρονται μορφές στις οποίες αυτός παρουσιάζεται , το προφίλ του ηλεκτρονικού εγκληματία καθώς και τα μέσα τέλεσης του εγκλήματος. Ακολούθως, αναλύονται τα εγκλήματα που τελούνται με τη χρήση ηλεκτρονικού υπολογιστή καθώς και διάφορες σχετικές έρευνες που έχουν πραγματοποιηθεί. Στη συνέχεια, καταγράφεται το νομοθετικό πλαίσιο που ισχύει για το ηλεκτρονικό έγκλημα ,τόσο σε τοπικό, σε ευρωπαϊκό ,όσο και σε παγκόσμιο επίπεδο. Επιπροσθέτως, γίνεται λόγος για θέματα ασφάλειας στη χρήση του ηλεκτρονικού υπολογιστή αλλά και αναγράφονται σημαντικές υποθέσεις αναλόγων εγκλημάτων. Τέλος, παρουσιάζεται ένα παράδειγμα ηλεκτρονικού εγκλήματος μέσω της χρήσης κώδικα.



## Abstract

The current master thesis handles the theme of electronic crime having as motive the rapid increase of this new form of crime. During its writing we make an attempt to approach and analyze this concept more specifically.

Firstly, the work begins with a historical view of the crime as topic and the basic differences between the classical and electronic one. The work continues with the addressing of that new concept and we also refer to the forms through which it is presented ,the profile of the e-criminal as well as the means of the performance of the crime. Moreover, we analyze the crimes which are done with the usage of the computer as well as various surveys about this subject. Furthermore, the laws concerning e-crime are referred locally and also at both a European and an international sphere. In addition, topics about security at the usage of the computer are written and very significant cases of such cimes. Finally, an example of e-crime is presented through a code.

Ευχαριστίες

Ευχαριστώ θερμά την καθηγήτριά μου ,κυρία Σινανιώτη καθώς και την βοηθό της ,Μαρία, για την καθοδήγησή τους σχετικά με το θέμα της εργασίας μου και την σωστή διεκπεραίωση της. Επιπροσθέτως ευχαριστώ τους καθηγητές του μεταπτυχιακού προγράμματος για τις γενικότερες γνώσεις που μου προσέφεραν στον τομέα της Πληροφορικής. Τέλος, ευχαριστώ ιδιαίτερα τον σύζυγό μου ,τον γιο μου και την οικογένειά μου για την πολύτιμη στήριξη και συμπαράστασή τους κατά την διάρκεια της ολοκλήρωσης της εργασίας μου.

# 1. Εισαγωγή

Η ραγδαία εξέλιξη της τεχνολογίας, η σταδιακή ανάπτυξη της πληροφορικής και η ευρύτατη χρήση του Διαδικτύου έχουν προκαλέσει επαναστατικές αλλαγές στο σύνολο των καθημερινών δραστηριοτήτων, στην παραγωγική διαδικασία, στις συναλλαγές, στην εκπαίδευση, στη διασκέδαση, ακόμα και στον τρόπο σκέψεως του σύγχρονου ανθρώπου. Μαζί με αυτές τις αλλαγές, οι οποίες κατά κανόνα βελτιώνουν την ποιότητα της ζωής μας, υπεισέρχονται και οι παράμετροι που ευνοούν την ανάπτυξη νέων μορφών εγκληματικότητας. Οι νέες αυτές μορφές εγκληματικότητας θεσμοθετούνται με τον όρο «Ηλεκτρονικό Έγκλημα».

Η πληροφορική τεχνολογία κατέστησε δυνατή τη διάπραξη ενός ευρέως φάσματος εγκληματικών πράξεων, οι οποίες απαιτούν εξειδίκευση και αυξημένη κατάρτιση. Ως «Ηλεκτρονικό Έγκλημα», λοιπόν, θεωρούνται οι αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία. Ανάλογα με τον τρόπο τέλεσης διαχωρίζονται σε εγκλήματα τελούμενα με τη χρήση Ηλεκτρονικών Υπολογιστών (computer crime) και σε Κυβερνοεγκλήματα (cyber crime), εάν τελέσθηκε μέσω του Διαδικτύου. Το ηλεκτρονικό έγκλημα , αποτελεί ένα φαινόμενο που διαρκώς αναπτύσσεται και εξελίσσεται ,ακολουθώντας τους γρήγορους ρυθμούς ανάπτυξης της τεχνολογίας .Οι ηλεκτρονικοί εγκληματίες χρησιμοποιούν τους ηλεκτρονικούς υπολογιστές ,τα κινητά τηλέφωνα και πολλές ακόμη συσκευές ηλεκτρονικής επεξεργασίας δεδομένων ,για να αποκτήσουν πρόσβαση σε δεδομένα και πληροφορίες ,με σκοπό το οικονομικό ή άλλο όφελος .Οι διωκτικές αρχές καλούνται να ακολουθήσουν τις νέες τεχνολογικές εξελίξεις και να προσαρμόσουν τις παραδοσιακές τεχνικές έρευνας προκειμένου να εντοπίσουν τα ηλεκτρονικά ίχνη των δραστών .

## 1.1 Ιστορική αναδρομή για το έγκλημα

Το έγκλημα αποτελεί αναπόσπαστο κομμάτι οποιασδήποτε οργανωμένης κοινωνίας . Ανεξάρτητα από τον τόπο και το χρόνο ,ορισμένοι άνθρωποι παραβαίνουν τους κοινωνικούς κανόνες ,με αποτέλεσμα να επιβάλλονται σε αυτούς διάφορες κυρώσεις .Το είδος της αντίδρασης της κοινωνίας ,όπως και το είδος της ποινής που θα επιβληθεί σε αυτόν που παρέβη έναν κανόνα, εξαρτώνται από την εποχή και τον πολιτισμό. Τρία είναι τα βασικά στοιχεία που συνθέτουν το εγκληματικό φαινόμενο: α)Ο κανόνας (ποινικός νόμος), που αποτελεί την έκφραση της κοινωνίας έναντι κάποιας συμπεριφοράς .Αν ο κανόνας προβλέπει και την επιβολή ποινών , τότε πρόκειται για ποινικό νόμο .Οι ποινικοί νόμοι δεν είναι σταθεροί ,αλλά αλλάζουν με το πέρασμα του χρόνου. Εξαρτώνται από πολλούς παράγοντες όπως κοινωνικούς ,ηθικούς , πολιτιστικούς ,οικονομικούς . β)η παράβαση(έγκλημα),το ποίο είναι κάτι το αναμενόμενο και φυσικό μέσα σε μια κοινωνία .Θα ήταν αδύνατο όλα τα μέλη μιας κοινωνίας να συμμορφώνονται με τους ίδιους κανόνες, καθώς είναι αδύνατο να έχουν την ίδια δομή προσωπικότητας ,την ίδια κοινωνική και οικονομική κατάσταση και να έχουν κοινωνικοποιηθεί με τον ίδιο τρόπο. Εκτός όμως από αναπόφευκτο ,το έγκλημα στα πλαίσια μιας κοινωνικής οργάνωσης ,όσο και αν έχει ταυτιστεί με κάτι αρνητικό ,είναι και χρήσιμο, είτε έμμεσα είτε άμεσα. Έμμεσα, υπό την έννοια ,ότι αποτελεί προϋπόθεση για κάθε ηθική και νομική αλλαγή ,η οποία είναι απαραίτητη για να μην περιέλθει η κοινωνία σε πλήρη αγκύλωση. Άμεσα ,υπό την έννοια ,ότι αποτελεί την πρόγευση της μέλλουσας ηθικής .Για παράδειγμα ,η ελευθερία σκέψης και έκφρασης που απολαμβάνουμε σήμερα δεν θα είχε επιτευχθεί ποτέ ,αν κάποιοι δεν παραβίαζαν τους κανόνες που κάποτε την περιόριζαν γ)η κύρωση(ποινή),που αποτελεί τη συνέπεια της παράβασης του κανόνα και δηλώνει ότι η συγκεκριμένη συμπεριφορά δεν είναι αποδεκτή από την κοινωνία .Ως προς την αιτιολογία επιβολής της ποινής έχουν κατά καιρούς διατυπωθεί διάφορες θεωρίες. Οι επικρατέστερες είναι της ανταπόδοσης και της κοινωνικής άμυνας. Στην περίπτωση της ανταπόδοσης ,η επιβολή της ποινής σκοπεύει στην επανόρθωση των επιβλαβών για την κοινωνία συνεπειών του εγκλήματος ,με την πληρωμή του κακού που έγινε με άλλο ισάξιο .Στην περίπτωση της άμυνας ,η ποινή έχει ως σκοπό ,να αποτρέψει κάποιον να

εγκληματήσει είτε με τον εκφοβισμό ,είτε με τη γενικότερη καλλιέργεια της ιδέας της αποστροφής προς την αδικία .

## 2. Χαρακτηριστικά του εγκλήματος

Τα κύρια χαρακτηριστικά του εγκλήματος είναι τα ακόλουθα:

Η παγκοσμιότητα: Όσο και αν οι μορφές ,η έκταση και το είδος της αντίδρασης της πολιτείας έναντι συγκεκριμένης συμπεριφοράς ποικίλλουν ανά χώρα ενδεχομένως και ανά συγκεκριμένη γεωγραφική περιοχή , το κοινωνικό αυτό φαινόμενο είναι κοινό παντού. Κοινωνία χωρίς έγκλημα δεν υπάρχει.

Η διαχρονικότητα: Η ιστορική έρευνα έχει αποδείξει ότι το εγκληματικό φαινόμενο υπήρξε σε όλες τις κοινωνίες, χωρίς καμιά εξαίρεση. Μπορεί να υπήρξαν διαφοροποιήσεις ως προς το περιεχόμενο των νόμων και τα επιμέρους χαρακτηριστικά των παραβάσεων και των παραβατών ,όμως πάντοτε υπήρξε παραβίαση κανόνων και επιβολή κυρώσεων .

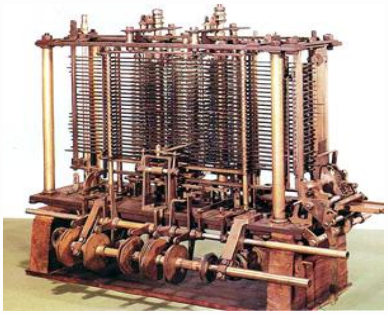
Η αλληλεξάρτηση των στοιχείων του εγκληματικού φαινομένου: Τα τρία βασικά στοιχεία του εγκληματικού φαινομένου , δηλαδή ο κανόνας ,το έγκλημα και η κύρωση αποτελούν έναν κύκλο, ο οποίος δεν μπορεί να διασπαστεί. Κανένα από τα τρία αυτά στοιχεία δεν μπορεί να υπάρξει χωρίς το άλλο .Δεν θα υπήρχε έγκλημα ,αν δεν υπήρχε κανόνας συμπεριφοράς ,για να παραβεί κάποιος .Η κοινωνική αντίδραση θα ήταν ανύπαρκτη χωρίς έγκλημα και εγκληματία.Η δυσχέρεια ορισμού του εγκλήματος: Όπως ήδη προαναφέρθηκε ,το έγκλημα είναι αναπόσπαστο κομμάτι κάθε κοινωνίας παράλληλα όμως χρησιμοποιεί διαφορετικούς κανόνες ανάλογα με το συγκεκριμένο καθεστώς ,πολιτικό, κοινωνικό, ηθικό, που επικρατεί σε κάθε οργανωμένο σύνολο ανθρώπων .Το γεγονός αυτό δυσχεραίνει τον ορισμό και προσδιορισμό του ,καθότι τόσο αυτή η διαφοροποίηση όσο και η συνεχής μετεξέλιξη των κοινωνιών καθιστά πολλές φορές δυσδιάκριτο το τί αποτελεί έγκλημα και τι όχι .

### 2.1 Από το συμβατικό στο ηλεκτρονικό έγκλημα

Το έγκλημα , ως μέρος κάθε κοινωνίας ,έχει την μορφή ενός ζωντανού οργανισμού. Συνεχώς μεταβάλλονται οι μορφές του ,τα μέσα διάπραξής του και η νομοθεσία που το διέπει .
Στις αρχές του 20$^{ου}$ αιώνα ,καινούριοι τρόποι-τεχνικές για τη διάπραξη εγκλημάτων έκαναν την εμφάνισή τους . Η βιομηχανική επανάσταση εκσυγχρόνισε τα μέσα τέλεσης του εγκλήματος .Το τηλέφωνο άρχισε να χρησιμοποιείται για απάτες και άλλα εγκλήματα ,τα μεταφορικά μέσα διευκόλυναν τη διάπραξη κλοπών και ληστειών ,ενώ διάφορα άλλα τεχνολογικά επιτεύγματα με τη χρήση και λειτουργία τους ,επέφεραν μια αρχική διαφοροποίηση στον τρόπο διάπραξης του εγκλήματος .Ίσως τότε κανείς δεν μπορούσε να φανταστεί τι θα επακολουθούσε .Με την εμφάνιση και ανάπτυξη της τεχνολογίας των ηλεκτρονικών υπολογιστών ,συντελούνται αλλαγές στο εγκληματικό φαινόμενο, που ποτέ πριν δεν είχε γνωρίσει η ανθρωπότητα .Οι εγκληματικές απειλές στηρίζονται πλέον σε πιο περίπλοκη τεχνολογία ,καταργώντας τα φυσικά όρια. Βέβαια τόσο το συμβατικό έγκλημα όσο και τα μέσα διάπραξής του συνεχίζουν να υπάρχουν ,όμως εμφανίζονται νέες μορφές με χαρακτηριστικότερη αυτή του ηλεκτρονικού εγκλήματος ,του εγκλήματος δηλαδή που ένας ηλεκτρονικός υπολογιστής ή παρόμοιες συσκευές ηλεκτρονικής επεξεργασίας δεδομένων ,διαδραματίζουν κυρίαρχο ρόλο..Α Αναζητώντας τις ρίζες του ηλεκτρονικού εγκλήματος ,διαπιστώνουμε ότι ταυτόχρονα με την εμφάνιση των υπολογιστών , έγιναν οι πρώτες προσπάθειες από τους επίδοξους <<ηλεκτρονικούς εγκληματίες >> να βρουν τρόπους να εκμεταλλευτούν τις νέες αυτές τεχνολογίες και να προσπορίσουν όφελος για τους εαυτούς τους ή για τρίτους .Η νέα τεχνολογία ,που αναπτύσσονταν με γοργούς ρυθμούς ,έδινε νέες ευκαιρίες για εύκολη διάπραξη πλήθους εγκλημάτων. Ακόμη όμως και τα πρώτα χρόνια έπειτα από την εμφάνιση των υπολογιστών ,το ηλεκτρονικό έγκλημα ήταν σπάνιο, διότι ο αριθμός τους ήταν περιορισμένος .Επιπλέον, οι υπάρχοντες υπολογιστές χρησιμοποιούσαν γλώσσα μηχανής, καθιστώντας αδύνατο για τους επίδοξους εγκληματίες να κατέχουν την

απαραίτητη γνώση ή τον εξοπλισμό. Ο ηλεκτρικός υπολογιστής αποτελούσε είδος πολυτέλειας και κατ' αυτή την έννοια το ηλεκτρονικό έγκλημα ήταν για λίγους .

Το πρώτο καταγεγραμμένο Ηλεκτρονικό Έγκλημα, χρονολογείται το 1820, όταν ο Γάλλος υφαντουργός Joseph-Marie Jacquard κατασκεύασε τον αργαλειό.



Η «συσκευή» αυτή επέτρεπε την επανάληψη μιας σειράς ομοίων βημάτων, κατά την ύφανση συγκεκριμένων υφασμάτων. Το γεγονός αυτό προκάλεσε ανησυχία στους υπαλλήλους του Jacquard, που φοβήθηκαν ότι απειλούνταν η παραδοσιακή τους εργασία. Έτσι προκαλούσαν συχνά δολιοφθορές στο μηχάνημα, για να αποθαρρύνουν τον Jacquard να χρησιμοποιήσει τη νέα τεχνολογία.
Χρονικά, η ανάπτυξη του ηλεκτρονικού εγκλήματος τοποθετείται στην τελευταία δεκαετία του περασμένου αιώνα ,σε μια εποχή που χαρακτηρίστηκε από την αλματώδη εξέλιξη των υπολογιστικών συστημάτων .Σήμερα, το μεγαλύτερο ποσοστό του πληθυσμού στις αναπτυγμένες χώρες ,έχει πρόσβαση σε ένα Η/Υ ,η δε χρήση του έχει απλοποιηθεί τόσο που ακόμη και ένα μικρό παιδί μπορεί να χειρίζεται έναν προσωπικό υπολογιστή με ιδιαίτερη δεξιότητα . Η μεγάλη επανάσταση στον τομέα του ηλεκτρονικού εγκλήματος ,επήλθε μετά την εμφάνιση των δικτύων .Τα δίκτυα ,δημιούργησαν νέες διόδους πρόσβασης προς την πληροφορία ,καθιστώντας μη αναγκαία την παρουσία του επιτιθέμενου στο χώρο όπου αυτή φυλάσσεται .Η τεράστια πληροφοριακή δεξαμενή που δημιουργήθηκε και συνεχίζει να επεκτείνεται ,αποτέλεσμα της διασύνδεσης εκατομμυρίων υπολογιστών ,ανά τον κόσμο, μετέβαλε ριζικά τον τρόπο ζωής του σύγχρονου ανθρώπου .Σήμερα οι υπολογιστές χρησιμοποιούνται σε όλες τις εκφάνσεις της καθημερινής μας δραστηριότητας και στους σκληρούς τους δίσκους αποθηκεύονται πληροφορίες για τα προσωπικά μας στοιχεία, τους προσωπικούς μας λογαριασμούς, τις συνήθειές μας και τις προτιμήσεις μας .
Το νέο περιβάλλον χαρακτηρίζεται από την ευρεία ανάπτυξη του ηλεκτρονικού εμπορίου ,την πραγματοποίηση τραπεζικών και συναλλαγματικών πράξεων μέσω του Διαδικτύου ,την άμεση επικοινωνία σε όλα τα επίπεδα με νέες διόδους (e-mail,chat,newsgroups..)αλλά και την εξ αποστάσεως εκπαίδευση, την πραγματοποίηση συναλλαγών με δημόσιες υπηρεσίες και την τηλεδιάσκεψη .Οι ευκαιρίες για ηλεκτρονική εγκληματικότητα είναι περισσότερες από ποτέ .Το ηλεκτρονικό έγκλημα είναι ευκολότερο ,οι δε δυνατότητες δίωξής του από τις αρμόδιες αρχές είναι περιορισμένες λόγω έλλειψης εμπειρίας στο σχετικό τομέα ,ελλιπούς εκπαίδευσης αλλά και ασαφούς νομοθετικού πλαισίου ,γεγονός που ενθαρρύνει τους επίδοξους εγκληματίες .

## 2.2 Ορισμός του ηλεκτρονικού εγκλήματος

Κατά καιρούς έχουν γίνει πολλές προσπάθειες να ορισθεί το ηλεκτρονικό έγκλημα. Ένας ορισμός που δόθηκε από τους Forester και Morrison (1994) προσδιόρισε το ηλεκτρονικό έγκλημα ως <<μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσής της >>.Ωστόσο το ηλεκτρονικό έγκλημα δεν είναι κάτι τόσο απλό, ούτε μπορούμε να το γενικεύσουμε. Υιοθετώντας μια τριπλή προσέγγιση που τείνει να επικρατήσει σήμερα ,μπορούμε να θεωρήσουμε το ηλεκτρονικό έγκλημα ως μια νέα μορφή

εγκλήματος ,που διαπράττεται με τη χρήση ηλεκτρονικών υπολογιστών ,μια παραλλαγή των ήδη υπαρχόντων εγκλημάτων ,τα οποία διαπράττονται με υπολογιστές και μια εγκληματική πράξη στην εκδήλωση της οποίας συμμετέχει καθ'οποιονδήποτε τρόπο ένας ηλεκτρονικός υπολογιστής .
Στην αγγλική γλώσσα οι όροι που χρησιμοποιούνται για να περιγράψουν το ηλεκτρονικό έγκλημα ποικίλλουν:e-crime ,cybercrime,computer-crime,internet related crime και hitech crime είναι οι συχνότερα χρησιμοποιούμενοι .Οι διαφορές των ανωτέρω όρων είναι ελάχιστες. Μπορούμε να θεωρήσουμε τους όρους :e-crime, computer-crime, hitech-crime ως γενικότερους και τους όρους cybercrime και internet related crime ως ειδικότερους ,καθώς στην δεύτερη περίπτωση περιλαμβάνεται υποχρεωτικά και το στοιχείο του Διαδικτύου .
Αντιστοίχως ,στην ελληνική γλώσσα οι όροι που χρησιμοποιούνται είναι ηλεκτρονικό έγκλημα, δικτυακό έγκλημα και έγκλημα του κυβερνοχώρου .Το στοιχείο της δικτύωσης περιλαμβάνεται στους δύο τελευταίους όρους .Βασικό συστατικό στοιχείο του ηλεκτρονικού εγκλήματος αποτελεί η ύπαρξη μιας συσκευής ηλεκτρονικής επεξεργασίας δεδομένων ,όπως ηλεκτρονικός υπολογιστής ,κινητό τηλέφωνο,palmtop ,notebook.Κυρίαρχο ρόλο διαδραματίζει ο Η/Υ ο οποίος μπορεί αρχικά να αποτελεί τον στόχο κάποιας επίθεσης .Στην περίπτωση αυτή μπορούμε να πούμε ότι ο υπολογιστής είναι το <<θύμα >>της επίθεσης .Έπειτα δύναται να αποτελεί το μέσο διάπραξης κάποιας επίθεσης, δηλαδή το εργαλείο που χρησιμοποιεί ο επιτιθέμενος για να πραγματοποιήσει τον εγκληματικό σκοπό του .Τέλος ο υπολογιστής μπορεί να αποτελεί ένα βοηθητικό μέσο για τη διάπραξη του εγκλήματος ,λόγου χάρη να αποθηκεύονται σ' αυτόν 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 που τον εξετάζουμε .Αν αυτός άπτεται της νομικής επιστήμης, απαιτείται πιο αυστηρός προσδιορισμός των όρων ,για να είναι δυνατή η στοιχειοθέτηση των εγκλημάτων .Η πολυπλοκότητα της μορφής αυτής της εγκληματικότητας ,δυσχεραίνει ακόμη και το νομοθέτη ,ο οποίος αποφεύγει να το ορίσει και είτε αφήνει την αρμοδιότητα αυτή στα δικαστήρια και την παραγόμενη νομολογία ,είτε δανείζεται τους χρησιμοποιούμενους από την τεχνολογία όρους .
Κρίνεται επίσης αναγκαίο να επισημανθεί ότι η εμπλοκή ενός ηλεκτρονικού υπολογιστή ή δικτύου δε σημαίνει αναγκαστικά ότι έχουμε να κάνουμε με ηλεκτρονικό έγκλημα. Για παράδειγμα ,αποτελεί ηλεκτρονικό έγκλημα ο βιασμός μιας γυναίκας από έναν άνδρα, τον οποίο γνώρισε μέσω ενός chat room στο Διαδίκτυο και ο χρόνος και τόπος συνάντησης ,που διαπράχθηκε το έγκλημα καθορίστηκε μέσω e-mail;Σαφώς ,η απάντηση είναι αρνητική. Πρόκειται για ένα συμβατικό έγκλημα,(το βιασμό ),που διαπράχθηκε με τη βοήθεια των δυνατοτήτων επικοινωνίας που προσφέρει το Διαδίκτυο(chat και e-mail).

## 3. Μοντέλο απειλών

### 3.1 Εισαγωγή

Σήμερα οι απειλές έναντι της ασφάλειας των πληροφοριακών συστημάτων είναι περισσότερες από ποτέ. Η εκτεταμένη χρήση των υπολογιστών σε όλες τις εκφάνσεις της ανθρώπινης δραστηριότητας και η συνεχής ανάπτυξη του Διαδικτύου ,έχουν συμβάλει προς την κατεύθυνση αυτή. Ο όρος απειλή ,όταν αναφέρεται 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 εσωτερικές ατέλειες του εξοπλισμού και του λογισμικού .Στις ανθρώπινες απειλές ,οι κακόβουλοι χρήστες ανήκουν στο εσωτερικό του συστήματος ή είναι εξωτερικοί χρήστες. Η επιτυχία των επιθέσεων αυτών εξαρτάται από πολλούς παράγοντες ,όπως η υπολογιστική ισχύς και οι γνώσεις ,οι δε δράστες μπορεί να επιδιώκουν οικονομικό όφελος ,εκδίκηση ή δημοσιότητα. Οι φυσικές απειλές (φωτιά, πλημμύρα) δεν μπορούν να αποτραπούν. Μπορούν όμως να ελαχιστοποιηθούν οι πιθανότητες πρόκλησης σοβαρών ζημιών , με τη λήξη των κατάλληλων προφυλάξεων. Τέλος ,τα προβλήματα στον εξοπλισμό και το λογισμικό ,δημιουργούνται συνήθως από τους ίδιους τους χρήστες των συστημάτων και οφείλονται στην ελλιπή εκπαίδευση .

## 3.1. Βασικές μορφές απειλών

Προσπαθώντας να οριοθετήσουμε το μοντέλο των απειλών έναντι της ασφάλειας ενός συστήματος ,μπορούμε να διακρίνουμε τρεις βασικές κατηγορίες: Τις εξωτερικές, τις εσωτερικές και την Κοινωνική Μηχανή( Social Engineering). Οι εξωτερικές απειλές ίσως είναι η πιο συνηθισμένη μορφή επιθέσεως. Οι επιθέσεις του τύπου αυτού ,προέρχονται από τους hackers και τους crackers, 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 . Οι εσωτερικές απειλές, 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 ασφάλειας του οργανισμού, ιδιαίτερα αν είχαν εργαστεί σε σημαντικές θέσεις (διευθυντικές θέσεις, προσωπικό ασφαλείας ). Εκτός όμως των επιθέσεων από άτομα ,στις εσωτερικές απειλές εντάσσουμε και προβλήματα που οφείλονται στον σχεδιασμό των συστημάτων , στις ευπάθειες λογισμικού και εξοπλισμού ,στις πολιτικές ασφάλειας ,ακόμη και στους ίδιους τους χρήστες, που ενδεχομένως, να υποπέσουν σε λάθη, ικανά να θέσουν σε κίνδυνο την ασφάλεια του συστήματος.
Τέλος , η Κοινωνική Μηχανή ,αποτελεί μια από τις πιο σοβαρές μορφές επιθέσεως .Ο επιτιθέμενος εκμεταλλεύεται τον ανθρώπινο παράγοντα(αφέλεια ,ευπιστία) ώστε να αποκτήσει πρόσβαση σε πληροφορίες που θα τον βοηθήσουν να εξαπολύσει μια επίθεση. Οι επιθέσεις Κοινωνικής Μηχανής προέρχονται είτε από το εσωτερικό είτε από το εξωτερικό περιβάλλον ενός οργανισμού ,ωστόσο τις εντάσσουμε σε χωριστή κατηγορία ,διότι ο επιτιθέμενος χρησιμοποιεί ιδιαίτερες τεχνικές και μεθόδους για να παρακάμψει την ασφάλεια του συστήματος-στόχου .

## 3.2. Εξωτερικές απειλές

### 3.2.1. Hackers

Στην σύγχρονη τεχνολογία των ηλεκτρονικών υπολογιστών ,ο όρος hacker έχει εισβάλει για τα καλά στη ζωή μας .Αντίστοιχο συνώνυμο δεν υπάρχει στην Ελληνική γλώσσα .Και στην αγγλική όμως γλώσσα , η προέλευση του όρου δεν είναι απόλυτα καθορισμένη. Μάλιστα υπάρχει η διχογνωμία για το τι σημαίνει hacker.Αρχικά ,χρησιμοποιήθηκε από το Ίδρυμα Τεχνολογίας MIT(Massachusetts Institute of Technology) για να δηλώσει γενικώς την ενδελεχή ασχολία με τον υπολογιστή .Ετυμολογικά, προέρχεται από τον όρο <<hack writer>> που σε ελεύθερη μετάφραση υποδηλώνει αυτόν που ελέγχει πάρα πολύ καλά το κείμενό του πριν το ολοκληρώσει (Barlow ,1990).Στην δεκαετία του ’60 και ’70 , ο όρος χρησιμοποιούνταν για τους τελειομανείς των υπολογιστών αλλά και για τον καθένα που επιτελούσε οποιαδήποτε δραστηριότητα που σχετίζονταν με πολύπλοκα συστήματα .Οι hackers προέρχονται από τους phreakers , που αποτελούν τους πρώτους ηλεκτρονικούς εγκληματίες .Εμφανίστηκαν πολύ πριν την εφεύρεση των ηλεκτρονικών υπολογιστών και κατάφεραν να εκμεταλλευτούν τα τηλεφωνικά δίκτυα , που μόλις τότε άρχιζαν να αναπτύσσονται ,για να πραγματοποιούν υπεραστικές τηλεφωνικές κλήσεις χωρίς χρέωση .Οι hackers ,αποτελούν άτομα με εξαιρετική γνώση της τεχνολογίας των ηλεκτρονικών υπολογιστών, που κατάφεραν 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 .

### 3.2.2. Το προφίλ του ηλεκτρονικού εγκληματία

Σε γενικές γραμμές ,μπορούμε να διακρίνουμε τις ακόλουθες κατηγορίες[1] .Αρχικά υπάρχουν οι amateurs(ερασιτέχνες).Πρόκειται για ανθρώπους χωρίς δεξιότητες στους υπολογιστές που προσπαθούν να εντοπίσουν μια ευπάθεια σε ένα υπολογιστικό σύστημα και στη συνέχεια να την εκμεταλλευτούν. Τα κίνητρά τους είναι η περιέργεια και η απόκτηση γνώσης ,χωρίς όμως να αποκλείεται και το γεγονός να αποσκοπούν σε οποιοδήποτε είδους όφελος(υλικό και μη). Χρησιμοποιούν σχεδόν πάντα έτοιμα εργαλεία ,καθότι στη συντριπτική πλειοψηφία των περιπτώσεων δεν κατέχουν τις απαραίτητες γνώσεις για να τα κατασκευάσουν . Είναι συνήθως εσωτερικοί εχθροί και ευθύνονται για το μεγαλύτερο ποσοστό των επιθέσεων .Έπειτα υπάρχουν οι hackers ,οι οποίοι είναι άριστοι γνώστες προγραμματισμού ,δικτύων Η/Υ και Internet.Τα εργαλεία που χρησιμοποιούν τα αναπτύσσουν οι ίδιοι .Σκοπός των επιθέσεών τους είναι η ικανοποίηση της περιέργειάς τους και η επιβεβαίωση της ικανότητάς τους για εισβολή σ' ένα σύστημα. Στη συνέχεια, έχουμε τους crackers ,οι οποίοι προέρχονται από τους hackers .Έχουν ως σκοπό την πρόκληση ζημιάς ή την αποκόμιση οφέλους από τα συστήματα στα οποία επιτίθενται .Οι δημιουργοί ιών και γενικότερα κακόβουλου λογισμικού μπορούν να θεωρηθούν ως crackers .Τέλος ,υπάρχουν οι επαγγελματίες εισβολείς(career criminals) ,οι οποίοι έχουν το επίπεδο γνώσεων των hackers .Οι επιθέσεις τους σχετίζονται με τα σοβαρότερα προβλήματα του κυβερνοχώρου ,όπως η βιομηχανική κατασκοπία .Κερδίζουν μέρος ή το σύνολο του εισοδήματος τους από επιθέσεις .

## 3.3. Εσωτερικές απειλές

### 3.3.1. Υπάλληλοι

Οι εσωτερικές απειλές ,συχνά είναι ο μεγαλύτερος κίνδυνος που καλείται να αντιμετωπίσει ένας οργανισμός .Διάφορες έρευνες εγκληματικότητας στο Διαδίκτυο έχουν καταδείξει ότι το 75% των επιθέσεων πραγματοποιείται από υπαλλήλους εταιρειών και μάλιστα διευθυντικών θέσεων .Τα κίνητρα των επιθέσεων ποικίλλουν .Μπορεί ο υπάλληλος να διαπράξει ένα ηλεκτρονικό έγκλημα για να προσπορίσει οικονομικό ή άλλο όφελος, για να βλάψει κάποιο συνεργάτη του ,ή ακόμα και για να εκδικηθεί κάποιο πρόσωπο ή την εταιρεία (απόλυση εργαζομένων) .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 ιδιαίτερα εύκολη ,και τον εντοπισμό της εξαιρετικά δυσχερή .

[1] Anderson 2001 ,Μάγκος 2004

### 3.3.2. Λάθη στο σχεδιασμό των συστημάτων – Ευπάθειες

Ένα σύστημα ,όσο καλά και αν έχει δοκιμαστεί ,πάντα θα έχει κάποια αδύνατα σημεία: τις ευπάθειες. 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 ασφαλείας που ακολουθούνται , που μπορεί κάποιος να εκμεταλλευτεί προκειμένου να παραβιάσει τη διαθεσιμότητα, ακεραιότητα ή εμπιστευτικότητα του εν λόγω συστήματος[2]>> .Τις πιο σημαντικές ευπάθειες τις συναντάμε στο λογισμικό , τόσο διότι ο σχεδιασμός του είναι πολύ πιο δύσκολος από το υλικό ,όσο και διότι ο σχεδιασμός ασφαλούς λογισμικού είναι ομολογουμένως μια διαδικασία δύσκολη ,σε σχέση με τη δημιουργία ασφαλούς υλικού. Σ' ένα σύστημα υπολογιστών ,το λειτουργικό σύστημα είναι το σημαντικότερο κομμάτι λογισμικού .Η ασφάλεια του λειτουργικού συστήματος αποτελεί κεφαλαιώδες ζήτημα για κάθε χρήστη που θέλει να προστατεύσει τα δεδομένα του, καθότι ,οι ευπάθειες του λειτουργικού συστήματος μπορούν να επηρεάσουν τις πληροφορίες ,τα δεδομένα καθώς και άλλες εφαρμογές λογισμικού που είναι εγκατεστημένες σε έναν υπολογιστή .Η US-CERT στην ετήσια έκθεσή της σχετικά με τις ευπάθειες των λειτουργικών συστημάτων[3], αναφέρει ότι για 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 τόσο από το λανθασμένο αρχικό σχεδιασμό τους όσο και από την ελλιπή συντήρηση και διαχείριση ,για την οποία ευθύνεται ο διαχειριστής του συστήματος .Κατά κύριο λόγο ,μια ευπάθεια γίνεται γνωστή και λαμβάνονται τα κατάλληλα μέτρα ,αφού κάποιος επιτιθέμενος έχει επιτύχει να την εκμεταλλευτεί ,ή κατόπιν ενδελεχούς μελέτης της ασφάλειας των συστημάτων Η/Υ και δικτύων του οργανισμού ,σύμφωνα με την πολιτική ασφάλειας που υλοποιείται .Ένας ορθολογικός σχεδιασμός ασφάλειας ενός συστήματος ,περιλαμβάνει κατ' ελάχιστον την δυνατότητα κρυπτογράφησης των δεδομένων, καθώς και ασφαλείς τεχνικές ελέγχου πρόσβασης και αυθεντικοποίησης ( επιλογή κάποιων συνθηματικών ,χρήση εναλλακτικών μεθόδων ταυτοποίησης, όπως η βιομετρία και οι έξυπνες κάρτες) .Όσο αφορά τα δίκτυα και τα υπολογιστικά συστήματα ,λάθη σχεδιασμού μπορούν να εντοπιστούν στην λειτουργία των firerwalls[4] (υλικό και λογισμικό ), στα συστήματα ελέγχου και καταγραφής συμβάντων καθώς και στο λογισμικό προστασίας από ιούς(antivirus).

### 3.3.3. Χρήστες Συστημάτων

Στους σημαντικότερους κινδύνους για την ασφάλεια των συστημάτων ,εντάσσουμε τους ίδιους τους χρήστες του συστήματος .Τα λάθη των χρηστών ,μπορεί να οδηγήσουν σε ολέθριες συνέπειες για ένα σύστημα είτε άμεσα είτε έμμεσα .Άμεσα ,υπό την έννοια ,ότι ένας χρήστης μπορεί για παράδειγμα να ανοίξει ένα συνημμένο αρχείο από ένα άγνωστο e-mail , το οποίο να εμπεριέχει κακόβουλο λογισμικό που μπορεί να προκαλέσει ζημιές στο σύστημα .Έμμεσα ,υπό την έννοια ,για παράδειγμα της πλημμελούς φύλαξης των κωδικών πρόσβασης που του έχουν δοθεί ,με αποτέλεσμα να διαρρεύσουν σε άτομα που δεν έχουν δικαίωμα πρόσβασης .Όλες οι απειλές σχετίζονται με την πολιτική ασφαλείας που εφαρμόζει ένας οργανισμός .Μια σωστά σχεδιασμένη και άρτια εφαρμόσιμη πολιτική ασφαλείας ,μειώνει κατά πολύ τους κινδύνους (είτε εσωτερικούς είτε εξωτερικούς) .

[2] Κανονισμός ΑΔΑΕ από ΦΕΚ Β' 88/26-1-2005, Αριθμ.633α .
[3] http://www.us-cert.gov/cas/bulletins/SB2005.html#Multiple
[4] http://www.cs.purdue.edu/homes/fahmy/papers/firewall-analysis.pdf

### 3.4 Κοινωνική Μηχανή

Η Κοινωνική Μηχανή αποτελεί την πλέον σοβαρή μορφή επιθέσεως και όσοι γνωρίζουν καλά την τεχνική αυτή ,σπάνια αποτυγχάνουν στις επιθέσεις τους .Οι κοινωνικοί μηχανικοί έχουν ξεπεράσει την ανάγκη χρήσης λιγότερο ή περισσότερο πολύπλοκων προγραμμάτων Η/Υ για να επιτύχουν το σκοπό τους .Βασίζονται σε κάτι πολύ απλό , δηλαδή στην 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 τον φόβο προς τους ανώτερούς του[5] .Σύμφωνα με την Κοινωνική Μηχανή ,το αδύνατο σημείο ενός συστήματος ασφαλείας ,είναι ο ανθρώπινος παράγοντας .Ένας επιδέξιος κοινωνικός μηχανικός ,θα προσπαθήσει να εκμεταλλευτεί την αδυναμία αυτή ,πριν σπαταλήσει χρόνο και προσπάθεια σε άλλους μεθόδους ,για παράδειγμα τη δημιουργία λογισμικού για την υποκλοπή των κωδικών πρόσβασης ενός συστήματος .

### 3.5 Μορφές επιθέσεων

#### 3.5.1 Τεχνικές επιθέσεις(Technical Attacks)

Στις επιθέσεις αυτές, δεν υπάρχει προσωπική επαφή του επιτιθέμενου με το θύμα. Ο επιτιθέμενος χρησιμοποιεί μηνύματα ηλεκτρονικού ταχυδρομείου, αναδυόμενα παράθυρα, δικτυακούς τόπους με παραπλανητικό περιεχόμενο και άλλα τεχνικά μέσα , με τα οποία προσπαθεί να πείσει το θύμα ότι είναι τεχνικός ή διαχειριστής δικτύου. Χρησιμοποιώντας την ιδιότητα αυτή επιχειρεί να αποσπάσει ευαίσθητες πληροφορίες που αφορούν λογαριασμούς χρηστών, όπως για παράδειγμα κωδικούς πρόσβασης. Στην κατηγορία αυτή εντάσσονται οι επιθέσεις phising.

#### 3.5.1.Εξατομικευμένες επιθέσεις (Ego-Attacks)

Στις περιπτώσεις αυτές ,ο επιτιθέμενος εκμεταλλεύεται τον εγωισμό ή την ματαιοδοξία του θύματος. Απευθύνεται σε υπαλλήλους που θεωρούν τους εαυτούς τους αδικημένους από την θέση στην οποία εργάζονται και έχουν την τάση να προσπαθούν να αποδείξουν στους προϊσταμένους τους ότι αξίζουν καλύτερη μεταχείριση. Εμφανίζεται ως κάποιο πρόσωπο με εξουσία ,με αποτέλεσμα ο υπάλληλος ,θεωρώντας ότι κάνει <<επίδειξη γνώσεων>> ,να δίνει πολύ εύκολα ευαίσθητες πληροφορίες .

[5] Mitnic,2002

3.5.2.Επιθέσεις Συμπάθειας (Sympathy Attacks)

Ο επιτιθέμενος συστήνεται ως συνάδελφος, προμηθευτής ή ανάδοχος έργου και ισχυρίζεται ότι πρέπει άμεσα να ολοκληρώσει κάποια επείγουσα εργασία ή να έχει πρόσβαση σε σημαντικές πληροφορίες. Ζητά από τον υπάλληλο να του προσφέρει βοήθεια, αφήνοντας να εννοηθεί ότι σε αντίθετη περίπτωση κινδυνεύει να χάσει τη δουλειά του. Η επιτυχία της επίθεσης εξαρτάται από το πόσο ο επιτιθέμενος θα κερδίσει τη συμπάθεια του θύματος. Συχνά απευθύνεται σε πολλούς υπαλλήλους, ώστε να βρεθεί ο κατάλληλος που θα τον βοηθήσει να επιτύχει το σκοπό του .

3.5.4 Επιθέσεις εκφοβισμού (Intimidation Attacks)

Ο επιτιθέμενος εμφανίζεται ως άτομα που κατέχει σημαντική εξουσία όπως διευθύνων σύμβουλος ή αξιωματικός της αστυνομίας και χρησιμοποιώντας την υποτιθέμενη εξουσία του, προσπαθεί να εξαναγκάσει το θύμα να συνεργαστεί μαζί του. Εάν το θύμα δεν ενδώσει στις πιέσεις ,το απειλεί ότι κινδυνεύει να χάσει τη δουλειά του ή ότι θα υπάρξουν νομικές συνέπειες εναντίον του, εφόσον δε συνεργαστεί. Οι προαναφερόμενες επιθέσεις, αποτελούν μια γενική προσέγγιση των τεχνικών[6] που χρησιμοποιούν συχνότερα ,οι κοινωνικοί μηχανικοί. Η επιτυχία των επιθέσεων κοινωνικής μηχανής, οφείλεται, πρωταρχικά, στο γεγονός ότι είναι μη προβλέψιμες. Έχουν περισσότερο ανθρωποκεντρικό χαρακτήρα, αφού η προσωπικότητα του επιτιθέμενου και του θύματος διαδραματίζουν τον σημαντικότερο ρόλο. Τα θύματα λόγω φόρτου εργασίας αλλά και εφησυχασμού, δεν αντιλαμβάνονται ότι πέφτουν θύματα τέτοιων επιθέσεων.

3.6.Τα μέσα τέλεσης του ηλεκτρονικού εγκλήματος

Για να αποκτήσουν πρόσβαση σε ένα δίκτυο ή υπολογιστικό σύστημα, οι hackers χρησιμοποιούν εργαλεία που εκμεταλλεύονται τις αδυναμίες των συστημάτων. Τα εργαλεία αυτά, έχουν δημιουργηθεί, για να χρησιμοποιούνται από τους διαχειριστές δικτύων, προκειμένου να ελέγχουν την ευπάθεια των συστημάτων. Οι hackers όμως, τα χρησιμοποιούν για το 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 .

3.6.1 Port Scanners

Έχουν τη δυνατότητα να ελέγχουν πολλές IP διευθύνσεις και να δίνουν στο χρήστη πληροφορίες για τις διαθέσιμες θύρες (ports), τα υπάρχοντα λειτουργικά συστήματα, εφαρμογές που εκτελούνται και άλλες σημαντικές πληροφορίες για το σύστημα[7].

3.6.2 Vulnerability Scanners

Τα εργαλεία αυτά, ελέγχουν το λογισμικό εφαρμογών ενός Η/Υ, προσπαθώντας να εντοπίσουν κάποια ευπάθεια. Συνήθως, χρησιμοποιούνται από τους διαχειριστές για να εντοπίσουν και επιδιορθώσουν τις ευπάθειες των συστημάτων. Οι επιτιθέμενοι τα χρησιμοποιούν για τον αντίθετο, ακριβώς, σκοπό[8].

3.6.3 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

[6] Kevin Mitnic,''The art of Deception'',2001
[7] http://netsecurity.about.com/cs/hackertools/a/aa121303.htm
[8] http://netsecurity.about.com/cs/hackertools/a/aa030404.htm

ότι απέκτησαν πρόσβαση σε ένα σύστημα ή δίκτυο. Τα εργαλεία αυτά[9] ,επιτελούν μια σειρά από διαδικασίες στο σύστημα στο οποίο επιτέθηκαν, όπως τροποποίηση των αρχείων καταγραφής και των εργαλείων του συστήματος, δημιουργία κρυφών σημείων πρόσβασης στο σύστημα και χρησιμοποίηση του συστήματος ως το αρχικό σημείο εξαπόλυσης επιθέσεως σε άλλα συστήματα .

3.6.4 Sniffers

Τα προγράμματα αυτά χρησιμοποιούνται για να αναγνώσουν τις πληροφορίες, που αφορούν την κίνηση σ' ένα τοπικό δίκτυο υπολογιστών. Πραγματοποιώντας το κατάλληλο φιλτράρισμα στα δεδομένα που συλλέγουν, έχουν τη δυνατότητα να ανακτούν ευαίσθητες πληροφορίες όπως ονόματα χρηστών, κωδικούς πρόσβασης και δεδομένα συναλλαγών, που διακινούνται σε ένα δίκτυο μέσω των πρωτοκόλλων επικοινωνίας TCP/IP. Οι επιθέσεις τύπου sniffing είναι ιδιαιτέρως αποτελεσματικές όταν δε γίνεται κρυπτογράφηση των δεδομένων που διακινούνται σε ένα δίκτυο[10] .

Anonymous re- mailers

Ένας ανώνυμος re- mailer είναι ένα πρόγραμμα, το οποίο εκτελείται σε κάποιον υπολογιστή στο Διαδίκτυο και επιτρέπει στον οποιοδήποτε, να στείλει μηνύματα σε ομάδες συζητήσεων ή σε μεμονωμένα άτομα, χωρίς να γίνει γνωστή η ταυτότητά του. Όταν ένα μήνυμα στέλνεται σε μια τέτοια διεύθυνση, το πρόγραμμα αφαιρεί το όνομα και την διεύθυνση του αποστολέα και το προωθεί στον προορισμό του. Μάλιστα, πολλές φορές, τα μηνύματα αυτά διέρχονται από διαδοχικούς re- mailers, με αποτέλεσμα να καθίσταται δύσκολη η παρακολούθηση ή ο εντοπισμός τους. Γεγονός είναι ότι πολλά εγκλήματα τελούνται με τη χρήση e-mail. Η χρησιμοποίηση των ανώνυμων re-mailers, δυσχεραίνει το έργο των διωκτικών αρχών, καθώς η εύρεση των ηλεκτρονικών ιχνών των δραστών και η αποκάλυψη της ταυτότητάς τους είναι εξαιρετικά δύσκολη .

Password Crackers

Οι password crackers είναι εργαλεία λογισμικού, τα οποία χρησιμοποιούνται για να ανακτήσουν τους κωδικούς πρόσβασης ενός συστήματος. Για το σκοπό αυτό οι password crackers κάνουν χρήση ενός αρχείου με πιθανούς κωδικούς, που συχνά αναφέρεται και ως <<λεξικό>> , ενώ η σχετική επίθεση ως <<επίθεση λεξικού>>. Οι επιθέσεις αυτές εκμεταλλεύονται τρεις βασικές ευπάθειες των συστημάτων ελέγχου πρόσβασης με κωδικούς. Πρώτον, το μήκος των κωδικών είναι μικρό με αποτέλεσμα ένα πρόγραμμα να είναι εύκολο να δοκιμάσει όλους τους κωδικούς μήκους 8 χαρακτήρων που επιλέγονται από τους 96, διαθέσιμους χαρακτήρες του πληκτρολογίου. Δεύτερον, οι χρήστες συχνά επιλέγουν εύκολους κωδικούς, όπως ημερομηνίες γέννησης, ονόματα ή τοπωνύμια κάτι που καθιστά το έργο των crackers ακόμη πιο εύκολο. Και τρίτον, τα αρχεία με τους κωδικούς των χρηστών δεν προστατεύονται σωστά, με αποτέλεσμα, να είναι συχνά εύκολη η υποκλοπή τους από τον διακομιστή όπου έχουν αποθηκευτεί[11].

Spoofers

Πρόκειται για 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 διεύθυνσή τους .

[9] http://rootkit.com
[10] http://rootshell.be/~dhar/downloads/Sniffers.pdf
[11] http://www.passwordportal.net

## 4.Μορφές ηλεκτρονικού εγκλήματος

### 4.1 Εισαγωγή

Το ηλεκτρονικό έγκλημα, σήμερα, έχει εισχωρήσει στη δομή και οργάνωση των ανεπτυγμένων κοινωνιών. Νέες μορφές εμφανίζονται και οι υπάρχουσες αναπτύσσονται με γοργούς ρυθμούς. Το ηλεκτρονικό έγκλημα περιλαμβάνει εγκλήματα, που τελούνται με οποιαδήποτε συσκευή ηλεκτρονικής επεξεργασίας δεδομένων. Πολλά από τα εγκλήματα του κοινού Ποινικού Δικαίου, υπήρχαν πολύ πριν την εμφάνιση των συσκευών αυτών, ωστόσο, οι νέες τεχνολογίες και κυρίως οι ηλεκτρονικού υπολογιστές και τα δίκτυα, διεύρυναν σε μεγάλο βαθμό τα μέσα διάπραξής τους. Παράλληλα δημιουργήθηκαν νέες εγκληματικές απειλές. Για την καταγραφή και ανάλυση των βασικότερων μορφών ηλεκτρονικού εγκλήματος διακρίνουμε δύο κατηγορίες. Αρχικά αυτά που δεν υπήρχαν πριν την εμφάνιση των ηλεκτρονικών υπολογιστών και των δικτύων. Τα εγκλήματα αυτά, τα χαρακτηρίζουμε ως <<γνήσια>>. Έπειτα ,έχουμε τα εγκλήματα που υπήρξαν και πριν από την εμφάνιση των ηλεκτρονικών υπολογιστών ή/και δικτύων.

### 4.2 Γνήσια ηλεκτρονικά εγκλήματα

#### 4.2.1 Κακόβουλες εισβολές σε δίκτυα

Η εισβολή σ' ένα δίκτυο υπολογιστών, το λεγόμενο hacking, αποτελεί βασικό στοιχείο πολλών διαδικτυακών εγκλημάτων. Ο hacker, έχει χαρακτηριστεί από πολλούς ως ο εγκληματίας του 21$^{ου}$ αιώνα. Οι τεχνικές που χρησιμοποιούν οι hackers για να διεισδύσουν σ' ένα δίκτυο ηλεκτρονικών υπολογιστών εξελίσσονται ταυτόχρονα με την ανάπτυξη των υπολογιστικών συστημάτων. Οι πιο συχνά χρησιμοποιούμενες είναι κατά πρώτο λόγο η εκμετάλλευση των cookies .Τα cookies, είναι πολύ μικρά αρχεία κειμένου, τα οποία τοποθετούνται στον Η/Υ από διάφορες τοποθεσίες του Διαδικτύου που επισκέπτεται ένας χρήστης. Τα αρχεία αυτά, περιέχουν διάφορες πληροφορίες, όπως τα στοιχεία του χρήστη, οι δραστηριότητές του ή οι συνήθειές του. Όταν πάνω σ' ένα αρχείο cookie εμπεριέχονται πληροφορίες, όπως το όνομα χρήστη και ο κωδικός πρόσβασης για μια υπηρεσία, ο hacker, έχει την δυνατότητα να τις ανακτήσει εκμεταλλευόμενος κάποια γνωστή ευπάθεια του φυλλομετρητή ή του Λειτουργικού Συστήματος. Έπειτα υπάρχει η ανίχνευση δικτυακών υπηρεσιών συστημάτων(probes, scans). Πρόκειται για μια από τις βασικές ενέργειες των hackers, η οποία είναι ο εντοπισμός πληροφοριών για το σύστημα στο οποίο θέλουν να επιτεθούν. Για να πετύχουν το σκοπό τους, χρησιμοποιούν την τεχνική της σάρωσης θυρών. Πρόκειται για μια διαδικασία αποστολής ερωτημάτων σε διακομιστές, με σκοπό, να ληφθούν πληροφορίες για τις υπηρεσίες που προσφέρουν, καθώς και για το χρησιμοποιούμενο επίπεδο ασφαλείας. Οι πληροφορίες αυτές, είναι πολύ σημαντικές, γιατί δίνουν τη δυνατότητα στον επιτιθέμενο να παραβιάσει την ασφάλεια του συστήματος, εκμεταλλευόμενος γνωστές αδυναμίες, λόγου χάριν του λειτουργικού συστήματος ή άλλων υπηρεσιών που προσφέρονται. Η ανίχνευση, επίσης, μπορεί να αποσκοπεί στην εύρεση και αξιοποίηση λογαριασμών χρηστών που δεν προστατεύονται με κωδικό πρόσβασης, για να επιτευχθεί εύκολη πρόσβαση στο σύστημα. Στη συνέχεια, κάνουμε λόγο για τους ανιχνευτές δικτυακών πακέτων(packet sniffers).Η ανίχνευση εδώ πραγματοποιείται με τις εφαρμογές λογισμικού packet sniffers, που έχουν τη δυνατότητα να εντοπίζουν όλα τα πακέτα, που κυκλοφορούν στο Διαδίκτυο. Εφόσον, τα πακέτα δεν είναι κρυπτογραφημένα, είναι δυνατή η απόσπαση πληροφοριών, όπως κωδικοί πρόσβασης ή αριθμοί πιστωτικών καρτών. Επιπλέον, λαμβάνονται πληροφορίες που αφορούν την τοπολογία ενός δικτύου, τις υπηρεσίες που προσφέρονται και τον αριθμό των υπολογιστών, που είναι στο δίκτυο. Όλες οι πληροφορίες, είναι δυνατόν να αποσπασθούν από πακέτα που διακινούνται για την επιτέλεση καθημερινών εργασιών, η δε ανίχνευση τέτοιων επιθέσεων είναι εξαιρετικά

δύσκολη. Έπειτα, γίνεται αναφορά στις πλαστές διευθύνσεις IP(IP Spoofing). Στην δεδομένη περίπτωση οι εισβολείς παρεμβαίνουν στις επικεφαλίδες των πακέτων που διακινούνται σε ένα δίκτυο και τις τροποποιούν ώστε το μήνυμα ν φαίνεται ότι προήλθε από αξιόπιστη πηγή. Με την μέθοδο αυτή, επιτυγχάνουν να χρησιμοποιήσουν μια IP διεύθυνση μέσα στο εύρος των διευθύνσεων που εμπιστευόμαστε και να αποκτήσουν πρόσβαση σε συνδυασμό με άλλες τεχνικές επιθέσεως. Λόγου χάριν, μπορεί να χρησιμοποιηθεί για να αποκρύψει την πραγματική IP διεύθυνση του επιτιθέμενου σε μια επίθεση Ping of Death .Τέλος, παρατηρούνται και οι επιθέσεις σε επίπεδο εφαρμογής, όπου γίνεται εκμετάλλευση γνωστών αδυναμιών των δικτυακών εφαρμογών. Για παράδειγμα, οι φυλλομετρητές όπως ο Internet Explorer, συχνά παρουσιάζουν σημαντικά προβλήματα ασφάλειας. Επιπλέον, οι σύγχρονες γλώσσες προγραμματισμού, όπως java, php, που χρησιμοποιούνται για τη δημιουργία δικτυακών τόπων με δυναμικό περιεχόμενο, εμφανίζουν σημαντικές αδυναμίες ασφάλειας.

### 4.2.2 Επιθέσεις Άρνησης Εξυπηρέτησης

Οι επιθέσεις άρνησης εξυπηρέτησης αποσκοπούν στην εξάντληση των πόρων ενός υπολογιστή, ώστε να μην μπορεί να εξυπηρετήσει άλλους υπολογιστές. Αυτό συχνά 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, καθώς και στην παρεμπόδιση της σύνδεσης μεταξύ δύο σημείων, κάτι που ενδεχομένως σημαίνει αδυναμία πρόσβασης σε συγκεκριμένες υπηρεσίες. Τέλος, οι επιθέσεις έχουν ως στόχο την αλλοίωση της ποιότητας μιας υπηρεσίας, που προσφέρεται σ' έναν χρήστη. Οι επιθέσεις άρνησης εξυπηρέτησης, δεν απαιτούν τη χρήση σύγχρονου υλικού και λογισμικού και ευρυζωνικών συνδέσεων. Ακόμη και ένας παλιός υπολογιστής με μια απλή dial-up σύνδεση, μπορεί να χρησιμοποιηθεί εναντίον μεγάλων συστημάτων υπολογιστών και δικτύων προκαλώντας την πλήρη κατάρρευσή τους. Αυτός ο τύπος επίθεσης χαρακτηρίζεται ως ασύμμετρη επίθεση(asymmetrical attack).

### 4.2.3 Τεχνικές επιθέσεων DOS

Ποικίλες 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[12]. Ενδεικτικά αναφέρουμε τις SYN Flood Attacks, στις οποίες ο επιτιθέμενος εκμεταλλεύεται τα πακέτα SYN και ACK. Όταν ένας Η/Υ (έστω Α)θέλει να συνδεθεί μ' έναν άλλο (έστω Β) του αποστέλλει ένα πακέτο SYN, στο οποίο ο Α απαντάει με ένα πακέτο SYN/ACK(acknowledge). Όταν ο Α λάβει το SYN/ACK, θεωρεί ότι, η σύνδεση έχει ολοκληρωθεί και στέλνει για επιβεβαίωση ένα ακόμη πακέτο ACK. Για να πραγματοποιηθεί η επίθεση, ο επιτιθέμενος στέλνει συνεχώς στο Β πακέτα SYN, αλλά όχι ACK. Ο Β απαντάει στα SYN και περιμένει τα ACK για επιβεβαίωση, τα οποία, όμως, ουδέποτε στέλνονται από το Β. Αποτέλεσμα είναι, η δέσμευση των πόρων του Α, που οδηγεί στην κατάρρευσή του. Κατόπιν, το ping of death, είναι μια δικτυακή εφαρμογή, με την οποία διαπιστώνεται αν μια δεδομένη διεύθυνση IP είναι προσβάσιμη. Ο επιτιθέμενος στέλνει έναν αριθμό πακέτων σε μια διεύθυνση Η/Υ, ο οποίος, απαντάει στέλνοντας παρόμοια μηνύματα (ping). Για να ολοκληρωθεί η επίθεση αρκεί η αποστολή πάρα πολλών μηνυμάτων ping στα οποία ο server είναι αναγκασμένος να απαντήσει δαπανώντας υπολογιστή ισχύ και bandwidth, με αποτέλεσμα οι πόροι του να εξαντλούνται και να μην μπορεί να προσφέρει άλλες υπηρεσίες. Τέλος, υπάρχει το fragmentation.Όταν δύο Η/Υ επικοινωνούν με το πρωτόκολλο TCP/IP, τα πακέτα δεδομένων που αποστέλλονται, περιέχουν μια σειρά από στοιχεία ελέγχου, μέσω των οποίων, ο παραλήπτης ελέγχει, αν έφτασαν σε καλή κατάσταση. Σε αρνητική περίπτωση, ο παραλήπτης

[12] Sinrod, E and Reilly, W.,(2000).Cyber-crimes: A practical approach to the application of Federal Computer Laws. Santa Clara Computer and high technology law journal.16(2)Σελ.14 κ.ε.

επικοινωνεί με τον αποστολέα και του ζητάει να ξαναστείλει τα πακέτα που αλλοιώθηκαν, κατά τη μεταφορά. Εκμεταλλευόμενος αυτό το χαρακτηριστικό, ο επιτιθέμενος στέλνει, συνεχώς, πακέτα με λανθασμένα στοιχεία ελέγχου. Έτσι, υποχρεώνει τον παραλήπτη, να σπαταλά υπολογιστική ισχύ και εύρος ζώνης(bandwidth) ,ζητώντας την επανάληψη της αποστολής τους. Αν η επίθεση συνεχιστεί για μεγάλο χρονικό διάστημα ή αν γίνεται από μια γρήγορη γραμμή, το θύμα θα υποχρεωθεί να αποσυνδεθεί από το δίκτυο.

4.2.4 Κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης

Οι κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης, χρησιμοποιούν ένα συνδιασμό τεχνικών και ολοκληρώνονται σε τέσσερα βήματα. Αρχικά, ο επιτιθέμενος εγκαθιστά προγράμματα απομακρυσμένης διαχείρισης σε ,συνήθως, μεγάλο αριθμό Η/Υ, που διαθέτουν ευρυζωνικές συνδέσεις στο Διαδίκτυο. Το πρόγραμμα απομακρυσμένου ελέγχου, κατόπιν εντολής του επιτιθέμενου (trigger), πραγματοποιεί απόπειρες σύνδεσης προς το θύμα. Στη συνέχεια, όταν ο επιτιθέμενος είναι έτοιμος να αρχίσει την επίθεσή 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[13]>>.Έπειτα, 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. Σε τελική ανάλυση αναφέρεται ότι ,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.

4.2.5 Κακόβουλο λογισμικό

Ένα από τα πιο διαδεδομένα εγκλήματα στο χώρο του Διαδικτύου, είναι η διασπορά κακόβουλου κώδικα (malicious code). Ο κακόβουλος κώδικας είναι κώδικας Η/Υ, που δημιουργείται με σκοπό να προκαλέσει ζημιά σε Η/Υ ή να εισχωρήσει σ' ένα Η/Υ, για την υποκλοπή, αλλοίωση ή διαγραφή δεδομένων και προγραμμάτων. Ο κακόβουλος κώδικας, όταν εισχωρήσει εισχωρήσει σ' ένα Η/Υ, έχει τη δυνατότητα να διαγράψει και να αλλοιώσει δεδομένα ή προγράμματα, να υποκλέψει δεδομένα και να παρεμποδίσει τη λειτουργία ενός συστήματος. Ο Sinrod (2000), διακρίνει τον κακόβουλο κώδικα σε τρεις βασικές κατηγορίες που είναι οι ιοί(viruses),τα σκουλήκια(worms) και τους δούρειους ίππους(Trojan Horses).
Αναλυτικότερα, οι ιοί, είναι το πιο συνηθισμένο είδος κακόβουλου κώδικα. Ένας ιός είναι ένα πρόγραμμα το οποίο επισυνάπτει τον εαυτό του σε αρχεία τα οποία υπάρχουν στον υπολογιστή, μια διαδικασία που είναι γνωστή ως μόλυνση. Μετά την μόλυνση, το αρχείο λειτουργεί κατά διαφορετικό τρόπο. Μπορεί, για παράδειγμα, να εμφανίζει ένα μήνυμα στην οθόνη, να τροποποιεί ή να διαγράφει αρχεία. Τα βασικά χαρακτηριστικά ενός ιού είναι τα ακόλουθα. Αρχικά, αποτελείται από μια σειρά εντολών, που εκτελούν συγκεκριμένες κακόβουλες ενέργειες σε ένα υπολογιστή. Έπειτα, 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 εκτέλεσή του. Κατ' αυτόν τον τρόπο ο εντοπισμός του λογισμικού γίνεται δυσχερής. Η εκτέλεση του ιού έχει δυο βασικές λειτουργίες που είναι η αναπαραγωγή του και η πρόκληση ζημιάς (payload).

[13] Έτσι αναφέρεται ένα σύστημα, το οποίο μέσω της χρήσης κατάλληλων εργαλείων λογισμικού, επιτρέπει στον επιτιθέμενο να το διαχειρίζεται από απόσταση.

Τέλος, προσπαθεί να μολύνει προγράμματα, τα οποία είναι πιθανό να σταλούν ή να μεταφερθούν σε άλλο υπολογιστικό σύστημα.

4.2.5.1.Σκουλήκια ( worms)

Τα σκουλήκια είναι παρόμοια με τους ιούς. Ωστόσο, η βασική διαφορά τους είναι ότι τα σκουλήκια πολλαπλασιάζονται χωρίς να απαιτείται κάποια ενέργεια από το χρήστη. Ένα σκουλήκι, μπορεί να διαδοθεί μέσω του Διαδικτύου, χωρίς να χρειαστεί να επισυναφθεί σε κάποιο αρχείο. 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 υποψηφίων θυμάτων. Το 2001 το σκουλήκι Code II[14] προκάλεσε μια από τις μεγαλύτερες καταστροφές στην ιστορία του Διαδικτύου. Σε χρονικό διάστημα 14 ωρών, προσέβαλε 359.000 συστήματα με ρυθμό 2000 συστήματα ανά λεπτό. Ο μολυσμένος πληθυσμός διπλασιάζονταν κάθε 37 λεπτά. Η συνολική οικονομική ζημιά, πολύ λίγο χρόνο μετά την εμφάνισή του, ξεπέρασε τα δύο δισεκατομμύρια δολάρια, με ρυθμό διακόσια εκατομμύρια δολάρια την ημέρα. Άλλα σύγχρονα σκουλήκια που προκάλεσαν σημαντικές ζημιές είναι τα Slammer, Blaster, So Big ,Beagle, My Doom και Netsky .

4.2.5.2.Δούρειοι Ίπποι

Οι Δούρειοι Ίπποι (Trojan Horses) 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 στον σκληρό δίσκο του υπολογιστή και εκτελούνται, κανονικά, μαζί με τα υπόλοιπα προγράμματα. Πολλές φορές, ο κακόβουλος κώδικας των προγραμμάτων αυτών μπορεί να εμπεριέχεται στα λεγόμενα δημοφιλή προγράμματα. Με την χρήση ενός δούρειου ίππου ο επιτιθέμενος επιτυγχάνει να αποκτήσει απομακρυσμένο έλεγχο του υπολογιστή του θύματος και να συλλέξει κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών ή να εξαπολύσει μια επίθεση άρνησης εξυπηρέτησης. Χαρακτηριστικό παράδειγμα της κατηγορίας αυτής, είναι το πρόγραμμα Back Office που εμφανίστηκε το 2000. Έφτανε στα υποψήφια θύματα με τη μορφή συνημμένου αρχείου σε μήνυμα ηλεκτρονικού ταχυδρομείου, που όταν εκτελούνταν από το θύμα εγκαθιστούσε στον υπολογιστή του ένα πρόγραμμα διακομιστή (server). Στη συνέχεια, ο επιτιθέμενος, εγκαθιστούσε στον δικό του υπολογιστή ένα πρόγραμμα πελάτη (client) και έδινε εντολές στον server του θύματος .Έτσι, εκτός από τον πλήρη έλεγχο του υπολογιστή του θύματος, ήταν ακόμη δυνατό, ο επιτιθέμενος να διαπράξει διαδικτυακά εγκλήματα, τα οποία να φαίνεται ότι τελέστηκαν από τον υπολογιστή του θύματός του.

4.2.5.4.Ad-aware, Spyware και dialers

Τα ad-aware και τα spyware είναι προγράμματα που περιέχουν κακόβουλο κώδικα. Θεωρούνται υποκατηγορία των δούρειων ίππων, ωστόσο τα εξετάζουμε χωριστά λόγω της μεγάλης εξάπλωσής τους. Τα ad-aware 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 εγκατάστασή τους. Σε αντίθετη περίπτωση θεωρούνται κακόβουλο λογισμικό. Σε αντίθεση με τα ad-aware, τα spyware είναι, κατεξοχήν, κακόβουλο λογισμικό που υποκλέπτει πληροφορίες, που αφορούν το χρήστη. Οι πληροφορίες αυτές αφορούν ευαίσθητα δεδομένα, όπως τα προσωπικά στοιχεία του χρήστη, τους κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών, στοιχεία λογαριασμών και συναλλαγών. Για την υποκλοπή των δεδομένων χρησιμοποιούνται διάφορες τεχνικές όπως λόγου χάριν λογισμικό keylogger, το οποίο υποκλέπτει κάθε χαρακτήρα που πληκτρολογεί ο χρήστης. Τα δεδομένα που υποκλάπηκαν είναι δυνατό να σταλούν στον επιτιθέμενο ακόμη και με e-mail.Συνήθως, τα spyware συνεργάζονται με τα ad-aware για τη δημιουργία προφίλ χρηστών, που αποσκοπούν

[14] http://www.cert.org/advisories/CA-2001-19.html

στην αποστολή στοχευόμενων διαφημίσεων, όμως, μπορούν να προκαλέσουν και μια σειρά από άλλα ανεπιθύμητα αποτελέσματα, όπως καταστροφή αρχείων, αποσταθεροποίηση του συστήματος, επιβράδυνση της περιήγησης στο Διαδίκτυο και της εν γένει λειτουργίας του υπολογιστή. Η απεγκατάστασή τους είναι εξαιρετικά δύσκολη. Χαρακτηριστική υποκατηγορία των προγραμμάτων spyware, είναι οι dialers. Οι dialers είναι μικρά προγράμματα(συνήθως μόνο 50 με 60 kb σε μέγεθος), τα οποία έχουν τη δυνατότητα να αποσυνδέουν την υπάρχουσα κλήση της τηλεφωνικής γραμμής με τον τοπικό πάροχο υπηρεσιών Internet (ISP) και να καλούν αυτόματα ένα υψηλής χρέωσης αριθμό (όπως 901 ή αριθμούς εξωτερικού) για πρόσβαση σε συγκεκριμένες υπηρεσίες χωρίς τη συνειδητή συγκατάθεση του χρήστη. Οι dialers προέρχονται από επισκέψεις σε συγκεκριμένες ιστοσελίδες. Αυτές μπορεί να παρέχουν πειρατικό λογισμικό, πορνογραφικό ή άλλο αμφιλεγόμενο περιεχόμενο. Οι ιδιοκτήτες αυτών των ιστοσελίδων έχουν το dialer λογισμικό ενσωματωμένο στον κώδικα του δικτυακού τους τόπου, ώστε να γίνεται αυτόματα λήψη (download) και να εγκαθίσταται στο σύστημα του χρήστη, χωρίς να γίνεται αντιληπτό και χωρίς να ζητείται απαραίτητα η συγκατάθεσή του. Ένας άλλος τρόπος μετάδοσης αυτών των προγραμμάτων, είναι με τη μορφή συνημμένων αρχείων σε μηνύματα ηλεκτρονικής αλληλογραφίας, Το συνημμένο αρχείο φέρει ένα συνηθισμένο όνομα το οποίο παραπλανά το χρήστη όταν όμως εκτελεστεί, εγκαθιστά χωρίς να το γνωρίζει μια εφαρμογή dialer. Αποτέλεσμα της χρήσης των dialers είναι ο πλουτισμός των κατόχων συγκεκριμένων δικτυακών τόπων, από τις υπέρογκες τηλεφωνικές χρεώσεις.

Κυριότερες μορφές ιών

Αρχικά υπάρχουν οι file-infectors ή parasitic viruses.Οι ιοί της μορφής αυτής, ενεργούν μολύνοντας ένα εκτελέσιμο πρόγραμμα, στο οποίο προσθέτουν τον κακόβουλο κώδικα. Παράλληλα γίνεται κάποια τροποποίηση του αρχείου-ξενιστή[15], ώστε να εξασφαλιστεί ότι ο κώδικας του ιού θα εκτελεστεί πρώτος. Αυτού του είδους ο ιός, μολύνει αρχεία με επεκτάσεις .com, .exe, .sys και .olv. Η μετάδοση του ιού γίνεται με οποιοδήποτε φυσικό μέσο αποθήκευσης ή μέσω δικτύου. Τους ιούς της κατηγορίας αυτής μπορούμε περαιτέρω να τους διακρίνουμε σε memory-resident, οι οποίοι παραμένουν στη μνήμη του υπολογιστή και έχουν τη δυνατότητα να μολύνουν οποιοδήποτε πρόγραμμα εκτελέσει ο χρήστης και σε non-resident ή direct-action viruses, οι οποίοι δεν παραμένουν στη μνήμη του υπολογιστή, αλλά προσκολλούνται σε ένα υπάρχον πρόγραμμα και μεταδίδονται όταν ο χρήστης εκτελέσει το πρόγραμμα αυτό. Οι ιοί αυτοί, ήταν πολύ δημοφιλείς την εποχή των λειτουργικών συστημάτων MS-DOS. Στη συνέχεια, υπάρχει ο boot Sector Virus. Ο ιός αυτός <<μολύνει>> εκτελέσιμο κώδικα συστήματος, που εντοπίζει σε συσκευές βοηθητικής μνήμης, στον Τομέα Εκκίνησης (boot Sector) ή στο MBR (Master Boot Record) του δίσκου. Ως αποτέλεσμα, ο ιός φορτώνεται στη μνήμη κατά την εκκίνηση(boot) του συστήματος. Περαιτέρω, ο ιός ενεργεί μολύνοντας κάθε δίσκο ή δισκέτα, που θα χρησιμοποιηθεί τοπικά στον Η/Υ. Κατόπιν είναι οι multi-partite viruses. Αυτοί ενεργούν συνδυάζοντας επιμέρους χαρακτηριστικά των δυο προαναφερθέντων ιών. Έχουν τη δυνατότητα να μολύνουν εκτελέσιμα αρχεία καθώς και τομείς εκκίνησης, με αποτέλεσμα, ένας Η/Υ να είναι δυνατό να μολυνθεί είτε όταν εκκινήσει από μολυσμένο δίσκο είτε όταν εκτελέσει ένα μολυσμένο πρόγραμμα. Ακολούθως, είναι οι companion Viruses. Ο ιός αυτός εκμεταλλεύεται μια ευπάθεια του λειτουργικού συστήματος DOS. Ειδικότερα, αν υπάρχουν δύο προγράμματα με το ίδιο όνομα σε έναν κατάλογο, το DOS εκτελεί πρώτα το αρχείο .com και μετά το .exe. Ο ιός δε μολύνει το αρχείο .exe ,αλλά δημιουργεί ένα αντίγραφο αυτού με την κατάληξη .com. Όταν ο χρήστης επιχειρήσει να εκτελέσει το αρχείο .exe, εκτελείται πρώτα το .com, που έχει αποθηκευτεί στον ίδιο κατάλογο και περιέχει τον κακόβουλο κώδικα. Συχνά, το αρχείο αυτό, μπορεί να είναι <<κρυφό>> και να παραμένει στη μνήμη του Η/Υ(memory-resident). Μεταδίδεται με αποσπώμενα αποθηκευτικά μέσα ή μέσω δικτύου. Επιπλέον, υπάρχουν οι ιοί Link και Flash Bios. Οι ιοί Link δε μολύνουν το πρόγραμμα καθ' αυτό. Λειτουργούν τροποποιώντας το αρχείο

[15] Έτσι ονομάζεται το αρχείο που αρχικά φιλοξενεί τον ιό.

FAT (file allocation table), 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 εκτελείται αυτός, αντί για το πρόγραμμα. Οι ιοί τύπου Flash Bios, προβαίνουν σε αντικατάσταση του λογισμικού BIOS στη μητρική πλακέτα με απρόβλεπτες συνέπειες, όπως η αδυναμία εκκίνησης του Η/Υ. Τέλος, έχουμε και τους macro viruses. Οι μακρο-ιοί είναι μια από τις πλέον γνωστές μορφές ιών. Βρίσκονται κρυμμένοι σε κάποιο αρχείο προγράμματος αυτοματισμού γραφείου (Microsoft Word, Excel) ,το οποίο, όταν το εκτελέσει ο χρήστης ενεργοποιεί μια μακροεντολή, η οποία μπορεί να εκτελέσει μια σειρά από ανεπιθύμητες ενέργειες.

Λογικές και ωρολογιακές βόμβες

Μια λογική βόμβα 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. Η ενεργοποίηση του προγράμματος γίνεται, είτε κατόπιν συγκεκριμένης ενέργειας από το χρήστη, είτε αυτόματα σε συγκεκριμένο χρόνο ή ημερομηνία.

Φάρσες

Μια φάρσα (hoax) είναι μια προειδοποίηση για έναν ιό, που δεν υπάρχει. Στην συνήθη μορφή, είναι μηνύματα ηλεκτρονικού ταχυδρομείου που στέλνονται στο χρήστη και τον προειδοποιούν για κάτι άσχημο, που θα συμβεί στον υπολογιστή του, χωρίς όμως αυτό να ανταποκρίνεται στην πραγματικότητα. Μια πρώτη σκέψη είναι ότι οι φάρσες δε θα έπρεπε να περιληφθούν στο κακόβουλο λογισμικό. Αναλογιζόμενοι όμως, ότι κατά καιρούς, έχουν χρησιμοποιηθεί για διάφορα επιβλαβή αποτελέσματα (κατανάλωση bandwidth, επιθέσεις DOS σε mail server) και έχουν προκαλέσει πανικό στους χρήστες, που οδηγήθηκαν ακόμη και στη διαγραφή χρήσιμων αρχείων από τους υπολογιστές τους, μπορούμε να τις θεωρήσουμε ως μια ιδιαίτερη μορφή λογισμικού, με κακόβουλες προεκτάσεις.

Τεχνικές απόκρυψης ιών

Οι περισσότεροι ιοί, λίγο χρόνο μετά τη δημιουργία τους, εντοπίζονται από τις εταιρείες αντιβιοτικού λογισμικού (antivirus software), οι οποίες ενημερώνουν τις βάσεις τους με το κατάλληλο λογισμικό, για την αντιμετώπισή τους. Ωστόσο, οι τεχνικές που χρησιμοποιούνται για την δημιουργία νέων ιών συνεχώς βελτιώνονται. Οι αόρατοι (stealth) ιοί, έχουν τη δυνατότητα, να παραμένουν ενεργοί στη μνήμη, να μολύνουν τα προγράμματα που εκτελούνται κατόπιν μιας νομικής εντολής του χρήστη και ταυτόχρονα να παρακάμπτουν το πρόγραμμα antivirus, όταν εκτελεί έλεγχο ακεραιότητας. Οι πολυμορφικοί ιοί (polymorphic, self- mutating) δημιουργούν αντίγραφα του εαυτού τους, τα οποία διαφέρουν μεταξύ τους, ωστόσο έχουν τα ίδια καταστροφικά αποτελέσματα. Τα καινούρια αντίγραφα εμπεριέχουν μια μορφή <<θορύβου>> (άσκοπες εντολές ή τροποποίηση της σειράς τους), με αποτέλεσμα τα προγράμματα antivirus να μην μπορούν να τους εντοπίσουν.

Ανεπιθύμητη Αλληλογραφία (Spamming)

Η ανεπιθύμητη αλληλογραφία ή spamming, ορίζεται ως η χρήση οποιουδήποτε ηλεκτρονικού μέσου για την αποστολή ανεπιθύμητων μηνυμάτων σε πολύ μεγάλες ποσότητες. Αν και ο μέσος όρος αναφέρεται, περισσότερο, στην αποστολή μεγάλων ποσοτήτων μηνυμάτων, με διαφημιστικό περιεχόμενο, χρησιμοποιείται, επίσης, για να καταδείξει την αποστολή οποιουδήποτε μηνύματος, το οποίο μπορεί να χαρακτηριστεί ενοχλητικό από αυτόν που το λαμβάνει. Ένα μήνυμα spam, αποστέλλεται με e-mail και περιλαμβάνει πληροφορίες για την προώθηση των προϊόντων μιας εταιρείας. Στην πορεία, πολλές άλλες μορφές και μέσα

διάδοσης ηλεκτρονικής αλληλογραφίας έχουν χρησιμοποιηθεί όπως instant messaging spam, Usenet newsgroup spam, Web search engines spam, web logs spam και mobile phone messaging spam[16]. Η δυνατότητα που προσφέρει το Διαδίκτυο, για φθηνή και άμεση αποστολή εκατομμυρίων μηνυμάτων, ωθεί τις ανά τον κόσμο εταιρείες, στην υιοθέτηση τέτοιων μεθόδων για την προώθηση των προϊόντων τους. Η συλλογή των ηλεκτρονικών διευθύνσεων, μπορεί να πραγματοποιηθεί με διάφορους τρόπους. Οι spammers παίρνουν τις διευθύνσεων από τους καταλόγους εταιρειών, που διατηρούν ηλεκτρονικά καταστήματα ή χρησιμοποιούν λογισμικό τύπου harvester, το οποίο σαρώνει όλο το internet και συλλέγει χιλιάδες διευθύνσεις από καταλόγους ή δωμάτια συζητήσεων newsgroups. Άλλοι, υποκλέπτουν ηλεκτρονικές διευθύνσεις από τους καταλόγους μελών των Εταιρειών Παροχής Internet(ISP). Τέλος, μπορεί να χρησιμοποιηθεί και ειδικό λογισμικό, το οποίο παράγει τεράστιες λίστες τυχαίων διευθύνσεων. Εκτός από διαφημιστικούς σκοπούς, το spamming μπορεί να χρησιμοποιηθεί και ως βασικό εργαλείο για μια σειρά άλλων επιθέσεων όπως τις Επιθέσεις Άρνησης Εξυπηρέτησης. Στις περιπτώσεις αυτές, οι επιτιθέμενοι κατακλύζουν το διακομιστή με πλήθος μηνυμάτων και τον οδηγούν έτσι σε υπερφόρτωση.

Επιθέσεις σε δικτυακούς τόπους

Πρόκειται για ένα είδος επίθεσης, το οποίο παρουσίασε ιδιαίτερη αύξηση τα τελευταία χρόνια. Οι επιθέσεις αυτές, πραγματοποιούνται από τους βάνδαλους (vandals). Τα κίνητρα των επιθέσεων ποικίλουν. Κυρίως, στρέφονται εναντίον κυβερνητικών οργανισμών και υπηρεσιών. Σε μια τυπική 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 από χιουμοριστικό έως προπαγανδιστικό. Όταν ο ιδιοκτήτης του δικτυακού τόπου αντιληφθεί ότι έχει υποστεί μια τέτοια επίθεση, θα διορθώσει τις προβληματικές σελίδες από εφεδρικά αρχεία. Το κρίσιμο ζήτημα τότε είναι ο χρόνος που θα απαιτηθεί για την επιδιόρθωση. Αν οι ζημιές που προκλήθηκαν είναι μεγάλες, ίσως να χρειαστεί ο δικτυακός τόπος να παραμείνει εκτός δικτύου για μεγάλο χρονικό διάστημα. Το πλήγμα που θα δεχθεί η εταιρεία, όταν ο δικτυακός τόπος, που ομολογουμένως αποτελεί την εικόνα της προς εξωτερικούς συνεργάτες και υποψήφιους πελάτες, πέσει θύμα μιας τέτοιας επίθεσης, είναι τεράστιο.

Πειρατεία ονομάτων χώρου

Η πειρατεία ονομάτων χώρου, γνώρισε ιδιαίτερη άνθηση κατά τα πρώτα χρόνια του Διαδικτύου. Διάφοροι επιτήδειοι, εκμεταλλευόμενοι το γεγονός πως μεγάλες εταιρείες δεν είχαν κατοχυρώσει ακόμη ονόματα χώρων για τους δικτυακούς τους τόπους, προέβαιναν σε κατοχύρωση ονομάτων διασήμων εταιρειών, με αποτέλεσμα να αποκτούν τα δικαιώματα της νέας διεύθυνσης. Στη συνέχεια, μπορούσαν να δράσουν με δύο διαφορετικούς τρόπους. Είτε να παραχωρήσουν την διεύθυνση στην εταιρεία που κατέχει το συγκεκριμένο όνομα, έναντι, βέβαια σημαντικού χρηματικού ποσού, είτε να προβούν στην ανάρτηση, στη συγκεκριμένη διεύθυνση, περιεχομένου προσβλητικού (πορνογραφία), γεγονός που επιφέρει σημαντικές συνέπειες στην εταιρεία. Στην πορεία, βέβαια, χρησιμοποιήθηκαν και άλλοι τρόποι για την πειρατεία ονομάτων χώρου. Χαρακτηριστικό παράδειγμα αποτελεί η μεταφορά πάνω από πενήντα διευθύνσεων σε διαφορετική διεύθυνση. Η ενέργεια αυτή πραγματοποιήθηκε από Σέρβους hackers, οι οποίοι απέστειλαν στην εταιρεία κατοχύρωσης ονομάτων χώρου, πλαστά μηνύματα ηλεκτρονικού ταχυδρομείου, με τα οποία πέτυχαν την μεταφορά των διευθύνσεων.

Phising και Pharming

Οι επιθέσεις τύπου phising, έχουν χρησιμοποιηθεί ευρέως από τους hackers τα τελευταία χρόνια. Με τη μορφή αυτού του εγκλήματος, επιχειρείται η απόσπαση προσωπικών

[16] http://www.wikipedia.org/wik/Spam_%28electronic%29#History/

πληροφοριών του θύματος, όπως ο αριθμός της πιστωτικής του κάρτας ή κωδικοί πρόσβασης προκειμένου να χρησιμοποιηθούν σε άλλες παράνομες δραστηριότητες. Κύριο χαρακτηριστικό των επιθέσεων αυτών είναι ότι επιχειρείται η εξαπάτηση του θύματος, η οποία συνήθως συντελείται με την αποστολή ενός e-mail με παραπλανητικό περιεχόμενο. Τρόπος δράσης: Το υποψήφιο θύμα δέχεται ένα e-mail λόγου χάριν από την υπηρεσία Ηλεκτρονικής Τραπεζικής της τράπεζας που χρησιμοποιεί, που τον πληροφορεί ότι είναι σε εξέλιξη κάποιες εργασίες συντήρησης του συστήματος και τον προτρέπει να επισκεφτεί την υπηρεσία Ηλεκτρονικής Τράπεζας 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.

Μελέτη περίπτωσης: Επίθεση phising εναντίον των χρηστών της υπηρεσίας Homebanking της Εθνικής Τράπεζας τον Νοέμβριο 2006.

Πολλοί χρήστες της υπηρεσίας Internet Banking της Εθνικής Τράπεζας έλαβαν ένα e-mail, που τους προέτρεπε να ακολουθήσουν το σύνδεσμο που υπήρχε σε αυτό, προκειμένου να εισέλθουν στο σύστημα On-line Banking και να επιβεβαιώσουν τους κωδικούς τους, αλλιώς ο λογαριασμός θα απενεργοποιούνταν. Ο σύνδεσμος στο μήνυμα, παρέπεμπε σε μια σελίδα σχεδόν όμοια με την πραγματική σελίδα της Εθνικής Τράπεζας. Όποιος χρήστης παρασυρόταν και πληκτρολογούσε τους κωδικούς του, αυτοί αυτόματα υποκλέπτονταν [17]. Οι επιθέσεις αυτές, έχουν πραγματοποιηθεί με διάφορες παραλλαγές, για να παραπλανήσουν τους χρήστες. Για παράδειγμα, μαζί με το e-mail αποστέλλεται και ένας δούρειος ίππος, ο οποίος εκτελείται στο παρασκήνιο και τη στιγμή που το θύμα θα επισκεφθεί ένα δικτυακό τόπο για να δώσει τα στοιχεία του, καταγράφονται αυτόματα και αποστέλλονται στον επιτιθέμενο. Άλλες φορές, ο χρήστης οδηγείται στο πραγματικό δικτυακό τόπο της υπηρεσίας Ηλεκτρονικής Τραπεζικής και εκεί, χωρίς να το αντιληφθεί εμφανίζεται ένα αναδυόμενο (pop- up) παράθυρο, στο οποίο ο χρήστης προτρέπεται να πληκτρολογήσει τα προσωπικά του στοιχεία. Το αναδυόμενο παράθυρο είναι αποτέλεσμα παρέμβασης του επιτιθέμενου, που επιχειρεί με αυτό τον τρόπο να υποκλέψει τα προσωπικά στοιχεία του χρήστη, τη στιγμή που πληκτρολογούνται.
Μια παραλλαγή των επιθέσεων phising αποτελούν οι επιθέσεις pharming. Και στην περίπτωση αυτή, ο σκοπός του εγκλήματος είναι ο ίδιος, δηλαδή η απόσπαση ευαίσθητ ων δεδομένων από το θύμα. Η διαφορά έγκειται στην τεχνική. Ο hacker επεμβαίνει στο Σύστημα Ονομάτων Χώρου (DSN) και όταν ο ανυποψίαστος χρήστης πληκτρολογεί τη διεύθυνση που χρησιμοποιεί, χωρίς να το γνωρίζει μεταφέρεται σε άλλο δικτυακό τόπο, όπου ο κακόβουλος θα επιχειρήσει να αποσπάσει το όνομα χρήστη και τον κωδικό πρόσβασης του θύματος.

Πειρατεία λογισμικού

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. Η ψηφιακή μορφή των εφαρμογών λογισμικού, καθιστά ιδιαίτερα εύκολη την αναπαραγωγή τους σε πολλαπλά αντίγραφα. Πριν την έλευση του Διαδικτύου , οι εφαρμογές λογισμικού διακινούνταν με φυσικό τρόπο. Η εξάπλωση όμως του Διαδικτύου και ιδιαίτερα των ευρυζωνικών συνδέσεων άνοιξε νέους ορίζοντες στην πειρατεία λογισμικού. Πλέον, το λογισμικό μπορεί να διακινηθεί με διάφορες υπηρεσίες που προσφέρει το Διαδίκτυο, όπως ηλεκτρονικό ταχυδρομείο (e-mail), chat, usenet, ftp και ιδιαίτερα με τις εφαρμογές ανταλλαγής αρχείων (pear to pear). Αν και οι

[17] www.e-politismos.gr

εταιρείες παραγωγής λογισμικού εφαρμόζουν στα προϊόντα τους διάφορα τεχνολογικά μέτρα, για να αποτρέψουν την αντιγραφή ή χρήση ους 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 χρησιμοποιούν έτοιμο λογισμικό <<crack>>, που διατίθενται ελεύθερα στο Διαδίκτυο και έχει τη δυνατότητα να απενεργοποιεί τα μέτρα προστασίας των εταιρειών παραγωγής λογισμικού. Σύμφωνα με την ετήσια έρευνα (2005) της εταιρείας λογισμικού Business Software Alliance, τα ποσοστά πειρατείας λογισμικού την τελευταία τριετία παρουσιάζουν τάσεις σταθεροποίησης. Ωστόσο, το σχετικά χαμηλό παγκόσμιο ποσοστό (35%), δεν ανταποκρίνεται σε απόλυτο βαθμό στην πραγματικότητα, καθότι τα χαμηλά ποσοστά που εμφανίζονται στις ΗΠΑ και την Ευρωπαϊκή Ένωση, επηρεάζουν σημαντικά το παγκόσμιο μέσο όρο. Παράλληλα, παρατηρείται μια αύξηση των οικονομικών απωλειών των εταιρειών λογισμικού, δυσανάλογη με τα ποσοστά πειρατείας.

### 4.3 Εγκλήματα που τελούνται με την χρήση Η/Υ

Πολλά από τα υπάρχοντα εγκλήματα του κοινού ποινικού δικαίου τελούνται με τη βοήθεια και χρήση των ηλεκτρονικών υπολογιστών. Ο υπολογιστής μπορεί να χρησιμοποιηθεί, ποικιλοτρόπως, στην τέλεση των εγκλημάτων αυτών όπως αρχικά, για την αποθήκευση δεδομένων, που σχετίζονται με πρόσωπα και αντικείμενα που εμπλέκονται σε μια παράνομη δραστηριότητα, λόγου χάριν προσωπικά στοιχεία εμπόρων ναρκωτικών. Έπειτα, ο Η/Υ δύναται να χρησιμοποιηθεί για την εύρεση πληροφοριών, σχετικών με μια παράνομη δραστηριότητα όπως για παράδειγμα πώς κατασκευάζεται μια βόμβα. Στη συνέχεια, για να διαδίδονται πληροφορίες ,για παράδειγμα, συκοφαντικών έναντι ενός ή περισσοτέρων προσώπων. Ακολούθως, για την τέλεση μέρους της εγκληματικής πράξης, για παράδειγμα, την αγορά αγαθών με χρήση πιστωτικών καρτών που έχουν κλαπεί με φυσικό τρόπο. Τέλος, για τη διακίνηση παράνομου οπτικοακουστικού υλικού, λόγου χάριν, παιδική πορνογραφία . Αναλυτικότερα περιγράφονται ορισμένα από τα εγκλήματα που χρησιμοποιούν τον ηλεκτρονικό υπολογιστή ως βοηθητικό μέσο .

#### 4.3.1 Απάτη στο Διαδίκτυο

Η απάτη στο συμβατικό κόσμο είναι ένα από τα πιο συνηθισμένα εγκλήματα. Η εμφάνιση όμως και ανάπτυξη του Διαδικτύου, μεγιστοποίησε τις δυνατότητες για διάπραξη νέων μορφών απάτης. Η τάση αυτή, αυξήθηκε ακόμα περισσότερο, με την εξάπλωση του ηλεκτρονικού εμπορίου, που είχε ως επακόλουθο την ανάπτυξη οικονομικών συναλλαγών με τη χρήση του Διαδικτύου. Ενδεικτικά αναφέρονται οι κυριότερες μορφές απάτης μέσω του Διαδικτύου.

#### 4.3.2 Απάτη με e-mail

Η απάτη, με τη χρήση του ηλεκτρονικού ταχυδρομείου, αποτελεί την συχνότερη μορφή επιθέσεως, έναντι των χρηστών του Διαδικτύου. Οι επαγγελματίες του είδους βρίσκουν νέους τρόπους για να εξαπατήσουν ανυποψίαστους χρήστες, χρησιμοποιώντας μηνύματα ηλεκτρονικού ταχυδρομείου, που προβάλλουν διάφορες δικαιολογίες, με μοναδικό σκοπό, την απόσπαση χρηματικών ποσών ή προσωπικών στοιχείων. Χαρακτηριστικές περιπτώσεις απάτης με e-mail ,αποτελούν οι νιγηριανές επιστολές και το ισπανικό λόττο. Στην πρώτη περίπτωση, το θύμα λαμβάνει ένα e-mail[18] από φερόμενο υπήκοο Αφρικανικής χώρας, ο οποίος, ζητάει την βοήθειά του για την μεταφορά μεγάλου χρηματικού ποσού από την χώρα του στο εξωτερικό. Ο αποστολέας προβάλλει διάφορες δικαιολογίες (πόλεμος, θάνατος γονέων, φυσικές καταστροφές), και ζητά από το θύμα, το άνοιγμα τραπεζικού λογαριασμού με συνδικαιούχο τον ίδιο, τη γνωστοποίηση των στοιχείων του και την κατάθεση χρηματικού ποσού για έξοδα κίνησης. Σε αντάλλαγμα, προσφέρει μεγάλο μερίδιο του μεταφερόμενου ποσού, όταν ολοκληρωθεί η συναλλαγή. Το θύμα ενδίδει και προχωρά στις ενέργειες που του έχουν υποδειχθεί .Ο δράστης, με διάφορες δικαιολογίες, αποσπά συνεχώς χρηματικά ποσά, μέχρι τη

[18] http://worldwidespam.info/email-scams

στιγμή που αποφασίζει να κλείσει το λογαριασμό, αφού προηγουμένως έχει μεταφέρει όλα τα χρήματα, που υπήρχαν μέχρι τότε, σε δικό του λογαριασμό. Στη δεύτερη περίπτωση, που είναι παρόμοια με τις Νιγηριανές επιστολές, Αφρικανών υπηκόων, κάτοικοι Ισπανίας, αποστέλλουν e-mails σε ανυποψίαστους χρήστες, ζητώντας τους προσωπικά στοιχεία και αριθμούς τραπεζικών λογαριασμών, προκειμένου να τους μεταβιβάσουν τα κέρδη από την υποτιθέμενη νίκη τους στο ισπανικό ΛΟΤΤΟ. Στη συνέχεια, εφόσον τα θύματα έχουν πεισθεί ότι έχουν κερδίσει, ζητούν να τους καταβληθούν χρήματα για διαδικαστικά έξοδα. Έτσι, κατορθώνουν να αποσπούν μεγάλα χρηματικά ποσά[19].

4.3.3 Απάτη με πιστωτικές κάρτες

Η χρήση πιστωτικών καρτών στο Διαδίκτυο, για τη διεκπεραίωση πάσης φύσεως συναλλαγές, έχει δημιουργήσει νέες δυνατότητες για τη διάπραξη εγκλημάτων. Η μη αυτοπρόσωπη παρουσία του αγοραστή και η άγνωστη ταυτότητα του πωλητή (ή υποψήφιου απατεώνα) έχουν συμβάλει στην αύξηση των περιπτώσεων απάτης, με τη χρήση πιστωτικών καρτών στο Διαδίκτυο. Με τη χρήση των σύγχρονων τεχνολογιών δεν απαιτείται πια 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 και εφαρμογές λογισμικού, που δημιουργούν αυτόματα αριθμούς πιστωτικών καρτών, χρησιμοποιώντας διάφορους λογάριθμους.

4.3.4 Κλοπή ταυτότητας

Η κλοπή Ταυτότητας (Identity Theft), είναι ένα από τα πλέον σοβαρά εγκλήματα του Διαδικτύου. Στην ψηφιακή εποχή που διανύουμε, τεράστιες ποσότητες δεδομένων είναι αποθηκευμένες σε ηλεκτρονικές βάσεις δεδομένων για διάφορους σκοπούς (εμπορικούς, ιατρικούς, διαφημιστικούς). Είναι εύκολο για τον καθέναν, να βρει στοιχεία ατόμων και να τα χρησιμοποιήσει για την διεκπεραίωση πάσης φύσεως συναλλαγών. Το έγκλημα της κλοπής ταυτότητας, ολοκληρώνεται σε δυο στάδια (Newman,2004). Στο πρώτο, ο επιτιθέμενος προσπαθεί να αποκτήσει τα στοιχεία της ταυτότητας ενός ατόμου με διάφορους τρόπους, συμβατικούς και ψηφιακούς όπως αφαιρώντας πορτοφόλια από τσάντες, αυτοκίνητα ή ακόμη και από την τσέπη ανυποψίαστων περαστικών. Έπειτα, υποκλέπτοντας την αλληλογραφία, παραβιάζοντας μη ασφαλή κιβώτια αλληλογραφίας, υποβάλλοντας ψευδή αλλαγή διεύθυνσης κατοικίας στο ταχυδρομικό γραφείο των νόμιμων παραληπτών. Ακολούθως, αποσπώντας τα ενημερωτικά σημειώματα των πιστωτικών καρτών, υποδυόμενος τον υπάλληλο ή συγγενικό πρόσωπο του νόμιμου κατόχου. Στη συνέχεια, εισβάλοντας στις βάσεις δεδομένων εταιρειών και οργανισμών, όπου φυλάσσονται προσωπικά δεδομένα. Κατόπιν, χρησιμοποιώντας ειδικό λογισμικό, το οποίο, έχει τη δυνατότητα, να αποσπά προσωπικά δεδομένα και άλλες πληροφορίες, παρακολουθώντας την κίνηση των πακέτων στο Διαδίκτυο. Το επόμενο βήμα είναι η χρησιμοποίηση των κλεμμένων στοιχείων. Αυτή μπορεί να πραγματοποιηθεί αρχικά, ανοίγοντας λογαριασμούς πιστωτικών καρτών με τα στοιχεία του θύματος, τους οποίους και χρησιμοποιεί για την αγορά αγαθών μέσω του Διαδικτύου. Μετά, ανοίγοντας τραπεζικούς λογαριασμούς, τους οποίους, χρεώνει με ακάλυπτες επιταγές. Επίσης, δημιουργώντας πλαστές πιστωτικές κάρτες, άδειες οδήγησης, διαβατήρια και ταυτότητες χρησιμοποιώντας τα στοιχεία του θύματος. Τέλος, υποβάλλοντας ψευδή φορολογικές δηλώσεις για να εισπράξει επιστροφή φόρου.

Ξέπλυμα χρήματος

Με το ξέπλυμα χρήματος (money laundering), επιχειρείται η εξαφάνιση χρήματος που έχει προέλθει από παράνομες δραστηριότητες. Η διαδικασία, που ακολουθείται από τους εγκληματίες για το ξέπλυμα χρήματος, περιλαμβάνει τρία στάδια. Στο πρώτο[20], επιχειρείται η μετατροπή των χρημάτων, που προέρχονται από παράνομες δραστηριότητες, σε μια μορφή λιγότερο ύποπτη για τις διωκτικές αρχές. Το παράνομο χρήμα περιέρχεται σε διάφορα

[19] http://www.internet-fraud.com/fraudforum/DCForumID34/100.html#

[20] ''Stages of the Money Laundering Process'', A report in accordance with paragraph 356 (c) of the USA PATRIOT Act http://www.fincen.gov/356report.pdf

οικονομικά ιδρύματα ή διοχετεύεται στο λιανεμπόριο. Στο δεύτερο στάδιο, επιχειρείται ο διαχωρισμός του χρήματος από την παράνομη πηγή του, χρησιμοποιώντας πολλαπλές οικονομικές συναλλαγές για να αποκρύψουν το χρήμα. Στο τελευταίο στάδιο, ολοκληρώνεται η μετατροπή του παράνομου χρήματος, ώστε, να έχει τη μορφή εισοδήματος, που προήλθε από νόμιμες επαγγελματικές δραστηριότητες. Η ανωνυμία του Διαδικτύου, δυσχεραίνει την πιστοποίηση της ταυτότητας των πελατών μιας εταιρείας. Ως αποτέλεσμα, πολλές εταιρείες, χωρίς να το γνωρίζουν, διευκολύνουν το ξέπλυμα χρήματος. Για παράδειγμα, έχει διαπιστωθεί η αγορά μέσω του Διαδικτύου ασυνήθιστα μεγάλων ποσοτήτων αγαθών από συγκεκριμένους πελάτες, που θέλουν, μ' αυτό τον τρόπο, να προωθήσουν χρήματα, που έχουν περιέλθει στην κατοχή τους από παράνομες δραστηριότητες. Άλλη μέθοδος ξεπλύματος χρημάτων είναι η κατάθεση μέσω του Διαδικτύου, σχετικά μικρών ποσών σε πολλαπλούς τραπεζικούς λογαριασμούς.

Διακίνηση πορνογραφικού υλικού

Η διακίνηση πορνογραφικού υλικού, δεν είναι ένα νέο έγκλημα. Η εξάπλωση, όμως, του Διαδικτύου, έχει διευκολύνει την διάπραξή του. Στατιστικές μελέτες έχουν καταδείξει, ότι η διακίνηση υλικού πορνογραφίας μέσω του Διαδικτύου, αποτελεί μια από τις πιο συχνές μορφές εγκλήματος[21]. Ειδικότερα υπάρχουν δικτυακοί τόποι με πορνογραφικό υλικό (4,2 εκατομμύρια), σελίδες με πορνογραφικό υλικό (372 εκατομμύρια), αιτήματα για πορνογραφικό υλικό σε μηχανές αναζήτησης (ανά ημέρα)(25% του συνόλου, ήτοι 68 εκατομμύρια), e-mail με πορνογραφικό περιεχόμενο (4,5 ανά χρήστη), δικτυακοί τόποι που προσφέρουν παιδική πορνογραφία (100 χιλιάδες). Ο μέσος όρος ηλικίας της πρώτης επαφής με τη πορνογραφία είναι 11 ετών ,η μεγαλύτερη κατανάλωση πορνογραφίας μεταξύ 12-17 ετών, το ποσοστό παιδιών ηλικίας 7-17 ετών που δίνουν ελεύθερα την διεύθυνση της κατοικίας τους είναι 20%, ενώ η σεξουαλική παρενόχληση των νέων σε δωμάτια συζητήσεων ανέρχεται σε ποσοστό 89%. Τα αδικήματα, που συνδέονται με τη μορφή αυτή του υλικού, σχετίζονται τόσο με την δημιουργία του υλικού όσο και με τη μη νόμιμη διακίνησή 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 οποιασδήποτε άλλης μορφής πολυμέσων. Ο καθένας μπορεί εύκολα να το <<κατεβάσει>> στον υπολογιστή του, χωρίς να χρειαστεί να αποκαλύψει την ταυτότητά 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 νέο υλικό, ως αντάλλαγμα.

Δικτυακή τρομοκρατία

Η τρομοκρατία είναι ένα φαινόμενο, που παρουσιάζει ιδιαίτερη έξαρση τα τελευταία χρόνια. Η ιστορία έχει καταγράψει αιματηρές τρομοκρατικές επιθέσεις με χιλιάδες αθώα θύματα. Τα μέσα, που χρησιμοποιούν οι τρομοκράτες για τις επιθέσεις τους, συνεχώς εκσυγχρονίζονται, με το Διαδίκτυο να διαδραματίζει πλέον σημαντικό ρόλο. Το FBI ορίζει την κυβερνοτρομοκρατία (cyber terrorism) ως την <<προσχεδιασμένη, πολιτικά υποκινούμενη επίθεση εναντίον 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[22]. Αρχικά, είναι φθηνότερο από τις παραδοσιακές τρομοκρατικές μεθόδους, οι ενέργειές 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 επίθεσή τους από οποιοδήποτε σημείο του κόσμου και μπορούν να επιτεθούν, ταυτόχρονα, σε πολλούς στόχους. Η μεγαλύτερη τρομοκρατική απειλή παγκοσμίως, θεωρείται η οργάνωση Al-Kaida. Η έρευνα για το χτύπημα στους δίδυμους πύργους της 11ης Σεπτεμβρίου 2001, κατέληξε στο συμπέρασμα ότι οι τρομοκράτες είχαν αναπτύξει ένα ευρύτατο δίκτυο επικοινωνίας με την χρήση του Διαδικτύου, το οποίο βοήθησε τα μέγιστα στο συντονισμό των ενεργειών τους. Η επίθεση αυτή δημιούργησε διάφορα σενάρια για τη νέα μορφή κυβερνοτρομοκρατίας που απειλεί την ανθρωπότητα. Για

[21] http://www.familysafemedia.com/pornography_statistics.html
[22] M.Elmusharaf (2004), ''Cyber terrorism, a new kind of terrorism''.

παράδειγμα, οι τρομοκράτες με τη χρήση του Διαδικτύου, θα έχουν τη δυνατότητα να παραβιάσουν τα συστήματα ελέγχου κρίσιμων υποδομών μιας χώρας, όπως οι ενεργειακές εγκαταστάσεις, το δίκτυο διανομής νερού και τα τηλεπικοινωνιακά συστήματα[23]. Εκτιμάται ότι, το βασικότερο όπλο των τρομοκρατών του μέλλοντος θα είναι ο ηλεκτρονικός υπολογιστής[24].

Επιθέσεις παρενόχλησης

Με τους όρους cyberstalking και harassment ή γενικότερα παρενόχληση, περιγράφεται μια εγκληματική συμπεριφορά όπου ο επιτιθέμενος με τη χρήση ηλεκτρονικών μέσων επικοινωνίας όπως το Διαδίκτυο και τα κινητά τηλέφωνα, εκφοβίζει και γενικότερα παρενοχλεί τα θύματά του, για διάφορους λόγους, όπως εκδίκηση, επίλυση προσωπικών διαφορών. Η συμπεριφορά αυτή υπήρξε και στο συμβατικό περιβάλλον, όμως με την διάδοση του Διαδικτύου και την δυνατότητα άμεσης επικοινωνίας, που προσφέρουν υπηρεσίες όπως το e-mail, το chat ή τα newsgroup, έχει λάβει τεράστιες διαστάσεις, με αποτέλεσμα το μεγαλύτερο ποσοστό των εγκλημάτων αυτών, να διαπράττονται μέσω του Διαδικτύου. Την παρενόχληση, που διαπράττεται μέσω του Διαδικτύου, μπορούμε να την διακρίνουμε σε δύο κατηγορίες. Η πρώτη είναι η άμεση παρενόχληση, που συντελείται όταν ο επιτιθέμενος αποστείλει απευθείας στο θύμα μηνύματα με προσβλητικό ή απειλητικό περιεχόμενο, άσχετα με το γεγονός, εάν οι απειλές πραγματοποιηθούν. Η άλλη είναι η έμμεση παρενόχληση, όταν το μήνυμα δεν στέλνεται αμέσως στο θύμα, αλλά σε τυχαίους χρήστες του Διαδικτύου και περιλαμβάνει προσβλητικό ή απειλητικό για το θύμα περιεχόμενο.

## 4.4 Άλλες μορφές Ηλεκτρονικού Εγκλήματος

Αν και ο όρος ηλεκτρονικό έγκλημα παραπέμπει, πρωταρχικά, σε εγκλήματα που τελούνται με τη χρήση των Η/Υ και του Διαδικτύου, η ενσωμάτωση προηγμένων λειτουργιών ηλεκτρονικής επεξεργασίας δεδομένων και σε άλλες συσκευές, όπως τα κινητά τηλέφωνα ή τα palmtops, έχουν δημιουργήσει νέες δυνατότητες διάπραξης εγκλημάτων, όπως με τη χρήση κινητών τηλεφώνων, παιχνιδομηχανών, μηχανημάτων αυτόματης ανάληψης μετρητών και τηλεπικοινωνιακών δικτύων.

### 4.4.1 Κινητή τηλεφωνία

Η κινητή τηλεφωνία έχει αναπτυχθεί ιδιαίτερα την τελευταία δεκαετία σε όλες, ανεξαιρέτως, τις προηγμένες χώρες. Αν και αρχικά, τα κινητά τηλέφωνα χρησιμοποιήθηκαν, ως μια <<κινητή>> επέκταση των σταθερών τηλεφώνων, με το πέρασμα των χρόνων, άρχισαν να ενσωματώνουν στις λειτουργίες τους και άλλες υπηρεσίες. Πολύ σύντομα, μέσα από τα κινητά τηλέφωνα άρχισαν να παρέχονται διαδικτυακές υπηρεσίες, με τη χρήση νέων πρωτοκόλλων επικοινωνίας (λόγου χάριν WAP) μετατρέποντας τις μικρές αυτές συσκευές σε κινητούς ηλεκτρονικούς υπολογιστές. Μαζί με τις νέες δυνατότητες, όμως, τα κινητά τηλέφωνα κληρονόμησαν και τις αδυναμίες των υπολογιστών. Έτσι ένα κινητό μπορεί να μολυνθεί με ιούς, σκουλήκια (worms), dialers 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 , μπορούν να ανακτηθούν από μακριά εφόσον το κινητό έχει το Bluetooth σε λειτουργία εμφάνισης της συσκευής, αλλά ακόμη και σε λειτουργία μη εμφάνισης. Επίσης, το κινητό μπορεί να ελεγχθεί από απόσταση και να πραγματοποιήσει κλήσεις με στόχο την υπερχρέωση ή την υποκλοπή των ομιλιών ή και να ενεργοποιήσει εκτροπές. Τέλος, το Bluetooth μπορεί να χρησιμοποιηθεί, εφόσον, στηθούν κατάλληλες υποδομές κεραιών, για τον εντοπισμό ατόμων που φέρουν τη συσκευή του κινητού μαζί τους[25] .Η πρόσφατη εμπειρία στη χώρα μας με τις υποκλοπές συνομιλιών από γνωστή εταιρεία κινητής τηλεφωνίας, κατέδειξε το μέγεθος του προβλήματος. Το λογισμικό νομίμων συνακροάσεων, που ήταν εγκατεστημένο στους κεντρικούς υπολογιστές της εταιρείας παραβιάστηκε, με αποτέλεσμα, να είναι δυνατή η ακρόαση και καταγραφή συνομιλιών προσώπων, που ανήκαν ακόμη και στα υψηλότερα κυβερνητικά στρώματα. Η τροποποίηση των λειτουργιών του λογισμικού ήταν τέτοια, που του

[23] B.Collin, ''The future of Cyberterrorism : Where the Physical and Virtual Worlds Converge''
[24] http://www.schneier.com/crypto-gam-0306.html#1
[25] B.Fadia, 2005, ''An Ethical Guide to hacking mobile phones, Macmillan India

επέτρεπε να λειτουργεί στο παρασκήνιο, σε σκιώδη κατάσταση, που ούτε οι τεχνικοί της εταιρείας κατάφεραν να αντιληφθούν.

4.4.2 Τηλεπικοινωνιακά Δίκτυα

Οι επιθέσεις σε τηλεπικοινωνιακά δίκτυα από τους phreakers, αποτέλεσαν τις πρώτες ηλεκτρονικές απειλές. Οι νέες τεχνολογίες, που αρχίζουν ήδη να υιοθετούνται στον τομέα των τηλεπικοινωνιών και η επέκταση της χρήσης του πρωτόκολλου IP (Internet Protocol) που αναμένεται να κυριαρχήσει τα αμέσως προσεχή χρόνια στις τηλεπικοινωνίες, δημιουργούν νέες δυνατότητες διάπραξης εγκλημάτων. Μέσω του πρωτοκόλλου IP μεταφέρεται φωνή (VoIP), video-τηλεόραση (TVoIP), εικόνες, κείμενα και μουσική. Οι πρώτες μορφές επιθέσεων στις νέες υπηρεσίες έχουν, ήδη, κάνει την εμφάνισή τους (DoS attacks, υποκλοπή επικοινωνιών, traffic analysis, εντοπισμός θέσης χρήστη).

4.4.3.Παιχνιδομηχανές

Οι σύγχρονες παιχνιδομηχανές παρουσιάζουν ιδιαίτερο ενδιαφέρον για τις διωκτικές αρχές. Η ενσωμάτωση σε 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. Παρόμοιες δυνατότητες φέρουν και οι υπολογιστές, που προορίζονται για χρήση σε αυτοκίνητα.

4.4.4 Μηχανήματα Αυτόματης Ανάληψης Μετρητών

Οι χρήστες των μηχανημάτων αυτόματης ανάληψης μετρητών (ATM) έχουν γίνει, πολλές φορές, στόχος επιθέσεων με τη χρήση διαφόρων τεχνικών. Έχουν, καταγραφεί περιπτώσεις τοποθέτησης μηχανισμών, που μπλοκάρουν τις πιστωτικές κάρτες, τοποθέτησης μικροκαμερών, που καταγράφουν τους αριθμούς πιστωτικών καρτών και τα PIN όταν αυτά πληκτρολογούνται, ακόμη και η τοποθέτηση πρόσθετων πληκτρολογίων πανομοιότυπων με των πραγματικών για την απόσπαση κωδικών.

Συστατικά στοιχεία για τις μορφές Ηλεκτρονικού Εγκλήματος

Σύμφωνα με την FBI Computer Crime Survey (2005), η διασπορά κακόβουλου λογισμικού κατέχει την πρώτη θέση και μάλιστα με υψηλό ποσοστό (83,7% οι ιοί και 79,5% τα spyware). Σημαντικό ποσοστό, επίσης, καταλαμβάνουν οι επιθέσεις, που έχουν σκοπό την καταστροφή δεδομένων ή δικτύου (22,7%) και άρνησης εξυπηρέτησης, ενώ, μικρότερα ποσοστά παρατηρούμε στις οικονομικές και τηλεπικοινωνιακές απάτες (8,4 και 5,3 % αντιστοίχως). Η e-Crime Watch Survey (2005),παρουσίασε παρόμοια αποτελέσματα. Αίσθηση όμως προκαλεί το υψηλό ποσοστό των επιθέσεων phising (57%). Τέλος, υψηλά ποσοστά παρατηρούνται σε όλες τις μορφές επιθέσεων που έχουν να κάνουν με την κακόβουλη εισβολή σε δίκτυα.

## Χαρακτηριστικά γνωρίσματα του εγκλήματος στον κυβερνοχώρο

Ο όρος ηλεκτρονικό έγκλημα ,χρησιμοποιείται όλο και πιο συχνά ,καθώς η νέα αυτή μορφή εγκλήματος φέρει ορισμένα ιδιαίτερα χαρακτηριστικά[26] που το διαφοροποιούν από το συμβατικό έγκλημα. Είναι γεγονός ότι το ηλεκτρονικό έγκλημα διαπράττεται άμεσα ,σε ελάχιστα δευτερόλεπτα. Ο επιτιθέμενος με τη χρήση ενός Η/Υ συνδεδεμένου στο διαδίκτυο ,μπορεί να εισβάλλει στα υπολογιστικά συστήματα μιας επιχείρησης ή ενός οργανισμού σε οποιοδήποτε σημείο του κόσμου .Δεν απαιτείται η φυσική μετακίνησή του , καθώς οι ενέργειές του μπορούν

[26] S.Michell and E.Banker(1998)Private Intrusion Response

να ολοκληρωθούν από την οικία του ή άλλο χώρο ,με τη χρήση ενός δικτυωμένου προσωπικού υπολογιστή .Φαινομενικά ,η εισβολή σε κάποιο υπολογιστικό σύστημα φαντάζει δύσκολη .Όμως η άποψη ότι απαιτούνται εξειδικευμένες γνώσεις για την εξαπόλυση τέτοιου είδους επίθεσης, αποτελεί μύθο .Στο διαδίκτυο διατίθενται ελεύθερα εφαρμογές λογισμικού ,που επιτρέπουν στους επίδοξους hackers την εισβολή σε δίκτυα και υπολογιστικά συστήματα ,τη διασπορά ιών και την πραγματοποίηση πλήθους άλλων ηλεκτρονικών υποθέσεων ,καθιστώντας περισσότερο εύκολη την διάπραξη του ηλεκτρονικού εγκλήματος σε σχέση με το συμβατικό . Επιπλέον ,το Διαδίκτυο προσφέρει μια σειρά από νέες δυνατότητες επικοινωνίας .Το ηλεκτρονικό ταχυδρομείο(e-mail) ,τα δωμάτια συζητήσεων (chat rooms) και οι ομάδες ειδήσεων (newsgroups) ,επιτρέπουν σε πολλά άτομα ταυτόχρονα να επικοινωνούν γρήγορα ,σε πραγματικό χρόνο ,χωρίς μετακίνηση ,εύκολα και ανέξοδα .Η επανάσταση αυτή στις επικοινωνίες συνέβαλε στη διάδοση εγκλημάτων όπως η παιδοφιλία ,η παιδική πορνογραφία, και η ανεπιθύμητη αλληλογραφία( spamming) .Στις περιπτώσεις αυτές ,τα υποψήφια θύματα αναζητούνται μέσω των νέων καναλιών. Παράλληλα, το ηλεκτρονικό έγκλημα έχει εισαγάγει νέους νομοθετικούς προβληματισμούς. Πολλές φορές ,καθίσταται αδύνατο να προσδιοριστεί ο τόπος τέλεσης του εγκλήματος ,διότι κάθε εγκληματίας μπορεί να το διαπράξει από οποιοδήποτε σημείο του κόσμου ,αρκεί να έχει στην διάθεσή του έναν ηλεκτρονικό υπολογιστή. Επίσης ,είναι δύσκολο να προσδιοριστεί και ο ακριβής χρόνος τέλεσής του ,καθώς τα θύματα συχνά αντιλαμβάνονται μια ηλεκτρονική επίθεση πολύ αργότερα από το χρόνο κατά τον οποίο αυτή συνέβη .Έπειτα ,συχνά είναι δυνατή η διαγραφή από τον εισβολέα των <<ίχνων>> του ηλεκτρονικού εγκλήματος κάτι που δυσχεραίνει ή εμποδίζει την ανίχνευσή του .Τέλος ,σε σύγκριση με τα συμβατικά εγκλήματα, η διερεύνηση του ηλεκτρονικού εγκλήματος παρουσιάζει ιδιαιτερότητες .Σε μια διαδικτυακή έρευνα ,συχνά απαιτείται η συνεργασία τουλάχιστον δύο κρατών ,τα δε αρμόδια όργανα των διωκτικών αρχών πρέπει να κατέχουν εξειδικευμένες γνώσεις και να εκπαιδεύονται συνεχώς στις νέες τεχνολογικές εξελίξεις .Σε ορισμένες περιπτώσεις ,τέτοιου είδους γνώσεις απαιτείται να κατέχουν και όσοι άλλοι ασχολούνται με τη δίωξη του ηλεκτρονικού εγκλήματος όπως δικαστές ,εισαγγελείς και δικηγόροι .Δυστυχώς ,δεν υπάρχουν επαρκή στατιστικά στοιχεία ακόμη ,όχι μόνο στον ελληνικό ,αλλά και στον διεθνή χώρο .Ελάχιστες περιπτώσεις εγκλημάτων του κυβερνοχώρου καταγγέλλονται ,και αυτό για να μην πλήττεται το κύρος των εταιρειών που τυγχάνουν θύματα τέτοιων επιθέσεων .Κατά συνέπεια ,οι διαστάσεις της εγκληματικότητας στο χώρο του Διαδικτύου είναι πιο δύσκολο να καθοριστούν από ότι στον <<κοινό>> εγκληματικό χώρο(θεωρία του παγόβουνου,Ζάννη,2005) .

Έρευνες ηλεκτρονικής εγκληματικότητας

Ο βαθμός εισχώρησης του φαινομένου του ηλεκτρονικού εγκλήματος στη σύγχρονη κοινωνία, αποτελεί αντικείμενο μελέτης πολλών επιστημονικών κλάδων. Στην Ελλάδα, ο κίνδυνος από ηλεκτρονικές επιθέσεις κρίνεται σχετικά μικρός, όμως σε άλλες χώρες (π.χ.ΗΠΑ), αποτελεί μια καθημερινή πραγματικότητα. Δυστυχώς ,δεν μπορούμε να έχουμε επαρκή εικόνα για το βαθμό εξάπλωσης του ηλεκτρονικού εγκλήματος, καθώς η συλλογή στατιστικών στοιχείων είναι δυσκολότερη από κάθε άλλη μορφή εγκλήματος.

Προβλήματα κατά τη συλλογή στατιστικών δεδομένων

Τα στατιστικά στοιχεία που διαθέτουμε για το ηλεκτρονικό έγκλημα και προέρχονται από τις διωκτικές αρχές ,δεν μπορούν να χαρακτηριστούν αξιόπιστα .Υπάρχουν δυο βασικά εμπόδια που δεν μας επιτρέπουν να έχουμε ακριβή στοιχεία(Kabay, 2001):
Η δυσκολία εντοπισμού του ηλεκτρονικού εγκλήματος: Το πρόβλημα της λεγόμενης

<<κρυφής>> εγκληματικότητας ,που το συναντάμε σε όλες τις μορφές εγκλημάτων , παρουσιάζει μεγάλη συχνότητα στην περίπτωση των ηλεκτρονικών εγκλημάτων. Ο όρος αναφέρεται σε εγκλήματα που έχουν τελεσθεί ,χωρίς να το έχουν αντιληφθεί τα θύματα .
Η διστακτικότητα αναφοράς από τα θύματα: Ακόμη κι αν το θύμα αντιληφθεί μια ηλεκτρονική επίθεση εναντίον του, διστάζει να την αναφέρει στις διωκτικές αρχές , με αποτέλεσμα, να μην είναι δυνατή η συστηματική συλλογή στατιστικών στοιχείων .Οι λόγοι για τη μη αναφορά των ηλεκτρονικών εγκλημάτων ποικίλλουν με κυρίαρχο τον φόβο της εταιρείας που δέχθηκε την επίθεση, ότι αν αποκαλυφθεί το γεγονός θα έχει αρνητικές συνέπειες στην εικόνα της προς τους πελάτες της. Εκτιμάται ότι τα στατιστικά στοιχεία που διαθέτουμε από τις διωκτικές αρχές, αντιπροσωπεύουν μόνον το 10% της πραγματικής έκτασης του φαινομένου .Για το λόγο αυτό ,η μέτρηση του ηλεκτρονικού εγκλήματος ,γίνεται με εναλλακτικές μεθόδους, όπως συνεντεύξεις και έρευνες σε συγκεκριμένες κατηγορίες ατόμων.

2005 FBI Computer Crime Survey

Η πλέον αξιόπιστη έρευνα στην Αμερική, πραγματοποιείται κάθε χρόνο από το Ομοσπονδιακό Γραφείο Ερευνών (Federal Bureau of Investigation-FBI) των Ηνωμένων Πολιτειών. Τα αποτελέσματα της έρευνας για το έτος 2005, βασίζονται στις απαντήσεις 2066 οργανισμών και σκοπός της έρευνας είναι ,να διαπιστωθεί το είδος των εγκλημάτων που διαπράττονται σε όλο το εύρος των οργανισμών ,που δραστηριοποιούνται στις ΗΠΑ.Η έρευνα βασίζεται σε ένα ερωτηματολόγιο 23 ερωτήσεων ,που σχετίζεται με πλήθος θεμάτων όπως ασφάλεια υπολογιστών ,χρησιμοποιούμενη τεχνολογία ,είδος επιθέσεων και τρόποι αντιμετώπισης αυτών .Οι ερωτώμενοι απαντούν διατηρώντας την ανωνυμία τους . Από την έρευνα αυτή συνάγονται ουσιαστικά συμπεράσματα για το ηλεκτρονικό έγκλημα .Ας δούμετις απαντήσεις ορισμένων χαρακτηριστικών ερωτήσεων σχετικά με την έκταση του φαινομένου :
α)Στην ερώτηση<<Πόσα συμβάντα παραβίασης της ασφάλειας των υπολογιστών έλαβαν χώρα κατά τους τελευταίους 12 μήνες>> το 51,5% απάντησε από 1-4,το 20,1% από 5-9 ,το 9,1% από 10-19 και το 19,2% από 20 και πάνω .Διαφαίνεται ότι οι απειλές έναντι της ασφάλειας των υπολογιστών ,είναι σύνηθες φαινόμενο για το 87% των επιχειρήσεων που ερωτήθηκαν και μάλιστα το 50% από αυτές ,έχει δεχθεί περισσότερες από 5 επιθέσεις . Εντυπωσιακό είναι επίσης το ποσοστό των επιχειρήσεων που δέχθηκαν πάνω από 20 επιθέσεις.
β) Ένας μύθος που θεωρεί ότι οι περισσότερες επιθέσεις προέρχονται από τις ΗΠΑ καταρρίφθηκε από τις απαντήσεις στην αντίστοιχη ερώτηση. Ναι μεν η έρευνα έδειξε ότι το μεγαλύτερο ποσοστό των επιθέσεων προέρχεται από τις ΗΠΑ(26,1%),όμως είναι πολύ μικρότερο από αυτό που κάποιος θα περίμενε. Στη δεύτερη θέση ακολουθεί η Κίνα με ποσοστό 23,9%.Συνολικά, εμφανίζονται 36 χώρες από τις οποίες προέρχεται το 75% των επιθέσεων, καταδεικνύοντας, ότι το ηλεκτρονικό έγκλημα είναι φαινόμενο παγκόσμιας κλίμακας .
γ) Όσον αφορά τις οικονομικές συνέπειες από τις επιθέσεις που υπέστησαν οι οργανισμοί, παρατηρούμε ότι, το συνολικό κόστος ανήλθε περίπου στα 30000000 δολάρια, δηλαδή 170000 δολάρια κατά μέσο όρο.

2005 e-Crime Watch Survey

Η e-Crime Watch Survey πραγματοποιήθηκε το 2005 από το περιοδικό CSO(Chief Security Officers)σε συνεργασία με δύο πολύ σημαντικούς οργανισμούς: (α) The US Secret Service Electronic Crimes Task Force και (β)Carnegie Mellon University Software Engineering Institute's CERT Coordination Center .Η έρευνα ,σκιαγραφεί τις τάσεις που υπάρχουν στο φαινόμενο του ηλεκτρονικού εγκλήματος. Πραγματοποιήθηκε on-line ,κατά το χρονικό διάστημα από 3 έως 14 Μαρτίου 2005 .Οι ερωτώμενοι, ο συνολικός αριθμός των οποίων ανερχόταν στους 819, αποτελούνταν μόνο από μέλη του περιοδικού CSO ή της US Secret Service's Electronic Crimes TaskForce. Αναφέρονται ορισμένα βασικά αποτελέσματα της έρευνας:
α) Στην ερώτηση αν το ηλεκτρονικό έγκλημα θα αυξηθεί κατά το έτος 2005 το 85% απάντησε θετικά ενώ μόλις το 1% απάντησε αρνητικά.
β) Στην κρίσιμη ερώτηση σχετικά με τον αριθμό των ηλεκτρονικών εγκλημάτων, που

διαπράχθηκαν το έτος 2005 ,το 68% των ερωτώμενων απάντησε ότι δέχθηκε τουλάχιστον μια επίθεση, ενώ το 36% ότι δέχθηκε παραπάνω από 10 επιθέσεις .
γ)Τέλος ,όσον αφορά το κόστος που υπέστησαν οι επιχειρήσεις από τις επιθέσεις που δέχθηκαν, το 62% από αυτές δεν κατέστη δυνατόν να προσδιορίσει έστω και κατά προσέγγιση το χρηματικό ποσό, το 19% δεν είχε καθόλου χρηματικές απώλειες ,ενώ ένα ποσοστό της τάξης του 16% είχε ζημιές που ανέρχονται στο ένα εκατομμύρια δολάρια . Αν και τα οικονομικά δεδομένα που παρουσιάζονται από την έρευνα αυτή δεν είναι πολύ υψηλά ,το ποσοστό 62% που δεν μπορεί να προσδιορίσει το ακριβές ποσό είναι το πλέον ανησυχητικό στοιχείο, καθώς ενισχύει την αβεβαιότητα για τις οικονομικές απώλειες του ηλεκτρονικού εγκλήματος .

## Η Συνθήκη της Βουδαπέστης[27]

Οι μορφές του Ηλεκτρονικού Εγκλήματος είναι ποικίλες και με τη συνεχή ανάπτυξη της τεχνολογίας και του Διαδικτύου πολλαπλασιάζονται. Για την αντιμετώπιση του κινδύνου αυτού ήταν απαραίτητη η διακρατική συνεννόηση και η εκπόνηση μιας αναλυτικής και αποτελεσματικής στρατηγικής. Ο στόχος αυτός επετεύχθη στο Συνέδριο για το Ηλεκτρονικό Έγκλημα (Convention on Cybercrime), που έγινε το 2001 στη Βουδαπέστη του οποίου όλα τα συμπεράσματα αποκρυσταλλώνονται στη Συνθήκη που υπεγράφη μετά το πέρας των εργασιών του Συνεδρίου στις 23.11.2001. Στη Συνθήκη της Βουδαπέστης, υπέγραψαν 26 υπουργοί ευρωπαϊκών κρατών, μεταξύ των οποίων και της Ελλάδας υπάρχουν επεξηγήσεις και ρυθμίσεις για όλα τα Ηλεκτρονικά Εγκλήματα. Ειδικότερα ,στη συνθήκη αυτή περιέχονται οι ορισμοί των εννοιών σύστημα ηλεκτρονικού υπολογιστή, δεδομένα Η/Υ κ.α. Υπάρχουν επεξηγήσεις και ρυθμίσεις για όλα τα ηλεκτρονικά εγκλήματα όπως είναι τα αδικήματα κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των συστημάτων Η/Υ. Τέτοια αδικήματα είναι η παράνομη πρόσβαση, η παράνομη υποκλοπή, η επέμβαση σε δεδομένα, η επέμβαση σε συστήματα και η κακή χρήση συσκευών. Έπειτα, είναι τα αδικήματα που σχετίζονται με τους υπολογιστές όπως η απάτη με η/υ και πλαστογραφία, αυτά που σχετίζονται με το περιεχόμενό τους, όπως είναι το αδίκημα της παιδικής πορνογραφίας και τέλος αναφέρονται και αδικήματα που σχετίζονται με καταπάτηση πνευματικής ιδιοκτησίας . Ταυτόχρονα ,περιέχει ρυθμίσεις για την συνέργια, την απόπειρα και την υποκίνηση ηλεκτρονικών εγκλημάτων καθώς και την ευθύνη των επιχειρήσεων. Ακόμα τονίζει την αναγκαιότητα της διεθνούς συνεργασίας μεταξύ των κρατών για την καταπολέμηση του ηλεκτρονικού εγκλήματος και θίγει το πολύ σημαντικό θέμα της αρμοδιότητας και της δικαιοδοσίας των δικαστηρίων σχετικά με τα εγκλήματα αυτά[28].

Λεπτομερειακά ,στο προοίμιο της σύμβασης αναφέρεται η ανάγκη θεσπίσεως νομοθεσίας σχετικής με το έγκλημα στο διαδίκτυο. Το Συμβούλιο της Ευρώπης επισημαίνει ότι επήλθαν θεμελιώδεις αλλαγές στο χώρο των ηλεκτρονικών υπολογιστών, ενώ εκφράζει την ανησυχία του για την εμφάνιση νέων μορφών εγκληματικότητας στο διαδίκτυο και την ολοένα αυξανόμενη παρουσία τέτοιων εγκληματικών δραστηριοτήτων.

Στο πρώτο κεφάλαιο δίνονται οι ορισμοί κάποιων εννοιών, όπως η έννοια του ηλεκτρονικού συστήματος (computer system), του ηλεκτρονικού δεδομένου (computer data) η του παροχέα πρόσβασης (service provider). Και τούτο προκειμένου να καθιερωθεί μια κοινά αποδεκτή ορολογία για ορισμένες βασικές τεχνικές και δύσκολα κατανοητές έννοιες και να διασφαλιστεί με τον τρόπο αυτό η ομοιογενής εννοιολογική προσέγγιση των όρων αυτών από τις εθνικές έννομες τάξεις. Στο πρώτο μέρος του δευτέρου κεφαλαίου αναφέρονται τα μέτρα που πρέπει να ληφθούν σε εθνικό επίπεδο. Ειδικότερα σχετικά με το ουσιαστικό ποινικό δίκαιο τα κράτη μέλη πρέπει να υιοθετήσουν νομοθετικά μέτρα για τα *εγκλήματα κατά της εμπιστευτικότητας (confidentiality) των δεδομένων* και *των συστημάτων* (νοώντας ως εμπιστευτικότητα των δεδομένων την ιδιότητα εκείνη των δεδομένων να καθίστανται προσπελάσιμα *μόνο* στους εξουσιοδοτημένους χρήστες του συστήματος), για τα *εγκλήματα της ακεραιότητας (integrity) των*

[27] Αγγελή Ι., «Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο», ΠοινΔικ 12/2001, σελ. 1218 κε, του ιδίου, «Διαδίκτυο (Internet) και ποινικό δίκαιο – Έγκλημα στον κυβερνοχώρο (Cybercrime-Internet Crime)», ΠοιΧρ Ν/2000, σελ. 680 και βλ. htt://www.lawnet.gr/lawnet/eofn/2/Cybercrime.asp

[28] http://www.go-online.gr/ebusiness/specials/article.html?article_id=367

*δεδομένων* και *των συστημάτων* (νοώντας ως ακεραιότητα των δεδομένων την ιδιότητα των στοιχείων να είναι ακριβή και να αντιπροσωπεύουν την πραγματικότητα, ενώ κάθε αλλαγή τους να είναι αποτέλεσμα εξουσιοδοτημένης ενέργειας) και για τα *εγκλήματα της διαθεσιμότητας (availability) των δεδομένων* και *των συστημάτων* (ως διαθεσιμότητα νοείται η ιδιότητα των πόρων ενός πληροφοριακού συστήματος να καθίστανται άμεσα προσπελάσιμοι στον εκάστοτε εξουσιοδοτημένο χρήστη του συστήματος). Η σημασία της θέσπισης των παραπάνω μέτρων κατά των 20 εγκλημάτων που περιγράφονται λαμβάνει την πραγματική της διάσταση, αν αναλογιστούμε ότι μέσω του διαδικτύου διακινείται πληθώρα δεδομένων άμεσα σχετιζόμενων με την προσωπική και ιδιωτική ζωή των χριστών του διαδικτύου ή και μη χρηστών (π.χ. ηλικία, θρήσκευμα, αριθμοί πιστωτικών καρτών). Αποτελεί, λοιπόν, αναφαίρετο δικαίωμα του καθενός να απαιτήσει τη μη διαρροή τέτοιου είδους προσωπικών δεδομένων και την ασφαλή διακίνησή τους. Σύμφωνα με τις διατάξεις της Σύμβασης κάθε μέλος που την αποδέχεται αναλαμβάνει την υποχρέωση να ποινικοποιήσει ορισμένες συμπεριφορές που σχετίζονται με τις δραστηριότητες στο διαδίκτυο.

Πιο συγκεκριμένα, κατά το άρθρο 2 της Σύμβασης κάθε μέλος υποχρεούται να λάβει νομοθετικά μέτρα για τη θεμελίωση της ειδικής υπόστασης του *εγκλήματος της παράνομης πρόσβασης (illegal access)* στις περιπτώσεις της εκ προθέσεως και χωρίς δικαίωμα πρόσβασης σε σύστημα ηλεκτρονικών υπολογιστών.

Ουσιαστικός σκοπός αυτής της διάταξης είναι να ποινικοποιήσει το κοινώς λεγόμενο hacking, δηλαδή την παράνομη διείσδυση με διάφορους τεχνικούς τρόπους σε ξένα συστήματα. Προστατευόμενο δε έννομο αγαθό είναι η ασφάλεια του ηλεκτρονικού συστήματος, δηλαδή η πρόληψη της πρόσβασης σε ένα σύστημα από μη εξουσιοδοτημένα άτομα. Αξίζει να σημειωθεί ότι αναφορικά με τη θεμελίωση της υποκειμενικής υπόστασης απαιτείται η ύπαρξη άμεσου δόλου, όπως αυτός νοείται στο εσωτερικό δίκαιο κάθε κράτους μέλους[29].

Σύμφωνα με το άρθρο 3 της Σύμβασης τα κράτη μέλη καλούνται να ποινικοποιήσουν την *αθέμιτη υποκλοπή δεδομένων ηλεκτρονικών υπολογιστών (illegal interception)* από, προς ή εντός ενός συστήματος υπολογιστών. Η διάταξη αυτή βρίσκει εφαρμογή σε κάθε μορφής υποκλοπή ηλεκτρονικών δεδομένων που διακινούνται στο διαδίκτυο με το πρωτόκολλο μεταφοράς αρχείων (File Transfer Protocol), το ηλεκτρονικό ταχυδρομείο (e-mail) και με άλλες παρόμοιες υπηρεσίες του διαδικτύου. Προστατευόμενο έννομο αγαθό είναι το δικαίωμα στην ιδιωτική ζωή και την ασφάλεια των τηλεπικοινωνιών στο διαδίκτυο. Και για την πλήρωση της υποκειμενικής υπόστασης αυτού του εγκλήματος απαιτείται - όπως και για το έγκλημα παράνομης πρόσβασης - το στοιχείο του άμεσου δόλου.

Σύμφωνα με το άρθρο 4 της Σύμβασης κάθε κράτος μέλος δεσμεύεται να λάβει τα απαραίτητα νομοθετικά μέτρα, προκειμένου να καθιερώσει ως ποινικό αδίκημα την *επέμβαση* σε *ηλεκτρονικά δεδομένα (data interference),* η οποία αναλύεται στην άνευ δικαιώματος καταστροφή (damaging), διαγραφή (deletion), φθορά (deterioration). μεταβολή (alteration) ή απόκρυψη (suppression) δεδομένων. Ο σκοπός της διάταξης αυτής είναι να προστατεύσει τα δεδομένα και τα προγράμματα των ηλεκτρονικών υπολογιστών από κάθε εξωτερική επέμβαση (interference) στον υλικό φορέα τους. Η υλική ακεραιότητα και η λειτουργία των δεδομένων και των ηλεκτρονικών προγραμμάτων είναι, λοιπόν, το προστατευόμενο έννομο αγαθό. Και στην περίπτωση αυτών των αδικημάτων, όπως και πριν απαιτείται η συνδρομή του άμεσου δόλου (πρόθεση).

Στη συνέχεια της διάρθρωσης της Σύμβασης και συγκεκριμένα στο άρθρο 5 υπαγορεύεται η ποινικοποίηση της *επέμβασης* σε *σύστημα*33 *(system interference),* η οποία τελείται με την εκ προθέσεως και άνευ δικαιώματος παρακώλυση της λειτουργίας ενός συστήματος υπολογιστών μέσω της εισαγωγής (inputting), μεταφοράς (transmitting), καταστροφής (damaging), διαγραφής (deleting), φθοράς (deterioration), μεταβολής (alteration) ή απόκρυψης (suppression) ηλεκτρονικών δεδομένων. Με τη διάταξη αυτή ποινικοποιείται το κοινά λεγόμενο computer sabotage (δολιοφθορά ηλεκτρονικού υπολογιστή).

Στο άρθρο 6 της Σύμβασης κάθε κράτος μέλος αναλαμβάνει την υποχρέωση να ποινικοποιήσει την *κατάχρηση των υπηρεσιών του διαδικτύου (misuse of devices),* νοώντας την εκ προθέσεως και χωρίς δικαίωμα παραγωγή, πώληση, προετοιμασία για χρήση, εισαγωγή, διανομή ή με οποιοδήποτε τρόπο διάθεση μιας συσκευής, συμπεριλαμβανομένου και

[29] Στην ελληνική έννομη τάξη υπάρχει ήδη τέτοια αντίστοιχη διάταξη και συγκεκριμένα το άρθρο 370Γ παρ. 2 ΠΚ.

προγράμματος υπολογιστή που έχει σχεδιαστεί ή προσαρμοστεί με σκοπό τη διάπραξη οποιουδήποτε αδικήματος των άρθρων 2 έως 5 της Σύμβασης.

Επιπλέον, τα κράτη καλούνται με την υπογραφή της Σύμβασης να θεσπίσουν ειδικές ποινικές διατάξεις για εγκλήματα σχετιζόμενα με υπολογιστές (computer related offences) και σ υγκεκριμένα αυτά της πλαστογραφίας και της απάτης. Ιδιαίτερη μνεία γίνεται για τα εγκλήματα που σχετίζονται με το περιεχόμενο, που διακινείται μέσω διαδικτύου και ειδικά σχετικά με την παιδική πορνογραφία. Παράλληλα ,στη σύμβαση συμπεριλαμβάνονται διατάξεις για αδικήματα σχετικά με παραβιάσεις πνευματικών και συγγενικών δικαιωμάτων (offences related to infringement of Copyright and related rights). Τέλος, το δεύτερο κεφάλαιο περιλαμβάνει διατάξεις δογματικού ποινικού χαρακτήρα για την απόπειρα, τη συμμετοχή και την ευθύνη των νομικών προσώπων.

Στο δεύτερο μέρος του δευτέρου κεφαλαίου βρίσκονται οι διατάξεις του ποινικού δικονομικού δικαίου. Πιο συγκεκριμένα, αναφέρονται σε θέματα34 ταχείας διαφύλαξης αποθηκευμένων δεδομένων σε ηλεκτρονικό υπολογιστή (expedited preservation of stored computer data), ταχείας διαφύλαξης και γνωστοποίησης διακινούμενων αρχείων (expedited preservation and disclosure of traffic data), εντολής παροχής πληροφοριών (production order) έρευνας και κατάσχεσης αποθηκευμένων σε ηλεκτρονικό υπολογιστή στοιχείων (search and seizure of stored computer data), πραγματικού χρόνου συλλογής διακινούμενων δεδομένων (real-time collection of traffic data), καθώς και παγίδευσης – υποκλοπής περιεχομένου δεδομένων (intercention of content data). Τέλος, στο τρίτο μέρος γίνεται αναφορά σε θέματα δικαιοδοσίας.

Το τρίτο κεφάλαιο περιλαμβάνει διατάξεις διεθνούς δικαστικής συνεργασίας που αναφέρονται στην έκδοση, σε γενικές αρχές σχετικά με την αμοιβαία συνδρομή, σε παροχή αυτοματοποιημένων πληροφοριών, στην ταχεία διαφύλαξη δεδομένων αποθηκευμένων σε υπολογιστή και στην ταχεία γνωστοποίηση των διαφυλαγμένων διακινούμενων δεδομένων.

Επιπρόσθετα, στις 28.1.2003 υπογράφηκε στο Στρασβούργο το συμπληρωματικό πρωτόκολλο προς συμπλήρωση της συμβάσεως της Βουδαπέστης για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο. Πρόκειται για το Πρόσθετο Πρωτόκολλο της Σύμβασης. Σ' αυτό ποινικοποιούνται πράξεις ρατσισμού και ξενοφοβίας που διαπράττονται μέσω του διαδικτύου

## Νομοθεσία για το ηλεκτρονικό έγκλημα

Το ηλεκτρονικό έγκλημα είναι μια νέα μορφή εγκλήματος , που οριοθετείται από δύο βασικά στοιχεία, τους ηλεκτρονικούς υπολογιστές και το Διαδίκτυο. Η προσέγγιση των νομικών θεμάτων που αφορούν το ηλεκτρονικό έγκλημα ενέχει τη δυσκολία ότι προϋποθέτει όχι μόνο νομικές ,αλλά και σε ένα βαθμό τεχνικές γνώσεις σε θέματα ηλεκτρονικών υπολογιστών και Διαδικτύου. Τα προβλήματα της νομοθεσίας επικεντρώνονται στη διαμόρφωση της κατάλληλης ορολογίας ,στην αρτιότερη εφαρμογή του Ποινικού και Δικονομικού Δικαίου, καθώς και σε ειδικότερα θέματα που άπτονται της διεθνούς συνεργασίας ,όπως η διεθνής δικαιοδοσία. 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 του γνώσεις και τα τεχνολογικά χαρακτηριστικά κάθε αντικειμένου. Στη νομική επιστήμη, ο προσδιορισμός των όρων είναι τελείως διαφορετικός. Για το νομικό, κάθε έννοια έχει το περιεχόμενο εκείνο που με ακρίβεια καθορίζει ο Νόμος .Σε περίπτωση που δεν υπάρχει νόμος ερευνάται η σχετική νομολογία και αν δεν υπάρχει ούτε νομολογία, η ανάλυση ανάγεται στους 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 την χρησιμοποιούμενη από την τεχνολογία, η οποία μπορεί να είναι ασαφής, γενική ,αόριστη ή ελλιπής ,κατά τρόπο που να εμποδίζει την ορθή απονομή της δικαιοσύνης . Το ηλεκτρονικό έγκλημα φέρει κάποια ιδιαίτερα χαρακτηριστικά, που το διαφοροποιούν από το συμβατικό έγκλημα. Τα χαρακτηριστικά αυτά, απαιτούν την υιοθέτηση ειδικών νομοθετικών ρυθμίσεων για την αντιμετώπισή του, τόσο στον τομέα του Ποινικού , όσο και στον τομέα του Δικονομικού Δικαίου. Από άποψη Ποινικού Δικαίου, γεγονός που πολλές φορές, καθιστά αδύνατη τη δίωξή του. Στον τομέα του δικονομικού δικαίου, οι παρεμβάσεις στην ισχύουσα νομοθεσία παγκοσμίως, είναι ελάχιστες ,με αποτέλεσμα να δημιουργούνται ανυπέρβλητα προβλήματα, όπως η δυσκολία ασφαλούς καθορισμού της δικαιοδοσίας των δικαστηρίων και της αρμοδιότητας των διωκτικών αρχών.

Με δεδομένο ότι η τεχνολογία προχωρά πολύ πιο γρήγορα από τη νομοθεσία, κάθε νομοθετική ρύθμιση υπόκειται πολύ γρήγορα σε αμφισβήτηση. Αυτό που σήμερα ορίζουμε ως ηλεκτρονικό έγκλημα, πολύ σύντομα δεν θα υπάρχει ως συμπεριφορά ή θα έχει τροποποιηθεί κατά τρόπο ουσιαστικό ,που θα καθιστά ανίσχυρο τον υπάρχοντα νόμο. Για την αντιμετώπιση του ηλεκτρονικού εγκλήματος δεν αρκεί μόνο ειδική νομοθεσία, αλλά απαιτείται συνεχής ενημέρωσή της, λαμβάνοντας υπ' όψιν τις τεχνολογικές εξελίξεις. Επιπλέον, για ένα άρτιο σύστημα απονομής δικαιοσύνης ,όλοι όσοι εμπλέκονται στη δίωξη του ηλεκτρονικού εγκλήματος όπως αστυνομικοί , εισαγγελείς ,δικαστές και δικηγόροι, πρέπει να κατέχουν τόσο νομικές ,όσο και τεχνικές γνώσεις, για τη νέα αυτή 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 δε συνέπειες της εγκληματικής συμπεριφοράς, μπορούν 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 δικαιοδοσία έκδοσης όσων έχουν διαπράξει ηλεκτρονικά εγκλήματα με διεθνή χαρακτήρα, είναι μερικά μόνο από τα ζητήματα ποτ επιτείνουν τους νομοθετικούς προβληματισμούς.

### 3.12.1 Νομοθετικοί προβληματισμοί
### Νομική προσέγγιση του Διαδικτύου

Κυρίαρχο νομικό ζήτημα για την αντιμετώπιση του ηλεκτρονικού εγκλήματος ,αποτελεί η νομική ρύθμιση του Διαδικτύου ,ενός <<χώρου >> τεράστιου και αχανούς, με δυσδιάκριτα όρια και απεριόριστες δυνατότητες ανταλλαγής πληροφοριών. Έως σήμερα, δεν υπάρχουν συγκεκριμένες διατάξεις που να ρυθμίζουν συνολικά τις προσφερόμενες ,μέσω του Διαδικτύου , υπηρεσίες .Επιπλέον ,οποιαδήποτε προσπάθεια ρύθμισης ,συναντά φραγμούς, που ανάγονται στις απόψεις δυο αντιμαχόμενων παρατάξεων. Αυτών που είναι υπέρ και αυτών που είναι κατά της οποιασδήποτε προσπάθειας ρύθμισης του Διαδικτύου.Τα επιχειρήματα υπέρ της ρύθμισης του Διαδικτύου είναι τα ακόλουθα. Το Διαδίκτυο είναι ανοιχτό σε όλους και απαιτείται η ρύθμισή του για τον έλεγχο του παράνομου περιεχομένου του. Έπειτα, αυτό δεν αποτελεί διαφορετικό μέσο επικοινωνίας ,σε σχέση με το ραδιόφωνο και την τηλεόραση, τα οποία υπόκεινται ήδη σε νομοθετικές ρυθμίσεις. Επίσης, υπάρχει πολύ επιβλαβές υλικό σε αυτό, όπως και αυξανόμενη εγκληματική δραστηριότητα, που γεννά την υποχρέωση της πολιτείας για τον έλεγχο και την αντιμετώπισή της. Ακολούθως, 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 μορφής ρύθμισης συνοψίζονται στα παρακάτω . Αρχικά, η ελευθερία του λόγου που προσφέρεται μέσω του Διαδικτύου είναι απόλυτο δικαίωμα κάθε πολίτη, προστατευόμενο από συνταγματικές διατάξεις. Έπειτα, το Διαδίκτυο είναι διαφορετικό από τα άλλα μέσα επικοινωνίας ,διαθέτοντας ιδιαίτερα χαρακτηριστικά όπως η ελευθερία, η ειλικρίνεια και ο πειραματισμός[30]. Ακολούθως, το Διαδίκτυο δεν μπορεί να ρυθμιστεί, διότι είναι τεράστιο και παγκόσμιο και οποιαδήποτε προσπάθεια ,θα έρχεται πάντα αντιμέτωπη με το ζήτημα της λογοκρισίας. Τέλος ,οι γονείς είναι υπεύθυνοι για να προστατεύσουν τα παιδιά από το παράνομο περιεχόμενο του Διαδικτύου και όχι τα κράτη με νομοθετικές ρυθμίσεις.

Το Διαδίκτυο ,με άξονα τη βασική του χρήση ως μέσο επικοινωνίας ,απασχόλησε τον νομοθέτη, ιδιαίτερα από το χρονικό σημείο που άρχισε να αναπτύσσεται και να επεκτείνεται . Στην Ελλάδα έως το 1990, οι υπηρεσίες που στηρίζονταν στην πληροφορική παρέχονταν μονοπωλιακά από τον ΟΤΕ. Το ίδιο συνέβαινε και σε άλλες ευρωπαϊκές χώρες. Το τοπίο διαφοροποιήθηκε με πρωτοβουλία της Ευρωπαϊκής Κοινότητας ,η οποία με δυο οδηγίες την 90/387 και την 90/388 ,κατήργησε το μονοπώλιο των εθνικών τηλεπικοινωνιακών οργανισμών, δίνοντας τη δυνατότητα σε οποιοδήποτε φορέα να προσφέρει τηλεπικοινωνιακές υπηρεσίες.

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

[30] ''Declaration of the Independence of Cyberpace'', John Perry Barlow

σε ισχύ. Με το νόμο αυτό, ιδρύθηκε ρυθμιστική αρχή, η <<Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων>>, με αποστολή τη διασφάλιση των συμφερόντων των χρηστών του Διαδικτύου. Η Αρχή αυτή έχει τη δυνατότητα να ελέγχει τους πάροχους τηλεπικοινωνιακών υπηρεσιών και να επιβάλλει κυρώσεις σε περίπτωση παραβίασης συγκεκριμένων δικαιωμάτων των χρηστών, όπως η διατήρηση του απόρρητου χαρακτήρα των επικοινωνιών τους.

### 3.12.2 ΕΛΛΗΝΙΚΗ ΝΟΜΟΘΕΣΙΑ

Άρθρα Ποινικού Κώδικα

**Άρθρο 348$^{A}$ -** Πορνογραφία ανηλίκων

**Άρθρο 370$^{A}$ -** Παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας

**Άρθρο 370Β -** Παραβίαση στοιχείων ή προγραμμάτων υπολογιστών που θεωρούνται απόρρητα.

**Άρθρο 370Γ -** Παράνομη αντιγραφή ή χρήση προγραμμάτων υπολογιστών και παράνομη πρόσβαση σε δεδομένα υπολογιστών.

**Άρθρο 386$^{A}$ –** Απάτη με υπολογιστή.

ΝΟΜΟΙ

**Ν. 2225/94** – «Προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας»

**Ν. 2472/97 και 2774/99** – «Περί προσωπικών δεδομένων»

**Ν. 2472/1997 –** «Για την προστασία των προσωπικών δεδομένων στο Διαδίκτυο»

**Ν. 2774/1999 –** «Για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα»

**Ν. 2867/2000 -** «Οργάνωση και Λειτουργία του τομέα των Τηλεπικοινωνιών»

**Ν. 2819/2000 –** «Προσθήκη στο Ν. 2121/1993 περί νομικής προστασίας βάσεων δεδομένων»

**Ν. 2225/1994 όπως τροπ. Με Ν. 3115/2003** – «Για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις»

**Ν. 3411/2006** – «Περί ηλεκτρονικών επικοινωνιών».

ΠΡΟΕΔΡΙΚΑ ΔΙΑΤΑΓΜΑΤΑ

**Π.Δ. 131/2003** – «Ηλεκτρονικό εμπόριο κλπ Υπηρεσίες της Κοινωνίας της Πληροφορίας»

**Π.Δ. 150/2001** - «Ηλεκτρονικές Υπογραφές»

**Π.Δ. 47/2005** – «Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και τη διασφάλισή του».

### 3.12.3 Η ΕΥΡΩΠΗ ΑΠΕΝΑΝΤΙ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Η πρώτη προσπάθεια νομικής προσέγγισης του ηλεκτρονικού εγκλήματος στον Ευρωπαϊκό χώρο, πραγματοποιήθηκε από το Συμβούλιο της Ευρώπης το 1976 στο Στρασβούργο, στις εργασίες του Συνεδρίου για τις Εγκληματολογικές πλευρές του Οικονομικού Εγκλήματος. Ήταν η πρώτη φορά που παρουσιάστηκαν οι μορφές του ηλεκτρονικού εγκλήματος ,συμπεριλαμβανομένης και της απάτης. Το 1986, συστήθηκε μια επιτροπή από το Ευρωπαϊκό Συμβούλιο, η οποία εξέτασε την ισχύουσα νομοθεσία στα κράτη- μέλη ,τα δε συμπεράσματά της συμπεριλήφθηκαν στη Σύσταση του 1989, η οποία όριζε εγκληματικές πράξεις , όπως απάτη και πλαστογραφία με ηλεκτρονικούς υπολογιστές, καταστροφή δεδομένων και λογισμικού, μη εξουσιοδοτημένη πρόσβαση ή μη εξουσιοδοτημένη αναπαραγωγή λογισμικού. Επίσης, η Σύσταση αυτή περιέλαβε και μια σειρά από Οδηγίες (μη υποχρεωτικές) μπρος τα κράτη –μέλη ,σχετικά με τη μεθοδολογία θέσπισης νομοθετικών κειμένων για το ηλεκτρονικό έγκλημα. Το Συμβούλιο της Ευρώπης αντιμετώπισε αποφασιστικότερα το ζήτημα της νομοθεσίας για το ηλεκτρονικό έγκλημα το 1996, εκδίδοντας δύο Συστάσεις No R (89)9 σχετικά με το έγκλημα που διαπράττεται με τη χρήση ηλεκτρονικού υπολογιστή και τη Σύσταση No R (95)13 για τα ποινικά δικονομικά προβλήματα που συνδέονται με την τεχνολογία των ηλεκτρονικών υπολογιστών. Οι συστάσεις αυτές αποτέλεσαν την βάση για τη Σύμβαση για το Κυβερνοχώρο του 2001.

### 3.12.4 Οδηγίες Ευρωπαϊκής Ένωσης

**Οδηγία 87/102/ΕΟΚ** του Συμβουλίου της 22ας Δεκεμβρίου 1986 για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη.

**Οδηγία 90/88/ΕΟΚ** του Συμβουλίου της 22ας Φεβρουαρίου 1990 για την τροποποίηση της οδηγίας 87/102/ΕΟΚ γι την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη.

**Οδηγία 90/387/ΕΟΚ** του Συμβουλίου της 28ης Ιουνίου 1990 για τη δημιουργία της εσωτερικής αγοράς στον τομέα των τηλεπικοινωνιακών υπηρεσιών μέσω της εφαρμογής της παροχής ανοικτού δικτύου (Open Networt Provision –ONP).

**Οδηγία 90/388/ΕΟΚ** της Επιτροπής της 28ης Ιουνίου 1990 σχετικά με τον ανταγωνισμό στις αγορές των τηλεπικοινωνιακών υπηρεσιών.

**Οδηγία 91/250/ΕΟΚ** του Συμβουλίου της 14ης Μαΐου 1991 για τη νομική προστασία των προγραμμάτων ηλεκτρονικών υπολογιστών

**Οδηγία 96/9/ΕΟΚ** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαρτίου 1996, σχετικά με τη νομική προστασία των βάσεων δεδομένων.

**Οδηγία 97/7/ΕΚ** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Μαΐου 1997 για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις.

**Οδηγία 1999/93/ΕΚ** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 1999,

σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.

**Οδηγία 2000/31/ΕΚ** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά («οδηγία για το ηλεκτρονικό εμπόριο»).

**Οδηγία 2002/19/ΕΚ** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με την πρόσβαση σε δίκτυα ηλεκτρονικών επικοινωνιών και συναφείς ευκολίες, καθώς και με τη διασύνδεσή τους (οδηγία για την πρόσβαση).

**Οδηγία 2002/20/ΕΚ** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, για την αδειοδότηση δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών (οδηγία για την αδειοδότηση).

**Οδηγία 2002/21/ΕΚ** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (οδηγία πλαίσιο).

**Οδηγία 2002/22/ΕΚ** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (οδηγία καθολικής υπηρεσίας).

**Οδηγία 2002/58/ΕΚ** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες).

**Οδηγία 2002/77/ΕΚ** της Επιτροπής, της 16ης Σεπτεμβρίου 2002, σχετικά με τον ανταγωνισμό στις αγορές δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών.

Διεθνείς Συμβάσεις

Συνθήκη των Βρυξελλών (1968) περί προσδιορισμού της δικαιοδοσίας

Σύμβαση για το Κυβερνοχώρο - Βουδαπέστη 23-11-2001

Η Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου του ΟΗΕ της 10-12-1948

Η Σύμβαση της Ρώμης «για την προάσπιση των δικαιωμάτων του ανθρώπου και των θεμελιωδών ελευθεριών» της 4-11-1 50 (ΕΣΔΑ)

ΑΠΟΦΑΣΕΙΣ

Η Υπουργική Απόφαση ε αριθ. 88141/1995 - «Κώδικα Δεοντολογίας Άσκησης Τηλεπικοινωνιακών Δραστηριοτήτων».

Η Απόφαση της Ε.Ε.Τ.Τ. με αριθ. 268/73/2002 - «Κανονισμός Διαχείρισης κα Εκχώρησης Ονομάτων Χώρου (Domain Names) με κατάληξη .gr»

Ανεξάρτητα όμως από το εάν ο ανωτέρω νόμος και οι διεθνείς συνεργασίες επαρκούν ή όχι για την ποινική κάλυψη των θεμάτων που προκύπτουν από την ανάπτυξη της Πληροφορικής, το βέβαιον είναι ότι, δεν επαρκούν για την τελεία αντιμετώπιση των εγκλημάτων που έχουν τελεστεί με τη χρήση του Διαδικτύου.

Πρόσφατα τέθηκε σε ισχύ το Π.Δ. 47/2005, από την Α.Δ.Α.Ε. (Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών), το οποίο αφορά τις διαδικασίες, τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και τη διασφάλισή του. Ενώ, σύντομα αναμένεται να τεθεί σε ισχύ η Συνθήκη της Βουδαπέστης.

Άρθρο 370Β

1. Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον 3 μηνών. Ως απόρρητα θεωρούνται κι εκείνα που ο νόμιμος κάτοχός τους από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.

2. Αν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων, καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας, επιβάλλεται φυλάκιση τουλάχιστον ενός έτους.

3. Αν πρόκειται για στρατιωτικό ή διαπλαστικό απόρρητο ή για απόρρητο που αναφέρεται στην ασφάλεια του κράτους, η κατά την παρ. 1 πράξη τιμωρείται κατά τα άρθρα 146 και 147.

4. Οι πράξεις που προβλέπονται στις παρ.1 και 2 διώκονται ύστερα από έγκληση.

Άρθρο 370Γ

1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μήνες και με χρηματική ποινή διακοσίων ενενήντα (290) ευρώ έως πέντε χιλιάδων εννιακοσίων (5.900) ευρώ.

2. Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον είκοσι εννέα ευρώ. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή την ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148.

3. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του

κατόχου ή αρμοδίου υπαλλήλου του.

4. Οι πράξεις των παρ. 1 έως 3 διώκονται ύστερα από έγκληση.

Άρθρο 386Α - Απάτη με υπολογιστή -

Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλο παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλο τρόπο, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημιάς είναι αδιάφορο αν παθόντες είναι ένα ή περισσότερα πρόσωπα. Νομοθεσία διαδικτυακών εγκλημάτων στην αλλοδαπή. Στην Αγγλία από τον Φεβρουάριο του 2001, οι hackers, αναλόγως με τη σημασία του χτυπήματος θεωρούνται και τρομοκράτες. Στην Αμερική θεωρείται τρομοκρατική οποιαδήποτε πράξη μη εξουσιοδοτημένης πρόσβασης σε Η/Υ, και τιμωρείται με φυλάκιση ως και ισόβια (ανάλογα με τη σημασία της εισβολής), χωρίς δυνατότητα μείωσης τις ποινής.

Αδυναμίες της νομοθεσίας

*Ο Προϊστάμενος του Τμήματος Ηλεκτρονικού Εγκλήματος της Δ/νσης Ασφάλειας Αττικής, Αστυνόμος Α΄ κ. Εμμανουήλ Σφακιανάκης παρατηρεί ότι "*οι νομοθετικές ρυθμίσεις που αφορούν το ηλεκτρονικό έγκλημα παρουσιάζουν εγγενείς αδυναμίες, τόσο στην Ελλάδα όσο και στις υπόλοιπες χώρες. Αυτό συμβαίνει διότι το Ηλεκτρονικό Έγκλημα αποτελεί εγκληματική δραστηριότητα αρκετά εξειδικευμένη και ανεπτυγμένη τεχνολογικά, με αποτέλεσμα να παρουσιάζονται προβλήματα στην οριοθέτηση των πράξεων που θα πρέπει να διώκονται ποινικά. Επιπλέον, οι νομοθέτες είναι αναγκασμένοι να ενημερώνονται διαρκώς για τις εξελίξεις στον τομέα της τεχνολογία των υπολογιστών, προκειμένου να εξοικειωθούν με τον τρόπο διάπραξης αδικημάτων μέσω αυτών." *(Σε ειδική έρευνα που έγινε στη Βρετανία από την Επιτροπή Πρόβλεψης και Πρόληψης Εγκλήματος (Foresight Crime Prevention Panel) διαπιστώθηκε ότι το έτος 2020 οι κακοποιοί θα γνωρίζουν στην εντέλεια τη λειτουργία των συστημάτων ασφαλείας των τραπεζικών κωδικών και των τεχνικών αναγνώρισης και θα έχουν την τεχνογνωσία να υπερκεράσουν οποιοδήποτε ηλεκτρονικό εμπόδιο).*[31]

Παγκόσμια νομοθεσία για το Ηλεκτρονικό Έγκλημα

Ηνωμένες Πολιτείες της Αμερικής

Το πρώτο νομοθέτημα σχετικά με το ηλεκτρονικό έγκλημα θεσπίστηκε στις Ηνωμένες Πολιτείες της Αμερικής, το 1984. Ο νόμος Computer Fraud and Abuse Act, προσπάθησε ,ανεπιτυχώς ίσως , να θέσει ένα βασικό νομικό πλαίσιο για τη νέα αυτή μορφή εγκλήματος. Η έλλειψη όρων σχετιζόμενων με τη νέα τεχνολογία των ηλεκτρονικών υπολογιστών ,αλλά και η αποτυχία προσδιορισμού των ορίων δικαιοδοσίας των δικαστηρίων ,ήταν από τα σημαντικότερα προβλήματα. Επιπλέον, 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. Τα προβλήματα αυτά, οδήγησαν πολύ γρήγορα στην πρώτη αναθεώρηση το 1986, στην οποία προστέθηκε μια ακόμη ενότητα ,που προέβλεπε ότι <<όποιος σκόπιμα αποκτά πρόσβαση σε ομοσπονδιακό υπολογιστικό σύστημα χωρίς εξουσιοδότηση και συνέπεια της πρόσβασης αυτής τροποποιεί, προκαλεί ζημιά ή καταστρέφει πληροφορίες που είναι αποθηκευμένες σε έναν ηλεκτρονικό υπολογιστή κρατικού ενδιαφέροντος ή εμποδίζει την εξουσιοδοτημένη χρήση ενός υπολογιστή ή των πληροφοριών που είναι αποθηκευμένες σε αυτών τιμωρείται με…>>. Στην τροποποίηση αυτή 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 αναφερόταν μόνο σε κρατικά υπολογιστικά συστήματα.

Η πιο σημαντική τροποποίηση του νομοθετήματος αυτού έγινε το 1994, η οποία επέφερε αλλαγές σε τρία σημαντικά σημεία. Αρχικά, η ισχύς του νομοθετικού πλαισίου επεκτάθηκε και σε ηλεκτρονικούς υπολογιστές, που χρησιμοποιούνται στο διαπολιτειακό εμπόριο. Έπειτα, αφαιρέθηκε ο όρος <<μη εξουσιοδοτημένη πρόσβαση >>, που σημαίνει ότι οι υπάλληλοι εταιρειών και οι εξουσιοδοτημένοι χρήστες θα μπορούσαν να διωχθούν και συγκεκριμένες μορφές επικίνδυνων και σκόπιμων ενεργειών θεωρούνται πλέον, παράνομες, όπως η διασπορά κακόβουλου λογισμικού και οι επιθέσεις άρνησης εξυπηρέτησης. Τέλος ,το 1996,

[31] http://www.e-crime.gr/nomothesia.htm

συμπληρώθηκε ο νόμος αυτός με τη National Information Infrastructure Protection Act (NIIPA), η οποία 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 ,ενώ εάν η πρόσβασή του είναι εξουσιοδοτημένη ,είναι ποινικά υπεύθυνος μόνο εάν η πρόσβαση του είναι εξουσιοδοτημένη, είναι ποινικά υπεύθυνος μόνο εάν έχει πρόθεση να προξενήσει ζημιά στο θύμα. Οι διατάξεις αυτές ,με μικρές τροποποιήσεις που έχουν επέλθει στη συνέχεια, ισχύουν και σήμερα, ενσωματωμένες στο κεφάλαιο 18, παράγραφος 1030 του Ποινικού Κώδικα των ΗΠΑ. Εκτός αυτών ,σε κάθε πολιτεία υπάρχουν σε ισχύ διάφορες διατάξεις , που αντιμετωπίζουν το ηλεκτρονικό έγκλημα με διαφορετικό τρόπο. Η απουσία ενιαίων διατάξεων σε όλα τα μήκη και πλάτη των ΗΠΑ ,αποτελεί τη μεγαλύτερη πληγή του δικαικού συστήματος.

Αυστραλία

Η Αυστραλία είναι η χώρα που έχει δώσει τη μεγαλύτερα προσοχή ,μετά τις ΗΠΑ, στην αντιμετώπιση του ηλεκτρονικού εγκλήματος. Ο νόμος <<Crime Act 1914>> προβλέπει τέσσερις βασικές μορφές ηλεκτρονικού εγκλήματος που είναι η παράνομη πρόσβαση σε δεδομένα αποθηκευμένα σε κρατικό ηλεκτρονικό υπολογιστή, η καταστροφή δεδομένων αποθηκευμένων σε κρατικό ηλεκτρονικό υπολογιστή , η πρόσβαση σε δεδομένα αποθηκευμένα σε ηλεκτρονικό υπολογιστή χρησιμοποιώντας μέσα κρατικής διευκόλυνσης και τέλος η καταστροφή δεδομένων σε ηλεκτρονικό υπολογιστή χρησιμοποιώντας μέσα κρατικής διευκόλυνσης.

Ο νόμος που σήμερα είναι σε ισχύ στην Αυστραλία ,αναφέρεται ως ‘’The Cybercrime Act 2001’’, ο οποίος προήλθε από την τροποποίηση του νόμου Crime Act και του Ποινικού Κώδικα που ψηφίστηκε το 1995. Ο νόμος προβλέπει τρεις βασικές κατηγορίες ηλεκτρονικών εγκλημάτων. Η πρώτη είναι η μη εξουσιοδοτημένη πρόσβαση ,η μετατροπή και φθορά δεδομένων, με σκοπό τη διάπραξη σοβαρού εγκλήματος. Στην περίπτωση αυτή, η ποινή είναι ισοδύναμη της αντίστοιχης που επιβάλλεται στο συμβατικό έγκλημα. Επίσης έχουμε την μη εξουσιοδοτημένη τροποποίηση δεδομένων ,που οδηγεί σε φθορά δεδομένων. Επιπλέον, υπάρχει η μη εξουσιοδοτημένη φθορά ηλεκτρονικών επικοινωνιών , για την οποία προβλέπεται ποινή έως δέκα ετών.

Παράλληλα, ο νόμος δημιούργησε τέσσερις νέες μορφές εγκλημάτων , οι οποίες είναι η μη εξουσιοδοτημένη πρόσβαση ή μετατροπή προστατευμένων δεδομένων, η παράνομη καταστροφή δεδομένων αποθηκευμένων σε δίσκους Η/Υ, η κατοχή ή έλεγχος δεδομένων, με σκοπό τη διάπραξη ηλεκτρονικών αδικημάτων και την παραγωγή ,προμήθεια ή απόκτηση δεδομένων, με σκοπό τη διάπραξη ηλεκτρονικού εγκλήματος. Στο νόμο ακόμη περιλαμβάνονται διατάξεις για τον τρόπο έρευνας ηλεκτρονικών αδικημάτων από τις διωκτικές αρχές και τις μεθόδους εξέτασης δεδομένων, που είναι αποθηκευμένα σε ηλεκτρονικά μέσα.

Αγγλία

Στην Αγγλία, το πρώτο νομοθέτημα για το ηλεκτρονικό έγκλημα ψηφίστηκε το 1990. Πρόκειται για το νόμο<<Computer Misuse Act>>, ένα από τα πλέον σημαντικά νομοθετικά κείμενα για το ηλεκτρονικό έγκλημα, το οποίο αποτέλεσε οδηγό για τις νομοθεσίες άλλων χωρών, όπως ο Καναδάς και η Ιρλανδία. Η νομοθετική αυτή πράξη καλύπτει σε μεγάλο εύρος το νομοθετικό κενό για το ηλεκτρονικό έγκλημα. Διακρίνει τρεις βασικές κατηγορίες αδικημάτων, που σχετίζονται με ηλεκτρονικό υπολογιστή. Αυτές είναι η μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες που είναι αποθηκευμένες σε ηλεκτρονικό υπολογιστή, η μη εξουσιοδοτημένη πρόσβαση με σκοπό τη διάπραξη αδικημάτων και η 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. Αν και πλήρης σε πολλά σημεία ,λαμβάνοντας υπ’ όψιν υη χρονική περίοδο κατά την οποία τέθηκε σε ισχύ ,ο νόμος αυτός χρειάζεται αναθεώρηση ,γιατί δεν έχει λάβει υπόψη ένα πολύ σημαντικό παράγοντα, το Διαδίκτυο. Η ανάπτυξη του Διαδικτύου δημιούργησε μια σειρά από νέα αδικήματα και μεθόδους τέλεσής τους που ήταν αδύνατον να προβλεφθούν την εποχή εκείνη. Μάλιστα ο νομοθέτης απέφυγε να ορίσει τι είναι ηλεκτρονικός υπολογιστής, καθώς δεν ήταν δυνατό να προβλεφθεί ,τότε, η σημερινή μορφή των ηλεκτρονικών υπολογιστών.

Αργεντινή

Στην Αργεντινή ,δεν υφίσταται συγκεκριμένο νομοθετικό πλαίσιο για το ηλεκτρονικό έγκλημα. Η ποινική αντιμετώπιση των εγκλημάτων της μορφής αυτής προέρχεται από τον κοινό 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 διωχθούν μόνο με διασταλτική ερμηνεία των ισχυουσών διατάξεων. Για παράδειγμα, τα άρθρα 128 και 129 του Ποινικού Κώδικα, σχετικά με την παιδική πορνογραφία, καθιστούν παράνομη τη δημοσίευση , δημιουργία, αναπαραγωγή και διάθεση τέτοιου υλικού χωρίς να προσδιορίσουν το μέσο με το οποίο θα πραγματοποιηθούν οι ενέργειες αυτές.

Κίνα

Η Κίνα, αντιμετωπίζει το ηλεκτρονικό έγκλημα με ειδική νομοθεσία που έχει θεσπιστεί για το σκοπό αυτό. Το άρθρο 23 του Νομοθετικού Διατάγματος 147, καθιστά παράνομη οποιαδήποτε δραστηριότητα σχετίζεται με τη διασπορά ιών ή άλλου είδους <<κακόβουλου>> λογισμικού ,σε ηλεκτρονικούς υπολογιστές. Παράνομη, επίσης, είναι η πώληση συστημάτων προστασίας υπολογιστών χωρίς άδεια. Οι κυρώσεις που προβλέπονται για την παραβίαση των παραπάνω διατάξεων ,περιλαμβάνουν χρηματικό πρόστιμο, που κυμαίνεται από 5000 έως 15000 γιέν ανάλογα με τη σοβαρότητα του εγκλήματος.

Το ζήτημα της πορνογραφίας αντιμετωπίζεται με την υπάρχουσα νομοθεσία, όπως συμβαίνει στις περισσότερες χώρες στον κόσμο. Το Διαδίκτυο, με το οποίο διακινούνται τεράστιες ποσότητες πορνογραφικού υλικού ,αποτελεί ένα ακόμη μέσο τέλεσης του εγκλήματος.

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, δημιουργώντας σαφή ερωτήματα για τα όρια της ελευθερίας του λόγου στο Διαδίκτυο.

Διεθνείς προσπάθειες

Σε διεθνές επίπεδο ,η Interpol προσέγγισε πρώτη το ζήτημα του ηλεκτρονικού εγκλήματος ,στο Τρίτο Διεθνές Συμπόσιο για την Απάτη ,στο Παρίσι ,το 1979. Διάφορες άλλες προσεγγίσεις έλαβαν χώρα κατά τα χρόνια που ακολούθησαν ,με πιο σημαντικές αυτές που αναπτύχθηκαν από τον OECD, τα Ηνωμένα Έθνη και την <<Ομάδα των Οκτώ>>.

Ο Οργανισμός για την Οικονομική Συνεργασία και Ανάπτυξη διόρισε στο Παρίσι ,το 1983, μια επιτροπή για το ζήτημα του ηλεκτρονικού εγκλήματος και την ανάγκη ,που αυτό δημιουργεί ,για την τροποποίηση των ποινικών διατάξεων στα κράτη- μέλη του οργανισμού. Η επιτροπή ,αφού εξέτασε 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 απαγόρευσαν 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, απαγόρευαν την πρόσβαση σε σύστημα Η/Υ χωρίς άδεια ,ενώ προστάτευαν και την παράνομη αντιγραφή και διεθνή διάθεση πακέτων λογισμικού.

Τα Ηνωμένα Έθνη παρουσίασαν ένα ψήφισμα ,σχετικά με τη νομοθεσία για το ηλεκτρονικό έγκλημα, στο 8$^{ο}$ 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 φαινομένου, τις μορφές του και την υπάρχουσα νομοθεσία σε διάφορες χώρες, και καταλήγει σε προτάσεις για την καλύτερη αντιμετώπισή του. Το συγκεκριμένο κείμενο, πρέπει να αναθεωρηθεί ,λόγω των τεχνολογικών εξελίξεων που συντελέστηκαν μετά την έκδοσή του. Αποτελεί, όμως, την πρώτη συστηματική διεθνή προσπάθεια νομοθετικής προσέγγισης του ηλεκτρονικού εγκλήματος. Για το λόγο αυτό. Θεωρείται η βάση πάνω στην οποία μπορούν να στηριχθούν μελλοντικές προσπάθειες.

Οι οκτώ ισχυρότερες χώρες του κόσμου ,δημιούργησαν το 1997μια Υποομάδα για το Έγκλημα Υψηλής Τεχνολογίας . 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 ηλεκτρονικού φαινομένου, σε όλες τις χώρες του κόσμου. Εκτός από τις Αρχές και Δράσεις ,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.

Η ασφάλεια στο Διαδίκτυο

Η ευρύτατη χρήση της τεχνολογίας της πληροφορικής και των επικοινωνιών, αποτελούν το βασικό χαρακτηριστικό τη σημερινή εποχή. Οι υπολογιστές, χρησιμοποιούνται σε όλες τις εκφάνσεις της ανθρώπινης δραστηριότητας, όπως στο εμπόριο, την εκπαίδευση, την ενημέρωση και την ψυχαγωγία. Ως αποτέλεσμα, η ασφάλεια των δεδομένων, που περιέχονται σε αυτούς, αποτελεί πρωταρχικό ζήτημα, καθότι οι κίνδυνοι καταστροφών, αλλοιώσεων ή μη εξουσιοδοτημένης χρήσης των δεδομένων και των υπολογιστικών πόρων

πολλαπλασιάζονται. Ο όρος ασφάλεια, χρησιμοποιείται συχνότατα στην καθημερινή μας ζωή. Προσδιορίζει μια ποικιλία από έννοιες. 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 από μη εξουσιοδοτημένη χρήση των πόρων του. Η ασφάλεια των πληροφοριακών συστημάτων σχετίζεται με την πρόληψη με εξουσιοδοτημένων ενεργειών έναντι ενός συστήματος, την ανίχνευση κάθε είδους επιθέσεως και τέλος, την αντίδραση δηλαδή τη λήψη μέτρων για την αποκατάσταση της ζημιάς που προκλήθηκε από τον επιτιθέμενο. Η πρόληψη, η ανίχνευση και η αντίδραση περιλαμβάνονται 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.

Βασικές έννοιες της Ασφάλειας

Η ασφάλεια των πληροφοριακών συστημάτων, προσδιορίζεται με τρεις βασικές έννοιες οι οποίες είναι κοινά αποδεκτές και αυτές είναι η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα. Αναφορικά με την εμπιστευτικότητα, αυτή 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 αυτά υπάρχουν. Για παράδειγμα, η ύπαρξη του φακέλου ενός εγκληματία, τυγχάνει της ίδιας προστασίας και με τα περιεχόμενα του φακέλου. Στην βιβλιογραφία, η εμπιστευτικότητα αναφέρεται εναλλακτικά ή και συμπληρωματικά με τους όρους ιδιωτικότητα (privacy), μυστικότητα (secrecy) και ανωνυμία (anonymity). Σχετικά με την ακεραιότητα, αυτή αναφέρεται στην πρόληψη μη εξουσιοδοτημένης μεταβολής των πληροφοριών. Η μεταβολή περικλείει τις έννοιες της προσθήκης, διαγραφής αλλά και μη εξουσιοδοτημένης δημιουργίας δεδομένων. Τέλος, η διαθεσιμότητα περιλαμβάνει τη δυνατότητα άμεσης προσπέλασης, χωρίς καθυστερήσεις, των πληροφοριών και υπηρεσιών ενός πληροφοριακού συστήματος. Ο μεγαλύτερος κίνδυνος, έναντι της διαθεσιμότητας, είναι οι επιθέσεις άρνησης εξυπηρέτησης, κατά τις οποίες, ο επιτιθέμενος στερεί από τους χρήστες την πρόσβαση στους πόρους του συστήματος ή του δικτύου.

Μέτρα πρόληψης

Η πρόληψη, αποτελεί τη βασική συνιστώσα της ασφάλειας του πληροφοριακού συστήματος ενός οργανισμού. Στοχεύει στην αποτροπή εκδήλωσης μιας επίθεσης, μέσω της αποθάρρυνσης του επιτιθέμενου και της αντίδρασης από το αρχικό στάδιο εκδήλωσης της επίθεσης.

Διαδικασίες αυθεντικοποίησης

Στον κόσμο της τεχνολογίας της πληροφορίας, με τον όρο αυθεντικοποίηση, νοείται η διαδικασία κατά την οποία διαπιστώνεται, ότι η ταυτότητα ενός χρήστη είναι αυθεντική. Για τον προσδιορισμό της ταυτότητας ενός ατόμου, υπάρχουν τρεις βασικές προσεγγίσεις. Αρχικά, πρόκειται για κάτι που ο χρήστης γνωρίζει (κωδικός πρόσβασης, PIN). Έπειτα, είναι κάτι που ο χρήστης έχει στην κατοχή του (έξυπνη κάρτα). Τελικά, πρόκειται για κάτι που ο χρήστης έχει ως προσωπικό φυσικό χαρακτηριστικό (δακτυλικό αποτύπωμα). Κάθε μια από τις προσεγγίσεις αυτές, φέρει τα προτερήματα και ελαττώματά της. Λόγου χάριν, ένας χρήστης μπορεί να ξεχάσει τον κωδικό πρόσβασης ή να τον αποκαλύψει από λάθος σε μη εξουσιοδοτημένα άτομα. Μια κάρτα εισόδου, μπορεί εύκολα να χαθεί. Ασφαλέστερη θεωρείται η χρήση προσωπικών χαρακτηριστικών, όμως για ένα σύστημα που απαιτεί υψηλό επίπεδο ασφάλειας, χρησιμοποιείται ένας συνδυασμός, όσο το δυνατόν περισσότερων τεχνικών.

Κωδικοί πρόσβασης

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 την βάση δεδομένων από κωδικούς, που έχει από πριν αποθηκευτεί και εφόσον διαπιστωθεί ταύτιση επιτρέπεται η είσοδος του χρήστη. Η μέθοδος αυτή, είναι από τις πιο παλιές και λόγω της απλότητάς της αλλά και της μεγάλης ασφάλειας που προσφέρει τυγχάνει ευρείας εφαρμογής. Σήμερα, οι κωδικοί πρόσβασης αποτελούν αναπόσπαστο κομμάτι οποιουδήποτε λειτουργικού συστήματος. Η διατήρηση της αξιοπιστίας ενός συστήματος, που χρησιμοποιεί κωδικούς πρόσβασης, εξαρτάται από τον βασικό παράγοντα του κατά πόσο οι κωδικοί πρόσβασης μπορούν να παραμείνουν μυστικοί. Υπάρχουν αρκετοί τρόποι με τους οποίους ένας κωδικός πρόσβασης μπορεί να αποκαλυφθεί, όπως για παράδειγμα, με τη χρήση απλών εργαλείων λογισμικού. Επιπλέον, ο ίδιος ο χρήστης, με τις πράξεις και παραλείψεις του, μπορεί άθελά του να συμβάλει στην αποκάλυψη των κωδικών του. Οι βασικότεροι κίνδυνοι εναντίον της ασφάλειας ενός συστήματος, που βασίζεται στη χρήση κωδικών πρόσβασης

είναι αρχικά η επιλογή τους. Ειδικότερα, η ορθή επιλογή του κώδικα πρόσβασης είναι πολύ σημαντική. Όταν οι χρήστες αφήνονται μόνοι τους να επιλέξουν τους κωδικούς που επιθυμούν, προτιμούν κωδικούς που μπορούν να θυμούνται εύκολα (ονόματα, ημερομηνίες γέννησης), με αποτέλεσμα κάποιος κακόβουλος να μπορεί να τους μαντέψει. Όταν η επιλογή των κωδικών δεν αφήνεται στους χρήστες, αλλά πραγματοποιείται από τους διαχειριστές ενός συστήματος, τότε επιτυγχάνεται μεγαλύτερη ασφάλεια, ενδέχεται όμως ο χρήστης, εάν ο κωδικός που του χορηγήθηκε είναι δύσκολο να απομνημονευτεί, να τον γράψει σε ένα φύλλο χαρτί, διευκολύνοντας την διαρροή του εφόσον το χαρτί απολεσθεί η κλαπεί. Έπειτα, αναφέρεται ο διαμοιρασμός των κωδικών πρόσβασης. Πολλές φορές, ένας υπάλληλος μπορεί να δώσει τον κωδικό του σε άλλο υπάλληλο, προκειμένου αυτός να έχει πρόσβαση στα αρχεία του, στη συνέχεια, να δοθεί για τον ίδιο λόγο σε κάποιον τρίτο. Τέτοιου είδους διαμοιρασμός των κωδικών πρόσβασης εγκυμονεί κινδύνους προερχόμενους, κυρίως, από τους κοινωνικούς μηχανικούς, οι οποίοι προσποιούμενοι ότι είναι υπάλληλοι μιας παραδείγματος χάριν θυγατρικής εταιρείας, επιτυγχάνουν την απόκτηση των κωδικών. Ταυτόχρονα, γίνεται λόγος για την παρακολούθηση των πακέτων που διακινούνται στο δίκτυο. Αυτό μπορεί να έχει ως αποτέλεσμα την ανάκτηση κωδικών πρόσβασης. Λόγου χάριν, η σύνδεση ενός απομακρυσμένου υπολογιστή με ένα κεντρικό υπολογιστή ενός προστατευμένου δικτύου, απαιτεί την εισαγωγή από το χρήστη κωδικών πρόσβασης, οι οποίοι, θα διακινηθούν μέσω του δικτύου. Σε τελική ανάλυση, επισημαίνεται και η πρόσβαση στο αρχείο αποθήκευσης των κωδικών. Οι συγκεκριμένοι κωδικοί αποθηκεύονται σε ένα αρχείο του διακομιστή, προκειμένου να είναι δυνατή η διαδικασία ταυτοποίησης .Εφόσον το αρχείο αυτό δεν φυλάσσεται καλά, ο επιτιθέμενος μπορεί να το ανακτήσει και να έχει, πλέον, στην κατοχή του όλους τους κωδικούς ενός οργανισμού.

Βιομετρικές τεχνικές

Βιομετρία είναι η επιστήμη που χρησιμοποιεί ψηφιακή τεχνολογία, για να αναγνωρίσει την ταυτότητα ατόμων, βάση κάποιων ιδιαίτερων και μοναδικών φυσιολογικών ή συμπεριφοριστικών χαρακτηριστικών τους. Η χρήση των βιομετρικών τεχνικών στον τομέα της ασφάλειας των πληροφοριακών συστημάτων στοχεύει καταρχάς στην επαλήθευση της ταυτότητας ενός χρήστη, η οποία επιτυγχάνεται με τη σύγκριση ενός χαρακτηριστικού του, με ένα χαρακτηριστικό μιας βάσης δεδομένων με σκοπό να βρεθεί ταίριασμα. Επίσης στοχεύει στην ταυτοποίηση ενός χρήστη, η οποία επιτυγχάνεται με τη σύγκριση ενός χαρακτηριστικού του, με το σύνολο των χαρακτηριστικών μιας βάσης δεδομένων με σκοπό να βρεθεί ταίριασμα. Οι σημαντικότερες βιομετρικές τεχνικές είναι οι ακόλουθες. Αρχικά αναφέρεται η σάρωση δακτυλικού αποτυπώματος. Συγκεκριμένα, η ταυτοποίηση δυο ατόμων με τη χρήση δακτυλικών αποτυπωμάτων, αποτελεί μια από τις πλέον κλασικές και αξιόπιστες μεθόδους ταυτοποίησης. Χρησιμοποιείται, ευρέως, από τις περισσότερες αστυνομικές υπηρεσίες του κόσμου. Έχει αποδειχθεί, ότι η πιθανότητα δύο ατόμων να έχουν το ίδιο δακτυλικό αποτύπωμα, είναι μία στο δισεκατομμύριο. Η λήψη των δακτυλικών αποτυπωμάτων γινόταν, παραδοσιακά, με την επικάλυψη των δακτύλων με μελάνη και την εναπόθεσή τους σε λευκή κόλλα χαρτί. Στη συνέχεια, πραγματοποιούνταν σάρωση του δακτυλικού αποτυπώματος. Σήμερα, η μέθοδος αυτή, τείνει να ξεπεραστεί, καθώς αρχίζουν να χρησιμοποιούνται ευρέως οπτικοί αναγνώστες, υπέρυθρες ακτίνες και τεχνολογίες σιλικόνης για τη λήψη των αποτυπωμάτων. Έπειτα, γίνεται λόγος για την αναγνώριση προσώπου (οπτική, θερμική), που αποτελεί μια από τις πλέον ταχύτατα αναπτυσσόμενες βιομετρικές τεχνικές. Τα πλεονεκτήματα της μεθόδου αυτής είναι ότι βρίσκεται πιο κοντά στον τόπο που καθημερινά οι άνθρωποι αναγνωρίζουμε τους συνανθρώπους μας. Επιπλέον, με τα σύγχρονα μηχανήματα είναι δυνατή η λήψη φωτογραφιών από μεγάλη απόσταση. 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 ή το κενό ανάμεσα στα φρύδια. Τα περισσότερα συστήματα δεν αντιμετωπίζουν πρόβλημα σε αλλαγές κόμμωσης και για καλύτερα αποτελέσματα δεν χρησιμοποιούν περιοχές του προσώπου κοντά στα μαλλιά. 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 ακόμη και εκατοντάδων χιλιάδων προσώπων. Όμως, πολλά συστήματα αντιμετωπίζουν δυσκολίες στο να πετύχουν μεγάλα επίπεδα απόδοσης, όταν το μέγεθος της βάσης δεδομένων αυξάνεται σε δεκάδες χιλιάδες ή και περισσότερο. Ακόλουθα, αναφέρουμε τη σάρωση φωνής. Τα σχετικά συστήματα λειτουργούν, αναγνωρίζοντας το μοναδικό ηχητικό σήμα που παράγει ο χρήστης, λέγοντας για συγκεκριμένη φράση κλειδί (pass- phrase). Το βασικό προτέρημα αυτής της τεχνολογίας, είναι η δυνατότητα για εξ αποστάσεως ταυτοποίηση. Δηλαδή, δεν είναι αναγκαίο ο χρήστης να βρίσκεται μπροστά σε κάποιο μηχάνημα ή συσκευή του συστήματος, όπως γίνεται κατά την αναγνώριση

δακτυλικού αποτυπώματος ή προσώπου, αλλά μπορεί να βρίσκεται χιλιόμετρα μακριά, χρησιμοποιώντας το τηλέφωνό του ή να βρίσκεται στο σπίτι του και να χρησιμοποιήσει ένα κοινό μικρόφωνο. Κατόπιν, υπάρχει η σάρωση της ίριδας του ματιού και του αμφιβληστροειδή χιτώνα. Η ίριδα, είναι το έγχρωμο μέρος, που περιβάλλει την κόρη του ματιού και έχει πλούσια και μοναδικά χαρακτηριστικά, όπως ραβδώσεις, νεύρα , δακτύλιοι ιστοί, αυλάκια, αγγεία και το δίκτυο κυττάρων. Σύμφωνα με μελέτες, η ανθρώπινη ίριδα έχει σχεδόν 250 χαρακτηριστικά και καθένα απ' αυτά είναι μοναδικό σε κάθε άτομο. Ο αριθμός των χαρακτηριστικών είναι δέκα φορές πάνω από τον αριθμό των γνωρισμάτων, που διαθέτουν τα δακτυλικά αποτυπώματα. Αυτό σημαίνει, ότι η πιθανότητα ο γενετικός κώδικας της ίριδας ενός ατόμου να ταιριάζει απόλυτα με το γενετικό κώδικα της ίριδας κάποιου άλλου ατόμου είναι τόσο απίθανη, σαν να είναι σχεδόν αδύνατο. Η αναγνώριση της ίριδας είναι ακόμα πιο αξιόπιστη και από την εξέταση DNA. Μαζί με τη σάρωση της ίριδας, η σάρωση του αμφιβληστροειδούς είναι η πιο ακριβής και αξιόπιστη βιομετρική τεχνολογία, όπως είναι και μεταξύ των πιο δύσκολων στη χρήση. Διάφορες έρευνες έχουν δείξει ότι η μορφή των αγγείων αίματος στο πίσω μέρος του ανθρώπινου ματιού είναι διαφορετική από άτομο σε άτομο, ακόμα και σε δίδυμα αδέρφια. Επίσης, ο αμφιβληστροειδής παραμένει ίδιος σε όλη τη ζωή του ανθρώπου , με την εξαίρεση ορισμένων τύπων εκφυλιστικών ασθενειών του ματιού, ή περιπτώσεις σοβαρών τραυμάτων στο κεφάλι. Επιπλέον, υφίσταται η σάρωση του χεριού. Αυτή 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 του χεριού έχει αποδειχθεί, ως η ιδανική λύση για χαμηλού επιπέδου εφαρμογές ασφάλειας. Έπειτα, έχουμε την σάρωση της υπογραφής. Αυτή είναι γνωστή και ως Δυναμική Εξακρίβωση Υπογραφής. Επειδή 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 δύσκολο έως αδύνατο, να αντιγράψει τον τρόπο με τον οποίο το άτομο αυτό υπογράφει. Ακόμα και αν η υπογραφή είναι τέλεια σχεδιασμένη, η ταχύτητα, η δύναμη και η πίεση θα διαφέρουν. Η σάρωση της υπογραφής δεν τυγχάνει ακόμη ευρείας χρήσεως, αναμένεται όμως πολύ σύντομα να βοηθήσει στην πιστοποίηση επίσημων εγγράφων. Τέλος, αναφέρουμε την σάρωση πατήματος πλήκτρου που είναι γνωστή και ως ρυθμός δακτυλογράφησης. Η μέθοδος αυτή, εξετάζει τον τρόπο με τον οποίο ένα άτομο δακτυλογραφεί ή πιέζει τα πλήκτρα σε ένα πληκτρολόγιο. Τα χαρακτηριστικά που αναλύονται είναι η δύναμη, η ταχύτητα, η συχνότητα λάθους, ο συνολικός χρόνος δακτυλογράφησης ενός συγκεκριμένου συνθηματικού και ο χρόνος που μεσολαβεί από το πάτημα ενός συγκεκριμένου πλήκτρου ως το πάτημα ενός άλλου.

Χρήση λογισμικού ασφαλείας

Η χρήση πακέτων λογισμικού κατά τον σχεδιασμό της ασφάλειας ενός συστήματος, αποτελεί πρωταρχική μέριμνα των διαχειριστών των συστημάτων. Οι πιο διαδεδομένες εφαρμογές είναι τα antivirus και τα firewalls. Σχετικά με το λογισμικό antivirus , όπως έχει αποδειχθεί από πολλές έρευνες, η διασπορά ιών είναι η πιο διαδεδομένη μορφή επιθέσεων στο Διαδίκτυο. Καθημερινά, δημιουργούνται χιλιάδες νέοι ιοί, που απειλούν, ποικιλοτρόπως, τα υπολογιστικά συστήματα. Η πιο σημαντική μέθοδος αντιμετώπισης των ιών είναι η χρήση αντιβιοτικών προγραμμάτων (antivirus, software).Το λογισμικό αντιμετώπισης ιών, είναι ένα από τα πιο πολύπλοκα εργαλεία λογισμικού. Ένα τέτοιο λογισμικό, επιτελεί τρεις βασικές λειτουργίες. Πρώτη και βασική είναι η ανίχνευση του συστήματος, για να εξακριβωθεί, αν έχει μολυνθεί από ιούς. Η διαδικασία αυτή, μπορεί να γίνει είτε κατόπιν ενέργειας του χρήστη, που επιλέγει μέσω του λογισμικού τον έλεγχο του σκληρού του δίσκου για ιούς, είτε, όπως συμβαίνει με τα σύγχρονα λογισμικά, πραγματοποιείται αυτόματα ,καθώς, το λογισμικό φορτώνεται στη μνήμη RAM του συστήματος και ελέγχει όλες τις εφαρμογές που εκτελούνται. Στη συνέχεια, εάν το σύστημά μας έχει προσβληθεί από κάποιο ιό, το λογισμικό θα μας ενημερώσει για την ταυτότητά του. Η δυνατότητα αυτή είναι πολύ σημαντική ,γιατί μας επιτρέπει να εκτιμήσουμε το μέγεθος της ζημιάς που έχει προκληθεί, όσο και να εκτελέσουμε τις απαραίτητες ενέργειες ,για την αποκατάσταση της ομαλής λειτουργίας του συστήματος. Στο τρίτο και τελευταίο στάδιο, αφού έχουν εντοπιστεί οι ιοί που μόλυναν το σύστημα ,θα πρέπει να αφαιρεθούν. Τα περισσότερα λογισμικά, όταν έχουν εντοπίσει έναν ιό, προτείνουν στον χρήστη τι ακριβώς πρέπει να κάνει. Οι πιο συνηθισμένες επιλογές είναι τρεις. Αρχικά, να επιδιορθώσει το αρχείο που έχει μολυνθεί με τον ιό, να θέσει το αρχείο σε καραντίνα, ώστε να μην μπορεί να χρησιμοποιηθεί και μετά, να διαγράψει το αρχείο.

Μέθοδοι εντοπισμού ιών

Η βασικότερη λειτουργία ενός λογισμικού αντιμετώπισης ιών, είναι ο εντοπισμός των ιών. Λόγω

καθημερινής δημιουργίας νέων ιών με ιδιαίτερα χαρακτηριστικά, 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 που προγράμματος με τους νέους ιούς, προκειμένου να είναι δυνατός ο εντοπισμός και η απομάκρυνσή τους. Κάθε ιός είναι διαφορετικός. Το στοιχείο που τον κάνει μοναδικό ονομάζεται αποτύπωμα ή υπογραφή του ιού. Στη βάση δεδομένων ενός προγράμματος antivirus, τηρείται μια 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.

Προηγμένες δυνατότητες εφαρμογών antivirus

Το μεγαλύτερο μειονέκτημα των εφαρμογών antivirus , είναι ότι για να εντοπιστεί ένας ιός θα πρέπει, πρωταρχικά, να έχει ενημερωθεί η Β.Δ. του προγράμματος με την υπογραφή του. Οι εταιρείες λογισμικού έχουν βελτιώσει, κατά πολύ, τη διαδικασία αυτή και μόλις λίγες ώρες μετά την εμφάνιση ενός νέου ιού ενημερώνουν άμεσα ,τις βάσεις τους με το απαιτούμενο λογισμικό απομάκρυνσής του. Όμως, μέσα σε αυτό το μικρό, σχετικά, χρονικό διάστημα, ο ιός ,θα έχει προλάβει να προξενήσει ζημιά σε αρκετές χιλιάδες υπολογιστές. Για το λόγο αυτό, οι εταιρείες λογισμικού αναζητούν νέες τεχνικές και μεθόδους για την αντιμετώπιση των προβλημάτων αυτών. Οι σχετικές τεχνολογίες ,που τυγχάνουν ευρείας ανάπτυξης τα τελευταία χρόνια, είναι η ευρετική ανάλυση και ο έλεγχος ακεραιότητας. Ειδικότερα, κατά τη χρήση ευρετικής ανάλυσης το πρόγραμμα δεν αναζητά τις υπογραφές των ιών, αλλά, ελέγχει τα εκτελέσιμα αρχεία και προσπαθεί να προσδιορίσει ,αν στον κώδικά τους περιέχεται εντολή ή εντολές, οι οποίες πιθανώς να αποτελούν ιούς .Τα ποσοστά επιτυχίας ,με τη χρήση της μεθόδου αυτής ,ανέρχονται στο 60% με 90%. Το μεγάλο πλεονέκτημα είναι ότι στην περίπτωση αυτή, δεν απαιτείται η ενημέρωση της Β.Δ. του προγράμματος ,ενώ ,αν υπάρχει η δυνατότητα εφαρμογής και των δυο τεχνικών τότε έχουμε ακόμη μεγαλύτερη προστασία. Όσο αφορά στον έλεγχο ακεραιότητας, είναι μια τεχνική που χρησιμοποιείται για την ανίχνευση μόνο των ιών , χωρίς να δίνει τη δυνατότητα προσδιορισμού της ταυτότητάς τους. Η τεχνική αυτή ολοκληρώνεται σε δύο στάδια. Στο πρώτο ,για κάθε αρχείο του συστήματος υπολογίζεται ένα άθροισμα ελέγχου. Το άθροισμα αυτό είναι ένας αριθμός , που προσδιορίζει μοναδικά ένα αρχείο, ενώ , κάθε τροποποίηση, έστω και ενός bit του αρχείου προκαλεί μεταβολή του αθροίσματος. Τα αθροίσματα αυτά αποθηκεύονται σε μια βάση δεδομένων. Στο δεύτερο στάδιο, γίνεται επανυπολογισμός των αθροισμάτων και αυτά συγκρίνονται με τα περιεχόμενα της βάσης δεδομένων. Εφόσον διαπιστωθεί διαφορά, πιθανολογείται ότι αυτή οφείλεται στην επίδραση ενός ιού.

Κριτήρια επιλογής λογισμικού ανίχνευσης ιών

Σήμερα, στην παγκόσμια αγορά, κυκλοφορούν πολλά πακέτα λογισμικού ανίχνευσης ιών. Τα κριτήρια, με τα οποία θα επιλέξουμε το λογισμικό, εξαρτάται από τις ανάγκες που θέλουμε να καλύψουμε. Οι βασικότερες προϋποθέσεις είναι οι ακόλουθες. Καταρχάς, να έχει εύχρηστο Interface και χαμηλή κατανάλωση πόρων, η προστασία να γίνεται σε πραγματικό χρόνο, η ενημέρωση να είναι αυτόματη, να υπάρχει προστασία ηλεκτρονικής αλληλογραφίας και προγραμματισμένος έλεγχος, δισκέτα εκκίνησης καθώς και καταγραφή συμβάντων.

## Firewalls

Ο όρος firewall ,είχε αρχικά χρησιμοποιηθεί από τις κατασκευαστικές εταιρείες, για να προσδιορίσουν τον τοίχο που χτιζόταν σε ένα κτίριο, ο οποίος, χώριζε δυο σημεία με σκοπό ,σε περίπτωση πυρκαγιάς ,να μην επεκταθεί η φωτιά. Ο όρος ,επίσης ,χρησιμοποιήθηκε για να περιγράψει τα περιβλήματα στα ντεπόζιτα καυσίμων και αγωνιστικών αυτοκινήτων ,τα οποία εμπόδιζαν τη διείσδυση της φωτιάς στα καύσιμα. Στην επιστήμη των υπολογιστών , ο όρος firewall προσδιορίζει μία συσκευή ή εργαλείο λογισμικού, 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>> δίκτυο , από ένα εξωτερικό μη ασφαλές δίκτυο ,όπως το Internet. Τα περισσότερα firewalls επιτελούν δύο βασικές λειτουργίες ασφαλείας . Η πρώτη αφορά το φιλτράρισμα των πακέτων, το οποίο βασίζεται στο να επιτρέπει ή να απαγορεύει την κίνηση των πακέτων που διακινούνται στο δίκτυο , με βάση την υιοθετούμενη πολιτική ασφαλείας. Η δεύτερη έχει να κάνει με τις πύλες εφαρμογών ,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 δύο. Η πολιτική προκαθορισμένης άδειας χρήσης όπου η κυκλοφορία πακέτων και η εκτέλεση εφαρμογών επιτρέπεται ελεύθερα ,εκτός των περιπτώσεων που υπάρχει ρητή απαγόρευση. Η άλλη πολιτική είναι αυτή της προκαθορισμένης απαγόρευσης της χρήσης, στην οποία το firewall ρυθμίζεται ,έτσι ,ώστε, να μην επιτρέπει καμιά κυκλοφορία πακέτων και καμία 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.

Βασικές τεχνικές προστασίας με χρήση firewalls

Με την ραγδαία ανάπτυξη του ηλεκτρονικού εγκλήματος , η χρήση των firewalls είναι περισσότερο αναγκαία από ποτέ. Η τεχνολογία, στο συγκεκριμένο τομέα ,αναπτύσσεται με γοργούς ρυθμούς και έχουν δημιουργηθεί firewalls, τα οποία επιτελούν πολλές εργασίες ταυτόχρονα. Επιχειρώντας ένα διαχωρισμό των firewalls , με κριτήριο την χρησιμοποιούμενη τεχνική ,μπορούμε να διακρίνουμε τρεις βασικές τεχνικές προστασίας . Η πρώτη είναι οι πύλες φιλτραρίσματος των πακέτων ,η δεύτερη οι πύλες εφαρμογών και η τελευταία οι υβριδικές πύλες. Η πρώτη τεχνική προστασίας είναι η πιο απλή τεχνική , που χρησιμοποιείται στα firewalls. Όλα τα πακέτα που διακινούνται στο δίκτυο και διέρχονται από το firewall φιλτράρονται ,με βάση κάποιους προκαθορισμένους κανόνες ,που τίθενται από το διαχειριστή. Οι επιλογές είναι δύο. Είτε να επιτραπεί η διέλευση του πακέτου ,είτε να απορριφθεί .Οι παράμετροι , που προσδιορίζουν τα κριτήρια επιλογής των πακέτων που θα εισέλθουν ή εξέλθουν είναι η διεύθυνση IP του αποστολέα και του παραλήπτη ,με δυνατότητα ομαδοποίησης των διευθύνσεων με τη χρήση μάσκας, η θυρίδα (port) προέλευσης και προορισμού και το χρησιμοποιούμενο πρωτόκολλο επικοινωνίας. Το μεγαλύτερο μειονέκτημα των firewall , που χρησιμοποιούν την τεχνική αυτή, είναι ότι το περιεχόμενο των IP- πακέτων δεν λαμβάνεται 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 του πακέτου. Οι πύλες εφαρμογών λειτουργούν στο υψηλότερο στρώμα επικοινωνίας , γνωστό και ως επίπεδο εφαρμογής. Κύριο χαρακτηριστικό των πυλών εφαρμογής είναι η ύπαρξη μιας υπηρεσίας διαμεσολάβησης ,που πραγματώνεται με τη χρήση ενός πακέτου λογισμικού proxy server. Η υπηρεσία proxy έχει τη δυνατότητα να ενεργεί, ταυτόχρονα ,ως πελάτης και διακομιστής. Όσον αφορά στους εσωτερικούς χρήστες λειτουργεί ως διακομιστής ,ενώ, όσον αφορά στους εξωτερικούς, λειτουργεί ως πελάτης. Το λογισμικό αυτό παρεμβάλλεται μεταξύ των πρωτοκόλλων επικοινωνίας και εκεί έχει ως βασικό σκοπό ,τον έλεγχο των επικοινωνιών. Για παράδειγμα, ένας εξωτερικός χρήστης για να αποκτήσει πρόσβαση σε μια υπηρεσία του προστατευόμενου δικτύου, θα πρέπει πρώτα να συνδεθεί με την proxy εφαρμογή, η οποία θα προβεί στην αναγνώριση και πιστοποίησή του και έπειτα, θα του επιτρέψει την πρόσβαση στην υπηρεσία που ζήτησε. Η αντίστροφή διαδικασία πραγματοποιείται, όταν ένας εσωτερικός χρήστης αιτείται τη χρήση μιας εξωτερικής υπηρεσίας. Με τον τρόπο αυτό ,οι πύλες εφαρμογών ελέγχουν και το περιεχόμενο των πακέτων που δρομολογούνται , όχι μόνο τις επικεφαλίδες ,γι' αυτό και έχουν τη δυνατότητα να αποτρέπουν επιθέσεις IP και DSN spoofing. Σε σχέση, όμως, με τις πύλες φιλτραρίσματος πακέτων υστερούν στην ταχύτητα. Τα firewalls όμως που τείνουν να επικρατήσουν σήμερα, είναι τα υβριδικά. Συνδυάζουν την ταχύτητα ελέγχου , που προσφέρουν οι πύλες φιλτραρίσματος και την αξιοπιστία των πυλών εφαρμογής. Ακόμη και τα καθαρά proxy firewalls διαθέτουν λογισμικό, που λειτουργεί ως πύλη φιλτραρίσματος πακέτων. Η νεότερη 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.

Κρυπτογραφία και Ασφάλεια

Η κρυπτογραφία αποτελεί μέρος της κρυπτολογίας, 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[32], είναι η επιστήμη που τους μαθηματικούς μετασχηματισμούς για την εξασφάλιση της ασφάλειας της πληροφορίας. Οι βασικότεροι στόχοι της κρυπτογραφίας στη 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 την αντίθετη διαδικασία , δηλαδή την αποκρυπτογράφηση, ο γρίφος αυτός επανέρχεται στην αρχική του μορφή και η

[32] http://www.wikipedia.gr

πληροφορία ,μπορεί να αναγνωριστεί. Η κρυπτογραφία, ως επιστήμη, είναι γνωστή από την αρχαιότητα. Τα πρώτα κρυπτογραφικά συστήματα βασίζονταν στη χρήση κωδικών συμβόλων, αντί, για τα σύμβολα της αλφάβητου. Τα βασικά στοιχεία που αποτελούν ένα σύγχρονο σύστημα κρυπτογράφησης είναι τέσσερα. Καταρχάς, υπάρχει το αρχικό μήνυμα, έπειτα το κρυπτογραφικό σύστημα , το οποίο αποτελείται από έναν αλγόριθμο κρυπτογράφησης και έναν αλγόριθμο αποκρυπτογράφησης. Τρίτο στοιχείο είναι το κρυπτογραφημένο κείμενο, το οποίο αποτελεί τα αποτέλεσμα της εφαρμογής του αλγορίθμου κρυπτογράφησης στο αρχικό μήνυμα , πριν αυτό σταλεί στον παραλήπτη. Και το τελευταίο στοιχείο είναι ένα κλειδί, το οποίο είναι μια συμβολοσειρά , η οποία χρησιμοποιείται από τους αλγόριθμους στη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης .
Από τεχνικής απόψεως , η κρυπτογραφία διακρίνεται σε δυο βασικές κατηγορίες που είναι η συμμετρική κρυπτογραφία, στην οποία χρησιμοποιείται ένα ιδιωτικό κλειδί και η ασύμμετρη κρυπτογραφία, στην οποία χρησιμοποιούνται δυο κλειδιά, ένα δημόσιο και ένα ιδιωτικό .Στην συμμετρική ,το βασικό χαρακτηριστικό είναι ότι χρησιμοποιείται το ίδιο κλειδί, τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση των δεδομένων. Βασική προϋπόθεση αποτελεί, το κλειδί να έχει δοθεί στους χρήστες ,που επιθυμούν να επικοινωνήσουν ,μέσω ενός ασφαλούς καναλιού επικοινωνίας. Η διαδικασία επικοινωνίας έχει ως ακολούθως. 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. Στην ασύμμετρη κρυπτογράφηση των δεδομένων, χρησιμοποιείται ένα κλειδί για την κρυπτογράφηση των δεδομένων και ένα διαφορετικό κλειδί για την αποκρυπτογράφηση. Κύριο χαρακτηριστικό των κλειδιών αυτών είναι ότι αν και σχετίζονται 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 η 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 συμμετρική και, επιπλέον ,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 δε αποκρυπτογράφηση γίνεται με το ιδιωτικό κλειδί που μόνο αυτός κατέχει. Το πρόβλημα της μεθόδου αυτής είναι ότι, απαιτούνται πολύ μεγαλύτερα κλειδιά απ' ότι στη συμμετρική κρυπτογράφηση για τον ίδιο βαθμό ασφαλείας. Χρησιμοποιώντας τη συμμετρική κρυπτογραφία λίγο διαφορετικά, μπορούμε να πετύχουμε την ταυτοποίηση του αποστολέα ενός μηνύματος. Στην περίπτωση αυτή, ο αποστολέας κρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί .Το μήνυμα μπορεί να αποκρυπτογραφηθεί μόνο με το δημόσιο κλειδί , που μπορεί να το έχει οποιοσδήποτε ,αλλά η αρχική κρυπτογράφηση με το ιδιωτικό κλειδί , που συνηθίζει να λέγεται ψηφιακή υπογραφή , προσδιορίζει και μοναδικά τον αποστολέα αυτού. Όπως προαναφέρθηκε, στη συμμετρική κρυπτογράφηση , το πρόβλημα είναι η εύρεση ασφαλούς καναλιού επικοινωνίας για την ανταλλαγή των μυστικών κλειδιών ,ενώ στην ασύμμετρη ,απαιτούνται μεγαλύτερα κλειδιά που καθιστούν τη διαδικασία κρυπτογράφησης-αποκρυπτογράφησης χρονοβόρα. Για την υπερκέραση των προβλημάτων αυτών, έχει επικρατήσει ένα υβριδικό σύστημα το οποίο φέρει στοιχεία και από τις δυο μεθόδους .Ειδικότερα, χρησιμοποιείται αρχικά, η ασύμμετρη κρυπτογραφία, για να γίνει 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.

## Διαχείριση δημοσίων κλειδιών –πιστοποιητικά

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 χρησιμοποιεί 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, εισάγοντας τη δυνατότητα διακρίβωσης για τα δημόσια κλειδιά μέσω μιας τρίτης οντότητας , την οποία εμπιστεύονται και τα δύο μέρη .Η τρίτη οντότητα, που καλείται επίσης αρχή πιστοποίησης ,υπογράφει με το δικό της ιδιωτικό κλειδί τα δημόσια κλειδιά και τα αντίστοιχα ονόματα ,προσθέτοντας επιπλέον κάποια στοιχεία. Το κομμάτι αυτό των δεδομένων , που έχει υπογραφεί από την αρχή πιστοποίησης , ονομάζεται πιστοποιητικό. Το πιστοποιητικό μπορεί να επαληθευτεί,

χρησιμοποιώντας το δημόσιο κλειδί της αρχής πιστοποίησης.

Επιθέσεις σε συστήματα κρυπτογράφησης

Η χρήση της κρυπτογράφησης οδήγησε στην ανάπτυξη μιας σχετικά παράλληλης, αλλά , αντίθετης επιστήμης, της κρυπτανάλυσης , που ασχολείται με την αποκρυπτογράφηση κειμένου. Οι μέθοδοι και οι τεχνικές της κρυπτανάλυσης αποτελούν τα βασικά εργαλεία των επιτιθέμενων , έναντι των συστημάτων κρυπτογράφησης. Πολύ σημαντικό ρόλο διαδραματίζει το υλικό, που 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, που απαιτείται από έναν κρυπταναλυτή για να βρει το κλειδί. Όσο περισσότερος κόπος ,αλλά και χρόνος απαιτείται για την εύρεση ενός κλειδιού σε ένα κρυπτογραφικό σύστημα ,τόσο ασφαλέστερο θεωρείται .Οι αλγόριθμοι κρυπτογράφησης μπορούν πολύ δύσκολα να σπάσουν. Όμως, αν υπάρχει αρκετός χρόνος και υπομονή, ένα πρόγραμμα ,που θα δοκιμάζει 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 διεκπεραίωσή 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. Η κρυπτογράφηση χρησιμοποιείται ευρέως για την ασφάλεια των ηλεκτρονικών συναλλαγών. Τα πρωτόκολλα SSL, PNG και SET, αποτελούν τις πιο διαδεδομένες εφαρμογές της κρυπτογραφίας στον τομέα αυτό.

Φυσική Ασφάλεια

Ένας από τους πιο σημαντικούς τομείς , που αφορά την ασφάλεια του πληροφοριακού συστήματος ενός οργανισμού, είναι η φυσική ασφάλεια. Οι περισσότεροι οργανισμοί , κατά την κατάρτιση της πολιτικής ασφαλείας τους, έχουν την τάση να παραμελούν τον πολύ σημαντικό αυτό τομέα ,θεωρώντας τον δευτερεύοντα, κυρίως διότι το κόστος είναι αρκετά υψηλό. Οι διαχειριστές των δικτύων θέτουν ,ως πρώτη προτεραιότητα, τον εξοπλισμό του οργανισμού, με σύγχρονο και εξελιγμένο υλικό και λογισμικό ,αγνοώντας ότι οι διακομιστές , οι δρομολογητές ,τα καλώδια των δικτύων και τόσες ακόμη συσκευές κινδυνεύουν από απ' ευθείας προσβολή. Με τον όρο φυσική ασφάλεια, αναφερόμαστε σε όλα εκείνα τα μέτρα , που είναι απαραίτητο να ληφθούν ,προκειμένου, να προστατευθεί η φυσική υπόσταση των συσκευών που απαρτίζουν έναν υπολογιστή ή ένα δίκτυο υπολογιστών. Όσο και αν προστατεύουμε ένα διακομιστή με εργαλεία λογισμικού , θα έχουμε αποτύχει πλήρως, αν κάποιος εισβολέας καταφέρει να φτάσει στη φυσική τοποθεσία όπου αυτός φυλάσσεται και να αφαιρέσει το σκληρό δίσκο ,που περιέχει όλα τα ευαίσθητα και σημαντικά δεδομένα του οργανισμού. Ο τομέας της φυσικής ασφάλειας , που παραμελείται περισσότερο από όλους, είναι 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 αποσοβήσουν τους κινδύνους αυτούς. Εκτός όμως από τους ηλεκτρονικούς υπολογιστές ,ιδιαίτερη σημασία, πρέπει να δίνεται και στον βοηθητικό εξοπλισμό .Για παράδειγμα, τα καλώδια είναι δυνατό να κινδυνεύσουν από απευθείας παρέμβαση, η οποία μπορεί να στοχεύει είτε στην καταστροφή του δικτύου είτε στην παρεμβολή συσκευών για την υποκλοπή δεδομένων. Επίσης, οι αφαιρούμενες αποθηκευτικές μονάδες, καθώς και τα δεδομένα που τυπώνονται ,δύναται να περιέχουν σημαντικές πληροφορίες για την ασφάλεια του συστήματος, γι' αυτό πρέπει να προστατεύονται με την ίδια επιμέλεια. Τέλος, οι μέθοδοι και τα συστήματα αυθεντικοποίησης μπορούν, επίσης, να χρησιμοποιηθούν για την φυσική ασφάλεια του εξοπλισμού. Ένα σύστημα αναγνώρισης φωνής ή ίριδας ,μπορεί να εμποδίσει την μη εξουσιοδοτημένη πρόσβαση ατόμων στους χώρους όπου φυλάσσονται οι διακομιστές ενός δικτύου ή άλλα ευπαθή μέρη του εξοπλισμού.

Ανίχνευση επιθέσεων

Τα μέτρα πρόληψης, που προαναφέρθηκαν ,έχουν ως σκοπό την αποτροπή μιας επίθεσης έναντι της

ασφάλειας ενός συστήματος και την παρεμπόδιση εκδήλωσής της. Στην περίπτωση που ο επιτιθέμενος καταφέρει να παραβιάσει τα μέτρα πρόληψης ,το σύστημα θα πρέπει να έχει τη δυνατότητα να εντοπίσει την επίθεση, προκειμένου ,να επιχειρήσει είτε να την αποτρέψει είτε να προβεί στην αποκατάσταση του συστήματος. Για την ανίχνευση μιας επίθεσης, χρησιμοποιούνται τα Συστήματα Ανίχνευσης Επιθέσεων (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. Αυτά είναι της ανίχνευσης ανωμαλιών, των υπογραφών και το υβριδικό μοντέλο. Αναφορικά με τα συστήματα ανίχνευσης ανωμαλιών, αυτά αυτοεκπαιδεύονται , υπό την έννοια ότι καταγράφουν ροές και διαδικασίες δεδομένων προσπαθώντας να κάνουν ένα είδος τυποποίησης. Οι τυποποιημένες αυτές διαδικασίες, χρησιμοποιούνται για να εντοπίσουν ανωμαλίες, που πιθανώς θα αποτελούν εισβολή ,σύμφωνα με τα όσα έχουν ήδη καταγραφεί. Κατά την ανίχνευση ανωμαλιών, υπάρχει η δυνατότητα να καταγράφονται δραστηριότητες , που ξεφεύγουν πέραν των συνηθισμένων, που έχουν, νομίμως, δοθεί σε μια ομάδα χρηστών. Για τη δημιουργία του γνωστικού τους περιεχομένου, τα συστήματα της κατηγορίας αυτής, χρησιμοποιούν ευρετικές μεθόδους, αξιοποιώντας με στατιστικά κριτήρια τα δεδομένα του συστήματος. Κατά συνέπεια, υπάρχει η πιθανότητα τα συστήματα, εφόσον δεν έχουν ρυθμιστεί κατάλληλα, να δίνουν λάθος συναγερμούς ή στην αντίθετη περίπτωση να μην εντοπίζουν μια επίθεση. Το κρίσιμο σημείο ισορροπίας πάνω ή κάτω από το οποίο , το σύστημα αποφαίνεται θετικά ή αρνητικά είναι υποκειμενικό, στηρίζεται στην πολιτική ασφάλειας και στην έμπνευση του διαχειριστή , για το λόγο αυτό η σχετική τεχνολογία θεωρείται ότι θα ωριμάσει έπειτα από πολλά χρόνια.
Αναφορικά με την ανίχνευση υπογραφών , τα συστήματα αυτά στηρίζονται στο γεγονός, ότι για κάθε επίθεση υφίσταται μια μοναδική μέθοδος ή υπογραφή η οποία και μπορεί να εντοπιστεί. Έστω και αν υπάρχει μια μικρή διαφορά, μεταξύ δυο υπογραφών και πάλι υπάρχει δυνατότητα εντοπισμού. Για την ταυτοποίηση των υπογραφών, απαιτείται μια βάση δεδομένων, στην οποία θα αποθηκεύονται οι υπογραφές των επιθέσεων, προκειμένου να υπάρχει η δυνατότητα σύγκρισης. Η λειτουργία των συστημάτων ανίχνευσης επιθέσεων της κατηγορίας αυτής, μπορεί να παρομοιαστεί με τη λειτουργία ενός λογισμικού ανίχνευσης ιών, καθώς απαιτείται ενημερωμένη βάση δεδομένων για να εντοπιστούν νέες επιθέσεις. Εφόσον η βάση των υπογραφών δεν είναι ενημερωμένη, δεν μπορεί να εντοπιστεί μια νέα μορφή επίθεσης. Σχετικά με το υβριδικό μοντέλο ανίχνευσης επιθέσεων, αναφέρουμε ότι λόγω των μειονεκτημάτων , που παρουσιάζουν τα προαναφερθέντα συστήματα, αρχίζουν να αναπτύσσονται υβριδικά μοντέλα, τα οποία και δανείζονται χαρακτηριστικά από ήδη υπάρχοντα. Η τεχνολογία των υβριδικών μοντέλων βρίσκεται ακόμη σε πρώιμο στάδιο. Περαιτέρω ,τα συστήματα ανίχνευσης επιθέσεων ,ανάλογα με το μέσο που παρακολουθούν ,μπορούμε να το διακρίνουμε σε συστήματα που συλλέγουν πληροφορίες από το δίκτυο (Network based IDS), σε αυτά που τις συλλέγουν από υπολογιστές(Host based IDS) και σε εκείνα που συλλέγουν πληροφορίες από εφαρμογές(Application Based IDS).Τα πρώτα συστήματα παρακολουθούν την κίνηση στο δίκτυο , με σκοπό να εντοπίσουν επιθέσεις. Είναι υπεύθυνα ,για τον εντοπισμό ανωμαλιών, δυσλειτουργιών, καθώς και δεδομένων, που πιθανώς να είναι κακόβουλα και επιβλαβή για το δίκτυο. Αν και εκ πρώτης όψεως, τα συστήματα αυτά θυμίζουν τα firewalls υπάρχουν σημαντικές διαφορές μεταξύ τους, με σημαντικότερη ότι τα ΣΑΕ λειτουργούν παθητικά, απλά παρακολουθούν την κίνηση στο δίκτυο και δεν επεμβαίνουν για να την διακόψουν ή αλλοιώσουν. Για το λόγο αυτό, είναι πολύ δύσκολο να εντοπιστούν από τον επιτιθέμενο ,σε αντίθεση με τα firewalls.Στη συνέχεια, σχετικά με τη δεύτερη κατηγορία συστημάτων, η δημιουργία τους προήλθε από την ανάγκη επιτήρησης μεμονωμένων υπολογιστών , που βρίσκονται στο εσωτερικό δίκτυο ενός οργανισμού. Οι απειλές έναντι της ασφάλειας ενός συστήματος δεν είναι μόνο εξωτερικές ,αλλά, και εσωτερικές προερχόμενες από τους ίδιους τους υπαλλήλους και χρήστες των συστημάτων του οργανισμού. Τα συστήματα αυτά ,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 υπεισέλθει κακόβουλη δραστηριότητα. Η τελευταία κατηγορία αποτελεί μια 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. Η χρήση των συστημάτων αυτών ,είναι λιγότερο συχνή από τις ανωτέρω δυο κατηγορίες. Προτιμούνται όταν θέλουμε να προστατεύσουμε μια πολύ σημαντική εφαρμογή ,όπως για παράδειγμα μια βάση δεδομένων με σημαντικές πληροφορίες.

Η αντίδραση των ΣΑΕ σε μια επίθεση

Ένα σύστημα ανίχνευσης επιθέσεων δεν περιορίζεται , μόνο, στην παρακολούθηση ενός δικτύου ή υπολογιστή. Όταν αντιληφθεί μια επίθεση, εκτελεί σε μια σειρά από εντολές ,ανάλογα με τις ρυθμίσεις που έχει επιλέξει ο διαχειριστής. Τις αντιδράσεις των ΣΑΕ μπορούμε να τις διακρίνουμε σε δύο κατηγορίες. Οι πρώτες είναι οι ενεργητικές .Όταν το σύστημα εμποδίσει μια επίθεση , προβαίνει σε μια σειρά από ενέργειες για την παρεμπόδισή της. Κάθε επίθεση και ο πιθανός κίνδυνος αξιολογείται. Όταν 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 , για να αποτρέψει την είσοδο του επιτιθέμενου στο δίκτυο. Έπειτα, υπάρχουν και οι παθητικές αντιδράσεις, όπου το ΣΑΕ δεν προβαίνει σε καμιά ενέργεια. Ειδοποιεί το διαχειριστή ή υπεύθυνο ασφαλείας του συστήματος ότι υπάρχει πρόβλημα. Και στην περίπτωση αυτή, γίνεται αξιολόγηση της σοβαρότητας της επίθεσης και τα μέσα και τρόποι ειδοποίησης του διαχειριστή εξαρτώνται άμεσα από τον παράγοντα αυτό.

Ειδικές κατηγορίες ΣΑΕ

Εκτός των βασικών κατηγοριών ΣΑΕ , υπάρχουν και επιμέρους συστήματα , τα οποία λόγω της απλότητας λειτουργίας τους, θα μπορούσαμε να τα ονομάσουμε εργαλεία ανίχνευσης εισβολών. Συγκεκριμένα υπάρχουν τα συστήματα ελέγχου ακεραιότητας (System Integrity Verifiers). Αυτά, παρακολουθούν κρίσιμα αρχεία ,όπως τα αρχεία συστήματος , προκριμένου να εντοπίσουν τυχόν μεταβολές. Έχουν ,επίσης, τη δυνατότητα να παρακολουθούν τους λογαριασμούς των χρηστών και να εντοπίζουν ,εάν κάποιος απλός χρήστης έχει αποκτήσει δικαιώματα διαχειριστή. Επίσης, έχουμε τα συστήματα παρακολούθησης αρχείων καταγραφής (Log File Monitors), τα οποία ,αρχικά, δημιουργούν έναν 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. Τέλος, υπάρχουν και τα honeypots, τα οποία είναι συστήματα εικονικά, που προσπαθούν να ξεγελάσουν τον επιτιθέμενο, δίνοντάς του την εντύπωση ότι είναι πολύ εύκολο να εισβάλει στο σύστημα. Όταν πραγματοποιηθεί η εισβολή ,το σύστημα θα έχει καταγράψει όλες τις μεθόδους και τεχνικές που χρησιμοποίησε ο επιτιθέμενος.

Έλεγχος (audit) συστημάτων

Ο έλεγχος των αρχείων καταγραφής (log files) του συστήματος, μπορεί να αποβεί πολύ σημαντικός και να βοηθήσει στον εντοπισμό μιας επίθεσης. Τα εργαλεία ελέγχουν υπάρχουν σε κάθε λειτουργικό σύστημα. Στις επαγγελματικές εκδόσεις των πρόσφατων λειτουργικών συστημάτων της Microsoft υπάρχουν τα ακόλουθα τρία βασικά αρχεία καταγραφής. Αρχικά, είναι τα application log, τα οποία περιέχουν μηνύματα, πληροφορίες κατάστασης και άλλα γεγονότα που αναφέρονται από μη ζωτικές υπηρεσίες των WINDOWS. Ακολούθως, υπάρχουν τα 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. Έπειτα, υπάρχει το security log, στο οποίο καταγράφονται αρχεία που σχετίζονται με την πολιτική ελέγχου που έχει καθοριστεί από το διαχειριστή του λειτουργικού συστήματος. Το τι θα παρακολουθείται και τι όχι είναι υποκειμενικό και υπόκειται σε μεταβολές. Ένας καλός διαχειριστής πρέπει να βρει τη χρυσή τομή και να παρακολουθεί μόνο τα δεδομένα και τις διαδικασίες που απαιτούνται για την επίτευξη του σκοπού του. Εξάλλου, το να παρακολουθούμε τα πάντα είναι ισοδύναμο με το να μην παρακολουθούμε τίποτα, καθώς εάν έχουμε να ελέγξουμε ένα τεράστιο πλήθος πληροφοριών από αρχεία και διαδικασίες ,πιθανώς δε θα μπορέσουμε να εντοπίσουμε το πρόβλημα .

Αντιμετώπιση καταστροφών από επιθέσεις

Στην περίπτωση που αποτύχουμε είτε να αποτρέψουμε είτε να αντιμετωπίσουμε μια επίθεση, ο επιτιθέμενος, προφανώς, θα προκαλέσει κάποιου είδους ζημιά, όπως απώλεια πληροφοριών και δεδομένων ή καταστροφή του συστήματος. Η απώλεια δεδομένων ενός οργανισμού μπορεί να έχει απρόβλεπτες συνέπειες και να οδηγήσει σε ολοκληρωτική οικονομική καταστροφή. Για τους λόγους αυτούς, είναι απαραίτητο ο κάθε οργανισμός , αλλά και κάθε μεμονωμένος χρήστης που αποθηκεύει σημαντικά δεδομένα σε ένα υπολογιστικό σύστημα ,να έχει την προνοητικότητα να εξασφαλίσει ότι σε περίπτωση που δεχθεί οποιαδήποτε επίθεση ή ακόμη και υποστεί τις συνέπειες μιας φυσικής καταστροφής ,θα έχουν τηρηθεί σε ασφαλές μέρος εφεδρικά αρχεία, τα οποία θα αποτελούν μέρος ή και το σύνολο των αποθηκευμένων δεδομένων που χάθηκαν Για τη λήψη των εφεδρικών αντιγράφων (back-up files) χρησιμοποιούνται μια σειρά από τεχνικές. Οι σημαντικότερες από αυτές αναλύονται ακολούθως.

Κατά κύριο λόγο αναφέρουμε τα Συστήματα Ανάνηψης από Καταστροφές, τα οποία αποτελούν αναπόσπαστο κομμάτι της πολιτικής ασφάλειας κάθε μεγάλου οργανισμού. Ένα σύστημα ανάνηψης από καταστροφές αποτελείται από αρκετά υποσυστήματα, τα οποία στοχεύουν στην εξασφάλιση της ακεραιότητας των δεδομένων του οργανισμού από διάφορους κινδύνους, που μπορεί να προκύψουν , όπως φυσικά φαινόμενα ,κακόβουλες επιθέσεις μέσω Διαδικτύου, σφάλματα υλικού και λογισμικού και λάθη χρηστών. Οι λειτουργίες ενός συστήματος ανάνηψης από καταστροφές είναι υποκειμενικές και εξαρτώνται από τις ανάγκες του οργανισμού. Τα κρίσιμα σημεία σχεδιασμού του συστήματος είναι το είδος των δεδομένων που θα αποθηκευτούν, κάθε πότε θα γίνεται η αποθήκευση και που θα αποθηκευτούν τα δεδομένα. Τα δεδομένα, που

θα αποθηκευτούν, εξαρτώνται από τις ανάγκες που θέλουμε να καλύψουμε, αλλά και από το κεφάλαιο που θα διαθέσουμε για την εργασία αυτή. Σε μικρές έως μεσαίες επιχειρήσεις αποθηκεύονται μόνο τα αρχεία ζωτικής σημασίας, σε μεγαλύτερες αποθηκεύεται το σύνολο των δεδομένων, ενώ μεγάλοι οργανισμοί αποθηκεύουν και περαιτέρω δεδομένα, όπως πληροφορίες συστήματος και εφαρμογών ή ρυθμίσεις δικτύου. Το χρονικό διάστημα που μεσολαβεί για την αποθήκευση των δεδομένων, εξαρτάται από μια σειρά από παράγοντες, όπως πόσο συχνά αλλάζουν τα δεδομένα, 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 μπορεί να γίνει η αποθήκευση των εφεδρικών αντιγράφων. Κατά την εξέταση των προηγούμενων παραγόντων και τη λήψη αποφάσεων , το κρίσιμο σημείο είναι αυτό μεταξύ των αναγκών, που θα πρέπει να καλυφθούν και του κόστους που απαιτείται για την κάλυψή τους. Η αποθήκευση των δεδομένων επηρεάζεται από το είδος του φυσικού μέσου αποθήκευσης και τη δυνατότητα για περαιτέρω διατήρησή του σε άρτια κατάσταση. Τα μέσα ,που χρησιμοποιούνται για την αποθήκευση εφεδρικών δεδομένων, ποικίλουν. Η αποθήκευση των δεδομένων μπορεί να γίνει σε μαγνητικά μέσα, όπως μαγνητικές ταινίες και σε άλλους τοπικούς ή απομακρυσμένους δίσκους. Αν υπάρχει οικονομική δυνατότητα ,μπορούν ν εγκατασταθούν εφεδρικοί υπολογιστές, στους οποίους θα γίνεται πλήρη αποθήκευση (disk mirroring) των δεδομένων που χρησιμοποιούνται στους βασικούς υπολογιστές.

Λήψη εφεδρικών αντιγράφων

Η λήψη εφεδρικών αντιγράφων αποτελεί, ένα μέρος του συστήματος ανάνηψης. Μια επιχείρηση ή ένας οργανισμός που αδυνατεί να διαθέσει τα κεφάλαια για την προμήθεια ενός πλήρους συστήματος ανάνηψης καταστροφών ,είναι απαραίτητο να εξασφαλίσει τα δεδομένα, με τη λήψη εφεδρικών αντίγραφων .Η διαδικασία αυτή, μπορεί να ολοκληρωθεί με τη χρήση διάφορων εφαρμογών, που κυκλοφορούν στο εμπόριο για το σκοπό αυτό. Κάθε εφαρμογή φέρει τα δικά της χαρακτηριστικά και μπορεί να χρησιμοποιηθεί για την κάλυψη διαφορετικών αναγκών. Για παράδειγμα ,η εφαρμογή snapshot, επιτρέπει την πλήρη αντιγραφή του σκληρού δίσκου χωρίς να απαιτείται ο τερματισμός του λειτουργικού συστήματος. Παράλληλα, είναι δυνατή η συνέχιση των εργασιών του χρήστη καθ' όλη την διάρκεια της αντιγραφής. Σε περίπτωση καταστροφής του πρωτότυπου δίσκου ,γίνεται πλήρης αποκατάσταση και ο νέος δίσκος περιέχει, ακριβώς ,τα δεδομένα που ήταν αποθηκευμένα στον παλαιό. Τη διαδικασία λήψης αντιγράφων ,μπορούμε να τη διακρίνουμε τρεις βασικές κατηγορίες, οι οποίες είναι η πλήρης λήψη αντιγράφων (full backup), κατά την οποία λαμβάνονται εφεδρικά αντίγραφα από όλα τα αρχεία του συστήματος, η λήψη τροποποιημένων αντιγράφων (incremental backup), κατά την οποία λαμβάνονται αντίγραφα μόνο από τα αρχεία, που έχουν τροποποιηθεί από την προηγούμενη χρονικά λήψη αντιγράφων και έχουμε και την λήψη διαφοροποιημένων αντιγράφων (differential backup), κατά την οποία γίνεται λήψη εφεδρικών αντιγράφων των αρχείων ,που έχουν διαφοροποιηθεί από την τελευταία πλήρη λήψη αντιγράφων ασφαλείας.

Άλλα θέματα που σχετίζονται με την ασφάλεια.

Ασφάλεια Ηλεκτρονικού Ταχυδρομείου

Το ηλεκτρονικό ταχυδρομείο είναι, αδιαμφισβήτητα, το πιο διαδεδομένο μέσο επικοινωνίας στο Διαδίκτυο. Οι επιθέσεις , με τη χρήση του ηλεκτρονικού ταχυδρομείου, αποτελούν καθημερινή πραγματικότητα. Τα ζητήματα ασφαλείας, που σχετίζονται με το ηλεκτρονικό ταχυδρομείο ανάγονται στις έννοιες της εμπιστευτικότητας ,της ακεραιότητας του μηνύματος και της αυθεντικοποίησης του αποστολές. Παράλληλα, το ηλεκτρονικό ταχυδρομείο γίνεται στόχος και άλλων επιθέσεων όπως άρνησης εξυπηρέτησης ,ενώ χρησιμοποιείται και για τη μετάδοση κακόβουλου λογισμικού. Τέλος, η μαζική αποστολή ανεπιθύμητων μηνυμάτων ,το λεγόμενο spamming αποτελεί επίσης ένα σημαντικό πρόβλημα. Για την αντιμετώπιση του προβλήματος των ιών ,απαιτείται η χρήση μιας εφαρμογής antivirus, η οποία ελέγχει όλα τα εισερχόμενα και εξερχόμενα μηνύματα. Παράλληλα, οι χρήστες δεν πρέπει να ανοίγουν επικίνδυνα συνημμένα αρχεία (κυρίως αυτά με καταλήξεις .exe,.bat,.dll, com) εφόσον δεν έχει ελεγχθεί από το antivirus και δεν έχει εξακριβωθεί η ταυτότητα του αποστολέα. Όσον αφορά την ενοχλητική αλληλογραφία, μερικοί βασικοί κανόνες ασφαλείας συνιστούν 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, τα οποία μπορούν να χρησιμοποιηθούν ,εφόσον υπάρχει σημαντικό πρόβλημα. Τα εργαλεία αυτά ρυθμίζονται ανάλογα με τις επιθυμίες του χρήστη.Τέλος, θα πρέπει να σημειωθεί ότι η επικοινωνία μέσω e-mail παρέχει ελάχιστη ασφάλεια, γι' αυτό και δεν πρέπει με το μέσο αυτό να διακινούνται ευαίσθητα δεδομένα, όπως αριθμοί πιστωτικών καρτών και λογαριασμών. Ειδικότερα, στους λογαριασμούς web-mail το πρόβλημα ασφαλείας είναι ακόμη εντονότερο, γι' αυτό και 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.

Ασφάλεια ηλεκτρονικών συναλλαγών

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, σήμερα, πραγματοποιούνται με τη χρήση πιστωτικών ή χρεωστικών καρτών, ηλεκτρονικού χρήματος και επιταγών, αυτόματης μεταφοράς κεφαλαίων. Η νέα αυτή μορφή συναλλαγών, πολύ γρήγορα ,έγινε στόχος κακόβουλων επιθέσεων, δημιουργώντας την ανάγκη για όσο το δυνατό ασφαλέστερα συστήματα συναλλαγών. Κύριο μέλημα , είναι η προστασία των δεδομένων των συναλλαγών που διακινούνται στο Διαδίκτυο. Για το λόγο αυτό, δημιουργήθηκαν μια σειρά από πρωτόκολλα επικοινωνίας , τα οποία στοχεύουν στην προστασία των δεδομένων αυτών. Τα πιο σημαντικά από αυτά ,από άποψη ευρύτητας χρήσεως, είναι το SSL και το SET.

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

Τον πρωτόκολλο SSL λειτουργεί ως εξής. Τη στιγμή που ο φυλλομετρητής συνδέεται με μια ‘’υψηλή ασφαλείας’’ σελίδα του Διαδικτύου, ο απομακρυσμένος διακομιστής στέλνει ένα μήνυμα καλωσορίσματος. Για να ξεκινήσει η σύνδεση ασφαλείας, ο φυλλομετρητής πρέπει να απαντήσει με ένα μήνυμα ‘’client hello’’ και ο διακομιστής με ένα ‘’server hello’’. Κατά την αρχική αυτή φάση, ο φυλλομετρητής και ο διακομιστής διαπραγματεύονται τις παραμέτρους ασφαλείας χρησιμοποιώντας το πρωτόκολλο χειραψίας (handshake),το πρώτο τμήμα του SSL. Το μήνυμα ‘’client hello’’, περιέχει έναν αριθμό, που ονομάζεται ταυτότητα συνδέσεως (session ID) και χαρακτηρίζει τον τύπο της client server σύνδεσης .Το μήνυμα περιέχει ακόμα πληροφορίες σχετικά με τους αλγόριθμους κρυπτογράφησης ,την έκδοση του SSL και τις μεθόδους συμπίεσης δεδομένων, που υποστηρίζει ο φυλλομετρητής .Τέλος, περιέχει και ένα τυχαίο αριθμό, που δημιουργεί ο φυλλομετρητής. Το μήνυμα ‘’server hello’’ απαντά με τη μέθοδο συμπίεσης και τον αλγόριθμο κρυπτογράφησης , που επέλεξε με βάση τις προτάσεις του φυλλομετρητή (πελάτης) , την έκδοση του SSL, ένα τυχαίο αριθμό και μια αποδεκτή ταυτότητα σύνδεσης .Στη συνέχεια, πελάτης και διακομιστής ανταλλάσουν ψηφιακά πιστοποιητικά ,που επιβεβαιώνουν ότι τα δυο μέρη είναι στην πραγματικότητα αυτά που ισχυρίζονται. Το πιστοποιητικό του διακομιστή μπορεί να περιέχει και ένα δημόσιο κλειδί για τον αλγόριθμο κρυπτογράφησης ιδιωτικού- δημοσίου κλειδιού, που έχει επιλεγεί κατά το handshake. Το κλειδί αυτό ωστόσο, θα χρησιμοποιηθεί για μικρό χρονικό διάστημα .Η συναλλαγή θα κωδικοποιηθεί με χρήση ενός συμβατικού αλγόριθμού κρυπτογράφησης. Το βασικότερο μειονέκτημα του πρωτοκόλλου SSL, είναι ότι δημιουργείται μεγάλος όγκος πρόσθετων δεδομένων, τα οποία και περιορίζουν την ταχύτητα μετάδοσής τους μέσω του Διαδικτύου. Για το λόγο αυτό, το πρωτόκολλο χρησιμοποιείται μόνο σε συγκεκριμένες σελίδες ενός δικτυακού τόπου οι οποίες σχετίζονται με τα στοιχεία των συναλλαγών και χρήζουν πρόσθετης ασφάλειας.

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 δεν ανταγωνίζεται το SSL, αλλά εστιάζει πάνω στις εμπιστευτικές συναλλαγές ,με παράλληλη ανάγκη πιστοποίησης της ταυτότητας των συναλλασσόμενων μερών. Έτσι, το SET επιχειρεί να εξασφαλίσει ,ότι κανείς δε 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 της αποκρυπτογραφεί και κάνει τη χρέωση. Πάντως, τα επιμέρους τεχνικά στοιχεία του και κυρίως το μήκος των κλειδιών που χρησιμοποιεί, χαρακτηρίζουν το SET ως πρωτόγονο και ίσως ανεπαρκές σε σύγκριση με την ασφάλεια που παρέχουν πακέτα όπως το PGP.

Ασφάλεια βάσεων δεδομένων

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 βάσεως δεδομένων. Οι απαιτήσεις ασφάλειας μιας βάσεως δεδομένων ,όσον αφορά την γενικότερη φιλοσοφία, δεν απέχουν και πολύ από την ασφάλεια οποιουδήποτε πληροφοριακού συστήματος. Εξετάζουμε όμως χωριστά την ασφάλεια των βάσεων δεδομένων ,για δυο βασικούς λόγους. Κατά πρώτον ,μια βάση δεδομένων έχει ιδιαίτερη δομή και μηχανισμούς διαχείρισης ,που απαιτούν τη χρήση εξειδικευμένων και πολύπλοκων εργαλείων για να επιτευχθεί ικανοποιητικό επίπεδο ασφάλειας και κατά δεύτερον τα δεδομένα, που αποθηκεύονται στις βάσεις δεδομένων, είναι ιδιαίτερα σημαντικά, συνήθως και

ευαίσθητα, η δε προστασία τους αποτελεί πρωτεύον στόχο κάθε οργανισμού.

Γενικές απαιτήσεις ασφάλειας συστήματος βάσης δεδομένων

Οι βασικές απαιτήσεις ασφάλειας ενός συστήματος βάσης δεδομένων δε διαφέρουν κατά πολύ από τις γενικότερες απαιτήσεις ενός πληροφοριακού συστήματος .Οι κυριότερες εκφάνσεις είναι οι ακόλουθες. Αρχικά υπάρχει η φυσική ακεραιότητα της βάσης δεδομένων, η οποία αναφέρεται στη φυσική ασφάλεια της βάσεως και ιδιαίτερα στην προστασία των υπολογιστικών συστημάτων, στα οποία έχει εγκατασταθεί από φυσικά προβλήματα όπως πτώση της τάσεως του ρεύματος ,πυρκαγιά ή πλημμύρα. Στη συνέχεια γίνεται λόγος για τη λογική ακεραιότητα της βάσης δεδομένων που αναφέρεται στην εξασφάλιση της λογικής δομής της βάσης. Τα προβλήματα ασφαλείας της λογικής ακεραιότητας μπορούν να ξεπεραστούν ,εφόσον εξ αρχής έχει γίνει σωστός σχεδιασμός .Κλασικό πρόβλημα ασφαλείας λογικής ακεραιότητας μιας βάσης ,έχουμε όταν η μεταβολή της τιμής ενός πεδίου επηρεάζει και τις τιμές άλλων πεδίων ,χωρίς αυτό να έχει προβλεφθεί. Έπειτα, αναφέρουμε την ακεραιότητα των πεδίων της βάσης δεδομένων, η οποία παράμετρος εγγυάται ότι οι τιμές των πεδίων της βάσης είναι σωστές. Επίσης, υπάρχει ο έλεγχος προσπέλασης. Ειδικότερα, 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. Επιπλέον, γίνεται λόγος για την αυθεντικοποίηση των χρηστών. Συγκεκριμένα, κάθε βάση, πτιν δεχθεί ένα χρήστη, θα πρέπει να πιστοποιήσει την ταυτότητά του. Στις βάσεις δεδομένων χρησιμοποιούνται κωδικοί πρόσβασης, ενώ σε πιο εξελιγμένα συστήματα είναι δυνατή και η ενσωμάτωση βιομετρικών μεθόδων. Τέλος ,υφίσταται και η διαθεσιμότητα, η οποία έχει ακριβώς, την ίδια έννοια που περιγράφθηκε ήδη, δηλαδή ότι τα δεδομένα της βάσης θα είναι ανά πάσα στιγμή άμεσα προσπελάσιμα. Η παράμετρος αυτή είναι ιδιαίτερα σημαντική στις βάσεις δεδομένων ,γιατί ενδέχεται να περιέχουν ευαίσθητα δεδομένα και απόρρητες πληροφορίες.

Σχεδιασμός ασφαλών συστημάτων βάσεων δεδομένων

Τα σημαντικότερα προβλήματα ασφαλείας , που παρουσιάζουν οι βάσεις δεδομένων, οφείλονται στον λανθασμένο σχεδιασμό. Τόσο οι εταιρείες που εμπορεύονται το συγκεκριμένο λογισμικό , όσο και οι οργανισμοί που το προμηθεύονται ,παραμελούν το σωστό σχεδιασμό για λόγους , κυρίως, οικονομικούς αλλά και πίεσης χρόνου. Όταν βέβαια, στη συνέχεια, παρουσιαστούν προβλήματα ασφαλείας αντιλαμβάνονται το τεράστιο λάθος, στο οποίο είχαν υποπέσει. Οι σημαντικότερες φάσεις, από πλευράς ασφαλείας ,κατά το σχεδιασμό ενός συστήματος βάσεων δεδομένων είναι οι ακόλουθες. Κατά κύριο λόγο, κάνουμε λόγο για την προκαταρκτική ανάλυση. Στο στάδιο αυτό, προσδιορίζονται οι στόχοι, σχετικά, με την ασφάλεια της βάσης δεδομένων και εξετάζονται οι πιθανοί κίνδυνοι ,όπως οι μη εξουσιοδοτημένες προσπελάσεις ,τα κακόβουλα προγράμματα, η φυσική ασφάλεια, η συμβατικότητα με τα υπάρχοντα συστήματα ασφαλείας και η θέση της βάσης στην πολιτική ασφάλειας του οργανισμού .Επιπλέον έχουμε την ανάλυση απαιτήσεων ασφαλείας. Κατά τη φάση αυτή του σχεδιασμού προσδιορίζονται οι χρήστες της βάσης και τα δικαιώματα ,που καταχωρούνται στον καθένα από αυτούς. Οι κρισιμότεροι παράγοντες, στη φάση αυτή, είναι το επίπεδο εξουσιοδότησης του χρήστη και ο βαθμός ευαισθησίας των δεδομένων. Μετά, υπάρχει ο σχεδιασμός λογικού μοντέλου, όπου στη φάση αυτή καθορίζεται επακριβώς, η πολιτική ασφαλείας της βάσης με τη χρήση ενός λογικού μοντέλου. Το μοντέλο αυτό ,περιλαμβάνει τα υποκείμενα της βάσης ,τα αντικείμενα ,τις διαδικασίες και τους επιτρεπτούς τρόπους προσπέλασης στη βάση. Το επόμενο βήμα, 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 στηρίζεται στο λογικό μοντέλο ασφαλείας. Το τελευταίο στάδιο σχεδιασμού είναι ο φυσικός σχεδιασμός. Ο σχεδιαστής ασφαλείας καθορίζει τις τελευταίες λεπτομέρειες και ειδικότερα τις παραμέτρους του συστήματος ,που σχετίζονται με την απόδοση ,την αντίδραση σε περίπτωση υπερφόρτωσης, την ευελιξία και την προσαρμοστικότητα.

Πολιτικές ασφαλείας

Οι μέθοδοι και οι τεχνικές που χρησιμοποιούνται για την ασφάλεια των πληροφοριακών συστημάτων και τα σύγχρονα εργαλεία υλικού και λογισμικού δεν μπορούν από μόνα τους να επιτύχουν το επίπεδο ασφαλείας που απαιτούν οι ανάγκες ενός σύγχρονου οργανισμού. Τα εργαλεία υλικού και λογισμικού δεν λειτουργούν αυτόβουλα, είναι συμπληρωματικά και επιπλέον δύναται να παραμετροποιηθούν ,ανάλογα με τις υπάρχουσες ανάγκες. Παράλληλα, σε κάθε σύστημα ασφαλείας ,σημαντικό ρόλο διαδραματίζουν και οι ίδιοι οι χρήστες ,οι οποίοι μπορούν με τις πράξεις και παραλείψεις τους ,να αποτελέσουν πηγή σημαντικών κινδύνων ασφαλείας. 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 δυο βασικά βήματα. Στο πρώτο βήμα και πριν την σύνταξη του κειμένου της πολιτικής ασφαλείας, προσδιορίζονται οι κίνδυνοι ασφαλείας που διατρέχει ο οργανισμός. Ειδικότερα καθορίζεται από το είδος των κινδύνων ασφαλείας, έναντι των οποίων είναι ευάλωτος ο οργανισμός ,η πιθανότητα να προκύψει ο κίνδυνος και το κόστος που θα έχει ο οργανισμός σε περίπτωση που αυτός πραγματοποιηθεί.
Η προσέγγιση αυτή ονομάζεται ποσοτική ανάλυση κινδύνου ,καθώς τα κριτήρια που λαμβάνονται υπ' όψιν και αξιολογούνται ανάγονται στην ψυχρή γλώσσα των αριθμών. Εκτός όμως από την ποσοτική ανάλυση, η χρήση της οποίας είναι περιορισμένη, ευρέως χρησιμοποιείται η ποιοτική ανάλυση κινδύνου. Στην ποιοτική ανάλυση δεν εφαρμόζεται η λογική των πιθανοτήτων ,αλλά εξετάζονται άλλοι παράγοντες ,όπως οι πιθανές απειλές και τα χαρακτηριστικά του συστήματος που το καθιστούν ευάλωτο έναντι των απειλών αυτών .Στο δεύτερο βήμα, γίνεται η σύνταξη του κειμένου της πολιτικής ασφάλειας .Το άτομο που θα αναλάβει να διεκπεραιώσει την απαιτητική αυτή διαδικασία ,εκτός από προηγούμενη συναφή εμπειρία και γνώση, θα πρέπει να ακολουθήσει και μια σειρά από βασικούς κανόνες. Κατ' αρχήν, το κείμενο θα πρέπει να χωρίζεται σε δύο βασικά έγγραφα, από τα οποία το πρώτο περιγράφει τις γενικές πολιτικές ,οι οποίες και αλλάζουν σπανιότερα ,ενώ το δεύτερο περιγράφει συγκεκριμένες διαδικασίες , οι οποίες αλλάζουν πιο συχνά, λόγω της αλματώδης εξέλιξης της τεχνολογίας και της εμφάνισης νέων πακέτων λογισμικού ασφαλείας .Πολύ σημαντικό στοιχείο είναι η γλώσσα γραφής, η οποία πρέπει να είναι απλή, χωρίς ειδικευμένους τεχνικούς όρους που το μόνο που θα επιτύχουν είναι να μπερδέψουν αυτούς που θα κληθούν να την εφαρμόσουν. Τέλος, για κάθε πολιτική η οποία θα υιοθετηθεί , θα πρέπει να γίνεται σαφής μνεία για τη σημασία της ,καθώς σε αντίθετη περίπτωση, κάποιοι υπάλληλοι μπορεί να την θεωρήσουν περιττή.

Βασική δομή πολιτικής ασφαλείας

Η πολιτική ασφαλείας είναι ένα ογκώδες κείμενο , με πολλές παραμέτρους και έννοιες ,που απαιτεί αρκετό χρόνο από τους χρήστες για εξοικείωση και εφαρμογή. Για το λόγο αυτό ,είναι ιδιαίτερα σημαντικό να έχει σωστή δομή, που θα καθοδηγεί τον αναγνώστη. Παράλληλα, η σωστή δομή βοηθά και στην ευκολότερη αναθεώρησή της, διαδικασία αναγκαία με βάση τους ρυθμούς ανάπτυξης των πληροφοριακών κινδύνων. Το μοντέλο, που έχει κυριαρχήσει σήμερα, είναι το ιεραρχικό, όπου στο υψηλότερο επίπεδο συναντάμε τις γενικές αρχές ,ακολουθούν οι πολιτικές ειδικού σκοπού και στο τελευταίο επίπεδο συναντάμε συγκεκριμένες διαδικασίες ασφάλειας ,οδηγίες και τεχνικά εγχειρίδια. Κατά πρώτο λόγο ,στο επίπεδο της γενικής πολιτικής ασφαλείας , περιλαμβάνονται οι γενικές αρχές για την ασφάλεια του οργανισμού και καθορίζονται οι στρατηγικοί στόχοι ,αλλά και οι πόροι για την επίτευξή τους. Ακολούθως, στο επίπεδο ειδικού σκοπού ή επιμέρους πολιτικές, γίνεται διαχωρισμός της γενικής πολιτικής ασφάλειας του οργανισμού σε επιμέρους πολιτικές (ασφάλειας δικτύων, χρηστών, ηλεκτρονικής αλληλογραφίας, φυσικής ασφάλειας ).Και εδώ κινούμαστε και πάλι σε υψηλό επίπεδο ,καθώς δεν καθορίζονται επιμέρους πρακτικές. Έπειτα, ο τρόπος υλοποίησης της πολιτικής ασφάλειας που έχει θέσει ο οργανισμός ,περιγράφεται στο στάδιο διαδικασίες ασφάλειας. 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. Στο τελευταίο στάδιο οδηγίες ασφάλειας και τεχνικά εγχειρίδια, παρέχεται ακόμη πιο λεπτομερής περιγραφή ,ειδικότερες οδηγίες και κατευθύνσεις για πάσης φύσεως θέματα, κυρίως τεχνικής φύσεως (εγχειρίδιο ρυθμίσεων του firewall ή του web server).

Ο ρόλος των χρηστών

Ο ρόλος των χρηστών στην πολιτική ασφάλειας ενός οργανισμού είναι πολύ σημαντικός. Στην πράξη έχει αποδειχτεί, ότι τα τελειότερα συστήματα ασφαλείας , που χρησιμοποιούν την τελευταία τεχνολογία ,δεν κατάφεραν να προστατεύσουν έναν οργανισμό λόγω λάθους ή παράλειψης ενός χρήστη. Ο παράγων άνθρωπος είναι ο πιο αδύναμος κρίκος στην αλυσίδα , που καθορίζει την ασφάλεια του οργανισμού. Στις επιθέσεις κοινωνικής μηχανής ,οι επιτιθέμενοι δεν αναλώνονται στη σπατάλη χρόνου με τη χρήση προγραμμάτων λογισμικού για την εύρεση παραδείγματος χάριν κωδικών πρόσβασης ,αλλά εκμεταλλεύονται τις αδυναμίες του παράγοντα άνθρωπος .Είναι ,λοιπόν, πολύ σημαντικό ,στην πολιτική ασφαλείας ενός οργανισμού να προβλέπεται η εκπαίδευση αλλά και συνεχής επιμόρφωση του προσωπικού. Μόνο ο συνδυασμός τεχνολογικών μέτρων προστασίας και εκπαίδευσης των χρηστών μπορεί να αποδώσει το μέγιστο (όχι όμως απόλυτα) επίπεδο ασφαλείας για κάθε οργανισμό. Ο κύριος στόχος ενός προγράμματος είναι να πείσει τους εργαζόμενους για την ανάγκη προστασίας του οργανισμού, ώστε και οι ίδιοι να θέλουν να ακολουθήσουν τους κανόνες πολιτικής ασφαλείας. Ο μεγαλύτερος κίνδυνος είναι ο εφησυχασμός, γι' αυτό οι εργαζόμενοι πρέπει να κατανοήσουν ,ότι ο οργανισμός μπορεί να δεχθεί επίθεση ανά πάσα στιγμή και αυτοί

αποτελούν τη βασική μονάδα άμυνας και όχι το firewall ή το antivirus. Οι επιτιθέμενοι εκμεταλλεύονται το φόρτο εργασίας ενός υπαλλήλου ή την κόπωση από συνεχόμενη εργασία και καταφέρνουν να αποσπάσουν ευαίσθητες πληροφορίες. Το πρόγραμμα εκπαίδευσης οφείλει να τονίσουν τον κίνδυνο αυτό και να παράσχει οδηγίες για την αντιμετώπισή του. Τέλος, το συνολικό πρόγραμμα εκπαίδευσης και η εφαρμογή του, θα πρέπει να αποτελεί πρώτη προτεραιότητα για τους υπαλλήλους, οι οποίοι θα πρέπει να κατανοήσουν ,ότι η ασφάλεια των πληροφοριών στον οργανισμό αποτελεί μέρος της δουλειάς τους.

Σημαντικές υποθέσεις ηλεκτρονικού εγκλήματος

Η πρώτη υπόθεση με χάκερ στην Ελλάδα , είναι εκείνη που αποκαλύφθηκε τον Ιούλιο του 2000, με τη σύλληψη ενός φοιτητή από την Ξάνθη, ο οποίος πραγματοποιούσε ηλεκτρονικές εισβολές, κυρίως στο Εθνικό Ίδρυμα Ερευνών. Ήταν ο πρώτος χάκερ, που είχε συλληφθεί στην Ελλάδα και ο οποίος, αμέσως μετά έκανε καριέρα και τώρα έχει προσληφθεί σε μεγάλη πολυεθνική εταιρεία για την ασφάλεια των υπολογιστικών συστημάτων της.

Η πιο δύσκολη υπόθεση με την οποία έχουν ασχοληθεί οι διωκτικές αρχές είναι μία συκοφαντική δυσφήμιση, μέσω Δορυφορικής Σύνδεσης στο Ίντερνετ. Ένας ναυτικός έστελνε υβριστικά μηνύματα σ' ένα ζευγάρι, με σκοπό να τους χωρίσει. Συκοφαντούσε το σύζυγο στη σύζυγό του κι αντιστρόφως. Έστελνε τα μηνύματα από φορητό υπολογιστή, από ένα καράβι που συνεχώς ταξίδευε μέσω δορυφορικής σύνδεσης. Ήταν βεβαίως εξαιρετικά δύσκολο να εντοπίσουμε το ηλεκτρονικό στίγμα του. Όμως, έκανε το λάθος να στείλει ένα μήνυμα, με σταθερή σύνδεση κι αυτό στάθηκε μοιραίο για αυτόν. Άρχισε αυτή την παρενόχληση το 2002 και τον εντοπίσανε στα μέσα του 2004. Αφορούσε έρευνα 2,5 χρόνων.

Άλλη υπόθεση που παρουσίασε παρόμοιες δυσκολίες, ήταν μία έρευνα που είχαν πραγματοποιήσει οι αρχές για εντοπισμό εμπόρων ναρκωτικών, που προωθούσαν το εμπόρευμά τους μέσω Ίντερνετ, σε πελατεία στο Κολωνάκι.

Έπειτα αναφορικά με ζητήματα Ασφάλειας Συστημάτων Τραπεζών ,στην Ελλάδα έχουν χειριστεί 18 τέτοιου είδους υποθέσεις, που αφορούν εισβολή σε συστήματα Τραπεζών μέσω των διαδικτυακών πελατών τους. Οι ηλεκτρονικοί "ληστές" στέλνουν τους επονομαζόμενους "TROYAN HORSES", τους "ΔΟΥΡΕΙΟΥΣ ΊΠΠΟΥΣ" δηλαδή, προκειμένου να υφαρπάξουν τους κωδικούς πρόσβασης των χρηστών του e-banking (των ηλεκτρονικών τραπεζικών συναλλαγών). Επίσης υφαρπάζουν τους κωδικούς πρόσβασης με τη μέθοδο PHISING. Το έχουν κατορθώσει αρκετές φορές. Χαρακτηριστική είναι η περίπτωση ενός κυκλώματος, με συμμετοχή Ελλήνων, Ρώσων & Ουκρανών, το οποίο εξαρθρώθηκε προ μερικών μηνών.

Ένα σοβαρό αδίκημα μέσω Ίντερνετ, που συχνά εξιχνιάζει το Τμήμα Αντιμετώπισης Ηλεκτρονικού Εγκλήματος είναι η παιδική πορνογραφία. Πράγματι, ένας κύριος όγκος της δουλειάς των υπευθύνων της δίωξης ηλεκτρονικού εγκλήματος είναι οι ηλεκτρονικοί παιδόφιλοι. Από το 2001, έχουν αντιμετωπίσει 47 υποθέσεις παιδικής πορνογραφίας με 99 κατηγορουμένους & 88 συλλήψεις. Μάλιστα, για όλες αυτές τις υποθέσεις έχουν συνολικά 17 προφυλακίσεις. Οι συλληφθέντες μπορεί να είναι από ιδιωτικοί υπάλληλοι μέχρι καταστηματάρχες, Ιατροί & Καθηγητές Πανεπιστημίου[33]. Επίσης, τον Σεπτέμβριο του 2004, ένας ανήλικος μαθητής Λυκείου στην Αθήνα αυτοκτόνησε κάνοντας λήψη ενός πολύ τοξικού γεωργικού φαρμάκου, αφού είχε λάβει προηγουμένως σχετικές οδηγίες από το Internet μέσω προγραμμάτων αλληλογραφίας και chat rooms. Καταλυτική υπήρξε η επικοινωνία του μ' έναν 25χρονο σμηνία από τα Χανιά, ο οποίος χρησιμοποιούσε γυναικείο ψευδώνυμο στις επικοινωνίες του με τον αυτόχειρα και ήταν αυτός που τον πληροφόρησε σχετικά με το δραστικό γεωργικό φάρμακο. Η Αστυνομία χρειάσθηκε πολύμηνες έρευνες για να φθάσει στα ίχνη του χρήστη-συμβούλου και αυτό γιατί ο τελευταίος χρησιμοποιούσε όχι τον υπολογιστή του σπιτιού του αλλά έναν από τους τρεις υπολογιστές ενός Internet Cafe στα Χανιά. Εις βάρος του 25χρονου σχηματίστηκε δικογραφία για παράβαση του άρθρου 501 «συμμετοχή σε αυτοκτονία», κατηγορία που είναι σε βαθμό πλημμελήματος. Κατά τη διάρκεια της ανάκρισης του 25χρονου προέκυψε νομικό κενό στην υπόθεση αυτή.

Επιπροσθέτως, ένας μεσήλικος 47χρονος οικογενειάρχης, τεχνικός υπολογιστών, συνελήφθη στην Κύπρο τον Απρίλιο του 2005 με την κατηγορία ότι έκανε πειρατεία στον υπολογιστή μιας 17χρονης και ενεργοποίησε την Web camera της για να καταγράφει την σεξουαλική της συμπεριφορά. Ο 47χρονος παγίδευσε την κοπέλα μέσα από έναν χώρο ή δωμάτιο συζήτησης (chat room) του Internet και της έστειλε ένα αρχείο τύπου trojan horse (δούρειος ίππος), μέσω του οποίου απέκτησε πρόσβαση στον υπολογιστή της. Μετά από λίγο απέστειλε στην κοπέλα ένα βίντεο κλιπ που την έδειχνε να βγαίνει από το μπάνιο και ύστερα να ντύνεται. Απελπισμένη η κοπέλα έσβησε αμέσως τον υπολογιστή της. Την επομένη ανακάλυψε ότι ο δράστης είχε

[33] www.securitymanager.gr

παραβιάσει τα αρχεία του υπολογιστή της, είχε κλέψει τα προσωπικά της δεδομένα και είχε μάθει τον αριθμό του κινητού της τηλεφώνου. Ο δράστης της έστελνε γραπτά μηνύματα και την έπαιρνε τηλέφωνο στο κινητό της. Η Αστυνομία της Κύπρου συνέλαβε τον δράστη με την κατηγορία της σεξουαλικής παρενόχλησης.

Τα Κυκλώματα Παιδικής Πορνογραφίας

Σε μάστιγα ή στην Λερναία Ύδρα του Internet κατ' άλλους, τείνει να εξελιχθεί το φαινόμενο της διακίνησης παιδικού πορνογραφικού υλικού (παιδοφιλία) μέσω του Διαδικτύου. Σύμφωνα με τα στατιστικά στοιχεία του Τμήματος Δίωξης Ηλεκτρονικού Εγκλήματος της Ασφάλειας Αττικής, από τις αρχές του 2004 έως τον Απρίλιο του 2005 έχουν εξιχνιασθεί 48 υποθέσεις διακίνησης υλικού παιδικής πορνογραφίας μέσω του Internet, έχουν συλληφθεί 68 άτομα και έχουν κατηγορηθεί συνολικά 90. Το Τμήμα αυτό έχει εξιχνιάσει 105 τέτοιες υποθέσεις το διάστημα 2002-2005, αλλά σχεδόν καμία δεν έχει λήξει δικαστικά. Η συγκεκριμένη μορφή εγκληματικότητας συνεχώς φουντώνει, παρουσιάζονται συνέχεια καινούργιες υποθέσεις και ιστοσελίδες ξεφυτρώνουν από το πουθενά. Ενώ στο εξωτερικό υπάρχουν οργανωμένα κυκλώματα, κυρίως στις ΗΠΑ και τη Ρωσία, στη χώρα μας οι συγκεκριμένοι δράστες δρουν ακόμα μεμονωμένα. Επίσης, σ' όλες τις υποθέσεις που έχουν αποκαλυφθεί, οι συλληφθέντες είναι και οι ίδιοι παιδόφιλοι.

Οι υποθέσεις που σχετίζονται με τη δημιουργία, διακίνηση και πώληση πορνογραφικού υλικού ανηλίκων μέχρι τον Οκτώβριο του 2002 τιμωρούνταν στη χώρα μας σύμφωνα με τον νόμο «περί ασέμνων» και το αδίκημα αντιμετωπιζόταν ως πλημμέλημα, ενώ σήμερα προβλέπονται ποινές έως και ισόβιας κάθειρξης. Σχετικός είναι ο *Ν.3064/2002* και μέχρι τώρα 80 άτομα έχουν διωχθεί ποινικά σε εφαρμογή του νόμου αυτού. Οι ποινικές διώξεις ήταν για πλημμελήματα και για κακουργήματα. Το κύριο πρόβλημα, όμως, μ' αυτές τις περιπτώσεις είναι να στοιχειοθετηθούν οι κακουργηματικές κατηγορίες. Το δικαστήριο δυσκολεύεται να ταυτοποιήσει τα στοιχεία των παιδιών – θυμάτων και να πάρει καταθέσεις απ' αυτά για το αν πράγματι τούς ασκήθηκε ψυχολογική ή άλλης μορφής πίεση. Τα άτομα που συλλαμβάνονται για τέτοιες υποθέσεις ισχυρίζονται συνήθως ότι δεν έχουν καμία σχέση με τη φωτογράφιση των ανηλίκων και ότι απλά κατέβασαν από το Internet κάποιες φωτογραφίες και τις τοποθέτησαν στις ιστοσελίδες τους. Ένας μάλιστα από τους συλληφθέντες ισχυρίσθηκε ότι χρησιμοποίησε αυτό το υλικό για την έρευνα που κάνει στο Πανεπιστήμιο. Η διαδικασία της συγκέντρωσης του αποδεικτικού υλικού για την τεκμηρίωση των σχετικών δικογραφιών αποδεικνύεται ιδιαίτερα δύσκολη και χρονοβόρα και μπορεί να πάρει μήνες. Πολλές μεγάλες υποθέσεις παιδοφιλίας βρίσκονται για πολύ καιρό στο στάδιο της εργαστηριακής διερεύνησης. Τα στοιχεία για την διακίνηση του παιδικού πορνογραφικού υλικού μέσω του Διαδικτύου είναι εντυπωσιακά :

- 100.000 ιστοσελίδες
- 1 δισ. ευρώ ο ετήσιος τζίρος
- 20.000 νέες φωτογραφίες προστίθενται κάθε εβδομάδα
- 20 παιδιά (2-12 ετών) εμφανίζονται κάθε μήνα σε τέτοιες ιστοσελίδες
- Οι ενδιαφερόμενοι πληρώνουν μέσω πιστωτικής κάρτας 30-50 ευρώ τον μήνα για να έχουν το δικαίωμα να κατεβάζουν φωτογραφίες ή βίντεο.
- Το 45-50% των ηλεκτρονικών εγκλημάτων αφορά παιδική πορνογραφία.
- Οι δράστες προέρχονται απ' όλες τις κοινωνικές ομάδες και απ' όλα τα μορφωτικά επίπεδα και πιστεύουν ότι το Διαδίκτυο τούς εξασφαλίσει ανωνυμία για την δράση τους και ότι μπορούν να παραποιήσουν την ταυτότητά τους.
- Τα περισσότερα παιδιά δεν επιβλέπονται όταν κάνουν πλοήγηση στο Internet.
- Το 86% των παιδιών που σερφάρουν στο Internet έχουν δεχθεί προτάσεις για να συναντηθούν με άτομα που γνώρισαν στο Διαδίκτυο.
- Το 16% των επισκεπτών σε ιστοσελίδες πορνογραφικού περιεχομένου είναι ανήλικοι.
- Η διαδικτυακή πορνογραφία είναι σταθερά το πιο «επιτυχημένο» προϊόν του Internet, με περισσότερα από 2,6 δισ. δολάρια έσοδα ανά έτος.

Οι φωτογραφίες αυτές προέρχονται κυρίως από το εξωτερικό αλλά τελευταία έχουν αποκαλυφθεί και υποθέσεις με Έλληνες παιδόφιλους που τραβούσαν οι ίδιοι τις επίμαχες φωτογραφίες. Χαρακτηριστικό είναι το γεγονός ότι πρόσφατα στην Πιερία δύο μαθητές αναγκάσθηκαν να αλλάξουν σχολείο επειδή δεχόντουσαν απειλές από συμμαθητές τους ότι θα ανέβαζαν (upload) στο Internet γυμνές φωτογραφίες τους από τα αποδυτήρια αν δεν τους έδιναν το χαρτζιλίκι τους. Ακόμη, ένας ιδιωτικός υπάλληλος στον Βόλο φωτογράφιζε

γυμνά παιδιά και καταχωρούσε τις φωτογραφίες τους στο Internet, αλλά δεν πρόσεξε ότι άθελά του φωτογράφιζε και κάποιες κολώνες της ΔΕΗ, απ' όπου οι αστυνομικοί εντόπισαν κάποιους αριθμούς, βρήκαν τις κολώνες και έφθασαν έτσι στον δράστη.

Η Αστυνομία της Μεγάλης Βρετανίας εξαπέλυσε πρόσφατα μια μεγάλη επιχείρηση στο Internet με την ονομασία *«Αρετή»* και με στόχο το κυνήγι των παιδεραστών. Συνέλαβε 1.300 άτομα. Από σχετικές έρευνες εντοπίσθηκαν περίπου 250.000 άτομα σ' όλον τον κόσμο που χρησιμοποίησαν τα στοιχεία της πιστωτικής τους κάρτας για να πληρώσουν και να κατεβάσουν στον υπολογιστή τους παιδικό πορνό. Το ερώτημα βέβαια είναι αν θεωρείται κάποιος ένοχος επειδή κατεβάζει παιδικό πορνό στον υπολογιστή του. Νέος νόμος που τέθηκε σε ισχύ στη Μεγάλη Βρετανία το 2003 αντιμετωπίζει ως ποινικό αδίκημα αυτό της «προετοιμασίας» των παιδιών, το οποίο περιλαμβάνει την επικοινωνία μέσω Internet μ' ένα παιδί, με απώτερο στόχο την διάπραξη σεξουαλικής πράξης μ' αυτό όταν γίνει μια συνάντηση μαζί του. Οι εξηγήσεις που δίνουν οι ειδικοί για τη ραγδαία εξάπλωση αυτού του φαινομένου είναι ψυχολογικές και κοινωνικές. Οι δράστες είναι συνήθως προσωπικότητες με ψυχοπαθολογικά στοιχεία που είναι πολύ πιθανό να κακοποιήθηκαν στην παιδική τους ηλικία. Το προφίλ των δραστών είναι άτομα με ανώτερη μόρφωση, οικογενειάρχες, οικονομικά ευκατάστατοι και ηλικίας συνήθως από 30 έως 50 ετών. Μεταξύ των δραστών εντοπίσθηκαν εκπαιδευτικοί και δικηγόροι. Υπάρχουν ειδικά προγράμματα – φίλτρα που έχουν την δυνατότητα να εντοπίσουν προσβλητικές λέξεις ή εκφράσεις σε μια ιστοσελίδα και να εμποδίσουν έτσι την πρόσβαση σ' αυτήν αλλά και πάλι οι επιτήδειοι μπορούν να το αντιμετωπίσουν αποφεύγοντας να χρησιμοποιούν τέτοιες λέξεις αλλά μόνο φωτογραφίες ή βίντεο με παράνομο υλικό. Ιστοσελίδες όπου μπορεί κάποιος να αναφέρει πορνογραφικό ή άλλο παράνομο υλικό που διακινείται μέσω του Διαδικτύου, είναι οι εξής[34] :

- http://www.inhope.org
- http://www.safeline.gr
- http://www.fraud.org

## Άλλα θέματα που έχουν σχέση με τη νομοθεσία
## Η προστασία των δικαιωμάτων πνευματικής ιδιοκτησίας

Η ανάπτυξη και διάδοση του Διαδικτύου έχει δημιουργήσει μεγάλο προβληματισμό σχετικά με το πώς στο νέο αυτό εικονικό κόσμο ,θα μπορέσουν να προστατευτούν τα δικαιώματα πνευματικής ιδιοκτησίας .Η ψηφιακή μορφή των πληροφοριών έχει μετατρέψει την αναπαραγωγή της σε εύκολη και γρήγορη διαδικασία ,η δε ενσωμάτωσή της σε πρότυπα όπως mp3 ή mpeg έχουν μειώσει κατά πολύ τον όγκο της, καθιστώντας ιδιαίτερα εύκολη την μετάδοσή της μέσω δικτύων. Ακόμη, το Διαδίκτυο ,ως μια τεράστια δεξαμενή πληροφοριών ,δημιουργεί εύλογα προβληματισμό για το αν θα πρέπει να αποτελεί μια <<κοινωνία κοινής κτήσης πληροφοριών>> ή θα πρέπει να μεταβληθεί σε μια <<αγορά πληροφοριών>> όπου η πρόσβαση στο αποθηκευμένο υλικό και στα πνευματικά δημιουργήματα θα είναι δυνατή μόνο μετά από πληρωμή. Το δίκαιο της πνευματικής ιδιοκτησίας έχει ,ως αντικείμενο προστασίας τα έργα του λόγου της τέχνης και της επιστήμης. Τα δυο 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.

Σχετικά με τα πνευματικά δικαιώματα έργων δημοσιευμένων στο Διαδίκτυο, αναμφισβήτητα, στο χώρο αυτό είναι εξαιρετικά δύσκολο να καθορίσουμε τι μπορεί να προστατευτεί με το δίκαιο της πνευματικής ιδιοκτησίας, και τι όχι. Υπό μια ευρεία έννοια μπορούμε να θεωρήσουμε ότι προστατεύονται τα γραπτά έργα, όπως τα μηνύματα του ηλεκτρονικού ταχυδρομείου, τα ηχητικά ή οπτικοακουστικά έργα, οι ψηφιακές εικόνες, τα προϊόντα λογισμικού, οι βάσεις δεδομένων και οι ιστοσελίδες. Ουσιαστικά, δεν υπάρχει κάτι στο Διαδίκτυο, που να μην προστατεύεται από τα δικαιώματα πνευματικής ιδιοκτησίας ,εφόσον βέβαια πληρούνται ορισμένες προϋποθέσεις όπως η πρωτοτυπία του έργου. Δύο είναι τα βασικότερα τεχνικά ζητήματα που έχουν σχέση με το Διαδίκτυο και το δίκαιο της πνευματικής ιδιοκτησίας ,τα οποία είναι η χρήση των συνδέσμων και το mp3 και άλλα σχετικά πρότυπα. Στην πρώτη περίπτωση ,η χρήση συνδέσμων που παραπέμπουν απευθείας σε σελίδες που περιλαμβάνουν προστατευόμενα έργα συνιστούν παραβίαση των πνευματικών δικαιωμάτων . Στη δεύτερη περίπτωση ,η ευρεία διάδοση μουσικών κομματιών σε μορφή mp3 ή και βιντεοταινιών με το

[34] http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-LawAndInternet.html

μορφή mpeg, χωρίς την έγκριση του δημιουργού ,αποτελούν σήμερα την πλέον διαδεδομένη προσβολή δικαιωμάτων πνευματικής ιδιοκτησίας των δημιουργών.

Ακολούθως ,σχετικά με τα πνευματικά δικαιώματα σε βάσεις δεδομένων, οι βάσεις αυτές πάντοτε υπήρχαν στη ζωή μας. Κλασικά παραδείγματα αποτελούν τα λεξικά, οι τηλεφωνικοί κατάλογοι και οι εγκυκλοπαίδειες. Σήμερα ,η μορφή των βάσεων δεδομένων είναι κυρίως ηλεκτρονική. Η νέα αυτή μορφή επέτρεψε την καλύτερη οργάνωση του περιεχομένου τους και την ευκολότερη ανάκτηση πληροφοριών , με αποτέλεσμα η χρήση τους να επεκταθεί σε μεγάλο βαθμό . Τα νομικά προβλήματα που προκύπτουν από την διάδοση των βάσεων δεδομένων, συναντώνται σε πολλά επίπεδα. 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 τον Ν.2121/1993 περί πνευματικής ιδιοκτησίας. Η Οδηγία κατ' αρχήν ορίζει ότι μια βάση δεδομένων είναι <<μια συλλογή έργων ,δεδομένων ή ανεξάρτητων μεταξύ τους στοιχείων διευθετημένων κατά τρόπο συστηματικό ή μεθοδικό που είναι ατομικώς προσιτή με ηλεκτρονικά μέσα ή κατ' άλλον τρόπο>>. Η Οδηγία προστατεύει τις βάσεις δεδομένων κατά δυο τρόπους, είτε ως πνευματικά δημιουργήματα ,λόγω της διευθέτησης του περιεχομένου τους ,είτε ως προϊόν ουσιαστικής επένδυσης του κατασκευαστή ,ο οποίος έχει το δικαίωμα ειδικής φύσης σε αυτές για 15 χρόνια από την κατασκευή της βάσης , δικαίωμα το οποίο απαγορεύει την εξαγωγή ή επαναχρησιμοποίηση ουσιώδους 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.

Πνευματικά δικαιώματα σε προγράμματα 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, τα οποία είναι τα ακόλουθα. Αρχικά, στην γλώσσα προγραμματισμού, η οποία αποτελείται από σύνθετα σύμβολα, τα οποία ακολουθούν συγκεκριμένους κανόνες. Οι πιο διαδεδομένες γλώσσες προγραμματισμού είναι η Basic, η Pascal, η Fortran και η Cobol. Έπειτα, στον κώδικα πηγής , η κατοχή του οποίου αποτελεί πλήρη απόδειξη των πνευματικών δικαιωμάτων και στον κώδικα μηχανής , ο οποίος χρησιμοποιεί μόνο 2 σύμβολα, το 0 και το 1.

Το βασικότερο ερώτημα που τίθεται όταν αναφερόμαστε σε προγράμματα Η/Υ ,είναι εάν τα παραπάνω μέρη θα πρέπει να προστατεύονται με βάση τη νομοθεσία για τα πνευματικά δικαιώματα ή θα πρέπει να θεωρηθούν ως ευρεσιτεχνίες και να προστατευτούν με τη σχετική νομοθεσία. Η Ευρωπαϊκή Ένωση , παρακολουθώντας τις εξελίξεις στις ΗΠΑ ,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 πρόγραμμα Η/Υ , οι οποίες είναι και ποινικές και αστικές ,με γνώμονα πάντα τη βασική του ελληνικού δικαίου ,ότι όποια αποζημίωση επιδικαστεί ,θα πρέπει να είναι αντίστοιχη της ζημιάς που προκλήθηκε.

Προσωπικά δεδομένα- προστασία απορρήτου

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 αλλαγή 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 αντιληφθεί ,πλήθος προσωπικών του πληροφοριών, που αφορούν την ταυτότητά του ,τις προτιμήσεις του ,την προσωπικότητά του ή τον αριθμό της πιστωτικής τους κάρτας .Τα cookies και πολλά άλλα προγράμματα ,<<φροντίζουν >> να συλλέξουν τις πληροφορίες αυτές και να τις στείλουν στους ιδιοκτήτες των δικτυακών τόπων, για περαιτέρω επεξεργασία.

Διεθνείς Συμβάσεις

Η Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου του ΟΗΕ της 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 της 4-11-1950 (ΕΔΣΑ),ορίζει ότι <<κάθε πρόσωπο έχει δικαίωμα για σεβασμό της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του >>.

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

Ελληνική Νομοθεσία

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 βάσει κοινοτικών οδηγιών. Στο Σύνταγμα της Ελλάδας ,περιλαμβάνονται μια σειρά από διατάξεις ,για την προστασία της ιδιωτικής σφαίρας του ατόμου. Η θεμελιώδης διάταξη του άρθρου 2 παρ.1 ,αναφέρει ότι <<ο σεβασμός και η προστασία της αξίας του ανθρώπου αποτελούν πρωταρχική υποχρέωση της πολιτείας >>. Σημαντικές διατάξεις περιλαμβάνονται στα άρθρα 9 και 19. Στο άρθρο 9, αναφέρεται ότι <<η ιδιωτική και οικογενειακή ζωή του ατόμου είναι απαραβίαστη>> διάταξη που απαγορεύει τη δημοσιοποίηση της ζωής του ανθρώπου. Το άρθρο 19 προστατεύει το απόρρητο των επιστολών και την ελεύθερη ανταπόκριση και επικοινωνία. 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 370Α 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 αφορά το άρθρο 370Α το οποίο κατά πολλούς, θεωρείται ότι δε μπορεί να τύχει εφαρμογής στο Διαδίκτυο ,αν και η σύνδεση γίνεται μέσω μισθωμένης τηλεφωνικής γραμμής . Το άρθρο 370Β ,παρέχει ικανοποιητική προστασία μόνο όμως 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 αποθηκευμένα σε Η/Υ. Το απόρρητο στην περίπτωση αυτή προστατεύεται υπό μια ευρεία έννοια. Δεν περιλαμβάνει μόνο δεδομένα τα οποία χαρακτηρίζονται από την φύση τους απόρρητα ,αλλά προστατεύεται το δικαίωμα του νομίμου κατόχου των δεδομένων να αποκλείει σε άλλους την πρόσβαση σε όλα τα δεδομένα ,που είναι αποθηκευμένα στον υπολογιστή του.

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 αποστολή ,την προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε τρόπο και την τήρηση των όρων και διαδικασιών άρσης του απορρήτου. Τα άρθρο 3 και 4, προβλέπουν ότι η άρση του απορρήτου είναι δυνατή μόνο εφόσον πρόκειται για θέμα εθνικής ασφάλειας ή για την 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 δημοσιεύει προσωπικές πληροφορίες των χρηστών του και γενικά όλες οι ενέργειές του να μην οδηγούν σε προσβολή των ατομικών και κοινωνικών 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 ,συγκρότηση 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 οδηγία, 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. Έπειτα, αναφέρονται στην προστασία του ατόμου από τη μεταφορά αρχείων με δεδομένα προσωπικού χαρακτήρα μέσω του Διαδικτύου και επίσης στην προστασία από 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 χαρακτήρα>>

Ο Νόμος 2774/1999 ,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 .Όσο αφορά το χώρο του Διαδικτύου, η προστασία επεκτείνεται και στο ηλεκτρονικό ταχυδρομείο, οι διατάξεις περί αγοράς και διαφήμισης απαγορεύουν η χρήση των cookies, ενώ προβλέπεται η προστασία από την ενοχλητική αλληλογραφία. Οι παραβάτες των διατάξεων του νόμου φέρουν αστικές και ποινικές ευθύνες.

Ν3431/2006 <<Περί ηλεκτρονικών επικοινωνιών >>

Ο νόμος αυτός, ενσωματώνεται στο εθνικό δίκαιο μια σειρά από οδηγίες της Ευρωπαϊκής Ένωσης, σχετικές με τον έλεγχο των ηλεκτρονικών επικοινωνιών οποιασδήποτε μορφής .Βασικές επιδιώξεις 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 πάροχους 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 ,η οποία, πλέον, αποτελεί ανεξάρτητη αρχή και απολαμβάνει διοικητικής και οικονομικής αυτοτέλειας . Οι αρμοδιότητές της εκτείνονται σε όλο το φάσμα των ηλεκτρονικών επικοινωνιών. Όσο αφορά τον κυβερνοχώρο ,η ΕΕΤΤ 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.

Νομοθεσία και Ηλεκτρονικό εμπόριο

Μια από τις πιο σημαντικές συνέπειες της ανάπτυξης του Διαδικτύου είναι η ενσωμάτωση σε αυτό εμπορικών δραστηριοτήτων. Αρχικά, το Διαδίκτυο λειτούργησε ως χώρος προβολής και διαφήμισης των επιχειρήσεων ,στην προσπάθειά τους να προσελκύσουν υποψήφιους πελάτες. Πολύ γρήγορα, οι προσφερόμενες υπηρεσίες μέσω του Διαδικτύου, αναπτύχθηκαν σε τέτοιο βαθμό που σήμερα είναι δυνατή η on-line παραγγελία ,πληρωμή και παράδοση αγαθών και υπηρεσιών. Η παγκόσμια αυτή αγορά, ήταν επόμενο να έχει και συνέπειες στην εφαρμοζόμενη νομοθεσία. Το νομοθετικό πλαίσιο ,για το <<συμβατικό εμπόριο>>, δεν μπορεί να τύχει εφαρμογής στο χώρο του Διαδικτύου. Οι διαδικτυακές συναλλαγές πραγματοποιούνται σε έναν εικονικό κόσμο, χωρίς τη φυσική παρουσία των συναλλασσόμενων, γεγονός που δημιουργεί δυσπιστία για την εγκυρότητα μιας συναλλαγής. Επιπλέον, διάφορα άλλα θέματα θα πρέπει να ρυθμιστούν , όπως η διαφήμιση ,οι ηλεκτρονικές υπογραφές ,τα ηλεκτρονικά έγγραφα και οι ηλεκτρονικές πληρωμές. Για τα θέματα αυτά, η Ευρωπαϊκή Κοινότητα έχει εκδώσει μια σειρά από Οδηγίες, οι περισσότερες από τις οποίες έχουν ενσωματωθεί στο ελληνικό δίκαιο. Η πιο σημαντική και πρόσφατη Οδηγία 2000/31/ΕΚ, ρυθμίζει τα θέματα του ηλεκτρονικού εμπορίου. Σκοπός της Οδηγίας δεν είναι η εναρμόνιση των ποινικών νόμων των κρατών-μελών, αλλά η εξασφάλιση της ελεύθερης κυκλοφορίας των υπηρεσιών της κοινωνίας της πληροφορίας μεταξύ των κρατών-μελών ,περιοριζόμενη από τις θεμελιώδεις ανάγκες για την προστασία των ανηλίκων και της ανθρώπινης αξιοπρέπειας και την προστασία του καταναλωτή και της δημόσιας υγείας.

Ελληνικό Δίκαιο

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 αρχικά 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 τακτικά μητρώα επιλογών ,όπου μπορούν να εγγράφονται τα φυσικά πρόσωπα που επιλέγουν να μη λαμβάνουν τέτοιες εμπορικές επικοινωνίες. Στη συνέχεια, 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 ενημερώνει πλήρως τον πελάτη για τις λεπτομέρειες της σύμβασης και μετά την παραγγελία ,αποστέλλει και ηλεκτρονικό μήνυμα επιβεβαίωσης . Κατόπιν, στο άρθρο 20, το οποίο εξαίρει την εφαρμογή του Διατάγματος από ορισμένες δραστηριότητες όπως για παράδειγμα τον φορολογικό τομέα και θέματα που ήδη ρυθμίζονται με το νόμο περί προστασίας των προσωπικών δεδομένων.

Το παραπάνω Προεδρικό Διάταγμα ,δεν ρυθμίζει μια σειρά από άλλα ζητήματα τα οποία έχουν άμεση σχέση με το ηλεκτρονικό εμπόριο, όπως τα ηλεκτρονικά έγγραφα, οι ηλεκτρονικές πληρωμές και η ηλεκτρονική υπογραφή. 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 για παράδειγμα 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 ισχύ το ΠΔ.150/2001, το οποίο προσάρμοσε την Οδηγία 99/93/ΕΚ, σχετικά με τις ψηφιακές υπογραφές στο Ελληνικό δίκαιο. Σύμφωνα με τις διατάξεις του ΠΔ., η ηλεκτρονική υπογραφή πρέπει να πληροί τους εξής όρους . Αρχικά θα πρέπει να συνδέεται μονοσήμαντα με τον υπογράφοντα, έπειτα να είναι ικανή να καθορίσει ,ειδικά και αποκλειστικά ,την ταυτότητα του υπογράφοντος ,να δημιουργείται η ηλεκτρονική υπογραφή με μέσα, τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο και τέλος να συνδέεται με τα δεδομένα, στα οποία αναφέρεται ,κατά τρόπο, ώστε να μπορεί να εντοπισθεί οποιαδήποτε μεταγενέστερη αλλοίωση των εν λόγω δεδομένων. Από τεχνικής πλευράς ,για την ψηφιακή υπογραφή χρησιμοποιείται η ασύμμετρη κρυπτογράφηση. Επιπλέον, το άρθρο 3 εξομοιώνει την ψηφιακή υπογραφή με την ιδιόχειρη. 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 στον χώρο του Διαδικτύου με τρεις κυρίους τρόπους. Αρχικά με την ηλεκτρονική μεταφορά κεφαλαίων, έπειτα με τη χρήση πιστωτικών καρτών και τέλος με την ύπαρξη ηλεκτρονικού χρήματος. Η πιο διαδεδομένη μέθοδος πληρωμής είναι μέσω πιστωτικών καρτών. 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 η Οδηγία97/7/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 πραγμάτων ή υπηρεσιών.

## Η διερεύνηση του ηλεκτρονικού εγκλήματος

### Εισαγωγή

Η διερεύνηση του ηλεκτρονικού εγκλήματος από τις αρμόδιες αρχές, έχει ως σκοπό την ανακάλυψη του δράστη και την νομική και επιστημονική τεκμηρίωση της υπόθεσης ,προκειμένου να καταστεί δυνατή η απόδειξη της αλήθειας. Με το πέρασμα των χρόνων, τα μέσα διάπραξης του εγκλήματος μεταβάλλονται. Η τεχνολογική εξέλιξη αποτελεί σύμμαχο των κακοποιών, οι οποίοι χρησιμοποιούν την τεχνολογία για την πραγμάτωση των εγκληματικών τους προθέσεων. Παράλληλα όμως ,η τεχνολογία έχει συνδράμει και στο έργο των διωκτικών αρχών, οι οποίες χρησιμοποιούν νέες μεθόδους διερεύνησης των εγκλημάτων, που βοηθούν στην ανεύρεση των ενόχων.

Η Εγκληματολογική Επιστήμη, ασχολείται με την ανακάλυψη ,ανάλυση και νομική τεκμηρίωση των αποδείξεων ,που συνδέουν μια αξιόποινη πράξη με ένα πρόσωπο ή γενικότερα πρόσωπα και αποδεικτικά στοιχεία. Η ανάλυση του DNA και η εξέταση των δακτυλικών αποτυπωμάτων είναι μερικές από τις δυνατότητες της επιστήμης αυτής.

Πολλές φορές έχει αναφερθεί ότι οι Η/Υ συμμετέχουν, ποικιλοτρόπως, στο εγκληματικό φαινόμενο. Τα υπολογιστικά συστήματα μπορούν να χρησιμοποιηθούν για τη διάπραξη εγκλημάτων, να περιέχουν πληροφορίες για το έγκλημα ή να αποτελούν το στόχο του εγκλήματος. Οι αρμόδιες διωκτικές αρχές για να εξιχνιάσουν ένα έγκλημα ,στο οποίο συμμετέχει με οποιαδήποτε μορφή ένας Η/Υ,θα πρέπει να εξετάσουν τις πληροφορίες που βρίσκονται αποθηκευμένες σε αυτόν και σε άλλα φορητά μέσα αποθήκευσης ή διακινούνται σε ένα δίκτυο.

Η Ηλεκτρονική Εγκληματολογία, είναι <<η επιστήμη που ασχολείται με την ανάγνωση ,διατήρηση , ανάλυση και παρουσίαση ψηφιακών αποδείξεων κατά τρόπο νομικά αποδεκτό>>. Όλο και πιο συχνά, οι αποδείξεις μιας αξιόποινης πράξης είναι κρυμμένες σε έναν 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 κατηγορούμενου . Παράλληλα, θα πρέπει να βεβαιώσουν ότι δεν έγινε κάποια παράλειψη που κατέστρεψε αποδείξεις σχετικές με την αθωότητα

του κατηγορούμενου.

Ψηφιακές αποδείξεις και δεδομένα

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 Οκτώβρη του 1999 προτυποποίησε τις αποδείξεις που έχουν ψηφιακή μορφή ,διαχωρίζοντάς τες αρχικά σε ψηφιακές αποδείξεις που αφορά πληροφορίες ,που έχουν αποδεικτική αξία σε μια ποινική υπόθεση και μπορούν να αποθηκευτούν ή να μεταδοθούν σε ψηφιακή μορφή. Έπειτα, έχουμε τα αντικείμενα δεδομένων, σχετικά με αντικείμενα ή πληροφορίες που έχουν αποδεικτική αξία σε μια ποινική υπόθεση και σχετίζονται με φυσικά αντικείμενα. Στη συνέχεια υπάρχουν τα φυσικά αντικείμενα, δηλαδή τα φυσικά μέσα όπου αποθηκεύονται ή μέσω των οποίων μεταδίδονται πληροφορίες και αντικείμενα δεδομένων. Επίσης, αναφέρουμε τις γνήσιες ψηφιακές αποδείξεις, που είναι φυσικά αντικείμενα και αντικείμενα δεδομένων τη στιγμή που συλλέγονται από τη σκηνή του εγκλήματος . Ακολούθως, υπάρχουν οι διπλότυπες ψηφιακές αποδείξεις, δηλαδή ένα ακριβές ψηφιακό αντίγραφο όλων των αντικειμένων δεδομένων που περιέχονται σε ένα γνήσιο ψηφιακό αντικείμενο. Τέλος, αναφέρουμε και το αντίγραφο, που πρόκειται για 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 ή κινητό τηλέφωνο καθώς και σε οποιοδήποτε μέσο αποθήκευσης, όπως δισκέτες, CDs,DVDs, κάρτες μνήμης .Βασικό χαρακτηριστικό των ψηφιακών αποδείξεων είναι ο μεγάλος βαθμός μεταβλητότητάς τους. Μπορούν πολύ εύκολα να τροποποιηθούν ή να καταστραφούν με τη χρήση διάφορων εργαλείων και μεθόδων. Ο ερευνητής ,λοιπόν, πρέπει να αναζητεί και να μεταχειρίζεται τις πληροφορίες αυτές με ιδιαίτερη δεξιότητα. Οι ψηφιακές αποδείξεις αποτελούνται από ψηφιακά δεδομένα. Μια πολύ σημαντική διάκριση των ψηφιακών δεδομένων είναι σε μεταβλητά δεδομένα και σε διαρκή δεδομένα . Τα μεταβλητά, είναι δεδομένα που αποθηκεύονται στην μνήμη του συστήματος και χάνονται αν σταματήσει η τροφοδοσία του υπολογιστή με ρεύμα, αν γίνει τερματισμός της λειτουργίας του ή επανεκκίνηση. Τα διαρκή δεδομένα είναι αποθηκευμένα στους σκληρούς δίσκους του συστήματος ή σε άλλες συσκευές μόνιμης αποθήκευσης ,όπως οδηγοί USB,CDs και κάρτες μνήμης. Τα δεδομένα αυτά δεν χάνονται ,όταν τερματιστεί η λειτουργία του υπολογιστή ή γίνει επανεκκίνηση.

Οι μέθοδοι εξέτασης των ψηφιακών τεκμηρίων

Η εργαστηριακή εξέταση των ψηφιακών αποδείξεων που συλλέγονται από τη σκηνή διάπραξης του εγκλήματος, είναι μια από τια σημαντικότερες εργασίες της προανακριτικής διαδικασίας. Τα ιδιαίτερα χαρακτηριστικά των ψηφιακών αποδείξεων ,όπως για παράδειγμα ο μεγάλος βαθμός μεταβλητότητας, απαιτούν την εφαρμογή ειδικών τεχνικών για τη συλλογή πληροφοριών με αποδεικτική αξία.

Ανάκτηση διαγεγραμμένων δεδομένων

Στα λειτουργικά συστήματα της Microsoft, η διαγραφή ενός αρχείου σημαίνει την 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, ακόμη και έμπειροι, πιστεύουν ότι διαγράφοντας ένα αρχείο από τον Κάδο Ανακύκλωσης ,χάνεται οριστικά. Ωστόσο, η διαγραφή δεν επηρεάζει το αποθηκευμένο αρχείο, που παραμένει αποθηκευμένο έως ότου ένα καινούριο εγγραφεί στον ίδιο αποθηκευτικό χώρο. Τα αρχεία σε ένα σκληρό δίσκο, αποθηκεύονται σε συστοιχίες ,οι οποίες είναι μονάδες αποτελούμενες από ένα συγκεκριμένο αριθμό bits. Κάθε αρχείο μπορεί να είναι αποθηκευμένο σε πολλές συστοιχίες ,διάσπαρτες στην επιφάνεια του δίσκου. Η θέση των συστοιχιών προσδιορίζεται από έναν δείκτη που χρησιμεύει για την ανάκληση του αρχείου. Ο δείκτης είναι αποθηκευμένος σε ένα μέρος του δίσκου που ονομάζεται Κύριος Πίνακας Αρχείων. Όταν διαγράφεται ένα αρχείο δεν διαγράφονται τα ψηφιακά δεδομένα που το αποτελούν .Το σύστημα διαχείρισης αρχείων, επεμβαίνει στο δείκτη του αρχείου ,ο οποίος επισημαίνει τις συστοιχίες στις οποίες παραπέμπει ως διαθέσιμο χώρο, που σημαίνει ότι στις συστοιχίες αυτές μπορεί να αποθηκευτεί ένα νέο αρχείο. Αν ο σκληρός δίσκος έχει μεγάλη χωρητικότητα, ενδέχεται να περάσει μεγάλο χρονικό διάστημα ώσπου να εγγραφούν νέα αρχεία στο συγκεκριμένο διαθέσιμο χώρο και να σβήσουν τα παλιά. Το διαγραμμένο αρχείο εξακολουθεί να υπάρχει στο 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 που κυκλοφορούν στο εμπόριο.

Ανάκτηση κρυπτογραφημένων δεδομένων

Η κρυπτογράφηση εκτός από εργαλείο ασφάλειας των πληροφοριακών συστημάτων , αποτελεί ταυτόχρονα

και βασικό εργαλείο των ηλεκτρονικών εγκληματιών, για την απόκρυψη της παραβατικής συμπεριφοράς τους. Δεδομένα που εμπεριέχονται σε μηνύματα ηλεκτρονικού ταχυδρομείου, έγγραφα, συμπιεσμένους φακέλους, αρχεία PDF ή λογιστικά φύλλα, ενδέχεται να έχουν κρυπτογραφηθεί, εφόσον περιέχουν σημαντικές πληροφορίες σχετικές 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 .[35]

Ανάκτηση κρυφών δεδομένων

Η απόκρυψη δεδομένων στο σκληρό δίσκο ενός υπολογιστή είναι μια τεχνική ,που χρησιμοποιείται πολύ συχνά από τους ηλεκτρονικούς εγκληματίες. Υπάρχουν πολλά σημεία που μπορούν να κρυφτούν δεδομένα σε έναν Η/Υ. Αρχικά στους μαγνητικούς δίσκους. Οι σκληροί δίσκοι είναι χωρισμένοι σε τομείς , μεγέθους συνήθως 512 bytes,που αποτελούν και το μικρότερο κομμάτι στο οποίο μπορούμε να έχουμε πρόσβαση. Λόγω της κατασκευής των δίσκων, ενδέχεται να παραμείνει 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 μπορούν 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 έναν σκληρό δίσκο πάνω σε παλιά, να παραμείνουν κάποια δείγματα των παλιών αρχείων ,τα οποία με τα κατάλληλα εργαλεία μπορούν να ανακτηθούν και να επανασυσταθούν.

Στη συνέχεια, αναφερόμαστε στα στενογραφικά δεδομένα. Η στενογραφία είναι μια τεχνική με την οποία είναι δυνατόν να κρυφτούν δεδομένα μέσα σε άλλα δεδομένα. Η διαδικασία εντοπισμού των δεδομένων που έχουν στενογραφηθεί ονομάζεται στεγανάλυση. Στο ψηφιακό περιβάλλον είναι δυνατή η ενσωμάτωση στεγανογραφικών δεδομένων σε αρχεία της μορφής jpg, gif, bmp, wav, voc, gz και txt. Η συχνότερα 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 εντοπιστεί από το 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 στενογραφικών 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 .

Ανάκτηση ΄΄ξεχασμένων'' δεδομένων

Μεγάλο πλήθος δεδομένων αποθηκεύεται σε έναν Η/Υ αυτόματα από διάφορες εκτελούμενες εφαρμογές, είτε εν γνώσει είτε χωρίς να το γνωρίζει ο χρήστης .Τα δεδομένα αυτά, ενδέχεται να αποτελέσουν σημαντικό αποδεικτικό υλικό σε μια διαδικτυακή έρευνα.

Σχετικά με την μνήμη cache, κατά την περιήγηση στο Διαδίκτυο, οι φυλλομετρητές αποθηκεύουν στην μνήμη αυτή 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 δικτυακών 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 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 λόγου χάριν η πορνογραφία. Ακολούθως , γίνεται λόγος για τα προσωρινά αρχεία .Πολλές εφαρμογές, ιδιαίτερα αυτές της σουίτας Microsoft Office, 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, έως ότου κάποιο άλλο αρχείο εγγραφεί στο σημείο που ήταν αποθηκευμένα. Ο εξερευνητής μπορεί να ανακτήσει από τα αρχεία αυτά σημαντικές πληροφορίες . Έπειτα, αναφέρουμε τα αρχεία σελιδοποίησης. Τα σύγχρονα λειτουργικά συστήματα χρησιμοποιούν την εικονική μνήμη για να <<ξεγελάσουν>> το σύστημα, το

[35] E.Casey, ''Practical Approaches to Recovering Encrypted Digital Evidence''

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 ή ιστοσελίδες αποθηκεύονται στα αρχεία σελιδοποίησης(page files) .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.

Επίσης ,δεν πρέπει να παραλείψουμε το γεγονός ότι οι περισσότεροι Η/Υ γνωρίζουν ότι διαγράφοντας ένα αρχείο ,μετακινείται αρχικά στον Κάδο Ανακύκλωσης .Έχει παρατηρηθεί ότι πολλοί χρήστες ξεχνούν τα δεδομένα αυτά στον Κάδο Ανακύκλωσης, δίνοντας εύκολα αποδεικτικά στοιχεία στους εξερευνητές. Άλλες φορές ,δεν γνώριζαν καν ότι τα αρχεία που διέγραψαν τοποθετήθηκαν στον Κάδο Ανακύκλωσης ,ιδιαίτερα στια περιπτώσεις που το εικονίδιο του Κάδου Ανακύκλωσης δεν εμφανιζόταν στην Επιφάνεια Εργασίας. Επομένως, είναι πολύ σημαντικό για τον εξερευνητή να ελέγξει τον Κάδο Ανακύκλωσης ,καθώς μπορεί να αποκτήσει σημαντικά δεδομένα εύκολα και άμεσα. Τέλος, επισημαίνουμε την ανάκτηση δεδομένων από εφεδρικά αρχεία. Ειδικότερα, ένας χρήστης, εφόσον θέλει να εξαφανίσει δεδομένα που είναι αποθηκευμένα σε έναν 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 ενδέχεται να έχει αποθηκεύσει ο χρήστης σε φορητά μέσα ή σε άλλους σκληρούς δίσκους και έχει ξεχάσει να διαγράψει.

Ο εντοπισμός του ηλεκτρονικού εγκλήματος στο Διαδίκτυο

Αρχεία καταγραφής (log files)

Τα αρχεία καταγραφής διαδραματίζουν σημαντικό ρόλο ,καθώς σε αυτά αποθηκεύονται πληροφορίες , που αφορούν τη λειτουργία του συστήματος. Στα λειτουργικά συστήματα της οικογένειας Windows,υπάρχουν τρία βασικά είδη αρχείων καταγραφής που είναι τα εξής Application log, System log και Security log. Ο εντοπισμός όλων των πληροφοριών, που αποθηκεύονται τα αρχεία καταγραφής, μπορεί να πραγματοποιηθεί 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 ασφαλείας 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. Εκτός από το λειτουργικό σύστημα ,αρχεία καταγραφής δημιουργούνται και από άλλες εφαρμογές. Το firewall, ως βασικό εργαλείο που ελέγχει την κίνηση από και προς ένα προστατευόμενο 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.

Επιπροσθέτως, αναφέρουμε ότι τα αρχεία καταγραφής είναι μόνο ένα είδος δεδομένων, που μπορούν να αντληθούν από τα firewalls. Τα firewalls μπορούν να προσφέρουν και άλλου είδους πληροφορίες όπως συναγερμούς (alarms). Ειδικότερα, 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. Η λειτουργία αυτή είναι πολύ σημαντική ,καθώς μπορεί μια επίθεση να αποφευχθεί στη γέννησή της. Έπειτα, παρέχονται πληροφορίες σχετικά με τις προειδοποιήσεις (alerts), τα οποία αποτελούν μια πιο ήπια μορφή συναγερμού. Η ενημέρωση του διαχειριστή, μπορεί να γίνει με τους προαναφερθέντες τρόπους. 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 . Επίσης δεν πρέπει να παραληφθούν οι αναφορές(reports). Αν και οι πληροφορίες ασφαλείας από το firewall αποθηκεύονται στα αρχεία καταγραφής ,οι αναφορές μπορούν να δώσουν επιπρόσθετα δεδομένα ,όπως την συχνότητα αποτυχημένων προσπαθειών απόκτησης μη εξουσιοδοτημένης πρόσβασης και την συχνότητα σφαλμάτων. Οι πληροφορίες ,που μπορεί να συλλέξει ο ερευνητής από τα firewalls, όπως το χρονικό σημείο στο 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 μπορούν να βοηθήσουν στον εντοπισμό του επιτιθέμενου.

Επιπλέον, επισημαίνουμε τον εντοπισμό ονόματος χώρου και διεύθυνσης IP. Ο εντοπισμός της διεύθυνσης αυτής ,αποτελεί βασική ενέργεια των διωκτικών αρχών για την εξιχνίαση πολλών υποθέσεων μη εξουσιοδοτημένης πρόσβασης σε ένα δίκτυο. Στις επιθέσεις αυτές οι εισβολείς χρησιμοποιούν πλαστές διευθύνσεις IP, προκειμένου να παραπλανήσουν τις διωκτικές αρχές. Κάθε διεύθυνση στο Διαδίκτυο έχει έναν

αντίστοιχο αριθμό IP. Το σύστημα ,που έχει αναλάβει τη διατήρηση των αντιστοιχιών μεταξύ μιας ηλεκτρονικής διεύθυνσης και του αντίστοιχου IP, είναι το DNS(Domain Name System). Κατά την μιας επίθεσης ,ο επιτιθέμενος πλαστογραφεί την διεύθυνσή του για να φαίνεται ότι είναι νόμιμος χρήστης ,δεν πλαστογραφεί όμως (ή δεν μπορεί να πλαστογραφήσει) τον αντίστοιχο αριθμό IP. Συνήθως, συσκευές, όπως 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 κληθεί να ελέγξει τις διευθύνσεις όλων όσων απέκτησαν πρόσβαση ,προκειμένου να εξακριβώσει από ποιόν προήλθε η κακόβουλη επίθεση. Η εργασία αυτή μπορεί να διεκπεραιωθεί με διάφορα εργαλεία λογισμικού ,τα οποία ελέγχουν αν οι ηλεκτρονικές διευθύνσεις αναλογούν σε σωστούς αριθμούς IP. Επίσης, υπάρχουν και δικτυακοί τόποι που επιτελούν on-line την εργασία αυτή. Για παράδειγμα στο www.dnsreport.com μπορεί να δοθεί μια ηλεκτρονική διεύθυνση ή διεύθυνση ηλεκτρονικού ταχυδρομείου και να ληφθούν διάφορες πληροφορίες για αυτή όπως το IP ή ο server.

Στη συνέχεια κάνουμε λόγο για τα μηνύματα του ηλεκτρονικού ταχυδρομείου. Αυτά, εκτός από μέσο άμεσης επικοινωνίας μεταξύ των χρηστών, χρησιμοποιούνται για την διάπραξη πολλών αδικημάτων , όπως μετάδοση ιών και άλλου κακόβουλου κώδικα, επιθέσεις άρνησης εξυπηρέτησης ,απάτες ,απειλές και δυσφήμιση. Για τους λόγους αυτούς ,η εύρεση του αποστολέα των μηνυμάτων ηλεκτρονικού ταχυδρομείου ,αποτελεί βασική εργασία στην αναζήτηση των ηλεκτρονικών ιχνών του επιτιθέμενου. Αν ο αποστολέας αναγράψει στο μήνυμα το όνομά του Κθ την διεύθυνσή του (και τα στοιχεία αυτά είναι αληθή) τότε ο εντοπισμός τους είναι εύκολος. Αυτό όμως, δε συμβαίνει σχεδόν ποτέ. Ο μόνος τρόπος για την εύρεση του αποστολέα του μηνύματος στις περιπτώσεις αυτές ,είναι η ανάγνωση και κατανόηση των επικεφαλίδων του μηνύματος. Τα μηνύματα ηλεκτρονικού ταχυδρομείου ,κατά τη μετάβασή τους από τον αποστολέα στον παραλήπτη, διέρχονται από πολλούς ενδιάμεσους υπολογιστές. Κάθε ένας από 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 στην οποία μπορούν να αποστέλλονται πιθανές απαντήσεις ,το μονοπάτι (διεύθυνση) προς τον αποστολέα και ,τέλος, τους διακομιστές από τους οποίους διήλθε το μήνυμα για να φτάσει στον τελικό του παραλήπτη. Η πρόσβαση στις πληροφορίες αυτές είναι δυνατή μέσω των χρησιμοποιούμενων εφαρμογών ηλεκτρονικού ταχυδρομείου. Ο εντοπισμός του αποστολέα ενός μηνύματος ηλεκτρονικού ταχυδρομείου είναι μια εξαιρετικά δύσκολη διαδικασία. Οι επιτιθέμενοι έχουν ανακαλύψει μια σειρά από μεθόδους για την απόκρυψη της ταυτότητάς τους. Για παράδειγμα, με την χρήση anonymous remailers είναι δυνατή η αποστολή μηνυμάτων χωρίς να φαίνεται η ταυτότητα του αποστολέα. Επίσης, στο Διαδίκτυο είναι δυνατή η εύρεση αναλυτικών οδηγιών για τη χειροκίνητη δημιουργία ψευδών επικεφαλίδων των διακινούμενων μηνυμάτων.

Τέλος, αναφέρουμε τα honeypots και honeynets. Αυτά 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 αληθινού στόχοι ,προκειμένου να ξεγελάσουν τον επιτιθέμενο και να τον ωθήσουν στην παραβίασή τους. Ένα honeynet είναι μιας 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 επιθέσεώς του. Σε αντίθεση με τα firewalls, τα honeypots λειτουργούν παθητικά, δηλαδή αναμένουν την επίθεση του χρήστη και δεν ενεργούν για την παρεμπόδισή της, απλά καταγράφουν τις ενέργειές του. Υπάρχουν δύο βασικές κατηγορίες honeypots, τα πραγματικά (real) και τα εικονικά (virtual). Ένα πραγματικό honeypot ,είναι ακριβώς αυτό που φαίνεται. Ένα εικονικό honeypot είναι ένας συνδυασμός υλικού και λογισμικού ,που προσομοιάζει σε ένα πραγματικό διακομιστή.

Μοντέλα Ηλεκτρονικής Εγκληματολογίας (Digital Forensic Models)

Η ηλεκτρονική Εγκληματολογία βρίσκεται στα πρώιμα στάδια της ανάπτυξής της, σε σχέση με άλλους τομείς της Εγκληματολογικής Επιστήμης .Έως τώρα, δεν έχει υιοθετηθεί μια 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 ερευνητών ,παρέχοντας ένα βασικό σκελετό ενεργειών και μεθόδων έρευνας ανεξαρτήτως του περιβάλλοντος ,στο οποίο αυτή διεξάγεται. Επιπλέον, θα βοηθούσε στην ανάπτυξη κατάλληλων εργαλείων για την υποβοήθηση του έργου των ερευνητών ,στην υιοθέτηση κοινής ορολογίας ,ενώ θα αποτελούσε ένα 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 και

άλλοι(2001), πρότειναν ένα μοντέλο έρευνας της σκηνής διάπραξης του εγκλήματος ,αποτελούμενο από τέσσερα βήματα βασικά, τα οποία είναι η αναγνώριση (recognition) που περιλαμβάνει τον εντοπισμό των αντικειμένων, που πιθανώς έχουν αποδεικτική αξία. Ο ερευνητής ,στο στάδιο αυτό ,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. Έπειτα λαμβάνει χώρα η ταυτοποίηση (Identification). Στο στάδιο αυτό περιλαμβάνεται η ταξινόμηση των αποδεικτικών στοιχείων και η μεταξύ τους σύγκριση με γνωστά πρότυπα. Επίσης, υπάρχει η εξατομίκευση (Individualization),δηλαδή εξετάζεται εάν τα αποδεικτικά στοιχεία φέρουν συγκεκριμένα μοναδικά χαρακτηριστικά ,που μπορούν να τα συνδέσουν με κάποιο άτομο. Βασική αρχή αποτελεί η αξιολόγηση όλων των αντικειμένων. Τέλος ,έχουμε το συμπέρασμα (Reconstruction). Το τελευταίο αυτό στάδιο περιλαμβάνει τη συγκέντρωση όλων των αποδεικτικών στοιχείων και σχετικών πληροφοριών και την σύνταξη 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. Η μη αναφορά των ψηφιακών αποδείξεων μειώνει την αξία του μοντέλου , όμως δεν θα έπρεπε να παραβλεφτεί ότι πολλά από τα στάδια έρευνας που περιγράφηκαν ,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 έρευνας του ηλεκτρονικού εγκλήματος. Η κοινοπραξία αποτελείται περισσότερο από μέλη της ακαδημαϊκής κοινότητας .Το 2001 πρότεινε ένα μοντέλο έρευνας αποτελούμενο από επτά βήματα, που είναι η αναγνώριση, η διατήρηση, η συλλογή, η εξέταση, η ανάλυση, η παρουσίαση και η απόφαση .Το μοντέλο αυτό προτάθηκε, με το σκοπό να αποτελέσει τη βάση για την ανάπτυξη στο μέλλον ενός πιο πλήρους μοντέλου, καθώς η έρευνα ,το συγκεκριμένο χρονικό σημείο, ήταν περιορισμένη.

Ένα από τα πιο πλήρη μοντέλα δικτυακών ερευνών ,προτάθηκε το 2004 ,από τον Ciardjuain. Αξιολογώντας, αλλά και συνθέτοντας τα υπάρχοντα μοντέλα ,ο Ciardjuain κατέληξε σε ένα πλήρες μοντέλο ερευνών ,αποτελούμενο από δεκατρία βήματα. Ο Ciardjuain θέλησε στο μοντέλο του να συμπεριλάβει όλες τις πτυχές της έρευνας του ηλεκτρονικού εγκλήματος και να μην περιοριστεί μόνο στη σκηνή διάπραξης ,όπως συνέβαινε με τα προηγούμενα μοντέλα. Τα βήματα που προτείνει είναι τα ακόλουθα. Αρχικά, είναι η επίγνωση. Το βήμα αυτό δεν υπήρχε σε προηγούμενα μοντέλα. Αναφέρεται στην ενημέρωση ενός αρμόδιου φορέα (αστυνομία) ότι έχει προκύψει η ανάγκη για τη διεξαγωγή μιας έρευνας. Θεωρείται σημαντικό, γιατί τα γεγονότα που προκάλεσαν μια έρευνα μπορούν να επηρεάσουν σημαντικά τον τύπο αυτής. Επίσης, έχουμε την εξουσιοδότηση. Στο βήμα αυτό ,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 αρμοδίου εισαγγελέα. Στη συνέχεια, το επόμενο βήμα είναι ο σχεδιασμός της έρευνας, κατά τον οποίο μπορεί να προκύψουν διάφορα προβλήματα, όπως η ανάγκη για περαιτέρω εξουσιοδότηση ,για το λόγο αυτό θα πρέπει να διεξάγεται με ιδιαίτερη προσοχή και επιμέλεια. Επιπλέον, γίνεται ενημέρωση ενός οργανισμού ή προσώπου ότι πρόκειται να διεξαχθεί η έρευνα. Το βήμα αυτό είναι δυνατόν να παραληφθεί σε περιπτώσεις που η έρευνα απαιτεί το στοιχείο του αιφνιδιασμού. Ακολούθως, έχουμε την αναζήτηση και αναγνώριση αποδεικτικών στοιχείων, η οποία δραστηριότητα περιλαμβάνει τον εντοπισμό και αναγνώριση των αποδεικτικών στοιχείων (υπολογιστές, αποθηκευτικά μέσα), που θα χρησιμοποιηθούν στο επόμενο βήμα, που είναι η συλλογή αποδεικτικών στοιχείων και αποτελεί το πλέον σημαντικό βήμα της όλης διαδικασίας. Ο ερευνητής καλείται να συλλέξει όλα τα αποδεικτικά στοιχεία που θα συναντήσει στη σκηνή του εγκλήματος. Έπειτα ένα εξίσου σημαντικό βήμα με την συλλογή των αποδείξεων αποτελεί η μεταφορά των αποδεικτικών στοιχείων, καθώς η λανθασμένη συσκευασία και μεταφορά τους μπορεί να οδηγήσει σε καταστροφή ή απώλεια σημαντικών πληροφοριών. Στη συνέχεια πραγματοποιείται αποθήκευση των αποδείξεων, μια διαδικασία που μπορεί να απαιτηθεί σε περίπτωση που δεν είναι δυνατή η άμεση εξέτασή τους. Και στο βήμα αυτό θα πρέπει να ληφθεί μέριμνα για να διατηρηθούν αναλλοίωτα τα αποδεικτικά στοιχεία. Ακολούθως, έχουμε το στάδιο της εξέτασης αποδείξεων, όπου απαιτείται η χρησιμοποίηση ποικίλων τεχνικών για την ανάκτηση σημαντικών δεδομένων. Εργαλεία υλικού και λογισμικού ενδέχεται να χρησιμοποιηθούν για την ανάκτηση δεδομένων από κατεστραμμένους δίσκους για τον εντοπισμό ηλεκτρονικών ίχνων και για την τελική επεξεργασία μεγάλων ποσοτήτων δεδομένων. Δεν πρέπει να παραλείψουμε την υπόθεση, που αποτελεί το συμπέρασμα της εξέτασης των ψηφιακών αποδείξεων .Στις αστυνομικές έρευνες ,η υπόθεση έχει τη μορφή της έκθεσης πραγματογνωμοσύνης ,στην οποία καταγράφονται όλα τα γεγονότα και αποδεικτικά στοιχεία που εξετάστηκαν κατά τη διάρκεια της έρευνας. Το κείμενο της υπόθεσης βοηθά τον ερευνητή να κατανοήσει καλύτερα τα αποτελέσματα της έρευνάς του. Έπειτα, έχουμε την παρουσίαση της υπόθεσης ,η οποία σε μια αστυνομική έρευνα ενεργείται ,συνήθως ενώπιων του αρμόδιου δικαστηρίου. Μετά γίνεται λόγος για την απόδειξη- υποστήριξη της υπόθεσης. Στις περισσότερες περιπτώσεις η υπόθεση θ' αμφισβητηθεί στο ακροατήριο από τα μέρη τα οποία θίγονται από αυτή. Στο στάδιο αυτό ,ο ερευνητής καλείται να υποστηρίξει

προφορικά, όλα όσα έχει αναφέρει στην έκθεσή του ,στηρίζοντάς τα σε επιστημονικά στοιχεία. Τέλος υπάρχει και η διανομή των πληροφοριών. Ειδικότερα, η διανομή των αποτελεσμάτων της έρευνας είναι το τελευταίο στάδιο του μοντέλου, που προτείνει ο Ciardjuain. Στοχεύει στη χρησιμοποίηση της τεχνογνωσίας που αποκτήθηκε από μια έρευνα σε παρεμφερείς περιπτώσεις που ενδεχομένως προκύψουν στο μέλλον.

Ο Ciardjuain επισημαίνει ότι η σειρά των βημάτων που περιλαμβάνονται στο μοντέλο δεν είναι αυστηρή και απόλυτη. Ενδέχεται κάποια από τα βήματα να παραληφθούν ,να μεταβληθεί η σειρά τους ή ακόμη το αποτέλεσμα ενός βήματος να έχει επιπτώσεις όχι μόνο στο επόμενο ,αλλά και στο προηγούμενο .Ο ερευνητής πρέπει και οφείλει να καθοδηγείται από την ίδια την έρευνα και όχι από το μοντέλο το οποίο ,απλά, βοηθά στην επίτευξη των στόχων της έρευνας. Στα πλεονεκτήματα του μοντέλου ,εκτός από αυτά που ήδη ισχύουν σε κάθε μοντέλο δικτυακών ερευνών , επισημαίνει ότι ο τρόπος με τον οποίο οι διεργασίες διαδέχονται η μια την άλλη ,θα βοηθήσει για την ανάπτυξη συγκεκριμένων εργαλείων εξέτασης και ελέγχου ψηφιακών τεκμηρίων. Αναγνωρίζει ,όμως, ότι η γενικότητα του μοντέλου ενδέχεται να παρουσιάσει ορισμένες δυσκολίες, όσο αφορά την εφαρμογή του στο συγκεκριμένο περιβάλλον ενός οργανισμού.

Παράδειγμα ηλεκτρονικής απάτης με τη χρήση κώδικα

Μέσω της χρήσης ενός κώδικα καταφέραμε και κάτω από την ιστοσελίδα μας παρουσιάζεται μια άλλη ιστοσελίδα και έτσι φαίνεται σαν να είναι δικιά μας. Αυτό είναι ένα είδος ηλεκτρονικής απάτης.

Ειδικότερα:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">

<HTML>

<HEAD>

<TITLE>LABTEL</TITLE>

 </HEAD>

<frameset cols="100%,*">

<frame name="labtel" src="http://www.parents.gr">

</frame>

</frameset>

</HTML>
```

Με τον παραπάνω κώδικα εμφανίζεται η παρακάτω σελίδα(parents.gr) ,η οποία έχει το όνομα labtel και φαίνεται να ανήκει στη διεύθυνση : C:\Users\ΛΑΜΠΡΙΝΗ\Desktop\kodikasistoselidas.html. Στη θέση αυτής της διεύθυνσης μπορεί να μπει οποιαδήποτε διεύθυνση, η οποία μέσω του κώδικα είναι σε θέση να παρουσιάσει στοιχεία άλλης διεύθυνσης ως δικά της και έτσι ,για παράδειγμα, μπορεί κάποιος να κάνει μέχρι και διαφημίσεις μέσω άλλης ιστοσελίδας και να κερδίζει έτσι πολλά λεφτά παρανόμως.

Ελληνική Εταιρία Ενημέρωσης Γονέων

Σύνδεσμοι Α-Ω | chat

0-2 | 3-5 | 6-12

ParentsCafé.gr

Parents.gr

fc ία & ασφάλεια διατροφή ψυχολογία δραστηριότητ ειδήσεις



Οδηγίες πλοήγησης

Ευγενικές προσφορές για τα μέλη του φόρουμ

**Επιστημονική εποπτεία της κατηγορίας "Ψυχολογία & Ανάπτυξη":**



Διαβάστε εδώ περισσότερα για την συνεργασία με την "Γραμμή - Σύνδεσμος" και την Ε.Ψ.Υ.Π.Ε

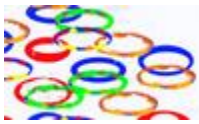
**Το φόρουμ της Ελληνικής Εταιρείας Ενημέρωσης Γονέων** 19/04/2009

Ειδήσεις : Ανακοινώσεις

Οι γονείς συζητούν για πολλά θέματα ανταλλάσοντας απόψεις, γνώσεις και συμβουλές μέσα απο το φόρουμ - δείτε εδώ οδηγίες για την εγγραφή.

**Ζωγραφιές με ρολλά χαρτιού υγείας και καλαμάκια!** 14/10/2010

Δραστηριότητες : Χρώματα



Παιχνίδια με τα χρώματα - με τί ? Αυτά τα τόσο απλά υλικά, έχουν πολύ εντυπωσιακό αποτέλεσμα στα χέρια των μικρών καλλιτεχνών. (Απο 18 μηνών!)

**Εκδηλώσεις και δραστηριότητες για παιδιά!** 21/10/2010

**Εμπνευσμένες Θεατρικές παραστάσεις για παιδιά!** 17/10/2010

Δραστηριότητες : Προτάσεις για εξορμήσεις

Παραστάσεις, κουκλοθέατρο, αλλά και αφηγήσεις παραμυθιών !

**Δράσεις και δραστηριότητες φορέων** 19/10/2010

Ειδήσεις : Διάφορα

22 Οκτωβρίου: Παγκόσμια Ημέρα Ευαισθητοποίησης για τον Τραυλισμό 24 Οκτωβρίου: Παιδικές Εκδηλώσεις με ελεύθερη είσοδο στα Εξάρχεια

**Τα πρώτα μας βίντεο! Origami για παιδιά** 30/04/2010

Δραστηριότητες : Προτάσεις για εξορμήσεις

Παιδικά εργαστήρια και εκδηλώσεις, σε οργανισμούς και σε μουσεία! Τι να κάνετε στον ελεύθερό σας χρόνο!

Ειδήσεις : Ανακοινώσεις

Πώς να φτιάξετε ένα κουτάκι? Τετράγωνο ή σαν πυραμίδα? Ένα ούφο? Μια μίνι ινδιάνικη σκηνή για τα πλειμομπίλ? Τα βίντεο έχουν όλα οδηγίες και υπότιτλους. Τα παιδιά μπορούν να εξασκηθούν στο διάβασμα (βλέπε υπότιτλοι) ενώ τα μεγαλύτερα μαθαίνουν παράλληλα και έννοιες της γεωμετρίας.

**Τηλεφωνική γραμμή στήριξης παιδιών και εφήβων** 14/12/2009

**Βασικοί κανόνες κυκλοφοριακής αγωγής για μικρά παιδιά** 20/09/2010

Υγεία και ασφάλεια


Νέα ευρωπαϊκή τηλεφωνική γραμμή στήριξης παιδιών και εφήβων 116 111

Υγεία και ασφάλεια : Ασφάλεια & Πρόληψη

Συμβουλές ενημέρωσης και ευαισθητοποίησης των μικρών μαθητών και των γονέων τους με στόχο την πρόληψη και μείωση των τροχαίων ατυχημάτων

ΒΙΒΛΙΟΓΡΑΦΙΑ

http://www.us-cert.gov/cas/bulletins/SB2005.html#Multiple
http://www.cs.purdue.edu/homes/fahmy/papers/firewall-analysis.pdf
Kevin Mitnic,''The art of Deception'',2001
http://netsecurity.about.com/cs/hackertools/a/aa121303.htm
http://netsecurity.about.com/cs/hackertools/a/aa030404.htm
http://rootkit.com
http://rootshell.be/~dhar/downloads/Sniffers.pdf
http://www.passwordportal.net
http://www.cert.org/advisories/CA-2001-19.html
http://www.wikipedia.org/wik/Spam_%28electronic%29#History/
www.e-politismos.gr
htt://www.lawnet.gr/lawnet/eofn/2/Cybercrime.asp
http://www.go-online.gr/ebusiness/specials/article.html?article_id=367
http://www.e-crime.gr/nomothesia.htm
http://worldwidespam.info/email-scams
http://www.internet-fraud.com/fraudforum/DCForumID34/100.html#
www.securitymanager.gr
http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-LawAndInternet.html
[1] http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-LawAndInternet.html
www.securitymanager.gr
http://www.fincen.gov/356report.pdf
http://www.wikipedia.gr
http://www.familysafemedia.com/pornography_statistics.html
http://www.schneier.com/crypto-gam-0306.html#1

Sinrod, E and Reilly, W.,(2000).Cyber-crimes: A practical approach to the application of Federal Computer Laws. Santa Clara Computer and high technology law journal.16(2)Σελ.14 κ.ε.

S.Michell and E.Banker(1998)Private Intrusion Response

Αγγελή Ι., «Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο», ΠοινΔικ 12/2001, σελ. 1218 κε, του ιδίου, «Διαδίκτυο (Internet) και ποινικό δίκαιο – Έγκλημα στον κυβερνοχώρο (Cybercrime-Internet Crime)», ΠοιΧρ Ν/2000, σελ. 680 και

''Declaration of the Independence of Cyberpace'', John Perry Barlow

''Stages of the Money Laundering Process'', A report in accordance with paragraph 356 (c) of the USA PATRIOT Act

E.Casey, ''Practical Approaches to Recovering Encrypted Digital Evidence''

M.Elmusharaf (2004), ''Cyber terrorism, a new kind of terrorism''.

B.Collin, ''The future of Cyberterrorism : Where the Physical and Virtual Worlds Converge''

B.Fadia, 2005, ''An Ethical Guide to hacking mobile phones, Macmillan India

[1] E.Casey, ''Practical Approaches to Recovering Encrypted Digital Evidence''

Κων/νος Βλαχόπουλος ,''Ηλεκτρονικό Έγκλημα'', Νομική βιβλιοθήκη,Έκδοση 2007