Κεφάλαιο 13. Ιδιωτικότητα στο Διαδίκτυο και Κυβερνοέγκλημα

Σύνοψη
Η χρήση της Τεχνολογίας Πληροφοριών και Επικοινωνιών (ΤΠΕ) έχει αλλάξει ριζικά τον τρόπο με τον οποίο λειτουργεί η σύγχρονη κοινωνία. Όλες οι μορφές της ανθρώπινης δραστηριότητας έχουν επηρεαστεί από την υιοθέτηση των νέων τεχνολογικών εργαλείων και μέσων που προσφέρονται και οδηγούν στην επέκταση της ανθρώπινης συμπεριφοράς με νέες μορφές διάδρασης. Όμως, άλλοτε ο άνθρωπος χρησιμοποιεί την τεχνολογία για καλό σκοπό και άλλοτε για κακό σκοπό. Το σύνολο της παραβατικής ανθρώπινης συμπεριφοράς, το οποίο περιλαμβάνει σε κάποιο στάδιο χρήση τεχνολογικών εργαλείων και μέσων, ονομάζεται ηλεκτρονικό έγκλημα. Από την εκδήλωση των πρώτων φαινομένων ηλεκτρονικού εγκλήματος έχει ενεργοποιηθεί η παγκόσμια κοινότητα με στόχο να ανακόψει ή να αποτρέψει αυτού του είδους την παραβατική συμπεριφορά. Για το σκοπό αυτό, έχουν θεσπιστεί νομικά και κανονιστικά πλαίσια σε περιφερειακό ή εθνικό επίπεδο τα οποία εξετάζουν τους τρόπους ηλεκτρονικού εγκλήματος και οδηγούν στην επιβολή κυρώσεων στους παραβάτες.Τα πλαίσια αυτά βρίσκονται σε συμφωνία με τα αντίστοιχα Ευρωπαϊκά και διεθνή νομικά και κανονιστικά πλαίσια. Η εξέλιξη του ηλεκτρονικού εγκλήματος στο Διαδίκτυο, είναι γνωστή ως Κυβερνοέγκλημα.

Προαπαιτούμενη γνώση
Για την κατανόηση του παρόντος κεφαλαίου απαιτείται γνώση των βασικών εννοιών και ζητημάτων ασφάλειας (Κεφ. 1).

13.1 Εισαγωγή

Οι τεχνολογίες πληροφορίας και επικοινωνιών (ΤΠΕ) κατέστησαν δυνατή τη διάπραξη ενός μεγάλου αριθμού εγκληματικών πράξεων, οι οποίες προϋποθέτουν εξειδίκευση και τεχνολογική κατάρτιση. Ο όρος «Ηλεκτρονικό Έγκλημα» περιλαμβάνει όλες εκείνες τις αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση υπολογιστών και δικτύων επικοινωνίας. Οι πράξεις αυτές τιμωρούνται με συγκεκριμένες ποινές από την ελληνική και τη διεθνή νομοθεσία. Λόγω της πολυπλοκότητας των ΤΠΕ, αλλά και των πολλών διαφορετικών τεχνολογιών που εμπλέκονται, είναι δύσκολο να κατηγοριοποιήσουμε το ηλεκτρονικό έγκλημα σε σχέση με την τεχνολογία που χρησιμοποιείται. Συνηθίζεται, ωστόσο, μια κατηγοριοποίηση σε σχέση με τον τρόπο τέλεσης των παραβατικών πράξεων. Έτσι έχουμε εγκλήματα τα οποία διαπράττονται με τη χρήση υπολογιστών (computer crime) χωρίς τη χρήση του διαδικτύου και εγκλήματα τα οποία διαπράττονται μέσω διαδικτύου, τα οποία είναι γνωστότερα ως Κυβερνοεγκλήματα (cyber crimes). Επίσης, ανάλογα με το περιεχόμενο της επίθεσης, τα εγκλήματα διακρίνονται σε

- Εγκλήματα κατά της προσωπικότητας και της ιδιωτικότητας.
- Εγκλήματα κατά της περιουσίας.
- Διακίνηση παράνομου και αθέμιτου / επιβλαβούς περιεχομένου.

Η διαδικτύωση έδωσε ένα παγκόσμιο χαρακτήρα στο ηλεκτρονικό έγκλημα, το οποίο δεν θα μπορούσε σε καμία περίπτωση να αντιμετωπιστεί μόνο σε εθνικό ή τοπικό επίπεδο. Η ανάγκη σχηματισμού ενός κοινού μετώπου οδήγησε σε μια διακρατική συνεννόηση και στην εκπόνηση μιας αποτελεσματικής στρατηγικής. Το 2001, οι υπουργοί 26 ευρωπαϊκών κρατών, καθώς επίσης και 4 χωρών – παρατηρητών (Καναδάς, Ιαπωνία, Νότιος Αφρική και ΗΠΑ), υπέγραψαν τη Συνθήκη της Βουδαπέστης (Convention on Cybercrime). Η σύμβαση της Βουδαπέστης έχει ως σκοπό να εναρμονίσει τις εθνικές ποινικές νομοθεσίες των κρατών στον τομέα της εγκληματικότητας στον κυβερνοχώρο. Στη συνθήκη αυτή υπάρχουν επεξηγήσεις και ρυθμίσεις για όλες τις μορφές ηλεκτρονικού εγκλήματος, ενώ θεσπίζονται γρήγοροι και αποτελεσματικοί κανόνες στον τομέα της διεθνούς συνεργασίας.

Η οικονομία, η διοίκηση αλλά και γενικότερα η κοινωνία εξαρτάται από την αποτελεσματικότητα, την αξιοπιστία και την ασφάλεια των πληροφοριακών συστημάτων, και των δικτύων. Το γεγονός αυτό καθιστά την αντιμετώπιση του ηλεκτρονικού εγκλήματος μία καθημερινή μάχη. Σε διαφορετική περίπτωση, ο σύγχρονος άνθρωπος θα βρεθεί στο μέσο μιας κοινωνίας γεμάτης κινδύνους, όπου θα λείπει η εμπιστοσύνη, ενώ η τεχνολογία θα αποτελεί έναν ανασταλτικό παράγοντα για την κοινωνική ανάπτυξη.

Υπάρχουν διάφοροι τρόποι με τους οποίους είναι δυνατό να εμπλακούν οι ΤΠΕ στο ηλεκτρονικό έγκλημα. Μπορεί, δηλαδή, να αποτελούν στόχο ή εργαλείο του εγκλήματος. Ένας σημαντικός παράγοντας που αυξάνει τη συχνότητα των ηλεκτρονικών εγκλημάτων είναι η ανωνυμία. Η ανωνυμία ενθαρρύνει τον κακόβουλο χρήστη στο να προχωρήσει σε παραβατική συμπεριφορά χωρίς φόβο. Έχουν αναπτυχθεί αρκετοί μηχανισμοί ασφάλειας οι οποίοι μας επιτρέπουν να συλλέξουμε πληροφορίες για κάθε δικτυακό κόμβο, άρα και για κάθε κακόβουλο χρήστη. Ωστόσο, αυτή η προσέγγιση δίνει αποτελέσματα μόνον εφόσον αυτοί οι μηχανισμοί είναι έγκαιρα ενεργοποιημένοι, στο πλαίσιο μιας συντονισμένης προσπάθειας πρόληψης των εγκληματικών πράξεων.

Ταυτόχρονα, η Ηλεκτρονική Εγκληματολογία (Digital Forensics), όπως είδαμε στο κεφάλαιο 12, απαιτεί αρκετές εργατοώρες και τεχνογνωσία προκειμένου να διαλευκάνει ένα ηλεκτρονικό έγκλημα. Ακόμη όμως και αν συμβεί αυτό, οι σχετικές εργασίες δεν εκτελούνται σε πραγματικό χρόνο, οπότε υπάρχει πάντα το ενδεχόμενο ο εισβολέας / θύτης να έχει καλύψει αρκετά από τα ίχνη του.

Ο διασυνοριακός χαρακτήρας του ηλεκτρονικού εγκλήματος συνοδεύεται από ακόμη ένα χαρακτηριστικό το οποίο διαφοροποιεί το ηλεκτρονικό έγκλημα από το έγκλημα με την συμβατική του έννοια. Η γνώση και η τεχνική κατάρτιση που απαιτείται για τα ηλεκτρονικά εγκλήματα είναι αυξημένη, ωστόσο τα τελευταία χρόνια υπάρχει πληθώρα αυτοματοποιημένων εργαλείων, τα οποία δίνουν τη δυνατότητα ακόμη και σε ένα μέσο χρήστη ηλεκτρονικού υπολογιστή να πάρει μέρος σε μία παράνομη δραστηριότητα, εφόσον το επιθυμεί. Κάτι τέτοιο καθιστά δυνητικό εγκληματία κάθε άνθρωπο που διαθέτει υπολογιστή.

13.2 Νομικό Πλαίσιο

Το νομικό πλαίσιο και οι σχετικοί κανόνες μπορούν να κατηγοριοποιηθούν σε τέσσερις ενότητες, που αφορούν τα ακόλουθα:

- Προστασία της προσωπικότητας / ιδιωτικότητας.
- Καταστολή του οικονομικού ηλεκτρονικού εγκλήματος.
- Προστασία της πνευματικής ιδιοκτησίας.
- Προστασία από παράνομο και αθέμιτο περιεχόμενο.

Για να στοιχειοθετηθεί ένα ηλεκτρονικό έγκλημα απαιτείται καταρχήν μία περιγραφή της πράξης ή της παράλειψης που τελέστηκε η οποία συνιστά ποινικά κολάσιμη συμπεριφορά. Χρειάζεται να γνωρίζουμε τον χρόνο και τον τόπο τέλεσης, καθώς και τα εμπλεκόμενα πρόσωπα (π.χ. ποιος είναι ο θύτης και ποιος το θύμα).

Ο τόπος τέλεσης ενός ηλεκτρονικού εγκλήματος είναι ιδιαίτερα σημαντικός για να προσδιοριστεί το εφαρμοστέο δίκαιο και τα αρμόδια δικαστήρια. Στην περίπτωση κυβερνοεγκλήματος, υπάρχει διαχωρισμός του τόπου εκδήλωσης της αξιόποινης συμπεριφοράς και του τόπου επιβολής των αποτελεσμάτων της αξιόποινης συμπεριφοράς. Γίνεται φανερό ότι υπάρχει μια δυσχέρεια στον προσδιορισμό του τόπου, ειδικότερα στα κυβερνοεγκλήματα, καθώς κανείς μπορεί από κάθε τόπο να αποκτήσει πρόσβαση στα δεδομένα ενός υπολογιστή που είναι συνδεμένος στο Διαδίκτυο. Επίσης, τις περισσότερες φορές γίνεται χρήση διαφορετικών ενδιάμεσων σταθμών οι οποίοι μεσολαβούν μέχρι να τελεστεί η αξιόποινη πράξη, λόγω του ότι ένας υπολογιστής συνδέεται με κάποιον άλλο χρησιμοποιώντας αρκετούς ενδιάμεσους κόμβους του Διαδικτύου, με εναλλακτικές διαδρομές εφόσον χρειαστεί.

Η Ελληνική νομοθεσία διαθέτει αρκετές νομοθετικές ρυθμίσεις για θέματα ηλεκτρονικού εγκλήματος. Αποσπασματικά αναφέρονται οι Νόμοι 370 και 370^{A} του Ποινικού Κώδικα περί ποινικής προστασίας του απορρήτου, που μεταξύ άλλων αφορούν:

- Αθέμιτη εισχώρηση σε ξένα απόρρητα γραπτά (ανάγνωση – αντιγραφή – αποτύπωση με οποιοδήποτε τρόπο), που τιμωρείται με φυλάκιση μέχρι 1 έτος.

- Αθέμιτη παγίδευση ή παρέμβαση σε συσκευή, σύνδεση ή δίκτυο – υλικό – λογισμικό με σκοπό γνώση – αποτύπωση επικοινωνίας - δεδομένων κίνησης, που τιμωρείται με κάθειρξη μέχρι 10 έτη.

- Αθέμιτη παρακολούθηση με ειδικά τεχνικά μέσα – αποτύπωση συνομιλίας ή μη δημόσιας πράξης άλλου, που τιμωρείται με κάθειρξη μέχρι 10 έτη.

- Χρήση πληροφορίας/υλικού φορέα, που τιμωρείται με κάθειρξη μέχρι 10 έτη.

Επίσης, ο Νόμος 292^{A} μεταξύ άλλων αφορά:

- Χωρίς δικαίωμα πρόσβαση σε σύνδεση ή δίκτυο παροχής υπηρεσιών τηλεφωνίας, που τιμωρείται με φυλάκιση τουλάχιστον 1 έτους και χρηματική ποινή (20.000-50.000 ευρώ).

- Παραβίαση διάταξης Κανονισμού ΑΔΑΕ ή Γενικής Άδειας ΕΕΤΤ, που τιμωρείται με φυλάκιση τουλάχιστον 2 ετών και χρηματική ποινή (100.000 - 500.000 ευρώ).

- Παράλειψη αποτροπής παράνομης πρόσβασης, που τιμωρείται με φυλάκιση τουλάχιστον 2 ετών και χρηματική ποινή (20.000 - 50.000 ευρώ).

Στη συνέχεια, αναφέρονται Νόμοι της Ελληνικής Νομοθεσίας, Προεδρικά Διατάγματα και Άρθρα Ποινικού Κώδικα, που είναι σχετικά με το ηλεκτρονικό έγκλημα και το κυβερνοέγκλημα:

Ν.2225/1994	«Προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας»
Ν. 2246/1994	«Οργάνωση και λειτουργία του τομέα τηλεπικοινωνιών»
Ν.2472/1997	«Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα»
Ν. 2672/1998	«Διακίνηση εγγράφων με ηλεκτρονικά μέσα»
Ν.2774/1999	«Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα»
Ν.2867/2000	«Οργάνωση και λειτουργία των τηλεπικοινωνιών»
Ν .3115/2003	«Αρχή διασφάλισης του απορρήτου των επικοινωνιών»
Ν.3431/2006	«Περί ηλεκτρονικών επικοινωνιών»
Ν. 3471/2006	«Προστασία Δεδομένων Προσωπικού Χαρακτήρα»

Πίνακας 13.1 *Νόμοι για το ηλεκτρονικό έγκλημα.*

Π.Δ. 150/2001	«Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές».
Π.Δ. 342/2002	«Διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο»
Π.Δ. 131/2003	«Προσαρμογή στην Οδηγία 2000/31 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά»
Π.Δ.47/2005	«Διαδικασίες για την Άρση του Απορρήτου των Επικοινωνιών»

Πίνακας 13.2 *Προεδρικά Διατάγματα για το ηλεκτρονικό έγκλημα.*

Άρθρο 3 48Α ΠΚ	Πορνογραφία ανηλίκων
Άρθρο 370Α	Παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας
Άρθρο 370 Β	Παραβίαση στοιχείων ή προγραμμάτων υπολογιστών που θεωρούνται απόρρητα
Άρθρο 370Γ	Παράνομη αντιγραφή ή χρήση προγραμμάτων υπολογιστών και παράνομη πρόσβαση σε δεδομένα υπολογιστών
Άρθρο 386Α	Απάτη με υπολογιστή

Πίνακας 13.3 *Άρθρα Ποινικού Κώδικα για το ηλεκτρονικό έγκλημα.*

Οδηγία 87/102/ΕΟΚ	Προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη (τροποποιείται με την Οδηγία 90/88/ΕΟΚ).
Οδηγία 90/387/ΕΟΚ	Δημιουργία της εσωτερικής αγοράς στον τομέα των τηλεπικοινωνιακών υπηρεσιών μέσω της εφαρμογής της παροχής ανοικτού δικτύου (Open Network Provision - ONP).
Οδηγία 91/250/ΕΟΚ	Νομική προστασία των προγραμμάτων ηλεκτρονικών υπολογιστών
Οδηγία 96/9/ΕΟΚ	Νομική προστασία των βάσεων δεδομένων.
Οδηγία 97/7/ΕΚ	Προστασία των καταναλωτών κατά τις εξ' αποστάσεως συμβάσεις.
Οδηγία 1999/93/ΕΚ	Κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.
Οδηγία 2000/31/ΕΚ	Νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά
Οδηγία 2002/19/ΕΚ	Πρόσβαση σε δίκτυα ηλεκτρονικών επικοινωνιών και συναφείς ευκολίες, καθώς και με τη διασύνδεσή τους
Οδηγία 2002/20/ΕΚ	Αδειοδότηση δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών
Οδηγία 2002/21/ΕΚ	Κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών
Οδηγία 2002/22/ΕΚ	Καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών
Οδηγία 2002/58/ΕΚ	Επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών
Οδηγία 2002/77/ΕΚ	Ανταγωνισμός στις αγορές δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών.

Πίνακας 13.4 *Ευρωπαϊκή νομοθεσία για το ηλεκτρονικό έγκλημα.*

Ιδιαίτερο ρόλο στο Κυβερνοέγκλημα διαδραματίζουν οι πάροχοι υπηρεσιών Διαδικτύου, καθώς οι ίδιοι αποτελούν το όχημα πρόσβασης και περιήγησης των χρηστών σε αυτό. Όταν η υπηρεσία που παρέχει ένας πάροχος αφορά στην απλή μετάδοση δεδομένων ή ακόμη και στην αποθήκευση των δεδομένων για μικρό χρονικό διάστημα (caching), τότε ο πάροχος δεν φέρει ευθύνη για το περιεχόμενο των δεδομένων.

Η αυτόματη ενδιάμεση και προσωρινή αποθήκευση των δεδομένων πραγματοποιείται από την πλευρά των παρόχων για να καταστεί αποτελεσματικότερη η μεταγενέστερη μετάδοσή τους και απαλλάσσει τους παρόχους από κάθε ευθύνη. Ο πάροχος επίσης δεν πρέπει να τροποποιεί ή να παρεμβαίνει με οποιονδήποτε τρόπο στα διακινούμενα δεδομένα. Αν ο πάροχος αντιληφθεί ότι τα δεδομένα έχουν αποσυρθεί από το σημείο αφετηρίας της μετάδοσής τους (π.χ. ιστοσελίδα), τότε έχει την υποχρέωση να αποσύρει άμεσα ή να καταστήσει αδύνατη την πρόσβαση σε αυτά τα δεδομένα που αποθήκευσε. Για την υπηρεσία φιλοξενίας ιστοσελίδας ο πάροχος δεν φέρει καμία ευθύνη εφόσον δεν γνωρίζει πραγματικά το τυχόν παράνομο περιεχόμενο της δραστηριότητας ή της πληροφορίας.

13.3 Κατηγορίες Ηλεκτρονικού Εγκλήματος

Η κατηγοριοποίηση των ηλεκτρονικών εγκλημάτων ποικίλει σε μεγάλο βαθμό και εξαρτάται κυρίως από την οπτική με την οποία τη δημιουργεί κανείς. Ένας διαχωρισμός ο οποίος χρησιμοποιείται αρκετά προέρχεται από την Εξεταστική Επιτροπή της Μεγάλης Βρετανίας, ένα ανεξάρτητο σώμα το οποίο από την ίδρυση του, στις αρχές της δεκαετίας του 1980, διενήργησε έρευνες με στόχο να εξακριβώσει την έκταση του ηλεκτρονικού εγκλήματος σε δημόσιο και ιδιωτικό τομέα. Στις κατηγορίες αυτές, μεταξύ άλλων, συμπεριλαμβάνονται τα ακόλουθα:

- Απάτη: αλλοίωση δεδομένων για προσωπικό όφελος.
- Κλοπή: δεδομένων ή λογισμικού.
- Χρήση λογισμικού χωρίς άδεια (π.χ. παράνομα αντίγραφα λογισμικού).
- Μη εγκεκριμένη χρήση των δυνατοτήτων του υπολογιστή για ίδιον όφελος.
- Κακή χρήση προσωπικών δεδομένων.
- Hacking.
- Σαμποτάζ: πρόκληση ζημιάς σε λογισμικό ή υλικό.
- Εισαγωγή πορνογραφικού υλικού στο Διαδίκτυο.

Σε αυτές τις γενικές κατηγορίες ή σε άλλες παρόμοιες ανήκουν διάφορες εκφάνσεις του ηλεκτρονικού εγκλήματος οι οποίες χαρακτηρίζονται από τα ιδιαίτερα εργαλεία λογισμικού που χρησιμοποιούνται σε κάθε περίπτωση. Είναι βέβαιο ότι εφόσον η τεχνολογία υλικού συνεχίζει να αλλάζει, το ίδιο θα συμβαίνει και με τις μεθόδους που θα χρησιμοποιούν οι εγκληματίες του κυβερνοχώρου. Στη συνέχεια, παρουσιάζονται αναλυτικότερα οι συνηθέστερες κατηγορίες

13.3.1 Αλίευση

Η επίθεση αλίευσης (phishing attack), περιλαμβάνει εκείνες τις περιπτώσεις όπου ο θύτης χρησιμοποιεί συνδυασμό μηνυμάτων email και πλαστών ιστοσελίδων προκειμένου να παραπλανήσει τον ανυποψίαστο χρήστη. Είναι ιδιαίτερα συνηθισμένη η περίπτωση όπου ο ανυποψίαστος χρήστης δέχεται μήνυμα ηλεκτρονικής αλληλογραφίας το οποίο εμφανίζεται μεταμφιεσμένο ώστε να δείχνει ότι προέρχεται από τραπεζικό ίδρυμα (πιθανόν από κάποιο τραπεζικό ίδρυμα με το οποίο και ο ίδιος έχει συναλλαγές) και του ζητά να εισέλθει στο πληροφοριακό σύστημα προκειμένου να αλλάξει κάποια στοιχεία επικοινωνίας του. Αν η επίθεση αυτού του τύπου πετύχει, τότε μόλις ο χρήστης εισάγει τα στοιχεία του (ιδιαίτερα το αναγνωριστικό και το συνθηματικό για τη σύνδεσή του με το πληροφοριακό σύστημα της τράπεζας) τότε αυτά αποστέλλονται μέσω του Διαδικτύου στο θύτη.

Οι μέθοδοι που χρησιμοποιούνται για αυτό τον τύπο εγκλήματος είναι συνήθως η ηλεκτρονική αλληλογραφία (email), η οποία μοιάζει να προέρχεται από έμπιστη πηγή. Ακόμη, χρησιμοποιούνται παραπλανητικού τύπου σύνδεσμοι (hyperlinks) με ονομασίες δημοφιλών διαδικτυακών τόπων ή παραπλανητικά γραφικά και διαφημιστικές πινακίδες με σκοπό να δελεάσουν τον ανυποψίαστο χρήστη. Ακόμη, μπορεί να συναντήσουμε χρήση παραθύρων pop-up για την ενσωμάτωση κακόβουλου κώδικα σε μια ιστοσελίδα. Ο κακόβουλος κώδικας εκμεταλλεύεται μια ευπάθεια του φυλλομετρητή ή του εξυπηρετητή (Web server) για να παρασύρει τον επισκέπτη σε λανθασμένες ενέργειες.

13.3.2 Παιδική πορνογραφία

Με την κατηγορία της κατοχής ή διακίνησης παιδικής πορνογραφίας κατηγορείται όποιος με πρόθεση παράγει, προσφέρει, πουλάει ή με οποιοδήποτε τρόπο διανέμει, διαβιβάζει, αγοράζει, προμηθεύεται ή κατέχει υλικό παιδικής πορνογραφίας. Η χρήση ηλεκτρονικού υπολογιστή ή του Διαδικτύου εντάσσει το έγκλημα αυτό στις κατηγορίες ηλεκτρονικού εγκλήματος και κυβερνοεγκλήματος, αντίστοιχα. Η τιμωρία της κατοχής ή διακίνησης παιδικής πορνογραφίας αφορά φυλάκιση τουλάχιστον 2 ετών και χρηματική ποινή τουλάχιστον 50.000 ευρώ.

Σύμφωνα με το «Προαιρετικό Πρωτόκολλο στη Σύμβαση για τα Δικαιώματα του Παιδιού σχετικά με την εμπορία παιδιών, την παιδική πορνεία και παιδική πορνογραφία», ο όρος *'παιδική πορνογραφία σημαίνει οποιαδήποτε αντιπροσώπευση, με οποιαδήποτε μέσα, ενός παιδιού που συμμετέχει σε πραγματικές ή προσομοιωμένες ρητές σεξουαλικές δραστηριότητες ή οποιαδήποτε αντιπροσώπευση των σεξουαλικών μελών ενός παιδιού για πρώτιστα σεξουαλικούς σκοπούς'*. Το φαινόμενο αυτό δεν είναι απόρροια της χρήσης του Διαδικτύου, αλλά το Διαδίκτυο ώθησε ακόμη μεγαλύτερη μερίδα ανθρώπων στην παρανομία, καθώς:

- Θεωρείται ευκολότερη η μυστικότητα και η ανωνυμία.
- Διευκολύνεται η άμεση ανταλλαγή του παράνομου υλικού.

Με βάση το άρθρο 348^{A} του Ποινικού Κώδικα, οι τρόποι εγκληματικής δράσης είναι:

- Κατασκευή υλικού πορνογραφίας.
- Κατοχή πορνογραφικού υλικού.
- Προμήθεια και αγορά υλικού πορνογραφίας.
- Μεταφορά πορνογραφικού υλικού.
- Κυκλοφορία πορνογραφικού υλικού.

13.3.3 Αθέμιτη υποκλοπή

Η αθέμιτη υποκλοπή περιγράφει εκείνο το ηλεκτρονικό έγκλημα κατά το οποίο διαπράττεται εκ προθέσεως υποκλοπή δεδομένων από, προς ή μέσα σε ένα σύστημα υπολογιστών και η οποία γίνεται με χρήση ηλεκτρονικών ή άλλων τεχνικών μέσων.

13.3.4 Παράνομη πρόσβαση

Ως παράνομη πρόσβαση χαρακτηρίζεται η εκ προθέσεως και χωρίς εξουσιοδότηση πρόσβαση σε ένα πληροφοριακό σύστημα. Η δραστηριότητα αυτή είναι γνωστότερη ως hacking ή cracking.

Hacking είναι η μη εξουσιοδοτημένη πρόσβαση μέσω διείσδυσης (δηλαδή ηθελημένης παραβίασης των μηχανισμών ελέγχου πρόσβασης) σε υπολογιστικά συστήματα, σκοπός της οποίας καταρχήν δεν είναι η δολιοφθορά, η καταστροφή ή η αποκόμιση οικονομικού οφέλους, αλλά η προσωπική ικανοποίηση από την παράκαμψη των συστημάτων ασφαλείας και η επιβεβαίωση των τεχνολογικών γνώσεων και δεξιοτήτων μέσω της εισβολής σε ένα ξένο υπολογιστικό σύστημα.

Η έννοια του hacking είναι ευρεία. Μπορεί να αφορά μια σειρά προγραμματιστικών δραστηριοτήτων που απαιτούν αυξημένες ικανότητες, ορισμένες από τις οποίες μπορούν να χαρακτηριστούν ως παράνομες ή και εγκληματικές. Η εισβολή σε ένα τρίτο σύστημα ακόμα και αν δεν είναι κακόβουλη, ενέχει παράνομο χαρακτήρα. Ο επιτιθέμενος, διεισδύοντας σε ένα τρίτο σύστημα αποκτά γνώσεις για το επίπεδο ασφάλειας του, εντοπίζει τα αδύνατα σημεία του και στη συνέχεια μπορεί να διαπράξει κακόβουλη επίθεση ή ακόμα και να δημοσιοποιήσει τις πληροφορίες που έχει συγκεντρώσει σε κάποιον τρίτο που θα προχωρήσει αργότερα σε μια ή περισσότερες επιθέσεις.

13.3.5 Επέμβαση σε δεδομένα

Επέμβαση σε δεδομένα θεωρείται η εκ προθέσεως καταστροφή, διαγραφή, μεταβολή ή απόκρυψη δεδομένων χωρίς προηγούμενη εξουσιοδότηση. Σε αυτή την περίπτωση, προστατευόμενο έννομο αγαθό είναι η ακεραιότητα και η κανονική χρήση των αποθηκευμένων δεδομένων ή των προγραμμάτων ηλεκτρονικών υπολογιστών.

13.3.6 Διασπορά κακόβουλου λογισμικού

Ως κακόβουλο λογισμικό (malware) θεωρούμε εφαρμογές οι οποίες έχουν ως στόχο την παραβίαση της ασφάλειας των υπολογιστών (host) στους οποίους εκτελούνται, με σκοπό να προκαλέσουν φθορές, υποβάθμιση ή διακοπή λειτουργίας, καθώς και να υποκλέψουν προσωπικά στοιχεία. Υπάρχουν αρκετοί τρόποι διασποράς κακόβουλου λογισμικού με τους γνωστότερους να είναι οι ιοί (virus), τα σκουλήκια (worms) και οι Δούρειοι Ίπποι (Trojan Horses).

Τα είδη του κακόβουλου λογισμικού διαρκώς πολλαπλασιάζονται, καθώς η εξέλιξη της τεχνολογίας λειτουργεί ευεργετικά και για τους κακόβουλους χρήστες. Δεν είναι σπάνια η εμφάνιση κακόβουλου λογισμικού με εξειδίκευση στη στόχευση αλλά και στον τρόπο λειτουργίας του. Χαρακτηριστικό παράδειγμα είναι η κατηγορία ransomware, όπου το κακόβουλο λογισμικό κάνει χρήση της Υποδομής Δημόσιου Κλειδιού (Public Key Infrastructure – PKI) και της κρυπτογραφίας ελλειπτικών καμπυλών προκειμένου να κρυπτογραφήσει όλα τα αρχεία κειμένου του ανυποψίαστου χρήστη και στη συνέχεια να απαιτήσει λύτρα (χρηματικό ποσό), προκειμένου να αποστείλει στον χρήστη το απαραίτητο ιδιωτικό κλειδί για να αποκρυπτογραφήσει τα αρχεία του υπολογιστή του. Οι συγγραφείς τέτοιων ransomware εφαρμογών εκμεταλλεύονται τεχνικές ανωνυμίας, κυρίως μέσω του δικτύου Tor ώστε να εισέλθουν στο λεγόμενο darknet και να εγκαταστήσουν εκεί τους εξυπηρετητές οι οποίοι είναι απαραίτητοι για να επιτελέσουν τους σκοπούς και να εξαπολύσουν «εκ τους ασφαλούς» τις επιθέσεις τους.

13.4 Εξιχνίαση

Η έρευνα για την εξιχνίαση των ηλεκτρονικών εγκλημάτων είναι μια αρκετά δύσκολη και ιδιαίτερα χρονοβόρος διαδικασία με σκοπό τον εντοπισμό των «ηλεκτρονικών ιχνών». Οι κακόβουλοι χρήστες έχουν στη διάθεσή τους και χρησιμοποιούν αρκετά μέτρα προστασίας τα οποία δυσχεραίνουν τη διαδικασία της εξιχνίασης και πολλές φορές την καθιστούν αδύνατη. Ορισμένες χώρες, κράτη-μέλη της Ευρωπαϊκής ένωσης ή και εκτός αυτής, στηρίζουν με την νομοθεσία τους την ανωνυμία μέσω υπηρεσιών Ιδεατών Ιδιωτικών Δικτύων (VPN) και με τον τρόπο αυτό βοηθούν τους θύτες να καλύψουν τα ίχνη τους. Ο λόγος χρήσης των VPN αφορά την υποστήριξη του δικαιώματος της ιδιωτικότητας του κάθε ανθρώπου. Ωστόσο, αυτό ακριβώς εκμεταλλεύονται και οι ηλεκτρονικοί εγκληματίες.

Σε όλες τις περιπτώσεις όπου διεξάγεται διαδικτυακή έρευνα γίνεται προσπάθεια να εντοπιστεί το «ηλεκτρονικό ίχνος» του δράστη. Το ηλεκτρονικό ίχνος κάθε χρήστη του διαδικτύου είναι μοναδικό και αποτελεί ένα από τα σημαντικότερα στοιχεία 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 και μπορεί να διατηρούνται για μεγάλα χρονικά διαστήματα.

Ειδικότερα, στα χαρακτηριστικά γνωρίσματα του εγκλήματος στον Κυβερνοχώρο συμπεριλαμβάνονται και τα ακόλουθα

- Το έγκλημα στον Κυβερνοχώρο είναι τις περισσότερες φορές γρήγορο, διαπράττεται σε ελάχιστο χρόνο και συνήθως δεν γίνεται αντιληπτό ούτε από το ίδιο το θύμα.

- Η διάπραξη του είναι εύκολη , για όσους κατέχουν τις ιδιαίτερες ικανότητες που απαιτούνται, ενώ τα ηλεκτρονικά ίχνη που αφήνει είναι ψηφιακά.

- Για την τέλεσή του απαιτούνται συνήθως ιδιαίτερα εξειδικευμένες γνώσεις.

- Ο δράστης μπορεί να διαπράξει το ηλεκτρονικό έγκλημα χωρίς να μετακινηθεί, από το σπίτι ή το γραφείο του, μέσω του υπολογιστή του.

- Δίνει τη δυνατότητα στους θύτες, όπως οι παιδόφιλοι, να επικοινωνούν γρήγορα ή και σε πραγματικό χρόνο, χωρίς μετακίνηση, εύκολα, ανέξοδα, να βρίσκονται πολλοί μαζί στις ίδιες ομάδες συζητήσεως (news groups) ή μέσα σε chat rooms που χρησιμοποιούνται για άλλους σκοπούς.

- Τις περισσότερες φορές οι κυβερνοεγκληματίες επικοινωνούν χρησιμοποιώντας ψευδείς ταυτότητες, τις οποίες χρησιμοποιούν για να αποστείλουν ηλεκτρονικά μηνύματα

- Το ηλεκτρονικό έγκλημα συνήθως διασχίζει τα εθνικά σύνορα και οι επιπτώσεις του επηρεάζουν ταυτόχρονα πολλούς τόπους.

- Είναι πολύ δύσκολο να προσδιοριστεί ο τόπος τέλεσής του και επίσης είναι αρκετά δύσκολη η διερεύνηση και ο εντοπισμός του δράστη. Υπάρχει ενδεχόμενο ο δράστης να εντοπισθεί σε μια χώρα και τα αποδεικτικά στοιχεία να βρίσκονται σε μια άλλη, απομακρυσμένη χώρα ή και να βρίσκονται ταυτόχρονα σε πολλές διαφορετικές χώρες.

- Είναι συνηθισμένη η συνεργασία δύο ή περισσότερων κρατών κατά την διερεύνηση ενός ηλεκτρονικού εγκλήματος. Περιπτώσεις εγκληματικής συμπεριφοράς στα όρια ενός μόνον κράτους είναι λιγοστές.

13.5 Ιδιωτικότητα

Η ραγδαία αύξηση του όγκου των πληροφοριών και των επικοινωνιακών ροών είναι γεγονός το οποίο γίνεται άμεσα αντιληπτό από το καθένα μας. Η πληροφορία αφορά κάθε ανθρώπινη δραστηριότητα αλλά και τον ίδιο τον άνθρωπο. Στοιχεία που αφορούν τον καθέναν από μας υπάρχουν πλέον ως δεδομένα σε πολλά και διαφορετικά πληροφοριακά συστήματα. Ταυτόχρονα, γνωρίζουμε ήδη ότι ο κυβερνοχώρος είναι ένα πεδίο στο οποίο μαίνονται «μάχες» ανάμεσα σε κυβερνοεγκληματίες και κυβερνοφύλακες. Κανείς δεν μπορεί να νιώθει ήσυχος σε μια τέτοια κατάσταση. Τα προσωπικά δεδομένα ή δεδομένα προσωπικού χαρακτήρα, δηλαδή αυτά που αφορούν / χαρακτηρίζουν ένα πρόσωπο και συνδέονται με την ταυτότητά του, θα πρέπει να διασφαλίζονται με τέτοιο τρόπο ώστε να μην υπάρχει ο κίνδυνος έκθεσής τους σε τρίτους.

Η ανάγκη για τη συνταγματική κατοχύρωση της ιδιωτικότητας (privacy) εμφανίζεται, για πρώτη φορά στη νεότερη ιστορία, το 1890 οπότε η έννοια της ιδιωτικότητας συνδέθηκε με το δικαίωμα να μείνει κανείς μόνος (the right to be left alone). Το 1950 η ευρωπαϊκή επιτροπή των ανθρώπινων δικαιωμάτων θέσπισε το δικαίωμα σεβασμού της ιδιωτικής ζωής των πολιτών της.

Η έννοια της ιδιωτικότητας προσδιορίζεται ανάλογα με το πλαίσιο στο οποίο αυτή εξετάζεται. Έτσι, έχουμε τις ακόλουθες παραλλαγές της:

- Πληροφοριακή Ιδιωτικότητα: σχετίζεται με τη συγκέντρωση, την αποθήκευση, την επεξεργασία και τη διάδοση των πληροφοριών που αποτελούν προσωπικά δεδομένα ενός ανθρώπου (προσώπου).

- Χωρική Ιδιωτικότητα: σχετίζεται με την προστασία της φυσικής περιοχής στην οποία βρίσκεται ένα πρόσωπο (π.χ. οικία, εργασιακός χώρος κλπ.).

- Σωματική Ιδιωτικότητα: σχετίζεται με την προστασία ενός του σώματος ενός προσώπου από αδικαιολόγητη παρέμβαση (π.χ. σωματικός έλεγχος κλπ.).

- Επικοινωνιακή Ιδιωτικότητα: σχετίζεται με την προστασία από μη εξουσιοδοτημένη παρακολούθηση της επικοινωνίας ενός προσώπου με άλλα πρόσωπα.

Ο πιο κοινά αποδεκτός ορισμός της Πληροφοριακής Ιδιωτικότητας προτάθηκε το 1967 από τον Alan F. Westin και αναφέρει ότι: «Ιδιωτικότητα είναι η αξίωση των ατόμων, των ομάδων και των ιδρυμάτων να αποφασίζουν από μόνοι τους για το πότε, πώς και μέχρι ποιο σημείο οι πληροφορίες που αφορούν αυτούς, θα διαβιβάζονται σε άλλους». Το σημαντικό στον παραπάνω ορισμό είναι ο διαχωρισμός της πληροφορίας σε δημόσια ή ιδιωτική. Συνήθως, ο διαχωρισμός αυτός βασίζεται στο ισχύον νομικό και κανονιστικό πλαίσιο.

Η έννοια της Πληροφοριακής Ιδιωτικότητας καθίσταται εξαιρετικά σημαντική στη διαχείριση και λειτουργία των πληροφοριακών συστημάτων, κυρίως εξαιτίας τόσο του χαρακτήρα των εργασιών που επιτελούνται, όσο και του σημαντικού όγκου δεδομένων που συλλέγονται, επεξεργάζονται και αποθηκεύονται σε αυτά. Για την προστασία δεδομένων, η Ευρωπαϊκή Οδηγία 1995/46/ΕΚ ορίζει τις αρχές της νομιμότητας και της δικαιοσύνης, την αρχή του καθορισμού του σκοπού της συλλογής των δεδομένων και της επεξεργασίας αυτών για το σκοπό που συλλέχθηκαν, την αρχή της αναγκαιότητας της συλλογής και επεξεργασίας των δεδομένων, την αρχή της παροχής πληροφόρησης, ενημέρωσης και πρόσβασης στους κατόχους των δεδομένων, την αρχή της ασφάλειας και της ακεραιότητας, καθώς και την αρχή της εποπτείας και επικύρωσης. Είναι σημαντικό να τονίσουμε ότι μια επίθεση σε ένα πληροφοριακό σύστημα δεν προσβάλει απαραίτητα το απόρρητο της επεξεργασίας προσωπικών δεδομένων. Τα αντίμετρα προστασίας τα οποία χρησιμοποιεί ένα πληροφοριακό σύστημα πολλές φορές δεν καλύπτουν τις ανάγκες προστασίας και ενίσχυσης της ιδιωτικότητας.

Η προστασία της ιδιωτικότητας είναι ένα ζήτημα το οποίο πολλές φορές μπορεί να έρθει σε σύγκρουση με τη χρήση άλλων μηχανισμών ασφάλειας. Για παράδειγμα, σε ένα εργασιακό χώρο είναι πιθανό η εταιρική πολιτική να ορίζει τη χρήση κάμερας για επιτήρηση ενός χώρου, κάτι όμως το οποίο παραβιάζει την ιδιωτικότητα των εργαζομένων. Άλλη παρόμοια περίπτωση συμβαίνει με την αξιοποίηση της τεχνολογίας DRM (digital rights management), όπου μπορεί να γίνεται αξιοποίηση μηχανισμών προσδιορισμού ταυτότητας, καταγραφής ηλεκτρονικών ιχνών και κατά συνέπεια εντοπισμού των χρηστών. Η επιβολή της απαραίτητης ισορροπίας είναι μια δύσκολη υπόθεση, καθώς η πληροφορία αποτελεί ένα σημαντικό παράγοντα ανάπτυξης και εδραίωσης για κάθε οργανισμό ή κράτος. Σε κάθε περίπτωση, οι μηχανισμοί ασφάλειας που υλοποιούνται

θα πρέπει να είναι συμβατοί με τις βασικές αρχές μιας δημοκρατικής κοινωνίας, όπως ορίζεται από τον ΟΟΣΑ: «Security should be implemented in a manner consistent with the values recognized by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency»

Βιβλιογραφία

Maniotis, D., Marinos, M.-T., Anthimos, A., Iglezakis, I., & Nouskalis, G. (2011). Cyber law in Greece. Alphen aan den Rijn, The Netherlands: Kluwer Law International.

Moore, A. D. (2010). Privacy rights: moral and legal foundations. University Park, Pa: Pennsylvania State University Press.

Nissenbaum, H. F. (2010). Privacy in context: technology, policy, and the integrity of social life. Stanford, Calif: Stanford Law Books.

Pedneault, S., & Davia, H. R. (2009). Fraud 101: techniques and strategies for understanding fraud (3rd ed., Fully rev). Hoboken, N.J: John Wiley & Sons.

Regan, P. M. (2009). Legislating privacy: technology, social values and public policy. Chapel Hill, NC: The Univ. of North Carolina Press.

Αρμαμέντος, Π., & Σωτηρόπουλος, Β. (2005). Προσωπικά δεδομένα - Ερμηνεία Ν. 2472/1997, Εκδόσεις Σάκκουλα.

Ηλεκτρονικό Έγκλημα - Υπ. Εσωτερικών και Διοικητικής Ανασυγκρότησης - Ελληνική Αστυνομία. (n.d.). Retrieved 30 September 2015, from http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414.

Λίλιαν Μήτρου.Προστασία Προσωπικών Δεδομένων [open]. Retrieved 30 September 2015 from https://eclass.aegean.gr/courses/ICSD117/

Λίλιαν Μήτρου.Κανονιστικές και Κοινωνικές Διαστάσεις της Κοινωνίας της Πληροφορίας [open].Retrieved 30 September 2015 from https://eclass.aegean.gr/courses/ICSD118/

Λίλιαν Μήτρου.Ειδικά Θέματα Δικαίου της Πληροφορίας [open].Retrieved 30 September 2015 from https://eclass.aegean.gr/courses/ICSD119/.

Κριτήρια αξιολόγησης

Απαντήστε στις ακόλουθες ερωτήσεις. Η κάθε ερώτηση μπορεί να έχει μοναδική ή περισσότερες απαντήσεις.

1. Ποιες από τις παρακάτω κατηγορίες θεωρούνται Κυβερνοεγκλήματα;
α) Εγκλήματα κατά της προσωπικότητας και της ιδιωτικότητας.
β) Εγκλήματα κατά της περιουσίας.
γ) Διακίνηση παράνομου και αθέμιτου / επιβλαβούς περιεχομένου.
δ) Όλα τα παραπάνω.

2. Ποιοι Νόμοι του Ποινικού Κώδικα αφορούν την προστασία του απορρήτου;
α) 360

β) 370
γ) 370Α
δ) 380

3. Η «Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών» καθορίζεται από το νόμο:
α) Ν.2472/1997
β) Ν.2774/1999
γ) Ν .3115/2003
δ) Ν.3431/2006

4. Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα και η προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών αναφέρεται στην Ευρωπαϊκή Οδηγία:
α) 2002/58/ΕΚ
β) 2002/20/ΕΚ
γ) 2000/31/ΕΚ
δ) 2002/77/ΕΚ

5. Τι σημαίνει ο όρος DRM;
α) Digital Recording Management
β) Digital Rights Manager
γ) Digital Recording Manager
δ) Digital Rights Management

6. Αν ο πάροχος αντιληφθεί ότι τα δεδομένα έχουν αποσυρθεί από το σημείο αφετηρίας της μετάδοσής τους οφείλει:
α) να συνεχίσει να προσφέρει πρόσβαση.
β) να ενημερώσει τον ιδιοκτήτη της πληροφορίας.
γ) να αποσύρει άμεσα ή να καταστήσει αδύνατη την πρόσβαση σε αυτά τα δεδομένα που αποθήκευσε.
δ) να μην κάνει κάτι από τα παραπάνω.

7.Ποιες από τις παρακάτω είναι κατηγορίες Ηλεκτρονικού Εγκλήματος;
α) Σαμποτάζ.
β) Καμουφλάζ.
γ) Απάτη.
δ) Αλίευση.

8. Ο όρος Hacking είναι συνώνυμος του Cracking;
α) Ναι.
β) Όχι.
γ) Ναι, τις περισσότερες φορές.
δ) Όχι, τις περισσότερες φορές.

9. Ποιες από τις παρακάτω έννοιες αφορούν την Ιδιωτικότητα;
α) Πληροφοριακή Ιδιωτικότητα.
β) Χωρική Ιδιωτικότητα.
γ) Σωματική Ιδιωτικότητα.
δ) Όλες οι παραπάνω.

10. Η Επικοινωνιακή Ιδιωτικότητα σχετίζεται με:
α) την προστασία από μη εξουσιοδοτημένη παρακολούθηση της επικοινωνίας πολλών προσώπων με ένα πρόσωπο.
β) την προστασία από εξουσιοδοτημένη παρακολούθηση της επικοινωνίας ενός προσώπου με άλλα πρόσωπα.
γ) την προστασία από μη εξουσιοδοτημένη παρακολούθηση της επικοινωνίας ενός προσώπου με άλλα πρόσωπα.
δ) κανένα από τα παραπάνω