ΣΧΟΛΗ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΕΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΠΡΟΣΤΑΣΙΑΣ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΤΟ ΣΚΟΤΕΙΝΟ ΔΙΑΔΙΚΤΥΟ

Παπουτσής Παναγιώτης

Επιβλέπων καθηγητής: Γκόγκος Χρήστος

Άρτα, Ιούλιος 2022

COMPUTER SECURITY AND PROTECTION ISSUES AND THE DARK WEB

Τριμελή εξεταστική επιτροπή:

Άρτα, 4-7-2022

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ:

1. Επιβλέπων καθηγητής
   Χρήστος Γκόγκος

2. Μέλος επιτροπής
   Νικόλαος Γιαννακέας

3. Μέλος επιτροπής
   Ευριπίδης Γλαβάς

Περίληψη

Η εργασία αποτελείται από τέσσερα συνολικά κεφάλαια και επιχειρεί να προβάλλει το διαχρονικό και υψίστης σημασίας θέμα της ασφάλειας καθώς και προστασίας των υπολογιστών από τους κινδύνους που υφίστανται, ενώ επιπλέον διεισδύει στο σκοτεινό κόσμο του Dark Web. Στο πρώτο κεφάλαιο γίνεται εισαγωγή, ερμηνεύοντας τον όρο της ασφάλειας και επισημαίνοντας τη σπουδαιότητα της ύπαρξής της. Επιπρόσθετα, παρατίθενται οι πιθανοί κίνδυνοι που διατρέχει ένας χρήστης στον χώρο του διαδικτύου. Στο κεφάλαιο δίνεται ο ορισμός του κακόβουλου λογισμικού και διευκρινίζονται τα λογισμικά που ανήκουν σε αυτή την κατηγορία. Ολοκληρώνεται με τρόπους που θα μπορούσε οι πιθανοί κίνδυνοι να αποφευχθούν προτείνοντας λύσεις. Εν συνεχεία, το δεύτερο κεφάλαιο ασχολείται με την προστασία των ηλεκτρονικών υπολογιστών. Αρχικά δίνονται ιστορικά δεδομένα, χαρακτηριστικά και προβλήματα, που αφορούν τα αντιιικά προγράμματα. Επιπλέον, δίνονται οι βασικές λειτουργίες τους καθώς επίσης δίνεται έμφαση στις μεθοδολογίες στις οποίες βασίζονται. Το κεφάλαιο ολοκληρώνεται παραθέτοντας ένα πλήθος προγραμμάτων σε συνδυασμό με τις λειτουργίες που προσφέρουν καθώς και τρόπους ενίσχυσης της ασφάλειας.

Το τρίτο κεφάλαιο ασχολείται με τον τρόπο δραστηριοποίησης ενός forum. Αρχικά, δίνεται ο ορισμός του forum και ακολουθούν τα πλεονεκτήματα και μειονεκτήματα αυτού. Στην συνέχεια δίνεται ιδιαίτερη έμφαση στην οργάνωση ενός forum και επισημαίνεται η ανάγκη ύπαρξης των διαχειριστών και εποπτών, όπου και δίνονται οι ορισμοί αυτών. Επιπλέον, παραθέτονται μέθοδοι επιλογής εποπτών και προτείνονται συγκεκριμένοι τρόποι για την επιλογή τους. Η εργασία ολοκληρώνεται με το τέταρτο κεφάλαιο το οποίο αφορά το Dark Web (σκοτεινό διαδίκτυο). Συγκεκριμένα σε αυτό παρουσιάζεται ο ορισμός του Dark Web και οι διαφορές του με το Deep Web (βαθύς ιστός). Επιπλέον, γίνεται μία ιστορική αναδρομή του Dark Web και προβάλλεται το εύρος της αναζήτησης που διαθέτει. Επίσης, επισημαίνονται τα πλεονεκτήματα και μειονεκτήματα αυτού καθώς επίσης παρουσιάζονται και οι τρόποι με τους οποίους μπορεί κανείς να αποκτήσει πρόσβαση σε αυτό. Το κεφάλαιο κλείνει υποδεικνύοντας εγκλήματα που διαπράχθηκαν και εξακριβώθηκαν εντός του Dark Web και γίνεται αναφορά για την εξέλιξη του.

Λέξεις κλειδιά: ασφάλεια, αντιιικό, μολυσμένο λογισμικό, forum, σκοτεινό διαδίκτυο

Abstract

The thesis consists of four chapters in total and attempts to highlight the timeless and most important issue of computer security and potection from the dangers that exist, while also penetrating into the dark web. In the first chapter there is an introduction interpreting the term "security" and pointing out the importance of its existence. In addition, the potential dangers that a user runs in the internet space are listed. This chapter defines the malware and clarifies the software that belongs to this category. This is completed in ways that potential risks could be avoided by proposing solutions. The second chapter deals with the protection of computers. Initially, historical data, characteristics and problems related to antivirus programmes are given. In addition, their basic functions are given, as well as emphasis is placed on the methodologies on which they are based. The chapter concludes by listing a number of programmes in conjunction with the features they offer, as well as ways to enhance security.

The third chapter deals with how a forum works. First, the forum is defined and its advantages and disadvantages follow. Then, special emphasis is given to the organization of a forum, and the need for administrators and moderators is pointed out, where their definitions are given. In addition, methods for selecting moderators are listed and specific ways are proposed for their selection. The thesis is completed with the fourth chapter which concerns the Dark web. Specifically, this presents the definition of the Dark web and its differences with the Deep web. In addition, a historical retrospective of the dark web is made and the range of its search is displayed. It also highlights the advantages and disadvantages of it and shows the ways in which it can be accessed. The chapter closes by pointing out crimes that were committed, identified and solved withing the dark web and a reference is made to its evolution.

Key words: security, antivirus, malware, forum, dark web

ΔΗΛΩΣΗ ΠΝΕΥΜΑΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ

Η παρούσα εργασία αποτελεί προϊόν αποκλειστικά δικής μου προσπάθειας. Όλες οι πηγές που χρησιμοποιήθηκαν περιλαμβάνονται στη βιβλιογραφία και γίνεται ρητή αναφορά σε αυτές μέσα στο κείμενο όπου έχουν χρησιμοποιηθεί.

Πίνακας περιεχομένων

Εισαγωγή

Σε αυτό το σημείο της εργασίας θα δοθεί ο σκοπός και οι στόχοι που επιθυμεί η ίδια να επιτύχει.

Σκοπός

Σκοπός της εργασίας είναι να θίξει το θέμα της ασφάλειας των ηλεκτρονικών υπολογιστών και να αναδείξει την σπουδαιότητα και την αναγκαιότητά της στον χώρο του διαδικτύου. Έχει σκοπό την ενημέρωση του αναγνώστη από πιθανούς κινδύνους που ενδέχεται να έρθει αντιμέτωπος προτείνοντάς του λύσεις αντιμετώπισης και αποφυγής. Επιπλέον, γνωστοποιεί στον ίδιο την χρησιμότητα, την λειτουργία και την οργάνωση ενός forum σε συνδυασμό με τα οφέλη που του προσφέρει και τους κινδύνους που διατρέχουν. Επιπρόσθετα, αναφέρεται στην ύπαρξη του Dark Web με σκοπό να πληροφορήσει τον αναγνώστη σχετικά με τα πλεονεκτήματα και μειονεκτήματα που διαθέτει καθώς επίσης να επισημάνει τους κινδύνους που ενέχουν.

Στόχος

Ο στόχος της εργασίας είναι μέσω της ενημέρωσης να προφυλάξει τον εκάστοτε χρήστη από τους διάφορους κινδύνους που υπάρχουν εντός του διαδικτύου. Συγκεκριμένα προτείνει τρόπους, που αν εφαρμοστούν έχουν ως αποτέλεσμα την αύξηση της ασφάλειας των χρηστών καθώς επίσης προτείνονται ενέργειες με τις οποίες οι αντίστοιχοι φορείς θα καταφέρουν να προφυλάξουν τους πολίτες. Επίσης, η εργασία παροτρύνει τους αναγνώστες να εγκαταστήσουν κάποιο αντιιικό λογισμικό για την αποφυγή ή/και την αντιμετώπιση μιας απειλής καθώς επίσης οι χρήστες να χρησιμοποιούν το Dark Web με σύνεση. Συμπερασματικά, στόχος της εργασίας είναι η προφύλαξη των χρηστών από τους εκάστοτε κινδύνους που διατρέχουν στο διαδίκτυο.

Κεφάλαιο 1ο: Ασφάλεια

Ο όρος της ασφάλεια είναι απλός και παράλληλα σύνθετος. Συνήθως, συνδέεται με την έννοια της προστασίας από τον κίνδυνο ή/και της απώλειας. Ωστόσο, μπορεί να υπονοεί και το περιβάλλον μέσα στο οποίο όταν κάποιος περικλείεται νιώθει σιγουριά και αυτοπεποίθηση. Από την άλλη πλευρά, η ασφάλεια των υπολογιστών είναι το κομμάτι της επιστήμης που επικεντρώνεται στην προστασία αυτών και των δικτύων, μέσω των οποίων αλληλεπιδρούν, έχοντας ως στόχο την διασφάλιση των δεδομένων που ανταλλάσσονται και την αποτροπή της μη εξουσιοδοτημένης πρόσβασης, αυτών. Στόχος της είναι η προστασία από κακόβουλα λογισμικά που στόχο έχουν να βλάψουν τους χρήστες και τις συσκευές τους [**Πηγή 1 Κεφ1**]. Ως επακόλουθο, η ασφάλεια αποτελεί κάτι που περιλαμβάνει και εμπεριέχει πολλές διαστάσεις. Επιπλέον, οι κίνδυνοι με τους οποίους μπορεί να έρθει αντιμέτωπος ένας χρήστης είναι τόσο γενικοί όσο και ειδικοί. Παράλληλα, για να επιτευχθεί η ασφάλεια των υπολογιστών, πρέπει να υπάρξει η κατάλληλη ενημέρωση και εκπαίδευση των χρηστών ηλεκτρονικών υπολογιστών και συσκευών. Αυτό θα έχει ως αποτέλεσμα, οι χρήστες να ενημερωθούν για τους πιθανούς κινδύνους και ταυτόχρονα θα αντιληφθούν τρόπους αποφυγής και πρόληψης αυτών.

1.1 Ανάγκη για Ασφάλεια

Σε αυτή την ενότητα της εργασίας, αναφέρονται οι λόγοι για τους οποίους είναι επιτακτική η ανάγκη της ασφάλειας των υπολογιστών. Συγκεκριμένα αναφέρονται και εν συνεχεία επεξηγούνται αναλυτικά οι λόγοι για τους οποίους είναι απαραίτητη η ασφάλεια στον κυβερνοχώρο. Αξίζει να σημειωθεί, ότι το διαδίκτυο εξελίσσεται συνεχώς και ταυτόχρονα αυξάνονται και οι χρήστες του. Από την άλλη πλευρά βέβαια, αυξάνονται και εξελίσσονται και οι κίνδυνοι με τους οποίους μπορεί να έρθει αντιμέτωπος ένας χρήστης.

Ενδεικτικά, οι κύριοι λόγοι για τους οποίους καθίσταται αναγκαία η παροχή ασφάλειας στο διαδίκτυο, είναι οι εξής:

- Πρόκειται για ένα ευαίσθητο περιβάλλον.
- Χαρακτηρίζεται από πολυπλοκότητα.
- Εξαρτάται από την τεχνολογική εξέλιξη και πρόοδο.
- Υπάρχει αυξανόμενη τάση, ως προς την χρήση του, από όλο και περισσότερους ανθρώπους.
- Διαθέτει άπειρο περιεχόμενο.

Πιο αναλυτικά:

-Πρόκειται για ένα ευαίσθητο περιβάλλον: Το περιβάλλον των υπολογιστών και συγκεκριμένα το internet, κατά γενική ομολογία, αποτελούν χώρους ευαίσθητους σε επιθέσεις και απειλές. Επιπλέον, τα δεδομένα είτε προσωπικού χαρακτήρα είτε όχι, κινδυνεύουν πάντα να διαρρεύσουν προκαλώντας αμέτρητα προβλήματα στο χρήστη. Κάθε αλληλεπίδραση με το διαδίκτυο δημιουργεί δεδομένα και ¨ταυτότητα¨ για τον εκάστοτε χρήστη, τα οποία είναι πιθανόν να κλαπούν από τρίτους.

-Χαρακτηρίζεται από πολυπλοκότητα: Οτιδήποτε είναι σύνθετο ως προς την μορφή του, την λειτουργία του, την λειτουργικότητα του αλλά και ως προς την δομή του, αμέσως κρίνεται επιτακτικό να προστατευτεί. Εφόσον το διαδίκτυο πληρεί τις παραπάνω προϋποθέσεις, η ασφάλεια του είναι αναγκαία. Η ουσία του και η σημασία του διαδικτύου είναι τεράστια και αδιαμφισβήτητη και αυτός είναι ο λόγος που το καθιστά πολύπλοκο.

-Εξαρτάται από την τεχνολογική εξέλιξη και πρόοδο: Τα περισσότερα τεχνολογικά και επιστημονικά επιτεύγματα βασίζονται στην εξέλιξη και την πρόοδο. Το διαδίκτυο διατηρεί μία σχέση εξάρτησης με την τεχνολογική εξέλιξη και την πρόοδο. Με βάση αυτά γίνεται γρηγορότερο και εμπλουτίζεται το περιεχόμενό του. Βέβαια, όσο εξελίσσεται το διαδίκτυο τόσο εξελίσσονται και εξειδικεύονται οι κίνδυνοι. Για αυτό το λόγο η ασφάλεια του κρίνεται απαραίτητη.

-Υπάρχει αυξανόμενη τάση, ως προς την χρήση του, από όλο και περισσότερους ανθρώπους: Το διαδίκτυο παγκοσμίως χρησιμοποιείται από όλο και περισσότερο κόσμο.

Η αύξηση της χρήσης του αυξάνει ταυτόχρονα και το εύρος των ηλικιών που το αξιοποιούν. Επομένως, το διαδίκτυο χρησιμοποιείται και από ανήλικους ανθρώπους, ή ακόμα και μικρά παιδιά. Για τον λόγο αυτό, κρίνεται σημαντική η ύπαρξη της ασφάλειας διότι, αν υπάρχει, ασφαλίζονται παράλληλα και οι άνθρωποι που το χρησιμοποιούν.

-Διαθέτει άπειρο περιεχόμενο: Στο διαδίκτυο περιέχεται μία πληθώρα περιεχομένου. Αρκετές φορές το περιεχόμενο αυτό, αντιστοιχεί σε παράνομα και επιβλαβή λογισμικά. Για τον προαναφερθέντα λόγο, θα ήταν θεμιτή η ύπαρξη της ασφάλειας των υπολογιστών. Με αυτόν τον τρόπο η συσκευή του χρήστη θα προστατεύεται, μέχρι ένα επίπεδο και θα του επιτρέπει την ασφαλή περιήγηση στο διαδίκτυο.

Λαμβάνοντας υπόψιν τα παραπάνω, γίνεται αντιληπτό ότι η ύπαρξη της ασφάλειας είναι αναγκαία σε ένα περιβάλλον όπως το διαδίκτυο. Αυτό το συμπέρασμα προκύπτει από τα χαρακτηριστικά του διαδικτύου, το οποίο είναι ένα περιβάλλον ευαίσθητο και περίπλοκο. Επιπλέον, η συνεχής τάση της εξέλιξης επιφέρει και την εξέλιξη των πιθανών κινδύνων που επιφυλάσσονται. Αυτό έχει σαν αποτέλεσμα η ασφάλεια μίας συσκευής, να κρίνεται ως σημαντική. Επιπρόσθετα, η ανάγκη της ασφάλειας ενισχύεται ακόμη περισσότερο όταν το διαδίκτυο χρησιμοποιείται από παιδιά, προκειμένου να προστατέψει τα ίδια και τις συσκευές τους.

1.2 Κίνδυνοι

Λόγω του ότι η χρήση του διαδικτύου γίνεται σε καθημερινή βάση από πάρα πολλούς ανθρώπους, υπάρχει η πεποίθηση πως η πρόσβαση και η χρήση αυτού είναι απλή. Η πραγματικότητα, όμως, διαψεύδει τον προαναφερθέντα ισχυρισμό. Οι προκλήσεις που καλείται να αντιμετωπίσει ο εκάστοτε χρήστης, ανεξάρτητα με τις γνώσεις του είναι πληθώρα. Συγκεκριμένα, ελλοχεύουν κίνδυνοι που δεν μπορούν να αγνοηθούν. Σε αυτούς τους κινδύνους στόχος είναι το ανήλικο αλλά και ενήλικο κοινό. Παρακάτω, γίνεται αναφορά και ανάλυση των κινδύνων, που είναι πιθανό να έρθει κάποιος αντιμέτωπος. Μερικοί από αυτού τους κινδύνους που μπορούν να εκθέσουν οικονομικά και ηθικά τον

εκάστοτε χρήστη είναι τα λογισμικά υποκλοπής, το ηλεκτρονικό ψάρεμα και οι ιοί [**Πηγή 2 Κεφ1**].

1.2.1 Προσωπικά Δεδομένα

Με την πάροδο του χρόνου το Internet έχει εξελιχθεί και συνεχίζει να αναπτύσσεται. Πάνω σε αυτό στηρίχθηκαν και αναπτύχθηκαν τα μέσα κοινωνικής δικτύωσης (social media). Στόχος αυτών, είναι η συντήρηση των ανθρωπίνων σχέσεων, η οποία επιτυγχάνεται με την αλληλεπίδραση και την επικοινωνία. Επιπλέον, μέσω των κοινωνικών δικτύων οι άνθρωποι, πέραν της επικοινωνίας, ψυχαγωγούνται και ενημερώνονται [**Πηγή 3 Κεφ1**]. Κάποια από τα δημοφιλή μέσα κοινωνικών δικτύων είναι το Facebook, το Twitter και το Instagram. Με την χρήση των μέσων κοινωνικής δικτύωσης, οι χρήστες δημιουργούν το δικό τους προσωπικό προφίλ (profile). Κάθε προφίλ εμπεριέχει δεδομένα που αντιστοιχούν σε έναν και μόνο έναν χρήστη και πληροφορίες που συνδέονται με τις προτιμήσεις του ίδιου. Αυτή η αντιστοιχία γίνεται με την χρήση των προσωπικών δεδομένων, όπως για παράδειγμα το όνομα, το επώνυμο, η διεύθυνση κατοικίας, ο αριθμός κινητού τηλεφώνου, ακόμα και ο αριθμός της πιστωτικής κάρτας. Αδιαμφισβήτητα, τα μέσα κοινωνικής δικτύωσης αναπτύχθηκαν, έχοντας ως στόχο την αλληλεπίδραση των ανθρώπων, κάνοντας την καθημερινότητα πιο εύκολη, αλλά η χρήση τους ενέχει αρκετούς κινδύνους.

Ένας από τους κύριους κινδύνους των μέσων κοινωνικής δικτύωσης είναι η διαρροή προσωπικών δεδομένων. Αρχικά, η διαρροή των προσωπικών δεδομένων είναι ένας κίνδυνος που συναντάτε αρκετά συχνά, όπου επιτήδειοι υποκλέπτουν όλα τα δεδομένα που έχει προσφέρει ο χρήστης στα μέσα κοινωνικής δικτύωσης. Ένας από τους διασημότερους τρόπους υποκλοπής προσωπικών δεδομένων είναι το Fishing. Αυτό επιτυγχάνεται, με την λήψη ενός μηνύματος ηλεκτρονικού ταχυδρομείου (e-mail), το όποιο υποδύεται μία εταιρία ή έναν οργανισμό και ζητά από τον χρήστη να του παραχωρήσει πληροφορίες που σχετίζονται με τον ίδιο. Με αυτό τον τρόπο, ο χρήστης μετατρέπεται σε θύμα των απατεώνων, οι οποίοι στην συνέχεια με την χρήση

πληροφοριών που σχετίζονται με τραπεζικούς λογαριασμούς να του αποσπάσουν μεγάλα χρηματικά ποσά.

Ένας ακόμα γνωστός κίνδυνος που συναντάται στα μέσα κοινωνικής δικτύωσης είναι ο εκφοβισμός (cyberbulling) που συναντάτε, συνήθως, στα παιδιά. Επιπλέον, η χρήση των κοινωνικών δικτύων και γενικότερα του διαδικτύου ενέχει τον κίνδυνο της έκθεσης και της προβολής ακατάλληλου περιεχομένου, κυρίως των παιδιών. Επιπλέον, στα κοινωνικά δίκτυα, επειδή χρησιμοποιούνται δεδομένα και πληροφορίες που σχετίζονται με τον χρήστη, όπως οι προτιμήσεις του ίδιου, είναι αρκετά πιθανό να του εμφανίζονται διαφημίσεις συναφείς με αυτές. Αποτέλεσμα αυτού είναι, να προβάλλονται στον χρήστη στοχευμένες διαφημίσεις οδηγώντας τον ίδιο στον υπερκαταναλωτισμό.

1.2.2 Κακόβουλο λογισμικό

Με τον όρο "κακόβουλο λογισμικό" νοείται οποιοδήποτε πρόγραμμα που μπορεί να επηρεάσει αρνητικά την λειτουργικότητα μίας συσκευής, όπως ο υπολογιστής, καθώς επίσης να εκθέσει τον ίδιο τον χρήστη, πολλές φορές ανεπανόρθωτα. Τέτοιου είδους λογισμικά έχουν αναπτυχθεί από γνώστες προγραμματισμού και ο στόχος τους είναι κυρίως το κέρδος. Χωρίζονται σε διάφορες κατηγορίες οι οποίες θα αναλυθούν παρακάτω:

- Worm (σκουλίκι): Είναι ένα είδος κακόβουλου λογισμικού που μπορεί να πολλαπλασιαστεί ώστε να μεταδοθεί σε άλλα συστήματα υπολογιστών μέσω κάποιου κοινού δικτύου. Ο χρήστης είναι πολύ πιθανό να μην έχει γνώση ότι η συσκευή του έχει προσβληθεί. Αυτό συμβαίνει διότι το Worm λογισμικό έχει την δυνατότητα να εκτελείται στο παρασκήνιο, χωρίς να έχει δοθεί αντίστοιχη εντολή από τον ίδιο [**Πηγή 4 Κεφ1**].

- Trojan (Δούρειος ίππος): Είναι ένα κακόβουλο λογισμικό που υποδύεται ένα αυθεντικό πρόγραμμα και ότι η λειτουργία του αφορά κάτι χρήσιμο. Με αυτό τον τρόπο παραπλανεί τον εκάστοτε χρήστη. Αφού ο χρήστης εξαπατηθεί και εκτελέσει

το λογισμικό, τότε το πρόγραμμα αποκτά την πλήρη πρόσβαση στην συσκευή του. Στην συνέχεια το λογισμικό έχει την δυνατότητα να υποκλέψει ή να καταστρέψει προσωπικά δεδομένα του χρήστη, καθώς επίσης να εγκαταστήσει επιπλέον κακόβουλα λογισμικά [**Πηγή 5 Κεφ1**].

- Ransomware: Είναι ένα είδος κακόβουλου λογισμικού το οποίο, μετά την επιτυχή εκτέλεσή του, επιτίθεται στον αποθηκευτικό χώρο της συσκευής όπου και κρυπτογραφεί όλα τα αρχεία που εμπεριέχονται σε αυτόν [**Πηγή 6 Κεφ1**], όπως βίντεο, φωτογραφίες, αρχεία κειμένου κ.α. Επιπλέον ¨κλειδώνει¨ τον υπολογιστή και τον καθιστά αδύνατον προς χρήση. Σχεδόν, όλες τις φορές που προσβάλλεται μια συσκευή από Ransomware λογισμικό εμφανίζεται στην οθόνη αυτής ένα μήνυμα, στο οποίο εμπεριέχονται οδηγίες για την αποδέσμευση των αρχείων. Οι οδηγίες αυτές, παροτρύνουν τον χρήστη να καταβάλλει συγκεκριμένο χρηματικό ποσό κυρίως σε μορφή Bitcoin, προκειμένου τα αρχεία να αποκρυπτογραφηθούν. Με αυτόν τον τρόπο θα επιστραφούν τα αρχεία στον χρήστη και θα επανέλθει η εύρυθμη λειτουργία της συσκευής του. Το τελευταίο διάστημα, τα Ransomware λογισμικά παρουσιάζονται με την μορφή διάσημων και κοινών προγραμμάτων, όπως ένα αρχείο Word (της MicroSoft Office), παραπλανώντας τους χρήστες.

- Rootkit: Τέτοιου είδους λογισμικά, όταν εγκαθιστώνται σε μία συσκευή, έχουν ως απώτερο σκοπό τον πλήρη έλεγχο της συσκευής του χρήστη. Συγκεκριμένα, δίνουν την δυνατότητα στους δημιουργούς του λογισμικού αυτού, να διαχειρίζονται τα αρχεία της συσκευής [**Πηγή 7 Κεφ1**].

- Rogue: Πρόκειται για κακόβουλα λογισμικά που παριστάνουν την λύση ενός προβλήματος. Συγκεκριμένα, οι δημιουργοί αυτών των λογισμικών, πείθουν τους χρήστες ότι η συσκευή τους έχει μολυνθεί από έναν ιό και τους παροτρύνουν να εγκαταστήσουν έναν επιπλέον πρόγραμμα που θα επιφέρει την λύση [**Πηγή 8 Κεφ1**]. Στην πραγματικότητα όμως, οι χρήστες εγκαθιστούν ένα λογισμικό που είναι πράγματι κακόβουλο. Σκοπός, αυτών, είναι να προκαλέσουν μία σύγχυση

στον εκάστοτε χρήστη και για αυτό ανήκουν στην κατηγορία ScareWare, με σκοπό να εγκαταστήσει στην συσκευή του το λογισμικό που του προτείνεται.

- Spyware: Τέτοιου είδους λογισμικά έχουν ως στόχο την κατασκοπία της δραστηριότητας του χρήστη. Εγκαθιστώνται στις συσκευές δίχως ο χρήστης να το συνειδητοποιήσει και εκτελούνται στο παρασκήνιο [**Πηγή 9 Κεφ1**]. Μετά την εγκατάστασή τους, ουσιαστικά συλλέγουν δεδομένα και πληροφορίες που σχετίζονται με την δραστηριότητα του χρήστη, τόσο της συσκευής όσο και του διαδικτύου. Εν συνεχεία αυτές οι πληροφορίες αποστέλλονται στους εκάστοτε δημιουργούς των κακόβουλων λογισμικών, οι οποίοι τα μεταπωλούν και αποκομίζουν κέρδος.

- Keylogger: Τέτοιου είδους λογισμικά, μετά την εγκατάστασή τους καταγράφουν οτιδήποτε πληκτρολογήσει ο χρήστης [**Πηγή 10 Κεφ1**] με απώτερο σκοπό να υποκλέψει κωδικούς email, μέσων κοινωνικής δικτύωσης (social media), ακόμη και αριθμούς τραπεζικών λογαριασμών. Όλα αυτά αποστέλλονται στους δημιουργούς αυτών των λογισμικών προκειμένου να λάβουν τον πλήρη έλεγχο σε λογαριασμούς κοινωνικής δικτύωσης, τους οποίους θα μπορούν να τους πουλήσουν ή να αποσπάσουν χρηματικά ποσά.

Λαμβάνοντας υπόψιν όλους τους παραπάνω κινδύνους, η ανάγκη για ασφάλεια είναι πολύ μεγάλη. Και με την πάροδο του χρόνου και την εξέλιξη της τεχνολογίας καθίσταται αναγκαία η ενημέρωση και η εκπαίδευση όλων μας. Οι προκλήσεις που πρέπει να αντιμετωπιστούν είναι πολλές και κρίσιμες. Χρειάζονται άμεσες, στοχευμένες και συλλογικές δράσεις. Ωστόσο, με σωστή καθοδήγηση από τους κατάλληλους φορείς, όπως θα αναλυθεί παρακάτω, υπάρχουν λύσεις προς την αντιμετώπιση.

1.3 Τρόποι ενημέρωσης και εκπαίδευσης

Μέσω της ενημέρωσης και της εκπαίδευσης από φορείς καθίσταται δυνατή η αντιμετώπιση από τους κινδύνους και τα προβλήματα του διαδικτύου. Προκειμένου να συμβεί κάτι τέτοιο, θα πρέπει η εκάστοτε κυβέρνηση να θέσει αρμόδιους ανθρώπους που θα συμβάλουν με αποφασιστικό τρόπο ώστε να εφαρμοστούν κατάλληλα μέτρα, να ληφθούν ορθές αποφάσεις και να δοθούν σωστές κατευθύνσεις προς τους πολίτες. Βέβαια, αυτή η δράση δεν χρειάζεται μόνο την κινητοποίηση του κράτους αλλά απαιτεί και την συνεργασία των γονέων, των παιδιών και του σχολείου [**Πηγή 11 Κεφ1**].

Πιο αναλυτικά:

- Γονείς:

  Η ιδέα είναι ότι για να μπορέσουν οι γονείς να προστατέψουν όχι μόνο τα παιδιά τους αλλά και τον εαυτό τους από τους κινδύνους, είναι να τους κατανοήσουν. Αρχικά, τα ψηφιακά μέσα, όπως ο υπολογιστής και το tablet, καλό είναι να βρίσκονται σε χώρους όπου είναι εύκολα προσβάσιμοι από όλη την οικογένεια. Με αυτό τον τρόπο οι γονείς θα μπορούν να ελέγχουν διακριτικά το παιδί, να θέτουν χρονικό όριο στη χρήση του υπολογιστή και γενικότερα να είναι σε θέση να επέμβουν άμεσα και αποτελεσματικά χωρίς να χρονοτριβούν. Κύριο μέλημα των γονιών πρέπει να είναι η συζήτηση και ο διάλογος ώστε να υπάρχει πάντα μια άμεση επαφή με τα παιδιά. Οι γονείς είναι σωστό να ενημερώνονται για τα νέα δεδομένα, για τους νέους κινδύνους από ειδικούς αλλά να ψάχνουν και οι ίδιοι.

  Έπειτα, μέσα από ουσιαστικούς διαλόγους τα παιδιά, θα ενημερώνονται ώστε να κατανοούν τους κινδύνους του διαδικτύου. Αυτό πρέπει να γίνεται με ήπιο τόνο και σε χαλαρό ύφος, διότι τα παιδιά είναι πολύ πιο πιθανό να ακούσουν, να καταλάβουν και να εφαρμόσουν τις συμβουλές των γονιών τους. Επίσης, όταν πραγματοποιούνται γνωριμίες μέσω διαδικτύου, τα παιδιά πρέπει να επιβλέπονται από τους γονείς, καθώς είναι επικίνδυνο και για τα ίδια. Τέλος, προτρέποντας ένας γονιός το παιδί του να χρησιμοποιεί συγκεκριμένους διαδικτυακούς ιστοτόπους,

ιδιαίτερα σε πιο νεαρή ηλικία, του δίνει την ικανότητα να φιλτράρει και να αξιολογεί το υλικό που του παρουσιάζεται.

- Σχολείο:

  Εφόσον η χρήση του υπολογιστή έχει γίνει αναπόσπαστο κομμάτι της νέας γενιάς δεν γίνεται να απαγορευτεί στα παιδιά η χρήση αυτού και η πλοήγηση στο διαδίκτυο. Το σχολείο μπορεί να οργανώνει εκπαιδευτικά σεμινάρια στα πλαίσια της ενημέρωσης και της πρόληψης σχετικά με την κυβερνοασφάλεια. Σε αυτά τα σεμινάρια, μπορούν να προστεθούν όχι μόνο θεωρητικά πλαίσια, αλλά και δραστηριότητες πρακτικού χαρακτήρα για να γίνει πιο ευχάριστο για τα παιδιά. Για παράδειγμα, κάποιο διαγώνισμα κατανόησης αντιπροσωπευτικό της ηλικίας του παιδιού ή ακόμη και εκπαιδευτικά παιχνίδια στον υπολογιστή. Καλλιέργεια κριτικής σκέψης στα παιδιά για να μπορούν να είναι σε θέση να αξιολογούν μόνα τους, τους κινδύνους. Εκμάθηση βασικών κανόνων περιήγησης στο διαδίκτυο. Τέλος, μια ακόμη πρόταση είναι να εισαχθεί ένα επιπλέον μάθημα εξειδικευμένο για την ενημέρωση, πρόληψη και εκπαίδευση των παιδιών που θα έδινε μια ευχάριστη και παράλληλα ουσιαστική νότα στην εκπαίδευση των παιδιών από μικρή ηλικία.

- Παιδιά:

  Το σημαντικότερο πράγμα που έχουν να κάνουν τα παιδιά από την πλευρά τους είναι να μιλούν και πιο ειδικά να ρωτάνε. Μέσω των ερωτήσεων θα διευρύνουν τις γνώσεις τους. Άρα θα μαθαίνουν καινούργια πράγματα χρήσιμα ως προς την ασφάλεια και τους κινδύνους. Επομένως καλό είναι τα παιδιά να μην ντρέπονται και να μην νιώθουν μειονεκτικά όταν παραθέτουν τις απορίες τους. Επίσης, μία πρόταση είναι να μην παρέχουν προσωπικά δεδομένα και γενικότερα δεδομένα στα μέσα κοινωνικής δικτύωσης. Σύμφωνα με τα παραπάνω, τα παιδιά θα είναι σε θέση να αντιληφθούν ένα πιθανό κίνδυνο και να τον αποφύγουν.

- Κράτος:

Από την πλευρά του το κράτος, θα πρέπει να αυστηροποιήσει το νομοθετικό πλαίσιο του κυβερνοεγκλήματος και αυτό είναι κάτι το οποίο πρέπει να πραγματοποιηθεί άμεσα. Επιπλέον, θα ήταν σκόπιμο να εξεταστούν τα κυβερνοεγκλήματα και να καταταχθούν σε κατηγορίες. Αυτό θα έχει σαν αποτέλεσμα να αξιολογείται κάθε παράνομη πράξη και να επιβάλλεται η εκάστοτε ποινή στους κακοποιούς που τις διαπράττουν. Επιπρόσθετα, το Υπουργείο Ψηφιακής Διακυβέρνησης, ως άμεσος υπεύθυνος για θέματα ασφάλειας στο διαδίκτυο θα ήταν ωφέλιμο να σχεδιάσει ένα πλάνο ενημέρωσης και εκπαίδευσης των πολιτών. Αυτό θα μπορούσε να επιτευχθεί, οργανώνοντας ημερίδες διά ζώσης και εξ αποστάσεως με σκοπό να ενημερώνει τους πολίτες. Η συνεργασία με άλλα κράτη, ενδεχομένως, περισσότερο τεχνολογικά προηγμένα, ενδέχεται να δημιουργήσει ένα περιβάλλον ασφάλειας αλλά και σιγουριάς για να αποτρέψει την κατάχρηση του διαδικτύου από τον απλό πολίτη. Επιπλέον, μέσω της συνεργασίας άλλων κρατών, θα ήταν εφικτό η εξ αποστάσεως ενημέρωση των πολιτών, όπου θα δινόταν η ευκαιρία σε ανθρώπους με γνώση του αντικειμένου ή/και θέση εργασίας στην ασφάλεια να ενημερώσουν και να προφυλάξουν τους πολίτες.

Εν κατακλείδι του κεφαλαίου αυτού και διαβάζοντας τα παραπάνω, εύκολα οδηγείται κανείς στο συμπέρασμα ότι υπάρχουν τρόποι πρόληψης και αποφυγής των κινδύνων μέσω του διαδικτύου. Προκειμένου όμως να αποδώσουν, χρειάζεται συνεργασία και οργάνωση, τόσο από τους πολίτες όσο και από τους φορείς.

Κεφάλαιο 2: Προστασία

Στο κεφάλαιο αυτό θα παρουσιαστούν οι κύριοι τρόποι με τους οποίους είναι εφικτό να προστατευτεί ο εκάστοτε χρήστης του διαδικτύου. Στο πρώτο μέρος του κεφαλαίου, θα γίνει αναφορά στα προγράμματα προστασίας, θα δοθούν βασικά ιστορικά δεδομένα και στη συνέχεια θα εξηγηθούν οι λειτουργίες και τα χαρακτηριστικά τους καθώς και τον τρόπο με τον οποίο προστατεύουν τον υπολογιστή. Στο δεύτερο μέρος, θα δοθεί έμφαση στις τεχνικές των υπολογιστών που μπορούν να εφαρμοστούν για να δημιουργηθεί ένα ασφαλές περιβάλλον χρήσης των υπολογιστών.

2.1 Προγράμματα

Αυτήν η ενότητα έχει ως στόχο να ενημερώσει τον αναγνώστη σχετικά με τα αντιιικά προγράμματα. Συγκεκριμένα περιέχει ιστορικά δεδομένα αυτών καθώς επίσης παρουσιάζονται κάποια από τα βασικά τους χαρακτηριστικά.

2.1.1 Ιστορικά

Ο πρώτος αναγνωρισμένος ιός (virus) υπολογιστών έκανε την εμφάνισή του το 1971 και ονομάστηκε "Creeper virus" [**Πηγή 1 Κεφ2**]. Με την πάροδο του χρόνου εμφανίστηκαν και άλλοι ιοί. Αυτό είχε σαν αποτέλεσμα την ανάγκη ύπαρξης ενός προγράμματος (antivirus) που θα περιόριζε την δράση αυτών. Έτσι, το 1987 δημιουργήθηκε το πρώτο antivirus [**Πηγή 2 Κεφ2**] από την G Data Software. Την ίδια χρονιά επίσης, δημιουργήθηκε το McAfee antivirus αλλά και το NOD antivirus [**Πηγή 2 Κεφ2**].

Σήμερα, υπάρχουν εκατοντάδες δεκάδες αντιιικών προγραμμάτων (antivirus) για χρήση. Επιπλέον, η χρήση τους δεν περιορίζεται μόνο για τον μέσο χρήστη αλλά κρίνεται

και ως κατάλληλη για χρήση από επιχειρήσεις και οργανισμούς. Υπάρχουν αρκετά antivirus και κάποια από τα πιο γνωστά προγράμματα είναι το Kaspersky, το Norton, το Avast, το AVG και το BitDefender. Οι επιλογές είναι πάρα πολλές καθώς το κάθε προϊόν έχει διαφορές τόσο στον τρόπο λειτουργίας όσο και στο user interface.

2.1.2 Χαρακτηριστικά

Όπως έχει ήδη αναφερθεί υπάρχουν αρκετά αντιιικά προγράμματα (antivirus) τα οποία προσφέρονται έναντι αμοιβής ή ακόμη και δωρεάν. Το κάθε ένα από αυτά, διαθέτει συγκεκριμένα χαρακτηριστικά και λειτουργίες που είναι παρόμοιες μεταξύ τους, έχοντας ως κοινό στόχο την προστασία των ηλεκτρονικών υπολογιστών. Οι λειτουργίες και τα χαρακτηριστικά που προσφέρουν αυτά τα προγράμματα για τους υπολογιστές έχουν, τις περισσότερες φορές, κοινά στοιχεία. Παρακάτω, παρουσιάζονται οι κύριες λειτουργίες των αντιικών προγραμμάτων.

- Signature-based detection: Η λειτουργία αυτή είναι μία από τις πιο κοινές λειτουργίες των αντιιικών προγραμμάτων. Ουσιαστικά το antivirus δημιουργεί και αποθηκεύει ένα μοναδικό αναγνωριστικό για κάθε γνωστή απειλή [**Πηγή 3 Κεφ2**]. Με αυτό τον τρόπο το αντιιικό πρόγραμμα θα είναι σε θέση να εντοπίσει μία πιθανή απειλή. Ουσιαστικά, το antivirus μπορεί να εντοπίσει ιούς που έχουν ήδη ανακαλυφθεί και είναι μέρος της βάσης δεδομένων του.

- Behavior Detection: Είναι μια σχετικά σύγχρονη τεχνολογία που έχει υιοθετηθεί από τις εταιρείες αντιικών προγραμμάτων. Στην ουσία, η συγκεκριμένη λειτουργία είναι ικανή στο να εμποδίσει ένα κακόβουλο πρόγραμμα από το να εισβάλει και να αναδιαμορφώσει βασικά δεδομένα του υπολογιστή όπως το boot sector. Αυτό το επιτυγχάνει με την ανίχνευση κακόβουλων λογισμικών κατά την εκτέλεσή τους και αποτρέπει την παραβίαση της συσκευής [**Πηγή 4 Κεφ2**].

- Heuristic based detection: Είναι η ανάλυση κακόβουλων προγραμμάτων, βάσει κάποιων κανόνων που έχουν δημιουργηθεί, παρακολουθώντας και καταγράφοντας τις συμπεριφορές παλαιότερων κακόβουλων προγραμμάτων [**Πηγή 5 Κεφ2**].

- Sandbox: Είναι μια μέθοδος που χρησιμοποιούν κάποια αντιικά προγράμματα ώστε να δίνουν την δυνατότητα να εκτελεστεί ένα πρόγραμμα σε ένα προστατευμένο περιβάλλον [**Πηγή 6 Κεφ2**] που έχει δημιουργηθεί από το antivirus ώστε να παρατηρήσουμε αν το πρόγραμμα που εκτελέσαμε είναι ασφαλές ή όχι.

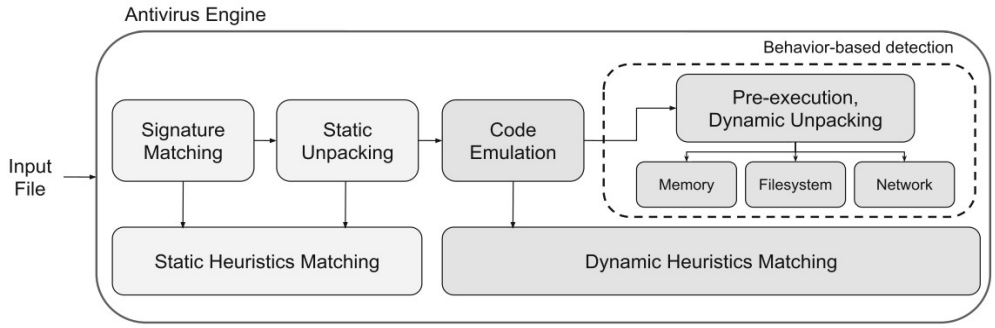
- Firewall: Είναι μια λειτουργία του antivirus που ελέγχει το δίκτυό μας για διάφορες κακόβουλες ενέργειες που μπορεί να γίνουν χωρίς την θέλησή μας. Είναι δηλαδή σαν μια πόρτα που εξετάζει τι δεδομένα θα λάβουμε και τι όχι, από το internet.

- HIPS (Host Intrusion Prevention System): Είναι μια λειτουργία παρόμοια με το Firewall, μόνο που εδώ προστατεύονται συγκεκριμένες λειτουργίες [**Πηγή 7 Κεφ2**] (π.χ. registry keys) του υπολογιστή παρακολουθώντας την συμπεριφορά του κώδικα από το πρόγραμμα που εκτελούμε σε αυτόν.

- Web protection: Πρόκειται για τον έλεγχο των ιστοσελίδων (site) που επισκέπτεται ο εκάστοτε χρήστης [**Πηγή 8 Κεφ2**]. Έτσι, πριν ο χρήστης εισέλθει στο site, πρώτα ελέγχεται αν η ιστοσελίδα είναι επιβλαβής ή όχι.

- Exploit protection: Λόγω κάποιας ευπάθειας ή/και κάποιου σφάλματος ενός ασφαλούς προγράμματος ή ακόμα και από τα ίδιο το λειτουργικό σύστημα, Windows, μπορεί να δημιουργηθεί κενό ασφαλείας με αποτέλεσμα ένα κακόβουλο λογισμικό να το εκμεταλλευτεί. Με την λειτουργία της Exploit protection εντοπίζονται και μετριάζονται οι ευπάθειες αυτές, με σκοπό την μέγιστη ασφάλεια [**Πηγή 9 Κεφ2**].

- Anti-ransomware protection ειδικό χαρακτηριστικό ενάντια των ransomware με δυνατότητα επαναφοράς αρχείων σε περίπτωση που έχουν επηρεαστεί.



Εικόνα 1: Λειτουργία antivirus και Behavior Detection
Πηγή:https://www.socinvestigation.com/most-common-antivirus-evasion-and-bypass-techniques/

Λαμβάνοντας υπόψη τα όσα αναφέρθηκαν, εύκολα διαπιστώνεται ότι ένα σύγχρονο antivirus μπορεί να προσφέρει μια αξιόπιστη προστασία όχι μόνο στο μέσο χρήστη αλλά και σε εταιρικό επίπεδο.

Προβλήματα

Σε αυτό το σημείο είναι σημαντικό να αναφερθεί ότι κανένα πρόγραμμα δεν είναι εντελώς αξιόπιστο. Κάθε λειτουργία που αναφέρθηκε έχει και την αδυναμία του. Για παράδειγμα, το Signature-based detection είναι αναποτελεσματικό σε πολύ καινούργιους ιούς, διότι δεν έχουν εντοπιστεί ώστε να μελετηθούν και να καταχωρηθούν στην βάση δεδομένων του αντιιικού προγράμματος. Επίσης, η λειτουργία Sandbox, στην περίπτωση που ο ιός εκτελεστεί στην συσκευή, ο ίδιος μπορεί να είναι προγραμματισμένος έτσι ώστε να αντιληφθεί ότι βρίσκεται σε εικονικό περιβάλλον, δηλαδή μέσα στο Sandbox, και να μην διαπράξει κακόβουλες ενέργειες. Όμως, όταν εκτελεστεί εκτός του Sandbox τότε θα το πράξει.

Σύμφωνα, με όλα τα παραπάνω, είναι σκόπιμο κάθε χρήστης να αναλύει προσεκτικά και συνειδητά τις συνήθειές του στο διαδίκτυο. Παρά το γεγονός ότι υπάρχουν

αρκετά αντιικά προγράμματα, κανένα από αυτά δεν προσφέρει πλήρη προστασία στην συσκευή του χρήστη και κατ' επέκταση στον ίδιο τον χρήστη. Επομένως, η επιλογή εγκατάστασης ενός αντιικού προγράμματος γίνεται με βάση την αξιοπιστία τους.

2.2 Διαφορετικά Προγράμματα και Τεχνικές των Windows

Εκτός από τα συνηθισμένα αντιικά προγράμματα και τις λειτουργίες που αναφέρθηκαν παραπάνω, υπάρχουν και άλλα προγράμματα αλλά και τεχνικές που ο χρήστης μπορεί να υιοθετήσει ώστε να έχει όσο το δυνατόν μεγαλύτερη προστασία. Υπάρχουν προγράμματα που μπορούν να λειτουργήσουν συμπληρωματικά με το antivirus. Για παράδειγμα, τα προγράμματα EXE Radar Pro και osarmor της εταιρείας novirusthanks έχουν σχεδιαστεί ώστε να μπορούν να "τρέχουν" ταυτόχρονα με όποιο antivirus υπάρχει στο σύστημα. Με αυτόν τον τρόπο εξασφαλίζεται η μέγιστη δυνατή ασφάλεια.

Τα συγκεκριμένα προγράμματα έχουν διαφορετικές μεθόδους αντιμετώπισης μολυσματικού λογισμικού. Δεν προορίζονται τόσο για τους απλούς χρήστες, επειδή είναι αρκετά σύνθετα, με την έννοια ότι έχουν αρκετές ρυθμίσεις ώστε να μεγιστοποιηθεί η ασφάλεια των υπολογιστών. Κύριο χαρακτηριστικό είναι η ρύθμιση που αποτρέπει όλα τα προγράμματα από το να εκτελεστούν ενώ επιτρέπεται να εκτελεστούν μόνο όσα έχει επιλέξει συνειδητά ο χρήστης. Παρόμοιο πρόγραμμα από διαφορετική εταιρεία είναι το AppGuard, που χρησιμοποιεί τρεις μηχανισμούς αντιμετώπισης επιβλαβούς λογισμικού: Zero Trust Space, Isolation, Inheritance.

Αναλυτικά, το Zero Trust Space είναι ένα μοντέλο ασφάλειας. Όπως προδίδεται και από την ονομασία που του έχει αποδοθεί, δηλαδή ¨μηδενική εμπιστοσύνη¨, το Zero Trust Space δεν επιτρέπει σε κανέναν χρήστη να έχει πρόσβαση σε δίκτυο και στους πόρους αυτού, χωρίς πρώτα ο ίδιος να πιστοποιηθεί ως εξουσιοδοτημένος χρήστης [**Πηγή 10 Κεφ2**]. Έτσι ο εκάστοτε χρήστης μπορεί να έχει πρόσβαση στους πόρους και στα στοιχεία εφόσον αρχικά πιστοποιηθεί η ταυτότητά του. Βάσει αυτής της τεχνικής προστατεύονται τα δεδομένα ενός δικτύου και μειώνονται οι κίνδυνοι από επιθέσεις κακόβουλων λογισμικών.

Επιπλέον, με την μέθοδο του Isolation οι εφαρμογές που βρίσκονται στο System Space ομαδοποιούνται σε δύο κατηγορίες [**Πηγή 11 Κεφ2**]. Η πρώτη κατηγορία είναι οι ¨υψηλού κινδύνου¨ εφαρμογές ενώ η δεύτερη είναι οι ¨κανονικές¨ εφαρμογές. Εν συνεχεία οι ¨υψηλού κινδύνου¨ εφαρμογές απομονώνονται και δεν επιτρέπεται να εκτελεστούν.

Σε συνδυασμό των δύο προηγούμενων, έρχεται να προστεθεί και η τεχνική του Inheritance. Με αυτή την τεχνική εξασφαλίζεται ότι ικανοποιούνται οι αρχές του Isolation [**Πηγή 11 Κεφ2**] προσαρμόζοντας αυτόματους ελέγχους για μεγαλύτερη ακρίβεια.

Ένα ακόμη είδος προγραμμάτων προστασίας είναι τα προγράμματα όπως το CatchPulse της εταιρείας SecureAge, το Crystal Security από τον developer Kardo Kristal και το VoodooShield από την εταιρεία VoodooSoft. Αυτά τα τρία προγράμματα έχουν ένα κοινό στοιχείο. Κάθε φορά που ο χρήστης εκτελεί ένα πρόγραμμα ή ανοίγει κάποιο αρχείο, αρχικά ελέγχεται με την χρήση όλων των υπόλοιπων αντιικών προγραμμάτων που υπάρχουν. Με αυτό τον τρόπο διαμορφώνεται ένα τελικό αποτέλεσμα βάσει του οποίου κρίνεται, αν το αρχείο είναι ασφαλές ή όχι. Το κύριο πρόβλημα που εντοπίζεται σε αυτού του είδους αντιικά προγράμματα είναι ότι η λειτουργία τους εξαρτάται από την χρήση του διαδικτύου. Επομένως, στην περίπτωση που τα προγράμματα αυτά είναι ενεργά στην συσκευή του χρήστη και δεν υπάρχει διαθέσιμο Internet, το αποτέλεσμα είναι να μπλοκάρουν το πρόγραμμα που επιθυμεί να εκτελέσει ο χρήστης και να απαγορεύσουν την εκτέλεσή του μέχρι να υπάρξει διαθέσιμο Internet.

Όπως έχει ήδη διαπιστωθεί, υπάρχουν αρκετές λύσεις που προσφέρουν ασφάλεια στους απλούς καθημερινούς χρήστες του διαδικτύου. Από την άλλη πλευρά υπάρχουν και αντίστοιχες λύσεις για τους προχωρημένους χρήστες που επιθυμούν περισσότερο έλεγχο που συνεπάγεται περισσότερη και αξιόπιστη προστασία. Αυτοί οι τρόποι μπορούν να επιτευχθούν με το SysHardener από την εταιρεία novirusthanks καθώς και με ένα άλλο πρόγραμμα, το Hard_Configurator από τον προγραμματιστή Andy Ful. Τα προγράμματα αυτά προσφέρουν πάρα πολλές ειδικές λειτουργίες μετατρέποντας τα Windows σε αρκετά ασφαλή λειτουργικά συστήματα χωρίς την χρήση κάποιου άλλου αντιικού προγράμματος. Κυρίως έχουν να κάνουν με το Software Restriction Policies (SRP) και το SmartScreen.

Όπως γίνεται αντιληπτό, υπάρχουν αρκετές επιλογές για να δημιουργηθεί ένα ασφαλές περιβάλλον στον υπολογιστή μας ώστε να είμαστε προστατευμένοι όσο το δυνατόν περισσότερο. Απαιτείται όμως να αφιερωθεί ένα εύλογο χρονικό διάστημα ώστε να αποφασιστούν οι κατάλληλες επιλογές που πραγματικά θα φανούν χρήσιμες και θα προστατεύσουν τόσο τον χρήστη όσο και τις συσκευές του.

Κεφάλαιο 3ο: Ασφάλεια και Προστασία σε Forum

Όπως είναι απαραίτητο να παρέχεται ένας βαθμός ασφάλειας και προστασίας στο διαδίκτυο, είναι σημαντικό να υπάρχει ασφάλεια και προστασία στα διάφορα forum. Όμως, υπάρχει μια διαφοροποίηση στους τρόπους με τους οποίους αυτό επιτυγχάνεται στο forum σε σύγκριση με το internet γενικά. Σε αυτό το κεφάλαιο, εκτός του ορισμού και της επεξήγησης του όρου forum, θα δοθούν παραδείγματα και θα αναφερθούν τα θετικά και αρνητικά χαρακτηριστικά του. Επιπλέον, θα εκφραστεί και η ανάγκη που υπάρχει για την οργάνωσή του. Στη συνέχεια, αφού αναφερθεί η έννοια του "επόπτη" και του "διαχειριστή" και οι τρόποι με τους οποίους διασφαλίζεται η ομαλή λειτουργία του φόρουμ, θα επισημανθεί η διαφάνεια αλλά και η εμπιστοσύνη του. Τέλος, θα αναφερθούν τα προβλήματα που μπορεί να προκύψουν και πώς μπορεί ο επόπτης να κάνει εφαρμογή των ικανοτήτων του στον επαγγελματικό τομέα.

3.1 Τι είναι forum

Το forum (ελληνικά: φόρουμ) είναι ένας τύπος ιστοσελίδων, όπου οι χρήστες μπορούν να συνομιλούν, να ανταλλάσουν ιδέες και απόψεις. Στο forum μπορεί να γίνει μέλος οποιοσδήποτε καθώς και να πάρει μέρος στις συζητήσεις. Οι θεματολογίες των forum είναι πάρα πολλές, για παράδειγμα αν κάποιος ενδιαφέρεται για την τεχνολογία μπορεί να επισκεφθεί τον ιστότοπο της Adslgr (https://www.adslgr.com/), αν πάλι ενδιαφέρεται για την αυτοκίνηση τότε μπορεί να επισκεφθεί τον ιστότοπο της Moto (https://www.moto.gr/). Ένα από τα πιο γνωστά forum παγκοσμίως είναι το Reddit (https://www.reddit.com/), όπου εκεί παρουσιάζονται άπειρα subreddits (ελληνικά: υπορέντιτ) που το κάθε ένα έχει διαφορετικές θεματολογίες. Τα τελευταία χρόνια όμως, έχει αναπτυχθεί με ραγδαίους ρυθμούς και το Discord, ένα πρόγραμμα που μία από τις λειτουργίες του είναι να δημιουργεί, ο ίδιος ο χρήστης, την δική του ομάδα που μπορεί να εξελιχθεί σε ένα μεγάλο φόρουμ. Τα forum συνήθως έχουν διάφορες κατηγορίες θεμάτων ώστε οι συζητήσεις να μην είναι μόνο πάνω στην κύρια θεματολογία του forum. Για παράδειγμα ένα forum τεχνολογίας υπάρχει περίπτωση να έχει και ειδικούς χώρους για

συζητήσεις εκτός θέματος (off topic), έτσι ώστε να προσφέρεται μία μεγάλη ποικιλία στο εύρος της θεματολογίας.

3.2 Θετικά και αρνητικά

Σε αυτή την ενότητα της εργασίας θα αναφερθούν τα πλεονεκτήματα και μειονεκτήματα των forum καθώς και οι λόγοι χρήσης αυτών. Αρχικά τα πλεονεκτήματα των forum είναι τα παρακάτω:

- Καθημερινά οι άνθρωποι βρίσκονται αντιμέτωποι με αρκετά προβλήματα, στα οποία δεν γνωρίζουν την λύση τους εκ των προτέρων. Αρκετές από αυτές τις φορές, η φύση του προβλήματος μπορεί να είναι αρκετά πολύπλοκη ώστε να μπορέσουν να καταλήξουν στην λύση μόνοι τους. Εφόσον ένας χρήστης είναι μέλος ενός forum, έχει την δυνατότητα να μοιραστεί ελεύθερα τον προβληματισμό του, ζητώντας καθοδήγηση και υποστήριξη από τα υπόλοιπα μέλη του ίδιου forum. Μέσω αυτού, είναι αρκετά πιθανό, ένας χρήστης να γνωρίζει την λύση του προβλήματος και την προσφέρει εντελώς δωρεάν. Έτσι, με την βοήθεια των forum δίνεται οι δυνατότητα στους ανθρώπους να ανταλλάσσουν αφιλοκερδώς σκόπιμες συμβουλές που θα φανούν χρήσιμες και βοηθητικές.

- Η συμμετοχή ενός χρήστη του διαδικτύου σε ένα forum, δεν περιέχει περιορισμούς, πέρα από την ηλικία σε μερικά από αυτά και είναι ανεξάρτητη της γεωγραφικής θέσης του χρήστη, της γλώσσας που ομιλεί, της οικονομικής του κατάστασης, του φύλου του, του χρώματος του δέρματος και της εθνικότητάς του. Σύμφωνα με το προαναφερθέν, σε ένα forum όλοι οι συμμετέχοντες αυτού είναι ίσοι.

- Επίσης, συζητώντας, οι χρήστες, με διαφορετικούς ανθρώπους από όλο τον κόσμο, ανταλλάσσουν ιδέες και απόψεις, διευρύνουν τους ορίζοντές τους, μαθαίνουν άλλα ήθη και έθιμα, νοοτροπίες και διαφορετικούς τρόπους σκέψης. Όλα αυτά βοηθούν

ως ένα βαθμό ώστε οι άνθρωποι να καλλιεργούν καλύτερη κριτική σκέψη, να γίνονται ανοιχτόμυαλοι, να βελτιώνουν τον τρόπο σκέψης και να εξελιχθούν σαν άνθρωποι.

- Τα forum συχνά χρησιμοποιούνται και για διασκέδαση, σε μια προσπάθεια οι χρήστες να ψυχαγωγηθούν. Μέσω των forum οι χρήστες είναι εφικτό να μοιραστούν μια διασκεδαστική ιστορία, να προτείνουν μία ταινία ή ένα βιβλίο που τους άφησε καλές εντυπώσεις, να παροτρύνουν τους υπόλοιπους χρήστες να συζητήσουν διάφορα θέματα της επικαιρότητας κ.α. Στην περίπτωση αυτή οι άνθρωποι αποσυμπιέζονται από την πίεση του χώρου εργασίας και διάφορους άλλους παράγοντες.

Με την παρουσίαση κάποιων από τα θετικά χαρακτηριστικά που μπορεί να μας προσφέρει το forum υπάρχουν και τα αρνητικά που δεν πρέπει να παραληφθούν:

- Συμμετέχοντας ενεργά σε forum και παίρνοντας μέρος σε συζητήσεις, ο χρήστης, αφιερώνει αρκετό χρόνο από την καθημερινότητά του και κατ΄ επέκταση από την ζωή του. Ουσιαστικά, σπαταλά χρόνο σε συζητήσεις με άτομα που στην πραγματικότητα δεν τα έχει γνωρίσει, που ίσως αργότερα τον εκθέσουν στον κίνδυνο. Ίσως θα ήταν καλύτερο, ο εκάστοτε χρήστης, να αφιερώσει χρόνο για να πραγματοποιήσει κάτι πιο παραγωγικό και εποικοδομητικό, όπως ένα χόμπι, κάποιο άθλημα ή να συναντηθεί με φίλους.

- Ένα πολύ σοβαρό πρόβλημα και επακόλουθο του προηγούμενου επιχειρήματος είναι αυτό του εθισμού. Το αίσθημα του να είναι ένας άνθρωπος αρεστός παίρνοντας μέρος σε διάφορες συζητήσεις, παραθέτοντας τις απόψεις του, βοηθώντας άλλα μέλη του forum, ίσως τον οδηγήσει σε αρνητικά αποτελέσματα. Αγνοώντας τις πραγματικές υποχρεώσεις που έχει ένας άνθρωπος σε βάθος χρόνου θα έχει επιπτώσεις τόσο σε προσωπικό όσο και κοινωνικό επίπεδο.

- Στην περίπτωση που ένας χρήστης μοιραστεί ένα πρόβλημα, με άλλους χρήστες, εντός ενός forum, ζητώντας μία λύση δεν είναι βέβαιο ότι θα λάβει την σωστή βοήθεια. Ίσως η φύση του προβλήματος να είναι τέτοια που μόνο ένας ειδικός θα μπορούσε να επιφέρει την λύση. Αυτό θα έχει σαν αποτέλεσμα η κατάσταση να χειροτερέψει, κάτι το οποίο θα προξενήσει επιπτώσεις.

Λαμβάνοντας υπόψιν όλα τα παραπάνω, διαπιστώνεται ότι τα forum διαθέτουν ισχυρά πλεονεκτήματα που μπορούν πράγματι να βοηθήσουν τους χρήστες του διαδικτύου. Όπως έχει ήδη ειπωθεί, τα forum προάγουν την ισότητα μεταξύ των ανθρώπων, διευρύνουν τους ορίζοντές τους και τους ψυχαγωγούν. Από την άλλη πλευρά βέβαια ενέχουν κινδύνους που ίσως οδηγήσουν σε μείωση του ελεύθερου χρόνου, να εθιστούν ή ακόμα και να μεγενθύνουν ένα πρόβλημα αντί να το επιλύσουν.

3.3 Ανάγκη οργάνωσης

Κατά την διάρκεια της ζωής ενός ανθρώπου, είναι πολύ πιθανό ο ίδιος να συμμετάσχει, έστω μια φορά, ως μέλος μιας ομάδας. Εντός κάθε ομάδας, είναι βέβαιο ότι υπάρχει κάποιος ή κάποιοι, που είναι υπεύθυνοι για την ομαλή λειτουργία της. Έτσι ακριβώς οργανώνεται και ένα forum. Συγκεκριμένα σε ένα σύνολο ανθρώπων που αλληλεπιδρούν μέσω internet, υπάρχουν οι επόπτες (ή συντονιστές) (αγγλικά: moderators) που είναι υπεύθυνοι για την ομαλή λειτουργία του forum. Και αυτό γίνεται διότι, η αυτοσυγκράτηση και οι κοινωνικοί κανόνες δεν επαρκούν για τη διατήρηση του πολιτικού λόγου.

Χωρίς τους επόπτες, ένα forum θα είχε αρκετά συχνά διαμάχες, απρεπές περιεχόμενο, τοξικό περιβάλλον, ασεβή σχόλια τα οποία θα κατέστρεφαν την φήμη του ίδιου. Ουσιαστικά, οι επόπτες είναι αυτοί που ρυθμίζουν και επιβλέπουν το περιεχόμενο που ανεβαίνει στο forum από τους χρήστες και φροντίζουν για την εύρυθμη λειτουργία του. Ένα forum ή μια ομάδα χωρίς κανόνες, χωρίς εποπτεία, είναι καταδικασμένο στην αποτυχία.

Κλείνοντας αυτή την ενότητα, γίνεται κατανοητό πως η επιτυχία ενός forum εξαρτάται από την οργάνωσή του. Είναι πολύ σημαντικό, οι δημιουργοί κάθε forum να αφιερώσουν ένα εύλογο χρονικό διάστημα, έτσι ώστε να επιλέξουν τα κατάλληλα άτομα που θα θέσουν ως επόπτες. Επιπλέον, αξίζει να σημειωθεί ότι ο συγγραφέας της παρούσης εργασίας είχε διατελέσει ως ανώτερος επόπτης για την εφαμοργή Blitz (https://blitz.gg/) του παιχνιδιού League of Legends στο Discord, όπου και διαπιστώθηκε πόσο υπεύθυνη και απαιτητική ήταν η εργασία ενός επόπτη αλλά και η αναγκαιότητα της ύπαρξής της .

3.4 Τι είναι εποπτεία και επόπτης

Όπως αναφέρθηκε και πιο πάνω η εποπτεία είναι αναγκαία για τα online forums διότι η αυτοσυγκράτηση δεν επαρκεί **[Πηγή 1 Κεφ3]**. Για αυτό τον λόγο υπάρχουν οι επόπτες σε κάθε σοβαρό forum. Ο ρόλος τους είναι σπουδαίος και δεν έχουν πρόθεση να φιμώσουν τους χρήστες του διαδικτύου ή να περιορίσουν τα δικαιώματα των ανθρώπων. Ουσιαστικά, ο στόχος τους είναι να διατηρούν την ομαλή λειτουργία του forum, εφαρμόζοντας τους όρους της κοινότητας και να τηρούν αυτά που πρεσβεύει το ίδιο.

Αν για παράδειγμα ένας χρήστης επισκεφτεί ένα κακής ποιότητας forum, στο οποίο αντικρίσει βωμολοχίες, άσχημες εικόνες ή ακόμη και απειλές μεταξύ των μελών τότε θα αναπτύξει μια λανθασμένη εικόνα για τους επόπτες και κατ΄ επέκταση για το forum. Ωστόσο οι επόπτες, εκτός της βασικής αρμοδιότητάς τους, έχουν την δυνατότητα να συμμετέχουν σε διάφορες συζητήσεις. Όμως τους δίνεται και το δικαίωμα να παρέμβουν όταν και όπου χρειαστεί.

3.5 Διαχειριστής

Ένας άλλος ρόλος που θα συναντάται σε ένα forum είναι αυτός του Διαχειριστή. Ο Διαχειριστής είναι ο άνθρωπος που ανέπτυξε το forum, επομένως είναι και ο ιδιοκτήτης αυτού. Ο ρόλος του είναι ανώτερος των εποπτών και είναι αυτός που θα αποφασίσει πότε είναι η κατάλληλη στιγμή για να επιλέξει και να αναθέσει νέους επόπτες, στην περίπτωση που οι συνθήκες το απαιτούν. Επιπλέον, είναι υπεύθυνος για τους κανόνες λειτουργίας του forum, καθώς και για τις διάφορες θεματολογίες των συζητήσεων εντός του forum.

Επίσης, είναι υπεύθυνος για τις εξωτερικές σχέσεις του forum, για παράδειγμα αν κάποιος επιθυμεί να διαφημίσει ένα προϊόν τότε θα πρέπει να απευθυνθεί στον διαχειριστή ή αν θέλει να οργανώσει κάποιο event, με το οποίο συμφωνεί και ο διαχειριστής, τότε ο τελευταίος είναι ο υπεύθυνος για την προώθηση του. Επιπλέον, ο διαχειριστής είναι το άτομο που φροντίζει και για τα μέλη που ανήκουν στο forum. Για παράδειγμα, στην περίπτωση που κάποιο μέλος του forum έχει κάποιο πρόβλημα με έναν από τους επόπτες ή με κάποιο άλλο μέλος του forum, τότε απευθύνεται στον διαχειριστή ώστε να αναλάβει την διευθέτηση του θέματος.

Συμπερασματικά όλων των παραπάνω, ο διαχειριστής ενός forum είναι ο ιδιοκτήτης αυτού. Χάρη στον ίδιο, το forum αποκτά χαρακτήρα, αφού αυτός είναι που καθορίζει την θεματολογία καθώς και τους κανόνες αυτού. Επιπλέον, αναλαμβάνει την πρωτοβουλία να επιλέξει και να αναθέσει τους κατάλληλους ανθρώπους ως ¨επόπτες¨, δίνοντάς τους οδηγίες για την συμπεριφορά και το ύφος που πρέπει να τηρείται. Ο ρόλος του βέβαια, επεκτείνεται και αφορά την ευχαρίστηση των μελών που το απαρτίζουν, λύνοντας προβλήματα που ίσως έχουν αναπτυχθεί μεταξύ των χρηστών με τους επόπτες. Αξίζει να σημειωθεί πως ένα forum δεν είναι απαραίτητο να απαρτίζεται από έναν και μόνο διαχειριστή αλλά μπορεί να αποτελείται από ένα πλήθος αυτών.

3.5.1 Διαφορές διαχειριστή-επόπτη

Βάσει των παραπάνω, γίνεται αντιληπτό ότι ο ρόλος του διαχειριστή διαφέρει από τον ρόλο του επόπτη. Υπάρχουν αρκετές διαφορές ανάμεσα στις δύο αυτές έννοιες, οι οποίες θα επισημανθούν σε αυτή την υπο-ενότητα.

Ο ρόλος του επόπτη είναι να ελέγχει τα μέλη του forum για το αν εφαρμόζουν τους κανόνες λειτουργίας. Επίσης, ελέγχει όλες τις συζητήσεις, διαλόγους, σε όλους τους τομείς διεξοδικά και πρέπει να είναι σε θέση να εντοπίζει παραπτώματα, διαφωνίες, απρεπείς συμπεριφορές μεταξύ των μελών. Ο διαχειριστής, έχει μεν την δικαιοδοσία να πράξει τον ρόλο του επόπτη μεταξύ των χρηστών και των εποπτών, αλλά αυτό είναι κάτι που επιλέγεται σε σπάνιες περιπτώσεις. Ο ρόλος του διαχειριστή είναι να θέτει τους κανόνες και να επεμβαίνει στα προβλήματα που προκύπτουν μεταξύ των χρηστών με τους επόπτες.

Βέβαια, κατά την ανάπτυξη ενός forum ο διαχειριστής ή οι διαχειριστές είναι αναγκασμένοι να διαπράξουν τον ρόλο του επόπτη έως οι ίδιοι αποφασίσουν τους κατάλληλους ανθρώπους για αυτό. Εκτός των διαφορών μεταξύ των διαχειριστών και των εποπτών υπάρχει ένας κοινός στόχος που χαρακτηρίζει και τους δύο ρόλους. Αυτός είναι η εύρυθμη λειτουργία του forum.

3.5.2 Αλληλοσυνεργασία

Ένα από τα σημαντικότερα ¨συστατικά¨, προκειμένου να επιτευχθούν οι στόχοι που έχουν τεθεί σε ένα forum, είναι η αναγκαία ύπαρξη της αλληλοσυνεργασίας μεταξύ των εποπτών και των διαχειριστών. Για παράδειγμα, οι επόπτες πρέπει να είναι σε θέση να ενημερώνουν τους διαχειριστές για τυχόν προβλήματα που μπορεί να προκύψουν, να γίνεται ανάλυση, επεξεργασία του προβλήματος και τέλος να εξάγεται ένα τελικό πόρισμα. Έπειτα, πρέπει να δημιουργείται σχέδιο με τρόπους αντιμετώπισης, για την αποφυγή παρόμοιου μελλοντικού προβλήματος.

Επίσης, οι επόπτες συλλέγουν σχόλια (ή ανατροφοδότηση) (αγγλικά: feedback). Το feedback περιέχει την γνώμη των χρηστών για το forum όπου οι επόπτες σε συνεργασία με

τους διαχειριστές συζητάνε για το κατά πόσο τα μέλη του forum είναι ικανοποιημένα από το περιβάλλον, τους κανόνες και για το γενικότερο κλίμα που επικρατεί ανάμεσα στους χρήστες. Η συνεχής συζήτηση των απόψεων των χρηστών για το forum, θα οδηγήσει στο να ληφθούν αποφάσεις που θα επιφέρουν την βελτίωση του ίδιου.

3.6 Θέσπιση ομάδας εποπτών

Η θέσπιση ομάδας εποπτών είναι μία αρκετά απαιτητική και χρονοβόρα διαδικασία που έχει να διεκπεραιώσει ο διαχειριστής κάθε forum **[Πηγή4 Κεφ3]**. Εφόσον το πλήθος των χρηστών του forum αυξάνεται, έχει σαν αποτέλεσμα οι καταστάσεις και συνθήκες να απαιτούν την εποπτεία. Έτσι, ο διαχειριστής πρέπει να αναλάβει αυτό το δύσκολο έργο.

Υπάρχουν αρκετοί τρόποι ώστε να "προσλάβει", ο διαχειριστής, τους επόπτες άλλα λίγοι από αυτούς είναι αποτελεσματικοί. Πρόκειται, πραγματικά για μία διαδικασία που απαιτεί λεπτό χειρισμό, αλλά αν γίνει με τον σωστό τρόπο τότε τα οφέλη θα είναι ορατά. Επιπλέον, ο λόγος για τον οποίο απαιτείται λεπτός χειρισμός είναι διότι πρέπει να τεθούν οι κατάλληλοι χρήστες, ως επόπτες, οι οποίοι είναι ικανοί να διατηρήσουν την εύρυθμη λειτουργία του forum.

Οι κυριότεροι λόγοι για τους οποίους είναι σημαντικό να αναζητηθούν και να τεθούν επόπτες σε ένα forum είναι:

- Λόγω αύξησης της επισκεψιμότητας. Ο ολοένα και αυξανόμενος αριθμός των χρηστών που συμμετέχουν σε ένα forum έχει ως αποτέλεσμα να διεξάγονται ταυτόχρονα συζητήσεις, κάτι το οποίο σημαίνει αύξηση της αλληλεπίδρασης μεταξύ των χρηστών. Επομένως είναι αναγκαίο να τεθεί εποπτεία έτσι ώστε να ελέγχεται το περιεχόμενο που αναρτάται.

- Για κάλυψη όλων των ωρών και των ημερών. Θέτοντας ένα πλήθος εποπτών, δίνεται η δυνατότητα να ελέγχεται το περιεχόμενο των αναρτήσεων εικοσιτέσσερις ώρες το εικοσιτετράωρο και εφτά μέρες την εβδομάδα.

- Προκειμένου να επιτευχθεί το προηγούμενο, είναι αναγκαίο το πλήθος των εποπτών να διαμοιραστεί σε βάρδιες έτσι ώστε ο φόρτος εργασίας να κατανέμεται ανάμεσα στους επόπτες.

Ένας από τους αποτελεσματικούς τρόπους εύρεσης εποπτών για ένα forum είναι να ανακοινωθεί στο διαδίκτυο από τους ίδιους τους διαχειριστές η ανάγκη για εποπτεία ενός forum. Μέσω αυτής της ¨αγγελίας¨ οι ενδιαφερόμενοι θα συμπληρώνουν ένα google form, το οποίο έχει συνταχθεί από τους διαχειριστές. Αυτή η ανακοίνωση μπορεί να πραγματοποιηθεί εντός του forum, έτσι ώστε οι ίδιοι ο χρήστες του να εκδηλώσουν ενδιαφέρον για να γίνουν επόπτες αυτού **[Πηγή4 Κεφ3]**. Χρησιμοποιώντας αυτή την μέθοδο, οι διαχειριστές θα είναι σε θέση να επιλέξουν τους κατάλληλους επόπτες μέσω ερωτήσεων που έθεσαν οι ίδιοι. Εν συνεχεία, βάσει των απαντήσεων που έχουν λάβει θα ορίσουν τους κατάλληλους επόπτες του forum. Μερικές από τις ερωτήσεις που θα μπορούσαν να θέσουν οι διαχειριστές, ως προς τους χρήστες, έτσι ώστε αυτοί να γίνουν επόπτες είναι οι παρακάτω:

1) Ποιά είναι η εμπειρία σας με την εποπτεία;

2) Πότε γίνατε μέλος στο forum;

3) Πιστεύετε ότι είστε ο κατάλληλος και αν ναι γιατί;

4) Σε ποιους τομείς υπερτερείτε;

5) Ποιές είναι οι αδυναμίες σας;

6) Σε ποια περιοχή είστε και σε ποια ζώνη ώρας;

7) Ποιες ώρες μπορείτε να είστε διαθέσιμος;

8) Πως θα διαχειριζόσασταν μια διαφωνία μεταξύ 2 ή περισσότερων ατόμων;

9)Τι θα κάνατε αν ένα μέλος του forum διαφωνούσε με την απόφασή σας;

Παρακάτω αναλύεται ο σκοπός κάθε ερώτησης που αναφέρθηκε:

1) Προφανώς και οι διαχειριστές θα πρέπει να είναι σε θέση να μάθουν αν υπάρχει αρκετή σχετική εμπειρία. Όπως γίνεται κατανοητό, όσο περισσότερο χρονικό διάστημα ο ενδιαφερόμενος ήταν επόπτης ενός forum στο παρελθόν τόσο καλύτερα θα γνωρίζει τις αρμοδιότητές του. Επίσης είναι σκόπιμο, σε αυτή την ερώτηση, να ερωτηθεί σε ποιο forum συμμετείχε πριν, στην περίπτωση που υπάρχει προηγούμενη εμπειρία. Έτσι οι διαχειριστές θα κατατοπιστούν σε μεγάλο βαθμό, για τις δυνατότητές του.

2) Πρέπει να υπάρχει εικόνα του πότε έγινε μέλος το συγκεκριμένο άτομο. Αν για παράδειγμα, η εγγραφή του πραγματοποιήθηκε μερικές ώρες πριν και επιθυμεί να γίνει επόπτης τότε είναι πιθανό αυτό το άτομο να μην είναι και το πιο αξιόπιστο και ίσως να θέλει ακόμη και να αποδυναμώσει το forum.

3) Αυτή η ερώτηση είναι αρκετά δύσκολη και αρκετά εύστοχη. Μέσω αυτής, οι διαχειριστές θα λάβουν μία εικόνα για τον χαρακτήρα του ενδιαφερόμενου και με βάση αυτή θα κριθεί, σε μεγάλο βαθμό. Ουσιαστικά, ο στόχος είναι να λάβουν μία αυτοκριτική του ίδιου. Αν για παράδειγμα, ο ενδιαφερόμενος απαντήσει “Δίνω βάση στη λεπτομέρεια ώστε να είμαι έτοιμος ανά πάσα στιγμή να βοηθήσω το κλίμα του forum να είναι υγιές”, τότε αυτός δίνει την εντύπωση ότι επιθυμεί να προσφέρει. Αν πάλι για παράδειγμα δώσει την απάντηση “Είμαι καλύτερος από τους άλλους”, αυτό θα φανέρωνε έναν αλαζονικό χαρακτήρα όπου καλό θα ήταν να μην επιλεχθεί τα συγκεκριμένο άτομο.

4) Από τις πιο βασικές ερωτήσεις, μέσω της οποίας αναδύονται τα χαρακτηριστικά του ατόμου και το πώς θα επιδράσουν με τους υπόλοιπους επόπτες αλλά και με τους χρήστες του forum. Οι διαχειριστές έχουν ως στόχο να αναζητήσουν κυρίως άτομα με υπομονή, κατανόηση, οργανωτικά, που μπορούν να λειτουργούν σε μια ομάδα, να επιβληθούν και να επιβάλουν τάξη.

5) Ακόμα μια βασική ερώτηση που μας δείχνει αν το άτομο είναι αρκετά ώριμο, έχει αυτογνωσία και θέλει να μάθει περισσότερα ώστε να μετριάσει ή ακόμα και να εξαλείψει τις αδυναμίες του. Ουσιαστικά, αυτή η ερώτηση αποτελεί συνέχεια της ερώτησης 3 (κατά σειράς) έτσι ώστε οι διαχειριστές να λάβουν μία επιπλέον εικόνα του ενδιαφερόμενου.

6) Είναι σίγουρο ότι πρέπει να υπάρχει γνώση της περιοχής από όπου βρίσκεται το άτομο και σε ποια ώρα ζώνης ανήκει. Αυτό θα βοηθήσει αρκετά τους διαχειριστές, έτσι ώστε σε περίπτωση επιλογής του ενδιαφερόμενου να γνωρίζουν τις πρωινές και βραδινές ώρες.

7) Αυτή η ερώτηση σε συνδυασμό με την προηγούμενη, είναι βασικές ως προς την οργάνωση του forum. Με αυτόν τον τρόπο οι διαχειριστές θα είναι σε θέση να θέσουν τους επόπτες, με βάση την χρονική ευχέρεια του καθενός.

8) Οι διαφωνίες είναι ένα αρκετά συχνό φαινόμενο τόσο στην καθημερινή ζωή όσο και στα forum. Επομένως αυτή η ερώτηση είναι αρκετά εύστοχη ώστε οι διαχειριστές να αντιληφθούν τον τρόπο αντιμετώπισης μιας διαφωνίας, από την πλευρά των εποπτών, καθώς και την μέθοδο με την οποία το επιτυγχάνουν. Για παράδειγμα, μία πιθανή απάντηση από την πλευρά των ενδιαφερόμενων, θα ήταν η παρότρυνση των μελών που διαφωνούν έντονα μεταξύ τους να συνεχίσουν την διαφωνία σε προσωπικά μηνύματα, στην περίπτωση που το forum δίνει αυτή την δυνατότητα. Αν πάλι από την άλλη δεν υπάρχει δυνατότητα προσωπικής επικοινωνίας, μέσω του forum, τότε ο επόπτης θα πρέπει να καθησυχάσει τα μέλη του forum και στην περίπτωση που δεν συμμορφωθούν να τους απαγορεύσει την ανάρτηση των απόψεών τους. Επιπλέον, είναι σημαντικό οι επόπτες να δρουν, βάσει των υποκειμενικών κριτηρίων του forum, που στόχο έχουν την επαναφορά της εύρυθμης λειτουργίας του forum και να μην προσπαθούν να υποστηρίξουν κάποιο μέλος βασισμένοι στις δικές τους πεποιθήσεις.

9) Σε αυτή την ερώτηση, οι διαχειριστές θέλουν να αντιληφθούν τον τρόπο διαχείρισης των εποπτών στην περίπτωση που οι χρήστες δεν σεβαστούν την απόφασή τους. Αρχικά, πρέπει ο επόπτης να είναι σε θέση να εξηγήσει αναλυτικά γιατί πάρθηκε μία συγκεκριμένη απόφαση ώστε να μην υπάρχουν δυσνόητα σημεία. Αν ακόμα ο χρήστης συνεχίσει να

διαφωνεί τότε μπορεί να του επιβληθούν κυρώσεις, όπως να μην μπορεί να δημοσιεύσει ξανά στο forum για ένα χρονικό διάστημα.

Ένας άλλος τρόπος εύρεσης εποπτών σε ένα forum είναι μιλώντας απευθείας στα μέλη του φόρουμ που είναι πολύ ενεργά. Έτσι, μπορεί να γίνουν ιδανικοί υποψήφιοι για να βοηθήσουν στην εποπτεία του forum. Μιλώντας μαζί τους οι διαχειριστές μπορούν να καταλάβουν τις σκέψεις τους για την κοινότητα, τι πραγματικά μπορεί να βελτιώσει το forum και γενικότερα τον τρόπο με τον οποίο μπορούν να βοηθήσουν.

Ανεξάρτητα από τον τρόπο που θα επιλεχθούν οι επόπτες, πρέπει να κοιτάξουμε το ιστορικό συζητήσεων του συγκεκριμένου ατόμου, έτσι ώστε να διαπιστωθεί η έντονη δραστηριότητά του. Επίσης, είναι ανεκτό οι διαχειριστές να επιλέξουν κάποιον ενδιαφερόμενο με ελάχιστη ή ακόμη και ανύπαρκτη εμπειρία εφόσον όμως διαθέτουν έμπειρους επόπτες, που θα τον καθοδηγήσουν.

3.6.1 Χαρακτηριστικά

Αν κάποιος ενδιαφερόμενος επιθυμεί να γίνει επόπτης σε ένα φόρουμ πρέπει να αναλογιστεί προσεκτικά κάποιες παραμέτρους. Για παράδειγμα, αν η φύση του φόρουμ είναι τέτοια που έρχεται αντιμέτωπη με τα πιστεύω του ή τις πεποιθήσεις του, τότε για να αποφύγει τις συγκρούσεις δεν θα πρέπει να επιλέξει το συγκεκριμένο. Η εποπτεία απαιτεί αρκετό χρόνο, έτσι αν ο ενδιαφερόμενος δεν διαθέτει αρκετό χρόνο τότε δεν υπάρχει λόγος να προορίζει τον εαυτό του σε κάτι τέτοιο. Οι επόπτες πρέπει να σκέφτονται, βάσει των υποκειμενικών κριτηρίων του forum, τις καταστάσεις που έρχονται αντιμέτωποι, καθώς και τους στόχους και τις πολιτικές του φόρουμ που εφαρμόζει το ίδιο.

Οι επόπτες είναι υπεύθυνοι για τον τόνο και την συμπεριφορά τους απέναντι στην κοινότητα. Επίσης, αυτοί είναι μια ομάδα και πρέπει να υπάρχει εσωτερική οργάνωση και επικοινωνία για την καλύτερη λειτουργία τους. Όπως επίσης και εμπιστοσύνη μεταξύ τους και σεβασμός στην κάθε γνώμη. Το πιο αποτελεσματικό εργαλείο των εποπτών είναι ο

αυτοέλεγχος αλλά και ο έλεγχος μεταξύ τους. Οι συντονιστές πρέπει να αιτιολογούν και να εξηγούν τον τρόπο με τον οποίο εποπτεύουν, τους κανόνες και τις πολιτικές τους στην κοινότητα των χρηστών. Είναι σημαντικό και οι χρήστες αλλά και οι επόπτες να αισθάνονται άνετα και να είναι πρόθυμοι να συμμετέχουν στις διάφορες συζητήσεις. Είναι επίσης σημαντικό όλοι να είναι πρόθυμοι να ακούσουν ο ένας τον άλλον, ώστε να μπορούν να βασίζονται στις ιδέες των άλλων. Για να το πετύχουν αυτό, πρέπει να συνεργάζονται αρμονικά.

Εν κατακλείδι, ο επόπτης πρέπει να δρα βάσει των υποκειμενικών κριτηρίων του forum στο οποίο ανήκει και να εκφράζει την γνώμη του μόνο αν υπάρχουν ασαφή σημεία **[Πηγή 5 Κεφ3]**. Επιπλέον, πρέπει να είναι διακριτικός, ευγενικός και εξυπηρετικός ακόμα και αν τα μέλη του φόρουμ είναι ασεβή και αγενή προς τον ίδιο. Επιπρόσθετα, οι επόπτες σε περίπτωση άγνοιας, θα πρέπει να συμβουλεύονται τους διαχειριστές πριν πράξουν κάποια διαδικασία και να αναφέρουν τους λόγους για τους οποίους επέβαλλαν πιθανές κυρώσεις σε έναν χρήστη.

3.6.2 Προβλήματα και αντιμετώπιση

Πολλά είναι τα προβλήματα που μπορεί να προκύψουν ανάμεσα στο προσωπικό (διαχειριστές και επόπτες). Οι μεγάλες ομάδες εποπτών είναι πολύ πιθανό να απορροφήσουν μη ενεργούς επόπτες. Σε αυτή την περίπτωση ο διαχειριστής πρέπει να μιλήσει με τον επόπτη ώστε να εντοπίσει το πρόβλημα και να το λύσει. Οι επόπτες δεν πρέπει να εφαρμόζουν προσωπικές προκαταλήψεις στην εποπτεία, αλλά αυτό δεν σημαίνει ότι πρέπει να προσποιούνται ότι όλοι είναι εξίσου ένοχοι εάν συμβεί κάτι. Η άρνηση συμμετοχής σε ένα θέμα που αφορά το φόρουμ μπορεί να είναι ένα ζήτημα γιατί ο κάθε επόπτης είναι ισότιμη φωνή και όλοι πρέπει να εκφράζουν τις απόψεις τους. Δεν πρέπει να αφαιρείται περιεχόμενο/σχόλια αν είναι αντίθετα με τις προσωπικές του απόψεις.

Επίσης, αν κάποιος επόπτης διαφωνεί με μια απόφαση του διαχειριστή και δεν υπάρχει δυνατότητα μέσης οδού, τότε είναι προτιμότερο ο επόπτης να εγκαταλείψει την ομάδα. Αν οι περισσότεροι επόπτες διαφωνούν με μια απόφαση του διαχειριστή και τα

επιχειρήματά τους είναι ισχυρά, τότε ο διαχειριστής θα πρέπει να βρει μόνος του ή με την βοήθεια των εποπτών άλλη λύση που να ικανοποιεί όλες τις πλευρές. Σε μια συζήτηση για ένα συγκεκριμένο θέμα, ο επόπτης πρέπει να είναι σε θέση να επιβλέπει ώστε η κουβέντα να μην παρεκτραπεί. Αν πάλι όμως το θέμα πάρει άλλες διαστάσεις, τότε ο επόπτης πρέπει εσπευσμένα να επαναφέρει την εύρυθμη λειτουργία του. Η σημασία αυτών των στοιχείων και η πραγμάτωση των στόχων που έχουν τεθεί παίζουν σημαντικό ρόλο για τον καθορισμό ενός γενικότερου συστήματος πλατιάς συμμετοχής.

3.7 Τρόποι διασφάλισης ομαλής λειτουργίας forum

Για να λειτουργήσει σωστά ένα forum υπάρχουν κάποιοι τρόποι. Όταν εφαρμοστούν αυτοί οι τρόποι τότε το forum θα μπορέσει να "αποδώσει" με τους ανθρώπους του. Οι τρόποι με τους οποίους επιτυγχάνεται αυτό είναι με την θέσπιση κανόνων, με την θέσπιση συστήματος παραβίασης κανόνων και την διαφάνεια. Παρακάτω θα αναλυθούν αυτοί οι τρόποι.

3.7.1 Θέσπιση κανόνων

Όπως υπάρχουν κανόνες για την σωστή λειτουργία των ομάδων στην καθημερινή ζωή έτσι πρέπει να υπάρχουν κανόνες και σε ένα φόρουμ. Αφενός για να θέτουν το πλαίσιο για υγιείς συζητήσεις, αφετέρου για να γνωρίζουν οι επόπτες πώς και τι να εποπτεύουν **[Πηγή 3 Κεφ3]**. Η εποπτεία είναι χρονοβόρα, επομένως οι κανόνες πρέπει να είναι απλοί τόσο στη διαχείριση όσο και στην κατανόηση. Οι κανόνες δημιουργούνται από τους διαχειριστές και εφαρμόζονται από τους επόπτες.

Είναι σκόπιμο οι επόπτες να είναι ανοιχτοί στις απόψεις άλλων εποπτών στο φόρουμ και να προσπαθούν να επιτύχουν μια συναίνεση για την καλύτερη λειτουργία. Τα μέλη πρέπει να καθοδηγούνται ως προς την τήρηση των κανόνων και όχι να

υποχρεώνονται να υπακούουν. Τέλος, πρέπει να γίνεται ενημέρωση των μελών στην περίπτωση που υπάρχει αλλαγή των κανόνων.

3.7.2 Θέσπιση συστήματος παραβίασης κανόνων

Εφόσον οι κανόνες έχουν δημιουργηθεί πρέπει να θεσπιστεί και σύστημα επιπτώσεων για τα μέλη που παραβιάζουν τους κανόνες. Αρχικά, η καλύτερη λύση είναι ο διάλογος με το μέλος που παραβίασε κάποιον κανόνα. Έτσι, ο επόπτης θα αντιληφθεί αν το έκανε εσκεμμένα ή ακούσια. Έπειτα, αν μετά τον διάλογο υπάρχει συνέχιση παραβίασης κανόνων, τότε το συγκεκριμένο άτομο θα πρέπει να αποκλειστεί από τη χρήση του φόρουμ. Είναι πρέπον το άτομο να περιοριστεί, ώστε να μην επηρεάσει και τα υπόλοιπα μέλη, την ευημερία του φόρουμ, και γενικότερα το περιβάλλον. Επομένως η θέσπιση κανόνων και επιπτώσεων ενός forum, καθώς επίσης και η συνεχής επιτήρηση βοηθά την ανάπτυξη και την βελτίωσή του.

3.8 Διαφάνεια (transparency)

Σε ένα φόρουμ στο οποίο οι επόπτες παίρνουν αποφάσεις σε πραγματικό χρόνο με βάση την κρίση και τους κανόνες που έχουν θεσπιστεί, τα μέλη θα θέλουν να μάθουν τι συμβαίνει. **[Πηγή 2 Κεφ3]**. Μια λογική απάντηση σε αυτή την δυναμική, είναι να δημιουργηθεί ένας χώρος στον οποίο οι επόπτες και οι διαχειριστές θα συνομιλούν με τους χρήστες για τις ενέργειές τους. Με τον όρο διαφάνεια, νοείται η δημοσίευση τον κανόνων του forum έτσι ώστε οι χρήστες να συμμορφώνονται με αυτούς. Με αυτόν τον τρόπο, στην περίπτωση επιβολής οποιασδήποτε κύρωσης στους ίδιους να αντιστοιχίζεται με τους κανόνες της κοινότητας και να μην αποδίδεται σε προσωπικούς λόγους.

Σε κάθε forum:

Οι επόπτες είναι εκπρόσωποι των μελών του φόρουμ και ενεργούν για το καλό της κοινότητας. Αντιμετωπίζουν όλους τους χρήστες ισότιμα, τεκμηριώνουν τους κανόνες και είναι σε θέση να εξηγήσουν γιατί υπάρχουν. Επιπλέον, προσθέτουν επεξήγηση και χρήσιμες συμβουλές σε καινούργιους ή "συγχυσμένους" χρήστες. Η τήρηση αυτών των αρχών στην ουσία οδηγεί τους χρήστες να κατανοήσουν γιατί οι επόπτες εποπτεύουν με αυτή την πολιτική. Επίσης, οι κανόνες θα πρέπει να είναι πρακτικοί, ξεκάθαροι και να συνάδουν με αυτό που η κοινότητα επιθυμεί συλλογικά.

Όμως οι άνθρωποι γενικά, κάνουν λάθη. Άρα, αν δεν υπάρχει αρκετή αλληλοεπικοινωνία τότε αυτά τα λάθη ερμηνεύονται εύκολα, από τα μέλη, ως κακόβουλη συμπεριφορά. Μερικά μέλη θα είναι δύσπιστα ως προς την ικανότητα του να λαμβάνουν αποφάσεις οι διαχειριστές και οι επόπτες. Η σοβαρή και ουσιαστική επικοινωνία μελών και εποπτών απαιτεί δεξιότητα και υπομονή και αυτά τα χαρακτηριστικά μπορεί να μην είναι σε ικανοποιητικό βαθμό σε όλους τους επόπτες του φόρουμ. Οι ενέργειες ή οι πράξεις που έχουν γίνει με κακή επικοινωνία, ακόμη και αν ήταν καλά μελετημένες μπορεί σε κάποιο βαθμό να κλονίσουν την κοινότητα, πόσο μάλλον αν υπάρχουν ήδη κάποια σημάδια, και να δημιουργήσουν εντάσεις ανάμεσα στους επόπτες.

Γνωρίζοντας τους κινδύνους και το ρίσκο μιας κακής επικοινωνιακής δράσης, προστίθεται άγχος στους επόπτες που αναμένεται να επικοινωνούν περισσότερο μεταξύ τους αλλά και με τους χρήστες του φόρουμ. Έτσι, μια αναμενόμενη αντίδραση σε αυτό, είναι να αποφεύγουν το άγχος, με αποτέλεσμα να μην είναι όσο ενεργοί θα πρέπει να είναι, και στον ίδιο χρόνο, τα μέλη του φόρουμ να ενδιαφέρονται ζητώντας απαντήσεις για τις παρούσες ενέργειες.

Σαφώς υπάρχουν και θετικά: Οι διαχειριστές με την διαφάνεια κοινοποιούν τις προσδοκίες τους στην κοινότητα. Παρατηρείται μείωση του θυμού. Οι συζητήσεις είναι πιο ξεκάθαρες. Οι κανόνες κατανοούνται καλύτερα. Το περιβάλλον είναι πιο υγιές για εποπτεία και υπάρχει περισσότερος σεβασμός στους επόπτες. Τα μέλη του φόρουμ γνωρίζοντας τις προσδοκίες των διαχειριστών είναι σε καλύτερη θέση να αντιληφθούν αν οι προσδοκίες ικανοποιούνται ή όχι.

Συμπερασματικά, όλων των παραπάνω γίνεται αντιληπτό ότι διατηρώντας ένα forum την διαφάνειά του, αποσαφηνίζει ποιές συμπεριφορές είναι αποδεκτές καθώς και το ύφος του. Με αυτό τον τρόπο επεξηγεί πως στην περίπτωση παράβασης των όρων, θα επέλθει παρατήρηση ή ακόμα και απαγόρευση ανάρτησης του χρήστη. Επιπλέον, με την δημοσιοποίηση των όρων της κοινότητας δίνεται η δυνατότητα οι χρήστες να σχολιάζουν και να προτείνουν τρόπους βελτίωσης της κοινότητας. Επομένως, η διαφάνεια ενός forum είναι πολύ σημαντική τόσο για την διατήρησή του όσο και για την εξέλιξή του.

3.9 Εμπιστοσύνη

Η εμπιστοσύνη δεν κερδίζεται, αλλά οικοδομείται. Πόσο μάλλον σε φόρουμ, που δεν υπάρχει πραγματική επαφή με τους ανθρώπους που αλληλεπιδρούν. Άρα, η εμπιστοσύνη πρέπει να δημιουργηθεί ανάμεσα στους επόπτες και στους ανθρώπους. Παρακάτω θα αναλυθούν εις βάθος καθώς και τυχόν προβλήματα αλλά και τρόποι επίλυσης.

3.9.1 Ανάμεσα στους επόπτες

Για την σωστή λειτουργία και συνεργασία των ομάδων είναι προτιμότερο να υπάρχει εμπιστοσύνη μεταξύ των μελών της. Πρέπει να δημιουργηθεί ένα περιβάλλον όπου είναι αποδεκτό ένας επόπτης να κάνει λάθη **[Πηγή 2 Κεφ3].** Εάν οι επόπτες δεν εμπιστεύονται τον τρόπο σκέψης και τις ικανότητες των άλλων εποπτών τότε δεν θα είναι πρόθυμοι να κρατήσουν την διαφάνεια που τα μέλη του φόρουμ επιθυμούν. Σε αυτό τον βαθμό, οι επόπτες πρέπει να είναι σε θέση να συνεργαστούν ώστε να αξιολογήσουν με σοβαρότητα και με την καλύτερη δυνατή κριτική σκέψη τα πιο αμφιλεγόμενα ζητήματα που θα προκύπτουν για να προσδιορίσουν ποια είναι η πιο ασφαλής και βέλτιστη πορεία δράσης που θα ωφελήσει προπάντων την κοινότητα αλλά και τους εαυτούς τους.

Είναι κρίσιμο οι επόπτες να κατανοούν το πόσο σοβαρό είναι ένα πρόβλημα και ότι το επόμενο βήμα στην επίλυσή του ίσως επηρεάσει σε γενικό βαθμό το forum. Έτσι, για να

συνεχίσουν να λειτουργούν με σωστό τρόπο οι διαδικτυακές ομάδες, οι επόπτες πρέπει να έχουν κατανοήσει πλήρως κάθε κανονισμό του forum και κάθε κατάσταση να την αντιμετωπίζουν με προσοχή και σύνεση ώστε να μπορούν να ανταπεξέρχονται στην εκάστοτε δυσκολία, σύμφωνα με τα όσα πρεσβεύει το forum στο οποίο έχουν τεθεί ως υπεύθυνοι.

3.9.2 Ανάμεσα στους ανθρώπους και τους επόπτες

Εφόσον υπάρχει εμπιστοσύνη ανάμεσα στους επόπτες πρέπει να υπάρχει εμπιστοσύνη και ανάμεσα στα μέλη του φόρουμ με τους επόπτες. Πρέπει να παρατηρηθεί από τους διαχειριστές με ποιον τρόπο αλληλεπιδρούν οι επόπτες με τα μέλη του φόρουμ και να γίνει γνωστό τι είδους σχόλια (feedback) λαμβάνει η ομάδα. Με αυτό τον τρόπο οι διαχειριστές, αν το κρίνουν απαραίτητο, θα προβούν στην προσπάθεια να υπάρξει αλληλοβοήθεια μεταξύ των ίδιων και των εποπτών και να διαμοιράζονται ιδέες για τον τρόπο με τον οποίο η ομάδα θα μπορέσει να βελτιωθεί. Αυτά είναι κάποια από τα στοιχεία μιας υγιούς αλληλεπίδρασης μεταξύ διαχειριστών, εποπτών και μελών του φόρουμ.

Κατά την διάρκεια συζητήσεων μεταξύ εποπτών και μελών, υπάρχει πεποίθηση για το ποια είναι η σωστή πορεία δράσης ως προς την βελτίωση του φόρουμ. Πρέπει να παρατηρηθεί αν υπάρχουν ειρωνικά και υποτιμητικά σχόλια από τους επόπτες και τα μέλη της κοινότητας. Αυτά είναι μερικά σημάδια μιας ανθυγιεινής επικοινωνιακής σχέσης και προπάντων έλλειψης εμπιστοσύνης. Ακόμα και αν υπάρχουν διαφωνίες με ορισμένα από τα μέλη, πρέπει να υπάρξει διάλογος για να μπορούν και οι δύο πλευρές να καταλάβουν την σωστή πορεία δράσης.

3.10 Συγκρούσεις και ανοικοδόμηση εμπιστοσύνης

Αρχικά, δεν είναι εφικτή η τέλεια λύση για να μπορεί να υπάρχει εμπιστοσύνη μεταξύ όλων των ανθρώπων που απαρτίζουν το φόρουμ. Αυτές οι σχέσεις είναι ρευστές

και εξελίσσονται καθημερινά. Πρέπει να βρίσκονται λύσεις που έχουν θετικό αντίκτυπο σε όσο το δυνατόν περισσότερα μέλη. Οι επόπτες πρέπει να σχηματίζουν μία εικόνα του πόσο δεκτικά στις ενέργειες και στις αποφάσεις του forum είναι τα μέλη του. Δηλαδή θα πρέπει να είναι σε θέση να γνωρίζουν αν τα μέλη συμφωνούν και προσαρμόζονται στα παραπάνω ή τα απορρίπτουν.

Για την καλύτερη λειτουργία του φόρουμ, τόσο οι διαχειριστές όσο και οι επόπτες, πρέπει να καταλαβαίνουν τον τρόπο σκέψεις και την οπτική γωνία των άλλων μελών της κοινότητας. Δεν είναι λίγες οι φορές που κάποιος συντονιστής θα επαναλάβει τους κανονισμούς και τους όρους σε διαφορετικούς ανθρώπους. Αυτό που πρέπει να παρατηρεί είναι την στάση των μελών, δηλαδή αν αποδέχονται και προσαρμόζονται στους όρους της κοινότητας. Είναι απολύτως λογικό να συμβαίνουν λάθη, από την πλευρά των μελών αλλά όταν γίνονται δεν είναι σωστό να ¨καλύπτονται¨. Πρέπει να επέρχεται μία απόφαση η οποία είτε έχει συμβουλευτικό χαρακτήρα είτε την επιβολή κάποιας κύρωσης στο μέλος. Το βέλτιστο είναι οι επόπτες να κρίνουν την σοβαρότητα του λάθους και να προσπαθήσουν να το διορθώσουν.

Σε αυτό το σημείο είναι σημαντικό να αναφερθεί ότι οι επόπτες και οι διαχειριστές πρέπει να λαμβάνουν σοβαρά υπόψιν τα σχόλια και τις κριτικές των μελών, με σκοπό να εφαρμόσουν κάποια από αυτά στην κοινότητα. Αν πραγματοποιηθεί το προαναφερθέν, οι χρήστες της κοινότητας θα αναγνωρίσουν ότι πράγματι οι επόπτες και οι διαχειριστές ενδιαφέρονται, προσπαθούν, και θέλουν να βελτιώσουν το φόρουμ. Μέσα από αυτό οι απλοί χρήστες του forum έχουν την δυνατότητα να επισημάνουν τις αδυναμίες του forum και να παροτρύνουν τους διαχειριστές να το κάνουν καλύτερο και αξιόπιστο. Με αυτόν τον τρόπο οικοδομείται η εμπιστοσύνη μεταξύ των μελών και του forum.

Από την άλλη πλευρά θα υπάρξουν περιπτώσεις όπου μια ομάδα μελών θα υποστηρίζει πως μια πορεία δράσης των διαχειριστών είναι σωστή ενώ οι επόπτες θα διαφωνούν με αυτό, ή ακόμη και το αντίθετο, επομένως αυτό οδηγεί σε μια αμφιλεγόμενη κατάσταση. Σε αυτές τις περιπτώσεις συμβαίνει μια σύγκρουση προσδοκιών. Στην περίπτωση αυτή οι διαχειριστές πρέπει να δράσουν, παίρνοντας ευέλικτες αποφάσεις που θα συντελούν σε μία μέση λύση έτσι ώστε να ικανοποιούνται και οι χρήστες αλλά και οι

επόπτες. Αυτό όμως πρέπει να επέλθει έπειτα από την εκτίμηση των επιχειρημάτων που θέτει ο κάθε άνθρωπος στο φόρουμ και όχι το πλήθος των ατόμων. Επιπλέον, οι διαχειριστές πρέπει να είναι δεκτικοί στα σχόλια των ατόμων που αποτελούν το forum και να είναι ανοιχτοί σε νέες ιδέες και αλλαγές. Πριν όμως προβούν σε μία αλλαγή, είναι απαραίτητο να είναι προσεκτικοί και να αναλογιστούν τις πιθανές επιπτώσεις αυτών των αλλαγών. Άρα πρέπει πρώτα να σκεφτούν πώς κάθε απόφαση θα επηρεάσει την λειτουργία του φόρουμ άμεσα ή έμμεσα αλλά και μακροπρόθεσμα.

Με βάση τα παραπάνω, συμπεραίνεται ότι η εμπιστοσύνη μεταξύ των μελών ενός forum οικοδομείται μέσω του διαλόγου. Σύμφωνα με αυτό οι διαχειριστές λαμβάνουν αποφάσεις που διατηρούν μία ισορροπία και ικανοποιούν τις προσδοκίες τόσο των χρηστών όσο και των εποπτών. Πριν όμως ληφθεί μία απόφαση που καθορίζει την πορεία του forum θα πρέπει πρώτα να κρίνεται διεξοδικά έτσι ώστε να μην το επηρεάσει αρνητικά. Επιπλέον, είναι αρκετά δύσκολο έως και ακατόρθωτο η κάθε απόφαση των διαχειριστών να ικανοποιεί πλήρως όλους τους χρήστες. Αυτό οδηγεί στην λήψη και εφαρμογή ευέλικτων αποφάσεων που πιθανότατα επαρκούν για όλους τους χρήστες. Η εμπιστοσύνη μπορεί να αποκτηθεί έπειτα από ένα εύλογο χρονικό διάστημα και να χαθεί κάποια στιγμή ακαριαία. Επομένως, οι διαχειριστές πρέπει να φροντίζουν και να διατηρούν μία σχέση εμπιστοσύνης με τα μέλη τους διότι αν κλονιστεί αυτή η εμπιστοσύνη, καθίσταται σχεδόν αδύνατη η ανοικοδόμησή της.

3.11 Εφαρμογή σε επαγγελματικούς τομείς

3.11.1 Human Resources jobs

Human Resources jobs (ελληνικά: Επαγγέλματα Ανθρώπινου Δυναμικού) είναι αυτά τα οποία ασχολούνται με τους ανθρώπους που δημιουργούν το ανθρώπινο δυναμικό σε μια επιχείρηση **[Πηγή 8 Κεφ3**]. Κάποια επαγγέλματα είναι τα εξής: HR Assistant, HR Manager, Recruiter και Recruiting Manager **[Πηγή 9 Κεφ3]**. Τα επαγγέλματα αυτά ασχολούνται με έναν από τους πιο πολύτιμους πόρους, τον άνθρωπο. Άρα, πρέπει να

γίνεται σωστή διαχείριση των ανθρώπων. Με τον όρο διαχείριση νοείται, η ανάπτυξη των ικανοτήτων για την ενίσχυση της ατομικής και οργανωτικής απόδοσης, αύξηση της καινοτομίας, της δημιουργικότητας και της ευελιξίας που απαιτούνται για την ενίσχυση της ανταγωνιστικότητας. Επιπλέον, τα παραπάνω επιτυγχάνονται μέσω της επικοινωνίας με τους ανθρώπους για την επίλυση προβλημάτων ώστε να υπάρχει εξάλειψη πιθανών προβλημάτων**[Πηγή 10Κεφ3]** .

Για αυτές τις εργασίες, πρέπει να υπάρχει ευφυΐα και γενικά νοητική δύναμη, ακεραιότητα χαρακτήρα και υπευθυνότητα. Εν κατακλείδι, αν κάποιος επιθυμεί να ασχοληθεί επαγγελματικά, θα πρέπει να πληρεί τις παραπάνω προϋποθέσεις και να είναι αρκετά επικοινωνιακός έτσι ώστε να φτάσει ή ακόμη και να ξεπεράσει τις απαιτήσεις και τις προσδοκίες που του έχουν τεθεί από τους προϊσταμένους.

3.11.2 Επόπτης προσωπικού

Η εποπτεία του προσωπικού είναι αρκετά δύσκολη και απαιτητική, όπως και σε ένα φόρουμ. Ο επόπτης ουσιαστικά πρέπει να εποπτεύει τους ανθρώπους στην ομάδα που του έχει ορίσει ο προϊστάμενος έτσι ώστε να είναι σε θέση να λύνει τα προβλήματα που μπορεί να προκύψουν και να ελέγχει αν οι εργασίες εκτελούνται σύμφωνα με τις εντολές που έχουν τεθεί **(Πηγή 6 Κεφ3)**. Με την ίδια λογική του φόρουμ, έτσι και εδώ ο επόπτης πρέπει να καθοδηγεί και να συμβουλεύει τους εργαζόμενους για να είναι πιο αποδοτικοί και να βελτιώνουν το έργο τους **(Πηγή 7 Κεφ3)** .

Επίσης, πρέπει να δημιουργούν ένα ιδανικό και υγιές περιβάλλον με τους υπαλλήλους τους. Δεν πρέπει να διατάζει, αλλά να συνεργάζεται και να εμπνέει τους εργαζόμενους, όμως πρέπει να ενεργεί έχοντας στον νου την πολιτική και τους κανόνες της εκάστοτε επιχείρησης. Με λίγα λόγια, με τον όρο εποπτεία νοείται ο χειρισμός του ανθρώπινου δυναμικού **(Πηγή 11 Κεφ3)**. Η επιμέλεια της οργάνωσης και προπάντων η ενδυνάμωση και η επέκταση των σχέσεων αποτελούν μια πολύ σημαντική βάση για ένα δυναμικό σύστημα που θα είναι ικανό να αντιμετωπίσει κάθε πρόκληση που θα επέλθει.

Κεφάλαιο 4ο: Σκοτεινό Διαδίκτυο (Dark Web)

Αυτό το κεφάλαιο της εργασίας είναι αφιερωμένο στο Dark Web (σκοτεινό διαδίκτυο). Συγκεκριμένα θα δοθεί η ερμηνεία σχετικά με το τι είναι το Dark Web, ποιες είναι οι διαφορές του με το Deep Web καθώς επίσης θα αναφερθούν τα πλεονεκτήματα και μειονεκτήματά του. Επιπλέον, επεξηγεί κατά πόσον είναι εύκολη η πρόσβαση στο Dark Web, πως μπορεί να έχει κάποιος πρόσβαση σε αυτό και τι απαιτείται. Φυσικά θα αναφερθούν το εύρος της αναζήτησης στο Dark Web καθώς και αν είναι αποτελεσματική και αποδοτική η αναζήτηση σε αυτό.

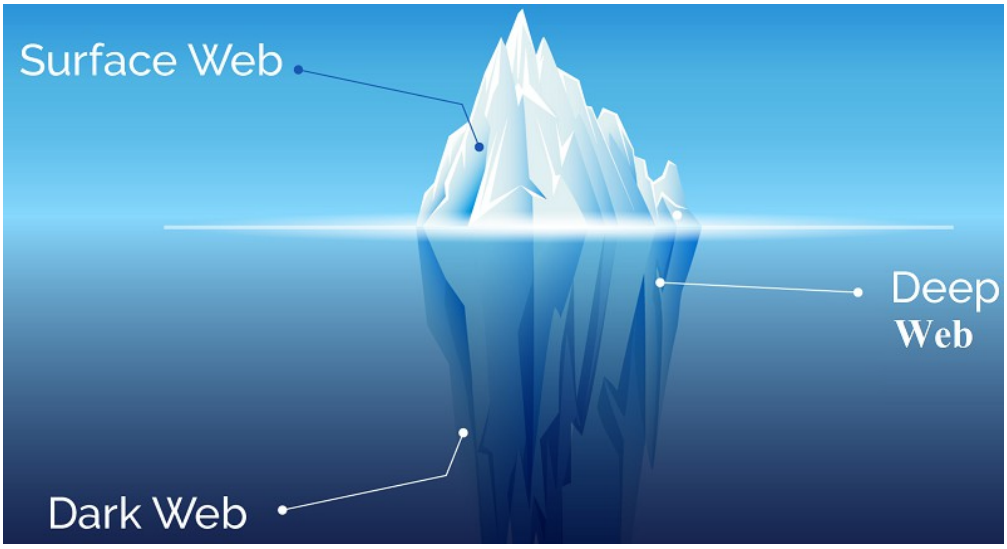
Επίσης, στο επίπεδο των χρηματικών συναλλαγών, θα περιγραφεί η ασφάλεια αυτών καθώς και τι νόμισμα χρησιμοποιείται. Στο τομέα της ασφάλειας θα δοθεί επεξήγηση σχετικά με την ασφάλεια του χρήστη κατά την πλοήγησή του στο Dark Web και αν ενέχουν κίνδυνοι για διαρροή προσωπικών δεδομένων. Βέβαια δεν θα παραληφθεί η αναφορά σε περιπτώσεις που το Dark Web έχει χρησιμοποιηθεί από αρχές και κυβερνήσεις διεθνώς, για την εξακρίβωση ή την ανακάλυψη εγκληματικών πράξεων. Ολοκληρώνοντας, θα περιγραφούν οι λόγοι οι οποίοι το κάνουν να ξεχωρίζει καθώς και η προοπτική του για το μέλλον.

4.1 Dark Web και Deep Web

Είναι σημαντικό να αναφερθούν οι περιγραφές των Dark Web και Deep Web, έτσι ώστε να υπάρχει αποσαφήνιση των όρων. Για αυτόν τον λόγο παρακάτω, θα δοθούν οι ερμηνείες του Dark Web και Deep Web καθώς επίσης θα αναφερθούν και οι διαφορές τους.

4.1.1 Τι είναι Deep Web

Συνήθως, όταν αναφερόμαστε στον όρο Internet (διαδίκτυο) αντιλαμβανόμαστε το Surface Web (επιφανειακός ιστός). Το Surface Web είναι το μέρος του διαδικτύου, το οποίο είναι προσβάσιμο από όλους τους γνωστούς και κοινούς Browser (φυλλομετρητές), όπως είναι το Google Chrome, Mozilla Firefox και ο Microsoft Edge καθώς επίσης το περιεχόμενό του είναι ανιχνεύσιμο από τις γνωστές και κοινές μηχανές αναζήτησης, όπως το Google, το Bing και άλλες. Συνοπτικά, το Surface Web περιέχει ιστοσελίδες που έχουν ευρετηριαστεί, κάνοντάς τες ανιχνεύσιμες από κοινούς Browser και μηχανές αναζήτησης που διαθέτουν τα ευρετήρια αυτών. Επίσης, αναφέρεται πως το Surface Web αποτελεί συνολικά μόλις το 5% του παγκόσμιου ιστού, ενώ όλο το υπόλοιπο αντιπροσωπεύεται από το Dark Web και Deep Web [**Πηγή 1 Κεφ 4**]. Για να γίνει κατανοητό το προαναφερθέν, παρακάτω παρουσιάζεται μία εικόνα η οποία απεικονίζει ένα παγόβουνο.



Εικόνα 2: Παρομοίωση παγόβουνου με Surface, Deep και Dark Web
Πηγή:https://www.kratikal.com/blog/surface-web-and-dark-web-exploring-layers-of-web/

Γνωρίζοντας ότι το εμφανές σημείο ενός παγόβουνου αντιστοιχεί στο 5% με 10% του συνολικού του όγκου, έτσι και στην περίπτωση του διαδικτύου, μόλις το 5% του συνόλου του είναι εμφανές σε όλους.

Σε αντίθεση με το Surface Web, το Deep Web αποτελεί το μέρος του Internet που δεν είναι ορατό και προσβάσιμο σε όλους. Ειδικότερα, κανένας δεν μπορεί να έχει πρόσβαση με την χρήση κάποιας μηχανής αναζήτησης, όπως το Google, σε συγκεκριμένες

πληροφορίες και περιεχόμενο εκτός από πιστοποιημένους χρήστες. Για παράδειγμα, το περιεχόμενο του προσωπικού λογαριασμού E-Mail (ηλεκτρονικό ταχυδρομείο) κάθε ανθρώπου αποτελεί κομμάτι του Deep Web. Προκειμένου να έχει πρόσβαση κάποιος στα εισερχόμενα και εξερχόμενα μηνύματα ή ακόμη και πληροφορίες σχετικά με τις ρυθμίσεις του λογαριασμού του θα πρέπει πρώτα να πιστοποιηθεί, με την χρήση Username (όνομα χρήστη) και Password (κωδικού πρόσβασης). Ένα άλλο παράδειγμα του Deep Web, είναι ο προσωπικός ηλεκτρονικός λογαριασμός (όπως e-banking), όπου για να επιτραπεί η είσοδος ενός χρήστη σε κάποιον λογαριασμό πρέπει να ακολουθήσει μία σειρά από διαδικασίες πιστοποίησης.

Επιπλέον, στην διάσημη πλατφόρμα αναπαραγωγής οπτικοακουστικού υλικού, YouTube, δίνεται η δυνατότητα στους χρήστες να ανεβάσουν υλικό το οποίο μπορούν να το δηλώσουν ¨ως μη καταχωρημένο¨. Με αυτό το χαρακτηριστικό δεν είναι εφικτή η εύρεση του από όλους τους χρήστες. Προκειμένου όμως, να πραγματοποιηθεί η αναπαραγωγή αυτού γίνεται αποκλειστικά με την χρήση ενός συνδέσμου, ο οποίος διακινείται μεταξύ των χρηστών. Είναι σημαντικό να τονισθεί ότι ακόμη και αυτό ανήκει στην κατηγορία του Deep Web. Επιπρόσθετα είναι σημαντικό να αναφερθεί ότι το Deep Web δεν παρέχει στους χρήστες του κάποια επιπλέον ανωνυμία, σε σύγκριση με το Surface Web.

Συνοψίζοντας όλα τα παραπάνω, προκύπτει ότι το Deep Web είναι ένα κομμάτι του Internet το οποίο δεν είναι ορατό και προσβάσιμο σε όλους, παρά μόνο σε μεμονωμένους ή/και πιστοποιημένους χρήστες.

4.1.2 Τι είναι Dark Web

Το Dark Web αποτελεί μέρος του διαδικτύου και ένα μικρό τμήμα του Deep Web. Φημολογείται ότι ο λόγος δημιουργίας του ήταν η ανώνυμη επικοινωνία καθώς επίσης και ο διαμοιρασμός αρχείων, σε επίπεδο διαδικτύου [**Πηγή 2 Κεφ4**]. Στο Dark Web περιέχονται ιστότοποι οι οποίοι δεν έχουν ευρετηριαστεί κάνοντας ανέφικτη την

πρόσβασή τους από κοινές μηχανές αναζήτησης. Προκειμένου να επιτευχθεί η πρόσβαση σε ιστοσελίδες που ανήκουν στο Dark Web θα πρέπει να χρησιμοποιηθούν αντίστοιχα προγράμματα, επειδή όλα τα δεδομένα που περιέχονται σε αυτό είναι κρυπτογραφημένα. Για αυτό τον λόγο το Dark Web αποκαλείται και ως κρυφό διαδίκτυο διότι δεν είναι εμφανές το περιεχόμενό του από τις παραδοσιακές μηχανές αναζήτησης.
Επιπλέον, το Dark Web χρησιμοποιείται για διάφορες παράνομες και μη δραστηριότητες, που θα αναφερθούν στις επόμενες ενότητες. Αυτό το χαρακτηριστικό προσελκύει χρήστες που δεν θέλουν να προβούν, απαραίτητα, σε μία ποινικά κολάσιμη πράξη.

4.1.3 Διαφορές μεταξύ Dark Web και Deep Web

Το Deep Web χρησιμοποιείται για νόμιμους σκοπούς και υιοθετεί την αυθεντικοποίηση για την πρόσβαση ενός χρήστη σε προσωπικές πληροφορίες, οι οποίες είναι κρυπτογραφημένες και δεν παρουσιάζονται στα ευρετήρια των κοινών προγραμμάτων περιήγησης και μηχανών αναζήτησης. Επιπλέον, εμφανίζεται κυρίως σε νόμιμες δραστηριότητες όπου, όπως προαναφέρθηκε, είναι το προσωπικό e-banking, ιστότοποι παροχής υπηρεσιών, όπως το Netflix και το email. Αντίθετα το Dark Web χρησιμοποιείται κυρίως για παράνομες δραστηριότητες. Επιπρόσθετα, η πρόσβαση στο Deep Web γίνεται με την χρήση username και password και συνήθως από παραδοσιακά προγράμματα περιήγησης, ενώ στο Dark Web απαιτείται η χρήση συγκεκριμένων προγραμμάτων, όπως το TOR, καθώς επίσης και η εφαρμογή τεχνολογιών VPN (Virtual Private Network) ή ακόμα και Virtual Machine, για την αύξηση του επιπέδου ασφαλείας οι οποίες θα αναλυθούν περαιτέρω στις επόμενες ενότητες.

4.2 Ιστορική Αναδρομή Dark Web

Παρόλο που το Dark Web είναι αρκετά δημοφιλές στις μέρες μας, δεν πρόκειται για μία τεχνολογία που δημιουργήθηκε πρόσφατα. Αντιθέτως, η ιστορία του ξεκινά από τα

τέλη της δεκαετίας του 1960. Πιο συγκεκριμένα το 1969 η ARPA (Advanced Research Projects Agency – Υπηρεσία Προηγμένων Ερευνητικών Προγραμμάτων), η οποία αποτελεί ένα κομμάτι του Υπουργείου Άμυνας των Ηνωμένων Πολιτειών Αμερικής, δημιούργησε ένα δίκτυο υπολογιστών, στο οποίο οι υπολογιστές μπορούσαν να αλληλεπιδρούν μέσω πακέτων δεδομένων.

Αυτό έγινε δημοφιλής ως δίκτυο της ARPA ή αλλιώς ARPANET. Χαρακτηριστικό της επανάστασης που έφερε το ARPANET, αποτελεί το γεγονός ότι χρησιμοποιήθηκε όχι μόνο από ανώτατα εκπαιδευτικά ιδρύματα των ΗΠΑ με σκοπό την αμφίδρομη επικοινωνία και την βελτίωση της τεχνολογίας, αλλά και στον στρατό. Το ARPANET αποδείχθηκε ότι αποτέλεσε βασικό πυλώνα τεχνολογίας για αυτό που ονομάζουμε σήμερα Internet (διαδίκτυο) [**Πηγή 3 Κεφ4**]. Επιπλέον, με την χρηματοδότηση της ARPA, το ARPANET ήταν ένα δίκτυο ιδιωτικοποιημένο επιτρέποντας την χρήση του μόνο σε πανεπιστήμια των ΗΠΑ, δίνοντας τους την ελευθερία να πειραματιστούν και να επιχειρήσουν διαφορετικά και παράτολμα πράγματα, στο όνομα των πειραμάτων και της εξέλιξης.

Το 1971 φοιτητές του πανεπιστημίου Stanford και συγκεκριμένα του Εργαστηρίου Τεχνητής Νοημοσύνης που χρησιμοποιούσαν το δίκτυο ARPANET, πραγματοποίησαν την πρώτη διαδικτυακή αγοροπωλησία μαριχουάνας [**Πηγή 3 Κεφ4**] . Ωστόσο, αξίζει να αναφερθεί ότι αυτό δεν αποτέλεσε διαδικτυακή χρηματική συναλλαγή, αλλά μέσω αυτής της τεχνολογίας ορίστηκε η τοποθεσία που θα πραγματοποιούνταν η συναλλαγή [**Πηγή 3 Κεφ4**].

Αργότερα η ARPA, επειδή τηρούσε μεγάλες δεσμεύσεις με την κυβέρνηση των ΗΠΑ, διασπάστηκε σε δύο μέρη και συγκεκριμένα αυτό πραγματοποιήθηκε το 1983 [**Πηγή 4 Κεφ4**]. Το πρώτο μέρος αφορούσε τον στρατό, το οποίο ονομάστηκε MILNET και αφορούσε στρατιωτικές υπηρεσίες, ενώ το δεύτερο παρέμεινε ως ARPANET, η οποία αποτελούσε την πολιτική έκδοση.

Στην συνέχεια το έτος 1989, ο Tim Berners-Lee ο οποίος εργαζόταν στο CERN (European Organization for Nuclear Research – Ευρωπαϊκός Οργανισμός Πυρηνικής Ενέργειας) επινόησε τις βασικές αρχές των ιστοτόπων που δεν ήταν άλλες από τις HTTP,

URL και HTML [**Πηγή 3 Κεφ4**]. Επιπλέον, δημιούργησε το πρώτο πρόγραμμα επεξεργασίας ιστοσελίδων και έπειτα τον πρώτο Web Server (εξυπηρετητή). Έτσι, φθάνοντας το 1991 με την κυκλοφορία του διαδικτύου, τα επιτεύγματα του Tim Berners-Lee βρήκαν την θέση τους σε αυτό. Εν συνεχεία, ο Tim Berners-Lee και οι συνεργάτες του προσπάθησαν αρκετά έτσι ώστε το διαδίκτυο να είναι ελεύθερο σε όλο τον κόσμο, γεγονός το οποίο συντελέστηκε το έτος 1993. Ακολούθως, το έτος 1994 συνέβη η πρώτη αγορά μέσω διαδικτύου και φημολογείται ότι πραγματοποιήθηκε κρυπτογραφημένα [**Πηγή 3 Κεφ4**], δίνοντας έμφαση στην προστασία των συναλλαγών.

Το έτος 2000 δόθηκε στην κυκλοφορία το Freenet [**Πηγή 4 Κεφ4**]. Το Freenet ήταν ένα λογισμικό που έδινε την δυνατότητα στους χρήστες να διαμοιράζονται αρχεία μεταξύ τους. Αυτό που έκανε το Freenet να ξεχωρίζει ήταν ότι πρόσφερε στον χρήστη ανωνυμία περιήγησης και επικοινωνίας. Αν και σαν εγχείρημα δεν είχε μεγάλη απήχηση, έπαιξε καθοριστικό ρόλο στην ανάγκη για ανώνυμη περιήγηση στο Internet [**Πηγή 4 Κεφ4**].

Το 2002 κυκλοφόρησε το πρόγραμμα περιήγησης TOR (The Onion Router), με το οποίο θα ασχοληθούμε στις επόμενες ενότητες. Το TOR στόχευε στην ανώνυμη περιήγηση του χρήστη στο Internet, παρέχοντάς του αφενός την ανωνυμία της επικοινωνίας και αφετέρου την ελευθερία του λόγου, σεβόμενο την ιδιωτικότητα. Αργότερα, το 2008, το TOR άρχισε να εξελίσσεται.

Το 2011 δημιουργήθηκε η Silk Road, ένας περίφημος ιστότοπος της σκοτεινής αγοράς, με εγκληματικές δραστηριότητες. Για να περιηγηθεί κάποιος σε αυτό θα έπρεπε να εξασφαλίζεται η ανωνυμία του. Το πρόγραμμα περιήγησης TOR παρείχε αυτήν την δυνατότητα στον χρήστη και έτσι έγινε το μέσον με το οποίο πραγματοποιούνταν η πρόσβαση στο Dark Web. Αποτέλεσμα της δημιουργίας του Silk Road ήταν η αύξηση των εγκληματικών ενεργειών στο διαδίκτυο.

4.3 Εύρος Αναζήτησης στο Dark Web

Σε αυτή την ενότητα του κεφαλαίου θα παρατεθούν οι κατηγορίες των προϊόντων και των υπηρεσιών που παρέχονται μέσω του Dark Web στον χρήστη. Συγκεκριμένα θα επιβεβαιωθεί ότι το Dark Web δεν διαθέτει μόνο παράνομο περιεχόμενο, αλλά αποτελεί χρήσιμο και νόμιμο εργαλείο σε κάποιες περιπτώσεις.

-Διακίνηση ναρκωτικών και ιατροφαρμακευτικών σκευασμάτων

Ένα από τα πιο συνήθη περιστατικά, είναι η αγοροπωλησία ναρκωτικών ουσιών [**Πηγή 5 Κεφ4**]. Κατά την περιήγηση στο Dark Web, ο χρήστης μπορεί να αναζητήσει τα ναρκωτικά που επιθυμεί να αγοράσει καθώς επίσης να δει και την τιμή αυτών. Επίσης, είναι σημαντικό να αναφερθεί ότι εκτός από την πώληση ναρκωτικών ουσιών, πωλούνται ακόμη και ιατροφαρμακευτικά σκευάσματα (χάπια, ενέσεις, αναβολικές ουσίες κ.α.) τα οποία υπόσχονται ότι αποτελούν θεραπεία κάποιων παθήσεων, δίχως όμως αυτά να έχουν λάβει έγκριση από κάποιο διεθνή οργανισμό και δίχως να είναι γνωστές οι παρενέργειές τους.

Η αγορά και η χρήση ναρκωτικών ουσιών ή/και ιατροφαρμακευτικών σκευασμάτων μπορεί να επιφέρει στον χρήστη ανεπανόρθωτες βλάβες στον οργανισμό του. Επιπλέον, διακινούνται συμπληρώματα διατροφής τα οποία παρουσιάζονται ως υψηλής διατροφικής αξίας αγαθά υποσχόμενα ευεξία καθώς επίσης και φάρμακα για ανύπαρκτες ασθένειες όπου εγγυώνται την ίαση τους. Επιπρόσθετα, προωθούνται φάρμακα τα οποία υποστηρίζουν ότι διαθέτουν το ελιξίριο της μακροζωίας, όπου αφελείς χρήστες τα αγοράζουν και τα χρησιμοποιούν δίχως να γνωρίζουν το περιεχόμενο αυτών των ουσιών, με αποτέλεσμα να τίθεται σε κίνδυνο η υγεία τους.

-Σωματεμπορία

Η σωματεμπορία (Trafficking) αποτελεί ένα από τα πιο γνωστά αδικήματα που λαμβάνουν χώρα μέσω Dark Web. Σε αυτό οι έμποροι λευκής σαρκός, οι οποίο έχουν σκοπό να αποκομίσουν παράνομο κέρδος, στρατολογούν και εξωθούν ανθρώπους να

προβαίνουν σε σεξουαλικές πράξεις έναντι αμοιβής. Είναι αρκετά συνηθισμένο σε αυτή την περίπτωση να συμμετέχουν μοντέλα, τα οποία οι έμποροι τους υπόσχονται μία καλύτερη ζωή και αξιοζήλευτη καριέρα. Επομένως, μέσω του Dark Web ένας χρήστης έχει την δυνατότητα να προγραμματίσει συνάντηση με εκδιδόμενα άτομα με σκοπό την ικανοποίηση των σεξουαλικών του επιθυμιών.

-Αγοραπωλησία ζωτικών οργάνων

Ένα απάνθρωπο αδίκημα που διαπράττεται στο Dark Web είναι αυτό της παράνομης αγοραπωλησίας ζωτικών οργάνων. Ειδικότερα, άτομα που ανήκουν στον ευρύτερο υπόκοσμο εκμεταλλευόμενοι το υπέρτατο αγαθό της ανθρώπινης ζωής, υπόσχονται στους χρήστες την εύρεση οργάνων έναντι αδράς αμοιβής. Ωστόσο, σε μεγάλο αριθμό περιπτώσεων οι χρήστες αφότου καταθέσουν το υπέρογκο ποσό που τους ζητήθηκε οι παράνομοι έμποροι εξαφανίζονται.

- Αγορά προσωπικών δεδομένων

Στο Dark Web μπορεί κανείς να αγοράσει πληροφορίες που έχουν διαρρεύσει και αφορούν προσωπικά δεδομένα ανθρώπων. Τα δεδομένα αυτά προέρχονται από τράπεζες ή διάφορες εταιρίες και οργανισμούς που στο παρελθόν είχαν πέσει θύματα Hacking και παρέχουν πληροφορίες όπως το ονοματεπώνυμο και κωδικούς πρόσβασης των πελατών καθώς και στοιχεία που αφορούν τους λογαριασμούς τραπέζης αυτών.

-Παιδική πορνογραφία

Το πιο αποκρουστικό, ίσως, από όλα τα αδικήματα που διαπράττονται στο Dark Web είναι αυτό της παιδικής πορνογραφίας. Σε αυτό περιέχονται εικόνες, βίντεο και γενικά οπτικοακουστικό υλικό ανήλικων παιδιών ακόμα και βρεφών στα οποία ασκούνται σεξουαλικές πράξεις αρκετές φορές με την συμμετοχή ενηλίκων. Το πιο δυσάρεστο γεγονός αυτού του αδικήματος είναι η αρκετά μεγάλη επισκεψιμότητα [**Πηγή 5 Κεφ4**] τέτοιου είδους ιστοτόπων.

-Εκδικητική πορνογραφία

Όσον αφορά το αδίκημα της εκδικητικής πορνογραφίας, σε αυτό περιέχονται οπτικοακουστικό υλικό γυναικών και ανδρών οι οποίοι συμμετέχουν σε σεξουαλικές πράξεις. Πολλές φορές το υλικό που ανεβαίνει είναι παράνομο διότι πρόκειται για προϊόν εκδίκησης μεταξύ των συντρόφων και μαγνητοσκοπείται εν αγνοία του θύματος.

-Proxying

Στο Dark Web υπάρχουν απατεώνες που μπορούν να εξαπατήσουν τους χρήστες αποσπώντας από αυτούς χρήματα κατά την πληρωμή ως αντίτιμο μιας υπηρεσίας. Οι απατεώνες κατευθύνουν τους χρήστες άθελα τους από ένα ασφαλές περιβάλλον σε ένα άλλο σύνδεσμο της επιθυμίας τους με αποτέλεσμα, όταν ο χρήστης προβεί στην διαδικασία της πληρωμής, τα χρήματα να μεταφερθούν στο απατεώνα.

-Εκβιασμοί

Εντός του Dark Web δημιουργούνται ομάδες οι οποίες εκβιάζουν με επιθέσεις DDOS (Distributed Denial Of Service). Πιο συγκεκριμένα αυτές οι ομάδες αποτελούνται από αρκετά μέλη που έχουν στόχο την παράλυση των Servers (εξυπηρετητών) μεγάλων εταιριών, εκβιάζοντάς τες με κυβερνοεπιθέσεις. Προκειμένου να μην προβούν σε τέτοιου είδους επιθέσεις ζητούν λύτρα, συνήθως σε μορφή κρυπτονομισμάτων.

-Διακίνηση όπλων

Άλλο ένα σύνηθες φαινόμενο στο Dark Web είναι η αγοροπωλησία όπλων και όχι μόνο. Μέσα από αυτό ο χρήστης μπορεί να αποκτήσει όπλα, χειροβομβίδες, εκρηκτικά υλικά έναντι αμοιβής. Μάλιστα αναφέρεται πως αυτό το φαινόμενο είναι ιδιαίτερα συχνό στην Ευρώπη, η οποία αποτελεί μία από τις μεγαλύτερες πηγές εμπορίου όπλων [**Πηγή 5 Κεφ4**].

-Onion cloning

Η τεχνική Onion cloning προσεγγίζει αυτή της τεχνικής Proxying. Με την τεχνική Onion cloning οι απατεώνες δημιουργούν ιστοτόπους παρόμοιους ή ακόμη και πιστά αντίγραφα με τους αυθεντικούς. Με αυτόν τον τρόπο ο χρήστης αντί να κατευθύνεται στους πραγματικούς ιστοτόπους, κατευθύνεται σε αυτούς που έχουν δημιουργήσει οι απατεώνες με αποτέλεσμα, κατά την διαδικασία της πληρωμής να εξαπατώνται και να τους αποσπώνται χρηματικά ποσά.

-Συμβόλαια θανάτου

Από τα πιο ανατριχιαστικά παράνομα περιστατικά του Dark Web είναι αυτά των συμβολαίων θανάτου. Ο χρήστης μπορεί να κλείσει συμφωνία, έναντι αμοιβής, με έναν επαγγελματία δολοφόνο προκειμένου να εξοντώσει έναν άνθρωπο με τον οποίο έχει διαφορές. Ουσιαστικά, ο χρήστης προσλαμβάνει έναν δολοφόνο για να σκοτώσει έναν άνθρωπο.

-Παρακολούθηση βασανιστηρίων

Σε αυτή την περίπτωση οι χρήστες πληρώνουν για να δουν μία πληθώρα από βίντεο, με περιεχόμενο τον βασανισμό ανθρώπων και παιδιών. Το περιεχόμενό τους επικεντρώνεται στην βία και στην κακοποίηση, κυρίως σωματικά, ενώ άλλες φορές συνδέεται και με σεξουαλικές πράξεις.

-Πλαστογραφία

Σε αυτή την περίπτωση ο χρήστης έχει την δυνατότητα να προσλάβει έναν πλαστογράφο, ο οποίος μπορεί να του δημιουργήσει ένα πλαστό πτυχίο πιστοποίησης ξένης γλώσσας ή ακόμη και πτυχίο από ανώτατο εκπαιδευτικό ίδρυμα. Επιπλέον, η γκάμα της πλαστογραφίας δεν περιορίζεται μόνο στα παραπάνω, αντιθέτως μπορεί κάποιος να αποκτήσει ένα δίπλωμα οδήγησης, μία ταυτότητα, ένα συμβολαιογραφικό έγγραφο, ένα πιστοποιητικό εμβολιασμού κατά της Covid-19, ένα διαβατήριο ακόμη και πλαστά χαρτονομίσματα.

-Πρόσληψη Hackers

Ο χρήστης με την πλοήγησή του στο Dark Web μπορεί να προσλάβει έναν επαγγελματία Hacker με σκοπό να αποσπάσει πληροφορίες από ανθρώπους της επιθυμίας του. Ουσιαστικά ο εκάστοτε hacker εισβάλλει στον ηλεκτρονικό υπολογιστή ή ακόμη και σε ηλεκτρονικές συσκευές (όπως κάμερες) του θύματος που του έχει υποδείξει ο πελάτης και στην συνέχεια αποσπώντας πληροφορίες του θύματος, τις αποστέλλει στον πελάτη. Επιπλέον, έχουν αναφερθεί περιπτώσεις όπου χρήστες είχαν προβεί στην πρόσληψη hackers με σκοπό οι τελευταίοι να εξαφανίσουν εγκληματικά στοιχεία [**Πηγή 23 Κεφ4**].

-Αγοροπωλησία προγραμμάτων

Στο Dark Web διακινούνται προγράμματα ηλεκτρονικών υπολογιστών τα οποία χρησιμοποιούνται στην καθημερινότητα. Τα προγράμματα αυτά πολλές φορές κοστίζουν πάρα πολύ, καθιστώντας την απόκτηση τους οικονομικά ασύμφορη από τους χρήστες. Αντιθέτως στο Dark Web η πρόσβαση και η λήψη αυτών μπορεί να γίνει με μία πολύ χαμηλότερη τιμή ή ακόμα πολλές φορές και δωρεάν.

-Αγοροπωλησία βιβλίων, ταινιών και σειρών

Επιπλέον στο Dark Web υπάρχει και διακίνηση βιβλίων, ταινιών ή σειρών μυθοπλασίας, επιμορφωτικού ή επιστημονικού περιεχομένου, ξανά δωρεάν ή σε αρκετά χαμηλή τιμή όπου κανονικά για την απόκτηση τους θα έπρεπε κάποιος να διαθέσει αρκετά χρήματα ή να είναι συνδρομητής για την προβολή τους.

-Ελεύθερη Ειδησεογραφία

Εκτός από όλα τα παραπάνω, στο Dark Web διατίθενται και ιστοσελίδες ειδησεογραφίας όπου υπάρχει μεγάλη πιθανότητα να αναφέρονται σε μη παραποιημένα

γεγονότα που λόγω κυβερνητικής λογοκρισίας δεν δημοσιεύονται. Αυτό συμβαίνει λόγω της ανύπαρκτης λογοκρισίας.

-Ψευδή Ειδησεογραφία

Εκτός από την ελεύθερη ειδησεογραφία που προαναφέρθηκε, στο Dark Web υπάρχουν και αναρτήσεις ειδήσεων που είναι ψευδείς. Πολλές φορές βασίζονται σε θεωρίες συνωμοσίας με αποτέλεσμα την παραπληροφόρηση του χρήστη ενώ άλλες ίσως έχουν δημοσιευτεί από τις εκάστοτε κυβερνήσεις, χρησιμοποιώντας το Dark Web ως ένα μέσο προπαγάνδας. Επομένως οι χρήστες πρέπει να είναι αρκετά προσεκτικοί σε ποιους εμπιστεύονται την πληροφόρησή τους.

-Επικοινωνία

Στο Dark Web υπάρχουν υπηρεσίες ηλεκτρονικού ταχυδρομείου που δίνουν την δυνατότητα στους χρήστες τους να επικοινωνούν και να ανταλλάσσουν μηνύματα μεταξύ τους, όπως και στο Surface Web. Αυτό όμως που το κάνει να ξεχωρίζει είναι ότι η αμφίδρομη επικοινωνία προστατεύεται και είναι ανώνυμη, δίνοντας πλεονέκτημα στους ανθρώπους που παρακολουθούνται από κρατικούς μηχανισμούς να ανταλλάσσουν πληροφορίες με άλλους χρήστες.

4.4 Πλεονεκτήματα και Μειονεκτήματα του Dark Web

Σε αυτή την ενότητα θα δοθούν τα θετικά χαρακτηριστικά του Dark Web καθώς επίσης και τα αρνητικά αυτού. Σκοπός της ενότητας αποτελεί η δημιουργία μίας σφαιρικής άποψης επί του θέματος, για τον εκάστοτε αναγνώστη.

4.4.1 Πλεονεκτήματα Dark Web

Αρχικά, από τα ισχυρότερα πλεονεκτήματα του Dark Web είναι ότι παρέχει στους χρήστες του ανωνυμία κάνοντας, μη εφικτή την εύρεση και την ταυτοπροσωπία αυτού έναντι τρίτων. Αυτό δείχνει ότι το Dark Web σέβεται την ιδιωτική ζωή του χρήστη. Επιπλέον, υπάρχουν άνθρωποι που ζουν σε χώρες των οποίων τα Μέσα Μαζικής Ενημέρωσης είναι ελεγχόμενα από τις εκάστοτε αυταρχικές ή μη κυβερνήσεις, προπαγανδίζοντας και αποκρύπτοντας από τον κόσμο την αλήθεια, διαστρεβλώνοντας την πραγματικότητα. Στο Dark Web, εκμεταλλευόμενοι οι χρήστες την ανωνυμία που τους προσφέρει, είναι αρκετά δύσκολο κάποιος να πιστοποιηθεί και να στοχοποιηθεί για τα λεγόμενά του, από άλλους.

Με αυτό τον τρόπο δεν υφίσταται λογοκρισία, με αποτέλεσμα ο καθένας να μπορεί να εκφράσει την γνώμη του ελεύθερα ή ακόμα και να αποκαλύψει ένα μεγάλο μυστικό, δίχως να διωχθεί. Πρόσφατα μάλιστα, με την έναρξη της πανδημίας COVID-19 που θεωρείται ότι ξεκίνησε στην πόλη Wuhan της Κίνας, οι γιατροί που ενημέρωναν τον κόσμο μέσω των μέσων μαζικής ενημέρωσης σχετικά με την απειλή που δημιουργήθηκε, λογοκρίθηκαν, στοχοποιήθηκαν και διώχθηκαν για αυτό από την κινεζική κυβέρνηση. Αντίθετα, κάποιοι από αυτούς διέφυγαν στο Dark Web όπου εκεί διέρρευσαν πληροφορίες σχετικά με τον νέο κορονοϊό (SARS-COV2) και την πάθηση COVID-19 την οποία προκαλεί, με απώτερο σκοπό την ενημέρωση των πολιτών [**Πηγή 6 Κεφ4**].

Επιπρόσθετα, όπως θα παρουσιαστεί παρακάτω, το Dark Web έχει χρησιμοποιηθεί ακόμη και από αστυνομικές αρχές και κυβερνήσεις, όπου βοήθησε να εξιχνιαστούν εγκληματικές πράξεις, κάτι το οποίο καταλογίζεται στα θετικά.

Ολοκληρώνοντας τα πλεονεκτήματα του Dark Web γίνεται σαφές ότι η χρήση του ενθαρρύνει και ενδυναμώνει τους χρήστες του. Επιπλέον, προτρέπει τους ανθρώπους να γίνονται περισσότερο εξωστρεφείς στο δόγμα της ελευθερίας της έκφρασης.

4.4.2 Μειονεκτήματα Dark Web

Παρά τα πλεονεκτήματα που αναφέρθηκαν στην προηγούμενη ενότητα, δυστυχώς το Dark Web χρησιμοποιείται κυρίως ως ένας χώρος για μία πληθώρα από σειρά εγκλημάτων. Οι χρήστες, εκμεταλλεύονται την ανωνυμία που τους παρέχει ο χώρος αυτός και προβαίνουν σε πράξεις ποινικά κολάσιμες και καταδικαστέες. Πιο συγκεκριμένα το Dark Web γίνεται ένα εργαλείο που χρησιμοποιείται από αρκετούς κακοποιούς και εγκληματίες ανά την υφήλιο για να προβούν σε ανήθικες πράξεις.

Στα πλεονεκτήματα του Dark Web αναφέρθηκε ότι διασφαλίζει το απόρρητο και ότι σέβεται την ιδιωτικότητα των χρηστών του. Αυτό πράγματι ισχύει αλλά ως προς τους χρήστες. Από την άλλη στο Dark Web διακινούνται προσωπικά δεδομένα ανθρώπων καθώς επίσης και ευαίσθητες πληροφορίες για αυτούς, όπως ιατρικό ιστορικό, ονόματα, επώνυμα, φωτογραφίες, λογαριασμοί κοινωνικών μέσων δικτύωσης, πιστωτικές κάρτες, λογαριασμοί τραπέζης κ.α. Αυτά τα δεδομένα, τις περισσότερες φορές, έχουν διαρρεύσει έπειτα από επίθεση Hacking ή κάποιες άλλες φορές από σφάλμα των ίδιων των εταιριών ή οργανισμών.

Επιπλέον, στο Dark Web είναι πολύ έντονη η αγοροπωλησία και διακίνηση ουσιών και όπλων. Κάνει αρκετά εύκολη την διαδικασία απόκτησης των παραπάνω με αποτέλεσμα να αυξάνεται συνεχώς η εγκληματικότητα.

Ένα ακόμη μειονέκτημα του Dark Web είναι ότι εντός αυτού διακινούνται πολλά λογισμικά για ηλεκτρονικούς υπολογιστές. Αυτά τα προγράμματα κανονικά πωλούνται σε αρκετά υψηλές τιμές κάνοντάς τα μη προσιτά ως προς τους χρήστες. Αντιθέτως στο Dark Web διαμοιράζονται σε αρκετά χαμηλή τιμή ή ακόμα, πολλές φορές και δωρεάν.

Εκτός από τον διαμοιρασμό λογισμικού, διακινούνται και βιβλία, εργασίες, έρευνες, ταινίες, σειρές ανεξαρτήτου περιεχομένου (είτε επιμορφωτικού είτε ψυχαγωγικού χαρακτήρα) τα οποία διατίθενται είτε με μικρό αντίτιμο είτε δωρεάν. Επιπρόσθετα, η διάθεση βιβλίων, ταινιών, σειρών, εργασιών και ερευνητικών έργων σε χαμηλή τιμή ή ακόμα και δωρεάν, αποτελεί ένα μεγάλο οικονομικό πλήγμα για τις εταιρίες και τους

εκπαιδευτικούς οργανισμούς που τα παράγουν καθώς επίσης παραβιάζουν τους όρους της πνευματικής ιδιοκτησίας.

Ένα άλλο μειονέκτημα του Dark Web είναι ότι προωθεί την εκδικητική πορνογραφία καθώς επίσης και την παιδική πορνογραφία. Με αυτόν τον τρόπο κάνει προσβάσιμο σε πολλούς την απεικόνιση διεστραμμένων και ανήθικων πράξεων, κάτι το οποίο είναι ποινικά κολάσιμο και κοινωνικά κατακριτέο.

Ακόμα, στο Dark Web είναι πολύ πιθανόν ο χρήστης να εξαπατηθεί κατά την πληρωμή, κάποιας υπηρεσίας που επέλεξε. Για παράδειγμα αν ο χρήστης επιλέξει να κατεβάσει ένα πρόγραμμα ηλεκτρονικού υπολογιστή, είναι πιθανό να κατευθυνθεί άθελά του και εν αγνοία του σε ένα μη αυθεντικό, αλλά πλαστό, περιβάλλον πληρωμής και τα χρήματα να μεταφερθούν σε κάποιον απατεώνα.

Επίσης, εκτός από την πώληση ναρκωτικών ουσιών και όπλων, προωθεί και την ανθρωποκτονία, διότι μέσα από Dark Web μπορεί κάποιος να προσλάβει ένα επαγγελματία δολοφόνο για να εξοντώσει έναν αντίπαλό του.

Εκτός των παραπάνω δίνει την δυνατότητα σε ανθρώπους να αποκτήσουν πλαστούς τίτλους σπουδών, διαβατήρια, ταυτότητες και διπλώματα οδήγησης ή ακόμα και πλαστά έγγραφα συμβολαιογράφων και δικηγόρων. Αυτό ενέχει πολλούς κινδύνους τόσο για τις εκάστοτε κυβερνήσεις ανά την υφήλιο όσο και για τους πολίτες που διαμένουν σε αυτές.

Από όλα τα παραπάνω, το Dark Web δεν προστατεύει τον χρήστη από το τι θα παρακολουθήσει, με την πλοήγησή του σε αυτό. Είναι πολύ πιθανό ο χρήστης να έρθει αντιμέτωπος με γεγονότα τα οποία θα τον τραυματίσουν ψυχικά.

Επιπλέον, όπως θα παρατεθεί και παρακάτω, η πλοήγηση στο Dark Web, ενέχει και πολλούς κινδύνους, ως προς τον χρήστη, που αφορούν την ασφάλεια του υπολογιστή του. Καθώς ο χρήστης πλοηγείται στο Dark Web είναι πιθανόν να πατήσει (σ.σ. να κάνει κλικ) σε κάποιον σύνδεσμο ο οποίος άθελα του να κατεβάσει και να εγκαταστήσει στον

υπολογιστή του κάποιο Malware (μολυσμένο λογισμικό) ή κάποιον ιό (virus), που μπορεί να αποδειχθεί επιβλαβές και για τον ίδιο.

Συνοψίζοντας τα μειονεκτήματα του Dark Web διαπιστώνεται ότι έχει μετατραπεί σε ένα μέσον που διευκολύνει την διεκπεραίωση των εγκλημάτων. Είναι επικίνδυνο για ανθρώπους που δεν έχουν πρόθεση να βλάψουν κάποιον ή που δεν ξέρουν πως να το χρησιμοποιούν, διότι μπορεί να τους δημιουργήσει ψυχικής και οικονομικής φύσεως προβλήματα. Επιπλέον, τα χρήματα που διακινούνται εντός αυτού δεν φορολογούνται με αποτέλεσμα να ζημιώνονται παγκόσμια οι κυβερνήσεις. Επίσης, προωθεί άσεμνες πράξεις εις βάρος ενηλίκων και ανήλικων ανθρώπων. Τέλος, οδηγεί στην αύξηση της εγκληματικότητας.

4.5 Πρόσβαση στο Dark Web

Σε αυτό το κεφάλαιο θα περιγραφεί ο τρόπος με τον οποίο μπορεί κάποιος να αποκτήσει πρόσβαση στο Dark Web και κατά πόσο είναι εύκολο κάποιος να περιηγηθεί και να χρησιμοποιήσει αυτό. Αδιαμφισβήτητα η πρόσβαση στο Dark Web ενέχει αρκετούς κινδύνους, αλλά είναι σημαντικό κάποιος να μην ξεχνά ότι σε αυτό δεν περιέχονται μόνο κίνδυνοι. Αντιθέτως, υπάρχει περιεχόμενο που δεν αποτελεί εγκληματική πράξη ή απειλή. Ενδεικτικά, τέτοιο περιεχόμενο είναι η ειδησεογραφία ή η αναζήτηση και απόκτηση σπάνιων εντύπων. Επομένως, είναι ξεκάθαρο ότι ένας χρήστης μπορεί να επιθυμεί την χρήση του Dark Web και για άλλους σκοπούς, πέρα του εγκλήματος.

Για την πρόσβαση στο Dark Web είναι αναγκαία η λήψη και η εγκατάσταση συγκεκριμένων προγραμμάτων περιήγησης, δηλαδή Browser. Από τους πιο γνωστούς Browser, που χρησιμοποιούνται για την περιήγηση στο Surface Web είναι το Google Chrome, το Mozilla Firefox και ο Microsoft Edge. Αντίστοιχα για την πρόσβαση των χρηστών στο Dark Web, έχουν αναπτυχθεί συγκεκριμένα λογισμικά και δίκτυα που το επιτυγχάνουν. Τέτοια είναι το I2P (Invisible Internet Project, το Freenet καθώς επίσης και

το πιο διαδεδομένο και αξιόπιστο πρόγραμμα, το οποίο είναι το TOR. Περισσότερες πληροφορίες σχετικά με το TOR θα δοθούν στη συνέχεια.

Επομένως, αν κάποιος χρήστης επιθυμεί να περιηγηθεί στο Dark Web, θα πρέπει πρώτα να εγκαταστήσει το αντίστοιχο πρόγραμμα. Για την απόκτηση αυτού του προγράμματος, ο χρήστης πρέπει να αναζητήσει το πρόγραμμα περιήγησης TOR μέσω οποιουδήποτε συμβατικού Browser, όπως το Google Chrome. Στη συνέχεια αφού το εντοπίσει, πραγματοποιεί την λήψη αυτού και έπειτα το εγκαθιστά στην συσκευή του. Μετά την εγκατάσταση ο χρήστης μπορεί να περιηγηθεί στο Dark Web, μέσω του προγράμματος, δίχως καμία παραπάνω απαίτηση ή επιπλέον εγκατάσταση λογισμικού.

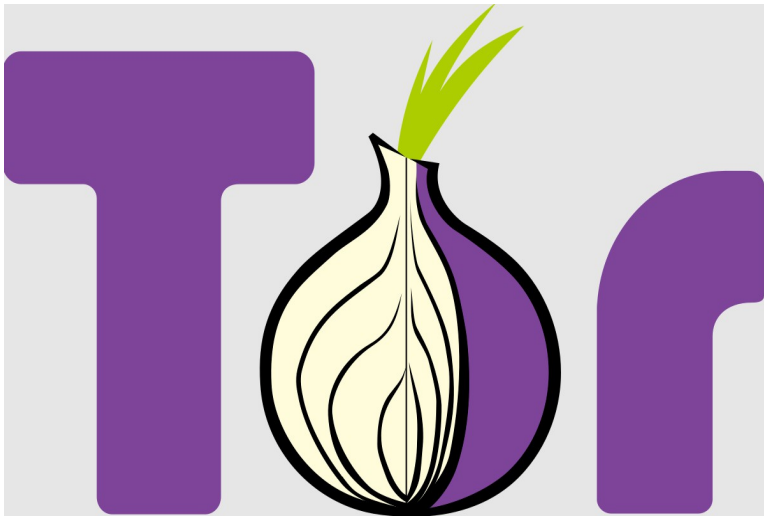
Με βάση τα παραπάνω, γίνεται αντιληπτό ότι η απόκτηση ενός προγράμματος περιήγησης, αναπτυγμένο και σχεδιασμένο για το Dark Web, μπορεί να το διαθέτει οποιοσδήποτε χρήστης που επιθυμεί την περιήγησή του σε αυτό, αρκετά εύκολα, γρήγορα και απλά.

4.6 Πρόγραμμα περιήγησης TOR

Σε αυτή την υποενότητα της εργασίας θα περιγραφεί το πρόγραμμα περιήγησης TOR καθώς επίσης θα αναφερθεί και η σκοπιμότητα για την οποία αναπτύχθηκε. Επιπλέον, θα περιγραφεί ο τρόπος λειτουργίας του, η ασφάλειά του και η ιστορία του.

4.6.1 Τι είναι το TOR

Το TOR, αποτελεί συντομογραφία της τεχνολογίας ¨The Onion Router¨ [**Πηγή 7 Κεφ4**] και είναι ένα λογισμικό ανοικτού κώδικα, το οποίο δίνει την δυνατότητα στον χρήστη να έχει πρόσβαση στον παγκόσμιο ιστό.



Εικόνα 3: Λογότυπο TOR

Πηγή:https://commons.wikimedia.org/wiki/File:Tor-logo-2011-flat.svg

Το κύριο χαρακτηριστικό του είναι ότι προσφέρει στον χρήστη την ανωνυμία κατά την πλοήγησή του στο διαδίκτυο. Για να διασφαλιστεί αυτό, το TOR χρησιμοποιεί πρωτόκολλα ασφαλείας και κρυπτογράφησης και με αυτόν τον τρόπο προστατεύει την ιδιωτικότητα των χρηστών.

Ο λόγος για τον οποίο η τεχνολογία ονομάστηκε Onion Router οφείλεται στο γεγονός ότι τα δεδομένα των χρηστών προστατεύονται από πολλά στρώματα ασφαλείας. Αυτό, παρομοιάζεται με την μορφή που έχει ένα κρεμμύδι, δηλαδή αποτελείται από αρκετά στρώματα τα οποία βρίσκονται, το ένα μέσα στο άλλο.

Επιπλέον, δίνει την δυνατότητα στους χρήστες του να έχουν πρόσβαση στο Dark Web σε ιστοσελίδες με την κατάληξη .onion οι οποίες δεν εμφανίζονται με τους συμβατικούς Browsers. Είναι σημαντικό να σημειωθεί, ότι λόγω αυτού του χαρακτηριστικού, δηλαδή της ελεύθερης πρόσβασης σε όλους τους ιστοτόπους, κάποιες χώρες έχουν απαγορεύσει την χρήση του [**Πηγή 7 Κεφ4**].

Επίσης, είναι σημαντικό να αναφερθεί ότι το TOR, ως προεπιλογή, δεν διατηρεί το ιστορικό περιήγησης και αναζήτησης του χρήστη αλλά το διαγράφει έπειτα από κάθε επίσκεψη στο πρόγραμμα [**Πηγή 7 Κεφ4**]. Αν ο χρήστης ενεργοποιήσει την διατήρηση

του ιστορικού, τότε αυτό αποθηκεύεται κρυπτογραφημένο καθώς επίσης και όλη η περιήγησή του.

Συνοψίζοντας, το TOR είναι ένα πρωτόκολλο αρκετά ασφαλές και κρυπτογραφημένο το οποίο παρέχει υψηλή ασφάλεια, όσον αφορά το απόρρητο των δεδομένων που ανήκουν στους χρήστες. Επιπρόσθετα, χρησιμοποιεί το δίκτυο TOR όπου μέσω ενός πλήθους ηλεκτρονικών υπολογιστών κρυπτογραφεί τα δεδομένα, την διεύθυνση IP και το ιστορικό περιήγησης του χρήστη καθώς επίσης προσφέρει στον ίδιο την ανωνυμία κατά την περιήγησή του.

4.6.2 Η ιστορία του TOR

Για την ανάπτυξη του TOR έχουν εργαστεί αρκετοί προγραμματιστές και ερευνητές, οι οποίοι έχουν κοινούς στόχους. Αυτοί οι στόχοι είναι η ανωνυμία του χρήστη κατά την περιήγηση, η διασφάλιση της ιδιωτικής πρόσβασης στο διαδίκτυο και η δημιουργία ενός δικτύου με ανύπαρκτη λογοκρισία.

Από την δεκαετία του 1990, ήταν ήδη σαφές ότι στο διαδίκτυο δεν υπάρχει ασφάλεια και ότι χρησιμοποιείται για μεθόδους παρακολούθησης. Έτσι το 1995 οι David Goldschlag, Mike Reed και Paul Syverson πρότειναν την δημιουργία ενός δικτύου βασισμένο στην τεχνολογία Onion Router [**Πηγή 8 Κεφ4**]. Με βάση αυτή την τεχνολογία, ο σκοπός τους ήταν να δημιουργήσουν ένα δίκτυο που να καθιστά ανέφικτη την απόσπαση πληροφοριών που ανταλλάσσονται εντός αυτού του δικτύου.

Επιπροσθέτως, στόχευαν στην ιδιωτικότητα των χρηστών κατά την πλοήγησή τους στο διαδίκτυο, προστατεύοντας την ταυτότητά τους. Η ιδέα για να πραγματοποιηθεί κάτι τέτοιο ήταν η δημιουργία ενός δικτύου στο οποίο να συμμετέχουν πολλά τερματικά (κόμβοι) όπου θα αναλάμβαναν την κρυπτογράφηση σε κάθε βήμα.

Το έτος 2000, άλλος ένας ερευνητής, με όνομα Roger Dingledine, συμμετείχε στο έργο αυτό και εργάζονταν για το Onion Router, σε συνεργασία με τον Paul Syverson. Εν

συνεχεία, προκειμένου το έργο του Onion Router να ξεχωρίζει από προηγούμενες προσπάθειες, με την χρήση της ίδιας τεχνικής, ο Roger Dingledine ονόμασε το έργο The Onion Routing (TOR). Είναι σημαντικό να αναφερθεί, ότι έπειτα από αυτό εντάχθηκε και άλλο μέλος στην προσπάθεια αυτή, ο οποίος ονομάζεται Nick Mathewson από το MIT (Ινστιτούτο Τεχνολογίας Μασαχουσέτης).

Η κύρια ιδέα του Onion Routing ήταν να βασίζεται σε ένα αποκεντρωμένο δίκτυο. Επομένως, το δίκτυο να λειτουργεί από οντότητες με διαφορετικά πρότυπα εμπιστοσύνης και το λογισμικό να είναι ελεύθερο και προσβάσιμο σε όλους. Το 2002 η τεχνολογία TOR είχε αναπτυχθεί αρκετά και διατέθηκε στο ευρύ κοινό ως ελεύθερο και ανοιχτού κώδικα λογισμικό [**Πηγή 3 Κεφ4**]. Έπειτα από αυτό στα τέλη του 2003 στο δίκτυο TOR συμμετείχαν τουλάχιστον δώδεκα κόμβοι εθελοντών.

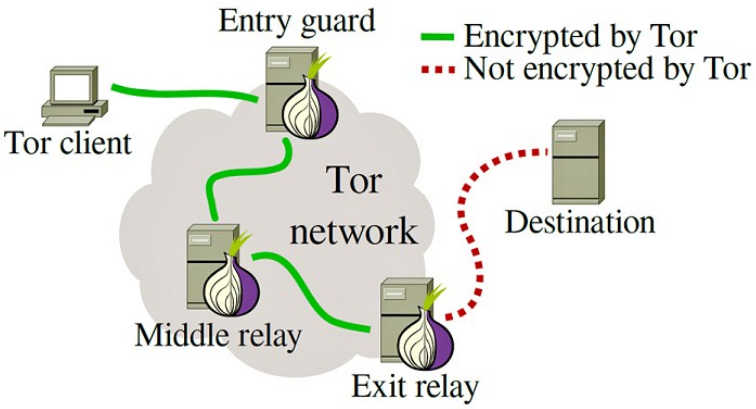
Εν συνεχεία, το έτος 2004, η Electronic Frontier Foundation άρχισε να χρηματοδοτεί το έργο του TOR, με αποτέλεσμα το 2006 να δημιουργηθεί μία μη κερδοσκοπική οργάνωση με όνομα Tor Project, η οποία θα αναλάμβανε την διατήρηση και την εξέλιξη του TOR.

Το 2007 άρχισαν να δημιουργούνται Bridges (γέφυρες) στο δίκτυο του TOR, προκειμένου να αντιμετωπιστεί η λογοκρισία και να δοθεί στους ανθρώπους η ευκαιρία να έχουν πρόσβαση σε αυτό. Επιπλέον, μέχρι τότε η πρόσβαση στο δίκτυο του TOR γίνονταν από ανθρώπους με γνώσεις τεχνολογίας, και μέσω αυτών και ακτιβιστών, το TOR άρχισε να γίνεται πιο δημοφιλές. Για αυτόν τον λόγο δημιουργήθηκε η ανάγκη για την δημιουργία ενός Browser, η οποία ξεκίνησε το 2008. Έπειτα από αυτό το TOR έγινε διαθέσιμο στο ευρύ κοινό.

4.6.3 Πως λειτουργεί το TOR

Όπως έχει γίνει αντιληπτό, το κύριο μέλημα της δημιουργίας και της χρήσης του TOR Browser είναι η προστασία του απορρήτου των χρηστών και η εμπόδιση της

άντλησης πληροφοριών που διακινούνται μεταξύ τους. Επομένως, κατά την περιήγησή μας στο TOR, είτε χρησιμοποιείται για επικοινωνία είτε για την πρόσβαση σε κάποιον ιστότοπο, το ίδιο το δίκτυο του TOR δεν συνδέει τον χρήστη απευθείας με τον εξυπηρετητή που επιθυμεί να ικανοποιήσει το αίτημά του. Αντίθετα, πριν το αίτημα σταλθεί στον τελικό εξυπηρετητή, περνά μέσα από ένα σύνολο άλλων τερματικών, που ανήκουν σε εθελοντές χρήστες του δικτύου TOR, όπου κρυπτογραφούνται τα στοιχεία του χρήστη και έπειτα τίθεται το αίτημα στον τελικό εξυπηρετητή [**Πηγή 9 Κεφ4**].



Εικόνα 4: Γραφική αναπαράσταση λειτουργίας του TOR
Πηγή:https://guardianproject.info/2020/06/02/onion-browser-release-2.6-tutorial/

Η λειτουργία του δικτύου TOR, απαιτεί την ύπαρξη αρκετών τερματικών που χρησιμοποιούνται για την κρυπτογράφηση των πληροφοριών. Επιπλέον, πρόκειται για ένα δίκτυο στο οποίο συμμετέχουν αρκετοί υπολογιστές, οι οποίοι ανήκουν σε χρήστες του δικτύου και αφορούν εθελοντές από όλο τον κόσμο. Φημολογείται ότι πρόκειται, για ένα σύμπλεγμα, με περισσότερα από 7.000 τερματικά εθελοντών [**Πηγή 10 Κεφ4**], τα οποία αποτελούν αναπόσπαστο κομμάτι του δικτύου και έχουν τον ρόλο του κόμβου. Το δίκτυο του TOR αποτελείται από ενδιάμεσους κόμβους και ορίζεται από την μεσολάβηση τριών επιπέδων [**Πηγή 11 Κεφ4**]. Αυτό σημαίνει, ότι για να φτάσει το αίτημα του χρήστη στον τελικό εξυπηρετητή που επιθυμεί, πρέπει πρώτα οι πληροφορίες του καθώς επίσης και το αίτημά του να δρομολογηθεί μέσα από τρείς (κόμβους) του δικτύου, με σκοπό την

κρυπτογράφηση αυτών και έπειτα να πλοηγηθεί στην ιστοσελίδα που ο ίδιος θέλει. Με αυτόν τον τρόπο εξασφαλίζεται η ανωνυμία

Κατά την χρήση του TOR Browser, ο χρήστης λαμβάνει μία λίστα από τους διαθέσιμους κόμβους που συμμετέχουν στο δίκτυο TOR. Βάσει αυτής της λίστας ο TOR Browser δρομολογεί το αίτημα και τις πληροφορίες του χρήστη, κρυπτογραφημένες, σε έναν τυχαίο κόμβο που ανήκει στο δίκτυο. Στην συνέχεια, αυτά τα κρυπτογραφημένα δεδομένα αποστέλλονται σε έναν ενδιάμεσο κόμβο και έπειτα σε έναν τρίτο κόμβο ξανά κρυπτογραφημένα. Ο τελευταίος κόμβος αναλαμβάνει την αποκρυπτογράφηση των στοιχείων που του έχουν σταλεί και είναι υπεύθυνος για την σύνδεση του χρήστη με τον τελικό εξυπηρετητή [**Πηγή 11 Κεφ4**]. Επιπρόσθετα, κάθε κόμβος του δικτύου γνωρίζει τον προηγούμενο και τον επόμενο κόμβο, που στάλθηκαν και που θα σταλθούν αντίστοιχα οι κρυπτογραφημένες πληροφορίες, δίχως να γνωρίζει τους υπόλοιπους κόμβους που συμμετέχουν στο δίκτυο.

Προκειμένου να γίνει περισσότερο ξεκάθαρη η κατανόηση των παραπάνω, παρατίθεται η παρακάτω εικόνα, όπου το βέλος με μπλε χρώμα αντιπροσωπεύει την ανταλλαγή πληροφοριών που αφορούν το δίκτυο TOR. Τα πράσινα βέλη αντιπροσωπεύουν την κρυπτογράφηση και αποστολή δεδομένων μεταξύ των κόμβων του δικτύου ενώ το κόκκινο βέλος αντιστοιχεί στην αποκρυπτογραφημένη αποστολή των δεδομένων και την σύνδεση με τον εξυπηρετητή προορισμού.

Εικόνα 5: Γραφική αναπράσταση της λειτουργίας του TOR Browser

Πηγή:https://www.csoonline.com/article/3287653/what-is-the-tor-browser-how-it-works-and-how-it-can-help-you-protect-your-identity-online.html

Όπως διακρίνεται, ο χρήστης χρησιμοποιώντας το πρόγραμμα περιήγησης του TOR λαμβάνει μία λίστα με όλους τους κόμβους που ανήκουν στο δίκτυο από τον Directory Server. Εν συνεχεία, το αίτημά του καθώς και στοιχεία που αφορούν τον υπολογιστή του (όπως η IP διεύθυνση) κρυπτογραφούνται και αποστέλλονται σε έναν τυχαίο κόμβο του δικτύου. Έπειτα, τα κρυπτογραφημένα δεδομένα αποστέλλονται σε έναν ενδιάμεσο κόμβο και αυτός με την σειρά του τα αποστέλλει σε έναν τρίτο. Ο τελικός κόμβος αναλαμβάνει την αποκρυπτογράφηση των δεδομένων και την σύνδεση του χρήστη με τον εξυπηρετητή που απαιτεί το αίτημά του.

Επιπλέον, λόγω της κρυπτογράφησης των IP διευθύνσεων είναι σύνηθες τα αποτελέσματα του χρήστη να αναφέρονται σε κάποια ξένη γλώσσα και αυτό οφείλεται στην αναγνώριση της IP διεύθυνσης η οποία μπορεί να εντοπίζεται ότι αντιστοιχεί σε κάποια ξένη χώρα. Επιπλέον, είναι σημαντικό να αναφερθεί ότι η διαδρομή που ακολουθούν τα κρυπτογραφημένα δεδομένα είναι τυχαία και δεν ορίζεται, καθώς επίσης για την αποστολή των δεδομένων χρησιμοποιείται πρωτόκολλο TCP (Transmission Control Protocol) [**Πηγή 11 Κεφ4**] εξασφαλίζοντας ότι τα δεδομένα δεν θα χαθούν στον προορισμό τους.

4.6.4 Νομιμότητα του TOR Browser

Λόγω της ανωνυμίας που προσφέρει ο TOR Browser, αρκετοί αναρωτιούνται για το αν είναι νόμιμη ή παράνομη η χρήση του. Αυτή η απορία είναι εύλογη διότι οι άνθρωποι σκέφτονται με την λογική ότι για να χρειάζεται κάποιος την ανωνυμία του τότε σίγουρα έχει την πρόθεση να προβεί σε μία παράνομη πράξη ή θέλει να καλύψει τα ίχνη του κάποιος που έχει διαπράξει ένα έγκλημα και δεν θέλει να αποκαλυφθούν πληροφορίες που μπορεί να οδηγήσουν στην σύλληψή του. Επιπλέον, αυτή η αντίληψη ενισχύεται όταν οι άνθρωποι συνδέουν τον TOR Browser ως μέσο πρόσβασης στο Dark Web όπου διαπράττονται μία πληθώρα καταδικαστέων πράξεων.

Όπως έχει προαναφερθεί, η χρήση του Dark Web δεν περιορίζεται μόνο σε εγκληματικές δράσεις για αυτό και η χρήση του TOR Browser δεν είναι ποινικά διώξιμη αλλά απολύτως νόμιμη. Οι περισσότεροι άνθρωποι ανά την υφήλιο μπορούν να έχουν πρόσβαση σε αυτό με εξαίρεση τους πολίτες που ζουν σε χώρες υπό αυστηρό καθεστώς.

Μία από αυτές τις χώρες είναι η Κίνα η οποία έχει θέσει εκτός λειτουργίας τις υπηρεσίες που παρέχουν ανωνυμία περιήγησης και την κυκλοφορία του TOR Browser. Σημαντικό παράδειγμα τέτοιας κίνησης είναι η Βενεζουέλα, η οποία έχει μπλοκάρει την κυκλοφορία του TOR Browser σε όλη την χώρα. Επιπλέον, υπάρχουν χώρες των οποίων οι κυβερνήσεις εμποδίζουν τους πολίτες τους να έχουν πρόσβαση στο Dark Web. Αυτές είναι η Ρωσία, η Σαουδική Αραβία και το Ιράν [**Πηγή 11 Κεφ4**].

Διαβάζοντας τα παραπάνω διαπιστώνεται ότι χώρες με αυστηρό καθεστώς προσπαθούν να απαγορεύσουν την πρόσβαση στο Dark Web με έμμεσο τρόπο. Αυτό έχει ως απώτερο σκοπό τον περιορισμό της ελευθερίας της έκφρασης και την φίμωση των πολιτών ώστε οι κυβερνήσεις να αποφασίζουν τις ειδήσεις και το περιεχόμενο αυτών. Επιπλέον, αυτό είναι χρήσιμο για τις εκάστοτε κυβερνήσεις έτσι ώστε να αντιλαμβάνονται τους αντιφρονούντες και να στοχοποιούν τους πολίτες που είναι αντίθετοι στις πράξεις ή τις απόψεις τους.

4.6.5 Ασφάλεια στον TOR Browser

Ο TOR Browser πράγματι προσφέρει στους χρήστες του ανωνυμία των ίδιων και της περιήγησής τους στο διαδίκτυο προστατεύοντας την ιδιωτική ζωή σε ένα πολύ υψηλό επίπεδο. Όμως, οι πληροφορίες μπορούν να διαρρεύσουν, μέσω του τελικού κόμβου.

Όπως έχει προαναφερθεί ο TOR Browser με την χρήση του TOR δικτύου, κρυπτογραφεί τα δεδομένα που διακινούνται σε αυτό με εξαίρεση τον τελευταίο κόμβο, ο οποίος τα αποκρυπτογραφεί και συνδέεται με τον τελικό εξυπηρετητή. Επομένως, κάποιος τρίτος (για παράδειγμα μια κυβέρνηση ή ένας πάροχος) έχει την δυνατότητα να παρακολουθήσει τις πληροφορίες που αποστέλλονται μεταξύ του κόμβου εξόδου και του τελικού εξυπηρετητή.

Επιπλέον, οι κόμβοι που περιέχονται στο δίκτυο TOR αναφέρονται σε μία συγκεντρωτική λίστα κόμβων, η οποία είναι ελεύθερη και δημόσια. Άρα οποιοσδήποτε κόμβος εξόδου μπορεί να παρακολουθείται και οποιαδήποτε μη κρυπτογραφημένη πληροφορία που εξέρχεται από αυτούς, ίσως να επιβλέπεται.

Επίσης, είναι σημαντικό να αναφερθεί ότι κατά την πλοήγησή του ο χρήστης, υπάρχει μεγάλη πιθανότητα να κατεβάσει κάποιο μολυσματικό λογισμικό στην συσκευή του που χρησιμοποιεί. Αυτό μπορεί να γίνει πατώντας σε κάποιο λανθασμένο σύνδεσμο ή ακόμα πολλές φορές να πραγματοποιηθεί και εν αγνοία του.

Συνοψίζοντας τα παραπάνω, ο TOR Browser ναι μεν παρέχει ασφάλεια ως προς τον χρήστη, όσον αφορά την ανωνυμία και την ιδιωτική ζωή, αλλά δεν τον προστατεύει ως προς την ασφάλεια των λογισμικών που διακινούνται εντός αυτού. Επομένως, κρίνεται σκόπιμη η χρήση του από εξοικειωμένους χρήστες που γνωρίζουν τρόπους και μπορούν να αυξήσουν την προστασία τους, τόσο για τους ίδιους όσο και τις συσκευές τους.

4.6.6 Προτεινόμενοι τρόποι ασφάλειας στον TOR Browser

Όπως είναι γνωστό ο TOR Browser παρέχει από μόνος του ασφάλεια της ιδιωτικότητας του χρήστη αλλά υπάρχουν επιπλέον μέθοδοι που αυξάνουν την προστασία του κατά την πλοήγησή του. Αυτοί οι μέθοδοι παρουσιάζονται παρακάτω.

Είναι πολύ σημαντικό ο χρήστης να μην αποκαλύπτει την ταυτότητα του κατά την περιήγησή του στο διαδίκτυο με την χρήση του TOR Browser. Επομένως, ο χρήστης δεν θα πρέπει να συνδεθεί με λογαριασμούς που φανερώνουν την ταυτότητά του, όπως το Google ή το Facebook.

Πολλές φορές ο τρόπος με τον οποίο πλοηγείται ένας χρήστης στο διαδίκτυο είναι αρκετά χαρακτηριστικός. Κατά συνέπεια ο χρήστης δεν θα πρέπει να πλοηγείται με κάποιο συγκεκριμένο μοτίβο, διότι μπορεί να προδώσει την ταυτότητά του [**Πηγή 11 Κεφ4**].

Επιπλέον, αποτελεί ισχυρή σύσταση η απενεργοποίηση της JavaScript του TOR Browser. Με αυτό τον τρόπο μειώνεται δραματικά ο κώδικας των ιστοσελίδων που μπορεί να αναγνώσει το πρόγραμμα περιήγησης, προστατεύοντας τον χρήστη από πιθανά σφάλματα που μπορούν να ¨τρέξουν¨ εν αγνοία του.

Επιπρόσθετα, μία από τις πιο βασικές μεθόδους που αυξάνουν την ασφάλεια του χρήστη είναι η χρήση και η επίσκεψη ιστοσελίδων με την πρόθεση HTTPS (Hypertext Transfer Protocol Secure). Τέτοιου είδος ιστοσελίδες εξασφαλίζουν το απόρρητο των δεδομένων που αποστέλλονται μεταξύ του τελικού κόμβου (του δικτύου TOR) και του τελικού εξυπηρετητή [**Πηγή 11 Κεφ4**].

Επίσης, συνιστάται η συχνή ενημέρωση του προγράμματος TOR Browser [**Πηγή 11 Κεφ4**]. Συνήθως, τα προγράμματα που ανανεώνονται περιέχουν επεκτάσεις που έχουν αναπτυχθεί για να γίνονται πιο φιλικά, γρήγορα και ασφαλή για τους χρήστες.

Άλλη μία μέθοδος που προτείνεται, για την ενίσχυση της ασφάλειας κατά την πλοήγηση του χρήστη μέσω του TOR Browser, είναι η χρήση κάποιας υπηρεσίας VPN (Virtual Private Network). Με την χρήση μιας τέτοιας υπηρεσίας η διεύθυνση IP της

συσκευής αντικαθίσταται με μία άλλη, κάνοντας αδύνατο τον εντοπισμό της πραγματικής IP και κατ΄ επέκταση της συσκευής. Είναι σημαντικό η υπηρεσία VPN να εφαρμόζεται πριν την έναρξη του TOR Browser, έτσι ώστε η πραγματική διεύθυνση IP να αποκρύπτεται από όλο το διαδίκτυο αλλά και από το ίδιο το πρόγραμμα περιήγησης TOR.

Ακόμη, η ασφάλεια περιήγησης τόσο της συσκευής όσο και του χρήστη μπορεί να ενισχυθεί με την εγκατάσταση και την χρήση ενός VM (Virtual Machine). Χρησιμοποιώντας ένα VM είναι σαν να δημιουργούμε έναν επιπλέον υπολογιστή στην ήδη υπάρχουσα συσκευή και με αυτόν τον τρόπο μπορεί να πραγματοποιηθεί η περιήγηση μέσω του TOR Browser. Αυτό θα έχει σαν αποτέλεσμα, ότι αν ο χρήστης κατεβάσει ένα μολυσματικό λογισμικό εν αγνοία του ή κατά λάθος, η μόλυνση θα δεσμευτεί στο VM δίχως να επηρεάσει την λειτουργία της πραγματικής συσκευής.

Συνεχίζοντας, είναι σημαντικό οι χρήστες του TOR Browser να μην προβαίνουν στην λήψη αρχείων. Αυτό προτείνεται διότι όταν ανοίξουν το αρχείο που έχουν κατεβάσει στον υπολογιστή, ίσως χρειαστεί ένα επιπλέον πρόγραμμα για την ανάγνωσή του, όπως το Word του Microsoft Office, το Libre Office, το Adobe Acrobat κ.α. Αυτά τα προγράμματα είναι πιθανόν να συνδεθούν στο διαδίκτυο αποκαλύπτοντας την πραγματική IP διεύθυνση της συσκευής.

Ολοκληρώνοντας την υποενότητα αυτή, είναι θεμιτό ο χρήστης να διαθέτει στην συσκευή του κάποιο πρόγραμμα Antivirus. Το λογισμικό αυτό θα πρέπει να είναι εγκατεστημένο και ενεργό. Με αυτό τον τρόπο, σε περίπτωση που εγκατασταθεί στην συσκευή κάποιο κακόβουλο λογισμικό, ο χρήστης, να έχει την δυνατότητα να το περιορίσει ή να το διαγράψει.

4.6.7 Πλεονεκτήματα TOR Browser

Σε αυτή την υποενότητα θα αναφερθούν τα πλεονεκτήματα που διαθέτει ο TOR Browser. Αυτά είναι τα εξής:

- Πρόκειται για ένα λογισμικό ανοιχτού κώδικα ελεύθερο προς όλους για λήψη και εγκατάσταση. Επιπλέον, έχει αναπτυχθεί έτσι ώστε να είναι συμβατό με οποιοδήποτε λειτουργικό σύστημα, όπως Windows, Linux και Mac OS [**Πηγή 12 Κεφ4**].

- Προσφέρει στον χρήστη προστασία της ιδιωτικής ζωής κατά την περιήγηση του στο διαδίκτυο. Αυτό το πράττει με την κρυπτογράφηση των πληροφοριών και της διεύθυνσης IP του χρήστη, δίχως κάποιος να μπορεί να προσδιορίσει την πραγματική διεύθυνση IP [**Πηγή 13 Κεφ4**].

- Προωθεί την ελευθερία της έκφρασης [**Πηγή 12 Κεφ4**] δίχως αυτή να λογοκρίνεται και δίνει την δυνατότητα στον χρήστη να δημοσιεύσει ή/και να αναγνώσει ό,τι επιθυμεί.

- Επιτρέπει την πρόσβαση στο Deep Web, όπως κάθε συμβατικό πρόγραμμα περιήγησης.

- Επιτρέπει την πρόσβαση στο Dark Web και σε ιστοσελίδες με την κατάληξη .onion [**Πηγή 12 Κεφ4**]. Είναι σημαντικό να αναφερθεί ότι αυτές οι ιστοσελίδες υποστηρίζονται μόνο από τον TOR Browser.

- Επιτρέπει την πρόσβαση σε ιστοσελίδες που δεν έχουν ευρετηριαστεί στις γνωστές μηχανές αναζήτησης, όπως Google, Bing κ.α.

4.6.8 Μειονεκτήματα TOR Browser

Σε αυτή την υποενότητα θα αναφερθούν τα μειονεκτήματα που διαθέτει ο TOR Browser. Συγκεκριμένα είναι τα παρακάτω:

- Λόγω της δρομολόγησης τριών επιπέδων που χρησιμοποιείται από τον TOR Browser, η πλοήγησή του είναι αρκετά αργή [**Πηγή 12 Κεφ4**].

- Η εκκίνησή του TOR Browser, σε αντίθεση με τα συμβατικά προγράμματα περιήγησης, είναι αρκετά αργή [**Πηγή 12 Κεφ4**].

- Η αποστολή ή/και η λήψη μεγάλου όγκου αρχείων καθίσταται ως αδύνατη [**Πηγή 12 Κεφ4**].

- Η παρακολούθηση βίντεο ή ήχου μέσω του TOR Browser είναι αρκετά δύσκολη [**Πηγή 12 Κεφ4**]. Αυτό συμβαίνει διότι η επισκεψιμότητα κάθε χρήστη περνά από τρεις κόμβους μέχρι να φτάσει στον τελικό εξυπηρετητή μειώνοντας την ταχύτητα της σύνδεσης. Δυστυχώς αυτό δεν μπορεί να αποφθεχθεί παρά μόνο να βελτιωθεί, ως ένα βαθμό, με την χρήση μεγαλύτερης ταχύτητας Internet.

- Ο TOR Browser πολλές φορές χρησιμοποιείται για μία πληθώρα από εγκληματικές ενέργειες.

- Το interface του TOR Browser δεν είναι αρκετά φιλικό σε σύγκριση με τα παραδοσιακά προγράμματα περιήγησης [**Πηγή 12 Κεφ4**].

- Ο TOR Browser δεν είναι εντελώς ασφαλής [**Πηγή 12 Κεφ4**]. Αυτό συμβαίνει διότι ο τελευταίος κόμβος, που συνδέεται με τον τελικό εξυπηρετητή, αποστέλλει τις πληροφορίες αποκρυπτογραφημένες με αποτέλεσμα κάποιος τρίτος να μπορεί να τις παρακολουθεί.

- Δεν προστατεύει τον χρήστη σχετικά με το περιεχόμενο που θα παρακολουθήσει.

- Δεν προστατεύει τον χρήστη από την λήψη μολυσματικών λογισμικών, που μπορούν να βλάψουν την συσκευή του και κατ επέκταση τον ίδιο.

- Αρκετές ιστοσελίδες έχουν απαγορεύσει την πρόσβασή τους σε χρήστες που προσπαθούν να εισέλθουν σε αυτές, με την χρήση το TOR Browser [**Πηγή 13 Κεφ4**].

4.6.9 Αποδοτικότητα TOR Browser

Όπως έχει αναφερθεί και στα μειονεκτήματα, ο TOR Browser υστερεί σε θέματα απόδοσης. Η απόδοσή του διασπάται και αξιολογείται σε δύο μέρη. Το πρώτο αφορά την απόδοσή του κατά την εκκίνηση και το δεύτερο την απόδοσή του κατά την πλοήγηση.

Όσον αφορά την απόδοσή του κατά την εκκίνηση ο TOR Browser χρειάζεται αρκετό χρόνο, σε σύγκριση με τα συμβατικά προγράμματα περιήγησης (όπως Google Chrome, Mozilla Firefox, Microsoft Edge κ.α.). Αυτό οφείλεται στον χρόνο που απαιτεί το πρόγραμμα προκειμένου να φορτώσει το αρχείο που περιέχει τους διαθέσιμους κόμβους του δικτύου TOR.

Ομοίως, το κομμάτι που αφορά την αποδοτικότητα της περιήγησης, χρειάζεται και αυτό αρκετό χρόνο για να εμφανίσει στον χρήστη τα αποτελέσματα που επιθυμεί. Αυτό συμβαίνει διότι η πληροφορία πρέπει να κρυπτογραφηθεί και να διαπεραστεί από συνολικά τρεις κόμβους του δικτύου TOR για να φτάσει στον τελικό εξυπηρετητή, κάτι που αποδεικνύεται ως μία χρονοβόρα διεργασία.

4.6.10 Πρόσβαση στο Dark Web μέσω του TOR Browser

Η πρόσβαση στο Dark Web επιτρέπεται μόνο από συγκεκριμένα προγράμματα περιήγησης. Ο TOR Browser αποτελεί ένα από αυτά και επιτρέπει στους χρήστες του να πλοηγούνται στο Dark Web εξασφαλίζοντας την ανωνυμία τους.

Η ιδιαιτερότητα του Dark Web είναι ότι οι διευθύνσεις URL των ιστοσελίδων που περιέχονται σε αυτό δεν διαθέτουν μία από τις συνηθισμένες καταλήξεις που συναντώνται στο Surface Web, όπως οι καταλήξεις .com, .org, .gr και άλλες. Αντιθέτως, οι ιστοσελίδες έχουν κατάληξη .onion. Επιπλέον, οι διευθύνσεις των URL αυτών των ιστοσελίδων αποτελούνται από τυχαίες συμβολοσειρές χαρακτήρων και αριθμών που τροποποιούνται αρκετά συχνά, κάνοντας μη εφικτή την εύρεσή τους συνεχώς από τους χρήστες. Για αυτό τον λόγο υπάρχουν ιστότοποι στο Dark Web που βοηθούν την εύρεση ιστοσελίδων διαθέτοντας μία λίστα από αυτές. Τέτοιοι ιστότοποι είναι, ενδεικτικά, ο The Hidden Wiki και ο Daniel [**Πηγή 14 Κεφ4**].

4.6.11 Γιατί ξεχωρίζει ο TOR Browser

Ο TOR Browser είναι ένα πρόγραμμα περιήγησης που εξασφαλίζει στον χρήστη την ανωνυμία του κατά την περιήγησή του στο διαδίκτυο. Επιτρέπει τόσο την πρόσβαση στο Surface και στο Deep Web όσο και στο Dark Web. Ουσιαστικά πρόκειται για έναν browser που μπορεί να χρησιμοποιηθεί σε όλα τα επίπεδα του διαδικτύου. Αυτός είναι και ο κύριος λόγος που τον κάνει να ξεχωρίζει.

Επιπλέον, δίνοντας πρόσβαση στο Dark Web, δίχως αυτό να αποκαλύπτει σε τρίτους την ταυτότητα του χρήστη, προωθεί την ελευθερία του λόγου και περιθωριοποιεί την λογοκρισία. Πρόκειται για ένα μέσο το οποίο λειτουργεί ακτιβιστικά σε χώρες που ίσως υφίστανται αυστηρό καθεστώς, δίνοντας διέξοδο στους πολίτες.

Ο TOR Browser, συνεργάζεται εύκολα και με υπηρεσίες VPN. Αυτό σημαίνει ότι το πρόγραμμα περιήγησης TOR μπορεί να λειτουργήσει ακόμα και σε χώρες που έχουν καταργήσει την διανομή του και επιθυμούν τον περιορισμό της χρήσης του.

Εκτός, από την πρόσβαση στο Dark Web, προάγει και την επικοινωνία εντός αυτού μεταξύ των χρηστών, παρέχοντας ανωνυμία. Η επικοινωνία πραγματοποιείται με την μορφή E-Mail από ιστοτόπους που βρίσκονται εντός του Dark Web. Τέτοιοι είναι, ενδεικτικά, ο Mail2Tor, ο ProtonMail και ο CTemplar.

4.7 Freenet

Το Freenet κυκλοφόρησε το έτος 2000 και αποτελούσε έργο του φοιτητή Ian Clarke του πανεπιστημίου του Εδιμβούργου. Από τότε μέχρι και σήμερα συνεχίζει να αναπτύσσεται με σκοπό την ελεύθερη επικοινωνία, την διανομή πληροφοριών και τον περιορισμό της λογοκρισίας.

Το Freenet είναι ένα δωρεάν και ελεύθερο λογισμικό ανοιχτού κώδικα και είναι προσιτό σε όλους τους χρήστες, αρκεί οι ίδιοι να προβούν στην λήψη του και την εγκατάστασή του. Επιπλέον βασίζεται σε ένα συγκεκριμένο δίκτυο τερματικών, μεταξύ των οποίων ανταλλάσσονται οι πληροφορίες και με την χρήση αυτού καθίσταται αδύνατη η πρόσβαση στον παγκόσμιο ιστό. Επιπρόσθετα, προστατεύει τους χρήστες του, όσον αφορά την ανωνυμία τους, αφού οι πληροφορίες που μεταφέρονται μεταξύ των ίδιων κρυπτογραφούνται και δρομολογούνται μέσω άλλων κόμβων [**Πηγή 15 Κεφ4**].

Το δίκτυο και η λειτουργία του Freenet βασίζεται αποκλειστικά στους χρήστες του. Συγκεκριμένα, οι χρήστες δεσμεύουν και παρέχουν στο δίκτυο έναν συγκεκριμένο χώρο αποθήκευσης από τον σκληρό δίσκο που διαθέτει ο προσωπικός τους υπολογιστής. Αυτός ο χώρος χρησιμοποιείται από το δίκτυο για την αποθήκευση των αρχείων [**Πηγή 15 Κεφ4**]. Επιπλέον, προκειμένου να μην δεσμεύεται περιττός χώρος στο δίκτυο, τα αρχεία που διακινούνται λιγότερο εντός αυτού διαγράφονται αυτόματα δίνοντας την δυνατότητα να διακινούνται μόνο τα αρχεία που είναι δημοφιλή.

Είναι σημαντικό να αναφερθεί ότι ο χρήστης πλοηγείται σε ένα δίκτυο, το οποίο ανήκει στο Freenet και ότι οι ιστοσελίδες που υπάρχουν σε αυτό ονομάζονται freesites. Τα freesites με την σειρά τους είναι ιστοσελίδες αναπτυγμένες από χρήστες, σε HTML ή με παρόμοια εργαλεία και είναι προσβάσιμες μόνο μέσω του δικτύου Freenet. Κάθε freesite δεν αποθηκεύεται σε έναν εξυπηρετητή του παγκόσμιου ιστού αλλά σε έναν κόμβο του δικτύου Freenet. Επομένως, γίνεται σαφές ότι για να αναζητηθεί μία πληροφορία πρέπει πρώτα να έχει πραγματοποιηθεί η εισαγωγή της στο δίκτυο.

Ολοκληρώνοντας αυτήν την υποενότητα, γίνεται αντιληπτό ότι η χρήση του Freenet απαιτεί από τους χρήστες να διαθέσουν ένα μέρος από τον αποθηκευτικό χώρο της

συσκευής τους. Είναι ένα λογισμικό που δίνει την δυνατότητα πρόσβασης σε ένα κατανεμημένο δίκτυο υπολογιστών και όχι στον παγκόσμιο ιστό παρέχοντας στους χρήστες ανωνυμία κατά την περιήγησή τους. Ακόμη, οι πληροφορίες που διακινούνται εντός του δικτύου ανταλλάσσονται μεταξύ των κόμβων που συμμετέχουν σε αυτό. Πρόκειται ουσιαστικά για ένα P2P (peer to peer) δίκτυο κοινής χρήσης αρχείων, όπου οι πληροφορίες που αναζητά ένας χρήστης δρομολογούνται και ανταλλάσσονται από κόμβο σε κόμβο του δικτύου μέχρι τον τελικό χρήστη.

Επιπλέον, στο δίκτυο Freenet ανάμεσα από τον χρήστη και τον τελικό εξυπηρετητή που θα μεταδώσει τις πληροφορίες που επιθυμεί ο πρώτος, μεσολαβούν αρκετοί επιπλέον εξυπηρετητές, όπου τα στοιχεία κρυπτογραφούνται και μεταφέρονται μεταξύ τους και κάθε κόμβος γνωρίζει μόνο τον επόμενο και προηγούμενο κόμβο που θα μεταδώσει και του μετέδωσε, αντίστοιχα, τις πληροφορίες δίχως να γνωρίζει ολόκληρη την διαδρομή που ακολουθήθηκε.

4.8 Εγκλήματα που εξιχνιάστηκαν μέσω του Dark Web

Το Dark Web, το οποίο αποτελεί ένα υποσύνολο του Deep Web, αναπτύχθηκε προκειμένου να προάγει το ισχυρότερο πλεονέκτημα της δημοκρατίας, δηλαδή αυτό της ελευθερίας του λόγου. Αυτό το επιτυγχάνει, με την χρήση του δικτύου TOR και με αντίστοιχα προγράμματα περιήγησης, όπως ο TOR Browser, τα οποία συνεργάζονται με τέτοιο τρόπο έτσι ώστε να παρέχεται στους χρήστες η απόκρυψη των στοιχείων τους. Πολλοί, όμως, εκμεταλλευόμενοι την ανωνυμία που τους εξασφαλίζει, χρησιμοποιούν το Dark Web ως ένα μέσο επίτευξης εγκληματικών ενεργειών. Σε αυτή την ενότητα θα αναφερθούν περιπτώσεις που το Dark Web χρησιμοποιήθηκε για παράνομες ενέργειες και με την βοήθεια του ίδιου εξακριβώθηκαν.

-No Fun Limits

Το No Fun Limits ήταν ένας από τους πιο γνωστούς ιστότοπους που εμπεριέχονταν στο Dark Web. Εντός αυτού διακινούνταν υλικό με περιεχόμενο τον βασανισμό και την σεξουαλική κακοποίηση ανήλικων παιδιών. Η παρακολούθηση αυτού του υλικού ήταν αρκετά σκληρή και φρικτή για οποιοδήποτε φυσιολογικό άνθρωπο.

Ο Peter Scully, ήταν ένας άνθρωπος με καταγωγή από την Αυστραλία όπου αργότερα μετανάστευσε στις Φιλιππίνες και εκεί δημιούργησε ένα κύκλωμα οπτικοακουστικού υλικού με τον βιασμό και την κακοποίηση ανήλικων παιδιών. Συγκεκριμένα, ο ίδιος προσέλκυε οικονομικά αδύναμες οικογένειες με παιδιά στις οποίες υπόσχονταν ότι τα τέκνα τους θα μεγαλώσουν μαζί του, με ασφάλεια παρέχοντάς τους μια φυσιολογική ζωή με εκπαίδευση και υγειονομική περίθαλψη [**Πηγή 16 Κεφ4**]. Αφού κατάφερνε να πείσει τις οικογένειες, τα παιδιά μεγάλωναν μαζί του και ήταν έρμαια των διαστροφικών του επιθυμιών.

Ο Peter Scully εκτός από την σεξουαλική κακοποίηση που διέπραττε, ασκούσε και βασανισμούς όπου πολλές φορές έφταναν και στον θάνατο των ανυπεράσπιστων παιδιών, βιντεοσκοπώντας τις πράξεις του. Εν συνεχεία, το οπτικοακουστικό υλικό που δημιουργούσε το διέθετε στο Dark Web και συγκεκριμένα στον ιστότοπο No Fun Limits έναντι αμοιβής. Η πιο ανατριχιαστική σειρά με βίντεο που διέθετε ήταν αυτή με το όνομα ¨Daisy's Destruction¨ (η καταστροφή της Daisy) και αφορούσε τον βιασμό και την κακοποίηση ενός κοριτσιού που τελικά κατέληξε στον θάνατο λόγω του βασανισμού. Αξίζει να σημειωθεί ότι ο Peter Scully στραγγάλισε ένα κορίτσι, ηλικίας 11 ετών και έθαψε το άψυχο σώμα του στην οικία του [**Πηγή 16 Κεφ4**].

Στην συνέχεια των παραπάνω, ένας άλλος παιδόφιλος που ονομάζονταν Matthew David Grahm, διατηρούσε και ο ίδιος έναν ιστότοπο με περιεχόμενο παρόμοιο του Peter Scully, ο οποίος αναδημοσίευσε ένα βίντεο του Scully στην ιστοσελίδα του. Οι αστυνομικές αρχές, που ερευνούσαν το Dark Web για τον εντοπισμό εγκληματιών, διαπίστωσαν ότι στα βίντεο υπήρχαν αποσπάσματα από άνθρωπο που μιλούσε με άπταιστη Αυστραλιανή προφορά. Έπειτα, παρακολουθώντας τα βίντεο συγκέντρωσαν αρκετά στοιχεία που ενοχοποίησαν τους δύο παραπάνω δράστες καταδικάζοντάς τους σε ποινή φυλάκισης.

-Shannon Grant McCoole

Μία ακόμη υπόθεση παρόμοια με αυτή του Peter Scully και του Matthew David Grahm είναι αυτή του Shannon Grant McCoole. Ο Shannon Grant McCoole ήταν εργαζόμενος σε μία υπηρεσία η οποία αφορούσε την παιδική προστασία.

Ο Shannon Grant McCoole δημιούργησε μία πλατφόρμα αναπαραγωγής οπτικοακουστικού υλικού με περιεχόμενο την σεξουαλική κακοποίηση παιδιών, προάγοντας την παιδική πορνογραφία. Ουσιαστικά, ο ιστότοπος παρουσίαζε εικόνες και βίντεο σεξουαλικού περιεχομένου με εμπλεκόμενους τον ίδιο και ανήλικα παιδιά.

Οι αστυνομικές αρχές που αναζητούσαν εγκληματίες μέσω του Dark Web ανέλυσαν μία πληθώρα από βίντεο και φωτογραφίες που εμπεριέχονταν στον ιστότοπο με αποτέλεσμα τα ευρήματα να καταλήξουν στον Shannon Grant McCoole. Ακολούθως της παραπάνω έρευνας κατασχέθηκε ο ηλεκτρονικός υπολογιστής του Shannon Grant McCoole στον οποίο εντοπίστηκε πορνογραφικό υλικό όπου και αναγκάστηκε να ομολογήσει τις πράξεις του και να καταδικαστεί σε ποινή φυλάκισης [**Πηγή 17 Κεφ4**].

-Hieu Minh Ngo

Ο Hien Minh Ngo ήταν ένας άνθρωπος με καταγωγή από το Βιετνάμ που διατηρούσε δύο ιστότοπους στο Dark Web, μέσω των οποίων πωλούσε προσωπικά δεδομένα χρηστών και πολιτών. Συγκεκριμένα ασχολούνταν με κυβερνοεπιθέσεις, ανιχνεύοντας τις ευπάθειες των συστημάτων και στην συνέχεια επιτίθονταν σε αυτές. Ο Hien Minh Ngo χάκαρε τις βάσεις δεδομένων από οργανισμούς και επιχειρήσεις με σκοπό να αντλεί δεδομένα προσωπικού χαρακτήρα. Τέτοια είναι τα ονόματα πολιτών και χρηστών, αριθμοί κοινωνικής ασφάλισης και πληροφορίες που αντιστοιχούσαν σε τραπεζικούς λογαριασμούς. Αφού αποκτούσε αυτά τα δεδομένα, τα διέθετε έναντι αμοιβής στο Dark Web. Επιπλέον, φημολογείται ότι κατάφερε να αποσπάσει δεδομένα περισσότερων από διακοσίων (200) εκατομμυρίων πολιτών [**Πηγή 18 Κεφ4**].

Το έτος 2013, ο Hieu Minh Ngo ταξίδεψε στις ΗΠΑ με την πεποίθηση ότι θα παραλάμβανε προσωπικά δεδομένα από έναν συγκεκριμένο άνθρωπο με τον οποίο είχε επικοινωνήσει, με σκοπό να τα πουλήσει στο Dark Web. Στην πραγματικότητα αυτός ο άνθρωπος είχε τοποθετηθεί από τις μυστικές υπηρεσίες των ΗΠΑ με αποτέλεσμα να συλληφθεί [**Πηγή 18 Κεφ4**]. Στην συνέχεια καταδικάστηκε σε ποινή φυλάκισης και ακολούθησε η διακοπή της λειτουργίας των ιστοτόπων που διατηρούσε στο Dark Web.

-Silk Road

Τον Φεβρουάριο του 2011 δημιουργήθηκε ένας ιστότοπος από τον Ross Ulbricht με το όνομα Silk Road, ο οποίος δραστηριοποιούνταν στο Dark Web. Εντός αυτού διακινούνταν προϊόντα και υπηρεσίες οι οποίες είχαν παράνομο και εγκληματικό χαρακτήρα.

Πιο συγκεκριμένα, ο Ross Ulbricht ανέπτυξε έναν ιστότοπο με όνομα Silk Road στον οποίο οι χρήστες μπορούσαν να πουλήσουν ή να αγοράσουν παράνομα προϊόντα και υπηρεσίες. Ουσιαστικά ο Silk Road αποτελούσε έναν μεσολαβητή ανάμεσα στον πωλητή και τον πελάτη, χρεώνοντας μια προμήθεια κατά την πληρωμή. Η περιήγηση στον ιστότοπο γινόταν με την χρήση του δικτύου TOR και ήταν αρκετά απλή και φιλική για τους χρήστες κάτι το οποίο αποτέλεσε ένας από τους κύριους λόγους που τον έκαναν διάσημο. Επιπλέον, μερικά από τα προϊόντα και τις υπηρεσίας που μπορούσε κάποιος να αγοράσει μέσω του Silk Road ενδεικτικά, ήταν ναρκωτικά, όπλα, πλαστά συμβόλαια, διαβατήρια, διπλώματα οδήγησης, παράνομα χάπια καθώς επίσης να προσλάβει hacker ή να αναθέσει και συμβόλαια θανάτου.

Όλη αυτή η εγκληματική δραστηριότητα, παρακίνησε τις αστυνομικές αρχές να ξεκινήσουν έρευνες για τον εντοπισμό και την σύλληψη του ιδιοκτήτη με σκοπό την διακοπή της λειτουργίας του παράνομο ιστοτόπου. Οι αρχές χρειάστηκαν περίπου δύο έτη για να κατορθώσουν την παύση της λειτουργίας του Silk Road και να συλλάβουν τον ιδιοκτήτη. Όλο αυτό το χρονικό διάστημα είχαν συλλέξει αρκετές πληροφορίες και είχαν καταφέρει να συλλάβουν αρκετούς από τους αγοραστές και πωλητές του ιστοτόπου, παρέχοντας οι τελευταίοι πληροφορίες σχετικά με τον τρόπο λειτουργίας του. Τελικά, οι

αρχές, παριστάνοντας τους πωλητές στην πλατφόρμα, απόκτησαν επικοινωνία με τον Ross Ulbricht. Αφού είχαν λάβει αρκετές πληροφορίες οι αστυνομικές αρχές συνέλαβαν τον ιδιοκτήτη του Silk Road τον Οκτώβριο του έτους 2013 και του απαγγέλθηκαν αρκετές κατηγορίες, όπως πειρατεία υπολογιστών, διακίνηση ναρκωτικών και απόπειρες δολοφονίας [**Πηγή 19 Κεφ4**] και καταδικάστηκε σε ποινή φυλάκισης. Η σύλληψή του έγινε στην βιβλιοθήκη Glen Park στο San Francisco [**Πηγή 19 Κεφ4**], όπου οι αστυνομικές αρχές συνέλαβαν τον Ross Ulbricht επ΄ αυτοφώρω την στιγμή που συνδέονταν στην ιστοσελίδα του στο Dark Web.

-Sheep Marketplace

Έπειτα της διακοπής της λειτουργίας του Silk Road και της σύλληψης του Ross Ulbricht, αναπτύχθηκε άλλος ένας ιστότοπος με το όνομα Sheep Marketplace. Συγκεκριμένα, το Sheep Marketplace δημιουργήθηκε τον Μάρτιο του 2013 όπου πωλούνταν παράνομα προϊόντα, κυρίως ναρκωτικά και η λειτουργία του ήταν παρόμοια με αυτή του Silk Road. Αυτός ο ιστότοπος κέρδισε αρκετά μεγάλη δημοσιότητα διότι θεωρούνταν η συνέχιση του Silk Road.

Τον Δεκέμβριο του 2013 ο ιστότοπος έπαψε να εξυπηρετεί τους χρήστες και τέθηκε εκτός λειτουργίας, με την αιτιολογία ότι κάποιος από τους πωλητές κατάφερε να εκμεταλλευτεί μία ευπάθεια λογισμικού που αφορούσε το κομμάτι των συναλλαγών, αποσπώντας ένα αρκετά μεγάλο ποσό σε μορφή κρυπτονομισμάτων. Ωστόσο, οι αστυνομικές αρχές, έπειτα και από την παύση της λειτουργίας του, συνέχισαν να πραγματοποιούν έρευνα για τον εντοπισμό του ιδιοκτήτη του ιστοτόπου με σκοπό την παύση της λειτουργίας του και την σύλληψη του.

Οι αρχές κατευθύνθηκαν σε έναν άνδρα με όνομα Thomas Jirlkovsky, ο οποίος ταυτοποιήθηκε από την σελίδα του στο Facebook [**Πηγή 20 Κεφ4**]. Ο άνδρας αρνούνταν την συμμετοχή του στον ιστότοπο Sheep Marketplace με αποτέλεσμα οι έρευνες να συνεχίζονται μέχρι οι υποψίες να επιβεβαιωθούν. Στην συνέχεια οι έρευνες στράφηκαν στην συζύγό του Thomas Jirlkovsky, που είχε παρατηρηθεί αύξηση του τραπεζικού λογαριασμού της με ποσό το οποίο προερχόταν από κρυπτονομίσματα, δίχως η ίδια να

μπορεί να το δικαιολογήσει. Ολοκληρώνοντας τις έρευνες, οι αρχές διαπίστωσαν ότι τα χρήματα αυτά προέρχονταν από την υποτιθέμενη κλοπή που είχε πραγματοποιηθεί στον ιστότοπο Sheep Marketplace από έναν πωλητή, όπου τελικά απεδείχθη ότι την διέπραξε ο ίδιος ο ιδιοκτήτης Thomas Jirlkovsky. Καταλυτικό ρόλο στην υπόθεση είχε η πληροφορία, για αγορά ενός ακριβού σπιτιού, του οποίου η αγοροπωλησία πραγματοποιήθηκε με κρυπτονομίσματα και τελικά διαπιστώθηκε ότι είχε αγοραστεί από τον Thomas Jirlkovsky, με τα κρυπτονομίσματα που είχαν κλαπεί.

4.9 Bitcoin και Dark Web

Αυτή η ενότητα του κεφαλαίου αφορά την σχέση μεταξύ του Dark Web και των κρυπτονομισμάτων. Συγκεκριμένα θα αναφερθεί το αντίτιμο με το οποίο πραγματοποιούνται οι συναλλαγές κατά την αγορά προϊόντων ή/και υπηρεσιών στο Dark Web, καθώς επίσης θα δοθεί και η αιτιολογία που συμβαίνει αυτό.

Κάθε χρήστης κατά την περιήγηση του στο Dark Web θα διαπιστώσει ότι το αντίτιμο για την αγορά μίας υπηρεσίες ή/και προϊόντος δεν είναι ένα από τα συνηθισμένα νομίσματα όπως το δολάριο ($) ή το ευρώ (€). Αντιθέτως θα αντιληφθεί ότι η πραγματοποίηση μίας συναλλαγής γίνεται με την χρήση κρυπτονομισμάτων. Το πιο δημοφιλές κρυπτονόμισμα που χρησιμοποιείται είναι το BitCoin.

Το Bitcoin είναι ένα ψηφιακό νόμισμα αποτελούμενο από ένα σύνολο πρωτοκόλλων και διαδικασιών [**Πηγή 21 Κεφ4**]. Φημολογείται ότι είναι το πιο επιτυχημένο ψηφιακό νόμισμα στο χώρο των κρυπτονομισμάτων λόγω της έντονης δημοτικότητάς του και της αξίας του, αφού μόλις ένα bitcoin ισοδυναμεί με αρκετά χιλιάδες δολάρια. Επιπλέον, χρησιμοποιεί δικλείδες ασφαλείας και σε συνδυασμό με την τεχνολογία Blockchain που εφαρμόζεται για την διεκπεραίωση μίας συναλλαγής κρίνεται ως ασφαλές. Επιπρόσθετα, με την τεχνολογία Blockchain οι συναλλαγές κρυπτογραφούνται και δεν είναι διαθέσιμες σε τρίτους, δηλαδή με λίγα λόγια κρίνεται χρήσιμο για ανώνυμες συναλλαγές.

Ο κύριος λόγος που χρησιμοποιείται το Dark Web, από τους χρήστες, είναι η δυνατότητα εξασφάλισης της ανωνυμίας τους. Για αυτό τον λόγο, κατά την πραγματοποίηση μίας ηλεκτρονικής συναλλαγής στο Dark Web δεν μπορεί να χρησιμοποιηθεί ο λογαριασμός μία τράπεζας, διότι η τράπεζα θα είναι σε θέση να γνωρίζει ποιός πελάτης απέστειλε χρήματα και ποιός πωλητής τα παρέλαβε, με αποτέλεσμα να μπορεί να διοχετεύσει πληροφορίες στην εκάστοτε κυβέρνηση με σκοπό οι αρχές να προβούν στην παρακολούθησή τους. Επομένως γίνεται ξεκάθαρο ότι αν πραγματοποιηθεί μία αγοροπωλησία στο Dark Web με την χρήση μίας τράπεζας, παύει πλέον να ισχύει η ανωνυμία του, διότι παρέχει στην τράπεζα πληροφορίες σχετικά με την συναλλαγή.

Για τον προαναφερθέντα λόγο, οι πωλητές που δραστηριοποιούνται στο Dark Web αναζητώντας διέξοδο έτσι ώστε οι συναλλαγές που πραγματοποιούνται μεταξύ των πελατών τους να παραμένουν ανώνυμες, κατέληξαν στην υιοθέτηση των κρυπτονομισμάτων και συγκεκριμένα του Bitcoin. Επομένως, με την χρήση του Dark Web και την εφαρμογή του Bitcoin για την διεκπεραίωση των συναλλαγών, οι αγοραστές και οι προμηθευτές θα διατηρούσαν ανώνυμο προφίλ κατά την περιήγησή τους και κατά την αγοροπωλησία προϊόντων ή/και υπηρεσιών.

Κλείνοντας αυτή την ενότητα, είναι σημαντικό να αναφερθεί ότι το Bitcoin έχει πράγματι αρκετά μεγάλη αξία αλλά αυτό είναι κάτι που διακυμαίνεται με την πάροδο του χρόνου. Ουσιαστικά η αξία του δεν είναι σταθερή με αποτέλεσμα να αυξάνεται και να μειώνεται συνεχώς, με μεγάλες διακυμάνσεις. Αυτό δημιουργεί προβλήματα στους προμηθευτές διότι θα πρέπει να προσδιορίζουν την τιμή των αγαθών τους με την ισοτιμία του Bitcoin. Για αυτό τον λόγο οι πωλητές του Dark Web έχουν διαφύγει στην χρήση άλλων κρυπτονομισμάτων που έχουν και αυτά διακυμάνσεις αλλά σαφώς μικρότερες.

4.10 Δημοφιλής επωνυμίες στο Dark Web

Σε αυτή την ενότητα θα αναφερθούν εταιρίες και ιστοσελίδες που είναι δημοφιλής στο Surface Web και δραστηριοποιούνται και στο Dark Web και είναι αρκετά αναγνωρισμένες.

Κάποιες από τις δημοφιλής εταιρίες και ειδησεογραφικές ιστοσελίδες, που εδρεύουν στο Surface Web διαθέτουν και εκδόσεις διαθέσιμες για το Dark Web. Στόχο έχουν την παράκαμψη της λογοκρισίας και τους περιορισμούς που έχουν τεθεί από τις εκάστοτε αυταρχικές και μη κυβερνήσεις των κρατών με σκοπό την ανάδειξη της αλήθειας και της επικοινωνίας μεταξύ των πολιτών. Μερικές από αυτές είναι:

- Το δημοφιλές μέσο κοινωνικής δικτύωσης Facebook
- Η γνωστή ειδησεογραφική ιστοσελίδα των New York Times [**Πηγή 14 Κεφ4**]
- Το διεθνές δίκτυο ενημέρωσης BBC News [**Πηγή 14 Κεφ4**]
- Το εδραιωμένο μέσο κοινωνικής δικτύωσης Twitter, το οποίο προώθησε την έκδοση του στο Dark Web έπειτα της απαγόρευσης του στην Ρωσία [**Πηγή 22 Κεφ4**] και την έναρξη του πολέμου μεταξύ της Ρωσίας και της Ουκρανίας κατά τον Φεβρουάριο 2022.

Επιπλέον, γνωστοί πάροχοι που δραστηριοποιούνται στο Dark Web, προσφέρουν την ανώνυμη επικοινωνία μεταξύ των χρηστών με την μορφή του ηλεκτρονικού ταχυδρομείου. Είναι σημαντικό να αναφερθεί ότι η πρόσβαση σε αυτές τις υπηρεσίες γίνεται μέσω του δικτύου TOR και του προγράμματος TOR Browser. Μερικές από αυτές είναι οι παρακάτω υπηρεσίες ηλεκτρονικού ταχυδρομείου (e-mail):

- Mail2Tor [**Πηγή 14 Κεφ4**]
- ProtonMail [**Πηγή 14 Κεφ4**]
- CTemplar [**Πηγή 14 Κεφ4**]

Επιπρόσθετα, στο Dark Web υπάρχουν πάροχοι που διαθέτουν στους χρήστες τους υπηρεσίες Cloud. Τέτοιες υπηρεσίες είναι το ανέβασμα (upload) και η αποθήκευση

αρχείων καθώς επίσης και ο διαμοιρασμός των αρχείων αυτών μεταξύ των χρηστών. Μερικοί από αυτούς είναι οι:

- MegaTor [**Πηγή 14 Κεφ4**]
- SecureDrop [**Πηγή 14 Κεφ4**]
- BlackCloud [**Πηγή 14 Κεφ4**]

Ολοκληρώνοντας αυτή την ενότητα γίνεται σαφές ότι στο Dark Web διατίθενται αρκετές βασικές υπηρεσίες και λειτουργίες που υπάρχουν και στο Surface Web. Αυτές είναι η ειδησεογραφία, η επικοινωνία μεταξύ των ανθρώπων, η ενημέρωση και οι λειτουργίες Cloud.

4.11 Η εξέλιξη του Dark Web

Όπως έχει αναφερθεί, ήδη, το Dark Web αναπτύχθηκε με στόχο να προασπίζεται την ανωνυμία των χρηστών που πλοηγούνται σε αυτό, με σκοπό την καταπολέμηση της λογοκρισίας που υφίσταται σε πολλές χώρες στον κόσμο. Χρησιμοποιείται ως ένα ακτιβιστικό μέσο, δίνοντας την δυνατότητα σε ανθρώπους που διώκονται από τις εκάστοτε κυβερνήσεις να ανακτήσουν την ελευθερία του λόγου τους. Επιπλέον, δίνει την δυνατότητα σε ανθρώπους που καταπιέζονται ή φοβούνται να μοιραστούν και να δημοσιεύσουν αντίθετες ή ακόμα και κακόβουλες πληροφορίες που μπορούν να βλάψουν τις κυβερνήσεις, να κάνουν χρήση της ανωνυμίας που τους προσφέρει το Dark Web δίχως να φοβούνται για την αποκάλυψη της ταυτότητας τους ή την δίωξή τους.

Παρά το γεγονός, ότι η δημιουργία και η χρήση του Dark Web προορίζονταν για την καταπολέμηση της λογοκρισίας και αναπτύχθηκε με τέτοιο τρόπο, έτσι ώστε να προάγει δημοκρατικά στοιχεία, είναι πολλοί που χρησιμοποιούν το Dark Web ως ένα δίκτυο για την διάπραξη πολλών αδικημάτων. Αυτό συμβαίνει, διότι οι εγκληματίες εκμεταλλευόμενοι την ανωνυμία που τους προσφέρει το Dark Web, καθίσταται αδύνατη η παρακολούθησή, η δίωξη και η σύλληψη τους. Δυστυχώς ο περιορισμός αυτών των εγκληματικών πράξεων δεν είναι εφικτός και δεν μπορεί να περιοριστεί ούτε από τις

αστυνομικές αρχές αλλά ούτε και από τους μη κερδοσκοπικούς οργανισμούς που έχουν αναλάβει την εξέλιξή του.

Ως αποτέλεσμα όλων των παραπάνω, οι διώξεις ηλεκτρονικών εγκλημάτων καταβάλλουν μεγάλες προσπάθειες για τον περιορισμό της χρήσης του Dark Web αποσκοπώντας στην παύση των εγκληματικών ενεργειών που διενεργούνται εντός του. Επιπλέον, σύμμαχοι σε αυτές τις προσπάθειες είναι οι εκάστοτε κυβερνήσεις που στοχεύουν στον περιορισμό της ελευθερίας του λόγου, με απώτερο σκοπό οι ίδιες να καθορίζουν το υλικό που θα διοχετεύεται στους χρήστες, στερώντας τις ελευθερίες και αποκρύπτοντας αλήθειες.

Το μέλλον του Dark Web είναι πραγματικά αβέβαιο διότι καταπολεμάται συνεχώς η χρήση του και περιορίζεται όλο και περισσότερο η πρόσβασή του σε πολλές χώρες. Από την άλλη βέβαια θα συνεχίσει να υποστηρίζει και να πρεσβεύει τους λόγους για τους οποίους αναπτύχθηκε. Είναι σίγουρο ότι όσο είναι υπαρκτό, θα δίνει την δυνατότητα στους ανθρώπους να διατηρούν την ανωνυμία κατά την περιήγησή τους και να τους ενθαρρύνει να δημοσιεύουν και να διαμοιράζονται ανησυχίες και γεγονότα μεταξύ τους.

Συμπερασματικά, θα συνεχίσει να καταπολεμά την λογοκρισία και να προάγει την ελευθερία της έκφρασης και του λόγου καθώς επίσης και να δίνει την δυνατότητα σε καταπιεσμένους ανθρώπους να δημοσιεύουν γεγονότα δίχως κανέναν περιορισμό και φόβο.

ΣΥΝΟΨΗ

Ολοκληρώνοντας, γίνεται αντιληπτό ότι η ασφάλεια των υπολογιστών είναι μία από τις σημαντικότερες παραμέτρους που πρέπει να ληφθούν υπόψιν από την πλευρά των χρηστών. Αποτελεί θεμέλιο της προστασίας τόσο της συσκευής τους όσο και των

δεδομένων που περιέχονται σε αυτήν και επιτυγχάνεται κυρίως με αντίστοιχα προγράμματα (Antivirus). Πριν την επιλογή του κατάλληλου προγράμματος είναι σωστό να γίνεται εκτίμηση και να επιλέγεται αυτό που προσφέρει την μεγαλύτερη αποτελεσματικότητα. Η έλλειψη της ασφάλειας μπορεί να επηρεάσει αρνητικά τους χρήστες, εκθέτοντας τους ίδιους ή ακόμη και να τους ζημιώσει οικονομικά και ηθικά. Επιπλέον, δεν αρκεί μόνο η προσπάθεια των χρηστών για να επιτευχθεί αλλά προϋποθέτει και την ενεργοποίση του κράτους και των αρμόδιων φορέων.

Επιπρόσθετα, ένας χρήστης μπορεί να αναζητήσει βοήθεια και συμβουλές σε ένα forum. Το forum πρέπει να είναι αξιόπιστο με συγκεκριμένη θεματολογία και να τηρεί την διαφάνεια. Επιπλέον, είναι σκόπιμο να αποτελείται από επόπτες που εφαρμόζουν τις πολιτικές που υιοθετεί το forum και οι διαχειριστές αυτού να είναι δεκτικοί και ανοιχτοί σε νέες ιδέες, λαμβάνοντας αποφάσεις που ικανοποιούν όσο το δυνατόν περισσότερους χρήστες. Με βάση τα παραπάνω ένα forum έχει θέσει τις βάσεις που το καθιστούν αξιόπιστο, έμπιστο και εξειδικευμένο.

Επιπλέον, το Dark Web είναι ένα μέρος του διαδικτύου που χρήζει μεγάλης προσοχής. Έχει πραγματικά να προσφέρει στους χρήστες πλεονεκτήματα αλλά ενέχει και αρκετούς κινδύνους. Ένα από τα κύρια πλεονεκτήματα που διαθέτει είναι αυτό της ελευθερίας του λόγου, ενώ ένα από τα κύρια μειονεκτήματα είναι ότι δεν προστατεύει το χρήστη, τόσο από την ασφάλεια του ίδιου όσο και από το περιεχόμενο που πιθανώς θα παρακολουθήσει.

Εν κατακλείδι, όπως έχει αναφερθεί στα προηγούμενα κεφάλαια, οι χρήστες του διαδικτύου πρέπει να είναι ιδιαίτερα προσεκτικοί ακόμη και στην περίπτωση που διαθέτουν κάποιο αντιιικό πρόγραμμα στον υπολογιστή τους. Αυτό διότι δεν υπάρχει κανένα πρόγραμμα που να διαβεβαιώνει ή να εξασφαλίζει στην πράξη την πλήρη προστασία των χρηστών. Όλα αυτά τα προγράμματα αποδίδουν έως ένα ποσοστό της αποτελεσματικότητά τους.

ΠΗΓΕΣ

Πηγές κεφαλαίου 1

1) https://asfalos-diplasas.gr/ti-einai-asfaleia/ **Τι είναι η ασφάλεια; και πως μπορώ να την αποκτήσω**
2) https://protectionplus.gr/%CE%BA%CE%AF%CE%BD%CE%B4%CF%85%CE%BD%CE%BF%CE%B9-%CE%BA%CE%B1%CE%B9-%CE%BA%CE%B1%CE%BD%CF%8C%CE%BD%CE%B5%CF%82-%CE%B1%CF%83%CF%86%CE%B1%CE%BB%CE%B5%CE%AF%CE%B1%CF%82-%CF%83%CF%84%CE%BF-%CE%B4%CE%B9/ **Κίνδυνοι και κανόνες ασφαλείας στο διαδίκτυο**
3) https://www.ijicc.net/images/vol_13/Iss_7/13755_Zeebaree_2020_E_R.pdf **Social Media Networks Security Threats, Risks and Recommendation: A Case Study in the Kurdistan Region**
4) https://www.vipre.com/resource/what-is-a-worm-virus/ **What Is A Worm Virus?**
5) https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html / **What is a Trojan? Is it a virus or is it malware?**
6) https://www.trellix.com/en-us/security-awareness/ransomware/what-is-ransomware.html **What is Ransomware?**
7) https://www.avast.com/c-rootkit#:~:text=A%20rootkit%20is%20a%20malicious,manipulate%20it%2C%20and%20steal%20data**. What is rootkit?**
8) https://www.bullguard.com/bullguard-security-center/pc-security/computer-threats/rogue-malware.aspx **Rogue malware infections - what you need to know – BullGuard**
9) https://www.techtarget.com/searchsecurity/definition/spyware **Spyware**
10) https://home.sophos.com/en-us/security-news/2019/what-is-a-keylogger **Demystifying a Keylogger-How They Monitor What Toy Type and What You Can Do About It?**
11) https://sites.google.com/site/egklhma/tropoi-antimetopises---symboules **Τρόποι αντιμετώπισης και συμβουλές**

Πηγές κεφαλαίου 2

1) https://www.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds#:~:text=The%20Brain%20Boot%20Sector%20Virus,a%20computer%20store%20in%20Pakistan. **A Brief History of Computer Viruses & What the Future Holds**
2) https://www.thepcinsider.com/who-invented-antivirus-history-timeline-evolution/ **Who Invented the Antivirus? A History of Antivirus Software.**

3) https://home.sophos.com/en-us/security-news/2020/what-is-a-signature **What are Signatures and How Does Signature-Based Detection Work?**
4) https://www.kaspersky.com/enterprise-security/wiki-section/products/behavior-based-protection **Behavior-Based Protection**
5) https://usa.kaspersky.com/resource-center/definitions/heuristic-analysis **What is Heuristic Analysis?**
6) https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-sandboxing/ **What is Sandboxing?**
7) https://www.techopedia.com/definition/4290/host-based-intrusion-prevention-system-hips#:~:text=A%20host%2Dbased%20intrusion%20prevention%20system%20(HIPS)%20is%20a,known%20and%20unknown%20malicious%20attacks. **Host-Based Intrusion Prevention System (HIPS)**
8) https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-protection-overview?view=o365-worldwide **Web Protection**
9) https://www.petervanderwoude.nl/post/working-with-exploit-protection-to-protect-devices-from-being-exploited/ **Working with Exploit Protection to protect devices from being exploited**
10) https://www.netskope.com/security-defined/what-is-zero-trust **What is Zero Trust?**
11) https://citrixready.citrix.com/content/dam/ready/partners/ap/appguard-inc/appguard/appguard-general-datasheet-brochures.pdf **Disrupt Malware Before it Does Damage**

Πηγές κεφαλαίου 3

1) https://www.reddit.com/r/ModeratorManifesto/comments/1yiyv2/hansjens47s_moderator_manifesto/
2) https://www.reddit.com/r/TheoryOfReddit/comments/3w4dld/incentives_to_help_build_trust_managing_trust/
3) https://www.redditinc.com/policies/moderator-guidelines?utm_source=reddit&utm_medium=usertext&utm_name=modhelp&utm_content=t5_2qy7w **Moderator Guidelines for Healthy Communities**
4) https://mods.reddithelp.com/hc/en-us/articles/360017854072-Recruiting-new-moderators **Recruiting new moderators**
5) https://psd.ca.uky.edu/files/moderate.pdf **TIPS FOR COMMUNITY FORUM MODERATORS**
6) http://repository.library.teiwest.gr/xmlui/bitstream/handle/123456789/1646/dikseo_0591.pdf?sequence=1&isAllowed=y **Η ΣΥΓΧΡΟΝΗ ΚΑΙ ΑΠΟΤΕΛΕΣΜΑΤΙΚΗ ΕΠΟΠΤΕΙΑ ΠΡΟΣΩΠΙΚΟΥ ΓΙΑ ΤΗΝ ΑΝΑΠΤΥΞΗ ΤΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ**

7) http://apothetirio.teiep.gr/xmlui/bitstream/handle/123456789/227/tlp_000168.pdf?sequence=1 **Οι ομάδες στο χώρο εργασίας και η αποτελεσματική ηγεσίας τους**
8) https://en.wikipedia.org/wiki/Human_resources **Human resources**
9) https://www.amazon.jobs/en/job_categories/human-resources **Human resources**
10) https://www.investopedia.com/terms/h/humanresources.asp **Human resources (HR)**
11) https://www.allbusinessschools.com/human-resources/job-description/ **What Does an HR Manager Do?**

Πηγές κεφαλαίου 4

1) https://www.kaspersky.com/resource-center/threats/deep-web **What is the Deep and Dark Web?**
2) https://sopa.tulane.edu/blog/everything-you-should-know-about-dark-web#:~:text=The%20dark%20web%20is%20known,communicate%20and%20share%20files%20online. **Everything You Should Know About the Dark Web**
3) https://fraudwatch.com/expert-explanation-history-of-the-dark-web/ **Expert Explanation: History of the Dark Web**
4) https://www.soscanhelp.com/blog/history-of-the-dark-web **HISTORY OF THE DARK WEB [TIMELINE]**
5) https://www.researchgate.net/profile/Sukhchandan-Randhawa/publication/338878596_Dark_Web_A_Web_of_Crimes/links/5f1600a84585151299ab503b/Dark-Web-A-Web-of-Crimes.pdf **Dark Web: A web of crimes, 2020, Shubhdeep Kaur – Sukhchandan Randhawa**
6) https://www.peraton.com/news/five-things-to-know-about-the-dark-web/#:~:text=There%20are%20some%20benefits%20to,is%20happening%20in%20their%20country. **Five things to know about the Dark Web**
7) https://vpnoverview.com/privacy/anonymous-browsing/tor/ **What is the Tor Browser?: A Guide to the Dark Browser**
8) https://www.torproject.org/about/history/
9) https://www.investopedia.com/terms/t/tor.asp#toc-how-tor-works **How Tor works**
10) https://cybernews.com/privacy/what-is-tor-and-how-does-it-work/
11) https://www.csoonline.com/article/3287653/what-is-the-tor-browser-how-it-works-and-how-it-can-help-you-protect-your-identity-online.html **What is the Tor Browser? And how it can help protect your identity**
12) https://www.itrelease.com/2021/05/advantages-and-disadvantages-of-tor-browser/ **Advantages and Disadvantages of the tor browser**
13) https://cybernews.com/privacy/what-is-tor-and-how-does-it-work/ **What is Tor and how does it work?**
14) https://vpnoverview.com/privacy/anonymous-browsing/the-dark-web/ **What is Dark Web? How to Access and What You Find**
15) https://freenetproject.org/pages/about.html **About WHAT IS FREENET?**

16) https://allthatsinteresting.com/peter-scully **Meet Peter Scully, The Depraved Predator Who Built A Child Pornography Empire On The Dark Web**
17) https://www.wizcase.com/blog/how-to-safely-use-the-dark-web/ **The Good People's Guide to the Dark Web (How to Stay Safe in 4 Easy Steps)**
18) https://en.wikipedia.org/wiki/Hieu_Minh_Ngo **Hieu Minh Ngo**
19) https://en.wikipedia.org/wiki/Silk_Road_(marketplace) **Silk Road (marketplace)**
20) https://thehackernews.com/2015/03/sheep-marketplace-thomas-arrested.html **Sheep Marketplace Owner Arrested While Trying to Buy Luxury Home**
21) https://www.investopedia.com/news/how-bitcoin-works/ **How Bitcoin works**
22) https://www.wionews.com/world/after-being-blocked-in-russia-twitter-launches-new-dark-web-service-460582 **After being blocked in Russia, Twitter launches new 'dark web' service**
23) https://www.linkedin.com/pulse/hackers-hire-matthew-hussey **Hackers for hire**