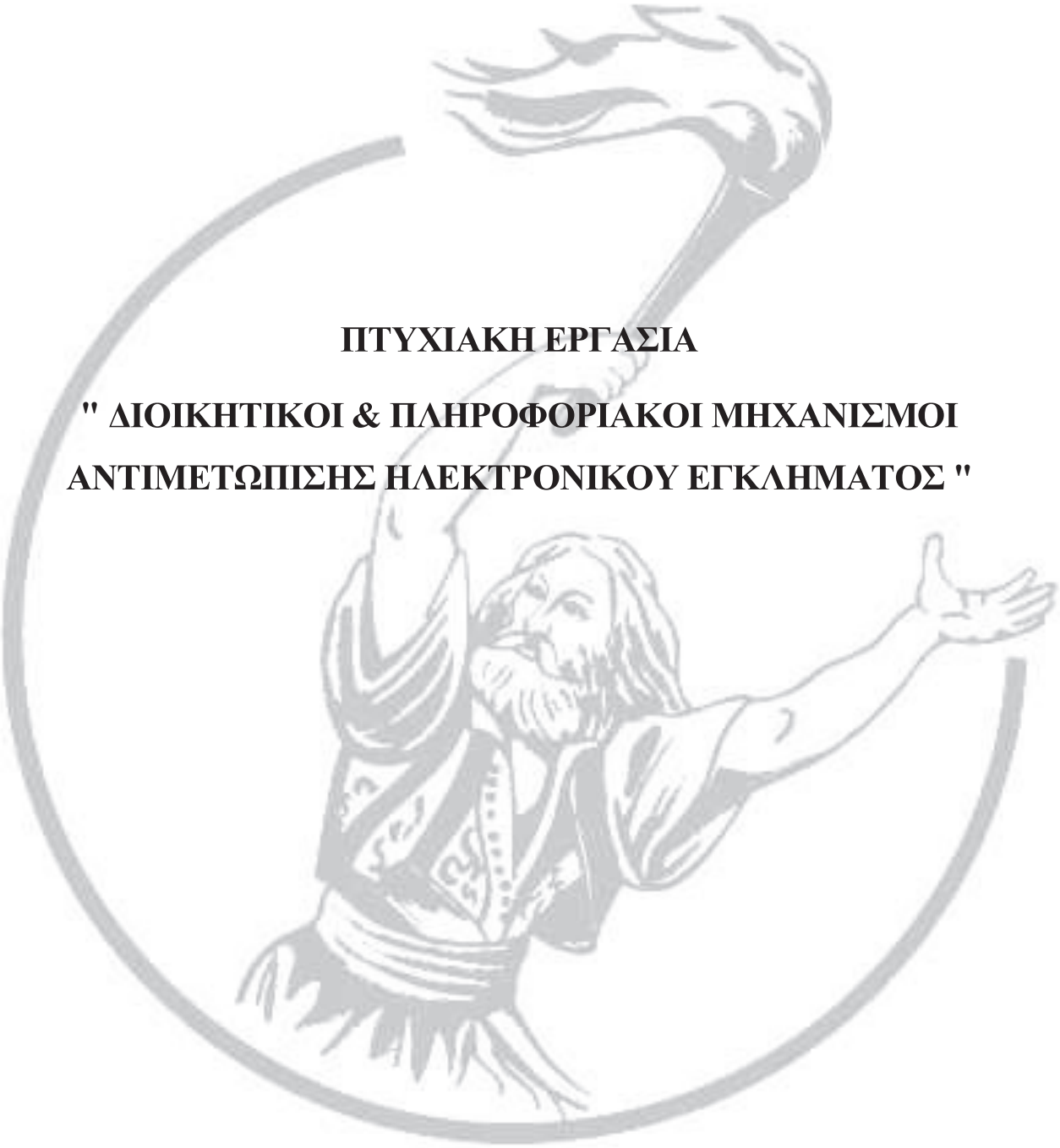
ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΜΕΣΟΛΟΓΓΙΟΥ

ΤΜΗΜΑ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ & ΔΙΚΤΥΩΝ



ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

" ΔΙΟΙΚΗΤΙΚΟΙ & ΠΛΗΡΟΦΟΡΙΑΚΟΙ ΜΗΧΑΝΙΣΜΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ "

ΣΠΟΥΔΑΣΤΗΣ: **ΠΑΠΑΝΔΡΕΟΥ ΓΕΩΡΓΙΟΣ**

ΕΠΙΒΛΕΠΩΝ: **ΑΣΗΜΑΚΟΠΟΥΛΟΣ ΓΕΩΡΓΙΟΣ**, Καθηγητής Εφαρμογών

ΝΑΥΠΑΚΤΟΣ 2013

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

Ναύπακτος, 22 Απριλίου 2012

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

Ασημακόπουλος Γεώργιος

Λούβρος Σπυρίδων

Ασαρίδης Ηλίας

Περίληψη

Η παρούσα εργασία μελετά το ηλεκτρονικό έγκλημα. Συγκεκριμένα παρουσιάζει και αναλύει όλες τις μορφές ηλεκτρονικού εγκλήματος και τους τρόπους αντιμετώπισής τους από την αστυνομία. Παράλληλα παρουσιάζει και την ισχύουσα νομοθεσία του ηλεκτρονικού εγκλήματος. Η μεθοδολογική προσέγγιση της παρούσας εργασίας βασίστηκε στη συλλογή δευτερογενών δεδομένων μέσα από άρθρα και βιβλία αλλά και από επίσημες ιστοσελίδες του διαδικτύου. Το βασικό συμπέρασμα που προκύπτει από την παρούσα εργασία είναι ότι το ηλεκτρονικό έγκλημα έχει πάρει τεράστιες διαστάσεις σήμερα με την ολοένα αυξανόμενη εξέλιξη του διαδικτύου. Κάθε οργανισμός πρέπει να μεριμνήσει για την πρόληψη εκδήλωσης των επιθέσεων, την ανίχνευση των επιθέσεων και, τέλος, την αντίδραση προς αποκατάσταση της ζημιάς που προκλήθηκε από μια επίθεση. Οι διωκτικές επίσης αρχές καλούνται, να αντιμετωπίσουν το έγκλημα.

Συγκεκριμένα το πρώτο κεφάλαιο θα εισαγάγει τον αναγνώστη στην έννοια του ηλεκτρονικού εγκλήματος, θα προβεί σε μια ιστορική αναδρομή του εγκλήματος και θα το οριοθετήσει. Το δεύτερο κεφάλαιο θα αναφέρει τις μορφές ηλεκτρονικού εγκλήματος και θα τις αναλύσει διεξοδικά. Θα μελετηθούν οι περιπτώσεις της διακίνησης πορνογραφικού υλικού, διαδικτυακής ηλεκτρονικής τρομοκρατίας, κακόβουλες εισβολές σε δίκτυα, ανεπιθύμητη αλληλογραφία, επιθέσεις σε δικτυακούς τόπους, πειρατεία ονομάτων χώρου, πειρατεία λογισμικού, απάτη μέσω διαδικτύου, μέσω e mail, μέσω πιστωτικών κρατών, κλοπή ταυτότητας και ξέπλυμα χρήματος. Το τρίτο κεφάλαιο θα αναλύσει τους πληροφοριακούς μηχανισμούς αντιμετώπισης. Συγκεκριμένα θα αναφέρει μέτρα όπως οι κωδικοί πρόσβασης, η χρήση λογισμικού ασφαλείας, το antivirus λογισμικό, τα firewalls, η κρυπτογραφία και η διαχείριση δημόσιων κλειδιών πιστοποιητικών. Το τέταρτο κεφάλαιο θα παρουσιάσει τη διεύρυνση του ηλεκτρονικού εγκλήματος και θα παραθέτει τον εντοπισμό του από την αστυνομία. Η διερεύνηση του ηλεκτρονικού εγκλήματος θα δούμε ότι πραγματοποιείται με ψηφιακές αποδείξεις και δεδομένα, με αρχεία καταγραφής, με συναγερμούς και προειδοποιήσεις αναφορές, με τον εντοπισμό ονόματος χώρου και με τη διεύθυνση IP που διαθέτει κάθε υπολογιστής. Το πέμπτο κεφάλαιο θα δώσει όλες τις βασικές πληροφορίες για το σχεδιασμό και ανάπτυξη του συστήματος που δημιουργήσαμε. Στο τέλος της εργασίας παρατίθενται τα τελικά μας συμπεράσματα και προτάσεις για την αντιμετώπιση του προβλήματος.

Πίνακας Περιεχομένων

Εισαγωγή

Είναι γενικά παραδεκτό ότι οι υπολογιστές έχουν μπει για τα καλά στη ζωή μας αφού σχεδόν όλες οι εργασίες ανεξάρτητα από το είδος τους, γίνονται με την χρήση ηλεκτρονικών υπολογιστών. Είναι παραδεκτό ότι η χρήση τους έχει βελτιώσει την ποιότητα ζωής σε αρκετές περιπτώσεις με τις δυνατότητες που παρέχουν στους χρήστες.

Το διαδίκτυο το οποίο επιτρέπει στους ανθρώπους να αλληλεπιδρούν ηλεκτρονικά τόσο για προσωπικά όσο και για επαγγελματικά θέματα, έχει δικαιολογημένα προκαλέσει αρκετό θόρυβο κατά την διάρκεια των τελευταίων χρόνων και όπως άλλωστε έχει συμβεί και στην περίπτωση άλλων καινοτομιών, το διαδίκτυο έγινε αντικείμενο εκμετάλλευσης από εγκληματικά στοιχεία κάτι που έχει ήδη αρχίσει να επηρεάζει το ευρύ κοινό.

Σκοπός της μελέτης είναι ο εντοπισμός των διαφόρων εγκλημάτων που διαπράττονται με ηλεκτρονικές διαδικασίες και ο προσδιορισμός των μέτρων νομοθετικών και άλλων που θα πρέπει να ληφθούν ώστε το κράτος και σε συνέχεια οι διωκτικές αρχές να είναι σε θέση να παίζουν ουσιαστικό ρόλο στην πρόληψη και εξιχνίαση τέτοιων εγκλημάτων.

Συγκεκριμένα το πρώτο κεφάλαιο θα εισαγάγει τον αναγνώστη στην έννοια του ηλεκτρονικού εγκλήματος.

Το δεύτερο κεφάλαιο θα αναφέρει τις μορφές ηλεκτρονικού εγκλήματος και θα τις αναλύσει διεξοδικά.

Το τρίτο κεφάλαιο θα αναλύσει τους πληροφοριακούς μηχανισμούς αντιμετώπισης.

Το τέταρτο κεφάλαιο θα παρουσιάσει τη διεύρυνση του ηλεκτρονικού εγκλήματος και θα παραθέτει τον εντοπισμό του από την αστυνομία.

Το πέμπτο κεφάλαιο θα δώσει όλες τις βασικές πληροφορίες για το σχεδιασμό και ανάπτυξη του συστήματος που δημιουργήσαμε.

Στο τέλος της εργασίας παρατίθενται τα τελικά μας συμπεράσματα και προτάσεις για την αντιμετώπιση του προβλήματος.

ΚΕΦΑΛΑΙΟ 1. Το ηλεκτρονικό έγκλημα

1.1. Ιστορική αναδρομή

Το έγκλημα, ως αναπόσπαστο κομμάτι κάθε κοινωνίας, έχει τη μορφή ενός ζωντανού οργανισμού. Συνεχώς μεταβάλλονται οι μορφές του, τα μέσα διάπραξης του και η νομοθεσία που το διέπει. Στις αρχές του 20ου αιώνα, καινούριοι τρόποι τεχνικές για τη διάπραξη εγκλημάτων έκαναν την εμφάνισή τους. Η βιομηχανική επανάσταση εκσυγχρόνισε τα μέσα τέλεσης του εγκλήματος. Το τηλέφωνο άρχισε να χρησιμοποιείται για απάτες και άλλα εγκλήματα, τα μεταφορικά μέσα διευκόλυναν τη διάπραξη κλοπών και ληστειών, ενώ διάφορα άλλα τεχνολογικά επιτεύγματα με τη χρήση και λειτουργία τους, επέφεραν μια αρχική διαφοροποίηση στον τρόπο διάπραξης του εγκλήματος[1].

Ίσως τότε κανείς δεν μπορούσε να φανταστεί τι θα επακολουθούσε. Με την εμφάνιση και ανάπτυξη της τεχνολογίας των ηλεκτρονικών υπολογιστών, συντελούνται αλλαγές στο εγκληματικό φαινόμενο, που ποτέ πριν δεν είχε γνωρίζει η ανθρωπότητα.

Οι εγκληματικές απειλές στηρίζονται πλέον σε πιο περίπλοκη τεχνολογία, καταργώντας τα φυσικά όρια. Βέβαια τόσο το συμβατικό έγκλημα όσα και τα μέσα διάπραξης του συνεχίζουν να υπάρχουν, όμως παράλληλα εμφανίζονται νέες μορφές με χαρακτηριστικότερη αυτή του ηλεκτρονικού εγκλήματος, του εγκλήματος δηλαδή που ένας ηλεκτρονικός υπολογιστής ή παρόμοιες συσκευές ηλεκτρονικής επεξεργασίας δεδομένων, διαδραματίζουν κυρίαρχο ρόλο.

Αναζητώντας τις ρίζες του ηλεκτρονικού εγκλήματος, διαπιστώνουμε ότι ταυτόχρονα με την εμφάνιση των υπολογιστών, έγιναν οι πρώτες προσπάθειες από τους επίδοξους «ηλεκτρονικούς εγκληματίες» να βρουν τρόπους να εκμεταλλευτούν τις νέες αυτές τεχνολογίες για να προσπορίσουν όφελος για τους εαυτούς τους ή για τρίτους.

Η νέα τεχνολογία, που αναπτύσσονταν με γοργούς ρυθμούς, έδινε νέες ευκαιρίες για εύκολη διάπραξη πλήθους εγκλημάτων. Ακόμη όμως και τα πρώτα χρόνια έπειτα από την εμφάνιση των υπολογιστών, το ηλεκτρονικό έγκλημα ήταν σπάνιο, διότι ο αριθμός τους ήταν περιορισμένος. Επιπλέον, οι υπάρχοντες υπολογιστές χρησιμοποιούσαν γλώσσα μηχανής, καθιστώντας αδύνατο για τους επίδοξους εγκληματίες να κατέχουν την απαραίτητη γνώση ή

[1] Goodman M., Brenner S., (2002). **«The Emerging Consensus on Criminal Conduct in Cyberspace»**. UCLA Journal and Technology.

τον εξοπλισμό. Ο ηλεκτρονικός υπολογιστής αποτελούσε είδος πολυτελείας και κατ' αυτήν την έννοια το ηλεκτρονικό έγκλημα ήταν έγκλημα για λίγους.

Χρονικά, η ανάπτυξη του ηλεκτρονικού εγκλήματος τοποθετείται στην τελευταία δεκαετία του περασμένου αιώνα, σε μια εποχή που χαρακτηρίστηκε από την αλματώδη εξέλιξη των υπολογιστικών συστημάτων.

Σήμερα, το μεγαλύτερο ποσοστό του πληθυσμού στις αναπτυγμένες χώρες, έχει πρόσβαση σε ένα Η/Υ, η δε χρήση του έχει απλοποιηθεί τόσο που ακόμη και ένα μικρό παιδί μπορεί να χειρίζεται έναν προσωπικό υπολογιστή με ιδιαίτερη δεξιότητα[2].

Η μεγάλη επανάσταση στον τομέα του ηλεκτρονικού εγκλήματος, επήλθε μετά την εμφάνιση των δικτύων. Τα δίκτυα, δημιούργησαν νέες διόδους πρόσβασης προς την πληροφορία, καθιστώντας μη αναγκαία την παρουσία του επιτιθέμενου στο χώρο όπου αυτή φυλάσσεται.

Η τεράστια πληροφοριακή δεξαμενή που δημιουργήθηκε και συνεχίζει να επεκτείνεται, αποτέλεσμα της διασύνδεσης εκατομμυρίων υπολογιστών ανά τον κόσμο, μετέβαλε ριζικά τον τρόπο ζωής του σύγχρονου ανθρώπου.

Σήμερα, οι υπολογιστές χρησιμοποιούνται σε όλες τις εκφάνσεις της καθημερινής μας δραστηριότητας και στους σκληρούς τους δίσκους αποθηκεύονται πληροφορίες για τα προσωπικά μας στοιχεία, τους τραπεζικούς μας λογαριασμούς, τις συνήθειες μας, τις προτιμήσει μας κ.ά.

Το νέο περιβάλλον, χαρακτηρίζεται από την ευρεία ανάπτυξη του ηλεκτρονικού εμπορίου, την πραγματοποίηση τραπεζικών και συναλλαγματικών πράξεων μέσω του Διαδικτύου, την άμεση επικοινωνία σε όλα τα επίπεδα με νέες διόδους (e-mail, chat, newsgroups κ.λ.π.), αλλά και την εξ' αποστάσεως εκπαίδευση, την τηλεδιάσκεψη, την πραγματοποίηση συναλλαγών με δημόσιες υπηρεσίες, κ.ά.

Οι ευκαιρίες για εγκληματική δραστηριότητα είναι περισσότερες από ποτέ. Το ηλεκτρονικό έγκλημα είναι ευκολότερο, οι δε δυνατότητες δίωξης του από τις αρμόδιες αρχές είναι περιορισμένες λόγω έλλειψης εμπειρίας στο σχετικό τομέα, ελλιπούς εκπαίδευσης αλλά και ασαφούς νομοθετικού πλαισίου, γεγονός που ενθαρρύνει τους επίδοξους εγκληματίες.

---

[2] Frey D. (2003). **«An Analysis of Cybercrime: Past, present and future»**, Buffalo University's Publications.

1.2. Οριοθέτηση Ηλεκτρονικού Εγκλήματος

Κατά καιρούς, έχουν γίνει πολλές προσπάθειες να ορισθεί το ηλεκτρονικό έγκλημα. Ένας ορισμός που δόθηκε από τους Forester & Morrison [3] προσδιόρισε το ηλεκτρονικό έγκλημα ως «μια εγκληματική πράξη στην οποίο ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσής της». Ωστόσο, το ηλεκτρονικό έγκλημα δεν είναι κάτι τόσο απλό, ούτε μπορούμε να το γενικεύσουμε. Υιοθετώντας μια τριπλή προσέγγιση που τείνει να επικρατήσει σήμερα, μπορούμε να θεωρήσουμε το ηλεκτρονικό έγκλημα ως:

- μια νέα μορφή εγκλήματος, που διαπράττεται με τη χρήση ηλεκτρονικών υπολογιστών
- μια παραλλαγή των ήδη υπαρχόντων εγκλημάτων, τα οποία διαπράττονται με υπολογιστές
- μια εγκληματική πράξη στην εκδήλωση της οποίας συμμετέχει καθ' οποιονδήποτε τρόπο ένας ηλεκτρονικός υπολογιστής.

Στην αγγλική γλώσσα οι όροι που χρησιμοποιούνται για να περιγράψουν το ηλεκτρονικό έγκλημα ποικίλουν: e-crime, cybercrime, computer-crime, internet related crime και hitech-crime είναι οι συχνότερα χρησιμοποιούμενοι. Οι διαφορές των ανωτέρω όρων είναι ελάχιστες. Μπορούμε να θεωρήσουμε τους όρους computer-crime, e-crime, hitech-crime και internet related crime ως ειδικότερους, καθότι στην δεύτερη περίπτωση περιλαμβάνεται υποχρεωτικά και το στοιχείο του Διαδικτύου.

Αντιστοίχως, στην ελληνική γλώσσα οι όροι που χρησιμοποιούνται είναι ηλεκτρονικό έγκλημα, δικτυακό έγκλημα και έγκλημα του κυβερνοχώρου. Το στοιχείο της δικτύωσης περιλαμβάνεται στους δύο τελευταίους όρους.

Βασικό συστατικό στοιχείο του ηλεκτρονικού εγκλήματος, αποτελεί η ύπαρξη μίας συσκευής ηλεκτρονικής επεξεργασίας δεδομένων, όπως ηλεκτρονικός υπολογιστής, κινητό τηλέφωνο, palmtop, notebook, κ.λ.π. Κυρίαρχο ρόλο διαδραματίζει ο Η/Υ, ο οποίος μπορεί:

- **Να αποτελεί τον στόχο κάποιας επίθεσης**. Στην περίπτωση αυτή μπορούμε να πούμε ότι ο υπολογιστής είναι το «θύμα» της επίθεσης.
- **Να αποτελεί το μέσο διάπραξης κάποιας επίθεσης**, δηλαδή το εργαλείο που χρησιμοποιεί ο επιτιθέμενος για να πραγματοποιήσει τον εγκληματικό σκοπό του (π.χ. εισβάλλοντας σε κάποιο άλλο υπολογιστή).

---

[3]Forester T., Morrison P., (1994). **«Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing»,** Massachousetts Institute of Technology

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

Παράλληλα, ο ορισμός του ηλεκτρονικού εγκλήματος εξαρτάται σε μεγάλο βαθμό από την οπτική γωνία που τον εξετάζουμε. Αν αυτός άπτεται της νομικής επιστήμης, απαιτείται πιο αυστηρός προσδιορισμός των όρων, για να είναι δυνατή η στοιχειοθέτηση των εγκλημάτων. Η πολυπλοκότητα της μορφής αυτής της εγκληματικότητας, δυσχεραίνει ακόμη και το νομοθέτη, ο οποίος αποφεύγει να το ορίσει και είτε αφήνει την αρμοδιότητα αυτή στα δικαστήρια και την παραγόμενη νομολογία, είτε δανείζεται τους χρησιμοποιούμενοι από την τεχνολογία όρους.

Κρίνεται επίσης σκόπιμο να επισημανθεί, ότι η εμπλοκή ενός ηλεκτρονικού υπολογιστή ή δικτύου δεν σημαίνει αναγκαστικά ότι έχουμε να κάνουμε με ηλεκτρονικό έγκλημα. Για παράδειγμα, αποτελεί ηλεκτρονικό έγκλημα ο βιασμός μίας γυναίκας από έναν άνδρα, τον οποίο γνώρισε μέσω ενός chat room στο Διαδίκτυο και ο χρόνος και τόπος συνάντησης, που διαπράχθηκε το έγκλημα, καθορίστηκε μέσω e-mail; Σαφώς, η απάντηση στο παραπάνω ερώτημα είναι αρνητική. Πρόκειται για ένα συμβατικό έγκλημα (το βιασμό), που διαπράχθηκε με την βοήθεια των δυνατοτήτων επικοινωνίας που προσφέρει το Διαδίκτυο (chat και e-mail).

1.3. Ορισμός Ηλεκτρονικού Εγκλήματος

Ο όρος ηλεκτρονικό έγκλημα, χρησιμοποιείται όλο και πιο συχνά, καθώς η νέα αυτή μορφή εγκλήματος φέρει ορισμένα ιδιαίτερα χαρακτηριστικά, που το διαφοροποιούν από το συμβατικό έγκλημα[4].

Είναι γεγονός ότι το ηλεκτρονικό έγκλημα διαπράττεται άμεσα, σε ελάχιστα δευτερόλεπτα. Ο επιτιθέμενος με τη χρήση ενός Η/Υ συνδεδεμένου στο Διαδίκτυο, μπορεί να εισβάλει στα υπολογιστικά συστήματα μιας επιχείρησης ή ενός οργανισμού σε οποιοδήποτε σημείο του κόσμου. Δεν απαιτείται η φυσική μετακίνηση ίου, καθώς οι ενέργειές του μπορούν να ολοκληρωθούν από την οικία του ή άλλο χώρο, με τη χρήση ενός δικτυωμένου προσωπικού υπολογιστή.

[4] Ζάννη Α. (2005). **«Το διαδικτυακό έγκλημα»**, Εκδόσεις Σάκκουλα.

Φαινομενικά, η εισβολή σε κάποιο υπολογιστικό σύστημα φαντάζει δύσκολη. Όμως, η άποψη ότι απαιτούνται εξειδικευμένες γνώσεις για την εξαπόλυση τέτοιου είδους επίθεσης, αποτελεί μύθο. Στο Διαδίκτυο διατίθενται ελεύθερα εφαρμογές λογισμικού, που επιτρέπουν στους επίδοξους hackers την εισβολή σε δίκτυα και υπολογιστικά συστήματα, τη διασπορά ιών και την πραγματοποίηση πλήθους άλλων ηλεκτρονικών επιθέσεων, καθιστώντας περισσότερο εύκολη την διάπραξη του ηλεκτρονικού εγκλήματος σε σχέση με το συμβατικό.

Επιπλέον, το Διαδίκτυο προσφέρει μια σειρά από νέες δυνατότητες επικοινωνίας. Το ηλεκτρονικό ταχυδρομείο (e-mail) τα δωμάτια συζητήσεων (chat rooms) και οι ομάδες ειδήσεων (newsgroups),επιτρέπουν σε πολλά άτομα ταυτόχρονα να επικοινωνούν γρήγορα, σε πραγματικό χρόνο, χωρίς μετακίνηση, εύκολα και ανέξοδα.

Η επανάσταση αυτή στις επικοινωνίες συνέβαλε στη διάδοση εγκλημάτων, όπως η παιδοφιλία, η παιδική πορνογραφία και η ανεπιθύμητη αλληλογραφία (spamming). Στις περιπτώσεις αυτές, τα υποψήφια θύματα αναζητούνται μέσω των νέων καναλιών επικοινωνίας, που προσφέρει το Διαδίκτυο[5].

Παράλληλα, το ηλεκτρονικό έγκλημα έχει εισαγάγει νέους νομοθετικούς προβληματισμούς. Πολλές φορές, καθίσταται αδύνατο να προσδιοριστεί ο τόπος τέλεσης του εγκλήματος, διότι κάθε εγκληματίας μπορεί να το διαπράξει από οποιοδήποτε σημείο του κόσμου, αρκεί να έχει στην διάθεση του έναν ηλεκτρονικό υπολογιστή. Επίσης, είναι δύσκολο να προσδιοριστεί και ο ακριβής χρόνος τέλεσης του, καθώς τα θύματα συχνά αντιλαμβάνονται μια ηλεκτρονική επίθεση πολύ αργότερα από το χρόνο κατά τον οποίο αυτή συνέβη. Επίσης συχνά είναι δυνατή η διαγραφή από τον εισβολέα των «ιχνών» του ηλεκτρονικού εγκλήματος κάτι που δυσχεραίνει ή εμποδίζει την ανίχνευσή του.

Τέλος, σε σύγκριση μετά συμβατικά εγκλήματα, η διερεύνηση του ηλεκτρονικού εγκλήματος παρουσιάζει ιδιαιτερότητες. Σε μια διαδικτυακή έρευνα, συχνά απαιτείται η συνεργασία τουλάχιστον δύο κρατών, τα δε αρμόδια όργανα των διωκτικών αρχών πρέπει να κατέχουν εξειδικευμένες γνώσεις και να εκπαιδεύονται συνεχώς στις νέες τεχνολογικές εξελίξεις. Σε ορισμένες περιπτώσεις, τέτοιου είδους γνώσεις απαιτείται να κατέχουν και όσοι άλλοι ασχολούνται με τη δίωξη του ηλεκτρονικού εγκλήματος όπως δικαστές, εισαγγελείς και δικηγόροι.

---

[5] United Nations (1995), **«International Review on Criminal Policy-United Nations Manual on the prevention and control of Computer Related crime»**, United Nations Edition

Δυστυχώς, δεν υπάρχουν επαρκή στατιστικά στοιχεία ακόμη, όχι μόνο στον ελληνικό, αλλά και στο διεθνή χώρο. Ελάχιστες περιπτώσεις εγκλημάτων του κυβερνοχώρου καταγγέλλονται, και αυτό για να μην πλήττεται το κύρος των εταιριών που τυγχάνουν θύματα τέτοιων επιθέσεων. Κατά συνέπεια, οι διαστάσεις της εγκληματικότητας στο χώρο του Διαδικτύου είναι πιο δύσκολο να καθοριστούν από ότι στον «κοινό» εγκληματικό χώρο (θεωρία του παγόβουνου).

1.4. Μορφές Ηλεκτρονικού Εγκλήματος

Συνοψίζοντας, διακρίνουμε τρεις βασικές κατηγόριες όσον αφορά στις μορφές του ηλεκτρονικού εγκλήματος [6]:

- Σε εγκλήματα που διαπράττονται τόσο σε συμβατικό περιβάλλον όσο και σε περιβάλλον ηλεκτρονικών υπολογιστών. Στην κατηγορία αυτή εντάσσουμε πολλές κατηγορίες εγκλημάτων. Για παράδειγμα, η συκοφαντική δυσφήμηση μπορεί να διαπραχθεί με τη δημοσίευση στο Διαδίκτυο μίας σελίδας με προσβλητικό περιεχόμενο για ένα πρόσωπο. Ουσιαστικά στην περίπτωση αυτή το Διαδίκτυο αποτελεί ένα ακόμη μέσο για την τέλεση ενός εγκλήματος.

- Σε εγκλήματα που διαπράττονται με τη χρήση υπολογιστών χωρίς την ύπαρξη δικτύωσης. Χαρακτηριστικό έγκλημα της κατηγορίας αυτής, είναι η παράνομη αντιγραφή λογισμικού.

- Σε εγκλήματα που έχουν να κάνουν αποκλειστικά με τη χρήση του Διαδικτύου. Η συνηθέστερη εγκληματική συμπεριφορά της κατηγόριας αυτής, είναι η διασπορά κακόβουλου λογισμικού (ιών).

Οι δύο τελευταίες περιπτώσεις, συνιστούν μια εντελώς νέα μορφή εγκλήματος, η οποία δεν υπήρχε πριν την εμφάνιση των ηλεκτρονικών υπολογιστών.

Από τα παραπάνω διαφαίνεται ότι το ηλεκτρονικό έγκλημα συμμετέχει ποικιλότροπα στο εγκληματικό φαινόμενο, τα δε επιμέρους συστατικά του είναι δύσκολο να καθοριστούν με σαφήνεια. Στην μελέτη αυτή, δίνουμε έμφαση στα εγκλήματα που διαπράττονται με τη χρήση ηλεκτρονικών υπολογιστών και την ύπαρξη δικτύωσης, στα οποία θα αναφερόμαστε με τον γενικό όρο ηλεκτρονικό έγκλημα, αναφέροντας περιληπτικά, βασικά στοιχεία για τις υπόλοιπες περιπτώσεις.

---

[6] Πάγκαλος Γ., Μαυρίδης Ι. (2002). **«Ασφάλεια πληροφοριακών συστημάτων και δικτύων»**, Εκδόσεις Ανίκουλα.

1.5. Αναφορές 1ου κεφαλαίου

1. Forester T., Morrison P., (1994). «**Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing»,** Massachousetts Institute of Technology
2. Frey D. (2003). «**An Analysis of Cybercrime: Past, present and future**», Buffalo University's Publications.
3. Goodman M., Brenner S., (2002). «**The Emerging Consensus on Criminal Conduct in Cyberspace**». UCLA Journal and Technology.
4. United Nations (1995), «**International Review on Criminal Policy-United Nations Manual on the prevention and control of Computer Related crime**», United Nations Edition
5. Ζάννη Α. (2005). «**Το διαδικτυακό έγκλημα**», Εκδόσεις Σάκκουλα.
6. Πάγκαλος Γ., Μαυρίδης Ι. (2002). «**Ασφάλεια πληροφοριακών συστημάτων και δικτύων**», Εκδόσεις Ανίκουλα.

ΚΕΦΑΛΑΙΟ 2. Ανάλυση μορφών ηλεκτρονικού εγκλήματος

2.1. Διακίνηση πορνογραφικού υλικού

Η διακίνηση πορνογραφικού υλικού, δεν είναι ένα έγκλημα νέο. Η εξάπλωση όμως, του Διαδικτύου, έχει διευκολύνει τη διάπραξή του. Τα αδικήματα που συνδέονται με τη μορφή αυτή του υλικού, σχετίζονται τόσο με τη δημιουργία του υλικού όσο και με τη μη νόμιμη διακίνησή του. παράνομη διακίνηση υλικού παιδικής πορνογραφίας έχει λάβει τεράστιες διαστάσεις, προκαλώντας ιδιαίτερη ανησυχία στις διωκτικές αρχές. Το πορνογραφικό υλικό, που διακινείται μέσω του Διαδικτύου, μπορεί να είναι σε μορφή φωτογραφιών, βίντεο ή άλλης μορφής πολυμέσων. Ο καθένας μπορεί εύκολα να το «κατεβάσει» στον υπολογιστή του, χωρίς να χρειαστεί να αποκαλύψει την ταυτότητα του. Τέτοιου είδους υλικό, βρίσκεται σε διάφορους δικτυακούς τόπους. Μάλιστα γίνεται ανταλλαγή υλικού, αντί να πληρώσεις τίμημα για το υλικό που προμηθεύεσαι, προσφέρεις νέο υλικό, ως αντάλλαγμα.

2.2. Παιδική πορνογραφία

Η σεξουαλική κακοποίηση ανηλίκων και γυναικών είναι μια από τις αρχαιότερες εγκληματικές συμπεριφορές. Με την εμφάνιση και τη διάδοση της χρήσης του Διαδικτύου, έχουμε απλά μια νέα γέφυρα προς το έγκλημα[7].

Η παιδική πορνογραφία στο διαδίκτυο εμφανίζεται με τη μορφή εικόνων, φωτογραφιών και μαγνητοσκοπημένων σκηνών στις οποίες παρουσιάζονται γυμνά κορμιά ανηλίκων, ανήλικοι να αυνανίζονται και ακόμα χειρότερα, ανήλικοι να κακοποιούνται σεξουαλικά από ενηλίκους. Αυξημένη ζήτηση υπάρχει στην κακοποίηση ανηλίκων από υπερήλικες και γενικά σε οτιδήποτε το αηδιαστικό. Η καινούρια τεχνολογία δίνει τη δυνατότητα παρακολούθησης ή και συμμετοχής σε ζωντανό «σόου».

Το πρόβλημα μπορεί να προσεγγισθεί από δυο διαφορετικές πλευρές, όσον αφορά το πώς επηρεάζεται η συμπεριφορά των παιδόφιλων με την είσοδό τους σε πορνογραφικές ιστοσελίδες. Ενδέχεται οι ορέξεις του δράστη να ικανοποιηθούν και να εκτονωθούν με τον τρόπο αυτό και να μην εκδηλωθούν οι διαστροφικές του τάσεις στο υπόλοιπο κοινωνικό περιβάλλον. Είναι όμως πολύ πιθανό τα θεάματα αυτά να του δημιουργήσουν ψύχωση, την

[7] Δήμου Γ., (2002), **«Η διαχείριση υποθέσεων σεξουαλικής κακοποίησης ανηλίκων»**, Αδημοσίευτη.

οποία θα εκδηλώσει στον κοινωνικό του περίγυρο, κακοποιώντας σεξουαλικά κάποιο ανήλικο άτομο. Επιπλέον οι παιδόφιλοι δημιουργούν τα δικά τους δωμάτια επικοινωνίας (chat rooms) στο Διαδίκτυο, στα οποία είναι μόνον αυτοί ευπρόσδεκτοι, ανταλλάσσοντας ιδέες, εμπειρίες και τακτικές προσέγγισης ανηλίκων.

Η σεξουαλική κακοποίηση των παιδιών για πορνογραφικούς σκοπούς, μπορεί να αποδειχθεί μια πολύ επικερδής επιχείρηση. Έτσι, με τη δουλειά αυτή ασχολούνται άτομα με τεράστια γνώση στο χώρο των υπολογιστών και μακρά πείρα χρήσης του μέσου.

Τα πιο αισχρά και πλέον διαδεδομένα κυκλώματα παιδικής πορνείας κρύβονται στο Διαδίκτυο, πίσω από κρυπτογραφημένες διευθύνσεις και κωδικούς που γνωρίζουν μόνον όσοι πληρώνουν αδρά.

Υπάρχουν δυστυχώς πάρα πολλοί δικτυακοί τόποι που έχουν πορνογραφικό περιεχόμενο και λειτουργούν ως "κλαμπ παιδεραστών" και τα οποία πουλούν φωτογραφίες και βιντεοταινίες ανήλικων πρωταγωνιστών. Πολλοί από αυτούς τους δικτυακούς τόπους διοργανώνουν ακόμα και ταξίδια σε χώρες όπως η Ιαπωνία ή η Ταϊλάνδη και υπόσχονται να ικανοποιήσουν ακόμα και τις πιο απαιτητικές διαστροφικές επιθυμίες των πελατών τους.

Οι δικτυακοί τόποι της παιδικής πορνείας δεν βρίσκονται επισήμως καταχωρημένοι στο διαδίκτυο. Ηλεκτρονικές διευθύνσεις με «μαλακό πορνό» οι ενδιαφερόμενοι μπορούν να τις αναζητήσουν μέσω άλλων ηλεκτρονικών διευθύνσεων ερωτικού ή συναφούς περιεχόμενου. Στις διευθύνσεις εκείνες όμως που έχουν πιο "σκληρό πορνό" μέσα στο δίκτυο μπορούν να φτάσουν μόνο όσοι γνωρίζουν καλά τα από κωδικούς και συνθηματικά.

Οι κωδικοποιημένες πορνογραφικές διευθύνσεις ανακοινώνονται ιδιωτικά, μέσω ηλεκτρονικού ταχυδρομείου (e-mail), ενώ οι παράνομες υπηρεσίες που προσφέρονται, διαφημίζονται μέσα από διάφορες ομάδες συζητήσεως, που καλύπτονται πίσω από παραπλανητικούς τίτλους και ενδιαφέροντα, όπως μουσική, ταξίδια ή αθλητισμός. Οι μηχανές αναζήτησης σπάνια θα καταδείξουν μία ηλεκτρονική διεύθυνση που έχει ως κύριο περιεχόμενο την παιδική πορνογραφία[8].

Χώρες όπως η Ρωσία, η Ιαπωνία, η Ταϊλάνδη, η Κορέα, οι Φιλιππίνες καθώς επίσης και οι χώρες της πρώην Σοβιετικής Ένωσης φαίνονται να έχουν τον πρωταγωνιστικό ρόλο στο εμπόριο της παιδικής αθωότητας στο Διαδίκτυο. Στις διάφορες φωτογραφίες που χρησιμοποιούνται ως δολώματα για τους επίδοξους παιδεραστές φιγουράρουν οι αθώοι

[8] Δήμου Γ., (2002), **«Η διαχείριση υποθέσεων σεξουαλικής κακοποίησης ανηλίκων»**, Αδημοσίευτη.

ανήλικοι πρωταγωνιστές και φαίνονται να χαμογελούν. Δυστυχώς όμως οι φωτογραφίες γυμνών εφήβων, μικρών αγοριών και κοριτσιών, να χαμογελούν και να ποζάρουν που προσφέρονται δωρεάν, είναι μόνο ο "κράχτης" που δελεάζει τους επίδοξους πελάτες.

Στο Διαδίκτυο παρουσιάζονται και διακινούνται χιλιάδες φωτογραφίες βασανιστηρίων χωρίς έλεγχο, οι οποίες χωρίς δυσκολία χαρακτηρίζονται αδικαιολόγητα ως «ερωτικές». Προκειμένου να στοχεύσουν σε κοινό με συγκεκριμένα ενδιαφέροντα οι έμποροι της παιδικής σάρκας διαφημίζουν την καταγωγή και την ηλικία των ανήλικων θυμάτων.

Η εξάπλωση του φαινομένου της πορνογραφίας και πορνείας ανηλίκων στο διαδίκτυο αλλάζει διαρκώς και αυτό οφείλεται στο γεγονός ότι αυτό είναι ο ιδανικός χώρος όπου οποιοσδήποτε μπορεί να περάσει από το πραγματικό στο φανταστικό, από έναν κόσμο με κανόνες ηθικής και νόμους σε έναν άλλον, όπου όλα επιτρέπονται, και δεν υπάρχουν ηθικοί ή άλλοι φραγμοί[9] .

Ο χρήστης του δικτύου που αναζητά πορνογραφικό υλικό, ζει σε έναν κόσμο φανταστικό όπου μπορεί να βγάλει στην επιφάνεια τις ερωτικές και σεξουαλικές του προτιμήσεις ελεύθερα, χωρίς τον κίνδυνο της αποκάλυψης, της κριτικής, του κοινωνικού ελέγχου, ή ακόμα και της ποινικής διώξεώς του.

Πολλοί από αυτούς τους χρήστες της αναζήτησης υλικού παιδικής πορνογραφίας είναι οικογενειάρχες, επαγγελματίες με υψηλό εισόδημα, ίσως και επιφανή μέλη κάποιας κοινωνίας, που δεν είχαν ευκαιρία να εξωτερικεύσουν ασφαλώς αυτή την ερωτική τους διαστροφή.

Μέσω όμως του Διαδικτύου δεν ρισκάρουν απολύτως τίποτα και νιώθουν ασφαλείς, φυσιολογικοί και νόμιμοι, αφού καλύπτονται πίσω από την ανωνυμία μιας τυχαίας διεύθυνσης ηλεκτρονικού ταχυδρομείου.

Είναι χαρακτηριστικό πως ο αριθμός των δικτυακών τόπων (web sites), που προβάλλουν την παιδική πορνογραφία έχει ξεπεράσει τις 120.000 και αυξάνεται διαρκώς. Όμως και οι επισκέπτες αυτών των sites αυξάνονται με γρήγορους ρυθμούς. Χαρακτηριστικό της δυναμικής αυτού του φαινομένου είναι το γεγονός ότι τον πρώτο μήνα λειτουργίας μίας τέτοιας ιστοσελίδας έγιναν 3.000 επισκέψεις, τον δεύτερο μήνα 90.000 και τον τρίτο μήνα (λίγο πριν κλείσει) ο αριθμός των επισκεπτών είχε φθάσει τα 3,2 εκατομμύρια.

---

[9] Δήμου Γ., (2002), **«Η διαχείριση υποθέσεων σεξουαλικής κακοποίησης ανηλίκων»**, Αδημοσίευτη.

Τα αίτια και η έκταση του προβλήματος. Προσεγγίζοντας την αιτιολογία του φαινομένου καταλήγουμε ότι η φτώχεια είναι ο κύριος καταλύτης, αλλά δεν μπορεί να εξηγήσει επαρκώς την εμπορική σεξουαλική εκμετάλλευση των παιδιών. Κατά συνέπεια θα πρέπει να εστιάσουμε την προσοχή μας στους ακόλουθους παράγοντες που συμβάλλουν ουσιαστικά στη δημιουργία δεξαμενής άντλησης της «πρώτης ύλης» αυτής της εγκληματικής συμπεριφοράς[10]:

- **Η ενδοοικογενειακή κακοποίηση και παραμέληση παιδιών**: Ένα μεγάλο ποσοστό που αγγίζει το 80% των παιδιών που βρίσκονται υπό σεξουαλική εκμετάλλευση έχουν υποστεί κάποιου είδους σωματική ή ψυχολογική κακοποίηση μέσα στις οικογένειες τους. Μερικά παιδιά που παρευρέθηκαν στη Σύνοδο Κορυφής του 1998 για τη σεξουαλικά κακοποιημένη νεολαία, ανέφεραν ότι εισήλθαν στην παιδική πορνεία όταν συνειδητοποίησαν ότι για τους γονείς τους ήταν ανεπιθύμητα λάθη.

- **Ένοπλες συγκρούσεις**: Πολλά παιδιά είναι συχνά χωρισμένα από τους γονείς τους, ενώ άλλα τους χάνουν στο σκληρό περιβάλλον ενόπλων συγκρούσεων και πολεμικών γεγονότων και μένουν ορφανά και απροστάτευτα. Στο πλαίσιο αυτό τα ανήλικα παιδιά καθίστανται ιδιαίτερα τρωτά στους εκμεταλλευτές. Είναι πολλές οι περιπτώσεις όπου έχουν αναφερθεί εξαφανίσεις παιδιών από στρατόπεδα προσφύγων, κατά την πορεία για αναζήτηση καλύτερης τύχης, στους τόπους προορισμού κλπ. Τα παιδιά αυτά αποτέλεσαν αντικείμενο εμπορικών πράξεων και συναλλαγών στους τόπους των συγκρούσεων και μεταφέρθηκαν για να ριχθούν στην πορνεία, σε πιο ασφαλείς χώρες, ή δυτικές χώρες.

- **Καταναλωτισμός**: Σε πολλές αναπτυγμένες χώρες κάποια παιδιά ωθούνται στην πορνεία, επιδιώκοντας μεγαλύτερα εισοδήματα με γρήγορους τρόπους. Αυτή η επιθυμία που δημιουργεί ο υπερκαταναλωτισμός, προσελκύει τα ανήλικα παιδιά και τα οδηγεί στο κύκλωμα της παιδικής πορνείας, αφού η επιδίωξη και ο στόχος τους είναι το άμεσο, υψηλό και γρήγορο κέρδος, με το οποίο θα μετέχουν σε απόλαυση αγαθών και υπηρεσιών πολυτελείας.

- **Ανήλικα ορφανά παιδιά λόγω ασθενειών και επιδημιών (AIDS κλπ.)**: Πρόκειται για εκατομμύρια παιδιά της Αφρικής κυρίως, ηλικίας κάτω των 15 ετών, που έχουν χάσει τον έναν ή και τους δύο γονείς τους από το AIDS ή και άλλες αιτίες. Αναμένεται ότι σε λίγα χρόνια, πολλές οικογένειες στην Αφρική θα αποτελούνται μόνον από τα αδέρφια, αφού οι γονείς έχουν αποβιώσει.

---

[10] Δήμου Γ., (2002), «**Η διαχείριση υποθέσεων σεξουαλικής κακοποίησης ανηλίκων**», Αδημοσίευτη.

- **Τα παιδιά των φαναριών**: Τα άστεγα παιδιά που περιφέρονται και ζουν στους δρόμους, καταφεύγουν συχνά στην πορνεία προκειμένου να επιζήσουν, αφού τους αποφέρει υψηλότερες αποδοχές από κάθε άλλη «δραστηριότητα».

- **Εθνοτικές, Κοινωνικές διακρίσεις:** Δεξαμενή άντλησης ανηλίκων παιδιών για εκμετάλλευση, αποτελούν διάφορες εθνοτικές ομάδες και ιδίως μειοψηφίες οικονομικά ασθενέστερων στρωμάτων, που έχουν χαμηλό μορφωτικό επίπεδο, αμφισβητείται η εθνική ταυτότητά τους και η πορεία ζωής αυτών προδιαγράφεται αρνητική, αφού περιορίζεται η πρόσβασή της στην εκπαίδευση και την εργασία.

2.3. Διαδικτυακή ηλεκτρονική τρομοκρατία

Ηλεκτρονική Διαδικτυακή Τρομοκρατία ονομάζεται η δραστηριότητα εκείνη που κατατείνει στην καταστροφή ή τη φθορά συστημάτων, που η λειτουργία των υποστηρίζεται από προσβάσιμους υπολογιστές, με σκοπό την αποσταθεροποίηση μιας χώρας ή την άσκηση πίεσης σε μια κυβέρνηση.

Κατά μια δεύτερη προσέγγιση, ως ηλεκτρονική τρομοκρατία θα μπορούσε να ορισθεί ότι είναι κάθε ενέργεια που αποσκοπεί στην αποσταθεροποίηση μιας χώρας ή στην άσκηση πίεσης σε μια κυβέρνηση, με την ανάπτυξη δραστηριότητας που περιλαμβάνει όλο το φάσμα των ηλεκτρονικών εγκλημάτων μέσω υπολογιστή, ή σε βάρος υπολογιστικού συστήματος μέσω του διαδικτύου [11].

Ένας τρίτος ορισμός της ηλεκτρονικής τρομοκρατίας θα μπορούσε να ορισθεί ως η έξυπνη εκμετάλλευση συστημάτων και ηλεκτρονικών υπολογιστών ή άλλων δικτυακών υποδομών και μέσων, εναντίον φυσικών προσώπων, ή ιδιωτικής περιουσίας για τον εκφοβισμό ή τον εξαναγκασμό κυβερνήσεων ή πληθυσμιακών ομάδων, για την προώθηση πολιτικών ή κοινωνικών στόχων.

Κατά μία τέταρτη εκδοχή, ως ηλεκτρονική τρομοκρατία μπορεί να ορισθεί η προμελετημένη επίθεση εθνικών υποομάδων ή μυστικών πρακτόρων με πολιτικά κίνητρα, εναντίον πληροφοριακών συστημάτων, ηλεκτρονικών υπολογιστών, προγραμμάτων λογισμικού και δεδομένων, που έχει βίαιες επιπτώσεις σε μη στρατιωτικούς στόχους.

---

[11] Γκόρτσος Β.Χ., (2008), **«Πρόληψη και αντιμετώπιση της απάτης στα ηλεκτρονικά μέσα και συστήματα πληρωμών»**, Επιστημονική Ημερίδα ΕΕΤ

Επίθεση εναντίον συστημάτων πληροφορικής μπορεί να εννοηθεί με τρεις τρόπους: φυσική καταστροφή του συστήματος και του περιβάλλοντος χώρου, τακτική επίθεση πρώτου επιπέδου στο λογισμικό του συστήματος και η τακτική επίθεση δευτέρου επιπέδου που είναι και η πλέον επικίνδυνη μέχρι να γίνει αντιληπτή[12].

- Η **φυσική επίθεση** αναφέρεται στην καταστροφή του χώρου λειτουργίας του υπολογιστικού συστήματος με τις συμβατικές μεθόδους (καταστροφή με εμπρησμό του χώρου, θραύση των υποδομών, κλοπή των κυρίων συστημάτων, πρόκληση εκρήξεων, πλημμύρων κ.λ.π.

- Η **τακτική επίθεση πρώτου επιπέδου** περιλαμβάνει την κρυφή αλλοίωση βασικών παραμέτρων του συστήματος, που έχει ως σκοπό την εισαγωγή καθυστερήσεως εκτέλεσης προγραμμάτων και την απρόβλεπτη συμπεριφορά του συστήματος.

- Η **τακτική επίθεση δευτέρου επιπέδου** αναφέρεται στην προσχεδιασμένη τροποποίηση των εισερχομένων και εξερχόμενων πληροφοριών ενός συστήματος, με τέτοιο τρόπο που οι χρήστες και διαχειριστές του συστήματος να εξακολουθούν να θεωρούν φυσιολογική λειτουργία και η ανταπόκρισή του, ενώ το σύστημα οδηγείται σταδιακά σε πλήρη σύγχυση, σε λανθασμένη εκτέλεση προγραμμάτων (κατά τη βούληση του επιτιθέμενου) και τελικά στην πτώση του.

Η ταυτότητα των επιθέσεων και του επιτιθέμενου

Η πρώτη περίπτωση επίθεσης εντάσσεται στις κλασσικές μορφές τρομοκρατίας και δεν χρήζει περαιτέρω αναλύσεως. Στην περίπτωση αυτή, επιτιθέμενος μπορεί να είναι ο μαθητής ενός Σχολείου που επιθυμεί την καταστροφή των στοιχείων ελέγχου της προόδου του, αναρχικές ομάδες εναντίον κρατικών υποδομών, φορολογούμενοι σε γραφεία ΔΟΥ, διάδικοι σε γραφεία Πρωτοδικείων κ.λ.π.

Οι επιθέσεις στη δεύτερη περίπτωση (τακτική επίθεση πρώτου επιπέδου) φαίνεται να κατευθύνονται σε συνδεδεμένα υπολογιστικά συστήματα με τις οποίες διαγράφονται αρχεία, γίνεται σκόπιμη εμφύτευση ενός ιού σε ένα δίκτυο, ώστε να προκληθεί λειτουργική ανωμαλία τόσο σε αυτό όσο και στην υποδομή των χρηστών, ή επιχειρείται ο «τηλεχειρισμός» υπολογιστή μέσω εμφύτευσης ειδικών προγραμμάτων από τους επιτιθέμενους. Ο επιτιθέμενος μπορεί να είναι δυσαρεστημένος υπάλληλος του χώρου, υπάλληλος ανταγωνιστικού χώρου, ή και κάποιος παράνομος εισβολέας (hacker) που δοκιμάζει τις

[12] Γκόρτσος Β.Χ., (2008), «**Πρόληψη και αντιμετώπιση της απάτης στα ηλεκτρονικά μέσα και συστήματα πληρωμών**», Επιστημονική Ημερίδα ΕΕΤ

προστασίες και τις αντοχές του συστήματος. Η επίθεση αυτή αφορά το συγκεκριμένο εργασιακό χώρο ή φορέα και δεν στρέφεται εναντίον της κρατικής εξουσίας, ούτε φαίνεται ικανή να απειλήσει την κρατική οντότητα[13].

Στην τρίτη περίπτωση, ο επιτιθέμενος σχεδιάζει τις ενέργειές του με ιδιαίτερη προσοχή και στοχεύει στην πρόκληση σοβαρής ανωμαλίας και εντέλει στην καταστροφή του υπολογιστικού συστήματος. Αν εξετάσουμε την ταυτότητα του επιτιθέμενου θα καταλήξουμε στη σκέψη ότι αυτός μπορεί να είναι οποιοσδήποτε ευφάνταστος εισβολέας, μέχρι την καλύτερα οργανωμένη τρομοκρατική οργάνωση.

Το διαδίκτυο μπορεί να χρησιμοποιηθεί κατάλληλα από έναν τρομοκράτη, αφού παρουσιάζει μια σειρά πλεονεκτημάτων. Ο τρομοκράτης μπορεί να ασκείται από απόσταση, να μην διαθέτει οικονομικούς πόρους για επιθέσεις και να αποφεύγει τις αιματηρές επιθέσεις με εκρηκτικά και άλλα ηχηρά μέσα, στην προσπάθεια της επιδίωξης της δημοσιότητας. Οι σοβαρές επιθέσεις στο διαδίκτυο ή και η προβολή θεμάτων τρομοκρατίας με έμμεση χρήση του διαδικτύου, γοητεύει κοινό και δημοσιογράφους.

Για τον τρομοκράτη, η αξία του Διαδικτύου είναι σημαντικότερη για τους επιδιωκόμενους σκοπούς, αφού και για αυτόν αποτελεί ένα αρκετά ασφαλές εργαλείο. Έχει διαπιστωθεί από διάφορες τρομοκρατικές ομάδες χρησιμοποιούν μονίμως το διαδίκτυο με καλυμμένο τρόπο για να συντονίζουν τις δραστηριότητές των και να τακτοποιούν οικονομικές υποθέσεις τους, παρά για να κάνουν καταστροφικές επιθέσεις, τουλάχιστον ενάντια στο ίδιο το διαδίκτυο.

Εξετάζοντας από μια άλλη οπτική γωνία και με σχετική αντικειμενικότητα το θέμα της διαδικτυακής τρομοκρατίας, θα διαπιστώσουμε ότι υπάρχει διάχυτη μια εικόνα αβεβαιότητος και συνεπακόλουθα μια τάση μεγαλοποίησης και υπερβολής των απειλών και των αποτελεσμάτων που αυτές θα επιφέρουν.

Κρίνοντας από τις μέχρι τώρα επιθέσεις κατά του Διαδικτύου, διαπιστώνουμε ότι οι περισσότερο καταστροφικές επιθέσεις, έχουν διαπραχθεί από διασπορά ιών και από hackers που περιφέρονται παντού ή διαμαρτύρονται για κάθε είδους ζητήματα και από άτομα που επιδιώκουν να κάνουν κακό σε προηγούμενους εργοδότες τους.

---

[13] Γκόρτσος Β.Χ., (2008), **«Πρόληψη και αντιμετώπιση της απάτης στα ηλεκτρονικά μέσα και συστήματα πληρωμών»**, Επιστημονική Ημερίδα ΕΕΤ

2.4. Κακόβουλες εισβολές σε δίκτυα

Η εισβολή σ' ένα δίκτυο υπολογιστών, το λεγόμενο hacking, αποτελεί βασικό στοιχείο πολλών διαδικτυακών εγκλημάτων. Ο hacker, έχει χαρακτηριστεί από πολλούς ως ο εγκληματίας του 21ου αιώνα. Η θεώρηση του hacking ως εγκλήματος, είναι ένα ζήτημα, που έχει νομικώς αντιμετωπιστεί με διαφορετικές προσεγγίσεις.

Οι hackers επιδιώκουν να αποκτήσουν πρόσβαση σε ξένο υπολογιστή ή σύστημα υπολογιστών χωρίς, κατ' αρχήν, να έχουν το σκοπό της υποκλοπής ή της οποιαδήποτε άλλης επιβλαβούς ενέργειας. Όμως, η εισβολή στο δίκτυο, έστω και αν δεν είναι κακόβουλη, υποκρύπτει έναν κακόβουλο χαρακτήρα, διότι ο επιτιθέμενος εισχωρώντας στο σύστημα αποκτά γνώσεις για την ασφάλειά του, εντοπίζει τις ευπάθειές του και μπορεί, πλέον, ευκολότερα να διαπράξει μια κακόβουλη επίθεση ή να διαθέσει τις πληροφορίες αυτές σε κάποιον που θέλει να διαπράξει την επίθεση.

Η διείσδυση ενός hacker σ' ένα δίκτυο υπολογιστών, αποσκοπεί στην απομακρυσμένη διαχείριση του συστήματος-στόχου. Ανάλογα με τα δικαιώματα, που αποκτά ο επιτιθέμενος στο σύστημα-στόχο, μπορούμε να διακρίνουμε 2 βασικές κατηγορίες. Την πλήρη διείσδυση με δικαιώματα διαχειριστή συστήματος, και τη διείσδυση με δικαιώματα απλού χρήστη συστήματος. Στην πρώτη περίπτωση η επίθεση είναι πιο επικίνδυνη, γιατί ο επιτιθέμενος με δικαιώματα διαχειριστή έχει τη δυνατότητα να επιφέρει σημαντικές αλλαγές στη λειτουργία του συστήματος. Στη δεύτερη περίπτωση ο κίνδυνος είναι μικρότερος αλλά εξίσου σημαντικός.

Βασικές τεχνικές των hackers

Τεχνικές που χρησιμοποιούν οι hackers για να διεισδύσουν σ' ένα δίκτυο ηλεκτρονικών υπολογιστών εξελίσσονται ταυτόχρονα με την ανάπτυξη των υπολογιστικών συστημάτων. Οι πιο συχνά χρησιμοποιούμενες είναι οι ακόλουθες: [14]

Η εκμετάλλευση των cookies: Τα cookies, είναι πολύ μικρά αρχεία κειμένου, τα οποία τοποθετούνται στον Η/Υ από διάφορες τοποθεσίες του Διαδικτύου που επισκέπτεται ένας χρήστης. Τα αρχεία αυτά, περιέχουν διάφορες πληροφορίες, όπως τα στοιχεία του χρήστη, οι δραστηριότητές του, οι συνήθειες του κ.λ.π. Στην περίπτωση, που σ' ένα αρχείο cookie εμπεριέχονται πληροφορίες, όπως το όνομα χρήστη και ο κωδικός πρόσβασης για μια

[14] Γκόρτσος Β.Χ., (2008), «**Πρόληψη και αντιμετώπιση της απάτης στα ηλεκτρονικά μέσα και συστήματα πληρωμών**», Επιστημονική Ημερίδα ΕΕΤ

υπηρεσία, ο hacker έχει την δυνατότητα να τις ανακτήσει εκμεταλλευόμενος κάποια γνωστή ευπάθεια του φυλλομετρητή ή του Λειτουργικού Συστήματος.

Ανίχνευση δικτυακών υπηρεσιών συστημάτων (probes, scans): Μια από τις βασικές ενέργειες των hackers είναι ο εντοπισμός πληροφοριών για το σύστημα στο οποίο θέλουν να επιτεθούν. Για να πετύχουν το σκοπό τους χρησιμοποιούν την τεχνική της σάρωσης θυρών (port scanning). Πρόκειται για μια διαδικασία αποστολής ερωτημάτων σε διακομιστεί, με σκοπό να ληφθούν πληροφορίες για τις υπηρεσίες που προσφέρουν, καθώς και για το χρησιμοποιούμενο επίπεδο ασφαλείας. Οι πληροφορίες αυτές είναι πολύ σημαντικές, γιατί δίνουν τη δυνατότητα στον επιτιθέμενο να παραβιάσει την ασφάλεια του συστήματος, εκμεταλλευόμενος γνωστές αδυναμίες π.χ. του λειτουργικού συστήματος ή άλλων υπηρεσιών που προσφέρονται. Η ανίχνευση, επίσης, μπορεί να αποσκοπεί στην εύρεση και αξιοποίηση λογαριασμών χρηστών που δεν προστατεύονται με κωδικό πρόσβασης, για να επιτευχθεί εύκολη πρόσβαση στο σύστημα[15].

Ανιχνευτές δικτυακών πακέτων (packet sniffers): Η ανίχνευση δικτυακών πακέτων, πραγματοποιείται με τις εφαρμογές λογισμικού packet sniffers, που έχουν τη δυνατότητα να εντοπίζουν όλα τα πακέτα, που κυκλοφορούν στο Διαδίκτυο. Εφόσον, τα πακέτα δεν είναι κρυπτογραφημένα, είναι δυνατή, η απόσπαση πληροφοριών, όπως κωδικοί πρόσβασης, αριθμοί πιστωτικών καρτών κ.ά. Επιπλέον, λαμβάνονται πληροφορίες που αφορούν την τοπολογία ενός δικτύου, τις υπηρεσίες που προσφέρονται και τον αριθμό των υπολογιστών, που είναι στο δίκτυο. Όλες οι πληροφορίες, είναι δυνατόν να αποσπασθούν από πακέτα που διακινούνται για την επιτέλεση καθημερινών εργασιών, η δε ανίχνευση τέτοιων επιθέσεων είναι εξαιρετικά δύσκολη.

Πλαστές διευθύνσεις IP (IP Spoofing): Στις επιθέσεις IP Spoofing, οι εισβολείς παρεμβαίνουν στις επικεφαλίδες των πακέτων που διακινούνται σε ένα δίκτυο και τις τροποποιήσουν ώστε το μήνυμα να φαίνεται ότι προήλθε από αξιόπιστη πηγή. Με την μέθοδο αυτή, επιτυγχάνουν να χρησιμοποιήσουν μια IP διεύθυνση μέσα στο εύρος των διευθύνσεων που εμπιστευόμαστε (εσωτερικές του δικτύου ή κάποιες από τις εξωτερικές) και να αποκτήσουν πρόσβαση σε δικτυακές υπηρεσίες, που προορίζονται για έμπιστους χρήστες του δικτύου. Η τεχνική IP Spoofing χρησιμοποιείται συνήθως σε συνδυασμό με άλλες τεχνικές επιθέσεως. Για παράδειγμα, μπορεί να χρησιμοποιηθεί για να αποκρύψει την πραγματική IP διεύθυνση του επιτιθέμενου σε μια επίθεση Ping of Death.

---

[15] Γκόρτσος Β.Χ., (2008), **«Πρόληψη και αντιμετώπιση της απάτης στα ηλεκτρονικά μέσα και συστήματα πληρωμών»**, Επιστημονική Ημερίδα ΕΕΤ

2.5. Κακόβουλο λογισμικό

Ένα από τα πιο διαδεδομένα εγκλήματα στο χώρο του Διαδικτύου, είναι η διασπορά κακόβουλου κώδικα (malicious code). Ο κακόβουλος κώδικας είναι κώδικας Η/Υ, που δημιουργείται με σκοπό να προκαλέσει ζημιά σε Η/Υ ή να εισχωρήσει σ' ένα Η/Υ, για την υποκλοπή, αλλοίωση ή διαγραφή δεδομένων και προγραμμάτων. Ο κακόβουλος κώδικας, όταν εισχωρήσει σ' ένα Η/Υ, έχει την δυνατότητα να διαγράψει δεδομένα ή προγράμματα, να αλλοιώσει δεδομένα ή προγράμματα, να υποκλέψει δεδομένα και να παρεμποδίσει τη λειτουργία ενός συστήματος (άρνηση εξυπηρέτησης). Ο Sinrod [16], διακρίνει τον κακόβουλο κώδικα σε τρεις βασικές κατηγορίες: *Ιούς*, (viruses), *σκουλήκια* (worms) και *δούρειους ίππους* (Trojan Horses).

2.5.1. Ιοί

Οι ιοί, είναι το πιο συνηθισμένο είδος κακόβουλου κώδικα. Ένας ιός είναι ένα πρόγραμμα το οποίο επισυνάπτει τον εαυτό του σε αρχεία τα οποία υπάρχουν στον υπολογιστή, μια διαδικασία που είναι γνωστή ως μόλυνση. Μετά την μόλυνση, το αρχείο λειτουργεί κατά διαφορετικό τρόπο. Μπορεί, για παράδειγμα, να εμφανίζει ένα μήνυμα στην οθόνη, να τροποποιεί ή να διαγράφει αρχεία. Τα βασικά χαρακτηριστικά ενός ιού, είναι τα ακόλουθα:

- Αποτελείται από μια σειρά εντολών, που εκτελούν συγκεκριμένες κακόβουλες ενέργειες σε ένα υπολογιστή.
- Η εκτέλεση του, έχει δυο βασικές λειτουργίες: Την αναπαραγωγή του και την πρόκληση ζημιάς (payload).
- Προσπαθεί να εγκατασταθεί σε κατάλληλη θέση στο σύστημα αρχείων του υπολογιστή, που θα του εξασφαλίζει, ότι οι οδηγίες του θα εκτελούνται κατά προτεραιότητα ώστε ο χρήστης να μην μπορεί να αντιληφθεί την εκτέλεση του.
- Προσπαθεί να μολύνει προγράμματα, τα οποία είναι πιθανό να σταλούν ή να μεταφερθούν σε άλλο υπολογιστικό σύστημα.

---

[16] Sinrod E., Reilly W., (2000). **«Cyber-crimes: A Practical approach to the application of Federal Computer Laws»**. Santa Clara Computer and high technology law journal.

Κυριότερες μορφές ιών[17]

File-infectors ή parasitic viruses: Οι ιοί της μορφής αυτής, ενεργούν μολύνοντας ένα εκτελέσιμο πρόγραμμα, στο οποίο προσθέτουν τον κακόβουλο κώδικα. Παράλληλα γίνεται κάποια τροποποίηση του αρχείου-ξενιστή ώστε να διασφαλιστεί ότι ο κώδικας του ιού θα εκτελεστεί πρώτος. Αυτού του είδους ο ιός, μολύνει αρχεία με επεκτάσεις : com, exe, sys και olv. Η μετάδοση του ιού γίνεται με οποιοδήποτε φυσικό μέσο αποθήκευσης ή μέσω δικτύου. Του ιούς της κατηγορίας αυτής, μπορούμε, περαιτέρω, να τους διακρίνουμε σε memory-resident, οι οποίοι παραμένουν στη μνήμη του υπολογιστή και έχουν τη δυνατότητα να μολύνουν οποιοδήποτε πρόγραμμα εκτελέσει ο χρήστης και σε non-Resident ή direct-action viruses, οι οποίοι δεν παραμένουν στη μνήμη του υπολογιστή, αλλά, προσκολλούνται σε ένα υπάρχον πρόγραμμα και μεταδίδονται όταν ο χρηστής εκτελέσει το πρόγραμμα αυτό. Οι ιοί αυτοί, ήταν πολύ δημοφιλείς την εποχή των λειτουργικών συστημάτων MS-DOS.

Boot Sector Virus: Ο ιός, «μολύνει» εκτελέσιμο κώδικα συστήματος, που εντοπίζει σε συσκευές βοηθητικής μνήμης, στον Τομές Εκκίνησης (boot sector) ή στο MBR (Master Boot Record) του δίσκου. Ως αποτέλεσμα, ο ιός φορτώνεται στη μνήμη κατά την εκκίνηση (boot) του συστήματος. Περαιτέρω, ο ιός ενεργεί μολύνοντας κάθε δίσκο, που θα χρησιμοποιηθεί τοπικά στον Η/Υ.

Multi-practice viruses: Ενεργούν συνδυάζοντας επιμέρους χαρακτηριστικά των δυο παραπάνω κατηγοριών. Έχουν τη δυνατότητα να μολύνουν εκτελέσιμα αρχεία καθώς και τομείς εκκίνησης, με αποτέλεσμα ένας Η/Υ να είναι δυνατόν να μολυνθεί είτε όταν εκκινήσει από μολυσμένο δίσκο είτε όταν εκτελεστεί ένα μολυσμένο πρόγραμμα.

2.5.2. Σκουλήκια

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

---

[17] Sinrod E., Reilly W., (2000). **«Cyber-crimes: A Practical approach to the application of Federal Computer Laws»**. Santa Clara Computer and high technology law journal.

2.5.3. Δούρειοι Ίπποι

Οι Δούρειοι Ίπποι (Trojan Horses) είναι φαινομενικά, «αθώα» προγράμματα, τα οποία, έχουν μια ή περισσότερες κρυμμένες λειτουργίες οι οποίες δεν είναι εύκολο να εντοπιστούν από τους χρήστες. Τα προγράμματα αυτά, φορτώνονται στο σκληρό δίσκο του υπολογιστή και εκτελούνται, κανονικά, μαζί με τα υπόλοιπα προγράμματα. Πολλές φορές, ο κακόβουλος κώδικας των προγραμμάτων αυτών μπορεί να εμπεριέχεται στα λεγόμενα δημοφιλή προγράμματα. Με τη χρήση ενός δούρειου ίππου ο επιτιθέμενος επιτυγχάνει να αποκτήσει απομακρυσμένο έλεγχο του υπολογιστή του θύματος και να συλλέξει κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών ή να εξαπολύσει μια επίθεση άρνησης εξυπηρέτησης.

2.5.4. Λογικές & ωρολογιακές βόμβες

Μια λογική βόμβα (logic-bomb) είναι ένα πρόγραμμα, το οποίο ενεργοποιείται, όταν συμβεί ένα συγκεκριμένο γεγονός. Το ενεργοποιημένο πρόγραμμα μπορεί να σταματήσει τη λειτουργία του υπολογιστή, να απελευθερώσει έναν ιό, να διαγράψει αρχεία ή να προβεί σε άλλες ζημιογόνες ενέργειες. Η ενεργοποίηση του προγράμματος γίνεται κατόπιν συγκεκριμένης ενέργειας από το χρήστη, είτε αυτόματα σε συγκεκριμένο χρόνο ή ημερομηνία, (ωρολογιακή βόμβα-time bomb).

2.5.5. Ανεπιθύμητη Αλληλογραφία

Η ανεπιθύμητη αλληλογραφία ή Spamming, ορίζεται ως, η χρήση οποιοδήποτε ηλεκτρονικού μέσου για την αποστολή ανεπιθύμητων μηνυμάτων σε πολύ μεγάλες ποσότητες. Αν και ο όρος αναφέρεται, περισσότερο, στην αποστολή μεγάλων ποσοτήτων μηνυμάτων, με διαφημιστικό περιεχόμενο, χρησιμοποιείται, επίσης, για να καταδείξει την αποστολή οποιοδήποτε μηνύματος, το οποίο μπορεί να χαρακτηριστεί ενοχλητικό από αυτόν που το λαμβάνει. Ένα μήνυμα spam, αποστέλλεται με e-mail και περιλαμβάνει πληροφορίες για την προώθηση των προϊόντων μιας εταιρείας. Στην πορεία, πολλές άλλες μορφές και μέσα διάδοσης ενοχλητικής ηλεκτρονικής αλληλογραφίας έχουν χρησιμοποιηθεί, όπως instant messaging spam, Usenet newsgroup spam, Web search engines spam, web logs spam, και mobile phone messaging spam [18].

[18] Wikipedia, (2007), «**Spam**», ανακτήθηκε από http://en.wikipedia.org/ wiki/Spam

Η δυνατότητα, που προσφέρει το Διαδίκτυο, για φθηνή και άμεση αποστολή εκατομμυρίων μηνυμάτων, ωθεί τις ανά τον κόσμο εταιρείες, στην υιοθέτηση τέτοιων μεθόδων για την προώθηση των προϊόντων τους. Η συλλογή των ηλεκτρονικών διευθύνσεων, μπορεί να πραγματοποιηθεί με διάφορους τρόπους. Οι spammers παίρνουν τις διευθύνσεις από τους καταλόγους εταιρειών, που διατηρούν ηλεκτρονικά καταστήματα ή χρησιμοποιούν λογισμικό τύπου harvester[19], το οποίο σαρώνει όλο το Ίντερνετ και συλλέγει χιλιάδες διευθύνσεις από καταλόγους δωμάτια συζητήσεων newsgroups κ.λ.π. Άλλοι, υποκλέπτουν ηλεκτρονικές διευθύνσεις από τους καταλόγους μελών των Εταιρειών Παροχής Internet (ISP). Τέλος, μπορεί να χρησιμοποιηθεί και ειδικό λογισμικό, το οποίο παράγει τεράστιες λίστες τυχαίων διευθύνσεων, όπως για παράδειγμα το εμπορικό λογισμικό Email Generator Platinum 9.0, έχει τη δυνατότητα όχι μόνο να παράγει τεράστιες λίστες τυχαίων διευθύνσεων αλλά να εξακριβώνει εάν είναι έγκυρες ή όχι[20].

Εκτός από διαφημιστικούς σκοπούς, το spamming, μπορεί να χρησιμοποιηθεί και ως βασικό εργαλείο για μια σειρά άλλων επιθέσεων, όπως τις *Επιθέσεις Άρνησης Εξυπηρέτησης*. Στις περιπτώσεις αυτές, οι επιτιθέμενοι κατακλύζουν το διακομιστή με πλήθος μηνυμάτων και τον οδηγούν έτσι σε υπερφόρτωση.

2.5.6. Επιθέσεις σε δικτυακούς τόπους

Πρόκειται για ένα είδος επίθεσης, το οποίο παρουσίασε ιδιαίτερη αύξηση τα τελευταία χρόνια. Οι επιθέσεις αυτές, πραγματοποιούνται από τους βάνδαλους (vandals). Τα κίνητρα των επιθέσεων ποικίλουν. Κυρίως, στρέφονται εναντίον κυβερνητικών οργανισμών και υπηρεσιών.

Σε μια τυπική επίθεση σ' έναν δικτυακό τόπο, το αποτέλεσμα είναι αναστρέψιμο. Ο βάνδαλος θα διαγράψει ορισμένες σελίδες ή γραφικά και θα ανεβάσει τις δικές τους σελίδες, το περιεχόμενο των οποίων, μπορεί να είναι από χιουμοριστικό έως προπαγανδιστικό. Όταν ο ιδιοκτήτης του δικτυακού τόπου αντιληφθεί ότι έχει υποστεί μια τέτοια επίθεση, θα διορθώσει τις προβληματικές σελίδες από εφεδρικά αρχεία. Το κρίσιμο ζήτημα, σ' αυτή την περίπτωση, είναι ο χρόνος που θα απαιτηθεί για την επιδιόρθωση. Αν οι ζημιές που

---

[19] Filedudes, (2010), **«Λογισμικό τύπου harvester»,** ανακτήθηκε από http://www.programurl.com/software/harvester.htm

[20] Email Generator Platinum, (2007), **«Εμπορικό λογισμικό»,** ανακτήθηκε από http://www.email-business.com/index_en.htm

προκλήθηκαν είναι μεγάλες, ίσως να χρειαστεί ο δικτυακός τόπος να παραμείνει εκτός δικτύου για μεγάλο χρονικό διάστημα.

Το πλήγμα, που θα δεχθεί η εταιρεία, όταν ο δικτυακοί της τόπος, που ομολογουμένως αποτελεί την εικόνα της προς εξωτερικούς συνεργάτες και υποψήφιους πελάτες, πέσει θύμα μιας τέτοιας επίθεσης, είναι τεράστιο.

2.5.7. Πειρατεία ονομάτων χώρου

Η πειρατεία ονομάτων χώρου, γνώρισε ιδιαίτερη άνθηση κατά τα πρώτο χρόνια του Διαδικτύου. Διάφοροι επιτήδειοι, εκμεταλλευόμενοι το γεγονός πως μεγάλες εταιρείες δεν είχαν κατοχυρώσει, ακόμη, ονόματα χώρων για τους δικτυακούς τους τόπους, προέβαιναν σε κατοχύρωση ονομάτων διασήμων εταιρειών, με αποτέλεσμα να αποκτούν τα δικαιώματα της νέας διεύθυνσης. Στη συνέχεια, μπορούσαν να δράσουν με δύο διαφορετικούς τρόπους: Είτε να παραχωρήσουν την διεύθυνση στην εταιρεία που κατέχει συγκεκριμένο όνομα, έναντι, βέβαια σημαντικού χρηματικού ποσού,[21] είτε να προβούν στην ανάρτηση, στην συγκεκριμένη διεύθυνση, περιεχομένου προσβλητικού (π.χ. πορνογραφία), γεγονός που επιφέρει σημαντικές συνέπειες στην εταιρεία.

2.6. Πειρατεία Λογισμικού

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

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

---

[21] Lipton. J., (2007), **«Beyond Cybersquatting Taking Domain Name Disputes past Trademark Policy»,** ανακτήθηκε από http://www.law.wfu.edu/prebuilt/w08-lipton.pdf

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

2.7. Εγκλήματα στο Διαδίκτυο

Η απάτη στο συμβατικό κόσμο είναι ένα από τα πιο συνηθισμένα εγκλήματα. Η εμφάνιση, όμως, και ανάπτυξη του Διαδικτύου, μεγιστοποίησε τις δυνατότητες για διάπραξη νέων μορφών απάτης. Η τάση αυτή, αυξήθηκε ακόμη περισσότερο, με την εξάπλωση του ηλεκτρονικού εμπορίου, που είχε ως επακόλουθο την ανάπτυξη οικονομικών συναλλαγών με τη χρήση του Διαδικτύου. Ας δούμε, ενδεικτικά, τις κυριότερες μορφές απάτης μέσω του Διαδικτύου[22]:

2.7.1. Απάτη με e-mail

Η απάτη, με τη χρήση του ηλεκτρονικού ταχυδρομείου, αποτελεί την συχνότερη μορφή επιθέσεως, έναντι των χρηστών του Διαδικτύου. Οι επαγγελματίες του είδους, συνεχώς, βρίσκουν νέους τρόπους για να εξαπατήσουν ανυποψίαστους χρήστες, χρησιμοποιώντας μηνύματα ηλεκτρονικού ταχυδρομείου, που προβάλλουν διάφορες δικαιολογίες, με μοναδικό σκοπό, την απόσπαση χρηματικών ποσών και προσωπικών στοιχείων.

2.7.2. Απάτη με πιστωτικές κάρτες

Η χρήση πιστωτικών καρτών στο Διαδίκτυο, για τη διεκπεραίωση πάσης φύσεως συναλλαγών (π.χ. μέσω του ηλεκτρονικού εμπορίου), έχει δημιουργήσει νέες δυνατότητες για

---

[22] Sinrod E., Reilly W., (2000). **«Cyber-crimes: A Practical approach to the application of Federal Computer Laws»**. Santa Clara Computer and high technology law journal.

τη διάπραξη εγκλημάτων. Η μη αυτοπρόσωπη παρουσία του αγοραστή και η άγνωστη ταυτότητα του πωλητή (ή υποψήφιου απατεώνα) έχουν συμβάλει στην αύξηση των περιπτώσεων απάτης, με την χρήση πιστωτικών καρτών στο Διαδίκτυο.

Με τη χρήση των σύγχρονων τεχνολογιών δεν απαιτείται, πλέον, ιδιαίτερη δεξιότητα για να αποκτήσει κάποιος τον αριθμό μιας πιστωτικής κάρτας και να πραγματοποιήσει αγορές μέσω του Διαδικτύου. Με την τεχνολογία «websniffer», παρακολουθείται η μετάδοση δεδομένων και ανακτώνται αυτόματα δεκαεξαψήφιοι αριθμοί πιστωτικών καρτών. Επιπλέον, είναι δυνατή η αγορά μέσω του Διαδικτύου, αριθμών πιστωτικών καρτών που έχουν υποκλαπεί. Τέλος, υπάρχουν και εφαρμογές λογισμικού, που δημιουργούν αυτόματα αριθμούς πιστωτικών καρτών,[23] χρησιμοποιώντας διάφορους λογάριθμους.

2.7.3. Κλοπή ταυτότητας

Η κλοπή ταυτότητας (Identity Theft) είναι ένα από τα πλέον σοβαρά εγκλήματα του Διαδικτύου. Στην ψηφιακή εποχή που διανύουμε, τεράστιες ποσότητες δεδομένων είναι αποθηκευμένες σε ηλεκτρονικές βάσεις δεδομένων για διάφορους σκοπούς (π.χ. εμπορικούς, ιατρικούς, διαφημιστικούς). Είναι εύκολο για τον καθέναν, να βρει στοιχεία ατόμων και να τα χρησιμοποιήσει για την διεκπεραίωση πάσης φύσεως συναλλαγών.

Το έγκλημα της κλοπής ταυτότητας, ολοκληρώνεται σε δυο στάδια:

Στο πρώτο, ο επιτιθέμενος προσπαθεί να αποκτήσει τα στοιχεία της ταυτότητας ενός ατόμου με διάφορους τρόπους, συμβατικούς και ψηφιακούς όπως:

- Αφαιρώντας πορτοφόλια από τσάντες, αυτοκίνητα ή ακόμη και από την τσέπη ανυποψίαστων περαστικών.
- Υποκλέπτοντας την αλληλογραφία, παραβιάζοντας μη ασφαλή κιβώτια αλληλογραφίας, υποβάλλοντας ψευδή αλλαγή διεύθυνσης κατοικίας στο ταχυδρομικό γραφείο των νόμιμων παραληπτών κ.ά.
- Αποσπώντας τα ενημερωτικά σημειώματα των πιστωτικών καρτών, υποδυόμενο τον υπάλληλο ή συγγενικό πρόσωπο του νόμιμου κατόχου.

---

[23] Whatprice (2012), «**Εργαλεία λογισμικού που δημιουργούν αυτόματα τυχαίους αριθμούς πιστωτικών καρτών και επιβεβαιώνουν την γνησιότητα τους**», ανακτήθηκε από http://www.whatprice.co.uk/financial.html

- Εισβάλλοντας στις βάσεις δεδομένων εταιρειών και οργανισμών, όπου φυλάσσονται προσωπικά δεδομένα.

- Χρησιμοποιώντας ειδικό λογισμικό, το οποίο, έχει τη δυνατότητα, να αποσπά προσωπικά δεδομένα και άλλες πληροφορίες, παρακολουθώντας την κίνηση των πακέτων στο Διαδίκτυο.

Το επόμενο βήμα είναι η χρησιμοποίηση των κλεμμένων στοιχείων και πραγματοποιείται[24]:

- Ανοίγοντας λογαριασμούς πιστωτικών καρτών με τα στοιχεία του θύματος, τους οποίους και χρησιμοποιεί για την αγορά αγαθών μέσω του Διαδικτύου.

- Ανοίγοντας τραπεζικούς λογαριασμούς, τους οποίους, χρεώνει με ακάλυπτες επιταγές

- Δημιουργώντας πλαστές πιστωτικές κάρτες, άδειες οδήγησης, διαβατήρια και ταυτότητες χρησιμοποιώντας τα στοιχεία του θύματος.

- Υποβάλλοντας ψευδείς φορολογικές δηλώσεις (και μέσω Διαδικτύου), για να εισπράξει επιστροφή φόρου.

2.7.4. Ξέπλυμα χρήματος

Με το ξέπλυμα χρήματος (money laundering), επιχειρείται η εξαφάνιση χρήματος που έχει προέλθει από παράνομες δραστηριότητες. Η διαδικασία, που ακολουθείται από τους εγκληματίες για το ξέπλυμα χρήματος, περιλαμβάνει τρία στάδια:

- Στο πρώτο επιχειρείται η μετατροπή των χρημάτων, που προέρχονται από παράνομες δραστηριότητες, σε μια μορφή λιγότερο ύποπτη για τις διωκτικές αρχές. Το παράνομο χρήμα περιέρχεται σε διάφορα οικονομικά ιδρύματα ή διοχετεύεται στο λιανεμπόριο.

- Στο δεύτερο στάδιο, επιχειρείται ο διαχωρισμός του χρήματος από την παράνομη πηγή του, χρησιμοποιώντας πολλαπλές οικονομικές συναλλαγές για να αποκρύψουν το χρήμα.

- Στο τελευταίο στάδιο, ολοκληρώνεται η μετατροπή του παράνομου χρήματος, ώστε, να έχει τη μορφή εισοδήματος, που προήλθε από νόμιμες επαγγελματικές δραστηριότητες.

Η ανωνυμία του Διαδικτύου, δυσχεραίνει την πιστοποίηση της ταυτότητας των πελατών μιας εταιρείας. Ως αποτέλεσμα, πολλές εταιρείες, χωρίς να το γνωρίζουν, διευκολύνουν το ξέπλυμα χρήματος. Για παράδειγμα, έχει διαπιστωθεί η αγορά μέσω του Διαδικτύου ασυνήθιστα μεγάλων ποσοτήτων αγαθών από συγκεκριμένους πελάτες, που θέλουν, μ' αυτό

[24] Newman, R. (2004). **«Identity Theft».** US Department of Justice.

τον τρόπο, να προωθήσουν χρήματα, που έχουν περιέλθει στην κατοχή τους από παράνομες δραστηριότητες. Άλλη μέθοδος ξεπλύματος χρημάτων είναι η κατάθεση μέσω του Διαδικτύου, σχετικά μικρών ποσών σε πολλαπλούς τραπεζικούς λογαριασμούς.

2.8. Αναφορές 2ου κεφαλαίου

1. Email Generator Platinum, (2007), **«Εμπορικό λογισμικό»,** ανακτήθηκε από http://www.email-business.com/index_en.htm
2. Filedudes, (2010), **«Λογισμικό τύπου harvester»,** ανακτήθηκε από http://www.programurl.com/software/harvester.htm
3. Lipton. J., (2007), **«Beyond Cybersquatting Taking Domain Name Disputes past Trademark Policy»,** ανακτήθηκε από http://www.law.wfu.edu/prebuilt/w08-lipton.pdf
4. Newman, R. (2004). **«Identity Theft»**. United States Department of Justice.
5. Sinrod E., Reilly W., (2000). **«Cyber-crimes: A Practical approach to the application of Federal Computer Laws»**. Santa Clara Computer and high technology law journal.
6. Whatprice (2012), **«Εργαλεία λογισμικού που δημιουργούν αυτόματα τυχαίους αριθμούς πιστωτικών καρτών και επιβεβαιώνουν την γνησιότητα τους»**, ανακτήθηκε από http://www.whatprice.co.uk/financial.html
7. Wikipedia, (2007), **«Spam»**, ανακτήθηκε από http://el.wikipedia.org/wiki/Spam
8. Γκόρτσος Β.Χ., (2008), **«Πρόληψη και αντιμετώπιση της απάτης στα ηλεκτρονικά μέσα και συστήματα πληρωμών»**, Επιστημονική Ημερίδα Ελληνικής Ένωσης Τραπεζών
9. Δήμου Γ., (2002), **«Η διαχείριση υποθέσεων σεξουαλικής κακοποίησης ανηλίκων»**, Αδημοσίευτη.

ΚΕΦΑΛΑΙΟ 3. Πληροφοριακοί μηχανισμοί αντιμετώπισης ηλεκτρονικού εγκλήματος

3.1. Η ασφάλεια στο Διαδίκτυο

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

Ο όρος ασφάλεια, χρησιμοποιείται συχνότατα στην καθημερινή μας ζωή. Προσδιορίζει μια ποικιλία από έννοιες. Στον τομέα των πληροφοριακών συστημάτων, η ασφάλεια σχετίζεται με την ικανότητα ενός οργανισμού να προστατεύει τις πληροφορίες του, από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Η ασφάλεια των πληροφοριακών συστημάτων σχετίζεται με την πρόσληψη μη εξουσιοδοτημένων ενεργειών έναντι ενός συστήματος, την ανίχνευση κάθε είδους επιθέσεως και τέλος την αντίδραση δηλαδή την λήψη μέτρων για την αποκατάσταση της ζημιάς, που προκλήθηκε από τον επιτιθέμενο. [25]

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

3.2. Μέτρα πρόληψης

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

---

[25] Πάγκαλος Γ., Μαυρίδης Ι. (2002). **«Ασφάλεια πληροφοριακών συστημάτων και δικτύων»**. Εκδόσεις Ανίκουλα.

3.3. Κωδικοί πρόσβασης

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

Η μέθοδος αυτή, είναι από τις πιο παλιές και λόγω της απλότητας της αλλά και της μεγάλης ασφάλειας που προσφέρει (εφόσον βέβαια τηρούνται οι απαραίτητες προϋποθέσεις), τυγχάνει ευρείας εφαρμογής. Σήμερα, οι κωδικοί πρόσβασης αποτελούν αναπόσπαστο κομμάτι οποιουδήποτε λειτουργικού συστήματος.

Η διατήρηση της αξιοπιστίας ενός συστήματος, που χρησιμοποιεί κωδικούς πρόσβασης, εξαρτάται από ένα βασικό παράγοντα: κατά πόσο οι κωδικοί πρόσβασης μπορούν να παραμείνουν μυστικοί. Υπάρχουν αρκετοί τρόποι με τους οποίους ένας κωδικός πρόσβασης μπορεί να αποκαλυφτεί, όπως για παράδειγμα, με την χρήση απλών εργαλείων λογισμικού. Επιπλέον, ο ίδιος ο χρήστης, με τις πράξεις και παραλείψεις του, μπορεί άθελα του να συμβάλει στην αποκάλυψη των κωδικών του.

Οι βασικότεροι κίνδυνοι εναντίον της ασφάλειας εντός συστήματος, που βασίζεται στην χρήση κωδικών πρόσβασης, είναι[26]:

Η επιλογή των κωδικών πρόσβασης: Η ορθή επιλογή του κωδικού πρόσβασης είναι πολύ σημαντική. Όταν οι χρήστες αφήνονται μόνοι τους να επιλέξουν τους κωδικούς που επιθυμούν, προτιμούν κωδικούς που μπορούν εύκολα να θυμούνται (π.χ. ονόματα, ημερομηνίες γέννησης κ.λ.π.), με αποτέλεσμα κάποιος κακόβουλος να μπορεί να τους μαντέψει. Όταν η επιλογή των κωδικών δεν αφήνεται στους χρήστες, αλλά πραγματοποιείται από τους διαχειριστές ενός συστήματος, τότε επιτυγχάνεται μεγαλύτερη ασφάλεια, ενδέχεται όμως ο χρήστης, εάν ο κωδικός που του χορηγήθηκε είναι δύσκολο να απομνημονευτεί, να τον γράψει σε ένα κομμάτι χαρτί, διευκολύνοντας την διαρροή του εφόσον το χαρτί απολεσθεί ή κλαπεί.

Διαμοιρασμός των κωδικών πρόσβασης: Πολλές φορές, ένας υπάλληλος μπορεί να δώσει τον κωδικό του σε άλλο υπάλληλο, προκειμένου αυτός να έχει πρόσβαση στα αρχεία του,

---

[26] Πάγκαλος Γ., Μαυρίδης Ι. (2002). **«Ασφάλεια πληροφοριακών συστημάτων και δικτύων»**. Εκδόσεις Ανίκουλα.

στην συνέχεια, να δοθεί για τον ίδιο λόγο σε κάποιο τρίτο κ.ο.κ. Τέτοιου είδους διαμοιρασμός των κωδικών πρόσβασης εγκυμονεί κίνδυνους προερχόμενοι, κυρίως, από τους κοινωνικούς μηχανικούς, οι οποίοι προσποιούμενοι ότι είναι υπάλληλοι μίας π.χ. θυγατρικής εταιρείας, επιτυγχάνουν την απόκτηση των κωδικών. [27]

Παρακολούθηση πακέτων: Η παρακολούθηση των πακέτων που διακινούνται στο δίκτυο, μπορεί να έχει ως αποτέλεσμα την ανάκτηση κωδικών πρόσβασης. Για παράδειγμα, η σύνδεση ενός απομακρυσμένου υπολογιστή με ένα κεντρικό υπολογιστή ενός προστατευμένου δικτύου, απαιτεί την εισαγωγή από το χρήση κωδικών πρόσβασης, οι οποίοι, θα διακινηθούν μέσω του δικτύου.

Πρόσβαση στο αρχείο αποθήκευσης των κωδικών: Οι κωδικοί πρόσβασης αποθηκεύονται σε ένα αρχείο του διακομιστή, προκειμένου, να είναι δυνατή η διαδικασία ταυτοποίησης. Εφόσον το αρχείο αυτό δεν φυλάσσεται καλά, ο επιτιθέμενος μπορεί να το ανακτήσει και να έχει, πλέον, στην κατοχή του όλους τους κωδικούς ενός οργανισμού.

3.4. Χρήση λογισμικού ασφαλείας

Η χρήση πακέτων λογισμικού κατά τον σχεδιασμό της ασφάλειας ενός συστήματος, αποτελεί πρωταρχική μέριμνα των διαχειριστών των συστημάτων. Οι πιο διαδεδομένες εφαρμογές είναι τα antivirus και firewalls.

3.5. Λογισμικό Antivirus

Όπως έχει αποδειχθεί από πολλές έρευνες, η διασπορά ιών είναι η πιο διαδεδομένη μορφή επιθέσεων στο Διαδίκτυο. Καθημερινά, δημιουργούνται χιλιάδες νέοι ιοί, που απειλούν, ποικιλοτρόπως, τα υπολογιστικά συστήματα. Η πιο σημαντική μέθοδος αντιμετώπισης των ιών είναι η χρήση αντιβιοτικών προγραμμάτων (antivirus software).

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

Ανίχνευση των ιών: για να εξακριβωθεί, εάν έχει μολυνθεί από ιούς. Η διαδικασία αυτή, μπορεί να γίνει είτε κατόπιν ενέργειας του χρήστη, που επιλέγει μέσω του λογισμικού τον έλεγχο του σκληρού του δίσκου για ιούς, είτε, όπως συμβαίνει μετά σύγχρονα λογισμικά,

---

[27] Πάγκαλος Γ., Μαυρίδης Ι. (2002). **«Ασφάλεια πληροφοριακών συστημάτων και δικτύων»**. Εκδόσεις Ανίκουλα.

πραγματοποιείται αυτόματα, καθώς, το λογισμικό φορτώνεται στην μνήμη RAM του συστήματος και ελέγχει όλες τις εφαρμογές που εκτελούνται.

Προσδιορισμός της ταυτότητας των ιών: Εάν το σύστημα μας έχει προσβληθεί από κάποιο ιό, το λογισμικό θα μας ενημερώσει για την ταυτότητα του. Η δυνατότητα αυτή είναι πολύ σημαντική, γιατί μας επιτρέπει να εκτιμήσουμε το μέγεθος της ζημιάς που έχει προκληθεί, όσο και να εκτελέσουμε τις απαραίτητες ενέργειες, για την αποκατάσταση της ομαλής λειτουργίας του συστήματος.

Καθαρισμός των ιών: Στο τρίτο και τελευταίο στάδιο, αφού έχουν εντοπιστεί οι ιοί που μόλυναν το σύστημα, θα πρέπει να αφαιρεθούν. Τα περισσότερα λογισμικά, όταν έχουν εντοπίσει έναν ιό, προτείνουν στον χρήστη τι ακριβώς να κάνει. Οι πιο συνηθισμένες επιλογές είναι τρεις. Να επιδιορθώσει το αρχείο που έχει μολυνθεί με τον ιό, να θέσει το αρχείο σε καραντίνα, ώστε να μην μπορεί να χρησιμοποιηθεί και να διαγράψει το αρχείο.

3.6. Firewalls

Στην επιστήμη των υπολογιστών όρος Firewall προσδιορίζει μια συσκευή ή εργαλείο λογισμικού (ή και συνδυασμό των ανωτέρω), που παρακολουθεί και φιλτράρει τα πακέτα που επιχειρούν είτε να εισέλθουν, είτε να εξέλθουν από ένα εσωτερικό προστατευμένο δίκτυο ή υπολογιστή. Είναι εργαλεία που ξεχωρίζουν ένα «ασφαλές» θα λέγαμε δίκτυο (π.χ. το Intranet μιας επιχείρησης), από ένα εξωτερικό μη ασφαλές δίκτυο, όπως είναι το Internet.

Τα περισσότερα Firewalls επιτελούν δυο βασικές λειτουργίες ασφαλείας[28]:

Α) Φιλτράρισμα πακέτων (packet filtering) το οποίο βασίζεται στο να επιτρέπει ή να απαγορεύει (permit or deny) την κίνηση των πακέτων που διακινούνται στο δίκτυο, με βάση την υιοθετημένη πολιτική ασφαλείας και

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

[28] Πάγκαλος Γ., Μαυρίδης Ι. (2002). **«Ασφάλεια πληροφοριακών συστημάτων και δικτύων»**. Εκδόσεις Ανίκουλα.

3.7. Κρυπτογραφία & ασφάλεια

Η κρυπτογραφία (cryptography) αποτελεί μέρος της κρυπτολογίας (cryptology), της επιστήμης που ασχολείται με τη μελέτη της ασφαλούς επικοινωνίας. Ο έτερος κλάδος της κρυπτολογίας, είναι η κρυπτανάλυση, που ασχολείται με την ανάλυση και το σπάσιμο των αλγορίθμων κρυπτογράφησης. Η κρυπτογραφία, σύμφωνα με τον ορισμό που δίνεται στη βικιπαίδεια,[29] είναι η επιστήμη που ασχολείται με τους μαθηματικούς μετασχηματισμούς για την εξασφάλιση της ασφάλειας της πληροφορίας.

Οι βασικότεροι στόχοι της κρυπτογραφίας στην γενικότερη ασφάλεια ενός συστήματος είναι η *εμπιστευτικότητα* (confidentiality) η *αυθεντικοποίηση* (authentication), η *ακεραιότητα* (integrity) και *η μη αποποίηση παραλαβή αποστολής* (non redudiation). [30]

Με την κρυπτογράφηση επιχειρείται η μετατροπή της πληροφορίας, από μια κατανοητή μορφή σε ένα γρίφο, ο οποίος παραμένει ακατανόητος. Με την αντίθετη διαδικασία, δηλαδή την αποκρυπτογράφηση, ο γρίφος αυτός επανέρχεται στην αρχική του μορφή και η πληροφορία μπορεί να αναγνωστεί. Η κρυπτογραφία, ως επιστήμη, είναι γνωστή από την αρχαιότητα. Τα πρώτα κρυπτογραφικά συστήματα βασιζόταν στην χρήση κωδικών συμβόλων, αντί, για τα σύμβολα της αλφαβήτου.

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

1. Το αρχικό μήνυμα (plaintext)
2. Το κρυπτογραφικό σύστημα (cryptosystem) το οποίο αποτελείται από έναν αλγόριθμο κρυπτογράφησης και ένα αλγόριθμο αποκρυπτογράφησης.
3. Το κρυπτογραφημένο κείμενο (ciphertext) το οποίο αποτελεί το αποτέλεσμα της εφαρμογής του αλγορίθμου κρυπτογράφησης στο αρχικό μήνυμα, πριν αυτό σταλεί στον παραλήπτη.
4. Ένα κλειδί (key), το οποίο είναι μια συμβολοσειρά, η οποία χρησιμοποιείται από τους αλγόριθμοι στην διαδικασία κρυπτογράφησα και αποκρυπτογράφησα.

---

[29] Wikipedia, (2012), «**Κρυπτογραφία**», ανακτήθηκε από http://el.wikipedia.org/wiki/Κρυπτογραφία

[30] **Εμπιστευτικότητα** σημαίνει ότι το μήνυμα δεν θα διαρρεύσει σε άτομο ή άτομα που δεν έχουν το δικαίωμα να το προσπελάσουν. **Αυθεντικοποίηση** είναι η επιβεβαίωση ότι το μήνυμα εστάλη από το άτομο που πραγματικά το έστειλε. **Ακεραιότητα** σημαίνει ότι το μήνυμα θα φτάσει στον αποδέκτη του χωρίς να έχει αλλοιωθεί ή μετατραπεί. Η **μη αποποίηση παραλαβή αποστολής** σημαίνει ότι ο αποστολέας ή ο παραλήπτης του μηνύματος, δεν θα αρνηθούν ότι έστειλαν ή παρέλαβαν το μήνυμα.

Από τεχνικής απόψεως, η κρυπτογραφία διακρίνεται σε δύο βασικές κατηγορίες. Τη συμμετρική κρυπτογραφία (symmetric cryptography) στην οποία χρησιμοποιείται ένα ιδιωτικό κλειδί και την ασύμμετρη κρυπτογραφία (asymmetric cryptography) στην οποία χρησιμοποιούνται δύο κλειδιά, ένα δημόσιο και ένα ιδιωτικό.

3.7.1. Συμμετρική κρυπτογραφία

Στην συμμετρική κρυπτογράφηση, το κύριο χαρακτηριστικό είναι ότι χρησιμοποιείται το ίδιο κλειδί, τόσο για την κρυπτογράφηση όσο και την αποκρυπτογράφηση των δεδομένων, βασική προϋπόθεση αποτελεί, το κλειδί να έχει δοθεί στους χρήστες, που επιθυμούν να επικοινωνήσουν, μέσω ενός ασφαλούς καναλιού επικοινωνίας. Η διαδικασία επικοινωνίας έχει ως εξής: Το αρχικό μήνυμα κρυπτογραφείται με το μυστικό κλειδί του αποστολέα και αποστέλλεται στον παραλήπτη μέσω του καναλιού επικοινωνίας. Ο παραλήπτης παραλαμβάνει το κρυπτογραφημένο μήνυμα και το αποκρυπτογραφεί με το ίδιο μυστικό κλειδί. [31]

3.7.2. Ασύμμετρη κρυπτογραφία

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

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

[31] Wikipedia, (2012), «**Κρυπτογραφία**», ανακτήθηκε από http://el.wikipedia.org/wiki/Κρυπτογραφία

συμμετρική κρυπτογράφηση για τον ίδιο βαθμό ασφαλείας.

Χρησιμοποιώντας την συμμετρική κρυπτογραφία λίγο διαφορετικά, μπορούμε να επιτύχουμε την ταυτοποίηση του αποστολέα ενός μηνύματος. Στην περίπτωση αυτή, ο αποστολέας κρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί. Το μήνυμα μπορεί να αποκρυπτογραφηθεί μόνο με το δημόσιο κλειδί, που μπορεί να το έχει οποιοσδήποτε, αλλά η αρχική κρυπτογράφηση με το ιδιωτικό κλειδί, που συνηθίζει να λέγεται ψηφιακή υπογραφή, προσδιορίζει και μοναδικά τον αποστολέα αυτού.

3.7.3. Διαχείριση δημοσίων κλειδιών

Το πρόβλημα, που προκύπτει από τη χρήση δημοσίων κλειδιών κατά τη διαδικασία της κρυπτογράφησης, είναι το πώς θα εξακριβωθεί ότι το δημόσιο κλειδί, που λαμβάνει ένας χρήστης, είναι πράγματι αυθεντικό. Η εξακρίβωση αυτή, είναι πολύ σημαντική, διότι κατά την επαλήθευση μιας ψηφιακής υπογραφής, ο χρήστης πρέπει να είναι βέβαιος, ότι το δημόσιο κλειδί που χρησιμοποιεί για την επαλήθευση της υπογραφής, είναι πραγματικά το δημόσιο κλειδί του υποτιθέμενα υπογράφοντος. Χωρίς πρόσθετα μέτρα, θα πρέπει κάθε χρήστης να εξακριβώνει εξωσυστημικά την αυθεντικότητα κάθε δημόσιου κλειδιού, πριν επιλέξει να το εμπιστευθεί. Η πολυπλοκότητα του ζητήματος μπορεί να μειωθεί, εισάγοντας τη δυνατότητα διακρίβωσης για τα δημόσια κλειδιά μέσω μιας τρίτης οντότητας, την οποία εμπιστεύονται και τα δύο μέρη. Η τρίτη οντότητα, που καλείται επίσης αρχή πιστοποίησης, υπογράφει με το δικό της ιδιωτικό κλειδί τα δημόσια κλειδιά και τα αντίστοιχα ονόματα, προσθέτοντας κάποια επιπλέον στοιχεία, π.χ. περίοδο εγκυρότητας. Το κομμάτι αυτό των δεδομένων, που έχει υπογραφεί από την αρχή πιστοποίησης, ονομάζεται πιστοποιητικό. Το πιστοποιητικό μπορεί να επαληθευτεί, χρησιμοποιώντας το δημόσιο κλειδί της αρχής πιστοποίησης.

3.8. Αναφορές 3ου κεφαλαίου

1. Wikipedia, (2012), «**Κρυπτογραφία**», ανακτήθηκε από http://el.wikipedia.org/wiki/Κρυπτογραφία
2. Πάγκαλος Γ., Μαυρίδης Ι. (2002). «**Ασφάλεια πληροφοριακών συστημάτων και δικτύων**». Εκδόσεις Ανίκουλα.

ΚΕΦΑΛΑΙΟ 4. Διοικητικοί μηχανισμοί αντιμετώπισης ηλεκτρονικού εγκλήματος

4.1. Εισαγωγή

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

Η Ηλεκτρονική Εγκληματολογία (Computer Forensic Science)[32] είναι «η επιστήμη που ασχολείται με την αναγνώριση, διατήρηση, ανάλυση και παρουσίαση ψηφιακών αποδείξεων κατά τρόπο νομικά αποδεκτό». Όλο και πιο συχνά, οι αποδείξεις μιας αξιόποινης πράξης είναι κρυμμένες σε έναν υπολογιστή. Είναι αρκετά δύσκολο, όχι μόνο να εντοπίσουμε τις αποδείξεις, αλλά και να τις συγκεντρώσουμε με τέτοιο τρόπο ώστε να είναι αποδεκτές στο δικαστήριο. Οι διωκτικές αρχές πρέπει να αποδείξουν, ότι τα στοιχεία που συλλέχθηκαν από τη σκηνή διάπραξης του εγκλήματος, διατηρήθηκαν αναλλοίωτα και τεκμηριώνουν την ενοχή του κατηγορουμένου. Παράλληλα, θα πρέπει να βεβαιώσουν ότι δεν έγινε κάποια παράλειψη που κατέστρεψε αποδείξεις σχετικές με την αθωότητα του κατηγορουμένου.

4.2. Ψηφιακές αποδείξεις & δεδομένα

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

[32] Παπαθεοδώρου Θ. (2002), «**Δημόσια ασφάλεια και αντεγκληματική πολιτική. Συγκριτική Προσέγγιση**», Νομική Βιβλιοθήκη.

Ψηφιακές αποδείξεις (digital Evidence): Πληροφορίες, που έχουν αποδεικτική αξία σε μια ποινική υπόθεση και μπορούν να αποθηκευτούν ή να μεταδοθούν σε ψηφιακή μορφή. [33]

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

Φυσικά αντικείμενα (physical items): Τα φυσικά μέσα όπου αποθηκεύονται ή μέσω τον οποίων μεταδίδονται πληροφορίες και αντικείμενα δεδομένων.

Γνήσιες ψηφιακές αποδείξεις (original digital evidence): Φυσικά αντικείμενα και αντικείμενα δεδομένων τη στιγμή που συλλέγονται από τη σκηνή του εγκλήματος.

Διπλότυπες ψηφιακές αποδείξεις (duplicate digital evidence): Ένα ακριβές ψηφιακό αντίγραφο όλων των αντικειμένων δεδομένων που περιέχονται σε ένα γνήσιο ψηφιακό αντικείμενο.

Αντίγραφο (copy): Μια ακριβής αναπαραγωγή των πληροφοριών που περιέχονται σε ένα γνήσιο φυσικό αντικείμενο, ανεξάρτητα από το αντικείμενο αυτό.

Οι ψηφιακές αποδείξει μπορεί να είναι αποθηκευμένες σε οποιαδήποτε συσκευή, όπως ηλεκτρονικό υπολογιστή, palmtop, κινητό τηλέφωνο κ.ά., καθώς και σε οποιοδήποτε μέσο αποθήκευσης, όπως CD's, DVD's, κάρτες μνήμης κ.α.

4.3. Εντοπισμός ηλεκτρονικού εγκληματία

4.3.1. Αρχεία καταγραφής (log files)

Τα αρχεία καταγραφής διαδραματίζουν σημαντικό ρόλο, καθώς σε αυτά αποθηκεύονται πληροφορίες, που αφορούν τη λειτουργία του συστήματος. Στα λειτουργικά συστήματα της οικογένειας Windows, υπάρχουν τρία βασικά είδη αρχείων καταγραφής: Application log, System log και Security log.

Ο εντοπισμός όλων των πληροφοριών, που αποθηκεύονται τα αρχεία καταγραφής, μπορεί να πραγματοποιηθεί μέσω της κονσόλας διαχείρισης των Windows.

Η χρησιμότητα των αρχείων καταγραφής των Windows μεγιστοποιείται, όταν έχουν ενεργοποιηθεί συγκεκριμένες πολιτικές ομάδων (group policies). Τα security logs είναι κενά,

---

[33] Παπαθεοδώρου Θ. (2002), «**Δημόσια ασφάλεια και αντεγκληματική πολιτική. Συγκριτική Προσέγγιση**», Νομική Βιβλιοθήκη.

εάν δεν έχει οριστεί συγκεκριμένη πολιτική ασφάλειας για μια ομάδα χρηστών. Η ευθύνη ορισμού πολιτικών ασφάλειας ανήκει στο διαχειριστή και υπεύθυνο ασφαλείας ενός συστήματος.

Από τα αρχεία καταγραφής, ο ερευνητής του ηλεκτρονικού εγκλήματος μπορεί να διαπιστώσει εάν χρησιμοποιήθηκε συγκεκριμένη εφαρμογή από ένα χρήστη, εάν κάποιος μη εξουσιοδοτημένος χρήστης απέκτησε πρόσβαση στο σύστημα, εάν χρησιμοποιήθηκε κάποια περιφερειακή συσκευή και πλήθος άλλων σημαντικών πληροφοριών.

Εκτός από το λειτουργικό σύστημα, αρχεία καταγραφής δημιουργούνται και από άλλες εφαρμογές. Το firewall, ως βασικό εργαλείο, που ελέγχει την κίνηση από και προς ένα προστατευόμενο δίκτυο ή υπολογιστή, αποθηκεύει σημαντικές πληροφορίες στα αρχεία καταγραφής του. Οι πληροφορίες των αρχείων αυτών, αποτελούν σημαντικό προανακριτικό αλλά και αποδεικτικό υλικό, σε περίπτωση μη εξουσιοδοτημένα πρόσβασης σε δίκτυα.

4.3.2. Συναγερμοί, προειδοποιήσεις, αναφορές

Τα αρχεία καταγραφής είναι ένα μόνο είδος δεδομένων, που μπορούν να αντληθούν από το firewall. Τα firewalls μπορούν να προσφέρουν και άλλου είδους πληροφορίες: [34]

Συναγερμοί (Alarms). Τα firewalls έχουν την δυνατότητα να αποστέλλουν μηνύματα υψηλής προτεραιότητας σε συγκεκριμένοι παραλήπτες σε περίπτωση που διαπιστωθεί κάποια ύποπτη δραστηριότητα. Ένα τέτοιο μήνυμα μπορεί να αποσταλεί με e-mail στο διαχειριστή του συστήματος, ή ακόμη να γίνει τηλεφωνική κλήση και παράλληλα η ύποπτη δραστηριότητα να αποθηκευτεί στα αρχεία καταγραφής. Η λειτουργία αυτή είναι πολύ σημαντική, καθώς μπορεί μια επίθεση να αποφευχθεί στη γέννηση της.

Προειδοποιήσεις (Alerts): Αποτελούν μια πιο ήπια μορφή συναγερμού. Η ενημέρωση του διαχειριστή, μπορεί να γίνει με τους τρόπους που αναφέρθηκαν παραπάνω. Η βασική διαφορά είναι, ότι τα μηνύματα δεν έχουν το χαρακτήρα του άμεσου κινδύνου, όπως στην προηγούμενη περίπτωση, αλλά προειδοποιούν για το ενδεχόμενο εκδήλωσης επίθεσης.

Αναφορές (Reports): Αν και οι πληροφορίες ασφαλείας από το firewall αποθηκεύονται στα αρχεία καταγραφής, οι αναφορές μπορούν να δώσουν επιπρόσθετα δεδομένα, όπως την

---

[34] Παπαθεοδώρου Θ. (2002), «**Δημόσια ασφάλεια και αντεγκληματική πολιτική. Συγκριτική Προσέγγιση**», Νομική Βιβλιοθήκη.

συχνότητα αποτυχημένων προσπαθειών απόκτησης μη εξουσιοδοτημένης πρόσβασης και τη συχνότητα σφαλμάτων

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

4.3.3. Εντοπισμός ονόματος & διεύθυνση IP

Ο εντοπισμός της διεύθυνσης IP, αποτελεί βασική ενέργεια των διωκτικών αρχών για την εξιχνίαση πολλών υποθέσεων μη εξουσιοδοτημένης πρόσβασης σε ένα δίκτυο. Στις επιθέσεις αυτές οι εισβολείς χρησιμοποιούν πλαστές διευθύνσεις IP, προκείμενου να παραπλανήσουν τις διωκτικές αρχές. Κάθε διεύθυνση στο Διαδίκτυο έχει έναν αντίστοιχο αριθμό IP.

Το σύστημα, που έχει αναλάβει την διατήρηση των αντιστοιχιών μεταξύ μιας ηλεκτρονικής διεύθυνσης και του αντίστοιχου IP, είναι το DNS (Domain Name System). Κατά την εκδήλωση μιας επίθεσης, ο επιτιθέμενος πλαστογραφεί την διεύθυνση του για να φαίνεται ότι είναι νόμιμος χρήστης, δεν πλαστογραφεί όμως (ή δεν μπορεί να πλαστογραφήσει) τον αντίστοιχο αριθμό IP. [35]

Συνήθως, συσκευές, όπως τα firewalls, έχουν την δυνατότητα να ελέγχουν αν μια διεύθυνση είναι αληθινή ή όχι και ανάλογα να επιτρέπουν ή να απαγορεύουν την πρόσβαση ενός χρήστη. Εφόσον το firewall δεν έχει ρυθμιστεί κατάλληλα, ο ερευνητής θα κληθεί να ελέγξει τις διευθύνσεις όλων όσων απέκτησαν πρόσβαση, προκειμένου να εξακριβώσει από ποιόν προήλθε η κακόβουλη επίθεση.

Η εργασία αυτή μπορεί να διεκπεραιωθεί με διάφορα εργαλεία λογισμικού, τα οποία ελέγχουν αν οι ηλεκτρονικές διευθύνσεις, αναλογούν σε σωστούς αριθμούς IP. Επίσης, υπάρχουν και δικτυακοί τόποι που επιτελούν on-line την εργασία αυτή. Για παράδειγμα στο www.dnsreport.com μπορεί να δοθεί μια ηλεκτρονική διεύθυνση ή διεύθυνση ηλεκτρονικού ταχυδρομείου και να ληφθούν διάφορες πληροφορίες για αυτή όπως το IP.

---

[35] Παπαθεοδώρου Θ. (2002), «**Δημόσια ασφάλεια και αντεγκληματική πολιτική. Συγκριτική Προσέγγιση**», Νομική Βιβλιοθήκη.

4.3.4. Μηνύματα ηλεκτρονικού ταχυδρομείου

Τα μηνύματα ηλεκτρονικού ταχυδρομείου, εκτός από μέσο άμεσης επικοινωνίας μεταξύ χρηστών, χρησιμοποιούνται για την διάπραξη πολλών αδικημάτων, όπως μετάδοση ιών και άλλου κακόβουλου κώδικα, επιθέσεις άρνησης εξυπηρέτησης, απάτες, απειλές, δυσφήμηση κ.ά.

Για τους λόγους αυτούς, η εύρεση του αποστολέα των μηνυμάτων ηλεκτρονικού ταχυδρομείου, αποτελεί βασική εργασία στην αναζήτηση των ηλεκτρονικών ιχνών του επιτιθέμενου. Αν ο αποστολέας αναγράψει στο μήνυμα το όνομά του και την διεύθυνσή του (και τα στοιχεία είναι αληθή) τότε ο εντοπισμός τους είναι εύκολος. Αυτό, όμως, δεν συμβαίνει σχεδόν ποτέ. Ο μόνος τρόπος για την εύρεση του αποστολέα του μηνύματος, στις περιπτώσει αυτές, είναι η ανάγνωση και κατανόηση των επικεφαλίδων του μηνύματος. [36]

Τα μηνύματα ηλεκτρονικού ταχυδρομείου, κατά την μετάβαση τους από τον αποστολέα στον παραλήπτη, διέρχονται από πολλούς ενδιάμεσοι υπολογιστές. Κάθε ένας από αυτούς, προσθέτει τις δικές του πληροφορίες στην επικεφαλίδα του μηνύματος.

Οι πληροφορίες στην επικεφαλίδα του μηνύματος καταγράφονται σε διάφορα πεδία, που αφορούν τις επικεφαλίδες του αποστολέα και του παραλήπτη, τις επικεφαλίδες ημερομηνίας και διάφορες άλλες. Κατά την αναζήτηση του αποστολέα κακόβουλων μηνυμάτων, οι σημαντικότερες πληροφορίες περιλαμβάνονται στις επικεφαλίδες του αποστολέα.

Από αυτές μπορούμε να συλλέξουμε τη διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα, τη διεύθυνση ηλεκτρονικού ταχυδρομείου στην οποία μπορούν να αποστέλλονται πιθανές απαντήσεις το μονοπάτι (διεύθυνση) προς τον αποστολέα και, τέλος, τους διακομιστές από τους οποίους διήλθε το μήνυμα για να φτάσει στον τελικό του παραλήπτη. Η πρόσβαση στις πληροφορίες αυτές, είναι δυνατή μέσω των χρησιμοποιούμενων εφαρμογών ηλεκτρονικού ταχυδρομείου.

4.4. Αστυνομία & ηλεκτρονικό έγκλημα

Μολονότι η Ελλάδα υπολείπεται ακόμα σημαντικά των άλλων ευρωπαϊκών χωρών στη χρήση των ηλεκτρονικών πληρωμών και στη διείσδυση του διαδικτύου, εντούτοις οι ρυθμοί

---

[36] Παπαθεοδώρου Θ. (2002), **«Δημόσια ασφάλεια και αντεγκληματική πολιτική. Συγκριτική Προσέγγιση»**, Νομική Βιβλιοθήκη.

ανάπτυξης αυξάνονται γεωμετρικά κατά τη διάρκεια της τελευταίας δεκαετίας. Με δεδομένη την πλευρά της ζήτησης, σημαντική – ίσως δε και καθοριστική – είναι και η πλευρά της προσφοράς. Οι τράπεζες της χώρας μας αντιμετωπίζοντας τον ολοένα και περισσότερο αυξανόμενο ανταγωνισμό από τις τράπεζες των υπολοίπων ευρωπαϊκών χωρών, παράλληλα με το συνεχή εκσυγχρονισμό της υποδομής των υποκαταστημάτων τους, προχωρούν και στην ανάπτυξη των εναλλακτικών δικτύων εξυπηρέτησης της πελατείας τους, αξιοποιώντας τις συνεχώς αυξανόμενες δυνατότητες που παρέχονται από τις εφαρμογές της πληροφορικής και των τηλεπικοινωνιών. Για το λόγο αυτό επενδύουν συνεχώς σε τεχνολογικές λύσεις που προσφέρουν στους συναλλασσόμενους, μέσω των εναλλακτικών δικτύων, το ίδιο επίπεδο ασφάλειας, με αυτό που απολαμβάνουν οι πελάτες που συνεχίζουν να συναλλάσσονται μέσω του παραδοσιακού δικτύου εξυπηρέτησης, δηλαδή του καταστήματος. [37]

Δυστυχώς, όμως, όσο αυξάνονται οι ηλεκτρονικές συναλλαγές πληρωμών, τόσο αυξάνεται, και στο πεδίο αυτό, η δράση του οργανωμένου εγκλήματος, το οποίο αναπτύσσει συνεχώς νέες τεχνικές εξαπάτησης με στόχο την υποκλοπή των προσωπικών στοιχείων των συναλλασσομένων, και την απόκτηση πρόσβασης στα ηλεκτρονικά μέσα με τα οποία αυτοί πραγματοποιούν τις ηλεκτρονικές πληρωμές τους. Η δράση δε αυτή είναι άκρως διεθνοποιημένη. Οι τράπεζες έχουν πλήρη κατανόηση ότι η δημιουργία και διατήρηση της εμπιστοσύνης στις ηλεκτρονικές συναλλαγές πληρωμών είναι ένα επιχειρηματικό ζήτημα στρατηγικής σημασίας που απαιτεί απόλυτα εξειδικευμένο και κατάλληλα εκπαιδευμένο προσωπικό και τεχνική υποστήριξη υψηλής τεχνολογίας. Στο πλαίσιο αυτό η δραστηριοποίησή τους είναι έντονη και η ανάληψη πρωτοβουλιών συνεχής, τόσο σε ενδοεπιχειρησιακό όσο και σε συλλογικό επίπεδο. Στο πλαίσιο αυτό, ο ρόλος που διαδραματίζει η Ελληνική Ένωση Τραπεζών (ΕΕΤ), ως φορέας εκπροσώπησης των τραπεζών που ασκούν δραστηριότητα στην Ελλάδα, πιστεύω ότι είναι σημαντικός. Ειδικότερα:

(α) Σε ευρωπαϊκό επίπεδο, Η ΕΕΤ συμμετέχει ενεργά σε επιτροπές που ασχολούνται με την καταπολέμηση, δηλαδή την πρόληψη και την καταστολή, του οικονομικού εγκλήματος, όπως το EAST (European ATM Security Team), το IT Fraud WG της Ευρωπαϊκής Τραπεζικής Ομοσπονδίας και το Information Security Expert Croup του Ευρωπαϊκού Συμβουλίου Πληρωμών. Με την εκπροσώπησή της στις εν λόγω επιτροπές έχει τη δυνατότητα να ενημερώνεται έγκαιρα και έγκυρα για τις διεθνείς πρακτικές που ακολουθούνται από τα άλλα κράτη μέλη της Ευρωπαϊκής Κοινότητας στα διάφορα θέματα που άπτονται της εν λόγω

[37] Πανούσης Γ., Βιδάλη Σ. (2001) «**Κείμενα για την αστυνομία και την αστυνόμευση**», Εκδόσεις Σάκκουλας.

θεματικής, τις τάσεις και τις ανάγκες που προκύπτουν και τις πρωτοβουλίες που σχεδιάζονται. Κυρίως, όμως, έχει τη δυνατότητα να συνεισφέρει και να συμμετέχει στη λήψη των αποφάσεων, στο βαθμό και στην έκταση που της αναλογεί. Οι εξελίξεις διαχέονται άμεσα στις τράπεζες-μέλη της, προσφέροντας τους την απαραίτητη τεχνογνωσία για τη λήψη των επιχειρηματικών τους αποφάσεων και τη χάραξη της μεσοπρόθεσμης ή/και μακροπρόθεσμης πολιτικής τους.

(β) Σε εθνικό επίπεδο, η ΕΕΤ συμμετέχει σε πρωτοβουλίες, όπως η Ομάδα Δράσης για τη Ψηφιακή Ασφάλεια DART της Ειδικής Γραμματείας Ψηφιακού Σχεδιασμού του Υπουργείου Οικονομίας και Οικονομικών και το E-business Forum που είναι ένα μόνιμο forum διαβούλευσης της Πολιτείας με τον επιχειρηματικό και τον ακαδημαϊκό κόσμο. Συνεργάζεται με φορείς όπως η Ελληνική Αστυνομία, η Γενική Γραμματεία Πληροφοριακών Συστημάτων του ΥΠΟΙΟ, η Εθνική Πύλη Ερμής, και η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων. Επίσης, συμμετέχει ενεργά σε νομοπαρασκευαστικές επιτροπές των αρμόδιων υπουργείων για θεσμικά και ρυθμιστικά θέματα που αφορούν τα ηλεκτρονικά μέσα και συστήματα πληρωμών με στόχο την αρτιότερη δυνατή ενσωμάτωση των διεθνών κανόνων και το διαρκή εκσυγχρονισμό του ελληνικού κανονιστικού πλαισίου. Το έργο της ΕΕΤ δεν εξαντλείται, όμως, στο πεδίο της εκπροσώπησης του κλάδου. Σε συνεργασία με τις τράπεζες-μέλη της, παρακολουθεί διεξοδικά τόσο τα θέματα που προκύπτουν από συγκεκριμένα κρούσματα απάτης, όσο και τα θέματα που αφορούν την πρόληψη κακόβουλων επιθέσεων κατά των τραπεζικών καταστημάτων, του εξοπλισμού τους, και των ηλεκτρονικών υποδομών των τραπεζών τόσο σε τεχνικό όσο και σε κανονιστικό επίπεδο με στόχο τη βελτίωση των μεθόδων μελλοντικής αντιμετώπισής τους. Με τη συνδρομή της ΕΕΤ έχει προωθηθεί σημαντικά η συνεργασία μεταξύ τραπεζών και των υπηρεσιών Ηλεκτρονικού και Οικονομικού Εγκλήματος της Ελληνικής Αστυνομίας, η οποία είναι απολύτως απαραίτητη για την αντιμετώπιση αυτού του είδους του εγκλήματος. Καθοριστικής σημασίας παράγοντας για την αντιμετώπιση του οικονομικού εγκλήματος είναι, βέβαια, και η ενημέρωση της πελατείας. Προς την κατεύθυνση αυτή οι τράπεζες και η ΕΕΤ έχουν προχωρήσει στην έκδοση οδηγιών οι οποίες επικοινωνούνται στην πελατεία με την κυκλοφορία ενημερωτικών φυλλαδίων, με τη δημοσίευση σχετικών, με τη συμμετοχή σε ημερίδες και εκδηλώσεις και με την ανάρτηση στις ιστοσελίδες της ΕΕΤ και των τραπεζών και στις οθόνες των ΑΤΜ χρηστικών πληροφοριών για το κοινό.

Η έρευνα των Ηλεκτρονικών Εγκλημάτων είναι αρκετά δύσκολη και ιδιαίτερα χρονοβόρος η διαδικασία του εντοπισμού των «ηλεκτρονικών ιχνών». Μία έρευνα μπορεί να διαρκέσει από

ένα μήνα έως και δύο χρόνια. Ο λόγος της μεγάλης διάρκειας είναι διότι οι χρήστες του Διαδικτύου που ερευνώνται και που έχουν καταγγελθεί στην υπηρεσία μας ότι έχουν διαπράξει μια αξιόποινη πράξη λαμβάνουν διάφορα διαδικτυακά μέτρα προστασίας, έτσι ώστε ο εντοπισμός του να καθίσταται αρκετά δύσκολος.

Σε κάθε διαδικτυακή έρευνα γίνεται προσπάθεια εντοπισμού του «ηλεκτρονικού ίχνους» του δράστη, το οποίο για κάθε χρήστη του Ιντερνέτ είναι μοναδικό, και αποτελεί σημαντικό στοιχείο για την αποδεικτική διαδικασία στο δικαστήριο. Η λεγομένη ηλεκτρονική απόδειξη (electronic evidence) δεν ταυτίζεται με τα παραδοσιακά αποδεικτικά μέσα. Τα τελευταία, έχουν κατά κανόνα υλική υπόσταση και μπορούν να εντοπιστούν σε συγκεκριμένο τόπο και χρόνο. Αντίθετα, τα ηλεκτρονικά αποδεικτικά μέσα είναι ψηφιακά!

Σύμφωνα με τον Προϊστάμενο του Τμήματος Ηλεκτρονικού Εγκλήματος/ΔΑΑ, Αστυνόμο Α΄ κ. Εμμανουήλ Σφακιανάκη «*ο σωστός συνδυασμός των τεχνικών μέσων μαζί με τον ανθρώπινο παράγοντα είναι η χρυσή συνταγή για καλά αποτελέσματα. Εάν υπάρχουν τα τεχνολογικά μέσα (η/υ μαζί με λογισμικό) χωρίς την κατάλληλη εξειδίκευση του αστυνομικού προσωπικού, τότε τα αποτελέσματα δεν θα είναι τα αναμενόμενα. Στην υπηρεσία μας πιστεύω ότι υπάρχει η σωστή αναλογία σε τεχνικά μέσα και προσωπικό*». [38]

Η Ελληνική αστυνομία αποκάλυψε κύκλωμα αλλοδαπών, κυρίως Ρουμάνων, οι οποίοι παγίδευαν τα ΑΤΜ Τραπεζών, με ηλεκτρονικά μηχανήματα αντιγραφής κωδικών και στοιχείων από κάρτες ανάληψης πελατών, αποκομίζοντας εκατοντάδες χιλιάδες ευρώ. Το κύκλωμα κατασκεύαζε πλαστές κάρτες και έκανε αναλήψεις από τους λογαριασμούς. Όπως ανακοινώθηκε από την αστυνομία, η απάτη έγινε γνωστή εδώ και έξι μήνες περίπου, μετά από καταγγελίες της Ελληνικής Ένωσης Τραπεζών, στο Τμήμα Οικονομικών Εγκλημάτων της Ασφάλειας Αττικής.

Από τη μέχρι στιγμής έρευνα έχει προκύψει ότι το κύκλωμα στο διάστημα αυτό είχε κάνει ανάληψη συνολικά 450 χιλιάδες ευρώ μόνο από μία τράπεζα, ενώ η συνολική ζημιά δεν έχει ακόμη προσδιοριστεί, γιατί δεν έχει γίνει γνωστό το ποσό που έχουν κάνει ανάληψη από άλλες τράπεζες. Επίσης, το κύκλωμα το οποίο ήταν οργανωμένο και διεθνές, δραστηριοποιούνταν και στη Γερμανία, Βέλγιο, Ολλανδία και Ιταλία.

---

[38] Πανούσης Γ., Βιδάλη Σ. (2001) «**Κείμενα για την αστυνομία και την αστυνόμευση**», Εκδόσεις Σάκκουλας.

Η Ελληνική αστυνομία σε συνεργασία και με άλλες υπηρεσίες δρα αποτελεσματικά στη δίωξη ηλεκτρονικού οικονομικού και μη εγκλήματος. Δεν είναι τυχαίο ότι είκοσι δυο (22) Υπηρεσίες της Ελληνικής Αστυνομίας βραβεύθηκαν από τη «VISA HELLAS» για την ουσιαστική συμβολή τους στην εξάρθρωση κυκλωμάτων απάτης και πλαστογραφίας με πιστωτικές κάρτες κατά το έτος 2008.[39]

Η αντιμετώπιση του ηλεκτρονικού εγκλήματος, από τις υπηρεσίες επιβολής του νόμου και ιδιαίτερα την αστυνομία, αποτελεί πρωταρχικό ζήτημα. Ο παραδοσιακός τρόπος προσεγγίσεως του εγκλήματος, δηλαδή της περιγραφής του δράστη με την κατάθεση του θύματος, της συλλογής πληροφοριών από πληροφοριοδότες, της διεξαγωγής έρευνας, κατάσχεσης κ.λ.π. δεν ισχύει στον κυβερνοχώρο. Για την έρευνα των ηλεκτρονικών εγκλημάτων, απαιτούνται εξειδικευμένες αστυνομικές υπηρεσίες με εκπαιδευμένο προσωπικό και σύγχρονα τεχνικά μέσα.

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

Οι κύριες αρμοδιότητες τηςUS-CERT είναι η ανάλυση των πιθανών διαδικτυακών απειλών και ευπαθειών και η καταβολή προσπαθειών για τον περιορισμό τους, η ενημέρωση των συναρμόδιων υπηρεσιών για πιθανές δικτυακές απειλές και ο συντονισμός των ενεργειών αντιμετώπισης συμβάντων σχετικών με το Διαδίκτυο.

---

[39] Γκόρτσος Β.Χ., (2008), «**Πρόληψη και αντιμετώπιση της απάτης στα ηλεκτρονικά μέσα και συστήματα πληρωμών**», Επιστημονική Ημερίδα ΕΕΤ

4.5. Ένα υβριδικό μοντέλο ερευνών

1ο Βήμα προπαρασκευαστικής ενέργειας[40]

Η ενημέρωση λαμβάνει δυο συνιστώσες. Η πρώτη αφορά την ενημέρωση ότι έλαβε χώρα το συμβάν. Η δεύτερη αφορά την ενημέρωση της αρμόδιας υπηρεσίας ότι έλαβε χώρα το συμβάν. Η αρμόδια υπηρεσία καθορίζεται από γεωγραφικά κριτήρια (τόπος τέλεσης του εγκλήματος), καθώς και από τη φύση του αδικήματος (ληστεία, ανθρωποκτονία κ.λ.π.). Η έγκαιρη και πλήρης ενημέρωση είναι σημαντική προκειμένου να είναι άμεση η εκδήλωση των ενεργειών που προβλέπονται από τα παρακάτω βήματα:

Εξουσιοδότηση: Η Εξουσιοδότηση λαμβάνεται από την υπηρεσία που καλείται να επιληφθεί το συμβάν. Ο τύπος και το είδος της εξουσιοδότησης, εξαρτώνται από το είδος του εγκλήματος και το νομικό καθεστώς της χώρας στην τελέστηκε. Για παράδειγμα, σύμφωνα με το Ειρηνικό δίκαιο, σε περίπτωση αυτόφωρων κακουργημάτων ή πλημμελημάτων, οι ανακριτικοί υπάλληλοι είναι υποχρεωμένοι να ενεργήσουν όλες τις απαραίτητες πράξεις για την βεβαίωση του εγκλήματος και την ανακάλυψη των δραστών, ειδοποιώντας με το ταχύτερο μέσο τον αρμόδιο εισαγγελέα

Προετοιμασία: Η προετοιμασία της έρευνας αφορά το γενικότερο σχεδιασμό για την άρτια ολοκλήρωση της, όπως τα μέσα, ο εξοπλισμός και το προσωπικό που θα απαιτηθεί για την διεξαγωγής της. Στην προετοιμασία, μπορεί να ενταχθεί όχι μόνο αυτή που ενεργείται κατόπιν ενημέρωσης για ένα συμβάν, αλλά και η γενικότερη προετοιμασία μιας υπηρεσίας από άποψη εκπαίδευσης, εξειδίκευσα, και διαθέσιμων τεχνικών μέσων για την αντιμετώπιση ενός συμβάντος εγκλήματος. Στο στάδιο αυτό ορίζεται και ο υπεύθυνος διεξαγωγής της έρευνας.

2ο βήμα:Έρευνα σκηνής διάπραξης του εγκλήματος

Σήμανση της σκηνής διάπραξης του εγκλήματος: Ο πρώτος αστυνομικός που θα φτάσει στη σκηνή διάπραξης του εγκλήματος, θα πρέπει να φροντίσει για την παροχή πρώτων βοηθειών σε τυχόν τραυματίες, την αναζήτηση μαρτύρων και υπόπτων και τον αποκλεισμό πρόσβασης σε άτομα που δεν έχουν λάβει σχετική εξουσιοδότηση. Παράλληλα, θα πρέπει να μεριμνήσει για τη σωστή σήμανση της σκηνής, προκειμένου να καταστεί δυνατή η διατήρηση των δεδομένων, ψηφιακών και συμβατικών, που περικλείονται σε αυτή.

---

[40] Βιδάλη Σ. (2001), **«Η ελληνική αστυνομία του 21ου αιώνα: ένα μεσογειακό μοντέλο αντεγκληματικής πολιτικής»**, Εκδόσεις Σάκκουλας.

Αναγνώριση – Διαφύλαξη: Πραγματοποιείται από τους αρμόδιους εξερευνητές των Εγκληματολογικών Εργαστηρίων. Καλούνται να αναγνωρίσουν αντικείμενα στην σκηνή διάπραξης του εγκλήματος, που ενδεχομένως έχουν αποδεικτική αξία. Τα αντικείμενα μπορεί να έχουν ψηφιακή ή συμβατική μορφή, όπως ηλεκτρονικοί υπολογιστές, κινητά τηλέφωνα, χειρόγραφες σημειώσεις, βιολογικό υλικό (π.χ. τρίχες, υγρά του σώματος), δαχτυλικά αποτυπώματα κ.λ.π. Σε πολύ σοβαρά αδικήματα, ενδέχεται να εμπλέκονται στο στάδιο αυτό εμπειρογνώμονες από διάφορα ερευνητικά πεδία. Η μεταξύ τους συνεργασία αποτελεί σημαντικό παράγοντα, για την διατήρηση όσο το δυνατόν περισσότερων αποδεικτικών στοιχείων.

Συλλογή: Η συλλογή των αποδεικτικών στοιχείων είναι από τα σημαντικότερα βήματα του μοντέλου. Ο εξερευνητής θα κληθεί να συλλέξει αποτυπώματα, αντικείμενα, βιολογικό υλικό, ψηφιακά δεδομένων κ.ά. που θα χρήζουν περαιτέρω ανάλυσης στο εργαστήριο.

Εφόσον στην σκηνή περιλαμβάνονται και συσκευές ηλεκτρονικής επεξεργασίας δεδομένων, θα πρέπει να καταβληθεί κάθε δυνατή προσπάθεια ώστε να ανακτηθούν άμεσα τυχόν μεταβλητά δεδομένα. Το κρίσιμο σημείο στη φάση αυτή είναι η συνεργασία μεταξύ του ερευνητών που αναζητούν συμβατικά και ψηφιακά δεδομένα. Όπως προαναφέρθηκε, μια προσπάθεια ανάκτησης ψηφιακών δεδομένων μπορεί να οδηγήσει στην καταστροφή των αντίστοιχων συμβατικών και το αντίθετο.

Μεταφορά: Η μεταφορά των αποδεικτικών στοιχείων, είναι εξίσου σημαντική με τη συλλογή. Κατά την μεταφορά, θα πρέπει να λαμβάνονται τέτοια μέτρα, για κάθε αντικείμενο που μεταφέρεται, ώστε τα αποδεικτικά στοιχεία, που πιθανώς περικλείει, να παραμείνουν αναλλοίωτα. Οι βασικότεροι παράγοντες, που πρέπει να ληφθούν σοβαρά υπόψη κατά τη μεταφορά, είναι η συσκευασία, ο τρόπος τοποθέτησης στο όχημα μεταφοράς και οι κλιματολογικές συνθήκες, που επηρεάζουν την αρτιότητα τόσο των συμβατικών όσο και των ψηφιακών δεδομένων.

3ο βήμα: Εργαστηριακή Έρευνα[41]

Εξέταση: Η εξέταση των αποδεικτικών στοιχείων στο χώρο του εργαστηρίου, αποσκοπεί στην άντληση όσο το δυνατόν περισσότερων πληροφοριών για κάθε αντικείμενο.

---

[41] Βιδάλη Σ. (2001), **«Η ελληνική αστυνομία του 21ου αιώνα: ένα μεσογειακό μοντέλο αντεγκληματικής πολιτικής»**, Εκδόσεις Σάκκουλας.

Αποθήκευση: Τα αποδεικτικά στοιχεία που εξετάστηκαν, θα πρέπει να αποθηκευτούν κατά τέτοιο τρόπο ώστε να διατηρηθούν αναλλοίωτα, για να μπορούν να επανεξεταστούν, σε περίπτωση που αμφισβητηθεί η αποδεικτικότητα τους στο ακροατήριο ή κριθεί ότι περιέχουν επιπλέον στοιχεία, που αρχικά δεν είχαν εντοπιστεί.

Τεκμηρίωση: Μετά την εξέταση όλων των αντικειμένων, συντάσσεται η έκθεση πραγματογνωμοσύνη η οποία τεκμηριώνει τα αποτελέσματα της έρευνας, με βάση τα δεδομένα που προέκυψαν από την εργαστηριακή εξέταση.

4ο βήμα: Ολοκλήρωση της έρευνας[42]

Συμπέρασμα: Η εξαγωγή συμπερασμάτων για το έγκλημα, πραγματοποιείται από αυτόν που έχει την κύρια ευθύνη της έρευνας. Αξιολογεί τόσο τις εκθέσεις πραγματογνωμοσύνη του αρμόδιου εργαστηρίου, όσο και τις λοιπές πληροφορίες, που συλλέχθηκαν κατά την διάρκεια της προανακριτικής διαδικασία, προκειμένου να καταλήξει σε ασφαλή συμπεράσματα για τα αίτια του εγκλήματος και την ταυτότητα των δραστών.

Διανομή: Η διανομή των πληροφοριών, αφορά την ενημέρωση συνεργαζόμενων υπηρεσιών, για την μεθοδολογία των δραστών, τα χρησιμοποιούμενα μέσα, και την εν γένει οργάνωση του εγκλήματος, προκειμένου να είναι δυνατή στο μέλλον η αντιμετώπιση παρόμοιων περιστατικών. Η ραγδαία ανάπτυξη του εγκλήματος υψηλής τεχνολογίας, έχει καταστήσει ιδιαίτερα σημαντική την διαδικασία αυτή και η αποκτούμενη τεχνογνωσία, αποτελεί βασικό παράγοντα αντιμετώπισής του.

Το προτεινόμενο, υβριδικό μοντέλο, φέρει όλα τα πλεονεκτήματα των υπαρχόντων έως σήμερα μοντέλων ερευνών, αλλά προσφέρει και ένα επιπρόσθετο όφελος. Αντιμετωπίζει το εγκληματικό φαινόμενο ως σύνολο, εντάσσοντας τα επιμέρους χαρακτηριστικά κάθε παραβατικής συμπεριφοράς, σε μια ενιαία και ευέλικτη διαδικασία ερευνητικών ενεργειών. Η περαιτέρω ομαδοποίηση των ενεργειών έρευνας του μοντέλου σε επιμέρους βήματα, βοηθά στην καλύτερη κατανόηση του, τόσο από τους εξερευνητές που καλούνται να το εφαρμόσουν, όσο και από τους εκπαιδευτικούς, που διδάσκουν τη μεθοδολογία έρευνας του εγκλήματος.

---

[42] Βιδάλη Σ. (2001), **«Η ελληνική αστυνομία του 21ου αιώνα: ένα μεσογειακό μοντέλο αντεγκληματικής πολιτικής»**, Εκδόσεις Σάκκουλας.

4.6. Υπηρεσία Cisco κατά του Ηλεκτρονικού Εγκλήματος

Η υπηρεσία Cisco κατά του ηλεκτρονικού εγκλήματος, βρίσκεται στη Ρωσία. Το σύστημα έχει δημιουργήσει μια πρακτική επιχειρησιακού μάρκετινγκ παγιδευμένων ιστοχώρων με τους όρους που χρησιμοποιούνται χαρακτηριστικά ως λέξεις κλειδιά στις διάφορες μηχανές αναζήτησης Διαδικτύου έτσι ώστε οι συνδέσεις τους να παρουσιάζονται στα αποτελέσματα ερώτησης.[43]

Επειδή τόσοι πολλοί καταναλωτές τείνουν να εμπιστευθούν και να μην είναι ύποπτοι των ταξινομήσεων στις κύριες μηχανές αναζήτησης, μπορούν εύκολα να μεταφορτώσουν ένα από τα πλαστά πακέτα λογισμικού που υποθέτουν ότι είναι νόμιμο. Οι απατεώνες του διαδικτύου κυνηγούν επίσης το θήραμα γρήγορα προσεγγίζοντας μεγάλο πληθυσμό των χρηστών κινητών τηλεφώνων με την αποστολή των μηνυμάτων κειμένων τεχνάσματος. Οι εγκληματίες έχουν πάρει στην αποστολή των γενικών μηνυμάτων κειμένων τους αριθμούς βασισμένους στους κώδικες περιοχής των τοπικών τραπεζών κατευθύνοντας τους ανθρώπους για να καλέσουν σε ένα κέντρο υπηρεσιών σε μια συγκεκριμένη διεύθυνση. Οι επισκέπτες συνδέονται με τα αυτοματοποιημένα συστήματα φωνής που, να αντιπροσωπεύουν τις τράπεζες, ζητούν από τους ανθρώπους να πληκτρολογήσουν τους προσωπικούς κωδικούς τους από λογαριασμούς και λοιπά προσωπικά στοιχεία και οποιαδήποτε άλλη προσωπική πληροφορία που μπορεί αργότερα να χρησιμοποιηθεί. Τα σε απευθείας σύνδεση κοινωνικά δίκτυα, σύμφωνα με τη Cisco, γίνονται όλο και πιο δημοφιλή για τους εγκληματίες cyber.

4.7. Υπηρεσίες αντιμετώπισηςτου Ηλεκτρονικού Εγκλήματος

Της παρακάτω πίνακες συνοψίζονται όλοι οι φορείς που δραστηριοποιούνται στην αντιμετώπιση του ηλεκτρονικού εγκλήματος μαζί με της της διευθύνσεις και ειδικές αρχές που υπάγονται σε αυτό. Παρουσιάζονται της τα πεδία δράσης της και οι ρόλοι που καλούνται να δραστηριοποιηθούν.

---

[43] Peterson P., (2009), **«Cyber crime lords using big business tactics: Cisco»,** ανακτήθηκε από http://www.physorg.com

Φορέας	Ειδικές Αρχές / Διευθύνσεις Ασφάλειας	Πεδίο δράσης	Ρόλοι						
			Ρυθμίσεις, κανονισμοί	Έλεγχοι εφαρμογής θεσμικού πλαισίου	Computer Forensics	Πιστοποίηση προϊόντων & υπηρεσιών ασφαλείας	Παροχή Προϊόντων Υποδομών Ασφάλειας	Συμβουλευτικές Υπηρεσίες Ασφάλειας	Εκπαίδευση σε θέματα ασφαλείας
ΓΕΕΘΑ - Εθνική Αρχή Ασφάλειας	Διεύθυνση Πληροφορικής/Τμήμα Ασφάλειας Συστημάτων Πληροφορικής Διεύθυνση Επικοινωνιών / Τμήμα Ασφάλειας Επικοινωνιών Διεύθυνση Επικοινωνιών/Τμήμα Ηλεκτρονικού Πολέμου Διεύθυνση Κυβερνοάμυνας	1) Αποτελεί την Εθνική Αρχή Ασφάλειας 2) Έκδοση του Εθνικού Κανονισμού Ασφαλείας (ΕΚΑ) (σε συνεργασία με την ΕΥΠ): Αφορά στην ασφάλεια των ηλεκτρονικά επεξεργασμένων, διαβαθμισμένων, εθνικά ευαίσθητων πληροφοριών και εφαρμόζεται σε όλους τους δημόσιους φορείς. 3) Το ΔΠΛΗ/Τμήμα Ασφάλειας Συστημάτων Πληροφορικής υλοποιεί το Κέντρο Συντονισμού Αντιμετώπισης Περιστατικών Ασφαλείας (CIRC). 4) Το ΔΕΠ/Τμήμα Ασφάλειας Επικοινωνιών είναι ο τεχνικός σύμβουλος της Εθνικής Αρχής Πιστοποίησης Ασφάλειας.	✓		✓				
ΕΥΠ	Αρχή Ασφάλειας Πληροφοριών (INFOSEC) (Τεχνικής φύσεως) Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (Εθνικό CERT)	1) Ασφάλεια Εθνικών Επικοινωνιών-Πληροφορικής (σύνταξη κανονισμών, πιστοποίηση συστημάτων) 2) Πρόληψη και Αντιμετώπιση Ηλεκτρονικών Επιθέσεων. 3) Συντάξη, με βάση τις πληροφορίες που διαθέτει, πληροφοριακών δελτίων, μελετών και εκθέσεων τις οποίες και διαβιβάζει στις κατά περίπτωση αρμόδιες αρχές. 4) Συμμετοχή στη σύνταξη του ΕΚΑ. Συγκεκριμένα είναι επιφορτισμένη με το τεχνικό μέρος του κανονισμού. 5) Έλεγχος της τήρησης του τεχνικού μέρους του ΕΚΑ από ΔΔ. 6) Συντονίζει, στο πλαίσιο των αποφάσεων του ΚΥ.Σ.Ε.Α., τη δράση των υπηρεσιών πληροφοριών και ασφάλειας της Χώρας στον τομέα συλλογής και διάθεσης των πληροφοριών, που έχουν σχέση με το αντικείμενο της αποστολής της. Παράλληλα, συνεργάζεται και ενημερώνει τη Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (Δ.Δ.Σ.Π.) και τις υπηρεσίες πληροφοριών των Επιτελείων που εποπτεύονται από αυτήν, για θέματα της αρμοδιότητάς τους.	✓	✓		✓		✓	

Φορέας	Ειδικές Αρχές / Διευθύνσεις Ασφάλειας	Πεδίο δράσης	Ρόλοι						
			Ρυθμίσεις, κανονισμοί	Έλεγχοι εφαρμογής θεσμικού πλαισίου	Computer Forensics	Πιστοποίηση προϊόντων & υπηρεσιών ασφαλείας	Παροχή Προϊόντων Υποδομών Ασφάλειας	Συμβουλευτικές Υπηρεσίες Ασφάλειας	Εκπαίδευση σε θέματα ασφαλείας
ΕΛΑΣ	Διεύθυνση Εγκληματολογικών Ερευνών – Τμημα εξέτασης ψηφιακών πειστηρίων	1) Εξέταση ψηφιακών πειστηρίων. 2) Παρέχει υποστήριξη στις διωκτικές Αρχές της χώρας.		✓	✓			✓	
	Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος	1) Διενέργεια προανακριτικών έλεγχων που αφορούν το ηλεκτρονικό έγκλημα.							
Υπουργείο Μεταφορών και Επικοινωνιών	Γενική Γραμματεία Επικοινωνιών (ΓΓΕ)	1) Αποτελεί την Αρχή Τηλεπικοινωνιών. 2) Χάραξη Πολιτικής Ασφάλειας (Εθνική Στρατηγική Ασφάλειας). 3) Έκδοση του Εθνικού σχεδίου αριθμοδότητσης (Ε.Σ.Α.). 4) Η Διεύθυνση Πιστοποίησης της Γενικής Γραμματείας Επικοινωνιών του ΥΜΕ έχει αρμοδιότητες για τα θέματα εναρμόνισης της οδηγίας RTTE στη χώρα μας. (Οδηγία 99/5/ΕΚ) 5) Υλοποίηση Πολιτικής για την Ασφάλεια Δημοσίων Δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών.	✓			✓			
	ΓΓΕ(Γενική Γραμματεία Επικοινωνιών)/Διεύθυνση Πιστοποίησης (Τμήμα Τυποποίησης και Πιστοποίησης)								
Τράπεζα Ελλάδος	Διεύθυνση Εποπτείας Πιστωτικού Συστήματος	1) Έκδοση συγκεκριμένων αρχών / κανονισμών ασφάλειας 2) Έλεγχος εφαρμογής των παραπάνω κανονισμών 3) Αξιολόγηση συστημάτων εσωτερικού ελέγχου	✓	✓					
Υπουργείο Εσωτερικών	Δ/νση Πολιτικής Σχεδίασης Έκτακτης Ανάγκης	1) Προπαρασκευή και ετοιμότητα των υπηρεσιών με σκοπό την ομαλή μετάπτωση από ειρηνική περίοδο σε πολεμική. 2) Σχέδια επικινδυνότητας / επιχειρησιακής συνέχειας	✓	✓				✓	
	ΓΓΔΔ&ΗΔ (Γενική Γραμματεία Δημόσιας Διοίκησης και Ηλεκτρονικής Διακυβέρνησης)/Υπηρεσία Ανάπτυξης Πληροφορικής	1) Αρχή Πιστοποίησης Ελληνικού Δημοσίου – ΑΠΕΔ. 2) Διαθεσιμότητα πληροφοριών στη ΔΔ/Σχέδια ανάκαμψης καταστροφών. 3) Καθορισμός Πλαισίου Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης • Ανάπτυξη διαδικτυακών τόπων και συστημάτων ΔΔ όπως επίσης και υπηρεσιών της ΔΔ. • Διασφάλιση Διαλειτουργικότητας των ΠΣ της ΔΔ.	✓	✓		✓	✓	✓	

Φορέας	Ειδικές Αρχές / Διευθύνσεις Ασφάλειας	Πεδίο δράσης	Ρόλοι						
			Ρυθμίσεις, κανονισμοί	Έλεγχοι εφαρμογής θεσμικού πλαισίου	Computer Forensics	Πιστοποίηση προϊόντων & υπηρεσιών ασφαλείας	Παροχή Προϊόντων Υποδομών Ασφάλειας	Συμβουλευ-τικές Υπηρεσίες Ασφάλειας	Εκπαίδευση σε θέματα ασφαλείας
Υπουργείο Οικονομικών	ΓΓΠΣ (Γενική Γραμματεία Πληροφοριακών Συστημάτων)/Γραφείο Ασφάλειας Πληροφοριακών Συστημάτων και Προστασίας Δεδομένων & Υποδομών	1) Σύνταξη προτύπων σχεδιασμού, ανάπτυξης και λειτουργίας πληροφοριακού συστήματος ασφάλειας και ποιοτικού ελέγχου (Στα ΠΣ του ΥΠΟΙΟ?). 2) Έλεγχος και διερεύνηση των επεισοδίων ασφάλειας στις ηλεκτρονικές υπηρεσίες της ΓΓΠΣ. 3) Έλεγχος ΠΣ για αξιολόγηση του βαθμού ασφάλειας. 4) Εκπαίδευση προσωπικού σε θέματα ασφάλειας ΠΣ.		✓		✓			✓
ΑΠΔΠΧ	Ανεξάρτητη Αρχή	1) Προστασία προσωπικών δεδομένων 2) Αρχείο Γνωστοποιήσεων – Έκδοση Αδειών 3) Διενέργεια Διοικητικών Ελέγχων 4) Εξέταση προσφυγών / καταγγελιών / ερωτημάτων 5) Έκδοση οδηγιών και κανονιστικών πράξεων 6) Απευθύνει συστάσεις και υποδείξεις	✓	✓				✓	
ΑΔΑΕ	Ανεξάρτητη Αρχή	1) Προστασία απορρήτου επικοινωνιών 2) Διενέργεια τακτικών και έκτακτων ελέγχων 3) Έκδοση κανονιτικών πράξεων 4) Γνωμοδοοτεί και απευθύνει συστάσεις 5) Εξέταση καταγγελιών 6) Προβαίνει σε κατάσχεση μέσων παραβίασης του απορρήτου.	✓	✓				✓	
ΕΕΤΤ	Ανεξάρτητη Αρχή	1) Αποτελεί την Εθνική Ρυθμιστική Αρχή Επικοινωνιών 2) Ρύθμιση θεμάτων τηλεπικοινωνιών 3) Υπεύθυνη αρχή για την εφαρμογή της Οδηγίας RTTE	✓	✓					
GRNET CERT		1) Προϊόντα και Υπηρεσίες ασφάλειας συστημάτων 2) Πληροφόρηση στους χρήστες του ΕΔΕΤ σε θέματα ασφάλειας. 3) Εκπαίδευση χρηστών σεθέματα ασφαλείας υπολογιστών και διαφύλαξης προσωπικού απορρήτου.					✓	✓	✓
ENISA		1) Παροχή συμβουλών και υποστήριξης στην ΕΕ και στα ΚΜ για την ασφάλεια πληροφοριών. 2) Συλλογή και ανάλυση δεδομένων σχετικά με περιστατικά ασφάλειας στη Ευρώπη. 3) Προώθηση μεθόδων αποτίμησης και διαχείρισης ρίσκου για τη βελτίωση της αντιμετώπισης απειλών σε θέματα ασφάλειας.						✓	

4.8. Αναφορές 4ου κεφαλαίου

1. Peterson P., (2009), ***«Cyber crime lords using big business tactics: Cisco»,*** ανακτήθηκε από http://www.physorg.com
2. Βιδάλη Σ. (2001), ***«Η ελληνική αστυνομία του 21ου αιώνα: ένα μεσογειακό μοντέλο αντεγκληματικής πολιτικής»***, Εκδόσεις Σάκκουλας.
3. Γκόρτσος Β.Χ., (2008), ***«Πρόληψη και αντιμετώπιση της απάτης στα ηλεκτρονικά μέσα και συστήματα πληρωμών»***, Επιστημονική Ημερίδα ΕΕΤ
4. Πανούσης Γ., Βιδάλη Σ. (2001) ***«Κείμενα για την αστυνομία και την αστυνόμευση»***, Εκδόσεις Σάκκουλας.
5. Παπαθεοδώρου Θ. (2002), ***«Δημόσια ασφάλεια και αντεγκληματική πολιτική. Συγκριτική Προσέγγιση»***, Νομική Βιβλιοθήκη.

ΚΕΦΑΛΑΙΟ 5. Ερευνητικό Μέρος

Οι διοικητικοί και πληροφοριακοί μηχανισμοί αντιμετώπισης του ηλεκτρονικού εγκλήματος, που παρουσιάζονται στην παρούσα πτυχιακή εργασία, οι οποίοι ολοκληρώνονται με την ανάπτυξη ενός ολοκληρωμένου πληροφοριακού συστήματος, συμβάλλουν στην αντιμετώπιση συμβάντων ηλεκτρονικού εγκλήματος.

Η υλοποίηση ενός ολοκληρωμένου πληροφοριακού συστήματος, για το οποίο κύριος του έργου μπορεί να είναι η Δίωξη Ηλεκτρονικού Εγκλήματος που υπάγεται στην Ελληνική Αστυνομία, σύμφωνα με τα αναφερόμενα στην παρούσα εργασία, θα συμβάλλει στην καλύτερη αντιμετώπιση υποθέσεων που χαρακτηρίζονται ως ηλεκτρονικά εγκλήματα.

Ειδικότερα για θέματα που άπτονται εγκλημάτων που αφορούν την Δημόσια Διοίκηση, θα μπορούν στο ολοκληρωμένο πληροφοριακό σύστημα να έχουν πρόσβαση εξουσιοδοτημένοι υπάλληλοι – υπεύθυνοι ασφαλείας των δημοσίων φορέων, οι οποίοι θα μπορούν να αναφέρουν περιστατικά προς διερεύνηση, με ηλεκτρονικό τρόπο, αλλά και να καταχωρούν αποδεικτικά στοιχεία, γρήγορα και χωρίς να υπάρχει χρονική καθυστέρηση.

Η υλοποίηση του ολοκληρωμένου πληροφοριακού συστήματος, δίνει την δυνατότητα δημιουργίας ενός δικτύου ειδικών, οι οποίοι θα ενημερώνονται άμεσα για θέματα που αφορούν ηλεκτρονικά εγκληματικά συμβάντα (π.χ ηλεκτρονικές επιθέσεις). Η δημιουργία μια βάσης η οποία θα περιέχει τέτοιου είδους πληροφορίες θα είναι σημαντική για την καλύτερη λειτουργία του δημοσίου.

Επιπλέον, η ενημέρωση των ενδιαφερομένων για την υπόθεσή τους μπορεί να είναι πιο άμεση, εφόσον στο πληροφοριακό σύστημα καταχωρείται η πληροφορία που αφορά την υπόθεσή τους. Η δημιουργία ενός μηχανισμού αυτόματης ενημέρωσής τους μέσω ηλεκτρονικού ταχυδρομείου, μόλις καταχωρείται οτιδήποτε αφορά την υπόθεση του, συμβάλλει στην εξάλειψη της γραφειοκρατίας.

Η εγκατάσταση και η λειτουργία ενός τέτοιου πληροφοριακού συστήματος, στο οποίο θα έχουν πρόσβαση χρήστες – δημόσιοι φορείς, θα προβλέπει την πρόσβασή του μόνο εντός του Δικτύου Δημοσίου Τομέα. Η περιμετρική ασφάλεια που προσφέρει το Δίκτυο του Δημοσίου Τομέα, αυξάνει σημαντικά την ασφαλή πρόσβαση σε ένα τέτοιο πληροφοριακό σύστημα, από τους χρήστες και μειώνει σημαντικά την πιθανότητα πρόσβασης σε αυτό χρηστών που δεν πρέπει να έχουν πρόσβαση.

Επίλογος

Η μορφή του εγκλήματος, όπως την γνωρίζουμε ως σήμερα, συνεχώς μεταβάλλεται. Οι νέες τεχνολογίες, αλλάζουν τους τρόπους και τα μέσα τέλεσης συμβατικών εγκλημάτων, ενώ νέες μορφές, αμιγώς ηλεκτρονικών εγκλημάτων, κάνουν την εμφάνισή τους.

Ως αποτέλεσμα, το έργο των διωκτικών αρχών, η νομοθεσία και γενικά όλοι οι τομείς που επηρεάζουν την μεθοδολογία διερεύνησης των εγκλημάτων και το σύστημα απονομής δικαιοσύνη σε κάθε χώρα, μεταβάλλονται.

Οι σύγχρονες τεχνολογίες, επέφεραν σημαντικές αλλαγές σε κάθε μορφή εγκληματικής συμπεριφοράς, που ως σήμερα χαρακτηριζόταν συμβατική.

Η εισχώρηση της τεχνολογίας στις καθημερινές δραστηριότητες του σύγχρονου ανθρώπου, η διείσδυση και χρήση ηλεκτρονικών συσκευών από το σύνολο του πληθυσμού, οδηγούν σε μια μάλλον υβριδική μορφή εγκλημάτων, όπου σε κάθε συμβατικό έγκλημα οι τεχνολογικά εξελιγμένες συσκευές, διαδραματίζουν κυρίαρχο ρόλο, χρησιμοποιούνται βοηθητικά ή αποτελούν φορείς σημαντικών αποδείξεων σε ψηφιακή μορφή.

Οι σύγχρονες εγκληματικές απειλές κινούνται σε δύο διαφορετικές διαστάσεις: Αφενός, προβάλλουν τα γνήσια εγκλήματα του κυβερνοχώρου, που δεν υπήρχαν πριν την εμφάνιση των ηλεκτρονικών υπολογιστών και του Διαδικτύου.

Κύρια χαρακτηριστικά αυτών, είναι η χρησιμοποίηση τεχνολογικά εξελιγμένων συσκευών και υψηλής τεχνογνωσίας. Αφετέρου, τα γνωστά συμβατικά εγκλήματα αποκτούν μια περισσότερο υβριδική μορφή, όπου οι νέες τεχνολογίες διαδραματίζουν σημαντικό ρόλο.

Για αντιμετώπιση των απειλών αυτών, κάθε οργανισμός πρέπει να μεριμνήσει για την πρόληψη εκδήλωσης των επιθέσεων, την ανίχνευση των επιθέσεων και, τέλος, την αντίδραση προς αποκατάσταση της ζημιάς που προκλήθηκε από μια επίθεση.

Το τρίπτυχο αυτό της ασφάλειας, υπάγεται στην γενικότερη πολιτική ασφάλειας, που αποτελεί ένα συνδυασμό τεχνολογικών μέτρων αλλά και συνεχούς εκπαίδευσης και επιμόρφωσης του προσωπικού, σε θέματα ασφάλειας.

Στο νέο αυτό περιβάλλον, οι διωκτικές αρχές καλούνται, επίσης, να αντιμετωπίσουν το έγκλημα κινούμενες προς δύο κατευθύνσεις:

(α) Να εκσυγχρονίσουν και να εκπαιδεύσουν τις υφισταμένες υπηρεσίες δίωξης ηλεκτρονικού εγκλήματος και τα εργαστήρια εξέτασης ψηφιακών τεκμηρίων στις υψηλές τεχνολογίες και

(β) να εκπαιδεύσουν το προσωπικό των υπηρεσιών στην μεθοδολογία διερεύνησης εγκλημάτων στα οποία συμμετέχει καθ' οποιονδήποτε τρόπο η ψηφιακή τεχνολογία. Το υβριδικό μοντέλο ερευνών που προτάθηκε έχει σκοπό να αντιμετωπίσει τη νέα υβριδική μορφή του εγκλήματος, στην οποία η ψηφιακή τεχνολογία αποτελεί αναπόσπαστο κομμάτι της.

ΠΑΡΑΡΤΗΜΑ Νομοθεσία & οργανισμοί σχετικά με το έγκλημα

Άρθρο 348Α. Πορνογραφία ανηλίκων

1. Όποιος από κερδοσκοπία παρασκευάζει, κατέχει, προμηθεύεται, αγοράζει, μεταφέρει, διακινεί, διαθέτει, πωλεί ή θέτει με οποιονδήποτε τρόπο σε κυκλοφορία πορνογραφικό υλικό τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή δέκα χιλιάδων έως εκατό χιλιάδων ευρώ.

2. Πορνογραφικό υλικό κατά την έννοια της προηγούμενης παραγράφου συνιστά κάθε περιγραφή ή πραγματική ή εικονική αποτύπωση, σε οποιονδήποτε υλικό φορέα, του σώματος ανηλίκου που αποσκοπεί στη γενετήσια διέγερση, καθώς και η καταγραφή ή αποτύπωση, σε οποιονδήποτε υλικό φορέα, πραγματικής, προσποιητής ή εικονικής ασελγούς πράξης που ενεργείται για τον ίδιο σκοπό από ή με ανήλικο.

3.Αν κάποια από τις πράξεις της πρώτης παραγράφου αφορά πορνογραφικό υλικό που συνδέεται με την εκμετάλλευση της ανάγκης, της πνευματικής αδυναμίας, της κουφότητας ή της απειρίας ανηλίκου ή με την άσκηση σωματικής βίας κατ' αυτού, επιβάλλεται κάθειρξη μέχρι δέκα ετών και χρηματική ποινή πενήντα χιλιάδων έως εκατό χιλιάδων ευρώ και αν η πράξη είχε ως αποτέλεσμα τη βαριά σωματική βλάβη του παθόντος, επιβάλλεται κάθειρξη τουλάχιστον δέκα ετών και χρηματική ποινή εκατό χιλιάδων έως πεντακοσίων χιλιάδων ευρώ.

Άρθρο 370Α. Παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας

1. Όποιος αθέμιτα παγιδεύει ή με οποιονδήποτε άλλον τρόπο παρεμβαίνει σε τηλεφωνική σύνδεση ή συσκευή με σκοπό να πληροφορηθεί ή να μαγνητοφωνήσει το περιεχόμενο τηλεφωνικής συνδιάλεξης μεταξύ τρίτων τιμωρείται με φυλάκιση τουλάχιστον ενός έτους. Η χρησιμοποίηση από τον δράστη των πληροφοριών ή μαγνητοταινιών που αποκτήθηκαν με αυτόν τον τρόπο θεωρείται επιβαρυντική περίπτωση.

2. Όποιος αθέμιτα παρακολουθεί με ειδικά τεχνικά μέσα ή μαγνητοφωνεί προφορική συνομιλία μεταξύ τρίτων που δεν διεξάγεται δημόσια ή μαγνητοσκοπεί μη δημόσιες πράξεις τρίτων, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους. Με την ίδια ποινή τιμωρείται και όποιος μαγνητοφωνεί ιδιωτική συνομιλία μεταξύ αυτού και τρίτου χωρίς τη συναίνεση του τελευταίου. Το δεύτερο εδάφιο της παραγράφου 1 αυτού του άρθρου εφαρμόζεται και σε αυτή την περίπτωση.

3. Με φυλάκιση τουλάχιστον ενός έτους τιμωρείται όποιος κάνει χρήση των πληροφοριών ή των μαγνητοταινιών ή των μαγνητοσκοπήσεων που αποκτήθηκαν με τους οποίους που προβλέπονται στις παραγράφους 1 και 2 αυτού του άρθρου,

4. Η πράξη της παραγράφου 3 δεν είναι άδικη, αν η χρήση έγινε ενώπιον οποιασδήποτε δικαστικής ή άλλης ανακριτικής αρχής για τη διαφύλαξη δικαιολογημένου συμφέροντος, που δεν μπορούσε να διαφυλαχθεί διαφορετικά.

5. Αν ο δράστης των πράξεων των παραγράφων 1, 2 και 3 αυτού του άρθρου ενεργεί ιδιωτικές έρευνες ή τελεί τις πράξεις αυτές κατ' επάγγελμα ή κατά συνήθεια ή απέβλεπε στην είσπραξη αμοιβής, επιβάλλεται φυλάκιση τουλάχιστον 2 ετών και χρηματική ποινή.

6. Όποιος διαθέτει στο εμπόριο ή με άλλον τρόπο προσφέρει για εγκατάσταση ειδικά τεχνικά μέσα για την τέλεση των πράξεων των παραγράφων 1 και 2 αυτού του άρθρου η δημόσια διαφημίζει ή προσφέρει τις υπηρεσίες του για την τέλεση τους, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και με χρηματική ποινή.

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

Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον 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 να λάβουν γνώση τους. 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 την παράγραφο 1 πράξη τιμωρείται κατά τα άρθρα 146 και 147.

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

1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μήνες και με χρηματική ποινή εκατό χιλιάδων έως δύο εκατομμυρίων δραχμών [διακοσίων ενενήντα (290,00) έως πέντε χιλιάδων εννιακοσίων (5.900) ευρώ].

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

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

Οι πράξεις, των παραγράφων 1 έως 3 διώκονται ύστερα έγκληση.

Άρθρο 386. Απάτη

Όποιος με σκοπό να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος βλάπτει ξένη περιουσία πείθοντας κάποιον σε πράξη, παράλειψη ή ανοχή με την εν γνώσει παράσταση ψευδών γεγονότων σαν αληθινών ή την αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών και αν η ζημία που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον δύο ετών. Οι διατάξεις του άρθρου 72 για το κατάστημα εργασίας εφαρμόζονται και εδώ. Επιβάλλεται κάθειρξη μέχρι δέκα ετών: α) αν ο υπαίτιος διαπράττει απάτες κατ' επάγγελμα ή κατά συνήθεια και το συνολικό όφελος ή η συνολική ζημία υπερβαίνουν το ποσό των πέντε εκατομμυρίων (5.000.000) δραχμών [δέκα πέντε χιλιάδων (15.000) ευρώ. Βλ. διατάξεις και τρόπο μετατροπής σε ευρώ στο άρθρο α] « ή β) αν το περιουσιακό όφελος ή η προξενηθείσα ζημία υπερβαίνει συνολικά το ποσό των είκοσι πέντε εκατομμυρίων (25.000.000) δραχμών».[εβδομήντα τριών χιλιάδων (73.000)ευρώ.] ».

Άρθρο 386^{Α}. Απάτη με υπολογιστή

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 άλλο τρόπο, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημίας είναι αδιάφορο αν παθόντες είναι ένα ή περισσότερα πρόσωπα.

ΝΟΜΟΙ

- Ν. 2225/1994 - «Προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας»
- Ν. 2472/1997 - «Για την προστασία των προσωπικών δεδομένων στο Διαδίκτυο»
- Ν**.** 2774/1999 - «Για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα»
- Ν. 2867/2000 - «Οργάνωση και Λειτουργία του τομέα των Τηλεπικοινωνιών»
- **Ν.** 2819/2000 - «Προσθήκη στο Ν. 2121/1993 περί νομικής προστασίας βάσεων δεδομένων»
- Ν. 2225/1994 όπως τροπ. με Ν. 311/2003 - «Για την προστασία της ελευθέριας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις»
- Ν. 3431/2006 - «Περί ηλεκτρονικών επικοινωνιών».

ΠΡΟΕΔΡΙΚΟ ΔΙΑΤΑΓΜΑ

- Π.Δ. 131/2003 - «Ηλεκτρονικό εμπόριο κλπ Υπηρεσίες της Κοινωνίας της Πληροφορίας»
- Π.Δ. 150/2001 - «Ηλεκτρονικές Υπογραφές»
- Π.Δ. 47/2005 - «Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και τη διασφάλιση του»

ΟΔΗΓΙΕΣ ΕΥΡΩΠΑΪΚΗΣ ΈΝΩΣΗΣ

- Οδηγία 87/102/ΕΟΚ του Συμβουλίου της22ας Δεκεμβρίου 1986 για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη.
- Οδηγία 90/88/ΕΟΚ του Συμβουλίου της 22ας Φεβρουαρίου 1990 για την τροποποίηση της οδηγίας 87/102/ΕΟΚ για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη.
- Οδηγία 90/387/ΕΟΚ του Συμβουλίου της 28ης Ιουνίου 1990 για τη δημιουργία της εσωτερικής αγοράς στον τομέα των τηλεπικοινωνιακών υπηρεσιών μέσω της εφαρμογής της παροχής ανοικτού δικτύου (Open Networt Provision ONP).
- Οδηγία 90/388/ΕΟΚ της Επιτροπής της 28ης Ιουνίου 1990 σχετικά με τον ανταγωνισμό στις αγορές των τηλεπικοινωνιακών υπηρεσιών.
- Οδηγία 91/250/ΕΟΚ του Συμβουλίου της 14ης Μαΐου 1991 για τη νομική προστασία των προγραμμάτων ηλεκτρονικών υπολογιστών

- Οδηγία 96/9/ΕΟΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαρτίου 1996, σχετικά με τη νομική προστασία των βάσεων δεδομένων.
- Οδηγία 97/7/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Μαΐου 1997 για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις.
- Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 1999, σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.
- Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά («οδηγία για το ηλεκτρονικό εμπόριο»).
- Οδηγία 2002/19/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με την πρόσβαση σε δίκτυα ηλεκτρονικών επικοινωνιών και συναφείς ευκολίες, καθώς και με τη διασύνδεση τους (οδηγία για την πρόσβαση).
- Οδηγία 2002/20/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, για την αδειοδότηση δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών (οδηγία για την αδειοδότηση).
- Οδηγία 2002/21/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (οδηγία πλαίσιο).
- Οδηγία 2002/22/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (οδηγία καθολικής υπηρεσίας).
- Οδηγία 2002/58/ΕΚτου Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες).
- Οδηγία 2002/77/ΕΚ της Επιτροπής, της 16ης Σεπτεμβρίου 2002, σχετικά με τον ανταγωνισμό στις αγορές δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών.

ΔΙΕΘΝΕΙΣ ΣΥΜΒΑΣΕΙΣ

- Συνθήκη των Βρυξελλών (1968) περί προσδιορισμού της δικαιοδοσίας
- Σύμβαση για τον Κυβερνοχώρο - Βουδαπέστη 23-11-2001

- Η Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου του Ο.Η.Ε. της 10-12-1948
- Η Σύμβαση της Ρώμης «για την προάσπιση των δικαιωμάτων του ανθρώπου και των θεμελιωδών ελευθεριών» της 4-11-1950 (ΕΣΔΑ)

ΟΡΓΑΝΙΣΜΟΙ ΓΙΑ ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΈΓΚΛΗΜΑ

- **Computer Crime Research Center:** Κέντρο ερευνών σχετικά με το ηλεκτρονικό έγκλημα. Το υλικό που φιλοξενείται στις σελίδες του είναι ιδιαίτερα σημαντικό και προσεγγίζει το σύνολο των θεμάτων για το έγκλημα στον κυβερνοχώρο. (hhttp://www.crime-research.org/)
- **High Tech Criminal Investigators Association:** Διεθνής οργανισμός που βασίζεται στην εθελοντική συμμετοχή για την ανταλλαγή πληροφοριών, τεχνογνωσίας και ιδεών, σχετικά με το έγκλημα υψηλής τεχνολογίας. (http://ww.htcia.org)

ΜΟΡΦΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

- **Anti-Phishing Working Group:** Διεθνής οργανισμός που στοχεύει στην αντιμετώπιση της απάτης που διαπράττονται με τις τεχνικές phising, spamming email, spoofing. (http://www.antiphishing.org/)
- **Identity Therf/Federal Trade Commission:** Δικτυακός τόπος που ασχολείται με την προστασία των καταναλωτών. (http://www.consumer.gov)
- **National Child Exploitation Coordination Center:** Ερευνητικό κέντρο στον Καναδά που αποσκοπεί στην αντιμετώπιση της σεξουαλικής εκμετάλλευσης των παιδιών μέσω του Διαδικτύου. (http://necc.ca/)

ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

- **CERT@Coordination Center:** Από τους πιο σημαντικούς οργανισμούς σχετικά με την ασφάλεια υπολογιστών και δικτύων.(http://www.cert.org/)

ΝΟΜΟΘΕΣΙΑ

- **Computer Crime Laws by State:** Κατάλογος νομοθεσίας που είναι σε ισχύ σε πολιτείες των Η.Π.Α. (nsi.org/Library/Compsec/computerlaw/statelaws.html)
- **Find Law Cubercrime Links:** Δικτυακή πύλη με συνδέσεις που παραπέμπουν σε νομοθετικά ζητήματα. (http://cuber.lp.findlaw.com/criminal/)

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Email Generator Platinum, (2007), **«Εμπορικό λογισμικό»,** ανακτήθηκε από http://www.email-business.com/index_en.htm
2. Filedudes, (2010), **«Λογισμικό τύπου harvester»,** ανακτήθηκε από http://www.programurl.com/software/harvester.htm
3. Forester T., Morrison P., (1994). **«Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing»,** Massachousetts Institute of Technology
4. Frey D. (2003). **«An Analysis of Cybercrime: Past, present and future»**, Buffalo University's Publications.
5. Goodman M., Brenner S., (2002). **«The Emerging Consensus on Criminal Conduct in Cyberspace»**. UCLA Journal and Technology.
6. Lipton. J., (2007), **«Beyond Cybersquatting Taking Domain Name Disputes past Trademark Policy»,** ανακτήθηκε από http://www.law.wfu.edu/prebuilt/w08-lipton.pdf
7. Newman, R. (2004). **«Identity Theft»**. United States Department of Justice.
8. Peterson P., (2009), **«Cyber crime lords using big business tactics: Cisco»,** ανακτήθηκε από http://www.physorg.com
9. Sinrod E., Reilly W., (2000). **«Cyber-crimes: A Practical approach to the application of Federal Computer Laws»**. Santa Clara Computer and high technology law journal.
10. United Nations (1995), **«International Review on Criminal Policy-United Nations Manual on the prevention and control of Computer Related crime»**, United Nations
11. Whatprice (2012), **«Εργαλεία λογισμικού που δημιουργούν αυτόματα τυχαίους αριθμούς πιστωτικών καρτών και επιβεβαιώνουν την γνησιότητα τους»**, ανακτήθηκε από http://www.whatprice.co.uk/financial.html
12. Wikipedia, (2007), **«Spam»**, ανακτήθηκε από http://el.wikipedia.org/wiki/Spam
13. Wikipedia, (2012), **«Κρυπτογραφία»**, ανακτήθηκε από http://el.wikipedia.org/wiki/Κρυπτογραφία
14. Βιδάλη Σ. (2001), **«Η ελληνική αστυνομία του 21ου αιώνα: ένα μεσογειακό μοντέλο αντεγκληματικής πολιτικής»**, Εκδόσεις Σάκκουλας.

15. Γκόρτσος Β.Χ., (2008), **«Πρόληψη και αντιμετώπιση της απάτης στα ηλεκτρονικά μέσα και συστήματα πληρωμών»**, Ημερίδα Ελληνικής Ένωσης Τραπεζών

16. Δήμου Γ., (2002), **«Η διαχείριση υποθέσεων σεξουαλικής κακοποίησης ανηλίκων»**.

17. Ζάννη Α. (2005). **«Το διαδικτυακό έγκλημα»**, Εκδόσεις Σάκκουλα.

18. Πάγκαλος Γ., Μαυρίδης Ι. (2002). **«Ασφάλεια πληροφοριακών συστημάτων και δικτύων»**, Εκδόσεις Ανίκουλα.

19. Πανούσης Γ., Βιδάλη Σ. (2001) **«Κείμενα για την αστυνομία και την αστυνόμευση»**, Εκδόσεις Σάκκουλας.

20. Παπαθεοδώρου Θ. (2002), **«Δημόσια ασφάλεια και αντεγκληματική πολιτική. Συγκριτική Προσέγγιση»**, Νομική Βιβλιοθήκη.