ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Ηλεκτρονικό Έγκλημα

Σαρτέρη Βερόνικα
41789

Εισηγήτρια: Αναστασία Ν. Βελώνη – Λέκτορας Εφαρμογών

UNIVERSITY OF WEST ATTICA

SCHOOL OF ENGINEERING

DEPARTMENT OF INFORMATICS AND COMPUTER ENGINEERING

DEGREE THESIS

Cyber Crime

Sarteri Veronika
41789

Supervisor: Anastasia N. Veloni, Application Lecturer

Σαρτέρη Βερόνικα

Ηλεκτρονικό Έγκλημα

Πτυχιακή Εργασία

Επιβλέπων Καθηγήτρια,

Αναστασία Ν. Βελώνη
Λέκτορας Εφαρμογών

Έλληνας Ιωάννης
.....
Εξεταστής

Αμοργίνος Ιωάννης
.....
Εξεταστής

Ημερομηνία:

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα πτυχιακή εργασία ολοκληρώθηκε μετά από επίμονες προσπάθειες, σε ένα ενδιαφέρον γνωστικό αντικείμενο, όπως αυτό του ηλεκτρονικού εγκλήματος. Την προσπάθειά μου αυτή υποστήριξε η επιβλέπων καθηγήτριά μου, την οποία θα ήθελα να ευχαριστήσω.

Ακόμα θα ήθελα να ευχαριστήσω την οικογένεια μου που με υποστήριξε όλα αυτά τα χρόνια για να ολοκληρώσω με επιτυχία τις σπουδές μου

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή εργασία ασχολείται με το ηλεκτρονικό έγκλημα και το πώς έχει εξελιχθεί με τη ραγδαία ανάπτυξη της τεχνολογίας. Υπάρχουν διάφορες μορφές του ηλεκτρονικού εγκλήματος ανάλογα με τον τύπο επίθεσης. Ξεκινάνε από επιθέσεις σε ανυποψίαστους πολίτες και ευάλωτες ομάδες πληθυσμού όπως παιδιά και μπορούν να φτάσουν μέχρι τρομοκρατικές επιθέσεις εναντίον κρατών ή και να προκαλέσουν παγκόσμια ανησυχία. Οι σκοτεινές πτυχές του διαδικτύου ,όπου παράνομες δραστηριότητες ανθίζουν, ολοένα απασχολούν περισσότερο την κοινή γνώμη. Παρόλο που χρειάζονται κάποιες σχετικά ανεπτυγμένες δεξιότητες στους υπολογιστές για να βρεθεί κανείς στο deep web ,όπως ονομάζεται, με τη βοήθεια από κάποιο ιστότοπο μπορεί σχεδόν ο καθένας να βρεθεί. Η ανωνυμία που προσφέρει το διαδίκτυο και η πρόσβαση από οποιοδήποτε μέρος του πλανήτη καθιστά δύσκολο το έργο εύρεσης του ένοχου. Νέα ζητήματα ασφαλείας προκύπτουν σχεδόν κάθε μέρα, τα κινητά και οι συσκευές αυτοματισμού στο σπίτι μπορεί να γίνουν στόχοι λόγω της σύνδεσης τους στο διαδίκτυο και την εγκατάσταση εφαρμογών, θέτοντας σε κίνδυνο ευάλωτες προσωπικές πληροφορίες. Υπάρχουν κάποια βασικά μέτρα ασφαλείας που είναι εύκολο να τα ακολουθήσουν άνθρωποι με βασικές γνώσεις στους υπολογιστές για την προστασία τους. Η ελληνική νομοθεσία περιλαμβάνει και τα ηλεκτρονικά εγκλήματα, ωστόσο δεν είναι εύκολο να καλυφθεί όλο το εύρος των εγκλημάτων λόγω της ξεχωριστής φύσης τους, με προσπάθειες να γίνονται με το πέρασμα των χρόνων να λυθεί το πρόβλημα αυτό. Το ηλεκτρονικό έγκλημα είναι ένας τομέας που εξελίσσεται καθημερινά και οι εγκληματίες βρίσκουν ολοένα και καινούργιους τρόπους για τις διαδικτυακές τους επιθέσεις. Αυτό δημιουργεί την ανάγκη εξειδίκευσης ατόμων στην αποτροπή αυτών τον επιθέσεων και αντιμετώπιση τους.

ΕΠΙΣΤΗΜΟΝΙΚΗ ΠΕΡΙΟΧΗ: Ηλεκτρονικό Έγκλημα

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Ηλεκτρονικό έγκλημα , μορφές, τρόποι ηλεκτρονικών επιθέσεων, ζητήματα ασφαλείας, μέτρα ασφαλείας, Ελληνική νομοθεσία.

ABSTRACT

The present thesis concerns cybercrime and how it has evolved with the rapid development of technology. There are various forms of cybercrime depending on the type of attack. They start with attacks on unsuspecting citizens and vulnerable population groups such as children and can go as far as terrorist attacks against nations or even cause global concern. The dark aspects of the internet, where illegal activities are flourishing, become a matter of concern to public opinion. Although it takes some relatively developed computer skills to find yourself on the deep web, as it is called, with the help of websites can almost anyone can find it. The anonymity offered by the internet and access from any part of the world makes it difficult to find the perpetrator. New security issues arise almost every day, mobiles and home automation devices can become targets due to their internet connection and app installation, endangering vulnerable personal information. There are some basic security measures that are easy for people with basic computer knowledge to follow to protect them. Greek legislation also includes electronic crimes, but it is not easy to cover the full range of crimes due to their distinct nature, with efforts to be made over the years to solve this problem. Cybercrime is an area that is evolving every day and criminals are finding increasingly new ways of their online attacks. This creates the need to specialize individuals in preventing these attacks and dealing with them.

SCIENTIFIC AREA: Cybercrime
KEY WORDS: Cybercrime, forms, types of attack, security issues, security measurements, Greek legislation.

Contents

ΕΙΣΑΓΩΓΗ

Στη σημερινή εποχή της πληροφορίας και των τεχνολογικών εξελίξεων παρατηρείται η ολοένα αυξανόμενη διείσδυση των ευρυζωνικών τεχνολογιών στην κοινωνία και διαφαίνεται η τάση για σύγκλιση των τηλεπικοινωνιακών δικτύων παροχής υπηρεσιών καθώς και για πρόσβαση «οποτεδήποτε», «από οπουδήποτε», και «με οτιδήποτε». Σε αυτό το συνεχώς μεταβαλλόμενο περιβάλλον, η έννοια του ηλεκτρονικού εγκλήματος αποκτά μια καινούρια διάσταση. Παραδοσιακές ηλεκτρονικές απειλές όπως: Κακόβουλο λογισμικό, μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές και συστήματα, ενοχλητικά ηλεκτρονικά μηνύματα, επιθέσεις κλοπής ηλεκτρονικής ταυτότητας κ.λπ., αναμένεται να βρουν νέα, εξίσου γόνιμα, εδάφη για την εξάπλωσή τους. Επιπλέον, η κακόβουλη χρήση των τεχνολογιών δικτύωσης μπορεί να διευκολύνει την τέλεση συμβατικών εγκλημάτων ή να ενισχύσει επιπλέον το καταστρεπτικό τους έργο. Σήμερα τα «εγκλήματα τελούμενα με υπολογιστή» αυξάνονται και γενικεύονται συνεχώς. Στις νέες μορφές εγκληματικότητας οι ηλεκτρονικοί υπολογιστές μπορούν:

- Να χρησιμοποιηθούν οι ίδιοι για να τελεστεί μια εγκληματική πράξη.
- Να καταστούν οι ίδιοι το προσβαλλόμενο αντικείμενο της εγκληματικής πράξης.
- Το αντικείμενο τους να τύχει εγκληματικής προσβολής.

ΣΚΟΠΟΣ ΤΗΣ ΕΡΓΑΣΙΑΣ

Η εργασία έχει ως σκοπό την διερεύνηση ηλεκτρονικών εγκλημάτων , δηλαδή τον τρόπο με τον οποίο εκδηλώνονται καθώς και το πώς αντιμετωπίζονται σε νομικό και τεχνικό επίπεδο. Συγκεκριμένα παρουσιάζονται διάφορες μορφές ηλεκτρονικού εγκλήματος, η πορεία τους και οι επιπτώσεις τους. Στη συνέχεια παρουσιάζονται τρόποι αντιμετώπισης των μορφών αυτών και το πως πρέπει να εφαρμόζονται προς αποφυγή παραπλάνησης. Τέλος αναφέρονται αρκετά ηθικά ερωτήματα στα οποία εμπλέκονται κυρίως «ευάλωτες» ηλικιακές ομάδες όπως τα παιδιά λόγω της άμεσης επαφής με το διαδίκτυο από πολύ μικρή ηλικία.

ΚΕΦΑΛΑΙΟ 1 - ΕΝΝΟΙΑ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

1.1 Τι είναι το Ηλεκτρονικό Έγκλημα

Η πληροφορική τεχνολογία κατέστησε δυνατή τη διάπραξη ενός ευρέως φάσματος εγκληματικών πράξεων, οι οποίες απαιτούν εξειδίκευση και αυξημένη κατάρτιση. Ως «Ηλεκτρονικό Έγκλημα»", λοιπόν, θεωρούνται οι αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία. Ανάλογα με τον τρόπο τέλεσης τους διαχωρίζονται σε εγκλήματα τελούμενα με τη χρήση Ηλεκτρονικών Υπολογιστών (computer crime) και σε Κυβερνοεγκλήματα (cyber crime), εάν τελέσθηκαν μέσω του Διαδικτύου.

1.2 Ιστορική Αναδρομή

Το ηλεκτρονικό έγκλημα εμφανίστηκε σχεδόν ταυτόχρονα με την εμφάνιση των ηλεκτρονικών υπολογιστών, καθώς τότε έγιναν και οι πρώτες προσπάθειες για την εκμετάλλευση αυτής της νέας τεχνολογίας προς όφελος τους καταφέρνοντας έτσι να αποκτάνε νέες ευκαιρίες για ευκολότερη και πιο γρήγορη διάπραξη εγκλημάτων. Τα πρώτα χρόνια το ηλεκτρονικό έγκλημα ήταν σπάνιο καθώς σημαντικός παράγοντας σ' αυτό έπαιζε και ο αριθμός των ηλεκτρονικών υπολογιστών που υπήρχαν και ο αριθμός αυτός ήταν πολύ μικρός.

Το ηλεκτρονικό έγκλημα εμφανίστηκε για πρώτη φορά τη δεκαετία του 1970 κυρίως στις τεχνολογικά ανεπτυγμένες χώρες. Κατά την πάροδο του χρόνου και της ανάπτυξης αυτό επεκτάθηκε και στις ανεπτυγμένες και στις αναπτυσσόμενες χώρες. Έπειτα την δεκαετία του 1980 το ηλεκτρονικό έγκλημα διαδόθηκε με πολύ μεγάλη ταχύτητα, πράγμα που προκάλεσε την απαρχή για συγκεκριμένες νομικές και εγκληματολογικές προσεγγίσεις αυτής της νέας μορφής εγκλήματος. Το 1986 ο Οργανισμός Συνεργασίας και Ανάπτυξης ανέθεσε σε μία ομάδα από άτομα ειδικευμένα στο ηλεκτρονικό έγκλημα, ώστε να μελετήσει τις νέες εκφάνσεις αυτής της μορφής του εγκλήματος, να επεξεργαστεί τα νέα δεδομένα και να καθορίσει εκ νέου την υπόσταση του εγκλήματος. Αυτή η μελέτη δίνει ένα νέο ορισμό για το ηλεκτρονικό έγκλημα, ο οποίος υπερέχει όλων των προηγουμένων. Στις μέρες μας, το μεγαλύτερο μέρος των ανθρώπων ανά τον κόσμο έχουν πρόσβαση σε ένα ηλεκτρονικό υπολογιστή και σε συνδυασμό με την απλούστευση της χρήση τους, κάνει την γνώση για αυτούς και την λειτουργία τους πιο εύκολη. Με λίγα λόγια, η ανάπτυξη του ηλεκτρονικού εγκλήματος οφείλεται στην δημιουργία νέων διόδων πρόσβασης σε νέες πληροφορίες. Με την δυνατότητα αυτή ο χρήστης έχει το πλεονέκτημα της ευρείας ανάπτυξης των γνώσεων που ήδη κατέχει όπως και των πρακτικών γνώσεων. Κατά καιρούς, έχουν γίνει πολλές προσπάθειες να ορισθεί το ηλεκτρονικό έγκλημα.Το 1994 οι Forester και Morrison όρισαν το Ηλεκτρονικό Έγκλημα (Computer Crime) σαν «μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως κυριότερο μέσο τέλεσης της». Υιοθετώντας μια τριπλή προσέγγιση (Αγγέλης, 2000) που τείνει να επικρατήσει σήμερα, μπορούμε να θεωρήσουμε το ηλεκτρονικό έγκλημα ως:

· μια νέα μορφή εγκλήματος, που διαπράττεται με τη χρήση ηλεκτρονικών υπολογιστών

· μια παραλλαγή των ήδη υπαρχόντων εγκλημάτων, τα οποία διαπράττονται με υπολογιστές

· μια εγκληματική πράξη στην εκδήλωση της οποίας συμμετέχει καθ΄ οποιονδήποτε τρόπο ένας ηλεκτρονικός υπολογιστής.

Στην αγγλική γλώσσα οι όροι που χρησιμοποιούνται για να περιγράψουν το ηλεκτρονικό έγκλημα ποικίλουν είναι: e-crime, cybercrime, computer-crime, internet related crime και hitech-crime .Αντιστοίχως, στην ελληνική γλώσσα οι όροι που χρησιμοποιούνται είναι ηλεκτρονικό έγκλημα, δικτυακό έγκλημα και έγκλημα του κυβερνοχώρου.

Βασικό συστατικό στοιχείο του ηλεκτρονικού εγκλήματος, αποτελεί η ύπαρξη μιας συσκευής ηλεκτρονικής επεξεργασίας δεδομένων, όπως ηλεκτρονικός υπολογιστής, laptop, κινητό τηλέφωνο, palmtop, notepad κλπ. Κυρίαρχο ρόλο διαδραματίζει ο Η/Υ,ο οποίος μπορεί:

Να αποτελεί τον στόχο κάποιας επίθεσης.

Να αποτελεί το μέσο διάπραξης κάποιας επίθεσης.

Να αποτελεί ένα βοηθητικό μέσο για τη διάπραξη του εγκλήματος.

Αν θέλαμε να ορίσουμε το «Ηλεκτρονικό Έγκλημα» θα μπορούσαμε να πούμε ότι γενικότερα είναι κάθε παράνομη δραστηριότητα που για την διάπραξη αλλά και για την αντιμετώπισή της απαιτείται η τεχνολογική γνώση. Ο ορισμός του ηλεκτρονικού εγκλήματος έχει να κάνει με την οπτική γωνία από την οποία εξετάζεται. Αυτή η πολυμορφία του εγκλήματος είναι που δυσχεραίνει και τον νομοθέτη, ο όποιος αποφεύγει να του προσδώσει έναν ορισμό και είτε αφήνει αυτήν την αρμοδιότητα στα δικαστήρια και στην παραγόμενη νομολογία, είτε δανείζεται τους χρησιμοποιούμενους από την τεχνολογία όρους.

1.3 Γνωρίσματα Ηλεκτρονικού Εγκλήματος

Το έγκλημα στον Κυβερνοχώρο είναι γρήγορο, διαπράττεται σε χρόνο δευτερολέπτων και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα.

- Είναι εύκολο στην διάπραξή του, φυσικά για όσους το γνωρίζουν, ενώ τα ίχνη που αφήνει είναι ψηφιακά.
- Για την τέλεσή του απαιτούνται άριστες και εξειδικευμένες γνώσεις.
- Μπορεί να διαπραχθεί χωρίς την μετακίνηση του δράστη, ο οποίος ενεργεί από το γραφείο ή το σπίτι του, μέσω του υπολογιστή του.
- Δίνει τη δυνατότητα σε άτομα με ιδιαιτερότητες όπως οι παιδόφιλοι (child pornography) 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.

- Οι "εγκληματίες του Κυβερνοχώρου" πολλές φορές δεν εμφανίζονται με την πραγματική τους ταυτότητα , αποστέλλουν ηλεκτρονικά μηνύματα(e-mail) με ψευδή στοιχεία.
- Είναι έγκλημα διασυνοριακό και τα αποτελέσματά του μπορεί να πραγματοποιούνται ταυτόχρονα σε πολλούς τόπους.
- Είναι πολύ δύσκολο να προσδιοριστεί ο τόπος τελέσεως του και επίσης είναι αρκετά δύσκολη η διερεύνηση και ο εντοπισμός του δράστη. Υπάρχει ενδεχόμενο ο δράστης να εντοπισθεί στην Α χώρα και τα αποδεικτικά στοιχεία μπορεί να βρίσκονται σε διαφορετική και απομακρυσμένη χώρα ή και να βρίσκονται ταυτόχρονα σε πολλές διαφορετικές χώρες.
- Η έρευνα απαιτεί κατά κανόνα συνεργασία δύο τουλάχιστον κρατών (του κράτους στο οποίο έγινε αντιληπτό το αποτέλεσμα της εγκληματικής συμπεριφοράς, και του κράτους όπου βρίσκονται τα αποδεικτικά στοιχεία). Περιπτώσεις εγκληματικής συμπεριφοράς στα όρια ενός μόνον κράτους είναι σπάνια.
- Η καταγραφή της εγκληματικότητας στον Κυβερνοχώρο δεν ανταποκρίνεται στην πραγματικότητα διότι ελάχιστες περιπτώσεις εγκλημάτων του Κυβερνοχώρου καταγγέλλονται διεθνώς. Κατά συνέπεια, το μέγεθος της εγκληματικότητας στο χώρο του Διαδικτύου είναι «ακόμα πιο σκοτεινό», από ότι στον «κοινό» εγκληματικό χώρο.

1.4 Μορφές Ηλεκτρονικών Εγκλημάτων

Τα εγκλήματα που προέκυψαν από την ανάπτυξη των τεχνολογιών πληροφορικής μπορούν να χωριστούν σε δύο μεγάλες κατηγορίες σε Διαδικτυακά και σε Οικονομικά.

Τα **διαδικτυακά** εγκλήματα αφορούν:

- Παράνομη είσοδο σε δεδομένα:
  Αφορά περιπτώσεις όπως **Hacking**, δηλαδή την πρόσβαση σε πληροφοριακό σύστημα με σκοπό την πρόκληση ζημιών ή το οικονομικό κέρδος χωρίς εξουσιοδότηση από τους εκάστοτε κατόχους. Δεύτερον **Crashing**, δηλαδή την καταστροφή προγραμμάτων καθώς και αρχείων δεδομένων. Τέλος **Cracking**, δηλαδή άρση της προστασίας των προγραμμάτων.
- Απάτες στο διαδίκτυο:
  Αφορά τις περιπτώσεις δημοσίευσης προσβλητικού και παράνομου περιεχομένου, την παράνομη διάθεση πορνογραφικού υλικού, καθώς και υλικού παιδικής πορνογραφίας, τη δημοσίευση πληροφοριών που υποστηρίζουν παράνομες πρακτικές (ανάπτυξη εμπορίου ναρκωτικών, όπλων, εκρηκτικών, σαμποτάζ), την προώθηση προπαγανδιστικών ιδεών (θρησκευτικών, ρατσιστικών κ.α.), την αποστολή απειλητικών μηνυμάτων και την αποστολή μεγάλου όγκου διαφημιστικών μηνυμάτων.
- Ιοί στο διαδίκτυο:
  Αφορούν προγράμματα που μεταφέρονται από χρήστη σε χρήστη χωρίς τη θέληση τους, ειδικότερα από οποιαδήποτε ηλεκτρονική συσκευή σε κάποια άλλη

με την προϋπόθεση ότι βρίσκονται σε κοινό δίκτυο, με στόχο την αλλοίωση ή τη διαγραφή των δεδομένων των παραληπτών.

Τα **οικονομικά** εγκλήματα αφορούν:

- Η απάτη μέσω Η/Υ:
  Αφορούν την παραποίηση λογιστικών λογαριασμών, την κατασκοπία επιχειρήσεων μέσω της υποκλοπής δεδομένων, την προσβολή τηλεφωνικών δικτύων, την παραποίηση ηλεκτρονικών πληρωμών.
- Η ηλεκτρονική αλλαγή παραδοσιακών εγκλημάτων:
  Αφορούν το ξέπλυμα μαύρου χρήματος, κλοπή ηλεκτρονικών υπηρεσιών, εκβιασμός επιχειρήσεων και εξαπάτηση λογιστικών δεδομένων.
- Η πειρατεία λογισμικού:Αφορούν την κλοπή πνευματικής ιδιοκτησίας, την αντιγραφή ή τροποποίηση ψηφιακών δεδομένων και τη εξουσιοδοτημένη χρήση λογισμικού.

ΚΕΦΑΛΑΙΟ 2 - ΗΛΕΚΤΡΟΝΙΚΑ ΕΓΚΛΗΜΑΤΑ

2.1 Hacking

Με απλά λόγια, το hacking είναι μια πράξη που διαπράττει ένας εισβολέας, αποκτώντας πρόσβαση στο σύστημα του υπολογιστή χωρίς άδειά. Οι χάκερ (οι άνθρωποι που κάνουν το «hacking») είναι προγραμματιστές υπολογιστών, οι οποίοι έχουν προηγμένη καταρτηση σε συστήματα υπολογιστών και συνήθως κάνουν κατάχρηση αυτής της γνώσης για παράνομους λόγους. Συνήθως είναι λάτρεις της τεχνολογίας που έχουν δεξιότητες επιπέδου εμπειρογνωμόνων σε ένα συγκεκριμένο πρόγραμμα ή γλώσσα προγραμματισμού. Όσον αφορά τα κίνητρα, θα μπορούσαν να υπάρχουν πολλά, αλλά τα πιο συνηθισμένα είναι αρκετά απλά και μπορούν να εξηγηθούν από μια ανθρώπινη τάση όπως η απληστία, η φήμη, η δύναμη κ.λπ.

Μερικοί άνθρωποι το κάνουν καθαρά για να επιδείξουν την εμπειρία τους,κάποιοι ασχολούνται με σχετικά αβλαβείς δραστηριότητες όπως η τροποποίηση λογισμικού για την εκτέλεση εργασιών που δεν εμπίπτουν στην πρόθεση του δημιουργού, και άλλοι απλώς θέλουν να προκαλέσουν καταστροφή. Μερικές φορές οι ηδονοβλεψικές τάσεις μπορεί να προκαλέσουν έναν χάκερ να εισέλθει σε συστήματα για να κλέψει προσωπικές τραπεζικές πληροφορίες, οικονομικά δεδομένα μιας εταιρείας, κ.λπ. Επίσης, δοκιμάζουν και τροποποιούν τα συστήματα, ώστε να μπορούν να εκτελούν εργασίες στις επιθυμίες τους. Οι χάκερ που εμφανίζουν τέτοια καταστροφική συμπεριφορά ονομάζονται επίσης «Crackers», ονομάζονται επίσης και «Black Hat» χάκερς. Από την άλλη πλευρά, υπάρχουν εκείνοι που αναπτύσσουν ενδιαφέρον για ηλεκτρονικές εισβολές μόνο λόγω πνευματικής περιέργειας. Ορισμένες εταιρείες προσλαμβάνουν αυτούς τους λάτρεις των υπολογιστών για να βρουν ελαττώματα στα συστήματα ασφαλείας τους και να βοηθήσουν να τα διορθώσουν. Αναφερόμενοι ως χάκερ "White Hat", αυτοί οι τύποι είναι κατά της κατάχρησης των συστημάτων υπολογιστών. Προσπαθούν να εισχωρήσουν σε συστήματα δικτύου καθαρά για να ειδοποιήσουν τους ιδιοκτήτες για ελαττώματα. Δεν είναι πάντοτε αλτρουιστικό, γιατί πολλοί το κάνουν και για τη φήμη, προκειμένου να προσληφθούν από κορυφαίες εταιρείες ή απλά να χαρακτηριστούν ως ειδικοί σε θέματα ασφάλειας.

Μερικές από τις πιο διάσημες ιδιοφυΐες υπολογιστών ήταν κάποτε χάκερ που συνέχισαν να χρησιμοποιούν τις δεξιότητές τους για εποικοδομητική τεχνολογική ανάπτυξη. Ο Dennis Ritchie και ο Ken Thompson, οι δημιουργοί του λειτουργικού συστήματος UNIX (προκάτοχος του Linux), ήταν δύο από αυτούς. Ο Shawn Fanning, ο προγραμματιστής του Napster, ο Mark Zuckerberg του Facebook και πολλά άλλοι είναι επίσης τέτοια παραδείγματα.

Οι πιο γνωστοί τρόποι Hacking χωρίζονται στις εξής κατηγορίες:

A. SQL Injections: Η SQL injection είναι μια τεχνική που επιτρέπει στους χάκερ να παίζουν με τις ευπάθειες ασφαλείας του λογισμικού που εκτελεί έναν ιστότοπο. Μπορεί να χρησιμοποιηθεί για να επιτεθεί σε οποιονδήποτε τύπο βάσης δεδομένων SQL που δεν προστατεύεται ή δεν προστατεύεται σωστά. Αυτή η διαδικασία περιλαμβάνει την εισαγωγή τμημάτων κώδικα SQL σε ένα πεδίο εισαγωγής φόρμας ιστού - συνηθέστερη

στα ονόματα χρηστών και κωδικούς πρόσβασης - για να δώσει στον hacker περαιτέρω πρόσβαση στο backend του ιστότοπου ή στον λογαριασμό ενός συγκεκριμένου χρήστη. Όταν εισάγετε πληροφορίες σύνδεσης σε πεδία σύνδεσης, αυτές οι πληροφορίες συνήθως μετατρέπονται σε εντολή SQL. Αυτή η εντολή ελέγχει τα δεδομένα που έχετε εισαγάγει σε σχέση με τον σχετικό πίνακα στη βάση δεδομένων. Εάν τα δεδομένα εισαγωγής σας ταιριάζουν με τα δεδομένα στον πίνακα, σας παρέχεται πρόσβαση, εάν όχι, λαμβάνετε το είδος του σφάλματος που θα είχατε δει όταν εισαγάγατε λάθος κωδικό πρόσβασης. Μια SQL injection είναι συνήθως μια πρόσθετη εντολή που όταν εισάγεται στη φόρμα ιστού, προσπαθεί να αλλάξει το περιεχόμενο της βάσης δεδομένων ώστε να αντικατοπτρίζει μια επιτυχημένη σύνδεση. Μπορεί επίσης να χρησιμοποιηθεί για την ανάκτηση πληροφοριών, όπως αριθμών πιστωτικών καρτών ή κωδικών πρόσβασης από μη προστατευμένους ιστότοπους.

Β. Κλοπή κωδικών πρόσβασης (FTP): Αυτός είναι ένας άλλος πολύ συνηθισμένος τρόπος παραβίασης ιστότοπων. Η παραβίαση κωδικού πρόσβασης FTP εκμεταλλεύεται το γεγονός ότι πολλοί webmasters αποθηκεύουν τις πληροφορίες σύνδεσης στον ιστότοπό τους σε υπολογιστές με χαμηλή προστασία. Ο κλέφτης αναζητά στο σύστημα του θύματος τα στοιχεία σύνδεσης FTP και στη συνέχεια τα μεταδίδει στον δικό του απομακρυσμένο υπολογιστή. Στη συνέχεια, συνδέεται στον ιστότοπο μέσω του απομακρυσμένου υπολογιστή και τροποποιεί τις ιστοσελίδες όπως θέλει.

C. Cross-site scripting. Επίσης γνωστό ως XSS (πρώην CSS), είναι ένας πολύ εύκολος τρόπος παράκαμψης ενός συστήματος ασφαλείας. Το Cross-site scripting είναι ένα κενό που είναι δύσκολο να βρεθεί σε έναν ιστότοπο, καθιστώντας το ευάλωτο σε επιθέσεις. Σε μια τυπική επίθεση XSS, ο εισβολέας μολύνει μια ιστοσελίδα με κακόβουλο κώδικα ή πρόγραμμα από την πλευρά του πελάτη. Όταν επισκέπτεστε ο πελάτης αυτήν την ιστοσελίδα, ο κώδικας μεταφορτώνεται αυτόματα στο πρόγραμμα περιήγησής σας και εκτελείται. Συνήθως, οι εισβολείς εισάγουν HTML, JavaScript, VBScript, ActiveX ή Flash σε μια ευάλωτη εφαρμογή για να σας εξαπατήσουν και να συλλέξουν εμπιστευτικές πληροφορίες.

2.2 Virus-Worms-Trojan Horses(Ιοί-Σκουλήκια-Δούρειοι ίπποι)

Οι ιοί (virus) είναι προγράμματα υπολογιστών που συνδέονται ή μολύνουν ένα σύστημα ή αρχεία και έχουν την τάση να κυκλοφορούν σε άλλους υπολογιστές σε δίκτυο. Διακόπτουν τη λειτουργία του υπολογιστή και επηρεάζουν τα αποθηκευμένα δεδομένα - είτε τροποποιώντας τα είτε διαγράφοντας τα εντελώς.

Τα σκουλήκια(worms) σε αντίθεση με τους ιούς δεν χρειάζονται έναν οικοδεσπότη για να προσκολληθούν. Απλώς αναπαράγονται έως ότου καταναλώσουν όλη τη διαθέσιμη

μνήμη στο σύστημα. Ο όρος «σκουλήκι » μερικές φορές χρησιμοποιείται για να σημαίνει αυτοαναπαραγούμενο «κακόβουλο λογισμικό».

Οι Δούρειοι ίπποι (Trojan Horses) είναι διαφορετικοί από τους ιούς στον τρόπο διάδοσής τους. Μεταμφιέζονται ως νόμιμο αρχείο, όπως συνημμένο email από έναν υποτιθέμενο φίλο με πολύ πιστό όνομα και δεν διαδίδονται. Ο χρήστης μπορεί επίσης να εγκαταστήσει ακούσια ένα πρόγραμμα που έχει μολυνθεί από Trojan μέσω λήψεων όταν επισκέπτεται έναν ιστότοπο , παίζει διαδικτυακά παιχνίδια ή χρησιμοποιεί εφαρμογές που βασίζονται στο Διαδίκτυο. Ένας Δούρειος ίππος μπορεί να προκαλέσει ζημιά παρόμοια με άλλους ιούς, όπως κλοπή πληροφοριών ή παρεμπόδιση / διαταραχή της λειτουργίας των υπολογιστικών.

Πώς προκαλείται η βλάβη; Ο κακόβουλος κώδικας ή ο ιός εισάγεται στην αλυσίδα εντολών έτσι ώστε όταν εκτελείται το μολυσμένο πρόγραμμα, εκτελείται επίσης ο ιικός κώδικας (ή σε ορισμένες περιπτώσεις, τρέχει αντί για το νόμιμο πρόγραμμα). Οι ιοί θεωρούνται συνήθως ως ξένος κώδικας που συνδέεται με ένα πρόγραμμα φιλοξενίας, αλλά αυτό δεν συμβαίνει πάντα. Μερικές φορές, το περιβάλλον παραποιείται έτσι ώστε η κλήση ενός νόμιμου μη μολυσμένου προγράμματος καλεί το πρόγραμμα ιό . Το πρόγραμμα ιός μπορεί επίσης να εκτελεστεί πριν από την εκτέλεση οποιουδήποτε άλλου προγράμματος. Αυτό μπορεί να μολύνει σχεδόν κάθε εκτελέσιμο αρχείο στον υπολογιστή, παρόλο που κανένας από αυτούς τους κωδικούς δεν έχει αλλοιωθεί. Οι ιοί που ακολουθούν αυτό το modus operandi περιλαμβάνουν ιούς "cluster" ή "FAT" (Πίνακας κατανομής αρχείων), οι οποίοι ανακατευθύνουν το σύστημα που οδηγεί σε μολυσμένα αρχεία, συσχετίζουν ιούς και ιούς που τροποποιούν τις καταχωρίσεις καταλόγου των Windows Registry έτσι ώστε ο δικός τους κώδικας να εκτελείται πριν από οποιονδήποτε άλλο νόμιμο πρόγραμμα. Οι ιοί υπολογιστών εξαπλώνονται συνήθως μέσω αφαιρούμενων μέσων ή του Διαδικτύου. Ένας δίσκος flash, CD-ROM, ή άλλη συσκευή αποθήκευσης που έχει μολυνθεί στον αρχικό υπολογιστή μολύνει όλους τους μελλοντικούς υπολογιστές στους οποίους χρησιμοποιείται. Ο υπολογιστής μπορεί επίσης να προσβληθεί από ιούς από συνημμένα email, ψευδο-ιστότοπους ή μολυσμένο λογισμικό. Και αυτά διαδίδονται σε κάθε άλλο υπολογιστή συνδεδεμένο στο ίδιο δίκτυο. Όλοι οι ιοί υπολογιστών προκαλούν άμεσες ή έμμεσες οικονομικές ζημιές. Με βάση αυτό, υπάρχουν δύο κατηγορίες ιών: 1) Αυτοί που δεν προκαλούν σκόπιμη βλάβη 2) Εκείνοι που έχουν προγραμματιστεί να προκαλέσουν βλάβη. Ωστόσο, ακόμη και με τη διάδοση, καταλαμβάνουν άφθονο χώρο μνήμης και χρόνο και πόρους που δαπανώνται για την εργασία καθαρισμού. Οι άμεσες οικονομικές ζημιές προκαλούνται όταν οι ιοί αλλάζουν τις πληροφορίες κατά την ψηφιακή μετάδοση. Σημαντικά έξοδα επιβαρύνουν άτομα, εταιρείες και αρχές για την ανάπτυξη και εφαρμογή των εργαλείων προστασίας από ιούς για την προστασία συστημάτων υπολογιστών.

2.3 Logic Bombs

Μια logic bomb, επίσης γνωστή ως "slag code", είναι ένα κομμάτι κακόβουλου κώδικα που εισάγεται σκόπιμα σε λογισμικό για την εκτέλεση μιας κακόβουλης εργασίας όταν ενεργοποιείται από ένα συγκεκριμένο συμβάν. Δεν είναι ιός, αν και συμπεριφέρεται συνήθως με παρόμοιο τρόπο. Εισάγεται κρυφά στο πρόγραμμα όπου βρίσκεται αδρανής έως ότου πληρούνται συγκεκριμένες προϋποθέσεις. Κακόβουλο λογισμικό όπως ιοί και worms συχνά περιέχουν λογικές βόμβες που ενεργοποιούνται σε ένα συγκεκριμένο κρίσιμο σημείο του κώδικα ή σε προκαθορισμένο χρόνο. Το κρίσιμο σημείο μιας λογικής βόμβας είναι άγνωστο στον χρήστη του λογισμικού και η εργασία που εκτελεί είναι προφανώς ανεπιθύμητη. Οι κώδικες του προγράμματος που έχουν προγραμματιστεί να εκτελεστούν σε μια συγκεκριμένη ώρα είναι γνωστοί ως "ωρολογιακές βόμβες". Για παράδειγμα, ο περίφημος ιός «Παρασκευή το 13ο» που επιτέθηκε στα συστήματα ξενιστή μόνο σε συγκεκριμένες ημερομηνίες, δηλαδή Παρασκευή που έπρεπε να είναι η δέκατη τρίτη μέρα του μήνα, προκαλώντας έτσι επιβράδυνση του συστήματος.

Οι logic bombs χρησιμοποιούνται συνήθως από δυσαρεστημένους υπαλλήλους που εργάζονται στον τομέα της πληροφορικής. Ευρέως γνωστό είναι το «σύνδρομο δυσαρεστημένων υπαλλήλων» όπου οι θυμωμένοι υπάλληλοι που έχουν απολυθεί χρησιμοποιούν logic bombs για να διαγράψουν τις βάσεις δεδομένων των εργοδοτών τους, να διακόψουν το δίκτυο για λίγο ή ακόμα και να κάνουν ανταλλαγή πληροφοριών από μέσα. Οι κανόνες ενεργοποίησης που σχετίζονται με την εκτέλεση logic bombs μπορεί να είναι μια συγκεκριμένη ημερομηνία και ώρα, μια καταχώριση που λείπει από μια βάση δεδομένων ή η μη εκτέλεση μιας εντολής τη συνηθισμένη ώρα, που σημαίνει ότι το άτομο δεν βρίσκεται πια εκεί. Οι περισσότερες logic bombs παραμένουν μόνο στο δίκτυο στο οποίο χρησιμοποιούνται. Έτσι, στις περισσότερες περιπτώσεις, είναι δουλειά εμπιστευτικών πληροφοριών. Αυτό τις καθιστά πιο εύκολο να σχεδιαστούν και να εκτελεστούν από έναν ιό.

Υπάρχει μια ακόμα χρήση των logic bombs αυτή είναι η πραγματοποίηση δοκιμών λογισμικού. Το ενσωματωμένο κομμάτι κώδικα καταστρέφει το λογισμικό μετά από μια καθορισμένη χρονική περίοδο ή το καθιστά άχρηστο έως ότου ο χρήστης πληρώσει για την περαιτέρω χρήση του. Αν και αυτό το κομμάτι κώδικα χρησιμοποιεί την ίδια τεχνική με μια logic bomb, έχει μια μη καταστρεπτική, μη κακόβουλη και διαφανή για τον χρήστη χρήση.

2.4 Επίθεση Άρνησης Υπηρεσιών (DOS)

Η επίθεση άρνησης υπηρεσίας (DoS) είναι μια απόπειρα από τους εισβολείς να αρνηθούν την υπηρεσία στους προοριζόμενους χρήστες αυτής της υπηρεσίας. Περιλαμβάνει την πλημμύρα ενός διακομιστή με περισσότερα αιτήματα από ό, τι μπορεί να χειριστεί και την κατανάλωση του διαθέσιμου εύρους ζώνης που έχει ως αποτέλεσμα υπερφόρτωση του . Αυτό αναγκάζει τον πόρο (π.χ. διακομιστή ιστού) να καταρρεύσει ή να επιβραδυνθεί σημαντικά, ώστε κανείς να μην έχει πρόσβαση σε αυτόν. Χρησιμοποιώντας αυτήν την τεχνική, ο εισβολέας μπορεί να καταστήσει έναν ιστότοπο μη λειτουργικό στέλνοντας τεράστιες ποσότητες επισκεψιμότητας στον στοχευμένο ιστότοπο. Ένας ιστότοπος μπορεί προσωρινά να δυσλειτουργεί ή να καταρρέει εντελώς,

σε κάθε περίπτωση με αποτέλεσμα την αδυναμία του συστήματος να επικοινωνήσει επαρκώς. Οι επιθέσεις DoS παραβιάζουν τις πολιτικές ορθής και αποδεκτής χρήσης σχεδόν όλων των παρόχων υπηρεσιών Διαδικτύου. Μια άλλη παραλλαγή μιας επίθεσης άρνησης υπηρεσίας είναι γνωστή ως επίθεση «Κατανεμημένη Άρνηση Υπηρεσίας» (DDoS) όπου ένας αριθμός γεωγραφικά διαδεδομένων δραστών πλημμυρίζει την κυκλοφορία του δικτύου. Οι επιθέσεις άρνησης υπηρεσίας συνήθως στοχεύουν διακομιστές ιστοτόπων υψηλού προφίλ που ανήκουν σε τράπεζες και πύλες πληρωμής με πιστωτική κάρτα.

2.5 Ηλεκτρονικό Ψάρεμα (Phising)

Αυτή είναι μια τεχνική εξαγωγής εμπιστευτικών πληροφοριών, όπως αριθμοί πιστωτικών καρτών και συνδυασμοί κωδικών πρόσβασης ονόματος χρήστη, μεταμφιέζοντας ως νόμιμη επιχείρηση. Το ηλεκτρονικό ψάρεμα πραγματοποιείται συνήθως μέσω πλαστογράφησης email.

Το κακόβουλο λογισμικό θα έχει εγκατασταθεί στον υπολογιστή σας και θα έχει κλέψει προσωπικές πληροφορίες. Οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν την κοινωνική μηχανική για να μας εξαπατήσουν ώστε να κατεβάσουμε κακόβουλο λογισμικό από το Διαδίκτυο ή να μας κάνουν να συμπληρώσουμε τα προσωπικά μας στοιχεία με ψευδείς προσχηματισμούς. Μια απάτη ηλεκτρονικού ψαρέματος (phishing) σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου μπορεί να αποφευχθεί, λαμβάνοντας υπόψη ορισμένα πράγματα. Ορθογραφικά λάθη στο κείμενο. Οι εγκληματίες στον κυβερνοχώρο δεν είναι γνωστοί για τη γραμματική και την ορθογραφία τους. Ο σύνδεσμος URL να ταιριάζει με αυτόν που αναγράφεται στο mail. Οι εισβολείς χρησιμοποιούν τα ονόματα και τα λογότυπα γνωστών ιστοτόπων για να εξαπατήσουν. Τα γραφικά και οι διευθύνσεις ιστού που χρησιμοποιούνται στο email είναι εντυπωσιακά παρόμοιες με τις νόμιμες, αλλά να οδηγούν σε ψεύτικους ιστότοπους.

Το ηλεκτρονικό ψάρεμα δεν γίνεται μόνο μέσω email ή ιστότοπων, περιλαμβάνει και κλήσεις σε θύματα που χρησιμοποιούν ψεύτικη ταυτότητα ώστε να ξεγελάσουν ότι η κλήση προέρχεται από έναν αξιόπιστο οργανισμό. Μπορεί να ισχυρίζονται ότι προέρχονται από τράπεζα και να ζητούν την κλήση σε έναν αριθμό (παρέχεται από την υπηρεσία VoIP και ανήκει σε εισβολέα) και την εισαγωγή στοιχείων λογαριασμού. Μολις γίνει αυτό, η ασφάλεια του λογαριασμού διακυβεύεται.

2.6 Email Bombing - Spamming

Ο βομβαρδισμός μέσω email χαρακτηρίζεται από έναν θύτη που στέλνει τεράστιους όγκους email σε μια ηλεκτρονική διεύθυνση με αποτέλεσμα ο λογαριασμός email του θύματος ή οι διακομιστές αλληλογραφίας να καταρρέουν. Το μήνυμα δεν έχει νόημα και είναι υπερβολικά μεγάλο για να καταναλώνει πόρους δικτύου. Εάν στοχεύονται πολλοί λογαριασμοί διακομιστή αλληλογραφίας, ενδέχεται να έχει αντίκτυπο στην άρνηση υπηρεσίας. Τέτοια μηνύματα που φθάνουν συχνά στα εισερχόμενά μπορούν εύκολα να εντοπιστούν από φίλτρα ανεπιθύμητης αλληλογραφίας. Ο βομβαρδισμός μέσω email πραγματοποιείται συνήθως χρησιμοποιώντας botnets (ιδιωτικούς υπολογιστές με

σύνδεση στο Διαδίκτυο των οποίων η ασφάλεια έχει παραβιαστεί από κακόβουλο λογισμικό και είναι υπό τον έλεγχο του εισβολέα) ως επίθεση DDoS.

Αυτός ο τύπος επίθεσης είναι πιο δύσκολος να ελεγχθεί λόγω πολλαπλών διευθύνσεων προέλευσης και των bots που έχουν προγραμματιστεί να στέλνουν διαφορετικά μηνύματα για να νικήσουν τα φίλτρα ανεπιθύμητων μηνυμάτων. Το "Spamming" είναι μια παραλλαγή του βομβαρδισμού μέσω email. Εδώ αποστέλλονται ανεπιθύμητα μαζικά μηνύματα σε μεγάλο αριθμό χρηστών. Το άνοιγμα συνδέσμων που παρέχονται σε ανεπιθύμητα μηνύματα ενδέχεται να οδηγήσει σε ιστότοπους ηλεκτρονικού ψαρέματος που φιλοξενούν κακόβουλο λογισμικό. Τα ανεπιθύμητα μηνύματα ενδέχεται επίσης να έχουν μολυσμένα αρχεία ως συνημμένα. Η αποστολή ανεπιθύμητων μηνυμάτων μέσω ηλεκτρονικού ταχυδρομείου επιδεινώνεται όταν ο παραλήπτης απαντά στο μήνυμα ηλεκτρονικού ταχυδρομείου προκαλώντας σε όλους τους αρχικούς παραλήπτες να λάβουν την απάντηση. Οι Spammers συλλέγουν διευθύνσεις ηλεκτρονικού ταχυδρομείου από λίστες πελατών, ομάδες συνομιλιών, αίθουσες συνομιλιών, ιστότοπους και ιούς που συλλέγουν βιβλία διευθύνσεων των χρηστών και τα πωλούν και σε άλλους spammers. Ένα μεγάλο αριθμό ανεπιθύμητων μηνυμάτων αποστέλλεται σε μη έγκυρες διευθύνσεις email.

Η αποστολή ανεπιθύμητων μηνυμάτων παραβιάζει την αποδεκτή πολιτική χρήσης (AUP) σχεδόν όλων των παρόχων υπηρεσιών διαδικτύου. Εάν το σύστημά ξαφνικά καθυστερήσει (το ηλεκτρονικό ταχυδρομείο φορτώνεται αργά ή δεν φαίνεται να αποστέλλεται ή να λαμβάνεται), ο λόγος μπορεί να είναι ότι ο mail server σας επεξεργάζεται μεγάλο αριθμό μηνυμάτων. Δυστυχώς, αυτήν τη στιγμή, δεν υπάρχει τρόπος να αποφευχθεί εντελώς η βομβιστική αλληλογραφία και τα ανεπιθύμητα μηνύματα, καθώς είναι αδύνατο να προβλεφθεί η προέλευση της επόμενης επίθεσης.

2.7 Web Jacking

Το web jacking έχει πάρει το όνομά του από την «πειρατεία». Εδώ, ο χάκερ παίρνει τον έλεγχο μιας ιστοσελίδας με δόλο. Μπορεί να αλλάξει το περιεχόμενο του αρχικού ιστότοπου ή ακόμα και να ανακατευθύνει τον χρήστη σε μια άλλη ψεύτικη παρόμοια σελίδα που ελέγχεται από αυτόν. Ο ιδιοκτήτης της ιστοσελίδας δεν έχει πλέον έλεγχο και ο εισβολέας μπορεί να χρησιμοποιήσει τον ιστότοπο για τα προσωπικά του συμφέροντα. Έχουν αναφερθεί περιπτώσεις όπου ο εισβολέας ζήτησε λύτρα, ή ακόμη δημοσίευσε και άσεμνο υλικό στον ιστότοπο.

Η μέθοδος επίθεσης Web jacking μπορεί να χρησιμοποιηθεί για να δημιουργήσει έναν κλώνο του ιστότοπου και να παρουσιάσει στο θύμα τον νέο σύνδεσμο λέγοντας ότι ο ιστότοπος έχει μετακινηθεί. Σε αντίθεση με τις συνήθεις μεθόδους ηλεκτρονικού ψαρέματος, όταν τοποθετείτε το δείκτη του ποντικιού πάνω από τον παρεχόμενο σύνδεσμο, η διεύθυνση URL που εμφανίζεται θα είναι η αρχική και όχι ο ιστότοπος του εισβολέα. Αλλά όταν κάνετε κλικ στο νέο σύνδεσμο, ανοίγει και αντικαθίσταται γρήγορα με τον κακόβουλο διακομιστή ιστού. Το όνομα στη γραμμή διευθύνσεων θα είναι ελαφρώς διαφορετικό από τον αρχικό ιστότοπο που μπορεί να εξαπατήσει τον χρήστη να

θεωρήσει ότι είναι ένας νόμιμος ιστότοπος. Για παράδειγμα, το "gmail" μπορεί να σας κατευθύνει στο "gmai1",το "1" στη θέση "L" μπορεί να αγνοηθεί εύκολα.

Το Web Jacking μπορεί επίσης να γίνει στέλνοντας ένα πλαστό μήνυμα στον καταχωρητή που ελέγχει την καταχώριση ονομάτων, με ψευδή ταυτότητα ζητώντας του να συνδέσει ένα όνομα στη διεύθυνση IP του webjacker, στέλνοντας έτσι ανυποψίαστους καταναλωτές που εισάγουν το συγκεκριμένο όνομα τομέα σε έναν ιστότοπο που ελέγχεται από τον webjacker. Ο σκοπός αυτής της επίθεσης είναι να προσπαθήσει να συλλέξει τα διαπιστευτήρια, τα ονόματα χρήστη, τους κωδικούς πρόσβασης και τους αριθμούς λογαριασμού των χρηστών χρησιμοποιώντας μια πλαστή ιστοσελίδα με έναν έγκυρο σύνδεσμο που ανοίγει όταν ο χρήστης ανακατευθύνεται σε αυτήν μετά το άνοιγμα του νόμιμου ιστότοπου.

2.8 Cyber Stalking (Καταδίωξη στον κυβερνοχώρο)

Η καταδίωξη στον κυβερνοχώρο είναι μια νέα μορφή εγκλήματος στο Διαδίκτυο, είναι όταν ένα άτομο επιδιώκεται ή παρακολουθείται στο Διαδίκτυο. Ένας καταδιώκτης στον κυβερνοχώρο δεν ακολουθεί φυσικά το θύμα του, το κάνει ουσιαστικά ακολουθώντας τη διαδικτυακή του δραστηριότητα για να συλλέξει πληροφορίες και να τον παρενοχλήσει και να κάνει απειλές χρησιμοποιώντας λεκτικό εκφοβισμό. Είναι μια εισβολή στο διαδικτυακό απόρρητο κάποιου. Η ηλεκτρονική καταδίωξη χρησιμοποιεί το Διαδίκτυο ή οποιοδήποτε άλλο ηλεκτρονικό μέσο και διαφέρει από τη καταδίωξη εκτός σύνδεσης, αλλά συνήθως συνοδεύεται από αυτό. Τα περισσότερα θύματα αυτού του εγκλήματος είναι γυναίκες που καταδιώκονται από άνδρες και παιδιά που καταδιώκονται από ενήλικες θηρευτές και παιδόφιλους. Οι διαδικτυακοί καταστολείς ευδοκιμούν σε άπειρους χρήστες του διαδικτύου που δεν γνωρίζουν καλά τη δικτυακή δικτύωση και τους κανόνες ασφάλειας του Διαδικτύου. Ένας καταδιώκτης του κυβερνοχώρου είναι συνήθως ένας άγνωστος προς το θύμα, αλλά θα μπορούσε εξίσου εύκολα να είναι κάποιος από το οικείο περιβάλλον του.

Οι διαδικτυακοί διώκτες παρενοχλούν τα θύματά τους μέσω email, chat room, ιστοσελίδων, φόρουμ συζητήσεων και ανοιχτών ιστότοπων δημοσίευσης (π.χ. blogs). Η διαθεσιμότητα δωρεάν χώρου ηλεκτρονικού ταχυδρομείου / ιστότοπου και η ανωνυμία που παρέχονται από τα δωμάτια συνομιλίας και τα φόρουμ συνέβαλαν στην αύξηση των περιστατικών στον κυβερνοχώρο. Ο καθένας έχει μια διαδικτυακή παρουσία στις μέρες μας και είναι πολύ εύκολο με μια αναζήτηση στο Google και να αποκτήσετε το όνομα, το ψευδώνυμο, τον αριθμό επικοινωνίας και τη διεύθυνση, συμβάλλοντας στην αύξηση της απειλής στον κυβερνοχώρο. Καθώς το Διαδίκτυο γίνεται ολοένα και περισσότερο αναπόσπαστο κομμάτι της προσωπικής και επαγγελματικής μας ζωής, οι καταδιώκτες μπορούν να επωφεληθούν από την ευκολία επικοινωνίας και τη διαθεσιμότητα προσωπικών πληροφοριών με λίγα μόνο κλικ με το ποντίκι. Η καταδίωξη στον κυβερνοχώρο γίνεται με δύο βασικούς τρόπους.

Διαδικτυακή καταδίωξη: Εδώ ο καταδιώκτης παρενοχλεί το θύμα μέσω του Διαδικτύου. Το ανεπιθύμητο μήνυμα ηλεκτρονικού ταχυδρομείου είναι ο πιο συνηθισμένος τρόπος απειλής κάποιου ατόμου και ο καταδιώκτης μπορεί ακόμη και να

στείλει άσεμνο περιεχόμενο και ιούς μέσω email. Ωστόσο, μόνο οι ιοί και τα ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου τηλεμάρκετινγκ δεν αποτελούν καταδίωξη στον κυβερνοχώρο. Εάν όμως το ηλεκτρονικό ταχυδρομείο αποστέλλεται επανειλημμένα σε μια προσπάθεια εκφοβισμού του παραλήπτη, μπορεί να θεωρηθεί ως καταδίωξη. Η καταδίωξη στο Διαδίκτυο δεν περιορίζεται στο ηλεκτρονικό ταχυδρομείο. Οι καταδιώκτες μπορούν να χρησιμοποιήσουν πληρέστερα το Διαδίκτυο για να παρενοχλήσουν τα θύματα. Οποιοδήποτε άλλο έγκλημα στον κυβερνοχώρο για το οποίο έχουμε ήδη διαβάσει, εάν γίνει με σκοπό να απειλήσει, να παρενοχλήσει ή να συκοφαντήσει το θύμα μπορεί να ισοδυναμεί με καταδίωξη στον κυβερνοχώρο.

Computer Stalking: Οι πιο τεχνολογικά προηγμένοι καταδιώκτες εφαρμόζουν τις δεξιότητές τους στον υπολογιστή για να τους βοηθήσουν στο έγκλημα. Αποκτούν μη εξουσιοδοτημένο έλεγχο του υπολογιστή του θύματος εκμεταλλευόμενοι τη λειτουργία του διαδικτύου και του λειτουργικού συστήματος των Windows. Αν και αυτό γίνεται συνήθως από έμπειρους, οι οδηγίες για το πώς να το επιτύχουν είναι εύκολα διαθέσιμες στο Διαδίκτυο.

Το Cyber stalking έχει πλέον απλώσει τα φτερά του και στην κοινωνική δικτύωση. Με την αυξημένη χρήση των κοινωνικών μέσων όπως το Facebook, το Twitter, το Flickr και το YouTube, το προφίλ, οι φωτογραφίες και οι ενημερώσεις κατάστασης είναι ανοιχτά προς τον κόσμο. Η διαδικτυακή παρουσία παρέχει αρκετές πληροφορίες ώστε οι διώκτες να βρίσκουν τα πιθανα θύματα καταδίωξης χωρίς καν αυτά να γνωρίζουν τον κίνδυνο. Με τα «check-in», τα «γεγονότα ζωής», τις εφαρμογές που έχουν πρόσβαση στα προσωπικά στοιχεία. Η τεχνολογία κοινωνικής δικτύωσης παρέχει μια κοινωνική και συνεργατική πλατφόρμα για τους χρήστες του Διαδικτύου να αλληλεπιδρούν, να εκφράζουν τις σκέψεις τους και να μοιράζονται σχεδόν τα πάντα για τη ζωή τους. Αν και προωθεί την κοινωνικοποίηση μεταξύ των ανθρώπων, στην πορεία συμβάλλει στην αύξηση των παραβιάσεων στο Διαδίκτυο.

2.9 Data Diddling

Το Data Diddling είναι μια μη εξουσιοδοτημένη αλλαγή δεδομένων πριν ή κατά τη διάρκεια της εισόδου σε ένα σύστημα υπολογιστή και η αλλαγή μετά την ολοκλήρωση της επεξεργασίας. Χρησιμοποιώντας αυτήν την τεχνική, ο εισβολέας μπορεί να τροποποιήσει την αναμενόμενη έξοδο και είναι δύσκολο να εντοπιστεί. Με άλλα λόγια, οι αρχικές πληροφορίες που πρέπει να εισαχθούν αλλάζουν, είτε από ένα άτομο που πληκτρολογεί τα δεδομένα, έναν ιό που έχει προγραμματιστεί να αλλάξει τα δεδομένα, τον προγραμματιστή της βάσης δεδομένων ή της εφαρμογής ή οποιονδήποτε άλλον εμπλέκεται στη διαδικασία δημιουργίας, εγγραφής , κωδικοποίησης, εξέτασης, ελέγχου, μετατροπής ή μετάδοσης δεδομένων.

Αυτή είναι μια από τις απλούστερες μεθόδους διάπραξης εγκλήματος που σχετίζεται με τον υπολογιστή, γιατί ακόμη και ένας ερασιτέχνης υπολογιστών μπορεί να το κάνει. Παρά το γεγονός ότι είναι μια εύκολη εργασία, μπορεί να έχει επιζήμια αποτελέσματα. Για παράδειγμα, ένα άτομο που είναι υπεύθυνο για τη λογιστική μπορεί να αλλάξει δεδομένα για τον εαυτό του ή έναν φίλο ή συγγενή του, δείχνοντας ότι

πληρώνονται πλήρως. Αλλάζοντας ή μη εισάγοντας τις πληροφορίες, μπορούν να κλέψουν την επιχείρηση. Άλλα παραδείγματα περιλαμβάνουν πλαστογράφηση ή παραποίηση εγγράφων και ανταλλαγή έγκυρων ταινιών ή καρτών υπολογιστή με έτοιμες αντικαταστάσεις.

2.10 Κλοπή Ταυτότητας και Πιστωτικής Κάρτας

Η κλοπή ταυτότητας συμβαίνει όταν κάποιος κλέβει την ταυτότητά ενός ατόμου και προσποιείται ότι είναι εκείνος για πρόσβαση σε πόρους όπως πιστωτικές κάρτες, τραπεζικούς λογαριασμούς και άλλα οφέλη στο όνομά του. Ο απατεώνας μπορεί επίσης να χρησιμοποιήσει την ταυτότητά για να διαπράξει άλλα εγκλήματα. Η «απάτη με πιστωτική κάρτα» είναι ένας ευρύς όρος για εγκλήματα που περιλαμβάνουν κλοπή ταυτότητας, όπου ο εγκληματίας χρησιμοποιεί την πιστωτική κάρτα για να χρηματοδοτήσει τις συναλλαγές του. Η απάτη με πιστωτική κάρτα είναι κλοπή ταυτότητας με την απλούστερη μορφή της. Η πιο συνηθισμένη περίπτωση απάτης με πιστωτικές κάρτες είναι η προ-εγκεκριμένη κάρτα να πέσει στα χέρια κάποιου άλλου.

Μπορεί να το χρησιμοποιήθει για την αγορά οτιδήποτε μέχρι να αναφέρθει στις αρχές η κλοπή και να γίνει μπλοκάρισμα την κάρτα. Το μόνο μέτρο ασφαλείας στις αγορές πιστωτικών καρτών είναι η υπογραφή στην απόδειξη, αλλά μπορεί και αυτή πολύ εύκολα να πλαστογραφηθεί. Ωστόσο, σε ορισμένες χώρες ο έμπορος μπορεί ακόμη και να ζητήσει ένα αναγνωριστικό ή έναν κωδικό PIN. Ορισμένες εταιρείες πιστωτικών καρτών διαθέτουν λογισμικό για την εκτίμηση της πιθανότητας απάτης. Εάν γίνει μια ασυνήθιστα μεγάλη συναλλαγή, ο εκδότης μπορεί ακόμη και να καλέσει για επαλήθευση.

Συχνά οι άνθρωποι ξεχνούν να παραλάβουν το αντίγραφο της απόδειξης της πιστωτικής κάρτας μετά το φαγητό τους σε εστιατόρια ή αλλού όταν πληρώνουν με πιστωτική κάρτα. Αυτές οι αποδείξεις έχουν τον αριθμό της πιστωτικής σας κάρτας και την υπογραφή για οποιονδήποτε μπορεί να τις δει και να τις χρησιμοποιήσει. Με μόνο αυτές τις πληροφορίες, κάποιος μπορεί να πραγματοποιήσει αγορές στο διαδίκτυο ή μέσω τηλεφώνου. Δεν θα γίνει αντιληπτό έως ότου εκδοθεί η μηνιαία κατάσταση λογαριασμού. Να γίνεται έλεγχος ότι ένας ιστότοπος είναι αξιόπιστος και ασφαλής όταν πραγματοποιούνται αγορές στο Διαδίκτυο. Ορισμένοι χάκερ μπορεί να κρατήσουν τον αριθμό της πιστωτικής κάρτας χρησιμοποιώντας τεχνικές ηλεκτρονικού ψαρέματος. Μερικές φορές εμφανίζεται ένα μικρό εικονίδιο λουκέτου στην αριστερή γωνία της γραμμής διευθύνσεων στο πρόγραμμα περιήγησής, το οποίο παρέχει υψηλότερο επίπεδο ασφάλειας για τη μετάδοση δεδομένων. Με ένα κλικ σε αυτό, φαίνεται το λογισμικό κρυπτογράφησης που χρησιμοποιεί.

Μια πιο σοβαρή ανησυχία είναι η χρήση των προσωπικών στοιχείων με τη βοήθεια κλεμμένων ή πλαστών εγγράφων για το άνοιγμα λογαριασμών (ή ακόμα χειρότερα, χρησιμοποιώντας τον υπάρχοντα λογαριασμό) για τη λήψη δανείου. Αυτοί οι αδίστακτοι άνθρωποι μπορούν να συλλέξουν τα προσωπικά στοιχεία από το γραμματοκιβώτιό ή τον κάδο απορριμμάτων.

Με τις αυξανόμενες περιπτώσεις απάτης με πιστωτικές κάρτες, πολλά χρηματοπιστωτικά ιδρύματα παρενέβησαν με λύσεις λογισμικού για την παρακολούθηση της πίστωσης και την προστασία της ταυτότητάς. Ασφάλιση κλοπής ταυτότητας μπορεί να ληφθεί για την ανάκτηση χαμένων μισθών και την αποκατάσταση της πίστωσής.

2.11 Salami Slicing

Η "salami slicing attack" ή "salami fraud" είναι μια τεχνική με την οποία οι εγκληματίες στον κυβερνοχώρο κλέβουν χρήματα ή πόρους λίγο κάθε φορά, έτσι ώστε να μην υπάρχει αισθητή διαφορά στο συνολικό μέγεθος. Ο δράστης ξεφεύγει με αυτά τα μικρά κομμάτια από μεγάλο αριθμό πόρων και έτσι συγκεντρώνει ένα σημαντικό ποσό για μια χρονική περίοδο. Η ουσία αυτής της μεθόδου είναι η αποτυχία εντοπισμού της κατάχρησης.

Οι εισβολείς εισάγουν ένα πρόγραμμα στο σύστημα για την αυτόματη εκτέλεση της εργασίας. Logic bombs μπορούν επίσης να χρησιμοποιηθούν από ανικανοποίητους άπληστους υπαλλήλους που εκμεταλλεύονται την τεχνογνωσία τους για το δίκτυο ή και την προνομιακή πρόσβαση στο σύστημα. Σε αυτήν την τεχνική, οι εγκληματίες προγραμματίζουν τους αριθμητικούς υπολογιστές για την αυτόματη τροποποίηση δεδομένων, όπως στους υπολογισμούς ενδιαφέροντος.

Η κλοπή χρημάτων ηλεκτρονικά είναι η πιο κοινή χρήση της τεχνικής Salami slicing, αλλά δεν περιορίζεται στη νομιμοποίηση εσόδων από παράνομες δραστηριότητες. Η salami slicing μπορεί επίσης να εφαρμοστεί για τη συλλογή μικρών πληροφοριών για μια χρονική περίοδο για να συναχθεί μια συνολική εικόνα ενός οργανισμού. Αυτή η πράξη συλλογής κατανεμημένων πληροφοριών μπορεί να είναι ενάντια σε άτομο ή οργανισμό. Τα δεδομένα μπορούν να συλλεχθούν από ιστοτόπους, διαφημίσεις, έγγραφα που συλλέγονται από κάδους απορριμμάτων και παρόμοια, δημιουργώντας σταδιακά μια ολόκληρη βάση δεδομένων πραγματικών πληροφοριών σχετικά με τον στόχο.

Δεδομένου ότι το ποσό της υπεξαίρεσης είναι ακριβώς κάτω από το όριο της αντίληψης, η προσεκτική εξέταση των περιουσιακών στοιχείων, των συναλλαγών και κάθε άλλης συναλλαγής, συμπεριλαμβανομένης της κοινοποίησης εμπιστευτικών πληροφοριών με άλλους, μπορεί να βοηθήσει στη μείωση των πιθανοτήτων επίθεσης με αυτήν τη μέθοδο.

2.12 Software Piracy (Πειρατεία Λογισμικού)

Χάρη στο Διαδίκτυο και τα torrents, είναι εύκολη η εύρεση σχεδόν οποιασδήποτε ταινίας , λογισμικού ή τραγουδιού από οποιαδήποτε προέλευση δωρεάν. Η πειρατεία στο Διαδίκτυο είναι αναπόσπαστο κομμάτι της ζωής μας στην οποία συνειδητά ή εν αγνοία μας συμβάλλουμε όλοι. Με αυτόν τον τρόπο, τα κέρδη των προγραμματιστών πόρων μειώνονται. Δεν πρόκειται μόνο για παράνομη χρήση της πνευματικής ιδιοκτησίας κάποιου άλλου, αλλά και για τη διανομή της μειώνοντας περαιτέρω τα έσοδα που τους αξίζουν.

Η πειρατεία λογισμικού είναι η μη εξουσιοδοτημένη χρήση και διανομή λογισμικού υπολογιστή. Οι προγραμματιστές λογισμικού εργάζονται σκληρά για την ανάπτυξη αυτών των προγραμμάτων και η πειρατεία περιορίζει την ικανότητά τους να παράγουν αρκετά έσοδα για να διατηρήσουν την ανάπτυξη εφαρμογών. Αυτό επηρεάζει ολόκληρη την παγκόσμια οικονομία καθώς τα κεφάλαια μεταφέρονται από άλλους τομείς που οδηγούν σε λιγότερες επενδύσεις στο μάρκετινγκ και την έρευνα. Τα ακόλουθα αποτελούν πειρατεία λογισμικού:

Φόρτωση λογισμικού χωρίς άδεια στον υπολογιστή.

Χρήση λογισμικού μίας άδειας σε πολλούς υπολογιστές.

Χρήση μίας γεννήτριας κλειδιών για την παράκαμψη της προστασίας αντιγραφής.

Διανομή αδειοδοτημένης ή μη αδειοδοτημένης («σπασμένης») έκδοσης λογισμικού μέσω Διαδικτύου και εκτός.

Η "κλωνοποίηση" είναι μια άλλη απειλή. Συμβαίνει όταν κάποιος αντιγράφει την ιδέα πίσω από το λογισμικό και γράφει τον δικό του κωδικό. Δεδομένου ότι οι ιδέες δεν προστατεύονται διαρκώς από αντιγραφή, αυτό δεν είναι απολύτως παράνομο. Ένα λογισμικό "crack" είναι μια παράνομα ληφθείσα έκδοση του λογισμικού που λειτουργεί ως προς την πρόληψη της κωδικοποίησης αντιγραφής. Οι χρήστες πειρατικού λογισμικού μπορούν να χρησιμοποιήσουν μια γεννήτρια κλειδιών για να δημιουργήσουν έναν «σειριακό» αριθμό που ξεκλειδώνει μια έκδοση αξιολόγησης του λογισμικού, καταργώντας έτσι την προστασία αντιγραφής. Το σπάσιμο του λογισμικού και η χρήση μη εξουσιοδοτημένων κλειδιών είναι παράνομες πράξεις παραβίασης πνευματικών δικαιωμάτων.

Η χρήση πειρατικών υλικών ενέχει τους δικούς της κινδύνους. Το πειρατικό λογισμικό μπορεί να περιέχει Trojans, ιούς, worms και άλλα κακόβουλα προγράμματα, καθώς οι πειρατές συχνά μολύνουν λογισμικό με κακόβουλο κώδικα. Οι χρήστες πειρατικών προγραμμάτων ενδέχεται να τιμωρηθούν από το νόμο για παράνομη χρήση υλικού που προστατεύεται από πνευματικά δικαιώματα. Επιπλέον, δεν λαμβάνεται η υποστήριξη λογισμικού που παρέχεται από τους προγραμματιστές. Για την προστασία του λογισμικό από την πειρατεία, θα πρέπει να εφαρμοστούν ισχυρές διασφαλίσεις. Ορισμένοι ιστότοποι πωλούν λογισμικό με «ψηφιακό δακτυλικό αποτύπωμα» που βοηθά στον εντοπισμό των πειρατικών αντιγράφων στην πηγή. Μια άλλη κοινή μέθοδος είναι το κλείδωμα υλικού. Χρησιμοποιώντας αυτό, η άδεια λογισμικού κλειδώνεται σε ένα συγκεκριμένο υλικό υπολογιστή, έτσι ώστε να λειτουργεί μόνο σε αυτόν τον υπολογιστή. Δυστυχώς, οι χάκερ συνεχίζουν να βρίσκουν το δρόμο τους για αυτά τα μέτρα.

2.13 Παιδική Πορνογραφία

Η παιδική πορνογραφία είχε εμφανιστεί και αποτελούσε ένα ακανθώδες ζήτημα και πριν την εμφάνιση του διαδικτύου. Το διαδίκτυο όμως, λόγω των ιδιαίτερων χαρακτηριστικών του και του περιβάλλοντος που προσφέρει, αποτέλεσε μέσο για την ανάπτυξη και τη διάδοση της παιδικής πορνογραφίας.

Εκτός από την εύκολη και άμεση πρόσβαση που έχει ο καθένας σε πορνογραφικό υλικό κάθε είδους από κάθε μέρος του πλανήτη, το διαδίκτυο έχει και άλλα χαρακτηριστικά που ευνοούν την ανάπτυξη της παιδική πορνογραφίας. Ο παιδόφιλος με την εγγραφή του σε σελίδες που περιέχουν υλικό παιδικής πορνογραφίας γίνεται μέρος μίας κοινότητας, μπορεί να ανταλλάξει ή να προμηθευτεί υλικό παιδικής πορνογραφίας, να συζητήσει και να μοιραστεί με άλλους τις σεξουαλικές του προτιμήσεις και γενικά να «νομιμοποιήσει» τις πράξεις του, δηλαδή να μην νιώθει ενοχές ή ότι παρανομεί κατά την διακίνηση ή συλλογή πορνογραφικού υλικού. Αυτή η συναναστροφή με άτομα που έχουν τις ίδιες σεξουαλικές προτιμήσεις και απόψεις του ενισχύει την αυτοπεποίθηση και του δημιουργεί ένα αίσθημα ασφάλειας και σιγουριάς.

Στον διαδικτυακό χώρο το κάθε άτομο μπορεί πια όχι μόνο να συλλέξει υλικό παιδικής πορνογραφίας, αλλά και να μιλήσει ζωντανά με ανήλικους ή με ενήλικους που έχουν παιδοφιλικές τάσεις, καθώς και να παρακολουθήσει ζωντανά (on-line) προγράμματα σεξουαλικών δραστηριοτήτων μεταξύ ανηλίκων και ενηλίκων. Ακόμα, ο καθένας μπορεί εύκολα να προμηθεύσει τον διαδικτυακό χώρο με προσωπικό πορνογραφικό υλικό που έχει καταγράψει ο ίδιος μέσα από τις σεξουαλικές του δραστηριότητες. Με αυτόν τον τρόπο γίνεται παραγωγός, ενώ μπορεί πολύ εύκολα να γίνει και έμπορος, διανέμοντας το πορνογραφικό υλικό που διαθέτει έναντι αμοιβής. Δεν θα πρέπει να αμελείται, εξάλλου, ότι τα κέρδη από την εμπορία υλικού παιδικής πορνογραφίας υπολογίζονται σε αρκετά δισεκατομμύρια δολάρια ετησίως, ενώ στον τομέα αυτό τα κυκλώματα και οι οργανώσεις που δραστηριοποιούνται είναι αρκετά ισχυρά και οργανωμένα.

Συχνό ερώτημα αποτελεί ο τρόπος με τον οποίο διακινείται το υλικό παιδικής πορνογραφίας στο διαδίκτυο και γιατί είναι δύσκολος ο εντοπισμός των κυκλωμάτων που δραστηριοποιούνται στον τομέα αυτό. Οι ιστοσελίδες που διαθέτουν υλικό παιδικής πορνογραφίας πολύ σπάνια το διαφημίζουν και το θέτουν σε κοινή θέα, ώστε να είναι προσβάσιμο στον κάθε χρήστη. Συνήθως, οι ιστοσελίδες αυτές προσφέρουν στην δυνατότητα στους χρήστες τους να απευθυνθούν στους διαχειριστές της ιστοσελίδας, με σκοπό οι τελευταίοι να στείλουν στους χρήστες υλικό παιδικής πορνογραφίας μέσω e-mail.

Στις περιπτώσεις αυτές η πληρωμή πραγματοποιείται μέσω πιστωτικής κάρτας. Με αυτόν τον τρόπο οι ιστοσελίδες φαίνονται προς τα έξω ότι παρέχουν απλώς πορνογραφικό υλικό νόμιμα, ενώ στην πράξη προμηθεύουν τους πελάτες τους με υλικό παιδικής πορνογραφίας. Το μειονέκτημα είναι ότι ο χρήστης θα πρέπει να γνωρίζει ή να έχει πληροφορηθεί ότι η εν λόγω σελίδα παρέχει υλικό παιδικής πορνογραφίας ώστε να απευθυνθεί στους διαχειριστές της και αυτοί να τον προμηθεύσουν με το υλικό αυτό.

ΚΕΦΑΛΑΙΟ 3 – ΨΗΦΙΑΚΗ ΤΡΟΜΟΚΡΑΤΙΑ

3.1 Ορισμός

Ο όρος ψηφιακή τρομοκρατία είναι προέκταση της κλασικής τρομοκρατίας και χρησιμοποιείται για να περιγράψει την επίθεση τρομοκρατών στον κυβερνοχώρο. Είναι ευρέως γνωστό ότι τα πληροφοριακά συστήματα έχουν ευάλωτα σημεία, συνεπώς είναι πολύ πιθανόν οι τρομοκράτες να χρησιμοποιήσουν αυτά τα σημεία για να επιτεθούν στους αντιπάλους τους και να πυροδοτήσουν έναν πόλεμο πληροφοριών. Συγκεκριμένα, όπως και στην κλασική τρομοκρατία, οι επιθέσεις χωρίζονται σε δύο κατηγορίες: οι επιθέσεις κατά των πολιτών και ο προσηλυτισμός ιδεαλιστικά αδύναμων ατόμων που μπορούν να πεισθούν από την ιδεολογία των τρομοκρατών και κατ' επέκταση να επηρεάσουν ένα μεγαλύτερο κοινό. Επιπλέον, ψηφιακή τρομοκρατία έχουμε όταν οι κυβερνοεπιθέσεις οδηγούν σε τέτοιου τύπου αναστάτωση που προκαλεί τρόμο ανάλογο με την πράξη της κλασικής τρομοκρατίας. Επίσης, ψηφιακή τρομοκρατία είναι όταν παράνομες ή πολιτικά υποκινούμενες κυβερνοεπιθέσεις έχουν ως σκοπό να εκφοβίσουν ή να εξαναγκάσουν την κυβέρνηση ή τους πολίτες να προάγουν έναν πολιτικό σκοπό ή να προκαλέσουν σοβαρή βλάβη είτε σωματική, είτε οικονομική. Συνεπώς, όποια δραστηριότητα ομάδων παρακινούμενων από πολιτική, θρησκευτική ή άλλου τύπου ιδεολογία που μέσω υπολογιστών, διαδικτύου, δικτύων και πληροφοριακών συστημάτων έχουν ως σκοπό να επέμβουν στην πολιτική, κοινωνική ή οικονομική λειτουργία μίας ομάδας, ενός οργανισμού ή ενός κράτους, όπως επίσης να προκαλέσουν σωματική βία ή φόβο, ονομάζεται ψηφιακή τρομοκρατία.

3.2 Κατηγορίες

Υπάρχουν διάφοροι τύποι τρομοκρατικών επιθέσεων στον κυβερνοχώρο που αναπτύσσονται από κυβερνοτρομοκράτες. Σύμφωνα με το Κέντρο για τη Μελέτη της Τρομοκρατίας και του Παράνομου Πολέμου στη Μεταπτυχιακή Σχολή του Ναυτικού στο Μοντερέι της Καλιφόρνια, οι δυνατότητες της κυβερνοτρομοκρατίας μπορούν να ομαδοποιηθούν σε τρεις βασικές κατηγορίες. "Απλή-μη δομημένη", "Προηγμένη δομή" και "σύνθετη-συντονισμένη".

- Απλή-μη δομημένη

Η ικανότητα διεξαγωγής βασικών παραβιάσεων κατά μεμονωμένων συστημάτων χρησιμοποιώντας εργαλεία που δημιουργήθηκαν από άλλους ανθρώπους. Αυτός ο τύπος οργάνωσης διαθέτει μικρή ανάλυση στόχου και δεξιότητες ελέγχου καθώς και περιορισμένη ικανότητα.

- Προηγμένη δομή

Η ικανότητα διεξαγωγής πιο εξελιγμένων επιθέσεων κατά πολλαπλών συστημάτων ή δικτύων και ενδεχομένως τροποποίηση ή δημιουργία βασικών εργαλείων εισβολής. Αυτός ο τύπος οργάνωσης διαθέτει στοιχειώδη ανάλυση στόχων και δεξιότητες διοίκησης και ελέγχου καθώς και σχετικά μέτρια μαθησιακή ικανότητα.

- Σύνθετη – συντονισμένη

Η ικανότητα συντονισμένων επιθέσεων ικανών να προκαλέσουν μαζικές διαταραχές ενάντια σε ολοκληρωμένες και ετερογενείς άμυνες. Οι τρομοκράτες έχουν την ικανότητα να δημιουργήσουν εξελιγμένα εργαλεία πειρατείας. Είναι επίσης πολύ ικανά να διεξάγουν ανάλυση στόχου και έλεγχο. Επίσης διαθέτουν προχωρημένη ικανότητα μάθησης.

Υπάρχουν πέντε βασικοί τύποι τρομοκρατικών επιθέσεων στον κυβερνοχώρο. Μερικές από αυτές τις επιθέσεις είναι πιο σοβαρές από τις άλλες και έχουν διαφορετικούς στόχους. Το σημαντικό είναι η αναγνώριση των διαφορετικών μεθόδων επίθεσης ώστε να υπάρχει αποτελεσματική αντιμετώπιση.

- Εισβολή

Αυτού του είδους οι επιθέσεις πραγματοποιούνται με σκοπό να αποκτήσουν πρόσβαση σε συστήματα υπολογιστών και δικτύων για λήψη ή τροποποίηση πληροφοριών. Αυτή η μέθοδος είναι πολύ κοινή και χρησιμοποιείται ευρέως με υψηλό ποσοστό επιτυχίας. Υπάρχουν πολλές τρύπες σε ανασφαλή συστήματα υπολογιστών και δικτύων και οι τρομοκράτες μπορούν να επωφεληθούν από τη λήψη και τροποποίηση ζωτικών πληροφοριών ,που μπορεί να χρησιμοποιηθεί για την πρόκληση περαιτέρω ζημιών στον οργανισμό ή για προσωπικό όφελος.

- Καταστροφή

Αυτή η μέθοδος επίθεσης χρησιμοποιείται για εισβολή σε συστήματα υπολογιστών και δίκτυα με κύριο σκοπό την πρόκληση σοβαρής ζημιάς ή την καταστροφή τους. Οι συνέπειες μιας τέτοιας επίθεσης μπορεί να είναι καταστροφικές, σύμφωνα με τις οποίες οι οργανισμοί θα μπορούσαν να αναγκαστούν να είναι εκτός λειτουργίας για απροσδιόριστο χρόνο, ανάλογα με τη σοβαρότητα των επιθέσεων. Μπορεί να αποδειχθεί πολύ δαπανηρό για τους πληγέντες οργανισμούς για να λειτουργήσουν εκ νέου τις δραστηριότητές τους και έτσι θα τους επηρεάσει σκληρά οικονομικά και επίσης βλάπτουν τη φήμη τους.

- Παραπληροφόρηση

Αυτή η μέθοδος χρησιμοποιείται για τη διάδοση φημών ή πληροφοριών που μπορεί να έχουν σοβαρές επιπτώσεις σε έναν συγκεκριμένο στόχο. Ανεξάρτητα από το αν οι φήμες είναι αληθινές ή όχι, η χρήση τέτοιων επιθέσεων μπορεί απερίσκεπτα να δημιουργήσει ανεξέλεγκτο χάος στο έθνος ή την οργάνωση. Αυτός ο τύπος επίθεσης είναι αρκετά δύσκολο να περιοριστεί αφού μπορεί να γίνει σχεδόν αμέσως χωρίς την ανάγκη πρόσβασης στον υπολογιστή και το δίκτυο των θυμάτων.

- Άρνηση υπηρεσίας

Οι επιθέσεις άρνησης υπηρεσίας ή επιθέσεις DOS καθώς είναι ευρύτερα γνωστές είναι επίσης μια κοινή μέθοδος επίθεσης. Ο αντίκτυπος τέτοιων επιθέσεων γίνεται αισθητός περισσότερο από το e-commerce της επιχείρησης που πουλά προϊόντα ή υπηρεσίες στο Διαδίκτυο. Δημόσιες ιστοσελίδες είναι μερικές φορές, οι ιστότοπο που αποτελούν στόχο αυτού του τύπου επίθεσης από τρομοκράτες στον κυβερνοχώρο. Ο κύριος στόχος των επιθέσεων DOS είναι να απενεργοποιήσετε ή να διακόψετε τις διαδικτυακές λειτουργίες,

πλημμυρίζοντας τους στοχευμένους διακομιστές με τεράστιο αριθμό πακέτων (αιτήματα) τα οποία θα οδηγούσαν τελικά τους διακομιστές στο να μην μπορούν να χειριστούν αιτήματα από νόμιμους χρήστες. Ο αντίκτυπος από τέτοιες επιθέσεις μπορεί να είναι καταστροφικός τόσο από οικονομική όσο και από κοινωνική άποψη, όπου μπορεί να προκαλέσει σε οργανώσεις να υποφέρουν από τεράστιες απώλειες.

- Αλλαγή ιστότοπων

Αυτός ο τύπος επίθεσης στοχεύει στην αφαίρεση των ιστοτόπων των θυμάτων. Οι ιστότοποι μπορεί είτε να αλλάξουν πλήρως ώστε να περιλαμβάνουν μηνύματα από τους τρομοκράτες του κυβερνοχώρου όπως προπαγάνδα ή να έχουν διαφημιστικούς σκοπούς που ενδέχεται να τους προκαλέσουν κατάργηση τους ή να επαναπροσανατολίσουν τους χρήστες σε άλλους ιστότοπους που ενδέχεται να περιέχουν παρόμοια μηνύματα. Ο αριθμός των περιπτώσεων τέτοιων επιθέσεων έχει μειωθεί τα τελευταία χρόνια χάρη σε μια μεγαλύτερη ευαισθητοποίηση για το θέμα. Ωστόσο, ένας μικρός αριθμός τέτοιων περιπτώσεων παραμένει και έτσι θα πρέπει να ληφθούν κατάλληλα μέτρα ασφαλείας ώστε να αποφευχθούν τέτοιες ενοχλητικές και οικονομικά καταστροφικές καταστάσεις από το να συμβούν πάλι.

3.3 Γνωστές Ηλεκτρονικές Επιθέσεις

Δισεκατομμύρια άνθρωποι έχουν πέσει θύματα ηλεκτρονικών hacks και ο αριθμός αυτός αναμένεται να αυξηθεί. Αυτές είναι κάποιες από τις μεγαλύτερες ηλεκτρονικες επιθέσεις στην ιστορία.

Yahoo

Τον Σεπτέμβριο του 2016, το yahoo ανακοίνωσε ότι ήταν το θύμα της μεγαλύτερης παραβίασης δεδομένων στην ιστορία. Η εταιρεία είπε ότι η επίθεση έθεσε σε κίνδυνο τα πραγματικά ονόματα, τις διευθύνσεις ηλεκτρονικού ταχυδρομείου, τις ημερομηνίες γέννησης και τους αριθμούς τηλεφώνου 500 εκατομμυρίων χρηστών. Στη συνέχεια, μερικούς μήνες αργότερα, αποκάλυψε ότι μια διαφορετική ομάδα χάκερ έθεσε σε κίνδυνο 1 δισεκατομμύριο λογαριασμούς.

Marriott - Starwood Hotels

Στις 30 Νοεμβρίου 2018, το ξενοδοχείο κολοσσός αποκάλυψε παραβίαση ασφάλειας για τις μάρκες Starwood Hotel που ενδέχεται να έχουν θέσει σε κίνδυνο τα δεδομένα έως και 500 εκατομμυρίων επισκεπτών.

Adult Friend Finder

Τον Οκτώβριο του 2016, ο ιστότοπος είπε ότι οι χάκερ μπόρεσαν να αποκτήσουν πρόσβαση σε περισσότερα από 20 χρόνια δεδομένων στις έξι βάσεις δεδομένων που περιλάμβαναν ονόματα, διευθύνσεις email και κωδικούς πρόσβασης.

Under Armour - MyFitnessPal

Τον Φεβρουάριο του 2018, η μάρκα αθλητικών ενδυμάτων Under Armor αποκάλυψε ότι ένας χάκερ απέκτησε την πρόσβαση σε διευθύνσεις ηλεκτρονικού ταχυδρομείου και πληροφορίες σύνδεσης σε 150 εκατομμύρια χρήστες του ιστότοπου διατροφής , MyFitnessPal.

eBay

Τον Μάιο του 2014, το eBay ανακοίνωσε ότι οι χάκερ μπήκαν στο δίκτυο της εταιρείας χρησιμοποιώντας τα διαπιστευτήρια τριών εταιρικών υπαλλήλων και είχαν πλήρη εσωτερική πρόσβαση για 229 ημέρες, κατά τη διάρκεια του οποίου κατάφεραν να συλλέξουν προσωπικά στοιχεία και των 145 εκατομμυρίων χρηστών του.

Equifax

Τον Σεπτέμβριο του 2017, ένα από τα μεγαλύτερα πιστωτικά γραφεία στις Η.Π.Α. αποκάλυψε προσωπικά στοιχεία, όπως αριθμούς κοινωνικής ασφάλισης, ημερομηνίες γέννησης, διευθύνσεις και, σε ορισμένες περιπτώσεις, παραβιάστηκαν οι αριθμοί άδειας οδήγησης.

Το 2020, τέσσερις Κινέζοι στρατιωτικοί χάκερς κατηγορήθηκαν ότι εισέβαλαν στα δίκτυα υπολογιστών του οργανισμού αναφοράς πίστωσης Equifax και έκλεψαν τα προσωπικά στοιχεία δεκάδων εκατομμυρίων Αμερικανών, ανακοίνωσε το Υπουργείο Δικαιοσύνης.

Heartland Payment Systems

Τον Ιανουάριο του 2009, η Heartland Payment Systems, ο έκτος μεγαλύτερος επεξεργαστής πληρωμών στις ΗΠΑ, ανακοίνωσε ότι τα συστήματα επεξεργασίας της παραβιάστηκαν το 2008, εκθέτοντας περισσότερους από 134 αριθμούς πιστωτικών καρτών πελατών και περισσότερες από 650 εταιρείες χρηματοοικονομικών υπηρεσιών.

Target Stores

Το 2013, ο γίγαντας του λιανικού εμπορίου δέχθηκε επίθεση λίγες ημέρες πριν από την Ημέρα των Ευχαριστιών, όταν οι χάκερς απέκτησαν πρόσβαση μέσω ενός τρίτου πωλητή HVAC στους αναγνώστες καρτών πληρωμής στο σημείο πώλησης (POS), οι οποίοι σε αντάλλαγμα συγκέντρωσαν δεδομένα έως 110 εκατομμυρίων πελατών.

Επιθέσεις εναντίον Κυβερνήσεων

Το 2000, μια ιαπωνική έρευνα αποκάλυψε ότι η κυβέρνηση χρησιμοποιούσε λογισμικό που αναπτύχθηκε από εταιρείες υπολογιστών που είναι συνδεδεμένες με τον Aum Shinrikyo, τη σέκτα της Ημέρας της Κρίσεως που είναι υπεύθυνη για την επίθεση αερίου sarin στο σύστημα του μετρό του Τόκιο το 1995. "Η κυβέρνηση βρήκε 100 τύπους προγραμμάτων λογισμικού που χρησιμοποιούν τουλάχιστον 10 ιαπωνικές κυβερνητικές υπηρεσίες, συμπεριλαμβανομένου του Υπουργείου Άμυνας, και περισσότερες από 80 μεγάλες ιαπωνικές εταιρείες, συμπεριλαμβανομένων των Nippon Telegraph και

Telephone. "Μετά την ανακάλυψη, η ιαπωνική κυβέρνηση ανέστειλε τη χρήση προγραμμάτων που αναπτύχθηκαν από την Aum λόγω του ότι οι συνδεδεμένες εταιρείες ενδέχεται να έχουν θέσει σε κίνδυνο την ασφάλεια παραβιάζοντας τείχη προστασίας. αποκτώντας πρόσβαση σε ευαίσθητα συστήματα ή πληροφορίες, επιτρέποντας εισβολή από τρίτους, φύτευση ιών που θα μπορούσαν να πυροδοτηθούν αργότερα ή φύτευση κακόβουλου κώδικα που θα μπορούσε να παραλύσει τα συστήματα υπολογιστών και το βασικό σύστημα δεδομένων.

Το Πακιστανικό Cyber Army είναι το όνομα που πήρε μια ομάδα χάκερ οι οποίοι είναι γνωστοί για την παραβίαση ιστότοπων, ιδίως ινδικών, κινεζικών και ισραηλινών εταιρειών και κυβερνητικών οργανώσεων, που ισχυρίζονται ότι εκπροσωπούν πακιστανικά εθνικιστικά και ισλαμικά συμφέροντα. Η ομάδα πιστεύεται ότι ήταν ενεργή τουλάχιστον από το 2008 και διατηρεί ενεργή παρουσία στα κοινωνικά μέσα, ειδικά στο Facebook. Τα μέλη της έχουν αναλάβει την ευθύνη για την παραβίαση ιστότοπων που ανήκουν στην Acer, BSNL, CBI της Ινδίας, Κεντρική Τράπεζα και την κρατική κυβέρνηση της Κεράλα.

Τον Μάρτιο του 2013, οι The New York Times ανέφεραν ένα μοτίβο επιθέσεων στον κυβερνοχώρο εναντίον χρηματοπιστωτικών ιδρυμάτων των ΗΠΑ που πιστεύεται ότι υποκινήθηκαν από το Ιράν, καθώς και περιστατικά που επηρέασαν τα χρηματοπιστωτικά ιδρύματα της Νότιας Κορέας που προέρχονται από την κυβέρνηση της Βόρειας Κορέας.

Τον Αύγουστο του 2013, εταιρείες μέσων όπως οι The New York Times, το Twitter και η Huffington Post έχασαν τον έλεγχο ορισμένων από τους ιστότοπούς τους, αφού χάκερ που υποστήριζαν τη συριακή κυβέρνηση παραβίασαν την αυστραλιανή εταιρεία Διαδικτύου που διαχειρίζεται πολλές σημαντικές διευθύνσεις ιστότοπων. Ο Συριακός Ηλεκτρονικός Στρατός, μια ομάδα χάκερ που έχει επιτεθεί στο παρελθόν σε οργανισμούς μέσων μαζικής ενημέρωσης που θεωρεί εχθρικές προς το καθεστώς του προέδρου της Συρίας Μπασάρ αλ-Άσαντ, πήρε την ευθύνη για τις εισβολές Twitter και Huffington Post σε μια σειρά μηνυμάτων Twitter. Ηλεκτρονικά αρχεία έδειξαν ότι το NYTimes.com, ο μόνος ιστότοπος με διακοπή λειτουργίας διάρκειας μιας ώρας, έστρεψε τους επισκέπτες σε έναν διακομιστή που ελέγχεται από τη Συριακή ομάδα πριν χαθεί.

ΚΕΦΑΛΑΙΟ 4 – ΣΚΟΤΕΙΝΟΣ ΙΣΤΟΣ

4.1 Deep Web

Τόσο ο deep web όσο και ο dark web δημιουργήθηκαν πρόσφατα, εμφανιζόμενοι για πρώτη φορά γύρω στο 2000–05. Το Dictionary.com ορίζει το deep web ως «το τμήμα του Διαδικτύου που κρύβεται από τις συμβατικές μηχανές αναζήτησης, όπως με την κρυπτογράφηση,το σύνολο των ιστοσελίδων που δεν έχουν καταχωρηθεί. Το Deep είναι μια παλιά λέξη, που καταγράφηκε για πρώτη φορά πριν από το έτος 900. Προέρχεται από το αγγλικό επίθετο dēop και σχετίζεται με την βουτιά. Έχει διάφορους ορισμούς, όπως «μυστηριώδες, σκοτεινό» και «φτάνοντας ή προχωρά πολύ κάτω».

4.2 Dark Web

Ο dark web, από την άλλη πλευρά, ορίζεται ως "το τμήμα του Διαδικτύου που είναι σκόπιμα κρυμμένο από τις μηχανές αναζήτησης, χρησιμοποιεί καλυμμένες διευθύνσεις IP και είναι προσβάσιμο μόνο με ένα ειδικό πρόγραμμα περιήγησης ιστού: μέρος του deep web. Το dark (που μπορεί να σημαίνει «κρυμμένο, μυστικό») βρέθηκε για πρώτη φορά πριν από το έτος 1000 και προέρχεται από τη μέση αγγλική λέξη derk. Όσον αφορά και τους δύο αυτούς όρους, η λέξη web είναι σύντομη για το World Wide Web, ένας όρος που βρέθηκε για πρώτη φορά το 1990–95. Το αξιοσημείωτο εδώ είναι ότι ο dark web είναι μέρος του deep web.

4.3 Διαφορά Deep Web – Dark Web

Υπάρχει μεγάλη σύγχυση σχετικά με τον τρόπο διάκρισης μεταξύ αυτών των δύο όρων, οι οποίοι και οι δύο ορίζουν κρυφές πτυχές του Διαδικτύου. Τόσο πολύ, που οι τεχνολογικές δημοσιεύσεις χρησιμοποιούν γενικά μια αποποίηση ευθυνών κατά τη συζήτηση του dark web , υπενθυμίζοντας στους αναγνώστες τους ότι δεν πρέπει να συγχέεται με το deep web, το οποίο σχετίζεται, αλλά δεν είναι το ίδιο πράγμα.

Αυτό που έχουν κοινό ο dark web και deep web είναι ότι και οι δύο κρύβονται από εμπορικές μηχανές αναζήτησης. Δεν υπάρχει πρόσβαση ούτε από το Google ούτε από το Bing. Ο deep web είναι ένας γενικός όρος «catch-all» που περιλαμβάνει όχι μόνο τον dark web, αλλά επίσης περιλαμβάνει πολύ «απλό περιεχόμενο».

Όταν οι άνθρωποι συζητούν την κρυφή πτυχή του Διαδικτύου όπου μπορεί να γίνει αγορά από κλεμμένα δεδομένα, ναρκωτικά, όπλα, παιδική πορνογραφία, δολοφονίες και βασικά οποιοδήποτε παράνομο αντικείμενο ή υπηρεσία υπάρχει, αυτός είναι ο dark web. Να σημειωθεί ότι ενώ ο deep web είναι τεράστιος και αντιπροσωπεύει το 90% περίπου του Διαδικτύου, ο dark web πιθανότατα αντιπροσωπεύει μόνο το 0,01%. Ο dark web, μερικές φορές αναφέρεται ως Darknet, είναι προσβάσιμος από το Tor (The Onion Router) ή το I2P (Invisible Internet Project), τα οποία χρησιμοποιούν καλυμμένες διευθύνσεις IP για να διατηρήσουν την ανωνυμία τους για τους χρήστες και τους ιδιοκτήτες ιστότοπων. Με αυτόν τον τρόπο, τα άτομα που χρησιμοποιούν τον Dark web για παράνομους σκοπούς δεν μπορούν να εντοπιστούν και είναι δύσκολο να πει κανείς ποιος φιλοξενεί έναν συγκεκριμένο ιστότοπο.

Ο dark web δεν είναι μόνο οι παράνομες συμφωνίες και άσχημες δεσμεύσεις, χρησιμοποιείται για διάφορους σκοπούς. Οι δημοσιογράφοι χρησιμοποιούν τον Dark web για να προστατεύσουν την ανωνυμία των πηγών τους και άλλοι χρησιμοποιούν τον dark web μόνο και μόνο επειδή πιστεύουν έντονα στο δικαίωμά τους στην ιδιωτική ζωή. Το Υπουργείο Άμυνας των ΗΠΑ ανέπτυξε το Tor, το οποίο τώρα λειτουργεί ως μη κερδοσκοπικός οργανισμός από εθελοντές. Χρηματοδοτείται από την κυβέρνηση των ΗΠΑ και το Εθνικό Ίδρυμα Επιστημών." Η κυβερνητική υποστήριξη για τον Tor συνεχίστηκε τα τελευταία χρόνια ως μέρος της ατζέντας της ελευθερίας στο Διαδίκτυο", εξηγεί ο Timothy B. Lee στο Vox, "που επιδιώκει να βοηθήσει τους ανθρώπους σε κατασταλτικά καθεστώτα να αποκτήσουν πρόσβαση σε πληροφορίες που λογοκρίνονται από τις κυβερνήσεις τους". Για παράδειγμα, το Facebook ξεκίνησε μια έκδοση του ιστότοπού του στον dark web για να "διευκολύνει την πρόσβαση στον ιστότοπο από χώρες που περιορίζουν την υπηρεσία, όπως η Κίνα και το Ιράν."

Δυστυχώς, ο dark web έλαβε πολλή προσοχή στα μέσα ενημέρωσης γύρω στο 2014–15 όταν ο ιδρυτής της διαδικτυακής μαύρης αγοράς Silk Road καταδικάστηκε για διάφορα εγκλήματα, συμπεριλαμβανομένων αρκετών απόπειρων δολοφονιών προς μίσθωση. Η Silk Road έτρεξε τις δραστηριότητές της στον dark web. Τον τελευταίο καιρό, οι χάκερ ήταν στα νέα λόγω απόπειρας πώλησης κλεμμένων δεδομένων στον dark web.

4.4 BlackHats

Οι χάκερ Blackhat, συχνά γνωστοί απλά με τον όρο blackhats, είναι οι κακοί του κόσμου των χάκερ. Αυτοί οι χάκερ συχνά δεν έχουν ιδιαίτερη φροντίδα για το κράτος δικαίου, τα συστήματα που διαταράσσουν ή για τις κακές επιπτώσεις που προκαλούν. Τα Blackhats διακρίνονται από τα whitehats, τους καλούς, που συχνά βρίσκονται να εργάζονται για να αποτρέψουν τις προσπάθειες των blackhats, και των Grayhats, που βρίσκονται στη γραμμή μεταξύ των δύο, συχνά διασχίζουν από τη μία πλευρά στην άλλη.

Η αναγνώριση ενός εισβολέα ως blackhat συνεπάγεται συχνά ότι κατέχουν ένα ορισμένο επίπεδο δεξιοτήτων στην επίθεση και την εκμετάλλευση συστημάτων και δικτύων, τουλάχιστον άνω του μέσου. Τα Blackhats ενδέχεται να επιτεθούν σε ένα σύστημα ή ένα δίκτυο με ποικίλα κίνητρα στο μυαλό. Μπορεί να το κάνουν μόνο για τη συγκίνηση της εκμετάλλευσης ενός συστήματος, μπορεί να είναι μετά από συγκεκριμένες πληροφορίες σχετικά με το σύστημα, μπορεί να χρησιμοποιούν το σύστημα ως «άξονα» για να επιτεθούν σε άλλα συστήματα στο ίδιο δίκτυο ή για πολλούς άλλους λόγους. Οι whitehats είναι επαγγελματίες ασφαλείας που ακολουθούν ηθική και νομική συμπεριφορά. Στόχος τους είναι να βοηθήσουν στη βελτίωση της ασφάλειας.Οι grayhat έχουν την πρόθεση να βελτιώσουν την ασφάλεια, αλλά θα κάνουν ανήθικα πράγματα, όπως μη εξουσιοδοτημένη πειρατεία ή πλήρη αποκάλυψη τρωτών σημείων χωρίς να παρέχουν προθεσμία στους προμηθευτές.

4.5 Γνωστοί BlackHats

Kevin Mitnick

Σημαντική φιγούρα στο αμερικανικό hacking, ο Kevin Mitnick ξεκίνησε ως έφηβος. Το 1981, κατηγορήθηκε για κλοπή εγχειριδίων υπολογιστή από την Pacific Bell. Το 1982, χάκαρε τη Διοίκηση Άμυνας της Βόρειας Αμερικής (NORAD), ένα επίτευγμα που ενέπνευσε την ταινία War Games του 1983. Το 1989, παραβίασε το δίκτυο της Digital Equipment Corporation (DEC) και έκανε αντίγραφα του λογισμικού τους. Επειδή η DEC ήταν κορυφαίος κατασκευαστής υπολογιστών εκείνη την εποχή, αυτή η πράξη έβαλε τον Mitnick στο χάρτη. Αργότερα συνελήφθη, καταδικάστηκε και στάλθηκε στη φυλακή. Κατά τη διάρκεια της υπό όρους κυκλοφορίας του, χάκαρε τα συστήματα φωνητικού ταχυδρομείου του Pacific Bell.

Καθ 'όλη τη διάρκεια της καριέρας του στο hacking, ο Mitnick δεν εκμεταλλεύτηκε ποτέ την πρόσβαση και τα δεδομένα που έλαβε. Πιστεύεται ευρέως ότι κάποτε απέκτησε τον πλήρη έλεγχο του δικτύου Pacific Bell απλώς για να αποδείξει ότι θα μπορούσε να γίνει. Εκδόθηκε ένταλμα για τη σύλληψή του για το περιστατικό Pacific Bell, αλλά ο Mitnick διέφυγε και έζησε κρυμμένος για περισσότερα από δύο χρόνια. Όταν πιάστηκε, εκτίσε χρόνο στη φυλακή για πολλές κατηγορίες απάτης μέσω καλωδίων και απάτης σε υπολογιστή. Αν και ο Mitnick έγινε τελικά whitehat, μπορεί να είναι μέρος της γκρι περιοχής των δύο καπέλων.

Anonymous

Το Anonymous ξεκίνησε το 2003 σε πίνακες μηνυμάτων 4chan σε ένα ανώνυμο φόρουμ. Η ομάδα παρουσιάζει μικρή οργάνωση και επικεντρώνεται χαλαρά στην έννοια της κοινωνικής δικαιοσύνης. Για παράδειγμα, το 2008 το γκρουπ ασχολήθηκε με την Εκκλησία της Σαηεντολογίας και άρχισε να απενεργοποιεί τους ιστότοπούς τους, επηρεάζοντας έτσι αρνητικά τις κατατάξεις αναζήτησής τους στο Google και κατακλύζοντας τις μηχανές φαξ με μαύρες εικόνες. Τον Μάρτιο του 2008, μια ομάδα "Anons" παρέλαβε τα κέντρα της Σαηεντολογίας σε όλο τον κόσμο φορώντας τη διάσημη μάσκα Guy Fawkes. Όπως σημείωσε ο The New Yorker, ενώ το FBI και άλλες υπηρεσίες επιβολής του νόμου έχουν εντοπίσει ορισμένα από τα πιο παραγωγικά μέλη της ομάδας, η έλλειψη πραγματικής ιεραρχίας καθιστά σχεδόν αδύνατο τον εντοπισμό ή την εξάλειψη του Anonymous στο σύνολό του.

Adrian Lamo

Το 2001, ο 20χρονος Adrian Lamo χρησιμοποίησε ένα μη προστατευμένο εργαλείο διαχείρισης περιεχομένου στο Yahoo για να τροποποιήσει ένα άρθρο του Reuters και να προσθέσει ένα ψεύτικο απόσπασμα που αποδόθηκε στον πρώην Γενικό Εισαγγελέα John Ashcroft. Ο Λάμο συχνά παραβίαζε συστήματα και έπειτα ειδοποιούσε

τόσο τον Τύπο όσο και τα θύματά του. Σε ορισμένες περιπτώσεις, θα βοηθούσε να καθαρίσει το χάος για να βελτιώσει την ασφάλειά τους. Όπως επισημαίνει ο Wired, ωστόσο, ο Λάμο πήρε τα πράγματα πολύ μακριά το 2002, όταν εισέπραξε το intranet των New York Times, προστέθηκε στον κατάλογο των ειδικών πηγών και άρχισε να διεξάγει έρευνα για υψηλού προφίλ δημόσιες προσωπικότητες. Ο Λάμο κέρδισε το "The Homeless Hacker" γιατί προτιμούσε να περιπλανηθεί στους δρόμους με κάτι περισσότερο από ένα σακίδιο και συχνά δεν είχε σταθερή διεύθυνση.

Albert Gonzalez

Σύμφωνα με τη New York Daily News , ο Γκονζάλες, που ονομάστηκε «soupnazi », ξεκίνησε ως ο «προβληματικός ηγέτης πακέτων υπολογιστών» στο γυμνάσιο του Μαϊάμι. Τελικά έγινε ενεργός στον ιστότοπο εγκληματικού εμπορίου Shadowcrew.com και θεωρήθηκε ένας από τους καλύτερους χάκερ και συντονιστές του. Στα 22, ο Γκονζάλες συνελήφθη στη Νέα Υόρκη για απάτη με χρεωστικές κάρτες που σχετίζονται με κλοπή δεδομένων από εκατομμύρια λογαριασμούς καρτών. Για να αποφύγει τη φυλακή, έγινε πληροφοριοδότης της μυστικής υπηρεσίας, βοηθώντας τελικά δεκάδες μέλη του Shadowcrew.

Κατά τη διάρκεια του χρόνου του ως πληρωμένος πληροφοριοδότης, ο Γκονζάλες συνέχισε τις εγκληματικές του δραστηριότητες. Μαζί με μια ομάδα συνεργών, ο Γκονζαλες έκλεψε περισσότερους από 180 εκατομμύρια λογαριασμούς καρτών πληρωμής από εταιρείες, συμπεριλαμβανομένων των OfficeMax, Dave και Buster's και Boston Market. Το περιοδικό The New York Times σημειώνει ότι η επίθεση του Γκονζαλες το 2005 στον αμερικανικό λιανοπωλητή TJX ήταν η πρώτη παραβίαση των πιστωτικών πληροφοριών. Χρησιμοποιώντας μια βασική SQL injection , αυτός ο διάσημος χάκερ και η ομάδα του δημιούργησαν πόρτες σε πολλά εταιρικά δίκτυα, κλέβοντας περίπου 256 εκατομμύρια δολάρια από την TJX μόνο. Κατά τη διάρκεια της καταδίκης του το 2015, ο ομοσπονδιακός εισαγγελέας χαρακτήρισε την ανθρώπινη θυματοποίηση του Γκονζάλες «απαράμιλλη».

Ο Matthew Bevan και ο Richard Pryce

Ο Matthew Bevan και ο Richard Pryce είναι μια ομάδα Βρετανών χάκερ που εισέβαλαν σε πολλά στρατιωτικά δίκτυα το 1996, συμπεριλαμβανομένης της βάσης Πολεμικής Αεροπορίας Griffiss, της Υπηρεσίας Πληροφοριακών Συστημάτων Άμυνας και του Κορεατικού Ινστιτούτου Ατομικής Έρευνας (KARI). Οι Bevan (Kuji) και Pryce (Datastream Cowboy) κατηγορήθηκαν ότι ξεκίνησαν σχεδόν έναν τρίτο παγκόσμιο πόλεμο μετά την απόρριψη της έρευνας KARI στα αμερικανικά στρατιωτικά συστήματα. Ο Bevan ισχυρίζεται ότι ήθελε να αποδείξει μια θεωρία συνωμοσίας UFO, και σύμφωνα με το BBC, η υπόθεσή του μοιάζει με αυτή του Gary McKinnon. Κακόβουλη πρόθεση ή όχι, οι Bevan και Pryce απέδειξαν ότι ακόμη και τα στρατιωτικά δίκτυα είναι ευάλωτα.

ΚΕΦΑΛΑΙΟ 5 – ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν πιο προηγμένα και επεκτάσιμα εργαλεία για να παραβιάσουν το απόρρητο των χρηστών και έχουν αποτελέσματα. Δύο δισεκατομμύρια αρχεία δεδομένων διακυβεύθηκαν το 2017 και περισσότερα από 4,5 δισεκατομμύρια αρχεία παραβιάστηκαν μόνο το πρώτο εξάμηνο του 2018.

Αυτά είναι κάποια από τα πιο πιεστικά ζητήματα ασφάλειας στον κυβερνοχώρο το 2019, καθώς και οι τάσεις για το 2020.

5.1 Επιθέσεις Απομακρυσμένης Πρόσβασης

Οι απομακρυσμένες επιθέσεις αυξάνονται σε αριθμό, καθώς επίσης γίνονται πιο περίπλοκες. Ένας από τους κύριους τύπους επίθεσης απομακρυσμένης πρόσβασης το 2018 ήταν το cryptojacking, το οποίο στοχεύει τους κατόχους κρυπτονομισμάτων. Ένας άλλος δημοφιλής τύπος είναι η επίθεση των περιμετρικών συσκευών.

Σύμφωνα με τη βάση δεδομένων των απειλων, οι επιθέσεις απομακρυσμένης πρόσβασης είναι από τους πιο κοινούς φορείς επίθεσης σε ένα συνδεδεμένο σπίτι. Οι χάκερ στοχεύουν υπολογιστές, smartphone, κάμερες πρωτοκόλλου διαδικτύου (IP) και συσκευές αποθήκευσης συνδεδεμένου δικτύου (NAS), καθώς αυτά τα εργαλεία πρέπει συνήθως να έχουν ανοιχτές θύρες και να προωθούνται σε εξωτερικά δίκτυα ή στο Διαδίκτυο.

5.2 Επιθέσεις μέσω Smartphone

Ένας από τους πιο συνηθισμένους φορείς επίθεσης στα smartphone σχετίζεται με μη ασφαλή περιήγηση (phishing, spear phishing, malware). Περισσότερο από το 60% της απάτης στο διαδίκτυο πραγματοποιείται μέσω πλατφορμών για κινητά, σύμφωνα με την RSA, και το 80% της απάτης για κινητά επιτυγχάνεται μέσω εφαρμογών για κινητά αντί για προγράμματα περιήγησης ιστού για κινητά.

Καθώς οι περισσότεροι άνθρωποι χρησιμοποιούν τα τηλέφωνά τους για τη διαχείριση οικονομικών λειτουργιών ή τη διαχείριση ευαίσθητων δεδομένων εκτός της ασφάλειας του οικιακού τους δικτύου, αυτό γίνεται μια εξέχουσα απειλή. Το γεγονός ότι οι χρήστες διατηρούν συνήθως όλες τις πληροφορίες τους στο τηλέφωνό τους και ότι τα smartphone χρησιμοποιούνται τώρα για έλεγχο ταυτότητας δύο παραγόντων - ένα από τα πιο ευρέως χρησιμοποιούμενα εργαλεία ασφάλειας στον κυβερνοχώρο - αυξάνει τον κίνδυνο ασφάλειας εάν η συσκευή χαθεί ή κλαπεί.

5.3 Internet of Things (IoT) και Αυτοματισμοί στο Σπίτι

Η βιομηχανία καταναλωτών στο Internet of Things (IoT) αναμένεται να αναπτυχθεί σε περισσότερες από επτά δισεκατομμύρια συσκευές έως το τέλος του 2020, σύμφωνα με τον Gartner. Πολλοί καταναλωτές δεν βλέπουν τις συσκευές IoT ως ευπάθεια, διότι ένα σημαντικό μέρος αυτών δεν έχουν διεπαφή χρήστη. Αυτό θα μπορούσε να οδηγήσει σε προβλήματα κατανόησης του είδους των δεδομένων που συλλέγει ή διαχειρίζεται η συσκευή.

Ωστόσο, οι συσκευές IoT δεν συλλέγουν μόνο πολύτιμα δεδομένα χρήστη. Θα μπορούσαν να γίνουν ένα σημείο εισόδου για έναν εισβολέα ή ένα εργαλείο για να ξεκινήσει μια κατανεμημένη επίθεση άρνησης υπηρεσίας (DDoS). Οι συσκευές IoT δεν είναι ασφαλείς από το σχεδιασμό, επειδή η εστίαση στην ασφάλεια θα αυξήσει σημαντικά τα έξοδα κατασκευής και συντήρησης.

Σύμφωνα με τα δεδομένα απειλής των αυτοματισμών (AI) από την CUJO AI, το 46% όλων των τύπων επίθεσης που βιώνουν αυτές οι συσκευές είναι απόπειρες απομακρυσμένης πρόσβασης και το 39% χρησιμοποιείται για τον εντοπισμό μοτίβων συμπεριφοράς. Με την εκθετική ανάπτυξη συνδεδεμένων συσκευών στο σπίτι, αυτές οι απειλές είναι πιθανό να αυξηθούν.

5.4 Αξιοποίηση Τεχνητής Νοημοσύνης

Οι περισσότερες από τις μεγαλύτερες βιομηχανίες χρησιμοποιούν ήδη μηχανική εκμάθηση (ML) και τεχνητή νοημοσύνη (AI) για να αυτοματοποιήσουν τις διαδικασίες τους και να βελτιώσουν τη συνολική απόδοση. Η ασφάλεια στον κυβερνοχώρο και το έγκλημα στον κυβερνοχώρο δεν αποτελούν εξαίρεση. Το AI θεωρείται συχνά μια τεχνολογία διπλής χρήσης - ενώ περισσότερες εταιρείες ασφάλειας στον κυβερνοχώρο εφαρμόζουν αλγόριθμους που βασίζονται σε AI για να αποτρέψουν τις απειλές, οι χάκερ εκμεταλλεύονται επίσης την ευκαιρία να γίνουν πιο αποτελεσματικοί. Η πλειονότητα των ικανοτήτων της τεχνητής νοημοσύνης εξυπηρετεί κακόβουλους σκοπούς. Τα συστήματα AI είναι φθηνά, επεκτάσιμα, αυτοματοποιημένα, ανώνυμα και παρέχουν φυσική και ψυχολογική απόσταση για τον εισβολέα, μειώνοντας την άμεση ηθική γύρω από το έγκλημα στον κυβερνοχώρο.

- Τεχνητή νοημοσύνη για αποφυγή κυβερνοασφάλειας.

Οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν διάφορες μεθόδους διαφυγής για να αποφύγουν τον εντοπισμό και το AI βοηθά στη βελτιστοποίηση διαφορετικών στοιχείων αυτής της διαδικασίας.

- Τεχνητή νοημοσύνη στο ηλεκτρονικό ψάρεμα.

Η τεχνητή νοημοσύνη θα μπορούσε να βοηθήσει στη δημιουργία περιεχομένου που μπορεί να περάσει από τυπικά φίλτρα ασφάλειας στον κυβερνοχώρο, όπως μηνύματα ηλεκτρονικού ταχυδρομείου που δεν διακρίνονται από αυτά που γράφονται από ανθρώπους.

- Τεχνητή νοημοσύνη στην κοινωνική μηχανική.

Ενώ η κοινωνική μηχανική είναι μια από τις πιο δημοφιλείς τεχνικές εισβολής, χρειάζεται πολύς χρόνος για να εφαρμοστεί σωστά. Η τεχνητή νοημοσύνη θα μπορούσε να βοηθήσει

όχι μόνο στη συλλογή πληροφοριών, αλλά και γράφοντας μηνύματα ηλεκτρονικού ταχυδρομείου ή καλώντας πιθανά θύματα.

Με τις νέες εξελίξεις στην τεχνολογία που βασίζεται στην τεχνολογία AI, η χρήση της τεχνητής νοημοσύνης στις επιθέσεις στον κυβερνοχώρο θα γίνει ακόμη πιο δημοφιλής και επικίνδυνη τάση.

ΚΕΦΑΛΑΙΟ 6 – ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

6.1 Βασικές Αρχές Ασφαλείας

Η Ασφάλεια Πληροφοριακών Συστημάτων στηρίζεται σε τρεις βασικές αρχές απαραίτητες για την σωστή λειτουργία των Πληροφοριακών Συστημάτων. Αυτές είναι η τριάδα Εμπιστευτικότητα-Ακεραιότητα-Διαθεσιμότητα ΕΑΔ – (Confidentiality-Integrity-Availability – CIA triad).

Συγκεκριμένα:

1. Εμπιστευτικότητα (confidentiality)

Στόχος της είναι η εξασφάλιση πως τα δεδομένα δε θα γίνουν διαθέσιμα, δε θα μπορούν να τα διαβάσουν δηλαδή, μη εξουσιοδοτημένα άτομα.Τα δεδομένα θα πρέπει να κατηγοριοποιούνται ανάλογα με την σημαντικότητά τους. Ανάλογα δηλαδή με το τι επιπτώσεις θα έχει η εμφάνισή τους σε λάθος άτομα. Έτσι, θα μπορούν να μπουν διαφορετικοί περιορισμοί σε κάθε κατηγορία που θα δημιουργηθεί.

Όσο σημαντικότερα είναι αυτά που πρέπει να προστατευτούν τόσο ισχυρότερα μέτρα θα πρέπει να λαμβάνονται (πχ απομόνωση από το δίκτυο συστημάτων με κρίσιμα δεδομένα, τοποθέτηση επιπλέον μέτρων προστασίας, απενεργοποίηση USB θυρών, κρυπτογράφηση και σε ακραία περίπτωση θα μπορούν να υπάρχουν μόνο τυπωμένα όσα θέλουμε να προστατευτούν πχ: σχέδια, οδηγίες κ.λπ.)

2. Ακεραιότητα (integrity)

Η αρχή της Ακεραιότητας εξασφαλίζει πως τα δεδομένα δε θα υποστούν καμία αλλοίωση από μη εξουσιοδοτημένα άτομα ή με μη ανιχνεύσιμο τρόπο. Σε περιπτώσεις τροποποίησης θα πρέπει να παράγονται σχετικά μηνύματα ειδοποίησης (π.χ. με χρήση ελέγχου αθροίσματος MD5, Αντιγράφων ασφαλείας κ.λπ.)

3. Διαθεσιμότητα (Availability)

Αυτή εξασφαλίζει πως το σύστημα θα μπορεί να παρέχει τις πληροφορίες του, όταν του ζητηθούν και μέσα σε αποδεκτά χρονικά όρια.Υπολογιστές, δίκτυα και συσκευές δικτύου θα πρέπει να επιδιορθώνονται όσο γίνεται γρηγορότερα. (π.χ. με Σχέδιο Αποκατάστασης από Καταστροφή – Disaster Recovery Plan και Σχέδιο Επιχειρησιακής Συνέχειας – Business Continuity)

6.2 Κρυπτογραφία και Ασφάλεια

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

στόχοι της κρυπτογραφίας στην γενικότερη ασφάλεια ενός συστήματος είναι η εμπιστευτικότητα (confidentiality) η αυθεντικοποίηση (authentication), η ακεραιότητα (integrity) και η μη αποποίηση παραλαβή – αποστο λής (non redudiation).Με την κρυπτογράφηση επιχειρείται η μετατροπή της πληροφορίας , από μια κατανοητή μορφή σε ένα γρίφο , ο οποίος παραμένει ακατανόητος . Με την αντίθετη διαδικασία , δηλαδή την αποκρυπτογράφηση , ο γρίφος αυτός επανέρχεται στην αρχική του μορφή και η πληροφορία μπορεί να αναγνωστεί .Τα βασικά στοιχεία , που αποτελούν ένα σύγχρονο σύστημα κρυπτογράφησης είναι τέσσερα :

α) Το αρχικό μήνυμα (plaintext)

β) Το κρυπτογραφικό σύστημα (cryptosystem) το οποίο αποτελείται από έναν αλγόριθμο κρυπτογράφησης και ένα αλγόριθμο αποκρυπτογράφησης .

γ) Το κρυπτογραφημένο κείμενο (ciphertext) το οποίο είναι το αποτέλεσμα της εφαρμογής του αλγορίθμου κρυπτογράφησης στο αρχικό μήνυμα , πριν αυτό σταλεί στον παραλήπτη.

δ) Ένα κλειδί (key), το οποίο είναι μια συμβολοσειρά , η οποία χρησιμοποιείται από τους αλγόριθμοι στην διαδικασία κρυπτογράφησης και αποκρυπτογράφησης .

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

- Συμμετρική κρυπτογραφία

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

- Ασύμμετρη κρυπτογραφία

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

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

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

- Διαχείριση δημοσίων κλειδιών - πιστοποιητικά

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

6.3 Προστασία στο Διαδίκτυο

- Επιλέξτε και εγκαταστήστε στον υπολογιστή ένα πρόγραμμα προστασίας από κακόβουλο λογισμικό (antivirus) μίας γνωστής και αξιόπιστης εταιρείας.
- Ενεργοποιήστε τη δυνατότητα αυτόματης ενημέρωσης, ώστε να προστατεύεται ο υπολογιστής από τις πιο πρόσφατες περιπτώσεις κακόβουλου λογισμικού. Κάποια προγράμματα υποστηρίζουν και λειτουργίες anti-spyware.
- Εγκαταστήστε ένα τείχος προστασίας στον υπολογιστή (firewall). Το firewall ελέγχει την επικοινωνία από και προς τον προσωπικό υπολογιστή, επιτρέποντας ή

απαγορεύοντας συγκεκριμένα είδη κίνησης, ώστε να προλαμβάνει τη διάδοση ιών και ανεπιθύμητων εφαρμογών. Ορισμένες εκδόσεις λειτουργικών συστημάτων (π.χ. WindowsXP/SP2) έχουν ενσωματωμένο προσωπικό firewall.

- Πραγματοποιήστε τακτικές ενημερώσεις στα προγράμματα πλοήγησης (browser) στο Διαδίκτυο (Internet Explorer, Firefox, Chrome, Opera, Safari κλπ.). Συνιστάται η ενεργοποίηση της αυτόματης ενημέρωσης και η πραγματοποίηση ενημέρωσης όταν λαμβάνετε μία σχετική ειδοποίηση.
- Χρησιμοποιήστε έναν ισχυρό κωδικό πρόσβασης με γράμματα, σύμβολα και αριθμούς, διαφορετικό για κάθε εφαρμογή στην οποία διατηρείτε λογαριασμό. Αποφύγετε τη χρήση κωδικών που είναι εύκολοι στην απομνημόνευση (όπως ημερομηνίες, γνωστούς όρους, ακολουθίες γραμμάτων ή κύρια ονόματα). Μία προτεινόμενη λύση για τη δημιουργία ενός κωδικού (password) είναι να επιλέξετε χρήση συνδυασμού πεζών - κεφαλαίων, γραμμάτων - αριθμών, με τουλάχιστον 8 ψηφία.
- Κρατήστε τους κωδικούς μυστικούς και αλλάζετέ τους σε τακτικά χρονικά διαστήματα (τουλάχιστον μια φορά ανά 6 μήνες).
- Ενεργοποιείτε πάντα τα ενσωματωμένα χαρακτηριστικά προστασίας των προγραμμάτων πλοήγησης όπως η φραγή των αναδυόμενων παραθύρων, διαχείριση των «Cookies» κλπ.
- Δώστε προσοχή σε ενδείξεις που μπορεί να σημαίνουν ότι ο υπολογιστής σας έχει προσβληθεί από κάποιον ιό, όπως οι παρακάτω:
    - το σύστημά γίνεται ξαφνικά αισθητά πιο αργό στην εκκίνησή του ή/και στη λειτουργία του
    - αργεί να ανοίξει τα αρχεία σας περισσότερο από το συνηθισμένο
    - κάποια αρχεία εμφανίζονται κατεστραμμένα ή δεν φορτώνουν
    - εμφανίζονται μηνύματα από το antivirus πρόγραμμά ή άλλα ασυνήθιστα μηνύματα

- Χρησιμοποιήστε προγράμματα μόνο από αξιόπιστες πηγές. Η χρήση προγραμμάτων που βρίσκετε στο Διαδίκτυο πρέπει να γίνεται μόνο όταν είστε βέβαιοι για την πηγή της προέλευσής τους.
- Αποφύγετε την προβολή άγνωστων αρχείων, μηνυμάτων ή συνδέσμων. Πριν ανοίξετε κάποιο αρχείο, ενεργοποιήστε το φίλτρο για ανίχνευση ιών (virus scanning).
- Βεβαιωθείτε ότι έχετε αποσυνδεθεί από τον λογαριασμό σε μια ιστοσελίδα ηλεκτρονικής υπηρεσίας (π.χ. ηλεκτρονικής τραπεζικής συναλλαγής) μέσω του προσφερόμενου συνδέσμου αποσύνδεσης (log out) πριν την εγκαταλείψετε.
- Αποφύγετε την ενεργοποίηση υπενθύμισης/απομνημόνευσης κωδικού κατά τη χρήση προγραμμάτων πλοήγησης, ειδικά όταν η πρόσβαση στο Διαδίκτυο γίνεται από κοινόχρηστους υπολογιστές.
- Επιβεβαιώστε ότι χρησιμοποιείτε μια ασφαλή σύνδεση όταν στέλνετε ευαίσθητες προσωπικές πληροφορίες μέσω του παγκόσμιου ιστού (Web). Αυτό φαίνεται από

το εικονίδιο του κλειδωμένου λουκέτου, ενώ η διεύθυνση που συνδέεστε πρέπει να αρχίζει με https:// αντί του http.

- Αν συνδέεστε στο Διαδίκτυο από δίκτυο δημόσιας χρήσης (internet café, ξενοδοχεία κλπ.), μη χρησιμοποιείτε και μη μεταδίδετε προσωπικά στοιχεία.
- Αποφύγετε να επισκέπτεστε σελίδες που πρέπει να χρησιμοποιήσετε προσωπικούς μυστικούς κωδικούς (passwords), ιδιαίτερα αν η ανταλλαγή πληροφορίας δεν πραγματοποιείται κρυπτογραφημένα (π.χ. https). Είναι πιθανό τα δίκτυα αυτά να μην είναι ασφαλή και να υποκλαπούν προσωπικά σας δεδομένα.

Μέτρα για την προστασία του απορρήτου κατά την ασύρματη πρόσβαση στο Διαδίκτυο

- Ενεργοποιήστε την κρυπτογράφηση στον ασύρματο δρομολογητή. Προτιμήστε την κρυπτογράφηση WPA ή ακόμα καλύτερα WPA2. Να χρησιμοποιείτε ισχυρούς κωδικούς για το κλειδί κρυπτογράφησης, τους οποίους να αλλάζετε συχνά. Αλλάζετε το όνομα του δικτύου (αναγνωριστικό SSID), δίνοντας δική σας ονομασία, διαφορετική από αυτή που έχει θέσει ο κατασκευαστής.
- Ρυθμίστε το ασύρματο δίκτυο ώστε να δέχεται συνδέσεις μόνο από συγκεκριμένους υπολογιστές, tablet και κινητά τηλέφωνα (MAC address filtering).
- Αλλάζετε το όνομα χρήστη και τον κωδικό ασφαλείας για τη διαχείριση του ασύρματου δρομολογητή από την τιμή που έχει θέσει ο κατασκευαστής (username και password admin).Επιπλέον, αλλάζετε τον κωδικό, που έχετε θέσει, σε τακτά χρονικά διαστήματα.
- Απενεργοποιήστε την απομακρυσμένη σύνδεση (remote management access) με τον δρομολογητή σε περίπτωση που η πρόσβαση αυτή δεν είναι ήδη απενεργοποιημένη από τον κατασκευαστή.
- Αλλάξτε τη ρύθμιση ώστε να μην επιτρέπεται η διαχείριση του δρομολογητή μέσω ασύρματης (wireless) σύνδεσης.
- Μπορείτε να ελέγξετε τον ασύρματο δρομολογητή για το ποιες συσκευές έχουν συνδεθεί ή αιτούνται σύνδεσης με αυτόν. Σε περίπτωση που παρατηρήσετε συνδέσεις από άγνωστες συσκευές, αλλάξτε άμεσα τους κωδικούς.

Μέτρα για την προστασία του απορρήτου στην ηλεκτρονική αλληλογραφία

- Αν ο λογαριασμός ηλεκτρονικής αλληλογραφίας σας παραβιάστηκε πρόσφατα ή αν τρίτοι απέκτησαν πρόσβαση σε αυτόν, θα πρέπει να αλλάξετε άμεσα τον κωδικό πρόσβασής.
- Μην χρησιμοποιείτε ποτέ τον κωδικό πρόσβασης του λογαριασμού για την πρόσβαση σε άλλους ιστότοπους.

- Μην ανοίγετε συνημμένα αρχεία που προέρχονται από άγνωστους τρίτους ή από μη έμπιστες πηγές. Όταν λαμβάνετε ηλεκτρονικό μήνυμα, ακόμη και από φαινομενικά έμπιστες πηγές (όπως π.χ. τράπεζες), εξετάστε προσεχτικά την προέλευσή του πριν ανοίξετε ένα σύνδεσμο που περιέχεται σε αυτό, γιατί μπορεί να σας οδηγήσει σε ιστοσελίδα που, ενώ φαίνεται ίδια με τη νόμιμη, είναι πλαστή.
- Μην στέλνετε τους κωδικούς πρόσβασής μέσω ηλεκτρονικού ταχυδρομείου. Οι νόμιμοι ιστότοποι, που προσφέρουν ηλεκτρονικά υπηρεσίες, δεν θα ζητήσουν ποτέ να στείλετε τους κωδικούς πρόσβασής μέσω ηλεκτρονικού ταχυδρομείου.
- Παρακολουθήστε τη δραστηριότητα των λογαριασμών ηλεκτρονικού ταχυδρομείου, όπως τις συνδέσεις στον λογαριασμό σας, τυχόν αλλαγές στον κωδικό πρόσβασης ή στα στοιχεία που χρησιμοποιούνται για την ανάκτηση των κωδικών (προσθήκη μιας εναλλακτικής διεύθυνσης ηλεκτρονικού ταχυδρομείου ή ενός αριθμού τηλεφώνου). Εάν παρατηρήσετε οποιαδήποτε ύποπτη ένδειξη, θα πρέπει άμεσα να αλλάξετε τον κωδικό πρόσβασης.
- Παρακολουθήστε την αποστολή και τη λήψη μηνυμάτων ηλεκτρονικού ταχυδρομείου. Εάν παρατηρήσετε ότι πολλά μηνύματα στον λογαριασμό δεν μπορείτε να τα βρείτε ή εάν παρατηρήσετε ότι από τον λογαριασμό σας στέλνονται άγνωστα μηνύματα, αλλάξτε άμεσα τον κωδικό πρόσβασης.
- Επιβεβαιώστε ότι η αλληλογραφία δεν προωθείται σε κάποια διεύθυνση που δεν έχετε ορίσει εσείς. Σε περίπτωση που διαπιστώσετε ανεπιθύμητη προώθηση, καταργήστε την άμεσα.
- Στην περίπτωση που είναι εφικτό, ενεργοποιήστε τη διαδικασία επαλήθευσης σε δύο βήματα (two step verification) για την πρόσβαση στον λογαριασμό (π.χ. με την αποστολή ειδικού κωδικού μιας χρήσης στο κινητό τηλέφωνο).
- Μην παραλείπετε να αποσυνδεθείτε από τον λογαριασμό, ειδικά εάν έχετε συνδεθεί από έναν κοινόχρηστο υπολογιστή (π.χ. από μια βιβλιοθήκη ή ένα Internet cafe). Έχετε υπόψη ότι μπορεί να εξακολουθείτε να είστε συνδεδεμένοι, ακόμα και αφού κλείσετε το πρόγραμμα πλοήγησης.
- Κρυπτογραφήστε μηνύματα ή συνημμένα αρχεία που περιέχουν εμπιστευτικές πληροφορίες.

ΚΕΦΑΛΑΙΟ 7 – ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ

7.1 Ελληνική Νομοθεσία

Η προσέγγιση των νομικών θεμάτων που άπτονται της προστασίας της ηλεκτρονικής πληροφορίας, ενός βασικού πλέον εννόμου αγαθού, ενέχει αρκετές δυσκολίες καθώς προϋποθέτει πέρα από νομικές και τεχνικές γνώσεις. Η νομική επιστήμη «σκοντάφτει» σε κρίσιμες παραμέτρους, με αποτέλεσμα να δυσχεραίνεται η πλήρης εφαρμογή των υπαρχόντων νόμων, ενώ στον χώρο του ποινικού δικαίου δεν είναι επιτρεπτή η αναλογική εφαρμογή των νόμων. Αυτό πρακτικά σημαίνει ότι αν δεν υφίσταται διάταξη που να ρυθμίζει το έγκλημα επακριβώς, δεν μπορεί να εφαρμοστεί αναλογικά κάποια άλλη διάταξη κι έτσι το ηλεκτρονικό έγκλημα παραμένει ατιμώρητο. Άλλο βασικό ζήτημα που αναφύεται στον χώρο του ποινικού δικαίου εντοπίζεται στη δυσκολία εύρεσης του δράστη λόγω της ανωνυμίας που προσφέρει το διαδίκτυο στον εκάστοτε χρήστη. Η ψεύτικη ταυτότητα πίσω από την οποία κρύβεται και νιώθει ασφαλής, τον καθιστά αόρατο και συνδυαστικά με σχεδόν ανύπαρκτα ψηφιακά ίχνη διάπραξης του εγκλήματός του, καθίσταται ιδιαίτερα δυσχερές το έργο των διωκτικών αρχών.

Στην Ελλάδα, πρέπει να διευκρινιστεί πως δεν υπάρχουν ειδικές διατάξεις για τα ηλεκτρονικά εγκλήματα. Οι περισσότερες μέχρι σήμερα υποθέσεις έχουν διωχθεί με τις διατάξεις του Ν.1805/1988 που αφορά τα εγκλήματα, τα διαπραχθέντα με ηλεκτρονικούς υπολογιστές (computer crimes) και στον βαθμό που τα προβλεπόμενα στον Ποινικό Κώδικα εγκλήματα (370 Β, 370 Γ, 386 Α) διαπράττονται και σε περιβάλλον Διαδικτύου (Internet), τότε τα άρθρα αυτά εφαρμόζονται και στις συγκεκριμένες περιπτώσεις. Βέβαια, τα άρθρα αυτά δεν αρκούν για τη δίωξη των σύγχρονων ηλεκτρονικών εγκλημάτων αφού δεν υπάρχει νόμος που να αναφέρεται αποκλειστικά σε θέματα Διαδικτύου. Αδικήματα φέρ' ειπείν που σχετίζονται με τη διασπορά κακόβουλου λογισμικού και με επιθέσεις άρνησης εξυπηρέτησης δεν μπορούν να τιμωρηθούν βάσει της ισχύουσας νομοθεσίας. 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 κενών. Μάλιστα, έχει υπογράψει την Ευρωπαϊκή Σύμβαση για το έγκλημα στον Κυβερνοχώρο που από τη στιγμή έναρξης της ισχύος της θα συνιστά σημαντικό βήμα της ελληνικής νομοθεσίας στον Ποινικό και στον Δικονομικό Τομέα.

Σχετικά πρόσφατα τέθηκε σε ισχύ το Π.Δ. 47/2005 από την Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών, που αφορά τις τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και τη διασφάλισή του.Ειδικότερα, οι βασικότερες κατηγορίες Ηλεκτρονικών Εγκλημάτων που αναφέρονται στον Ελληνικό Π.Κ. είναι:

– Απάτη με υπολογιστή

– Δυσφήμηση

– Παράνομη αντιγραφή ή χρησιμοποίηση προγραμμάτων υπολογιστών/πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή

– Πορνογραφία ανηλίκων

Σε κάθε περίπτωση, ενδέχεται να έχουμε συρροή διατάξεων τόσο του Π.Κ. όσο και ειδικότερων νόμων που επισύρουν ποινικές διώξεις- κυρώσεις. Μια πράξη δηλαδή, που συνιστά ηλεκτρονικό έγκλημα είναι πιθανό να τιμωρηθεί με επίκληση μίας, ίσως και περισσότερων διατάξεων. Για παράδειγμα, η διάδοση ιών με σκοπό την αλλοίωση/αχρήστευση δεδομένων μπορεί να συνεπάγεται και φθορά ξένης ιδιοκτησίας, ενώ υφίστανται και περιπτώσεις διάδοσης κάποιου ιού, η οποία συνεπάγεται και τη μεταβολή στοιχείων του αρχείου ή και τροποποίηση της διαδικασίας πρόσβασης σε αυτό, οπότε αποτελεί και παράνομη πρόσβαση σε στοιχεία που έχουν εισαχθεί σε Η/Υ.

7.2 Συνθήκη Βουδαπέστης

Οι μορφές του Ηλεκτρονικού Εγκλήματος είναι ποικίλες και με τη συνεχή ανάπτυξη της τεχνολογίας και του Διαδικτύου πολλαπλασιάζονται. Για την αντιμετώπιση του κινδύνου αυτού ήταν απαραίτητη η διακρατική συνεννόηση και η εκπόνηση μιας αναλυτικής και αποτελεσματικής στρατηγικής. Ο στόχος αυτός επετεύχθη στο Συνέδριο για το Ηλεκτρονικό Έγκλημα (Convention on Cybercrime), που έγινε το 2001 στη Βουδαπέστη του οποίου όλα τα συμπεράσματα αποκρυσταλλώνονται στη Συνθήκη που υπεγράφη μετά το πέρας των εργασιών του Συνεδρίου στις 23.11.2001. Στη Συνθήκη της Βουδαπέστης, υπέγραψαν 26 υπουργοί ευρωπαϊκών κρατών, μεταξύ των οποίων και της Ελλάδας υπάρχουν επεξηγήσεις και ρυθμίσεις για όλα τα Ηλεκτρονικά Εγκλήματα.

Καταρχάς με το Νόμο 4411/2016 κυρώθηκαν η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο (Σύμβαση της Βουδαπέστης) καθώς και το Πρόσθετο Πρωτόκολλο αυτής αναφορικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης που διαπράττονται μέσω συστημάτων υπολογιστών.

Η Σύμβαση της Βουδαπέστης αποτελεί ένα σημαντικό εργαλείο για την αντιμετώπιση του εγκλήματος στον Κυβερνοχώρο. Ωστόσο η ενσωμάτωσή της έγινε με μεγάλη καθυστέρηση (τέθηκε σε ισχύ περίπου το 2003), γεγονός προβληματικό, ιδιαιτέρως δεδομένης της ταχύτατης εξέλιξης των εργαλείων αλλά και των μεθόδων που χρησιμοποιούνται για την διάπραξη τέτοιας φύσεως εγκλημάτων.

Με το Πρόσθετο Πρωτόκολλο της Σύμβασης της Βουδαπέστης διευρύνεται το πεδίο εφαρμογής της Σύμβασης για το έγκλημα στον Κυβερνοχώρο, προκειμένου να αντιμετωπισθούν ξενοφοβικής και ρατσιστικής φύσης πράξεις, εναρμονίζεται το ισχύον στα Συμβαλλόμενα Μέρη ουσιαστικό ποινικό δίκαιο, σχετικά με τη διακίνηση, μέσω του Διαδικτύου, υλικού ξενοφοβικής και ρατσιστικής φύσης, ενώ παρέχεται σε αυτά η δυνατότητα χρήσης των προβλεπόμενων από τη Σύμβαση για το έγκλημα στον Κυβερνοχώρο δικονομικών μέσων.

Ιδιαίτερα σημαντικές είναι οδηγίες του Ευρωπαϊκού Κοινοβουλίου σχετικά με τη νομοθεσία για τις επιθέσεις κατά των συστημάτων πληροφοριών, οι οποίες έχουν ως στόχο τη διευκόλυνση της πρόληψης των αδικημάτων σε σχέση με τα συστήματα πληροφοριών και τη βελτίωση της συνεργασίας μεταξύ δικαστικών και άλλων αρμόδιων αρχών των κρατών-μελών της ΕΕ.

7.3 Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ)

Ο ΓΚΠΔ καθορίζει λεπτομερώς τις απαιτήσεις για τη συλλογή, την αποθήκευση και τη διαχείριση προσωπικών δεδομένων από επιχειρήσεις και οργανισμούς. Οι απαιτήσεις ισχύουν για ευρωπαϊκούς οργανισμούς που επεξεργάζονται προσωπικά δεδομένα ατόμων στην ΕΕ, αλλά και για οργανισμούς εκτός της ΕΕ οι οποίοι στοχεύουν άτομα που ζουν στην ΕΕ.

Ο ΓΚΠΔ εφαρμόζεται εάν:

- Μια επιχείρησή επεξεργάζεται προσωπικά δεδομένα και εδρεύει στην ΕΕ, ανεξάρτητα από το πού γίνεται η πραγματική επεξεργασία των δεδομένων.
- Η επιχείρησή εδρεύει εκτός της ΕΕ αλλά επεξεργάζεται προσωπικά δεδομένα τα οποία αφορούν την παροχή προϊόντων ή υπηρεσιών σε άτομα εντός της ΕΕ, ή παρακολουθεί τη συμπεριφορά ατόμων εντός της ΕΕ
- Επιχειρήσεις που δεν εδρεύουν στην ΕΕ αλλά επεξεργάζονται δεδομένα πολιτών της ΕΕ οφείλουν να διορίζουν εκπρόσωπο στην ΕΕ.

Προσωπικά δεδομένα είναι όλες οι πληροφορίες που αφορούν έναν ταυτοποιημένο ή ταυτοποιήσιμο πρόσωπο, το οποίο καλείται υποκείμενο των δεδομένων. Τα προσωπικά δεδομένα περιέχουν πληροφορίες όπως:

-όνομα

-διεύθυνση

-αριθμός δελτίου ταυτότητας/διαβατηρίου

-εισόδημα

-πολιτισμικό προφίλ

-κωδικός πρωτοκόλλου διαδικτύου (IP)

-δεδομένα που διατηρούν νοσοκομεία ή γιατροί (με αποκλειστικό σκοπό την ταυτοποίηση προσώπου για ιατρικούς λόγους).

Κατά την επεξεργασία τους, τα προσωπικά δεδομένα μπορεί να περάσουν από διάφορες επιχειρήσεις ή οργανισμούς. Μέσα σ΄αυτόν τον κύκλο, υπάρχουν δύο βασικά προφίλ που ασχολούνται με την επεξεργασία των προσωπικών δεδομένων:

-ο υπεύθυνος επεξεργασίας, οποίος αποφασίζει τον σκοπό και τον τρόπο επεξεργασίας των προσωπικών δεδομένων

-ο εκτελών την επεξεργασία, ο οποίος φυλάσσει και επεξεργάζεται τα δεδομένα για λογαριασμό του υπευθύνου επεξεργασίας.

Ο υπεύθυνος προστασίας δεδομένων (ΥΠΔ) που μπορεί να έχει οριστεί από την επιχείρηση, είναι αρμόδιος να παρακολουθεί την επεξεργασία των προσωπικών δεδομένων, καθώς και να ενημερώνει και να συμβουλεύει τους υπαλλήλους επεξεργασίας των προσωπικών δεδομένων σχετικά με τις υποχρεώσεις τους. Ο ΥΠΔ συνεργάζεται επίσης με την Αρχή Προστασίας Δεδομένων (ΑΠΔ), λειτουργώντας ως σημείο επαφής μεταξύ της ΑΠΔ και μεμονωμένων ατόμων.

Σύμφωνα με τους κανόνες της ΕΕ για την προστασία δεδομένων, η επεξεργασία πρέπει να γίνεται με θεμιτό και σύννομο τρόπο, για έναν συγκεκριμένο και νόμιμο σκοπό και να καλύπτει μόνο τα δεδομένα που είναι αναγκαία για την επίτευξη αυτού του σκοπού. Για να επεξεργάζεστε προσωπικά δεδομένα πρέπει να διασφαλίσετε ότι πληροίτε έναν από τους παρακάτω όρους :

-έχετε τη συγκατάθεση του συγκεκριμένου υποκειμένου των δεδομένων

-χρειάζεστε τα προσωπικά δεδομένα για να τηρήσετε συμβατική υποχρέωση έναντι του υποκειμένου των δεδομένων

-χρειάζεστε τα προσωπικά δεδομένα για να εκπληρώσετε νομική υποχρέωση

-χρειάζεστε τα προσωπικά δεδομένα για να προστατεύσετε ζωτικά συμφέροντα του υποκειμένου των δεδομένων

-επεξεργάζεστε προσωπικά δεδομένα για να διεκπεραιώσετε αποστολή δημοσίου συμφέροντος

-ενεργείτε προς όφελος των νομίμων συμφερόντων της επιχείρησής σας, εφόσον δεν θίγονται σοβαρά τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επεξεργάζεστε. Αν τα δικαιώματα του υποκειμένου υπερισχύουν των συμφερόντων της επιχείρησής σας, δεν μπορείτε να επεξεργαστείτε τα προσωπικά του δεδομένα.

Ο ΓΚΠΔ ορίζει αυστηρούς κανόνες για την επεξεργασία δεδομένων βάσει συγκατάθεσης. Σκοπός των κανόνων αυτών είναι να διασφαλιστεί ότι το υποκείμενο των δεδομένων κατανοεί για τι πραγματικά έχει δώσει τη συγκατάθεσή του. Αυτό σημαίνει ότι η συγκατάθεση πρέπει να δίνεται ελεύθερα, συγκεκριμένα και χωρίς ασάφειες με δήλωση διατυπωμένη σε απλή και κατανοητή γλώσσα. Η συγκατάθεση πρέπει να δίνεται με καταφατική πράξη, π.χ. με την επιλογή τετραγωνιδίου σε ιστοσελίδα ή με την υπογραφή δήλωσης.

Όταν έχει δοθεί συγκατάθεση για την επεξεργασία προσωπικών δεδομένων, μπορείτε να επεξεργαστείτε τα δεδομένα μόνο για τους σκοπούς για τους οποίους δόθηκε η συγκατάθεση. Πρέπει επίσης να δίνετε στο υποκείμενο των δεδομένων τη δυνατότητα να αποσύρει τη συγκατάθεσή του.

Σε ορισμένες περιπτώσεις, το υποκείμενο των δεδομένων μπορεί να ζητήσει από τον υπεύθυνο επεξεργασίας να διαγράψει τα προσωπικά του δεδομένα, π.χ. όταν τα

δεδομένα αυτά δεν χρειάζονται πλέον για την επίτευξη του σκοπού της επεξεργασίας. Ωστόσο, η επιχείρησή σας δεν υποχρεούται να πράξει κάτι τέτοιο, εφόσον:

-η επεξεργασία είναι απαραίτητη προκειμένου να τηρηθεί η ελευθερία της έκφρασης και της πληροφόρησης

-οφείλετε να αποθηκεύσετε τα προσωπικά δεδομένα προκειμένου να συμμορφωθείτε με νομική υποχρέωση

-υπάρχουν άλλοι λόγοι δημόσιου συμφέροντος για την αποθήκευση των προσωπικών δεδομένων, όπως σκοποί δημόσιας υγείας ή επιστημονικής και ιστορικής έρευνας

-οφείλετε να αποθηκεύσετε τα προσωπικά δεδομένα προκειμένου να εγείρετε νομική αξίωση.

Η μη τήρηση των κανόνων του ΓΚΠΔ μπορεί να οδηγήσει σε σημαντικά πρόστιμα που μπορούν να φθάσουν μέχρι τα 20 εκατομμύρια ευρώ ή το 4% του συνολικού κύκλου εργασιών της επιχείρησης για ορισμένες παραβάσεις. Η Αρχή Προστασίας Δεδομένων μπορεί επίσης να επιβάλει συμπληρωματικά διορθωτικά μέτρα, π.χ., να σας διατάξει να διακόψετε την επεξεργασία προσωπικών δεδομένων.

7.4 Πνευματικά Δικαιώματα

Πνευματικό δικαίωμα είναι το δικαίωμα που αποκτά κάποιος πάνω σε ένα πρωτότυπο πνευματικό δημιούργημα, π.χ. μουσική, συγγραφικό έργο, εικαστικό έργο, θεατρικό έργο, οπτικοακουστικό έργο, λογισμικό κ.λπ. Πνευματική ιδιοκτησία είναι το σύνολο των εξουσιών που δίνει ο νόμος στον ιδιοκτήτη ενός πνευματικού έργου (συγγραφέα, συνθέτη, προγραμματιστή κ.λπ.) να προστατεύσει, να διαχειριστεί και να αμειφθεί ακόμη από τρίτους, όταν εκείνοι εκμεταλλεύονται την πνευματική του περιουσία.

Στο Διαδίκτυο το ψηφιακό υλικό (κείμενα, εικόνες, μουσική, βίντεο κ.λπ.) που αναρτάται ή διακινείται προστατεύεται εξίσου από τη νομοθεσία περί πνευματικής ιδιοκτησίας. Μάλιστα οι περισσότεροι ιστότοποι περιέχουν αναλυτική αναφορά στην πνευματική τους ιδιοκτησία (copyright). Αν θέλουμε να χρησιμοποιήσουμε σε εργασία μας υλικό από το Διαδίκτυο, θα χρειαστεί πολλές φορές να ενημερώσουμε τον δημιουργό του και να ζητήσουμε την έγγραφη έγκρισή του. Σε περιπτώσεις που δεν γίνεται ρητή αναφορά σε πνευματικά δικαιώματα καλό είναι να αναφέρουμε τις πηγές μας.

Η προώθηση μέσω του Διαδικτύου παράνομων αντιγράφων έργων πνευματικής ιδιοκτησίας (π.χ. μουσικής, ταινιών, ηλεκτρονικών βιβλίων, προγραμμάτων) θεωρείται άδικη και παράνομη πράξη, και τιμωρείται. Το ζήτημα των πνευματικών δικαιωμάτων είναι δύσκολο να αντιμετωπιστεί λόγω της έκτασης και της πολυπλοκότητας του Διαδικτύου. Ο καθένας προσωπικά θα πρέπει να σέβεται τους δημιουργούς πνευματικών έργων και να δρα έντιμα και ηθικά.

ΚΕΦΑΛΑΙΟ 8 – ΕΠΙΛΟΓΟΣ

Με τη συνεχή ανάπτυξη της τεχνολογίας ακόμα και μια απλή περιήγηση στο διαδίκτυο θα πρέπει να γίνεται με προσοχή και να ακολουθείτε από κάποιος κανόνες ασφαλείας, για την προστασία μας από απειλές.

Οι δράστες εκμεταλλεύονται την ανωνυμία και κάνει πιο εύκολη την τέλεση εγκλημάτων που μπορεί με παραδοσιακούς τρόπους να μην εκτελουσαν. Ακόμα και ένα χακαρισμα μπορεί να γίνει με σκοπό της ανάπτυξης των ικανοτήτων του χάκερ στοχεύοντας κλιμακωτά σε μεγαλύτερα εγκλήματα.

Γνωστά εγκλήματα και τρόποι δράσεις έχουν οδηγήσει σε τρόπους αντιμετώπισης. Ωστόσο σε αυτά τα εγκληματα δεν υπάρχει μόνο ένα συμβατικός τύπος αντιμετώπισης καθώς τα συστήματα και οι κώδικες ποικίλουν και μπορεί να υπάρχει κάθε φορά διαφορετική πόρτα εισόδου για τους δράστες.

Η αναγνώριση ως έγκλημα είναι το βήμα για την συνεχή εξέλιξη στον τομέα ώστε να αποτρέπονται αυτές οι επιθέσεις και η συνεχής ενημέρωση και εκμάθηση του κοινού ώστε να είναι υπόψισμενο και να μην πέφτει εύκολο θύμα των δραστών. Όπως επίσης και από την πλευρά του νόμου οι νέες νομοθεσίες να καλύπτουν την πλειονότητα των εγκλημάτων για την προστασία των πολιτών.

ΚΕΦΑΛΑΙΟ 9 – ΑΝΑΦΟΡΕΣ / LINKS

https://sites.google.com/site/elektronikoenklema2012/ti-einai-elektroniko-enklema

http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414&Itemid=0&langENENENEN

https://sites.google.com/site/electroniccrime09/reminderoffieldtripnextweek

https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/the-12-types-of-cyber-crime.html

https://www.provataslaw.gr/%CE%BD%CE%AD%CE%B1/%CF%84%CE%BF-%CE%B4%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF-%CF%89%CF%82-%CE%BC%CE%AD%CF%83%CE%BF-%CF%80%CF%81%CE%BF%CF%8E%CE%B8%CE%B7%CF%83%CE%B7%CF%82-%CF%84%CE%B7%CF%82-%CF%80%CE%B1%CE%B9%CE%B4%CE%B9%CE%BA%CE%AE%CF%82-%CF%80%CE%BF%CF%81%CE%BD%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1%CF%82

https://www.google.com/amp/s/astinomiko.gr/%25CE%25BC-%25CF%2583%25CF%2586%25CE%25B1%25CE%25BA%25CE%25B9%25CE%25B1%25CE%25BD%25CE%25AC%25CE%25BA%25CE%25B7%25CF%2582-%25CE%25B4%25CE%25B9%25CE%25B1%25CE%25B4%25CE%25AF%25CE%25BA%25CF%2584%25CF%2585%25CE%25BF-%25CE%25BA%25CE%25B1%25CE%25B9-%25CF%2584%25CF%2581%25CE%25BF%25CE%25BC%25CE%25BF%25CE%25BA%25CF%2581%25CE%25B1/amp/

https://www.foxbusiness.com/lifestyle/the-worst-cyber-attacks-of-the-past-10-years

https://en.m.wikipedia.org/wiki/Cyberterrorism

https://www.dictionary.com/e/dark-web/

https://www.sciencedirect.com/topics/computer-science/black-hat-hacker

https://www.kaspersky.com/resource-center/threats/top-ten-greatest-hackers

https://www.weforum.org/agenda/2019/03/here-are-the-biggest-cybercrime-trends-of-2019/

https://sites.google.com/site/hlektronikoegklima2013/prostasia-prosopikon-dedomenon

https://blogs.sch.gr/infosec/5-2-2-%CE%B2%CE%B1%CF%83%CE%B9%CE%BA%CE%AD%CF%82-%CE%B1%CF%81%CF%87%CE%AD%CF%82-%CE%B1%CF%83%CF%86%CE%B1%CE%BB%CE%B5%CE%AF%CE%B1%CF%82%CF%80%CE%BB%CE%B7%CF%81%CE%BF%CF%86%CE%BF%CF%81%CE%B9%CE%B1/

http://www.avgi.gr/article/10965/7878979/metra-gia-asphale-periegese-sto-diadiktyo-kai-prostasia-aporretou-ton-epikoinonion

https://www.offlinepost.gr/2020/05/27/%CF%84%CE%BF-%CE%B7%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CF%8C-%CE%AD%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1-%CE%BA%CE%B1%CE%B9-%CF%84%CE%BF-%CE%B5%CE%BB%CE%BB%CE%B7%CE%BD%CE%B9%CE%BA/

https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm

https://www.google.com/amp/s/www.ethnos.gr/kosmos/33134_se-efarmogi-oi-neoi-nomoi-gia-ta-pneymatika-dikaiomata-sto-internet%3famp

https://sites.google.com/site/bkasiolas/plerophories-pneumatika-dikaiomata-kai-peirateia-logismikou-sto-diadiktyo/pneumatika-dikaiomata