

ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

ΜΑΘΗΤΕΣ ΠΟΥ ΕΡΓΑΣΤΗΚΑΝ:

Σέρη Αντωνίου

Ελένη Γιαννουκάκη

Αναστασία Κατσιφή



Ο ορισμός του ηλεκτρονικού εγκλήματος:

- ▶ Ως ηλεκτρονικό έγκλημα ορίζονται οι αξιόποινες πράξεις που τελούνται με την χρήση ηλεκτρονικών υπολογιστών και γενικότερα με διάφορα ηλεκτρονικά μέσα.

Το ηλεκτρονικό έγκλημα θεωρείται ως:

- ▶ μια νέα μορφή εγκλήματος
- ▶ μια παραλλαγή των ήδη υπαρχόντων εγκλημάτων
- ▶ μια εγκληματική πράξη στην εκδήλωση της οποίας συμμετέχει καθοιονδήποτε τρόπο ένας ηλεκτρονικός υπολογιστής.

Χαρακτηριστικά γνωρίσματα του εγκλήματος στον Κυβερνοχώρο:

- Το έγκλημα στον Κυβερνοχώρο είναι γρήγορο (σε χρόνο δευτερολέπτων).
- Γι' αυτούς που γνωρίζουν είναι εύκολο στην διάπραξη του.
- Για την τέλεση του απαιτούνται άριστες και εξειδικευμένες γνώσεις. Μπορεί να διαπραχθεί χωρίς μετακίνηση.
- Δίνει τη δυνατότητα σε άτομα με ιδιαιτερότητες όπως οι παιδόφιλοι, να επικοινωνούν γρήγορα, σε πραγματικό χρόνο, χωρίς μετακίνηση και εύκολα.
- Οι εγκληματίες του “Κυβερνοχώρου” πολλές φορές δεν εμφανίζονται με την πραγματική τους ταυτότητα.
- Είναι έγκλημα διασυνοριακό και τα αποτελέσματα μπορεί να πραγματοποιούνται ταυτόχρονα σε πολλούς τόπους.
- Είναι πολύ δύσκολο να προσδιοριστεί ο τόπος τελέσεως του και επίσης είναι δύσκολη η διερεύνηση και ο εντοπισμός του δράστη.
- Η έρευνα απαιτεί κατά κανόνα συνεργασία δυο τουλάχιστον κρατών (του κράτους στο οποίο έγινε αντιληπτό το αποτέλεσμα της εγκληματικής συμπεριφοράς και του κράτους όπου βρίσκονται τα αποδεικτικά στοιχεία).
- Η καταγραφή της εγκληματικότητας στον Κυβερνοχώρο δεν ανταποκρίνεται στην πραγματικότητα διότι ελάχιστες περιπτώσεις εγκλημάτων του Κυβερνοχώρου καταγγέλλονται διεθνώς.

Διαδικασία έρευνας:

- Η έρευνα ηλεκτρονικών εγκλημάτων είναι σε μεγάλο επίπεδο δύσκολη και χρονοβόρα, όπως και ο εντοπισμός των ηλεκτρονικών ιχνών, τα οποία είναι ένα από τα πιο σημαντικά αποδεικτικά στοιχεία. Συγκεκριμένα μια έρευνα μπορεί να διαρκέσει από έναν μήνα έως και δύο χρόνια. Και ο λόγος αυτής της μεγάλης διάρκειας είναι πως οι χρήστες που έχουν καταγγείλει (οι πολίτες) παίρνουν διάφορα διαδικτυακά μέτρα προστασίας.

○ τέλειος συνδυασμός είναι:

- η κατάλληλη εξειδίκευση του αστυνομικού προσωπικού
- και τα κατάλληλα τεχνολογικά μέσα

Μετά τη διεξαγωγή του ηλεκτρονικού εγκλήματος θα πρέπει να ληφθούν άμεσα μέτρα.

- προστασία συσκευών εντός της περιμέτρου
- προστασία προσωρινών στοιχείων ή αν αυτό είναι αδύνατο, φωτογράφιση και καταγραφή τους
- αποσύνδεση συσκευών

Διαδικασία έρευνας(συνέχεια) :

Αφού μεταφερθούν τα αρχεία σε κατάλληλους χώρους ξεκινά η προσεκτική εξέτασή τους με την παρακάτω μεθοδολογία:

- Προστασία του υποκείμενου σε έρευνα συστήματος από οποιαδήποτε επίθεση, εκούσια ή ακούσια.
- Ανακάλυψη όλων των αρχείων στο σύστημα
- Επαναφορά διαγραμμένων αρχείων.
- Αποκάλυψη περιεχομένου κρυμμένων και προσωρινών αρχείων
- Απόκτηση πρόσβασης σε προστατευμένα αρχεία με νόμιμο τρόπο αν αυτό είναι δυνατό
- Ανάλυση των δεδομένων που βρίσκονται σε ειδικές περιοχές του δίσκου
- Εκτύπωση του τελικού αποτελέσματος της έρευνας.
- Εξέταση της ανάλυσης από πραγματογνώμονες



Νομοθεσία:

- ▶ Η συνθήκη Βουδαπέστης:

Λόγω του ότι οι μορφές του ηλεκτρονικού εγκλήματος είναι ποικίλες και πολλαπλασιάζονται παράλληλα με ανάπτυξη της τεχνολογίας έπρεπε να γίνει μια διακρατική συνεννόηση. Ο στόχος αυτός επετεύχθη στο Συνέδριο για το Ηλεκτρονικό Έγκλημα που έγινε το 2001 στη Βουδαπέστη, όπου υπέγραψαν 26 υπουργοί Ευρωπαϊκών κρατών, μέσα σε αυτούς και της Ελλάδας.

- ▶ Στο εξωτερικό:

Στην Αγγλία από το 2001 αναλόγως του επιπέδου του χτυπήματος μπορεί να θεωρηθεί ως τρομοκρατία. Επιπλέον, στην Αμερική θεωρούνται όλες οι πράξεις χωρίς εξουσιοδότηση πρόσβασης σε Η/Υ τρομοκρατικές και τιμωρούνται με φυλάκιση μέχρι και ισόβια χωρίς να μπορεί να μειωθεί η ποινή.

Νομοθεσία (συνέχεια) :

Νομοθεσία στην Ελλάδα:

- Στην Ελληνική νομοθεσία δεν υπάρχουν νόμοι που να αναφέρονται στα θέματα Διαδικτύου και στην ρύθμιση συμπεριφοράς χρηστών. Όμως υπάρχει συνεργασία με τα κράτη της Ευρωπαϊκής Ένωσης, του Συμβουλίου Ευρώπης και άλλων Εθνικών Οργανισμών. Σίγουρα όμως όλη αυτή η συνεργασία δεν επαρκεί για την τέλεια αντιμετώπιση των εγκλημάτων Διαδικτύου.

Αδυναμίες νομοθεσίας:

- Επειδή το ηλεκτρονικό έγκλημα είναι εξειδικευμένο και ανεπτυγμένο ηλεκτρονικά υπάρχουν κάποια προβλήματα.
- Παρουσιάζονται προβλήματα για την οριοθέτηση των πράξεων που πρέπει να διώκονται ποινικά.
- Οι νομοθέτες πρέπει συνεχώς να ενημερώνονται για τις εξελίξεις της τεχνολογίας των υπολογιστών ώστε να εξοικειωθούν με τον τρόπο διάπραξής τους.

Σύμφωνα με έρευνα στη Βρετανία από επιτροπή πρόβλεψης και πρόληψης εγκλήματος το 2020 οι κακοποιοί θα μπορούν να γνωρίζουν σε υψηλό επίπεδο την λειτουργία των συστημάτων ασφαλείας τραπεζικών κωδικών, δηλαδή θα μπορούν να ξεπεράσουν κάθε ηλεκτρονικό εμπόδιο.



ΕΥΧΑΡΙΣΤΟΥΜΕ ΓΙΑ ΤΗΝ ΠΡΟΣΟΧΗ ΣΑΣ

ΤΕΛΟΣ.

