Ερευνητική εργασία **«Εγκλήματα στο Κυβερνοχώρο»**

Τάξη ΒΘ3

Α΄ τετράμηνο 2015-16

Υπεύθυνη καθηγήτρια : Μαίρη Τζιομάλλου

ΠΕΡΙΕΧΟΜΕΝΑ

Εννοιολογική προσέγγιση-Χαρακτηριστικά-Αίτια

Οι μαθητές:

- Π. Κ.
- Ρ. Δ.
- Ρ. Ε.
- Τ. Γ.
- Τ. Γ.

Περιεχόμενα

1. Ορισμός ,έννοια του ηλεκτρονικού εγκλήματος
2. Χαρακτηριστικά στοιχεία ηλεκτρονικού εγκλήματος στον κυβερνοχώρο
3. Αίτια εμφάνισης του ηλεκτρονικού εγκλήματος

ΟΡΙΣΜΟΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Ως «Ηλεκτρονικό Έγκλημα» θεωρούνται οι αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων. Είναι πράξεις άδικες , ανήθικες, παράνομες και χωρίς έγκριση, καταλογιστέες στο δράστη τους, που τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία. Ανάλογα με τον τρόπο τέλεσης διαχωρίζονται σε εγκλήματα τελούμενα μόνο με τη χρήση Ηλεκτρονικών Υπολογιστών χωρίς τη σύνδεση στο διαδίκτυο (computer crime) και σε Κυβερνοεγκλήματα (cyber crime), εάν τελέσθηκε μέσω του Διαδικτύου. Η άποψη ότι το έγκλημα στον κυβερνοχώρο (cyber crime) αποτελεί τον ίδιο τύπο εγκλήματος με το «κοινό» ή «συμβατικό» έγκλημα και η μόνη διαφορά που το διακρίνει από αυτό είναι ότι διαπράττεται σε διαφορετικό περιβάλλον (δηλαδή σε ηλεκτρονικό περιβάλλον και σε περιβάλλον δικτύου) και δεν ανταποκρίνεται στην πραγματικότητα. Υπάρχουν βέβαια εγκλήματα, που διαπράττονται τόσο σε κοινό, όσο και σε ηλεκτρονικό περιβάλλον.

ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Το Ηλεκτρονικό Έγκλημα, ανεξάρτητα από το εάν προσεγγιστεί από την στενή ή την ευρεία έννοια του, εμπεριέχει ορισμένα χαρακτηριστικά γνωρίσματα που το διαχωρίζουν από το παραδοσιακό έγκλημα. Τέτοια σημεία είναι τα εξής :

1. Το έγκλημα στον κυβερνοχώρο είναι γρήγορο, διαπράττεται σε πραγματικό χρόνο, ακόμα και σε δευτερόλεπτα, και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα.

2. Είναι εύκολο στη διάπραξή του για όσους το γνωρίζουν, ενώ τα ίχνη που αφήνει είναι ψηφιακά.

3. Για την τέλεση του απαιτούνται άριστες και εξειδικευμένες γνώσεις

4. Οι κυβερνο-εγκληματίες πολλές φορές δεν εμφανίζονται με την πραγματική τους ταυτότητα, αποστέλλοντας ηλεκτρονικά μηνύματα (e-mails) με ψευδή στοιχεία.

5. Μπορεί να διαπραχθεί από οποιοδήποτε μέρος, καθώς δεν απαιτείται η μετακίνηση του δράστη, και τα αποτελέσματά του να γίνονται ταυτόχρονα αισθητά σε πολλούς στόχους ανεξαρτήτου εδαφικού περιορισμού. Για αυτό, άλλωστε, και το αποκαλούν «έγκλημα χωρίς πατρίδα».

6. Ο εντοπισμός ενός ψηφιακού εγκληματία, κατά κανόνα, είναι πολύ δύσκολος (αλλά όχι ακατόρθωτος) να προσδιοριστεί καθώς επίσης και ο (πραγματικός) τόπος τέλεσής του και αυτό γιατί μπορεί ο δράστης να εντοπιστεί σε ένα συγκεκριμένο τόπο, τα αποδεικτικά στοιχεία, όμως, να βρίσκονται σε διαφορετική και απομακρυσμένη χώρα ή και να βρίσκονται ταυτόχρονα σε πολλές διαφορετικές χώρες.

7. Καθώς ο κίνδυνος ανακάλυψης του ηλεκτρονικού δράστη είναι μικρός, το ηλεκτρονικό έγκλημα αποδίδει μεγάλα κέρδη.

8. Ο αριθμός των θυμάτων τους συγκρινόμενος με εκείνο των παραδοσιακών εγκλημάτων είναι κατά πολύ μεγαλύτερος.

9. Οι οικονομικές απώλειες που προξενούνται στα «ψηφιακά» εγκλήματα είναι πολύ μεγαλύτερες από εκείνες των θυμάτων των παραδοσιακών εγκλημάτων.

10.Καθώς για την διάπραξή του δεν απαιτείται φυσική μετακίνηση του δράστη, δίνει τη δυνατότητα σε άτομα με ορισμένες ιδιαιτερότητες, όπως για παράδειγμα παιδόφιλοι, να επικοινωνούν γρήγορα ή και σε πραγματικό χρόνο, χωρίς μετακίνηση, εύκολα, ανέξοδα, να βρίσκονται μαζί στις ίδιες ομάδες συζήτηση (π.χ. Newsgroups) ή μέσα από διαδικτυακά άμεσα αναμεταδιδόμενες συζητήσεις (π.χ. Internet Relay Chat).

11.Η καταγραφή της εγκληματικότητας στον Κυβερνοχώρο δεν ανταποκρίνεται στην πραγματικότητα γιατί ελάχιστες περιπτώσεις κυβερνο-εγκλημάτων καταγγέλλονται διεθνώς με άμεση συνέπεια, το μέγεθος της εγκληματικότητας στο χώρο του διαδικτύου να χαρακτηρίζεται ακόμα πιο «σκοτεινό» από ότι το έγκλημα του πραγματικού κόσμου.

12.Η αστυνομική διερεύνηση του είναι πολύ δύσκολη και απαιτεί άριστη εκπαίδευση και εξειδικευμένες γνώσεις.

13.Οι οποίες εξειδικευμένες γνώσεις απαιτούνται και σε όσους, εκτός αστυνομίας, ασχολούνται με τη συγκεκριμένη μορφή εγκλήματος, όπως είναι οι εισαγγελείς, οι δικαστές, οι δικηγόροι.

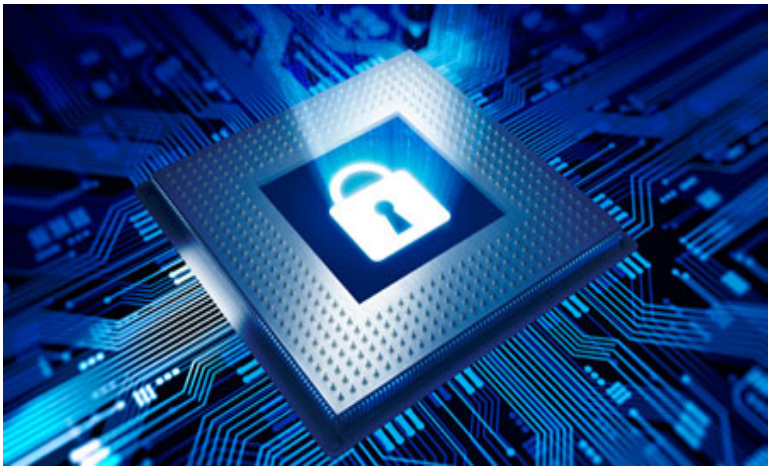
14. Για την διερεύνησή του απαιτείται συνεργασία τουλάχιστον δύο κρατών : του κράτους που γίνεται αντιληπτή η εξωτερίκευση του εγκλήματος και του κράτους όπου βρίσκονται αποθηκευμένα τα αποδεικτικά στοιχεία.

ΑΙΤΙΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Συχνά οι νέοι οδηγούνται στον Διαδικτυακό εκφοβισμό εξαιτίας της βίωσης έντονων συναισθημάτων όπως θυμός, απόγνωση είτε πάλι και εκδίκηση, που μπορεί να προέρχεται τόσο από τις προβληματικές σχέσεις που υπάρχουν στο οικογενειακό περιβάλλον όσο και εξαιτίας μιας ευρύτερης κοινωνικής δυσλειτουργικότητας που παρουσιάζει το άτομο. Σε μερικές περιπτώσεις ο Διαδικτυακός εκφοβισμός αποτελεί μορφή ψυχαγωγίας στοχεύοντας στην εκδήλωση ποικίλων αντιδράσεων και στην ικανοποίηση αναγκών που σχετίζονται με την επιβολή εξουσίας και ελέγχου. Συχνά άλλες αιτίες που οδηγούν τους νέους σε αυτήν την απαίσια και απαράδεκτη πράξη είναι η προσπάθεια αύξησης της δημοτικότητας και η επιδίωξη της φήμης. Επίσης πολλές είναι οι περιπτώσεις όπου τα αίτια είναι πιο… απλά! Έχουν υπάρξει φαινόμενα διαδικτυακού εκφοβισμού που ξεκίνησαν «για πλάκα» ή επειδή κάποιος «βαριέται».Σπανιότερα, η αποστολή μηνυμάτων σε λάθος παραλήπτες μπορεί να αποτελέσει αιτία του φαινομένου.

Το cyber bullying φαντάζει ίσως αθώο αστείο μεταξύ των παιδιών. Μπορεί όμως να έχει πολύ σοβαρές συνέπειες για τη ζωή του θύματος. Συμπεριφορές όπως αποχή από τα μαθήματα, κοινωνική απομόνωση,

απότομη πτώση στις σχολικές επιδόσεις, εκτέλεση πράξεων αντίθετων με τον χαρακτήρα του παιδιού ή παράνομες πράξεις λόγω εκβιασμού, επίμονη επιθυμία του παιδιού να αλλάξει σχολείο ή το όνομα του, κατάθλιψη ακόμη και αυτοκτονία, θα πρέπει να μας προβληματίσουν.



ΒΙΒΛΙΟΓΡΑΦΙΑ

- http://www.sepchiou.gr/docs/imerida-asfaleia/kevopoulos%20-%20ilektroniko%20egklima.pdf
- http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414
- https://sites.google.com/site/elektronikoenklema2012/charakteristika-tou-elektronikou
- https://el.wikipedia.org/wiki/%CE%94%CE%B9%CE%B1%CE%B4%CE%B9%CE%BA%CF%84%CF%85%CE%B1%CE%BA%CF%8C%CF%82_%CE%B5%CE%BA%CF%86%CE%BF%CE%B2%CE%B9%CF%83%CE%BC%CF%8C%CF%82
- http://www.madlink.gr/cyberbullying/

<u>Θέμα Ομάδας</u>:

«Μορφές Ηλεκτρονικού Εγκλήματος»

<u>Οι μαθητές</u>: Ι. Σ.

Τ. Η.

Φ. Α.

Χ. Γ.

ΠΕΡΙΕΧΟΜΕΝΑ

Παιδική πορνογραφία

«Το να βρει κάποιος υλικό παιδικής πορνογραφίας στο Διαδίκτυο είναι σαν να ανοίγει την πόρτα μιας τράπεζας. Τόσο εύκολο. Αλλά να προσπαθήσει να μπει στο μυαλό αυτού που το αποθηκεύει στον υπολογιστή του και το πουλάει, το αγοράζει, το διακινεί ή κάθεται μπροστά στην οθόνη του τα βράδια και το χαζεύει με την ατμόσφαιρα να κατακλύζεται από τη διεστραμμένη του αποχαύνωση είναι άλλο. Είναι σαν να προσπαθεί να βρει το συνδυασμό στο χρηματοκιβώτιο της τράπεζας. Τόσο δύσκολο, δηλαδή αδύνατον», αναφέρετε χαρακτηριστικά στην «Ελευθεροτυπία».

Είναι η οποιαδήποτε απεικόνιση με οποιαδήποτε μέσα ενός παιδιού που συμμετέχει σε πραγματικές ή εικονικές σεξουαλικές δραστηριότητες, με κίνητρο πρώτιστα την ικανοποίηση σεξουαλικών σκοπών, αλλά και το οικονομικό όφελος. Σύμφωνα με το άρθρο 348 Α του Ποινικού Κώδικα «όποιος από κερδοσκοπία παρασκευάζει, κατέχει, προμηθεύεται, αγοράζει, μεταφέρει, διακινεί ή θέτει με οποιοδήποτε τρόπο σε κυκλοφορία πορνογραφικό υλικό, τιμωρείται με φυλάκιση ενός έτους και χρηματική ποινή», ενώ επιβαρυντική περίπτωση τιμωρούμενη με κάθειρξη συνιστά η διακίνηση πορνογραφικού υλικού συνδεόμενου με την εκμετάλλευση της ανάγκης ή της πνευματικής αδυναμίας.

Στην κορωνίδα του άμεσου ποινικού ενδιαφέροντος βρίσκονται όλες εκείνες οι εγκληματικές πράξεις που μπορούν να βλάψουν τα παιδιά είτε θίγοντας τη γενετήσια αξιοπρέπειά τους είτε βλάπτοντας την ψυχική και σωματική τους υγεία. Εδώ εντάσσεται η διακίνηση παιδικής πορνογραφίας, η προσέλκυση παιδιών για γενετήσιους λόγους, η σεξουαλική παρενόχληση και η προσβολή της γενετήσιας αξιοπρέπειας, περιπτώσεις οι οποίες αναλύονται εκτενέστερα στο αρχείο παρακάτω. Στα εγκλήματα κατά των ανηλίκων χρηστών εντάσσεται επίσης η προτροπή σε αυτοκτονία (άρθρο 301 Ποινικού Κώδικα), φαινόμενο ιδιαίτερα συχνό στο χώρο του Διαδικτύου, καθώς επίσης και ο λεγόμενος κυβερνοεκφοβισμός (cyber bullying).

Ειδικότερα, στελέχη της Δίωξης Ηλεκτρονικού Εγκλήματος, μετά από αστυνομική διαδικτυακή έρευνα, πραγματοποίησαν τον τελευταίο μήνα παράλληλες επιχειρήσεις σε Αττική, Θεσσαλονίκη, Ροδόπη, Ηράκλειο και Χανιά, όπου διαπιστώθηκε ότι 15 κατηγορούμενοι κατείχαν σε ψηφιακή μορφή «σκληρό» υλικό παιδικής πορνογραφίας.

Από την περαιτέρω ψηφιακή ανάλυση των ηλεκτρονικών ιχνών, προέκυψε ότι δύο από τους κατηγορούμενους προσέλκυαν ανήλικους, μέσω forums, chat-rooms και των social media καθώς προφασιζόμενοι ότι είναι συνομήλικοι τους, αποσπούσαν ερωτικές τους φωτογραφίες και βίντεο και στη συνέχεια τους εκβίαζαν για να συνευρεθούν ερωτικά μαζί τους. Επιπλέον διαπιστώθηκε ότι διαμοίραζαν υλικό παιδικής πορνογραφίας σε άλλους χρήστες του διαδικτύου, ενώ ακόμα επιδίωκαν την ανταλλαγή και την πώληση του υλικού αυτού.

Στο πλαίσιο της συνεργασίας με τις αντίστοιχες Υπηρεσίες της Interpol και της Europol, διαπιστώθηκε ότι πέντε από τους συλληφθέντες είχαν καταβάλλει μεγάλα χρηματικά ποσά, είτε για την αγορά ψηφιακού υλικού παιδικής πορνογραφίας, είτε για την απευθείας παρακολούθηση υλικού κακοποίησης ανηλίκων, από «κρυφή» ιστοσελίδα του εξωτερικού. Παράλληλα διαμοίραζαν αυτό το υλικό σε άλλους χρήστες του διαδικτύου, μέσω ιστοσελίδων και προγραμμάτων ανταλλαγής αρχείων.

Κυβερνοπόλεμος - Κυβερνοτρομοκρατία

Ο κυβερνοπόλεμος περιλαμβάνει πολεμικές επιθέσεις ενάντια στο στρατιωτικό σώμα ενός έθνους, παράδειγμα μιας τέτοιας επίθεσης μπορεί να είναι διακοπή κρίσιμων τηλεπικοινωνιακών διαύλων. Οι κυβερνοεπιθέσεις έχουν ως στόχο την υποδομή, είτε αυτή αφορά τις πληροφορίες γενικότερα τα αποτέλεσμα των οποίων μπορεί να είναι πιο επιζήμια για τις χώρες που διαθέτουν σημαντικές υποδομές δικτύων Η/Υ, είτε αφορά δίκτυα κοινά σε όλους τους πολίτες ενός κράτους, όπως για παράδειγμα δίκτυα ενέργειας, μεταφορών, επικοινωνιών κ.τ.λ.

Τον τελευταίο καιρό έχουν ακουστεί πολλά για το θέμα της τρομοκρατίας μέσα από το Internet και υπάρχουν αρκετοί οι οποίοι πιστεύουν πως ο πρώτος κυβερνοπόλεμος έλαβε ήδη χώρα πριν από μερικούς μήνες όταν Ινδονήσιοι "χτύπησαν" τους ιρλανδικούς servers στους οποίους στεγαζόταν το domain tp (Ανατολικό Τιμόρ).

Μέχρι σήμερα όμως καμία από αυτές τις αναφορές οι οποίες έρχονται κατά καιρούς στη δημοσιότητα δεν είχε επιβεβαιωθεί επίσημα. Έτσι, θα μπορούσαμε να πούμε πως η ακόλουθη είδηση, που μας έρχεται από την Ιαπωνία, αποτελεί την πρώτη τεκμηριωμένη προσπάθεια τρομοκρατών να διεισδύσουν σε τηλεπικοινωνιακά δίκτυα.

Σύμφωνα με την Ιαπωνική αστυνομία, τους τελευταίους μήνες πολλές κρατικές οργανώσεις και μεγάλες επιχειρήσεις της χώρας έγιναν στόχος δικτυακών επιθέσεων με άγνωστη προέλευση. Οι ερευνητές της αστυνομίας παρατήρησαν πως το κοινό χαρακτηριστικό όλων των θυμάτων ήταν κατασκευή των δικτύων τους από την ίδια εταιρεία η οποία, όπως αποδείχθηκε αργότερα, ανήκε στην παραθρησκευτική οργάνωση Aleph. Κατά την αστυνομία, η εταιρεία αυτή είχε εγκαταστήσει στα δίκτυα όλων των πελατών της security trapdoors χάρη στα οποία είχε πρόσβαση σε κάθε σημείο του δικτύου τους, όποτε το επιθυμούσε. Η ίδια εταιρεία μάλιστα είχε κατασκευάσει και ένα "ασφαλές" τηλεπικοινωνιακό δίκτυο για το ιαπωνικό υπουργείο άμυνας.

Αξίζει να σημειωθεί πως η οργάνωση Aleph δεν είναι άγνωστη στο διεθνές κοινό. Το παλαιό της όνομα ήταν Aum Shinri Kyo και οι οπαδοί της ήταν υπεύθυνοι για την επίθεση με το αέριο των νεύρων Σαρίν στο μετρό του Τόκιο πριν από μερικά χρόνια.

Φυσικά, δεν είναι μόνο οι φανατικοί θρησκευόμενοι που προσπαθούν να αποκτήσουν τον έλεγχο σημαντικών κρατικών δραστηριοτήτων μέσω του hacking. Σύμφωνα με ανακοίνωση του ρωσικού υπουργείου εσωτερικών, την οποία μετέδωσε το Associated Press, Hackers εισέβαλαν πρόσφατα στα υπολογιστικά συστήματα της Gazprom (της μεγαλύτερης ρωσικής εταιρείας πετρελαίου) και "απέκτησαν τον έλεγχο του συστήματος διαχείρισης της ροής φυσικού αερίου μέσα από τους αγωγούς της χώρας"!

Σε άλλο άρθρο μου, το οποίο θα δημοσιευθεί σύντομα στο Έθνος και αργότερα εδώ, υποστηρίζω πως ο κίνδυνος για τους hackers και τους ιούς δεν είναι τόσο μεγάλος ώστε να δικαιολογείται η παγκόσμια υστερία που καταλαμβάνει κατά καιρούς τα μέσα ενημέρωσης. Νομίζω όμως πως οι ελληνικές κρατικές αρχές μάλλον θα πρέπει να δώσουν μεγαλύτερη προσοχή στα θέματα προστασίας της πληροφοριακής υποδομής της χώρας μας. Αν μια μεγάλη βιομηχανική δύναμη όπως η Ιαπωνία αποδείχθηκε ευάλωτη, τότε παρόμοιες επιθέσεις είναι σίγουρα δυνατές παντού.

Hacking - Cracking

Το “**Hacking - Cracking**” αποτελεί μία από τις μορφές του Ηλεκτρονικού Εγκλήματος. Η μορφή αυτή έχει να κάνει με την πρόσβαση ενός έμπειρου χρήστη υπολογιστή σε ολόκληρο ή μέρος ενός συστήματος ηλεκτρονικών υπολογιστών, λογαριασμούς κλπ, χωρίς κανένα απολύτως δικαίωμα και με παράνομους σκοπούς. Τους "εγκληματίες του Κυβερνοχώρου" μπορούμε να τους διακρίνουμε σε δύο κατηγορίες ανάλογα με τον τρόπο διείσδυσης και το επιδιωκόμενο αποτέλεσμα: στους **hackers** και τους **crackers**.

Hacker ονομάζεται κάποιος που αντλεί ευχαρίστηση από τη βαθειά κατανόηση της εσωτερικής λειτουργίας ενός συστήματος, ειδικότερα ενός υπολογιστή ή δικτύου υπολογιστών, στον οποίο, όμως, δεν έχει δικαίωμα πρόσβασης. Στην πραγματικότητα, ο hacker είναι ένας έξυπνος προγραμματιστής ή άτομο με ιδιαίτερες ικανότητες στην κατανόηση και το χειρισμό υπολογιστικών συστημάτων. Η διεθνής κοινότητα των hackers πιστεύει ότι η πρόσβαση στην πληροφορία αποτελεί παγκόσμιο κοινό αγαθό και ότι είναι ηθικό καθήκον τους να μοιράζονται τις ικανότητές τους τόσο δημιουργώντας λογισμικό ανοιχτού κώδικα, όσο και διευκολύνοντας την πρόσβαση σε πληροφορίες και υπολογιστικούς πόρους, όπου αυτό είναι εφικτό. Έχουν, επίσης, την αμφιλεγόμενη πεποίθηση ότι το «σπάσιμο» και η «εξερεύνηση» ενός υπολογιστικού συστήματος, τόσο σε επίπεδο υλικού όσο και (κυρίως) λογισμικού είναι ηθικά αποδεκτή, εφόσον ο hacker δεν διαπράττει κλοπή, βανδαλισμό ή παραβίαση εμπιστευτικότητας. Οι hackers εμφανίστηκαν για πρώτη φορά στα τηλεπικοινωνιακά δρώμενα τη δεκαετία του 1970 στις Η.Π.Α.

Σε αντίθεση με το hacker, ο **cracker** είναι άτομο (ή ομάδα ατόμων) που αποπειράται να αποκτήσει πρόσβαση σε υπολογιστικό σύστημα για την οποία όχι

μόνο δε διαθέτει εξουσιοδότηση, αλλά με στόχο να το βλάψει με οποιοδήποτε τρόπο. Οι crackers είναι εξ ορισμού κακόβουλοι, αντίθετα προς τους hackers, ενώ διαθέτουν και πολλά εργαλεία για τις κακόβουλες ενέργειές τους. Η ουσία του προβλήματος του cracking δεν εντοπίζεται σε επιθέσεις που γίνονται στην αρχική ιστοσελίδα (Home Page) του δικτυακού τόπου μιας δημόσιας υπηρεσίας ή ενός μεγάλου οργανισμού, κάτι που είναι εύκολο να αντιληφθεί αλλά στις «ύπουλες» υποθέσεις. Στην τροποποίηση, δηλαδή, χωρίς να γίνει αντιληπτό σημαντικών δεδομένων που τηρούνται από δημόσιες υπηρεσίες, όπως για παράδειγμα η αλλαγή της σειράς επιτυχίας σε έναν διαγωνισμό, η πιστή αντιγραφή ολόκληρων διαδικτυακών τόπων μεγάλων εταιρειών που κάνουν πωλήσεις μέσω διαδικτύου ή και μεγάλων οργανισμών ή δημόσιων υπηρεσιών και η εξαπάτηση ανυποψίαστων χρηστών των διαδικτυακών τόπων.

Διασπορά κακόβουλων λογισμικών

Το «**κακόβουλο λογισμικό>>** αποτελεί μείζον πρόβλημα για την ασφάλεια των Πληροφοριακών Συστημάτων. Το λογισμικό χαρακτηρίζεται ως *κακόβουλο* όταν βάσει των προθέσεων του προγραμματιστή το λογισμικό που προκύπτει διαθέτει τις απαιτούμενες εντολές προκειμένου να βλάψει ένα υπολογιστικό σύστημα. Το κακόβουλο λογισμικό μπορεί να χωριστεί σε δύο κατηγορίες. Σε αυτό που χρειάζεται ένα πρόγραμμα *«ξενιστή»* και σε αυτό που δεν χρειάζεται *«ξενιστή»* και μπορεί να εκτελεστεί από μόνο του όπως κάθε άλλο πρόγραμμα. Επιπλέον το κακόβουλο λογισμικό μπορεί να διαχωριστεί και με διαφορετικό τρόπο σε δύο άλλες κατηγορίες. Το *ιομορφικό λογισμικό* και το *μη ιομορφικό λογισμικό*. Στο ιομορφικό λογισμικό ανήκουν τα προγράμματα που μπορούν και αναπαράγονται από μόνα τους και στο μη ιομορφικό λογισμικό τα προγράμματα που δεν αναπαράγονται χωρίς την ανάμειξη του ανθρώπινου παράγοντα.

Είδη κακόβουλου λογισμικού

Ιός (Virus): είναι κακόβουλο λογισμικό το οποίο έχει τη δυνατότητα να εξαπλώνεται εύκολα σε χρήσιμα προγράμματα ενός ξένου υπολογιστή με αποτέλεσμα να βλάψει χρήσιμα αρχεία ενός χρήστη. Η μετάδοσή του σε άλλους υπολογιστές μπορεί να γίνει πολύ εύκολα με τη βοήθεια κάποιας εξωτερικής συσκευής όπως μια φορητή μνήμη USB ή ένας εξωτερικός σκληρός δίσκος. Ένα στοιχείο που διαφοροποιεί τους ιούς από τα άλλα προγράμματα είναι ότι μπορεί να μεταδοθεί οπουδήποτε έχει τη δυνατότητα. Τέλος οι επιπτώσεις που μπορεί να έχει ένας ιός είναι από το να διαγράψει κάποια δεδομένα έως και να οδηγήσει στην κατάρρευση ολόκληρου του συστήματος.

Δούρειος ίππος (Trojan): είναι κακόβουλο λογισμικό που χρησιμοποιεί το στοιχείο της παραπλάνησης. Λογισμικό αυτού του είδους παριστάνει ότι είναι χρήσιμο για τον υπολογιστή αλλά στην πραγματικότητα μέσα από αυτό κάποιοι εγκληματίες καταφέρνουν να κλέψουν σημαντικά αρχεία ή να αποκτήσουν τον έλεγχο του συστήματος. Τις περισσότερες φορές το συγκεκριμένο λογισμικό δεν έχει στόχο τη μόλυνση του υπολογιστή, δηλαδή δεν αναπαράγεται, και για αυτό τα προγράμματα αυτά δεν χαρακτηρίζονται και επίσημα ως ιοί.

Σκουλήκι (Worm): είναι κακόβουλο λογισμικό το οποίο μπορεί να μεταδοθεί άμεσα με τη χρήση κάποιας δικτυακής υποδομής όπως τα τοπικά δίκτυα ή μέσω κάποιου μηνύματος e-mail. Η ικανότητά του να πολλαπλασιάζεται αυτόματα στο σύστημα στο οποίο βρίσκεται του δίνει τη δυνατότητα να αποστέλλει προσωπικά δεδομένα ή κωδικούς πρόσβασης, ώστε αυτός που θα κάνει την επίθεση να έχει πρόσβαση στη σύνδεση δικτύου. Τέλος, ένα άλλο αρνητικό χαρακτηριστικό είναι ότι επιβαρύνουν το δίκτυο, φορτώνοντάς το με άχρηστη δραστηριότητα.

Rootkit: είναι λογισμικό το οποίο μπορεί να ανήκει πολύ εύκολα σε οποιαδήποτε από τις παραπάνω κατηγορίες. Αυτό το λογισμικό έχει την ιδιαιτερότητα να κρύβει κάποια κακόβουλα προγράμματα ώστε να μη γίνονται ορατά από το λογισμικό ασφαλείας. Αυτά τα προγράμματα κάποιες φορές λειτουργούν προστατευτικά για τους χάκερ διαγράφοντας τις πληροφορίες του εισβολέα.

ΑΠΑΤΕΣ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ

Οι συνηθέστερες μορφές διαδικτυακής απάτης είναι οι ακόλουθες:

α) Χρεώσεις της πιστωτικής κάρτας πολιτών μέσω του διαδικτύου για αγορές, οι οποίες δεν πραγματοποιήθηκαν από τους ίδιους.

• Στις περιπτώσεις αυτές, κάποιος κακόβουλος χρήστης του διαδικτύου δημιουργεί μια πλασματική ιστοσελίδα και με αυτόν τον τρόπο καταφέρνει να συγκεντρώνει στοιχεία κι αριθμούς πιστωτικών καρτών χρηστών του διαδικτύου, οι οποίοι έχοντας εξαπατηθεί, νομίζουν ότι πρόκειται για κάποιο διαδικτυακό κατάστημα και κάνουν τις αγορές τους.

• Επιπλέον, αρκετές είναι οι περιπτώσεις όπου επιτήδειοι καταφέρνουν να αποκτούν φυσική πρόσβαση στα στοιχεία πιστωτικών καρτών πολιτών τα οποία εν συνεχεία χρησιμοποιούν σε διαδικτυακές αγορές, καθώς για τις αγορές αυτές δεν είναι απαραίτητη η φυσική κατοχή της πιστωτικής κάρτας, παρά μόνο τα στοιχεία αυτής.

• Επιπροσθέτως, σε αρκετές περιπτώσεις οι χρήστες του διαδικτύου δίνουν οι ίδιοι άθελά τους τα στοιχεία σε κακόβουλους χρήστες του διαδικτύου (phishing). Ειδικότερα, ο ανυποψίαστος πολίτης λαμβάνει μήνυμα ηλεκτρονικού ταχυδρομείου από Πιστωτικό Ίδρυμα, στο οποίο τηρεί λογαριασμό, με το οποίο του ζητείται να συμπληρώσει τα στοιχεία του (ονοματεπώνυμο, αριθμό λογαριασμού και πιστωτικής κάρτας κλπ.), για λόγους πχ. ενημέρωσης των αρχείων της τράπεζας. Το μήνυμα, μέσω υπερσυνδέσμου, τους οδηγεί σε μια πλασματική ιστοσελίδα της τράπεζας, με αποτέλεσμα ο πολίτης να πείθεται και να χορηγεί τα επίμαχα στοιχεία.

β) Διακίνηση μηνυμάτων με απατηλό περιεχόμενο, που επιδιώκουν την εξαπάτηση ανυποψίαστων πολιτών.

• Ειδικότερα, ο τρόπος δράσης των κακόβουλων δραστών στην εν λόγω μορφή απάτης, που περιγράφεται υπό τον όρο «Ισπανικό Λόττο», είναι η μαζική αποστολή μηνυμάτων ηλεκτρονικής αλληλογραφίας σε τυχαίους χρήστες του διαδικτύου, με τα οποία τους ενημερώνουν ότι έχουν κερδίσει ένα μεγάλο χρηματικό ποσό της τάξεως των εκατομμυρίων δολαρίων σε ηλεκτρονική κλήρωση του διαδικτύου.

• Οι δημιουργοί των μηνυμάτων αυτών, για να γίνουν πιστευτοί, χρησιμοποιούν παραπλήσια ονόματα μεγάλων

εταιρειών (πχ. Microsoft , Yahoo κλπ) και συνοδεύουν τα μηνύματα που αποστέλλουν με πλαστά πιστοποιητικά όσον αφορά στην υποτιθέμενη ηλεκτρονική κλήρωση.

• Η απάτη έγκειται στο γεγονός ότι ζητούν από τους υποτιθέμενους νικητές την προπληρωμή κάποιων φόρων ή/και εξόδων εκταμίευσης των χρημάτων, ποσό που συνήθως είναι της τάξης των μερικών χιλιάδων δολαρίων.

γ) «Απάτες 419» ή «Νιγηριανές Απάτες»

• Στις περιπτώσεις αυτές αποστέλλονται, μηνύματα σε τυχαίους χρήστες του διαδικτύου, με τα οποία τους πληροφορούν ότι κάποιος κάτοχος ιδιαίτερα μεγάλης περιουσίας έχει αποβιώσει και είτε δεν υφίσταται κανείς κληρονόμος και ο παραλήπτης του μηνύματος έχει επιλεγεί ούτως ώστε να κληρονομήσει αυτός την περιουσία, είτε για να καταστεί δυνατό να αποδεσμευτεί η περιουσία, χρειάζεται αυτή να μεταφερθεί σε τραπεζικό λογαριασμό του εξωτερικού και ο παραλήπτης του μηνύματος ενημερώνεται ότι εάν διαθέσει το λογαριασμό του, θα αποκτήσει κάποιο ποσοστό επί της περιουσίας αυτής.

• Σε άλλες περιπτώσεις, άτομα από τη Νιγηρία αναζητούν τη βοήθεια επιχειρηματιών ή ελεύθερων επαγγελματιών με σκοπό να μεταφέρουν τα κεφάλαιά τους, τα οποία προέρχονται από εγκληματικές πράξεις (λαθρεμπόριο,

απάτες, δωροδοκία κλπ.), υποσχόμενοι για τη συνεργασία

αυτή υψηλό ποσοστό αμοιβής. Για το σκοπό αυτό, κάνουν

χρήση τίτλων επίσημων φορέων της χώρας τους

(Υπουργεία, Κεντρική Τράπεζα, Εθνική Εταιρεία Πετρελαίων Νιγηρίας κλπ.),

χρησιμοποιούν τίτλους κυβερνητικών ή στρατιωτικών παραγόντων με υπαρκτά

και ψεύτικα ονόματα ή προφασίζονται σχέση τους με

«διάσημα» ή «σημαντικά» πρόσωπα.

• Η απάτη έγκειται στο γεγονός ότι οι αποστολείς των μηνυμάτων

ζητούν από τους παραλήπτες να τους αποστείλουν τα προσωπικά τους στοιχεία,

τα στοιχεία των τραπεζικού λογαριασμού και πιστωτικής κάρτας κλπ. Προκειμένου επιτευχθεί η συνεργασία τους και η αποκόμιση των χρηματικών ποσών.

ΘΕΜΑ ΟΜΑΔΑΣ

«ΔΙΩΞΗ – ΣΥΝΕΠΕΙΕΣ – ΚΙΝΔΥΝΟΙ – ΠΟΙΝΕΣ – ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ ΑΠΟ ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ»

ΣΥΜΜΕΤΕΧΟΝΤΕΣ: Π. Ε.

Τ. Μ.

Τ. Ε.

Τ. Δ.

Χ. Α.

ΟΝΟΜΑ ΟΜΑΔΑΣ: eγκληματίε$

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Είναι γεγονός αναμφισβήτητο ότι οι ηλεκτρονικοί υπολογιστές και το διαδίκτυο αποτελούν πλέον ένα από τα πιο σπουδαία επιτεύγματα της τεχνολογίας. Έχουν φέρει τη δική τους επανάσταση στη ανθρωπινή καθημερινότητα, στην επιστήμη, στην εκπαίδευση. Οι άπειρες δυνατότητες που προσφέρουν είναι ο λόγος για τη συνεχή προσπάθεια του ανθρώπου να ανακαλύψει, να εξελίξει, και να εκμεταλλευτεί περαιτέρω δυνατότητες. Ο ηλεκτρονικός υπολογιστής και το διαδίκτυο είναι κάτι πολύ περισσότερο από ένα βοήθημα για τον άνθρωπο αφού σε πολλές περιπτώσεις εκεί εκθέτονται στοιχειά προσωπικών δεδομένων ενός πολίτη ή στοιχειά που οδηγούν πολύ εύκολα στον εντοπισμό πληροφοριών αυτού. Ελλοχεύει λοιπόν ο κίνδυνος κάθε είδους απατής από επίσης καλούς γνώστες της τεχνολογίας που θέτουν αυτή ως μέσο πραγματοποίησης παρανομών πράξεων και έτσι η τεχνολογία με αυτό το χειρισμό αποτελεί «όπλο» στραμμένο στον πολίτη - χρήστη.

Οι δυνατότητες δίωξης από τις αρμόδιες αρχές δεν αποτελούν εμπόδιο αυτής της μορφής εγκλήματος αφού, οι εν λόγο δυνατότητες είναι περιορισμένες λόγω έλλειψης εμπειρίας και επαρκούς εκπαίδευσης στο τομέα αυτό ενώ το σχετικό νομοθετικό πλαίσιο είναι ασαφές.

Το 1994 οι Forester και Morrison όρισαν το Ηλεκτρονικό Έγκλημα σαν «μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως κυριότερο μέσο τέλεσης της». Ένας τέτοιος ορισμός θα μπορούσε να χαρακτηριστεί υπεραπλουστευμένος. Θα χαρακτηρίζαμε το Ηλεκτρονικό Έγκλημα σαν μια νέα μορφή εγκλήματος με μοναδικό μέσο εκτέλεσης την ιδία τη χρήση των ηλεκτρονικών υπολογιστών. Πρόκειται για μια παραλλαγή των ήδη υπαρχόντων εγκλημάτων με μοναδική διαφορά την εκτέλεση αυτών μέσω ενός υπολογιστή. Στην ελληνική γλώσσα οι οροί που χρησιμοποιούνται είναι ηλεκτρονικό έγκλημα, δικτυακό έγκλημα και έγκλημα του κυβερνοχώρου.

Βασική προϋπόθεση στο ηλεκτρονικό έγκλημα είναι η ύπαρξη ενός ηλεκτρονικού υπολογιστή. Ο υπολογιστής μπορεί να αποτελεί ένα βοηθητικό μέσο για την διάπραξη του εγκλήματος ή να είναι το ίδιο το μέσο με το όποιο θα εκτελεστεί κάποια επίθεση ενώ φυσικά μπορεί να αποτελέσει και το ίδιο το «θύμα» της επίθεσης.

ΚΙΝΔΥΝΟΙ

Το ερώτημα που τίθεται είναι κατά πόσο ασφαλές μπορεί να είναι το διαδίκτυο. Πόσο ασφαλή είναι τα δεδομένα που καταθέτουμε σε αυτό;

Αναμφισβήτητα το διαδίκτυο έχει γίνει πολύτιμος σύμμαχος για τους εγκληματίες, οι όποιοι επιδιώκουν με κάθε τρόπο την απόσπαση χρηματικών ποσών από ανυποψίαστα θύματα.

- ✓ Ένας τέτοιος εύκολος και ανέξοδος τρόπος είναι η αποστολή e-mail. Ο εγκληματίας αποστέλλει μαζικά e-mails σε θύματα με περιεχόμενο παραπλανητικό αλλά αρκετά έξυπνο και καλά οργανωμένο. Ο επιτιθέμενος συντάσσει ένα e-mail παράκλησης στο όποιο αναφέρει πως προέρχεται από αφρικανική χωρά κι έχει σκοπό να μετακινηθεί στη χωρά του θύματος προφασιζόμενος αιτίες που θα συγκινήσουν το θύμα (πόλεμος, φυσικές καταστροφές κτλ). Ζητάει λοιπόν από το θύμα να ανοίξει ένα τραπεζικό λογαριασμό με συνδικαιούχο τον ίδιο υποσχόμενος πως όταν η διαδικασία μεταφοράς χρημάτων ολοκληρωθεί, θα ανταμείψει το θύμα. Ο σκοπός είναι να αποσπάσει το χρηματικό πόσο που κατέθεσε το θύμα για τα έξοδα κίνησης και ύστερα να καταργήσει το λογαριασμό.
- ✓ Τα εγκλήματα με πιστωτικές κάρτες αυξηθήκαν με τη βελτίωση και εξάπλωση του ηλεκτρονικού εμπορίου, ιδιαίτερα τώρα που αρκεί ο τραπεζικός λογαριασμός ώστε ο χρήστης να μπορεί να διεκπεραιώσει κάθε είδους εμπορική συναλλαγή εξ αποστάσεως. Επομένως έχουμε την διάθεση αριθμών τραπεζικού λογαριασμού στο διαδίκτυο, διαδικασία όχι ιδιαίτερα δύσκολη, αφού με την τεχνολογία «web sniffer» παρακολουθείται η μετάδοση δεδομένων και ανακτώνται αυτόματα οι αριθμοί αυτοί.
- ✓ Κλοπή ταυτότητας Από τα σοβαρότερα εγκλήματα θα μπορούσε να θεωρηθεί η κλοπή της ταυτότητας, η οποία με τη βοήθεια του δικτύου μπορεί να γίνει ακόμα πιο επικίνδυνη. Αρχικά ο επιτιθέμενος συγκεντρώνει πληροφορίες του υποψήφιου θύματος με όποιο τρόπο μπορεί, είτε κλέβοντας μια τσάντα που περιείχε την ταυτότητα, είτε κλέβοντας την αλληλογραφία (π.χ. λογαριασμούς) που παρέχει προσωπικά στοιχειά ή ακόμα και εισβάλοντας σε βάσεις δεδομένων όπου φυλάσσονται προσωπικά δεδομένα. Μετά την ανάκτηση των πληροφοριών προβαίνει στη δημιουργία πλαστής ταυτότητας, στη δημιουργία τραπεζικών λογαριασμών και πιστωτικών καρτών.
- ✓ Το ξέπλυμα χρήματος είναι η διαδικασία απόκρυψης χρημάτων που περιήλθαν στην κατοχή κάποιου με παράνομες διαδικασίες. Στην περίπτωση αυτή ο εγκληματίας επιχειρεί τη μετατροπή των χρημάτων σε μια μορφή λιγότερο ύποπτη, στη συνέχεια το χρήμα διαχωρίζεται από την παράνομη πηγή του και διαχέεται σε διαφορές οικονομικές συναλλαγές με σκοπό την απόκρυψη του και τέλος ολοκληρώνεται η διαδικασία μετατροπής του παράνομου χρήματος σε ένα νόμιμο εισόδημα. Το

διαδίκτυο κρατεί την ανωνυμία του πελάτη κι έτσι είναι δύσκολο να εντοπιστούν οι κάτοχοι.

- ✓ Διακίνηση πορνογραφικού υλικού Η δημιουργία και η διακίνηση πορνογραφικού υλικού είναι μια διαδικασία που προϋπήρχε και το διαδίκτυο κάνει πιο εύκολη την εξάπλωσή του. Η διαδικασία αυτή είναι παράνομη και είναι δύσκολος ο εντοπισμός της πηγής. Το υλικό αυτό μπορεί να είναι είτε σε μορφή φωτογραφιών, είτε σε μορφή βίντεο και η ανάκτηση του είναι εύκολη από οποιονδήποτε κάτοχο internet. Τα παιδιά μπορούν να εκτεθούν σε ακατάλληλο πορνογραφικό ή προσβλητικό περιεχόμενο.
- ✓ Η δικτυακή τρομοκρατία είναι ένα είδος τρομοκρατίας που έχει σαν μοναδικό εργαλείο εκτέλεσης το διαδίκτυο. Στις μέρες μας συναντάμε αυτή τη μορφή τρομοκρατίας, η οποία έχει τραγικά αποτελέσματα. Το δίκτυο βοηθάει στην άριστη επικοινωνία και οργάνωση των επιθέσεων, όχι μόνο επειδή είναι οικονομικό αλλά επειδή καθιστά αδύνατο τον εντοπισμό της τοποθεσίας.
- ✓ Η παρενόχληση σαφώς προϋπήρχε των υπολογιστικών συστημάτων. Το δίκτυο όμως και η αποστολή e-mail διευκολύνει σε μεγάλο βαθμό τη διαδικασία αυτή. Τα e-mails αποστέλλονται μαζικά με οικονομικό τρόπο και κυρίως ο εντοπισμός της πηγής είναι αδύνατος. Υπάρχει η άμεση παρενόχληση στην οποία το θύμα παίρνει απευθείας το μήνυμα με το απειλητικό ή προσβλητικό περιεχόμενο και η έμμεση παρενόχληση κατά την οποία το μήνυμα με το προσβλητικό ή απειλητικό περιεχόμενο αποστέλλεται σε τυχαίους παραλήπτες.

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ

Προληπτικά μέτρα προστασίας πρέπει πάντα να λαμβάνονται από τους χρήστες διαδικτύου, διότι οι κίνδυνοι από ιούς, παράνομες εισβολές και υπερβολικές χρεώσεις σε τηλεφωνικούς λογαριασμούς είναι συχνότατοι.

Εφόσον το επιθυμεί, ο χρήστης έχει δικαίωμα να χρησιμοποιεί υπηρεσίες ανωνυμοποιημένης πρόσβασης, ώστε τα ίχνη της δικτυακής του παρουσίας να μη μπορούν να χρησιμοποιηθούν για σκοπό που δεν έχει επιλέξει. Σήμερα οι περισσότεροι δικτυακοί τόποι παρέχουν ενημέρωση σχετικά με τα προσωπικά δεδομένα που συλλέγουν και επεξεργάζονται. Η ενημέρωση αυτή είναι ταυτόχρονα υποχρέωση των υπευθύνων των δικτυακών τόπων αλλά και δικό μας δικαίωμα. Επίσης, οφείλει να προτιμά αναγνωρισμένες και επώνυμες ηλεκτρονικές ιστοσελίδες αντί να συνδέεται με άγνωστες και ύποπτης προέλευσης. Συνιστάται επίσης στον κάθε χρήστη να εγκαθιστά στον προσωπικό υπολογιστή του λογισμικό προστασίας από ιούς (antivirus, firewalls). Απαγορεύεται ρητά στον χρήστη να παρέχει προσωπικές πληροφορίες εάν του ζητηθούν για οποιονδήποτε λόγο. Συνιστάται ακόμα στον χρήστη να μην απαντά σε μηνύματα άγνωστης

προέλευσης, αφού το πιθανότερο είναι αυτά να στοχεύουν στην εξαπάτησή του. Ομοίως, πρέπει να αποφεύγει να ανοίγει συνημμένα αρχεία σε μηνύματα ηλεκτρονικού ταχυδρομείου προερχόμενα από άγνωστο αποστολέα, διότι είναι πιθανό να περιέχουν ιούς. Οι γονείς των ανήλικων καταναλωτών έχουν επίσης την υποχρέωση εποπτείας και επιμέλειας των τέκνων τους, τα οποία δεν πρέπει να κάνουν ανεξέλεγκτη χρήση του υπολογιστή, που πρέπει να είναι εγκατεστημένος σε ελεγχόμενο χώρο. Χρήσιμη είναι επίσης η εγκατάσταση ειδικού λογισμικού, ως φίλτρου ελεγχόμενης πρόσβασης των παιδιών σε ιστοσελίδες που ενδεχομένως περιέχουν χυδαίες λέξεις και επιβλαβές και παράνομο περιεχόμενο για τους ανηλίκους (όπως ρατσισμός, τρομοκρατία, πορνογραφία) και συμμετοχής σε ομάδες συζήτησης (chatrooms) με άγνωστα άτομα καλυπτόμενα υπό ψευδώνυμο.

- ✓ Οι κωδικοί πρόσβασης λόγω της απλότητάς τους έχουν γίνει πλέον από τους πιο διαδεδομένους τρόπους προστασίας δεδομένων, αφού αρκεί μόνο η εισαγωγή του username και του κωδικού που είναι ξεχωριστοί κάθε φορά για τον καθένα. Είναι εύκολο να απομνημονευτούν αλλά και να αλλαχτούν από τον ίδιο τον χρηστή όταν αυτό είναι απαραίτητο. Όπως όμως αναφέρθηκε και προηγουμένως ακόμα και αυτή η μέθοδος είναι αμφιλεγόμενη αφού η αποκάλυψη ενός κωδικού πρόσβασης πλέον είναι πολύ εύκολη και απλή διαδικασία. Αρκεί μονό η εφαρμογή απλών εργαλείων λογισμικού. Σε πολλά συστήματα από αυτά που χρησιμοποιεί ο χρηστής οι κωδικοί πρόσβασης καθορίζονται από τον ίδιο και μπορούν να αντικατασταθούν κάθε στιγμή. Συνήθως ο χρήστης επιλεγεί κωδικούς που είναι εύκολο να απομνημονευτούν και που σημαίνουν κάτι για αυτόν όπως είναι η ημερομηνία γέννησης, το τηλέφωνό του κ.α. όμως αυτούς τους κωδικούς είναι εύκολο για κάποιον να τους μαντέψει. Σε κάποιες άλλες περιπτώσεις οι κωδικοί πρόσβασης δίνονται από τους ίδιους τους διαχειριστές του συστήματος και αυτό καθιστά πιο δύσκολη την απόσπασή τους από άλλους. Επιπλέον η παρακολούθηση των πακέτων που διακινούνται στο δίκτυο μπορεί να έχει σαν αποτέλεσμα την ανάκτηση κωδικών πρόσβασης. Σε περίπτωση που το αρχείο δεν φυλάσσεται επαρκώς ο εισβολέας μπορεί να ανακτήσει τον κωδικό αυτό.

- ✓ Antivirus. Οι ιοί είναι η πιο γνωστή και διαδεδομένη μορφή επίθεσης. Υπάρχουν ιοί που μπορούν να προκαλέσουν μεγάλη και ανεπανόρθωτη ζημία, αλλά υπάρχουν και ιοί που είναι λιγότερο ζημιογόνοι. Σε κάθε περίπτωση η εγκατάσταση λογισμικού ασφάλειας είναι απαραίτητη σε κάθε υπολογιστικό σύστημα. Η δημιουργία του λογισμικού antivirus έπεται της δημιουργίας κάθε νέου ιού έτσι ώστε να μπορέσει να προσφέρει την ανάλογη ασφάλεια. Οι ιοί δημιουργούνται και μεταδίδονται μαζικά καθημερινά απειλώντας τα υπολογιστικά συστήματα. Ο χρηστής κατά την εγκατάσταση του αντιβιοτικού έχει μια βασική προστασία. Όμως, όπως ήδη

ειπώθηκε, δημιουργούνται χιλιάδες ιοί καθημερινά οι οποίοι απειλούν τα υπολογιστικά συστήματα και για αυτό οι εταιρείες λογισμικού δίνουν τη δυνατότητα στο χρηστή για on-line ενημέρωση της βάσης δεδομένων του προγράμματος με τους νέους ιούς. Με την εμφάνιση ενός ιού ενημερώνεται και η βάση δεδομένων από τις εταιρίες σε ένα αρκετά γρήγορο χρονικό διάστημα.

- ✓ Firewalls. Με τον όρο firewall εννοείται ένα τοίχος προστασίας. Στην επιστήμη των υπολογιστών σαν firewall προσδιορίζεται μια συσκευή ή εργαλείο λογισμικού που παρακολουθεί και φιλτράρει τα πακέτα που επιχειρούν να εισέλθουν ή να εξέλθουν από ένα εσωτερικό προστατευμένο δίκτυο ή υπολογιστή. Ουσιαστικά είναι ένα τείχος που προστατεύει ένα ασφαλές εσωτερικό «χώρο» από ένα μη ασφαλές εξωτερικό, όπως είναι το διαδίκτυο. Δυο είναι οι βασικές λειτουργίες ασφάλειας που επιτελούν τα firewalls: Φιλτράρισμα πακέτων (packet filtering), όπου με τη διαδικασία αυτή επιτρέπεται ή απαγορεύεται αντίστοιχα η κίνηση των πακέτων που διακινούνται στο δίκτυο σύμφωνα με την πολιτική ασφάλειας του οργανισμού.
  Πύλες εφαρμογών (application proxy gateways), όπου προσφέρονται υπηρεσίες στους εσωτερικούς χρήστες και ταυτόχρονα προστατεύονται οι hosts από εξωτερικές απειλές. Η λειτουργία που θα επιτελέσει το firewall έχει να κάνει με την πολιτική ασφάλειας που ακολουθεί ο οργανισμός. Σήμερα που το ηλεκτρονικό έγκλημα έχει πάρει τεράστιες διαστάσεις, η χρήση των firewalls είναι επιτακτική ανάγκη. Η τεχνολογία στον τομέα αυτό βελτιώνεται συνεχώς παρέχοντας στο χρήστη μεγαλύτερη ασφάλεια και προστασία, προσφέροντας firewalls ικανά να επιτελούν πολλές εργασίες ταυτόχρονα.

ΔΙΩΞΗ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας, στο πλαίσιο της προληπτικής της δράσης έχει σκοπό να ενημερώνει τους πολίτες για την πρόληψη και αποφυγή εξαπάτησής τους από τις συνεχώς μεταλλασσόμενες μορφές απάτης, μέσω του διαδικτύου.

Συγκεκριμένα, η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος ενημερώνει για διάφορες και πολλές **περιπτώσεις εξαπάτησης** και συνακόλουθης εκβίασης πολιτών, από επιτήδειους που μετέρχονται συγκεκριμένης μεθοδολογίας.

Πιο αναλυτικά άγνωστα άτομα πραγματοποιούν τηλεφωνικές κλήσεις σε ανυποψίαστους πολίτες και τους ενημερώνουν ψευδώς ότι κάποιος οικείος τους ή συγγενικό τους πρόσωπο αντιμετωπίζει σοβαρό πρόβλημα υγείας.

Μάλιστα για να προσδώσουν την απαραίτητη αληθοφάνεια παρουσιάζονται ως γιατροί και προτρέπουν τους πολίτες να πραγματοποιήσουν βιντεοκλήση, μέσω διαδικτύου, αφαιρώντας τα ενδύματα τους, προκειμένου να «εξεταστούν» από τους δήθεν γιατρούς, ώστε να «αντιμετωπισθεί» η πάθηση του οικείου τους.

Στη συνέχεια και αφού προηγουμένως έχουν καταγράψει το οπτικοακουστικό υλικό, προβαίνουν σε εκβίαση των θυμάτων τους, απαιτώντας να τους καταβάλουν χρηματικά ποσά, για να μην δημοσιεύσουν στο διαδίκτυο το υλικό της καταγραφής

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος παρακαλεί τους πολίτες να είναι ιδιαίτερα προσεκτικοί, για την αποφυγή πιθανής εξαπάτησης τους και προστασίας των προσωπικών τους δεδομένων και συστήνει:

Να μην ανταποκρίνονται και να μην πείθονται σε ανάλογες προτροπές .

Να είναι ιδιαίτερα προσεκτικοί κατά την πραγματοποίηση βιντεοκλήσεων με άγνωστα άτομα μέσω του διαδικτύου.

Να μην ανταλλάσσουν ψηφιακό υλικό προσωπικών δεδομένων με αγνώστους στο διαδίκτυο, καθώς κινδυνεύει η ασφάλειά τους.

Συνάμα αυτοί που ασκούν εκφοβισμό, χρησιμοποιούν τις νέες τεχνολογίες για να παρενοχλήσουν, να απειλήσουν, να εκφοβίσουν, να εκβιάσουν, να δυσφημήσουν και, σε μερικές περιπτώσεις, να υποδυθούν τρίτους ή να υποκλέψουν την ταυτότητά τους. Μερικές από τις πιο κοινές μεθόδους είναι οι εξής:

- Αποστολή κειμένων, e-mail, ή άμεσων μηνυμάτων με προσβλητικό περιεχόμενο (σε instant messengers ή chatrooms).

- Η κακόβουλη δημοσίευση φωτογραφιών σε μέσα κοινωνικής δικτύωσης (social networks), ιστολόγια (blogs) ή άλλες ιστοσελίδες με μοναδικό σκοπό την παρενόχληση.

- Διάδοση φημών και ψευδών γεγονότων με σκοπό την δυσφήμιση σε τρίτους σε μέσα κοινωνικής δικτύωσης, ιστολόγια, ιστοσελίδες κ.λπ.

- Ανώνυμες κλήσεις και μηνύματα με σκοπό τον φόβο και την ταραχή.
- Χρήση του ονόματος ξένου χρήστη με σκοπό τη διάδοση φημών για κάποιον τρίτο (κλοπή ταυτότητας).

- Η δημιουργία ιστοσελίδων που στοχοποιούν συγκεκριμένα άτομα καλώντας άλλους να δημοσιεύσουν μηνύματα μίσους.

- Η αποστολή ειδικών προγραμμάτων trojan horses (δούρειοι ίπποι) σκόπιμα για να δημιουργήσουν πρόβλημα, με την υποκλοπή κωδικών.

- Εκφοβισμός στη διάρκεια ενός διαδραστικού online παιχνιδιού.

ΕΠΙΠΤΩΣΕΙΣ ΣΤΗΝ ΠΟΛΙΤΙΚΗ, ΣΤΗΝ ΚΟΙΝΩΝΙΑ

-Στις μέρες μας είναι πλέον ευρέως γνωστές οι ηλεκτρονικές επιθέσεις σε ιστοσελίδες διαφόρων υπουργείων, σε προσωπικά blogs των υπουργών και άλλων πολιτικών, σε ηλεκτρονικούς λογαριασμούς αυτών, στα e-mail τους. Για ποικίλους λόγους όπως, προειδοποιήσεις, εκφοβισμούς, αντιδράσεις, διαμαρτυρίες ομάδες από hackers συχνά επιτίθενται σε βάρος αυτών των υπηρεσιών προκειμένου να πετύχουν το σκοπό τους και να προξενήσουν οικονομικές και κοινωνικές καταστροφές. Συχνά διαπομπεύουν πολιτικά πρόσωπα δημοσιεύοντας προσωπικές συζητήσεις, συνομιλίες, πλάνα εργασιών και σε άλλες περιπτώσεις "ασχολούνται" με τραπεζικούς λογαριασμούς και με περισσότερο προσωπικά θέματα. Οι παραπάνω ενέργειες αφορούν το hacktivism, μια μορφή ηλεκτρονικής δράσης και έκφρασης, που εμφανίζεται παράλληλα με τις κοινές που γνωρίζουμε (στους δρόμους, σε πορείες, κλπ.). Πέραν αυτών, κακόβουλες ενέργειες μπορούν να σημειωθούν σε δημόσιες υπηρεσίες όπως στην υγεία, για παράδειγμα, ή σε ιδιωτικές τράπεζες, γεγονός που δημιουργεί πολλά προβλήματα στη κοινωνία αλλά και στα ίδια τα άτομα που αδυναμούν να χρησιμοποιήσουν τις παραπάνω

υπηρεσίες όταν τις χρειάζονται. Αν επίσης οι επιθέσεις είναι σοβαρές και μεγάλης διάρκειας επιφέρουν καταστροφές μεγάλης αξίας και στη κοινωνία (αδυναμία χρήσης δημόσιας ηλεκτρονικής υπηρεσίας). Ένας ακόμη παράγοντας του hacking που προκαλεί κατά κάποιο τρόπο προβλήματα στη κοινωνία αλλά κυρίως σε συγκεκριμένα άτομα και οργανισμούς είναι η ηλεκτρονική πειρατεία. Η δυνατότητα παράνομης αντιγραφής και δωρεάν χρήσης πολυμέσων όπως μουσική, ταινίες, φωτογραφίες, λογισμικά, που σε κανονικές συνθήκες έπρεπε να αγοράζονται, έχει ως αποτέλεσμα την εμφάνιση οικονομικών θεμάτων τόσο για τους δημιουργούς όσο και για το ευρύτερο κοινό. Όσες προσπάθειες και να πραγματοποιούνται για την εξάλειψη της ηλεκτρονικής πειρατείας, με την εφαρμογή πιο αποτελεσματικών τρόπων προστασίας, υπάρχουν άτομα που είναι ικανά να τις παραβιάσουν.

ΕΠΙΠΤΩΣΕΙΣ ΣΤΙΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

- Μια επίθεση σε κάποιον οργανισμό που διαθέτει servers ή ηλεκτρονικές υπηρεσίες μπορεί να δημιουργήσει ζημία υψηλού κόστους. Οι πιθανές καταστροφές πολύτιμων αρχείων κατά την επίθεση επηρεάζουν σημαντικά τη λειτουργία της εταιρείας. Η υποκλοπή δεδομένων από μια βάση σε μια ιστοσελίδα και οι πληροφορίες που μπορεί να περιέχουν, τόσο για τους εργαζομένους όσο και για τους πελάτες, επιδρούν αρνητικά στην επιχείρηση. Όπως αναφέρθηκε στις μεθόδους επιθέσεων, κατά τη διάρκεια μιας DoS ή DDoS επίθεσης (αλλά και αργότερα) οι επιτιθέμενες υπηρεσίες δεν είναι διαθέσιμες στους πελάτες. Αυτό είναι πολύ σημαντικό αφού μπορεί να τους στρέψει σε άλλες, ίδιου τύπου, που να έχουν την ικανότητα να λειτουργούν συνεχώς και να προστατεύουν σε μεγαλύτερο βαθμό τα προσωπικά τους δεδομένα (account information). Χάνεται έτσι η φήμη της εταιρείας. Ακόμη, μετά από μία πιθανή επίθεση δαπανώνται χρήματα για την βελτίωση της ασφάλειας καθώς και για τις υπερωρίες που γίνονται συνήθως από το εργατικό προσωπικό. Το 57% των επιχειρήσεων στις Ηνωμένες Πολιτείες αναφέρουν ότι "χάνουν" περισσότερα χρήματα λόγω του ηλεκτρονικού εγκλήματος παρά λόγω του κοινού. Πολλές φορές οι ίδιες οι επιχειρήσεις διαθέτουν "κρυφές" ομάδες από hackers με τους οποίους είτε προστατεύονται από ηλεκτρονικές απειλές είτε επιτίθενται στους ανταγωνιστές τους και κατα συνέπεια δημιουργούν προβλήματα και καταστροφές σε αυτούς κερδίζοντας ενδεχομένως χρήματα και πελάτες.

ΠΟΙΝΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Ο Ν. 1805/88, αφορά τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές (computer crimes) και στο βαθμό που τα προβλεπόμενα εγκλήματα διαπράττονται και σε περιβάλλον Διαδικτύου (Internet), τότε εφαρμόζονται τα παρακάτω άρθρα.

Στην ελληνική νομοθεσία, ωστόσο, δεν υπάρχει νόμος που να αναφέρεται αποκλειστικά σε θέματα Διαδικτύου και να ρυθμίζει τη συμπεριφορά των χρηστών του Διαδικτύου από άποψη Ποινικού Δικαίου. Ως εκ τούτου, η Ελλάδα συνεργάζεται με τα άλλα κράτη της Ευρωπαϊκής Ένωσης, του Συμβουλίου της Ευρώπης, καθώς και άλλων διεθνών οργανισμών, για την αντιμετώπιση των σχετικών θεμάτων.

Ανεξάρτητα όμως από το εάν ο ανωτέρω νόμος και οι διεθνείς συνεργασίες επαρκούν ή όχι για την ποινική κάλυψη των θεμάτων που προκύπτουν από την ανάπτυξη της Πληροφορικής, το βέβαιον είναι ότι, δεν επαρκούν για την τέλεια αντιμετώπιση των εγκλημάτων που έχουν τελεστεί με τη χρήση του Διαδικτύου.

Πρόσφατα τέθηκε σε ισχύ το Π.Δ. 47/2005, από την Α.Δ.Α.Ε. (Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών), το οποίο αφορά τις διαδικασίες, τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και τη διασφάλισή του. Ενώ, σύντομα αναμένεται να τεθεί σε ισχύ η Συνθήκη της Βουδαπέστης που αποσκοπεί στην αντιμετώπιση του Ηλεκτρονικού Εγκλήματος.

Οι ποινές που προκύπτουν από τα σχετικά άρθρα είναι οι εξής:

Άρθρο 348Α παρ. 2

Όποιος με πρόθεση (και όχι πλέον από κερδοσκοπία) παράγει, προσφέρει, πωλεί ή με οποιοδήποτε τρόπο διανέμει, διαβιβάζει, αγοράζει, προμηθεύεται ή κατέχει υλικό παιδικής πορνογραφίας δια συστήματος ηλεκτρονικού υπολογιστή και μέσω διαδικτύου τιμωρείται με φυλάκιση τουλάχιστον 2 ετών και χρηματική ποινή 50.000-300.000 €.

Άρθρο 348Β

Όποιος με πρόθεση, μέσω της τεχνολογίας των πληροφοριών και επικοινωνιών, προτείνει σε ανήλικο που δεν συμπλήρωσε τα δεκαπέντε έτη, να συναντήσει αυτόν ή τρίτον, με σκοπό την αποπλάνηση ή πορνογραφία του ανηλίκου, όταν η πρόταση αυτή ακολουθείται από περαιτέρω πράξεις που οδηγούν σε μια τέτοια συνάντηση, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή πενήντα χιλιάδων έως διακοσίων χιλιάδων ευρώ.

Άρθρο 370Β

1. 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 3 μηνών. Ως απόρρητα θεωρούνται κι 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.
2. 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.

3. Αν πρόκειται για στρατιωτικό ή διπλωματικό απόρρητο ή για απόρρητο που αναφέρεται στην ασφάλεια του κράτους, η ανάλογη ποινή είναι κάθειρξη μέχρι δέκα χρόνια ενώ σε καιρό πολέμου ο υπαίτιος τιμωρείται με ισόβια ή πρόσκαιρη κάθειρξη τουλάχιστον δέκα ετών. Όποιος γίνεται από αμέλεια υπαίτιος κάποιας από τις πράξεις που αναφέρθηκαν, τιμωρείται με φυλάκιση μέχρι τριών ετών.
4. Οι πράξεις που προβλέπονται στις παρ. 1 και 2 διώκονται ύστερα από έγκληση(μήνυση).

Άρθρο 370Γ

1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μήνες και με χρηματική ποινή διακοσίων ενενήντα (290) ευρώ 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 κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον είκοσι εννέα (29) ευρώ. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή την ασφάλεια του κράτους, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους. Αν όμως ο υπαίτιος ενήργησε με σκοπό να χρησιμοποιήσει τα ανωτέρω στοιχεία για να τα διαβιβάσει σε άλλον ή να τα ανακοινώσει έτσι ώστε να μπορούν να εκθέσουν σε κίνδυνο το συμφέρον του κράτους και ιδίως την ασφάλειά του ή κάποιου από τους συμμάχους του τιμωρείται με ποινή κάθειρξης και σε καιρό πολέμου, με ισόβια κάθειρξη ή θάνατο.
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 αρμοδίου υπαλλήλου του.
4. Οι πράξεις των παρ. 1 έως 3 διώκονται ύστερα από έγκληση.

Άρθρο 386Α

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 φυλάκιση τουλάχιστον τριών μηνών και αν η ζημιά που προξενήθηκε είναι μεγάλη, με φυλάκιση τουλάχιστον δύο ετών. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημιάς είναι αδιάφορο αν παθόντες είναι ένα ή περισσότερα πρόσωπα.

Νομοθεσία διαδικτυακών εγκλημάτων στην αλλοδαπή

Στην Αμερική θεωρείται τρομοκρατική οποιαδήποτε πράξη μη εξουσιοδοτημένης πρόσβασης σε Η/Υ, και τιμωρείται με φυλάκιση ως και ισόβια (ανάλογα με τη σημασία της εισβολής), χωρίς δυνατότητα μείωσης τις ποινής.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Ποινικό δίκαιο
- http://www.hellenicpolice.gr/newsite.php?&lang
- http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414
- http://www.pi.ac.cy/InternetSafety/primary_kyndinoi.html
- http://www.itsecuritypro.gr/contents_article.php?id=5&catid=6

<u>Θέμα ομάδας</u> : Πρόληψη-Προστασία-Αντιμετώπιση Ηλεκτρονικού Εγκλήματος

<u>Οι μαθητές</u>

Σ. Σ.

Δ. Τ.

Κ. Τ.

Π. Φ.

Δ. Χ.

<u>ΠΕΡΙΕΧΟΜΕΝΑ</u>

1. 10 Συμβουλές για ασφαλείς αγορές μέσω διαδικτύου

Ας το δούμε ξεκάθαρα, υπάρχουν πολλοί λόγοι για κάποιον να ψωνίσει στο διαδίκτυο. Προσφορές, αμέτρητη ποικιλία σε είδη, ασφαλείς αγορές, γρήγορα ψώνια! Τα ψώνια ποτέ δεν ήταν πιο εύκολη και άνετη υπόθεση για τους καταναλωτές. Τι γίνεται όμως με τις απάτες? Ύστερα από μελέτες φαίνεται ότι η χρήση των phishing επιθέσεων (όπου οι ληστές προσπαθούν να βάλουν τον πελάτη να υπογράψει με τα στοιχεία του και ακόμα και να δώσει τα στοιχεία της πιστωτικής του, καθώς υποκρίνονται ότι είναι ένα κανονικό website ή τράπεζα) είχε μειωθεί περίπου 8% το 2011. Πολύ καλά νέα αλλά η ίδια μελέτη αναφέρει ότι οι ιστότοποι με malware (βλαβερός κώδικας που στοχεύει στην υποκλοπή στοιχείων και προσωπικών δεδομένων) αυξήθηκε κατά 89%! Παρόλο που αυτά τα στατιστικά φαίνονται ανησυχητικά, δεν θα πρέπει να μας αποτρέπουν από το να κάνουμε τις αγορές μας Online. Απλά χρειαζόμαστε πρακτικές συμβουλές και λογική σκέψη, που ακολουθούν παρακάτω:

1. Χρησιμοποιήστε γνωστές ιστοσελίδες
Ξεκινήστε με ένα αξιόπιστο δικτυακό τόπο και όχι απλά ψάχνοντας για αγορά μέσω μηχανή αναζήτησης. Αν γνωρίζετε την ιστοσελίδα, οι πιθανότητες του να πρόκειται για απάτη είναι ελάχιστες. Γνωρίζουμε όλοι φερ 'ειπείν το Amazon.com. Επίσης, πολλά μεγάλα καταστήματα λιανικής πώλησης έχουν και ηλεκτρονικό κατάστημα από το οποίο μπορούμε να κάνουμε αγορές. Προσοχή στα ορθογραφικά λάθη ή σε ιστοσελίδες που χρησιμοποιούν διαφορετικό top-leveldomain (η σελίδα τελειώνει σε .net αντί του .com, για παράδειγμα).

2. Ψάξτε τι είδους ασφάλεια προσφέρει η σελίδα
Δεν πρέπει να αγοράζουμε τίποτα με χρήση πιστωτικής κάρτας από μια τοποθεσία που δεν έχει SSL κρυπτογράφηση (SecureSocketsLayer) ! Γνωρίζουμε αν η περιοχή έχει SSL, εάν η διεύθυνση URL για την ιστοσελίδα ξεκινάει με HTTPS:// (και όχι μόνο με HTTP://). Μια εικόνα με ένα κλειδωμένο λουκέτο θα εμφανιστεί, συνήθως στη γραμμή κατάστασης στον browser σας κάτω, ή δίπλα στη διεύθυνση URL στη γραμμή διευθύνσεων (πάνω μέρος). Εξαρτάται από το πρόγραμμα περιήγησής σας, αλλά ο πιο εύκολος τρόπος να διαπιστώσουμε είναι απλά να δούμε το εικονίδιο. Επίσης, δεν δίνουμε ΠΟΤΕ στοιχεία πιστωτικής μέσω e-mail σε κανένα.

3. Όσο λιγότερα στοιχεία, τόσο το καλύτερο
Κανένα ηλεκτρονικό κατάστημα δεν χρειάζεται την ημερομηνία των γενεθλίων μας ή κάποιον άλλο αριθμό, για να γίνουν οι συναλλαγές. Ωστόσο, αν πέσουν στα χέρια κακοποιών θα μπορούν να κάνουν αρκετή ζημιά σε συνδυασμό με τον αριθμό της πιστωτικής σας. Όσο περισσότερα γνωρίζουν, τόσο πιο εύκολο είναι να γίνει η κλοπή. Άρα, προσπαθούμε να δίνουμε όσο το δυνατόν λιγότερες πληροφορίες.

4. Συχνός έλεγχος λογαριασμού της κάρτας (balance)
Μην περιμένετε τον λογαριασμό της κάρτας στο τέλος του μήνα. Ακόμα και σε περίοδο διακοπών ελέγχετε ηλεκτρονικά την πιστωτική/χρεωστική σας κάρτα για οποιαδήποτε κίνηση. Βεβαιωθείτε ότι όλες οι χρεώσεις είναι σωστές και θεμιτές, ακόμα και αν δείχνουν να πηγαίνουν σε site όπως το PayPal. Εάν δείτε οτιδήποτε

παράξενο, τηλεφωνήστε για την άμεση διευθέτηση του θέματος. Σε περίπτωση που η κάρτα είναι πιστωτική, πληρώστε το λογαριασμό εφόσον γνωρίζεται ότι οι χρεώσεις είναι οι σωστές. Έχετε χρονικό περιθώριο 30 ημερών για να ενημερώσετε/ειδοποιήσετε την τράπεζα ή τον εκδότη της πιστωτικής, ότι υπάρχει πρόβλημα. Πέραν αυτού του χρονικού ορίου, μπορεί να είστε εσείς υπεύθυνος/-η για τις χρεώσεις.

5. "Εμβολιάστε" τον υπολογιστή σας

Οι απατεώνες δεν κάθονται στην αναμονή για να τους δώσετε τα στοιχεία σας... Προστατέψτε τον υπολογιστή σας από κακόβουλο λογισμικό με τακτικές ενημερώσεις στο anti-virus πρόγραμμα σας. Επίσης θωρακίστε το PC σας με ένα αξιόλογο πρόγραμμα firewall.

6. Χρησιμοποιήστε ισχυρούς κωδικούς πρόσβασης

Ακούμε συνεχώς την συμβουλή για χρήση δύσκολων κωδικών πρόσβασης, αλλά τίποτε δεν είναι πιο σημαντικό από αυτό, στις online τραπεζικές συναλλαγές και αγορές. Πρακτικά χρειαζόμαστε κωδικούς που: Να είναι ίσοι ή μεγαλύτεροι από 8 χαρακτήρες (γράμματα ΚΑΙ αριθμούς) Να περιέχει σύμβολα όπως: !$%&* Να μην θυμίζει κάτι γνωστό σε μάς ή αν είναι κάποια λέξη, αντικαταστήστε μερικά γράμματα με αριθμούς. Εάν η ιστοσελίδα στην οποία δημιουργούμε τον κωδικό μας το επιτρέπει, βάζουμε και κεφαλαία και μικρά γράμματα. Πχ: η λέξη Internet θα μπορούσε να γίνει %1Nt3Rn3T$ χρησιμοποιώντας τους παραπάνω κανόνες, δημιουργώντας κωδικό με το μεγαλύτερο δυνατό ποσοστό ασφαλείας.

7. Αποφύγετε την χρήση δημόσιων υπολογιστών για αγορές (Internet Cafe)

Εάν για κάποιο λόγο παρόλα αυτά χρειαστεί να χρησιμοποιήσετε δημόσιο υπολογιστή, θυμηθείτε να κάνετε logout (αποσύνδεση) κάθε φορά! Ακόμα και εάν απλά τσεκάρατε το email σας. Τι γίνεται όμως αν χρησιμοποιούσατε το δικό σας laptop, όσο ήσασταν καθ'οδόν; Σε δημόσιους χώρους (όπως σε μια καφετέρια) είναι αρκετά εύκολο κάποιος να δει στοιχεία της κάρτας σας καθώς τα εισάγετε σε ένα website. Αν και πάλι είναι ανάγκη προσπαθήστε να σιγουρευτείτε ότι δεν σας βλέπει κανείς και καθήστε σε γωνιακό σημείο στο καφέ.

8. Wi-Fi

Εάν αποφασίσετε να βγείτε έξω και να ψωνίσετε μέσω του laptop σας, θα χρειαστείτε μια ασύρματη σύνδεση Wi-Fi. Χρησιμοποιήστε το μόνο εάν έχετε πρόσβαση στο Net μέσω εικονικού ιδιωτικού δικτύου (VPN). Επίσης μην χρησιμοποιείτε άγνωστα προς εσάς hotspots. Συνδεθείτε μόνο σε γνωστά δίκτυα ακόμα και αν είναι δωρεάν, όπως αυτά που προσφέρονται σε αλυσίδες καταστημάτων, καφετέριες, εστιατόρια, και βιβλιοθήκες.

9. Δωροκάρτες

Οι δωροκάρτες είναι το πιο περιζήτητο δώρο συνεχώς. Συνεχίστε να αγοράζετε Giftcards από την ίδια πηγή, διότι απατεώνες πουλάνε κάρτες με ελάχιστες έως καθόλου μονάδες σε site όπως το eBay.

10. Διαφημίσεις

Θα έχετε παρατηρήσει πολλές φορές διαφημίσεις πως μοιράζονται δωρεάν iPad (ένα πολυπόθητο gadget) ή ακόμα και δωρεάν διακοπές. Πολλές από αυτές τις "προσφορές" θα τις δείτε μέσω των socialmedia. Προσοχή ακόμα και στους φίλους

σας, οι οποίοι θα μπορούσαν να διαβιβάσουν αθώα κάτι τέτοιο. Να είστε πολύ επιφυλακτικοί ακόμα και αν λάβετε ένα μήνυμα από φίλο που ισχυρίζεται ότι έχει πέσει θύμα ληστείας, ειδικά ένα φίλο στο εξωτερικό που ψάχνει για χρήματα για τραπεζικό έμβασμα, εκτός και άν μπορείτε να το διασταυρώσετε. Το να είστε επιφυλακτικοί είναι η καλύτερη αντιμετώπιση.

2.Αντιμετώπιση του εγκλήματος στον κυβερνοχώρο (e-crime)

Η χρήση του Διαδικτύου έχει κυριολεκτικά εκτιναχθεί στα ύψη τα τελευταία χρόνια και η εμφάνιση νέων φαινομένων και νέων τεχνικών έχει δημιουργήσει μια κατάσταση αυξημένης ανασφάλειας.
Οι ταχύρρυθμες εξελίξεις του Διαδικτύου και άλλων συστημάτων πληροφοριών έχουν δημιουργήσει έναν εντελώς νέο οικονομικό τομέα και νέες ταχύρρυθμες ροές πληροφοριών, προϊόντων και υπηρεσιών οι οποίες διέρχονται διαμέσω των εσωτερικών και εξωτερικών συνόρων της ΕΕ.
Το γεγονός αυτό είχε βεβαίως πολυάριθμες θετικές συνέπειες για τους καταναλωτές και τους πολίτες. Εντούτοις, οι εξελίξεις αυτές έχουν επίσης ανοίξει πολλές νέες δυνατότητες για τους κακοποιούς. Είναι σαφώς ορατό το πρότυπο νέων αξιόποινων δραστηριοτήτων κατά του Διαδικτύου, ή μέσω της χρήσης συστημάτων πληροφοριών ως μέσου διάπραξης αδικημάτων.
Οι μορφές αυτών των αξιόποινων δραστηριοτήτων εξελίσσονται διαρκώς, πράγμα που καθιστά προφανώς δύσκολο για τη νομοθεσία και την επιχειρησιακή επιβολή του νόμου να ακολουθήσουν τον ίδιο ρυθμό. Ο εγγενής διασυνοριακός χαρακτήρας αυτού του νέου είδους αδικημάτων δημιουργεί επίσης την ανάγκη βελτίωσης της διασυνοριακής συνεργασίας στον τομέα της επιβολής του νόμου. Το έγκλημα στον κυβερνοχώρο πλήττει όλους τους τομείς της κοινωνίας εκ τούτου, η πολιτική για την αντιμετώπισή του θα είναι επίσης ορατή σχεδόν παντού.
Δεδομένου του πολύ μεγάλου αριθμού πολιτών οι οποίοι χρησιμοποιούν ιδιωτικούς υπολογιστές, η πλειονότητα των πολιτών (ήδη υπό την ιδιότητά των δυνητικών θυμάτων) μπορεί επίσης να υπόκειται στις επιπτώσεις οποιασδήποτε πρωτοβουλίας στον τομέα της καταπολέμησης του εγκλήματος στον κυβερνοχώρο.
Εντούτοις, υπάρχουν επίσης σαφείς ενδείξεις σύμφωνα με τις οποίες έχουν αυξηθεί οι αξιόποινες δραστηριότητες που στρέφονται κατά συγκεκριμένων ομάδων θυμάτων. Ως εκ τούτου, μια αποτελεσματική πολιτική για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο θα μπορούσε να έχει σαφείς ευεργετικές συνέπειες για τις ομάδες αυτές.
Δεδομένης της εμβέλειας και του εύρους των απειλών για την ασφάλεια, η ανάγκη αντιμετώπισης των απειλών του εγκλήματος στον κυβερνοχώρο εξακολουθεί να υφίσταται και ενδέχεται να αυξηθεί. Τα ζητήματα ασφάλειας που συνδέονται με το έγκλημα στον κυβερνοχώρο έχουν παγκόσμια διάσταση και δεν μπορούν συνεπώς να αντιμετωπίζονται μόνο σε εθνικό επίπεδο. Η απειλή είναι διεθνής και το ίδιο διεθνής πρέπει να είναι ένα μέρος τουλάχιστον της απάντησης.
Είναι αναμφισβήτητο ότι η καταπολέμηση του εγκλήματος στον κυβερνοχώρο θα εξακολουθήσει να είναι πιο σημαντική και αποτελεσματική σε εθνικό επίπεδο, υπάρχει όμως σαφής ανάγκη διασύνδεσης και ενδεχομένως συμπλήρωσης των εθνικών προσπαθειών στο ευρωπαϊκό επίπεδο.
Οποιαδήποτε πολιτική για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο είναι πολύπτυχη, λόγω της ίδιας της φύσης του προβλήματος. Για να είναι λοιπόν πραγματικά αποτελεσματική, θα πρέπει να συνδυάζει παραδοσιακές

δραστηριότητες επιβολής του νόμου με άλλα εργαλεία, όπως αυτορρυθμιζόμενα στοιχεία και δημιουργία δομών για τη συνεργασία μεταξύ των διαφόρων συμμετεχόντων.
Για την επίτευξη αυτών των στόχων, χρειάζεται ένας ορισμένος αριθμός διαφορετικών και συνδυασμένων μέτρων. Η Επιτροπή των Ευρωπαϊκών Κοινοτήτων έχει, επί τη βάσει των εκτεταμένων διαβουλεύσεων τις οποίες διοργάνωσε, καταλήξει ότι η ενδεδειγμένη στρατηγική που πρέπει να ακολουθηθεί από εδώ και στο εξής για την πρόληψη και την επίλυση ως ένα βαθμό των προβλημάτων που δημιουργούνται είναι η συνεκτική στρατηγική προσέγγιση. Αυτή η προσέγγιση θα σήμαινε ότι εισάγεται στο επίπεδο της ΕΕ συνεκτική στρατηγική για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Το κυριότερο στοιχείο της είναι η δημιουργία στρατηγικού πλαισίου για κοινοτική πολιτική καταπολέμησης του εγκλήματος στον κυβερνοχώρο, με γενικό στόχο τη διαμόρφωση βελτιωμένων προσανατολισμών για συγκεκριμένες δράσεις και βελτιστοποίηση των υφιστάμενων πόρων.
Άλλες σημαντικές επιχειρησιακές πτυχές αυτής της στρατηγικής είναι οι ακόλουθες:
- Βελτίωση της συνεργασίας για την επιβολή του νόμου στο επίπεδο της ΕΕ
- Καθιέρωση στρατηγικής δομής για τη συνεργασία μεταξύ του δημόσιου και του ιδιωτικού τομέα για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο
- Προώθηση της δημιουργίας πλαισίου για τη διεθνή συνεργασία παγκοσμίως στον εν λόγω τομέα
- Λήψη στοχοθετημένων νομοθετικών μέτρων όταν χρειάζεται.
Η εναλλακτική λύση που συνίσταται στο να μη ληφθεί κανένα μέτρο στον οικείο τομέα δεν φαίνεται να είναι βιώσιμη. Μια παθητική στάση θα οδηγούσε πιθανώς στην παράταση της ισχύος πολλών διμερών προγραμμάτων συνεργασίας για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, χωρίς να υπάρχει καμία δυνατότητα να επωφεληθούμε από την οριζόντια ανταλλαγή βέλτιστων πρακτικών ή από επιπτώσεις συνεργίας.
Η λήψη νομοθετικών μέτρων γενικής φύσης για τη δημιουργία νέων οργανισμών στο επίπεδο της ΕΕ, για την εναρμόνιση των ορισμών των αδικημάτων και για τη διασαφήνιση των αρμοδιοτήτων και των ευθυνών όλων των συμμετεχόντων θα μπορούσε να παρουσιάζει ενδιαφέρον, όμως από μια ανάλυση της πολιτικής κατάστασης φάνηκε σαφώς ότι είναι πολύ μικρές οι πιθανότητες να υποβληθούν προτάσεις για λήψη νομοθετικών μέτρων γενικής και οριζόντιας φύσης. Εντούτοις, η λήψη νομοθετικών μέτρων γενικής φύσης ενδέχεται να παρουσιάζει ενδιαφέρον σε μακροπρόθεσμη προοπτική.
Οι συζητήσεις που διοργανώθηκαν έδειξαν σαφώς ότι η «συνεκτική στρατηγική» είναι η λύση με την οποία είναι πιθανότερο να επιτευχθούν οι στρατηγικοί στόχοι της πολιτικής. Η στρατηγική αυτή είναι πιθανόν ότι θα έχει σημαντικές θετικές επιπτώσεις για την καταπολέμηση του διασυνοριακού εγκλήματος στον κυβερνοχώρο, δεδομένου ότι οι αρμοδιότητες και οι ρόλοι όλων των συμμετεχόντων κατά την καταπολέμηση αυτή θα διασαφηνιστούν και θα ενισχυθούν. Θα συμβάλλει επίσης στη βελτίωση του διαλόγου και της κατανόησης μεταξύ του δημόσιου και του ιδιωτικού τομέα, πράγμα που με τη σειρά του θα μπορούσε να έχει πολλές θετικές παράπλευρες επιπτώσεις.
Από οικονομική άποψη, η προτιμητέα εναλλακτική λύση μπορεί να οδηγήσει σε σημαντικά αποτελέσματα συνεργίας, σε μείωση του της βλάβης που προξενούν οι αξιόποινες δραστηριότητες και μείωση του κόστους των διαφόρων προγραμμάτων ασφάλειας.

Είναι εντούτοις πιθανό ότι θα χρειαστούν κάποια χρόνια μέχρις ότου υλοποιηθούν τα αναμενόμενα αποτελέσματα της επιλεγείσας εναλλακτικής λύσης. Είναι, κατά συνέπεια, δύσκολο να αξιολογηθούν από τώρα όλες οι εν δυνάμει επιπτώσεις της, πόσο μάλλον που οι συγκεκριμένες λεπτομέρειες της πολιτικής αυτής δεν έχουν ακόμα αποφασιστεί. Ως εκ τούτου, θα χρειαστεί να αξιολογηθούν μεταγενέστερα οι ειδικές επιπτώσεις των συγκεκριμένων στοιχείων αυτής της πολιτικής.

3. Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος

Η αποστολή της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος συμπεριλαμβάνει την πρόληψη, την έρευνα και την καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών, που διαπράττονται μέσω του διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας. Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος είναι αυτοτελής κεντρική Υπηρεσία και υπάγεται απευθείας στον κ. Αρχηγό της Ελληνικής Αστυνομίας.
Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, στην εσωτερική της δομή, αποτελείται από πέντε τμήματα που συμπληρώνουν όλο το φάσμα προστασίας του χρήστη και ασφάλειας του Κυβερνοχώρου. Έτσι, στη νέα αναβαθμισμένη δομή της αποτελείται από:

α. Τμήμα Διοικητικής Υποστήριξης και Διαχείρισης Πληροφοριών,
β. Τμήμα Καινοτόμων Δράσεων και Στρατηγικής,
γ. Τμήμα Ασφάλειας Ηλεκτρονικών και Τηλεφωνικών Επικοινωνιών και Προστασίας Λογισμικού και Πνευματικών Δικαιωμάτων,
δ. Τμήμα Διαδικτυακής Προστασίας Ανηλίκων και Ψηφιακής Διερεύνησης και
ε. Τμήμα Ειδικών Υποθέσεων και Δίωξης Διαδικτυακών Οικονομικών Εγκλημάτων

ΒΙΒΛΙΟΓΡΑΦΙΑ

- http://www.itlawyers.gr/αρχειο/122-ηλεκτρονικο-εγκλημα
- http://www.crimestories.gr/index.php/prevention
- http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=8194&Itemid=378&lang
- http://www.hellenicpolice.gr/index.php?option=ozo_content&perform=view&id=135&Itemid=128&lang

ΕΓΚΛΗΜΑΤΑ ΛΕΥΚΟΥ ΚΟΛΑΡΟΥ

Οι μαθήτριες

- ***Χ. Μ.***
- ***Τ. Ε.***
- ***Τ. Ν.***
- ***Τ. Σ.***

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΓΚΛΗΜΑΤΑ ΛΕΥΚΟΥ ΚΟΛΛΑΡΟΥ

- *Ο όρος «εγκλήματα λευκού κολάρου» και «εγκλήματα μπλε κολάρου» και συγκεκριμένα ο όρος «εγκληματικότητα λευκού κολάρου»* προήλθε Από τον Αμερικανό εγκληματολόγο ***E.H. Sutherland (1883-1950) .*** Συγκεκριμένα στο γνωστό του άρθρο με τίτλο ***«White- Collar Criminality»*** το 1940 τόλμησε να επισημάνει την εγκληματική συμπεριφορά ατόμων με *«υψηλή κοινωνική θέση»* ορίζοντας ως έγκλημα λευκού κολάρου την παράβαση του ποινικού δικαίου από άτομα ανώτερης κοινωνικοοικονομικής τάξης στο πλαίσιο των επαγγελματικών τους δραστηριοτήτων.

- Εκεί για πρώτη φορά συναντάμε τη γνωστή σε όλους ορολογία των εγκλημάτων του λευκού κολάρου. Πρόκειται για όρο ευρύ και πολυχρησιμοποιημένο, που άλλοτε ταυτίζεται με τα οικονομικά εγκλήματα, άλλοτε με τη διαφθορά και άλλοτε με τις παράτυπες επιχειρηματικές δραστηριότητες.

- Στις περιπτώσεις των εγκλημάτων όπου οι δράστες άνηκαν σε *«κατώτερη κοινωνικοοικονομική τάξη»* τα εγκλήματα αυτά διακρίνονταν σε *«εγκλήματα μπλε κολάρου»*

- Οι οικονομικής φύσεως εγκληματίες όταν εκτός από τα συγκεκριμένα εγκλήματα φθάσουν να οδηγηθούν σε ***δολοφονική πράξη***, τότε αποκαλούνται ***«εγκληματίες ερυθρού κολάρου»*** (red -collar – criminals) και τα άτομα που διαπράττουν ταυτόχρονα φόνο και απάτη εμφανίζονται να έχουν ψυχοπαθητικά χαρακτηριστικά.

ΣΥΝΕΠΕΙΕΣ ΕΓΚΛΗΜΑΤΩΝ ΛΕΥΚΟΥ ΚΟΛΛΑΡΟΥ

- ***Το κρίσιμο μέγεθος της κοινωνικής βλάβης***

  Η τωρινή οξύτατη οικονομική κρίση έγινε η αφορμή για να έρθουν στην επιφάνεια πολύκροτα σκάνδαλα, συνδεόμενα με επιβλαβείς πρακτικές πλήρως ενσωματωμένες στην επίσημη οικονομία, ως συνέπεια της απορρύθμισης της αγοράς, και προσαρμοσμένες τόσο στις δραστηριότητες όσο και στους ηθικούς κώδικες επίσημων οικονομικών φορέων και στρατηγικών επιχειρηματικών παραγόντων παγκόσμιας εμβέλειας. Παρά τα απογοητευτικά αποτελέσματα και τις ανησυχητικές μέχρι σήμερα συνέπειες για την οικονομία και την πολιτική σταθερότητα ιδίως των χωρών του ευρωπαϊκού νότου, με εξέχουσα την ελληνική περίπτωση, οι προτεινόμενες λύσεις φαίνεται ότι αντί να συνηγορούν υπέρ της άμβλυνσης των δομικών δυσλειτουργιών, συμβάλλουν στην περαιτέρω όξυνσή τους.

- Σε μια τέτοια βάση, το θεωρητικά και λογικά παράδοξο που θέλει τα εγκλήματα του λευκού κολάρου να «εξαφανίζονται» μέσω της δομικής και πολιτισμικής ενσωμάτωσής τους στο παραγωγικό σύστημα ενώ τη διαφθορά να διαχέεται στην κοινωνία ευθυνόμενη για την εθνική ταπείνωση, προβάλλεται ως η επιτομή του πολιτικά ορθού.

- Ο λογικός συνειρμός καταλήγει να επιμερίζει εξίσου την ευθύνη, έτσι ώστε να μην ευθύνεται κανείς αποκλειστικά, προσδίδει τεχνική ταυτότητα στο φαινόμενο της

διαφθοράς, αφαιρώντας του την παράμετρο της κατάχρησης εξουσίας και ως εκ τούτου επικεντρώνει το φαινόμενο κατά κανόνα στα μικρομεσαία στρώματα, προσδίδοντας μεγαλύτερη έμφαση στη «ζήτηση» της διαφθοράς παρά στην «προσφορά» της.

- Η οικονομική ζημιά αυτών των εγκλημάτων (λευκού κολάρου) είναι πολύ σημαντική. Τα εγκλήματα αυτά προδίδουν την εμπιστοσύνη και επιφέρουν αναξιοπιστία ,που με τη σειρά της εξασθενεί την κοινωνική ηθική και παράγει κοινωνική αποδιοργάνωση σε ευρεία κλίμακα.

ΠΑΡΑΔΕΙΓΜΑΤΑ ΕΓΚΛΗΜΑΤΩΝ ΛΕΥΚΟΥ ΚΟΛΑΡΟΥ

- Εγκλήματα έσχατης προδοσίας , προδοσίας της χώρας και εναντίον ξένων κρατών.
- Εγκλήματα πολιτικών σωμάτων και εγκλήματα κατά των εκλογών (π.χ. αρπαγή κάλπης)
- Προσβολές κατά της πολιτειακής εξουσίας.
- Επιβουλή της δημόσιας τάξης.
- Επιβουλή της θρησκευτικής ειρήνης (π.χ. εξύβριση κληρικών)
- Εγκλήματα σχετικά με το νόμισμα (π.χ. παραχάραξη)
- Εγκλήματα σχετικά με τα υπομνήματα (π.χ. πλαστογραφίες , ψευδείς βεβαιώσεις)
- Εγκλήματα σχετικά με την απονομή της δικαιοσύνης (π.χ. δωροδοκίες δικαστών)
- Εγκλήματα σχετικά με την υπηρεσία (π.χ. δωροδοκίες υπαλλήλων)
- Κοινώς επικίνδυνα εγκλήματα (π.χ. εμπρησμός, καταστροφή)
- Εγκλήματα κατά της ζωής (π.χ. δολοφονίες)
- Εγκλήματα κατά των ηθών.
- Παραβάσεις ειδικών ποινικών νόμων (π.χ. λαθρεμπόριο, διακίνηση ναρκωτικών)
- Αδικήματα στρατιωτικού ποινικού κώδικα
- Εγκλήματα σχετικά με την οικονομία και το δημόσιο εισόδημα.

ΠΡΑΓΜΑΤΙΚΑ ΕΓΚΛΗΜΑΤΑ ΛΕΥΚΟΥ ΚΟΛΑΡΟΥ

- Το σκάνδαλο της Αγροτικής Ασφαλιστικής. Πέραν των παρανομιών που αποκαλύφθηκαν και της διασπάθισης δημοσίου χρήματος, εξασφάλιζε, την δεύτερη τετραετία του ΠΑΣΟΚ, στα διευθυντικά της στελέχη, μισθούς από 25 έως 33 εκατομμύρια δρχ. μηνιαίως, με τη μέθοδο των προμηθειών.

- ΕΤΒΑ 1: Σκάνδαλο 1,5 δισ. δραχμών σε βάρος της ΕΤΒΑ και δύο θυγατρικών ναυτιλιακών εταιρειών της με την αγορά πλοίων από δύο άγνωστες κυπριακές εταιρείες φαντάσματα, οι οποίες εμφανίζονταν χωρίς κεφάλαια και χωρίς μετόχους.

  - ΕΤΒΑ 2: 2002 Σκάνδαλο πολλών δισεκατομμυρίων δραχμών στην ΕΤΒΑ Finance, θυγατρική εταιρεία της ΕΤΒΑ. Κύκλωμα στο οποίο συμμετείχαν ανώτερα στελέχη της εταιρείας προέβαινε σε παράνομες τοποθετήσεις κεφαλαίων της ΕΤΒΑ Finance ζημιώνοντας τόσο την τράπεζα όσο και το ελληνικό δημόσιο.
- Σκάνδαλο πλαστογραφίας στο υπουργικό συμβούλιο! Ο γραμματέας του υπουργικού συμβουλίου Κώστας Ζώρας διώχθηκε για πλαστογραφία με σκοπό την παράνομη παράταση δύο νομικών συμβούλων της Τραπέζης της Ελλάδος.

- - «Υπόθεση Γιώργου Δρέγου» :ο πολυθεσίτης (ένας εκ των πολλών) δικηγόρος του ΠΑΣΟΚ. Ως νομικός σύμβουλος του Οργανισμού Σχολικών Κτιρίων απαίτησε «λάδωμα» 15 εκατομμυρίων δραχμών από ιδιοκτήτη οικοπέδου για να συμπεριληφθεί το οικόπεδό του, στους σχεδιασμούς του Οργανισμού.

- - ΠΡΟΜΕΤ 1: «Ο πικρός καφές»: Ενώ η επίσημη τιμή του εισαγόμενου καφέ κατά τόνο ήταν 1500 δολάρια, η κρατική ΠΡΟΜΕΤ τον εισήγαγε λαθραία, υπερτιμολογώντας στα 2000 δολάρια τον τόνο.

- - ΠΡΟΜΕΤ 2: «Τα σάπια ξύλα». Η ΠΡΟΜΕΤ αγόρασε από φιλανδική εταιρεία εξαγωγών ξυλείας ποσότητες καυσόξυλων έναντι του εξωφρενικού τότε ποσού των 250 εκατομμυρίων δρχ., η οποία κρίθηκε ακατάλληλη από τους Έλληνες ξυλουργούς και τελικά σάπισε στο λιμάνι της Ελευσίνας

- - Σκάνδαλο ΑΓΡΕΞ: Σειρά από κομπίνες και υπεξαιρέσεις αποκαλύφθηκαν και στις «Αγροτικές Εξαγωγές» (ΑΓΡΕΞ)

- - Αριστείδης Χρήστου. Καταχράστηκε από την Εθνική Τράπεζα 147 εκατομμύρια δρχ. Στην υπόθεση εμπλέκονταν και η πρώην γραμματέας του Μένιου Κουτσόγιωργα.

- - Αθανάσιος Πόπωτας: Ο φιλόδοξος εκδότης φιλοπασοκικών εντύπων, εκ των οποίων όλες αποδείχτηκαν βραχύβιες, τιμωρήθηκε με ποινή φυλάκισης πέντε ετών για κατάχρηση 57 εκατομ. δρχ. από την Εθνική Τράπεζα της Ελλάδος. Εξαφανίστηκε για να μην εκτίσει την ποινή του. Ακόμη αγνοείται η τύχη του... Η υπόθεση Πόπωτα εκφράζει ακριβώς αυτή τη νοοτροπία που εισήχθη στην Ελλάδα με τις πρώτες κυβερνήσεις του ΠΑΣΟΚ. Αυτή δηλαδή του μικρομεσαίου στελέχους που χρησιμοποίησε τους κομματικούς μηχανισμούς για να ανελιχθεί οικονομικά.

- - Μαυράκης 1: Διοικητής της ΔΕΗ που απηλλάγη δια βουλευμάτων από δύο υποθέσεις που τον βάρυναν. έγραψε ιστορία με το δωράκι που «έδωσε στον εαυτό του», των 500 εκατομμυρίων δρχ.

  - Μαυράκης 2: Ο Μαυράκης βρέθηκε ξανά στην επικαιρότητα με τη συμφωνία για αγορά ηλεκτρικής ενέργειας από την Αλβανία, προκαλώντας ζημιά 120 εκατομμυρίων δρχ. στη ΔΕΗ, σύμφωνα και με το απαλλακτικό βούλευμα που αφορούσε την υπόθεση. Κλασσική περίπτωση «απαλλακτικής ατιμωρησίας».

- - ΚΥΔΕΠ: «Το σκάνδαλο του σταριού». Ένα σκάνδαλο που ζημίωσε τους Έλληνες αγρότες με το ποσό των 910 εκατομμυρίων δρχ. Χρησιμοποιήθηκαν δύο εταιρείες, ως μεσάζοντες, για το ξεπούλημα των προϊόντων της ΚΥΔΕΠ με αποτέλεσμα να κερδίσουν δισεκατομμύρια οι δύο αυτές εταιρείες εις βάρος του ελληνικού δημοσίου.

- - Μιχάλης Σταματελάτος. Ο υποδιευθυντής του υποκαταστήματος της Ιονικής & Λαϊκής Τράπεζας (απορροφήθηκε αργότερα απο τη EuroBank), που υπεξαίρεσε 230 εκατομμύρια δρχ. Θεωρείται ότι τμήμα του ποσού δόθηκε για τις προεκλογικές ανάγκες υποψήφιων βουλευτών του ΠΑΣΟΚ.

- - Θεοφάνης Τόμπρας, ο άνθρωπος με το ...κουμπούρι!: Ο κατ' εξακολούθηση εγκληματίας αυτός, αντί να βρισκόταν σε κάποιο κελί του Κορυδαλλού, ο...μεγάλος "σουλτάνος" της Ελλάδας Α. Παπανδρέου τον είχε τοποθετήσει ...διοικητή του ...ΟΤΕ!!! Παρακολουθήσεις και καταγραφές συνομιλιών στα σκοτεινά υπόγεια του ΟΤΕ και της ΚΥΠ. Οι καταγραφές πωλούνταν στους «ενδιαφερόμενους» ή «στην Ομόνοια», με ό,τι αυτό συνεπάγεται … Εξυπηρετήσεις, εκβιασμοί, πολιτική ανωμαλία κ.ά.

- - «Σκάνδαλο Κοσκωτά»: Επρόκειτο για το σχέδιο της οικονομικής επικράτησης «νέων τζακιών» προσαρμοσμένων στις πολιτικές επιλογές του ΠΑΣΟΚ. Ο ιδιωτικός τομέας που δημιουργήθηκε πήρε υπό τον έλεγχό του όλα σχεδόν τα μέσα ενημέρωσης που βρισκόταν στην κεντροδεξιά πλευρά, ανέλαβε δηλαδή τη χειραγώγηση του ελληνικού λαού και σε δεύτερη φάση απαιτούσε όλα τα κονδύλια του κράτους, διαφημιστικά πακέτα και τα δημόσια έργα. «Εκβίαζε» δηλαδή και την κοινή γνώμη και τα κόμματα. Το ΠΑΣΟΚ βοήθησε στην επικράτηση μιας νέας οικονομικής υπερεξουσίας που ναι μεν κινείται πολιτικά στο χώρο του δήθεν σοσιαλισμού, μετατράπηκε όμως σε ελεγκτή της πολιτικής ζωής του τόπου. Η νέα μεγαλοαστική τάξη, έσπασε μεν τους δεσμούς της με τη «Δεξιά», αντί όμως να περάσει στον ανταγωνισμό, στην πραγματική ιδιωτική πρωτοβουλία και στην παραγωγή έγινε κρατικοδίαιτη και απόλυτα εξαρτώμενη από τα κρατικά ταμεία. Επίκεντρο του σκανδάλου αυτού, που στην εποχή του θεωρήθηκε ως το μεγαλύτερο στην ιστορία του νέου Ελληνικού Κράτους, ήταν ο 33 χρόνος τότε, Γιώργος Κοσκωτάς, ο οποίος από απλός υπάλληλος μιας μικρής τότε τράπεζας, της Τράπεζας Κρήτης, βρέθηκε μέσα σε λίγες μέρες, ...μεγαλομέτοχός της! Μέσα σε 5 χρόνια, ο Κοσκωτάς στη κυριολεξία "μάδησε" τη τράπεζά του, αγοράζοντας εφημερίδες και Ρ/Σ, αλλά και...λαδώνοντας τους περισσότερους πολιτικούς του ΠΑΣΟΚ, μηδέ εξαιρουμένου του ιδίου του Ανδρέα Παπανδρέου!

- - Σκάνδαλο ΕΒΟ (Ελληνική Βιομηχανία Όπλων): Ο Στάθης Γιώτας υφυπουργός Εθνικής Αμύνης, παραιτούμενος, υπέβαλλε δύο μηνυτήριες αναφορές που έστειλαν στον Κορυδαλλό τον πρώην πρόεδρο της ΕΒΟ, Σταμάτη Καμπάνη και τους συγκατηγορούμενούς του, Δημήτρη Κυριακαράκο και Δημήτρη Χαλατσά, για πράξεις και παραλείψεις με τις οποίες ζημιώθηκε η ΕΒΟ. Στη δεύτερη μηνυτήρια αναφορά γίνεται λόγος για μίζες δισεκατομμυρίων μέσω εταιρειών φαντασμάτων. Περιέργως εμπλέκεται και εδώ ο Μένιος Κουτσόγιωργας.

«Καλύτερα να αποτύχεις έντιμα παρά να επιτύχεις με ΑΠΑΤΗ»
Σοφοκλής, 495-406 π.Χ

Βιβλιογραφία – Πηγές

www.wikipedia.gr

www.nomosophia.blogspot.gr

www.provataslaw.gr

www.phychografimata.com

www.static.eudoxus.gr