Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**ΤΟ ΕΓΚΛΗΜΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ** **ΜΟΡΦΕΣ , ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΑΙ ΝΟΜΙΚΗ ΠΡΟΣΤΑΣΙΑ**
Ονοματεπώνυμο Φοιτητή	**ΠΑΝΑΓΙΩΤΙΔΗΣ ΠΑΝΑΓΙΩΤΗΣ**
Πατρώνυμο	**ΚΩΝΣΤΑΝΤΙΝΟΣ**
Αριθμός Μητρώου	**ΜΠΠΛ/ 08048**
Επιβλέπων	**ΣΙΝΑΝΙΩΤΗ ΑΡΙΣΤΕΑ , ΚΑΘΗΓΗΤΡΙΑ**

Ημερομηνία Παράδοσης **Μάϊος 2011**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Σινανιώτη Αριστέα Καθηγήτρια	Δουληγέρης Χρήστος Καθηγητής	Αλεξανδρής Νικόλαος Καθηγητής

«Οι υπολογιστές είναι απίστευτα γρήγοροι, ακριβείς και ηλίθιοι
οι άνθρωποι είναι απίστευτα αργοί, ανακριβείς και ευφυείς
και οι δυο μαζί είναι ισχυροί πέρα από κάθε φαντασία».

Albert Einstein

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Η τεχνολογική έκρηξη την τελευταία δεκαετία μας έφερε όλους ποιό κοντά στον παγκόσμιο ιστό και στην χρήση του υπολογιστη ως εργαλείο που ικανοποιεί τις περισσότερες ανάγκες μας όπως η ηλεκτρονική υποβολή δηλώσεων στην εφορία(www.taxisnet.gr) , πραγματοποίηση online τραπεζικών συναλλαγών (http://www.atebank.gr/ATEbank/WebBanking/Retail , https://secure.alpha.gr) , αγόρες απο ηλεκτρονικά καταστήματα στην Ελλάδα ή στο εξωτερικό (www.e-shop.gr , www.amazon.com) , συμμετοχή σε δημοπρασίες σε πραγματικό χρόνο (www.e-bay.com www.ricardo.gr , http://www.bidbang.com). Άρα, με την ανάπτυξη του διαδικτύου και της τεχνολογίας, έχουμε και άνθιση νέου είδους εγκληματικότητας που αναπτύσσεται με την χρήση της ψηφιακής τεχνολογίας και των ηλεκτρονικών υπολογιστών. Ετσι αναπτύχθηκε και το αντίστοιχο νομικό πλαίσιο που μας προστατεύει απο τέτοιου είδους εγκλήματα.Στην παρούσα μεταπτυχιακή διατριβή θα δούμε και θα αναλύσουμε πως μπορούμε να προστατευτούμε από τέτοιου είδους εγκλήματα και πως προστατευόμαστε απο νομικής πλευράς.

ABSTRACT

Technological explosion in the last decade has brought us all very close the World Wide Web and we use the computer as a tool that can satisfy most of our's requirements such as the electronic submission of tax declarations (www.taxisnet.gr), perform online banking (http://www.atebank.gr/atebank/webbanking/retail , https://secure.alpha.gr), we can buy from online stores in Greece or abroad (www.e-shop.gr , www.amazon.com), participation in auctions in real time (www.e-bay.com , www.ricardo.gr , http://www.bidbang.com). Therefore, the development of Internet and technology boom a new type of crime is growing use of digital technology and computers. Thus was developed and the corresponding legal framework that protects us from such crimes.In this thesis will look at and analyze how we can protect ourselves against such crimes and how it protects from a legal standpoint.

ΚΕΦΑΛΑΙΟ 1ο

Η ΕΞΕΛΙΞΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ : 1960 ΩΣ ΣΗΜΕΡΑ

1.1 ΤΟ ΠΡΩΤΟ ΒΗΜΑ

Όλα ξεκίνησαν στα τέλη της δεκαετίας του ‘60, όταν ο οργανισμός ARPA (Advanced Research Projects Agency) στις ΗΠΑ, προσανατολισμένος σε ερευνητικά προγράμματα υψηλής τεχνολογίας, ξεκίνησε μια ερευνητική δραστηριότητα σχετικά με τα δίκτυα μεταγωγής δεδομένων, τα λεγόμενα Packet Switched Networks. Η τεχνική στα δίκτυα αυτής της υλοποίησης (η οποία σήμερα χρησιμοποιείται ευρύτατα) βασίζεται στον τεμαχισμό σε πακέτα των δεδομένων που πρόκειται να μεταφερθούν. Τα πακέτα αυτά δρομολογούνται από κόμβο σε κόμβο και συναρμολογούνται ξανά όταν φτάσουν στον προορισμό τους.

Το 1962 ανατέθηκε στον Paul Baran της κρατικών συμφερόντων εταιρείας RAND να μελετήσει τον τρόπο με τον οποίο θα μπορούσε η αμερικανική πολεμική αεροπορία να διατηρήσει τον έλεγχο των πυραύλων και των βομβαρδιστικών της μετά από πυρηνική επίθεση. Η έρευνα για ένα αποκεντρωμένο – και άρα λιγότερο τρωτό - σύστημα διοίκησης καταλήγει στην πρόταση ενός δικτύου μεταγωγής πακέτων (packet switched network): κάθε μήνυμα θα χωρίζεται σε πακέτα τα οποία θα διαθέτουν ετικέτα με τον προορισμό τους, θα δρομολογούνται ανεξάρτητα από τον ένα υπολογιστή στον άλλον και θα συναρμολογούνται μετά τη συνολική παράδοση. Έτσι, αν οποιαδήποτε σύνδεση του δικτύου καταστραφεί τα δεδομένα θα μπορέσουν ν α σταλούν από άλλο μονοπάτι. Ο Baran ονόμασε την ιδέα του hot potato routing. Την εποχή εκείνη, ο Ψυχρός Πόλεμος ήταν μεγάλη απειλή για τις ΗΠΑ. Υπήρχε ένα μεγάλο πρόβλημα, σχετικά με τον τρόπο της επιτυχούς επικοινωνίας μεταξύ των αμερικάνικων αρχών, μετά από έναν ενδεχόμενο πυρηνικό πόλεμο. Η Αμερική χρειαζόταν ένα δίκτυο διοίκησης κι ελέγχου που θα συνέδεε πόλεις, πολιτείες και στρατιωτικές βάσεις. Το πρόβλημα όμως ήταν ότι η τεχνική υποδομή ενός τέτοιου δικτύου θα ήταν πάντα τρωτή σε επίθεση, με τα κέντρα οργάνωσης του δικτύου να είναι ευάλωτα και ν’ αποτελούν προφανείς στρατιωτικούς στόχους. Η RAND κατέληξε σε μία πρωτοποριακή για εκείνη την εποχή λύση: Εκ κατασκευής, το δίκτυο δεν θα διέθετε κανένα κέντρο οργάνωσης αλλά ούτε κάποιον κεντρικό υπολογιστή (εξυπηρετητή-server). Ο κάθε κόμβος θα ήταν ίσος με τους υπόλοιπους, όσον αφορά στη δικαιοδοσία του να λαμβάνει και να στέλνει μηνύματα και θα ήταν αυτόνομος και ανεξάρτητος από όλους τους άλλους. Τα μηνύματα θ’ αποστέλλονταν σε μορφή πολλών πακέτων, με κάθε πακέτο να περιλαμβάνει την ηλεκτρονική διεύθυνση του αποστολέα και του παραλήπτη. Αυτά τα πακέτα πληροφοριών θα έπαιρναν το δρόμο τους μέσα στο δίκτυο και θα ταξίδευαν από κόμβο σε κόμβο.

Ο δρόμος που ακολουθούν τα πακέτα θα μπορούσε να είναι διαφορετικός για το κάθε ένα από αυτά: Από τη στιγμή που δεν υπήρχαν χρονικοί περιορισμοί, σημασία είχε μόνο να φτάσει το πακέτο στον προορισμό του κι όχι ο τρόπος με τον οποίον θα έφτανε εκεί. Θα μπορούσε δηλαδή το πρώτο μέρος ενός μηνύματος να περάσει από δέκα πολιτείες και το δεύτερο μέρος μόνον από δύο. Σε περίπτωση που το δεύτερο μέρος θα έφτανε νωρίτερα από το πρώτο, ένας μηχανισμός ανασχηματισμού στον κόμβο προορισμού θα αναλάμβανε την αναδιάταξη των πακέτων δεδομένων ώστε να τοποθετούνται πάντα στη σωστή σειρά. Εάν κάποιος κόμβος έβγαινε εκτός λειτουργίας, τότε τα πακέτα που τυχόν είχε προς μετάδοση θα έμεναν εκεί, μέχρι ν’ αποκατασταθεί η λειτουργία του. Εάν κάποιοι κόμβοι καταστρέφονταν, τότε τα πακέτα τους θα έμεναν σε κάποιους άλλους κόμβους που ίσως τύχαιναν καλύτερης μοίρας. Το δίκτυο θα χαρακτηρίζονταν από μια μορφή πλήρους αναρχίας, ακριβώς επειδή ο κάθε κόμβος θα ήταν ανεξάρτητος αφού δεν θα υπήρχε ούτε συντονιστικό όργανο αλλά ούτε κεντρική διαχείριση. Ακριβώς αυτός ο λόγος θα έκανε το δίκτυο ανθεκτικό σε οποιαδήποτε εχθρική επίθεση. [1]

1.2 ARPANET : Ο ΠΡΟΓΟΝΟΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Κατά τις δεκαετίες του '50 και '60, ο Ψυχρός Πόλεμος βρισκόταν στο αποκορύφωμά του και οι Ηνωμένες Πολιτείες βρίσκονταν σε συνεχή στρατιωτικό και τεχνολογικό ανταγωνισμό με το αντίπαλο δέος, τη Σοβιετική Ένωση. Το 1955 ο Αμερικανός πρόεδρος Eisenhower ανακοίνωσε

[1] http://pacific.jour.auth.gr/internet/page1.1.htm

την πρόθεση της χώρας του να θέσει σε τροχιά γύρω από τη Γη έναν μικρό δορυφόρο, δίνοντας έτσι το σύνθημα για μία κούρσα για την κατάκτηση του Διαστήματος. Η κούρσα αυτή τερματίστηκε μόλις δύο χρόνια αργότερα, με την εκτόξευση του δορυφόρου Sputnik I στις 4 Οκτωβρίου 1957. Το πλήγμα που δέχθηκε το γόητρο των ΗΠΑ ήταν τόσο ισχυρό, ώστε για πρώτη φορά μετά τη ρίψη της ατομικής βόμβας δεκατρία χρόνια νωρίτερα η χώρα ένιωσε τρωτή.

Το γεγονός αυτό τροφοδότησε τη στροφή της Αμερικής προς την τεχνολογία και σχεδόν αμέσως **το Υπουργείο Άμυνας (Department of Defense - DoD) ίδρυσε τον οργανισμό ARPA (Advanced Research Projects Agency),** με σκοπό να συντονίσει και να προωθήσει την τεχνολογική έρευνα μεταξύ των διάφορων ερευνητικών ινστιτούτων και εκπαιδευτικών ιδρυμάτων σε όλη την επικράτειας της χώρας. Προτεραιότητα δόθηκε στην ανάπτυξη των υπολογιστών και της πληροφορικής, κλάδοι που είχαν μόλις εμφανιστεί αλλά παρουσίαζαν ήδη ισχυρή ανάπτυξη, με πολλά πειραματικά προγράμματα, λειτουργικά συστήματα και αρχιτεκτονικές πλατφόρμες.

Αρχικά, το ενδιαφέρον του ARPA[2] επικεντρώθηκε σε τεχνολογικά θέματα στρατιωτικού ενδιαφέροντος, που θα εξασφάλιζαν την εδαφική ακεραιότητα των ΗΠΑ, όπως η έρευνα για το Διάστημα, η βαλλιστική πυραύλων, η διεξαγωγή και παρακολούθηση πυρηνικών δοκιμών. Πολύ σύντομα μετατράπηκε στο σημαντικότερο ερευνητικό κέντρο στρατιωτικών θεμάτων, διαθέτοντας έναν τεράστιο προϋπολογισμό, προσλαμβάνοντας δεκάδες κορυφαίους επιστήμονες και προωθώντας τη συνεργασία με τα πιο αξιόλογα ερευνητικά εργαστήρια στη χώρα. Έτσι, η ανάγκη για συνεχή επικοινωνία και συνεργασία με ιδρύματα που βρίσκονταν διάσπαρτα σε διάφορες και αρκετά απέχουσες μεταξύ τους τοποθεσίες, οδήγησε αναπόφευκτα στην έρευνα στον τομέα των επικοινωνιών.

Η πρώτη καταγεγραμμένη περιγραφή ενός δικτύου κατά τα πρότυπα του σημερινού Internet έγινε τον Αύγουστο του 1962 από τον **J.C.R. Licklider του MIT**. Μέσω μία σειράς ανεπίσημων μηνυμάτων, ο Licklider περιέγραψε ένα παγκόσμιο δίκτυο συνδεδεμένων υπολογιστών που ονόμασε "Galactic Network". Μέσω αυτού, κάθε άνθρωπος θα είχε πρόσβαση σε δεδομένα και προγράμματα από οποιαδήποτε γεωγραφική περιοχή. Μόλις λίγους μήνες αργότερα, και συγκεκριμένα στις 4 Οκτωβρίου 1962, ο οργανισμός ARPA ξεκίνησε ένα νέο ερευνητικό πρόγραμμα με την ονομασία Defense Advanced Research Projects Agency (DARPA), τοποθετώντας ως επικεφαλής τον John Licklider. Κατά τη θητεία του στο πρόγραμμα αυτό, ο Licklider κατάφερε να πείσει και τους διαδόχους του **Ivan Sutherland, Bob Taylor και Lawrence G.Roberts**, για τη σπουδαιότητα της ιδέας του δικτύου μεταξύ υπολογιστών.

Παράλληλα με τη θεωρητική σύλληψη του Διαδικτύου, ο **Leonard Kleinrock**[3], που ήδη εργαζόταν για το ARPA, ανέπτυσσε εναλλακτικούς τρόπους για την αποστολή δεδομένων. Θεώρησε ότι η διαδικασία κατάτμησης της αρχικής πληροφορίας σε "πακέτα", αποστολής τους ξεχωριστά και επανασύνδεσής τους στον τελικό προορισμό, ήταν περισσότερο συμφέρουσα και ευέλικτη από τη συμβατική πρακτική, που υπαγόρευε το "άνοιγμα" μίας και μοναδικής γραμμής και αποστολή της πληροφορίας μέσω αυτής. Η νέα μέθοδος πλεονεκτούσε στο ότι δεν βασιζόταν σε μία μόνο γραμμή για την αποστολή των δεδομένων, ενώ παράλληλα με την κατάτμηση των δεδομένων σε πακέτα γίνονταν δυσκολότερες η παρεμβολή και σύλληψη της αρχικής πληροφορίας. Τα δύο αυτά πλεονεκτήματα δημιουργούσαν ένα πιο αξιόπιστο και ασφαλές δίκτυο, οδηγώντας το Leonard Kleinrock στη δημοσίευση της πρώτης εργασίας του με θέμα την τεχνολογία "packet switching" τον Ιούλιο του 1964.

Ο J.C.R. Licklider ήταν ο πρώτος που περιέγραψε ένα δίκτυο κατά τα σημερινά πρότυπα του Internet.

Ο Leonard Kleinrock αποκαλείται και "πατέρας του Internet", λόγω της εργασίας του για τα δίκτυα packet-switching.

Κατά τα δύο επόμενα χρόνια, η έρευνα για την ανάπτυξη του πρώτου δικτύου επιταχύνθηκε και στα τέλη του 1966 **ο νέος επικεφαλής του προγράμματος DARPA, Lawrence G. Roberts, παρουσίασε τα πρώτα σχέδια για το ARPANET.** Στο συνέδριο όπου ανακοίνωσε το

[2] http://www.dei.isep.ipp.pt/~acc/docs/arpa--1.html

[3] http://www.lk.cs.ucla.edu/index.html

γεγονός αυτό, έγινε προφανές ότι χωρίς να γνωρίζουν η μία για την έρευνα της άλλης, οι ομάδες έρευνας του MIT, National Physics Laboratory και RAND Corporation, εργάζονταν ταυτόχρονα για την ανάπτυξη δικτύων ευρείας περιοχής (Wide Area Networks), και έτσι οι καλύτερες τεχνολογίες που είχαν ήδη αναπτυχθεί ενσωματώθηκαν στο σχεδιασμό του ARPANET.

Η τελική απαίτηση πριν από την υλοποίηση του δικτύου ήταν η ανάπτυξη του πρωτοκόλλου που υα επέτρεπε στους υπολογιστές την αποστολή και λήψη μηνυμάτων και δεδομένων, γνωστού και ως **Interface Message Processor [4](IMP)**. Ο σχετικός διαγωνισμός έληξε τον Δεκέμβριο του 1968 και η εταιρεία που προσλήφθηκε για την ανάπτυξή του ήταν η Bolt Beranek and Newman (BBN). Τον Οκτώβριο του 1969 ήρθε, επιτέλους, η στιγμή για να δοκιμαστεί και στην πράξη η θεωρία των δικτύων. Σε υπολογιστές των Πανεπιστημίων UCLA και Stanford εγκαταστάθηκαν IMP και στόχος του πρώτου αυτού πειράματος ήταν η σύνδεση (login) των φοιτητών του UCLA στους υπολογιστές του Stanford, η πρόσβαση στις βάσεις δεδομένων του τελευταίου και η αποστολή πληροφοριών. Επειτα από ορισμένες αποτυχημένες προσπάθειες, η σύνδεση επιτεύχθηκε και το δίκτυο ARPANET είχε μόλις δημιουργηθεί.

Μέχρι τον Δεκέμβριο του 1969 το δίκτυο αποτελούσαν τέσσερις συνολικά hosts, αφού στους αρχικούς υπολογιστές προστέθηκαν τα ερευνητικά κέντρα της Santa Barbara και Utah. Κατά τους μήνες που ακολούθησαν, οι επιστήμονες εργάστηκαν για τη βελτιστοποίηση του λογισμικού και την επέκταση των δυνατοτήτων του δικτύου. Παράλληλα, τον Δεκέμβριο του 1970 το Network Working Group (NWG), υπό την εποπτεία του S.Crocker, ολοκλήρωσε το αρχικό πρωτόκολλο Host-to-Host ομαζόμενο Network Control Protocol (NCP), και η εγκατάστασή του σε ολόκληρο το δίκτυο επέτρεψε την παραγωγή των πρώτων εφαρμογών. Καθ' όλο το χρονικό αυτό διάστημα, η ανάπτυξη του ARPANET ήταν συνεχής και τον Δεκέμβριο του 1971 το δίκτυό του συνέδεε 23 hosts μεταξύ τους.

1.3 ΑΠΟ ΤΟ ARPANET ΣΤΟ INTERNET

Τον Οκτώβριο του 1972 το ARPANET γνώρισε για πρώτη φορά τα φώτα της δημοσιότητας στο πλαίσιο του πρώτου Διεθνούς Συνεδρίου για Υπολογιστές και Επικοινωνίες (International Computer Communication Conference ICCC), που έγινε στην Ουάσινγκτον. Ο **Bob Kahn[5]**, καθηγητής στο MIT και μετέπειτα ερευνητής στην εταιρεία BBN, οργάνωσε μία πολύ μεγάλη και επιτυχημένη παρουσίαση του δικτύου συνδέοντας υπολογιστές από σαράντα διαφορετικές τοποθεσίες. Το επίτευγμα αυτό κέντρισε το ενδιαφέρον της επιστημονικής κοινότητας και σύντομα έκαναν την εμφάνισή τους πολλά ακόμη δίκτυα. Στην επιτάχυνση της ανάπτυξης και διάδοσης του ARPANET συνέβαλε τα μέγιστα και η εφεύρεση του ηλεκτρονικού ταχυδρομείου από τον **Ray Tomlinson.** Σκοπός του Tomlinson, που εργαζόταν στην εταιρεία BBN, ήταν η διευκόλυνση των ερευνητών του ARPANET για τη μεταξύ τους επικοινωνία και συνεργασία, ενώ σύντομα ενσωμάτωσε στο βασικό πρόγραμμα αρκετές δυνατότητες που επέτρεπαν μία περιορισμένη διαχείριση των emails. [6]

Το 1973 οι ερευνητές του ARPA (Khan), σε στενή συνεργασία με επιστήμονες από το Stanford (**Vint Cerf**), ξεκίνησαν ένα νέο ερευνητικό πρόγραμμα με σκοπό την ανάπτυξη τεχνικών που θα επέτρεπαν τη σύνδεση ετερογενών δικτύων που βασίζονταν στην τεχνολογία packet switching. Το πρόγραμμα αυτό ονομάστηκε Internetting και το σύστημα δικτύων που προέκυψε από τη συγκεκριμένη έρευνα έγινε γνωστό ως Internet. Έναν χρόνο αργότερα, ολοκληρώθηκε η ανάπτυξη μίας κοινής "γλώσσας" που θα επέτρεπε στα διαφορετικά αυτά δίκτυα να επικοινωνούν μεταξύ τους. Η γλώσσα αυτή έγινε γνωστή ως Transmission Control Protocol/Internet Protocol ή απλώς TCP/IP και η ανάπτυξή της σηματοδότησε μία κρίσιμη καμπή στην ανάπτυξη των δικτύων.

Ενα από τα κυριότερα χαρακτηριστικά του TCP/IP ήταν η ανοικτή αρχιτεκτονική του με τελικό σκοπό την υλοποίηση του οράματος του Licklider για το "Galactic Network[7]". Έτσι, κάθε

---

[4] http://www.livinginternet.com/i/ii_imp.htm

[5] http://en.wikipedia.org/wiki/Bob_Kahn

[6] http://www.epaggelmaties.com/writer/2001-2003/internethistory.html

[7] http://www.thehistoryof.net/history-of-web-hosting.html

δίκτυο στο εσωτερικό του θα έπρεπε να μπορεί να λειτουργεί ανεξάρτητα από τα υπόλοιπα, χωρίς παράλληλα να τίθενται περιορισμοί και να απαιτούνται μετατροπές για τη συνεργασία του με το Internet. Επίσης, μέσα σε κάθε δίκτυο θα έπρεπε να υπάρχει κάποια πύλη (gateway), που θα επέτρεπε τη σύνδεσή του με τον "εξωτερικό κόσμο". Η πύλη αυτή θα ήταν ένας υπολογιστής αρκετά ισχυρός ώστε να ανταποκρίνεται στην κίνηση του δικτύου, ο οποίος θα εκτελούσε το απαραίτητο λογισμικό που θα αναλάμβανε την αποστολή και λήψη των "πακέτων". Ταυτόχρονα, το λογισμικό θα έπρεπε να μη συγκρατεί πληροφορίες για τη διερχόμενη κίνηση, με τελικό στόχο τη μείωση του φόρτου εργασίας του υπολογιστή, την επιτάχυνση των δικτύων και την απομάκρυνση του κινδύνου ελέγχου και λογοκρισίας των διερχόμενων μηνυμάτων.

Ως προς τη λειτουργία του πρωτοκόλλου, ο σχεδιασμός του προέβλεπε την προώθηση των "πακέτων" διαμέσου της ταχύτερης διαδρομής, ενώ στην περίπτωση που κάποιος υπολογιστής είχε τεθεί εκτός λειτουργίας ή καθυστερούσε σημαντικά, τα "πακέτα" θα ακολουθούσαν εναλλακτικό δρόμο. Τέλος, μία εξίσου σημαντική αρχή του TCP/IP είναι ο χαρακτηρισμός του ως πρωτόκολλο best effort. Με απλά λόγια αυτό σήμαινε ότι σε περίπτωση που κάποιο "πακέτο" δεν έφτανε στον προορισμό του, τότε θα έπρεπε ο αποστολέας να το ξαναστείλει αυτόματα.

Ένα σημαντικό σημείο στο οποίο θα πρέπει να σταθούμε είναι ότι το σύστημα αυτό σχεδιάστηκε για έναν κόσμο που βασιζόταν σε mainframes ιδιοκτησίας ορισμένων πολύ μεγάλων εταιρειών, κυβερνήσεων και πανεπιστημίων. Επομένως, το σύστημα θεωρούσε δεδομένο ότι το Internet θα αποτελούνταν από ένα πολύ περιορισμένο αριθμό υπο-δικτύων, υπόθεση που στη συνέχεια ανατράπηκε. Ετσι, αν και το πρωτόκολλο TCP/IP πρωτοπαρουσιάστηκε κατά το έτος 1974, απαιτήθηκαν πολλές μετατροπές και επανασχεδιάσεις μέχρις ότου ολοκληρωθεί και να γίνει συνολικά αποδεκτό. Μία από τις σημαντικότερες παραδοχές, που στη συνέχεια ξεπεράστηκαν από τις εξελίξεις, αφορούσε στη χωρητικότητα του συστήματος διευθύνσεων IP. Οι 32-bit διευθύνσεις χρησιμοποιούσαν τα πρώτα 8 bit για τη σήμανση του δικτύου και τα υπόλοιπα 24 bit για τον καθορισμό του συγκεκριμένου host στο δίκτυο. Οι ερευνητές είχαν την εποχή εκείνη υπόψη τους ένα μοντέλο Internet που θα λειτουργούσε σε εθνικό επίπεδο και θα συνέδεε έναν μικρό αριθμό δικτύων. Για το λόγο αυτόν, τα 256 δίκτυα που υποστήριζε και συνεχίζει να υποστηρίζει το σύστημα φαίνονταν να επαρκούν. Στη σημερινή εποχή, οι δεκάδες εκατομμύρια υπολογιστές που υπάρχουν δεν είναι δυνατόν να εξυπηρετηθούν κατά τον ίδιο τρόπο, και έτσι τη λύση υπόσχεται να δώσει το πρωτόκολλο IPv6.

1.4 ΒΑΣΙΚΕΣ ΥΠΗΡΕΣΙΕΣ ΤΟΥ INTERNET

Το Internet προσφέρει μία σειρά από υπηρεσίες στους χρήστες του, οι σημαντικότερες από τις οποίες είναι:

i. **E-mail:** για την αποστολή ηλεκτρονικών μηνυμάτων
ii. **USENET newsgroups:** ειδικές θεματικές ομάδες συζητήσεων
iii. **TELNET:** για τον χειρισμό υπολογιστών εξ' αποστάσεως
iv. **FTP *(File Transfer Protocol)*:** για την μεταφορά αρχείων από ένα υπολογιστικό σύστημα σε κάποιο άλλο
v. **IRC *(Internet Relay Chat)*:** γραπτή συνομιλία που επιτρέπει την επικοινωνία σε πραγματικό χρόνο
vi. **WWW *(World Wide Web)*:** για την παρουσίαση πληροφοριών και δεδομένων μέσω του διαδικτύου υπό την μορφή κειμένου, εικόνα, ήχου και video

Η εργασία του Lawrence G. Roberts του MIT αποτέλεσε το προσχέδιο του επερχόμενου ARPANET.

Οι C.S. Carr, S. Crocker και Vincent G. Cerf (στη φωτογραφία) εξέδωσαν το 1970 την πρώτη εργασία για το αρχικό πρωτόκολλο του ARPANET.

Η έρευνα του Paul Baran για τα δίκτυα packet-switching αποτέλεσε το θεμέλιο του σημερινού Διαδικτύου.

1.4.1 Η ΓΕΝΝΗΣΗ ΤΟΥ World Wide Web

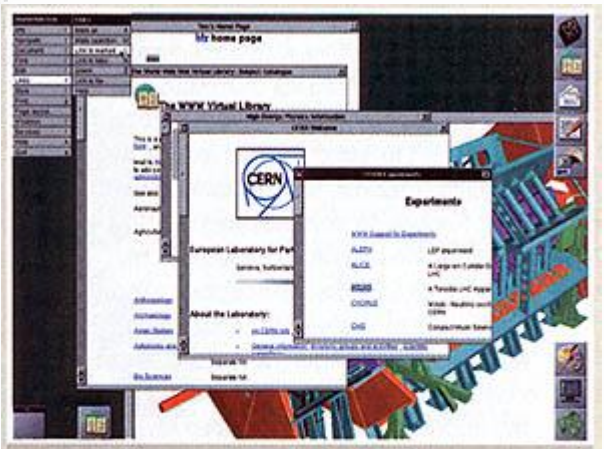
Η ιδέα του World Wide Web πρωτοεμφανίστηκε το 1989 από τον Tim Berners-Lee και άλλους επιστήμονες του οργανισμού CERN στη Γενεύη. Στόχος του ήταν η δημιουργία ενός δικτύου από sites, που θα επέτρεπαν την αναζήτηση και μεταφορά των πληροφοριών που περιέχουν μέσω ενός ειδικού πρωτοκόλλου που έγινε γνωστό ως Hypertext Transfer Protocol (HTTP). Εναν χρόνο αργότερα, ο Tim Berners-Lee ανέπτυξε ένα πρόγραμμα "browser/editor", το οποίο ονόμασε World Wide Web και άρχισε να το διαθέτει δωρεάν μέσω ενός FTP site. Το επόμενο βήμα ήταν η ανάπτυξη ενός βελτιωμένου "browser", δηλαδή ενός συστήματος που θα επέτρεπε σε συνδέσμους (links) να "κρύβονται" μέσα στο κείμενο και για το σκοπό αυτό χρησιμοποίησε τη γλώσσα HyperText Markup Language (HTML).

Αρχικά, η ανάπτυξη του WWW ήταν μικρή και μέχρι το τέλος του 1992 υπήρχαν μόλις 50 Web sites. Εναν χρόνο μετά, ο αριθμός αυτός αυξήθηκε σε 150. Το 1993 ο Mark Andreesen του NCSA (National Center for SuperComputing Applications) στο Illinois κυκλοφόρησε το Mosaic X. Το πρόγραμμα ήταν εύκολο στην εγκατάσταση και τη χρήση, ενώ συνοδευόταν από 24-ωρη τεχνική υποστήριξη. Η δοκιμαστική έκδοσή του παραχωρήθηκε δωρεάν σε διάφορα πανεπιστήμια και σύντομα γνώρισε τεράστια διάδοση. Εως το 1994 δεκάδες χιλιάδες αντίγραφά του είχαν εγκατασταθεί σε υπολογιστές παγκοσμίως. Οι υπηρεσίες που παρείχε οδήγησαν όχι μόνο στην περαιτέρω ανάπτυξη του World Wide Web, αλλά και στην εξάπλωση των προσωπικών υπολογιστών. Ο Παγκόσμιος Ιστός είχε γίνει πραγματικότητα και το μέγεθος καθώς και οι υπηρεσίες που προσφέρει αυξάνονται έκτοτε εκθετικά.

Ο "πατέρας" του World Wide Web είναι ο Βρετανός φυσικός Tim Berners-Lee. Σήμερα είναι 44 χρόνων (2002) και εργάζεται στο MIT (Massachusetts Institute of Technology), ενώ τον Μάρτιο του 1999 αναδείχθηκε από το "Time magazine" ως ένας από τους σημαντικότερους εκατό ανθρώπους του 20ου αιώνα. Σύμφωνα με τον ίδιο, η δημιουργία και διάδοση του Παγκόσμιου Ιστού υπήρξαν περισσότερο δύσκολες απ' ό,τι πιστεύουν οι περισσότεροι. Σε συζητήσεις που είχε την εποχή εκείνη με συναδέλφους του στα εργαστήρια του CERN (Ελβετία) και εταιρείες παραγωγής λογισμικού, η ιδέα αντιμετωπίστηκε μάλλον "χλιαρά". Η κυριότερη αιτία πίσω από την απρόσμενη αυτή αντίδραση ήταν η δυσκολία που παρουσίαζε η περιγραφή της. "Πριν να εφευρεθεί ο World Wide Web, ήταν πολύ δύσκολο να εξηγήσει κανείς τι ακριβώς ήταν...", απαντά συχνά ο ίδιος.

Απαιτήθηκαν αλλεπάλληλες κρούσεις προς τους προϊσταμένους του, ώστε να λάβει τελικά την έγκρισή τους για να ασχοληθεί με το συγκεκριμένο πρόγραμμα. Το 1991, συνεργαζόμενος με το Βέλγο συνάδελφό του Robert Cailliau, κατάφερε να σχεδιάσει τα βασικά hypertexts πρωτόκολλα και την πλατφόρμα browser-server, που σήμερα αποτελούν τον πυρήνα του Παγκόσμιου Ιστού. Ανάλογα, όμως, προβλήματα αντιμετώπισε και με την εύρεση της κατάλληλης ονομασίας για τον εικονικό κόσμο που οραματιζόταν. Αφού απέρριψε όρους όπως "Mesh" (ηχητικά παρεμφερής με την λέξη "mess" που σημαίνει ακαταστασία), "MOI" (Mine Of Information, δηλαδή "ορυχείο πληροφοριών") και "TIM" (The Information Mine), κατέληξε στον όρο "World Wide Web", αντιπροσωπεύοντας την πολλαπλή συνδεσιμότητα μεταξύ των πληροφοριών.

Σήμερα, ο Tim Berners-Lee, αποτελεί τη ζωντανή απόδειξη ότι η υπομονή και επιμονή ενός ανθρώπου μπορεί όντως να αλλάξει τον κόσμο. Η έμπνευση, η ικανότητα και η συστηματική εργασία του οδήγησαν στη δημιουργία του Παγκόσμιου Ιστού, μίας έννοιας που έχει πλέον εισβάλει στην καθημερινή ζωή μας. Το σημαντικότερο, όμως, είναι ότι η έλλειψη υποστήριξης εκ μέρους πολλών οργανισμών και εταιρειών δεν κατάφερε να σταθεί εμπόδιο στα σχέδιά του, αποδεικνύοντας έτσι την αφοσίωση που επέδειξε σε όλη τη διάρκεια ανάπτυξης του World Wide Web.



Screenshot από τον πρώτο browser με γραφικό περιβάλλον που αναπτύχθηκε το 1990 και ονομαζόταν "World Wide Web". Ετρεχε σε υπολογιστή NeXT και διέθετε χρώματα και εικόνες.

1.5 ΣΤΑΤΙΣΤΙΚΑ ΣΤΟΙΧΕΙΑ ΧΡΗΣΗΣ INTEPNET

Αν μία εικόνα αξίζει χίλιες λέξεις, τότε ο καλύτερος τρόπος για να εμπεδώσουμε την εξέλιξη του Internet και να συνειδητοποιήσουμε το βαθμό διείσδυσής του σε παγκόσμια κλίμακα είναι να μελετήσουμε τα διαγράμματα που παραθέτουμε σε αυτήν την ενότητα. Μέσα από αυτά αναδεικνύεται το θετικό αποτέλεσμα που είχε η συνδυασμένη προσπάθεια εκατοντάδων

WORLD INTERNET USAGE AND POPULATION STATISTICS

World Regions	Population (2009 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2009	Users % of Table
Africa	991,002,342	4,514,400	**86,217,900**	8.7 %	1,809.8 %	4.8 %
Asia	3,808,070,503	114,304,000	**764,435,900**	20.1 %	568.8 %	42.4 %
Europe	803,850,858	105,096,093	**425,773,571**	53.0 %	305.1 %	23.6 %
Middle East	202,687,005	3,284,800	**58,309,546**	28.8 %	1,675.1 %	3.2 %
North America	340,831,831	108,096,800	**259,561,000**	76.2 %	140.1 %	14.4 %
Latin America/Caribbean	586,662,468	18,068,919	**186,922,050**	31.9 %	934.5 %	10.4 %
Oceania / Australia	34,700,201	7,620,480	**21,110,490**	60.8 %	177.0 %	1.2 %
WORLD TOTAL	6,767,805,208	360,985,492	**1,802,330,457**	**26.6 %**	399.3 %	100.0 %

ερευνητών και επιστημόνων σε πολλές χώρες παγκοσμίως, οι οποίοι εργάστηκαν για τη δημιουργία του συνδεδεμένου κόσμου που γνωρίζουμε σήμερα. Μελετώντας προσεκτικά το διάγραμμα που αναφέρεται στο μέγεθος του Internet, παρατηρούμε ότι κατά τα πρώτα 10 χρόνια (από το 1980 έως το 1989), ο ρυθμός διάδοσής του υπήρξε μάλλον βραδύς. Αν και ο συνολικός αριθμός των συνδεδεμένων υπολογιστών (hosts) αυξήθηκε από τους 213 στους 159.000, αλλαγή αρκετά εντυπωσιακή, η πραγματικά εκθετική αύξησή του συντελείται κατά τα χρόνια που ακολουθούν, φθάνοντας σήμερα σε περίπου 100 εκατομμύρια hosts.

Η ανάπτυξη και η σταδιακή καθιέρωση του Παγκόσμιου Ιστού, επέτρεψε σε ανθρώπους με ελάχιστες τεχνικές γνώσεις να εκμεταλλευτούν τον τεράστιο πλούτο ηλεκτρονικών πληροφοριών. Σε αντίθεση, όμως, με την πορεία του Internet, το μέγεθος του World Wide Web παρουσιάζει έντονα σημάδια κορεσμού. Κατά το τελευταίο έτος ο αριθμός των δικτυακών τόπων παγκοσμίως αυξήθηκε με έναν ιδιαίτερα αργό ρυθμό, ενώ αξίζει να σημειωθεί ότι τους τελευταίους δύο μήνες του 2001 ο αριθμός των sites παγκοσμίως μειώθηκε! Είναι, μάλιστα, η δεύτερη φορά που παρατηρείται το φαινόμενο αυτό. Η πρώτη ήταν πριν από περίπου 10 χρόνια, ενώ οι αιτίες θα πρέπει να αναζητηθούν στην κρίση που διέρχεται τον τελευταίο καιρό το ηλεκτρονικό εμπόριο, οδηγώντας πολλές online επιχειρήσεις στη χρεοκοπία. Τα δυσάρεστα αυτά νέα, πάντως, δεν αρκούν για να επισκιάσουν το λαμπρό μέλλον του Διαδικτύου, αφού ο αριθμός των χωρών και των χρηστών με πρόσβαση στο Internet συνεχίζει να αυξάνεται.

Βλέπουμε λοιπόν ότι την τελευταία δεκαετία έχει υπάρξει διείσδυση στην χρήση του Ιντερνετ στο 26,6% του παγκόσμιου πληθυσμού σημειώνοντας αύξηση κοντά στο 400% απο την προηγούμενη δεκαετία. Η μεγαλύτερη ανάπτυξη παρατηρήται στην Αφρική ,1.809 %, όμως παρόλα αυτά η χρήση στο σύνολο του πληθυσμού της είναι ιδαίτερα χαμηλή μόλις 8,7%.Στην Ευρώπη οστόσο ο μισός πλήθυσμος κάνει χρήση του ιντερνετ παρουσιάζοντας αύξηση κατα 305%.Η Βόρεια Αμερική έχει την πρωτιά αφού τα ¾ του πληθυσμού είναι χρήστες του ιντερνετ και πως θα γινόταν διαφοφορετικά εξάλλου αφού απο εκεί ξεκίνησε αυτη η τεχνολογική επανάσταση.

Στην Ελλάδα βλέπουμε μια θεαματική αύξηση των χρηστών του internet την τελευταία δεκαετία κατά 393% καταφέρνοντας να αγγίξουμε σχεδόν το 50 % απο το σύνολο του πληθυσμού.Επιπλέον οι ευρυζωνικές συνδέσεις στο internet ξεπέρασαν το 1,5 εκ μέχρι το τέλος του 2009.[8]

[8] http://www.internetworldstats.com/stats.htm

Internet Usage in Europe

EUROPE	Population (2009 Est.)	Internet Users, Latest Data	Penetration (% Population)	User Growth (2000-2009)	% Users Europe
Estonia	1,299,371	888,100	68.3 %	142.3 %	0.2 %
Faroe Islands	48,856	37,500	76.8 %	1,150.0 %	0.0 %
Finland	5,250,275	4,382,700	83.5 %	127.4 %	1.0 %
France	62,150,775	43,100,134	69.3 %	407.1 %	10.1 %
Germany	82,329,758	61,973,100	75.3 %	158.2 %	14.6 %
Gibraltar	28,796	9,853	34.2 %	515.8 %	0.0 %
Greece	10,737,428	4,932,495	45.9 %	393.2 %	1.2 %
Guernsey & Alderney	65,484	46,100	70.4 %	130.5 %	0.0 %
Hungary	9,905,596	5,873,100	59.3 %	721.4 %	1.4 %
Iceland	306,694	285,700	93.2 %	70.1 %	0.1 %
Ireland	4,203,200	2,830,100	67.3 %	261.0 %	0.7 %

ΚΕΦΑΛΑΙΟ 2ο

Cyber - CRIME

2.1 ΟΡΙΣΜΟΙ

Ως **ηλεκτρονικό έγκλημα** (electronic crime) θα μπορούσε να *θεωρηθεί* κάθε παράνομη πράξη για τη διάπραξη, αλλά και για την αντιμετώπιση της οποίας θεωρείται απαραίτητη η γνώση της ψηφιακής τεχνολογίας.

Στα ηλεκτρονικά εγκλήματα έχει διαπιστωθεί ότι συνήθως εμπλέκεται είτε από την πλευρά του δράστη είτε από την πλευρά του θύματος, ένας τουλάχιστον ηλεκτρονικός υπολογιστής (Η/Υ). Ο ηλεκτρονικός αυτός υπολογιστής στην περίπτωση αυτή μπορεί να είναι αντικείμενο , μέσο ακόμα και "τόπος" διάπραξης του εγκλήματος αυτού.

Ετσι ο υπολογιστής αυτός θα ήταν δυνατό να είναι το προϊόν κλοπής ή ληστείας ή να χρησιμοποιήθηκε για παράνομη εισβολή του χρήστη του στα αρχεία ενός άλλου υπολογιστή ή για την τέλεση απάτης σε βάρος κάποιου άλλου χρήστη ή τέλος στο σκληρό του δίσκο να μπορεί να βρει κανείς ίχνη τέλεσης κάποιας αξιόποινης πράξης όπως π.χ. πορνογραφικό υλικό το οποίο έχει διακινηθεί μέσω του διαδικτύου.

Τα ηλεκτρονικά εγκλήματα μπορούμε να υποθέσουμε ότι διαφέρουν από τα παραδοσιακά εγκλήματα στα εξής χαρακτηριστικά σημεία:

- Διαπράττονται συνήθως από μακρινή απόσταση,
- Ο εντοπισμός του ηλεκτρονικού εγκληματία είναι τεχνολογικά περίπλοκος,
- Αποδίδουν μεγάλα κέρδη με μικρό κίνδυνο ανακάλυψης του δράστη τους,
- Ο αριθμός των θυμάτων τους συγκρινόμενος με εκείνο των παραδοσιακών εγκλημάτων είναι κατά πολύ μεγαλύτερος
- Οι οικονομικές απώλειες που προξενούνται στα "ψηφιακά" θύματα είναι πολύ μεγαλύτερες από εκείνες των θυμάτων των παραδοσιακών εγκλημάτων και
- Στο μεγαλύτερο μέρος τους δεν καταγράφονται από καμμία επίσημη αρχή.

Τα τέσσερα δε τελευταία από τα παραπάνω χαρακτηριστικά τους πιστεύουμε ότι τα κατατάσσουν στο χώρο των οικονομικών εγκλημάτων.

"Τόπος" τέλεσής τους είναι ο αποκαλούμενος **κυβερνοχώρος** ο οποίος προσδιορίζεται[9] ως, "*....το σύνολο των ηλεκτρονικών κόσμων, όπως το Διαδίκτυο, όπου οι άνθρωποι έρχονται σε αλληλεπίδραση μέσω συνδεδεμένων υπολογιστών. Καθοριστικό χαρακτηριστικό του κυβερνοχώρου είναι ότι η επικοινωνία είναι ανεξάρτητη από την υλική υπόσταση."*

Το σύνολο επομένως, των ψηφιακών εγκλημάτων που τελούνται στον κυβερνοχώρο (cyberspace) συνιστούν την ***ψηφιακή εγκληματικότητα (digital criminality).***

Στη σημερινή εποχή παρατηρείται μεγάλη αύξηση των ψηφιακών εγκλημάτων και γενικά της ψηφιακής εγκληματικότητας, η οποία είναι ανάλογη με την συνεχώς αυξανόμενη χρήση του Ιντερνετ. Ανάλογη είναι και η ποικιλία των μορφών των διαφόρων ψηφιακών εγκλημάτων.

Σημαντική ώθηση προς την κατεύθυνση αυτή έχει δώσει η διάδοση του ηλεκτρονικού εμπορίου (e-commerce). Οι εμπορικές συναλλαγές που πραγματοποιούνται στον κυβερνοχώρο προσφέρουν τη δυνατότητα διάπραξης διαφόρων οικονομικών εγκλημάτων. Απάτες, κλοπές πνευματικής ιδιοκτησίας και βιομηχανική κατασκοπεία είναι ορισμένα από αυτά. Τράπεζες και διάφοροι άλλοι οικονομικοί οργανισμοί υφίστανται τεράστιες οικονομικές απώλειες εξαιτίας της παράνομης δραστηριότητας οργανωμένων και μη ψηφιακών εγκληματιών που επεκτείνουν τη δράση τους σε όλη την υφήλιο εκμεταλλευόμενοι τις δυνατότητες μεταφοράς μεγάλων χρηματικών ποσών, που τους προσφέρει το διαδίκτυο. Το γεγονός αυτό έχει επικεντρώσει το ενδιαφέρον μεγάλων και μικρών επιχειρήσεων αλλά και ιδιωτών χρηστών στο θέμα της ασφάλειας των υπολογιστικών τους συστημάτων, αλλά και γενικότερα της ασφάλειας των δικτυακών τους δραστηριοτήτων την οποία θα μπορέσουν να επιτύχουν με τη βοήθεια σχετικών τεχνολογικών μέσων όπως π.χ. αντiικών προγραμμάτων (antivirus), τειχών προστασίας (firewalls) κ.ά.

Στην επίτευξη της ασφάλειας αυτής έχει στρέψει την προσοχή του βέβαια, και ο νομοθέτης με τη θέσπιση διατάξεων πρόβλεψης και τιμωρίας της εγκληματικής συμπεριφοράς που την απειλεί. Για το λόγο αυτό απαιτούνται διαρκώς νέοι νόμοι που θα προσδιορίζουν επακριβώς την τεχνολογικά προηγμένη αυτή εγκληματική συμπεριφορά και θα επιτρέπουν την πέραν πάσης αμφιβολίας καταδίκη των ψηφιακών δραστών.

Για την αντιμετώπιση όμως ενός σύνθετου κοινωνικού φαινομένου όπως είναι η ψηφιακή εγκληματικότητα είναι απαραίτητη η καταγραφή της, η οποία γίνεται με σκοπό τη διαπίστωση των πραγματικών της διαστάσεων. Ωστόσο θα πρέπει να παρατηρήσουμε πως η ψηφιακή εγκληματικότητα,

---

[9] *"Λεξικό Διαδικτύου και Δικτύων της Microsoft"* (σελ. 90 - 1)

όπως είδαμε όταν παραπάνω προσδιορίσαμε την έννοιά της, εκδηλώνεται στον κυβερνοχώρο δηλ. σε έναν "τόπο εγκλήματος" που δεν έχει υλικές διαστάσεις. Το γεγονός αυτό καθώς και οι τεχνολογικά εξειδικευμένες μορφές των ψηφιακών εγκλημάτων που τη συνιστούν καθιστά ακόμα δυσκολότερη την ακριβή καταγραφή της, αλλά και τον με τον παραδοσιακό τρόπο, προσδιορισμό του τόπου εκδήλωσής της .

Το αποτέλεσμα είναι ότι μπορούμε να υποθέσουμε βάσιμα λαμβάνοντας υπόψη την εμπειρία μας από την καταγραφή της παραδοσιακής εγκληματικότητας, ότι και η αφανής ψηφιακή εγκληματικότητα είναι κατά πολύ μεγαλύτερη της εμφανούς, εκείνης δηλ. η οποία παρουσιάζεται στα ΜΜΕ ή μέσα από επίσημες στατιστικές - εφόσον υπάρχει και σε αυτές πρόβλεψη καταγραφής της - ή ακόμα και από κοινωνιολογικές έρευνες με ερωτηματολόγια, συνεντεύξεις κ.ά.

Τα στοιχεία όμως, τα οποία έχουμε στη διάθεσή μας από την εμφανή ψηφιακή εγκληματικότητα αποτελούν μια ισχυρή ένδειξη για το μεγεθός και της αφανούς. Με τον τρόπο αυτό η χρησιμότητά τους καθίσταται προφανής. Για το λόγο αυτό θα αναφερθούμε στη συνέχεια τόσο σε σχετικά ερευνητικά δεδομένα όσο και στη παράθεση πρόσφατων σχετικών περιπτώσεων ψηφιακών εγκλημάτων που είδαν το φως της δημοσιότητας μέσα από έγκριτες δημοσιογραφικές αναφορές τόσο του ελληνικού όσο και του διεθνούς έντυπου και ηλεκτρονικού τύπου. Προηγουμένως όμως, θα επιχειρήσουμε να δώσουμε έναν όσο το δυνατόν πληρέστερο κατάλογο των διαφόρων ψηφιακών εγκλημάτων που συνιστούν την ψηφιακή εγκληματικότητα.

2.2 ΚΑΤΗΓΟΡΙΕΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΓΚΛΗΜΑΤΩΝ

Σχετικά με την κατηγοριοποίηση των διαφόρων ηλεκτρονικών εγκλημάτων θα πρέπει να σημειώσουμε πως δεν παρατηρείται ομοφωνία μεταξύ των διαφόρων συγγραφέων που ασχολούνται με τον προσδιορισμό τους. Στη συνέχεια θα αναφέρουμε ενδεικτικά τις απόψεις ορισμένων από αυτούς και κατόπιν θα παραθέσουμε και τη δική μας.

Σύμφωνα λοιπόν, με τον **Neil Barrett (1997)**[10] τα ψηφιακά εγκλήματα διακρίνονται σε δύο κατηγορίες :

- Σε εκείνα που στρέφονται κατά των Η/Υ και στα οποία περιλαμβάνεται η κλοπή των υλικών μερών ενός Η/Υ, η εισβολή σε ηλεκτρονικά αρχεία και ο ψηφιακός βανδαλισμός καθώς και η διασπορά καταστρεπτικών ιών και
- Σε εκείνα που υποστηρίζονται από Η/Υ και στα οποία περιλαμβάνονται η πορνογραφία, η πειρατεία λογισμικού, οι διάφορες απάτες και το ξέπλυμα βρώμικου χρήματος που γίνεται ηλεκτρονικά.

Ο **Donald Pipkin (2003)**[11] αντιθέτως κατατάσσει τα ψηφιακά εγκλήματα σε τέσσερες κατηγορίες :

- Στην πρώτη από αυτές ανήκουν τα παραδοσιακά εγκλήματα τα οποία τελούνται με τη χρήση Η/Υ και σαν τέτοια αναφέρει την απάτη, την κλοπή στοιχείων των ιδιοκτητών πιστωτικών κατρών και την κλοπή της (ηλεκτρονικής) ταυτότητας.
- Στη δεύτερη υπάγονται τα ειδικά εγκλήματα των Η/Υ και σαν τέτοια ο συγγραφέας θεωρεί την επίθεση άρνησης παροχής υπηρεσιών, την άρνηση πρόσβασης σε πληροφορίες και τη διασπορά καταστρεπτικών ιών.
- Στην τρίτη κατηγορία ο Pipkin τοποθετεί τα εγκλήματα που στρέφονται κατά της πνευματικής ιδιοκτησίας όπως είναι η κλοπή πληροφοριών και η εμπορία, εναποθήκευση, έκθεση (διαστρέβλωση) και καταστροφή πληροφοριών που έχουν κλαπεί.
- Τέλος στην τέταρτη κατηγορία κατά τη γνώμη του συγγραφέα υπάγονται τα ψηφιακά εγκλήματα που στρέφονται κατά του προσωπικού απορρήτου και σαν τέτοιο θεωρεί τη διακίνηση πορνογραφικού υλικού με ανήλικους που γίνεται μέσω του Διαδικτύου.

Οι **Σουρής, Πατσός και Γρηγοριάδης (2005)** διακρίνουν εξάλλου τα ψηφιακά (ηλεκτρονικά) εγκλήματα σε τρεις κατηγορίες :

- Στην πρώτη ανήκουν τα εγκλήματα σε υπολογιστή, όπως η μη εξουσιοδοτημένη πρόσβαση σε υπολογιστικό σύστημα και η διασπορά κακόβουλων προγραμμάτων.

---

[10] Halting the hacker: a practical guide to computer security

[11] Digital crime: policing the cybernation (1997)

- Στη δεύτερη κατατάσσονται τα εγκλήματα που σχετίζονται με Η/Υ, όπως η ηλεκτρονική πορνογραφία και η πειρατεία λογισμικού και
- Στην τρίτη υπάγονται τα εγκλήματα που διαπράττονται με τη βοήθεια Η/Υ, όπως η απάτη σε ηλεκτρονικές συναλλαγές, η υποκλοπή στοιχείων πιστωτικών καρτών και η πλαστογράφηση εντύπων.

Εξάλλου σύμφωνα με τη διεθνή σύμβαση για το κυβερνοέγκλημα του 2001 (Convention on Cyber Crime 2001)[12] οι κύριες ψηφιακές παραβάσεις (εγκλήματα) είναι οι ακόλουθες :

- Παράνομη πρόσβαση
- Παράνομη υποκλοπή
- Παρεμβολή σε δεδομένα
- Παρεμβολή σε συστήματα
- Κακή χρήση συσκευών
- Κλοπή που σχετίζεται με υπολογιστή
- Απάτη που σχετίζεται με υπολογιστή
- Παιδική πορνογραφία
- Προστασία πνευματικών δικαιωμάτων ηλεκτρονικών πληροφοριών

Τέλος και για τις ανάγκες της ετήσιας έρευνας που διεξάγεται από το Computer Security Institute και το FBI ως ηλεκτρονικά εγκλήματα θεωρούνται :

- οι επιθέσεις ιών
- η επίθεση άρνησης παροχής υπηρεσιών
- η κλοπή πνευματικής ιδιοκτησίας
- οι παραβιάσεις υπαλλήλων που σχετίζονται με Η/Υ
- οι παράνομες ακροάσεις τηλεπικοινωνιών
- οι οικονομικές απάτες
- οι κλοπές φορητών Η/Υ
- οι παράνομες εισβολές σε σύστημα Η/Υ
- οι τηλεπικοινωνιακές απάτες
- η παραποίηση ιστοσελίδων
- το σαμποτάζ.

Κατά τη γνώμη μας, τα ψηφιακά εγκλήματα, θα μπορούσαμε να τα χωρίσουμε σε δύο μεγάλες κατηγορίες με κριτήριο τα μέσα τέλεσης και εξιχνίασής τους. Έτσι έχουμε,

1) **Τα γνήσια ψηφιακά εγκλήματα τα οποία τελούνται αλλά και εξιχνιάζονται, αποκλειστικά και μόνο με τη χρήση της ψηφιακής τεχνολογίας**
   - Η χωρίς νόμιμη εξουσιοδότηση είσοδος σε Η/Υ (hacking),
   - Η κλοπή, η παραποίηση και η καταστροφή αρχείων Η/Υ,
   - Η προσωρινή ή οριστική διακοπή της λειτουργίας συστήματος Η/Υ που αποτελεί συνέπεια της λεγόμενης "επίθεσης άρνησης παροχής υπηρεσιών" (Denial of service attack - DoS)
   - Η διασπορά κακόβουλων προγραμμάτων (ιών (virus), σκουληκιών (worms), Δούρειων Ιππων (Trojan Horses - Trojans), dialers κλπ.) και
   - Η πειρατεία λογισμικού δηλ.προγραμμάτων Η/Υ που αφορά την παράνομη αντιγραφή τους και τη στη συνέχεια διάθεσή τους στην αγορά - και μέσω του Διαδικτύου - σε πολύ χαμηλότερη τιμή από εκείνη του πρωτοτύπου.
2) Τα παραδοσιακά εγκλήματα τα οποία τελούνται αλλά και εξιχνιάζονται, τόσο με την υποστήριξη της ψηφιακής τεχνολογίας όσο και χωρίς τη βοήθειά της.

Σε αυτήν την κατηγορία εντάσσονται όσα τελέσθηκαν και με τη χρήση της ψηφιακής τεχνολογίας, και υπάγονται :

Διάφορα κοινά εγκλήματα. Σαν τέτοια μπορούμε να θεωρήσουμε π.χ. την κλοπή ενός Η/Υ, τμημάτων του - *μνήμης, μητρικής κλπ.- ή* περιφερειακών *του - εκτυπωτών, σκάνερς κλπ.- Στην κατηγορία αυτή ανήκουν επίσης και εγκλήματα που τελούνται με τη βοήθεια του ηλεκτρονικού ταχυδρομείου (e-mail) ή ιστοσελίδων (websites), όπως* απάτες, εξυβρίσεις, εκβιασμοί, δυσφημίσεις, πωλήσεις απαγορευμένων προϊόντων (ναρκωτικών, μη εγκεκριμένων φαρμάκων), παροχή υπηρεσιών call-girls, η κυκλοφορία πορνογραφικού υλικού - *που αφορά κυρίως ανηλίκους (παιδική πορνογραφία)* - και η παρενόχληση χρηστών με

[12] http://conventions.coe.int/treaty/en/treaties/html/185.htm

ανεπιθύμητα διαφημιστικά μηνύματα (spamming). *Εδώ υπάγονται επίσης, κατά τη γνώμη μας και οι* προσβολές της πνευματικής ιδιοκτησίας, οι ανταλλαγές πληροφοριών μέσω του ηλεκτρονικού ταχυδρομείου μεταξύ τρομοκρατικών οργανώσεων αλλά και συμμοριών του κοινού ποινικού δικαίου καθώς και το ηλεκτρονικό ξέπλυμα βρώμικου χρήματος.

Η κατασκοπεία είτε αυτή χαρακτηρίζεται σαν βιομηχανική ή σαν κρατική ή σαν πολιτική και οι υποκλοπές τηλεφωνικών συνομιλιών που έχουν σαν συνέπεια την προσβολή του προσωπικού απορρήτου των συνομιλούντων.

2.2.1 ΔΙΑΔΕΔΟΜΕΝΕΣ ΜΟΡΦΕΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΓΚΛΗΜΑΤΩΝ

Έχοντας ως σκοπό την κατηγοριοποίηση των ηλεκτρονικών εγκλημάτων παραθέτουμε τις ποιό γνωστές και περισσότερο διαδεδομένες κατηγορίες ηλεκτρονικών εγκλημάτων όπως έχουν καταγραφεί έως τις μέρες μας.

1- Μη νόμιμη εξουσιοδότηση είσοδο σε Η/Υ.

Η δραστηριότητα αυτή που είναι γνωστή σαν hacking προσδιορίζεται στον Ποινικό μας Κώδικα ως η,

«....πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους » **(ά. 370Γ & 2 Π.Κ.)**

Βλέπουμε λοιπόν εδώ ότι η συγκεκριμένη εγκληματική συμπεριφορά αφορά απλά και μόνο την παράνομη διείσδυση σε συστήματα και επικοινωνίες υπολογιστών, η οποία τελείται με την παραβίαση των μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους και ανεξάρτητα από τους λόγους για τους οποίους την επιχειρεί ο δράστης.

Νόμιμοι κάτοχοι των συστημάτων αυτών βέβαια, εννοείται πως μπορεί να είναι τόσο άτομα (φυσικά πρόσωπα) όσο και επιχειρήσεις ή οργανισμοί του ιδιωτικού ή του δημόσιου τομέα (νομικά πρόσωπα).Μιλώντας δε για «επικοινωνία υπολογιστών» αναφερόμαστε στην τηλεφωνική τους σύνδεση με βάση την οποία γεννήθηκε και αναπτύχθηκε το Διαδίκτυο.

2. - Για την κλοπή, την παραποίηση ή την καταστροφή αρχείων Η/Υ.

Αποκτώντας πρόσβαση σε ένα δίκτυο ο ψηφιακός εγκληματίας έχει τη διακριτική ευχέρεια να κλέψει, να μεταβάλλει ή να καταστρέψει αρχεία πληροφοριών ή προγραμμάτων και γενικά να κάνει οποιαδήποτε άλλη ενέργεια θα τα αχρηστεύσει μόνιμα ή προσωρινά, επιφέροντας με τον τρόπο αυτό ανυπολόγιστες οικονομικές ζημιές στα θύματά του.

Αν μάλιστα τα αρχεία αυτά περιέχουν οικονομικές πληροφορίες τα πράγματα είναι ιδιαίτερα επικίνδυνα. Στην περίπτωση αυτή το θύμα είναι κατά κύριο λόγο χρηματοπιστωτικό ίδρυμα, συνήθως Τράπεζα. Ο ψηφιακός εγκληματίας με την είσοδό του στο σύστημα επιδιώκει είτε το σπάσιμο των κωδικών λογαριασμών των πελατών με σκοπό τη μεταφορά του περιεχομένου τους στο δικό του λογαριασμό είτε την με αντίστοιχο τρόπο επιβάρυνση των λογαριασμών των κατόχων πιστωτικών καρτών με αγορές που οι ίδιοι δεν έχουν κάνει.

Για το θέμα αυτό ο Pipkin[13] παρατηρεί χαρακτηριστικά τα εξής :

«Σημειώνεται πως εάν κάποιος ληστεύσει μια Τράπεζα με πιστόλι θα διωχθεί με κάθε μέσο οπουδήποτε κι αν πάει. Αλλά αν την ληστεύσει με τον Η/Υ του, είναι πάρα πολύ πιθανό η Τράπεζα να μην παραδεχθεί την ληστεία αυτή προκειμένου να αποφύγει τη δημοσιότητα. Τα παρακάτω στατιστικά στοιχεία αποδεικνύουν του λόγου το αληθές. Κατά μέσον όρο ένας ένοπλος ληστής αποκομίζει από 2500 έως 7500 δολ. διατρέχοντας τον κίνδυνο να τον πυροβολήσουν και να τον σκοτώσουν. Ποσοστό πενήντα έως 60% από τους ένοπλους ληστές συλλαμβάνεται και από αυτούς το 80% καταδικάζεται και φυλακίζεται κατά μέσο όρο για πέντε χρόνια. Ο μέσος ηλεκτρονικός εγκληματίας θα αποκομίσει από 50 έως 500.000 δολ. και ο μεγαλύτερος κίνδυνος που διατρέχει είναι να χάσει τη δουλειά του και να πάει φυλακή. Ποσοστό 10% από τους εγκληματίες αυτούς ανακαλύπτεται και μόνο το 15% από αυτούς παραδίδεται στις αρχές. Πάνω από 50% από αυτούς τους τελευταίους δεν δικάζονται ποτέ γιατί δεν μπορεί να θεμελιωθεί κατηγορία σε βάρος τους ελλείψει αποδείξεων ή επειδή το θύμα τους δεν επιθυμεί τη δημοσιότητα. Το 50% αυτών που τελικά δικάζονται και καταδικάζονται μένει στη φυλακή για χρονικό διάστημα όχι μεγαλύτερο των 5 ετών».

3.- Για την επίθεση άρνησης παροχής υπηρεσιών (Denial of service attack - DoS).

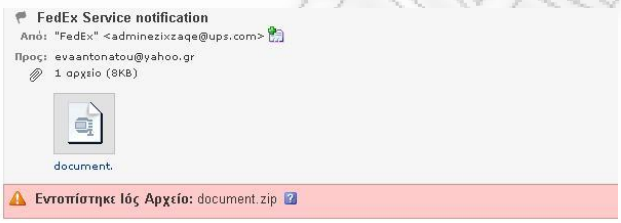
Η πιο συνηθισμένη μορφή της επίθεσης αυτής είναι εκείνη κατά την οποία ένας διακομιστής του Παγκόσμιου Ιστού κατακλύζεται με πολυάριθμες αιτήσεις σύνδεσης, οι οποίες όμως δεν είναι δυνατό να

[13] Digital crime: policing the cybernation(1997)

ικανοποιηθούν. Αυτό τον υποχρεώνει να απασχολείται τόσο πολύ με το να προσπαθεί να απαντήσει στις συγκεκριμένες αιτήσεις, έτσι ώστε να αγνοεί άλλες καλοπροαίρετες αιτήσεις σύνδεσης. Παράδειγμα αυτής της μορφής επίθεσης αποτελεί και το γνωστό ως "κατακλυσμός SYN" όπου κατακλύζονται οι θύρες εισόδου του διακομιστή με ψευδή μηνύματα σύνδεσης. Επίσης άλλη μορφή της επίθεσης αυτής είναι και η γνωστή ως το "θανατηφόρο πίνγκ", κατά την οποία ο ψηφιακός δράστης στέλνει μια διαταγή πίνγκ με ένα υπερβολικά μεγάλο πακέτο IP, με αποτέλεσμα το πάγωμα ή την αναγκαστική επανεκκίνηση του διακομιστή του θύματός του.

4.- Για τη διασπορά κακόβουλων προγραμμάτων όπως ιών, σκουληκιών, Δούρειων Ίππων και Dialers.

Ο ιός (virus) είναι ένα πρόγραμμα Η/Υ που έχει σχεδιασθεί με σκοπό να μολύνει άλλα προγράμματα με αντίγραφά του. Επειδή δε έχει τη δυνατότητα να αναπαράγεται συνεχώς μπορεί να μεταδοθεί από ένα σύστημα σε άλλο, με σκοπό να εκτελέσει την αποστολή του, η οποία περιλαμβάνει την δυσλειτουργία ή και την καταστροφή ολόκληρων συστημάτων, τη διαγραφή αρχείων ή το σβύσιμο του συνόλου του περιεχομένου σκληρών δίσκων.



Τα σκουλήκια (worms) είναι και αυτά προγράμματα Η/Υ που χρησιμοποιούνται σαν ένας μηχανισμός μεταφοράς άλλων προγραμμάτων. Για το λόγο αυτό χρησιμοποιούν τις δυνατότητες κυκλοφορίας που τους παρέχει ένα δίκτυο με σκοπό να μεταφέρουν κάποιο καταστρεπτικό πρόγραμμα δηλ. έναν ιό στα διάφορα συστήματα του δικτύου αυτού. Η διαφορά τους με τους ιούς αναφέρεται στο ότι δεν απαιτείται η ανθρώπινη παρεμβολή για την ενεργοποίησή τους. Πολλά worms βρίσκονται μέσα σε μηνύματα ηλεκτρονικού ταχυδρομείου (worms e-mail). Τα τελευταία χρόνια ιδιαίτερα γνωστά τέτοια σκουλήκια ήταν το "I Love You"[14], ο "Klez[15]" και ο "botnet[16]" (Sorensen, 2005).

Οι Δούρειοι Ίπποι (Trojan Horses, Trojans), είναι επίσης προγράμματα Η/Υ που ενώ φαίνεται ότι λειτουργούν κανονικά, παράλληλα εκτελούν και κάποιες άλλες μη επιτρεπόμενες ενέργειες. Έτσι, ένα τέτοιο κακόβουλο πρόγραμμα μπορεί να έχει συνήθως την μορφή παιχνιδιού, αυτό που κάνει όμως στην πραγματικότητα είναι το να κλέβει τα ονόματα (usernames) και τους κωδικούς (passwords) των ανυποψίαστων χρηστών του Διαδικτύου. Οι ψηφιακοί εγκληματίες χρησιμοποιούν επομένως τα προγράμματα αυτά για να κάνουν έμμεσα ενέργειες που δεν μπορούν να κάνουν άμεσα, παραπλανώντας έτσι για τις πραγματικές τους προθέσεις, τα θύματά τους.

Τέλος, μία ακόμη από τις μορφές "κακόβουλου λογισμικού" (malware) που αποτελεί ολοένα και μεγαλύτερο πρόβλημα σήμερα είναι τα προγράμματα που χαρακτηρίζονται με τον όρο "dialers". Αυτά είναι μικρά προγράμματα τα οποία καλούν τηλεφωνικούς αριθμούς για την πρόσβαση σε συγκεκριμένες υπηρεσίες (συνήθως υψηλής χρέωσης). Αρχικά αυτό το είδος προγραμμάτων διανέμονταν ελεύθερα από εταιρείες παροχής Internet, για να βοηθούν τους πελάτες τους να συνδέονται στους servers τους. Αργότερα αναπτύχθηκαν και άλλες υπηρεσίες οι οποίες ήταν προσπελάσιμες από υπολογιστές. Οι υπηρεσίες αυτές, πολλές εκ των οποίων σχετίζονται με την πορνογραφία, ήταν διαθέσιμες μόνο μέσω ειδικών τηλεφωνικών αριθμών υψηλής χρέωσης, και σαν αποτέλεσμα αναπτύχθηκαν προγράμματα dialer τα οποία επέτρεπαν την πρόσβαση των χρηστών σε αυτές.

Σύντομα, ορισμένοι κακόβουλοι χρήστες αντιλήφθηκαν ότι, εάν χρησιμοποιηθούν με έναν συγκεκριμένο τρόπο, τα dialers για την πρόσβαση σε αυτές τις υπηρεσίες θα μπορούσαν να είναι εξαιρετικά κερδοφόρα. Από τότε τα προγράμματα αυτά άρχισαν να εισάγονται σε διάφορα sites τα οποία είναι ειδικά σχεδιασμένα ώστε να μεταφέρουν, να εγκαθιστούν και να εκτελούν αυτόματα ένα τέτοιο

[14] http://en.wikipedia.org/wiki/ILOVEYOU

[15] http://en.wikipedia.org/wiki/Klez

[16] http://en.wikipedia.org/wiki/Botnet

πρόγραμμα το οποίο συνδέει αυτόματα τον επηρεαζόμενο υπολογιστή με τηλεφωνικές υπηρεσίες υψηλής χρέωσης χωρίς να λαμβάνει γνώση ο χρήστης.

Όταν εκτελείται ένα πρόγραμμα dialer, το αποτέλεσμα είναι η δημιουργία μιας νέας dial-up (μέσω τηλεφώνου) σύνδεσης δικτύου. Επιπλέον, ο συγκεκριμένος αριθμός τηλεφώνου θα χρησιμοποιείται σαν προεπιλεγμένος για την σύνδεση του χρήστη στο Internet. Μία άλλη, ακόμη πιο επικίνδυνη συνέπεια αυτής της διαδικασίας είναι ότι μπορεί να καταργήσει την dial-up σύνδεση που χρησιμοποιεί κανονικά ο χρήστης, με αποτέλεσμα ο χρήστης να συνδέεται όχι στους servers της εταιρείας παροχής Internet που χρησιμοποιεί, αλλά σε έναν αριθμό υψηλής χρέωσης. Σε κάθε περίπτωση, το αποτέλεσμα είναι το ίδιο: ο χρήστης αντιμετωπίζει αναπάντεχα αυξημένους λογαριασμούς τηλεφώνου. Η αύξηση αυτή είναι τόσο μεγάλη, που σε ορισμένες περιπτώσεις απασχόλησε τα μέσα ενημέρωσης. Το χειρότερο είναι ότι το μεγαλύτερο μέρος αυτού του κόστους πηγαίνει κατευθείαν στην τσέπη του δημιουργού του προγράμματος που εγκατέστησε το dialer στον υπολογιστή. Θα πρέπει να επισημάνουμε ότι τα dialers μπορούν να προκαλέσουν προβλήματα μόνο στους υπολογιστές που συνδέονται στο Internet μέσω dial-up δικτύων (δηλ. μέσω modem και τηλεφωνικών γραμμών), δεδομένου ότι οι άλλες μορφές σύνδεσης - π.χ. συνδέσεις ευρείας ζώνης ή καλωδιακές - λειτουργούν διαφορετικά και δεν απαιτούν την κλήση ενός αριθμού.

Η καλύτερη προστασία για την αντιμετώπιση των dialers είναι η εγκατάσταση στον Η/Υ μιας εφαρμογής η οποία θα μπορεί να εξακριβώνει εάν πρόκειται να πραγματοποιηθεί μία κλήση μέσω ενός αριθμού διαφορετικού από τον κανονικό, και θα ειδοποιεί τον χρήστη. Επιπλέον, επειδή υπάρχουν ιοί ειδικά σχεδιασμένοι ώστε να εγκαθιστούν dialers στους Η/Υ που μολύνουν χωρίς να το γνωρίζει ο χρήστης, η ιδανική λύση είναι ο συνδυασμός της προστασίας έναντι των dialers και της προστασίας έναντι των ιών σε ένα και μόνο προϊόν.

Ολοκληρώνοντας το τμήμα αυτό και επειδή συνήθως γίνεται μεγάλος λόγος τόσο στο ευρύ κοινό όσο και στην ψηφιακή κοινότητα για τους ιούς των Η/Υ, θα πρέπει στη συνέχεια να αναφέρουμε τα ακόλουθα διευκρινιστικά ζητήματα γι' αυτούς:

Οι ιοί των υπολογιστών δεν ξεκίνησαν στην αρχή σαν εργαλεία (tools) των ψηφιακών εγκληματιών αλλά σαν πνευματικά παιχνίδια των ερευνητών σε επιστημονικά εργαστήρια αμερικάνικων πανεπιστημίων όπως του M.I.T. ή εταιρειών προϊόντων υψηλής τεχνολογίας όπως η AT&T, η XEROX , η BELL κλπ.

Οι ερευνητές και οι προγραμματιστές των ερευνητικών αυτών κέντρων, κατά τη διάρκεια του ελεύθερου χρόνου τους διασκέδαζαν τους εαυτούς τους και τους συναδέλφους τους μπαίνοντας στην κεντρική μνήμη των υπολογιστικών μηχανημάτων τους. Αλλάζοντας όμως τον κώδικα της μνήμης αυτής διεπίστωσαν ότι προγράμματα τα οποία είχαν σχεδιασθεί για να ταξινομήσουν αρχεία μπορούσαν επίσης και να τα καταστρέψουν! Στην ανακάλυψη αυτή στηρίχθηκε και το παιχνίδι «Core Wars» στο οποίο οι προγραμματιστές δοκίμαζαν την εξυπνάδα τους γράφοντας προγράμματα τα οποία μπορούσαν να αναπαράγουν τον εαυτό τους και στη συνέχεια να καταστρέψουν τα προγράμματα των αντιπάλων παικτών.

Οι ιοί που δημιουργήθηκαν μέσα στα πλαίσια των «Core Wars» δεν έγιναν ευρύτερα γνωστοί έξω από τους υπολογιστές των εργαστηρίων επειδή οι προγραμματιστές που τους χρησιμοποιούσαν κρατούσαν τις λεπτομέρειες της κατασκευής τους μόνο για τον εαυτό τους. Έτσι δεν αποτελούσαν απειλή για τον εξωτερικό κόσμο.

Ολα αυτά μέχρι το 1983. Τη χρονιά αυτή ο δημιουργός του λειτουργικού συστήματος UNIX, Ken Thompson μιλώντας στην «Association for Computing Machines» έκανε λόγο για τα «Core Wars». Αυτό ήταν το πρώτο λάθος. Την επόμενη χρονιά έγινε το δεύτερο και πιο αποφασιστικό. Το περιοδικό Scientific American δημοσίευσε ένα άρθρο που αναφερόταν στους ιούς και στο οποίο περιλαμβανόταν λεπτομέρειες για το πως θα μπορούσε κανείς να γράψει τέτοια προγράμματα που αντέγραφαν τον εαυτό τους. Η ραγδαία ανάπτυξη των ιών που επακολούθησε ήταν πια θέμα χρόνου. Τα πλαίσια των επιστημονικών εργαστηρίων ήταν πλέον πολύ στενά γι' αυτούς!

Στην αρχή βέβαια εμφανίστηκαν σαν ακίνδυνα προγράμματα που έδειχναν ένα μήνυμα στη οθόνη του Η/Υ ή έπαιζαν κάποιο ήχο σε συγκεκριμένη ώρα κάθε ημέρας. Ακίνδυνα μεν ενοχλητικά δε, θα μπορούσε να παρατηρήσει κανείς. Όπως ακριβώς όμως συνέβη και με τους hackers που ξεκίνησαν τη δράση τους για να διευρύνουν τις γνώσεις τους και εξελίχθηκαν στο να κάνουν παράνομες πράξεις, έτσι και οι δημιουργοί ιών από κάποιο σημείο και μετά κατάλαβαν τη δύναμη που είχαν στα χέρια τους και άρχισαν να δημιουργούν ιούς που προξενούσαν καταστροφές όχι μόνο σε αρχεία αλλά και σε ολόκληρα δίκτυα υπολογιστών. Δεν ήσαν δε λίγες οι περιπτώσεις που ζήτησαν -εκβιαστικά - οικονομικά ανταλλάγματα για να μην τους χρησιμοποιήσουν.

Οι καταστροφικές τους δυνατότητες υπογραμμίστηκαν μεταξύ άλλων και από τον Δρ. Peter S. Tippet, διευθυντή παραγωγής προϊόντων ασφαλείας της Symantec Corporation, ο οποίος καταθέτοντας σε μία υποεπιτροπή του Αμερικάνικου Κογκρέσσου το 1993, υπογράμμισε πως,

«.... μια εταιρεία που έχει 1000 υπολογιστές προσβάλλεται από ένα ιό κάθε τέταρτο της ώρας, το κόστος για την αντιμετώπιση των ιών αυτών ανέρχεται σε 170.000$ το χρόνο τώρα και σε 500.000$ για τον

επόμενο χρόνο και ότι εάν προσθέσουμε τα κόστη αυτά από το 1990 και μετά θα δούμε πως η μάχη κατά των ιών των υπολογιστών έχει κοστίσει στους Αμερικανούς πολίτες περισσότερο από 1 δισεκατομμύριο δολλάρια» *(Quarantiello, 1997*[17]*).*

Οι περισσότεροι ιοί έχουν σαν στόχο τους προγράμματα (software) των υπολογιστών. Εξαιτίας δε των διαφόρων μορφών που μπορεί να πάρει ένας ιός από τις παρεμβάσεις που κάνει συνήθως στη δομή του ένας ψηφιακός εγκληματίας, είναι αρκετά δύσκολη η ακριβής περιγραφή του και η κατάταξή του σε συσγκεκριμένη κατηγορία. Ωστόσο ο John McAfee της "Computer Virus Industry Association", γνωστός για τα αντιικά (anti - virus) προγράμματα που έχει κυκλοφορήσει στη διεθνή αγορά, υποστηρίζει την άποψη πως σαν κριτήρια διάκρισης των ιών μπορούν να θεωρηθούν :

i. η δομή του προγράμματος που προσβάλλουν,
ii. το μέγεθος της καταστροφής που προξενούν και
iii. η περιοχή του συστήματος στο οποίο εγκαθίστανται [18]

Ο Kyas (1997) εξάλλου, με κριτήρια το μέρος του υπολογιστή που προσβάλλουν και τις προσπάθειες που καταβάλλουν για να μην γίνονται αντιληπτοί, διαχωρίζει τους ιούς σε εκείνους :

a. Που μολύνουν τον τομέα εκκίνησης ενός σκληρού δίσκου (ή των δισκεττών) ο οποίος περιέχει εντολές εκκίνησης του υπολογιστή (boot viruses),
b. Που μολύνουν το σύστημα και οι οποίοι προσκολλώνται σε διάφορα τμήματα του λειτουργικού ή στο πρόγραμμα ελέγχου εφαρμογών (system (cluster) viruses),
c. Που προσβάλλουν προγράμματα υπολογιστών και οι οποίοι βρίσκονται κρυμμένοι μέσα σε εκτελέσιμα αρχεία (.exe) και τρέχουν μόλις ξεκινήσει το πρόγραμμα που έχουν μολύνει (software viruses),
d. Που έχουν τη δυνατότητα να αναπαράγονται με πολλούς και διαφορετικούς τρόπους έτσι ώστε να είναι ανθεκτικοί στα διάφορα anti - virus προγράμματα (polymorphous viruses),
e. Που έχουν τη δυνατότητα να καμουφλάρουν τις αλλαγές που κάνουν στον τομέα εκκίνησης ενός συστήματος ή ενός αρχείου επεμβαίνοντας στο λογισμικό του συστήματος που προσβάλλουν (stealth viruses),
f. Που προσπαθούν να καταστρέψουν ή να σβήσουν εντελώς προγράμματα anti - virus (retroviruses)
g. που προσβάλλουν τις μακρο - εντολές σύγχρονων προγραμμάτων εφαρμογών (data viruses).

Λαμβάνοντας υπόψη τα σημερινά δεδομένα θα πρέπει να παρατηρήσουμε πως το Διαδίκτυο αποτελεί πλέον, τον περισσότερο διαδεδομένο τρόπο μετάδοσης των ιών είτε μέσω του ηλεκτρονικού ταχυδρομείου - σε προσαρτώμενα (attachments) - είτε μέσω των διαφόρων ιστοσελίδων. Ακόμα, στα ιδιαίτερα διαδεδομένα δίκτυα peer- to-peer, όπου μπορεί να βρει κανείς οποιοδήποτε αρχείο, μπορεί να διαπιστώσει αργότερα ότι το μουσικό αρχείο MP3 που κατέβασε, δεν ήταν παρά ένας καλά καμουφλαρισμένος ιός.

Διάσημοι και ιδιαίτερα καταστροφικοί ιοί που έχουν κυκλοφορήσει ευρέως τα τελευταία χρόνια είναι ο Brain (1986), ο Moris (1988), ο Michaelangelo (1992), ο Melissa (1999), ο Iloveyou (2000), ο Anna Kournikova (2001), ο bugbear (2002), ο Blaster (2003), ο MyDoom (2004) και σχετικά πρόσφατα ο Sasser για τον οποίο συνελήφθη στις 7/5/04 ο 18χρονος Γερμανός Sven Jaschan ο οποίος ένα χρόνο περίπου αργότερα καταδικάστηκε από Γερμανικό δικαστήριο σε ποινή φυλάκισης 21 μηνών με αναστολή και σε 30 ώρες κοινωνική προσφορά. Σημειωτέον ότι ο Sasser προκάλεσε σημαντικότατα προβλήματα σε εκατοντάδες χιλιάδεες Η/Υ παγκοσμίως.

Ο καλύτερος τρόπος αντιμετώπισης των ιών είναι η πρόληψη. Το πρώτο βήμα προς την κατεύθυνση αυτή έχει να κάνει με τη διερεύνηση όλων των τρόπων με τους οποίους μπορούν αυτοί να διεισδύσουν σε ένα σύστημα. Το μπλοκάρισμα των τρόπων αυτών αποτελεί το επόμενο βήμα. Έτσι συστήματα ευάλωτα στην προσβολή τους από ιούς - όπως είναι εκείνα που έχουν σύνδεση με το Internet ή εκείνα που έχουν πολλούς χρήστες - θα πρέπει να διασφαλίζονται με τη χρήση του κατάλληλου διερευνητικού software ή με τη δημιουργία backups των αρχείων τους. Η χρήση πρόσφατα ενημερωμένων προγραμμάτων, διαγνωστικών των ιών που θα ενεργοποιούνται με την έναρξη της λειτουργίας του συστήματος είναι απαραίτητη στην προκειμένη περίπτωση δεδομένου ότι έτσι μειώνονται και οι πιθανότητες ενεργοποίησης ιών που το έχουν ήδη μολύνει.

Από τη στιγμή που μέσω ενός τέτοιου προγράμματος - κυκλοφορούν άφθονα στην αγορά και μάλιστα κάποια, όπως το AVG, δωρεάν - διαπιστωθεί η ύπαρξη ιού ή ιών η λειτουργία του συστήματος σταματάει και με ειδικά πάλι αντιικά προγράμματα θα πρέπει να καταστραφούν οι ιοί που το έχουν ήδη

[17] http://scholarcommons.usf.edu/etd/308/

[18] http://www.vmyths.com/hmul/5/7/

μολύνει. Η διαγραφή όλων των μολυσμένων αρχείων και η αντικατάστασή τους με «καθαρά» αντίγραφά τους συνιστάται στη συγκεκριμένη περίπτωση.

Οι ενέργειες αντιμετώπισης ενός ιού ολοκληρώνονται με τη διερεύνηση του τρόπου και του λόγου εισόδου του στο σύστημα. Η απάντηση στα σχετικά ερωτήματα θα βοηθήσει στη θεραπεία των αδυναμιών του συστήματος και στην μη επανάληψή τους στο μέλλον.

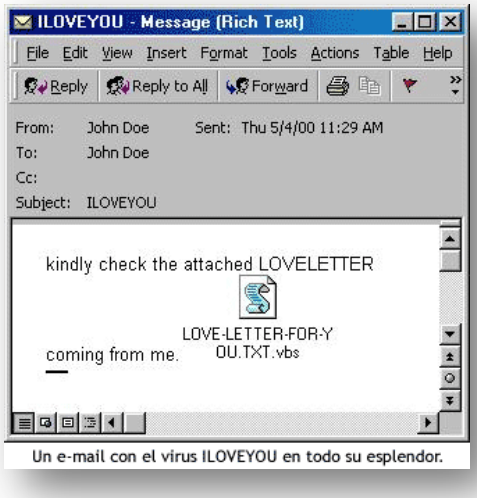
5.- Για τις απάτες που γίνονται μέσω του Διαδικτύου.

Οι μορφές των πλέον διαδεδομένων απατών που τελούνται τα τελευταία χρόνια, μέσω του Διαδικτύου είναι οι ακόλουθες:

Η απάτη με τα Νιγηριανά μηνύματα του ηλεκτρονικού ταχυδρομείου (Nigerian e-mail fraud).[19] Στην περίπτωση αυτή το υποψήφιο θύμα λαμβάνει ένα e-mail με το οποίο ο απατεώνας τού υπόσχεται μεγάλη χρηματική αμοιβή αν τον βοηθήσει να μεταφέρει χρήματα από τον τραπεζικό του λογαριασμό στο λογαριασμό του θύματος. Οι λόγοι τους οποίους επικαλείται ο απατεώνας για τη μεταφορά αυτή ποικίλλουν κατά περίπτωση, συνήθως όμως αφορούν γνωστούς διπλωμάτες, επιχειρηματίες ή γόνους πλουσίων οικογενειών που θα πρέπει να εγκαταλείψουν τη χώρα τους εξαιτίας πολιτικών συγκρούσεων. Προτού όμως το θύμα εισπράξει το χρηματικό ποσό που του υποσχέθηκε ο απατεώνας, θα πρέπει να καταβάλει ορισμένα χρήματα για τα έξοδα μεταφοράς ή να δώσει για το λόγο αυτό τα στοιχεία του τραπεζικού του λογαριασμού. Εννοείται ότι στην πρώτη περίπτωση αμέσως μετά την αποστολή των χρημάτων θα διακοπεί η επικοινωνία με τον απατεώνα, ενώ στη δεύτερη το θύμα είναι πολύ πιθανό να χάσει όλα τα χρήματα του τραπεζικού του λογαριασμού. Φυσικά υπάρχει και το ενδεχόμενο με τον τρόπο αυτό ο απατεώνας έχοντας στη διάθεσή του τα στοιχεία της ταυτότητας του θύματος να το χρεώσει στη συνέχεια, με μεγάλα χρηματικά ποσά. Τα Νιγηριανά e-mail ονομάζονται επίσης και **"419" από το άρθρο του Νιγηριανού Ποινικού Κώδικα** που παραβιάζουν.

Η απάτη με το phishing mail (ηλεκτρονικό μήνυμα "ψαρέματος"). Στην περίπτωση αυτή ο απατεώνας προσπαθεί μέσω των μηνυμάτων που στέλνει, να αποσπάσει από το θύμα του προσωπικά του οικονομικά δεδομένα, όπως τα στοιχεία της πιστωτικής του κάρτας ή του τραπεζικού του λογαριασμού. Στην αρχή το υποψήφιο θύμα λαμβάνει ένα e-mail, αποστολέας του οποίου φαίνεται να είναι η τράπεζά του. Με αυτό του ζητείται να επιβεβαιώσει το username και το password του τραπεζικού του λογαριασμού που διακινεί μέσω του Διαδικτύου (Web banking). Η σχετική ομολογία αναφέρεται σε προβλήματα στους Η/Υ της τράπεζας ή σε υποψίες ότι ο συγκεκριμένος λογαριασμός έχει ήδη παραβιασθεί και αν δεν γίνει η επιβεβαίωση, θα κλειδωθεί. Το email αυτό έχει σύνδεσμο (link) προς τον δικτυακό τόπο της τράπεζας, ο οποίος όμως δεν είναι πραγματικός και μιμείται απλά τον αυθεντικό και έτσι το θύμα στέλνει τα στοιχεία που του έχουν ζητηθεί κατευθείαν στον απατεώνα. Η σωστή αντίδραση κάποιου που θα δεχθεί ένα τέτοιο e-mail θα πρέπει να είναι το να μην ακολουθήσει το σύνδεσμο που περιλαμβάνεται σε αυτό, αλλά να πληκτρολογήσει από την αρχή τη διεύθυνση του δικτυακού τόπου της τράπεζάς του και να προσπαθήσει να διαπιστώσει από εκεί - κάτι που μπορεί να το κάνει και τηλεφωνικά - αν το e-mail που του στάλθηκε προέρχεται από την αρμόδια υπηρεσία της.

Άλλος ένας ακόμη τρόπος ψηφιακής απάτης είναι εκείνος που αφορά τη λήψη από το υποψήφιο θύμα ενός e-mail ή ενός Pop-up window που του εμφανίζεται κατά τη διάρκεια ττης περιήγησής του στον Ιστό, με το οποίο του γίνεται γνωστό ότι κέρδισε ένα μεγάλο χρηματικό ποσό σε κάποια κλήρωση. Για να το πάρει δε, θα πρέπει να καταβάλει ορισμένα χρήματα σε συγκεκριμένο λογαριασμό. Εννοείται ότι μετά την καταβολή των χρημάτων αυτών ο απατεώνας εξαφανίζεται και τα θύματα δεν παραλαμβάνουν κανένα νέο e-mail με το οποίο να τους γνωστοποιείται το πώς θα εισπράξουν τα υποτιθέμενα "κέρδη" τους.



Un e-mail con el virus ILOVEYOU en todo su esplendor.

Η απάτη με τα sites - "μαϊμούδες". Στην περίπτωση αυτή ο ψηφιακός απατεώνας προσπαθεί να οδηγήσει το υποψήφιο θύμα του - χρήστη του Διαδικτύου για να κάνει μια οικονομική συναλλαγή, στο πιστό αντίγραφο του δικτυακού τόπου της τράπεζάς του ή του ηλεκτρονικού καταστήματος που επισκέπτεται , το οποίο έχει δημιουργήσει και ελέγχει πλήρως ο ίδιος. Το

[19] http://www.potifos.com/fraud

[19] http://www.e-telescope.gr/gr/cat03/art03_010622.html

ανυποψίαστο θύμα πιστεύοντας ότι βρίσκεται στο site της τράπεζάς του ή ενός υπεράνω πάσης υποψίας ηλεκτρονικού καταστήματος δίνει όλα τα απαιτούμενα για τη συναλλαγή του στοιχεία (αριθμούς πιστωτικής κάρτας, λογαριασμού, κωδικούς πρόσβασης κτλ), τα οποία ο απατεώνας μπορεί να τα χρησιμοποιήσει στη συνέχεια είτε για να αδειάσει τον τραπεζικό λογαριασμό του θύματός του είτε για να επιβαρύνει την πιστωτική του κάρτα με αγορές τις οποίες αυτό ουδέποτε έχει πραγματοποιήσει

Η απάτη με τις επιταγές. Στη συγκεκριμένη περίπτωση, ένας απατεώνας αγοραστής σε μια δικτυακή δημοπρασία είναι δυνατό να συμφωνήσει με τον πωλητή να πληρώση με επιταγή. Το υποψήφιο θύμα καταθέτει την επιταγή και ο πωλητής στέλνει το εμπόρευμα, όμως στις περισσότερες περιπτώσεις οι τράπεζες εμφανίζουν τα χρήματα στο λογαριασμό του θύματος προτού να ελεγχθεί η γνησιότητα της επιταγής. Λίγες ημέρες μετά η τράπεζα διαπιστώνει ότι η επιταγή είναι ακάλυπτη ή πλαστή και αφαιρεί το αντίστοιχο χρηματικό ποσό από το λογαριασμό του θύματος.

Για την πειρατεία λογισμικού. Η πειρατεία αυτή η οποία ουσιαστικά συνιστά κλοπή λογισμικού (δηλ. προγραμμάτων Η/Υ) γίνεται από τον ψηφιακό δράστη με σκοπό να χρησιμοποιήσει το συγκεκριμένο πρόγραμμα ο ίδιος ή να το πωλήσει σε τρίτους. Το πρόγραμμα αυτό ο δράστης είναι δυνατό να το κατεβάσει (downloading) στο δικό του Η/Υ από το site της επιχείρησης στην οποία ανήκει η εμπορική εκμετάλλευσή του. Είναι γνωστό πως για κάθε πρόγραμμα Η/Υ υπάρχει άδεια χρήσης του - εκτός κι αν είναι freeware - ή περιορισμένης χρήσης (shareware ή demo), η οποία πιστοποιείται κατά την εγκατάστασή του ή με την έναρξη της λειτουργίας του από συγκεκριμένο κωδικό που δίνεται στο νόμιμο κάτοχό του. Ο δράστης στην προκειμένη περίπτωση έχει «σπάσει» τον κωδικό αυτό και μπορεί να χρησιμοποιεί ο ίδιος ή να πουλάει και μέσω του Internet το πρόγραμμα αυτό σε τρίτους. Η οικονομική ζημιά που υφίσταται το θύμα από την παράνομη αυτή κυκλοφορία του προϊόντος του είναι τόση όσος και ο αριθμός των πωλήσεων που πραγματοποιούνται με τον τρόπο αυτό.Σχετικά με την πειρατεία λογισμικού μάλιστα σε μία μελέτη που έγινε απο το Business Software Alliance (BSA)[20] σχετικά με την πειρατεια λογισμικού έδειξε ότι η Ελλάδα για το 2010 το 59% των συνολικά εγκατεστημένων προγραμμάτων είναι

	Piracy Rates					Commercial Value of Unlicensed Software ($M)				
	2010	2009	2008	2007	2006	2010	2009	2008	2007	2006
Western Europe										
Austria	24%	25%	24%	25%	26%	$209	$212	$184	$157	$147
Belgium	25%	25%	25%	25%	27%	$233	$239	$269	$223	$222
Cyprus	48%	48%	50%	50%	52%	$17	$16	$15	$14	$12
Denmark	26%	26%	25%	25%	25%	$208	$203	$215	$193	$183
Finland	25%	25%	26%	25%	27%	$193	$175	$194	$160	$149
France	39%	40%	41%	42%	45%	$2,579	$2,544	$2,760	$2,601	$2,676
Germany	27%	28%	27%	27%	28%	$2,096	$2,023	$2,152	$1,937	$1,642
Greece	59%	58%	57%	58%	61%	$301	$248	$238	$198	$165
Iceland	49%	49%	46%	48%	53%	$16	$11	$23	$33	$32
Ireland	35%	35%	34%	34%	36%	$137	$125	$118	$106	$92
Italy	49%	49%	48%	49%	51%	$1,879	$1,733	$1,895	$1,779	$1,403
Luxembourg	20%	21%	21%	21%	—	$31	$30	$21	$16	—
Malta	43%	45%	45%	46%	45%	$6	$7	$8	$7	$7
Netherlands	28%	28%	28%	28%	29%	$591	$525	$563	$502	$419
Norway	29%	29%	28%	29%	29%	$261	$195	$229	$195	$181
Portugal	40%	40%	42%	43%	43%	$228	$221	$212	$167	$140
Spain	43%	42%	42%	43%	46%	$1,105	$1,014	$1,029	$903	$865
Sweden	25%	25%	25%	25%	26%	$411	$304	$372	$324	$313
Switzerland	26%	25%	25%	25%	26%	$424	$344	$345	$303	$324
United Kingdom	27%	27%	27%	26%	27%	$1,846	$1,581	$2,181	$1,837	$1,670
TOTAL WE	**33%**	**34%**	**33%**	**33%**	**34%**	**$12,771**	**$11,750**	**$13,023**	**$11,655**	**$10,842**
TOTAL WORLDWIDE	**42%**	**43%**	**41%**	**38%**	**35%**	**$58,754**	**$51,443**	**$52,998**	**$47,809**	**$39,698**

πειρατικά με συνολική αποτίμηση της αξίας τους στα 301 εκατομμύρια δολλάρια.Σε αυτή την έρευνα το υψηλότερο ποσοστό το κατέχει η Γεωργία με 93% και συνολική αξία 46 εκατομμυρίων δολλαρίων.

Για τη βιομηχανική, κρατική και πολιτική κατασκοπεία. Τόσο οι επιχειρήσεις όσο και οι κυβερνήσεις αλλά και κάποιες πολιτικές οργανώσεις, είναι πιθανό να θέλουν να γνωρίζουν εκ των προτέρων τις κινήσεις των ανταγωνιστών/αντιπάλων τους. Τα νέα ηλεκτρονικά σύνορα τους προσφέρουν πολλές ευκαιρίες για να έχουν πρόσβαση σε μέχρι τώρα απρόσιτες πληροφορίες αυτών των τελευταίων. Έτσι πολλές επιχειρήσεις - κυρίως - επιδιώκουν την απόκτηση τέτοιων πληροφοριών, οι οποίες ξεκινούν από τον τρόπο παραγωγής των προϊόντων των ανταγωνιστών τους και τις εμπορικές τους συμφωνίες με τρίτους και φτάνουν μέχρι τις στρατηγικές marketing που χρησιμοποιούν. Πολύ συχνά λοιπόν, η παράνομη εισβολή στο δίκτυο Η/Υ μιας επιχείρησης μέσω του Internet μπορεί να είναι έργο των ανταγωνιστών της που στοχεύουν με τον τρόπο αυτό στο να της αποσπάσουν κρίσιμα εμπορικά μυστικά της, για προσωπικό τους οικονομικό όφελος.

[20] http://portal.bsa.org/globalpiracy2010/

2.3 ΚΑΤΑΓΡΑΦΗ ΤΩΝ ΨΗΦΙΑΚΩΝ ΕΓΚΛΗΜΑΤΩΝ

Όπως είναι γνωστό επίσημα στατιστικά δεδομένα που να καταγράφουν τα **ψηφιακά** εγκλήματα σαν ιδιαίτερη κατηγορία εγκλημάτων, δεν υπάρχουν μέχρι σήμερα ούτε στη χώρα μας ούτε και σε άλλες ξένες χώρες. Προκειμένου όμως να παρουσιάσουμε το μέγεθος της σύγχρονης ψηφιακής εγκληματικότητας, το κενό αυτό θα προσπαθήσουμε να το καλύψουμε με την παράθεση σχετικών **ερευνητικών δεδομένων** αλλά και με **δημοσιογραφικές αναφορές** οι οποίες είδαν το φως της δημοσιότητας τόσο στον ελληνικό όσο και στον ξένο γραπτό και ηλεκτρονικό τύπο.

2.3.1 ΕΡΕΥΝΗΤΙΚΑ ΔΕΔΟΜΕΝΑ

α) Έρευνα της Riptech με θέμα την προστασία ενάντια στις απειλές του διαδικτύου (Riptech Internet Security Threat Report-2002)[21].

Η παρούσα έρευνα αποτελεί μια ποσοτική ανάλυση των επιθέσεων που δέχθηκαν μέσω του διαδικτύου εκατοντάδες επιχειρήσεις και οργανισμοί κατά το πρώτο εξάμηνο του 2002. Η έρευνα διεξήχθη από την εταιρεία Riptech ενώ ο προσδιορισμός του δείγματος πραγματοποιήθηκε με τη χρήση του πελατολογίου της. Ειδικότερα, οι επιχειρήσεις που συμμετείχαν υπήρξαν συνδρομητές της συγκεκριμένης εταιρείας για την παροχή υπηρεσιών ασφαλείας και παρακολούθησης τους τελευταίους έξι μήνες ενώ ο τελικός αριθμός του δείγματος έφτασε τις 400.

Οι επιχειρήσεις που αποτέλεσαν το δείγμα της έρευνας είναι εγκατεστημένες σε περισσότερες από 30 χώρες, ενώ η υποδομή ασφαλείας που διαθέτουν προστατεύει ταυτόχρονα εκτός από τις ίδιες και εκατομμύρια χρηστών του Internet. Επίσης, οι επιχειρήσεις που συμμετείχαν προέρχονταν από διαφορετικούς βιομηχανικούς τομείς και διαφοροποιούνταν τόσο ως προς το μέγεθος όσο και το ιδιοκτησιακό τους καθεστώς αλλά και ως προς το διάστημα συνδρομής τους στην Riptech. Ειδικότερα, οι επιχειρήσεις με την μεγαλύτερη αντιπροσώπευση στο δείγμα, προέρχονταν από τον κλάδο των βιομηχανικών υπηρεσιών (business services) και το αντίστοιχο ποσοστό ανερχόταν στο 25%. Όσον αφορά το μέγεθος των επιχειρήσεων, η πλειοψηφία εμφανίζεται να απασχολεί λιγότερους από 500 υπαλλήλους (67%) ενώ αναφορικά με το ιδιοκτησιακό τους καθεστώς, το 68% από αυτές ανήκε σε ιδιώτες σε σύγκριση με το 21% που ήσαν δημόσιες.

Η βάση δεδομένων της Riptech, η οποία χρησιμοποιήθηκε, αποτελεί την μεγαλύτερη και την πιο αξιόπιστη στον κόσμο όσον αφορά τις επιθέσεις μέσω Διαδικτύου, γεγονός που καθιστά τα ευρήματα της έρευνας ιδιαίτερα σημαντικά. Στο σημείο αυτό θα πρέπει να αναφερθεί ότι από τη φύση των δεδομένων που χρησιμοποιήθηκαν για περαιτέρω ανάλυση γίνεται αντιληπτό πως η πλειοψηφία των επιθέσεων προερχόταν από εξωτερικές απειλές.

Συγκεκριμένα, μόνο για το διάστημα των έξι μηνών κατά το οποίο διεξήχθη η έρευνα, η Riptech εξέτασε περισσότερες από ένα εκατομμύριο πιθανές επιθέσεις εναντίον των πελατών της. Τα αποτελέσματα της έρευνας θεωρούνται ιδιαίτερα αξιόπιστα καθώς προέρχονται από την μελέτη και την ανάλυση συγκρίσιμων στοιχείων από ειδικούς αναλυτές με συνέπεια να παρουσιάζεται μια πιο ολοκληρωμένη εικόνα της ασφάλειας στο Διαδίκτυο.

Όσον αφορά τη μεθοδολογία που ακολουθήθηκε, έχει ήδη αναφερθεί ότι τα αποτελέσματα της έρευνας προήλθαν από την ανάλυση των επιθέσεων που δέχθηκαν μέσω Διαδικτύου επιχειρήσεις και οργανισμοί που περιλαμβάνονταν στο πελατολόγιο της Riptech. Το τελικό δείγμα που χρησιμοποιήθηκε προσδιορίστηκε στις 400 επιχειρήσεις οι οποίες υπήρξαν συνδρομητές για την παροχή υπηρεσιών παρακολούθησης κατά τη διάρκεια των τελευταίων έξι πριν από την έρευνα, μηνών. Κάθε επίθεση που πραγματοποιήθηκε προσδιορίστηκε, μελετήθηκε, σχολιάσθηκε και ταξινομήθηκε κατάλληλα από τους αναλυτές του Κέντρου Ελέγχων Ασφάλειας (Security Operations Center) της Riptech.

---

[21] http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_ii.pdf

Το διάστημα των έξι μηνών που διήρκεσε η έρευνα ελέγχθηκαν και κατηγοριοποιήθηκαν περισσότερες από 1 εκατομμύριο ενδεχόμενες επιθέσεις και 180.000 αποδεδειγμένες επιθέσεις ατομικών data points με την μορφή firewall logs και IDS alerts.

Η Riptech[22] προκειμένου να εξασφαλίσει μια λεπτομερή και κατανοητή ανάλυση των επιθέσεων χρησιμοποίησε τις εξής τρεις βασικές ταξινομήσεις στη μεθοδολογία της:

- **Αναγνώριση και ταξινόμηση των επιθέσεων:** Στην συγκεκριμένη περίπτωση η Riptech συνδύασε την τεχνολογία με την εξειδίκευση του προσωπικού της προκειμένου να επιτύχει μια ολοκληρωμένη ανάλυση των δεδομένων ώστε τα συμπεράσματα που στη συνέχεια θα εξαχθούν να κρίνονται αξιόπιστα. Κατά τη διάρκεια αυτής της διαδικασίας αναλύεται κάθε καταγραφή που γίνεται από το τείχος προστασίας (firewall log) και κάθε συναγερμού που ανέφερε το σύστημα ανίχνευσης εισβολής (Intrusion Detection System - IDS - alert) που παράγεται από τις συσκευές των πελατών και στη συνέχεια μελετάται ολόκληρη η διαδοχή των επιθέσεων σε πραγματικό χρόνο. Η συγκεκριμένη διαδικασία περιλαμβάνει τα εξής τέσσερα στάδια:
  - ✓ συλλογή και κανονικοποίηση των δεδομένων ασφαλείας από το πελατολόγιο
  - ✓ επιλογή των δεδομένων ασφαλείας
  - ✓ συσχετισμό και παρουσίαση των γεγονότων
  - ✓ ταξινόμηση των επιθέσεων.
- **Ταξινόμηση των πελατών :** Κάθε πελάτης-επιχείρηση κατηγοριοποιείται με βάση μια ευρεία κλίμακα κριτηρίων, όπως το είδος της επιχείρησης, το μέγεθος, την ιδιοκτησία, την παρουσία της ως πολυεθνική, την τοποθεσία της κ.ά. Οι πληροφορίες που είναι απαραίτητες για την ταξινόμηση αυτή αντλούνται είτε από τους ίδιους τους πελάτες είτε από δημόσιες πηγές.
- **Ταξινόμηση των επιθέσεων :** Η κατηγοριοποίηση των επιθέσεων έγινε με σκοπό να ανακαλυφθούν οι πραγματικές τάσεις της ψηφιακής εγκληματικότητας και συγκεκριμένα να προσδιορισθεί η φύση των επιθέσεων μέσω του Διαδικτύου εναντίον επιχειρήσεων και οργανισμών. Έτσι, η Riptech προχώρησε στην ταξινόμηση των επιθέσεων με βάση το συνολικό αριθμό τους, τη σοβαρότητα της επίθεσης, τον τύπο της, την πηγή της, τον σκοπό αυτών που επιτίθενται, το προφίλ τους κ.ά. Μέσω αυτής της κατηγοριοποίησης γίνεται αντιληπτό κατά πόσο ορισμένες επιχειρήσεις είναι περισσότερο επιρρεπείς από κάποιες άλλες στις επιθέσεις.

Συμπεραίνεται λοιπόν, από τη διεξαγωγή της συγκεκριμένης έρευνας καταρχήν ότι οι επιθέσεις μέσω Διαδικτύου αποτελούν σημαντική απειλή για όλους τους τύπους των επιχειρήσεων και οργανισμών. Ειδικότερα τα ευρήματα της έρευνας συνοψίζονται στα εξής :

- ❖ Όσον αφορά τις τάσεις των επιθέσεων γενικά, αυτό που διαπιστώνεται είναι ότι η επιθετική δραστηριότητα κατά τη διάρκεια του εξαμήνου που πραγματοποιήθηκε η έρευνα ήταν κατά 28% υψηλότερη από την δραστηριότητα που αναφέρθηκε στη διάρκεια του προηγούμενου εξαμήνου.
- ❖ Κατά μέσο όρο, η κάθε επιχείρηση δέχθηκε 32 επιθέσεις την εβδομάδα κατά τη διάρκεια του εξαμήνου της έρευνας σε σύγκριση με 25 επιθέσεις που υπολογίζεται ότι δέχθηκε η κάθε επιχείρηση κατά το προηγούμενο εξάμηνο.
- ❖ Ενώ ο καθημερινός όγκος των επιθέσεων ποικίλει σημαντικά, η Riptech παρατήρησε μια σταθερή και βαθμιαία αύξηση των κυβερνο-επιθέσεων.

Πολύ «επιθετικές» επιθέσεις ήταν 26 φορές πιθανότερο να προέρχονται από μία σοβαρή επίθεση παρά από μέτριες επιθέσεις.

- ○ Το 3,57% των πολύ «επιθετικών» επιθέσεων προέρχονταν από μία σοβαρή επίθεση σε σύγκριση με μόνο το 0,14% που προερχόταν από μέτριες επιθέσεις. Αυτό αποδεικνύει ότι παρά το γεγονός ότι οι ιδιαίτερα «επιθετικές» επιθέσεις δεν αποτελούν συχνό φαινόμενο, ωστόσο, εξακολουθούν να θεωρούνται σημαντικότερη απειλή για τις επιχειρήσεις και τους οργανισμούς.
- ○ Το 99,99% των λιγότερων «επιθετικών» επιθέσεων ήταν μη σοβαρές είτε λόγω του ότι αυτές διεκόπησαν από τον «δράστη» είτε γιατί εντοπίστηκαν από το σύστημα ασφαλείας.

[22] http://www.symantec.com/press/2002/n020717b.html

Οι επιχειρήσεις του δείγματος ήταν λιγότερο πιθανό να πέσουν θύματα σοβαρών επιθέσεων κατά τη διάρκεια του περασμένου εξαμήνου, αποδεικνύοντας ότι αυτές οι επιχειρήσεις κατόρθωσαν με επιτυχία να προστατεύσουν τα δίκτυά τους.

- Το 23% των επιχειρήσεων υπέφεραν έστω και μία φορά από σοβαρή επίθεση κατά τη διάρκεια του εξαμήνου που διεξήχθη η έρευνα σε σύγκριση με το 43% των επιχειρήσεων που έπεσαν θύματα κατά τη διάρκεια του προηγούμενου εξαμήνου.
- Η μικρή πιθανότητα θυματοποίησης από σοβαρής μορφής επίθεση αποδίδεται κατά κάποιο τρόπο στην βαθμιαία ενίσχυση και ενδυνάμωση των μεθόδων ασφαλείας από την πλευρά των επιχειρήσεων που αποτελούσαν το δείγμα της έρευνας.

Η επιθετική δραστηριότητα εξακολούθησε να αποτελεί ένα καθημερινό και 24ωρο φαινόμενο. Παρ' όλα αυτά, κατά τη διάρκεια του εξεταζόμενου εξαμήνου οι επιχειρήσεις κινδύνευαν να πέσουν θύματα περισσότερο κατά τη διάρκεια της εβδομάδας και λιγότερο τα Σαββατοκύριακα.

- Ο αριθμός των επιθέσεων ανά ημέρα ήταν 36% μεγαλύτερος τις καθημερινές σε σύγκριση με τον αντίστοιχο αριθμό που σημειώθηκε τα Σαββατοκύριακα, ενώ το συνολικό ποσοστό της επιθετικής δραστηριότητας ήταν κατά 19% μεγαλύτερο κατά τη διάρκεια της εβδομάδας.
- Το ποσοστό των σοβαρών επιθέσεων ήταν δύο φορές υψηλότερο τις καθημερινές και το ποσοστό των πολύ «επιθετικών» επιθέσεων ήταν τρεις φορές υψηλότερο τις καθημερινές, υποδηλώνοντας ότι τελικά οι επιχειρήσεις αντιμετωπίζουν μεγαλύτερο κίνδυνο θυματοποίησης από τη Δευτέρα έως την Παρασκευή.

Επιθέσεις από τις χώρες που ανήκουν στη λίστα των χωρών κυβερνο- τρομοκρατίας ήταν μέτριες σε ένταση αλλά διαφοροποιούνταν ως προς τα βασικά χαρακτηριστικά τους.

- Από το σύνολο των χωρών που περιλαμβάνονταν στην λίστα παρακολούθησης για την τρομοκρατία στον κυβερνοχώρο, προήλθε λιγότερο από το 1% των επιθέσεων κατά τη διάρκεια του εξεταζόμενου εξαμήνου, ενώ το 84% αυτής της δραστηριότητας προήλθε από το Κουβέιτ, το Πακιστάν, την Αίγυπτο, την Ινδονησία και το Ιράν.
- Οι επιθέσεις που ανιχνεύτηκαν προέρχονταν μόνο από τις τρεις από τις συνολικά εφτά χώρες που είχαν χαρακτηριστεί από την αμερικανική κυβέρνηση ως «Επίσημοι Υποστηρικτές της Τρομοκρατίας», ενώ το Ιράκ, η Συρία, η βόρεια Κορέα, και η Λιβύη δεν συμμετείχαν σε καμία επίθεση το συγκεκριμένο εξάμηνο.
- Οι τρόποι ανάλυσης και σάρωσης διαφέρουν ανάμεσα στις χώρες που ανήκουν στην λίστα παρακολούθησης για την τρομοκρατία στο κυβερνοχώρο και σε όλες τις άλλες, γεγονός που αποδεικνύει ότι το modus operandi (τρόπος δράσης) του τρόπου δράσης των ατόμων που επιτίθενται μέσω του Διαδικτύου, διαφοροποιείται αντίστοιχα.

Οι πελάτες που δέχονταν για μεγάλο χρονικό διάστημα υπηρεσίες που αφορούσαν την ασφάλεια των συστημάτων τους είχαν λιγότερες πιθανότητες να δεχθούν επίθεση σε σχέση με τους νεότερους πελάτες.

- Περίπου το 30% των εταιρειών που υπήρξαν πελάτες για διάστημα μικρότερο των 12 μηνών δέχθηκαν τουλάχιστον μία σοβαρή επίθεση κατά τη διάρκεια του εξαμήνου διεξαγωγής της έρευνας, σε σύγκριση με μόνο το 17% των εταιρειών που ήταν πελάτες για διάστημα μεγαλύτερο των 12 μηνών.
- Περίπου το 3% των εταιρειών που υπήρξαν πελάτες για διάστημα μικρότερο των 12 μηνών δέχθηκαν τουλάχιστον μία ιδιαίτερα «επιθετική» επίθεση, σε σύγκριση με το αντίστοιχο 19% των επιχειρήσεων που υπήρξαν πελάτες για μεγαλύτερο διάστημα από αυτό των 12 μηνών. Διαπιστώνεται λοιπόν, ότι οι μακροχρόνιοι πελάτες αναγκάζουν κατά κάποιο τρόπο τους δράστες να προσφύγουν σε επιθετικότερες τακτικές προκειμένου να επιτύχουν τον στόχο τους.
- Συνοπτικά, συμπεραίνεται ότι τόσο η ένταση όσο και ο βαθμός «επιθετικότητας» των επιθέσεων αυξάνεται με το χρόνο.

Οι εταιρείες που ανήκουν στον βιομηχανικό τομέα ήταν εκτεθειμένες στον κίνδυνο επιθέσεων και αυτό δεν διαφοροποιήθηκε σημαντικά κατά την διάρκεια των εξαμήνων που εξετάσθηκαν, δηλ. του εξαμήνου που διεξήχθη η έρευνα και του προηγούμενου.

- Οι εταιρείες που σχετίζονταν με την υψηλή τεχνολογία, αυτές που παρείχαν οικονομικές υπηρεσίες και αυτές που παρείχαν ηλεκτρισμό και ενέργεια εμφάνισαν τα μεγαλύτερα ποσοστά θυματοποίησης από επιθέσεις κατά τη διάρκεια και των δύο εξαμήνων.
- Το 70% των εταιρειών παροχής ηλεκτρισμού και ενέργειας δέχτηκαν μία πολύ «επιθετική» επίθεση κατά τη διάρκεια του εξεταζόμενου εξαμήνου σε σχέση με το αντίστοιχο 57% που σημειώθηκε το προηγούμενο εξάμηνο.

Οι εταιρείες που ανήκουν στον δημόσιο τομέα συνέχισαν να εμφανίζουν μεγαλύτερο κίνδυνο θυματοποίησης σε σχέση με μη κερδοσκοπικές και μη - κυβερνητικές οργανώσεις.

- Οι εταιρείες του δημόσιου τομέα δέχθηκαν συνολικά επιθέσεις το ποσοστό των οποίων είναι κατά 50% υψηλότερο από το μέσο ποσοστό του δείγματος.
- Οι εταιρείες του δημόσιου τομέα ήταν επίσης κατά 2 φορές πιθανότερο να δεχθούν τουλάχιστον μία σοβαρή επίθεση και 2 φορές πιθανότερο να δεχθούν μια πολύ «επιθετικής» μορφής σε σύγκριση με αυτές του ιδιωτικού τομέα, τις μη κερδοσκοπικές και τις κυβερνητικές οργανώσεις.

Όσον αφορά την ανάλυση των επιθέσεων με βάση τη χώρα προέλευσή τους δεν διαφαίνονται σημαντικές διαφοροποιήσεις στα δύο εξάμηνα.

- Η πλειοψηφία των επιθέσεων μέσω Διαδικτύου, δηλαδή περίπου το 80%, σημειώθηκαν από τις πρώτες 10 χώρες στη λίστα των επιθέσεων.
- Το μέσο ποσοστό επιθέσεων ανά χρήστη Internet είναι, για τις χώρες με 100.000 έως 1 εκατομμύριο χρήστες, περίπου 50% υψηλότερο από το αντίστοιχο μέσο ποσοστό για τις χώρες με περισσότερους από 1 εκατομμύριο χρήστες.
- Ανάμεσα στις χώρες με λιγότερο από 1 εκατομμύριο χρήστες, το Ιράν και το Κουβέιτ εμφανίζουν το υψηλότερο ποσοστό επιθέσεων ανά 10.000 χρηστών Internet.

Η ανάλυση του προφίλ των δραστών αλλά και του modus operandi καταδεικνύει την ύπαρξη νέων δεδομένων χωρίς ταυτόχρονα να αναιρεί τις παλαιότερες διαπιστώσεις.

- Το ποσοστό των επιθέσεων που εμφανίζονται να έχουν στόχο μία συγκεκριμένη επιχείρηση παρέμεινε σχεδόν σταθερό, δηλ. ανέρχεται στο 37% το εξάμηνο κατά το οποίο διεξήχθη η έρευνα και στο 39% το προηγούμενο.
- Το 93% των επιθέσεων υπήρξαν ενεργές για μία μόνο μέρα, γεγονός που αποδεικνύει την ύπαρξη πλήθους χρηστών που δρουν από το σπίτι και αλλάζουν συνεχώς την διεύθυνση Πρωτοκόλλου Διαδικτύου (IP address).

Παρά το γεγονός ότι τα σκουλήκια (worms) εξακολουθούν να θεωρούνται μία από τις σοβαρότερες ενδεχόμενες απειλές, από τα δεδομένα της έρευνας αποδεικνύεται ότι η δράση τους το συγκεκριμένο εξάμηνο ήταν σχετικά υψηλή, αποτελώντας όμως μιας μέτριας μορφής απειλή για τις επιχειρήσεις του δείγματος.

- Το 44% του συνόλου των επιθέσεων προέρχονταν από worms κατά τη διάρκεια του συγκεκριμένου εξαμήνου σε σύγκριση με το αντίστοιχο ποσοστό του προηγούμενου εξαμήνου που ανήλθε στο 63%.
- Τρεις είναι κυριότερες μορφές worms (Code Red, Nimda, SQL Spinda) που χρησιμοποιήθηκαν ευρέως για τέτοιου είδους δραστηριότητα. Παρ' όλα αυτά, διαπιστώθηκε ότι κατά τη διάρκεια διεξαγωγής της έρευνας, λιγότερο από 1% των επιχειρήσεων του δείγματος δέχθηκαν σοβαρή επίθεση από worms.
- Η πλειοψηφία των επιχειρήσεων θεώρησαν τις επιθέσεις από worms περισσότερο σαν ενόχληση παρά σαν σοβαρή απειλή.

β) Ηλεκτρονικά εγκλήματα κατά επιχειρήσεων και οργανισμών στις ΗΠΑ το 2004.[23]

Η θυματολογική αυτή έρευνα πραγματοποιείται σε ετήσια βάση, έχει σαν θέμα της το ηλεκτρονικό (ψηφιακό) έγκλημα και την ασφάλεια των υπολογιστών στις ΗΠΑ και διεξάγεται από το 1995 μέχρι σήμερα, από το Ινστιτούτο Ασφάλειας Υπολογιστών **(Computer Security Institute - CSI)** σε συνεργασία με το **FBI.** Αξιοσημείωτο είναι ότι η έρευνα αυτή διεξήχθη για 9η συνεχόμενη χρονιά και θεωρείται ότι αποτελεί τη μεγαλύτερη θυματολογική έρευνα που τελείται στο πεδίο του ηλεκτρονικού εγκλήματος και της ασφάλειας των υπολογιστών. Η έρευνα αυτή αφορούσε τα περιστατικά που σημειώθηκαν σε βάρος επιχειρήσεων και οργανισμών το 2004 και τα πλήρη στοιχεία της μπορεί να τα βρει κάθε ενδιαφερόμενος στο δικτυακό τόπο του **CSI**.[24]

Όπως συνέβη στις προηγούμενες ερευνητικές προσπάθειες, έτσι και σε αυτήν, οι κυριότεροι λόγοι πραγματοποίησής της, ήταν η ενημέρωση για τα προβλήματα ασφάλειας που είναι πιθανό να αντιμετωπίσουν οι επιχειρήσεις και οι οργανισμοί που πραγματοποιούν

[23] http://gocsi.com/

[24] http://www.csiannual.com/

ηλεκτρονικές συναλλαγές, ο προσδιορισμός των βασικών τάσεων της ηλεκτρονικής (ψηφιακής) εγκληματικότητας και της ασφάλειας των

πληροφορικών συστημάτων και τέλος η επισήμανση των σημαντικών αλλαγών που κρίνεται αναγκαίο να επέλθουν στον τομέα της ασφάλειας των πληροφοριών.

Η έρευνα του 2004[25] - όπως και εκείνες των προηγουμένων ετών - πραγματοποιήθηκε με τη συμπλήρωση σχετικού ερωτηματολογίου, το οποίο απεστάλη με το κοινό ταχυδρομείο στους ειδικούς ασφάλειας επιχειρήσεων και κρατικών οργανισμών που χρησιμοποιούν στις συναλλαγές τους Η/Υ. Σε αυτό απάντησαν 494 ειδικοί ασφαλείας Η/Υ.

Ανά τομέα δραστηριότητας, οι παραπάνω απαντήσεις ελήφθησαν από επιχειρήσεις και κρατικούς οργανισμούς που ήταν σε αντίστοιχα ποσοστά:

Επιχειρήσεις & Κρατικοί οργανισμοί	Ποσοστά %
Οικονομικές	19
Υψηλής Τεχνολογίας	13
Κυβερνητικοί Οργανισμοί	13
Κατασκευαστικές	12
Εκπαιδευτικές	7
Φαρμακευτικές	6
Βοηθητικές	5
Μεταπωλήσεων	3
Τηλεπικοινωνιών	2
Μεταφορικές	1
Νομικών Υπηρεσιών	1
Άλλες	18

Επιπρόσθετα, το *19%* αυτών που απάντησαν προερχόταν από επιχειρήσεις και οργανισμούς που απασχολούσαν από 1 έως 99 άτομα προσωπικό, το *15%* από 100 έως 499, το *13%* από 500 έως 1.499, το *31%* από 1.500 έως 9.999, το *14%* από 10.000 έως 49.999 και το *7%* περισσότερα από 50.000.

Επίσης, όσον αφορά τα ετήσια έσοδα των παραπάνω, προέκυψαν τα εξής: το *20%* είχε ετήσια έσοδα μέχρι 10.000.000 δολάρια, το *23%* από 10.000.000 έως 99.000.000, το *20%* από 100.000.000 έως 1.000.000.000 και το *37%* περισσότερα από 1.000.000.000 δολάρια.

Σύμφωνα με τα ερευνητικά δεδομένα το *46%* αυτών που απάντησαν δήλωσαν ότι οι οργανισμοί τους διέθεταν από 1 έως 5% του συνολικού προϋπολογισμού του τομέα της τεχνολογίας πληροφοριών, στην ασφάλεια των πληροφορικών τους συστημάτων. Αντίστοιχα, το *23%* υπόδειξε ότι οι οργανισμοί τους διέθεταν παραπάνω από το 5%, το *16%* λιγότερο από το 1% και το *14%* δεν γνώριζε τίποτα για το θέμα αυτό.

Η έρευνα του 2004 αφενός μεν παρουσίασε τα σπουδαιότερα θέματα, τα οποία είχαν μελετήσει οι προηγούμενες έρευνες, διευκολύνοντας έτσι την ανάλυση και την κατανόηση των σύγχρονων τάσεων της ασφάλειας των πληροφορικών συστημάτων και αφετέρου παρουσίασε νέα καίρια ζητήματα που αναδύονται στο χώρο, τα οποία οι έρευνες που τελέστηκαν τα προηγούμενα χρόνια δεν τα έλαβαν υπόψη τους.

Σε γενικές γραμμές τα νέα σημαντικά θέματα που πραγματεύεται η εν λόγω έρευνα είναι τα εξής:

- ✓ Τον τρόπο με τον οποίο οι επιχειρήσεις - οργανισμοί εκτιμούν την επίδοση των επενδύσεων τους πάνω στην ασφάλεια των πληροφορικών τους συστημάτων.
- ✓ Τι τμήμα του προϋπολογισμού της τεχνολογίας πληροφοριών των επιχειρήσεων, παρέχεται για την ασφάλεια των πληροφορικών τους συστημάτων.
- ✓ Τις ανάγκες εκπαίδευσης των υπαλλήλων των οργανισμών για θέματα ασφάλειας.
- ✓ Το χρηματικό πόσο που διαθέτουν για επενδύσεις στον τομέα της ασφάλειας.
- ✓ Τον αντίκτυπο της ανάθεσης δραστηριοτήτων που αφορούν ζητήματα ασφάλειας σε άλλες εταιρείες.

[25] http://www.csiannual.com/

- ✓ Την επίδραση του νόμου Sarbanes - Oxley του 2002 στις δραστηριότητες που σχετίζονται με την ασφάλεια των πληροφορικών τους συστημάτων.
- ✓ Τη χρησιμότητα των ελέγχων ασφαλείας και της εξωτερικής ασφάλισης.

Συνεπώς, διαπιστώνεται ότι τα θέματα που αναφέρθηκαν αφορούν τις αποφάσεις που καλούνται οι επιχειρήσεις να πάρουν, όσον αφορά τα οικονομικά ζητήματα της ασφάλειας των πληροφορικών τους συστημάτων και τον τρόπο που θα διαχειριστούν τους κινδύνους που σχετίζονται με την ενδεχόμενη παραβίαση της ασφάλειας των συστημάτων τους.

Τα σημαντικότερα αποτελέσματα της έρευνας, τα οποία προέκυψαν από τις απαντήσεις των ερωτηθέντων υπευθύνων ηλεκτρονικής ασφάλειας ήταν τα εξής:

- Το 82% των επιχειρήσεων και των οργανισμών διενέργησαν ελέγχους ασφαλείας στα πληροφορικά τους συστήματα.
- Συγκριτικά με τα αποτελέσματα των ερευνών των προηγουμένων ετών, στην έρευνα του 2004 τα περιστατικά που αφορούσαν την παραβίαση της ασφάλειας των συστημάτων τους ήσαν αρκετά λιγότερα. Αντίστοιχα, το ίδιο συνέβαινε και με τα ετήσια χρηματικά ποσά που χάνονταν, λόγω της παραβίασης των συστημάτων ασφαλείας τους.
- Εν αντιθέσει με τα προηγούμενα χρόνια, διαπιστώθηκε πως οι μεγαλύτερες οικονομικές ζημιές δεν αφορούσαν τις κλοπές πνευματικής ιδιοκτησίας, αλλά τις επιθέσεις από ιούς που προσέβαλαν τα συστήματα τους και την άρνηση παροχής υπηρεσιών από το σύστημα τους.
- Μάλιστα, οι ερωτηθέντες ανέφεραν ζημιές ύψους 55.053.900 δολαρίων που οφείλονταν αποκλειστικά στις επιθέσεις από ιούς.
- Παρατηρήθηκε ότι το ποσοστό των επιχειρήσεων - οργανισμών που καταγγέλλουν τις παραβιάσεις των πληροφορικών τους συστημάτων στους επίσημους φορείς επιβολής του νόμου, είναι σε συνεχόμενη πτώση. Ο κυριότερος λόγος που δεν αναφέρθηκαν τα περιστατικά αυτά, από την πλευρά των επιχειρήσεων, σχετιζόταν με την ενδεχόμενη αρνητική δημοσιότητά τους.
- Η πλειονότητα των ερωτηθέντων πίστευαν ότι η εκπαίδευση σε θέματα ασφάλειας και οι γνώσεις που αποκτούνταν πάνω σε αυτόν τον τομέα ήταν ζήτημα πρώτης προτεραιότητας για αυτούς, μολονότι κατά μέσο όρο οι ερωτηθέντες από όλους τους τομείς θεωρούσαν ότι οι επιχειρήσεις τους δεν επενδύουν αρκετά σε αυτόν τον τομέα.
- Η πλειοψηφία των οργανισμών δεν εκχωρούν - αναθέτουν δραστηριότητες για θέματα ασφάλειας των πληροφορικών τους συστημάτων σε τρίτους. Από αυτούς που αναθέτουν κάποιες δραστηριότητες, το ποσοστό που αφορά δραστηριότητες ασφάλειας είναι πολύ μικρό.
- Διαφαίνεται ότι ο νόμος Sarbanes - Oxley[26] του 2002 έχει επιφέρει αποτελέσματα στην ασφάλεια των πληροφοριών σε μερικές βιομηχανίες.
- Οι περισσότεροι από τους οργανισμούς επιχείρησαν μια οικονομική εκτίμηση των δαπανών τους για θέματα ασφάλειας. Έτσι, τέθηκε σχετική ερώτηση για να εξακριβώσουν τη δημοτικότητα τριών οικονομικών δεικτών, αξιολογώντας ταυτόχρονα με αυτόν τον τρόπο τα κόστη και τα οφέλη που θα προκύψουν από τις επενδύσεις τους σε θέματα ασφάλειας των πληροφορικών τους συστημάτων.
- το *55%* έκανε χρήση της απόδοσης επενδύσεως *(Return on Investment)*
- το *28%* χρησιμοποίησε την αναμενόμενη απόδοση επένδυσης *(Internal Rate* of Return) και
- το *25%* έκανε χρήση της καθαρής παρούσας αξίας *(Net Present Value).*
- Το *54%* (269 σε απόλυτο αριθμό) των ερωτηθέντων προσδιόρισαν τις ζημιές τους από την παραβίαση της ασφάλειας των συστημάτων τους στο ύψος των 141.496.560 δολαρίων, από τα χαμηλότερα ποσά που έχουν καταγραφθεί από την πρώτη χρονιά διεξαγωγής αυτής της έρευνας. Ενδεικτικά το 2003 το ύψος των ζημιών είχε φτάσει τα 201.797.340 δολάρια.
- Το *20%* όσων διαπίστωσαν παραβάσεις στην ασφάλεια των συστημάτων τους τον τελευταίο χρόνο, ανέφεραν από 6 έως 10 περιστατικά, το *47%* από 1 έως 5 και το *12%* περισσότερα από 10.

[26] http://www.soxlaw.com/

- Το *89%* όσων διαπίστωσαν επίθεση κατά της ιστοσελίδας (site) τους κατά τους τελευταίους 12 μήνες ανέφεραν από 1 έως 5 περιστατικά, το *6%* από 6 έως 10 και μόλις το *5%* περισσότερα από 10.
- Το 99% δήλωσε ότι χρησιμοποιεί λογισμικό ασφάλειας δικτύων για να αντιμετωπίσει επιθέσεις από ιούς.
- Το *71%* χρησιμοποίησε λίστες ελέγχου πρόσβασης στις εφαρμογές του διακομιστή τους.
- Το *64%* δήλωσε ότι για να προστατεύσει τις πληροφορίες καθώς μεταφέρονται χρησιμοποιούν τη μέθοδο της κρυπτογράφησης των δεδομένων κατά τη μεταφορά τους.
- Παρά το γεγονός ότι η έρευνα διεξάγεται από επίσημους φορείς, δε σημειώθηκε αύξηση της διάθεσης - από την πλευρά των οργανισμών - των πληροφοριών που αφορούν τις παράνομες διεισδύσεις στα πληροφορικά τους συστήματα.
- Το *50%* αυτών που απάντησαν δηλώνουν ότι γνωστοποιούν στις αρμόδιες αρχές, πληροφορίες για την παραβίαση των συστημάτων ασφάλειας τους.
- Το *50%* από αυτούς που δεν αναφέρουν τις παράνομες διεισδύσεις στα συστήματα ασφαλείας τους στους φορείς επιβολής του νόμου, προβάλουν την άποψη ότι η αρνητική δημοσιότητα θα βλάψει το κεφάλαιο και την εικόνα των οργανισμών τους. Επιπρόσθετα, το 35% πιστεύει ότι οι ανταγωνιστικές εταιρείες θα εκμεταλλευτούν το γεγονός αυτό προς όφελος τους.
- Το 63% δήλωσε ότι δεν εκχωρούν σε άλλους φορείς λειτουργίες που σχετίζονται με την ασφάλεια των πληροφορικών τους συστημάτων. Κάποια άλλα σημαντικά στατιστικά αποτελέσματα είναι και τα ακόλουθα:
- Μόνο το 53% διαπίστωσε παραβιάσεις στην ασφάλεια των συστημάτων τους, ποσοστό το οποίο είναι το μικρότερο, αν συγκριθεί με εκείνα τα αντίστοιχα ποσοστά των ερευνών από το 1999 - τότε εμφανίστηκε η σχετική ερώτηση - και μετά. Στο σημείο αυτό πρέπει να επισημανθεί ότι το ποσοστό αυτών που απάντησαν ότι δε γνωρίζουν αν είχε συμβεί κάποια παραβίαση των συστημάτων τους έφτασε το 11%.
- Οι επιχειρήσεις που απασχολούσαν 1.500 και περισσότερα άτομα προσωπικό συγκέντρωσαν το 52% του δείγματος της έρευνας.
- Το 53% από αυτούς που απάντησαν κατείχαν - όσον αφορά τη θέση εργασίας - τον τίτλο του Διευθυντή ασφαλείας του οργανισμού. Επιπλέον, διαπιστώνεται ότι οι υπεύθυνοι ασφαλείας διαθέτουν ένα σημαντικό τμήμα του χρόνου και του κόπου τους, για να χειριστούν οικονομικές πλευρές της ασφάλειας των πληροφοριών. Αξίζει να τονιστεί ότι οι όλοι σχεδόν οι ερωτηθέντες είχαν σημαντικές αρμοδιότητες και ευθύνες, που αφορούσαν τον τρόπο διαχείρισης της ασφάλειας των πληροφορικών συστημάτων των οργανισμών.
- Παρατηρείται ότι καθώς αναπτύσσεται οικονομικά ένας οργανισμός, ταυτόχρονα μειώνονται οι δαπάνες του στην εκπαίδευση των εργαζομένων σε θέματα ασφάλειας, καθώς επίσης και οι δαπάνες σχετικά με τα συστήματα ασφάλειας των πληροφοριών.
- Λιγότερο από το 30% δήλωσαν ότι χρησιμοποιούν εξωτερική βοήθεια από άλλες εταιρείες, όσον αφορά τη διαχείριση κινδύνων της ασφάλειας των συστημάτων τους.

Στο σημείο αυτό κρίνεται αναγκαίο να γίνει μια σύντομη αναφορά στην **οικονομική ζημιά,** την οποία υπέστησαν οι επιχειρήσεις και οι οργανισμοί από τα ψηφιακά εγκλήματα, τα οποία τελέστηκαν σε βάρος τους. Ετσι, σύμφωνα με τα ερευνητικά δεδομένα υπολογίστηκαν ανά ηλεκτρονικό αδίκημα, οι παρακάτω οικονομικές ζημιές:

- 55.053.900 δολαρίων από επιθέσεις ιών,
- 26.064.050 δολαρίων από άρνηση παροχής υπηρεσιών,
- 11.460.000 δολαρίων από κλοπές πνευματικής ιδιοκτησίας,
- 10.601.055 δολαρίων από παραβιάσεις υπαλλήλων,
- 10.159.250 δολαρίων από παράνομες ακροάσεις τηλεπικοινωνιών,
- 7.670.500 δολαρίων από οικονομικές απάτες,
- 6.734.500 δολαρίων από κλοπές φορητών Η/Υ,
- 4.278.205 δολαρίων από παράνομες εισβολές στο σύστημα,
- 3.997.500 δολαρίων από τηλεπικοινωνιακές απάτες,
- 2.747.000 δολαρίων από κακή χρήση των ανακοινωμένων εφαρμογών τους στον Παγκόσμιο ιστό,
- 958.100 δολαρίων από παραποίηση των ιστοσελίδων τους,
- 901.500 δολαρίων από παράνομη διείσδυση - μη εξουσιοδοτημένη πρόσβαση υπαλλήλων τους στο σύστημα και
- · 871.000 δολαρίων από σαμποτάζ.

Συμπερασματικά, η θυματολογική έρευνα του Ινστιτούτου Ασφαλείας Υπολογιστών (CSI[27]) και του FBI για την ψηφιακή εγκληματικότητα κατά των επιχειρήσεων και των οργανισμών στις ΗΠΑ το 2004 διαπιστώνει πως:

- παρατηρείται μείωσή της όσον αφορά τα περιστατικά που σημειώθηκαν κατά επιχειρήσεων και οργανισμών το 2004 σε σύγκριση με τα προηγούμενα έτη διεξαγωγής της έρευνας.
- Είναι γεγονός ότι η εγκληματικότητα γενικότερα ως φαινόμενο και ειδικότερα οι διάφορες σύγχρονες μορφές της έχουν σημειώσει ραγδαία ανάπτυξη τα τελευταία χρόνια. Μάλιστα η ψηφιακή εγκληματικότητα παρουσιάζει στις μέρες μας μια ιδιαίτερη έξαρση. Συνεπώς, για να περιοριστεί το φαινόμενο δεν επαρκεί μόνο η γνώση της σύγχρονης τεχνολογίας αλλά κρίνεται επιτακτική η ανάγκη συνεργασίας της Κυβέρνησης με τους ιδιωτικούς φορείς.

Αναμφισβήτητα, τις τελευταίες δεκαετίες τα συστήματα διαχείρισης πληροφοριών μέσω ηλεκτρονικών υπολογιστών αποτελούν θέμα ζωτικής σημασίας για την πλειονότητα των επιχειρήσεων και των οργανισμών. Από τα μέσα της δεκαετίας του '90 το Διαδίκτυο (Internet) έχει αναδείξει τον κεντρικό ρόλο των ηλεκτρονικών υπολογιστών, στον τρόπο λειτουργίας των σύγχρονων οργανισμών. Από τη στιγμή που εμφανίστηκε το Διαδίκτυο η ασφάλεια των πληροφορικών συστημάτων έχει βρεθεί στο επίκεντρο του ενδιαφέροντος.

Στα πρώιμα της στάδια η πληροφορική ασφάλεια εστίασε το ενδιαφέρον της σε τεχνικά θέματα, όπως η κρυπτογράφηση, τα συστήματα ελέγχου πρόσβασης και τα συστήματα ανίχνευσης παράνομων εισβολών στα πληροφοριακά συστήματα. Όπως έχει ήδη επισημανθεί, σύμφωνα με τα αποτελέσματα της παρούσας έρευνας, η οικονομική και η οπτική πλευρά της διαχείρισης του κινδύνου της ασφάλειας των πληροφορικών συστημάτων έχουν αναχθεί σε καθοριστικής σημασίας θέματα για τον τρόπο λειτουργίας των σύγχρονων επιχειρήσεων. Αναντίρρητα, τα ενδιαφέροντα που προαναφέρθηκαν περισσότερο συμπληρώνουν παρά αντικαθιστούν τα τεχνικά ζητήματα που σχετίζονται με την πληροφορική ασφάλεια.

Αποτελεί κοινή παραδοχή, ότι όσο αυξάνεται το μέγεθος των γνώσεων - πληροφοριών που συλλέγονται για τις αιτίες και τις επιπτώσεις που προκύπτουν από την παραβίαση της ασφάλειας των πληροφοριακών συστημάτων, όπως επίσης και των τρόπων με τους οποίους οι επιχειρήσεις διαχειρίζονται τα ζητήματα ασφάλειας των συστημάτων τους αυτών, τόσο αυξάνονται οι πιθανότητες να βελτιωθεί η ασφάλεια τους.

γ) Έρευνα με θέμα τα ηλεκτρονικά εγκλήματα και την ασφάλεια των υπολογιστών στην Αυστραλία το 2004.[28]

Η έρευνα που επιχειρείται να παρουσιαστεί συνοπτικά στο παρακάτω κείμενο αφορά τα ψηφιακά εγκλήματα σε βάρος επιχειρήσεων και οργανισμών και διεξήχθη στην Αυστραλία το έτος 2004 με την συνεργασία της Ομοσπονδιακής Αστυνομίας και των περιφερειακών τμημάτων της με το Εθνικό Κέντρο Εγκλήματος Υψηλής Τεχνολογίας (AHTCC) και την Εθνική Ομάδα Άμεσης Επέμβασης σε θέματα υπολογιστών (AusCERT). Η συγκεκριμένη θυματολογική έρευνα βασίστηκε κατά κύριο λόγο στην αντίστοιχη έρευνα του FBI και του Ινστιτούτου Ασφάλειας Υπολογιστών (CSI) ενώ εμπλουτίστηκε με νέες ερωτήσεις σχεδιασμένες με τρόπο ώστε να συμβάλλουν στην διεξοδικότερη μελέτη και κατανόηση του ηλεκτρονικού εγκλήματος καθώς και των παραγόντων που συμβάλλουν σε αυτό.

Μέσω της έρευνας αυτής επιχειρείται η επίσημη ανάλυση των τάσεων του φαινομένου του ψηφιακού εγκλήματος, τόσο από επιθέσεις σε δίκτυα υπολογιστών όσο και από παράνομη πρόσβαση σε υπολογιστή ή από κακή χρήση, που σημειώθηκαν στην Αυστραλία το 2004. Βασικός στόχος της είναι η ευαισθητοποίηση και η ενημέρωση σε θέματα που σχετίζονται με το ψηφιακό έγκλημα, καθώς και η προώθηση αποτελεσματικότερων μέτρων πρόληψης και στρατηγικών για την αντιμετώπισή του.

---

[27] http://gocsi.com/survey

[28] http://www.auscert.org.au/render.html?it=4125

Στην έρευνα συμμετείχαν επιχειρήσεις και οργανισμοί από διάφορους βιομηχανικούς τομείς, συμπεριλαμβανομένου τόσο του ιδιωτικού όσο και του δημόσιου τομέα. Συγκεκριμένα, οι επιχειρήσεις με τη μεγαλύτερη αντιπροσώπευση ήσαν αυτές που προέρχονταν από τον τομέα της εκπαίδευσης (18%), το δημόσιο τομέα (13%) και τον κατασκευαστικό τομέα (9%). Επίσης, η πλειοψηφία των ερωτηθέντων επιχειρήσεων αποτελούταν από μεγάλους σε μέγεθος οργανισμούς που απασχολούσαν μεγάλο αριθμό υπαλλήλων και τα έσοδα και οι δαπάνες τους ήσαν ιδιαίτερα υψηλά. Ειδικότερα, το 52% των ερωτηθέντων προέρχονταν από οργανισμούς με 1000 και περισσότερους υπαλλήλους, ενώ το 17% απασχολούσε πάνω από 5000 υπαλλήλους. Επιπλέον, το 57% των ερωτηθέντων αποτελείταν από επιχειρήσεις με ετήσιο εισόδημα ή ετήσιες δαπάνες που ανέρχονταν από 10 έως 500 εκατ. δολλάρια.

Όσον αφορά τη μεθοδολογία που ακολουθήθηκε κατά την διεξαγωγή της έρευνας, γίνεται κατανοητό από τη μορφή των ερωτήσεων ότι πρόκειται για μια καθαρά ποσοτική ανάλυση που βασίστηκε στη χρήση δομημένων αυτοσυμπληρούμενων ερωτηματολογίων. Τα ερωτηματολόγια απεστάλησαν στους υπευθύνους ασφάλειας πληροφοριών τριακοσίων πενήντα (350) επιχειρήσεων της Αυστραλίας, ενώ τους ζητήθηκε είτε να απαντήσουν σε αυτά μέσω Internet και κάνοντας χρήση ασφαλούς δικτύου είτε να τα επιστρέψουν συμπληρωμένα μέσω συστημένου φακέλου. Ο βαθμός ανταπόκρισης τελικά ανήλθε στο 68,6% καθώς απάντησαν 240 επιχειρήσεις.

Το γεγονός ότι η έρευνα βασίζεται στην εθελούσια συμπλήρωση του ερωτηματολογίου από την πλευρά των επιχειρήσεων, καθώς και στην τήρηση της ανωνυμίας, προκαλεί ερωτηματικά σχετικά με την αξιοπιστία και την εγκυρότητα των αποτελεσμάτων. Επιπλέον, λόγω της διεξαγωγής της σε ετήσια βάση, γίνονται αλλαγές και διορθώσεις στη διατύπωση των ερωτήσεων, όπου κρίνεται απαραίτητο, με αποτέλεσμα να θεωρείται ανέφικτη η απόλυτη συγκρισιμότητα των στοιχείων.

Παρ' όλα αυτά, η διεξαγωγή της συγκεκριμένης έρευνας συμβάλλει στην κατανόηση των νέων μορφών του ψηφιακού εγκλήματος καθώς και των νέων τάσεων που εμφανίζονται σχετικά με την ασφάλεια των πληροφορικών συστημάτων.

Τα σημαντικότερα αποτελέσματα της έρευνας συνοψίζονται στα ακόλουθα:

- Η πλειοψηφία των επιχειρήσεων και οργανισμών έπεσε θύμα ηλεκτρονικών επιθέσεων με αποτέλεσμα να θίγεται η εμπιστευτικότητα, η ακεραιότητα ή η διαθεσιμότητα των δεδομένων του δικτύου ή του συστήματος (49% το 2004 σε σύγκριση με το 42% το 2003).
- Οι περισσότερες από τις επιθέσεις προήλθαν από εξωτερική πηγή (88% σε σύγκριση με αυτές που προήλθαν εσωτερικά και ανήλθαν μόνο στο 36%), αλλά παρ' όλα αυτά ήταν κατά σημαντικό ποσοστό λιγότερες από αυτές που σημειώθηκαν το προηγούμενο έτος (91% το 2003). Επίσης, η πλειοψηφία των ερωτώμενων θεωρεί ότι η βλάβη προήλθε από εκούσια και κακόβουλα κίνητρα (62%).
- Οι πιο κοινές μορφές ηλεκτρονικών επιθέσεων που αναφέρθηκαν από τους ερωτώμενους για τρίτη συνεχόμενη χρονιά, ήσαν οι μολύνσεις των συστημάτων από ιούς, σκουλήκια ή Δούρειους Ίππους. Μάλιστα, οι συγκεκριμένες μορφές επιθέσεων αποτελούσαν την μεγαλύτερη αιτία οικονομικών απωλειών και έφταναν το 45% του συνόλου των οικονομικών απωλειών για το 2004.
- Η αμέσως επόμενη πιο συνηθισμένη αιτία οικονομικών απωλειών ήταν η κλοπή φορητών υπολογιστών και η κατάχρηση ή η κακή χρήση του δικτύου πρόσβασης. Η μέση ετήσια απώλεια από κατάχρηση ή κακή χρήση του δικτύου πρόσβασης αυξήθηκε σε σύγκριση με το 2003 και ανήλθε κατά μέσο όρο σε 116.212 δολάρια ανά οργανισμό ή επιχείρηση.
- Διαπιστώνεται ότι οι οργανισμοί που διαθέτουν πληροφορικά συστήματα απαραίτητα για την λειτουργία τους και την παροχή των υπηρεσιών τους, δέχονταν περισσότερες και πιο επιβλαβείς ηλεκτρονικές επιθέσεις συγκριτικά με αυτούς για τους οποίους η χρήση των πληροφορικών συστημάτων δεν έπαιζε τόσο αποφασιστικό ρόλο στην λειτουργία τους (το 50% του συνόλου ήσαν οργανισμοί βασικών υποδομών πληροφόρησης (CNII- Critical national information infrastructure) ενώ το 42% όχι (non-CNII). Οι ηλεκτρονικές επιθέσεις σε επιχειρήσεις και οργανισμούς που σχετίζονται με τηλεπικοινωνίες, τραπεζικές λειτουργίες ή παροχή υδροηλεκτρικών υπηρεσιών μεταφράζονται ταυτόχρονα σε κοινωνικό κόστος, στοιχείο το οποίο τις καθιστά ευάλωτες σε τέτοιου είδους επιθέσεις.
- Οι οργανισμοί για τους οποίους τα πληροφορικά συστήματα ήσαν πρωταρχικής σημασίας (CNII organizations) έχουν οικονομικές απώλειες κατά μέσο όρο διπλάσιες από εκείνους
- για τους οποίους η χρήση των συστημάτων αυτών δεν θεωρούταν και τόσο σημαντική.

- Η ετοιμότητα των οργανισμών σχετικά με την προστασία των πληροφοριακών τους συστημάτων έχει βελτιωθεί σημαντικά σε τρία βασικά επίπεδα: εφαρμόζουν πολιτικές προστασίας των πληροφορικών τους συστημάτων, υιοθετούν κοινά πρότυπα με σκοπό την προστασία και την ασφάλεια των συστημάτων αυτών και τέλος, όλο και μεγαλύτερος αριθμός οργανισμών διαθέτουν εξειδικευμένο και εκπαιδευμένο προσωπικό. Ειδικότερα, η απόλυτη πλειοψηφία, δηλαδή το 100% των οργανισμών χρησιμοποιεί για την ασφάλεια των συστημάτων τους προστασία ενάντια στους ιούς (anti-virus) και κάνει συχνά ελέγχους πρόσβασης. Όσον αφορά την εκπαίδευση του προσωπικού, αν και γίνονται σημαντικές προσπάθειες, οι περισσότεροι ερωτώμενοι εκφράζουν σχετική δυσαρέσκεια και θεωρούν ότι η υπάρχουσα ενημέρωση είναι ανεπαρκής τόσο για το προσωπικό γενικών καθηκόντων (85%) όσο και για το αντίστοιχο προσωπικό που είχε διοικητικά καθήκοντα (80%).
- Παρά τις βελτιώσεις που επήλθαν τα τελευταία χρόνια στις πρακτικές και τους τρόπους αντιμετώπισης του ψηφιακού εγκλήματος και στην προστασία των πληροφορικών συστημάτων, όλο και λιγότεροι οργανισμοί και επιχειρήσεις ήσαν σε θέση να αντιμετωπίσουν αποτελεσματικά το πρόβλημα. Έτσι, το ποσοστό των ερωτηθέντων που αναφέρουν ότι το πρόβλημα αντιμετωπίζεται, έφτασε μόλις το 5% το 2004 σε σύγκριση με το 2003 που ήταν διπλάσιο και άγγιζε το 11%. Παρ' όλα αυτά, η πλειοψηφία των οργανισμών δηλώνει ότι έχει αυξήσει τις ετήσιες δαπάνες προκειμένου να ασφαλίσει τα
- πληροφοριακά συστήματα (70% για το έτος 2004 και 67% για το 2003).
- Ιδιαίτερα σημαντική θεωρήθηκε από την πλειοψηφία των ερωτηθέντων (45%) η ανάγκη υποστήριξης από την ανώτερη διοίκηση σε θέματα σχετικά με την ασφάλεια των πληροφοριακών συστημάτων.
- Ως κυριότεροι παράγοντες που ευνοούν την εμφάνιση επιβλαβών ηλεκτρονικών επιθέσεων αναφέρθηκαν από τους ερωτηθέντες οι εξής: η εκμετάλλευση της ευπάθειας του λογισμικού, και ειδικά σε περιπτώσεις που αυτό δεν προστατεύεται (60%), και η ανεπαρκής εκπαίδευση, εξειδίκευση και ενημέρωση του προσωπικού σε θέματα ασφάλειας των πληροφορικών συστημάτων (49%).
- Οι μεγαλύτερες δυσκολίες που αντιμετωπίζουν οι οργανισμοί προκειμένου να καταστήσουν ασφαλή τα πληροφορικά τους συστήματα είναι καταρχήν η συνεχής αλλαγή στη στάση και συμπεριφορά των χρηστών (δηλαδή του προσωπικού) όσον αφορά την προστασία των συστημάτων αυτών (και ανέρχεται στο 65% του συνόλου των ερωτηθέντων) και η ανάγκη συνεχούς ενημέρωσης σχετικά με τις νέες απειλές που προκύπτουν (61% των ερωτηθέντων).
- Παρατηρείται ότι το μεγαλύτερο ποσοστό των ερωτηθέντων επιχειρήσεων και οργανισμών δεν είναι διατεθειμένοι να αναφέρουν τα περιστατικά σε φορείς του επίσημου κοινωνικού ελέγχου και συγκεκριμένα το 75% επιλέγει να μην αναφέρει ένα ή περισσότερα περιστατικά σε οποιονδήποτε έξω από το περιβάλλον της επιχείρησης ενώ βασικότερος λόγος μη αναφοράς του περιστατικού είναι ότι ο οργανισμός σε πολλές περιπτώσεις δεν αποτελεί σαφώς προσδιορισμένο στόχο (69%).
- Τέλος, συμπεραίνεται ότι οι προσπάθειες που καταβάλουν οι ερωτηθέντες οργανισμοί και επιχειρήσεις προκειμένου να βρίσκονται σε ετοιμότητα και να προστατέψουν αποτελεσματικότερα τα πληροφοριακά τους συστήματα κρίνονται ανεπαρκείς, αν ληφθεί υπόψη ότι η φύση των κινδύνων που τα απειλούν εξελίσσεται διαρκώς. Αυτό, όπως είναι φυσικό, περιλαμβάνει την ταχύτατη διάδοση των ιών και των απειλών μέσω του Internet.

Συμπερασματικά και με βάση τα αποτελέσματα της παραπάνω ερευνητικής προσπάθειας, θα μπορούσε να ειπωθεί ότι ολοένα και μεγαλύτερος αριθμός οργανισμών και επιχειρήσεων στην Αυστραλία πέφτουν θύματα ηλεκτρονικών επιθέσεων, γεγονός που τις έχει ωθήσει στη λήψη μέτρων για την όσο το δυνατόν αποτελεσματικότερη αντιμετώπιση του φαινομένου.

δ) Έρευνα του παρατηρίου για το ηλεκτρονικό έγκλημα για το 2004 (2004 E-Crime Watch Survey)[29]

Η έρευνα αυτή πραγματοποιήθηκε από τους ειδικούς σε θέματα ασφαλείας του περιοδικού CSO σε συνεργασία με την μυστική υπηρεσία των Ηνωμένων Πολιτειών και το Ινστιτούτο Software Engineering του Πανεπιστημίου Carnegie Mellon (CERT Coordination Center)[30], με σκοπό τη σε βάθος διερεύνηση των τάσεων του ηλεκτρονικού εγκλήματος καθώς και την εμφάνιση των νέων τεχνικών που σχετίζονται με τη διάπραξή του.

Έτσι, η έρευνα πραγματοποιήθηκε μέσω του διαδικτύου με ερωτηματολόγιο που απευθύνθηκε σε συνδρομητές του περιοδικού και σε μέλη της μυστικής υπηρεσίας που ασχολούνταν με το ηλεκτρονικό έγκλημα και διήρκεσε από 15-26 Απριλίου του 2004. Το δείγμα της έφτασε τελικά, τα 500 συμπληρωμένα ερωτηματολόγια. Τα αποτελέσματά της δε συνοψίζονται στα εξής:

- Παρατηρείται αύξηση του αριθμού των ηλεκτρονικών εγκλημάτων σε σύγκριση με τον προηγούμενο χρόνο σύμφωνα με τις απαντήσεις των ερωτώμενων. Το 43% υποστηρίζει αυτή την αύξηση και το 70% αναφέρει ότι είχε τουλάχιστον ένα κρούσμα ηλεκτρονικού εγκλήματος ή εισβολή στο σύστημα του οργανισμού τους.
- Διαπιστώνεται ότι στην πλειοψηφία των περιπτώσεων οι απώλειες δεν ήταν μόνο οικονομικές. Το 56% αναφέρει ότι υπέστη λειτουργικές ζημιές, το 25% οικονομικές απώλειες ενώ το 12% δηλώνει απώλειες άλλου τύπου.
- Όσον αφορά την προστασία ενάντια στο ηλεκτρονικό έγκλημα το μεγαλύτερο ποσοστό των ερωτώμενων (51%) δηλώνει ότι ο οργανισμός τους εφαρμόζει διαδικασίες για την ανίχνευση και τον εντοπισμό πιθανών προσπαθειών διάπραξης ηλεκτρονικού εγκλήματος.
- Επιπλέον, διαπιστώνεται αρκετά μεγάλο ποσοστό εξοικείωσης με τους πολιτειακούς και τους ομοσπονδιακούς νόμους που αφορούν το ηλεκτρονικό έγκλημα (39%) ενώ άγνοια παρατηρείται σχετικά με το διεθνές δίκαιο.
- Σχετικά με τους δράστες των ηλεκτρονικών εγκλημάτων το μεγαλύτερο ποσοστό των ερωτώμενων (71%) θεωρεί ότι προέρχονται από το εξωτερικό περιβάλλον ενώ μόνο το 29% υποστηρίζει ότι σχετίζονται με το περιβάλλον της επιχείρησης.
- Επιπλέον, οι εξωτερικοί hackers συνιστούν τη μεγαλύτερη απειλή καθώς οι επιθέσεις τους είναι συχνότερες (40%) σε σύγκριση με αυτές που διαπράττονται από υπαλλήλους.
- Αναφορικά με τα είδη των ψηφιακών εγκλημάτων που διαπράττονται σε βάρος οργανισμών διαπιστώνεται ότι η παράνομη πρόσβαση σε πληροφορίες, συστήματα ή δίκτυα αποτελεί τη συχνότερη μορφή. Συγκεκριμένα, το 36% των οργανισμών που πήραν μέρος στην έρευνα έχουν διαπιστώσει παράνομη πρόσβαση σε πληροφορίες, συστήματα ή δίκτυα από άτομα που ανήκουν στο περιβάλλον του οργανισμού σε σύγκριση με το 27% που έχει διαπιστώσει την ίδια μορφή ψηφιακού εγκλήματος από άτομα του εξωτερικού περιβάλλοντος. Αντίθετα, μορφές όπως το σαμποτάζ και ο εκβιασμός αποδεικνύεται ότι διαπράττονται εξίσου από άτομα είτε του εξωτερικού είτε του εσωτερικού περιβάλλοντος του οργανισμού.
- Η συντριπτική πλειοψηφία των οργανισμών (80%) δηλώνει ότι παρακολουθούν τα ηλεκτρονικά τους συστήματα και τα δίκτυα προκειμένου να αποφεύγεται η κακή χρήση τους, από το προσωπικό. Επίσης το 49% θεωρεί ότι η εισβολή στο σύστημα μπορεί να αντιμετωπιστεί με την επιβολή των νόμων που σχετίζονται με το ψηφιακό έγκλημα.
- Τέλος, όσον αφορά τα μέτρα που λαμβάνουν οι οργανισμοί για την καταπολέμηση του ψηφιακού εγκλήματος, διαπιστώνεται ότι ιδιαίτερα συχνή είναι η χρήση firewalls (98%), ενώ ταυτόχρονα
- θεωρείται και ο πιο αποτελεσματικός τρόπος αντιμετώπισης του προβλήματος (71%).

---

[29] http://www.cert.org/archive/pdf/2004eCrimeWatchSummary.pdf

[30] http://www.cert.org/

2.3.2 ΔΗΜΟΣΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

α) Εκατόν είκοσι χιλιάδες καταγγελίες για ηλεκτρονικά εγκλήματα έγιναν το 2003[31].

Εκατόν είκοσι χιλιάδες καταγγελίες για ηλεκτρονικά εγκλήματα έγιναν το 2003, στο ειδικό Κέντρο Παραπόνων στο internet. «Πρωταθλητής» στις online παρανομίες αναδεικνύεται η Ρουμανία. Ειδικότητά τους η απάτη καταναλωτών μέσω ψεύτικων ηλεκτρονικών καταστημάτων, η εκταμίευση μετρητών από εταιρείες, που γίνεται αφού οι χάκερ αποκτήσουν τον έλεγχο των κεντρικών τους μηχανημάτων, αλλά και ο σχεδιασμός και η διάδοση επικίνδυνων ιών. «Η Ρουμανία μαστίζεται από ένα σωρό οικονομικά και κοινωνικά προβλήματα», αναφέρεται σε πρόσφατη έκθεση του Κέντρου Παραπόνων για τις Ηλεκτρονικές Απάτες (Internet Fraud Complaint Center- IFCC), το οποίο εδρεύει στη Δυτική Βιρτζίνια των Ηνωμένων Πολιτειών. «Παράλληλα όμως φιλοξενεί ένα σημαντικό ποσοστό πανέξυπνων και εξαιρετικά ικανών σε θέματα προγραμματισμού και πληροφορικής νέων ανθρώπων, οι οποίοι δεν διστάζουν να δοκιμάσουν το ταλέντο τους online και να το αξιοποιήσουν για να κερδίσουν χρήματα».

Νομοθεσία για την καταπολέμηση των ηλεκτρονικών εγκλημάτων θεσπίστηκε στη Ρουμανία στις αρχές του 2003 κι από τότε μέχρι σήμερα έχουν συλληφθεί συνολικά 60 άτομα. Το 2003, σύμφωνα με το ειδικό Κέντρο Παραπόνων για ηλεκτρονικά εγκλήματα IFCC, ήταν ούτως η άλλως «η χρονιά της ηλεκτρονικής απάτης». Το IFCC είναι μία μη κερδοσκοπική εταιρεία που δραστηριοποιείται αποκλειστικά στο Internet και χρηματοδοτείται από το αμερικανικό FBI. Ιδρύθηκε τον Μάιο του 2000 και φέτος κατέγραψε συνολικά 120.000 καταγγελίες για ηλεκτρονικά εγκλήματα κάθε λογής - 60% δηλαδή περισσότερες απ' ό,τι το 2002 (ο συνολικός αριθμός τότε ήταν 75.000).

Το Κέντρο IFCC ή IC3, κατά το Internet Crime Complaint Center, που είναι ο πρόσφατα ανανεωμένος τίτλος του) απασχολεί προσωπικό 63 ατόμων, που δέχεται και αναλύει καθεμιά από τις καταγγελίες, πριν τις προωθήσει για περαιτέρω έρευνα στις αρμόδιες υπηρεσίες του FBI. Εκτός από επιθέσεις χάκερ σε ηλεκτρονικούς υπολογιστές, τα ειδικευμένα στελέχη του Κέντρου έρχονται καθημερινά αντιμέτωπα με περιστατικά ξεπλύματος χρήματος, ηλεκτρονικούς εκβιασμούς, κλοπές πνευματικής ιδιοκτησίας, ενώ διαθέτει επίσης την τεχνολογία εντοπισμού των υπολογιστών εγκληματιών (τουλάχιστον για τις περιπτώσεις όπου η τεχνολογία αυτή μπορεί να εφαρμοστεί).

β) Κοροϊδία α λα ελληνικά[32]

«Έκρηξη» ηλεκτρονικών εγκλημάτων σημειώθηκε το 2003 και στην Ελλάδα - αν κρίνει κανείς από τα περιστατικά με τα οποία ασχολήθηκαν οι ειδικές υπηρεσίες της Ασφάλειας Αττικής τους μήνες που πέρασαν. Επιπλέον, μία από τις πιο διάσημες κομπίνες στο Διαδίκτυο, γνωστή ως «Νιγηριανή απάτη», οργανώθηκε με εγκέφαλο έναν ελληνικής καταγωγής Αυστραλό πολίτη, τον 39χρονο Νίκο Μαρινέλλη, ο οποίος, μέσω e-mail, υποσχόταν (κυρίως σε Έλληνες και Κύπριους) κέρδη από επιχειρηματικές συνεργασίες, λαχεία ή κληρονομιές, τα οποία οι δήθεν δικαιούχοι θα εισέπρατταν, αφού πρώτα πλήρωναν τα σχετικά «έξοδα».

Το κύκλωμα σατανιστών που εξαρθρώθηκε τον περασμένο Δεκέμβριο, «στρατολογούσε» μέλη μέσω του Internet και ιστοσελίδων που είχαν δημιουργήσει ένας 19χρονος σπουδαστής από τη Θεσσαλονίκη και ένας 23χρονος μπάρμαν από τον Πύργο Ηλίας. Υλικό, φωτογραφίες από σατανιστικές τελετές και κείμενα αντίστοιχου περιεχομένου, διακινούσαν, επίσης μέσω του Internet, μαθητές και σπουδαστές από ολόκληρη την Ελλάδα.

---

[31] http://www.apath.com/Introduction.htm

[32] ΤΑ ΝΕΑ , 05/01/2004 , Σελ.: P21 Κωδικός άρθρου: A17832P211 ID:397461

Επίσης, τον Φεβρουάριο του 2003, συνελήφθη (και λίγες ημέρες αργότερα αυτοκτόνησε στα κρατητήρια της Ασφάλειας) ο 55χρονος Αλέξανδρος Ε. Καλλίας, βασικός κατηγορούμενος για το κύκλωμα, που μέσω ιστοσελίδων αιμομεικτικού και παιδοφιλικού περιεχομένου οργάνωνε συναντήσεις και σόου με πρωταγωνιστές ανήλικους, σε μπαρ, στο κέντρο της Αθήνας.

Ειδική νομοθεσία για τα εγκλήματα που διαπράττονται στο Internet δεν υπάρχει στη χώρα μας, αλλά εφαρμόζεται το Κοινό Ποινικό Δίκαιο. Χώρες, όπως η Βρετανία, έχουν θεσπίσει εξαιρετικά αυστηρή νομοθεσία (από το 2001, εκεί, οι χάκερ θεωρούνται τρομοκράτες), ενώ στις Ηνωμένες Πολιτείες ορίζεται ως τρομοκρατία οποιαδήποτε πράξη μη εξουσιοδοτημένης πρόσβασης σε Η/Υ και η ποινή που επιβάλλεται στον παραβάτη μπορεί να φθάσει στην ισόβια φυλάκιση.

γ) Διεθνής επιχείρηση αποκαλύπτει κυκλώματα warez[33]

Διακόσιοι υπολογιστές κατασχέθηκαν στις ΗΠΑ και σε δέκα ακόμα χώρες στη μεγαλύτερη επιχείρηση κατά της πειρατείας στο Διαδίκτυο που έχει πραγματοποιηθεί ποτέ, ανακοίνωσε την Παρασκευή το αμερικανικό υπουργείο Δικαιοσύνης. Πάνω από 100 άτομα κατηγορούνται ότι αντέγραφαν και διακινούσαν τραγούδια, ταινίες και παιχνίδια.

Ένας από τους 30 διακομιστές που χρησιμοποιούνταν για την αποθήκευση και τη διανομή του υλικού φέρεται μάλιστα να περιείχε 65.000 τίτλους.

Η επιχείρηση είχε στόχο τις οργανώσεις που ευθύνονται για το μεγαλύτερο μέρος του πειρατικού υλικού που διακινείται στα δίκτυα ανταλλαγής αρχείων στο Διαδίκτυο (γνωστού με τον όρο warez), δήλωσε ο υπουργός Δικαιοσύνης των ΗΠΑ Τζον Ασκροφτ.

Πράκτορες του FBI και ξένων υπηρεσιών πραγματοποίησαν την Τετάρτη και την Πέμπτη επιδρομές σε 27 αμερικανικές πολιτείες, τη Βρετανία, τη Δανία, το Βέλγιο, τη Γαλλία, τη Γερμανία, την Ουγγαρία, τη Σουηδία, την Ιρλανδία το Ισραήλ και τη Σιγκαπούρη.

Συλλήψεις δεν ανακοινώθηκαν, ωστόσο ο Ασκροφτ δήλωσε ότι θα ασκηθούν διώξεις κατά ορισμένων από τους υπόπτους. Θα αντιμετωπίσουν την κατηγορία της παραβίασης πνευματικών δικαιωμάτων, μεταξύ άλλων, η οποία στις ΗΠΑ τιμωρείται με ποινή φυλάκισης έως και πέντε ετών για κάθε περίπτωση.

Οι κατηγορούμενοι αποκτούσαν πρόσβαση σε υλικό που καλύπτεται από πνευματικά δικαιώματα μέσω διαφόρων παράνομων οδών. Μεταξύ άλλων, έσπαγαν κωδικούς σε προστατευμένα προγράμματα, συνεργάζονταν με άτομα που εργάζονται στη βιομηχανία του κινηματογράφου, της μουσικής και του λογισμικού καθώς και με προγραμματιστές που δοκιμάζουν προγράμματα για λογαριασμό τρίτων.

Ο Ασκροφτ αρνήθηκε να αποκαλύψει τις τοποθεσίες όπου έγιναν οι επιδρομές, σχολίασε όμως ότι οι ομάδες του warez συχνά χρησιμοποιούν τους υπολογιστές κολεγίων και πανεπιστημίων.

Σύμφωνα με το Reuters, το 2001 οι αμερικανικές διωκτικές αρχές εξάρθρωσαν κύκλωμα warez με την ονομασία DrinkOrDie και πέτυχαν την καταδίκη των δύο ηγετών του.

[33] gsm.forum.gr/forum - Ημερομηνία 28 - 4 - 2004

δ) Ιοί υπολογιστών στην υπηρεσία του οργανωμένου εγκλήματος[34]

Οι ιοί των ηλεκτρονικών υπολογιστών αποκτούν τώρα έναν νέο ρόλο: Γίνονται η «μηχανή» που προσφέρει κέρδη σε πάσης φύσεως εγκληματίες.

Όταν ο ιός Sobig χτύπησε υπολογιστές σε όλο τον κόσμο, όλοι ανησύχησαν. Το 2003 έγινε πρωτοσέλιδο, όταν μόλυνε ένα εκατομμύριο υπολογιστές προκαλώντας προβλήματα που κόστισαν στις εταιρείες δισεκατομμύρια δολάρια, καθώς μπλόκαρε την κίνηση στο Διαδίκτυο, κατέστησε ανενεργούς δεκάδες εξυπηρετητές δικτύου (server) και δημιούργησε αναστάτωση σε μεγάλες επιχειρήσεις, όπως ο αερομεταφορέας Air Canada και η σιδηροδρομική εταιρεία-κολοσσός CSX Corp.

Η επόμενη γενιά ιών υπολογιστών, όμως, θα είναι πολύ πιο επικίνδυνη - και βρίσκεται ήδη εδώ. Τον Ιούνιο εμφανίστηκε ένας νέος ιός με το όνομα Scob. Αρχικά δεν τράβηξε την προσοχή των ειδικών, αν και έκανε την εμφάνισή του με τρόπο εντυπωσιακό στις οθόνες υπολογιστών. Ο Scob, όμως, λειτούργησε υπόγεια. Όταν κάποιος επισκέπτεται μια μολυσμένη ιστοσελίδα, ο υπολογιστής του μολύνεται με τον αόρατο ιό, ο οποίος αρχίζει να συλλέγει αριθμούς πιστωτικών καρτών, κωδικούς και άλλα ψηφιακά μυστικά που αποκαλύπτει κανείς όταν κάνει ψώνια στο Διαδίκτυο. Έπειτα, ο Scob στέλνει αυτά τα δεδομένα σε οργανωμένες συμμορίες στη Ρωσία, από όπου πιθανώς μεταπωλούνται σε τρίτους.

Οι περισσότεροι ιοί εκμεταλλεύονται κάποιες γνωστές «τρύπες» στο λογισμικό της Microsoft, όμως ο Scob βρίσκει «τρύπες» που κανείς δεν είχε εντοπίσει νωρίτερα. Όταν πρωτοχτύπησε, το έκανε χωρίς προειδοποίηση. Όταν η Microsoft έμαθε για τον Scob, συμβούλεψε τους χρήστες να απενεργοποιήσουν κάποια λειτουργία του Internet Explorer, ώστε να αναχαιτιστεί ο ιός. Μερικές εβδομάδες μετά, η Microsoft χτύπησε το καμπανάκι του κινδύνου σε εκατομμύρια πελάτες, διαθέτοντας ταυτόχρονα ένα αρχείο αναβάθμισης για να σταματήσει το Scob. Η εταιρεία δεν γνωρίζει, όμως, πόσοι χρήστες «κατέβασαν» αυτό το αρχείο.

Ο Scob εξακολουθεί να κυκλοφορεί στο Διαδίκτυο ακόμη και σήμερα μολύνοντας υπολογιστές. Τον Σεπτέμβριο μεγάλη αμερικανική εταιρεία πωλήσεων λιανικής ανακάλυψε πως ο Scob είχε μπει σε κεντρικούς της υπολογιστές και ιδιαίτερα σε αυτούς που χρησιμοποιούνταν για την εκκαθάριση συναλλαγών με πιστωτικές κάρτες. Ένας υπάλληλος είχε χρησιμοποιήσει τον υπολογιστή για να «κατεβάσει» τραγούδια από μια ιστοσελίδα που είχε μολύνει ο ιός.

Όταν οι δημιουργοί του Scob - πιθανώς οργανωμένη συμμορία με έδρα τη Ρωσία - έβαλαν στο μάτι τον υπολογιστή, κατάφεραν να εγκαταστήσουν σε αυτόν πρόγραμμα της κατηγορίας των «Δούρειων ίππων» που χρησιμοποιούνται για τη συλλογή πληροφοριών σχετικά με πιστωτικές κάρτες κ.λπ. Τα στοιχεία αυτά τα έστειλαν έπειτα μέσω Ίντερνετ σε 16 διαφορετικούς υπολογιστές στη Ρωσία. «Αυτό γινόταν συνεχώς επί τέσσερις μήνες», λέει ο Bryan Sartin, ειδικός στην ασφάλεια υπολογιστών, τον οποίο κάλεσε να αναλάβει δράση μεγάλη τράπεζα που συνεργαζόταν με την αλυσίδα λιανικών πωλήσεων (καμία από τις δύο εταιρείες δεν αφήνει τον Sartin να αποκαλύψει ποιες είναι).

Οι ιοί των υπολογιστών που κάποτε ήταν έργο εφήβων που αναζητούσαν την αναγνώριση, σήμερα αποτελούν το μέσο με το οποίο το οργανωμένο έγκλημα κερδίζει πολλά χρήματα. Χρησιμοποιούνται από εγκληματίες για να «κλέψουν» οικονομικά στοιχεία χρηστών. Πλαστογράφοι διαβατηρίων στη Βουλγαρία συνεργάζονται με χάκερς στην Αριζόνα και δημιουργούν ιστοσελίδες στο New Jersey για να κάνουν απάτες με πιστωτικές κάρτες. Μεσάζοντες από τη Λετονία σε συνεργασία με δημιουργούς ιών εκβιάζουν εταιρείες να τους καταβάλουν λύτρα απειλώντας να πλήξουν τους server τους με ιούς.

Και οι ιοί συνεχίζουν να εξαπλώνονται. Ο γνωστός Sobig «δεν ήταν κάτι που έφτιαξε κάποιος μέσα σε ένα Σαββατοκύριακο», λέει ο John Watters, διευθύνων σύμβουλος της Idefense, εταιρείας που ειδικεύεται στην καταπολέμηση εγκλήματος από το Διαδίκτυο, και προσθέτει: «Χρειάστηκαν μήνες για να δημιουργηθεί ο Sobig και οι πρώτες εκδόσεις του ιού

---

[34] http://www.tanea.gr/rendered.htm

ήταν δοκιμαστικές, ώστε αργότερα να επιτευχθεί μεγαλύτερη υποκλοπή οικονομικών στοιχείων».

Φαίνεται ότι οι ημέρες που οι ιοί δημιουργούνταν από εφήβους που ήθελαν να διασκεδάσουν έχουν παρέλθει και πολλοί θα τις αναπολήσουν.

Μετά τον Sobig, μια νέα απειλή έκανε την εμφάνισή της: Ο ιός Mimail εμφάνιζε μια φόρμα στην οποία οι χρήστες καλούνταν να συμπληρώσουν τα οικονομικά τους στοιχεία, όπως είναι οι αριθμοί πιστωτικών καρτών. Στη συνέχεια ο Mimail έστελνε τα δεδομένα αυτά με ηλεκτρονικό ταχυδρομείο στη Ρωσία. Δεν είναι τυχαίο ότι πρόσφατα υπήρξε εκβιασμός με θύμα μεγάλη βρετανική εταιρεία που δραστηριοποιείται στα στοιχήματα μέσω του Διαδικτύου. Η σπείρα ζήτησε από την εταιρεία να καταθέτει 50.000 δολάρια τον μήνα σε λογαριασμό στη Λετονία, προκειμένου να αποφύγει μελλοντικές επιθέσεις στους υπολογιστές της.

ε) Ιστοσελίδα κλέβει κάρτες[35]

Μία ιστοσελίδα που «κλέβει» αριθμούς πιστωτικών καρτών και ευαίσθητα προσωπικά δεδομένα θεωρείται πλέον από τους ειδικούς ως η πιο σημαντική ηλεκτρονική απειλή αυτής της περιόδου στο Διαδίκτυο.

Εμφανίστηκε για πρώτη φορά τον περασμένο Απρίλιο και από τότε μέχρι σήμερα έχει «χτυπήσει» περισσότερους από 12 εκατομμύρια ηλεκτρονικούς υπολογιστές σε ολόκληρο τον κόσμο. Μέχρι στιγμής, παραμένει άγνωστος ο αριθμός των κομπιούτερ που έχουν χτυπηθεί στη χώρα μας - ωστόσο, εκφράζονται ανησυχίες ότι είναι αρκετά μεγάλος...

Όλα αρχίζουν με ένα μήνυμα που φτάνει στο ηλεκτρονικό ταχυδρομείο από κάποια φαινομενικά γνωστή διεύθυνση (συνήθως από κάποιο ηλεκτρονικό κατάστημα ή από κάποια τράπεζα). Το μήνυμα καλεί τον αποδέκτη - πριν προχωρήσει σε μία ηλεκτρονική συναλλαγή - να επισκεφθεί μία συγκεκριμένη ιστοσελίδα, ακολουθώντας το σχετικό link, για να επιβεβαιώσει εκεί την ορθότητα ευαίσθητων προσωπικών δεδομένων, όπως για παράδειγμα οι αριθμοί πιστωτικών του καρτών.

Ακολουθώντας το link, ο χρήστης μεταφέρεται σε ένα site, το οποίο μοιάζει με τις επίσημες ιστοσελίδες γνωστών εταιρειών. Μόνον αν κοιτάξει κανείς προσεκτικά τα στοιχεία της διεύθυνσης καταλαβαίνει πως είναι πλαστή. Αν κάνει το λάθος και ακολουθήσει τις οδηγίες και συμπληρώσει τα στοιχεία του στη φόρμα που παρέχεται... την πάτησε. Τα συγκεκριμένα sites έχουν σχεδιαστεί για να υποκλέπτουν πολύτιμα στοιχεία και τα e-mail μπορεί να δείχνουν ότι προέρχονται από τράπεζες, εταιρείες παροχής υπηρεσιών πρόσβασης στο Internet, ακόμα και από ινστιτούτα ερευνών, όμως στην πραγματικότητα είναι μηνύματα που κρύβουν έναν επικίνδυνο ιό. Το όνομά του είναι HTML/Phishing. gen και ανήκει στην κατηγορία των «trojan» - των ιών δηλαδή που εγκαθίστανται στον υπολογιστή και δρουν ως δούρειος ίππος, σύμφωνα με το Virus Radar Online, ένα γνωστό ηλεκτρονικό παρατηρητήριο ιών στο Διαδίκτυο.

Τρόποι προφύλαξης

«Καμία σοβαρή εταιρεία δεν ζητάει ευαίσθητα προσωπικά δεδομένα με τον τρόπο αυτό και οι χρήστες δεν θα πρέπει σε καμία περίπτωση να δίνουν επιπόλαια τα στοιχεία τους στο Δίκτυο», τονίζει ο κ. Χαράλαμπος Νικόπουλος, από την εταιρεία Adaox. «Αυτός είναι ο πιο απλός τρόπος προφύλαξης», τονίζει.

Σύμφωνα με τον κ. Josematren Swinkels, υπεύθυνο της εταιρείας Inter, η οποία έχει την έδρα της στη Λάρισα, «η λογική είναι η πρώτη άμυνα απέναντι στις ψηφιακές απειλές - να δει δηλαδή κανείς τι είναι το μήνυμα που δέχεται και από πού προέρχεται. Όμως, κρίνοντας από τον αριθμό των θυμάτων, οι περισσότεροι χρήστες μοιάζει να είναι επιπόλαιοι και όχι καλά ενημερωμένοι».

---

[35] ΤΑ ΝΕΑ , 21/07/2005 , Σελ.: Ν17 Κωδικός άρθρου: Α18294Ν171 ID:477260

2.3.3 ΠΡΟΣΩΠΙΚΕΣ ΑΝΑΦΟΡΕΣ

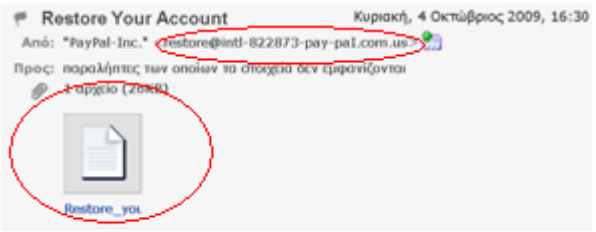
Αναφέρεθήκαμε προηγούμενα με τις μορφές που έχουν οι απάτες μέσω του διαδικτύου.Είναι ώρα λοιπόν να μπούμε στον ρόλο του θύματος και να δούμε μερικές «επιθέσεις» που έχουμε καταγράψει και εμείς οι ίδιοι ως χρήστες του διαδικτύου.

Phising Mails

Τα μηνύματα αυτά τις περισσότερες φορές αποσκοπούν στην εκμέευση προσωπικών πληροφοριών από το θύμα όπως στοιχεία λογαριασμών,στοιχεια πιστωτικών καρτων,στοιχεια καρτων αναληψης απο ΑΤΜ και γενικότερα οποιοδήποτε στοιχειο μπορεί να αποφέρει ένα άμεσο οικονομικό όφελος.Τις περίσότερες φορές είναι εύκολα αντιληπτά απο τους χρήστες αλλά υπάρχουν και περιπτώσεις όπου μέσα απο την άγνοια μας πέφτουμε εύκολα θύματα εξαπάτησης απο επιτήδειους.

α) PayPal (www.paypal.com)

Ως χρήστης του Paypal δέχθηκα ένα μύνημα που ανέφερε ότι ο λογαριασμός μου έχει δεσμευθεί και ως θα πρέπει να συμπληρώσω και να αποστείλω την φόρμα που μου είχαν επισυνάψει.Για να δούμε όμως πως μπορούμε να διαπιστώσουμε αν αυτό είναι πραγματικότητα.Πρώτον μπορούμε να κάνουμε login στο λογαριασμό μας και να δούμε αν κάτι πάει στραβά και αν όντως έχει δεσμευθεί.Δεύτερον παρατηρούμε ότι η διεύθυνση αποστολής έχει την μορφή restore@intl-822873-pay-pal.com.us πράγμα που μας βάζει σε υποψίες καθώς δεν ακολουθεί την μορφή που έχουν τα e-mail δηλαδη user@domain.com/gr etc με το πρώτο μέρος να αναφέρεται στον χρήστη και το δέυτερο να αναφέρεται στον κάτοχο του domain και τρίτον το συνημμένο που είναι σε html μορφή δεν συνδέεται με ασφαλή κρυπτογραφημένη 256 bit σύνδεση (htpps) που συνδέονται αυτές οι υπηρεσίες για την μετάδοση τέτοιων πληροφοριών.



Restore your account

You have received this file because your PayPal Account has been temporarily suspended.Please fill out and submit this form in order to restore your account

Please fill in all fields.

Για να δούμε και την μορφή που είχε όμως η συγκεκριμένη html σελίδα που μας στάλθηκε.Απ'ότι βλέπουμε μας ζητάνε όλα τα προσωπικα μας στοιχεία όπως το ονοματεπώνυμο, την διεύθυνση , το social security number που είναι το ΑΜΚΑ , ημερομηνία γέννησης και όσο συνεχιζουμε βλέπουμε ότι μας ζητάνε και τα στοιχεία που τους ενδιαφέρουν περισσότερο όπως τον αριθμό της πιστωτικής ή της χρεωστικής κάρτας που έχουμε , την ημερομηνία λήξης , την τράπεζα έκδοσης και στο τέλος το PIN.

Εμείς τώρα θα το πάμε ένα βήμα παραπάνω για να δούμε που καταλήγουν όλα αυτά τα στοιχεία που συλλέγονται και παράλληλα πως μπορούν να εντοπιστούν και να αντιμετωπίσουν την νομική πλευρά του πράγματος.Με την επιθεώρηση στοιχείου του google chrome βλέπουμε τον κώδικα που αντιστοιχεί στην html σελίδα που μας στείλανε . Εκεί παρατηρούμε την διεύθυνση που αντιστοιχεί στο σημείο που αποστέλονται όλα αυτά τα στοιχεία που συλλέγονται.Η διεύθυνση αυτή έχει την IP address 76.12.120.203 που αντιστοιχεί στον πάροχο του web hosting και τον τόπο που συλλέγονται όλες αυτές οι πληροφορίες.Πράγματι με σύμμαχο το διαδικτύο και ένα πρόγραμμα για IP Tracing[36] βλέπουμε τα επακριβή στοιχεία αλλά και την τοποθεσία των servers του συγκεκριμένου web hoster όπου έγινε η φιλοξενία της βάσης δεδομένων που θα δεχόταν όλες αυτές της πληροφορίες.Έτσι λοιπόν γνωρίζοντας το πού εύκολα μπορούμε να εντοπίσουμε το ποίος βρίσκοντας την IP που έχει αυτός που έφτιαξε το account με την βάση δεδομένων.

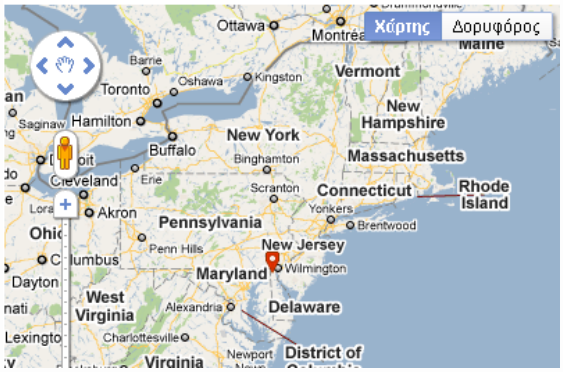

General IP Information

Hostname: 76.12.120.203
ISP: HostMySite
Organization: HostMySite
Proxy: None detected
Type: Corporate
Assignment: Static IP
Blacklist: Blacklist Check

Geolocation Information

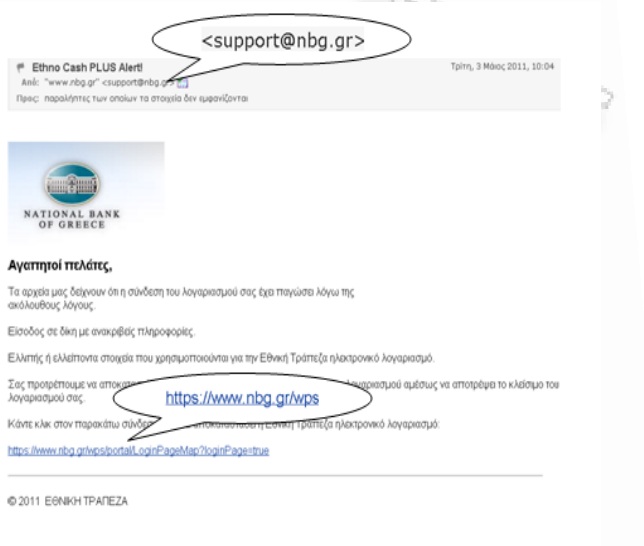
Country: United States
State/Region: Delaware
City: Newark
Latitude: 39.6155
Longitude: -75.7044
Area Code: 302
Postal Code: 19702

Geolocation Map

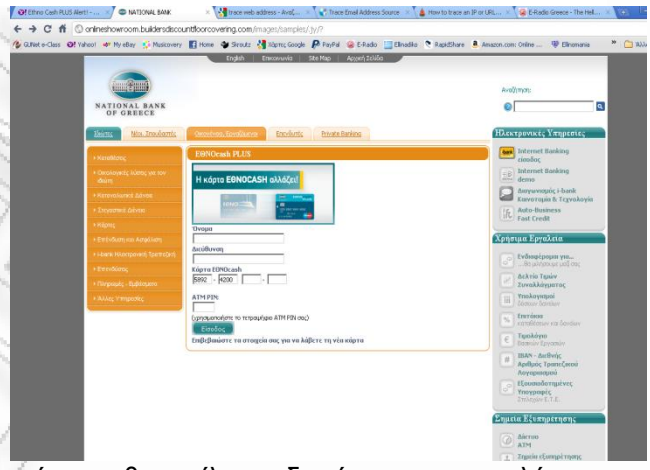


[36] http://www.ip-adress.com/ip_tracer

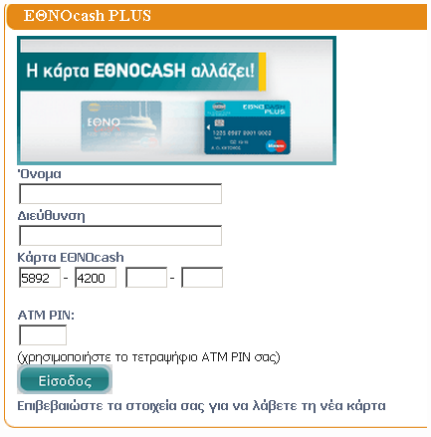
β)Εθνική Τράπεζα (www.nbg.gr)



Η δεύτερη περίπτωση είναι κυρίως ελληνική με στόχο πελάτες της Εθνικής Τράπεζας που είναι χρήστες του e-banking και όχι μόνο. Με ένα e-mail μας ενημερώνουν ότι ο λογαριασμός μας έχει παγώσει και πρέπει να κάνουμε κλίκ στον σύνδεσμο που μας στέλνεται έτσι ώστε να αποκτήσουμε και πάλι πρόσβαση στον λογαριασμό μας.Αντίθετα με την προηγούμενη περίπτωση(Paypal) εδώ το e-mail το μόνο αρνητικό χαραστηριστικό που έχει εντοπίζεται στην σύνταξη του κειμένου το οποίο όμως είναι ικανό να μας προϊδεάσει ότι δεν είναι έγκυρο.Η διεύθυνση αποστολής (support@nbg.gr) , το link που μας δίνεται να ακολουθήσουμε είναι έγκυρα καθώς βλέπουμε ότι η μέν διεύθυνση αποστολής έχει έγκυρη μορφή και το δε link φαινομενικά συνδέεται σε ασφαλή σύνδεση για να γίνει η αποστολή των δεδομένων.Για να δούμε όμως τι γίνεται με το link που έχουμε και που μας έχουν στείλνει.



Κάνοντας κλίκ λοιπόν πάνω στον υπερσύνδεσμο οδηγούμαστε στην σελίδα που βλέπουμε δεξιά μας.Παρατηρούμε λοιπόν ότι η διέθυνση στην οποία συνδεθήκαμε με την διεύθυνση που αναφερόταν στο e-mail δεν συμπίπτουν και για την ακριβεία συνδεθήκαμε στην http://onlineshowroom.buildersdiscountfloorcovering.com πράγμα που σημαίνει ότι τα στοιχεία που θα στείλουμε δεν έχουν ως παραλήπτη την τράπεζα αλλά κάποιον επιτήδιο με σκοπό την εξαπάτησή μας.



Επίσης μας ζητάνε να εισάγουμε τα στοιχεία της cashcard που έχουμε για ανάληψη χρημάτων από ATM όπως όνομα,διεύθυνση τον αριθμό της κάρτας και το pin με την πρόφαση ότι θα μας στείλουν καινούργια. *Παρεμπιπτόντως σε τηλεφωνιακή επικοινωνία που είχα με την τράπεζα μου ανέφεραν ότι όντως η Cashcard αλλάζει αλλά η διαδικασία που ακολουθείται είναι διαφορέτικη.*Άρα είναι προφανώς μία σελίδα που ως στόχο έχει να εξαπατήσει πελάτες της τράπεζας

ΚΕΦΑΛΑΙΟ 3

ΟΙ ΣΥΝΧΡΟΝΟΙ ΕΓΚΛΗΜΑΤΙΕΣ

3.1 ΟΡΙΣΜΟΣ

Λαμβάνοντας υπόψη τη διάκριση των ψηφιακών εγκλημάτων, σε γνήσια και σε παραδοσιακά που τελούνται με τη χρήση της ψηφιακής τεχνολογίας, θα πρέπει να πούμε πως ιδιαίτερη κατηγορία εγκληματικής συμπεριφοράς, που χρήζει παραπέρα ανάλυσης, αποτελεί εκείνη την οποία επιδεικνύει **ο δράστης των γνήσιων ηλεκτρονικών εγκλημάτων.** Αυτός δραστηριοποιείται αποκλειστικά στον κυβερνοχώρο και αυτός χρησιμοποιεί αποκλειστικά και μόνο την ψηφιακή τεχνολογία για να παραβεί το νόμο. Τα από εγκληματολογική άποψη χαρακτηριστικά των δραστών των παραδοσιακών εγκλημάτων - εκβιαστών, απατεώνων, τρομοκρατών κλπ. - είναι ήδη γνωστά και δεδομένα και δεν αλλάζουν από το γεγονός ότι αλλάζει ο τόπος - "κυβερνοχώρος/Διαδίκτυο" - και το μέσο εκδήλωσης - "ψηφιακή τεχνολογία" - της εγκληματικής τους συμπεριφοράς.

Με βάση τις παραπάνω σκέψεις μας θα θεωρήσουμε λοιπόν, ως ηλεκτρονικό εγκληματία εκείνον που διαπράττει τα γνήσια ηλεκτρονικά εγκλήματα.

Ο ψηφιακός αυτός εγκληματίας είναι γνωστός τόσο στο ευρύ κοινό όσο και στη βιβλιογραφία αλλά και στα ΜΜΕ κυρίως ως **Hacker** αλλά και ως C**racker (σπάστης)** ή **Cyberpunk (κεβερνοπάνκ).**

Για τη λέξη Hacker **το 21st Century Dictionary of Computer Terms σημειώνει πως,**

«...Είναι μια λέξη της αγγλικής αργκό που αναφέρεται σε κάποιον που δεν έχει εκπαιδευτεί στη χρήση των Η/Υ, για τους οποίους όμως επιδεικνύει πολύ μεγάλο ενδιαφέρον. Το άτομο αυτό μαθαίνει πειραματιζόμενο με τους Η/Υ, κάτι που συνεπάγεται συχνά το ότι αποπειράται να μπει σε βάσεις δεδομένων ή σε συστήματα Η/Υ χωρίς να έχει σχετική εξουσιοδότηση από τον ιδιοκτήτη τους. Ενας hacker μπορεί ή δεν μπορεί να ενδιαφέρεται να αποκτήσει πληροφορίες στις οποίες δεν έχει νόμιμη πρόσβαση...»

Πιο σύντομος, αλλά ουσιαστικά ίδιος, είναι ο ορισμός που δίνει η Quarantiello (1997) [37]στον hacker λέγοντας πως αυτός είναι,

«....ένα *πρόσωπο που με πρόθεση εισβάλλει σ' ένα σύστημα Η/Υ, χωρίς προηγούμενη* εξουσιοδότηση...» ***και πως***

«..ο όρος αυτός χρησιμοποιείται επίσης για να δηλώσει εκείνον που λατρεύει τους Η/Υ και ο οποίος απολαμβάνει τα υπερ και τα κατά της ενασχόλησής του αυτής».

Από τους ορισμούς αυτούς μας ενδιαφέρει φυσικά ο πρώτος γιατί αυτή είναι εκείνος που αφορά δραστηριότητα που χαρακτηρίζεται σαν εγκληματική από τον Ποινικό μας Κώδικα[38] .

Παρόμοιος είναι και ο ορισμός που δίνει για τον **Cracker** το "Λεξικό διαδικτύου και Δικτύων της Microsoft" το οποίο σημειώνει πως αυτός είναι,

... διαρρήκτης, σπάστης... Κάποιος που παρακάμπτει τα μέτρα ασφαλείας ενός συστήματος υπολογιστή και αποκτά μη εξουσιοδοτημένη πρόσβαση..."

Ο όρος αυτός χρησιμοποιείται αποκλειστικά και μόνο για να περιγράψει εκείνον που ασχολείται με τη διαγραφή ή με την καταστροφή των αρχείων του συστήματος στο οποίο απέκτησε παράνομη πρόσβαση. Στην περίπτωση αυτή δηλ. θεωρείται δεδομένη η πρόθεση του εισβολέα να βλάψει τα αρχεία του συστήματος αυτού, πράγμα που συνήθως το κάνει για να αποκομίσει οικονομικό όφελος.

Όσον αφορά τον όρο Cyberpunk το παραπάνω λεξικό δηλώνει πως μεταξύ άλλων αναφέρεται και σε,

". πρόσωπο ή μυθιστορηματικό χαρακτήρα που μοιάζει με τους ήρωες των έργων κυβερνοπάνκ[39]**"**

---

[37] http://lists.virus.org/isn-9807/msg00036.html

[38] ά. 370Γ παρ. 2,3 Π.Κ.

[39] δηλ. επιστημονικής φαντασίας

Ανεξάρτητα από το ποιος από τους παραπάνω όρους χρησιμοποιείται για να υποδηλώσει τον ψηφιακό εγκληματία η συγκεκριμένη συμπεριφορά του θεωρείται και είναι εγκληματική. Τόσο η χωρίς εξουσιοδότηση είσοδος κάποιου σε ξένο υπολογιστή, σε δίκτυο κλπ. όσο και οι παραπέρα ενέργειές του οποιεσδήποτε και αν είναι αυτές, θεωρούνται ποινικά κολάσιμες ανεξάρτητα από το κίνητρο που τον ώθησε στην διάπραξή τους.

Επειδή όμως, ο όρος **hacker** είναι ο συνηθέστερα αναφερόμενος, είναι αυτός που θα χρησιμοποιήσουμε στη συνέχεια μιλώντας για τον ψηφιακό εγκληματία.

Με βάση τα προηγούμενα λοιπόν θα σημειώσουμε αρχικά πως είναι διαπιστωμένο ότι οι hackers αγαπούν την πρόκληση και ότι ασκούν πάνω τους μια παράξενη γοητεία και οι παραμικρές λεπτομέρειες από την τεχνολογία των Η/Υ. Είναι αυτή η γοητεία που τους παρασύρει τις περισσότερες φορές στο να παραβαίνουν το νόμο χρησιμοποιώντας τους Η/Υ τους.

Ο δρ. **Percy Black,** Καθηγητής Ψυχολογίας στο Πανεπιστήμιο Pace της Νέας Υόρκης προσπαθώντας να τους προσεγγίσει από τη σκοπιά της επιστήμης του, υποστηρίζει ότι τα άτομα αυτά αναζητούν την εξουσία ορμώμενα από ένα βαθιά ριζωμένο μέσα τους συναίσθημα αδυναμίας. Έτσι τα εγκλήματα με τη χρήση των Η/Υ που διαπράττουν τα βοηθούν να ξεπεράσουν τα συναισθήματα μειονεξίας που συχνά νοιώθουν. Η προφανής ανωριμότητα ενός hacker, κατά τον δρ. Black μπορεί να αποτελεί την έκφραση συναισθημάτων μειονεξίας και αδυναμίας που τον διακατέχουν, τα οποία εμείς οι υπόλοιποι τα ξεπερνούμε καθώς ωριμάζουμε (Quarantiello, 1997).

Ο **Donn Parker** (1998)[40] επίσης, ειδικός σε θέματα ασφάλειας Η/Υ υποστηρίζει τις ακόλουθες απόψεις:

- Οι άνθρωποι που διαπράττουν τα εγκλήματα υπολογιστών διαφέρουν μεταξύ τους ανάλογα με τις δεξιότητες, τη γνώση, τους πόρους και τα κίνητρά τους.
- Οι ψηφιακοί εγκληματίες μπορούν να έχουν διαφορετικά επίπεδα ικανοτήτων που στηρίζονται στη βασική τους εκπαίδευση, τις
- κοινωνικές τους αλληλεπιδράσεις και στην εμπειρία τους στη χρήση των ηλεκτρονικών υπολογιστών.
- Υπάρχουν τρεις κατηγορίες ψηφιακών εγκληματιών: οι κατασκευαστές εργαλείων, οι χρήστες εργαλείων και οι συγγραφείς προγραμμάτων.
- Τα κίνητρά τους περιλαμβάνουν την πλεονεξία, την ανάγκη (για να λύσουν τα προσωπικά τους προβλήματα, όπως η πληρωμή χρεών από τυχερά παιχνίδια), την αδυναμία να κατανοήσουν τη ζημιά που προξενούν σε άλλους, την προσωποποίηση των υπολογιστών (τους θεωρούν ως αντιπάλους τους σε ένα παιχνίδι) και το σύνδρομο του Robin Hood (που τους κάνει να βλέπουν τις εταιρίες τόσο πλούσιες ώστε η οικονομικές ζημιές που τους προκαλούν να δικαιολογούνται ηθικά).
- Πολλοί *χάκερ* θεωρούν ότι η απλή εισβολή σε συστήματα, ο βανδαλισμός τους ή η προφανής παραβίαση της εμπιστευτικότητάς τους είναι ένα αβλαβές και ηθικά αποδεκτό χόμπι.
- Μερικοί χάκερ θεωρούν ότι η εισβολή σε συστήματα έχει και τη θετική της πλευρά με την έννοια ότι με τον τρόπο αυτό συμβάλλουν στη βελτίωση της ασφάλειάς τους.
- Οι περισσότεροι ενεργοί χάκερ είναι νέοι άνδρες, ηλικίας 12 έως 24 ετών.
- Πολλοί γονείς χάκερ δεν έχουν καμία ιδέα για το τι κάνουν τα παιδιά τους με τον ακριβό εξοπλισμό υπολογιστών που τους έχουν κάνει δώρο.
- Μερικοί υποστηρικτές χάκερ κατηγορούν τα θύματα των χάκερ για τα ανεπαρκή μέτρα ασφάλειας που έχουν λάβει και ελαχιστοποιούν τα ηθικά ζητήματα που τυχόν προκύπτουν.
- · Μερικοί τέλος, υποστηρικτές χάκερ περιγράφουν τις επιθέσεις τους ως δικαιολογημένες διαμαρτυρίες ή άμεση δράση ενάντια στους εχθρούς του περιβάλλοντος ή της κοινωνίας γενικά.

Επίσης και δύο ειδικοί από τον χώρο της ψυχολογίας και της διερεύνησης των ψηφιακών εγκλημάτων, ο **Marc Rogers** κοινωνικός ερευνητής στο Πανεπιστήμιο Manitoba στο Winnipeg του Καναδά και ο **Jerrold M. Post,** ψυχίατρος - ερευνητής στο Πανεπιστήμιο George Washington των ΗΠΑ έχουν διακρίνει ορισμένα βασικά ψυχολογικά χαρακτηριστικά της συμπεριφοράς των hackers. Σύμφωνα με τον πρώτο, ένα από αυτά είναι το ότι αυτοί έχουν την τάση να ελαχιστοποιούν ή να παρερμηνεύουν τις συνέπειες των πράξεών τους, υποστηρίζοντας ότι με αυτές επιτελούν κοινωνικό έργο. Ο δεύτερος υποστηρίζει την άποψη ότι οι ίδιοι οι hackers

[40] http://www.flipkart.com/fighting-computer-crime-donn-parker-book-0471163783

μοιράζονται μεταξύ τους μια "ηθική ευκαμψία", η οποία σημαίνει ότι εφόσον η ανθρώπινη επαφή ελαχιστοποιείται εξαιτίας της χρήσης των υπολογιστών, η εισβολή σε αυτούς μοιάζει με ένα παιχνίδι του οποίου οι συνέπειες δεν θα πρέπει να λαμβάνονται υπόψη. Γι αυτό πιστεύουν πως όλοι όσοι κάνουν hacking δεν θα πρέπει να θεωρούνται αληθινοί εγκληματίες. Καταλήγοντας οι παραπάνω συγγραφείς δέχονται και αυτοί την άποψη ότι οι hackers διαπνέονται από ένα βαθύ συναίσθημα κατωτερότητας. Η βαθειά γνώση της τεχνολογίας των υπολογιστών και τα επιτεύγματά τους που στηρίζονται σε αυτή τους δίνουν όμως μια έντονη αίσθηση υπεροχής. *"Αποτελούν μια ομάδα του πληθυσμού που βρίσκει καταφύγιο στους υπολογιστές, επειδή οι σχέσεις τους στον πραγματικό κόσμο είναι προβληματικές"* υπογραμμίζει ο Post, και συμπληρώνει *"προξενώντας ζημιές εκατομμυρίων δολλαρίων αποτελεί γι' αυτούς μια πραγματική επίδειξη της κρυμμένης δύναμής τους".*[41]

Ο **Καστέλς** (2005)[42] τέλος, παρατηρεί χαρακτηριστικά,

"Υπάρχουν μερικοί μύθοι των που περιβάλλουν την κουλτούρα των χάκερς τους οποίους αξίζει τον κόπο να διαλύσουμε. Ένας είναι ο περιθωριακός ψυχολογικός χαρακτήρας της. Είναι αλήθεια ότι μεταξύ των χάκερς είναι διαδεδομένο το αίσθημα της ανωτερότητας έναντι του υπόλοιπου κόσμου που είναι αγράμματος στον τομέα των ηλεκτρονικών υπολογιστών, όπως υπάρχει και η τάση των χάκερς να επικοινωνούν με τον ηλεκτρονικό υπολογιστή η με άλλους ανθρώπους μέσω Η/Υ εστιάζοντας ουσιαστικά σε ζητήματα λογισμικού, τα οποία είναι ακατανόητα στους υπόλοιπους ανθρώπους. Μπορούμε επίσης να δούμε μια στενή σχέση τον κόσμο της μουσικής, της τέχνης της λογοτεχνίας στο γεγονός ότι οι χάκερ νοιώθουν μόνιμα τον πειρασμό να κόψουν τους δεσμούς επικοινωνίας με την κοινωνία και να κινηθούν ταχύτατα μέσα στις τυπικές δομές της υπολογιστικής. Εν τούτοις, είναι δίκαιο να πούμε ότι οι περισσότεροι χάκερς, ζουν φυσιολογική ζωή, τουλάχιστον εξίσου φυσιολογική με εκείνη των περισσοτέρων ανθρώπων, κάτι που δεν σημαίνει αναγκαστικά ότι οι χάκερς (ή οποιοσδήποτε άλλος) ταιριάζουν με τον ιδανικό φυσιολογικό τύπο σύμφωνα με την κυρίαρχη ιδεολογία η οποία επικρατεί στις κοινωνίες μας. Ο Λίνους Τόρβαλντς, μεταξύ πολλών άλλων, είναι αφοσιωμένος οικογενειάρχης, ο οποίος ζει μια κανονική ζωή τη γυναίκα του και τα παιδιά του σε ένα προάστιο της Σίλικον Βάλεϊ. Ναι, αν πάτε σε κάποια συνδιάσκεψη χάκερς, θα δείτε πολλούς ντυμένους στα μαύρα, ή μερικούς με μούσι (αν είναι αρκετά μεγάλοι για να προλάβουν να μεγαλώσουν τα γένια τους) και τους περισσότερους να φορούν προκλητικά μπλουζάκια (π.χ. ΚΑΨΤΕ το επιχειρηματικό κεφάλαιο ΚΑΨΤΕ). Συχνά μπορεί να βρείτε αναφορά στις εμβληματικές, αγαπημένες ταινίες τους ανάλογα με την ηλικιακή ομάδα τους: «Πόλεμος των άστρων», «Μάτριξ», «Εχθρός του κράτους». Όμως αυτό το φολκλόρ δεν χαρακτηρίζει αποκλειστικά τους χάκερς: Είναι μια από τις πολλές εκφράσεις της κουλτούρας των νέων στην εποχή και στα μέρη που ζουν χάκερς. Πράγματι, οι σοβαροί χάκερς υπάρχουν πρωταρχικά ως χάκερ on - line. Αν μεταμοντέρνοι ανθρωπολόγοι αποβιβάζονταν σε μια συνάντηση χάκερς και προσπαθούσαν να εντοπίσουν τις φυλές στη βάση αυτών των συμβόλων, θα έχαναν την ουσία της κουλτούρας. Και αυτό γιατί, όπως τονίζει ο Γουέινερ, η κουλτούρα των χάκερς και οι εσωτερικές διακρίσεις της αφορούν πνευματικές κατασκευές και τεχνολογικές διαιρέσεις."

Ένα συνηθισμένο slogan των hackers που είναι το ότι « **Η γνώση αποτελεί δύναμη** » και το οποίο αποδίδεται στον Αγγλο φιλόσοφο και πολιτικό του 17ου αιώνα **Francis Bacon,** εκφράζει με τον καλύτερο τρόπο τις αντιλήψεις τους. Η γνώση είναι βέβαιο ότι δίνει τη μεγαλύτερη δύναμη σ' όσους την κατέχουν και μάλιστα στη σημερινή εποχή με τις χιλιάδες βάσεις δεδομένων τις οποίες διαχειρίζονται κυβερνητικοί οργανισμοί και επιχειρήσεις και για την πρόσβαση των οποίων είναι απαραίτητο το Internet. Ιδού λοιπόν ο χώρος στον οποίο ο hacker θα ξεδιπλώσει σήμερα τις απεριόριστες - όπως υποστηρίζει - ικανότητές του !

Πώς όμως ξεκίνησαν οι hackers ;

Η σημερινή πορεία τους ξεκίνησε από τους νεαρούς Αμερικανούς «phone phreaks» της δεκαετίας του '60 και του '70, οι οποίοι προσπαθούσαν να ξεγελάσουν ηλεκτρονικά τα συστήματα της αμερικανικής τηλεφωνικής εταιρείας AT&T με σκοπό να κάνουν μακράς διάρκειας υπεραστικά τηλεφωνήματα χωρίς φυσικά και να τα πληρώνουν!

Η συναρπαστική τέχνη της διερεύνησης ενός συστήματος Η/Υ με σκοπό τη διαπίστωση του τρόπου λειτουργίας του ξεκίνησε ουσιαστικά στις αρχές της δεκαετίας του '70 από τους προγραμματιστές που εργαζόντουσαν στα τμήματα Η/Υ και ηλεκτρονικής μηχανικής του M.I.T.

---

41 http://tlc.discovery.com/convergence/hackers/articles/psych.html

42 http://www.geof.net/research/2005/castells-network-society

(Massahusetts Institute of Technology), του Πανεπιστημίου του Stanford καθώς και άλλων αμερικανικών Πανεπιστημίων. Ο μοναδικός σκοπός των ατόμων αυτών ήταν να μάθουν, εξερευνώντας τους Η/Υ, κάθε τι που αφορούσε τον χειρισμό τους και γενικότερα τις αλλαγές που θα μπορούσαν να τους κάνουν για να αυξήσουν την υπολογιστική ισχύ τους. Αυτοί μπορούμε να πούμε πως ήταν και οι πρώτοι hackers, η βασική φιλοσοφία των οποίων ήταν να μην κλέψουν ή να καταστρέψουν τίποτα από ένα σύστημα αλλά να μάθουν τα πάντα γι' αυτό!

Άποψή τους ήταν πως είχαν κάθε δικαίωμα να μπαίνουν σε ένα σύστημα χωρίς κανένα περιορισμό εφόσον είχαν τη δυνατότητα να κάνουν κάτι τέτοιο. Δεν είχαν πρόθεση να προξενήσουν καμμία βλάβη στη λειτουργία του και το μόνο σημάδι που άφηναν για την εισβολή τους ήταν συνήθως ένα μήνυμα για τον υπεύθυνο ασφαλείας με το οποίο του επεσήμαναν τις αδυναμίες του συστήματος. Συνήθως δε του τόνιζαν ότι χάρις σε αυτές πέτυχαν να εισβάλλουν σε αυτό και πως οποιαδήποτε ενέργειά του για να αποτρέψει μια μελλοντική εισβολή τους δεν θα είχε καμμία πιθανότητα επιτυχίας!

Έτσι το hacking θεωρήθηκε αρχικά σαν μια ενδιαφέρουσα «περιπέτεια» η οποία όχι μόνο δεν προξενούσε καμμία ζημιά σε κανένα αλλά αντίθετα μπορούσε ίσως να εξυπηρετεί ακόμα και εκπαιδευτικούς σκοπούς!

Στις δεκαετίες του '60 και του '70 οι hackers είχαν τις ακόλουθες έξι «αρχές» οι οποίες όμως θα πρέπει να σημειωθεί πως με τα σημερινά δεδομένα θεωρούνται μερικά ξεπερασμένες :

1) Η πρόσβαση στα συστήματα Η/Υ (και σε ο,τιδήποτε δείχνει πως ο κόσμος δουλεύει) θα πρέπει να είναι ελεύθερη και απεριόριστη για όλους.
2) Ολες οι πληροφορίες είναι ελεύθερες.
3) Μην εμπιστεύεσαι τις αρχές, υποστήριξε την αποκέντρωση.
4) Οι hackers θα πρέπει να κρίνονται από αυτά που κάνουν και όχι από την ηλικία, τη φυλή ή την κοινωνική τους θέση ή από τα γράμματα που ακολουθούν το όνομά τους.
5) Οι Η/Υ μπορούν επίσης να χρησιμοποιηθούν για να δημιουργήσουν τέχνη και ομορφιά.
6) Οι Η/Υ μπορούν να αλλάξουν τη ζωή προς το καλύτερο.

Η εμπορευματοποίηση της πληροφορίας και η ανακάλυψη των διαφόρων ιών (viruses) των Η/Υ δεν άργησε να σημάνει το τέλος της ρομαντικής εποχής των πρώτων hackers, - γύρω στις αρχές της δεκαετίας του '80 - ίχνη της οποία συναντούμε ακόμη και σήμερα με τις εισβολές που γίνονται σε κυβερνητικές υπηρεσίες διαφόρων κρατών - κυρίως στις ΗΠΑ - με σκοπό να αποδείξουν την ανεπάρκεια των συστημάτων ασφαλείας τους.

Αναφερόμενος όμως στη δράση των hackers της δεκαετίας του '90 ο Kyas (1997) παρατηρεί χαρακτηριστικά :

«... Από τις αρχές της δεκαετίας του 1990, ο αναρχικός υπόκοσμος των υπολογιστών έχει σταδιακά διαβρωθεί από τους επαγγελματίες hackers. Ενώ οι μεγάλες τηλεφωνικές εταιρείες ήσαν κάποτε τα θύματα, οι επαγγελματίες έχουν σαν στόχο τους σήμερα τις τράπεζες και τις επιχειρήσεις. Τον Ιούλιο του 1995, π.χ. ο Vladimir Levin, ένας Ρώσος, κατάφερε να αποσπάσει 90.000.000 δολλάρια από τη Citibank της Νέας Υόρκης και από άλλες τράπεζες. Πολλές από τις επαγγελματικές περιπτώσεις hacking δεν γίνονται ποτέ ευρύτερα γνωστές, με αποτέλεσμα η έκταση των εγκλημάτων με Η/Υ να είναι κάτι για το οποίο σήμερα μόνο υποθέσεις μπορούμε να κάνουμε....»

Θα πρέπει ολοκληρώνοντας να παρατηρήσουμε ότι σύμφωνα με την άποψη του Mckenzie Wark (2004)[43] τα νέα συνθήματα τα οποία διέπουν το κίνημα των σημερινών hackers είναι σε γενικές γραμμές τα ακόλουθα:

«... Η πληροφορία θέλει την ελευθερία αλλά παραμένει αλυσοδεμένη,
Ο κόσμος μας που κατέχει μόνο το όνειρο της νέας εποχής, πρέπει να την συνειδητοποιήσει για να μπορέσει να τη ζήσει,
Το hacking είναι μια παλαιά πρακτική που αναφέρεται στη δημιουργική απαλλοτρίωση και ελεύθερη χρήση όλου του πλούτου. Η μεγαλύτερη κλοπή είναι η ίδια η ατομική

[43] http://www.law.suffolk.edu/highlights/stuorgs/jhtl/book_reviews/2004_2005/bjornlund.pdf

ιδιοκτησία. Πολύ χειρότερο από το να ληστεύεις ένα παροχέα ίντερνετ είναι το να φτιάχνεις ένα νέο.
Τα ταξικά συμφέροντα των hackers δεν είναι η ιδιοκτησία, αλλά η χειραφέτηση της πληροφορίας από τα υλικά της δεσμά,
Για τους καπιταλιστές η εκπαίδευση ήταν το μέσον για το κέρδος. Για την τάξη - φορέα της καταπίεσης, η εκπαίδευση γίνεται το μοναδικό περιεχόμενο του κέρδους.
Οι φιλόσοφοι μέχρι τώρα ήθελαν να ερμηνεύσουν ή να αλλάξουν τον κόσμο. Για μας το ζήτημα είναι να αλλάξουμε και να κοινωνικοποιήσουμε την ουσία της πληροφορίας
Η εκπαίδευση είναι σκλαβιά. Η τάξη των hackers Μου επιθυμεί τη γνώση και όχι την εκπαίδευση.
Ο hacker κατακτά την ελευθερία της γνώσης για να χαρίσει σε όλη την κοινωνία τη γνώση της ελευθερίας,
Η βία κατά του κράτους είναι επιθυμία της εξουσίας. Η βία κατά της νέας ψηφιακής τάξης είναι η κατάκτηση της επιθυμίας,
Το κίνημα κατά της παγκοσμιοποίησης αποτελεί την παιδική ασθένεια της επανάστασης των hackers.
Ο Λένιν έλεγε «τσακίστε την παλιά κρατική μηχανή σπουδών». Εμείς λέμε τσακίστε όλα τα δίκτυα και τους μηχανισμούς του κέρδους, Θέλουμε να σπάσουμε τους κωδικούς της εκμετάλλευσης, σε έναν κόσμο που αρκείται να αποκρυπτογραφεί τον "Κώδικα Ντα Βίντσι"...»

3.2 ΚΑΤΗΓΟΡΙΕΣ HACKER

Οι **Kovacich** και **Boni** (2000)[44] υποστηρίζουν ότι μια επιχείρηση ή ένας οργανισμός που είναι τα συνήθη θύματα των ψηφιακών εγκληματιών, μπορούν να αναζητήσουν τους hackers που έχουν τη δυνατότητα να προσβάλλουν τα συστήματά τους, σε μία από τις ακόλουθες πέντε κατηγορίες ατόμων :

- ✓ Στους φοιτητές Πανεπιστημίων και Κολλεγίων καθώς και στους
- ✓ μαθητές μέσης εκπαίδευσης.
- ✓ Ανάμεσα στους υπαλλήλους τους,
- ✓ Σε εκείνους που κινούνται στον υπόκοσμο των Η/Υ,
- ✓ Σε παλιούς εγκληματίες από τον κόσμο των ναρκωτικών και του
- ✓ οργανωμένου εγκλήματος και τέλος

Στους επαγγελματίες που έχουν ως αντικειμενό τους τη βιομηχανική κατασκοπεία και οι οποίοι εργάζονται για λογαριασμό των ανταγωνιστών τους.

Για από τις ομάδες αυτές ο συγγραφέας παρατηρεί σε γενικές γραμμές τα ακόλουθα:

Για τους φοιτητές και τους μαθητές.

Σ' αυτούς οφείλονται οι περισσότερες απόπειρες εισβολών σε δίκτυα επιχειρήσεων, χωρίς αυτό να σημαίνει πως οι ενέργειές τους στέφονται πάντοτε από επιτυχία. Το γεγονός ότι έχουν στη διάθεσή τους τα πανίσχυρα υπολογιστικά συστήματα του Πανεπιστημίου τους με ελεύθερη και δωρεάν πρόσβαση στο Internet, το ότι γνωρίζουν πολύ καλά το χειρισμό τους καθώς και το ότι διαθέτουν αρκετό ελεύθερο χρόνο, σε συνδυασμό με μια χιουμοριστική διάθεση που είναι ένα από τα βασικά χαρακτηριστικά της ηλικίας τους, τους καθιστά ίσως τους πιο επικίνδυνους hackers. Στις περισσότερες περιπτώσεις βέβαια τα άτομα αυτά κάνουν hacking ορμώμενα από ένα συνδυασμό χιούμορ, περιέργειας και επίδειξης των ικανοτήτων τους στους συνομηλίκους τους. Η αναζήτηση συγκεκριμένων πληροφοριών δεν είναι το ζητούμενο από αυτά. Αυτό που τους «μετράει» ιδιαίτερα είναι αυτή η ίδια η παράνομη είσοδός τους σε ένα σύστημα για την οποία θα μπορούν στη συνέχεια να υπερηφανεύονται στους φίλους τους. Η λήψη των κατάλληλων μέτρων από τον υπεύθυνο ασφαλείας ενός δικτύου μπορεί να αποτρέψει πολλές από τις εισβολές αυτών των hackers για τους οποίους το hacking αποτελεί θα λέγαμε ένα είδος χόμπυ, στο οποίο μάλιστα δεν επιδίδονται και πολύ συχνά. Εξάλλου αυτό που κύρια τους νοιάζει και που τους καθιστά παράλληλα και κάπως ακίνδυνους για τα θύματά τους είναι το γεγονός ότι ενδιαφέρονται για το πως θα σπάσουν τους κωδικούς ενός συστήματος και θα μπουν σ' αυτό χωρίς παράλληλα να τους ενδιαφέρουν και οι πληροφορίες που αυτό διαθέτει. Εξαιρούνται φυσικά οι περιπτώσεις εκείνες όπου το hacking αφορά τα αρχεία με τις βαθμολογίες

[44] http://www.getcited.org/pub/100423921

τους, του εκπαιδευτικού ιδρύματος στο οποίο φοιτούν που όπως είναι φυσικό η "διορθωτική" παρέμβασή τους αποτελεί και τον κύριο στόχο τους .

Για τους υπαλλήλους της επιχείρησης - θύματος.

Εχει διαπιστωθεί ότι οι μεγαλύτερες ζημιές σε συστήματα Η/Υ επιχειρήσεων οφείλονται σε υπαλλήλους τους οι οποίοι είναι υπεύθυνοι για τη λειτουργία τους. Σε πολλές περιπτώσεις υπάλληλοι δυσαρεστημένοι από την απέναντί τους πολιτική της επιχείρησης στην οποία εργάζονται - χαμηλοί μισθοί, παράλειψη από προαγωγές, εύνοια σε συναδέλφους τους κλπ - αντιδρούν καταστρέφοντας αρχεία ή σαμποτάροντας το δίκτυο των Η/Υ της. Οι τρόποι που μεταχειρίζονται γι' αυτό ξεκινούν από το ανοιγοκλείσιμο του ηλεκτρικού ρεύματος στο τμήμα Η/Υ όταν δεν βρίσκεται κανείς άλλος εκεί και φτάνουν μέχρι τις κλοπές και τις διαγραφές αρχείων και την εισαγωγή στο σύστημα καταστρεπτικών ιών. Δεν είναι λίγες όμως και οι περιπτώσεις όπου υπάλληλοι είναι εκείνοι που βοηθούν με την αθέλητη μη λήψη των κατάλληλων μέτρων ασφαλείας, εξωτερικούς εχθρούς της επιχείρησης να αποκτήσουν πρόσβαση σ' αυτό. Μία από τις μεθόδους που χρησιμοποιεί ένας εξωτερικός hacker για να αποκτήσει πρόσβαση σε ένα δίκτυο Η/Υ είναι και η γνωστή σαν «κοινωνική μηχανική» (social engineering) για την οποία θα μιλήσουμε ξεχωριστά παρακάτω. Αντί λοιπόν, να ξοδεύει το χρόνο του προσπαθώντας να βρει τον κωδικό για την είσοδό του στο δίκτυο αυτό προσποιείται πως είναι ένας δυσαρεστημένος χρήστης ή πελάτης και ζητάει από τον υπάλληλο να αλλάξει τον κωδικό του ή να φτιάξει ένα νέο προσωρινό τρόπο εισόδου. Ευκολόπιστοι ή αμελείς υπάλληλοι χαλαρώνουν τα μέτρα ασφαλείας δίνοντας έτσι την ευκαιρία στον hacker να μπει στο δίκτυο αποφεύγοντας με τον τρόπο αυτό τα περίπλοκα συστήματα ασφαλείας που έχουν θεσπισθεί για την προστασία του.

Για τους hackers που κινούνται στον υπόκοσμο των Η/Υ[45].

Στην προκειμένη περίπτωση έχουμε να κάνουμε με την αφρόκρεμα των hackers. Πολλοί από αυτούς είναι αυτοδίδακτοι, δεν έχουν κάνει πανεπιστημιακές σπουδές και βασικά προέρχονται από τους λεγόμενους «phone - phreakers» οι οποίοι στις δεκαετίες του 1960 και του 1970 έσπαζαν κωδικούς τηλεφώνων στις ΗΠΑ με σκοπό βέβαια την αποφυγή της πληρωμής τηλεφωνικών τελών. Απαραίτητη προϋπόθεση για να γίνει κάποιος μέλος της κοινότητάς τους είναι η ικανότητά του να μπαίνει σε δίκτυα την οποία θα πρέπει να αποδείξει με την ανταλλαγή των σχετικών πληροφοριών σε ειδικά συστήματα ηλεκτρονικών συστημάτων ανακοινώσεων, τα γνωστά σαν BBS (Bulletin Board Systems) τα οποία και λόγω της βραχυχρόνιας ύπαρξής τους αλλά και εξαιτίας της καλής προστασίας τους από τον ιδιοκτήτη τους καθιστούν ιδιαίτερα δύσκολη την πρόσβασή τους σε κάθε τρίτο μη μέλος τους. Έτσι λοιπόν, όποιος ενδιαφέρεται να ενταχθεί σε μια κοινότητα hackers θα πρέπει να εντοπίσει μια σχετική BBS και να κερδίσει την εμπιστοσύνη των μελών της αναφέροντας τις περιπτώσεις hacking που έχει κάνει και απαντώντας σε «τεχνικές» ερωτήσεις πάνω σε σχετικά ζητήματα. Τα ζητούμενα ξεκινούν από τον μη καταχωρημένο σε τηλεφωνικό κατάλογο αριθμό τηλεφώνου ενός συστήματος Η/Υ και φτάνουν μέχρι το όνομα του λογαριασμού και τον κωδικό ενός καλά προστατευμένου αρχείου πληροφοριών. Η διαδικασία αυτή εξάλλου δυσκολεύει την πρόσβαση των BBS αυτών από τρίτους και από την αστυνομία. Το μεγαλύτερο επίτευγμα των υποψήφιων μελών είναι η είσοδός τους σε ένα σύστημα υψηλής ασφαλείας και η έξοδός τους από αυτό χωρίς να τους πάρει είδηση κανένας. Κανόνας είναι στην περίπτωση αυτή η μη διαγραφή ή καταστροφή αρχείων.

Η ευρύτατη διάδοση των προσωπικών υπολογιστών τα τελευταία χρόνια, έχει κάνει τις κοινότητες των hackers αυτών λιγότερο ομοιογενείς από ότι ήσαν στο παρελθόν πράγμα που είχε σαν αποτέλεσμα να αλλάξουν και οι λόγοι για τους οποίους κάνει κανείς hacking.

Ενας από τους σκοπούς που επιδιώκει ο σημερινός υπόκοσμος των hackers έχει να κάνει με την άποψη που λέει ότι η κοινωνία θα πρέπει να αλλάξει τη στάση της απέναντι στη σύγχρονη τεχνολογία και να κατανοήσει τους κινδύνους που αυτή περικλείει. Αυτό θα έχει σαν συνέπεια το ότι θα πρέπει να δείξει κανείς τόσο στις επιχειρήσεις όσο και στο κοινό τα προβλήματα που παρουσιάζουν τα συστήματα ασφαλείας των δικτύων Η/Υ που χρησιμοποιούν.

Οι **Crackers** μάλιστα, - που αποτελούν την πιο επικίνδυνη κατηγορία του υπόκοσμου των hackers - πηγαίνουν παραπέρα έχοντας σαν σκοπό τους όχι μόνο την πρόσβαση σ' ένα σύστημα αλλά και την προσωρινή ή μόνιμη αχρήστευσή του στα πλαίσια της επίθεσης που είναι γνωστή σαν "άρνηση παροχής υπηρεσιών" (Denial of service attack) και στην οποία έχουμε ήδη

[45] http://www.getcited.org/pub/100423921

αναφερθεί. Τα άτομα αυτά έχει παρατηρηθεί πως είναι νεαρά αγόρια με ηλικία που ξεκινάει από την εφηβική και φτάνει τα 30 το πολύ χρόνια, μαθαίνουν εύκολα και εγκαταλείπουν συχνά το σχολείο εξαιτίας της υπερβολικής αγάπης τους για ό,τι έχει σχέση με τους Η/Υ. Κατά τη μετεφηβική τους ηλικία καταφέρνουν συνήθως να βρουν μια δουλειά που σχετίζεται με το μεγάλο πάθος τους δηλ. τους Η/Υ, μη προκαλώντας καμμιά υποψία δεδομένου ότι είναι πολύ δύσκολο μέχρι τότε να έχουν ήδη καταδικασθεί για κάποια σχετική παράνομη πράξη. Οι Crackers έχουν μια φοβερή ικανότητα να παραβιάζουν ακόμα και τα περισσότερο περίπλοκα από άποψη ασφαλείας συστήματα. Οι τεράστιες τεχνικές τους γνώσεις σε συνδυασμό με την αφοπλιστική ικανότητά τους να κερδίζουν την εμπιστοσύνη των άλλων τους δίνουν τη δυνατότητα να αποσπάσουν τις απαραίτητες πληροφορίες από τους ανύποπτους υπαλλήλους μιας επιχείρησης, οι οποίες θα τους βοηθήσουν στη συνέχεια να αποκτήσουν εύκολη πρόσβαση στα συστήματά της.

Για τους εγκληματίες από τον κόσμο των ναρκωτικών και του οργανωμένου εγκλήματος.

Κίνητρα για τη χρησιμοποίηση του Internet από τα άτομα αυτά είναι αφενός μεν η ευρύτατη διάδοσή του αφετέρου δε η αδυναμία των διωκτικών αρχών να παρακολουθήσουν εύκολα τα τεκταινόμενα σ' αυτό. Οι επαφές για τη διακίνηση ναρκωτικών αλλά και για την τέλεση και άλλων αξοίποινων πράξεων - όπως π.χ. κυκλοφορία πορνογραφικού υλικού, κυρίως με ανηλίκους - βρίσκουν πρόσφορο έδαφος στον κυβερνοχώρο. Η περαιτέρω δε ενασχόληση των εγκληματικών οργανώσεων με εγκλήματα που τελούνται με τη χρήση Η/Υ καθιστά πιθανούς στόχους τους τις συναλλαγές επιχειρήσεων με τους πελάτες τους. Σαν τέτοιες περιπτώσεις θα μπορούσαν να αναφερθούν π.χ. η υποκλοπή του αριθμού μιας πιστωτικής κάρτας μέσω της οποίας ένας πελάτης πληρώνει την οφειλή του on - line ή η οποιαδήποτε συναλλαγή με μια επιχείρηση - μαϊμού η οποία εισπράττει το οικονομικό αντίτιμο προϊόντων ή υπηρεσιών τις οποίες ουδέποτε παρέχει. Δεν θα πρέπει ακόμη να μας διαφεύγει την προσοχή ότι πίσω από ανύπαρκτες επιχειρήσεις στο Internet μπορεί να κρύβονται και εγκληματικές οργανώσεις που συναλλασσόμενες κάνουν ξέπλυμα βρώμικου χρήματος.

Για τους επαγγελματίες hackers - βιομηχανικούς κατασκόπους.

Η όλο και μεγαλύτερη διείσδυση του Internet στον χώρο του ηλεκτρονικού εμπορίου έχει ανοίξει την όρεξη των επαγγελματιών κλεπτών δεδομένων. Ορισμένοι από αυτούς προέρχονται από τον υπόκοσμο των Η/Υ και οι υπόλοιποι είναι ειδικοί που εργάζονται στους Η/Υ. Τα άτομα αυτά ψάχνουν συνήθως για να βρουν πληροφορίες που θα τα οδηγήσουν στο σπάσιμο των κωδικών ενός συστήματος, με σκοπό να τις πουλήσουν. Άλλες ανάλογες πληροφορίες που θα πέσουν κατά τύχη στα χέρια τους, τις πωλούν σε όποιον τους προσφέρει τα περισσότερα χρήματα. Τα άτομα αυτά πιστεύεται πως στρατολογούνται είτε από κυβερνητικές υπηρεσίες είτε από επιχειρήσεις προκειμένου να κάνουν βιομηχανική κατασκοπεία.

Ενδιαφέρον παρουσιάζει επίσης και η διάκριση των hackers στις ακόλουθες τέσσερες κατηγορίες, την οποία επιχειρούν οι **Rogers και Post**[46]:

- **Old School Hackers:** αυτοί ενδιαφέρονται για τη δημιουργία προγραμμάτων και την ανάλυση συστημάτων, αλλά ό,τι κάνουν δεν αποτελεί - κατά τη γνώμη τους - παράνομη δραστηριότητα. Δεν έχουν κακές προθέσεις, παρότι δεν εκτιμούν ιδιαίτερα την ιδιωτική ζωή των ατόμων αλλά και το απόρρητο των πληροφοριών στον κυβερνοχώρο, επειδή πιστεύουν πως το Διαδίκτυο είναι σχεδιασμένο για να είναι ένα ανοικτό σε όλους σύστημα.
- **Script Kiddies, ή Cyber-Punks:** είναι εκείνοι που τα ΜΜΕ αποκαλούν hackers. Η ηλικία τους κυμαίνεται από τα 12 έως τα 30 χρόνια, είναι συνήθως λευκοί άνδρες και έχουν τελειώσει τουλάχιστον τη μέση εκπαίδευση. Συχνά συλλαμβάνονται από τις αρχές γιατί υπερηφανεύονται δημόσια για τα κατορθώματά τους. Οι γνώσεις τους στην τεχνολογία και στους Η/Υ είναι άριστες και τους αρέσει να εισβάλλουν σε συστήματα με σκοπό να τους προξενήσουν ζημιές, απλά και μόνο γιατί έτσι διασκεδάζουν την ανία τους.
- **Professional Criminals ή Crackers:** αυτοί είναι οι πραγματικοί ψηφιακοί εγκληματίες, εισβάλλοντας σε συστήματα και προξενώντας τους ζημιές, με σκοπό το προσωπικό οικονομικό τους όφελος. Συχνά τα άτομα αυτά κάνουν βιομηχανική ή και στρατιωτική κατασκοπεία. Δεν είναι δε σπάνιες και οι περιπτώσεις που ανήκουν σε εγκληματικές συμμορίες ή τρομοκρατικές ομάδες και οι

[46] http://pipl.com/directory/name/Hacking/Roger

- **Coders and Virus Writers:** γι' αυτούς δεν είναι γνωστά πολλά πράγματα. Πάντως θεωρούν τους εαυτούς τους την ελιτ του είδους τους. Διαθέτουν άριστες γνώσεις προγραμματισμού και γράφουν επιβλαβή προγράμματα τα οποία δεν χρησιμοποιούν οι ίδιοι, αλλά τα πωλούν σε τρίτους.

Εκτός από τις παραπάνω διακρίσεις των hackers αξιοσημείωτη είναι ακόμη και η διάκρισή τους σε δύο μόνο κατηγορίες που κάνει ο Pipkin (2003). Σύμφωνα με αυτόν οι hackers διακρίνονται :

- **στους** εσωτερικούς **(internal hackers)**
- **στους** εξωτερικούς **(external hackers)**

Στους πρώτους κατά τον συγγραφέα ανήκουν αφενός μεν οι δυσαρεστημένοι υπάλληλοι της επιχείρησης - θύματος, αφετέρου δε οι περιστασιακά συνεργαζόμενοι μαζί της. Στους δεύτερους ανήκουν εκείνοι που έχουν το hacking για διασκέδαση (recreational hackers) και οι επαγγελματίες (professional hackers) που έχουν εξειδικευθεί στη με κάθε ηλεκτρονικό μέσο κλοπή πληροφοριών.

Λαμβάνοντας υπόψη τις παραπάνω κατηγορίες των ψηφιακών εγκληματιών διατυπώνουμε την άποψη ότι εφόσον κριτήριο διάκρισης είναι η επιχείρηση/οργανισμός - θύμα, οι hackers που πιθανόν να προσβάλλουν τα συστήματά τους μπορεί να προέρχονται είτε :

- **Από την ίδια (υπάλληλοι, πελάτες, συνεργάτες) και τότε θα μπορούσαμε να τους ονομάσουμε** εσωτερικούς **hackers**
- **Από το εξωτερικό της περιβάλλον (ανταγωνιστές, φοιτητές, επαγγελματίες κλέφτες δεδομένων, βιομηχανικοί κατάσκοποι κλπ) οπότε όπως είναι εύλογο θα μπορούσαμε να τους αποκαλέσουμε** εξωτερικούς **hackers.**

Και για τις δύο αυτές κατηγορίες hackers γίνεται πρόβλεψη στον ελληνικό Π.Κ. Έτσι το ά. 370Γ παρ. 2 αναφέρεται στον **εξωτερικό** hacker ενώ για τον **εσωτερικό** συνάδελφό του γίνεται αναφορά στην παρ. 3 του ά. 370Γ. Αυτός δε ο τελευταίος θεωρείται εκείνος που είναι στην υπηρεσία του κατόχου των στοιχείων (πράγμα που προφανώς υποδηλώνει την ύπαρξη σχέσης εργασίας ή σύμβασης έργου μεταξύ τους) και η πρόσβασή του σε αυτά απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμοδίου υπαλλήλου του.

Θα πρέπει να σημειώσουμε ακόμη πως η **επικινδυνότητα** των hackers εξαρτάται από τα **κίνητρά** τους. Αν τα κίνητρά τους είναι η διασκέδαση ή η επιθυμία τους να αναγνωριστούν στον κύκλο τους ως αυθεντίες στους Η/Υ ή να μάθουν τον τρόπο λειτουργίας του συστήματος μιας επιχείρησης ή ενός οργανισμού, η παράνομη πρόσβασή τους σε αυτό σταματάει μέχρις εκεί και εκείνο που έχει υποστεί βλάβη πραγματικά είναι το ....γόητρο του συστήματος ασφαλείας της συγκεκριμένης επιχείρησης ή οργανισμού. Αν όμως το κίνητρό τους είναι το **προσωπικό οικονομικο όφελος,** το οποίο μπορούν να επιτύχουν βλάπτοντας με οποιοδήποτε τρόπο το σύστημα ή τα αρχεία δεδομένων των θυμάτων τους ή πουλώντας σε τρίτους τις πληροφορίες που απεκόμισαν από αυτά, τότε οι ζημιές αυτών των τελευταίων όπως ήδη έχουμε δει είναι ανυπολόγιστες.

Η σύγχρονη πρακτική θέλει δυστυχώς ένα αρκετά μεγάλο αριθμό από τους σημερινούς hackers να έχει οικονομικά κίνητρα πράγμα που αυτόματα αυξάνει τον επικίνδυνο χαρακτήρα τους.

3.3 ΑΔΥΝΑΜΙΕΣ ΤΟΥ ΔΙΑΔΥΚΤΙΟΥ ΚΑΙ ΜΕΣΑ ΕΠΙΘΕΣΗΣ ΤΩΝ HACKER

Δεδομένου ότι το Διαδίκτυο σαν σύστημα είναι ιδιαίτερα περίπλοκο είναι αδύνατο να μην παρουσιάζει αρκετά προβλήματα που συχνά κάνουν κάθε άλλο παρά εύρυθμη τη λειτουργία του. Αυτό έχει σαν βασική συνέπεια ότι οποιαδήποτε αρχεία ή προγράμματα διακινούνται μέσω αυτού διατρέχουν τον κίνδυνο να φτάσουν σε αποδέκτη ο οποίος δεν έχει δικαίωμα να τα χρησιμοποιήσει.

Ένας από τους κυριότερους λόγους για τους οποίους παρουσιάζονται πολλά προβλήματα ασφάλειας στο Internet είναι η βασική αρχιτεκτονική των πρωτοκόλλων TCP/IP και UDP που χρησιμοποιούνται σε αυτό. Κανένα από αυτά δεν σχεδιαστηκε αρχικά με σκοπό να παράσχει αληθινά ασφαλή επικοινωνιακά μονοπάτια. Έτσι όταν στέλνει κανείς στοιχεία χρησιμοποιώντας το πρωτόκολλο TCP/IP, δεν μπορεί να γνωρίζει ποιους ακριβώς επικοινωνιακούς 'διαύλους' θα ακολουθήσουν αυτά για να φτάσουν στον προορισμό τους. Αν κάποιος hacker καταφέρει να εγκαταστήσει σε κάποιον από τους 'διαύλους' αυτούς ένα πρόγραμμα γνωστό σαν «sniffer», τότε θα μπορέσει να υποκλέψει όλα τα διαβιβαζόμενα με τον τρόπο αυτό στοιχεία.

Ένας ακόμη λόγος για τον οποίο οι hackers έχουν σοβαρές πιθανότητες να επιτυγχάνουν τον στόχο τους είναι αυτή η ίδια η διαμόρφωση ενός συστήματος η οποία κάθε άλλο παρά προϋποθέτει την προληπτική λήψη κάποιων μέτρων ασφαλείας και μάλιστα εκείνων με τα οποία θα ελέγχεται η είσοδος κάποιου από το Internet.

Σε γενικές γραμμές θα μπορούσαμε να εντοπίσουμε τις αδυναμίες των διαφόρων συστημάτων στα εξής :

- Στην ανυπαρξία μέτρων ασφαλείας (π.χ. ύπαρξη firewalls),
- Στην ατελή διαμόρφωση και διαχείρισή τους,
- Σε βασικά προβλήματα ασφάλειας σε σχέση με τα πρωτόκολλα επικοινωνίας (IP, TCP, UDP) που χρησιμοποιούν,
- Σε προβλήματα ασφαλείας σε σχέση με τις υπηρεσίες (WWW, FTP κλπ.) του Internet που χρησιμοποιούν και
- Στο μη ικανοποιητικό service που τους παρέχεται.

Εκτός όμως από τα παραπάνω προβλήματα ασφαλείας που αφορούν τεχνικά καθαρώς ζητήματα, οι αδυναμίες των επιχειρήσεων και των οργανισμών να αντιμετωπίσουν αποτελεσματικά μια εισβολή στα συστήματά τους είναι δυνατό να εντοπισθούν και σε αυτή την ίδια την οργάνωσή τους. Έτσι δεν είναι λίγες οι περιπτώσεις που τους λείπει το εξειδικευμένο προσωπικό ασφαλείας και η διαχείριση των συστημάτων τους έχει ανατεθεί σε μη απόλυτα ειδικούς στα σχετικά θέματα. Παράλληλα η απουσία συγκεκριμένης στρατηγικής για την αντιμετώπιση των επιθέσεων των hackers έχει σαν αποτέλεσμα την χωρίς ιδιαίτερο κόπο επιτυχημένη εισβολή αυτών των τελευταίων στα αφύλακτα συστήματά τους.

Η επιτυχημένη αυτή εισβολή έχει να κάνει και με τα μέσα επίθεσης (hacking attacks) *που χρησιμοποιούν οι hackers.*

Σύμφωνα με τον σχετικό κατάλογο της ***Computer Emergency Response Team (CERT)*** *- ο οποίος είναι ένας μη κυβερνητικός οργανισμός που ιδρύθηκε στις ΗΠΑ το 1988 και εξειδικεύεται σε θέματα ασφάλειας υπολογιστικών συστημάτων και ο οποίος συνεργάζεται με το Πανεπιστήμιο Carnegie Mellon - το υπ' αρθ. ένα μέσο επίθεσης των hackers έχει να κάνει με τη χρήση των λεγομένων* ***sniffers*** *("λαγωνικά"). Το* ***sniffer*** *είναι ένα* μικρό πρόγραμμα το οποίο χωρίς να γίνεται αντιληπτό εισχωρεί σ' ένα σύστημα όπου ψάχνει και αναλύει τα αρχεία του με σκοπό τη συλλογή συγκεκριμένων πληροφοριών τις οποίες διαβιβάζει στη συνέχεια στον χρήστη του.

Ένα ακόμη εξίσου αποτελεσματικό μέσο για hacking σύμφωνα με το CERT, αποτελεί το λεγόμενο **IP Spoofing** (παραπλάνηση IP). Στην περίπτωση αυτή *ο hacker προσπαθεί να αποκτήσει πρόσβαση σε ένα σύστημα προσποιούμενος ότι είναι εγκεκριμένος (authorized) χρήστης του. Αυτό το πετυχαίνει με την παραποίηση των στοιχείων της ηλεκτρονικής του ταυτότητας.*

Τον παραπάνω κατάλογο της CERT (βλ. σχετ. CERT Annual Report 1995), συμπληρώνουν ακόμα τρία μέσα επίθεσης :

- Αυτά που γίνονται στον mail server (sendmail attacks),
- Αυτά που γίνονται μέσω των αρχείων του συστήματος (NFS - Network File System attacks) και
- Αυτά που γίνονται μέσω της Υπηρεσίας Πληροφοριών του Συστήματος (NIS - Network Information Service attacks) *(Pipkin, 2003).*

Εξετάζοντας στη συνέχεια τον τρόπο δράσης (modus operandi) των hackers θα μας δοθεί η ευκαιρία να αναφερθούμε ειδικότερα, στη μέθοδο που ακολουθούν και η οποία σε συνδυασμό με τις παραπάνω αδυναμίες του Internet και τα μέσα που χρησιμοποιούν για τις επιθέσεις τους, τους βοηθάει στην παραβίαση των ηλεκτρονικών απορρήτων του θύματός τους.

3.4 Ο ΤΡΟΠΟΣ ΔΡΑΣΗΣ (MODUS OPERANDI) ΤΩΝ HACKER

Η πρόσβαση ενός hacker στο σύστημα του υποψήφιου θύματός του προϋποθέτει δύο στάδια: ένα **προπαρασκευαστικό και ένα κύριο.** Στο πρώτο ο hacker κάνει όλες εκείνες τις ενέργειες οι οποίες του είναι απαραίτητες για να αποκτήσει πρόσβαση στο σύστημα που τον ενδιαφέρει ενώ στο δεύτερο συλλέγει τις πληροφορίες που αναζητούσε και αποχωρεί από αυτό προσπαθώντας να μην αφήσει ίχνη της εισβολής του, διατηρώντας παράλληλα το «δικαίωμα» της επανεισόδου του.

Έτσι στο *προπαρασκευαστικό στάδιο* ο hacker,

α.- *συγκεντρώνει πληροφορίες* (information gathering) για το σύστημα που επιθυμεί να προσβάλλει και

β.- *προσπαθεί να αποκτήσει πρόσβαση σ' αυτό* «σπάζοντας» τους κωδικούς εισόδου (password cracking), αποκτώντας έτσι τα δικαιώματα (privileges) ενός νόμιμου χρήστη του συστήματος.

Στο *κύριο στάδιο* ο hacker, επιδιώκει την εκπλήρωση των σκοπών για τους οποίους μπήκε παράνομα στο συγκεκριμένο σύστημα και αποχωρεί από αυτό προσπαθώντας να μην αφήσει ίχνη που θα μπορούν να οδηγήσουν στην ανακάλυψη της ταυτότητάς του, ενώ παράλληλα φροντίζει να διατηρήσει το δικαίωμα επανεισόδου του στο σύστημα, όποτε πάλι ο ίδιος το επιθυμήσει.

Για καθένα από τα βήματα αυτά του hacker θα μπορούσαμε να πούμε τα ακόλουθα :

3.4.1 Συλλογή πληροφοριών για το σύστημα.

Το βήμα αυτό αποτελεί ίσως το βασικότερο σκαλοπάτι στην κλίμακα ενός επιτυχημένου hacking. Η ρήση του Francis Bacon[47] ότι **«η πληροφορία αποτελεί δύναμη»** βρίσκει την πλήρη εφαρμογή της στους hackers. Όσα περισσότερα γνωρίζει ένας hacker για ένα σύστημα τόσο περισσότερο αυξάνονται οι πιθανότητες που έχει για να εισβάλλει σ' αυτό χωρίς μάλιστα να γίνει αντιληπτός.

Οι πιθανές ερωτήσεις για τις οποίες οι απαντήσεις που θα πάρει θα αποδειχθούν σημαντικές, έχουν να κάνουν συνήθως τόσο με το ανθρώπινο δυναμικό (διαχειριστές, μηχανικούς, χειριστές, χρήστες) του συστήματος όσο και με το ίδιο το σύστημα (hardware, λειτουργικό που χρησιμοποιεί, ενδεχόμενες ιδιομορφίες του κλπ.). Τις πληροφορίες αυτές ο hacker μπορεί να τις πάρει από :

- ✓ το ίδιο το σύστημα,
- ✓ την επιχείρηση στην οποία αυτό ανήκει,
- ✓ ειδικούς (τεχνικούς, επιστήμονες) των Η/Υ και
- ✓ άλλους συναδέλφους του.

Σχετικά με το ίδιο το σύστημα οι πληροφορίες διακρίνονται σ' εκείνες που μπορεί να πάρει ο hacker προτού εισβάλλει σε αυτό και σε εκείνες που μπορεί να πάρει μετά την εισβολή του. Οι πρώτες πιθανόν να μην είναι ιδιαίτερα σημαντικές γι'αυτόν δεδομένου ότι είτε απευθύνονται γενικότερα στο κοινό είτε περιέχουν ένα μήνυμα με το οποίο δηλώνεται ότι για να προχωρήσει κανείς παρακάτω θα πρέπει να δώσει ένα password, με λίγα λόγια ότι η παραπέρα πρόσβαση αφορά μόνον εξουσιοδοτημένους χρήστες. Εάν ο hacker βρει το password και καταφέρει να διεισδύσει στο σύστημα οι πληροφορίες που μπορεί να πάρει πλέον γι' αυτό είναι δυνατό να αποκαλύπτουν το υλικό του μέρος (hardware), τον τρόπο διαχείρησής του, τα δικαιώματα των νόμιμων χρηστών του κλπ.

Στη δεύτερη αυτή περίπτωση ο hacker θα έχει στη διάθεσή του μια σειρά εντολών για να εξερευνήσει το συγκεκριμένο σύστημα. Θα προσπαθήσει φυσικά η εξερεύνησή του αυτή να μην τραβήξει την προσοχή των υπεύθυνων για την ασφάλειά του. Βασικά όμως εκείνο το οποίο θα κάνει θα είναι να ελέγξει τα μέτρα ασφαλείας του συστήματος, κάτι που θα του καθορίσει αποφασιστικά και την παραπέρα δράση του.

Έχει επανειλλημένα αποδειχθεί ότι είναι πιο εύκολο να αποκτήσει κανείς μία πληροφορία που του χρειάζεται εκμεταλλευόμενος τις γνωριμίες που έχει παρά προσπαθώντας να την κλέψει. Γιατί λοιπόν ένας hacker να προσπαθήσει να κλέψει μια πληροφορία που τον ενδιαφέρει για το σύστημα - στόχο του και να μην την πάρει δημιουργώντας απλά το κατάλληλο φιλικό περιβάλλον με εκείνον που πιθανότατα την κατέχει ; Αυτός ο τελευταίος μπορεί θαυμάσια να είναι - ή να ήταν παλαιότερα - ένας από **τους υπαλλήλους της επιχείρησης - στόχου** που του αρέσει ίσως να μιλάει πολύ τόσο για τα προσωπικά όσο και για τα επαγγελματικά του θέματα. Αν μάλιστα ήταν παλιός υπάλληλος που κατά τη γνώμη του απολύθηκε άδικα, τότε και η διάθεσή του να εκδικηθεί τους τέως εργοδότες του θα διευκολύνει την συνεργασία του με όποιον του υποσχεθεί κάτι τέτοιο. Ο εντοπισμός του προσώπου αυτού από τον hacker και η στα πλαίσια μιας κοινωνικής επαφής απόκτηση της εμπιστοσύνης του - γνωστά στη γλώσσα των hackers σαν **social enginneering (κοινωνική μηχανική)** - μπορεί να αποτελέσει γι' αυτόν μια σημαντικότατη πηγή πληροφόρησης. Το πρόβλημα που υπάρχει στη συγκεκριμένη περίπτωση είναι ότι αρκετοί hackers κάθε άλλο παρά σαν κοινωνικά άτομα θα μπορούσαν να χαρακτηρισθούν, πράγμα που όπως είναι φυσικό τα εμποδίζει αρκετά στις κοινωνικές τους επαφές. Θα πρέπει πάντως να σημειώσουμε πως οι περισσότερες περιπτώσεις χρήσης της μεθόδου του social engineering περνούν απαρατήρητες δεδομένου ότι οι ερωτήσεις που

[47] http://www.iep.utm.edu/bacon/

απευθύνει ο hacker είναι συνήθως αποσπασματικές δεν αφορούν δηλ. όλα τα στοιχεία της λειτουργίας ενός συστήματος, ενώ στη συνέχεια ο ερωτών φροντίζει να εξαφανισθεί. Με τον τρόπο αυτό φυσικά, σπάνια δημιουργεί υποψίες για το άτομό του και τον σκοπό τον οποίο επιδιώκει.

"Κοινωνική μηχανική" μπορεί επίσης να θεωρηθεί ότι γίνεται και μέσω λογισμικού με τη χρήση «Δούρειων ίππων» (Trojan horses). Έτσι μέσω παιχνιδιών που ζητούν από το νόμιμο χρήστη τους κωδικούς ο hacker που παίζει με τον υπάλληλο της επιχείρησης μπορεί να πάρει μια ιδέα και για τους κωδικούς που ενδεχόμενα χρησιμοποιούνται στην εργασία αυτού του τελευταίου!

Δεν είναι λίγες και οι περιπτώσεις που ο hacker προσπαθώντας να μάθει τα μυστικά του συστήματος από το προσωπικό της επιχείρησης - στόχου επιδιώκει με κάποια πρόφαση - π.χ. ότι έρχεται να κάνει συντήρηση από την εταιρεία που έχει εγκαταστήσει το δίκτυο ή ότι είναι υπάλληλος της ηλεκτρικής ή της τηλεφωνικής εταιρείας και ήλθε για να επιδιορθώσει μια βλάβη κλπ. - να περιηγηθεί στους χώρους της, να συζητήσει για τη λειτουργία των διαφόρων μηχανημάτων και ίσως και για να πάρει για ....επιδιόρθωση στο εργαστήριό του κάποιους Η/Υ, όπου βέβαια θα τους «δει» με όλη του την άνεση. Σχετικές οδηγίες για το πως μπορεί να προσληφθεί κανείς σε μια επιχείρηση που κάνει συντήρηση Η/Υ έχουν δοθεί επανειλλημένα από ομάδες συζητήσεων (newsgroups) hackers!

Ο **Κέβιν Μίτνικ**[48] είναι ο πιο πολυσυζητημένος χάκερ του κόσμου. Οι New York Times, τον θεώρησαν ως τον υπ' αριθμόν ένα δημόσιο κίνδυνο στον κυβερνοχώρο. Συνελήφθη και κρατήθηκε προφυλακισμένος τεσσεράμισι χρόνια και έχουν ήδη γραφτεί τέσσερα βιβλία για τη διαδρομή, τη σύλληψη και τη φυλάκισή του. Ζωντανός μύθος, ελεύθερος εδώ και τέσσερα περίπου χρόνια, μιλάει πια ο ίδιος για την προσφιλή του δραστηριότητα - συντασσόμενος αυτή τη φορά με το νόμο.

Στο βιβλίο του **"The art of deception"»,** (βλ. ελλην.μτφρ. "Η τέχνη της απάτης", 2004) που έγραψε μαζί με τον **Ουίλιαμ Σάιμον,** εξηγεί, μέσα από φανταστικές ιστορίες παραβίασης συστημάτων και παράνομης πρόσβασης σε δεδομένα, γιατί τελικά ο αδύναμος κρίκος στην αλυσίδα της ασφάλειας είναι ο ίδιος ο άνθρωπος. Ετσι, αναφέρεται στην έννοια της "κοινωνικής μηχανικής", την οποία προσδιορίζει ως *"την τέχνη της απόσπασης, με ποικίλες μεθόδους, καίριων πληροφοριών από ανθρώπους και της άνομης χρησιμοποίησης τους*." Σε σχέση με την παρανομία, όμως, είναι πολύ σημαντικό να διευκρινίσουμε ότι υπάρχει μια διαβάθμισή της, η οποία αρχίζει από την απλή παραβίαση ενός υπολογιστή, ενός λειτουργικού συστήματος, για τη χαρά της παραβίασης και μόνο, και καταλήγει στην καταστροφή ή τη χρησιμοποίηση δεδομένων για προσωπικό όφελος ή στην πρόκληση μεγάλων καταστροφών των δεδομένων πολλών πληροφοριακών συστημάτων.

Στο βιβλίο των Μίτνικ - Σάιμον, παρουσιάζεται η άποψη ότι οι αδυναμίες των συστημάτων ασφαλείας δεν είναι ό,τι χειρότερο μπορεί να υπάρχει σε μιαν επιχείρηση ή έναν οργανισμό. Το χειρότερο από όλα είναι η αφέλεια του προσωπικού του, το οποίο με ευκολία χειρίζονται οι "κοινωνικοί μηχανικοί"· άνθρωποι πολύ έξυπνοι και με ξεχωριστές τεχνολογικές ικανότητες, οι οποίοι συνδυάζοντας διάφορες πληροφορίες και προσεγγίζοντας φιλικά κάποιους υπαλλήλους, καταφέρνουν να έχουν τα στοιχεία που θα τους επιτρέψουν να «επιτεθούν» στο πληροφοριακό σύστημα που επιθυμούν.

Ο Μίτνικ ξεκινάει από την προσωπική του εμπειρία, για να τονίσει ότι το πρωταρχικό κίνητρο των "χάκερ-κοινωνικών μηχανικών", που δεν επιδιώκουν τον παράνομο πλουτισμό, την εξαπάτηση και την πρόκληση καταστροφών, είναι η περιέργεια και η θέληση για την απόκτηση της πληροφορίας, ως υπέρτατης μορφής δύναμης.

Οι ιστορίες που διαβάζουμε, όμως, μπορούν πραγματικά να μας τρομοκρατήσουν, αφού οι περισσότεροι από μας είμαστε ευεπίφοροι, όπως φαίνεται, στην άσκηση πίεσης από τους "κοινωνικούς μηχανικούς". Η εικόνα που σχηματίζουμε είναι ότι δεν υπάρχει κανένα απολυτα ασφαλές σύστημα, επειδή ακριβώς μεταξύ των μηχανών παρεμβάλλεται ο άνθρωπος, που αισθάνεται φόβο, συμπόνια, μπερδεύεται, βαριέται κ.λπ. Οι συμβουλές, με τις οποίες ο Μίτνικ προσπαθεί να απαλύνει το αίσθημα της καθολικής και γενικευμένης ανασφάλειας που δημιουργούν οι ιστορίες του, ελάχιστα παρηγορούν τον απλό αναγνώστη - αν και είναι προφανώς πολύτιμες για τους υπεύθυνους ασφαλείας των επιχειρήσεων και των οργανισμών.

Τέλος, σημαντικές πληροφορίες από την ίδια την επιχείρηση - στόχο μπορεί να πάρει ο hacker - όσο κι αν αυτό φαίνεται απίθανο - ψάχνοντας στα **....σκουπίδια** της **(dumpster**

[48] http://www.webster.edu/philosophy/~umbaugh/courses/frosh/dairy/mitnick.htm

diving). Είναι συνηθισμένο φαινόμενο πολλές πληροφορίες να πετιούνται στα σκουπίδια με τη μορφή άχρηστων σημειωμάτων που περιέχουν μισοσβησμένους κωδικούς ή αντίγραφα αναφορών για διάφορα εμπιστευτικά ζητήματα που έχουν τυπωθεί σε εκτυπωτή ή αποδείξεων πληρωμής λογαριασμών πιστωτικών καρτών ή αποκομμάτων εφημερίδων και περιοδικών ή εγχειριδίων (manuals) Η/Υ που δεν περιέχουν μόνο οδηγίες για τη χρήση τους αλλά και σημειώσεις που γράφτηκαν στο περιθώριο από τους χρήστες τους κλπ. Οι πληροφορίες που περιλαμβάνονται σε όλα αυτά είναι πολύ πιθανό να αναφέρονται σε χαρακτηριστικά του συστήματος, σε κωδικούς καθώς και σε κάθε είδους ζητήματα λειτουργίας των διαφόρων μηχανημάτων. Η αξία τους για τον hacker μπορεί φυσικά να θεωρηθεί ανυπολόγιστη όπως μπορεί να είναι και οι ζημιές που ίσως προκληθούν στην επιχείρηση από την αμέλεια των υπαλλήλων της να τηρήσουν τους κανόνες ασφαλείας που επιβάλλονται για την συγκεκριμένη περίπτωση.

Οι **δημοσιεύσεις για θέματα ασφάλειας συστημάτων Η/Υ,** που γίνονται σε επιστημονικά περιοδικά, σε πρακτικά συνεδρίων, σε βιβλία, σε sites, σε newsgroups και σε mailing lists από επιστήμονες της πληροφορικής και από ειδικούς του χώρου αυτού αποτελούν μία ακόμη σημαντική πηγή πληροφόρησης για τους hackers. Όσο χρήσιμη είναι η πληροφόρηση αυτή για τους υπεύθυνους ασφαλείας των διαφόρων συστημάτων άλλο τόσο είναι και για τους ίδιους τους hackers. Γνωρίζοντας με τον τρόπο αυτό αυτοί οι τελευταίοι τα μέτρα που παίρνονται για την αντιμετώπισή τους, μπορούν εύκολα να πάρουν τα κατάλληλα αντί - μετρα.

Οι hackers περνούν αρκετό από το χρόνο τους ψάχνοντας να βρουν δικτυακούς τόπους ή ανεξάρτητες BBS με πληροφορίες που τους αφορούν και τις οποίες έχουν με τον τρόπο αυτό θέσει στη διάθεσή τους άλλοι συνάδελφοί τους. Είναι γεγονός πως sites με πληροφορίες και εργαλεία (tools) για hacking αφθονούν στον Παγκόσμιο Ιστό. Η ανεύρεσή τους μάλιστα δεν είναι διόλου δύσκολη παρότι δεν μένουν σταθερά για πολύ χρόνο στην ίδια διεύθυνση. Ακόμα πολλοί hackers συνεργάζονται μεταξύ τους ανταλλάσσοντας πληροφορίες με ηλεκτρονικό ταχυδρομείο (e - mail) ή συνομιλώντας σε ειδικά chat rooms. Βεβαίως και υπάρχει και το επίσημο (!) έντυπο των hackers, το **«2600 : The Hacker Quarterly»,** που κυκλοφορεί από το 1984 - μηνιαία κυκλοφορία 20.000 εντύπων το 1995 - (και σε ηλεκτρονική μορφή **(**http://www.2600.com**)** καθώς και άλλα παρόμοια περιοδικά σε ηλεκτρονική κυρίως, μορφή. Τέλος, οποιοσδήποτε χρήστης Η/Υ μπορεί να βρει εύκολα συλλογές προγραμμάτων για hacking σε CD-ROM που κυκλοφορούν ελεύθερα στο εμπόριο - και στη χώρα μας - και σε προσιτή μάλιστα, τιμή.

3.4.2 Εισβολή στο σύστημα : Σπάσιμο» των κωδικών εισόδου και απόκτηση των δικαιωμάτων ενός νόμιμου χρήστη.

Σχεδόν όλοι οι hackers γνωρίζουν ότι ένα από τα βασικά μυστικά της επιτυχίας τους είναι η αδυναμία των διαφόρων συστημάτων να εμποδίσουν την εισβολή τους σε αυτά. Ένα σύστημα λειτουργεί σωστά από τη στιγμή που ο μηχανισμός αναγνώρισης της ταυτότητας (πιστοποίηση) των νόμιμων χρηστών του είναι αξιόπιστος.

Η μέθοδος που χρησιμοποιείται περισσότερο για την **πιστοποίηση** ενός χρήστη είναι αυτή που στηρίζεται στο **όνομά του (user's ID)** σε συνδυασμό μ' ένα **συνθηματικό/κωδικό εισόδου (password),** τα οποία θα πρέπει να δώσει ο χρήστης προκειμένου να του επιτραπεί η είσοδός του στο σύστημα. Εννοείται ότι και τα δύο θα πρέπει να είναι «γνωστά» σε αυτό για να καταστεί δυνατή η σχετική αναγνώριση. Τα στοιχεία αυτά βρίσκονται συνήθως αποθηκευμένα στο αρχείο **«passwd»** που υπάρχει στο σύστημα, εφόσον αυτό χρησιμοποιεί

Unix, κάτι που ισχύει για τους εξυπηρετητές (servers) των περισσοτέρων συστημάτων που είναι στο Internet. Επιδίωξη του hacker είναι να μάθει τα στοιχεία αυτά. Πώς μπορεί να το πετύχει αυτό ;

Μπορούμε να πούμε πως υπάρχουν οι ακόλουθοι πέντε τρόποι για να μάθει ένας hacker το password (και το Id) που θέλει :

1. Να το μαντέψει,
2. Να διερευνήσει συστηματικά το αρχείο «passwd» με ειδικά προγράμματα για την αποκάλυψη κωδικών (special password guessing programs) που υπάρχουν άφθονα στο Web,
3. Αναλύοντας πρωτόκολλα επικοινωνίας με ειδικά προγράμματα διερεύνησης δικτύων,
4. Απομονώνοντας τα passwords με τη χρήση προγράμμάτων που μένουν στη μνήμη (TSR) του συστήματος ή «Δούρειων Ιππων» και τέλος
5. Με κοινωνική μηχανική (social hacking /enginnering).

Παρενθετικά θα πρέπει να παρατηρήσουμε πως η επιλογή των passwords είναι ένα θέμα πολύ μεγάλης σημασίας για την ασφάλεια ενός συστήματος. *Ασφαλές password είναι*

εκείνο που δεν μπορεί να ανακαλύψει ένας hacker οποιαδήποτε μέθοδο κι αν χρησιμοποιήσει και το οποίο μπορεί να απομνημονευθεί εύκολα. Οι οδηγίες που θα πρέπει να δίνονται στους χρήστες όταν επιλέγουν το Id και το password που θα χρησιμοποιούν για την είσοδό τους στο σύστημα θα πρέπει να τους συνιστούν να αποφεύγουν : · το μικρό τους όνομα ή το επώνυμο και οποιοδήποτε συνδυασμό αυτών των δύο, το παρωνύμιό τους, τα ονόματα των παιδιών τους, των συζύγων τους, των συντρόφων τους, των στενών τους φίλων, των συγγενών τους, ονόματα από μυθιστορήματα, από σειρές της τηλεόρασης ή από γνωστά κινηματογραφικά έργα, ονόματα τοποθεσιών, χωρών, πόλεων, μάρκες αυτοκινήτων κλπ.

αριθμούς τηλεφώνων, ημερομηνίες γέννησης, αριθμούς αυτοκινήτων και άδειας οδήγησης, σειρά αριθμών π.χ. 4,5,6,7,8 κλπ.

λέξεις που βρίσκονται σε λεξικό οποιασδήποτε γλώσσας ή που δεν τις συναντά κανείς στα συνηθισμένα λεξικά,

συνηθισμένες φράσεις ή αρχή παροιμίας,

σειρά γραμμάτων του πληκτρολογίου π.χ. ζ,χ,ψ,ω κλπ.,

ένα μόνο γράμμα ή αριθμό,

λέξεις ή συνθήματα που εκφράζουν τις πολιτικές, αθλητικές κλπ. προτιμήσεις τους ή τα ενδιαφέροντά τους και

κωδικούς που είχαν χρησιμοποιήσει στο παρελθόν.

Οι δυσκολίες που θα συναντήσει ένας hacker, ενδεχόμενα θα είναι αρκετές εάν ο χρήστης :

αλλάζει τον κωδικό του κάθε 2 ή 4 το πολύ μήνες,

χρησιμοποιεί κωδικό αποτελούμενο από μικρά και από κεφαλαία γράμματα ή από διαφορετικά αλφάβητα ή από αριθμούς και ειδικούς χαρακτήρες π.χ. 3,8@$-9,A!#6*,

χρησιμοποιεί σαν κωδικό μια φράση χωρίς διαστήματα π.χ. «φίλοιμουκαληνύχτα»

δεν χρησιμοποιεί κωδικούς με λιγότερους από 8 χαρακτήρες.

Ακόμα όμως και οι πιο δύσκολοι κωδικοί και τα προστατευόμενα με τον ασφαλέστερο τρόπο αρχεία «passwd» ενός συστήματος δεν είναι δυνατό να μην αποκαλυφθούν στον hacker που έχει καταφέρει να εγκαταστήσει σ' αυτό ένα πρόγραμμα sniffer[49], με το οποίο θα έχει τη δυνατότητα να καταγράφει όλα τα πατήματα του πληκτρολογίου του χρήστη.

Ο hacker χρησιμοποιώντας ακόμα ειδικά προγράμματα που περιέχουν καταλόγους με λέξεις (wordlists) - που μπορεί να βρει εύκολα στο Internet - αυξάνει σημαντικά τις πιθανότητες να ανακαλύψει τον κωδικό και το Id που θα του επιτρέψουν να κινηθεί μέσα σε ένα σύστημα αποκτώντας τελικά όλα τα δικαιώματα ενός νόμιμου χρήστη του.

3.4.3 Ο hacker μέσα στο σύστημα.

Από τη στιγμή που ο hacker θα αποκτήσει πρόσβαση στο σύστημα του στόχου του το τι θα κάνει στη συνέχεια εξαρτάται από το σκοπό για τον οποίο έκανε το hacking. Ανεξάρτητα από το ποιο είναι πάντως το βασικό του κίνητρο είναι βέβαιο πως μεταξύ άλλων θα συγκεντρώσει πληροφορίες και για τη λειτουργία του συστήματος αυτού καθώς και ότι θα προσπαθήσει να εκμεταλλευτεί τις δυνατότητές του και γενικότερα τα δικαιώματα που παρέχονται στους νόμιμους χρήστες του. Ολοκληρώνοντας δε την «επίσκεψή» του θα προσπαθήσει να εξαφανίσει τα ίχνη της και παράλληλα να αφήσει «ανοικτή την πόρτα» και για μελλοντικές ανάλογες δραστηριότητες στο ίδιο σύστημα.

Ο hacker λοιπόν, ευρισκόμενος μέσα στο σύστημα του στόχου του θα έχει την ευχέρεια :

- να συγκεντρώσει τις πληροφορίες που τον ενδιαφέρουν,
- να διαστρεβλώσει πληροφορίες που ήδη υπάρχουν εκεί,
- να το χρησιμοποιήσει γενικά όπως ο ίδιος επιθυμεί,
- να εγκαταστήσει σε αυτό κακόβουλα προγράμματα που θα το βλάψουν,
- να εξαφανίσει τα ίχνη της «επίσκεψής» του και
- να δημιουργήσει κερκόπορτες (backdoors) χρήσιμες για ανάλογες μελλοντικές δραστηριότητές του.

Εφόσον ο hacker «επισκέπτεται» ένα σύστημα για να πάρει συγκεκριμένες πληροφορίες, μόλις τις βρεί τις παίρνει και φεύγει. Υπάρχει βέβαια και η πιθανότητα ανάλογες πληροφορίες να εισάγονται περιοδικά στο σύστημα, οπότε στην περίπτωση αυτή το επισκέπτεται σε τακτά χρονικά διαστήματα, προσπαθώντας να μην αφήνει κάθε φορά ίχνη των

[49] http://www.tucows.com/preview/202818

επισκέψεών του αυτών ή έχει εγκαταστήσει σ' αυτό ειδικά προγράμματα (π.χ. Snoopers) τα οποία του επιτρέπουν να παρακολουθεί την κίνηση των δεδομένων. Εφόσον τα αρχεία που τον ενδιαφέρουν δεν έχουν μεγάλη έκταση και εμφανίζονται με τη μορφή απλού κειμένου (text,doc,pdf), η μεταφορά τους στον Η/Υ του, γίνεται καθώς εμφανίζονται στην οθόνη του υπολογιστή του θύματός του και μάλιστα σε ελάχιστο χρόνο. Αν όμως η έκτασή τους είναι μεγάλη τότε η μεταφορά τους θα πρέπει να γίνει είτε μ' ένα πρόγραμμα μεταφοράς αρχείων (FTP ή UUCP) ή ο hacker θα τα στείλει με e - mail στον εαυτό του. Εάν όμως είναι υπάλληλος του θύματος, πράγμα που σημαίνει ότι μπορεί να χειρίζεται και ο ίδιος κάποιον υπολογιστή του, τότε δεν έχει παρά να αντιγράψει τα σχετικά αρχεία σε CD, DVD, Flash Memory Sticks, δισκέτες ή σε οποιοδήποτε άλλο μέσο μεταφοράς αρχείων.

Υπάρχει ενδεχόμενο ένας hacker να θέλει να διαστρεβλώσει το περιεχόμενο πληροφοριών ενός συστήματος με σκοπό να ζημιώσει τις συναλλαγές της επιχείρησης στην οποία αυτό ανήκει. Η επέμβασή του στα σχετικά αρχεία μετά την αναγνώρισή τους μπορεί να είναι καταλυτική και οι ζημιές που θα επέλθουν από τη χρήση εσφαλμένων στοιχείων που θα έχει εισαγάγει σ' αυτά θα είναι σημαντική για το ανύποπτο θύμα του.

Η χρησιμοποίηση των δυνατοτήτων ενός συστήματος από τον ίδιο τον hacker έχει συνήθως να κάνει με την επιθυμία του αφενός μεν να το ελέγξει - έστω και για λίγο - αφετέρου δε να εμποδίσει τη χρήση του από τους νόμιμους χρήστες του. Και στις δύο αυτές περιπτώσεις οι ζημιές του θύματος είναι δεδομένο πως μπορεί να είναι πολύ μεγάλες.

Ανεξάρτητα για ποιο λόγο ένας hacker εισβάλλει σε ένα σύστημα, προκειμένου να επιτύχει τους στόχους του θα χρειασθεί να χρησιμοποιήσει σε πολλές περιπτώσεις, κάποια προγράμματα τα οποία εγκαθιστώμενα σε αυτό θα του προσφέρουν σημαντική βοήθεια. Τέτοια προγράμματα μπορεί να είναι τα εξής :

Spoofs **:** τα οποία είναι προγράμματα που υποδύονται ότι είναι άλλα, κρύβοντας έτσι την πραγματική τους ταυτότητα. Σκοπός τους είναι η συλλογή πληροφοριών. Γενικότερα δε **spoofing** είναι η απόπειρα που κάνει κάποιος να διεισδύσει σε ένα σύστημα προσποιούμενος πως είναι νόμιμος χρήστης του.

Logic bombs: που είναι προγράμματα που παραμένουν ανενεργά στη μνήμη ενός Η/Υ και ενεργοποιούνται είτε σε προκαθορισμένη χρονική στιγμή **(time bombs)** είτε μετά από κάποιο συγκεκριμένο χειρισμό. Σκοπός τους είναι η καταστροφή αρχείων εξαιτίας της οποίας προκαλείται η σταδιακή κατάρρευση ενός συστήματος.

Worms : και σε αυτά έχουμε ήδη αναφερθεί.

Snoopers: τα οποία είναι προγράμματα που παρακολουθούν δεδομένα που διακινούνται μέσα σε ένα σύστημα, ψάχνοντας να βρουν ένα συγκεκριμένο είδος πληροφοριών. Ένα τέτοιο πρόγραμμα μπορεί να εγκατασταθεί στον κεντρικό εξυπηρετητή ενός δικτύου ή στο σκληρό δίσκο ενός Η/Υ και να παρακολουθεί με τον τρόπο αυτό τα δεδομένα που διακινούνται σε αυτά και τέλος

Viruses **:** οι γνωστοί ιοί των Η/Υ για τους οποίους έχει γίνει πολύς λόγος από τότε που εμφανίστηκαν και για τους οποίους ήδη μιλήσαμε.

Ευρισκόμενος ο hacker μέσα στο σύστημα της επιχείρησης - στόχου του επιθυμεί να αφήσει όσο το δυνατό λιγότερα ίχνη από την εκεί παρουσία του. Βασικό του μέλημα λοιπόν είναι να σβήσει όσα περισσότερα από αυτά μπορεί αλλά και όσα απομένουν να τα περιπλέξει με τέτοιο τρόπο έτσι ώστε να μην μπορούν να οδηγήσουν σ' αυτόν. Γνωρίζοντας ότι η αποκάλυψη της ταυτότητάς του θα καταστρέψει το «έργο» του οι προσπάθειές του για την εξάλειψη των ιχνών της παρουσίας του ξεκινούν από τη στιγμή της εισόδου του στο σύστημα και ολοκληρώνονται με την έξοδό του από αυτό.

Τέλος από τη στιγμή που ένας hacker αποκτά τη δυνατότητα πρόσβασης σε ένα σύστημα επιθυμία του είναι να εξακολουθήσει να έχει πρόσβαση στο σύστημα αυτό ακόμα κι αν αποκαλυφθεί η παράνομη είσοδός του. Για να το πετύχει αυτό θα πρέπει να δημιουργήσει τις λεγόμενες *κερκόπορτες (backdoors)* δηλ. εναλλακτικούς τρόπους παράνομης επαναδιείσδυσής του στο σύστημα. Για το λόγο αυτό πολλοί hackers έχουν στη διάθεσή τους τα κατάλληλα προγράμματα με τα οποία θα μπορέσουν να εκμεταλλευτούν τα προβλήματα ασφαλείας του συστήματος και γενικότερα τις ατέλειές του και με τον τρόπο αυτό θα μπορέσουν να ανοίξουν και άλλες διόδους πρόσβασης σ'αυτό.

Ολοκληρώνοντας στο σημείο αυτό την περιγραφή του modus operandi των hackers δεν τρέφουμε την ψευδαίσθηση ότι έχουμε καλύψει τα πάντα γι' αυτό. Η μεθοδολογία του hacking ανανεώνεται καθημερινά και στους κατοίκους του κυβερνοχώρου η φαντασία περισσεύει γιατί είναι απαραίτητο στοιχείο για την επιβίωσή τους μέσα στα όριά του!

ΚΕΦΑΛΑΙΟ 4

ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΓΚΛΗΜΑΤΩΝ

4.1 ΑΝΤΙΜΕΤΩΠΙΖΟΝΤΑΣ ΤΗΝ ΕΙΣΒΟΛΗ

Όσα μέχρι τώρα έχουμε πεί για τους τρόπους δράσης των ψηφιακών εγκληματιών αποτελούν το υπόβαθρο με βάση το οποίο θα πρέπει να δούμε ποια θα είναι η **πολιτική** που θα πρέπει να ακολουθήσει μία επιχείρηση - που είναι και το πλέον συνηθισμένο θύμα, λόγω των αυξημένων οικονομικών της συναλλαγών - προκειμένου να προστατεύσει το σύστημα της από την παραβίασή του.

Η πολιτική αυτή θα πρέπει να χαρακτηρίζεται από τα ακόλουθα:

- Τον προσδιορισμό των κινδύνων που απειλούν την ασφάλεια των δεδομένων του συγκεκριμένου δικτύου,
- Την οριοθέτηση των ευπαθών σημείων του
- Την επισήμανση των αναγκών εκείνων που το χρησιμοποιούν.

Η καταγραφή των παραπάνω θα πρέπει να οδηγήσει στη λήψη συγκεκριμένων μέτρων τα οποία θα πρέπει να στοχεύουν :

- Στην προληπτική προστασία του συστήματος,
- Στη διαπίστωση της εισβολής και
- Στις ενέργειες που θα πρέπει να γίνουν για την αποκατάσταση της «τάξης» στο σύστημα - θύμα (Pipkin, 1997).

Για καθένα από αυτά θα πρέπει να παρατηρήσουμε σε γενικές γραμμές, τα ακόλουθα :

4.1.1 Η ΠΡΟΛΗΠΤΙΚΗ ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ

Με σκοπό την εκ των προτέρων προστασία του συστήματός της μία επιχείρηση οφείλει :

1. - *Να προστατεύσει με κάθε δυνατό μέσο τη διαρροή πληροφοριών σε τρίτους,* οι οποίες αφορούν την ίδια, το σύστημά της, τους χρήστες του καθώς και τα προγράμματα που τρέχουν σ' αυτό. Όπως ήδη έχουμε σημειώσει το μεγαλύτερο και συνάμα σπουδαιότερο όπλο των hackers είναι η πληροφόρηση για ό,τι αφορά τον μελλοντικό τους στόχο.

Έτσι μεταξύ των ζητημάτων που τους ενδιαφέρουν περιλαμβάνεται π.χ. το είδος του συστήματος, τα προγράμματα που τρέχουν σε αυτό, τα ονόματα και οι κωδικοί των χρηστών που το χρησιμοποιούν και φυσικά ό,τιδήποτε έχει σχέση με την επιχείρηση στην οποία αυτό ανήκει. Όλες αυτές οι πληροφορίες θα αποτελέσουν τμήματα του σταυρόλεξου που θα πρέπει να λύσει ο hacker προκειμένου να φτάσει στο στόχο του. Ειδικότερα κάθε είδους πληροφορία - εμπιστευτική ή μη, για το ιδιοκτησιακό καθεστώς ή για το προσωπικό (ονόματα, διευθύνσεις κατοικίας, ημερομηνίες γέννησης, μισθολόγιο) - της επιχείρησης/στόχου μπορεί να αποδειχθεί χρήσιμη για τον hacker, εφόσον του δίνεται η δυνατότητα να την αξιοποιήσει για την εισβολή του. Επομένως θα πρέπει να γίνεται μία εκ των προτέρον κατάταξη και διαβάθμιση των πληροφοριών αυτών που θα έχει να κάνει με την βαρύτητά τους και να λαμβάνονται τα κατάλληλα μέτρα για την αποτροπή της διαρροής τους σε κάθε τρίτο μη εξουσιοδοτημένο πρόσωπο. Είναι ακόμη εύλογο πως πληροφορίες που αφορούν τα ονόματα και τους κωδικούς των χρηστών δεν θα πρέπει να είναι γνωστές σε κανένα άλλο εκτός από τον διαχειριστή του συστήματος. Επίσης θα πρέπει να δοθεί ιδιαίτερη προσοχή σε προγράμματα που με την αρχική σύνδεση δίνουν κάποια από τα χαρακτηριστικά του συστήματος ακόμα και σε μη εξουσιοδοτημένους χρήστες. Γι' αυτά θα πρέπει να γίνει ειδική ρύθμιση έτσι ώστε να πάψουν να λειτουργούν με τον τρόπο αυτό.

2. - *Να περιορίζει την ελεύθερη και χωρίς καμμία διάκριση πρόσβαση στο σύστημά της* ακόμα και από τους ίδιους τους χρήστες της. Αυτό θα το πετύχει επιτρέποντας στους χρήστες - εξωτερικούς ή εσωτερικούς - να το χρησιμοποιούν αποκλειστικά και μόνο μέσα στα πλαίσια των δικαιωμάτων ή των καθηκόντων που τους έχουν ανατεθεί από την ίδια την επιχείρηση. Έτσι ο κάθε χρήστης θα έχει τη δυνατότητα να χρησιμοποιεί το σύστημα μόνο για υπηρεσίες για τις οποίες εκ των προτέρον θα του έχει επιτραπεί η πρόσβαση σε αυτό. Η υπέρβαση των δικαιωμάτων του θα πρέπει να καταγράφεται και στη συνέχεια να του ζητούνται εξηγήσεις γι' αυτή.

3. - *Να στηρίζει τη λειτουργία του σύστηματός της σε σύγχρονο λογισμικό.*

Ο βαθμός ασφαλείας ενός συστήματος εξαρτάται σε μεγάλο βαθμό από το πόσο νέο είναι το λογισμικό που χρησιμοποιείται για τη λειτουργία του. Παλαιά προγράμματα που έχουν ήδη αποδειχθεί ευάλωτα σε επιθέσεις hackers δεν αποτελούν αξιόπιστη λύση, δεδομένου ότι αυτοί οι τελευταίοι γνωρίζουν το πως να εκμεταλλευτούν τις αδυναμίες που είχαν παρουσιάσει στο παρελθόν. Μόνο η εγκατάσταση του πλέον σύγχρονου λογισμικού θα είναι δυνατό να εγγυηθεί σε ικανοποιητικό σημείο την ασφάλεια ενός συστήματος και

4. - *Να διαγράψει από το σύστημα κάθε τι (αρχείο, πρόγραμμα κλπ.) που δεν χρησιμοποιείται*. Ο γενικός κανόνας λέει πως αν κάτι δεν το χρησιμοποιείς πλέον, θα πρέπει να το πετάξεις. Αυτό στην προκειμένη περίπτωση ισχύει για αρχεία,για δεδομένα, για προγράμματα και για λογαριασμούς χρηστών που δεν είναι πλέον ενεργοί. Η διαγραφή όλων αυτών θα δυσκολεύσει τις προσπάθειες των hackers που ενδεχόμενα τα ήξεραν και τα είχαν χρησιμοποιήσει στο παρελθόν. Ιδιαίτερη προσοχή θα πρέπει να δίνεται στους λογαριασμούς των χρηστών. Η γνώση ενός από αυτούς από ένα hacker του δίνει τη δυνατότητα να χρησιμοποιεί το σύστημα για αρκετό χρονικό διάστημα χωρίς να γίνεται αντιληπτός από κανένα.

5. - *Να χρησιμοποιεί ισχυρά και πλήρως ενημερωμένα αντιικά (antivirus) προγράμματα, firewalls και μεθόδους κρυπτογράφησης δεδομένων.*

Τα firewalls (τείχη προστασίας) θα πρέπει να πούμε πως είναι προγράμματα ασφαλείας που βρίσκονται σε κάποιο κόμβο του δικτύου. Σκοπός τους είναι η προστασία των δεδομένων του εξυπηρετητή από κάθε ανεπιθύμητη επέμβαση. Στα μειονεκτηματά τους καταλογίζονται το υψηλό οικονομικό τους κόστος, η δυσκολία να ρυθμιστούν με τρόπο αποτελεσματικό για την εκπλήρωση της αποστολής τους και τέλος το γεγονός ότι η προστασία που παρέχουν είναι εντελώς σχετική. Είναι γνωστό π.χ. πως τα modems είναι ένα σημείο εισόδου στο δίκτυο το οποίο υπερφαλαγγίζει κάθε firewall.

Η μέθοδος της κρυπτογράφησης των δεδομένων όμως μπορεί να δώσει ικανοποιητικά αποτελέσματα εφόσον συνδυασθεί με τη δημιουργία καταλόγου νόμιμων χρηστών, οι οποίοι θα αποκτούν πρόσβαση στο δίκτυο με τη χρήση κωδικών. Η κρυπτογράφηση έρχεται να εξασφαλίσει το απόρρητο των προσωπικών πληροφοριών. Πρόκειται για μια επιστήμη που βασίζεται στα μαθηματικά για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων. Οι μέθοδοι κρυπτογράφησης καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι. Εξασφαλίζουν έτσι το απόρρητο στις ψηφιακές επικοινωνίες αλλά και στην αποθήκευση ευαίσθητων πληροφοριών. Το αρχικό μήνυμα ονομάζεται απλό κείμενο (plaintext), ενώ το ακατάληπτο μήνυμα που προκύπτει από την κρυπτογράφηση του απλού κειμένου ονομάζεται κρυπτογράφημα (ciphertext).

Αποκρυπτογράφηση είναι η ανάκτηση του απλού κειμένου από το κρυπτογράφημα με την εφαρμογή αντίστροφου αλγορίθμου. Η κρυπτογραφημένη επικοινωνία είναι αποτελεσματική, όταν μόνο τα άτομα που συμμετέχουν σε αυτήν μπορούν να ανακτήσουν το περιεχόμενο του αρχικού μηνύματος. Η κρυπτογραφία δεν πρέπει να συγχέεται με την κρυπτανάλυση, που ορίζεται ως η επιστήμη για την ανάλυση και αποκωδικοποίηση κωδικοποιημένων πληροφοριών χωρίς τη χρήση του αντίστροφου αλγορίθμου κρυπτογράφησης.

Ο αλγόριθμος κρυπτογράφησης είναι μια μαθηματική συνάρτηση που χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση πληροφοριών. Όσο αυξάνεται ο βαθμός πολυπλοκότητας του αλγορίθμου, τόσο μειώνεται η πιθανότητα να τον προσπελάσει κάποιος. Ο αλγόριθμος κρυπτογράφησης λειτουργεί σε συνδυασμό με ένα κλειδί (key), για την κρυπτογράφηση του απλού κειμένου. Το ίδιο απλό κείμενο κωδικοποιείται σε διαφορετικά κρυπτογραφήματα όταν χρησιμοποιούνται διαφορετικά κλειδιά.

Προς την κατεύθυνση της πρόληψης επίσης, κινούνται και τα δέκα μέτρα που αναφέρονται στην προστασία των μικρομεσαίων επιχειρήσεων που δραστηριοποιούνται στο Διαδίκτυο και τα οποία παραθέτουμε στη συνέχεια[50] :

1. ***Μείνετε Ενημερωμένοι:*** *Παρακολουθήστε δικτυακούς τόπους με προγράμματα προστασίας και εγγραφείτε σε mailing list που ενημερώνουν μέσω ηλεκτρονικού ταχυδρομείου για τις νέες απειλές. Είναι βασικό να γνωρίζετε τις απειλές πριν διαδοθούν ευρέως. Έτσι μπορείτε να τις αντιμετωπίσετε καλύτερα.*

2. ***Διαλέξτε «δύσκολα» συνθήματα:*** *Τα προγράμματα των χάκερ στο Διαδίκτυο περιλαμβάνουν δεκάδες χιλιάδες πιθανών συνθημάτων. Με αυτά τα προγράμματα, όταν το σύνθημα είναι συνηθισμένο και απλό να βρεθεί οι χάκερ μπορούν να εισβάλουν στα συστήματα των υπολογιστών. Ένα ιδανικό σύνθημα μπορεί να είναι ο συνδυασμός συμβόλων και αριθμών όπως π.χ. το 45#B&90!*

3. ***Αλλάξτε συχνά το σύνθημά σας:*** *Ακόμα και να το βρουν οι χάκερ, εσείς ήδη θα χρησιμοποιείτε ένα καινούργιο.*

4. ***Βεβαιωθείτε ότι έχετε ενημερώσει το πρόγραμμα προστασίας που έχετε:*** *Πολλές εταιρείες λογισμικού προσφέρουν ανανεώσεις και συμπληρώματα στα προγράμματα ασφαλείας που παρέχουν, για να μπορούν*
αυτά να ανταποκρίνονται στις νέες απειλές. Οι μικρές επιχειρήσεις θα πρέπει να ελέγχουν τακτικά το πρόγραμμα ασφαλείας που διαθέτουν και να το ανανεώνουν για να μπορεί να αντιμετωπίζει τις απειλές που εμφανίζονται.

5. ***Προστατέψτε τα συστήματα ηλεκτρονικού ταχυδρομείου που χρησιμοποιεί η επιχείρηση:*** *Διαλέξτε συστήματα e-mail που μπορούν να «μπλοκάρουν» ιούς που μπορεί να περιέχονται σε mail που λαμβάνει μια επιχείρηση. Οι υπάλληλοι της επιχείρησης θα πρέπει να εκπαιδευθούν για να μην ανοίγουν συνημμένα αρχεία (file attachments) από πηγές που δεν γνωρίζουν, και που είναι ο συνηθέστερος τρόπος για να εισέλθει ένας ιός στον υπολογιστή.*

6. ***Τεστάρετε το σύστημα για αδυναμίες:*** *Πραγματοποιήστε τακτικά τεστ για να βρείτε τυχόν αδυναμίες του συστήματος. Αυτά τα τεστ μπορούν να γίνουν τόσο μέσα από το δίκτυο της εταιρείας όσο και με εργαλεία που μπορούν να βρεθούν στο διαδίκτυο. Για παράδειγμα, μπορείτε με ένα πρόγραμμα που «σπάει» συνθήματα να δείτε αν πρέπει να αλλαχθούν τα συνθήματα πρόσβασης των χρηστών της εταιρείας.*

7. ***Εκπαιδεύστε τους υπαλλήλους σας:*** *Οι υπάλληλοι της εταιρείας πρέπει να κατανοήσουν πόσο σημαντικό είναι εταιρικά στοιχεία και πληροφορίες να παραμένουν εμπιστευτικά και κυρίως να μην κυκλοφορούν ευρέως στο Διαδίκτυο.*

8. ***Διατηρείστε τα προγράμματα σας και το λειτουργικό σύστημα ενημερωμένα:*** *Διατηρείστε το λειτουργικό σας σύστημα και τα προγράμματα σας ενημερωμένα και εγκαταστήστε τις τελευταίες ενημερώσεις. Έτσι και το σύστημα θα είναι πιο σταθερό και οι νέες συμπληρώσεις στα προγράμματα ασφαλείας θα λειτουργούν καλύτερα.*

9. ***Αντι-ιϊκά παντού:*** *Όλα τα συστήματα, από φορητούς υπολογιστές μέχρι τους εξυπηρετητές (servers) της επιχείρησης θα πρέπει προστατεύονται από ιούς. Αν έχετε εγκαταστήσει τέτοια προγράμματα βεβαιωθείτε ότι έχουν ρυθμιστεί κατάλληλα. Επίσης βεβαιωθείτε ότι οι υπάλληλοι της εταιρείας δεν έχουν το δικαίωμα να απενεργοποιήσουν αυτά τα συστήματα.*

10. ***Δημιουργείστε Εταιρική Πολιτική Ασφαλείας:*** *Καταγράψτε την πολιτική ασφαλείας της επιχείρησης σας και ανανεώστε την ανά τακτά χρονικά διαστήματα για να περιγράφει και να ανταποκρίνεται καλύτερα σε νέες απειλές που προκύπτουν. Φροντίστε όλοι οι υπάλληλοι να εφαρμόζουν τις αρχές αυτής της πολιτικής."*

[50] http://www.go-online.gr/ebusiness/specials/article.html?article_id=1592

4.1.2 Η ΔΙΑΠΙΣΤΩΣΗ ΤΗΣ ΕΙΣΒΟΛΗΣ

Ασχετα με τα μέτρα που λαμβάνονται για την εκ των προτέρον προστασία ενός συστήματος το σύστημα αυτό δεν είναι σε κάθε περίπτωση άτρωτο. Τα μέτρα αυτά αποτελούν απλώς το πρώτο βήμα που πρέπει να γίνει για την προστασία των δεδομένων που κινούνται σε αυτό. Και αυτό το οποίο τελικά μόνο μπορούν να πετύχουν τα μέτρα αυτά είναι το να **περιορίσουν** τις πιθανότητες προσβολής του συστήματος από ένα hacker, ιδίως δε αν αυτός δεν είναι και ιδιαίτερα έμπειρος.

Είναι εξάλλου κοινός τόπος το γεγονός πως καθημερινά σε ένα σύστημα ανακαλύπτονται και νέα προβλήματα ασφαλείας, πράγμα που απαιτεί τη συνεχή βελτίωση των τρόπων αντιμετώπισής τους. Το γεγονός αυτό καθιστά την προστασία ενός συστήματος μια συνεχή διεργασία με αρχή αλλά χωρίς τέλος. Ο «πόλεμος» ανάμεσα στους επίδοξους hackers και στους διαχειριστές των συστημάτων έχει ημερομηνία έναρξης εκείνη που άρχισε να λειτουργεί το σύστημα και ημερομηνία λήξης εκείνη που το σύστημα αυτό παύει να είναι ενεργό! Ανάμεσα σ' αυτές όμως είναι σημαντική η καταγραφή των ημερομηνιών των «μαχών - εισβολών» που διαδραματίζονται στο συγκεκριμένο σύστημα.

Η **καταγραφή** κάθε απόπειρας - επιτυχημένης ή μη - παράνομης εισόδου ή χρησιμοποίησης του συστήματος μιας επιχείρησης, η διαπίστωση δηλ. της εισβολής που επιχειρείται στα δεδομένα της, αποτελεί το αμέσως μετά τα προληπτικά μέτρα που ήδη αναφέραμε, αναγκαίο για την ασφάλειά της, μέτρο. Χωρίς αυτήν δεν μπορεί να γνωρίζει ούτε ότι δέχθηκε επίθεση ούτε πότε την δέχθηκε και σε τελική ανάλυση θα αγνοεί το ότι το σύστημά της δεν είναι πλέον ασφαλές.

Για να γίνει η καταγραφή αυτή θα πρέπει **να παρακολουθείται σε 24ωρη βάση** η λειτουργία του συστήματος και να σημειώνεται κάθε τι που δεν συμβαίνει συνήθως σε αυτό. Η διαπίστωση μιας ασυνήθιστης λειτουργίας του είναι δυνατό να αποκαλύψει την επίθεση που δέχθηκε το σύστημα από hackers. Ανάλογη παρακολούθηση των χαρακτηριστικών των αρχείων του συστήματος που θα δείξει την οποιαδήποτε αδικαιολόγητη μεταβολή τους μπορεί να οδηγήσει στο ίδιο συμπέρασμα.

Η παρακολούθηση τόσο του συστήματος όσο και των αρχείων του γίνεται με τη χρήση του κατάλληλου κατά περίπτωση λογισμικού για την ανίχνευσή της. Η διαπίστωση δε της συγκεκριμένης εισβολής θα αποδώσει περισσότερο, εφόσον παράλληλα αποκαλυφθούν οι ζημιές που είχε προξενήσει για να καταστεί δυνατή η άμεση αποκατάστασή τους.

4.1.3 Η ΑΠΟΚΑΤΑΣΤΑΣΗ ΤΗΣ ΤΑΞΗΣ ΣΤΟ ΣΥΣΤΗΜΑ - ΘΥΜΑ

Μετά τη διαπίστωση της εισβολής hackers σε ένα σύστημα και της καταμέτρησης των ζημιών που προκλήθηκαν σ' αυτό θα πρέπει να επακολουθήσει μια σειρά ενεργειών οι οποίες θα αποσκοπούν στο να επαναφέρουν τα πράγματα στην πριν από την επίθεση κατάσταση. Οι ενέργειες αυτές θα πρέπει κατά τον Pipkin (1997) να περιλαμβάνουν τα εξής :

- Αποκατάσταση των αρχείων που καταστράφηκαν.
- Επαναλειτουργία του συνόλου των υπηρεσιών του συστήματος προς τους χρήστες του.
- Διάγνωση και επιδιόρθωση του προβλήματος ασφαλείας του συστήματος με σκοπό να αποφευχθεί η επανάληψή του στο μέλλον.
- Προσπάθεια για τον εντοπισμό των hackers για να παραδοθούν στις διωκτικές αρχές με τελικό σκοπό την παραπομπή τους στη δικαιοσύνη.

- Παρουσίαση του περιστατικού στο κοινό με τέτοιο τρόπο ώστε να μην βλάπτεται το καλό όνομα της επιχείρησης - θύματος και
- Ανάλυση των επιμέρους στοιχείων του όλου συμβάντος με την οποία θα διαπιστωθούν τα κενά στην πολιτική της ασφάλειας του συστήματος με προοπτική την απόκτηση εμπειριών οι οποίες θα είναι χρήσιμες για την αντιμετώπιση ανάλογων περιστατικών στο μέλλον.

Ολοκληρώνοντας οφείλουμε να επισημάνουμε πως υπάρχει και ένας μεγάλος αριθμός εφαρμογών λογισμικού που χρησιμοποιούνται σήμερα από τις διάφορες επιχειρήσεις προκειμένου να ελέγξουν την ασφάλεια του δικτύου τους. Στην κατηγορία αυτή ανήκουν μεταξύ άλλων τα προγράμματα SATAN, Pingware, Netprobe κ.ά.

4.2 ΒΑΣΙΚΑ ΣΤΟΙΧΕΙΑ ΓΙΑ ΤΗΝ ΔΙΕΡΕΥΝΗΣΗ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΓΚΛΗΜΑΤΩΝ

Η προληπτική αποτροπή του μεγαλύτερου αριθμού των ψηφιακών εγκλημάτων είναι δύσκολη, ανεξαρτήτως του πόσο λεπτομερειακούς νόμους και πόσο αυστηρούς ελεγκτικούς μηχανισμούς δημιουργεί ένα κράτος ή πόσο προηγμένη τεχνολογία διαθέτει. Πέραν της αναποτελεσματικότητας μίας τέτοιας προσέγγισης, οι ζημίες για τη δημοκρατία, το εμπόριο και την εξέλιξη της τεχνολογίας, θα μπορούσαν να ήταν πολύ μεγάλες. Η αποτελεσματική εξιχνίαση των ψηφιακών εγκλημάτων και η σωστή απόδοση δικαιοσύνης, είναι η καταλληλότερη προσέγγιση και για την αποτροπή τους. Προς αυτήν την κατεύθυνση, οι διωκτικές αρχές είναι επιφορτισμένες με το έργο να προστατέψουν τους φιλόνομους πολίτες, οδηγώντας τους συστηματικούς παραβάτες στη δικαιοσύνη.

Η διερεύνηση των ψηφιακών εγκλημάτων (forensics) αποσκοπεί στην εξασφάλιση και αξιοποίηση ψηφιακών/ηλεκτρονικών αποδεικτικών στοιχείων, με σκοπό να γίνει η μεταγενέστερη επίκλησή τους στην ποινική διακαιοσύνη. Προς την κατεύθυνση αυτήν, απαιτείται:

- Η αναγνώριση των ψηφιακών πειστηρίων,
- Η συλλογή, η ενδελεχής παρατήρηση και η ασφαλής διατήρησή τους,
- Η ανάλυση και προσεκτική επαλήθευσή τους.

Η διερεύνηση των ψηφιακών εγκλημάτων αρχίζει, αφού προηγηθεί καταγγελία για την τέλεσή τους και εκδοθεί ένταλμα εισαγγελικής έρευνας. Ο ειδικός που συνοδεύει τον εισαγγελέα και τους αστυνομικούς, θα πρέπει να αναγνωρίσει τα ψηφιακά αποδεικτικά στοιχεία που βρίσκονται στον υπό έρευνα χώρο, να τα καταγράψει λεπτομερώς επιτόπου, να τα αφαιρέσει από εκεί που βρίσκονταν, προσέχοντας παράλληλα να μην τα αχρηστεύσει ή τα παραποιήσει κάνοντας κάποιο λάθος χειρισμού και να τα συνοδέψει στον τομέα εξέτασης ψηφιακών πειστηρίων για ανάγνωση, εξέταση, αρχειοθέτηση και αξιολόγηση.

Τα ψηφιακά αποδεικτικά στοιχεία βρίσκονται σε αποθηκευτικά μέσα, όπως οι σκληροί δίσκοι, οι δισκέτες, τα CD-ROM και τα DVD, αλλά μπορεί να βρίσκονται και σε λιγότερο προφανή μέσα, όπως compact flash cards, PCMCIA σκληρούς δίσκους, microdrives, USB memory stick κλπ.

Τα δεδομένα των σκληρών δίσκων, ευρισκόμενα σε επανεγγράψιμα μέσα, πρέπει να αντιγραφούν σε άλλους δίσκους και σε καμμία περίπτωση να μη γίνει επανεκκίνηση του υπολογιστή που κατασχέθηκε. Κατά την εκκίνηση, ένας υπολογιστής ενημερώνει διάφορα στοιχεία στα αρχεία του συστήματος και σβήνει διάφορα προσωρινά αρχεία και αυτό μπορεί να οδηγήσει στην καταστροφή αποδεικτικών στοιχείων ή σε ισχυρισμούς, κατά την εκδίκαση της υπόθεσης στο δικαστήριο, περί μεταβολής του περιεχομένου τους.

Η αντιγραφή των δεδομένων ενός σκληρού δίσκου, γίνεται, αφού αφαιρεθεί από τον κατασχεθέντα υπολογιστή και τοποθετηθεί σε άλλο υπολογιστή, για τη δημιουργία πιστού αντιγράφου του.

Για την ανάγνωση των δεδομένων από το αντίγραφο του δίσκου, χρησιμοποιούνται προγράμματα όπως το Forensic Toolkit Explorer, που επιτρέπει να διαβαστεί το αντίγραφο ενός δίσκου και να βρεθούν συγκεκριμένα αρχεία, αλλά και να επαναφερθούν σβησμένα αρχεία. Για την αποφυγή γραψίματος σε δίσκους υπό εξέταση, υπάρχουν συσκευές που εξουδετερώνουν κάθε προσπάθεια του συστήματος να γράψει στη συσκευή. Πέραν των λύσεων hardware όμως, υπάρχει η δυνατότητα χρήσης λογισμικού, για το κλείδωμα των εγγραφών στους δίσκους. Το ψάξιμο για στοιχεία στο δίσκο με τη χρήση linux, χρησιμοποιεί πάμπολλες εντολές και μικρά προγράμματα ή scripts, που δέχονται regular expressions, προσφέροντας εξαιρετικές δυνατότητες εντοπισμού στοιχείων, αρχειοθέτησης των ευρημάτων και καταγραφής όλων των βημάτων της έρευνας[51].

[51] Kevin Mandia - Chris Prosise, Άμεση Δράση - Η έρευνα του ηλεκτρονικού εγκλήματος, 2002

ΚΕΦΑΛΑΙΟ 5

ΝΟΜΟΘΕΣΙΑ

5.1 ΕΙΣΑΓΩΓΗ

Οι νομοθετικές ρυθμίσεις που αφορούν τα ψηφιακά εγκλήματα παρουσιάζουν αδυναμίες, τόσο στην Ελλάδα όσο και σε άλλες χώρες. Με δεδομένο ότι η ψηφιακή εγκληματικότητα αποτελεί δραστηριότητα αρκετά εξειδικευμένη και ανεπτυγμένη τεχνολογικά, παρουσιάζει προβλήματα στην οριοθέτηση των πράξεων που θα πρέπει να διώκονται ποινικά. Επιπλέον ο νομοθέτης είναι αναγκασμένος να ενημερώνεται συνεχώς για τις εξελίξεις στον τομέα της τεχνολογίας των υπολογιστών, προκειμένου να εξοικειωθεί με τον τρόπο διάπραξης των σχετικών αξιόποινων πράξεων.

Οι διώξεις των ψηφιακών εγκλημάτων κινούνται σε χαμηλά επίπεδα, εφόσον και οι καταγγελίες είναι περιορισμένες. Γενικά, θα πρέπει να παρατηρήσουμε πως οι επιχειρήσεις - κυρίως - αποφεύγουν να καταγγείλουν παραβάσεις, γιατί φοβούνται επανάληψη των αδικημάτων και πλήγμα στη φήμη τους. Επίσης, θέλουν να αποφεύγουν τα υψηλά δικαστικά έξοδα και το γεγονός ότι δεν γίνεται εύκολη χρηματική και αξιακή αποτίμηση των οικονομικών ζημιών που τελικά υφίστανται. Οι δυσκολίες που αντιμετωπίζουν οι αστυνομικές και οι δικαστικές αρχές στον εντοπισμό και την περαιτέρω δίωξη, σχετίζονται, κυρίως, με το συνήθως, χαμηλό επίπεδο πληροφορικής κατάρτισης των στελεχών τους.

Επίσης απαιτείται συνήθως αρκετός χρόνος, για να διευκρινιστούν οι υποθέσεις, που είναι συνήθως πολύπλοκες και απαιτούν συνεργασία και με άλλες υπηρεσίες. Πολλές φορές οι δικαστές υποβαθμίζουν τη σημασία των ψηφιακών εγκλημάτων, με τη δικαιολογία ότι το σύστημα της ποινικής δικαιοσύνης δεν θα πρέπει να επιβαρυνθεί με τέτοιου είδους εγκληματίες, εφόσον η ποινή που τους επιβάλλεται, δεν είναι ικανή να τους αποτρέψει από την επανάληψη της πράξης.

Ο διεθνής εξάλλου χαρακτήρας του συγκεκριμένων εγκλημάτων δίνει τη δυνατότητα στους δράστες να έχουν γρήγορη πρόσβαση στα στοιχεία, αλλά και εύκολη προσβολή των δεδομένων στα συστήματα Η/Υ παγκοσμίως. Βασικό στοιχείο που εμποδίζει την διωκτική προσπάθεια είναι η διασύνδεση των πιο επικίνδυνων από τους ψηφιακούς εγκληματίες με το οργανωμένο έγκλημα. Θα πρέπει επιπρόσθετα να σημειώσουμε πως τα ψηφιακά εγκλήματα διακρίνονται και για: το μεγάλο όγκο των δεδομένων τους, τον μη οπτικό χαρακτήρα των αποδείξεων, τη δυνατότητα «μεταμφίεσης» τους καθώς και την ταχεία εξαφάνιση των αποδεικτικών στοιχείων από τη μεριά των εγκληματιών.

Ο τεράστιος αριθμός δεδομένων που είναι καταχωρημένα στο Διαδίκτυο και η παγκοσμιότητά του αποτελούν εμπόδιο στην αντιμετώπιση αξιόποινων πράξεων που διαπράττονται σε αυτό. Επιπλέον, υπάρχει το πρόβλημα της δικαιοδοσίας, αφού ο καθένας όπου και αν βρίσκεται μπορεί να έχει πρόσβαση σε οποιαδήποτε πληροφορία θελήσει. Είναι δύσκολο να ορισθεί ο τόπος τέλεσης του αδικήματος και η αρμοδιότητα του δικαστηρίου που θα πρέπει να εκδικάσει την υπόθεση. Στην Ελλάδα και την Ευρώπη κυριαρχεί η θεωρία του βαρύνοντος τόπου, δηλαδή ο τόπος του αδικήματος εντοπίζεται στο κράτος που εκδηλώθηκε το έγκλημα. Και σε αυτό όμως, παρουσιάζονται προβλήματα, εφόσον είναι δύσκολο να καθοριστεί ο τόπος τέλεσης ενός διαδικτυακού αδικήματος.

Με δεδομένη όμως, την αύξηση των μορφών των ψηφιακών εγκλημάτων η ειδική και εξειδικευμένη νομοθετική αντιμετώπισή τους θεωρείται επιβεβλημένη. Για το λόγο αυτό σχεδόν όλα τα κράτη του κόσμου έχουν θεσπίσει νομοθετικές διατάξεις, σχετικές με τα ψηφιακά εγκλήματα. Ωστόσο, το νομοθετικό πλαίσιο που να αφορά ειδικότερα το ζήτημα είναι σε αρκετές περιπτώσεις εξαιρετικά ελλιπές και συνήθως καλύπτεται από γενικότερες διατάξεις.

5.2 ΕΛΛΗΝΙΚΗ ΝΟΜΟΘΕΣΙΑ

5.2.1 ΠΕΡΙΛΗΠΤΙΚΑ

Στην Ελλάδα δεν υπάρχει νόμος που να αναφέρεται *αποκλειστικά* σε θέματα Internet και ειδικότερα να ρυθμίζει τη συμπεριφορά των χρηστών του διαδικτύου από την πλευρά του ποινικού δικαίου. Ο νόμος **1805/1988** αφορά εγκλήματα που διαπράττονται γενικά με ηλεκτρονικούς υπολογιστές. Συγκεκριμένα: Με το άρθρο 3 του νόμου αυτού προσετέθησαν τρία νέα άρθρα στον Ποινικό Κώδικα, τα ***370Β, 370Γ και 386Α.*** *Σύμφωνα με το* ***370Β*** *του Ποινικού Κώδικα,* "..όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα ηλεκτρονικών υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι. 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. Αν πρόκειται για στρατιωτικό ή διπλωματικό απόρρητο ή για απόρρητο που αναφέρεται στην ασφάλεια του κράτους, η κατά τα ανωτέρω πράξη τιμωρείται με κάθειρξη μέχρι δέκα ετών".

Σύμφωνα με το άρθρο ***370Γ παρ. 1*** *του Ποινικού Κώδικα,* "όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα ηλεκτρονικών υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μηνών και με χρηματική ποινή εκατό χιλιάδων έως δύο εκατομμυρίων δραχμών. (293,47 και 5869,41 Ευρώ αντίστοιχα) "

Σύμφωνα με τα άρθρα ***386 και 386Α*** *του Ποινικού* μας Κώδικα, "όποιος με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον 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 άλλον τρόπο, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών, και αν η ζημία που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον δύο ετών. Επιβάλλεται δε κάθειρξη μέχρι δέκα ετών, αν ο υπαίτιος διαπράττει απάτες (κατά τον ανωτέρω τρόπο) κατ' επάγγελμα ή κατά συνήθεια και το συνολικό όφελος ή η συνολική ζημία υπερβαίνουν το ποσόν των πέντε εκατομμυρίων (5.000.000) δραχμών, ή, εάν ανεξαρτήτως της κατ' επάγγελμα ή κατά συνήθεια τέλεσης η προξενηθείσα ζημία υπερβαίνει συνολικά το ποσόν των εικοσιπέντε εκατομμυρίων (25.000.000) δραχμών."

Σύμφωνα με το άρθρο **13στ** του Ποινικού Κώδικα, κατ' επάγγελμα τέλεση του εγκλήματος συντρέχει, όταν από την επανειλημμένη τέλεση της πράξης ή από την υποδομή που έχει διαμορφώσει ο δράστης με πρόθεση επανειλημμένης τέλεσης της πράξης προκύπτει ο σκοπός του για πορισμό εισοδήματος. Κατά συνήθεια τέλεση του εγκλήματος συντρέχει κατά το ανωτέρω άρθρο του Ποινικού Κώδικα, όταν από την επανειλημμένη τέλεση της πράξης προκύπτει σταθερή ροπή του δράστη προς τη διάπραξη του συγκεκριμένου εγκλήματος ως στοιχείο της προσωπικότητάς του.

Για τα εγκλήματα κατά της ηθικής και της αξιοπρέπειας, την προστασία των ανηλίκων από τη διάδοση πορνογραφικού υλικού και γενικότερα τη δυσφήμιση μέσω Διαδικτύου στην Ελλάδα ισχύουν τα άρθρα **361, 362, 366 και 367** του Ποινικού Κώδικα.

Για την προστασία της πνευματικής ιδιοκτησίας ισχύει ο **Ν. 2121/1993** με τίτλο *«Πνευματική ιδιοκτησία, συγγενικά δικαιώματα και πολιτιστικά θέματα».* Με το νόμο αυτό ρυθμίζονται θέματα σχετικά με το δίκαιο της πνευματικής ιδιοκτησίας, το σήμα, τη λειτουργία του, τον τρόπο κτήσης του δικαιώματος, την απολυτότητα του δικαιώματος, τον χρονικό περιορισμό του, τον φορέα του.

Επίσης, ισχύει το άρθρο ***14 του Ν. 2672/1998*** *(*Διακίνηση εγγράφων με ηλεκτρονικά μέσα) *καθώς και ο* ***Ν. 2472/1997*** (Προστασία του ατόμου από τη επεξεργασία δεδομένων προσωπικού χαρακτήρα).

Τέλος, σχετικά με το spamming (αποστολή ανεπιθύμητων διαφημιστικών e-mail) στη χώρα μας ισχύει η νομοθεσία η οποία αναφέρεται στην προστασία των καταναλωτών.

5.2.2 ΝΟΜΟΣ 1805/1988

Με τον νόμο 1805/1988 του συντάγματος επαναπροσδιορίζεται η έννοια του «εγγράφου».Πλεον σαν έγγραφο θεωρείται και κάθε μέσο που χρησιμοποιείται απο υπολογιστή η περιφεριακή μνήμη υπολογιστη με ηλεκτρονικό ή άλλο τρόπο για εγγραφή, αποθήκευση παραγωγή ή αναπαραγωγή στοιχείων.Έτσι λοιπόν σαν αποδεικτικά στοιχεία μπορούν να χρησιμοποιηθούν οποιοδήποτε έγγραφα σε ψηφιακή μορφή που έχουν την δυνατότητα να αποδείξουν γεγονότα που έχουν έννομη σημασία.

Επίσης οριοθετούνται και οι ποινές που επιβάλονται, έτσι λοιπόν σύμφωνα με το άρθρο 370 Β του ποινικού κώδικα έχουμε φυλάκιση έως τρείς μήνες για όποιον αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή παραβιάζει στοιχεία ή προγράμματα υπολογιστώνπου συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή του ιδιωτικού τομέα όμως αν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων καθως και αν το απόρρητο έγγραφο που διέρευσε είναι μεγάλης οικονομικής σημασίας τότε επιβάλλεται φυλάκιση τουλάχιστον ενός έτους.Πάράλληλα με το άρθρο 370/Γ μέχρι έξι μήνες φυλάκιση και με χρηματικό πρόστιμο απο 300 έως 3000 ευρώ αντιμετωπίζει όποιος χωρίς δικαίωμα αντιγράφει και χρησιμοποιεί προγράμματα υπολογιστών, μέχρι 30 εύρω ή 3 μήνες φυλάκιση αντιμετωπίζει όποιος όπιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστη ή σε περιφερειακή μνήμη ή μεταδίδονται με συστήματα τηλεποικοινωνιών εφόσων οι πράξεις αυτές έγιναν χωρίς δικαίωμα.Τέλος μετά το άρθρο 386 του ποινικού κώδικα προστίθεται νέο άρθρο που λαμβάνει τον αριθμό 386Α όποιος με σκοπό να διοχετεύση στον εαυτό του ή σε άλλον παράνομο περουσιακό όφελος έιτε με παραποίηση των στοιχείων του υπολογιστή είτε με την μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατα την εφαρμογή του τημωρείται με τις ίδιες ποινες που προβλέπονται στο άρθρο 370 Γ αδιαφορώντας αν οι παθόντες είναι ένα η περισσότερα πρόσωπα.

5.2.3 ΝΟΜΟΣ 2121/1993

Σύμφωνα με τον Ν. 2121/93 , οι όροι χρήσης δεν είναι κενοί νομικής δεσμευτικότητας, σύμφωνα με το ελληνικό δίκαιο. Συμφωνα με το **άρθρο 66Β** το οποίο προστέθηκε στο νόμο το έτος 2002, ως ενσωμάτωση κοινοτικού δικαίου ("Πληροφορίες για το καθεστώς των δικαιωμάτων"):

1. Ως "πληροφορία για το καθεστώς των δικαιωμάτων" νοείται κάθε παρεχόμενη από τον δικαιούχο πληροφορία, η οποία επιτρέπει την αναγνώριση του έργου ή άλλου προστατευόμενου αντικειμένου με συγγενικό δικαίωμα ή με το δικαίωμα ειδικής φύσης του κατασκευαστή βάσης δεδομένων, καθώς και την αναγνώριση του δημιουργού ή οποιουδήποτε άλλου δικαιούχου. Νοούνται επίσης οι πληροφορίες σχετικές με τους όρους και τις προϋποθέσεις χρήσης του έργου ή άλλων προστατευόμενων αντικειμένων, καθώς και κάθε αριθμός ή κωδικός που αντιπροσωπεύει τις πληροφορίες αυτές. (άρθρο 7 παρ. 2 Οδηγίας 2001/29).

2. Απαγορεύεται σε κάθε πρόσωπο να προβαίνει εν γνώσει του χωρίς την άδεια του δικαιούχου σε οποιαδήποτε από τις ακόλουθες ενέργειες:

α) αφαίρεση ή αλλοίωση οποιασδήποτε πληροφορίας με ηλεκτρονική μορφή σχετικά με τη διαχείριση των δικαιωμάτων,

β) διανομή, εισαγωγή προς διανομή, ραδιοτηλεοπτική μετάδοση, παρουσίαση στο κοινό ή διάθεση στο κοινό έργων ή άλλων προστατευόμενων αντικειμένων με συγγενικό δικαίωμα ή με το δικαίωμα ειδικής φύσης του κατασκευαστή βάσης δεδομένων, από τα οποία έχουν αφαιρεθεί ή αλλοιωθεί άνευ αδείας οι πληροφορίες ηλεκτρονικής μορφής σχετικά με τη διαχείριση των δικαιωμάτων, αν το πρόσωπο αυτό γνωρίζει ή έχει βάσιμο λόγο να γνωρίζει ότι με την ενέργεια αυτή προτρέπει, επιτρέπει, διευκολύνει ή συγκαλύπτει προσβολή του δικαιώματος του δημιουργού ή των συγγενικών δικαιωμάτων ή του δικαιώματος ειδικής φύσης του κατασκευαστή βάσης δεδομένων. (άρθρο 7 παρ. 1 Οδηγίας 2001/29)

3. Η παράβαση των ανωτέρω διατάξεων τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή 2.900 -15.000 ευρώ και συνεπάγεται τις αστικές κυρώσεις του άρθρου 65 του Ν. 2121/1993, όπως ισχύει. Το Μονομελές Πρωτοδικείο μπορεί να διατάξει ασφαλιστικά μέτρα σύμφωνα με τον Κ.Πολ.Δ., εφαρμοζομένης και της ρύθμισης του άρθρου 64 του Ν. 2121/1993, όπως ισχύει. (άρθρο 7 Οδηγίας 2001/29).

Ο νόμος λοιπόν προστατεύει τους όρους χρήσης ως αναπόσπαστο στοιχείο του ίδιου του έργου που προστατεύεται με την έννοια ότι απαγορεύεται η αφαίρεσή τους από τρίτον, αλλά και η διάθεση στο κοινό αυτών των έργων με σκόπιμη αφαίρεση των όρων χρήσης, προκειμένου να διευκολυνθεί η προσβολή των δικαιωμάτων.

Επισης, αναδημοσίευση κειμένων χωρίς άδεια: ποινικές κυρώσεις
Η νομική προστασία σε αυτές τις περιπτώσεις, ολοκληρώνεται με το ποινικό μέρος μιας υπόθεσης. Ο νόμος 2121 προβλέπει σοβαρές ποινές για όσους προσβάλλουν την πνευματική ιδιοκτησία.

Ποιό αναλυτικά με το **άρθρο 66** έχουμε :

1. Τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή 2.900 -15.000 ευρώ όποιος χωρίς δικαίωμα και κατά παράβαση των διατάξεων του παρόντος νόμου ή διατάξεων των κυρωμένων με νόμο πολυμερών διεθνών συμβάσεων για την προστασία της πνευματικής ιδιοκτησίας εγγράφει έργα ή αντίτυπα, αναπαράγει αυτά άμεσα ή έμμεσα, προσωρινά ή μόνιμα, με οποιαδήποτε μορφή, εν όλω ή εν μέρει, μεταφράζει, διασκευάζει, προσαρμόζει ή μετατρέπει αυτά, προβαίνει σε διανομή αυτών στο κοινό με πώληση ή με άλλους τρόπους ή κατέχει με σκοπό διανομής, εκμισθώνει, εκτελεί δημόσια, μεταδίδει ραδιοτηλεοπτικά κατά οποιονδήποτε τρόπο, παρουσιάζει στο κοινό έργα ή αντίτυπα με οποιονδήποτε τρόπο, εισάγει αντίτυπα του έργου που παρήχθησαν παράνομα στο εξωτερικό χωρίς τη συναίνεση του δημιουργού και γενικά εκμεταλλεύεται έργα, αντίγραφα ή αντίτυπα που είναι αντικείμενο πνευματικής ιδιοκτησίας ή προσβάλλει το ηθικό δικαίωμα του πνευματικού δημιουργού να αποφασίζει για τη δημοσίευση του έργου στο κοινό, καθώς και να παρουσιάζει αυτό αναλλοίωτο χωρίς προσθήκες.
2. Αν το όφελος που επιδιώχθηκε ή η ζημία που απειλήθηκε από τις πράξεις των παρ. 1 και 2 είναι ιδιαίτερα μεγάλα, επιβάλλεται φυλάκιση τουλάχιστο δύο ετών και χρηματική ποινή 2 έως 10 εκατομμυρίων δραχμών. Αν ο υπαίτιος τελεί τις παραπάνω πράξεις κατ' επάγγελμα ή αν οι περιστάσεις κάτω από τις οποίες έγινε η πράξη μαρτυρούν ότι ο υπαίτιος είναι ιδιαίτερα επικίνδυνος για την προστασία της πνευματικής ιδιοκτησίας ή των συγγενικών δικαιωμάτων, επιβάλλεται κάθειρξη μέχρι 10 ετών και χρηματική ποινή 5 έως 20 εκατομμυρίων δραχμών, καθώς και αφαίρεση της άδειας λειτουργίας της επιχείρησης στα πλαίσια της οποίας εκτελέσθηκε η πράξη. Θεωρείται ότι η πράξη έχει τελεσθεί κατ' επάγγελμα και όταν ο δράστης έχει καταδικασθεί για αδικήματα του παρόντος άρθρου ή για παράβαση των διατάξεων περί πνευματικής ιδιοκτησίας που ίσχυαν πριν απ' αυτό με αμετάκλητη απόφαση σε ποινή στερητική της ελευθερίας. Η προσβολή της πνευματικής ιδιοκτησίας και των συγγενικών δικαιωμάτων σε μορφή κακουργήματος εκδικάζεται από το αρμόδιο Τριμελές Εφετείο Κακουργημάτων.
3. Σε περίπτωση μετατροπής της στερητικής της ελευθερίας ποινής το ποσό της μετατροπής ορίζεται στο δεκαπλάσιο των ορίων του ποσού της μετατροπής που προβλέπονται κάθε φορά στον Ποινικό Κώδικα.
4. Αν συντρέχουν ελαφρυντικές περιστάσεις, η χρηματική ποινή δεν μπορεί να μειωθεί κάτω από το ήμισυ του ελάχιστου ορίου που προβλέπεται κατά περίπτωση στον παρόντα νόμο.
5. Σε κάθε περίπτωση το δικαστήριο μπορεί να διατάζει δημοσίευση περίληψης της καταδικαστικής απόφασης με δαπάνη εκείνου που καταδικάστηκε.
Παρατηρείται ότι οι κυρώσεις που επιφυλάσσει ο ποινικός νομοθέτης είναι βαρύτατες. Ειδικά η κατ' επάγγελμα προσβολή της πνευματικής ιδιοκτησίας αποτελεί κακουργηματική μορφή τέλεσης του εγκλήματος.

Αναδημοσιεύσεις κειμένων χωρίς άδεια: οι αποζημιώσεις.
Η αναδημοσίευση κειμένου, χωρίς άδεια, επιτρέπεται μόνο σε τρεις περιπτώσεις:

1. Το κείμενο αποτελεί απλή αναπαραγωγή είδησης ή ενός γεγονότος ή συνίσταται σε παράθεση απλών στοιχείων (οπότε δεν θεωρείται «έργο» κατά τη νομοθεσία).
2. Η αναδημοσίευση περιορίζεται σε παράθεση σύντομων αποσπασμάτων για την υποστήριξη γνώμης ή άσκηση κριτικής, εφόσον η έκταση των αποσπασμάτων

δικαιολογείται από τον επιδιωκόμενο σκοπό και εφόσον συνοδεύεται πάντοτε από την ένδειξη της πηγής και του ονόματος του δημιουργού.

3. Για λόγους ενημέρωσης επί επίκαιρων γεγονότων επιτρέπεται αναδημοσίευση πολιτικών λόγων, προσφωνήσεων, κηρυγμάτων, δικανικών αγορεύσεων ή άλλων έργων παρόμοιας φύσης.

Σε όλες τις άλλες περιπτώσεις, αναδημοσίευση χωρίς άδεια του δημιουργού απαγορεύεται. Και επειδή καμία απαγόρευση δεν θεωρείται ολοκληρωμένη χωρίς έννομες συνέπειες, ας δούμε σήμερα πως εξισορροπεί το δίκαιο τη διαφορά που προκύπτει από αυτές τις παραβάσεις.

Σε πρώτη φάση, εξετάζω την αστική προστασία, αξιώσεις αποζημίωσης ή χρηματικής ικανοποίησης λόγω ηθικής βλάβης.

Διαβάζουμε στο άρθρο 65 του Ν.2121/1993:

1. Σε κάθε περίπτωση προσβολής της πνευματικής ιδιοκτησίας ο δημιουργός μπορεί να αξιώσει την αναγνώριση του δικαιώματός του, την άρση της προσβολής και την παράλειψή της στο μέλλον.

2. Οποιος υπαιτίως προσέβαλε την πνευματική ιδιοκτησία άλλου υποχρεούται σε αποζημίωση και ικανοποίηση της ηθικής βλάβης. Η αποζημίωση δεν μπορεί να είναι κατώτερη από το διπλάσιο της αμοιβής που συνήθως ή κατά νόμο καταβάλλεται για το είδος της εκμετάλλευσης που έκανε χωρίς την άδεια ο υπόχρεος.

3. Το δικαστήριο καταδικάζοντας σε παράλειψη πράξης απειλεί για κάθε παράβαση χρηματική ποινή τριακοσίων χιλιάδων έως ενός εκατομμυρίου δραχμών υπέρ του δημιουργού ή του δικαιούχου συγγενικού δικαιώματος προβλεπομένου στα άρθρα 46 έως 48 και 51 του παρόντος νόμου καθώς και προσωπική κράτηση έως ένα έτος.

Παρατηρούμε δηλαδή ότι αν ένα έντυπο, χωρίς άδεια, δημοσίευσε ένα κείμενό σας, για το οποίο θα πλήρωνε τον columnist του -για κείμενο αντίστοιχης έκτασης- 100 ευρώ, έχετε δικαίωμα να αποζημιωθείτε με τουλάχιστον 200 ευρώ και επιπλέον να ζητήσετε όποιο ποσό θεωρείτε ότι θα σας καλύψει ως χρηματική ικανοποίηση λόγω ηθικής βλάβης. Εννοείται ότι δεν είναι απαραίτητο η επίλυση της διαφοράς να γίνει ενώπιον του δικαστηρίου, γιατί το αυταπόδεικτο του πράγματος επιτρέπει τον εξώδικο διακανονισμό. Η 4η παράγραφος όμως μπορεί να διαταχθεί ως μέτρο μόνο από το δικαστήριο και αφορά την καταδίκη του δράστη να μην ξαναδημοσιεύσει, γιατί εφόσον το ξανακάνει θα πρέπει να σας καταβάλει τα ποσά που αναφέρει το δικαστήριο στην απόφασή του (900 – 3.000 ευρώ) και να κρατηθεί έως ένα έτος (βέβαια, για την κράτηση δεν ξέρω αν συμφέρει γιατί θα πρέπει να του πληρώνετε τα έξοδα διατροφής στη φυλακή. Για λόγους ενημέρωσης επί επίκαιρων γεγονότων επιτρέπεται αναδημοσίευση πολιτικών λόγων, προσφωνήσεων, κηρυγμάτων, δικανικών αγορεύσεων ή άλλων έργων παρόμοιας φύσης.

Στις 9.2.2006 η Google ανακοίνωσε μια νέα εφαρμογή του Google Desktop, το λογισμικό θα αποθηκεύσει αντίγραφα απο έγγραφα Word, PDF κλπ, προκειμένου να διευκολύνει το ψάξιμο από όλους τους χρήστες του υπολογιστή. Το EFF[52] καλεί τους καταναλωτές να μη χρησιμοποιήσουν αυτη την εφαρμογή, επειδή θα καταστήσει τα προσωπικά τους δεδομένα επιδεχόμενα απειλών από την διοίκηση, τους ιδιώτες και τους hackers.

Το EFF επισημαίνει ότι το πρόβλημα παρουσιάζεται επειδή ο Electronic Communication Privacy Act του 1986 παρέχει περιορισμένη προστασία στα emails και σε αλλα αρχεία που αποθηκεύονται από παρόχους online υπηρεσιών. Άλλη μια αναφορά στο ανεπαρκές σύστημα προστασίας προσωπικών δεδομένων στις ΗΠΑ.

Επίσης, τους τελευταίους μήνες παρατηρείται έντονα το φαινόμενο της αναδημοσίευσης σε εφημερίδες κειμένων που βρίσκονται αναρτημένα σε ιστολόγια, χωρίς προηγούμενη ενημέρωση των συντακτών των κειμένων και φυσικά χωρίς προηγούμενη συγκατάθεσή τους. Αξίζει, λοιπόν,

[52] http://eff.org/news/archives/2006.02.php#004400

να συμβουλευτούμε το σχετικό θεσμικό πλαίσιο για να διερευνηθεί κατά πόσον υπάρχει δικαίωμα αναδημοσίευσης και αν υφίσταται υποχρέωση τέτοιας ανοχής. Θα ξεκινήσω από τη βάση της έννομης τάξης, το ελληνικό Σύνταγμα. (Εξάλλου η αναδημοσίευση και η κυκλοφορία των εφημερίδων λαμβάνει χώρα σε ελληνικό έδαφος, οπότε αν υποτεθεί ότι υπάρχει άδικο, εφαρμοστέο είναι το δίκιο της τέλεσης του αδίκου). Στο **άρθρο 5Α**[53] διαβάζουμε ότι:

Καθένας έχει δικαίωμα στην πληροφόρηση, όπως νόμος ορίζει. Περιορισμοί στο δικαίωμα αυτό είναι δυνατόν να επιβληθούν με νόμο μόνο εφόσον είναι απολύτως αναγκαίοι και δικαιολογούνται για λόγους εθνικής ασφάλειας, καταπολέμησης του εγκλήματος ή προστασίας δικαιωμάτων και συμφερόντων τρίτων.

Καθένας έχει δικαίωμα συμμετοχής στην Κοινωνία της Πληροφορίας. Η διευκόλυνση της πρόσβασης στις πληροφορίες που διακινούνται ηλεκτρονικά, καθώς και της παραγωγής, ανταλλαγής και διάδοσής τους αποτελεί υποχρέωση του Κράτους, τηρουμένων πάντοτε των εγγυήσεων των άρθρων 9, 9Α και 19.

Από αυτό το άρθρο, η εφημερίδα αντλεί το δικαίωμα στην πληροφόρηση -και την πρόσβαση στα κείμενα που βρίσκονται στο Διαδίκτυο- στην παθητική (λήψη πληροφοριών) και την ενεργητική της μορφή

Παρατηρούμε ότι το δικαίωμα αυτό πρέπει να το ασκήσει μέσα στους όρους που επιβάλει ο νόμος (επιφύλαξη υπέρ της νομιμότητας). Περιορισμοί του δικαιώματος αυτού χωρούν εφόσον είναι απολύτως αναγκαίοι (εμφατική αναφορά στην αρχή της αναλογικότητας), επιβάλλονται με νόμο (αρχή της νομιμότητας του περιορισμού) και δικαιολογούνται για λόγους, inter alia, προστασίας δικαιωμάτων και συμφερόντων τρίτων (πρακτική εναρμόνιση αντίρροπων δικαιωμάτων).

Μία τέτοια δέσμη προστασίας δικαιωμάτων και συμφερόντων τρίτων που περιορίζουν το δικαίωμα του τύπου για ενεργητική πληροφόρηση είναι τα δικαιώματα που έχουν οι κάτοχοι επί των προϊόντων της διάνοιάς τους, κατά την έκφραση του Αστικού Κώδικα (άρθρο 60) Όποιος προσβάλλεται παράνομα στο αποκλειστικό δικαίωμά του επάνω στα προϊόντα της διάνοιάς του έχει δικαίωμα να απαιτήσει κατά τους όρους του νόμου, να αρθεί η προσβολή και να μην επαναληφθεί στο μέλλον.

Αξίζει να συγκρατήσουμε ότι το δίκαιωμα πνευματικής ιδιοκτησίας περιλαμβάνεται στα θεμελιώδη δικαιώματα που απαριθμεί ο Χάρτης των Θεμελιωδών Δικαιωμάτων της ΕΕ (άρθρο 17§2)[54], ο οποίος αποτελεί και το Μέρος ΙΙ της Σύμβασης για τη θέσπιση Συντάγματος της Ευρώπης.

Το εσωτερικό δίκαιο προστασίας της πνευματικής ιδιοκτησίας περιλαμβάνεται κυρίως στον Νόμο υπ' αρ. 2121/1993. Ο νόμος αυτός ορίζει ότι το δικαίωμα πνευματικής ιδιοκτησίας αποκτά κάποιος με την δημιουργία ενός έργου, χωρίς να απαιτείται καμία απολύτως τυπική διατύπωση (εγγραφή σε μητρώο, κατάθεση σε συμβολαιογράφο κλπ- αυτά έχουν απλώς και μόνο αποδεικτική αξία, όχι συστατική του δικαιώματος και κυρίως περιττή εφόσον κάτι έχει δημοσιευτεί ήδη στο Διαδίκτυο). Η πνευματική ιδιοκτησία περιλαμβάνει το δικαίωμα εκμετάλλευσης του έργου (περιουσιακό δικαίωμα) και το δικαίωμα προστασίας του προσωπικού δεσμού του δημιουργού με αυτό (ηθικό δικαίωμα). Οι δύο αυτοί πυλώνες της πνευματικής ιδιοκτησίας αναλύονται σε ειδικότερες εξουσίες.

Τι είναι όμως το «έργο» που προστατεύει ο νόμος; Ο ορισμός του έργου που απολαμβάνει προστασίας δίνεται από **το άρθρο 2§1**:

Ως έργο νοείται κάθε πρωτότυπο πνευματικό δημιούργημα λόγου, τέχνης ή επιστήμης, που εκφράζεται με οποιαδήποτε μορφή, ιδίως τα γραπτά ή προφορικά κείμενα, οι μουσικές συνθέσεις, με κείμενο ή χωρίς, τα θεατρικά έργα, με μουσική ή χωρίς, οι χορογραφίες και οι παντομίμες, τα οπτικοακουστικά έργα, τα έργα των εικαστικών τεχνών, στα οποία περιλαμβάνονται τα σχέδια, τα έργα ζωγραφικής και γλυπτικής, τα χαρακτικά έργα και οι λιθογραφίες, τα αρχιτεκτονικά έργα, οι φωτογραφίες, τα έργα των εφαρμοσμένων τεχνών, οι εικονογραφήσεις, οι χάρτες, τα τρισδιάστατα έργα που αναφέρονται στη γεωγραφία, την τοπογραφία, την αρχιτεκτονική ή την επιστήμη.

---

[53] http://www.parliament.gr/politeuma/syntagmaDetails.asp?ArthroID=6

[54] http://www.europarl.eu.int/charter/pdf/text_el.pdf

Η **§2** επεκτείνει (κατά πλάσμα δικαίου) την προστασία και σε μερικές κατηγορίες έργων που θα μπορούσε να αμφισβητηθεί αν εντάσσονται στην έννοια «πρωτότυπο πνευματικό δημιούργημα λόγου, τέχνης ή επιστήμης» :

Νοούνται επίσης ως έργα οι μεταφράσεις, οι διασκευές, οι προσαρμογές και οι άλλες μετατροπές έργων ή εκφράσεων της λαϊκής παράδοσης, καθώς και οι συλλογές έργων ή συλλογές εκφράσεων της λαϊκής παράδοσης ή απλών γεγονότων και στοιχείων, όπως οι εγκυκλοπαίδειες "και" οι ανθολογίες "(παραλείπονται λέξεις)" εφόσον η επιλογή ή η διευθέτηση του περιεχομένου τους είναι πρωτότυπη. Η προστασία των έργων της παρούσας παραγράφου γίνεται με την επιφύλαξη των δικαιωμάτων στα προϋπάρχοντα έργα, που χρησιμοποιήθηκαν ως αντικείμενο των μετατροπών ή των συλλογών.

Ας σημειώσουμε ότι όταν ο νόμος αναφέρει «πρωτότυπο» έργο δεν αναφέρεται βέβαια στην έννοια της πνευματικής μοναδικότητας, αλλά στο γεγονός ότι λόγω της διατύπωσής του και μόνο (εξωτερικό στοιχείο), παρουσιάζει αναγνωρίσιμη αυτονομία, αυτοτέλεια και δεν ταυτίζεται με άλλα έργα, όσο κι αν μοιάζει ίσως με αυτά. Δηλαδή ακόμη κι αν πείτε την κοκκινοσκουφίτσα με «δικά» σας λόγια, το έργο θεωρείται πρωτότυπο: ο ελληνικός νόμος προστατεύει την διατύπωση, όχι την «ιδέα» ή την «ουσία». Μόνο σε ακραίες περιπτώσεις «κλοπής» της ιδέας (ενός σεναρίου π.χ.), στο βαθμό που αυτό προσβάλλει ξεκάθαρα τον δημιουργό του αρχικού έργου και, ακόμη χειρότερα, με κερδοσκοπικές προθέσεις, ο δημιουργός προστατεύεται.

Πάντως, ο νόμος σπεύδει να ορίσει στην **§4** ότι:

Η προστασία του παρόντος νόμου είναι ανεξάρτητη από την αξία και τον προορισμό του έργου, καθώς και από το γεγονός ότι το έργο προστατεύεται ενδεχομένως και από άλλες διατάξεις.

Επομένως, όσο μικρό, ανούσιο, βλακώδες, μη εμπορικά αξιοποιήσιμο κι αν είναι ένα κείμενο, εφόσον έχει τα χαρακτηριστικά του «προστατευόμενου έργου», καλύπτεται από τις εγγυήσεις του νόμου 2121 που θα αναλύσουμε πιο κάτω.

Ας δούμε τώρα **ποια έργα εξαιρούνται** ρητά από την προστασία της πνευματικής ιδιοκτησίας[55].

Η προστασία του παρόντος νόμου δεν εκτείνεται σε επίσημα κείμενα με τα οποία εκφράζεται η άσκηση πολιτειακής αρμοδιότητας και ιδίως σε νομοθετικά, διοικητικά ή δικαστικά κείμενα, καθώς και στις εκφράσεις της λαϊκής παράδοσης, στις ειδήσεις και στα απλά γεγονότα ή στοιχεία.Σε αυτό το σημείο βρίσκεται μια διάταξη κλειδί: αν ένα κείμενο αποτελεί ταυτόχρονα και «είδηση», δεν προστατεύεται από τις διατάξεις της πνευματικής ιδιοκτησίας. Ο λόγος του πρωθυπουργού είναι είδηση. Η είδηση δεν μπορεί να είναι «ιδιοκτησία» κανενός, λέει ο νόμος. Είναι κοινό κτήμα της κοινωνίας της πληροφορίας. Προσοχή όμως: το γεγονός ότι ο πρωθυπουργός δημοσίευσε ένα βιβλίο και το γεγονός ότι αυτό είναι είδηση, δεν καθιστά και το περιεχόμενο του βιβλίου «κοινό κτήμα της κοινωνίας της πληροφορίας». Η εξαίρεση από την προστασία αφορά το ίδιο το γεγονός καθαυτό και μπορεί να δικαιολογήσει και την παράθεση ορισμένων αποσπασμάτων από αυτό στον τύπο, μόνο και μόνο όμως για την διάνθιση και την τεκμηρίωση της είδησης.

Είναι σαφές ότι το γεγονός πως ο συγγραφέας είναι ο πρωθυπουργός δεν τον απογυμνώνει από το θεμελιώδες δικαίωμά του στην πνευματική ιδιοκτησία. Δεν επιτρέπεται η δημοσίευση όλου του έργου στον τύπο. Επιτρέπεται η παράθεση των αποσπασμάτων που τεκμηριώνουν την είδηση (αρχή αναλογικότητας και πρακτική εναρμόνιση δικαιωμάτων). Παράδειγμα: το γεγονός ότι οι εφημερίδες και η τηλεόραση ανακάλυψαν τα weblogs ως τάση («είδηση») δεν σημαίνει ότι τα ίδια τα κείμενα που είναι αναρτημένα σε αυτά είναι «είδηση», ώστε να μην καλύπτονται από την προστασία της πνευματικής ιδιοκτησίας.
Η περιγραφή ενός «απλού γεγονότος» ή η παράθεση ενός στοιχείου, όπως για παράδειγμα μια φωτογραφία που απλώς καταγράφει ένα συμβάν, χωρίς να ενέχει ένα στοιχείο δημιουργικότητας και πρωτοτυπίας (κατά την ανωτέρω έννοια), δεν προστατεύεται ως «έργο». Προσοχή όμως: άλλο το «απλό γεγονός» κι άλλο η είδηση που καταγράφεται με τόσο έντονα στοιχεία δημιουργικότητας ώστε να καθίσταται τελικά πρωτότυπο δημιούργημα. Αν ένας (μη

[55] (§5)

τηλεοπτικός) σκηνοθέτης κινηματογραφήσει με δικούς του καλλιτεχνικούς όρους, αλλά live την εκλογή του Προέδρου της Δημοκρατίας, δεν σημαίνει ότι το έργο του χάνει τον πρωτότυπο και δημιουργικό χαρακτήρα που μπορεί να έχει, μόνο και μόνο επειδή, εκτός των άλλων, συνιστά και είδηση.

Παράδειγμα: το απλό γεγονός ότι ένας blogger έγραψε ένα άρθρο δεν σημαίνει ότι το άρθρο του εντάσσεται στην έννοια του απλού γεγονότος και ότι ως εκ τούτου ξεφεύγει από την προστασία της πνευματικής ιδιοκτησίας.

Ο δημιουργός είναι ο απόλυτος κύριος του έργου του και έχει σε αυτό τα δικαιώματα να επιτρέψει ή να απαγορέψει την εγγραφή, την αναπαραγωγή, την μετάφραση, την διασκευή, την αναμετάδοση και κάθε μορφή διακίνησης του έργου («περιουσιακό δικαίωμα», άρθρο 3). Έχει επίσης το δικαίωμα να αποφασίζει αυτός το χρόνο που το έργο θα γίνει προσιτό στο κοινό (δημοσίευση), την μνεία του ονόματός του σε κάθε χρήση του έργου ή αντίθετα να κρατάει την ανωνυμία του ή να χρησιμοποιεί ψευδώνυμο, την απαγόρευση κάθε περικοπής, παραμόρφωσης ή άλλης αλλοίωσης του έργου του κλπ («ηθικό δικαίωμα», άρθρο 4). Το ηθικό δικαίωμα είναι ανεξάρτητο από το περιουσιακό και παραμένει στον δημιουργό ακόμη και μετά τη μεταβίβαση του περιουσιακού δικαιώματος. Με λίγα λόγια, ενώ ο δημιουργός έχει το δικαίωμα να εκμεταλλευτεί το έργο του, συνάπτοντας συμβάσεις και δίνοντας άδειες χρήσης, δεν χωρεί παραίτηση από το ηθικό του δικαίωμα (προστατευτική λειτουργία του νόμου για το δημιουργό). Ο δημιουργός είναι δικαιούχος της πνευματικής ιδιοκτησίας για όλη του τη ζωή και το έργο προστατεύεται για 70 χρόνια μετά το θάνατό του. (Όμως: «για τα ανώνυμα ή ψευδώνυμα έργα η πνευματική ιδιοκτησία διαρκεί εβδομήντα (70) χρόνια από την 1η Ιανουαρίου του έτους που έπεται εκείνου κατά το οποίο το έργο κατέστη νομίμως προσιτό στο κοινό, εκτός εάν, πριν από την πάροδο αυτής της χρονικής περιόδου, ο δημιουργός αποκαλύψει την ταυτότητά του ή το υιοθετηθέν από το δημιουργό ψευδώνυμο δεν αφήνει καμία αμφιβολία για την ταυτότητά του, οπότε εφαρμόζονται οι γενικοί κανόνες.», **άρθρο 31**)

Αφού περιγράψαμε σε γενικές γραμμές το περιεχόμενο των δικαιωμάτων πνευματικής ιδιοκτησίας επί των έργων του λόγου, προχωρούμε στους περιορισμούς του δικαιώματος που προβλέπει ο νόμος.

Πότε δηλαδή επιτρέπεται αναπαραγωγή του έργου χωρίς άδεια του δημιουργού. Για ένα νόμιμα δημοσιευμένο κείμενο (όχι «υποκλοπή» δηλαδή), επιτρέπεται η αναπαραγωγή χωρίς άδεια του δημιουργού και χωρίς αμοιβή:για ιδιωτική χρήση εκείνου που την κάνει (άρθρο 18) αλλά μόνο ως παράθεση σύντομων αποσπασμάτων για τη υποστήριξη γνώμης εκείνου που παραθέτει ή την κριτική της γνώμης του άλλου, εφόσον η παράθεση είναι σύμφωνη προς τα χρηστά ήθη και η έκταση των αποσπασμάτων δικαιολογείται από τον επιδιωκόμενο σκοπό. Η παράθεση του αποσπάσματος πρέπει να συνοδεύεται από την ένδειξη της πηγής και των ονομάτων του δημιουργού, εφόσον το όνομα [ή ψευδώνυμο, εννοείται] εμφανίζεται στην πηγή (άρθρο 19) σε σχολικά βιβλία και/ ή για διδασκαλία μόνο όμως εφόσον πρόκειται για μικρό τμήμα της συνολικής δημιουργίας του συγγραφέα και εφόσον δεν εμποδίζει την κανονική εκμετάλλευση του έργου, με ένδειξη της πηγής κλπ (άρθρα 20,21) , ενός πρόσθετου αντιτύπου από μη κερδοσκοπικές βιβλιοθήκες ή αρχεία, που έχουν αντίτυπο του έργου στην μόνιμη συλλογή τους, προκειμένου να διατηρήσουν το αντίτυπο αυτό ή να το μεταβιβάσουν σε άλλη, μη κερδοσκοπική, βιβλιοθήκη ή αρχείο. Η αναπαραγωγή επιτρέπεται μόνο αν είναι αδύνατη η προμήθεια ενός τέτοιου αντιτύπου από την αγορά σε σύντομο χρόνο και με εύλογους όρους. (άρθρο 22) στο μέτρο που δικαιολογείται από τον επιδιωκόμενο σκοπό: α) η αναπαραγωγή και η διάδοση στο κοινό, για λόγους περιγραφής επίκαιρων γεγονότων με μέσα μαζικής επικοινωνίας έργων, που βλέπονται ή ακούγονται κατά τη διάρκεια ενός τέτοιου γεγονότος, β) η αναπαραγωγή και η διάδοση στο κοινό με μέσα μαζικής επικοινωνίας προς το σκοπό της ενημέρωσης επί επίκαιρων γεγονότων πολιτικών λόγων, προσφωνήσεων, κηρυγμάτων, δικανικών αγορεύσεων ή άλλων έργων παρόμοιας φύσης, καθώς και περιλήψεων ή αποσπασμάτων από διαλέξεις, εφόσον τα έργα αυτά παρουσιάζονται δημόσια. Η αναπαραγωγή και η διάδοση στο κοινό πρέπει, όταν αυτό είναι δυνατό , να συνοδεύονται από την ένδειξη της πηγής και του ονόματος του δημιουργού (άρθρο 25).

Σε αυτήν την τελευταία περίπτωση ερχόμαστε πάλι στην προβληματική της «είδησης». Όπως εκτέθηκε, η ίδια η είδηση, τα απλά γεγονότα και στοιχεία βρίσκονται εκτός της προστασίας. Στο άρθρο 25 έχουμε έναν περιορισμό της προστασίας για κείμενα που ήδη

καταλαμβάνονται από το πεδίο εφαρμογής της. Τηρουμένης της αρχής της αναλογικότητας, τέτοιας φύσης κείμενα μπορούν να αναπαραχθούν στον τύπο για λόγους ενημέρωσης.

Επισης, ενημερωτικά, η Ελλάδα είναι το μοναδικό Κράτος-μέλος της ΕΕ από τα 25 που δεν έχει ενσωματώσει στο εσωτερικό της δίκαιο την Οδηγία 58/2002/ΕΚ για την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες.

Η Οδηγία αυτή αντικατέστησε την Οδηγία 97/66 (προστασία δεδομένων στον τηλεπικοινωνιακό τομέα), την λεγόμενη "Οδηγία ISDN", την οποία το ελληνικό δίκαιο ενσωμάτωσε με το Ν.2774/1999. Και ενώ όλη η ΕΕ κινείται στο πεδίο της Οδηγίας 2002, εμείς εφαρμόζουμε ακόμη την προηγούμενη! Με αποτέλεσμα να απειλούνται ήδη πρόστιμα κατά της χώρας μας για μη προσαρμογή του εσωτερικού δικαίου προς το κοινοτικό.

5.2.4 ΝΟΜΟΣ 2472/1997

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

Οι διατάξεις του Ν 2472/97 εφαρμόζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα, τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε αρχείο. Οι διατάξεις του παρόντος νόμου δεν εφαρμόζονται στην επεξεργασία δεδομένων η οποία πραγματοποιείται:

α) από φυσικό πρόσωπο για την άσκηση δραστηριοτήτων αποκλειστικά προσωπικών ή οικιακών,

β) από τις δικαστικές - εισαγγελικές αρχές και τις υπηρεσίες που ενεργούν υπό την άμεση εποπτεία τους στο πλαίσιο της απονομής της δικαιοσύνης ή για την εξυπηρέτηση των αναγκών της λειτουργίας τους με σκοπό τη βεβαίωση εγκλημάτων, που τιμωρούνται ως κακουργήματα ή πλημμελήματα με δόλο και ιδίως εγκλημάτων κατά της ζωής, κατά της γενετήσιας ελευθερίας, της οικονομικής εκμετάλλευσης της γενετήσιας ζωής, κατά της προσωπικής ελευθερίας, κατά της ιδιοκτησίας, κατά των περιουσιακών δικαιωμάτων, παραβάσεων της νομοθεσίας περί ναρκωτικών, επιβουλής της δημόσιας τάξης, ως και τελουμένων σε βάρος ανηλίκων θυμάτων.

Στις ποιό πάνω περιπτώσεις εφαρμόζονται οι ισχύουσες ουσιαστικές και δικονομικές ποινικές διατάξεις.

Στις περιπτώσεις άσκησης από τους πολίτες του δικαιώματος του συνέρχεσθαι κατά το άρθρο 11 του Συντάγματος επιτρέπεται η απλή λειτουργία συσκευών καταγραφής ήχου ή εικόνας ή άλλων ειδικών τεχνικών μέσων με σκοπό την καταγραφή εφόσον συντρέχουν οι προϋποθέσεις του επόμενου εδαφίου.

Η καταγραφή ήχου ή εικόνας με οποιασδήποτε τεχνικής μορφής συσκευές με σκοπό τη βεβαίωση τέλεσης των παραπάνω εγκλημάτων γίνεται μόνον κατόπιν εντολής εκπροσώπου της εισαγγελικής αρχής και εφόσον επίκειται σοβαρός κίνδυνος για τη δημόσια τάξη και ασφάλεια.

Σκοπός της καταγραφής αυτής είναι μόνον η χρησιμοποίηση του βεβαιούντος την τέλεση των εγκλημάτων υλικού ως αποδεικτικού στοιχείου ενώπιον οποιασδήποτε ανακριτικής, εισαγγελικής αρχής και δικαστηρίου. Η επεξεργασία κάθε άλλου υλικού που δεν είναι αναγκαίο προς εξυπηρέτηση του παραπάνω σκοπού για τη βεβαίωση των εγκλημάτων απαγορεύεται, το δε σχετικό υλικό καταστρέφεται με πράξη του αρμόδιου Εισαγγελέα.

γ) από δημόσια αρχή με τη λειτουργία ειδικών τεχνικών μέσων καταγραφής ήχου ή εικόνας σε δημόσιους χώρους για τη διαφύλαξη της ασφάλειας του κράτους, της άμυνας, της δημόσιας ασφάλειας, για την οποία είναι αρμόδια, και ιδίως για την προστασία προσώπων και πραγμάτων, καθώς και για τη διαχείριση της κυκλοφορίας. Το υλικό που συλλέγεται από τα ανωτέρω μέσα, εφόσον δεν εμπίπτει στην περίπτωση β', τηρείται για χρονικό διάστημα επτά (7) ημερών, μετά το πέρας των οποίων καταστρέφεται με πράξη του αρμόδιου εισαγγελέα. Η παράβαση των διατάξεων του προηγούμενου εδαφίου τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους, αν δεν τιμωρείται βαρύτερα από άλλη διάταξη.

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

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

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

*** Το πρώην στοιχείο γ της παρ. 3 του παρόντος άρθρου αναριθμήθηκε ως στοιχείο β μετά την κατάργηση του πρώην στοιχείου β σύμφωνα με το άρθρο 19 παρ. 1 Ν. 3471/2006.(ΦΕΚ Α/133/2006)

*** Το πρώτο εδάφιο στο νέο στοιχείο β (πρώην γ) της παρ. 3 του παρόντος άρθρου τροποποιήθηκε ως άνω σύμφωνα με το άρθρο 19 παρ. 2 Ν. 3471/2006.

*** Στην παράγραφο 2 του παρόντος άρθρου, όπως είχε αντικατασταθεί με την παράγραφο 1 του άρθρου όγδοου του Ν. 3625/2007 (ΦΕΚ Α/290/2007) προστέθηκε η περίπτωση γ', σύμφωνα με το άρθρο 12 παρ. 1 Ν. 3783/2009, (ΦΕΚ Α/136/2009).

5.2.5 ΝΟΜΟΣ 3471/2006

Ο νόμος 3471/2006Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Ενσωμάτωση της Οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, ΕΕ L 201/37 της 31ης Ιουλίου 2002)

Σκοπός των διατάξεων των άρθρων 1 έως 17 του 3471/2006 είναι η **προστασία** των θεμελιωδών δικαιωμάτων των ατόμων και ιδίως της **ιδιωτικής ζωής** και η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη **διασφάλιση του απορρήτου των επικοινωνιών** στον τομέα των ηλεκτρονικών επικοινωνιών.

Οι διατάξεις των άρθρων 1 έως 17 του παρόντος νόμου έχουν εφαρμογή κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών, στο πλαίσιο της παροχής διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών σε δημόσια δίκτυα ηλεκτρονικών επικοινωνιών. Για την επεξεργασία δεδομένων προσωπικού χαρακτήρα που πραγματοποιείται στο πλαίσιο μη διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, εφαρμόζεται ο ν. 2472/1997 (ΦΕΚ 50 Α'), όπως ισχύει.

Ο ν. 2472/1997, όπως ισχύει, και οι εκτελεστικοί του άρθρου 19 του Συντάγματος νόμοι, όπως ισχύουν, εφαρμόζονται για κάθε ζήτημα σχετικό με την παροχή υπηρεσιών ηλεκτρονικών επικοινωνιών, που δεν ρυθμίζεται ειδικότερα από τον παρόντα νόμο.

Οι διατάξεις των άρθρων 8 και 9 εφαρμόζονται στις γραμμές συνδρομητών που συνδέονται με ψηφιακά κέντρα και, όταν αυτό είναι τεχνικώς εφικτό, σε γραμμές συνδρομητών που συνδέονται με αναλογικά κέντρα, εφόσον τούτο δεν συνεπάγεται δυσανάλογη οικονομική επιβάρυνση. Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.) διαπιστώνει τις περιπτώσεις όπου η σύνδεση με αναλογικά κέντρα είναι τεχνικώς αδύνατη ή απαιτεί δυσανάλογη επένδυση, και ενημερώνει σχετικώς την Ευρωπαϊκή Επιτροπή.

Οποιαδήποτε χρήση των υπηρεσιών ηλεκτρονικών επικοινωνιών που παρέχονται μέσω δημοσίου δικτύου επικοινωνιών και των διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και των συναφών δεδομένων κίνησης και θέσης, όπως ορίζονται στις διατάξεις του άρθρου 2 του παρόντος νόμου, προστατεύεται από το απόρρητο των επικοινωνιών.

Η άρση του απορρήτου είναι επιτρεπτή μόνο υπό τις προϋποθέσεις και τις διαδικασίες που προβλέπονται από το άρθρο 19 του Συντάγματος.

Απαγορεύεται η ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των ηλεκτρονικών επικοινωνιών και των συναφών δεδομένων κίνησης και θέσης, εκτός αν προβλέπεται άλλως από το νόμο.

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

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

Απαγορεύεται η χρήση των δικτύων ηλεκτρονικών επικοινωνιών για την αποθήκευση πληροφοριών ή την απόκτηση πρόσβασης σε πληροφορίες αποθηκευμένες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη, ιδίως δε με την εγκατάσταση κατασκοπευτικών λογισμικών, κρυφών αναγνωριστικών στοιχείων και άλλων παρόμοιων διατάξεων. Κατ' εξαίρεση, επιτρέπεται η οποιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια ή διευκόλυνση της διαβίβασης μίας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή η οποία είναι αναγκαία μόνο για την παροχή υπηρεσίας στην κοινωνία των πληροφοριών, την οποία έχει ζητήσει ρητά ο χρήστης ή ο συνδρομητής. Στην τελευταία αυτή περίπτωση η χρησιμοποίηση τέτοιων διατάξεων επιτρέπεται μόνον εάν παρέχονται στον συγκεκριμένο συνδρομητή ή χρήστη σαφείς και εκτεταμένες πληροφορίες, σύμφωνα με το άρθρο 11 του ν. 2472/1997, όπως ισχύει, και ο υπεύθυνος ελέγχου των δεδομένων παρέχει στον συνδρομητή ή χρήστη το δικαίωμα να αρνείται την επεξεργασία αυτή. Με πράξη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ορίζονται ειδικότερα οι τρόποι παροχής πληροφοριών, παροχής του δικαιώματος άρνησης ή αίτησης συγκατάθεσης.

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

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνον εφόσον:

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

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

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

Ο φορέας παροχής δημοσίου δικτύου ή και διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών δεν επιτρέπεται να χρησιμοποιεί τα δεδομένα προσωπικού χαρακτήρα και τα δεδομένα κίνησης και θέσης ή να τα διαβιβάζει σε τρίτους για άλλους σκοπούς, εκτός εάν ο συνδρομητής ή ο χρήστης έχει ρητά και ειδικά δώσει τη συγκατάθεση του. Εξαιρούνται οι σκοποί που συνδέονται με την παροχή υπηρεσιών ηλεκτρονικών επικοινωνιών ή την παροχή υπηρεσιών προστιθέμενης αξίας που έχει ζητήσει ο συνδρομητής ή χρήστης, όπως η διαφήμιση ή η εμπορική έρευνα αγοράς προϊόντων και υπηρεσιών.

Για τα δεδομένα κίνησης, ο φορέας παροχής των υπηρεσιών οφείλει να ενημερώσει τον συνδρομητή ή τον χρήστη πριν από τη χορήγηση της συγκατάθεσης του σχετικά με τον τύπο των δεδομένων κίνησης που υποβάλλονται σε επεξεργασία και τη διάρκεια της επεξεργασίας αυτής.

Όταν τα δεδομένα διαβιβάζονται σε τρίτους, η συγκατάθεση απαιτείται να είναι έγγραφη. Δεν θεωρούνται ως τρίτοι οι φορείς παροχής δημοσίου δικτύου ή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών, όσον αφορά στη διαβίβαση σε αυτούς από αντίστοιχο φορέα δεδομένων κίνησης, με αποκλειστικό σκοπό τη χρέωση των παρεχομένων υπηρεσιών, υπό τον όρο ότι ο συνδρομητής ή ο χρήστης έχει ενημερωθεί κατά την κατάρτιση της σύμβασης εγγράφως. Η συγκατάθεση μπορεί να ανακληθεί οποτεδήποτε. Αν ανακληθεί και εφόσον τα δεδομένα έχουν εν τω μεταξύ ανακοινωθεί σε τρίτους, η ανάκληση ανακοινώνεται σε αυτούς με φροντίδα του υπεύθυνου επεξεργασίας. Ο φορέας παροχής δημοσίου δικτύου ή/ και διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών απαγορεύεται να εξαρτά την παροχή των υπηρεσιών αυτών προς τον συνδρομητή ή τον χρήστη από τη συγκατάθεση του στην επεξεργασία των δεδομένων αυτών για σκοπούς άλλους από εκείνους που εξυπηρετούν άμεσα την παροχή των υπηρεσιών στις οποίες αφορούν τα άρθρα 1 έως 17.

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

Ο φορέας παροχής διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει, στο βαθμό που αυτό είναι τεχνικώς εφικτό, και επιτρέπεται από τον παρόντα νόμο, να καθιστά δυνατή τη πληρωμή των υπηρεσιών αυτών ανωνύμως ή με ψευδώνυμο. Σε περίπτωση αμφισβήτησης της τεχνικής δυνατότητας της ανώνυμης και ψευδώνυμης πληρωμής των υπηρεσιών αυτών, γνωμοδοτεί η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.)

5.3 ΕΥΡΩΠΑΙΚΗ ΝΟΜΟΘΕΣΙΑ

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, συμπεριλαμβανόμενης 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 συμπεριλήφθησαν στη Σύσταση του 1989, η οποία όριζε εγκληματικές πράξεις, όπως απάτη και πλαστογραφία με ηλεκτρονικούς υπολογιστές, καταστροφή δεδομένων και λογισμικού, μη εξουσιοδοτημένη πρόσβαση, μη εξουσιοδοτημένη αναπαραγωγή λογισμικού κ.ά. Επίσης, η Σύσταση αυτή περιελάμβανε και μια σειρά από Οδηγίες (μη υποχρεωτικές) προς 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: τη Σύσταση 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 Η/Υ. Οι συστάσεις αυτές αποτέλεσαν τη βάση για τη Σύμβαση για τον Κυβερνοχώρο του 2001.

Οι εργασίες για τη δημιουργία μιας Σύμβασης για τον Κυβερνοχώρο ξεκίνησαν το 1997, όταν συστήθηκε μια επιτροπή ειδικών στον τομέα του ηλεκτρονικού εγκλήματος, με σκοπό να εξετάσει τα νομοθετικά προβλήματα που προκύπτουν από την εγκληματική δραστηριότητα, που αναπτύσσεται και συνεχών διευρύνεται στον κυβερνοχώρο. Αν και αρχικά η περαίωση των εργασιών της επιτροπής, είχε προσδιοριστεί για το 1999, τα ιδιαίτερα προβλήματα που συνάντησαν τα μέλη της, έθεσαν νέα προθεσμία το έτος 2000.

Τελικά, το κείμενο της *«Σύμβασης για το Έγκλημα στον Κυβερνοχώρο»,* υπογράφηκε στις 23-11-2001[31], στη Βουδαπέστη, από τα περισσότερα μέλη του Ευρωπαϊκού Συμβουλίου[56]. Στη Σύμβαση, υπάρχουν επεξηγήσεις και ρυθμίσεις για όλα τα ηλεκτρονικά εγκλήματα:

- για 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,
- για τα αδικήματα που σχετίζονται με τους υπολογιστές, όπως η απάτη με Η/Υ και **πλαστογραφία,**
- για τα αδικήματα σχετικά με το περιεχόμενο όπως είναι το αδίκημα της παιδικής πορνογραφίας &
- για τα αδικήματα που σχετίζονται με καταπάτηση πνευματικής ιδιοκτησίας.

Επιπρόσθετα περιλαμβάνονται ρυθμίσεις για τη συνέργια, την απόπειρα και την υποκίνηση ηλεκτρονικών εγκλημάτων, καθώς και την ευθύνη των επιχειρήσεων. Ακόμα τονίζεται η αναγκαιότητα της διεθνούς συνεργασίας μεταξύ των κρατών για την καταπολέμηση του ηλεκτρονικού εγκλήματος και θίγεται το πολύ σημαντικό θέμα της αρμοδιότητας και της δικαιοδοσίας των δικαστηρίων σχετικά με τα εγκλήματα αυτά. Η εν λόγω Σύμβαση έχει χαρακτηρισθεί από πολλούς ως το πιο άρτιο κείμενο σχετικά με το ηλεκτρονικό κείμενο στην Ευρωπαϊκή Ένωση και έχει ήδη υπογραφεί από 33 κράτη συμπεριλαμβανομένων των ΗΠΑ, Καναδά, Ν. Αφρική και Ιαπωνία. Φυσικά δεν λείπουν οι επικριτές της[57].

Παράλληλα υπάρχουν και άλλα γενικά νομοθετήματα που βοηθούν **στην καταπολέμηση του ηλεκτρονικού εγκλήματος.** Ενδεικτικά αναφέρουμε τα ακόλουθα που ισχύουν στην Ευρωπαϊκή Ένωση:

1. Η Σύσταση του Συμβουλίου με αριθμό 9193/01, με την οποία καλούνται τα κράτη μέλη να συμμετάσχουν στο δίκτυο πληροφόρησης της Ομάδας των Οκτώ, το οποίο λειτουργεί 24 ώρες το εικοσιτετράωρο, για την καταπολέμηση του εγκλήματος υψηλής τεχνολογίας.
2. Η Σύσταση του Συμβουλίου No R (89) 9 σχετική με το έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή (Recommendation No R (89) 9 on Computer related crime).
3. Η Σύσταση του Συμβουλίου No R (95) 13 για τα ποινικά δικονομικά προβλήματα που συνδέονται με την τεχνολογία των πληροφοριών (Recommendation No R (95) 13 Problems of criminal procedural Law connected with information technology). Η σπουδαιότητα της σύστασης αυτής είναι μεγάλη, διότι καθιερώνονται για πρώτη φορά σε διε-

---

[56] Η Σύμβαση έχει υπογραφεί ως σήμερα από τις ακόλουθες χώρες:
2001: Αλβανία, Αρμενία, Αυστρία, Βέλγιο, Βουλγαρία, Κροατία, Κύπρο, Εσθονία, Φιλανδία, Γαλλία, Γερμανία, Ελλάδα, Ουγγαρία, Ισλανδία, Ιταλία, Μολδαβία, Ολλανδία, Νορβηγία, Πολωνία, Πορτογαλία, Ρουμανία, Ισπανία, Σουηδία, Ελβετία, Σκόπια, Ουκρανία, Αγγλία, Καναδά, Ιαπωνία, Νότια Αφρική, Η.Π.Α.
2002: Ιρλανδία, Μάλτα, Σλοβενία. 2003: Δανία, Λιθουανία, Λουξεμβούργο. 2004: Λετονία.
2005: Βοσνία-Ερζεγοβίνη, Τσεχία, Σερβία, Σλοβακία, Μαυροβούνιο.
Ο αριθμός των χωρών που έχουν εναρμονίσει την εθνική τους νομοθεσία σύμφωνα με τις επιταγές της Σύμβασης: Αλβανία (2004), Βοσνία - Ερζεγοβίνη (2006), Βουλγαρία (2005), Κροατία (2004), Κύπρος (2005), Δανία (2005), Εσθονία (2004), Γαλλία (2006), Ουγγαρία (2004), Λιθουανία (2004), Νορβηγία (2006), Ρουμανία (2004), Σλοβενία (2005), Σκόπια (2005) και Ουκρανία (2006). **Στην Ελλάδα αναμένεται να τεθεί σε ισχύ.**

[57] Βλαχόπουλος Κ. (2007) όπ. παρ., σελ. 142-144.

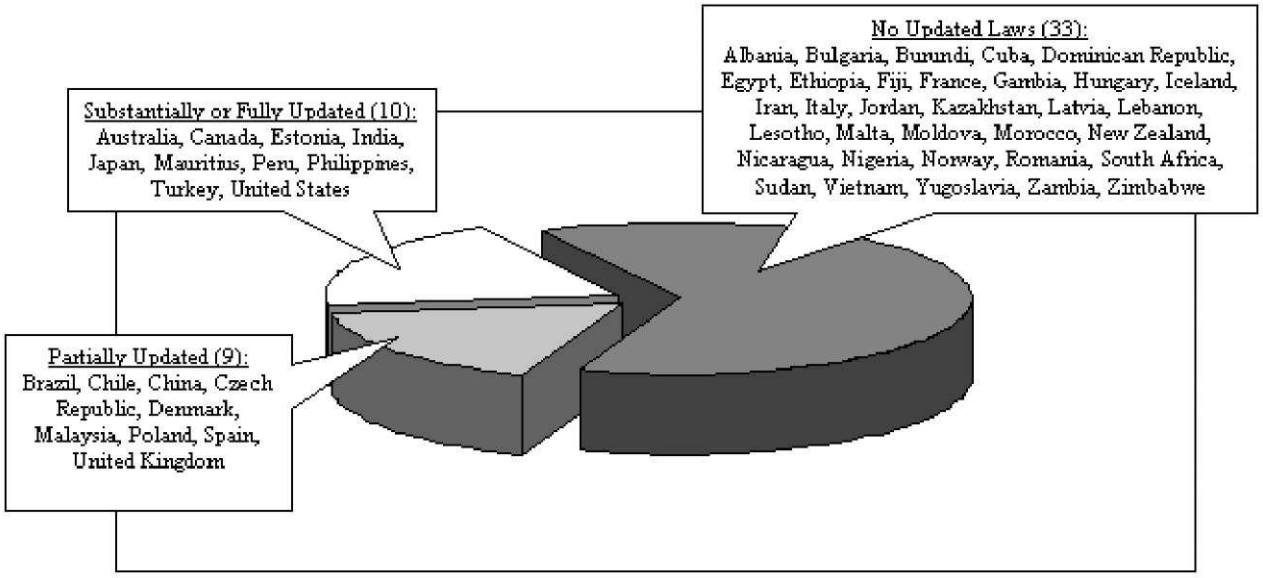
θνές νομικό κείμενο, οι γενικές δικονομικές αρχές που πρέπει να ισχύουν κατά την έρευνα των ηλεκτρονικών εγκλημάτων.

4. [58]Το Ψήφισμα του Συμβουλίου με αριθμό 2003/ C 48/01, για την ασφάλεια των δικτύων και των πληροφοριών.
5. Το Ψήφισμα 97/C70/01 του Συμβουλίου και το άρθρο 2 της Σύμβασης της Europol (ν. 2605/1998).
6. Η Σύσταση του Συμβουλίου με αριθμό 95/144/ΕΚ, όπου αναφέρονται οι προτροπές του Συμβουλίου σχετικά με την ασφάλεια των συστημάτων πληροφορικής.
7. Η Κοινή θέση της 27ης Μαΐου 1999 (1999/364/ΔΕΥ), όπου τα κράτη μέλη υποστηρίζουν την κατάρτιση του σχεδίου σύμβασης του Συμβουλίου της Ευρώπης σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και ότι φροντίζουν ώστε να περιληφθούν στη σύμβαση διατάξεις που θα διευκολύνουν την αποτελεσματική διερεύνηση και δίωξη εγκλημάτων που άπτονται των ηλεκτρονικών συστημάτων και δεδομένων.
8. Το Ψήφισμα του Συμβουλίου με αριθμό 2002/C 43/02 για κοινή προσέγγιση και ειδικές δράσεις στον τομέα της ασφάλειας των πληροφοριών και των δικτύων.
9. Το έγγραφο με αριθμό 2000/C 124/01 σχετικά με τη στρατηγική της Ευρωπαϊκής Ένωσης για την πρόληψη και τον έλεγχο του οργανωμένου εγκλήματος. Στο έγγραφο αυτό αναλύονται διεξοδικά τα μέτρα που πρέπει να ληφθούν για την πρόληψη και την καταπολέμηση του οργανωμένου εγκλήματος όπου εντάσσονται και πολλές μορφές του ηλεκτρονικού εγκλήματος.
10. Το Σχέδιο Δράσης με αριθμό 97/C 251/01 για την καταπολέμηση του οργανωμένου εγκλήματος.

Διεθνώς επικρατεί ανάλογος αναβρασμός, σύμφωνα και με τα αποτελέσματα έρευνας που τιτλοφορείται «Cyber Crime... and Punishment»[59] και διεξήχθη το Δεκέμβριο του 2000 από την εταιρεία 'McConnell International' σε 52 χώρες. Κατεδείχθη λοιπόν ότι 33 από τις 52 χώρες δεν έχουν ακόμη προβεί σε κανενός είδους τροποποίηση της νομοθεσίας τους, προκειμένου να διώκονται κάποια από τα αδικήματα που τελούνται στον κυβερνοχώρο

[58] Βλ. Αργυρόπουλος Α. , «Ηλεκτρονική εγκληματικότητα» ,
[59] http://www.mcconnellinternational.com/services/cybercrime.htm

Figure 1: Extent of Progress on Updating Cyber Crime Laws



Οι Φιλιππίνες είναι η μόνη χώρα της οποίας η νομοθεσία έχει τροποποιηθεί, έτσι ώστε να αντιμετωπίζει ως ποινικό αδίκημα και τους δέκα τύπους εγκλημάτων στον κυβερνοχώρο. Στις ΗΠΑ δεν διώκεται ποινικά η πλαστογραφία και στην Ιαπωνία από την τσιμπίδα του νόμου ξεφεύγει η διασπορά ιών. Αξίζει να σημειωθεί ότι, ακόμη και όταν η νομοθεσία προβλέπει νομική δίωξη των κυβερνοεγκλημάτων, οι ποινές που ορίζονται δεν είναι ικανές να αποτρέψουν τα αδικήματα αυτά.

5.3.1 ΚΟΙΝΟΤΙΚΗ ΟΔΗΓΙΑ 95/46/ΕΕ

Η Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών έχει διπλό στόχο: την προστασία των θεμελιωδών δικαιωμάτων και της ιδιωτικής ζωής του ατόμου και την εξασφάλιση της ελεύθερης κυκλοφορίας των προσωπικών δεδομένων στα κράτη μέλη της Ευρωπαϊκής Ένωσης, για την επίτευξη οικονομικής και κοινωνικής προόδου και συνεργασίας, καθώς και τεχνικής και επιστημονικής συνεργασίας στην ολοένα αναπτυσσόμενη κοινωνία της πληροφορικής και των τηλεπικοινωνιών.Η Οδηγία 95/46/ΕΚ αποτελεί το κείμενο αναφοράς, σε ευρωπαϊκό επίπεδο, στα θέματα προστασίας των δεδομένων προσωπικού χαρακτήρα. Θεσπίζει ένα κανονιστικό πλαίσιο που αποσκοπεί στην εγκαθίδρυση μιας ισορροπίας μεταξύ ενός υψηλού επιπέδου προστασίας της ιδιωτικής ζωής των προσώπων και της ελεύθερης κυκλοφορίας των δεδομένων προσωπικού χαρακτήρα στην Ευρωπαϊκή Ένωση. Η εν λόγω Οδηγία ορίζει ως «δεδομένα προσωπικού χαρακτήρα» κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί το πρόσωπο στο οποίο αναφέρονται τα δεδομένα.Οι διατάξεις της παρούσας οδηγίας εφαρμόζονται στην αυτοματοποιημένη, εν όλο ή εν μέρει, επεξεργασία δεδομένων προσωπικού χαρακτήρα

(π.χ. πληροφοριακή βάση δεδομένων πελατών).

Κάθε κράτος μέλος εφαρμόζει τις εθνικές διατάξεις που θεσπίζει δυνάμει της παρούσας οδηγίας σε κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα, εφόσον η επεξεργασία εκτελείται στα πλαίσια των δραστηριοτήτων υπευθύνου εγκατεστημένου στο έδαφος του κράτους μέλους. Συνεπώς η Ελλάδα είναι υπεύθυνη για την προστασία των δεδομένων προσωπικού χαρακτήρα που επεξεργάζονται οι οργανισμοί ηλεκτρονικού εμπορίου που είναι εγκατεστημένοι στα γεωγραφικά όρια της Ελλάδας. Στη συνέχεια ακολουθούν κάποιες γενικές προϋποθέσεις, που ορίζει η Οδηγία 95/46/ΕΚ, σχετικά με τη θεμιτή επεξεργασία δεδομένων προσωπικού χαρακτήρα:

Αρχές που Πρέπει να Τηρούνται ως Προς την Ποιότητα των Δεδομένων

Τα κράτη μέλη καθορίζουν τις προϋποθέσεις υπό τις οποίες η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι σύννομη. Προβλέπεται ότι τα δεδομένα προσωπικού χαρακτήρα πρέπει να υφίστανται σύννομη και θεμιτή επεξεργασία και να συλλέγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς και η μεταγενέστερη επεξεργασία τους να συμβιβάζεται με τους σκοπούς αυτούς. Θα πρέπει εξάλλου τα δεδομένα αυτά να είναι ακριβή και, αν χρειάζεται, να ενημερώνονται.

Βασικές Αρχές της Νόμιμης Επεξεργασίας Δεδομένων

Τα κράτη μέλη προβλέπουν ότι επεξεργασία δεδομένων προσωπικού χαρακτήρα μπορεί να γίνεται μόνον εάν το πρόσωπο στο οποίο αναφέρονται τα δεδομένα έχει δώσει τη ρητή συγκατάθεσή του ή αν η επεξεργασία είναι απαραίτητη:

1. Για την εκτέλεση σύμβασης της οποίας το υπόψη πρόσωπο αποτελεί συμβαλλόμενο μέρος.
2. Για την τήρηση νομικής υποχρέωσης στην οποία υπόκειται ο υπεύθυνος της επεξεργασίας.
3. Για τη διαφύλαξη ζωτικού συμφέροντος του υπόψη προσώπου.
4. Για την εκτέλεση αποστολής δημόσιου συμφέροντος.
5. Για την υλοποίηση του θεμιτού συμφέροντος που επιδιώκεται από τον υπεύθυνο της επεξεργασίας.

Ειδικές Κατηγορίες Επεξεργασίας

Τα κράτη μέλη απαγορεύουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνική καταγωγή, τις δημόσιες απόψεις, τις φιλοσοφικές ή θρησκευτικές πεποιθήσεις, τη συνδικαλιστική τοποθέτηση, καθώς και την επεξεργασία δεδομένων σχετικά με την υγεία και την ερωτική ζωή. Η διάταξη αυτή συνοδεύεται από επιφυλάξεις που αφορούν π.χ. την περίπτωση κατά την οποία η επεξεργασία είναι απαραίτητη για την υπεράσπιση των ζωτικών συμφερόντων του υπόψη προσώπου ή για σκοπούς προληπτικής ιατρικής και ιατρικής διάγνωσης.

- **Ενημέρωση του Ενδιαφερόμενου Προσώπου**

Τα κράτη μέλη προβλέπουν ότι ο υπεύθυνος της επεξεργασίας ή ο εκπρόσωπός του πρέπει να παρέχει στο πρόσωπο από το οποίο συλλέγονται δεδομένα που το αφορούν πληροφορίες για την ταυτότητα του υπευθύνου της επεξεργασίας, για τους σκοπούς της επεξεργασίας για την οποία προορίζονται τα δεδομένα καθώς και άλλες πληροφορίες, όπως για παράδειγμα τους αποδέκτες των δεδομένων κλπ.

- **Εξαιρέσεις και Περιορισμοί**

Τα κράτη μέλη μπορούν να περιορίζουν με νομοθετικά μέτρα την εμβέλεια των υποχρεώσεων και δικαιωμάτων που προβλέπονται στην παρούσα οδηγία όταν ο περιορισμός αυτός απαιτείται για τη διαφύλαξη της ασφάλειας του κράτους, της άμυνας, της δημόσιας ασφάλειας και της πρόληψης, διερεύνησης, διαπίστωσης και δίωξης παραβάσεων του ποινικού νόμου ή της δεοντολογίας των νομοθετικά κατοχυρωμένων επαγγελμάτων.

- **Απόρρητο και Ασφάλεια της Επεξεργασίας**

Κάθε πρόσωπο που ενεργεί υπό την εξουσία του υπευθύνου της επεξεργασίας δεν δύναται να επεξεργαστεί τα προσωπικά δεδομένα παρά κατόπιν εντολής του υπευθύνου επεξεργασίας. Εξάλλου, ο υπεύθυνος της επεξεργασίας θα πρέπει να εφαρμόζει τα ενδεδειγμένα μέτρα για την προστασία των δεδομένων προσωπικού χαρακτήρα έναντι τυχαίας ή παράνομης καταστροφής, τυχαίας απώλειας, αλλοίωσης, διάδοσης ή πρόσβασης χωρίς άδεια.

Τα κράτη μέλη προβλέπουν ότι κάθε πρόσωπο θα πρέπει να έχει τη δυνατότητα νομικής προσφυγής στην περίπτωση παραβίασης των δικαιωμάτων που εγγυώνται οι εθνικές διατάξεις οι οποίες ισχύουν για τη σχετική επεξεργασία δεδομένων. Εξάλλου, τα άτομα που έχουν υποστεί βλάβη λόγω μιας παράνομης επεξεργασίας των προσωπικών τους δεδομένων έχουν το δικαίωμα να επιτύχουν αποκατάσταση της ζημίας που υπέστησαν.

Επιτρέπονται οι μεταβιβάσεις δεδομένων προσωπικού χαρακτήρα από κράτος μέλος σε τρίτη χώρα, υπό την προϋπόθεση ότι η εν λόγω τρίτη χώρα διαθέτει το κατάλληλο επίπεδο προστασίας. Αντίθετα, οι εν λόγω μεταβιβάσεις δεν μπορούν να πραγματοποιηθούν προς τρίτες χώρες οι οποίες δεν διαθέτουν το κατάλληλο επίπεδο προστασίας, εκτός από συγκεκριμένες περιπτώσεις παρέκκλισης οι οποίες απαριθμούνται περιοριστικά.

Κάθε κράτος μέλος προβλέπει τη δημιουργίας μίας ή περισσότερων ανεξάρτητων κρατικών αρχών οι οποίες επιφορτίζονται με την εποπτεία της εφαρμογής, στο εθνικό έδαφος, των εθνικών διατάξεων που έχουν θεσπιστεί από τα κράτη μέλη, κατ' εφαρμογή της παρούσας οδηγίας.

5.3.2 ΚΟΙΝΟΤΙΚΗ ΟΔΗΓΙΑ 2002/58/Ε.Ε

Η Οδηγία 2002/58/ΕΚ αναθεωρεί και αναπροσαρμόζει την προηγούμενη Οδηγία 97/96/ΕΚ περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα, προκειμένου να ληφθούν υπόψη οι νέες υπηρεσίες και τεχνολογικές εξελίξεις. Η Οδηγία 2002/58/ΕΚ αποτελεί βασικό στοιχείο του κανονιστικού πλαισίου που επιδιώκει να εξασφαλίσει τη συνέχιση της ανάπτυξης του τομέα ηλεκτρονικών επικοινωνιών, με οφέλη για το σύνολο των εταιρειών και των ιδιωτών που χρησιμοποιούν τις υπηρεσίες ηλεκτρονικών επικοινωνιών..

Η εν λόγω Οδηγία επιβάλλει τη θέσπιση ειδικών νομικών και τεχνικών διατάξεων για την προστασία βασικών δικαιωμάτων και ελευθεριών. Η δυνατότητα προστασίας των δεδομένων προσωπικού χαρακτήρα των χρηστών αποτελεί προϋπόθεση για την ανάπτυξη του ηλεκτρονικού εμπορίου. Με την Οδηγία 2002/58/ΕΚ εναρμονίζονται οι διατάξεις των κρατών μελών οι οποίες απαιτούνται προκειμένου να διασφαλίζεται ισοδύναμο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών, ιδίως το δικαίωμα στην ιδιωτική ζωή, όσον αφορά την επεξεργασία προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, καθώς και να διασφαλίζεται η ελεύθερη κυκλοφορία των δεδομένων αυτών και των εξοπλισμών και υπηρεσιών ηλεκτρονικών επικοινωνιών στην Ευρωπαϊκή Ένωση.

(Για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών)

Η Οδηγία 2002/58/ΕΚ αναθεωρεί και αναπροσαρμόζει την προηγούμενη Οδηγία 97/96/ΕΚ περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα, προκειμένου να ληφθούν υπόψη οι νέες υπηρεσίες και τεχνολογικές εξελίξεις. Η Οδηγία 2002/58/ΕΚ αποτελεί βασικό στοιχείο του κανονιστικού πλαισίου που επιδιώκει να εξασφαλίσει τη συνέχιση της ανάπτυξης του τομέα ηλεκτρονικών επικοινωνιών, με οφέλη για το σύνολο των εταιρειών και των ιδιωτών που χρησιμοποιούν τις υπηρεσίες ηλεκτρονικών επικοινωνιών.

Η εν λόγω Οδηγία επιβάλλει τη θέσπιση ειδικών νομικών και τεχνικών διατάξεων για την προστασία βασικών δικαιωμάτων και ελευθεριών. Η δυνατότητα προστασίας των δεδομένων προσωπικού χαρακτήρα των χρηστών αποτελεί προϋπόθεση για την ανάπτυξη του ηλεκτρονικού εμπορίου. Με την Οδηγία 2002/58/ΕΚ εναρμονίζονται οι διατάξεις των κρατών μελών οι οποίες απαιτούνται προκειμένου να διασφαλίζεται ισοδύναμο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών, ιδίως το δικαίωμα στην ιδιωτική ζωή, όσον αφορά την επεξεργασία προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, καθώς και να διασφαλίζεται η ελεύθερη κυκλοφορία των δεδομένων αυτών και των εξοπλισμών και υπηρεσιών ηλεκτρονικών επικοινωνιών στην Ευρωπαϊκή Ένωση.

Η Οδηγία λοιπόν για την προστασία προσωπικών δεδομένων στηρίζεται στις εξής βασικές αρχες :

- Η επεξεργασία προσωπικών δεδομένων πρέπει να είναι πάντοτε θεμιτή και νόμιμη.
- Τα προσωπικά δεδομένα πρέπει πάντα να συλλέγοντας για ρητώς καθορισμένους και νόμιμους σκοπούς και να χρησιμοποιούνται ανάλογα.
- Τα προσωπικά δεδομένα πρέπει να είναι κατάλληλα και να μην υπερβαίνουν τα απολύτως αναγκαία για τους σκοπούς της επεξεργασίας τους

- Τα δεδομένα που αποκαλύπτουν την ταυτότητα των προσώπων δεν πρέπει να φυλάσσονται για περισσότερο χρόνο απ' όσο είναι απαραίτητο
- Τα δεδομένα πρέπει να είναι ακριβή και, όπου χρειάζεται, να ενημερώνονται
- Οι κάτοχοι δεδομένων οφείλουν να παρέχουν στα πρόσωπα που αφορούν τα δεδομένα αυτά εύλογα μέσα για τη διόρθωση, τη διαγραφή ή τη δέσμευση ανακριβών δεδομένων
- Πρέπει να λαμβάνονται τα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα για την αποτροπή της παράνομης ή χωρίς άδεια επεξεργασίας προσωπικών δεδομένων
- Τα προσωπικά δεδομένα δεν πρέπει να μεταφέρονται σε χώρες ή επικράτειες εκτός του Ευρωπαϊκού Οικονομικού Χώρου, εκτός εάν αυτές εγγυώνται "επαρκές επίπεδο προστασίας" για τα πρόσωπα που αφορούν τα δεδομένα

Η οδηγία επιβάλλει επίσης στα κράτη μέλη την υποχρέωση να συστήσουν μία η περισσότερες ανεξάρτητες εποπτικές Αρχές για να παρακολουθούν την εφαρμογή της. Ένα από τα καθήκοντα αυτών των Αρχών είναι να τηρούν ενημερωμένο δημόσιο μητρώο, ώστε το κοινό να μπορεί να γνωρίζει τα ονόματα όλων των κατόχων προσωπικών δεδομένων και το είδος της επεξεργασίας στην οποία τα υποβάλλουν. Επίσης ο φορέας παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, οφείλει να λαμβάνει από κοινού με τους φορείς παροχής δημόσιων δικτύων επικοινωνιών, καθόσον αφορά την ασφάλεια του δικτύου, τα ενδεδειγμένα τεχνικά και οργανωτικά μέσα προκειμένου να προστατεύεται η ασφάλεια των υπηρεσιών του. Οι εν λόγω φορείς υποχρεώνονται να ενημερώνουν τους συνδρομητές σε περίπτωση που υπάρχει ιδιαίτερος κίνδυνος για την ασφάλεια του δικτύου.

Απόρρητο των Επικοινωνιών

Το απόρρητο των επικοινωνιών που διενεργούνται μέσω δημόσιου δικτύου επικοινωνιών και των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, αποτελεί βασικό δικαίωμα του πολίτη και ως τέτοιο κατοχυρώνεται από την εκάστοτε ισχύουσα εθνική νομοθεσία.

Γενικά, στο πλαίσιο της διασφάλισης του απορρήτου απαγορεύεται η ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των επικοινωνιών και των συναφών δεδομένων κίνησης από πρόσωπα πλην των χρηστών, χωρίς τη συγκατάθεση των ενδιαφερόμενων χρηστών, εκτός αν υπάρχει σχετική νόμιμη άδεια (π.χ. για περιπτώσεις της δημόσιας ασφάλειας).

Η πιο πάνω απαγόρευση δεν επηρεάζει οποιαδήποτε επιτρεπόμενη από το νόμο καταγραφή συνδιαλέξεων όταν πραγματοποιούνται κατά τη διάρκεια νόμιμης επαγγελματικής πρακτικής με σκοπό την παροχή αποδεικτικών στοιχείων μιας εμπορικής συναλλαγής.

5.4 ΠΑΓΚΟΣΜΙΑ ΝΟΜΟΘΕΣΙΑ

5.4.1 Ηνωμένες Πολιτείες Αμερικής

Το πρώτο νομοθέτημα σχετικά με το ηλεκτρονικό έγκλημα θεσπίστηκε στις Ηνωμένες Πολιτείες

της Αμερικής, το 1984. Ο νόμος 'Computer Fraud and Abuse Act[60]', προσπάθησε, ανεπιτυχώς θα λέγαμε, 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 Η.Π. Α.

Τα προβλήματα αυτά, οδήγησαν πολύ γρήγορα στην πρώτη αναθεώρηση61, 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..». 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 αναφέρονταν μόνο σε κρατικά υπολογιστικά συστήματα.

Η πιο σημαντική τροποποίηση του νομοθετήματος αυτού έγινε το 1994, η οποία επέφερε αλλαγές σε τρία σημαντικά σημεία:

α) η ισχύς του νομοθετικού πλαισίου επεκτάθηκε και σε ηλεκτρονικού υπολογιστές, που χρησιμοποιούνται στο διαπολιτειακό εμπόριο

β) αφαιρέθηκε ο όρος, «μη εξουσιοδοτημένη πρόσβαση», που σημαίνει ότι οι υπάλληλοι εταιρειών και οι εξουσιοδοτημένοι χρήστες θα μπορούσαν να διωχθούν και γ) συγκεκριμένες μορφές επικίνδυνων και σκόπιμων ενεργειών θεωρούνταν, πλέον, παράνομες, όπως η διασπορά κακόβουλου λογισμικού.

Τέλος, το 1996, συμπληρώθηκε ο νόμος αυτός με τη National Information Infrastructure Protection Act, 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 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 Η.Π.Α.

Εκτός των ανωτέρω, 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 Η.Π.Α, αποτελεί τη μεγαλύτερη πληγή του δικαϊκού συστήματος.

---

[60] http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act

[61] Συνολικά πραγματοποιήθηκαν 8 αναθεωρήσεις έως το 1996.

5.4.2 Αυστραλία

Η Αυστραλία είναι η χώρα που έχει δώσει τη μεγαλύτερη, μετά τις Η.Π.Α, προσοχή στην αντιμετώπιση του ηλεκτρονικού εγκλήματος. Ο νόμος 'Crime Act 1914' προβλέπει τέσσερις βασικές μορφές ηλεκτρονικού εγκλήματος:

Παράνομη πρόσβαση σε δεδομένα αποθηκευμένα σε κρατικό ηλεκτρονικό υπολογιστή.

Καταστροφή δεδομένων αποθηκευμένων σε κρατικό ηλεκτρονικό υπολογιστή.

Πρόσβαση σε δεδομένα αποθηκευμένα σε ηλεκτρονικό υπολογιστή χρησιμοποιώντας μέσα κρατικής διευκόλυνσης.

Καταστροφή δεδομένων σε ηλεκτρονικό υπολογιστή χρησιμοποιώντας μέσα κρατικής διευκόλυνσης.

Ο νόμος, που σήμερα είναι σε ισχύ στην Αυστραλία, αναφέρεται ως 'The Cybercrime Act 2001'[62], 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:

Μη εξουσιοδοτημένη πρόσβαση, μετατροπή και φθορά δεδομένων, με σκοπό τη διάπραξη σοβαρού εγκλήματος. Στην περίπτωση αυτή, η ποινή είναι ισοδύναμη της αντίστοιχης που επιβάλλεται στο συμβατικό έγκλημα.

Μη εξουσιοδοτημένη τροποποίηση δεδομένων, που οδηγεί σε φθορά δεδομένων.

Μη εξουσιοδοτημένη φθορά ηλεκτρονικών επικοινωνιών, για την οποία προβλέπεται ποινή έως δέκα ετών.

Παράλληλα, ο νόμος δημιούργησε τέσσερις νέες μορφές εγκλημάτων:

Μη εξουσιοδοτημένη πρόσβαση ή μετατροπή προστατευομένων δεδομένων.

Παράνομη καταστροφή δεδομένων αποθηκευμένων σε δίσκους Η/Υ.

Κατοχή ή έλεγχος δεδομένων, με σκοπό τη διάπραξη ηλεκτρονικών αδικημάτων.

> Παραγωγή, προμήθεια ή απόκτηση δεδομένων, με σκοπό τη διάπραξη ηλεκτρονικού εγκλήματος.

Στο νόμο περιλαμβάνονται ακόμη, διατάξεις για τον τρόπο έρευνας ηλεκτρονικών αδικημάτων από τις διωκτικές αρχές και τις μεθόδους εξέτασης δεδομένων, που είναι αποθηκευμένα σε η-λεκτρονικά μέσα.

5.4.3 Κίνα[63]

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 5.000 έως 15.000 γιεν, ανάλογα με τη σοβαρότητα του εγκλήματος.

Εξαιρετικό ενδιαφέρον παρουσιάζουν ορισμένες διατάξεις της νομοθεσίας στην Κίνα, τις οποίες

---

[62] http://www.findlaw.com.au/article/1408.htm
[63] http://www.cecar.info/category5.html

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

5.4.4 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».

α) Organization for Economic Cooperation and Development (OECD)[64]

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

β) Οργανισμός Ηνωμένων Εθνών[65]

Τα Ηνωμένα Έθνη παρουσίασαν ένα ψήφισμα, σχετικά με τη νομοθεσία για το ηλεκτρονικό έγκλημα, στο 8ο Συνέδριο για την Πρόληψη του Εγκλήματος και την Μεταχείριση των Παραβατών. Το Εγχειρίδιο για την Πρόληψη και τον Έλεγχο του Ηλεκτρονικού Εγκλήματος εκδόθηκε το 1994. Το Εγχειρίδιο αυτό αντιμετωπίζει συνολικά το ζήτημα του ηλεκτρονικού εγκλήματος παρουσιάζοντας την έκταση του 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 έκδοση 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.

γ) Ομάδα των Οκτώ - Group of Eight (08)[66]

Οι οκτώ ισχυρότερες χώρες του κόσμου, δημιούργησαν το 1997 μια Υποομάδα για το Έγκλημα

---

64 http://www.oecd.org/home/0,2987,en_2649_201185_1_1_1_1_1,00.html

65 http://www.un.org/en/

66 http://www.go8.edu.au/

Υψηλής Τεχνολογίας. Η Υποομάδα αυτή σε μια συνάντηση που πραγματοποιήθηκε τον ίδιο χρόνο στην Ουάσινγκτον, με τη συμμετοχή των υπουργών Εσωτερικών και Δικαιοσύνη των οκτώ χωρών, κατέληξε σε *«Δέκα Αρχές»* και *«Δέκα Τομείς Δράσης»* για την αντιμετώπιση του ηλεκτρονικού εγκλήματος. Οι αρχές αυτές είχαν ως σκοπό τη διασφάλιση της ενιαίας αντιμετώπισης του εγκληματικού φαινομένου, σε όλες τις χώρες του κόσμου.

Web Page Source Code

Main Page

Source Code

```
<html xmlns="http://www.w3.org/1999/xhtml">

<head>

<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-7" />

<title>Crime on the internet...</title>

<meta name="Keywords" content="" />

<meta name="Description" content="" />

<link href="default.css" rel="stylesheet" type="text/css" />

</head>


<body>

<div id="header">

        <h1><center>Cybercrime</center></h2>

        <ul>
```

```
                <li><a href="index.php">Αρχική</a></li>
                <li><a href="cybercrime.php">Cybercrime</a></li>
                <li><a href="hackers.php">Hackers</a></li>
                <li><a href="law.php">Νομοθεσία</a></li>
          <li><a href="links.php">Χρήσιμοι Σύνδεσμοι</a></li>
                <li><a href="contact.php">Επικοινωνία</a></li>
        <br><br><br>
          </ul>
</div>
<div id="content">


          <div id="colTwo">
                <div class="bg2">
                      <h2><em>Εισαγωγή</h2>
                      <p><img src="images/img5.jpg" alt="" class="image" /></p>
                      <p>
```

Η τεχνολογική έκρηξη την τελευταία δεκαετία μας έφερε όλους ποιό κοντά στον παγκόσμιο ιστό και στην χρήση του υπολογιστη ως

εργαλείο που ικανοποιεί τις περισσότερες ανάγκες μας όπως η ηλεκτρονική υποβολή δηλώσεων στην εφορία(www.taxisnet.gr) ,

πραγματοποίηση online τραπεζικών συναλλαγών (http://www.atebank.gr/ATEbank/WebBanking/Retail , https://secure.alpha.gr) ,

αγόρες απο ηλεκτρονικά καταστήματα στην Ελλάδα ή στο εξωτερικό (www.e-shop.gr , www.amazon.com) ,

συμμετοχή σε δημοπρασίες σε πραγματικό χρόνο (www.e-bay.com www.ricardo.gr , http://www.bidbang.com).

Άρα, με την ανάπτυξη του διαδικτύου και της τεχνολογίας, έχουμε και άνθιση νέου είδους εγκληματικότητας που αναπτύσσεται

με την χρήση της ψηφιακής τεχνολογίας και των ηλεκτρονικών υπολογιστών.

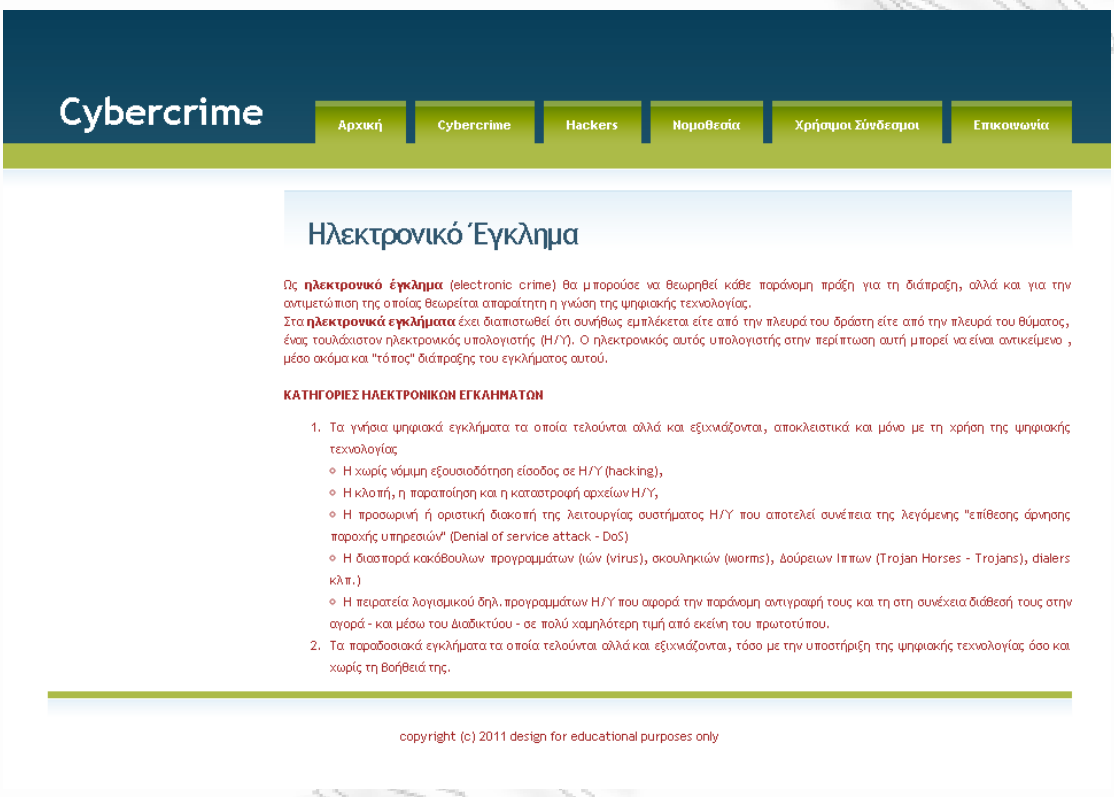
Ετσι αναπτύχθηκε και το αντίστοιχο νομικό πλαίσιο που μας προστατεύει απο τέτοιου είδους εγκλήματα.

Στην παρούσα μεταπτυχιακή διατριβή θα δούμε και θα αναλύσουμε πως μπορούμε να προστατευτούμε από τέτοιου είδους εγκλήματα

και πως προστατευόμαστε απο νομικής πλευράς.

```
                    </p>
                </div>
            </div>
</div>
<div id="footer">
            <p>Copyright (c) 2011  Design for educational purposes only</p>
</div>
</body>
</html>
```

Cybercrime



Source Code

```
<html xmlns="http://www.w3.org/1999/xhtml">

<head>

<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-7" />

<title>Crime on the internet...</title>

<meta name="Keywords" content="" />

<meta name="Description" content="" />

<link href="default.css" rel="stylesheet" type="text/css" />
```

```
</head>
<body>
<div id="header">
<h1><center>Cybercrime</center></h2>
        <ul>
                <li><a href="index.php">Αρχική</a></li>
                <li><a href="cybercrime.php">Cybercrime</a></li>
                <li><a href="hackers.php">Hackers</a></li>
                <li><a href="law.php">Νομοθεσία</a></li>
         <li><a href="links.php">Χρήσιμοι Σύνδεσμοι</a></li>
                <li><a href="contact.php">Επικοινωνία</a></li>
       <br><br><br>
        </ul>
</div>
<div id="content">
        <div id="colOne">
        </div>
        <div id="colTwo">
                <div class="bg2">
                        <h2>Ηλεκτρονικό Έγκλημα</h2>
                </div>
                        Ως <b>ηλεκτρονικό έγκλημα </b>(electronic crime) θα μπορούσε να
θεωρηθεί κάθε παράνομη πράξη για τη διάπραξη,
αλλά και για την αντιμετώπιση της οποίας θεωρείται απαραίτητη η γνώση της ψηφιακής
τεχνολογίας.<br> Στα <b>ηλεκτρονικά εγκλήματα </b>έχει διαπιστωθεί ότι συνήθως
εμπλέκεται είτε από την πλευρά του δράστη είτε από την πλευρά του θύματος,
```

ένας τουλάχιστον ηλεκτρονικός υπολογιστής (Η/Υ). Ο ηλεκτρονικός αυτός υπολογιστής στην περίπτωση αυτή μπορεί να είναι αντικείμενο ,

μέσο ακόμα και "τόπος" διάπραξης του εγκλήματος αυτού.

ΚΑΤΗΓΟΡΙΕΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΓΚΛΗΜΑΤΩΝ

Τα γνήσια ψηφιακά εγκλήματα τα οποία τελούνται αλλά και εξιχνιάζονται,

αποκλειστικά και μόνο με τη χρήση της ψηφιακής τεχνολογίας

Η χωρίς νόμιμη εξουσιοδότηση είσοδος σε Η/Υ (hacking),

Η κλοπή, η παραποίηση και η καταστροφή αρχείων Η/Υ,

Η προσωρινή ή οριστική διακοπή της λειτουργίας συστήματος Η/Υ που αποτελεί συνέπεια της λεγόμενης

"επίθεσης άρνησης παροχής υπηρεσιών" (Denial of service attack - DoS)

Η διασπορά κακόβουλων προγραμμάτων (ιών (virus), σκουληκιών (worms), Δούρειων Ιππων

(Trojan Horses - Trojans), dialers κλπ.)

Η πειρατεία λογισμικού δηλ.προγραμμάτων Η/Υ που αφορά την παράνομη αντιγραφή τους και τη στη συνέχεια διάθεσή τους

στην αγορά - και μέσω του Διαδικτύου - σε πολύ χαμηλότερη τιμή από εκείνη του πρωτοτύπου.

 Τα παραδοσιακά εγκλήματα τα οποία τελούνται αλλά και εξιχνιάζονται, τόσο με την υποστήριξη της ψηφιακής τεχνολογίας όσο και χωρίς τη βοήθειά της.

 Copyright (c) 2011 Design for educational purposes only </body></html>

Hackers

Source Code

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-7" />
<title>Crime on the internet...</title>
<meta name="Keywords" content="" />
<meta name="Description" content="" />
<link href="default.css" rel="stylesheet" type="text/css" />
</head>
<body>
```

```
<div id="header">
        <h1><center>Cybercrime</center></h1>
        <ul>
                <li><a href="index.php">Αρχική</a></li>
                <li><a href="cybercrime.php">Cybercrime</a></li>
                <li><a href="hackers.php">Hackers</a></li>
                <li><a href="law.php">Νομοθεσία</a></li>
         <li><a href="links.php">Χρήσιμοι Σύνδεσμοι</a></li>
                <li><a href="contact.php">Επικοινωνία</a></li>
       <br><br><br>
        </ul>
</div>
<div id="content">
        <div id="colOne">
        </div>
        <div id="colTwo">
                <div class="bg2">
                        <h2>Hackers</h2>
                </div>
                Ο <b>Hacker </b>ενδιαφέρεται για τις μυστικές και ενίοτε κρυφές λειτουργίες
ενός λειτουργικού συστήματος,
                  προσπαθώντας να ανακαλύψει τα κενά στα συστήματα υπολογιστών καθώς
και τους λόγους ύπαρξής τους.
```

Αναζητά συνέχεια πρόσθετες γνώσεις και μοιράζεται ελεύθερα ότι έχει ανακαλύψει στο διαδίκτυο,

χωρίς να καταστρέφει δεδομένα σκοπίμως.

Οι περισσότεροι από αυτούς τους hackers δεν έχουν τόσο απίστευτες γνώσεις και χρησιμοποιούν ορισμένα απλά εργαλεία για να κάνουν την

πλάκα τους ή να εκθέσουν δημόσια πρόσωπα και να διεκδικήσουν μια θέση στο πάνθεον της διασημότητας.

ΚΑΤΗΓΟΡΙΕΣ HACKERS

White hat hackers :Ατομα που τους αρέσει να σπάνε την ασφάλεια συστημάτων για όχι κακόβουλους σκοπούς.

Τους αρέσει η γνώση, το να κατανοούν πως λειτουργεί κάποιο πρόγραμμα ή μηχανισμός.
</br>

Crackers ή Black hat hackers:Οι crackers (criminal hackers) θεωρούνται ως οι κακόβουλοι hackers και έχουν ως στόχο την

πρόκληση ζημιάς σε δίκτυα υπολογιστών, την εισβολή σε υπολογιστές χρηστών χωρίς εξουσιοδότηση, την δημιουργία ιών,

την παραβίαση κωδικών ασφαλείας,

την καταστροφή ή και την αλλοίωση δικτυακών τόπων (Web sites) όπου αφήνουν

περήφανα την δικτυακή τους σφραγίδα με το ψευδώνυμό τους, την δημιουργία πειρατικών αντιγράφων

προγραμμάτων ή τραγουδιών ή βίντεο κ.ά.
</br>

Script kiddie:Είναι άτομα χωρίς πολλές γνώσεις, που χρησιμοποιούν έτοιμα προγράμματα για να κάνουν

επιθέσεις ή φιγούρα στους φίλους τους. Είναι άτομα που καλά καλά δεν χαρακτηρίζονται hackers.
</br>

Hacktivists ή νέο-hackers:Είναι άτομα που χρησιμοποιούν τις γνώσεις τους με σκοπό να πουν ή προωθήσουν μια κοινωνική,

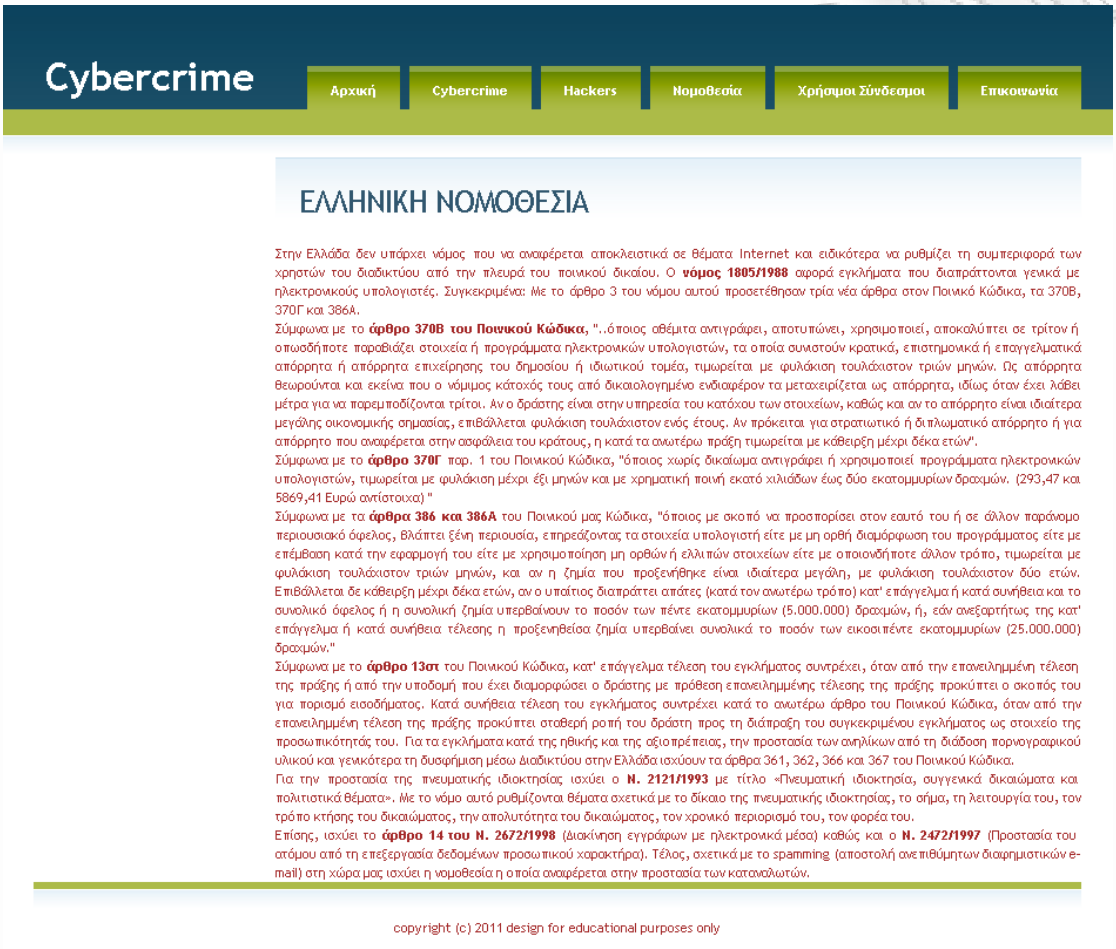
ιδεολογική, θρησκευτική ή πολιτική γνώμη. Στις περισσότερες περιπτώσεις καταστρέφουν την κεντρική σελίδα από γνωστά site ή

το αλλάζουν με σκοπό να γελοιοποιήσουν τον ιδιοκτήτη.

Σπάνια, χρησιμοποιούν τις γνώσεις τους στο όνομα της interneto-τρομοκρατίας.

Copyright (c) 2011 Design for educational purposes only </body></html>

Νομοθεσία



Source Code

```
<head>

<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-7" />

<title>Crime on the internet...</title>

<meta name="Keywords" content="" />

<meta name="Description" content="" />
```

```
<link href="default.css" rel="stylesheet" type="text/css" />
</head>
<body>
<div id="header">
        <h1><center>Cybercrime</center></h1>
        <ul>
                <li><a href="index.php">Αρχική</a></li>
                <li><a href="cybercrime.php">Cybercrime</a></li>
                <li><a href="hackers.php">Hackers</a></li>
                <li><a href="law.php">Νομοθεσία</a></li>
         <li><a href="links.php">Χρήσιμοι Σύνδεσμοι</a></li>
                <li><a href="contact.php">Επικοινωνία</a></li>
       <br><br><br>
        </ul>
</div>
<div id="content">
        <div id="colOne">
        </div>
        <div id="colTwo">
                <div class="bg2">
                        <h2>ΕΛΛΗΝΙΚΗ ΝΟΜΟΘΕΣΙΑ</h2>
        </div>
```

Στην Ελλάδα δεν υπάρχει νόμος που να αναφέρεται αποκλειστικά σε θέματα Internet και ειδικότερα να ρυθμίζει τη συμπεριφορά των χρηστών του διαδικτύου από την πλευρά του ποινικού δικαίου. Ο νόμος 1805/1988 αφορά εγκλήματα που διαπράττονται γενικά με ηλεκτρονικούς υπολογιστές. Συγκεκριμένα: Με το άρθρο 3 του νόμου αυτού προσετέθησαν τρία νέα άρθρα στον Ποινικό Κώδικα, τα 370Β, 370Γ και 386Α.
Σύμφωνα με το άρθρο 370Β του Ποινικού Κώδικα, "..όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα ηλεκτρονικών υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι. 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. Αν πρόκειται για στρατιωτικό ή διπλωματικό απόρρητο ή για απόρρητο που αναφέρεται στην ασφάλεια του κράτους, η κατά τα ανωτέρω πράξη τιμωρείται με κάθειρξη μέχρι δέκα ετών".

Σύμφωνα με το άρθρο 370Γ παρ. 1 του Ποινικού Κώδικα, "όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα ηλεκτρονικών υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μηνών και με χρηματική ποινή εκατό χιλιάδων έως δύο εκατομμυρίων δραχμών. (293,47 και 5869,41 Ευρώ αντίστοιχα) "

Σύμφωνα με τα άρθρα 386 και 386Α του Ποινικού μας Κώδικα, "όποιος με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον 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 άλλον τρόπο, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών, και αν η ζημία που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον δύο ετών. Επιβάλλεται δε κάθειρξη μέχρι δέκα ετών, αν ο υπαίτιος διαπράττει απάτες (κατά τον ανωτέρω τρόπο) κατ' επάγγελμα ή κατά συνήθεια και το συνολικό όφελος ή η συνολική ζημία υπερβαίνουν το ποσόν των πέντε εκατομμυρίων (5.000.000) δραχμών, ή, εάν ανεξαρτήτως της κατ' επάγγελμα ή κατά συνήθεια τέλεσης η προξενηθείσα ζημία υπερβαίνει συνολικά το ποσόν των εικοσιπέντε εκατομμυρίων (25.000.000) δραχμών."

Σύμφωνα με το άρθρο 13στ του Ποινικού Κώδικα, κατ' επάγγελμα τέλεση του εγκλήματος συντρέχει, όταν από την επανειλημμένη τέλεση της πράξης ή από την υποδομή που έχει διαμορφώσει ο δράστης με πρόθεση επανειλημμένης τέλεσης της πράξης προκύπτει ο σκοπός του για πορισμό εισοδήματος. Κατά συνήθεια τέλεση του εγκλήματος συντρέχει κατά το ανωτέρω άρθρο του Ποινικού Κώδικα, όταν από την επανειλημμένη τέλεση της

πράξης προκύπτει σταθερή ροπή του δράστη προς τη διάπραξη του συγκεκριμένου εγκλήματος ως στοιχείο της προσωπικότητάς του.

Για τα εγκλήματα κατά της ηθικής και της αξιοπρέπειας, την προστασία των ανηλίκων από τη διάδοση πορνογραφικού υλικού και γενικότερα τη δυσφήμιση μέσω Διαδικτύου στην Ελλάδα ισχύουν τα άρθρα 361, 362, 366 και 367 του Ποινικού Κώδικα.

Για την προστασία της πνευματικής ιδιοκτησίας ισχύει ο Ν. 2121/1993 με τίτλο «Πνευματική ιδιοκτησία, συγγενικά δικαιώματα και πολιτιστικά θέματα». Με το νόμο αυτό ρυθμίζονται θέματα σχετικά με το δίκαιο της πνευματικής ιδιοκτησίας, το σήμα, τη λειτουργία του, τον τρόπο κτήσης του δικαιώματος, την απολυτότητα του δικαιώματος, τον χρονικό περιορισμό του, τον φορέα του.

Επίσης, ισχύει το άρθρο 14 του Ν. 2672/1998 (Διακίνηση εγγράφων με ηλεκτρονικά μέσα) καθώς και ο Ν. 2472/1997 (Προστασία του ατόμου από τη επεξεργασία δεδομένων προσωπικού χαρακτήρα).

Τέλος, σχετικά με το spamming (αποστολή ανεπιθύμητων διαφημιστικών e-mail) στη χώρα μας ισχύει η νομοθεσία η οποία αναφέρεται στην προστασία των καταναλωτών.

Copyright (c) 2011 Design for educational purposes only

</body>

</html>

Χρήσιμοι Σύνδεσμοι

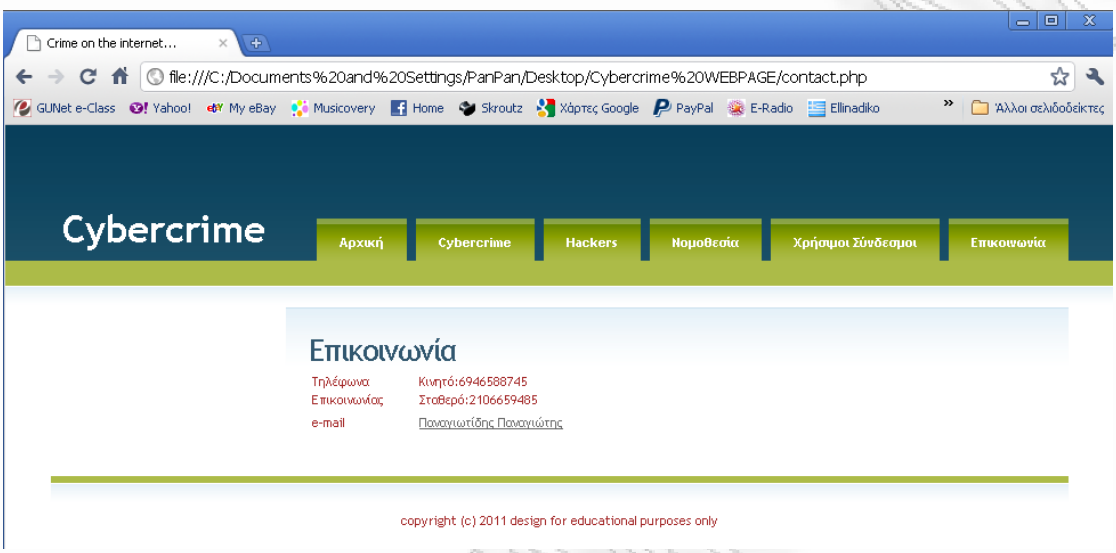
Source Code

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-7" />
<title>Crime on the internet...</title>
<meta name="Keywords" content="" />
<meta name="Description" content="" />
<link href="default.css" rel="stylesheet" type="text/css" />
</head>
<body>
<div id="header">
        <h1><center>Cybercrime</center></h1>
        <ul>
                <li><a href="index.php">Αρχική</a></li>
                <li><a href="cybercrime.php">Cybercrime</a></li>
```

```
                <li><a href="hackers.php">Hackers</a></li>
                <li><a href="law.php">Νομοθεσία</a></li>
            <li><a href="links.php">Χρήσιμοι Σύνδεσμοι</a></li>
                <li><a href="contact.php">Επικοινωνία</a></li>
        <br><br><br>
        </ul>
</div>
<div id="content">
        <div id="colOne">
        </div>
        <div id="colTwo">
                <div class="bg2">
                        <h2>Χρήσιμοι Σύνδεσμοι</h2>
                </div>
        <ul>
                <li><a href="http://www.comodo.com/products/free-
products.php">Antivirus</a> </li>
                <li><a href="http://www.malwarebytes.org/">Antispyware-malware</a></li>
                <li>Για να κατεβάσετε την Ετήσια Έκθεση σχετικά με την πειρατεία λογισμικού
πατήστε
                <a
href="http://portal.bsa.org/globalpiracy2010/downloads/study_pdf/2010_BSA_Piracy_Study-
Standard.pdf">εδώ</a></li>
```

```
        <li><a
href="http://www.bsa.org/sitecore/shell/Controls/Rich%20Text%20Editor/~/media/Files/idc_studies/bsa_idc_greece_final%20pdf.ashx">

            Οικονομικά οφέλη για την Ελλάδα</a> από την καταπωλέμηση της πειρατείας λογισμικού</li>

</ul>

        </div>

</div>

<div id="footer">

        <p>Copyright (c) 2011  Design for educational purposes only</p>

</div></body></html>
```

Επικοινωνία



Source Code

```
<body>

<div id="header">

<h1><center>Cybercrime</center></h2>

        <ul>

                <li><a href="index.php">Αρχική</a></li>

                <li><a href="cybercrime.php">Cybercrime</a></li>

                <li><a href="hackers.php">Hackers</a></li>

                <li><a href="law.php">Νομοθεσία</a></li>

         <li><a href="links.php">Χρήσιμοι Σύνδεσμοι</a></li>

                <li><a href="contact.php">Επικοινωνία</a></li>
```

```
        <br><br><br>
          </ul>
</div>
<div id="content">
          <div id="colTwo">
                    <div class="bg2">
                              <h2>Επικοινωνία</h2>
<table border="0" width="500px">
<tr>
<td valign="top" width="90px">
Τηλέφωνα
<br>
Επικοινωνίας
</td>
<td valign="top">
Κινητό:6946588745<br>Σταθερό:2106659485
</td></tr><tr><td>e-mail</td>
<td align="left">
<a href="mailto:panagiotidispan@gmail.com">Παναγιωτίδης Παναγιώτης</a></td>
</tr>
</table><br></form></td></tr></table>                    </div>   </div>
</div> <div id="footer"> <p>Copyright (c) 2011  Design for educational purposes only</p>
</div>
</body> </html>
```

ΒΙΒΛΙΟΓΡΑΦΙΑ

Α)ΠΗΓΕΣ ΑΠΟ ΒΙΒΛΙΑ

Μαρίνος Μ. (2004), Δίκαιο Πνευματικής Ιδιοκτησίας Εκδ.Σάκουλα

Βλαχόπουλος Κ. (2007), Ηλεκτρονικό Έγκλημα Εκδ. Νομική Βιβλιοθήκη

Βασιλάκη Ε.Ε. (1993), Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών, Ποινικά 40, Αθήνα - Κομοτηνή, Σάκκουλας.

Κάτσικας Σ.- Γκρίτζαλης Δ. - Γκρίτζαλης Στ, (Επιστ. Επιμ), (2004), Ασφάλεια Πληροφοριακών Συστημάτων, Αθήνα, Εκδόσεις Νέων Τεχνολογιών.

Κιούπης Δ., ((1999), Ποινικό Δίκαιο και Ίντερνετ, Ποινικά 57, Αθήνα - Κομοτηνή, Σάκκουλας.

Αγγελή Ι., Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο (Convention on Cyber-crime) »

Κομνηνός Θ. - Σπυράκης Π., (2002), Ασφάλεια Δικτύων & Υπολογιστικών Συστημάτων, Αθήνα, Ελληνικά Γράμματα.

Αλεξανδρής Νικόλαος , Μπελεσιώτης Β.Σ. , Παναγιωτόπουλος Θ. , Εισαγωγή στην Επιστήμη των Υπολογιστών , Εκδόσεις Βαρβαρήγου

Νικολαϊδης Χρ., (1999), Η Σκοτεινή πλευρά του Ίντερνετ, Αθηνα, Anubis.

Λάζος Γρ., (2001), Πληροφορική & Εγκλημα, Αθήνα, Νομική Βιβλιοθήκη.

Πάγκαλος Γ. - Μαυρίδης Ι., (2002), Ασφάλεια πληροφοριακών συστημάτων και δικτύων, Θεσσαλονίκη, Ανίκουλα.

Δουληγέρης Χρήστος , Μαυροπόδη Ρόζα , Κοπανάκη Εύη (2004) , Τεχνολογίες Διαδικτύου , Έκδοση Νηρηίδες

Σουρής Α. - Πατσός Δ. - Γρηγοριάδης Ν., (2004), Ασφάλεια της πληροφορίας στους υπολογιστές, στο Internet, στην καθημερινή μας ζωή, Αθήνα, Εκδόσεις Νέων Τεχνολογιών.

Αγγελή Ι., «Διαδίκτυο (internet) και ποινικό δίκαιο – Έγκλημα στον κυβερνοχώρο (Cybercrime-Internet Crime)»

Σινανιώτη – Μαρούδη Αριστέα , Φαρσαρώτας Ιωάννης (2005) Ηλεκτρονική Τραπεζική , Εκδόσεις Σάκουλα

Μίτνικ Κ. - Σάιμον Ο., (2003), Η τέχνη της απάτης - Ο ανθρώπινος παράγοντας στην ασφάλεια, μτφρ. Λ. Καρατζάς, Αθήνα, Ωκεανίδα.

Parker Donn B., (1998), Fighting Computer Crime, New York, John Wiley & Sons, Inc.

Pipkin L.D., (1997), (2003), Halting the Hacker : A Practical Guide to Computer Security, New Jersey, Prentice Hall.

Sorensen B. T., (2005), Προστατέψτε το PC σας, επιμ.-μτφρ. Ξανθούλης Στ., Τζοβελέκης Κ., Αθήνα, Ελέκτορ ΕΠΕ.

Β)ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΗΓΕΣ

1999 U.S. Attorney General's Report on Cyberstalking
http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm

AARP: Telemarketing Fraud
http: //www.aarp.org/fraud/home.htm

Canadian Security Establishment -- Information Technology Security Links
http: //www.c se.dnd.ca/cse/english/links.html

Cisco Systems Network Security Services
http://www.cisco.com/warp/public/732/Security

Computer and Internet Security Resources
http://virtuallibrarian.com/legal

Computer Crime
http://www.ifs.univie.ac.at/~pr2gq1/rev4344.html#crime

Computer Crime and International Review of Criminal Policy
http://www.ifs.univie.ac.at/~pr2gq1/rev4344.html#crime

Computer Crime Essay
http://www.rbs2.com/ccrime.htm

Computer Crime Research Resources
http://mailer.fsu.edu/~btf1553/ ccrr/wel come.htm

Computer Security Institute (CSI)
http://www.gocsi.com

Cops on the Internet
http://www.wcsooh.org/law.html

Cryptography for encryption, digital signatures and authentication page
http://www.ozemail.com.au/~firstpr/crypto

CyberCop Home Page
http://www.cybercops.org

CyberCop Intrusion Detection Devices for Networks
http://www.3dg.com/cyb ercop

CyberCop Security Resources
http://www.3dg.com/cybercop/resources/resources.html

Electronic Crime
http://police.sas.ab.ca/prl/elect.html

Federal Guidelines for Searching and Seizing Computers
http://www.usdoj.gov/criminal/cybercrime/search_docs/search.htm

Federal Prosecution of Violations of Intellectual Property Rights
http://www.usdoj.gov/criminal/cybercrime/intell_prop_rts/toc.htm

Financial Crimes Enforcement Network
http://www.ustreas.gov/fincen

FindLaw Cybercrime Links
http://cyber.lp.findlaw.com/criminal/

High Technology Crime Investigation Association
http://htcia.org

ICSA.NET (Information and Computer Security)
http://www.icsa.net

Information Systems Security Association
http://www.issa-intl.org/
Inspection Service Consumer Fraud
http://www.usps.gov/websites/depart/inspect/consmenu.htm

International Computer Security Association (ICSA)
http://www.icsa.net

Internet ScamBusters
http://scambusters.com/

Model State Computer Crimes Code
http://www.cybercrimes.net/98MSCCC/MSCCCMain.html

National Fraud Information Center
http://www.fraud.org/welcome.htm

National Fraud Information Center
http://www.fraud.org/welmes.htm

National Institute of Justice Office of Science and Technology
http://www.nlectc.org

National Institute of Standards and Technology -- Computer Security Resource Clearinghouse
http://csrc.nist.gov/welcome.html

National Security Institute -- Computer Security Resources
http://nsi.org/compsec.html

RSA Data Security
http://www.rsa.com

Securities Fraud/Investor Protection on Web
http://www.securitieslaw.com

Spam: Where to Complain About Frauds & Scams on the Internet
http://www.elsop.com/wrc/complain.htm

Supplement to Federal Guidelines for Searching and Seizing Computers
http://www.usdoj.gov/criminal/cybercrime/supplement/ssgsup.htm

The CERT Coordination Center
http://www.cert.org

The Electronic Frontier Foundation (EFF)
http://www.eff.org

The FBI's Computer Crime Squad
http://www.emergency.com/fbi-nccs.htm
The Secure Zone: The Computer Security Information Center
http://www.securezone.com

The University of Dayton School of Law
http://cybercrimes.net/

The World Wide Web Security FAQ
http://www.w3.org/Security/Faq/www-security-faq.html

U.S. Code -- Computer Crime section
http://mailer.fsu.edu/~btf1553/ccrr/federal.htm#statutes

U.S. Dept. of Justice Antitrust Division
http://www.usdoj.gov/atr

VeriSign Corporation
http://www.verisign.com

Yahoo's Computer Security Page
http://www.yahoo.com/Business_and_Economy/Companies/Computers/Security

ASR Consulting Services
http://www.auldenfire.com/asr/consulting.shtml

Computer Crime Ready Reference

http://www.virtuallibrarian.com/legal