ΤΕΙ ΜΕΣΟΛΟΓΓΙΟΥ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΣΤΕΛΕΧΩΝ ΣΥΝΕΤΑΙΡΙΣΤΙΚΩΝ
ΟΡΓΑΝΩΣΕΩΝ ΚΑΙ ΕΚΜΕΤΑΛΛΕΥΣΕΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΗΛΕΚΤΡΟΝΙΚΗ ΟΙΚΟΝΟΜΙΚΗ ΠΑΡΑΒΑΤΙΚΟΤΗΤΑ

Επιβλέπων:
Χρ.Τσουραμάνης,Καθηγητής.
Σπουδάστρια:
Νικολέτα Θεοδωροπούλου

Μεσολόγγι 2003

ΗΛΕΚΤΡΟΝΙΚΗ

ΟΙΚΟΝΟΜΙΚΗ

ΠΑΡΑΒΑΤΙΚΟΤΗΤΑ

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΡΟΛΟΓΟΣ

Η σπουδαιότητα των Η/Υ και της πληροφορικής τεχνολογίας είναι κοινώς αποδεκτό ότι βρίσκεται σε ύψιστο σημείο. Σε συνδυασμό και με την έλλειψη ηθικής όσον αφορά τους χρήστες Η/Υ έχει επέλθει σε κατάσταση αναγκαίου κακού. Χωρίς την χρήση της πληροφορικής δεν νοείται πλέον η ομαλή λειτουργία της κοινωνίας.

Με την χρήση της, όμως, τα προβλήματα που δημιουργούνται έχουν αντίκτυπο στο κοινωνικό σύνολο γενικότερα. Έχει έτσι δημιουργηθεί το δίλλημα όσον αφορά την χρήση ή όχι της πληροφορικής τεχνολογίας, και η μόνη λογικοφανής και εφικτή απάντηση είναι ότι καθίσταται πλέον απαραίτητη η χρήση των Η/Υ αλλά με ηθικούς φραγμούς και την ύπαρξη δεοντολογίας από πλευράς των χρηστών. Να μην παραβιάζονται όρια που αποτελούν την κόκκινη γραμμή προς την δυσλειτουργία της κοινωνίας.

Στις ενότητες που ακολουθούν γίνεται ανάλυση σχετικά με αιτίες, μορφές και προτάσεις αντιμετώπισης της ηλεκτρονικής παραβατικότητας. Συγκεκριμένα:

Στο πρώτο κεφάλαιο προσεγγίζεται η ηλεκτρονική οικονομική παραβατικότητα. Γίνεται ανάλυση της έννοιάς της και αναφορά στην σταδιακή εξέλιξη αφενός στον τομέα της τεχνολογίας και εφετέρου στην χρήση της και στην αναγκαιότητα ύπαρξης της στο κοινωνικό σύνολο. Αναφέρονται περιστατικά που καθόρισαν αυτήν την

πορεία καθώς και στατιστικά δεδομένα και ερευνητικά στοιχεία που έχουν προκύψει από την εξέλιξη αυτή.

Στο κεφάλαιο αυτό γίνεται αναφορά και σύντομη ανάλυση στις μορφές που έχει η παραβατικότητα στο διαδίκτυο και πώς λειτουργεί στα πλαίσια της κοινωνίας.

Στην επόμενη ενότητα διαχωρίζονται οι πρωταγωνιστές του φαινομένου σε δράστες και θύματα. Σ'αυτούς που "δημιουργούν"το φαινόμενο, το συντηρούν και το εξελίσουν σε μεταγενέστερες μορφές . Απ'την άλλη πλευρά βρίσκονται τα θύματα που είναι απλοί δέκτες,απλά παρατηρούν και επινοούν τρόπους άμυνας.

Στα δύο τελευταία κεφάλαια αναφέρονται κάποιοι τρόποι αντιμετώπισης και άμυνας από πλευράς του μεγάλου αριθμού χρηστών και αναφέρονται ενδεικτικά μέτρα ασφαλείας ώστε να μην δημιουργούνται ανεπανόρθωτες βλάβες. Τέλος, σύμφωνα με την ως τώρα παρατήρηση των γεγονότων και σχετική πρόβλεψη για την εξέλιξη του φαινομένου γίνεται αναφορά στις μελλοντικές βλέψεις όσον αφορά τα μέτρα προστασίας αλλά και στην εξέλιξη που αναμένεται να έχει η συγκεκριμένη παραβατική συμπεριφορά.

1.-ΗΛΕΚΤΡΟΝΙΚΗ ΟΙΚΟΝΟΜΙΚΗ ΠΑΡΑΒΑΤΙΚΟΤΗΤΑ

α.-Έννοια

Το πληροφορικό έγκλημα εντοπίστηκε στα μέσα της δεκαετίας του '70 από ειδικούς επιστήμονες, σαν παρεμβολή στην ομαλή ως τότε λειτουργία του διαδικτύου. Ύστερα από την "γνωριμία " με το νέο αυτό φαινόμενο, έγιναν προσπάθειες για τον προσδιορισμό του ως προς την οικονομική, κοινωνική, νομική φύση του. Κάτι τέτοιο, όμως, αποδείχτηκε ιδιαίτερα δύσκολο λόγω του πολυδιάστατου "προσώπου"του. Έγιναν, δηλαδή, προσεγγίσεις από διαφορετικά επίπεδα ανάλυσης. Το γεγονός, επίσης, ότι η εξέλιξή του γίνεται με ιδιαίτερα γρήγορους ρυθμούς, καθώς και η διαφοροποίηση της νομοθεσίας από κράτος σε κράτος, αποτέλεσαν καθοριστικούς παράγοντες.

Βασικό κατασταλτικό στοιχείο, όμως,υπήρξε το γεγονός ότι ως την χρονική αυτή περίοδο ελάχιστα περιστατικά είχαν καταγραφεί. Τα στοιχεία, συνεπώς, δεν επαρκούσαν για μια αξιόπιστη και πλήρη μελέτη του φαινομένου. Το γεγονός, ακόμα, ότι τα λίγα γεγονότα που είχαν ήδη σημειωθεί κατατάσσονταν σε υποκατηγορία του οικονομικού εγκλήματος δεν απέδιδε την σπουδαιότητα στην συγκεκριμένη μορφή για ένα υγιές μέλλον στην πληροφορική.

Συνέπεια των παραγόντων αυτών ήταν να μην υπάρξει ένας γενικός ορισμός του πληροφορικού εγκλήματος, ή όπως αλλιώς αναφέρεται, της ηλεκτρονικής παραβατικότητας, γεγονός το οποίο οδηγεί σε επιμέρους προβλήματα. Χωρίς την ύπαρξη ενός ορισμένου

εννοιολογικού φάσματος του φαινομένου δεν είναι δυνατό να προσδιορίσουμε πότε τελικά πρωτοεμφανίστηκε, είναι αδύνατη η ανεύρεση αποτελεσματικών λύσεων και ακόμα, οδηγούμαστε σε συμπεράσματα, παρατηρήσεις και ενέργειες λανθασμένες και συνεπώς μή αποτελεσματικές.

Παρόλο που ένα μέρος επιστημόνων (Wasik,Parker, Forchut)(1) τελικά εστιάζουν την προσοχή όχι στην ύπαρξη ενός ¨κλειστού¨ περιοριστικού ορισμού αλλά μιας γενικότερης έννοιας η οποία θ'αναφέρεται σε όλο το φάσμα αρνητικών επιπτώσεων μέσω ηλεκτρονικού υπολογιστή, όπως η γενικότερη κακοχρησία του, η τροποποίηση και καταστροφή αρχείων, η κλοπή πληροφοριών και προγραμμάτων, η χρέωση ξένων λογαριασμών, η βιομηχανική κατασκοπεία. Ένας ορισμός αντιπροσωπευτικός ο οποίος είναι ευρύτερα αποδεκτός είναι: ¨***το πληροφορικό έγκλημα περιλαμβάνει κάθε παράνομη πράξη για την τέλεση της οποίας είναι απαραίτητη η γνώση της τεχνολογίας των ηλεκτρονικών υπολογιστών***¨***(2).***

Αναφερόμενοι σε παράνομη πράξη εκτός από την νομική παρέκκλιση εννοούμε και κάθε ενέργεια η οποία αντιβαίνει στην ηθική, την ιδεολογία και τους κανόνες που έχουν διαμορφωθεί σ'ένα κοινωνικό σύνολο.

β.-Περιστατικά

Καθημερινά πέφτουν στην αντίληψή μας γεγονότα και περιστατικά τα οποία αφορούν παράβαση των κανόνων και χρήση του διαδικτύου με σκοπιμότητα.

Έχουν μείνει στην ιστορία τεράστιας σημασίας πληροφορικά εγκλήματα και επώνυμοι χάκερς, οι οποίοι έχουν προκαλέσει το δίλλημα αν οι ηλεκτρονικοί υπολογιστές είναι μέσο γρηγορότερης, αμεσότερης επικοινωνίας και πολιτιστικής εξέλιξης ή τελικά είναι ένα απαραίτητο εργαλείο μεν, επιπρόσθετο πρόβλημα δε.

Σαν τέτοια περιστατικά παραθέτονται στη συνέχεια όλως ενδεικτικά τα ακόλουθα:

<u>Α.Ομάδα κακοποίησης παιδιών στο Internet</u>

Ο Scott Edward Yigling, σύμβουλος εταιρείας ηλεκτρονικών υπολογιστών ο οποίος στο χώρο του διαδικτύου ¨κυκλοφορούσε¨ με το ψευδώνυμο ¨chckrflag¨, στην προσπάθεια αναζήτησης πελατών απευθύνθηκε στον Craig Luecke. Πρόκειται για έναν χρήστη του internet,ο οποίος σερφάροντας στο διαδίκτυο έλαβε ένα μήνυμα το οποίο του προσέφερε ερωτικές εμπειρίες με παιδιά.

Συνεχίζοντας για κάποιες μέρες την επικοινωνία με τον άγνωστο αποστολέα επιβεβαιώθηκε οτι πρόκειται για οργανωμένη προώθηση της παιδικής πορνείας και αμέσως κάλεσε την αστυνομία.

Επί μέρες παρακολουθούσαν τις συνομιλίες των δύο αυτών ανδρών, στις οποίες μάλιστα, αναφέρονταν ακόμα και περιγραφές ερωτικών πράξεων με παιδιά, και εν συνεχεία προτάθηκε συγκεκριμένο ραντεβού με 5χρονο κοριτσάκι.

Η αστυνομία ύστερα από μεθοδευμένες ενέργειες κατάφερε να εντοπίσει τον "chckrflag" και τους συνεργάτες του, στους οποίους αποδόθηκαν κατηγορίες σεξουαλικής κακοποίησης και εκμετάλλευσης ανηλίκων.

Β.Έφηβος κατηγορείται ως hacker

Ο Jay Satira αντιμετωπίζει την καταδίκη σε 15 χρόνια φυλάκιση, δεχόμενος τις κατηγορίες που του αποδόθηκαν για παράνομη εισβολή στους υπολογιστές της εταιρείας AOL (American On Line's Internal) στην πόλη Westchester.

Χρησιμοποιώντας τον Η/Υ του, άλλαξε τα προγράμματα της εταιρείας προκαλώντας ζημιά 50.000 δολλαρίων, σύμφωνα με τον απολογισμό της ίδιας της εταιρείας. Ο Satira εκμεταλλεύτηκε την συλλογή στοιχείων και γνώσης που είχε αποκτήσει από την εθελοντική του εργασία στο τμήμα τεχνικής υποστήριξης της AOL και με την βοήθεια άλλων χάκερς κατάφερε να πραγματοποιήσει την εισβολή του.

Γ.Υπόθεση Mitnick

Ο Kevin Mitnick το 1987 καταδικάζεται για παράνομες εισβολές στο διαδίκτυο, η ποινή του, όμως, τελικά μειώθηκε στα 3

χρόνια και αποχή από την χρήση ηλεκτρονικών υπολογιστών. Το 1988 με την ιδέα ν'αποκτήσει ένα αντίγραφο του κώδικα του VMS (λειτουργικό σύστημα) της Digital Electronics, εισβάλλει κάθε νύχτα στο διαδίκτυο μέχρι που καταλαβαίνει ότι τα περιθώρια στένεψαν.

Ένα χρόνο μετά οδηγείται στις φυλακές. Λόγω, όμως, της ψυχικής εξάρτησης την οποία το δικαστήριο έκρινε πως είχε, καταδικάστηκε σε 1 χρόνο φυλάκιση. Μετά την τριετή απουσία του εμφανίστηκε πάλι το 1992 με εισβολές σε βάσεις δεδομένων του Αμερικανικού στρατού και των εταιρειών Motorola και Nokia.

Ύστερα από αυτά, το 1994, πραγματοποιεί μια ακόμα επίθεση η οποία τον τοποθέτησε ψηλά στην ιεραρχεία των χάκερς. Εισέβαλλε στον Η/Υ του Τσιτόμου Σικομούρα (ειδικού σε θέματα ασφαλείας συστημάτων πληροφορικής) και του αφαίρεσε σημαντικά προγράμματα ελέγχου συστημάτων ασφαλείας του στρατού. Ο Σικομούρα ξεκίνησε την αναζήτηση του Mitnick, ο οποίος ύστερα από 2 μήνες συνελήφθη.

Ο Mitnick έμεινε 5 χρόνια στη φυλακή, χωρίς όμως, ν'αποδεχτεί την κατηγορία για την τελευταία αυτή πράξη.

Δ.Επιθέσεις χάκερ με οικονομικές ζημιές

Ο Ratrick W.Gregory, γνωστός στο χώρο του Internet με το ψευδώνυμο "Most Hated" αντιμετωπίζει ποινή φυλάκισης έως 5 χρόνων και πρόστιμο 2,5 εκατομμύρια δολλάρια. Ο 19χρονος χάκερ από το Τέξας ήταν μέλος της ομάδας χάκερ "global Hell", η οποία είχε πραγματοποιήσει ηλεκτρονικές επιθέσεις κατά συρροή, με ζημιές

περίπου 1,5 εκατομμύρια δολλάρια. Στόχοι του είχαν υπάρξει ακόμα και ο Λευκός Οίκος και ο Αμερικανικός στρατός.

Ο νεαρός δέχτηκε να παραδεχτεί την συμμετοχή του στην ομάδα αυτή, καθώς και τα αδικήματα που είχε διαπράξει, ευελπιστώντας ελαφρύτερη ποινή. Απώτερος στόχος του ήταν η πραγματοποίηση της επιθυμίας του: η συγκρότηση δικής του εταιρείας ασφάλειας υπολογιστών !!!

Ε.Δωρεάν τηλεφωνήματα με μια σφυρίχτρα

Ο πρώτος άνθρωπος που φυλακίστηκε για απάτη στο Internet ήταν ο John Draper στα τέλη της δεκαετίας του '70. Με το ψευδώνυμο Captain Crunch κατάφερε να κάνει δωρεάν τηλεφωνήματα με μια παιδική σφυρίχτρα. Παραβίασε το καλά οργανωμένο τηλεφωνικό δίκτυο των ΗΠΑ και εν συνεχεία κατασκεύασε και το Blue Box (μια συσκευή που εξυπηρετούσε τον σκοπό του). 'Υστερα απ'αυτόν ακολούθησαν και άλλοι με παρόμοιες ενέργειες. Ενδεικτικό παράδειγμα αποτελούν οι ιδρυτές της εταιρείας Apple, οι οποίοι ξεκίνησαν την καριέρα τους πουλώντας συσκευές που βοηθούσαν στην εξαπάτηση μέσω τηλεφωνικών γραμμών (αντίγραφα του Blue Box).

ΣΤ.Κυβέρνηση των ΗΠΑ εναντίον οργανωμένης ομάδας χάκερ

Το 1984 ο Phiber Optik εντάσσεται σε μια ομάδα χάκερ, στην οποία άνηκαν ήδη τα μεγαλύτερα ονόματα του χώρου. 'Υστερα

από μία διαφωνία αποφάσισε να αποχωρήσει και να ιδρύσει την δική του ομάδα, την Masters of Deception. Μετά απ'αυτό άρχισαν επιθέσεις χωρίς όρια.

Η κυβέρνηση των ΗΠΑ αφού δέχτηκε τις επιθέσεις αποφάσισε να δράσει ιδρύοντας μια ομάδα, την Legion Of Doom. Η απόπειρα αυτή απέτυχε και η επόμενη προσπάθεια έγινε μετά από ένα χρόνο. Ιδρύθηκε η ομάδα Redux και τελικά κατάφεραν να σταματήσουν την δράση της οργάνωσης. Μάλιστα συνελλήφθησαν και τέσσερα άτομα, συμπεριλαμβανομένου και του ιδρυτή, ο οποίος φυλακίστηκε.

Ζ.Κινέζοι crackers εισβάλλουν σε τραπεζικό δίκτυο

Ο Hao Jinglong και ο Hao Jingwen, δυο Κινέζοι crackers εισβάλλοντας το 1998 στο τραπεζικό δίκτυο της χώρας τους καταχράστηκαν 260 χιλιάδες yuan. Πρόκειται για δύο αδέρφια, που εκμεταλλεύτηκαν την πρώην ιδιότητα του πρώτου ως ταμία στην Βιομηχανική και Εμπορική Τράπεζα της Κίνας, και τοποθέτησαν μια συσκευή ελέγχου σ'ένα τερματικό στο συγκεκριμένο υποκατάστημα της Τράπεζας.

Έχοντας, προηγουμένως, ανοίξει 16 λογαριασμούς σε διάφορα ονόματα μετέφεραν χρήματα σ'άυτούς και εν'συνεχεία, απέσπασαν ένα μεγάλο τμήμα τους. Περισσότερες πληροφορίες δεν δόθηκαν στην δημοσιότητα, παρά μόνο ότι τα δύο αδέρφια καταδικάστηκαν σε θανατική ποινή, σύμφωνα με τη δημοσίευση στην εφημερίδα Hui Daily στις 28 Δεκεμβρίου του 1998.

Η.Δεκαεννιάχρονος cracker καταδικάζεται σε 3ετή ψυχιατρική φροντίδα.

Ο Raphael Gray, κάτοικος της Δυτ.Ουαλίας, και σπουδαστής πληροφορικής, δημοσίευσε αριθμούς πιστωτικών καρτών σε web sites του το 1999. Χρησιμοποιώντας "τρωτά σημεία" της Microsoft εισέβαλλε σε sites ηλεκτρονικού εμπορίου σε ΗΠΑ, Καναδά, Ταϊλάνδη, Ηνωμένο Βασίλειο. Βρήκε αριθμούς πιστωτικών καρτών, μερικές από τις οποίες ανήκαν σε διάσημα άτομα (Bill Clinton, Bill Gates) και περίπου 6500 απ'αυτούς δημοσιεύτηκαν σε 2 web sites του, χρησιμοποιώντας το ψευδώνυμο "Gurad". Σ'αυτές ανέφερε ότι το ηλεκτρονικό εμπόριο πρέπει να είναι καλύτερα δομημένο και περισσότερο ασφαλές για τους ανθρώπους που συναλλάσσονται μέσω του διαδικτύου, και καλούσε τους επισκέπτες των σελίδων αυτών να τον ψηφίσουν ως άγιο ή αμαρτωλό για την πράξη του αυτή.

Μάλιστα, πραγματοποίησε και μια φάρσα εις βάρος του Bill Gates και παρήγγειλε δεκάδες κουτιά με χάπια Viagra και τα έστειλε. Το δικαστήριο αποφάσισε για τον Gray τριετή παρακολούθηση από ειδικούς και την ψυχιατρική του θεραπεία. Κρίθηκε από τον δικαστή για την προσπάθεια χλευασμού του διάσημου αυτού προσώπου και για τις οικονομικές ζημιές που προκάλεσε σε πολλούς ανθρώπους.

γ.Ερευνητικά δεδομένα

Λέγοντας οικονομική παραβατικότητα ή πληροφορικό έγκλημα αναφερόμαστε στο συνολικό αριθμό παραβάσεων που τελούνται στον διαδικτυακό χώρο, με οποιαδήποτε μορφή, και χρησιμοποιούν ως μέσο τον Η/Υ. Αναφερόμενοι σ'αυτόν τον χαρακτηρισμό κατά κανόνα εννοούμε το ηλεκτρονικό οικονομικό έγκλημα.

Ακριβέστερα, τα οικονομικά εγκλήματα απαρτίζουν τον κύριο όγκο των πληροφορικών εγκλημάτων. Σύμφωνα με την διεθνή βιβλιογραφία, σε κάθε 12 περιπτώσεις πληροφορικού οικονομικού εγκλήματος αντιστοιχεί μόνο μια περίπτωση ηλεκτρονικού εγκλήματος άλλης κατηγορίας (π.χ.κατασκοπεία).

Παράγοντες που συνετέλεσαν σ'αυτήν την αναλογία ,η οποία προκαλεί το ενδιαφέρον λόγω της περίεργης κατανομής των παραβάσεων μεταξύ οικονομικών και άλλων είναι οι εξής:

α. -Ένα πληροφορικό οικονομικό έγκλημα γίνεται ευκολότερα αντιληπτό και αποδείξιμο.

β. -Είναι ένα είδος ηλεκτρονικού εγκλήματος που ενδιαφέρει και αφορά στο μέγιστο τις επιχειρήσεις και τους οργανισμούς λόγω της φύσης του. Κατά κύριο λόγο τα οικονομικά εγκλήματα μέσω διαδικτύου αναφέρονται σε τεράστια ποσά. Μια επιχείρηση δεχόμενη ένα τέτοιο πλήγμα κρίνεται ως προς την βιωσιμότητά της. Η εξακρίβωση και καταγραφή των παραβάσεων προσφέρει κάποια σχετική ασφάλεια.

γ. -Η μορφή αυτή είναι ευκολότερα ανακοινώσιμη στο ευρύ κοινό καθώς είναι δυνατή η ακριβής πληροφόρησή του με αριθμούς και λεπτομερή γεγονότα. Κάτι τέτοιο δεν ισχύει με άλλες μορφές, π.χ. τα εγκλήματα κατά των ηθών.

Παράλληλα, με την αύξηση του αριθμού των περιστατικών ηλεκτρονικής παραβατικότητας άρχισαν να γίνονται και οι πρώτες συστηματικές έρευνες. Το χρονικό αυτό σημείο είναι η δεκαετία του '70 οπότε κρίθηκε αναγκαία η περισσότερο μεθοδική έρευνα και εξαγωγή αποτελεσμάτων λόγω της συχνότητας των περιστατικών.

Σύμφωνα με μελέτη που πραγματοποίησε στις ΗΠΑ το SRI International, και άρχισε το 1971, σε τρεις 10ετίες, περίπου, σημειώθηκαν 1600 περιπτώσεις ηλεκτρονικής παραβατικότητας. Ύστερα από την πρώτη αυτή έρευνα διενεργήθηκαν και επόμενες και είχαν σκοπό την απόδοση της πραγματικής εικόνας του φαινομένου. Το AICPA μοιράζοντας σε τράπεζες και ασφαλιστικούς οργανισμούς ερωτηματολόγια , εξήγαγε τα εξής αποτελέσματα:

Το 2%, 105 από τις 5.127 των εταιριών που απάντησαν ανέφεραν ότι είχαν γίνει θύμα εξαπάτησης μέσω Η/Υ. Όσον αφορά τις ασφαλιστικές εταιρίες, από τις 854 οι 40 είχαν δεχτεί επίθεση (3%).

Μια άλλη έρευνα που διεξήχθη την ίδια περίοδο από την Επιτροπή Δράσης όσον αφορά το Πληροφορικό Έγκλημα, έφτασε στο συμπέρασμα ότι από τους 257 οργανισμούς το 27% είχε δεχτεί επίθεση με ζημιά άνω των 100.000 δολλαρίων, και 19 οργανισμοί είχαν μεγαλύτερες απώλειες.

Μετέπειτα, η έρευνα που πραγματοποιήθηκε το 1986 από τον Οργανισμό Forbes και το κολέγιο Mercy έδειξε ότι το 56% των εταιριών είχαν υπάρξει θύματα. Εν συνεχεία, το 1988 στην Florida το τμήμα δικαιοσύνης έφτασε ύστερα από μελέτη στο αποτέλεσμα ότι το

24,2% των επιχειρήσεων είχαν βρεθεί στο στόχαστρο των ηλεκτρονικών παραβατών. Αξιοσημείωτο είναι, επίσης, το γεγονός ότι οι χάκερς εμπλέκονται μόλις στο 19% των περιπτώσεων και στο 50-85 % οι υπάλληλοι των ίδιων των εταιριών.

Στις ΗΠΑ έγινε η αρχή των οργανωμένων ερευνών λόγω της έκτασης που είχε λάβει το φαινόμενο στην συγκεκριμένη γεωγραφική περιοχή.

Και στην Μ. Βρετανία, όμως, το φαινόμενο έδειξε να κάμπτεται ως το 1998. Από ποσοστό 30% που κατείχε το 1987, μεταβλήθηκε σε 14% το 1990, σε 3% το 1994 και σε 11% το 1998.

Στην Γερμανία λόγω της πολυμορφίας των παραβάσεων δεν υπήρξαν γενικά συγκεντρωτικά στατιστικά στοιχεία. Σχετικές έρευνες έδειξαν ότι η μορφή παραβατικότητας που σημείωσε κατακόρυφη άνοδο ήταν η κλοπή λογισμικού και αυτό εξ'αιτίας της αύξησης του αριθμού των εφήβων και νεαρών ατόμων που ασχολούνταν με το Internet. Παράλληλα, υπήρξε και ταυτόχρονη αύξηση των κρουσμάτων. Έτσι, από 9 υποθέσεις που καταγράφηκαν το 1980, 8 το 1981, 9 το 1982 και 11 το 1983, το 1984 ο αριθμός εκτοξεύτηκε στα 212 περιστατικά.(3)

Όσον αφορά το χρηματικό κόστος από τις παράνομες ενέργειες δεν πρόκειται για αμελητέα μεγέθη. Σύμφωνα με τους εμπορικούς οργανισμούς BSA και SPA και την έκθεση των αποτελεσμάτων τους το 1998, από τα 274 εκατομμύρια εφαρμογές που πραγματοποιήθηκαν, τα 228 εκατομμύρια ήταν παράνομες. Πρόκειται, δηλαδή, για 4 στις 10 πειρατικές εφαρμογές και σύμφωνα με την ίδια έρευνα, η αναλογία αυτή σημείωσε αύξηση σύμφωνα με τα προηγούμενα έτη.

Το αποτέλεσμα είναι το κόστος της πειρατείας ν'ανέρχεται σε 11,4 δισεκατομμύρια δολλάρια και βασική αιτία

θεωρείται η αύξηση των τιμών στα προϊόντα λογισμικού. Οι χώρες που σημείωσαν τις μεγαλύτερες απώλειες είναι: ΗΠΑ, Μ.Βρετανία, Γερμανία, Γαλλία, Καναδάς, Κορέα, Ιταλία, Βραζιλία, Κίνα, Ιαπωνία.

Εάν εξετάσουμε την οικονομία σε συνάρτηση με τον πληροφορικό εξοπλισμό της και το πώς είναι συνδεδεμένες οι δύο έννοιες, θα δούμε οτι:

Η κίνηση χρήματος ΄΄τοις μετρητοις΄΄ έχει αντικατασταθεί από το λογιστικό χρήμα, κυρίως στις ανεπτυγμένες χώρες. Αναφερόμαστε στο ηλεκτρονικό χρήμα, το οποίο εξοικονομεί χρόνο, μειώνει το κόστος και εξασφαλίζει την ακρίβεια των συναλλαγών. Η αυξανόμενη, όμως, αντικατάσταση του ρευστού χρήματος θα οδηγήσει στον πολλαπλασιασμό των εγκλημάτων της πληροφορικής απάτης, καθώς σταδιακά θ'αποτελέσει την αποκλειστική μορφή συναλλαγών. Η εξάλειψή του φαινομένου αυτού αποτελεί φενάκη, η αντιμετώπισή του, ωστόσο εστιάζεται στο γεγονός ότι πρέπει να υπάρξει ταχύτερη εξέλιξη της πληροφορικής τεχνολογίας στον οικονομικό τομέα για ν'αντιμετωπίσει το ηλεκτρονικό οικονομικό έγκλημα.

Κάτι τέτοιο κρίνεται άμεση προτεραιότητα αν λάβουμε υπ' όψιν ότι μέσω EFTS (συστήματα ηλεκτρονικής μεταφοράς χρηματικών οικονομικών μεγεθών), τα ποσά που διακινήθηκαν στις ΗΠΑ το 1986 σε εθνικό επίπεδο ήταν 300 δισεκατομμύρια δολλάρια/ημέρα, και σε διεθνές επίπεδο, 600 δισεκ/ρια δολλάρια /ημέρα, το δε 1996, 7πλασιάστηκαν.

Μια ενδεικτική εικόνα μπορούμε να έχουμε από τ'αποτελέσματα της έρευνας που διεξήχθη το 1989 στις ΗΠΑ. Η κακοχρησία και η σκοπιμότητα δείχνουν οτι οι απώλειες και οι ζημιές

μπορούν να επηρεάσουν αρνητικά όλους τους τομείς σε μια κοινωνία, περισσότερο ή λιγότερο ανεπτυγμένη.

Το 45 % των πληροφορικών εγκλημάτων είχαν γίνει με σκοπό την εξοικονόμηση χρήματος για τους χάκερς, το 2 % και 10 % για παραβίαση ασφαλείας και κλοπής κλοπή δεδομένων αντίστοιχα. Ένα ποσοστό 12 % αποσκοπούσε στην τροποποίηση δεδομένων, το 16 % σε βλάβη στο software, και τέλος, ένα 16 % στην κλοπή πληροφοριών από προγράμματα.

Ενδιαφέρον, επίσης, παρουσιάζει και η έρευνα που έγινε το 1999, η οποία αναφέρεται στην οικονομία των ΗΠΑ και στο κόστος του πληροφορικού εγκλήματος. Εκτιμήθηκε, λοιπόν, ότι το κόστος αυτό ανέρχεται σε 202 εκατομμύρια δολλάρια τον χρόνο με αυξητικές τάσεις. Επίσης, ότι για το 90 % των ηλεκτρονικών εγκλημάτων ευθύνονται οι ίδιοι οι υπάλληλοι των επιχειρήσεων και ότι ένα τέτοιο έγκλημα διαπράττεται κάθε 20 δευτερόλεπτα στο διαδίκτυο.

Όσον αφορά στα Ελληνικά δεδομένα, 80 δισεκατομμύρια δραχμές φτάνει ο τζίρος από τις απάτες στα τηλεφωνικά δίκτυα μέσω Η/Υ και 300-350 είναι οι επιθέσεις κάθε χρόνο. Οι τρόποι εξαπάτησης που έχουν μέχρι τώρα εντοπιστεί στην Ελλάδα ανέρχονται σε 50.

Μία απάτη την ημέρα πραγματοποιείται από Έλληνες ή ξένους χάκερς με τους διάφορους τρόπους που έχουν επινοήσει. Ένα απλό μήνυμα σ'έναν τηλεφωνητή είναι αρκετό για να βρούν τον κωδικό που θα τους επιτρέψει να τηλεφωνήσουν στην Αμερική, στην Νέα Γουϊνέα κτλ.

Γενικά συμπεράσματα από έρευνες που πραγματοποιήθηκαν, όσον αφορά στην ηλεκτρονική παραβατικότητα είναι τα εξής: (4)

1. Οι επιχειρήσεις αποτελούν τα συχνότερα θύματα των ηλεκτρονικών παραβατών, συνεπώς επηρεάζονται άμεσα από τις ενέργειες αυτές. Η γενικότερη και πιο μεθοδευμένη ασφάλεια των πληροφοριών τους θα συνέβαλε στην επέκταση της δραστηριότητάς τους, καθώς κάθε τους κίνηση θα κατευθυνόταν προς εποικοδομητικές ενέργειες.

2. Ο φόβος της κακής δημοσιότητας από την γνωστοποίηση ενός τέτοιου γεγονότος οδηγεί τις επιχειρήσεις συχνά στην αποσιώπηση των επιθέσεων εναντίον τους.

3. Τα περιστατικά που καταγγέλλονται αποτελούν ενδεικτική εικόνα του όλου φαινομένου. Στην πραγματικότητα τα θύματα είναι πολύ περισσότερα.

4. Δεν είναι πλέον δεδομένο και σταδιακά αμφισβητείται η άποψη ότι οι χάκερς είναι κυρίως έφηβοι που για εμπειρία και μόνο οδηγούνται σε παράνομες πράξεις στο διαδίκτυο.

5. Απαιτείται συνεργασία τεχνολογίας, κυβερνητικών οργανισμών και ιδιωτικού τομέα για την ελαχιστοποίηση του φαινομένου.

Η έρευνα και η στατιστική προσέγγιση σύμφωνα με τον Parker συμβάλλει στο να διαμορφωθεί το απαραίτητο πρακτικό δυναμικό για την ασφαλή χρήση των Η/Υ.

Με τον πειραματισμό και την συγκεντρωτική άποψη για τους πιθανούς τρόπους "παράβασης" δημιουργούνται ασφαλή συστήματα ηλεκτρονικών υπολογιστών. Κάτι τέτοιο, παράλληλα, αποτελεί και προστασία για τα υποψήφια θύματα ενημερώνοντάς τα για τις πιθανότητες εξαπάτησής τους και πώς ν'αποφύγουν κάτι τέτοιο.

Εναλλακτικές μορφές είναι η ¨θυματολογική έρευνα¨ (victim survey) και η δημιουργία ¨συλλογών ¨ (case books)(5). Οι δύο αυτές μορφές που αφορούν την συμπλήρωση ερωτηματολογίου από χρήστες για το αν και κατά πόσο έχουν πέσει θύματα και την καταγραφή και την συγκέντρωση των περιστατικών αποτελούν μεθόδους μελέτης της οικονομικής παραβατικότητας.

Ο άμεσος και κυρίαρχος στόχος σε κάθε μια από τις παραπάνω περιπτώσεις είναι κοινός. Να εξάγουμε συμπεράσματα και συνεπώς τρόπους προστασίας από κάθε επίδοξο μελλοντικό εξαπατητή μας.

2.-ΜΟΡΦΕΣ

Κάθε έγκλημα που τελείται στον κυβερνοχώρο αποτελεί ένα νέο κρούσμα ηλεκτρονικής παραβατικότητας και πολύ συχνά έχει μια νέα μορφή. Οι περιπτώσεις εγκληματικότητας στο Internet και η αλματώδης αύξησή τους είναι ανάλογα του πολλαπλασιασμού των χρηστών. Σήμερα μιλάμε πλέον για εκατομμύρια χρήστες και άπειρες περιπτώσεις εγκλήματος, οι οποίες για λόγους καλύτερης εξέτασης και μελέτης και κρίνοντας από κάποια κοινά γνωρίσματα που έχουν, κατατάσσονται στις εξής κατηγορίες:

(α). Μια αρκετά συχνή μορφή, αν όχι την συνηθέστερη, ηλεκτρονικής παραβατικότητας, αποτελεί η παράνομη εισαγωγή σε ξένα συστήματα επεξεργασίας δεδομένων. Οι hackers εισβάλλουν και μετατρέπουν, αλλοιώνουν, και καταστρέφουν δεδομένα ,αποσυντονίζουν προγράμματα και παραποιούν πληροφορίες και ήδη υπάρχοντα στοιχεία τα οποία ανήκουν είτε σε οικιακούς χρήστες, είτε σε επιχειρήσεις, οργανισμούς κτλ. Κάτι τέτοιο μπορεί να συμβεί σε στιγμές ψυχαγωγίας ενός χάκερ, απλά για να κάνει αισθητή την παρουσία του, είτε για καθαρά ανταγωνιστικά κίνητρα.

Κάτι ανάλογο συνέβη το 1997 και στο site του κόμματος των Εργατικών της Βρεττανίας, στο οποίο χάκερ πραγματοποίησε την παράνομη είσοδό του και φόντισε να κάνει αισθητά τα ίχνη της ¨επιδρομής¨ του. Παραποίησε λογότυπα και φράσεις που χρησιμοποιούσε το συγκεκριμένο κόμμα στο site του, προσανατολίζοντάς τα προς τις πολιτικές πεποιθήσεις του. Φράση όπως ¨νέες πληροφορίες¨ πήραν την

ερμηνεία ¨ίδια ψέμματα, νέο περιτύλιγμα¨. Παρουσίαση προϊόντων (διαφημιστικών, κονκάρδων) συνοδεύτηκε από την φράση ¨αγοράστε τα σκουπίδια μας¨ και αρκετά ακόμα εφευρετικά λογότυπα του χάκερ.

(β). Ακόμα μια περίπτωση, εξίσου συχνή, είναι και η παρείσδυση στον κυβερνοχώρο με σκοπό την οικονομική ωφέλεια και την προσφορά παράνομων προϊόντων και υπηρεσιών. Ραντεβού κλείνονται με παιδιά έναντι αμοιβής. Επιτήδιοι έχουν προσεγγίσει ανήλικα θύματα και παρουσιάζοντάς τα στο διαδίκτυο τα ¨προσφέρουν¨ σε πελάτες που δείχνουν ενδιαφέρον και προσφέρουν την προκαθορισμένη αμοιβή. Με παρόμοιο τρόπο λειτουργούν και τα κυκλώματα που κανονίζουν συναντήσεις με αλλοδαπές για να αφιερώσουν χρόνο έναντι αμοιβής σε μοναχικούς χρήστες.

Η στρατηγική και ο τρόπος δράσης είναι ίδια όσο αφορά και τα ναρκωτικά. Ο ¨ηλεκτρονικός πωλητής¨ παρουσιάζει τα προσφερόμενα προϊόντα και αναζητά υποψήφιους αγοραστές.

(γ).Η βιομηχανική κατασκοπεία ανθεί στο χώρο του Internet. Προϊόντα και υπηρεσίες υψηλής τεχνολογίας γίνονται στόχος από επίδοξους χάκερς. Ευρεσιτεχνίες, πνευματικά δικαιώματα, απόρρητα δεδομένα και στοιχεία δεν υπάρχουν στο λεξιλόγιο ενός χάκερ, αντιθέτως αποτελούν ισχυρότατο κίνητρο. Στις περισσότερες περιπτώσεις ο απώτερος στόχος είναι το κέρδος.

Περιστατικά, όμως, μας δείχνουν ότι κάτι τέτοιο πολλές φορές αποτελεί κίνητρο ως η επίτευξη του δύσκολου και απαραβίαστου. Εξάλλου οι ίδιοι οι κυβερνοπειρατές υποστηρίζουν ότι ένας

¨καθαρόαιμος¨ χάκερ δεν αποβλέπει στο όφελος αλλά δρά για την πρόκληση, για την επίτευξη του απίθανου.

(δ). Η ηλεκτρονική κλοπή πιστωτικών καρτών και κωδικών τραπεζών αποτελεί, επίσης, αχχίλειο πτέρνα στον κόσμο των χρηστών του Internet. Ανυποψίαστοι κάτοχοι καρτών παρουσιάζονται να πραγματοποιούν τεράστιες συναλλαγές με τράπεζες και αγορές. Οι κωδικοί τους έχουν κλαπεί και επιβαρύνονται με τεράστια ποσά. Κάτι ανάλογο συμβαίνει και με τις χρηματιστηριακές συναλλαγές στις οποίες πωλούνται μετοχές φαντάσματα, ή ακόμα, τους ενημερώνουν με ψευδείς πληροφορίες με σκοπό την παρότρυνσή τους για την αγορά των συγκεκριμένων μετοχών.

Χαρακτηριστικό παράδειγμα μεταξύ άλλων αποτελεί το σκάνδαλο της χρηματιστηριακής εταιρείας ¨Δέλτα¨. Διαδόθηκαν ψευδείς πληροφορίες μέσω του internet και δημιουργήθηκε τεχνητή ζήτηση, επομένως και κατακόρυφη αύξηση της τιμής των μετοχών της. Μ΄αυτόν τον τρόπο οι κάτοχοι μεγάλου αριθμού μετοχών κατάφεραν να τις πωλήσουν σε ιδιαίτερα υψηλή τιμή.

(ε). Στις τηλεπικοινωνίες οι παραβάσεις μέσω Η/Υ έχουν εξίσου μεγάλη συχνότητα εμφάνισης. Διεθνείς ή υπεραστικές κλήσεις με τον κατάλληλο προγραμματισμό και ¨σπάσιμο¨ κωδικών χρεώνονται ως αστικές. Δεν έχουν λείψει, βέβαια, και οι οργανωμένες ομάδες παραβατών που νοικιάζουν με την ώρα τις τηλεφωνικές γραμμές, κυρίως για διεθνείς κλήσεις, και καρπώνονται τεράστια ποσά.

Κάτι ανάλογο συνέβη στην Κρήτη, όπου Σύριοι καταχραστές χρησιμοποιώντας 19 γραμμές ISDN (με κάθε τέτοια γραμμή μιλούν συγχρόνως 3 άτομα) χρέωναν τον ΟΤΕ. Ταυτόχρονα

στην Συρία, στον στον ειδικά διαμορφωμένο χώρο που είχαν δημιουργήσει, πελάτες πλήρωναν "ενοίκιο"για να τηλεφωνήσουν. Το κόστος για τον ΟΤΕ από την υπόθεση αυτή ανήλθε στα 480 εκατομμύρια δραχμές σε έναν μήνα, ποσό που αυξανόταν επικίνδυνα αν η σπείρα δεν εξαρθρωνόταν εγκαίρως.

(στ). Στον κυβερνοχώρο βρίσκουν ιδιαίτερα πρόσφορο έδαφος πολιτικοί φανατισμοί, ακραίες ιδεολογίες και ρατσιστικές πεποιθήσεις. Άτομα ταυτισμένα με κάποια ιδέα αγωνίζονται ώστε ν'αυξηθεί ο αριθμός των ομοϊδεατών τους, εκθέτοντας συχνά υπερβολικές πληροφορίες και ψευδή στοιχεία προκειμένου να πείσουν όσο το δυνατόν περισσότερα άτομα.

Συχνά γίνονται και επιθέσεις προς μια άλλη ομάδα με κάποιο διαφορετικό χαρακτηριστικό. Άνθρωποι με κριτήριο το χρώμα,τον τόπο προέλευσης ή κατοικίας τους, τα πιστεύω τους βρίσκονται συχνά στο στόχαστρο τέτοιων επιθέσεων.

(ζ). Η διασπορά ιού αποτελεί μια βασική μορφή ηλεκτρονικού βανδαλισμού. Καθώς κάθε σύστημα έχει τα τρωτά του σημεία και τις ατέλειές του, παρουσιάζονται οι ιοί για να τις χρησιμοποιήσουν. Κατά έναν παράξενο τρόπο οι ιοί έχουν πάντα τον τρόπο να "προσπερνάνε" τα έως τότε ήδη υπάρχοντα συστήματα ασφαλείας (anti-virus) και να προκαλούν αποπροσανατολισμό προγραμμάτων, την αχρήστευση πληροφοριών και την μείωση της αξιοπιστίας ενός συστήματος επεξεργασίας δεδομένων. Αν λάβουμε υπ'όψιν και το χαρακτηριστικό τους ότι έχουν την δυνατότητα να μένουν για μεγάλο χρονικό διάστημα μέχρι να δράσουν και δύσκολα γίνονται αντιληπτοί, τότε αναφερόμαστε στην επικινδυνότητα ενός ιού.

Τ'αποτελέσματα μπορεί να είναι από την απλή λήψη πρωτοβουλίας από τον Η/Υ χωρίς την κατάλληλη εντολή, μέχρι μια καταστροφή του σκληρού δίσκου του.

Χαρακτηριστικό παράδειγμα αποτελεί ο ιός Melissa που εμφανίστηκε το 1998 και προκάλεσε πανικό σε πολλούς Η/Υ και χρήστες αυτών. Όταν ανοιχτεί το μήνυμα γίνεται αυτόματη μόλυνση του Η/Υ και εν συνεχεία αποστέλλεται και σ'όλες τις διευθύνσεις e-mail που υπάρχουν με σκοπό να εξαπλωθεί και να μολύνει και άλλα συστήματα.

(η).Ένα μεγάλο ποσοστό λογισμικού εκτίθεται σε παράνομη προσφορά. Καταπατώντας το δικαίωμα του αποκλειστικού δικαιώματος και της πνευματικής ιδιοκτησίας, χάκερς ιδιωτικοποιούνται προγραμμάτων Η/Υ και τα πωλούν σε πολύ χαμηλές τιμές. Έτσι, το ποσοστό επικινδυνότητας για έναν χρήστη να πέσει θύμα αγοράς παράνομου λογισμικού φτάνει το 60 % , καθώς οι καταχραστές έχουν ποικίλους τρόπους να προωθούν τα προϊόντα τους χωρίς να γίνονται αντιληπτοί.

Οι μορφές με τις οποίες κάποιος μπορεί να δεχτεί ή να πέσει θύμα ηλεκτρονικού βανδαλισμού είναι πολλές, καθώς με την τεράστια αύξηση του αριθμού των χρηστών του Internet αυξάνονται ανάλογα και οι crackers, οι οποίοι βλέπουν από άλλη οπτική γωνία τον χώρο του διαδικτύου.

3.ΠΡΩΤΑΓΩΝΙΣΤΕΣ

α.-Δράστες

Ο όρος χάκερ εμφανίστηκε σχεδόν ταυτόχρονα με τους ηλεκτρονικούς υπολογιστές. Αρχικά, τα άτομα αυτά ασχολήθηκαν εκτενέστερα με την χρήση των Η/Υ και την τεχνολογία τους, με απώτερο σκοπό την εξέλιξη στον τομέα αυτόν. Ήταν οι επιστήμονες των Η/Υ, οι οποίοι υπερβαίνοντας τα δεδομένα και ήδη γνωστά, σημείωσαν τεράστια άλματα προόδου. Σταδιακά, όμως, ο ρόλος τους αλλοιώθηκε και "πέρασε" στο αντίθετο στρατόπεδο.

Οι "ειδήμονες" στον χώρο του Internet έχουν προσδιορίσει κάπως έτσι τον ορισμό του χάκερ: "***Είναι, κυρίως, προγραμματιστές με ιδιαίτερα υψηλό επίπεδο γνώσεων όσον αφορά τα λειτουργικά συστήματα και τις γλώσσες προγραμματισμού***". Το σημείο, όμως, που εστιάζουν οι χάκερς είναι το απόκρυφο μέρος ενός λειτουργικού συστήματος, όπου προσπαθούν ν'ανακαλύψουν τυχόν "αδυναμίες", ελλείψεις ή κενά, τους λόγους ύπαρξης αυτών, καθώς και με ποιό τρόπο μπορούν να "δουλέψουν" πάνω σ'αυτά και να τα χρησιμοποιήσουν.

Ένας χάκερ ποτέ δεν καταστρέφει. Διεισδύει καταχρηστικά σε δεδομένα,αρχεία, προγράμματα και σε οτιδήποτε άλλο αποτελεί τον στόχο του, συλλέγει πληροφορίες και εγκαταλείπει αφήνοντας πάντα αναγνωριστικά σημάδια.

Χαρακτηρίζονται ως άτομα με κατάρτση και έντονο ενδιαφέρον για το αντικείμενο με το οποίο ασχολούνται, καθώς επίσης,

τους διέπει η προδιάθεση για έρευνα σε τομείς που περιέχουν άλυτα θέματα, σύμφωνα με τις ήδη υπάρχουσες εφαρμοσμένες συμβατικές μεθόδους.

Κατά συνέπεια, αναφερόμαστε σε άτομα που δεν δημιουργούν τυχαίες λύσεις ή αποτελέσματα ευνοϊκής στιγμής, αλλά εξάγουν αποτελέσματα βαθιάς έρευνας (συνήθως όχι μακροχρόνιας) και εξειδικευμένης γνώσης. Η θεωρία και ταυτόχρονα κίνητρο των χάκερ που στηρίζει και διατηρεί έντονο τον ενθουσιασμό και την επιμονή τους αυτή, αποτελεί η πεποίθηση ότι δεν υπάρχει άλυτο πρόβλημα και μέρος του διαδικτύου στο οποίο δεν μπορούν να εισβάλλουν. Θεωρούν, επίσης, ότι έχουν πολύ δουλειά ακόμα καθώς υπάρχει πληθώρα προβλημάτων που περιμένουν την λύση τους.

Ένα άλλο βασικό σημείο στην ιδεολογία των χάκερ είναι ότι η υπερβολική προσπάθεια πρέπει να έχει αποτέλεσμα, αλλιώς είναι σπατάλη χρόνου. Πάνω σ΄αυτό βασίζεται και ο κανόνας ότι ένα πρόβλημα εφόσον βρεί την λύση του, πρέπει να γνωστοποιηθεί σ'όλα τα μέλη της κοινότητάς τους ώστε να μην χαθεί χρόνος από άλλα άτομα στην προσπάθεια να λύσουν το συγκεκριμένο. Η μοναδική περίπτωση που ¨επιτρέπεται¨ κάποιος ν'ακολουθήσει τα ίδια βήματα είνα μόνο όταν αποβλέπει σε κάτι περαιτέρω της ήδη υπάρχουσας λύσης.

Βασικές αρχές που διέπουν τους χάκερς είναι η ελευθερία των πληροφοριών και των ήδη κεκτημένων γνώσεων. Υπάρχει ιδιαίτερα έντονη αμφισβήτηση της εξουσίας και εναντίωση σ'αυτήν. Ο ρατσισμός δεν υφίσταται στον χώρο αυτό. Όλοι είναι ίσοι χωρίς να διαχωρίζονται βάσει την μόρφωση, την ηλικία, τα σωματικά γνωρίσματα, την εργασία ή οτιδήποτε άλλο διαχωρίζει τους ανθρώπους στην καθημερινή κοινωνική ζωή. Δεν αποδέχονται την λογοκρισία και την απαγόρευση ή περιορισμό των κινήσεών τους και αντιδρούν έντονα σ'αυτό.

Οι περισσότεροι χάκερς είναι άτομα ιδιαίτερα έξυπνα με τεχνολογική ευφυΐα, όμως, κοινωνικά απομονωμένα. Δεν ενδιαφέρονται για την ενεύρεση μιας νόμιμης εργασίας και δεν αποβλέπουν, ασχολούμενοι με τον κυβερνοχώρο, στο κέρδος. Εστιάζουν την προσοχή τους, κυρίως, στην φήμη που θ'αποκτήσουν με την ενασχόληση αυτή και στην καταξίωση που δεν έχουν βρεί στην κοινωνική τους ζωή. Με την εισβολή τους και αφήνοντας τα σημάδια τους, υπενθυμίζουν στην κοινωνία και στα μέλη της που μέχρι τότε τους αγνοούσαν ότι υπάρχουν και μάλιστα έχουν ισχύ,δύναμη και εξειδικευμένες ικανότητες.

Όλα τα παραπάνω υποστηρίζονται από την Βρεττανική Επιτροπή Πρόγνωσης και Πρόληψης Εγκλήματος (6), η οποία τονίζει ότι υπάρχουν αυξημένες πιθανότητες ένας διαδικτυακός παραβάτης να εντάσσεται σε κάποιες κατηγορίες .

Συνήθως είναι άτομα πάνω από 15-45 ετών, κυρίως άνδρες, άνεργοι καθώς πρόκειται κυρίως για άτομα νεαρής ηλικίας, και έχουν γνωρίσματα κοινωνικής απομόνωσης. Με την ενασχόλησή τους σ'αυτόν τον τομέα δεν νιώθουν αδύναμα μόρια της κοινωνίας. Επιπλέον, ο διαδικτυακός χώρος είναι ιδιαίτερα προσφιλής εφόσον δεν απαιτεί ιδιαίτερα σωματικά χαρίσματα, φυσικές δυνάμεις. Έχουν όλοι τις ίδιες ευκαιρίες.

Όπως αναφέρθηκε, οι χάκερς παρόλο που διεισδύουν σε ξένα προγράμματα και λειτουργικά συστήματα, δεν στοχεύουν στο να προκαλέσουν ζημιά. Αποσπούν ενδιαφέροντα γι'αυτούς στοιχεία και αποχωρούν (απλά αφήνοντας κάποια σημάδια). Κάτι τέτοιο, αντιθέτως, δεν ισχύει με τους crackers οι οποίοι αποβλέπουν σε περαιτέρω δραστηριότητα προς όφελός τους.

Εισβάλλουν παράνομα και προκαλούν ζημιές. Αφού αποσπάσουν τις πληροφορίες που τους ενδιαφέρουν καταστρέφουν τα πάντα. Διαγράφουν αρχεία, αποσυντονίζουν προγράμματα, διαγράφουν σκληρούς δίσκους, μπλοκάρουν ακόμα τεράστια και καλά οργανωμένα συστήματα.

Σε αντίθεση με τους χάκερς που κατευθύνονται από την σταδιακή συλλογή και επεξεργασία γνώσεων, οι crackers δεν κατέχουν γνωστικά το αντικείμενο και της τεχνολογίας των Η/Υ και τους ενδιαφέρει μόνο ο άμεσος στόχος τους, η καταστροφή.

Παρόλο που οι χάκερς διαχωρίζουν την ¨κοινότητά ¨τους από αυτή των cracker, για την αποφυγή ομοιοποίησής τους (δεν θα ήθελαν σε καμία περίπτωση να χαρακτηριστούν ασυνείδητοι καταστροφείς και βάνδαλοι του διαδικτύου), οι crackers επιδιώκουν το ακριβώς αντίθετο για την αφομοίωση τους από την ¨εκλεκτή ¨κοινωνία των χάκερς.

Εξετάζοντας τα περιστατικά που έχουν καταγραφεί και αφορούν περιπτώσεις ηλεκτρονικού βανδαλισμού καθώς και μαρτυρίες, καταλήγουμε σε καταγραφή κινήτρων τα οποία με ωφελιμιστική ή μη σκοπιμότητα καθορίζουν τον τρόπο δράσης των χάκερ.

Αναφερόμενοι στον ηλεκτρονικό βανδαλισμό οδηγούμαστε σε δύο μορφές του. Η πρώτη είναι η ηλεκτρονική παρείσδυση, κατά κύριο λόγο αυθαίρετη, στον διαδικτυακό χώρο και ειδικότερα σε ιδιωτικά μέρη. Η δεύτερη αφορά στην πρόκληση ζημιάς σ'ολόκληρο το σύστημα ή σε τμήμα του και στα περιεχομενά του.

Μια ακόμα μορφή επίθεσης εξίσου διαδεδομένη είναι και οι ιοί, για τους οποίους θα γίνει λόγος παρακάτω.

Κατατάσσοντας, λοιπόν, τα διαδικτυακά εγκλήματα αναλόγως με την αιτιολογία τους, μπορούμε να πούμε ότι οφείλονται σε:

(α) Οικονομικά κίνητρα

Αποτελούν τις συχνότερες αιτίες παράνομης δραστηριότητας στο Internet.Οι δράστες καταπατώντας τα δικαιώματα και την πνευματική ιδιοκτησία άλλων προσπαθούν να αποσπάσουν στοιχεία, να τα χρησιμοποιήσουν προς όφελός τους και ν' αποκομήσουν κέρδη.

Μια τέτοια περίπτωση αποτελεί η κλοπή πνευματικών δικαιωμάτων και δημιουργημάτων, ευρεσιτεχνιών και η μετέπειτα παράνομη πώλησή τους. Επίσης, η διακίνηση πορνογραφικού υλικού σε ιστοσελίδες, καθώς και η προώθηση της πορνείας των ανηλίκων μέσω του Internet.

(β) Κοινωνικά κίνητρα

Την κατηγορία αυτή μπορούμε να την εξετάσουμε σε δύο παραμέτρους. Η πρώτη αφορά άτομα τα οποία επιζητούν την κοινωνική καταξίωση και αναγνώριση. Ένιωθαν ως τότε μειονεκτικά και ίσως παραμερισμένα από την κοινωνία και μέσω μιας τέτοιας ενέργειας θέλησαν ν'αποδείξουν τις δυνατότητές τους.

Η άλλη περίπτωση αναφέρεται σε άτομα που αποσκοπούν αρχικά στην αναγνώριση σαν αξιόλογοι χάκερς και μετέπειτα στην επαγγελματική σταδιοδρομία τους. Πολλοί από αυτούς

προσλαμβάνονται από μεγάλες εταιρείες σαν σύμβουλοι ασφάλειας με υψηλές αποδοχές καθώς είναι ιδιαίτερα χρήσιμοι. Επίσης, αρκετά συχνά hackers συνεταιρίζονται και δημιουργούν εταιρείες συμβουλών ασφαλείας επιχειρήσεων. Αντιπροσωπευτικό παράδειγμα αποτελεί η περίπτωση του Kevin Mitnick, του διασημότερου χάκερ.

(γ) Φιλομαθή κίνητρα

Αυτή η περίπτωση αν και λιγότερο συνηθισμένη, αντιπροσωπεύει ένα ποσοστό των χάκερς. Αναφερόμαστε στους ¨καλούς¨ χάκερς οι οποίοι διακατέχονται από αυξημένη περιέργεια και δεν ικανοποιούνται από την ¨νόμιμη ¨ γνώση και επιζητούν την λιγότερο γνωστή στο ευρύ κοινό και κατά την άποψή τους πιο σημαντική πληροφόρηση. Στις αρχές τους ανήκει το ρητό ¨ο σκοπός αγιάζει τα μέσα!¨

(δ) Πολιτικά κίνητρα

Είναι μία αρκετά συνηθισμένη αιτία δράσης στο κόσμο του Internet. Αποτελεί έναν τρόπο επανάστασης και εναντίωσης στο ήδη υπάρχων πολιτικό σύστημα του οποίου η αξιοπιστία χάνεται απέναντι στο ευρύ κοινό μ'αυτόν τον τρόπο, καθώς γνωστοποιούνται οι αδυναμίες του.

Ιδιαίτερα συνηθισμένη περίπτωση είναι η κατασκοπεία.Στο βωμό της πολιτικής πεποίθησης επιτρέπεται η παράνομη παρακολούθηση και καταγραφή στοιχείων. Σε πολλές περιπτώσεις οι χάκερς καθοδηγούνται από κυβερνήσεις ή μεγάλες εταιρείες.

β.Θύματα

Η ασφάλεια των υπολογιστών είναι ένα επίκαιρο θέμα το οποίο μας αφορά όλους άμεσα, λόγω των τεράστιων διαστάσεων που έχει καταλάβει, είτε είμαστε χρήστες του Internet, είτε απλοί παρατηρητές των γεγονότων.

Το ερώτημα που αποτελεί την βάση των πραγμάτων και η απάντησή του μας κατευθύνει προς την σωστή αναζήτηση , είναι το γιατί κάποιος γίνεται στόχος ενός hacker.

Ένας χάκερ αναζητά τα θύματά του μεταξύ χιλιάδων διευθύνσεων. Υπάρχει το ενδεχόμενο τυχαίας επιλογής ενός θύματος. Ο χάκερ χρησιμοποιώντας μια τυχαία διεύθυνση ενός χρήστη αρχίζει την επίθεση . Συνήθως, όμως, υπάρχει συγκεκριμένος λόγος επίθεσης οπότε και επιλέγει με τα σχετικά κριτήρια τα θύματά του. Με την βοήθεια ενός σαρωτή θυρών (πχ nmap)(7) και εισάγοντας ένα μεγάλο αριθμό διευθύνσεων, ύστερα από την κατάλληλη διαδικασία καταλήγει στα υποψήφια θύματά του, τα οποία αποτελούν τρωτούς στόχους.

Πιθανές αιτίες που κρίνουν κάποιον ως ιδανικό στόχο είναι ποικίλες. Οι συνηθέστερες είναι η εξοικονόμηση χρημάτων, η δυσφήμιση, η κλοπή πληροφοριών.

Κριτήριο για το εάν ένας χρήστης από την στιγμή που θα εισέλθει στον χώρο του Internet αποτελεί στόχο είναι τί είδους χρήστης είναι, ανάλογα με την βαρύτητα που έχει ως άτομο. Κάποιος που εργάζεται σε μια μεγάλη εταιρεία και έχει στην κατοχή του πληροφορίες και στοιχεία ιδιαιτέρως ενδιαφέροντα και προσοδοφόρα, κρίνεται, σαφώς, πιθανότερος στόχος.

Χαρακτηριστικό παράδειγμα αποτελεί η Microsoft η οποία αποτελεί καθημερινό στόχο επίδοξων χάκερ, καθώς αποτελεί μια

εταιρεία με το πλουσιότερο λογισμικό του πλανήτη. Οι επιχειρηματικές πληροφορίες που θα αποσπούσε κάποιος που θα έφτανε στο στόχο του θα ήταν ανεκτίμητης αξίας.

Καταλήγοντας,θα μπορούσαμε να ταξινομήσουμε τα θύματα στις εξής κατηγορίες:

1.Οικιακοί χρήστες και μικρές επιχειρήσεις

Τα άτομα που ανήκουν στην κατηγορία αυτή κρίνουν ως δευτερεύουσας σημασίας το θέμα ασφάλειας των συστημάτων τους. Θεωρούν ότι λαμβάνοντας τα τυπικά παραδοσιακά μέτρα ασφαλείας είναι προστατευμένοι από κάθε είδους διαδικτυακή επίθεση. Σ'αυτό συμβάλλει και η άγνοιά τους ως ερασιτέχνες με αποτέλεσμα να γίνονται συχνά στόχος.

Επιπλέον, η απασχόληση ενός διαχειριστή συστημάτων σε μια μικρή ή μέτρια επιχείρηση αποτελεί ένα έξοδο που κρίνεται περιττό. Έτσι, αρκούνται σε τυπικά μέτρα ασφαλείας που ίσως να είναι ήδη τρωτά και "απαρχαιωμένα". Οι επιθέσεις που συνήθως δέχονται είναι η άρνηση υπηρεσιών και οι ιοί.

2.Μεγάλες επιχειρήσεις και Οργανισμοί

Εταιρείες και Οργανισμοί κολλοσσοί στο χώρο τους, με απώτερο σκοπό των εισβολέων την εξοικονόμηση χρημάτων μέσω της κλοπής πληροφοριών, ή και την δυσφήμισή τους γίνονται στόχοι των crackers. Οι επιθέσεις αποσκοπούν σε φθορές, άρνηση υπηρεσιών,

κλοπή δεδομένων των πελατών των επιχειρήσεων, κλοπή κωδικών πιστωτικών καρτών και μια λίστα με άλλες παραβάσεις. Από το στόχαστρο δεν έχουν λείψει κατά καιρούς και εταιρίες ασφάλειας δικτύων, οι οποίες αποτελούν ισχυρή πρόκληση για τους εισβολείς.

Κάτι τέτοιο συνέβη τον Οκτώβριο του 2000 στην Microsoft όταν ένας εργαζόμενος ανοίγοντας ένα E-mail μ'έναν Δούρειο Ίππο έδωσε την δυνατότητα πρόσβασης στο δίκτυο της εταιρείας, απ'όπου διέρρευσαν πληροφορίες.

3.Οικονομικοί Οργανισμοί

Τράπεζες, πιστωτικά ιδρύματα και άλλες μορφές οικονομικών οργανισμών αποτελούν τους πιθανότερους στόχους επίθεσης λόγω της οικονομικής φύσης τους. Οι εισβολείς αποβλέπουν στο χρηματικό όφελος καθαρά και όχι μόνο στην αναγνώρησή τους ως ικανοί εισβολείς.

Από την άλλη πλευρά, οι οργανισμοί έχουν ιδιαίτερα εξελιγμένα συστήματα προστασίας διαθέτοντας αξιοσέβαστα χρηματικά ποσά για τον σκοπό αυτόν. Αποτελεί πρώτιστη ανάγκη η διασφάλιση της φήμης τους, της αξιοπιστίας προς τους πελάτες τους και η συνέχιση της ύπαρξής τους. Έτσι, αν και συχνότατα γίνονται στόχος, μεμονωμένες είναι οι περιπτώσεις που τελικά υπήρξαν θύματα με σημαντικές απώλειες.

4. Κυβερνητικά και Στρατιωτικά Ινστιτούτα

Παρόλο το γεγονός ότι στις περιπτώσεις αυτές τα επίπεδα ασφαλείας είναι ιδιαίτερα υψηλών προδιαγραφών και η

απόπειρα εισβολής στα συστήματά τους τιμωρείται αυστηρά, (π.χ. στις ΗΠΑ θεωρείται ομοσπονδιακό έγκλημα), καθημερινά καταγράφονται προσπάθειες παραβίασής τους .

Παρά την αυξημένη προστασία τους υπάρχουν και επιτυχείς επιθέσεις crackers χωρίς, όμως, να εντοπίζονται,καθώς για να καταφέρει κάποιος να πραγματοποιήσει την εισβολή του θεωρείται ιδιαίτερα ικανός και ευέλικτος στον χώρο αυτόν. Συνήθως, οι επιτιθέμενοι προέρχονται από άλλη χώρα (κάτι που συμβάλλει στον μη εντοπισμό τους) και έχουν ανταγωνιστικές βλέψεις, κυρίως σε εθνικό επίπεδο.

Ιοί

Ο πιο συνηθισμένος τρόπος επίθεσης στο χώρο του Internet είναι οι ιοί. Οι χάκερς χρησιμοποιώντας τους σαν "εργαλείο" εισβάλλουν στα προγράμματα που έχουν αδύνατα σημεία.

Καθώς, όμως, οι ιοί χαρακτηρίζονται ως μια μορφή προγράμματος (ίσως και "αντιπρογράμματος", αν μπορούμε να δεχτούμε τον όρο αυτό), εισχωρούν και εκτελούν την προκαθορισμένη τους "αποστολή ". Συνήθως, προκαλούν άρνηση λειτουργίας συστήματος και άλλες φορές καταστροφές σε προγράμματα. Μέχρι τώρα, όμως, δεν έχουν σημειωθεί καταστροφές σε εξοπλισμό (hardware). Έχουν, ακόμα, το γνώρισμα ότι δεν ενεργοποιούνται αμέσως αλλά σε προκαθορισμένη μελλοντική στιγμή.

Ο όρος "computer virus" χρησιμοποιήθηκε για πρώτη φορά το 1984, αν και αρκετά νωρίτερα είχαν κάνει την εμφάνισή τους ,όταν ο Fred Cohen έδωσε έναν ορισμό. Σύμφωνα με τον τότε φοιτητή του πανεπιστημίου της Καλιφόρνια " ***ιός είναι κάθε***

πρόγραμμα το οποίο μπορεί να μολύνει τα άλλα προγράμματα, ώστε να συμπεριλαμβάνουν ένα εξελιγμένο αντίγραφό του¨(8)

Αν κάνουμε μια αναδρομή θα δούμε ότι οι ιοί στην πρώϊμη μορφή τους χρησιμοποιήθηκαν από τους χάκερς την δεκαετία του ΄60 ως μέσο ψυχαγωγίας μεταξύ τους. Ύστερα από εκτενή παρατήρηση είδαν ότι ο Η/Υ δεχόμενος τον ιό και ύστερα από μικρό χρονικό διάστημα ¨σκέψης¨, δημιούργησε νέους κανόνες δράσης, αγνοώντας τους ήδη υπάρχοντες, για να καταφέρει ν'ανταπεξέλθει και να μην αποσυντονιστεί. Σαν ¨πρόγραμμα σκέψης¨ χρησιμοποίησαν το σκάκι του οποίου οι κινήσεις υπάγονται σε κανόνες. Έτσι, ο Η/Υ έκανε κινήσεις οι οποίες ήταν εκτός των κανόνων αυτών.

Η χρησιμοποίηση ενός ιού δεν έχει πάντα τον ίδιο τρόπο δράσης και τα ίδια αποτελέσματα. Οι τρείς συνηθισμένες περιπτώσεις είναι:

-Στην πρώτη περίπτωση ο ιός σβήνει αρχεία και καταστρέφει δεδομένα. Η καταστροφή είναι ολοκληρωτική.

-Το περιεχόμενο των αρχείων και τα δεδομένα αποκτούν κωδικοποιημένη σημασία, κάτι το οποίο καθιστά αδύνατο στον χρήστη να έχει πρόσβαση σ'αυτά.

-Η Τρίτη, λιγότερο επικίνδυνη, αλλά εξίσου αποτελεσματική περίπτωση δράσης των χάκερ είναι η καθήλωση του συστήματος. Αυτό λειτουργεί μετά την εισβολή του ιού με εξαιρετικά αργούς ρυθμούς, τόσο που είναι αρκετά δύσκολο, αν όχι αδύνατον, να λειτουργήσει. Έτσι, ανάλογα με την δράση ενός ιού έχουμε και την ένταξή του σε κατηγορία. Οι βασικότερες, διεθνώς γνωστές είναι οι ¨Δούρειοι Ιπποι¨ (Trojan Horses),οι λογικές βόμβες¨ logic bombs¨ σκουλήκια¨worms¨.

Οι "Δούρειοι Ιπποι" (Trojan Horses) είναι η πιο συνηθισμένη περίπτωση ιού. Πρόκειται για πρόγραμμα κρυμμένο το οποίο διαγράφει κείμενα ,στατιστικά στοιχεία στον σκληρό δίσκο και οποιοδήποτε άλλο πρόγραμμα. Συνηθισμένος τρόπος μετάδοσης είναι ακόμα και μια απλή δισκέτα που περιέχει ένα μολυσμένο πρόγραμμα και εν συνεχεία θα χρησιμοποιηθεί σ'έναν άλλο Η/Υ. (9)

Οι "λογικές βόμβες" (Logic Bombs) προγραμματίζονται για να δράσουν σε προκαθορισμένη στιγμή ή ακόμα μετά από ένα συγκεκριμένο γεγονός. Η βασική διαφορά από τις άλλες μορφές είναι ότι δεν μολύνουν ένα συγκεκριμένο τμήμα του Η/Υ (π.χ. ένα στατιστικό πίνακα) αλλά ολόκληρο το λογισμικό του.(10)

Τα "σκουλήκια" (Worms) μετακινούνται αυτόνομα και μέσω του μηχανισμού των Η/Υ μολύνουν σταδιακά όλες τις συνδεδεμένες μονάδες. Η διαφοροποίηση από τις άλλες περιπτώσεις είναι ότι δεν χρησιμοποιούν την "περίεργη λογική "τους αλλά απλά κινούνται από σύστημα σε σύστημα.(11)

Ακριβής απάντηση στο ερώτημα ποιοί κατασκευάζουν τους ιούς και γιατί δεν μπορεί να δοθεί για τον λόγο ακριβώς ότι η απάντηση στο ερώτημα θ'αποτελούσε και την λύση του προβλήματος. Οι περισσότεροι δημιουργοί ιών έχουν διατηρήσει την ανωνυμία τους για την αποφυγή των συνεπειών. Υπάρχουν,όμως, και κάποιες ομάδες, κυρίως νεαρά άτομα, που το κάνουν για λόγους καθαρά επίδειξης των ικανοτήτων τους.

Να επισημάνουμε ότι στην αλματώδη εξάπλωση των ιών συνετέλεσαν καθοριστικά δυο παράγοντες. Ο πρώτος είναι η πλέον προηγμένη τεχνολογία που τους έκανε ισχυρότερους. Όπως ακριβώς ένας βιολογικός ιός με την χορήγηση αντιβιοτικών ενδυναμώνεται,έτσι και τα anti-virus προγράμματα κάνουν τους ιούς πιο ευέλικτους, ώστε

τελικά να επιτύχουν τον στόχο τους και να πραγματοποιήσουν την αποστολή τους.

Ένας ακόμα καθοριστικός παράγοντας διάδοσής τους είναι η σύνδεση των Η/Υ σ'ένα τεράστιο δίκτυο. Πλέον αναφερόμαστε σε εκατομμύρια χρήστες οι οποίοι έχουν όλοι πρόσβαση μεταξύ τους. Εκτός, όμως, από την συμβατότητα που υπάρχει μεταξύ Η/Υ, χρησιμοποιούνται και κοινά λογισμικά, προγράμματα και λειτουργικά συστήματα για εξοικονόμηση χώρου, χρήματος και χρόνου. Ακόμα και ιστοσελίδες "εκπέμπουν" ιούς που μεταδίδονται σ'αυτούς που συλλέγουν στοιχεία απ'αυτές .

4.ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ – ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

Παράγοντες όπως η έλλειψη χειροπιαστών αποδείξεων, η πολυμορφία των διαδικτυακών παραβάσεων, η ύπαρξη μεγάλου αριθμού δεδομένων και η κωδικοποίηση και εξαφάνιση των αποδείξεων, καταστέλλουν το έργο της ουσιαστικής αντιμετώπισης της ηλεκτρονικής παραβατικότητας. Κυρίως, αν προσθέσουμε και το γεγονός ότι οι διωκτικές αρχές δεν διαθέτουν πλήρη, ουσιαστική εικόνα της πληροφορικής τεχνολογίας και επιστημονική κατάρτηση πάνω στον τομέα αυτό. Συνέπεια αυτού είναι η καθαρά εγκληματική προσέγγιση των κρουσμάτων και η απλή καταγραφή τους στο ιστορικό των παραβάσεων ως κοινωνικών και νομικών παρεκκλίσεων.

Όσον αφορά τα μέτρα ασφαλείας που μπορεί να λάβει ένας χρήστης του Internet,που ίσως πρόκειται για ένα μελλοντικό θύμα, σχεδόν ταυτίζονται με τους τρόπους αντιμετώπισης. Οι ενέργειες είναι οι ίδιες ώστε ν'αποφευχθεί μια επίθεση προς έναν εξειδικευμένο ή έναν λιγότερο έμπειρο χρήστη.Συνοπτικά:

(1.) Οποιοδήποτε e-mail ή αρχείο που λαμβάνει ένας Η/Υ μέσω του διαδικτύου είναι πιθανό να περιέχει κάποιον ιό, ιδίως όταν η προέλευσή του είναι άγνωστη. Σε μια τέτοια περίπτωση η διαγραφή του θ' αποτελούσε την γνωστικότερη ενέργεια από μέρους του χρήστη.

(2.) Η συλλογή αρχείων από τοποθεσίες του διαδικτύου που δεν είναι ικανοποιητικά αξιόπιστες προσφέρει γόνιμο έδαφος σε οποιονδήποτε που ¨κυκλοφορεί ¨εκεί να εισέλθει στον Η/Υ. Η προσεκτικότερη αναζήτηση πληροφοριών και μόνο από αξιόπιστες

πηγές (π.χ. Microsoft) αποτελούν μια βασική προϋπόθεση συνέχισης της υγιούς λειτουργίας του Η/Υ.

(3.) Η συνεχής αναβάθμιση της βάσης δεδομένων του προγράμματος αντιμετώπισης ιών (anti-virus) είναι μια ενέργεια που μειώνει τις πιθανότητες πρόληψης από κάποιον ιό, καθώς εισάγονται νέα "εργαλεία" αντιμετώπισής τους.

(4.) Μια ικανή μέθοδος αντιμετώπισης των ιών είναι τα αντίγραφα ασφαλείας. Λαμβάνοντας αντίγραφα για όλα τα αρχεία δεδομένων, σε οποιαδήποτε πιθανή μόλυνση από κάποιον ιό η επανεγκατάστασή τους είναι μια εύκολη και καθόλου χρονοβόρα διαδικασία.

(5.) Η ηθική διαπαιδαγώγηση των χρηστών θεωρείται πρωτεύουσα ανάγκη. Οποιονδήποτε ρόλο και αν κατέχει κάποιος (μαθητης, εργαζόμενος, γονέας, κτλ) θα πρέπει να έχει παιδεία όσον αφορά την χρήση Η/Υ.

Ειδικότερα, τα άτομα που έχουν πρόσβαση σ'έναν Η/Υ θα πρέπει να είναι άτομα εξουσιοδοτημένα και απόλυτης εμπιστοσύνης,ιδιαίτερα όταν πρόκειται για επιχείρηση. Για την πρόσβασή τους πρέπει να καθορίζονται κωδικοί πρόσβασης (passwords), οι οποίοι να ανανεώνονται συχνά για την αποφυγή κλοπής από μη εξουσιοδοτημένα άτομα. Ακόμα και η πρόσβαση ενός χρήστη, όμως, πρέπει να έχει περιορισμένες δυνατότητες εφαρμογών και λειτουργίας,κάτι που πρέπει να έχει προκαθοριστεί.

Η διατήρηση αντιγράφων ασφαλείας (BACKUP)(12) αποτελεί απαραίτητη προϋπόθεση για έναν χρήστη, ιδίως όταν

πρόκειται για επιχείρηση, ώστε να αποφύγει την αχρήστευση ή την δυσλειτουργεία τμήματος του εξοπλισμού για κάποιο χρόνικό διάστημα. Τα αντίγραφα αναφέρονται και στον εξοπλισμό, αλλά και στα δεδομένα που έχουν εγκατασταθεί σ'έναν Η/Υ. Στην πρώτη περίπτωση όταν εμφανιστεί πρόβλημα σ'ένα υλικό κομμάτι του Η/Υ, με τ'αντίγραφα ασφαλείας γίνεται επαναφορά του συστήματος αναπτύσσοντας μια διαδικασία αντιμετώπισης του σφάλματος.

Όσον αφορά τ'αντίγραφα ασφαλείας δεδομένων, σε περίπτωση απώλειας λόγω αποτυχίας του προγράμματος, δυσλειτουργείας του υλικού κτλ, εξασφαλίζουν την εξολοκλήρου παραμονή τους και δεν υπάρχει απώλεια τμημάτων αυτών.

Στους προσωπικούς Η/Υ η πιο συνηθισμένη μέθοδος ασφάλειας είναι η χρησιμοποίηση κλειδιών, τα οποία, όμως είναι εύκολο να παρακαμφθούν από κάποιον γνώστη του αντικειμένου. Μια άλλη μορφή είναι η χρησιμοποίηση του κατάλληλου λογισμικού για το κλείδωμα ενός τμήματος των πληροφοριών χωρίς να "κλειδωθεί" ολόκληρος ο Η/Υ.

Τα δεδομένα, δηλαδή, του συγκεκριμένου χρήστη τοποθετούνται σ'έναν δίσκο ο οποίος είναι κλειδωμένος και όλα τα στοιχεία που περιέχονται είναι κρυπτογραφημένα. Συνεπώς, η χρησιμοποίησή τους γίνεται μόνο από τον συγκεκριμένο χρήστη που χρησιμοποιεί τον κωδικό.

Όταν αναφερόμαστε σ'ένα δίκτυο ή ομάδα δικτύων, η χρησιμοποίηση ενός Firewall(13) αποτελεί προστασία από οποιονδήποτε μη εξουσιοδοτημένο χρήστη θέλει να εισέλθει. Πρόκειται για έναν μηχανισμό ελέγχου πρόσβασης σ'ένα δίκτυο με την μορφή μιας ειδικά κατασκευασμένης και εξειδικευμένης συσκευής, η οποία μπορεί να είναι και ένας αυτόνομος Η/Υ, ο οποίος εκτελεί ένα ειδικά προσαρμοσμένο λογισμικό σύστημα.

Οποιαδήποτε προσπάθεια εισόδου στο δίκτυο από κάποιον άλλο χρήστη περνάει από επεξεργασία, "φιλτράρεται" και βασιζόμενο σε κανόνες και κριτήρια εισαγωγής προκαθορισμένα, αποφασίζεται ή όχι η εισαγωγή του.

Η χρησιμοποίηση anti-virus βοηθημάτων προστατεύει από την ύπαρξη και την εισαγωγή από ιούς. Προκειται για γενικό λογισμικό που περιλαμβάνει λογισμικό ανίχνευσης αλλαγών που πραγματοποιούνται στο σύστημα, και παρατήρησης διαφοροποιημένων συμπεριφορών.

Τα προγράμματα αυτά μπορεί να είναι μόνιμα τοποθετημένα ή να χρησιμοποιούνται κατ'απαίτηση και να σταματούν μόλις ολοκληρώσουν το έργο τους. Anti-virus(14) προγράμματα έχουν κυκλοφορήσει πολλές εταιρείες προστασίας λογισμικού. Μερικά ευρύτερα γνωστά είναι: Anti-Viral Toolkit Pro, Network Associates, Norton Anti-virus, Sophos Anti-Virus, κτλ.

Όσον αφορά τους τρόπους αντιμετώπισης του πληροφορικού εγκλήματος και της προσπάθειες εξάλειψής του, ,η ποινική νομοθεσία κατέχει κυρίαρχο ρόλο στη μορφή της παραδειγματικής τιμωρίας για αποφυγή νέων περιστατικών. Οι υποστηρικτές της άποψης ότι ο παραδειγματισμός αποτελεί κατασταλτικό παράγοντα της ηλεκτρονικής παραβατικότητας ενισχύουν την άποψη ότι η τιμωρία των συγκεκριμένων παραβατών πρέπει να είναι περισσότερο δραστική και αυστηρή για να έχει θετικά αποτελέσματα.

Πρέπει να είναι ανάλογη της παράβασης και ν'αποτελεί ταυτόχρονα και προστασία για τα άτομα που δέχονται τις συνέπειες τέτοιων ενεργειών, τα θύματα. Να υπάρχει σε κάθε περίπτωση διερεύνηση ώστε να μην τιμωρούνται τυχαία περιστατικά και ταυτόχρονα, τα μέτρα που θα ληφθούν να περιλαμβάνουν και κάθε νέα μορφή ηλεκτρονικής παραβατικότητας.

Κάτι τέτοιο, όμως, για να πραγματοποιηθεί πρέπει να υπάρξει σύμπραξη των ειδικών σε θέματα ασφαλείας ώστε να υπάρξει μεθοδευμένη και αποτελεσματική προσέγγιση. Απαραίτητη,όμως, είναι και η συμβολή των χάκερς που έχουν πια ενταχθεί στην "ομάδα" καταπολέμησης του ηλεκτρονικού εγκλήματος.

Όλος αυτός ο σχεδιασμός δράσης αναφέρεται σε κάθε μονάδα-έθνος. Επειδή, όμως, το φαινόμενο απασχολεί την διεθνή κοινότητα, η μεμονωμένη δράση δεν υφίσταται ως αποτελεσματική αντιμετώπιση. Η άποψη αυτή που έχει τις ρίζες της στα μέσα της δεκαετίας του '80, υποστηρίζει ότι πρέπει να υπάρξει διεθνής νομοθεσία, εναρμόνιση μεταξύ των δικαίων όλων των κρατών για την ομοιόμορφη απονομή δικαιοσύνης.

Σύμφωνα με τα αποτελέσματα παρατήρησης που εξήγαγε ο ΟΗΕ από το 1990 και έπειτα δεν έχουν γίνει βήματα προόδου στο ζήτημα της διεθνούς συνεργασίας και αυτό οφείλεται σε σε κάποιους παράγοντες, η υπέρβαση των οποίων θα επέφερε την οριστική αντιμετώπιση. Οι παράγοντες αυτοί είναι οι εξής:

1. Διαφωνία από τα κράτη όσον αφορά τη συμπεριφορά των ατόμων που οδηγούνται σε πληροφορικέςπαραβάσεις.

2. Δεν υπάρχει, επίσης, ομοφωνία στο όρο και την μορφή της παραβατικής συμπεριφοράς.

3. Οι υπεύθυνοι και τα άτομα που έχουν τον κυρίαρχο ρόλο στην προστασία και την αντιμετώπιση του φαινομένου (αστυνομία,δικαστήρια,κτλ) δεν διαθέτουν εμπειρία και επαρκή θεωρητική κατάρτιση.

4. Όσον αφορά την νομική αντιμετώπιση των παραβατών και τα άτομα που είναι υπεύθυνα γι'αυτό δεν έχουν πλήρη γνώση των ηλεκτρονικών υπολογιστικών συστημάτων.

5. Έλλειψη διεθνούς συνεργασίας μεταξύ των κρατών για την αμοιβαία έκδοση των παραβατών και βοήθειας για την κοινή δίωξη αυτών.

5. ΜΕΛΛΟΝΤΙΚΕΣ ΠΡΟΟΠΤΙΚΕΣ

Για κάθε χρήστη υπάρχουν πιθανότητες μόλυνσής του από κάποιον ιό. Έστω και αν το ποσοστό δεν μας φαίνεται ικανό να μας ανησυχήσει, θα πρέπει να υπάρχουν τ'απαραίτητα μέτρα ασφαλείας. Ο αριθμός των χρηστών του Internet αυξάνεται κατακόρυφα κάτι το οποίο σημαίνει ότι ανά πάσα στιγμή (έστω και τυχαία ή κατά λάθος) ενδέχεται να γίνουμε στόχος.

Τα προγράμματα ασφαλείας εξελίσσονται συνεχώς. Παράλληλη,όμως, είναι και η εφεύρεση από τους χάκερς νέων τρόπων επίθεσης. Μελλοντικά, αφενός ο αριθμός των χρηστών αυξάνει και αφετέρου τα άτομα που ασχολούνται συστηματικά είναι, πλέον, πλήρως καταρτισμένα επιστημονικά, συνεπώς, η επίθεση πρός τους λιγότερο έμπειρους χρήστες είναι εύκολη υπόθεση.

Ακριβώς αυτή η ανάγκη έχει οδηγήσει στην σχεδίαση συσκευών οι οποίες θ'αναγνωρίζουν προσπάθειες χρήσης λειτουργιών χωρίς έγκριση. Επίσης , έχουν δημιουργηθεί, και μελλοντικά θα κυκλοφορήσουν ευρέως, συσκευές που θ'αναγνωρίζουν την ταυτότητα του χρήστη από κάποια φυσικά χαρακτηριστικά του . Πρόκειται για τις βιομετρικές συσκευές που παρέχουν πλήρη στοιχεία του χρήστη, όπως μέρος που βρίσκεται,πότε πραγματοποίησε είσοδο στο σύστημα κτλ.

Όλα τα παραπάνω σε συνδυασμό με την εκπαίδευση πάνω στην ασφάλεια των πληροφορικών συστημάτων ενώ τώρα αποτελούν όχι κάτι απαραίτητο και άμεσης ανάγκης ενέργεια, μελλοντικά εκτιμάται ότι θα είναι βασικές προϋποθέσεις χρήσης ενός Η/Υ.

Υποστηρικτές της άποψης ότι η ποινική νομοθεσία πρέπει να εντατικοποιήσει τις προσπάθειες δίωξης των πληροφορικών

παραβάσεων, θέτουν επίσης το ζήτημα της πιο σκληρής τιμωρίας των παραβατών και την ελαχιστοποίηση των μέτρων που προστατεύουν τα άτομα αυτά. Θεωρούν ότι η τιμωρία πρέπει να είναι ανάλογη του εγκλήματος και καθόλου ελαστική, ώστε να υπάρξει πράγματι παραδειγματισμός και αποφυγή παρόμοιων πράξεων μελλοντικά.

Έτσι, τα μέτρα που θα ισχύσουν πρέπει να περιλαμβάνουν κάθε νέα μορφή παράβασης που θα εμφανιστεί. Θεωρείται, ακόμα, απαραίτητη η συμβολή ακόμα και χάκερ μαζί με άλλα εξειδικευμένα άτομα για την προστασία των συστημάτων και την αποτροπή παράνομων ενεργειών.

Υπάρχει, επίσης, και η άποψη αυτών που υποστηρίζουν ότι υπάρχει μεν το πρόβλημα, γίνεται, όμως, περισσότερο διογκωμένο καθώς αποβλέπει στην απορρόφηση του λογισμικού που κυκλοφορεί. Πραγματοποιείται, δηλαδή, μια διαφημιστική καμπάνια με σκοπό την επαγρύπνηση, αν όχι τον εκφοβισμό του, κάτι που τελικά επιφέρει τα επιθυμητά γι'αυτοαποτελέσματα.

ΕΠΙΛΟΓΟΣ

Οι πρώτοι χρήστες του Internet ως το 1970 δεν είχαν συνειδητοποιήσει τί θα επακολουθούσε. Τα κρούσματα ηλεκτρονικής παραβατικότητας που είχαν σημειωθεί ως τότε τα θεωρούσαν τυχαία. Μετά από μία δεκαετία, όμως, το φαινόμενο είχε πλέον "συστηματοποιηθεί" και οι περιπτώσεις ήταν καθημερινό φαινόμενο. Για άμυνα προς την δυσλειτουργία αυτή οι χρήστες αναγκάστηκαν ν'αναπτύξουν τις τεχνικές τους, κάτι που ταυτόχρονα συνέβη και από την αντίπερα όχθη,τους χάκερς. Έτσι δημιουργήθηκε η κατάσταση που αντιμετωπίζουμε στις μέρες μας, την επικινδυνότητα χρήσης του διαδικτύου.

Προσπάθειες καταστολής της δράσης των χάκερ έφεραν επιστήμονες και στοχαστές σε αντιπαράθεση. Χαρακτηριστικό παράδειγμα αποτελεί η επιχείρηση "Sun Devil " που δημιούργησε το δίλλημα εάν θα πρέπει να υπάρχει άμεση τιμωρία του παράνομου εισβολέα ή να γίνει απλά ένα είδος επίπληξής του.

. Ο λόγος που ένα μέρος επιστημόνων ισχυρίστηκε κάτι τέτοιο είναι ότι η άμεση ποινική τιμωρία ενός χάκερ, που ίσως ενεργούσε με τέτοιο παράνομο τρόπο για πρώτη φορά, ίσως τον στρέψει προς την συστηματική παραβίαση τοποθεσιών του διαδικτύου. Στην δεύτερη περίπτωση μια απλή παρατήρησή του ή έστω η τιμωρία του για πταίσμα θα τον συνετούσε.

ΠΑΡΑΠΟΜΠΕΣ

(1) Λάζος Γρ.(2001),Πληροφορική και Έγκλημα, Αθήνα, Νομική Βιβλιοθήκη,σελ.46.

(2) McEwen,Dedicated Computer Crime Units, U.S.Dept of Justice,1989.

(3) Βλ.σχ.Λάζος Γρ.,ό.π.,σελ.179-186.

(4)Βλ.σχ.ΤσουραμάνηςΧρ.(1996),Οικονομική παραβατικότητα,Αθήνα, Έλλην,σελ.95-96.

(5) Βλ.σχΛάζος Γρ.,ό.π.,σελ.198.

(6) Βλ.σχ.A.Bequai,Technocrimes,Lexington,Massachusetts,1987.

(7) Βλ.σχ. Ανώνυμος, Maximum Security, Β.Γκιούρδας, σελ.324 και 822.

(8) Βλ.σχ.Λάζος Γρ.,ό.π.,σελ 110.

(9) Βλ.RichardMansfield,Οι χάκερ επιτίθενται, μτφρ.Ε.Γκαγκάτσιου, Αθήνα,Μ.Γκιούρδας,σελ.241.

(10) Βλ.Richard Mansfield,ό.π.,σελ.241.

(11) Βλ.Richard Mansfield,ό.π.,σελ.241-242.

(12)Βλ.Δρ.Δ.Γιαννακόπουλου-Ι.Παπουτσή,Πληροφοριακά Συστήματα Διοίκησης,Β Έκδοση,Αθήνα 2000, Έλλην, σελ.300-302.

(13) Βλ.Ανώνυμος,ό.π.,σελ.169-170.

(14) Βλ.Ανώνυμος,ό.π.,σελ.342-343.

ΠΗΓΕΣ

Α.ΒΙΒΛΙΑ

-Ανώνυμος (2002), Maximum Security, μεταφρ.ομάδα Β. Γκιούρδας Αθήνα, "Β. Γκιούρδας".

-Δρ.Γιαννακόπουλος Διον.-Παπουτσής Ιωάν.(2000), Πληροφοριακά Συστήματα Διοίκησης, β΄Έκδοση,"Έλλην",Αθήνα.

-Λάζος Γρ. (2001), Πληροφορική και Έγκλημα,Αθήνα, "Νομική Βιβλιοθήκη".

-Mansfield R. (2000), Οι χάκερ επιτίθενται, μετάφρ.Ε.Γκαγκάτσιου, Αθήνα, Μ. Γκιούρδας.

-Τσουραμάνης Χρ.(1996),Οικονομική Παραβατικότητα,Αθήνα,"Έλλην"

Β.ΑΡΘΡΑ

1."Η σκοτεινή πλευρά του κυβερνοχώρου", On Line, Μάρτιος 2003.

2.Τάνια Μποζανίνου , ¨Διάσημες Κυβερνοπειρατίες¨, Το Βήμα, 7 Δεκεμβρίου 1997.

3. ¨Συνταξιούχοι και νεαροί χάκερ ¨, New Gen, 6 Απριλίου 2000.

4. ¨Χάκερ μισθοφόροι ¨, New Gen, 13 Απριλίου 2000.

5. Ουρανία Γκόλτσιου, ¨Το χάκινγκ έχει την δική του ιστορία ¨, Info Tech, 22 Φεβρουαρίου 2000.

6.Το αμφιλεγόμενο Internet,Ram,Νοέμβριος 1997,σελ.73.
7. ¨Αύξηση της ψηφιακής εγκληματικότητας¨,PC MAGAZINE, Μάϊος 2002,σελ.28-30.

8. ¨Μάτι και αυτί κατά της πλαστοπροσωπείας ¨, Τα Νέα, 4-5 Μαρτίου 2000.

9. ¨Το πινάκιο του κυβερνο-εγκλήματος¨,BHMARAM,5 Απριλίου 2000,σελ.39.

10. ¨Τζίρος 80 δις.από...τα''τρύπια τηλέφωνα''¨,Εθνος της Κυριακής,1 Ιουλίου 2001,σελ.40.

11.¨Εργαλεία λογισμικού για ελαχιστοποίηση της απάτης¨,netbit2,σελ.21.

12.¨Οι απατεώνες με το πληκτρολόγιο¨,Το βήμα, 29 Σεπτεμβρίου 2002,σελ.42.

13.¨Ο κυνηγός των χάκερ¨,Έθνος της Κυριακής,16 Ιανουαρίου 2000,σελ.63.

14.¨Τμήμα δίωξης ηλεκτρονικού εγκλήματος¨,Τα Νέα,7-8 Ιουλίου 2001,σελ.64.

15.Κατερίνα Τζαβάρα,¨Χάκερς μεγάλου μήκους¨,Info tech,22 Φεβρουαρίου 2000,σελ.12.

Γ. Άλλες πηγές

-Μπασακάρη Ε.,Εγκλήματα στο Internet το 1999,Πτυχιακή εργασία ΤΕΙ Μεσολογγίου,2001.

-www.hack.gr

-www.cybercrime .gov

- www.e-consumer.gr

- www.nipc.gov