

Ιόνιο Πανεπιστήμιο

Τμήμα Πληροφορικής



~ Πτυχιακή εργασία ~

«Ηλεκτρονικό Έγκλημα & Κυβερνοπόλεμος»

Φοιτητής : Αλέξανδρος Βυθούλκας

Επιβλέπουσα : Αναπληρώτρια καθηγήτρια Αγγελική Τσώχου

Μέλη της επιτροπής : Καθηγητής Εμμανουήλ Μάγκος, Επίκουρος
καθηγητής Χριστόφορος Νταντογιάν

Σεπτέμβριος 2023

Ευχαριστίες

Θα ήθελα να ευχαριστήσω την επιβλέπουσα Αναπληρώτρια Καθηγήτρια κυρία Αγγελική Τσώχου, για την πολύτιμη βοήθειά και καθοδήγηση που μου προσέφερε έτσι ώστε να μπορέσω να ολοκληρώσω την παρούσα εργασία.

Ακόμα, θέλω να ευχαριστήσω την οικογένεια μου που τόσο καιρό με στηρίζει και με ενθαρρύνει, για να μπορέσω να εκπληρώσω τα όνειρά μου.

Περιεχόμενα

Περίληψη.....	5
Abstract	6
Εισαγωγή.....	1
Κεφάλαιο 1 Βασικές έννοιες	2
1.1 Δίκτυο.....	2
1.2 Διαδίκτυο.....	2
1.3 Κυβερνοχώρος - Cyberspace.....	3
1.4 Κυβερνοέγκλημα – Ηλεκτρονικό έγκλημα	3
1.4.1 Ηλεκτρονικό Έγκλημα	3
1.4.2 Κυβερνοέγκλημα.....	4
Κεφάλαιο 2 Κατηγορίες ηλεκτρονικού εγκλήματος.....	8
2.1 Ηλεκτρονικό έγκλημα και οι διαφορές του από την παραβίαση ασφάλειας.....	8
2.2 Επιθέσεις	8
2.2.1 Ενεργητικές επιθέσεις	8
2.2.2 Παθητικές επιθέσεις	9
2.3 Μορφές ηλεκτρονικού εγκλήματος.....	10
2.3.1 Γνήσια ηλεκτρονικά εγκλήματα.....	10
2.3.1.α Διασπορά κακόβουλου λογισμικού.....	11
2.3.1.α1 Trojan Horses – Δούρειοι Ίπποι	11
2.3.1.α2 Computer Viruses – Ηλεκτρονικοί Ιοί	14
2.3.1.α3 Worms – Ηλεκτρονικά Σκουλήκια.....	17
2.3.1.α4 Spyware – Λογισμικό κατασκοπείας.....	18
2.3.1.α5 Rootkits	21
2.3.1.α6 Ransomware	22
2.3.1.α7 Bots-botnets-zombies	24
2.3.1.α8 Επιθέσεις DDoS	27
2.3.1.α9 Λογικές βόμβες – Logic bombs.....	28
2.3.1.α10 Bacteria – Ηλεκτρονικά βακτήρια.....	29
2.3.1.β Κακόβουλες εισβολές σε δίκτυα υπολογιστών	29
2.3.1.β1 Hacking	30
2.3.1.β2 Cracking	33
2.3.1.γ Phishing – Ηλεκτρονικό Ψάρεμα	33
2.3.1.δ Spamming – Ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου	34
2.3.1.ε Software Piracy - Πειρατεία Λογισμικού	36
2.3.2 Παραδοσιακά ηλεκτρονικά εγκλήματα	37

2.3.2.α Computer – Internet Fraud / Απάτη Μέσω Υπολογιστή - Διαδικτύου.....	37
2.3.2.β Πλαστογραφία – Forgery	39
2.3.2.γ Cybersex Trafficking and Child Pornography – Διακίνηση Λευκής Σαρκός και Παιδικής Πορνογραφίας Μέσω Διαδικτύου.....	40
2.3.2.δ Online Harassment - Διαδικτυακή παρενόχληση	42
2.3.2.ε Drugs Trafficking – Λαθρεμπόριο Ναρκωτικών Μέσω Διαδικτύου.....	44
2.3.2στ Cyberterrorism – Κυβερνοτρομοκρατία	45
Κεφάλαιο 3 Εμβάθυνση στον κυβερνοπόλεμο.....	48
3.1 Ο ορισμός του κυβερνοπόλεμου	48
3.2 Χαρακτηριστικά και μορφές του κυβερνοπολέμου.....	49
3.3 Στόχοι κυβερνοπολέμου	53
3.4 Κυβερνοόπλα.....	57
3.4.1 Επιθετικά κυβερνοόπλα.....	58
3.4.2 Αμυντικά κυβερνοόπλα	58
3.4.3 Κυβερνοόπλα διπλής χρήσης	58
3.5 Επιπτώσεις ενός κυβερνοπολέμου	59
3.6 Περιπτώσεις διεξαγωγής κυβερνοπολέμου	64
3.6 .1 Η περίπτωση της Εσθονίας.....	64
3.6.2 Η περίπτωση της Γεωργίας.....	64
3.6.3 Η περίπτωση του Ιράν	66
3.6.4 Η περίπτωση της Ουκρανίας	66
3.7 Η σχέση μεταξύ κυβερνοπολέμου και τρομοκρατίας.....	68
Κεφάλαιο 4 Τρόποι πρόληψης στον κυβερνοχώρο	70
4.1 Αντικά λογισμικά (antivirus).....	70
4.2 Τείχη προστασίας (firewall)	71
4.2.1 Τείχη προστασίας φιλτραρίσματος πακέτων.....	74
4.2.2 Τείχη προστασίας επιθεώρησης κατάστασης.....	76
4.2.3 Τείχη προστασίας εφαρμογών.....	77
4.2.4 Πύλες πληρεξούσιων εφαρμογών.....	78
4.2.5 Εξειδικευμένοι διακομιστές μεσολάβησης.....	79
4.2.6 Εικονικά ιδιωτικά δίκτυα - VPN	80
4.2.7 Έλεγχος πρόσβασης δικτύου	81
4.2.8 Ενοποιημένη διαχείριση απειλών (UTM)	81
4.2.9 Τείχη προστασίας εφαρμογών ιστού	82
4.2.10 Τείχη προστασίας για εικονικές δομές	82
4.3 Αυθεντικοποίηση – ταυτοποίηση χρήστη και τεχνικές.....	82

4.4 Κρυπτογραφία	85
4.5 Ενέργειες που πρέπει να ακολουθήσει ο χρήστης για να παραμείνει ασφαλής από ηλεκτρονικά εγκλήματα	87
4.6 Ενέργειες που πρέπει να ακολουθήσει ένας οργανισμός και τα μεγάλα στελέχη του για να παραμείνουν ασφαλείς από ηλεκτρονικά εγκλήματα	89
Κεφάλαιο 5 Ανίχνευση επιθέσεων και η αντιμετώπισή τους.....	91
5.1 Εισαγωγή στα συστήματα ανίχνευσης επιθέσεων.....	91
5.2 Λόγοι χρήσης συστημάτων ανίχνευσης εισβολών	93
5.3 Διαχείριση των εισβολών από ένα Σύστημα Διαχείρισης Εισβολών – IDS.....	94
5.4 Κατηγοριοποίηση Συστημάτων Ανίχνευσης Εισβολών – IDS και χρονισμός της ανάλυσης	95
5.5 Κατηγοριοποίηση των Συστημάτων Ανίχνευσης Εισβολών σύμφωνα με την πηγή πληροφοριών	96
5.6 Πιθανές αντιδράσεις των Συστημάτων Ανίχνευσης Εισβολών.....	96
5.7 Αντιμετώπιση πιθανών καταστροφών από επιθέσεις στον κυβερνοχώρο	97
Κεφάλαιο 6 Συμπεράσματα και προτάσεις βελτίωσης.	99
Βιβλιογραφία.....	101

Περίληψη

Με την πάροδο του χρόνου και την εξέλιξη της τεχνολογίας βλέπουμε ότι, ολοένα και περισσότερο η πληροφορική, οι ηλεκτρονικοί υπολογιστές και το διαδίκτυο έχουν σημαντικό ρόλο στην καθημερινότητα του ανθρώπου καθώς συμβάλλουν στην βελτίωση της ποιότητας ζωής. Οι δυνατότητες που παρέχουν οι ηλεκτρονικοί υπολογιστές αυξάνονται μέρα με την μέρα και την ανάπτυξη της τεχνολογίας. Η χρήση ηλεκτρονικών υπολογιστών βοηθάει στο να απλοποιηθούν κάποιες εργασίες, που στο παρελθόν απαιτούσαν περισσότερο χρόνο και κόπο για να πραγματοποιηθούν, κάνει την οργάνωση πληροφοριών και την διαχείριση μεγάλου όγκου δεδομένων πιο εύκολες διαδικασίες. Αυτές είναι μόνο λίγες από τις ωφέλειες, που μπορεί να έχει ο σύγχρονος άνθρωπος από την χρήση των ηλεκτρονικών υπολογιστών.

Η αυξανόμενη χρήση και η εξάρτηση της ζωής μας από τον υπολογιστή στην καθημερινότητά μας οφείλεται και στην ταυτόχρονη εξέλιξη του διαδικτύου. Η εύκολη επικοινωνία σε όλους τους τομείς μέσω του διαδικτύου, είτε αυτή είναι μια χρηματική συναλλαγή διεθνή ή μη, είτε κάποιο απλό mail ή και επαγγελματικό ακόμα, είναι μερικές πτυχές του διαδικτύου, που κάνουν όλο και περισσότερους ανθρώπους να χρησιμοποιήσουν ηλεκτρονικό υπολογιστή. Συνεπώς η εικονική κοινωνία του διαδικτύου μεγαλώνει και γίνεται πλέον αντιληπτό ότι χρειάζεται η σωστή οργάνωση και ο έλεγχός του για την εύρυθμη λειτουργία του.

Σε αντίθεση όμως από όλα τα θετικά που έχει η χρήση του ηλεκτρονικού υπολογιστή και του διαδικτύου, υπάρχουν και κάποιες πτυχές που δεν μπορούν να χαρακτηριστούν και τόσο θετικές και φιλικές ως προς τον χρήστη τους. Οι ηλεκτρονικοί υπολογιστές μαζί με το διαδίκτυο μπορούν να αποτελέσουν πρόσφορο έδαφος για την ανάπτυξη όχι και τόσο νόμιμων ενεργειών και να αποτελέσουν χρήσιμο εργαλείο για κάθε μορφής εγκλήματος. Επομένως, μαζί με την ταχύτατη ανάπτυξη της τεχνολογίας των ηλεκτρονικών υπολογιστών και του διαδικτύου εξελίσσεται και το ηλεκτρονικό έγκλημα, το οποίο αρχίζει να αποκτά σύγχρονες και πιο σοβαρές μορφές με την πιο επίκαιρη και σοβαρή μορφή αυτή του κυβερνοπολέμου.

Παρ' όλα αυτά, καθώς αναπτύσσονται οι τεχνικές διεξαγωγής του κυβερνοεγκλήματος στον κυβερνοχώρο, αναπτύσσονται και οι τρόποι και οι τεχνικές της αποτροπής κάθε μορφής ηλεκτρονικού εγκλήματος αλλά και οι τρόποι πρόληψης που κάθε οντότητα που βρίσκεται στον κυβερνοχώρο οφείλει να ακολουθεί, έτσι ώστε να μην φτάσει ποτέ στο σημείο να κινδυνεύσει από κάποιο επίδοξο κυβερνοεγκληματία. Η παρακάτω εργασία θα πραγματοποιήσει μια αναφορά σε όλους τους τρόπους υλοποίησης του κυβερνοεγκλήματος και στην συνέχεια θα εστιάσει στον κυβερνοπόλεμο καθώς και στους τρόπους με τους οποίους μπορεί να αποτραπεί.

Abstract

With the passage of time and the advancement of technology, we can see that increasingly, computer science, electronic computers, and the internet play a significant role in people's daily lives as they contribute to improving the quality of life. The capabilities provided by electronic computers are increasing day by day with the development of technology. The use of electronic computers helps simplify certain tasks that in the past required more time and effort to accomplish, making information organization and the management of large volumes of data easier processes. These are just a few of the benefits that modern humans can have from the use of electronic computers.

The increasing use and dependence on computers in our daily lives are also attributed to the simultaneous evolution of the internet. The easy communication in all areas through the internet, whether it is an international or domestic financial transaction, a simple email, or even professional communication, are some aspects of the internet that make more and more people use electronic computers. Therefore, the virtual community of the internet is growing, and it is now evident that proper organization and control are needed for its smooth operation.

However, despite all the positives of using electronic computers and the internet, there are aspects that cannot be considered as positive or user-friendly. Electronic computers, along with the internet, can create fertile ground for the development of activities that are not entirely legal and can serve as useful tools for various forms of crime. Therefore, along with the rapid development of computer technology and the internet, cybercrime is also evolving, taking on modern and more serious forms, with the most current and serious form being cyber warfare.

Nevertheless, as the techniques of conducting cybercrime in cyberspace evolve, so do the methods and techniques of preventing all forms of electronic crime, as well as the preventive measures that every entity in cyberspace must follow, so as never to be endangered by a potential cybercriminal. The following work will provide an overview of all the methods of implementing cybercrime and then will focus on cyber warfare and the ways in which it can be prevented.

Εισαγωγή

Η παρακάτω πτυχιακή εργασία εστιάζει στις σύγχρονες μορφές του ηλεκτρονικού εγκλήματος, δίνοντας μια επιπλέον έμφαση στο πόλεμο που διεξάγεται αποκλειστικά και μόνο μέσω ηλεκτρονικών υπολογιστών και δικτύων. Επίσης, αναλύονται οι τρόποι αντιμετώπισης αλλά και τα όλα τα μέτρα πρόληψης από τέτοιου είδους εγκλήματα.

Η έρευνα που πραγματοποιήθηκε για την εργασία βασίστηκε σε επιστημονικές αναφορές, άρθρα τα οποία έχουν δημοσιευτεί και σε κρατικές ιστοσελίδες διαφόρων κρατικών υπηρεσιών τόσο στην Ελλάδα όσο και σε κράτη του εξωτερικού. Οι πηγές αυτές αντλήθηκαν κυρίως από το διαδίκτυο.

Στο πρώτο κεφάλαιο γίνεται αναφορά σε σημαντικούς ορισμούς όπως ορισμοί για το δίκτυο, το διαδίκτυο, τον κυβερνοχώρο, το ηλεκτρονικό έγκλημα και το κυβερνοέγκλημα. Στην συνέχεια, στο δεύτερο κεφάλαιο παρουσιάζεται η κατηγοριοποίηση του ηλεκτρονικού εγκλήματος, ξεκινώντας από τις απειλές και τις επιθέσεις και καταλήγοντας στις μορφές του ηλεκτρονικού εγκλήματος. Γίνεται αρχική ανάλυση στην κατηγοριοποίηση των ηλεκτρονικών εγκλημάτων σε γνήσια και παραδοσιακά ηλεκτρονικά εγκλήματα και στην συνέχεια περιγράφει τις υποκατηγορίες που περιέχονται σε κάθε μια από τις δύο αυτές αρχικές κατηγορίες.

Στο τρίτο κεφάλαιο η έρευνα εστιάζει σε μια μόνο μορφή των ηλεκτρονικών εγκλημάτων, τον κυβερνοπόλεμο. Περιγράφεται λεπτομερώς ο ορισμός του κυβερνοπολέμου, τα χαρακτηριστικά του, οι μορφές του, τα κυβερνοόπλα που χρησιμοποιούνται κατά την διεξαγωγή του, οι πιθανοί στόχοι ενός κυβερνοπολέμου και ποιες οι επιπτώσεις που μπορεί να έχει ένας κυβερνοπόλεμος. Επίσης, στο τρίτο κεφάλαιο αναφέρονται και περιπτώσεις διεξαγωγής κυβερνοπολέμου και η σχέση του με την κυβερνοτρομοκρατία.

Στο τέταρτο κεφάλαιο αναφέρονται οι τρόποι πρόληψης στον κυβερνοχώρο. Συγκεκριμένα αναλύονται τα αντικά λογισμικά, τα τείχη προστασίας, η αυθεντικοποίηση και η ταυτοποίηση του χρήστη, η κρυπτογραφία, οι ενέργειες του χρήστη έτσι ώστε να παραμείνει ασφαλής και οι ενέργειες ενός οργανισμού που πρέπει να ακολουθήσει αντίστοιχα για να αντιμετωπίσει πιθανές επιθέσεις στον κυβερνοχώρο.

Στο πέμπτο κεφάλαιο παρουσιάζεται εκτενώς η ανίχνευση των κυβερνοεπιθέσεων και η αντιμετώπιση τους. Σε αυτό το σημείο της η εργασία εστιάζει στους λόγους χρήσης των συστημάτων ανίχνευσης εισβολών, την διαχείριση των εισβολών από τα συστήματα ανίχνευσης, στον διαχωρισμό των συστημάτων ανίχνευσης εισβολών, στις πιθανές αντιδράσεις που μπορεί να έχει ένα σύστημα ανίχνευσης εισβολών και στην αντιμετώπιση των καταστροφών που προκλήθηκαν από επιθέσεις στον κυβερνοχώρο.

Τέλος, στο έκτο κεφάλαιο γίνεται μια αναφορά στα συμπεράσματα που προκύπτουν από την βιβλιογραφική αυτή έρευνα, καθώς επίσης και σε κάποιους πιθανούς τρόπους αντιμετώπισης ή καλύτερης διαχείρισης μια κατάστασης κατά την οποία διαπράττεται ένα ηλεκτρονικό έγκλημα ή κάποια κυβερνοεπίθεση.

Κεφάλαιο 1 Βασικές έννοιες

1.1 Δίκτυο

Με τον όρο δίκτυο αναφερόμαστε σε ένα σύνολο συνδεδεμένων κόμβων που βρίσκονται σε αλληλεπίδραση. Οι κόμβοι αυτοί διαθέτουν τον κατάλληλο δικτυακό εξοπλισμό έτσι ώστε, να μπορούν να συνδέονται με άλλους αντίστοιχους κόμβους, οι οποίοι δεν βρίσκονται απαραίτητα κοντά σε κάποιον άλλο κόμβο. Οι συνδέσεις των κόμβων αυτών μπορούν να γίνουν με δύο τρόπους, ενσύρματα και ασύρματα [1].

Τα δίκτυα υπολογιστών διακρίνονται από τα υπόλοιπα δίκτυα (π.χ. τηλεφωνικά) από την γενικότητα που τα χαρακτηρίζει. Τα δίκτυα υπολογιστών κατασκευάζονται κυρίως από γενικής χρήσης προγραμματίσιμο υλικό και δεν είναι βελτιστοποιημένα για συγκεκριμένες εφαρμογές, όπως η τηλεφωνική κλήση ή η παράδοση τηλεοπτικών σημάτων. Αντίθετα, μπορούν να μεταφέρουν πολλούς διαφορετικούς τύπους δεδομένων και υποστηρίζουν μια μεγάλη και αυξανόμενη ποικιλία εφαρμογών[2].

1.2 Διαδίκτυο

Σαν συνέχεια του προηγούμενου ορισμού χρησιμοποιούμε τον όρο διαδίκτυο (Internet) για να αναφερθούμε σε μια αυθαίρετη συλλογή δικτύων που διασυνδέονται για να παρέχουν κάποιου είδους υπηρεσίας παράδοσης πακέτων από υπολογιστή υπηρεσίας σε υπολογιστή υπηρεσίας. Για παράδειγμα, μια εταιρεία με πολλές εγκαταστάσεις μπορεί να δημιουργήσει ένα ιδιωτικό δίκτυο συνδέοντας τα τοπικά δίκτυα (LAN) των διάφορων εγκαταστάσεών της με συνδέσμους από σημείο σε σημείο, τους οποίους θα μισθώσει από μια εταιρεία τηλεπικοινωνιών. Όταν αναφερόμαστε στο ευρείας χρήσης παγκόσμιο διαδίκτυο που συνδέει πλέον ένα μεγάλο ποσοστό δικτύων, εννοούμε το διαδίκτυο ως έχει γίνει κοινώς αποδεκτό και συνδέει υπολογιστές και δίκτυα παγκοσμίως. [3].

Με πιο απλά λόγια το διαδίκτυο ορίζεται ως ένα δίκτυο ηλεκτρονικών υπολογιστών οι οποίοι επικοινωνούν μεταξύ τους, που επιτρέπει την ανταλλαγή δεδομένων μεταξύ οποιουδήποτε διασυνδεδεμένου υπολογιστή. Το διαδίκτυο είναι πραγματικά ένα εργαλείο όπου χρήστες όλων των ηλικιών μπορούν να βρεθούν σε έναν απέραντο εικονικό χώρο γεμάτο εκατομμύρια πληροφορίες. Μπορούν να παίξουν παιχνίδια, να αναζητήσουν πληροφορίες, να αλληλογραφήσουν μέσω email ή και να συνομιλήσουν μέσω των κοινωνικών δικτύων και να βρουν αρχεία κάθε είδους. Με την ολοένα και περισσότερη εξέλιξη της τεχνολογίας, οι χρήστες του διαδικτύου είναι πια σε θέση να πραγματοποιούν ηλεκτρονικές αγορές, συναλλαγές με το Δημόσιο και τις τράπεζες και να ασχοληθούν με την εκπαίδευση και την εργασία εξ αποστάσεως.

Όλα τα παραπάνω οι ανήλικοι τα κάνουν συνήθως χωρίς επίβλεψη, με μια ελευθερία που υπό κανονικές συνθήκες δεν υπάρχει στην πραγματική τους ζωή. Συνεπώς, ένα θέμα που απασχολεί πολλούς ερευνητές είναι για τους κινδύνους που εγκυμονούν στο διαδίκτυο, για τους οποίους έχουν γραφτεί τα τελευταία χρόνια πολλά άρθρα [4]. Αναμφίβολα το διαδίκτυο ασκεί μεγάλη γοητεία σε άτομα όλων των ηλικιών αλλά επίσης έχει γίνει και σημαντικό κομμάτι της καθημερινότητάς μας για όλους τους λόγους που αναφέρθηκαν πιο πάνω. Ο σημαντικός ρόλος που έχει πλέον στην καθημερινότητα μας το διαδίκτυο το κάνει αυτόματα και ένα μέσο ή έναν χώρο για να το θέσουμε πιο σωστά, για να ανθίσουν κάθε είδους εγκλήματα όπως και αυτό του κυβερνοπολέμου.

1.3 Κυβερνοχώρος - Cyberspace

Με την έννοια του κυβερνοχώρου αναφερόμαστε σε έναν χώρο, που αποτελείται και διαμορφώνεται από δίκτυα επικοινωνιών που χρησιμοποιούν ηλεκτρονικούς υπολογιστές. Προκειμένου να αναλύσουμε με περισσότερη ακρίβεια τον ορισμό του Κυβερνοχώρου μπορούμε να αναφερθούμε στην ετυμολογία της λέξης. Σύμφωνα με την ελληνική γλώσσα η σύνθετη λέξη αυτή αποτελείται από δύο μικρότερες λέξεις. Το πρώτο συνθετικό είναι η λέξη «Κυβερνήτης», δηλαδή ο καπετάνιος που διοικεί και ελέγχει ένα πλοίο ενώ η άλλη λέξη «χώρος» είναι στη συγκεκριμένη περίπτωση η θάλασσα και τα χαρακτηριστικά και οι εκάστοτε συνθήκες που τη συνοδεύουν. Ο Κυβερνοχώρος σε αντιστοιχία με τη σύγχρονή του έννοια αναφέρεται στην ικανότητα ενός ατόμου να χειρίζεται, να κατευθύνει και να ελέγχει με δική του πρωτοβουλία και χρησιμοποιώντας απλά τον ηλεκτρονικό υπολογιστή, ο οποίος είναι το μέσο της δημιουργίας της εικονικής πραγματικότητας, η οποία αντιπροσωπεύεται από τον ίδιο τον Κυβερνοχώρο [5].

Δηλαδή, είναι το εικονικό περιβάλλον μέσα στο οποίο λαμβάνουν χώρα ηλεκτρονικές επικοινωνίες και οι συνδέσεις μεταξύ υπολογιστών, όπως το διαδίκτυο η ανταλλαγή ηλεκτρονικών μηνυμάτων και πλέον μεγάλο μέρος των εμπορικών και τραπεζικών συναλλαγών κ.α. Ο κυβερνοχώρος αποτελεί ένα παγκόσμια διασυνδεδεμένο δίκτυο ψηφιακών πληροφοριών και επικοινωνιακών υποδομών.

1.4 Κυβερνοέγκλημα – Ηλεκτρονικό έγκλημα

Η χρήση του υπολογιστή και των δικτύων γίνεται ολοένα πιο σημαντικό και αναπόσπαστο κομμάτι της σύγχρονης ζωής. Σε αυτό συμβάλλει ο σύγχρονος τρόπος ζωής που εξελίσσεται ανάλογα με την ανάπτυξη της τεχνολογίας και ταυτόχρονα οι νέες ανάγκες που προκύπτουν από την εξέλιξη αυτή. Οι Η/Υ παρέχουν στους χρήστες δυνατότητες, που με την πάροδο του χρόνου αυξάνονται και που έχουν ξεπεράσει κάθε προσδοκία που δημιουργήθηκε από όταν εισήχθησαν οι υπολογιστές στην καθημερινότητα του ανθρώπου για πρώτη φορά. Παράλληλα όμως, δημιουργήθηκαν και δημιουργούνται οι δυνατότητες, οι προϋποθέσεις και οι συνθήκες εκείνες για την εμφάνιση καινούργιων μορφών παραβατικής συμπεριφοράς. Άρα με μια πρώτη προσέγγιση κυβερνοέγκλημα είναι κάθε είδους έγκλημα που διαπράττεται μέσω του κυβερνοχώρου.

1.4.1 Ηλεκτρονικό Έγκλημα

Η τεχνολογία της πληροφορικής κατέστησε δυνατή τη διάπραξη ενός ευρέως φάσματος εγκληματικών πράξεων καθώς η ελευθερία χρήσης του διαδικτύου και η μη ασφάλεια των πληροφοριών του συνεπάγονται και την κακή χρήση του από μη εγκεκριμένους χρήστες που εισχωρούν στον κυβερνοχώρο, οι οποίοι επεξεργάζονται στοιχεία και αρχεία παράνομα, δημιουργώντας νέες μορφές εγκληματικότητας. Σύμφωνα με τη Δίωξη Ηλεκτρονικού Εγκλήματος, ως ηλεκτρονικό έγκλημα «θεωρούνται οι αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία». Επομένως, το Ηλεκτρονικό Έγκλημα θα μπορούσε να χαρακτηριστεί σαν μια νέα μορφή εγκλήματος με μέσο εκτέλεσης τους Ηλεκτρονικούς Υπολογιστές[6]. Πρόκειται για μια παραλλαγή των ήδη υπάρχοντων εγκλημάτων με μοναδική διαφορά την εκτέλεση αυτών μέσω ενός υπολογιστή. Οι έννοιες ηλεκτρονικό έγκλημα, δικτυακό έγκλημα και έγκλημα του κυβερνοχώρου είναι άρτια συνδεδεμένες. Υπάρχει όμως ένας βασικός διαχωρισμός των ηλεκτρονικών εγκλημάτων. Τα ηλεκτρονικά εγκλήματα μπορούν να διακριθούν σε τρεις κατηγορίες

1. Σε περιπτώσεις εγκλημάτων που υλοποιούνται τόσο σε κοινό περιβάλλον όσο και στο διαδίκτυο, για παράδειγμα συκοφαντική δυσφήμιση που γίνεται μέσω ηλεκτρονικού ταχυδρομείου, ή αντιγραφή πνευματικών έργων όπως μουσικών τραγουδιών ή προγραμμάτων υπολογιστή, όταν το έγκλημα αυτό διαπράττεται στο περιβάλλον του διαδικτύου, με τη χρήση υπολογιστή, τότε αναφερόμαστε σε έγκλημα που σχετίζεται με τον κυβερνοχώρο ή σε έγκλημα που διαπράττεται με τη βοήθεια του διαδικτύου (internet related crime).
2. Σε περιπτώσεις εγκλημάτων που υλοποιούνται αποκλειστικά σε περιβάλλον ηλεκτρονικών υπολογιστών, χωρίς τη χρήση του διαδικτύου. Μέσα σε αυτά περιλαμβάνονται εγκλήματα που περιγράφονται στο άρθρο 370 Γ παράγραφος 1 του Ποινικού Κώδικα. Ένα παράδειγμα είναι η παράνομη αντιγραφή προγράμματος από δισκέτα ή CD-ROM σε ηλεκτρονικό υπολογιστή χωρίς να έχει δοθεί η απαραίτητη άδεια.
3. Οι "Γνήσια εγκλήματα κυβερνοχώρου" (cyber crimes) αναφέρονται στην ποινικοποίηση συμπεριφοράς που αφορά αποκλειστικά τον κυβερνοχώρο. Ένα παράδειγμα τέτοιας αξιόποινης συμπεριφοράς θα μπορούσε να είναι η παράνομη μεταβίβαση κρυπτογραφημένων κειμένων χωρίς την αναγκαία άδεια ή η διάδοση παιδικής πορνογραφίας μέσω του κυβερνοχώρου [7].

Τα κύρια χαρακτηριστικά του ηλεκτρονικού εγκλήματος είναι πολλά. Το ηλεκτρονικό έγκλημα είναι γρήγορο, διαπράττεται σε χρόνο δευτερολέπτων και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα. Είναι εύκολο στη διάπραξή του – φυσικά για όσους το γνωρίζουν – ενώ τα ίχνη που αφήνει είναι ψηφιακά. Για την πραγματοποίηση του χρειάζονται άριστες και εξειδικευμένες γνώσεις. Μπορεί να διαπραχθεί χωρίς τη μετακίνηση του δράστη, ο οποίος ενεργεί από το γραφείο ή το σπίτι του χωρίς φυσική παρουσία, χρησιμοποιώντας ηλεκτρονικές συσκευές που μπορεί να έχει στην κατοχή του όπως υπολογιστή, smart phone, tablet . Δίνει τη δυνατότητα σε άτομα με ιδιαιτερότητες, όπως οι παιδόφιλοι, να επικοινωνούν γρήγορα ή και σε πραγματικό χρόνο, χωρίς μετακίνηση, εύκολα, ανέξοδα, να βρίσκονται πολλοί μαζί στις ίδιες ομάδες συζητήσεων (new groups) ή μέσα σε “chat rooms”. Οι «εγκληματίες του κυβερνοχώρου» πολλές φορές δεν εμφανίζονται με την πραγματική τους ταυτότητα, αποστέλλουν ηλεκτρονικά μηνύματα (emails) με ψευδή στοιχεία. Είναι έγκλημα χωρίς πατρίδα και τα αποτελέσματά του μπορεί να πραγματοποιούνται ταυτόχρονα σε πολλούς τόπους και σε διαφορετικές χώρες, ενώ είναι πολύ δύσκολο να προσδιοριστεί ο τόπος τέλεσής του. Η αστυνομική διερεύνησή του είναι πάρα πολύ δύσκολη, απαιτεί άριστη εκπαίδευση και εξειδικευμένες γνώσεις. Η καταγραφή της εγκληματικότητας στον κυβερνοχώρο δεν ανταποκρίνεται στην πραγματικότητα, διότι ελάχιστες περιπτώσεις εγκλημάτων του κυβερνοχώρου καταγγέλλονται, όχι μόνο στον ελληνικό, αλλά και στο διεθνή χώρο. Κατά συνέπεια, ο σκοτεινός αριθμός της εγκληματικότητας στο χώρο του διαδικτύου είναι ακόμη πιο σκοτεινός, απ’ ότι στον κοινό εγκληματικό χώρο [8].

1.4.2 Κυβερνοέγκλημα

Για να δώσουμε λοιπόν έναν πλήρη ορισμό για το κυβερνοέγκλημα σύμφωνα με την επίσημη σελίδα της εταιρείας “Kaspersky”, κάθε είδους εγκληματική δραστηριότητα που είτε χρησιμοποιεί είτε έχει ως στόχο τους ηλεκτρονικούς υπολογιστές ή και δίκτυα ηλεκτρονικών υπολογιστών ονομάζεται κυβερνοέγκλημα ή αλλιώς ηλεκτρονικό έγκλημα. Τα περισσότερα κυβερνοεγκλήματα διαπράττονται από κυβερνοεγκληματίες ή hackers οι οποίοι έχουν ως στόχο το χρηματικό κέρδος. Παρόλα αυτά το κυβερνοέγκλημα, κάποιες φορές, στοχεύει να καταστρέψει ηλεκτρονικούς υπολογιστές ή δίκτυα για λόγους εκτός του οικονομικού κέρδους

όπως πολιτικοί λόγοι ή προσωπικοί. Το κυβερνοέγκλημα μπορεί να εκτελεστεί μεμονωμένα από ένα άτομο ή από οργανισμούς. Επιπροσθέτως, κάποιοι από τους κυβερνοεγκληματίες είναι καλά οργανωμένοι και τεχνικά αρκετά επιδέξιοι χρησιμοποιώντας πολύ εξελιγμένες τεχνικές ενώ άλλοι βρίσκονται σε πρωταρχικό επίπεδο ακόμα [9].

Σύμφωνα με τον παραπάνω ορισμό που δόθηκε για το ηλεκτρονικό έγκλημα, τα γνήσια εγκλήματα του κυβερνοχώρου διαπράττονται αποκλειστικά με την χρήση του διαδικτύου. Χαρακτηριστικά ο Casey λέει: «Το cybercrime αναφέρεται σε κάθε έγκλημα που περιλαμβάνει υπολογιστές και υπολογιστικά δίκτυα περιλαμβάνοντας εγκλήματα που δεν στηρίζονται έντονα στους υπολογιστές». Αυτός ο γενικός όρος είναι απαραίτητος για να περιγράψει περιπτώσεις όπου ένα υπολογιστικό δίκτυο δεν χρησιμοποιείται για να διαπραχθεί ένα έγκλημα αλλά παρόλα αυτά συνεχίζει να περιλαμβάνει ψηφιακά δεδομένα που είναι σχετιζόμενα με το έγκλημα. Αν ο υπολογιστής λειτουργεί αυτόνομα χωρίς σύνδεση στο Διαδίκτυο, οποιοδήποτε εγκληματική ενέργεια που διαπράττεται θεωρείται έγκλημα που διαπράττεται με τη χρήση ηλεκτρονικού υπολογιστή (ηλεκτρονικό έγκλημα).

Σε σχέση με τα εγκλήματα, στα οποία «εμπλέκεται» ο υπολογιστής και το δίκτυο προκύπτει και η εξής ταξινόμηση :

1. **Ο υπολογιστής ως στόχος.** Σε αυτήν την κατηγορία περιλαμβάνονται εγκλήματα που σχετίζονται με την κακόβουλη παρείσφρηση σε ηλεκτρονικά συστήματα υπολογιστών ή δίκτυα υπολογιστών, την κακόβουλη παρείσφρηση σε λειτουργικά συστήματα και προγράμματα, την κλοπή πληροφοριών, εγκλήματα που σχετίζονται με την παραβίαση πνευματικής ιδιοκτησίας, όπως την παράνομη αντιγραφή λογισμικού υπολογιστών, την τεχνολογική καταστροφή και την τεχνολογική παραβίαση. Περιλαμβάνονται εγκλήματα κατά τα οποία διαπράττεται κλοπή πνευματικής ιδιοκτησίας, κλοπή πληροφοριών μάρκετινγκ (παραδείγματος χάριν, λίστες πελατών, τιμοκαταλόγους, η πλάνα μάρκετινγκ) ή εκβιασμό με βάση τις πληροφορίες που έχουν αποκτηθεί από μηχανογραφημένα αρχεία (π.χ. ιατρικές πληροφορίες, προσωπικό ιστορικό, η σεξουαλική προτίμηση), σαμποτάζ πνευματικής ιδιοκτησίας ή σαμποτάζ λειτουργικών συστημάτων και προγραμμάτων με σκοπό τη διάλυση ή δημιουργία χάους σε επιχειρηματικές δραστηριότητες. Παράνομη πρόσβαση στη δικαιοσύνη και σε άλλα κυβερνητικά έγγραφα αποτελούν εγκλήματα τα οποία έχουν τον υπολογιστή ως στόχο, περιλαμβάνοντας αλλαγές στο ιστορικό ενός εγκληματία ή αλλαγή στην εγγύησή του όπως επίσης δημιουργία επίσημων εγγράφων καθώς και διαβατήρια και διπλώματα οδήγησης. Άλλο ένα έγκλημα σε αυτή την κατηγορία είναι το «πέρασμα» από έναν υπολογιστή απλά για να διερεύνηση. Σε αυτές τις περιπτώσεις ο εισβολέας απλά κοιτάζει ένα αρχείο, αλλά ακόμη και αυτό παραβιάζει τα προσωπικά δεδομένα του ιδιοκτήτη.
2. **Ο υπολογιστής ως συμβολή του εγκλήματος.** Σύμφωνα με την κοινή νομοθεσία, η χρήση νόμιμων μέσων μπορεί να τροποποιηθεί με σκοπό να διευκολυνθεί η διάπραξη ενός εγκλήματος. Σε αυτήν την κατηγορία εγκλημάτων, οι διαδικασίες του υπολογιστή, και όχι τα περιεχόμενα των αρχείων, συντελούν στη διάπραξη του εγκλήματος. Ουσιαστικά, ο δράστης εισάγει νέο κώδικα (οδηγίες προγραμματισμού) για να ελέγξει τις αναλυτικές διαδικασίες του υπολογιστή. Μια άλλη μέθοδος περιλαμβάνει τον μετασχηματισμό νόμιμων υπολογιστικών διαδικασιών για παράνομους σκοπούς. Σε αυτήν την κατηγορία εμπίπτουν οι απάτες με αυτόματες ταμειολογιστικές μηχανές (ATM), οι απάτες με ηλεκτρονικές μεταφορές χρημάτων και συναλλαγών (μεταβιβάσεις μετοχών, πωλήσεις ή τιμολογήσεις, απάτες με

πιστωτικές κάρτες, απάτες τηλεπικοινωνιών). Για παράδειγμα η διαδικτυακή απάτη, απάτες πιστωτικών καρτών, απάτες που περιλαμβάνουν τις ηλεκτρονικές μεταφορές χρημάτων, απάτες τηλεπικοινωνιών και απάτες σχετικά με το ηλεκτρονικό εμπόριο και την ηλεκτρονική ανταλλαγή δεδομένων.

3. **Ο υπολογιστής ως «συνεργός/πλατφόρμα» σε άλλα εγκλήματα.** Σε αυτήν την κατηγορία, ο υπολογιστής δεν είναι απαραίτητος για τη διάπραξη ενός εγκλήματος, αλλά σχετίζεται με την εγκληματική πράξη. Αυτό σημαίνει ότι το έγκλημα θα μπορούσε να συμβεί και χωρίς την τεχνολογία, αλλά η ψηφιοποίηση βοηθάει στην ταχύτερη εκτέλεσή του, διευκολύνει την επεξεργασία μεγάλου όγκου πληροφοριών και καθιστά πιο δύσκολη την ανίχνευση και εντοπισμό του εγκλήματος. Τέτοια εγκλήματα περιλαμβάνουν το ξέπλυμα χρήματος, παράνομες τραπεζικές συναλλαγές και συστήματα ανακοινώσεων που υποστηρίζουν παράνομη δραστηριότητα ή τη διακίνηση ναρκωτικών και παιδική πορνογραφία. Όπως η εξάπλωση ναρκωτικών, το ξέπλυμα χρημάτων και παράνομες τραπεζικές συναλλαγές, παιδική πορνογραφία, διαδικτυακά φόρουμ που προωθούν παράνομες δραστηριότητες και τζόγος στο Διαδίκτυο.
4. **Εγκλήματα σχετικά με την εξάπλωση των υπολογιστών** όπως για παράδειγμα, πειρατεία λογισμικού/ πλαστογράφηση, παραβίαση πνευματικών δικαιωμάτων των προγραμμάτων υπολογιστών, πλαστός εξοπλισμός, μαύρος εξοπλισμός υπολογιστών αγοράς και προγράμματα [10]. Η παρουσία των υπολογιστών και ιδιαίτερα των μικροϋπολογιστών δημιουργεί νέες εκδοχές των παραδοσιακών εγκλημάτων. Σε αυτές τις περιπτώσεις, η τεχνολογική ανάπτυξη ουσιαστικά δημιουργεί νέους στόχους εγκλήματος, όπως πλαστογράφηση λογισμικών προγραμμάτων, παραβίαση πνευματικών δικαιωμάτων προγραμμάτων υπολογιστών, μαύρη αγορά εξοπλισμού και προγραμμάτων υπολογιστών καθώς και κλοπή τεχνολογικού εξοπλισμού [10][11].

Το κυβερνοέγκλημα παρουσιάζει τα ακόλουθα χαρακτηριστικά, τα οποία δυσκολεύουν τη δικαστική του δίωξη :

- Ταχύτητα – Ο χρόνος που απαιτείται για τη διάπραξη των σχετικών πράξεων είναι εξαιρετικά μικρός και συχνά δεν γίνεται αντιληπτή από το θύμα.
- Ευκολία – Οι σχετικές πράξεις είναι εύκολες να διαπραχθούν από τον δράστη μέσω ενός υπολογιστή και στον οικείο - ιδιωτικό του χώρο.
- Ανωνυμία – Οι εγκληματικές ενέργειες στον κυβερνοχώρο εκμεταλλεύονται την υπάρχουσα ανωνυμία που παρέχουν ορισμένες τεχνολογικές υποδομές του διαδικτύου.
- Διασυνοριακός Χαρακτήρας – Οι ενέργειες προετοιμασίας, οι πράξεις και τα αποτελέσματα των κυβερνοεγκλημάτων συνήθως εκτελούνται ταυτόχρονα σε πολλές νομικές δικαιοδοσίες.
- Δυσχέρεια στην Διερεύνηση – Η διασυνοριακή φύση και οι ψηφιακές αποτυπώσεις των κυβερνοεγκλημάτων καθιστούν πιο δύσκολη την έρευνα και αποκάλυψή τους.
- Διακρατική Συνεργασία – Η διασυνοριακή φύση των κυβερνοεγκλημάτων καθιστά αναγκαία τη συνεργασία μεταξύ των διωκτικών αρχών διαφόρων χωρών.
- Έλλειψη Επαρκούς Καταγραφής – Το μέγεθος των τελούμενων κυβερνοεγκλημάτων είναι δυσανάλογα μεγαλύτερο των καταγραφόμενων περιστατικών [12].

Τέλος αξίζει να σημειωθεί ότι το κυβερνοέγκλημα εξελίσσεται διακρατικά. Η περίπλοκη φύση αυτού του είδους εγκλήματος που συμβαίνει στο χωρίς σύνορα «βασιλείο» του

κυβερνοχώρου είναι συντεθειμένο από την ολοένα και αυξανόμενη εμπλοκή καλά οργανωμένων εγκληματικών οργανώσεων. Οι ηλεκτρονικοί εγκληματίες και τα θύματα τους μπορούν να βρίσκονται σε διαφορετικές εθνότητες και μέρη παγκοσμίως και τα αποτελέσματα του κυβερνοεγκλήματος μπορούν να εξαπλωθούν σε όλες τις κοινωνίες ανά τον κόσμο, επισημαίνοντας την ανάγκη για την άμεση έναρξη μιας δυναμικής και παγκόσμιας ανταπόκρισης [13].

Κεφάλαιο 2 Κατηγορίες ηλεκτρονικού εγκλήματος

Με βάση την παραπάνω προσπάθεια που έγινε για την περιγραφή των βασικών ορισμών για το τι είναι κυβερνοέγκλημα και τι ηλεκτρονικό έγκλημα, στο παρόν κεφάλαιο θα προσπαθήσουμε να δώσουμε μια πιο αναλυτική περιγραφή για τις κατηγορίες αυτών των δύο μορφών παραβατικότητας. Παρά το γεγονός ότι δεν υπάρχει κοινά αποδεκτός νομικός ορισμός για το έγκλημα στον κυβερνοχώρο στη διεθνή και εθνική νομοθεσία, φαίνεται ότι οι όροι "έγκλημα που διαπράττεται μέσω ηλεκτρονικών υπολογιστών," "ηλεκτρονικό έγκλημα," ή "έγκλημα στον κυβερνοχώρο" χρησιμοποιούνται εναλλάξ για να περιγράψουν "αξιόποινες ενέργειες που πραγματοποιούνται μέσω ηλεκτρονικών δικτύων επικοινωνίας και πληροφορικών συστημάτων ή εναντίον αυτών των δικτύων και συστημάτων [14]. Συνεπώς η ταξινόμηση των κατηγοριών αυτών θα γίνει με γνώμονα αμφοτέρων. Όμως αρχικά πρέπει να γίνει μια κατηγοριοποίηση των απειλών και των επιθέσεων.

2.1 Ηλεκτρονικό έγκλημα και οι διαφορές του από την παραβίαση ασφάλειας

Ένας περιεκτικός όρος έχει δοθεί από τους Tomas & Loader οι οποίοι αντιλαμβάνονται το κυβερνοέγκλημα ως εκείνες τις δραστηριότητες που διενεργούνται μέσω υπολογιστή και είναι είτε παράνομες είτε θεωρούνται παράνομες από ορισμένα μέρη και μπορούν να διεξαχθούν μέσω παγκόσμιων ηλεκτρονικών δικτύων. Η ειδικότητα του κυβερνοεγκλήματος θεωρείται ότι έγκειται στο νεοσύστατο περιβάλλον αλληλεπίδρασης στο οποίο λαμβάνει χώρα, δηλαδή το 'εικονικό χώρο' (συχνά αποκαλούμενο 'κυβερνοχώρο') που δημιουργείται από την αλληλοσύνδεση των υπολογιστών σε ένα παγκόσμιο δίκτυο ανταλλαγής πληροφοριών, κυρίως το Internet [15].

Η παραβίαση ασφάλειας (violation) ή αλλιώς ρήγμα (breach) μπορεί να θεωρηθεί κάθε συμβάν κατά το οποίο κάποιο αγαθό υφίσταται ζημιά. Ως αγαθό ορίζεται οτιδήποτε χρειάζεται προστασία, λογισμικό ή υλικό. Κατά την παραβίαση ασφαλείας γίνεται παραβίαση των μέτρων ασφαλείας ενός δικτύου ή ενός υπολογιστικού συστήματος. Αυτό μπορεί να συμβεί είτε από κακόβουλες ενέργειες όπως το χάκινγκ (hacking), είτε από ατυχήματα ή παραλείψεις. Η παραβίαση ασφάλειας μπορεί να οδηγήσει στην παράνομη πρόσβαση σε προσωπικά δεδομένα ή επιχειρηματικές πληροφορίες, αλλά δεν είναι απαραίτητα ανάγκη να περιλαμβάνει εγκληματική πρόθεση. Αντιθέτως το ηλεκτρονικό έγκλημα διαπράττεται ηθελημένα μέσω ενεργειών που θεωρούνται παράνομες ή εγκληματικές [16].

2.2 Επιθέσεις

Με τον όρο επίθεση αναφερόμαστε στην προσβολή της ασφάλειας του συστήματος που προέρχεται από μια έξυπνη απειλή δηλαδή, μια ευφυής πράξη που αποτελεί σκόπιμη απόπειρα (ειδικά με την έννοια της μεθόδου ή της τεχνικής) για την παράκαμψη των υπηρεσιών ασφαλείας και την παραβίαση ενός συστήματος. Οι επιθέσεις είναι 2 ειδών :

- Ενεργητικές
- Παθητικές

2.2.1 Ενεργητικές επιθέσεις

Στις ενεργητικές επιθέσεις εντάσσονται επιθέσεις κατά τις οποίες γίνεται κάποια τροποποίηση της ροής δεδομένων, του μηνύματος για παράδειγμα που στέλνει ένας χρήστης σε κάποιον άλλον, ή την δημιουργία μιας ψεύτικης ροής δεδομένων όπως για παράδειγμα μεταξύ μιας ανταλλαγής μηνυμάτων να στέλνει και μια τρίτη οντότητα με την ταυτότητα

ενός εκ των δυο άλλων οντοτήτων οι οποίες θα έπρεπε υπό κανονικές συνθήκες να έχουν την επικοινωνία. Αυτές οι επιθέσεις μπορούν να χωριστούν σε τέσσερις κατηγορίες : μεταμφίεση, επανεκπομπή, τροποποίηση και άρνηση εξυπηρέτησης.

Μεταμφίεση (masquerade)

Στην περίπτωση της μεταμφίεσης, μια οντότητα παριστάνει ψευδώς μια άλλη οντότητα. Συνήθως, αυτή η επίθεση συνδυάζεται με άλλες μορφές επιθέσεων. Για παράδειγμα, μπορεί να γίνει υποκλοπή και επανεκπομπή ακολουθιών πιστοποίησης ταυτότητας μετά από την εκτέλεση μιας έγκυρης ακολουθίας πιστοποίησης, με σκοπό μια εξουσιοδοτημένη οντότητα με περιορισμένα δικαιώματα να αποκτήσει πρόσθετα δικαιώματα παριστάνοντας μια άλλη οντότητα που διαθέτει αυτά τα προνόμια.

Επανεκπομπή (replay)

Περιλαμβάνει την παθητική υποκλοπή μιας μονάδας δεδομένων και στην συνέχεια την αναμετάδοση της ώστε να παράγει ένα μη εξουσιοδοτημένο αποτέλεσμα.

Τροποποίηση μηνυμάτων (modification of messages)

Κατά την επίθεση αυτή μπορούμε να πούμε ότι ένα τμήμα ενός μηνύματος έχει τροποποιηθεί ή ότι τα μηνύματα υπόκεινται σε καθυστέρηση ή αναδιάταξη με σκοπό να δημιουργηθεί ένα αποτέλεσμα που δεν είναι αποδεκτό ή εξουσιοδοτημένο. Παραδείγματος χάριν, ένα μήνυμα το οποίο λέει «Δώσε πρόσβαση στον Γιώργο να επεξεργαστεί τον φάκελο με τα λογιστικά αρχεία» μπορεί να τροποποιηθεί έτσι ώστε να λέει «Δώσε άδεια στον Νίκο να επεξεργαστεί τον φάκελο με τα λογιστικά αρχεία».

Άρνηση εξυπηρέτησης (denial of service – DOS)

Με την άρνηση της εξυπηρέτησης αποτρέπεται ή παρεμποδίζεται η κανονική χρήση και η διαχείριση των επικοινωνιακών δομών. Αυτή η επίθεση μπορεί να έχει συγκεκριμένο σκοπό. Παραδείγματος χάριν, μια οντότητα μπορεί να παρεμποδίζει και να κρατάει τα μηνύματα που προορίζονται για έναν συγκεκριμένο προορισμό. Ένα άλλο παράδειγμα επίθεσης άρνησης εξυπηρέτησης είναι η προσωρινή διακοπή της λειτουργίας ενός ολόκληρου δικτύου είτε με την αχρηστία του, είτε με την υπερφόρτωσή του με μηνύματα, με σκοπό τη σημαντική μείωση της απόδοσής του.

2.2.2 Παθητικές επιθέσεις

Παθητική μπορεί να είναι μια επίθεση κατά την οποία πραγματοποιείται είτε μια υποκλοπή, είτε μια παρακολούθηση μιας μετάδοσης. Ο επιτιθέμενος έχει ως στόχο να αποκτήσει πληροφορίες καθώς εκείνες μεταδίδονται στο δίκτυο. Δύο από τα είδη των παθητικών επιθέσεων είναι η απελευθέρωση του περιεχομένου ενός μηνύματος και η ανάλυση κυκλοφορίας.

Μια τηλεφωνική συνομιλία, ένα email ή ένα αρχείο που μεταφέρεται μέσω του διαδικτύου μπορεί να περιέχει ευαίσθητες ή εμπιστευτικές πληροφορίες. Για αυτόν τον λόγο, είναι σημαντικό να αποφεύγουμε τη διαρροή τέτοιου είδους πληροφοριών σε αντιπάλους ή εχθρούς.

Ένα πιο περίπλοκο είδος παθητικών επιθέσεων είναι η ανάλυση κίνησης. Ας υποθέσουμε ότι έχουμε έναν τρόπο να αποκρύπτουμε τα περιεχόμενα των μηνυμάτων και

άλλων πληροφοριών που διανέμονται μέσω ενός δικτυακού καναλιού, μην επιτρέποντας στον επιτιθέμενο να αντλήσει πληροφορίες από το μήνυμα ακόμα και αν το αποκτήσει. Η πιο διαδεδομένη τεχνική για την απόκρυψη των περιεχομένων της διάδοσης είναι η κρυπτογράφηση. Αν έχει εφαρμοστεί κρυπτογράφηση για προστασία, ο επιτιθέμενος ίσως μπορέσει να παρατηρήσει τη μορφή των μηνυμάτων, να ανιχνεύσει την τοποθεσία και την ταυτότητα των χρηστών που επικοινωνούν, καθώς και τη συχνότητα και το μέγεθος των ανταλλασσόμενων μηνυμάτων. Αυτή η πληροφορία μπορεί να αποδειχθεί χρήσιμη για τη διαμόρφωση ενός σεναρίου σχετικά με τη φύση της επικοινωνίας που λαμβάνει χώρα τη συγκεκριμένη στιγμή.

Κλείνοντας την αναφορά για το είδος των επιθέσεων αξίζει να σημειωθεί ότι, οι παθητικές επιθέσεις είναι πολύ δύσκολο να γίνουν άμεσα αντιληπτές σε σχέση με τις ενεργητικές επιθέσεις. Αυτό οφείλεται στο γεγονός ότι με τις παθητικές επιθέσεις ο επιτιθέμενος δεν προκαλεί τροποποιήσεις των δεδομένων. Τα μηνύματα συνήθως στέλνονται και παραλαμβάνονται με φαινομενικά φυσιολογικό τρόπο, χωρίς να καταλαβαίνει ο αποστολέας και ο παραλήπτης αν το μήνυμα κατά την διάρκεια της αποστολής του έχει διαβαστεί ή έχει παρατηρηθεί το μοντέλο της επικοινωνίας από κάποιον τρίτο. Η μέθοδος της κρυπτογράφησης χρησιμοποιείται συνήθως για να αποτρέψει τέτοιου είδους επιθέσεις, άρα γίνεται αντιληπτό ότι σε τέτοιου είδους επιθέσεις δίνεται περισσότερο έμφαση στην αποτροπή αυτών, παρά στην ανίχνευση.

Οι ενεργητικές επιθέσεις από την άλλη μεριά έχουν ακριβώς αντίθετα χαρακτηριστικά. Μια ενεργητική επίθεση δεν είναι τόσο εύκολο να αποτραπεί όπως μια παθητική επίθεση, αφού κάτι τέτοιο θα απαιτούσε την συνεχή φυσική προστασία όλων των επικοινωνιακών δομών και καναλιών. Αντιθέτως, στόχος είναι η ανίχνευση των επιθέσεων και η ανάκαμψη του δικτύου από τυχόν διακοπή καθυστέρηση και δυσλειτουργία στην κανονική του λειτουργία [17].

2.3 Μορφές ηλεκτρονικού εγκλήματος

Πολλοί ερευνητές και ειδικοί κατανέμουν τα ηλεκτρονικά εγκλήματα σε διάφορες κατηγορίες. Σε μια από αυτές, συγκαταλέγονται τα εγκλήματα σε υπολογιστή, όπως η μη εξουσιοδοτημένη πρόσβαση, σε μια άλλη κατηγορία, εμπίπτουν τα εγκλήματα που σχετίζονται με Η/Υ, όπως η ηλεκτρονική πορνογραφία και η πειρατεία λογισμικού, ενώ σε μια τρίτη κατηγορία, συγκαταλέγονται τα εγκλήματα που διαπράττονται με τη βοήθεια Η/Υ, όπως η απάτη σε ηλεκτρονικές συναλλαγές και η κλοπή στοιχείων πιστωτικών καρτών. Άλλοι επιστήμονες τα κατατάσσουν στα εγκλήματα εκείνα που αποσκοπούν στην καταστροφή των Η/Υ και στα οποία συγκαταλέγονται η κλοπή υλικών στοιχείων ενός Η/Υ, η παραβίαση ηλεκτρονικών αρχείων και ο ψηφιακός βανδαλισμός, καθώς και η εξάπλωση καταστροφικών ιών. Ωστόσο, όλες αυτές οι κατηγορίες, σύμφωνα με τον κύριο Τσουραμάνη, αποτελούν υποκατηγορίες δύο γενικών κατηγοριών. Τα γνήσια ηλεκτρονικά εγκλήματα εκτελούνται αλλά και ερευνώνται αποκλειστικά και μόνο με τη χρήση ψηφιακής τεχνολογίας, ενώ τα παραδοσιακά εγκλήματα διαπραγματεύονται με την υποστήριξη της ψηφιακής τεχνολογίας αλλά και χωρίς αυτήν. [18]. Παρακάτω θα αναλυθούν περισσότερο οι δύο αυτές κατηγορίες αναφέροντας για την καθεμία τις μορφές των ηλεκτρονικών εγκλημάτων που περιέχουν.

2.3.1 Γνήσια ηλεκτρονικά εγκλήματα

Τα γνήσια ηλεκτρονικά εγκλήματα είναι εκείνες οι νέες μορφές εγκλημάτων οι οποίες εμφανίστηκαν με την εμφάνιση των ηλεκτρονικών υπολογιστών και του διαδικτύου .

Ήδη όπως αναφέρθηκε και προηγουμένως, τα ηλεκτρονικά εγκλήματα μπορούν να κατηγοριοποιηθούν σε γνήσια εγκλήματα του κυβερνοχώρου αφού ποινικοποιούνται συμπεριφορές που έχουν σχέση αποκλειστικά με τον κυβερνοχώρο [19].

2.3.1.α Διασπορά κακόβουλου λογισμικού

Με την διασπορά κακόβουλου λογισμικού, στα αγγλικά Malware από τις λέξεις malicious & software, αναφερόμαστε στην διασπορά λογισμικού το οποίο μπορεί να είναι οι Δούρειοι Ίπποι (Trojan Horses), τα Spyware – Adware, τα Ransomware, οι Ηλεκτρονικοί Ιοί (Viruses), τα Ηλεκτρονικά Σκουλήκια (Worms), τα Rootkits, τα Bots – Zombies, τα Dialers, οι Λογικές βόμβες (logic bombs) και τα Βακτήρια (bacteria). Ο κοινός παρονομαστής όλων των παραπάνω είναι η κακόβουλη πρόθεση των δημιουργών τους.

Οι δημιουργοί κακόβουλων προγραμμάτων είναι πλέον πολύ δημιουργικοί. Τα κακόβουλα λογισμικά τους εξαπλώνονται μέσω ευπαθών σημείων σε μη ενημερωμένα συστήματα, διαπερνούν τα μέτρα ασφάλειας, κρύβονται μέσα στη μνήμη ή μιμούνται τις νόμιμες εφαρμογές για να μην εντοπίζονται.

Ωστόσο, ακόμη και σήμερα ένας από τους πιο αποτελεσματικούς τρόπους για τη διάδοση της μόλυνσης είναι ο ασθενέστερος κρίκος της αλυσίδας - δηλαδή ο ανθρώπινος παράγοντας. Καλά γραμμένα μηνύματα ηλεκτρονικού ταχυδρομείου με κακόβουλα συνημμένα έχουν αποδειχθεί ο πιο αποτελεσματικός και φθηνός τρόπος να μολυνθεί ένα σύστημα. Ένα λάθος κλικ αρκεί για την επίτευξη των κακόβουλων στόχων των κυβερνοεγκληματιών .

Υπάρχουν διάφοροι τρόποι με τους οποίους οι δημιουργοί malware δημιουργούν έσοδα από τις κακόβουλες δραστηριότητές τους. Κάποια malware προσπαθούν να γλιστρήσουν μέσα σε ένα σύστημα, να υποκλέψουν όσο το δυνατόν περισσότερα ευαίσθητα δεδομένα τα οποία μετά θα πουληθούν ή θα χρησιμοποιηθούν για να εκβιάσουν το θύμα. Μια δημοφιλής μέθοδος μεταξύ των κυβερνοεγκληματιών είναι η κρυπτογράφηση των δεδομένων ή του δίσκου του χρήστη και η απαίτηση λύτρων για το ξεκλείδωμά του.

Επιπλέον, υπάρχουν ομάδες κυβερνοεγκληματιών που δεν έχουν ως κίνητρο απαραίτητα το οικονομικό κέρδος. Είναι δύσκολο να πούμε πώς κερδίζουν χρήματα για να χρηματοδοτήσουν τις δραστηριότητές τους. Μπορούμε μόνο να υποθέσουμε ότι τα χρήματα προέρχονται από συγκεκριμένες κυβερνήσεις, παράνομες δραστηριότητες του dark web ή ποιος ξέρει τι άλλο. Αυτό που μπορούμε να πούμε με βεβαιότητα είναι ότι ορισμένες από αυτές τις επιχειρήσεις είναι εξελιγμένες, οργανωμένες και καλά χρηματοδοτούμενες [20].

2.3.1.α1 Trojan Horses – Δούρειοι Ίπποι

Ένας δούρειος ίππος από την σκοπιά του κακόβουλου λογισμικού είναι ένας τύπος κακόβουλου λογισμικού το οποίο μπορεί ένας χρήστης να το κάνει λήψη άθελά του αφού, τέτοιου είδους λογισμικά είναι «μεταμφιεσμένα» σαν νόμιμα και ασφαλή λογισμικά. Η μέθοδος που ένας επιτιθέμενος μεταδίδει τέτοιου είδους λογισμικό γίνεται μέσα από ένα μεγάλο εύρος επιθέσεων που στοχεύουν στο να παρθεί ο έλεγχος των ανθρώπινων συναισθημάτων και αλληλεπιδράσεων έτσι ώστε να μπορέσουν να χειραγωγήσουν τον εκάστοτε χρήστη. Αυτό έχει ως αποτέλεσμα να γίνεται απόκρυψη του βλαβερού και επικίνδυνου κώδικα μέσα σε ένα φαινομενικά νόμιμο και ασφαλές πρόγραμμα που μόλις ο χρήστης το εγκαταστήσει στον υπολογιστή του ο επιτιθέμενος θα αρχίσει να έχει πρόσβαση στο σύστημα του κάθε χρήστη που έχει εξαπατηθεί.

Με πιο απλά λόγια δούρειος ίππος ονομάζεται το είδος του κακόβουλου λογισμικού που κρύβεται στις επισυνάψεις ενός email, ή μέσα σε ένα δωρεάν προς λήψη αρχείο-λογισμικό και τα οποία αυτά μεταφέρονται στην συσκευή του χρήστη. Όταν γίνει η λήψη του κακόβουλου κώδικα, αυτός με την σειρά του θα εκτελέσει τις διεργασίες για τις οποίες σχεδιάστηκε από τον επιτιθέμενο, όπως παράνομη πρόσβαση σε εταιρικά συστήματα, κατασκόπηση της δραστηριότητας των χρηστών στο διαδίκτυο και κλοπή ευαίσθητων δεδομένων. Ηλεκτρονικοί υπολογιστές και συσκευές που έχουν μολυνθεί από έναν δούρειο ίππο είναι δύσκολο να γίνουν αντιληπτοί από τους χρήστες καθώς, οι συσκευές συνεχίζουν να δουλεύουν χωρίς κάποιο πρόβλημα.

Σε αντίθεση με τους ηλεκτρονικούς ιούς, ένα κακόβουλο λογισμικό της ομάδας των δούρειων ίππων δεν μπορεί να εκδηλωθεί από μόνο του, για αυτόν τον λόγο χρειάζεται έναν χρήστη να κάνει λήψη το κομμάτι του διακομιστή της εφαρμογής. Αυτό σημαίνει ότι το εκτελέσιμο αρχείο θα πρέπει να εισέλθει σε διαδικασία εφαρμογής και το πρόγραμμα να εγκατασταθεί στο σύστημα του χρήστη έτσι ώστε το κακόβουλο μέρος του κώδικα να μπορέσει να εξαπολύσει επίθεση στο σύστημα αυτό. Όταν ένας δούρειος ίππος διαδίδεται μέσω email, αυτό ανοιχτεί και γίνει λήψη του επιβλαβούς αρχείου που έχει γίνει επισύναψη, ο διακομιστής του κακόβουλου λογισμικού θα γίνει εγκατάσταση στο σύστημα και θα τρέχει αυτόματα κάθε φορά που ο χρήστης ενεργοποιεί τον ηλεκτρονικό του υπολογιστή. Επίσης, αξίζει να σημειωθεί ότι σύμφωνα με αυτό που αναφέρθηκε πριν περί την μετάδοση τέτοιων μορφών λογισμικών μέσα από τεχνικές που στοχεύουν στο να παρθεί ο έλεγχος των ανθρώπινων συναισθημάτων και αλληλεπιδράσεων έτσι ώστε να μπορέσουν να χειραγωγήσουν τον εκάστοτε χρήστη να κατεβάσει και να εγκαταστήσει τέτοιου είδους λογισμικού, αυτό μπορεί να είναι κρυμμένο είτε σε κάποιο κρυφό διαφημιστικό banner, είτε σε κάποια pop-up διαφήμιση, είτε υπερσύνδεσμοι σε κάποιο διαδικτυακό τόπο. Τέλος, πρέπει να αναφερθεί ότι ένας υπολογιστής που έχει μολυνθεί από τέτοιου είδους λογισμικό, μπορεί να το μεταδώσει και σε άλλους υπολογιστές. Ο επιτιθέμενος μπορεί να μετατρέψει τον υπολογιστή αυτόν σε έναν “zombie” υπολογιστή, δηλαδή ο επιτιθέμενος μπορεί να έχει απομακρυσμένη πρόσβαση στον υπολογιστή που έχει μολυνθεί και σε συνδυασμό με την άγνοια που μπορεί να έχει ο χρήστης λόγω της δύσκολης αντίληψης της ύπαρξης τέτοιου είδους λογισμικού, ο επιτιθέμενος μπορεί να συνεχίσει να διαδίδει το κακόβουλο λογισμικού του μέσω διαδικτύου.

Οι πιο γνωστοί τύποι δούρειων ίππων είναι :

- 1) **Backdoor Trojan :** Δίνει την δυνατότητα σε έναν επιτιθέμενο να αποκτήσει απομακρυσμένη πρόσβαση σε έναν υπολογιστή και να πάρει τον έλεγχό του χρησιμοποιώντας μια πίσω πόρτα του συστήματος, δηλαδή μια ευπάθεια. Ο επιτιθέμενος μπορεί να κάνει ότι θελήσει στο σύστημα όπως το να διαγράψει αρχεία, να το επανεκκινήσει τον υπολογιστή, να κλέψει δεδομένα ή και να διαδώσει το κακόβουλό του λογισμικό.
- 2) **Banker Trojan :** Είναι σχεδιασμένο να στοχεύει τους λογαριασμούς τραπεζής των χρηστών και σκοπό έχει να υποκλέπτει δεδομένα λογαριασμών για πιστωτικές και χρεωστικές κάρτες, δεδομένα συστημάτων ηλεκτρονικών πληρωμών και συστημάτων ebanking.
- 3) **Distributed denial-of-service (DDoS) Trojan :** Αυτό το είδος Trojan πραγματοποιεί επιθέσεις οι οποίες υπερφορτώνουν με πακέτα το δίκτυο, δημιουργώντας δυσλειτουργία στην κυκλοφορία των πακέτων μέσα στο δίκτυο. Στέλνει πολλαπλά αιτήματα από έναν υπολογιστή ή μια ομάδα υπολογιστών σε μια διαδικτυακή

διεύθυνση που έχει ως στόχο, για να την κατακλείσει με πακέτα έτσι ώστε να της προκαλέσει δυσλειτουργία στην εξυπηρέτηση των υπόλοιπων χρηστών.

- 4) **Downloader Trojan** : Έχουν ως στόχο υπολογιστές και συσκευές που έχουν ήδη μολυνθεί με κάποιο άλλο malware με αποτέλεσμα να κάνουν λήψη και να εγκαταστήσουν περισσότερα κακόβουλα λογισμικά σε αυτόν τον υπολογιστή, όπως για παράδειγμα συμπληρωματικά ως προς το αρχικό malwares ή κάποιο άλλο είδος malware όπως adware κ.τ.λ.
- 5) **Exploit Trojan** : Περιέχουν κώδικα ή δεδομένα τα οποία θα εκμεταλλευτούν συγκεκριμένες ευπάθειες μιας εφαρμογής ή ενός συστήματος. Ο επιτιθέμενος θα στοχεύσει χρήστες μέσα από την μέθοδο του ηλεκτρονικού ψαρέματος και μετά θα χρησιμοποιήσει ένα τέτοιου είδους δούρειο ίππο για να εκμεταλλευτεί μια γνωστή σε αυτόν ευπάθεια.
- 6) **Fake antivirus Trojan** : Ένας τέτοιος δούρειος ίππος προσομοιώνει τις λειτουργίες ενός ασφαλούς αντιικού προγράμματος . Στην συνέχεια αφού εντοπίσει και αφαιρέσει απειλές όπως ένα συνηθισμένο αντιικό πρόγραμμα, θα απαιτήσει από τον χρήστη χρηματικό ποσό για να καθαρίσει το σύστημά του από απειλές που ίσως να μην υπάρχουν.
- 7) **Game-thief Trojan** : Είναι ειδικά σχεδιασμένα κακόβουλα λογισμικά για να κλέβουν τις πληροφορίες των λογαριασμών των χρηστών παίζοντας ηλεκτρονικά παιχνίδια.
- 8) **Instant messaging (IM) Trojan** : Αυτοί οι δούρειοι ίπποι είναι σχεδιασμένοι για να κλέβουν στοιχεία εισόδου χρηστών που χρησιμοποιούν εφαρμογές και προγράμματα άμεσης ανταλλαγής μηνυμάτων όπως Skype, ICQ, Telegram κ.τ.λ.
- 9) **Infostealer Trojan** : Μπορεί να έχουν δύο χρήσεις. Η μια είναι να χρησιμοποιηθούν για εγκαταστήσουν άλλους δούρειους ίππους μέσα στο σύστημα και η άλλη είναι να αποτρέψει τον χρήστη να εντοπίσει την ύπαρξη ενός malware μέσα στον υπολογιστή του. Τα στοιχεία που συνθέτουν έναν τέτοιου είδους δούρειο ίππο κάνουν δύσκολο τον εντοπισμό του από τις σαρώσεις που πραγματοποιούν τα αντιικά προγράμματα σε τακτά χρονικά διαστήματα.
- 10) **Mailfinder Trojan** : Το είδος αυτό των δούρειων ίππων στοχεύει στο να συλλέξει και να κλέψει όλες τις διευθύνσεις ηλεκτρονικού ταχυδρομείου που έχουν αποθηκευτεί σε έναν υπολογιστή.
- 11) **Ransom Trojan** : Αναζητά να προκαλέσει βλάβη στην λειτουργία ενός υπολογιστή ή να μπλοκάρει δεδομένα μιας συσκευής έτσι ώστε ο χρήστης να μην μπορεί πλέον να έχει πρόσβαση ή να τα χρησιμοποιήσει. Στην συνέχεια, ο επιτιθέμενος θα κρατήσει αυτό το κακόβουλο λογισμικό σε λειτουργία μέχρι ο χρήστης ή ο οργανισμός που έχει μολυνθεί από αυτό πληρώσει το χρηματικό ποσό – λύτρα που απαιτεί ο επιτιθέμενος για να διορθώσει ο χρήστης την βλάβη ή για να του ξεκλειδώσει τα δεδομένα του.
- 12) **Remote access Trojan** : Είναι παρόμοιο με το backdoor Trojan, και δίνει στον επιτιθέμενο τον ολοκληρωτικό έλεγχο του υπολογιστή. Ο κυβερνοεγκληματίας αποκτά πρόσβαση στην συσκευή μέσω μιας δικτυακής σύνδεσης, την οποία χρησιμοποιεί για να κλέψει πληροφορίες ή για να κατασκοπεύσει τον χρήστη.
- 13) **Rootkit Trojan** : Ο τύπος αυτός έχει την ιδιότητα να αποκρύπτεται σε έναν υπολογιστή κάποιου χρήστη. Σκοπός του είναι να κάνει μην ανιχνεύσιμα άλλα κακόβουλα λογισμικά από τον υπολογιστή και ως αποτέλεσμα έχει να διευκολύνει τα κακόβουλα λογισμικά να παραμένουν ενεργά σε έναν υπολογιστή ο οποίος έχει μολυνθεί χωρίς να παρθούν μέτρα αντιμετώπισης για μεγαλύτερο χρονικό διάστημα.

- 14) **Short message service (SMS) Trojan** : Αυτό το είδος προσβάλλει συσκευές κινητών τηλεφώνων και είναι ικανό να στέλνει και να υποκλέπτει γραπτά μηνύματα. Σε αυτό συμπεριλαμβάνεται και η αποστολή μηνυμάτων σε υπερχρεώσιμους τηλεφωνικούς αριθμούς όπως για παράδειγμα σε τηλεφωνικούς αριθμούς που βρίσκονται σε άλλη χώρα.
- 15) **Spy Trojan** : Όπως λέει και το όνομά τους, αυτού του είδους δούρειοι ίπποι είναι σχεδιασμένοι για να μολύνουν έναν υπολογιστή και στην συνέχεια να κατασκοπεύσουν την δραστηριότητα του χρήστη. Σε αυτό συμπεριλαμβάνεται η καταγραφή της δραστηριότητας του πληκτρολογίου, η αποθήκευση εικονικών στιγμιότυπων, η πρόσβαση σε εφαρμογές που χρησιμοποιεί ο χρήστης καθώς και η παρακολούθηση τα δεδομένα πρόσβασης που χρησιμοποιεί ο χρήστης για να συνδεθεί σε κάποια εφαρμογή ή ηλεκτρονική υπηρεσία.
- 16) **Sunburst Trojan** : Αυτός ο δούρειος ίππος κυκλοφόρησε σε πολλές SolarWinds Orion πλατφόρμες. Τα θύματα συμβιβαζόντουσαν με τις μεταμφιεσμένες σε νόμιμες και ασφαλείς εκδόσεις ενός αρχείου των SolarWinds που ονομάζονταν : SolarWinds.Orion.Core.BusinessLayer.dll. Αυτό το αρχείο ήταν μια ευπάθεια για αυτές τις πλατφόρμες. Αν κάποια στιγμή ένας υπολογιστής είχε μπει στο στόχαστρο, θα έμενε αδρανής για ένα χρονικό διάστημα δύο εβδομάδων και μετά με εντολές ανάκτησης θα επέτρεπε στον υπολογιστή να μεταφέρει, να εκτελέσει, να αναγνωρίσει να επανεκκινήσει και να παύσει τις υπηρεσίες του συστήματος. Η επικοινωνία πραγματοποιείται μέσω του http πρωτόκολλου σε προκαθορισμένους υπερσυνδέσμους URL [21].

2.3.1.α2 Computer Viruses – Ηλεκτρονικοί Ιοί

Οι ηλεκτρονικοί ιοί είναι και αυτοί με την σειρά τους ένα είδος κακόβουλου λογισμικού το οποίο μεταδίδεται μεταξύ υπολογιστών και προκαλεί φθορές σε δεδομένα και λογισμικά. Οι ηλεκτρονικοί ιοί στοχεύουν στο να διαταράσσουν τα συστήματα, προκαλώντας μεγάλης έκτασης λειτουργικά προβλήματα που θα οδηγήσουν σε απώλεια και διαρροή δεδομένων. Ένα σημαντικό πράγμα που πρέπει να είναι γνωστό για τους ηλεκτρονικούς ιούς είναι ότι, έχουν σχεδιαστεί να εξαπλώνονται μεταξύ συστημάτων και προγραμμάτων. Τυπικά, οι ιοί είναι προσαρτημένοι σε ένα εκτελέσιμο αρχείο – ξενιστής, το οποίο σαν αποτέλεσμα έχει την εκτέλεση του ιογενή κώδικα όταν αυτό το αρχείο ανοιχτεί. Ο ιός μετά εξαπλώνεται από αρχείο ή το λογισμικό στο οποίο είναι προσκολλημένο μέσω δικτύων, από υπηρεσίες drive για αποθήκευση αρχείων σε clouds, από προγράμματα για διαμοιρασμό εγγράφων και από επισυναπτόμενα αρχεία σε μηνύματα ηλεκτρονικού ταχυδρομείου που περιέχουν το ιό.

Τα κύρια σημάδια που εμφανίζονται σε ένα υπολογιστικό σύστημα όταν αυτό έχει μολυνθεί από κάποιο ηλεκτρονικό ιό είναι :

- Η αργή ταχύτητα του συστήματος. Όταν ένας υπολογιστής έχει μολυνθεί με κάποιον ιό, έχει ως αποτέλεσμα να εκτελεί πιο αργά τις λειτουργίες όπως για παράδειγμα εφαρμογές, προγράμματα ακόμα και η ταχύτητα του δικτύου ίσως επηρεαστεί, σε σχέση με την ταχύτητα που τις εκτελεί υπό κανονικές συνθήκες.
- Ανεπιθύμητα pop-up παράθυρα εμφανίζονται στον υπολογιστή ή σε κάποιο πρόγραμμα περιήγησης.
- Προγράμματα αρχίζουν να εκτελούνται από μόνα τους. Επίσης, κάποιες φορές οι 2 εφαρμογές αποτυγχάνουν να φορτώσουν όταν προσπαθεί ο χρήστης να τα ανοίξει

από την Έναρξη ή από το εικονίδιο συντόμευσης που βρίσκεται στην επιφάνεια εργασίας.

- Αποσύνδεση του χρήστη από έναν λογαριασμό μιας εφαρμογής. Κάποιοι ιοί είναι σχεδιασμένοι να επηρεάζουν συγκεκριμένες εφαρμογές, οι οποίοι θα προκαλέσουν σε αυτές αδυναμία ανταπόκρισης ή θα εξαναγκάζουν τον χρήστη να αποσυνδεθεί αυτόματα από την υπηρεσία τους.
- Η κατάρρευση του συστήματος και οι απενεργοποιήσεις του υπολογιστή από μόνος του είναι και αυτά σημάδια ότι ένας υπολογιστής έχει μολυνθεί με κάποιον ιό. Ακόμα, μπορεί να συμβαίνουν και τα εξής : άνοιγμα αρχείων χωρίς να το επιθυμεί ο χρήστης, πάτημα τυχαίων πλήκτρων του πληκτρολογίου ή και εμφάνιση μηνυμάτων σφάλματος.
- Μεγάλο πλήθος με emails στέλνονται από τον λογαριασμό που έχει ο χρήστης σε υπηρεσίες ηλεκτρονικού ταχυδρομείου. Οι ιοί μπορούν να εξαπλωθούν και μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου αφού κάποιος hacker θα μπορούσε να χρησιμοποιήσει το ηλεκτρονικό ταχυδρομείο άλλων χρηστών για να μεταδώσει το κακόβουλο λογισμικό του και να εκτελέσει κυβερνοεπιθέσεις. Επιπροσθέτως, αν υπάρχουν εξερχόμενα μηνύματα ηλεκτρονικού ταχυδρομείου τα οποία δεν τα έχει στείλει ο χρήστης τότε, θα μπορούσε να είναι σημάδι ηλεκτρονικού ιού.

Ο τρόπος λειτουργίας των ηλεκτρονικών ιών έχει διαφοροποιηθεί με τα χρόνια. Τον πρώτο καιρό που εμφανίστηκαν οι ηλεκτρονικοί υπολογιστές, οι ιοί μεταδιδόντουσαν από υπολογιστή σε υπολογιστή μέσω αποθηκευτικών δισκετών τα γνωστά και ως floppy disks. Στην σύγχρονη εποχή, μπορούν ακόμα οι ιοί να μεταδοθούν μέσω συσκευών αποθήκευσης όπως οι σκληροί δίσκοι και τα usb (Universal Serial Bus), ωστόσο, ο πιο πιθανός και εύκολος τρόπος να εξαπλωθούν είναι μέσω του διαδικτύου. Ο τρόπος που μπορεί να μεταδοθεί ένας ιός είναι όπως προείπαμε μέσω επισυναπτόμενων αρχείων σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου, ή σε άλλες περιπτώσεις μπορεί ο ιός να παραβιάσει το λογισμικό του ηλεκτρονικού ταχυδρομείου και να μεταδοθεί. Άλλοι μπορεί να είναι προσκολλημένοι σε κάποιο άλλο και φαινομενικά ασφαλές λειτουργικό ή να είναι διαθέσιμοι προς λήψη χωρίς ωστόσο να είναι ευρέως γνωστό ότι πρόκειται για ηλεκτρονικό ιό σε διάφορα ηλεκτρονικά καταστήματα εφαρμογών. Το κύριο χαρακτηριστικό που έχουν οι ηλεκτρονικοί ιοί είναι ότι χρειάζονται ένα θύμα για να εκτελέσει τον κώδικά τους, που σημαίνει ότι η εφαρμογή-ξενιστής του ιού πρέπει να έχει εκτελεστεί από τον χρήστη.

Οι κύριοι τύποι ηλεκτρονικών ιών είναι :

- 1) **Οι ιοί που μολύνουν εφαρμογές όταν αυτές εκτελεστούν.** Αυτό το είδος ιών πολλαπλασιάζεται όταν μολύνει εφαρμογές σε έναν υπολογιστή που έχει ήδη μολυνθεί από τον ιό. Σε αντίθετη περίπτωση υπάρχουν οι ιοί που είναι ικανοί να μολύνουν εκτελέσιμα αρχεία κάποιας εφαρμογής χωρίς να εκτελεστεί από τον χρήστη.
- 2) **Οι πολυμερείς ιοί.** Ένας τέτοιος ιός χρησιμοποιεί πολλούς διαφορετικούς τρόπους να μολύνει και να μεταδοθεί από υπολογιστή σε υπολογιστή. Αυτός τυπικά θα παραμείνει στην μνήμη του υπολογιστή και μολύνει τον σκληρό δίσκο. Στην συνέχεια, θα εξαπλωθεί στις εφαρμογές τροποποιώντας το περιεχόμενό τους. Αυτό θα έχει ως αποτέλεσμα την καθυστέρηση στην λειτουργία του συστήματος και στην ανεπάρκεια μνήμης.

- 3) **Οι ιοί άμεσης δράσης.** Οι ιοί αυτοί εισβάλλουν στην κύρια μνήμη ενός υπολογιστή και μολύνουν στην συνέχεια όλα τα προγράμματα, τα αρχεία και τους φακέλους που βρίσκονται στο autoexec.bat μονοπάτι, πριν αυτοί διαγραφούν από μόνοι τους. Τυπικά αυτοί οι ιοί μεταβάλλουν την λειτουργία του συστήματος και είναι ικανοί να καταστρέψουν όλα τα δεδομένα σε όλα τα αποθηκευτικά μέσα που είναι συνδεδεμένα με τον υπολογιστή (σκληροί δίσκοι, usb sticks κτλ.). Οι ιοί άμεσης δράσης είναι εύκολο να εντοπιστούν και μπορούν να αντιμετωπιστούν με την χρήση κάποιου αντιϊκού προγράμματος σαρώνοντας τα αρχεία που έχουν μολυνθεί και αποκαθιστώντας το πρόβλημα.
- 4) **Οι ιοί που παραβιάζουν το πρόγραμμα περιήγησης.** Σε αυτή την περίπτωση, ο επιτιθέμενος αλλάζει τις ρυθμίσεις των προγραμμάτων περιήγησης όπως το να αλλάξει την αρχική σελίδα, να επεξεργαστεί την σελίδα νέας καρτέλας και να αλλάξει την προεπιλεγμένη μηχανή αναζήτησης. Τεχνικά, αυτό το είδος δεν είναι ιός επειδή δεν μπορεί να επηρεάσει με κάποιον τρόπο αρχεία αλλά μπορεί να προκαλέσει εκνευρισμό στον χρήστη ο οποίος δεν θα μπορεί να επαναφέρει την μηχανή αναζήτησης και την αρχική σελίδα της αρεσκείας του. Επίσης, μπορεί να περιέχει και κάποια λογισμικά για διαφημίσεις, τα λεγόμενα adware, τα οποία μπορούν να προκαλέσουν ανεπιθύμητα πολλά αναδυόμενα παράθυρα διαφημίσεων.
- 5) **Οι ιοί επεγγραφών.** Οι ιοί αυτής της κατηγορίας είναι εξαιρετικά επικίνδυνοι, αφού όπως λέει η λέξη επεγγραφή, είναι ικανοί να διαγράψουν δεδομένα και να τα αντικαταστήσουν με δικά τους αρχεία ή κώδικα. Μόλις ένα αρχείο μολυνθεί από τέτοιο ιό, δεν μπορεί να αντικατασταθεί. Ο μόνος τρόπος για να αφαιρεθεί ένας τέτοιος ιός είναι να διαγράψει ο χρήστης όλα τα αρχεία που έχουν μολυνθεί. Αυτό όμως μπορεί να είναι καταστροφικό για το σύστημα αφού μπορεί να διαγραφούν και αρχεία που χρειάζονται για την εύρυθμη λειτουργία του συστήματος. Ο καλύτερος τρόπος να προστατευτεί κάποιος από τους ιούς επεγγραφών είναι να κάνει χρήση αντιϊκού προγράμματος.
- 6) **Οι ιοί web scripting.** Χρησιμοποιώντας τις γλώσσες προγραμματισμού σεναρίων, αυτοί οι ιοί μπορούν να επιτεθούν στην ασφάλεια ενός προγράμματος περιήγησης, επιτρέποντας στον επιτιθέμενο να εισάγει σε ιστοσελίδες κακόβουλο κώδικα. Έτσι ο κυβερνοεγκληματίας καταφέρνει να επιτεθεί σε μεγάλες ιστοσελίδες όπως σελίδες κοινωνικών δικτύων, σελίδες υπηρεσιών ηλεκτρονικού ταχυδρομείου κ.τ.λ. Ο επιτιθέμενος μπορεί να χρησιμοποιήσει το ιό για να στείλει ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου, να διαπράξει δόλιες και ανέντιμες ενέργειες και να καταστρέψει αρχεία κάποιου διακομιστή. Ο τρόπος για να προστατευθεί ένας χρήστης από τέτοιου είδους ιούς είναι να χρησιμοποιήσει σε πραγματικό χρόνο λογισμικό για την προστασία των προγραμμάτων περιήγησης.
- 7) **Οι ιοί που μολύνουν αρχεία.** Αυτοί οι ιοί είναι οι πιο διαδεδομένοι σε σχέση με τα υπόλοιπα είδη ιών. Αυτοί οι ιοί επεγγράφουν αρχεία και εξαπλώνονται αστραπιαία μεταξύ συστημάτων και δικτύων. Κυρίως επηρεάζουν εκτελέσιμα αρχεία, δηλαδή, αρχεία με καταλήξεις .exe και .com. Και εδώ ο καλύτερος τρόπος για να προστατευτεί ο χρήστης από τέτοιου είδους ιούς είναι να κάνει χρήση κάποιου αντιϊκού λογισμικού.
- 8) **Οι ιοί δικτύων.** Η μεγάλη επικινδυνότητα που διέπει αυτούς τους ιούς προκύπτει από το γεγονός είναι ικανοί να «παραλύσουν» και να καταστρέψουν ολόκληρα δίκτυα υπολογιστών. Είναι δύσκολο να ανακαλυφθούν επειδή, οι ιοί αυτοί μπορεί να κρύβονται μέσα σε οποιονδήποτε ηλεκτρονικό υπολογιστή ή σε οποιοδήποτε δίκτυο που έχει μολυνθεί. Ακόμα, αξίζει να σημειωθεί ότι, χαρακτηρίζονται για την ευκολία

τους μεταδοθούν και να αναπαραχθούν χρησιμοποιώντας το διαδίκτυο ως μέσο για μεταφερθούν σε συσκευές που είναι συνδεδεμένες με το δίκτυο. Τα ισχυρά αντιαυτοκινητά λογισμικά και η χρήση εξελιγμένων τεχνολογιών firewalls είναι καίριας σημασίας για την προστασία των χρηστών από τέτοιους ιούς.

- 9) **Οι ιοί που στοχεύουν στον τομέα εκκίνησης ενός υπολογιστή.** Αυτοί οι ιοί στοχεύουν τους τομείς εκκίνησης μιας συσκευής, οι λεγόμενοι και ως Master Boot Record. Ο ιός τοποθετεί τον κώδικά του μέσα στον πίνακα διαχωρισμάτων του σκληρού δίσκου και στην συνέχεια ο ιός μετακινείται στην κύρια μνήμη όπου και περιμένει την στιγμή που θα γίνει επανεκκίνηση στον υπολογιστή. Οι επιπτώσεις που μπορεί να υπάρξουν σε έναν υπολογιστή από την παρουσία ενός τέτοιου ιού είναι προβλήματα κατά την εκκίνηση του υπολογιστή, προβλήματα στην λειτουργία του, ενδεχομένως κάποιες λειτουργίες να μην δουλεύουν σωστά ενώ άλλες μπορεί και καθόλου, και ο σκληρός δίσκος δεν μπορεί να εντοπιστεί μετά από το σύστημα. Οι σύγχρονοι υπολογιστές διαθέτουν πλέον, δικλίδες ασφαλείας για τους τομείς εκκίνησης που περιορίζουν την αποτελεσματικότητα αυτών των ιών. Κάποιες ενέργειες για να προστατευτεί κάποιος χρήστης από τέτοιου είδους ιούς είναι, να σιγουρευτεί ότι οι δίσκοι και τα μέσα αποθήκευσης που χρησιμοποιούνται για την λειτουργία του υπολογιστή είναι προστατευόμενα από εγγραφές ή διαγραφές αρχείων και να μην εκκινεί τον υπολογιστή με συνδεδεμένα εξωτερικά μέσα αποθήκευσης που δεν είναι αξιόπιστα [22].

2.3.1.α3 Worms – Ηλεκτρονικά Σκουλήκια

Τα ηλεκτρονικά σκουλήκι ή αλλιώς worm είναι ένα κακόβουλο πρόγραμμα το οποίο αναπαράγεται αυτόματα από μόνο του και εξαπλώνεται μέσω ενός δικτύου. Για να αποδοθεί πιο σωστά ο ορισμός για το τι είναι ηλεκτρονικό σκουλήκι πρέπει να αναφερθεί ότι τα ηλεκτρονικά σκουλήκια εκμεταλλεύονται ευπάθειες στο λογισμικό ασφαλείας που χρησιμοποιεί ο κάθε χρήστης, έτσι ώστε να κλέψουν πολύτιμες πληροφορίες, να εγκαταστήσουν λογισμικά που εκμεταλλεύονται ευπάθειες του συστήματος και ο επιτιθέμενος να μπορέσει να τις χρησιμοποιήσει, για να αποκτήσει πρόσβαση στο σύστημα, καθώς και να καταστρέψουν διάφορα αρχεία.

Τα ηλεκτρονικά σκουλήκια καταναλώνουν μεγάλη χωρητικότητα μνήμης αλλά και μεγάλο εύρος ζώνης, δηλαδή, τον μέγιστο ρυθμό μεταφοράς δεδομένων ή γνωστό και ως bandwidth. Αυτό οδηγεί σε υπερφόρτωση και κατ' επέκταση σε δυσλειτουργία διακομιστών, ατομικών συστημάτων και δικτύων. Όμως ένα ηλεκτρονικό σκουλήκι είναι διαφορετικό από έναν ιό, επειδή ένα σκουλήκι μπορεί να λειτουργεί από μόνο του σε αντίθεση με έναν ιό που χρειάζεται έναν ηλεκτρονικό υπολογιστή – ξενιστή.

Συνήθως, τα ηλεκτρονικά σκουλήκια μεταφέρονται σε έναν υπολογιστή, αξιοποιώντας πιθανές ευπάθειες που μπορεί να έχει το λογισμικό του. Μπορούν επίσης, να μεταφερθούν μέσω επισυνάψεων ενός μηνύματος ηλεκτρονικού ταχυδρομείου ή ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου ή και μέσω άμεσων μηνυμάτων (IRC). Μόλις ένα αρχείο ανοιχτεί, αυτό είτε θα συνδέσει το χρήστη με κάποια κακόβουλη ιστοσελίδα είτε μπορεί να κατεβάσει το σκουλήκι στον υπολογιστή του χρήστη αυτόματα. Από την στιγμή που το ηλεκτρονικό σκουλήκι βρεθεί μέσα στον υπολογιστή του χρήστη, τον μολύνει χωρίς ο χρήστης να το καταλάβει. Τα ηλεκτρονικά σκουλήκια έχουν την ικανότητα να διαγράφουν και να τροποποιούν αρχεία. Επιπροσθέτως, μπορούν να μεταφέρουν περισσότερα κακόβουλα λογισμικά μέσα σε έναν υπολογιστή ή κάποια άλλη συσκευή.

Κάποιες φορές, η κύρια αποστολή που μπορεί να έχει ένα ηλεκτρονικό σκουλήκι είναι να αναπαραχθεί συνεχόμενα έτσι ώστε να σπαταλήσει όλους τους πόρους του συστήματος όπως το εύρος ζώνης δικτύου (bandwidth) και την χωρητικότητα του σκληρού δίσκου ενός υπολογιστή. Τα ηλεκτρονικά σκουλήκια μπορούν επίσης να υποκλέψουν ευαίσθητα δεδομένα και ανοίξουν τον δρόμο σε κάποιον hacker να αποκτήσει πρόσβαση σε έναν υπολογιστή.

Τα ηλεκτρονικά σκουλήκια μπορούν να ταξινομηθούν ως εξής :

- **Email-worms ή αλλιώς σκουλήκια ηλεκτρονικού ταχυδρομείου.** Σε αυτή την κατηγορία εντάσσονται σκουλήκια που έχουν την ικανότητα να μπορούν να αναπαράγονται από μόνα τους και να εξαπλώνονται μέσω επισυναπτόμενων αρχείων σε μηνύματα ηλεκτρονικού ταχυδρομείου.
- **Instant Messaging-worms ή αλλιώς σκουλήκια άμεσης ανταλλαγής μηνυμάτων.** Είναι ένα είδος ηλεκτρονικού σκουληκιού που μπορεί να μεταδοθεί μέσω δικτύων άμεσης ανταλλαγής μηνυμάτων. Όταν ένα IM-worm βρίσκεται σε λειτουργία, βρίσκει το βιβλίο διευθύνσεων που ανήκει στον χρήστη και προσπαθεί να μεταδώσει μια αντιγραφή του εαυτού του σε όλες τις επαφές του χρήστη, που έχει βρει από το βιβλίο διευθύνσεων.
- **IRC-worms ή αλλιώς σκουλήκια υπηρεσιών συνδιαλέξεων σε πραγματικό χρόνο.** Τα σκουλήκια αυτής της κατηγορίας χρησιμοποιούν τα δίκτυα που χρησιμοποιούνται για υπηρεσίες συνδιαλέξεων πραγματικού χρόνου για να εξαπλωθούν και στους άλλους υπολογιστές που έχουν πάρει μέρος σε μια συνδιάλεξη – συνομιλία. Ένα IRC-worm περνάει ένα script-σενάριο μέσα στον φάκελο IRC του πελάτη που βρίσκεται στον υπολογιστή που έχει μολύνει.
- **NET-worms ή αλλιώς σκουλήκια δικτύων.** Είναι τα σκουλήκια εκείνα τα οποία μπορούν να βρουν νέους ξενιστές-υπολογιστές για να μολύνουν μέσω του διαμοιρασμού αρχείων όταν αυτά μεταβιβάζονται από έναν χρήστη σε κάποιον άλλο μέσα στο δίκτυο. Αυτό ολοκληρώνεται με την χρησιμοποίηση ενός διακομιστή ή κάποιου σκληρού δίσκου όπου πολλαπλοί υπολογιστές έχουν πρόσβαση μέσω ενός τοπικού δικτύου (local-area network - LAN).
- **P2P-worms ή αλλιώς σκουλήκια δικτύων όπου κάθε υπολογιστής μοιράζεται τους πόρους του ισοδύναμα με τους υπόλοιπους υπολογιστές, δηλαδή, έχουν ίσα δικαιώματα.** Ένα τέτοιο σκουλήκι μπορεί να εξαπλωθεί μέσω P2P δικτύων και χρησιμοποιεί P2P διασυνδέσεις για να στείλει αντίγραφα του εαυτού του στους χρήστες [23].

2.3.1.α4 Spyware – Λογισμικό κατασκοπείας

Το λογισμικό κατασκοπείας είναι ένα είδος κακόβουλου λογισμικού που εισβάλλει σε έναν υπολογιστή κάποιου χρήστη, συγκεντρώνει δεδομένα από την συσκευή και τον χρήστη και στην συνέχεια τα στέλνει σε τρίτα πρόσωπα χωρίς την συγκατάθεσή του. Μια κοινά αποδεχόμενη ερμηνεία είναι μια υποκατηγορία κακόβουλου λογισμικού που είναι σχεδιασμένο να αποκτά πρόσβαση και να καταστρέφει μια συσκευή χωρίς την συγκατάθεση του χρήστη. Το λογισμικό κατασκοπείας συλλέγει προσωπικές και ευαίσθητες πληροφορίες οι οποίες στέλνονται σε διαφημιστές, σε εταιρείες συλλογής δεδομένων, ή σε κακόβουλους φορείς για κέρδος. Οι επιτιθέμενοι το χρησιμοποιούν για να παρακολουθήσουν, να κλέψουν και να πουλήσουν δεδομένα χρηστών όπως η χρήση που κάνει ο χρήστης του διαδικτύου,

στοιχεία πιστωτικών καρτών και λογαριασμών τραπεζής, ακόμα και τα διαπιστευτήρια κάποιου χρήστη έτσι ώστε να πλαστογραφήσουν την ταυτότητά του.

Το λογισμικό κατασκοπείας είναι από τις πιο γνωστές και χρησιμοποιούμενες μεθόδους κυβερνοεπιθέσεων καθώς είναι δύσκολο για τους απλούς χρήστες αλλά και τις επιχειρήσεις να τις αναγνωρίσουν και μπορούν να προκαλέσουν σοβαρή βλάβη σε δίκτυα. Επίσης, αφήνει τις επιχειρήσεις ευάλωτες σε παραβιάσεις και κακομεταχειρίσεις δεδομένων. Συχνά, επηρεάζει την εύρυθμη λειτουργία συσκευών και δικτύων και επιβραδύνει την δραστηριότητα του χρήστη. Ο όρος «λογισμικό κατασκοπείας» ξεπρόβαλε πρώτη φορά σε διαδικτυακές συζητήσεις την δεκαετία του 1990, αλλά μόνο στις αρχές της δεκαετίας του 2000 οι εταιρείες που δραστηριοποιούνταν στον τομέα της κυβερνοασφάλειας το χρησιμοποίησαν για να περιγράψουν το ανεπιθύμητο λογισμικό που κατασκοπεύει τους υπολογιστές και την δραστηριότητα των χρηστών. Το πρώτο λογισμικό αντικατασκοπείας κυκλοφόρησε τον Ιούνιο του 2000.

Όλοι οι τύποι λογισμικού κατασκοπείας εισχωρούν στον υπολογιστή κάποιου χρήστη και κατασκοπεύουν την δραστηριότητά του, τους ιστότοπους που επισκέπτεται και τα δεδομένα που συγκεντρώνει ή μοιράζεται. Το κάνουν αυτό με στόχο την εποπτεία της δραστηριότητας του χρήστη, την παρακολούθηση πληροφοριών σύνδεσης και κωδικών και τον εντοπισμό ευαίσθητων δεδομένων. Κάποια λογισμικά κατασκοπείας μάλιστα, είναι ικανά να εγκαθιστούν επιπλέον λογισμικά στην συσκευή του χρήστη, το οποίο δίνει την δυνατότητα στον επιτιθέμενο να κάνει αλλαγές στην συσκευή. Τυπικά όμως, τα λογισμικά κατασκοπείας ακολουθούν μια διαδικασία τριών βημάτων από την στιγμή που αυτά θα εγκατασταθούν σε έναν υπολογιστή μέχρι την στιγμή που θα στείλουν ή θα πουλήσουν σε τρίτους τις πληροφορίες που έχουν υποκλέψει. Τα βήματα αυτά είναι :

1. **Διείσδυση** : Το λογισμικό κατασκοπείας είναι εγκατεστημένο σε μια συσκευή μέσω της χρήσης κάποιου πακέτου εγκατάστασης μιας εφαρμογής, ή μιας κακόβουλης ιστοσελίδας ή και ενός επισυναπτόμενου αρχείου.
2. **Παρακολούθηση και αποθήκευση δεδομένων** : Όταν το λογισμικό κατασκοπείας εγκατασταθεί σε έναν υπολογιστή, ξεκινάει την δουλειά του ακολουθώντας τον χρήστη στο διαδίκτυο, αποθηκεύοντας τα δεδομένα που χρησιμοποιεί, και κλέβοντας τα πιστοποιητικά, τους κωδικούς και τις πληροφορίες σύνδεσης από διάφορους ιστότοπους που έχει επισκεφθεί. Αυτό γίνεται μέσω σύλληψης στιγμιότυπων της οθόνης του, τεχνολογίας πληκτρολόγησης και παρακολούθησης κωδικών.
3. **Αποστολή ή πώληση των δεδομένων** : Με τα δεδομένα και τις πληροφορίες που έχει υποκλέψει, ο επιτιθέμενος θα χρησιμοποιήσει τα δεδομένα αυτά ή για να τα αποθηκεύσει για προσωπική του χρήση ή θα τα πουλήσει σε τρίτα πρόσωπα και οντότητες. Εάν ο επιτιθέμενος κρατήσει τα δεδομένα για προσωπική χρήση τότε, μπορεί να χρησιμοποιήσει τα δεδομένα για πλαστογραφήσει την ταυτότητα των θυμάτων του ή να τα χρησιμοποιήσει ως μέσο για την διεξαγωγή μιας μεγαλύτερης εμβέλειας κυβερνοεπίθεσης σε κάποια επιχείρηση ή οργανισμό. Σε αντίθετη περίπτωση που ο επιτιθέμενος επιλέξει να πουλήσει τα δεδομένα που έχει συλλέξει σε τρίτους τότε, μπορεί να βγάλει οικονομικό κέρδος από την συναλλαγή αυτή με οργανισμούς που ασχολούνται με δεδομένα χρηστών, με άλλους hackers ή αναρτώντας τα στον κόσμο του μαύρου διαδικτύου.

Αξίζει να σημειωθεί ότι, οι πληροφορίες που ένας επιτιθέμενος μπορεί να συλλέξει μέσα από την διαδικασία ενός λογισμικού κατασκοπείας είναι οι ηλεκτρονικές διευθύνσεις και οι

κωδικοί των χρηστών, οι πληροφορίες χρήσης διαδικτύου όπως το ιστορικού κάποιου εξυπηρετητή καθώς και οικονομικές πληροφορίες και προσωπικούς κωδικούς ταυτοποίησης (pins).

Ο επιτιθέμενος προσεκτικά μεταμφιέζει το λογισμικό κατασκοπείας έτσι ώστε να διεισδύσει και να μολύνει κάποιον υπολογιστή, χωρίς να γίνει αντιληπτό. Αυτό επιτυγχάνεται κρύβοντας τα κακόβουλα αρχεία μέσα σε συνηθισμένες λήψεις αρχείων ή ιστοσελίδες που ενθαρρύνουν τον χρήστη να τις ανοίξει, συχνά χωρίς να το συνειδητοποιήσει. Το λογισμικό κατασκοπείας θα καθίσει παραπλεύρως με έμπιστα προγράμματα και ιστοσελίδες, μέσω ευπαθειών του κώδικά τους ή μέσα σε κατά παραγγελία φτιαγμένες δόλιες ιστοσελίδες και εφαρμογές.

Μια συνηθισμένη μέθοδος για την μεταφορά των λογισμικών κατασκοπείας είναι μέσω δεσμίδων πακέτων λογισμικού (bundlware), οι οποίες είναι ενσωματωμένες σε άλλα προγράμματα τα οποία ο χρήστης είτε τα έκανε λήψη είτε τα έχει εγκαταστήσει στον υπολογιστή του. Αυτό έχει ως αποτέλεσμα, να εγκατασταθεί το κακόβουλο λογισμικό κατασκοπείας χωρίς ο χρήστης να το γνωρίζει. Επίσης, κάποιες δεσμίδες λογισμικού αναγκάζουν τον χρήστη να συμφωνήσει στην λήψη μιας ολοκληρωμένης δεσμίδας λογισμικού, που περιέχει κάποιο λογισμικό κατασκοπείας και έτσι ο χρήστης εθελοντικά μολύνει τον υπολογιστή του με τέτοιου είδους λογισμικό. Τέλος, ένα λογισμικό κατασκοπείας μπορεί να διεισδύσει μέσα σε έναν υπολογιστή χρησιμοποιώντας και τις διόδους που χρησιμοποιούν και οι άλλες μορφές κακόβουλου λογισμικού όπως πλαστές ιστοσελίδες και μέσω κακόβουλων επισυναπτόμενων αρχείων κάποιου μηνύματος ηλεκτρονικού ταχυδρομείου.

Τα αποτελέσματα των λογισμικών κατασκοπείας είναι ευρείας γκάμας. Κάποια από αυτά μπορούν να παραμείνουν κρυμμένα, χωρίς ο χρήστης να γνωρίζει ότι ο υπολογιστής του έχει μολυνθεί, για μήνες ακόμα και για χρόνια. Μπορούν ακόμα να προκαλέσουν κάποια ανεπαίσθητα προβλήματα χωρίς ο χρήστης να καταλάβει ότι έχει πέσει θύμα κάποιου επιτιθέμενου. Κάποιες μορφές λογισμικού κατασκοπείας μπορούν να προκαλέσουν μέχρι και οικονομικές ζημιές ή ζημιές στην φήμη του θύματος. Άλλα συνηθισμένα αποτελέσματα που μπορούν να προκαλέσουν τα λογισμικά κατασκοπείας είναι :

1. Κλοπή δεδομένων
2. Πλαστοπροσωπία
3. Ζημιές στις συσκευές των θυμάτων
4. Δυσλειτουργίες στην περιήγηση του χρήστη στο διαδίκτυο.

Κάθε είδος κακόβουλου λογισμικού συγκεντρώνει δεδομένα για τον επιτιθέμενο. Οι πιο απλοί τύποι παρακολουθούν και στέλνουν δεδομένα σε τρίτα πρόσωπα. Οι πιο εξελιγμένοι τύποι όμως λογισμικού κατασκοπείας μπορούν επίσης να κάνουν τροποποιήσεις στο σύστημα του χρήστη που θα οδηγήσουν στη έκθεση των θυμάτων σε επιπλέον απειλές. Μερικοί από τους πιο συνηθισμένους τύπους λογισμικού κατασκοπείας είναι :

1. **Adware – Λογισμικό διαφημίσεων.** Εισχωρεί στον υπολογιστή του χρήστη και παρακολουθεί την δραστηριότητα του. Μόλις συγκεντρώσει δεδομένα του χρήστη, τα στέλνει σε διαφημιστές, ή σε κακόβουλους φορείς ή εμφανίζει κακόβουλες διαφημίσεις.

2. **Infostealer – Υποκλοπέας πληροφοριών.** Αυτός ο τύπος συλλέγει πληροφορίες από την συσκευή του χρήστη. Πραγματοποιεί σάρωση με σκοπό να κλέψει συγκεκριμένα δεδομένα και συνομιλίες από εφαρμογές άμεσης ανταλλαγής μηνυμάτων.
3. **Keylogger – Υποκλοπέας πληροφοριών πληκτρολογίου.** Είναι μια υποκατηγορία του infostealer με την μόνη διαφορά ότι αυτός ο τύπος καταγράφει μόνο πληροφορίες σχετικές με το πληκτρολόγιο, όπως τα πλήκτρα που έχει πατήσει ο χρήστης και στην συνέχεια αποθηκεύει τις κινήσεις αυτές σε ένα κρυπτογραφημένο αρχείο καταγραφής. Με αυτόν τον τρόπο ο επιτιθέμενος μπορεί να συλλέξει δεδομένα που ο χρήστης έχει πληκτρολογήσει στην συσκευή του όπως μηνύματα κειμένου, κωδικούς πρόσβασης και ονόματα χρηστών, δεδομένα μηνυμάτων ηλεκτρονικού ταχυδρομείου κ.τ.λ.
4. **Rootkits.** Αυτός ο τύπος επιτρέπει στον επιτιθέμενο να διεισδύσει βαθιά μέσα σε μια συσκευή, εκμεταλλεύοντας τις ευπάθειες στην ασφάλεια της συσκευής, ή να συνδεθεί ως διαχειριστής. Τα rootkits συχνά είναι δύσκολο ή ακόμα και αδύνατο να εντοπιστούν.
5. **Red shell.** Αυτό το λογισμικό κατασκοπείας εγκαθίσταται από μόνο του σε μια συσκευή ενώ, ο χρήστης κάνει εγκατάσταση κάποια συγκεκριμένα ηλεκτρονικά παιχνίδια και στην συνέχεια παρακολουθεί την δραστηριότητα του θύματος στο διαδίκτυο. Γενικά, χρησιμοποιείται από προγραμματιστές για να βελτιώσουν τα παιχνίδια τους και τις στρατηγικές προώθησης τους.
6. **System monitors – Επιτηρητές συστημάτων.** Και αυτά όπως και οι άλλοι τύποι που αναφέρθηκαν πριν, παρακολουθούν την δραστηριότητα των χρηστών στον υπολογιστή τους και αποθηκεύουν πληροφορίες όπως τα μηνύματα ηλεκτρονικού ταχυδρομείου που έχουν αποσταλεί, κοινωνικά δίκτυα και ιστοσελίδες που έχουν επισκεφτεί οι χρήστες κ.τ.λ.
7. **Tracking cookies.** Τα cookies παρακολούθησης μπορούν να βρεθούν μέσα σε μια συσκευή μέσω ιστοσελίδων που έχει επισκεφθεί κάποιος χρήστης και στην συνέχεια χρησιμοποιούνται για να παρακολουθούν την δραστηριότητα του χρήστη στο διαδίκτυο.
8. **Trojan horses spywares.** Ένα δούρειος ίππος μπορεί να εκτελέσει λειτουργίες και σαν λογισμικό κατασκοπείας [24].

2.3.1.α5 Rootkits

Τα rootkits μπορούν να θεωρηθούν ως μια υποκατηγορία των προαναφερθέντων λογισμικών κατασκοπείας. Είναι ένας τύπος κακόβουλου προγράμματος που επιτρέπει στον κυβερνοεγκληματία, να αποκτήσει πρόσβαση και να διεισδύσει σε δεδομένα κάποιου υπολογιστή, χωρίς να γίνει αντιληπτός. Αυτά τα λογισμικά εμπεριέχουν διάφορες εργαλειακές που είναι σχεδιασμένες να μολύνουν υπολογιστές, να δίνουν τον απομακρυσμένο έλεγχο των υπολογιστών αυτών στον επιτιθέμενο, καθώς και να βοηθήσουν τα λογισμικά αυτά να παραμείνουν κρυμμένα για μεγάλο χρονικό διάστημα. Σαν αποτέλεσμα, τα rootkits είναι ένας από τους πιο δύσκολους τύπους κακόβουλου λογισμικού ως προς τον εντοπισμό τους και την απομάκρυνσή τους, και συχνά χρησιμοποιούνται για κατασκοπεύσουν τους χρήστες και να εξαπολύσουν επιθέσεις σε διάφορες υπολογιστικές μηχανές.

Τα λογισμικά rootkits εμπεριέχουν πολλά κακόβουλα εργαλεία, τα οποία τυπικά περιλαμβάνουν αυτοματοποιημένα υπολογιστικά προγράμματα (bots), για να εξαπολύσουν κατανεμημένες άρνησης εξυπηρέτησης επιθέσεις (Distributed Denial-of-Service), να

υποκλέψουν τραπεζικές και οικονομικές πληροφορίες, κωδικούς και αρχεία καταγραφής ιστορικού δραστηριότητας ηλεκτρολογίου. Συχνά, τα rootkits παρέχουν στον επιτιθέμενο λογισμικά που εκμεταλλεύονται τις ευπάθειες μιας συσκευής και με αυτόν τον τρόπο ο επιτιθέμενος να μπορέσει να αποκτήσει πρόσβαση στον υπολογιστή που έχει μολυνθεί και να αλλάξει ή να διαγράψει λογισμικά και άλλα δομικά στοιχεία του συστήματος όποτε αυτός θελήσει.

Τα rootkits μπορούν να εγκατασταθούν στον υπολογιστή κάποιου χρήστη με διάφορες μεθόδους, αλλά τυπικά αυτό που στοχεύουν είναι μια ευπάθεια στο λειτουργικό σύστημα του υπολογιστή ή ευπάθεια σε κάποια εφαρμογή που είναι εγκατεστημένη στον υπολογιστή. Οι επιτιθέμενοι θα στοχεύσουν σε γνωστές ευπάθειες και κατά την επίθεση σε κάποια συσκευή θα χρησιμοποιήσουν τον κατάλληλο κώδικα που θα τους βοηθήσει να τις εκμεταλλευτούν. Αργότερα, θα εγκαταστήσουν το rootkit και άλλα βοηθήματα που θα τους δώσουν απομακρυσμένη πρόσβαση.

Άλλη μια κοινή μέθοδος εγκατάστασης ενός rootkit είναι μέσω αποθηκευτικών μέσων USB. Ο επιτιθέμενος αφήνει σε δημόσια σημεία το USB stick, με την ελπίδα να το βρει κάποιος αφελής χρήστης και αφού το βρει να το συνδέσει με τον υπολογιστή του. Το κακόβουλο λογισμικό που θα βρίσκεται μέσα στο USB stick, θα εγκατασταθεί σαν μέρος κάποιας νόμιμης και ασφαλούς εφαρμογής ή αρχείου. Όμως πέρα από την κακόβουλη χρήση, ένα rootkit μπορεί να χρησιμοποιηθεί και από οργανισμούς και τους φορείς επιβολής του νόμου για να παρακολουθούν τους εργαζόμενους, ώστε να τους επιτρέψει να ερευνήσουν τους υπολογιστές τους και να αντιμετωπίσουν πιθανές ηλεκτρονικές απειλές [25].

2.3.1.α6 Ransomware

Τα ransomware είναι ένας τύπος κακόβουλου λογισμικού όπου, οι κυβερνοεγκληματίες το χρησιμοποιούν σαν εργαλείο για να κλέψουν ευαίσθητα δεδομένα και να τα κρατήσουν δεσμευμένα, δηλαδή σε ομηρία. Αυτά τα δεδομένα ο κυβερνοεγκληματίας θα τα απελευθερώσει όταν, λάβει ένα χρηματικό ποσό – λύτρα το οποίο έχει ζητήσει. Οι οργανισμοί που είναι πιο ευπαθείς στις επιθέσεις με ransomware, είναι αυτοί που έχουν στην κατοχή τους ευαίσθητα δεδομένα όπως, προσωπικές πληροφορίες, οικονομικά δεδομένα και πνευματική ιδιοκτησία (μουσικά κομμάτια, ταινίες κ.τ.λ.) Τα ransomware χρονολογούνται από την δεκαετία 1980 αλλά δεν έγινε εκτεταμένο θέμα συζήτησης μέχρι τις αρχές του 2000. Σήμερα, οι κυβερνοεπιθέσεις που χρησιμοποιούν σαν εργαλεία τα ransomware είναι οι τρίτες πιο χρησιμοποιούμενες παγκοσμίως. Η εμφάνιση των κρυπτονομισμάτων έκαναν αυτά τα λογισμικά ακόμα πιο ελκυστικά αφού απλοποιούν σημαντικά τον τρόπο πληρωμής των λύτρων για την απελευθέρωση των δεδομένων. Σημαντικό ρόλο έχει και η εξέλιξη της τεχνολογίας αφού οι κυβερνοεγκληματίες συνεχώς βελτιώνουν τις μεθόδους τους για την άμεση πρόσβαση σε δεδομένα και την κρυπτογράφηση τους. Παρόλο που ο σκοπός των ransomware παραμένει ίδιος από τότε που πρωτοεμφανίστηκαν, αυτό που έχει αλλάξει είναι ο τρόπος εξάπλωσής τους. Από τις δισκέτες του 1980, στην μετάδοσή τους μέσω του διαδικτύου με μηνύματα ηλεκτρονικού ταχυδρομείου, με αρχεία προς λήψη, ηχητικά ή βίντεο ακόμα και σε αρχεία εικόνων. Τα τελευταία χρόνια τα ransomware έχουν γίνει πολύτιμο εργαλείο για τους cryptominers, όπου χρειάζονται μεγάλη υπολογιστική ισχύ για την εξόρυξη κρυπτονομισμάτων, και το οποίο το χρησιμοποιούν για να εξαναγκάσουν κάποιον άλλον χρήστη απομακρυσμένα να κάνει αυτός την εξόρυξη των κρυπτονομισμάτων για αυτούς και έτσι να γλιτώσουν το κόστος της υπερόγκης ηλεκτρικής ενέργειας που χρειάζεται.

Οι ενημερώσεις του υλικολογισμικού, δηλαδή του λογισμικού που περιέχει βασικές οδηγίες μηχανής που επιτρέπουν στο υλικό να λειτουργεί και να επικοινωνεί με άλλα λογισμικά που τρέχουν στην συσκευή, επιτρέπει στο υλικό των συσκευών να συνεχίσουν να λειτουργούν αποτελεσματικά και με ασφάλεια. Αυτές οι ενημερώσεις τυπικά εμπλέκουν κάποιο είδος μεταποίησης προγράμματος το οποίο διορθώνει ένα γνωστό σφάλμα ή μπαλώνει συγκεκριμένες ευπάθειες. Όταν ένα ransomware εισέλθει σε έναν υπολογιστή τον μολύνει χωρίς να γίνει αντιληπτό. Το κακόβουλο λογισμικό μετά συνεχίζει με την επίθεση σε αρχεία και εισέρχεται και τροποποιεί τα πιστοποιητικά του χρήστη, χωρίς αυτός να το γνωρίζει. Ως αποτέλεσμα, η υποδομή του υπολογιστή βρίσκεται αποτελεσματικά σε ομηρία από το άτομο που ελέγχει το ransomware.

Με πιο απλά λόγια, αυτό που γίνεται με τα ransomware είναι η κρυπτογράφηση των αρχείων του θύματος, που βρίσκονται στον προσωπικό του υπολογιστή. Συνεπώς, ο χρήστης δεν μπορεί να ψάξει ή να εισέλθει σε αυτά τα αρχεία εάν δεν προβεί σε καταβολή των λύτρων που ζητάει ο επιτιθέμενος. Μάλιστα μερικές φορές, ο επιτιθέμενος κλειδώνει ολόκληρο τον υπολογιστή και στην συνέχεια απαιτεί από τον χρηματικό ποσό για να φανερώσει στο θύμα τον νέο κωδικό. Τέλος, ο επιτιθέμενος με την χρήση των λογισμικών leakware και doxware, απειλεί να βγάλει στην δημοσιότητα ευαίσθητες πληροφορίες που έχει υποκλέψει από το θύμα εάν δεν του καταβληθεί το χρηματικό ποσό που αξιώνει. Επίσης, εταιρείες με ιδιόκτητες πληροφορίες όπως πατέντες και καινοτομίες, μπορούν να θεωρηθούν αγαπημένοι στόχοι για κάποιον κυβερνοεγκληματία που χρησιμοποιεί ransomware, leakware και doxware.

Οι κυβερνοεγκληματίες εστιάζουν συνήθως σε μεσαίας κατηγορίας εταιρείες και επιχειρήσεις, επειδή δεν έχουν επαρκή μέτρα ασφαλείας. Επίσης, τέτοιες επιχειρήσεις δεν έχουν κάποιο τμήμα πληροφορικής και τηλεπικοινωνιών το οποίο μπορεί να εντοπίσει μια κυβερνοεπίθεση με ransomware όταν αυτή συμβεί. Στόχος των ransomware μπορούν να είναι και εταιρείες, όπου η ανάγκη τους για πρόσβαση στα αρχεία τους είναι ζωτικής σημασίας για αυτές και βασίζονται σε βάσεις δεδομένων ή εφαρμογές για τις καθημερινές τους δραστηριότητες. Ωστόσο, γίνεται αντιληπτό ότι ο κάθε χρήστης είτε είναι ολόκληρος οργανισμός είτε ένα μεμονωμένο άτομο που θέλει να κρατήσει τις πληροφορίες του απόρρητες, μπορεί να πέσει θύμα μιας κυβερνοεπίθεσης με ransomware. Επομένως, τα ransomware δεν χρειάζονται να σταλούν απευθείας από τον επιτιθέμενο στον υπολογιστή του θύματος. Αντιθέτως, μπορεί να μεταδοθεί από μόνο του μέσω του διαδικτύου. Για παράδειγμα, κακόβουλος κώδικας μπορεί να εμπεριέχεται σε μια φαινομενικά κανονική διαφήμιση. Ο καθένας μπορεί να πατήσει με τον κέρσορα του πάνω στην διαφήμιση αυτή και να καταλήξει ο υπολογιστής του, το κινητό του τηλέφωνο ή το tablet του μολυσμένο από ransomware. Υπάρχουν διάφοροι τύποι ransomware, ωστόσο οι πιο δημοφιλείς είναι οι παρακάτω:

- **Scareware**. Αυτός ο τύπος κακόβουλου λογισμικού χρησιμοποιεί την κοινωνική μηχανική, για να τρομάξει ή να προκαλέσει κρίσεις άγχους στο θύμα. Το θύμα μετά χειραγωγείται για να αγοράσει λογισμικό που στην πραγματικότητα δεν χρειάζεται. Συχνά τα scareware λένε στον χρήστη ότι έχει εκτεθεί σε έναν ψεύτικο ιό ή κάποιο άλλο είδος κακόβουλου λογισμικού.
- **Screen locking ransomware**. Αυτό το είδος ransomware κλειδώνει την οθόνη του υπολογιστή και με αυτόν τον τρόπο γίνεται αδύνατο για τον χρήστη να έχει πρόσβαση στον υπολογιστή του. Αντί η οθόνη να έχει την συνηθισμένη μορφή της, ο

χρήστης ίσως αντικρίσει ένα μήνυμα όπου ο επιτιθέμενος να απαιτεί χρηματική πληρωμή, πριν επιτρέψει ξανά την πρόσβαση στον χρήστη. Αυτό που προτείνεται από τις αρχές σε αυτούς που έχουν πέσει θύματα ενός τέτοιου ransomware, είναι να μην πληρώσουν το χρηματικό ποσό αλλά να χρησιμοποιήσουν το αντίγραφο ασφαλείας που έχουν κρατήσει, για να επαναφέρουν την συσκευή τους σε μια κατάσταση κατά την οποία δεν είχε μολυνθεί από ransomware.

- **Encrypting ransomware.** Αυτά τα ransomwares χρησιμοποιούν εξελιγμένους αλγορίθμους κρυπτογράφησης, για να κρυπτογραφήσουν τα δεδομένα στην συσκευή του θύματος. Μετά δίνεται μια ειδοποίηση στο θύμα, που εξηγεί πόσα χρήματα πρέπει να δώσει, για να αποκτήσει ξανά πρόσβαση στα αρχεία του. Είναι παρόμοια με τα screen locking ransomwares.
- **Κάποιες αναπτυσσόμενες απειλές.** Όσο παρουσιάζονται νέα μέτρα ασφάλειας, οι κυβερνοεγκληματίες αναπτύσσουν ολοένα και περισσότερους τρόπους για να εισβάλουν σε ατομικούς ή εταιρικούς υπολογιστές. Μια τέτοια απειλή που γίνεται όλο και πιο συνηθισμένη είναι τα Ransomware-as-a-Service (RaaS). Με αυτόν τον τρόπο κάποιος μπορεί να αγοράσει ή να ενοικιάσει ένα ολοκληρωμένο πακέτο ransomware και στην συνέχεια να το απελευθερώσει σε οποιονδήποτε θελήσει. Κάποιες φορές τα κέρδη μοιράζονται με τον πάροχο Raas [26].

2.3.1.α7 Bots-botnets-zombies

Με τον όρο botnet αναφερόμαστε σε μια συλλογή από υπολογιστές, που είναι συνδεδεμένοι αναμεταξύ τους, για να πραγματοποιήσουν μια συγκεκριμένη διεργασία. Τα botnets από μόνα τους δεν είναι απειλή για το δίκτυο των χρηστών. Για παράδειγμα, κάποια botnets εκτελούν χρήσιμες διεργασίες, όπως η διαχείριση δωματίων συνομιλιών ή συνεχόμενη καταγραφή πόντων σε ένα διαδικτυακό παιχνίδι. Όμως, όταν τα botnets κακομεταχειρίζονται για κακόβουλους σκοπούς, μπορούν να γίνουν πολύ επικίνδυνα. Αυτό γίνεται επειδή ένα δίκτυο botnet μπορεί να ελέγξει τον υπολογιστή κάποιου χρήστη και επιπλέον να τον χρησιμοποιήσει για να εκτελέσει κυβερνοεπιθέσεις. Στην ουσία, botnet είναι ένα δίκτυο υπολογιστών που έχουν μολυνθεί από ένα κακόβουλο λογισμικό και είναι υπό τον έλεγχο μιας ομάδας που διενεργεί επιθέσεις, γνωστή και ως “bot-herder”. Κάθε υπολογιστής ξεχωριστά που βρίσκεται υπό τον έλεγχο μιας ομάδας bot-herder ονομάζεται “bot”. Στην ουσία το “bot” είναι μια εφαρμογή που έχει προγραμματιστεί να κάνει συγκεκριμένες διεργασίες, και η εφαρμογή αυτή μπορεί να εκτελεστεί από μόνης ακολουθώντας τις προγραμματιστικές οδηγίες που της έχουν δοθεί, χωρίς να χρειάζεται ένα άτομο για να την εκκινήσει.

Αρχικά, τα botnets δημιουργήθηκαν για να κάνουν τις χρονοβόρες διεργασίες πιο εύκολες. Ένα παράδειγμα ήταν η εποπτεία των δωματίων συνομιλίας και να θέσουν εκτός δωματίου άτομα που έκαναν πράγματα, που δεν ήταν σύμφωνα με τις πολιτικές του δωματίου, όπως η χρήση ακατάλληλης γλώσσας και εκφράσεων. Επειδή όμως, το botnet είχε την ικανότητα να εκτελεί κώδικα μέσα σε κάποιον άλλο υπολογιστή, οι άνθρωποι ξεκίνησαν να το χρησιμοποιούν για την υποκλοπή κωδικών ή για να παρακολουθούν το αρχείο καταγραφής του ιστορικού δραστηριότητας των πληκτρολογίων των χρηστών. Αργότερα τα botnets χρησιμοποιήθηκαν και για την χρησιμοποίηση των υπολογιστών άλλων χρηστών από τους επιτιθέμενους για να εξαπολύσουν επιθέσεις εναντίον ανυποψίαστων συσκευών. Η δημοφιλία των botnets έχει αυξηθεί, επειδή μπορούν να χρησιμοποιηθούν για οικονομικό κέρδος, ελκύοντας το ενδιαφέρον άπληστων κυβερνοεγκληματιών.

Όπως τα περισσότερα συστήματα που είναι βασισμένα στο διαδίκτυο, τα botnets είναι σχεδιασμένα σύμφωνα με αυστηρές δομές. Η δομή των botnets είναι τυπικά βασισμένη, είτε σε μοντέλο client/server – πελάτη/διακομιστή είτε σε peer-to-peer (P2P) μοντέλο όπου όλοι οι κόμβοι έχουν ίσα δικαιώματα.

1. **Client/server μοντέλο.** Με το μοντέλο αυτό ένα δίκτυο καθιερώνεται και ένας μόνος διακομιστής δουλεύει σαν “botmaster” (κύριο μποτ). Αυτός ο διακομιστής στην συνέχεια ασκεί έλεγχο για το πόση πληροφορία θα σταλεί μεταξύ των πελατών, εγκαθιστώντας μια επίθεση διοίκησης και ελέγχου (Command & Control – C&C), πάνω στους υπολογιστές πελάτες. Η επίθεση διοίκησης και ελέγχου (C&C) είναι ένας τύπος επίθεσης, που περιλαμβάνει εργαλεία για να επικοινωνήσει ο επιτιθέμενος με έναν μολυσμένο υπολογιστή ή ένα μολυσμένο δίκτυο και να τα ελέγξει. Το μοντέλο πελάτη/διακομιστή λειτουργεί χρησιμοποιώντας εξειδικευμένο λογισμικό, που επιτρέπει στο botmaster να διατηρεί τον έλεγχο του πάνω στους υπολογιστές πελάτες κάτω από αυτό. Η δομή αυτού το μοντέλου αποτελείται από μόνο ένα κεντρικό σημείο ελέγχου, οπότε μερικοί κυβερνοεγκληματίες επιλέγουν άλλα μοντέλα που είναι δύσκολο να εντοπιστούν και να καταστραφούν. Υπάρχουν τρεις υποκατηγορίες για το μοντέλο πελάτη διακομιστή ανάλογα με την τοπολογία του διακομιστή.

- a. **Τοπολογία δικτύου σε σχήμα αστεριού.** Εδώ χρησιμοποιείται η δομή ακτίνα-κόμβος μέσα σε ένα δίκτυο υπολογιστών. Κάθε εξυπηρετητής είναι συνδεδεμένος με έναν κεντρικό κόμβο στο κέντρο του δικτύου. Ο κεντρικός αυτός κόμβος λειτουργεί σαν αγωγός αποστολής μηνυμάτων στους υπολογιστές μέσα δίκτυο-αστέρι. Τα δεδομένα μέσα στο δίκτυο-αστέρι μεταφέρονται μέσω ενός κεντρικού κόμβου πριν φτάσουν στον τελικό τους προορισμό.
- b. **Τοπολογία δικτύου με πολλούς διακομιστές.** Η δομή αυτών των δικτύων είναι παρόμοια με αυτή των δικτύων-αστέρι, με την μόνη διαφορά ότι υπάρχουν περισσότεροι από έναν διακομιστή που στέλνουν αι λαμβάνουν δεδομένα σε κάθε ένα από τα bots.
- c. **Τοπολογία δικτύου με ιεραρχία.** Στα μοντέλα ιεραρχικών δικτύων, ένας διακομιστής βρίσκεται στην κορυφή της ιεραρχίας των υπολογιστών. Αυτός ο διακομιστής στέλνει και δεδομένα, χρησιμοποιώντας τα άλλα bots χαμηλότερα στην ιεραρχία. Υπάρχει τουλάχιστον έναν επίπεδο διαχωρισμού μεταξύ του διακομιστή και των χαμηλότερων ιεραρχικά bots.

2. **Peer-to-peer (P2P) μοντέλο.** Αυτά τα botnets εμπεριέχουν κάθε συσκευή που είναι συνδεδεμένη στο δίκτυο και κάθε μια από αυτές λειτουργεί ανεξάρτητα, και σαν πελάτης και σαν διακομιστής. Οι συσκευές συντονίζονται με τις υπόλοιπες για να μεταφέρουν και να ενημερώνουν τις πληροφορίες από την μια πλευρά του συστήματος στην άλλη. Επειδή δεν υπάρχει κεντρικός έλεγχος, ένα botnet peer-to-peer είναι ισχυρότερο και δυσκολότερο να εντοπιστεί.

Υπάρχουν διάφοροι τύποι επιθέσεων σε botnets και κάθε μια έχει τα δικά της χαρακτηριστικά. Παρακάτω θα αναφερθεί κάθε τύπος, ανάλογα με το μέσο που χρησιμοποιεί ο καθένας τους.

1. **Botmaster – κύριο bot.** Αναφέρεται σε ένα ξεχωριστό bot το οποίο εκτελεί τις επιθέσεις command & control (C&C) των botnets. Μπορούν να εκτελούν τις

λειτουργίες των botnets απομακρυσμένα και να ξεκινήσουν distributed denial-of-service (DDoS) επιθέσεις ή και άλλους τύπους επιθέσεων. Οι χρήσεις του botmaster των botnets είναι συνήθως εγκατεστημένες σε υπολογιστές, χρησιμοποιώντας διάφορες τεχνικές για απομακρυσμένη εγκατάσταση. Τα botmasters αποκρύπτουν την ταυτότητά τους χρησιμοποιώντας διαμεσολαβούμενους διακομιστές (proxies), μια διεύθυνση IP (Internet Protocol address), ή το λογισμικό ανώνυμης περιήγησης στο διαδίκτυο «The Onion Router» (Tor), το οποίο δουλεύει σε συνδυασμό με το dark web. Τα bots που αναπτύσσει το botmaster, δημιουργούνται έτσι ώστε να επιτρέπουν τις επιθέσεις command & control όταν η λέξη κλειδί ή ο κωδικός εισαχθεί. Όταν τα κλειδιά έρθουν σε συμβιβασμό, οι επιτιθέμενοι μπορούν να διεισδύσουν στα botnets των ανταγωνιστών τους και μετά να εξαπολύσουν επιθέσεις distributed denial-of-service ή και άλλου τύπου επιθέσεις.

2. **Zombies.** Σε μια επίθεση zombie, ένας υπολογιστής που είναι συνδεδεμένος στο διαδίκτυο ελέγχεται από έναν επιτιθέμενο ή ένα κακόβουλο λογισμικό. Το πιο πιθανό είναι η εγκατάσταση του bot να έχει γίνει μέσω ενός δούρειου ίππου (Trojans). Η λειτουργία του υπολογιστή που έχει μολυνθεί γίνεται «παράλογη» όπως ένα zombie, κάνοντάς το ο επιτιθέμενος ή το κακόβουλο λογισμικό που τον ελέγχουν να πραγματοποιεί κακόβουλες ενέργειες.
3. **Spamming – Ανεπιθύμητη ηλεκτρονική αλληλογραφία.** Ένα botnet με αποστολή ανεπιθύμητων μηνυμάτων ηλεκτρονικής αλληλογραφίας (spamming botnet ή spambot), αναφέρεται σε έναν ηλεκτρονικό υπολογιστή ο οποίος διανέμει τα ανεπιθύμητα αυτά μηνύματα σε άλλους υπολογιστές. Αυτά τα emails τείνουν να έχουν διαφημίσεις για προϊόντα όπως πορνογραφία, ψεύτικα αντικαταστάματα ή εμπορεύματα απομιμήσεων. Ακόμα, αυτά τα emails μπορεί να περιέχουν και ηλεκτρονικούς ιούς. Πολλές φορές οι επιτιθέμενοι (spammers) αγοράζουν ένα botnet, που έχει ήδη μολύνει αρκετούς υπολογιστές και στην συνέχεια στέλνουν ανεπιθύμητα ηλεκτρονικά μηνύματα, σε μια προσπάθεια να μολύνουν τις συσκευές αυτές με κάποιο κακόβουλο λογισμικό. Με αυτή την μέθοδο, είναι δυσκολότερο να ανακαλυφθεί από πού πραγματικά προήλθε μια κυβερνοεπίθεση.
4. **Spyware – Λογισμικό κατασκοπείας.** Ένας επιτιθέμενος που χρησιμοποιεί λογισμικό κατασκοπείας, έχει την δυνατότητα μέσω ενός botnet να προτρέψει να κλικαριστούν διαδικτυακοί σύνδεσμοι για διαφημίσεις ή για ιστοσελίδες. Επειδή αυτά τα “clicks” συχνά αποφέρουν έσοδα για τους διαφημιστές, τα spyware botnets μπορούν να χρησιμοποιηθούν από ερηματικούς εγκληματίες για να βγάλουν σταθερό εισόδημα.
5. **Dial-up bots.** Τα dial-up bots λειτουργούν όταν συνδέονται με dial-up modems και τα οποία εξαναγκάζουν να πληκτρολογούν τηλεφωνικούς αριθμούς. Με αυτόν τον τρόπο μπορούν να εγκλωβίσουν μια τηλεφωνική σύνδεση και έτσι να αναγκάσουν τον χρήστη να αλλάξει τηλεφωνικούς αριθμούς. Σε άλλες περιπτώσεις, το botnet μπορεί να καλέσει αριθμούς με ειδική χρέωση, όπως αριθμοί εξωτερικού για παράδειγμα, που δημιουργήσουν στον χρήστη μεγάλο τηλεφωνικό λογαριασμό. Όμως, αυτού του τύπου επιθέσεις χάνουν με την πάροδο του χρόνου την δημοφιλία τους επειδή, τα dial-up modems δεν χρησιμοποιούνται σχεδόν ποτέ.
6. **Web crawler – Ανιχνευτής ιστού.** Το web crawler, γνωστό και ως spider bot, είναι ένα bot στις μηχανές αναζήτησης το οποίο κατεβάζει και καταλογογραφεί τα περιεχόμενα ιστοσελίδων. Ο σκοπός αυτού του είδους bot είναι να καταλαβαίνει για ποιο πράγμα είναι η κάθε ιστοσελίδα. Με αυτόν τον τρόπο, μια ιστοσελίδα μπορεί να ταιριάζει με την αναζήτηση-ερώτημα του χρήστη όταν είναι απαραίτητο. Τα bot αυτά

«έρπονται» σε όλο τον ιστό, συγκεντρώνοντας και οργανώνοντας – κατηγοριοποιώντας πληροφορίες που αφορούν ιστοσελίδες.

2.3.1.α8 Επιθέσεις DDoS

Οι κατανεμημένες άρνησης εξυπηρέτησης επιθέσεις (Distributed Denial-of-Service, DDoS) είναι ένα είδος κυβερνοεγκλήματος κατά το οποίο, ο επιτιθέμενος κατακλύζει έναν διακομιστή με μεγάλη ροή δεδομένων, για να αποτρέψει τους χρήστες να αποκτήσουν πρόσβαση σε διαδικτυακές υπηρεσίες και ιστοσελίδες. Τα κίνητρα για την διεξαγωγή μιας επίθεσης DDoS διαφέρουν σε μεγάλο βαθμό, ανάλογα με το πώς διαφέρουν οι επιτιθέμενοι που θέλουν να διαπράξουν αυτό το είδος κυβερνοεπίθεσης, είτε σε ατομικό επίπεδο είτε σε συλλογικό όπως οι οργανισμοί. Κάποιες επιθέσεις υλοποιούνται από δυσαρεστημένα άτομα για διάφορα κοινωνικά θέματα όπως, οι “hacktivists” , και τα άτομα αυτά θέλουν να θέσουν εκτός λειτουργίας τους διακομιστές μιας εταιρείας, ως έναν τρόπο διαμαρτυρίας ή για δική τους ευχαρίστηση εκμεταλλευόμενοι πιθανές ευπάθειες στην ασφάλεια των συστημάτων.

Τα κίνητρα μιας κατανεμημένης άρνησης εξυπηρέτησης επίθεσης μπορούν να είναι και οικονομικά. Τέτοιες επιθέσεις μπορούν να είναι μεταξύ ανταγωνιστών, διακόπτοντας ή απενεργοποιώντας ολοκληρωτικά τις διαδικτυακές επιχειρηματικές δραστηριότητες μιας επιχείρησης και στο ενδιάμεσο να ξεφύγουν διακριτικά χωρίς να γίνουν αντιληπτοί. Άλλες DDoS επιθέσεις εμπεριέχουν και εκβιασμό, στις οποίες ο δράστης επιτίθεται σε μια εταιρεία και εγκαθιστά λογισμικό ομηρίας (hostageware) ή ransomware στους διακομιστές της και στην συνέχεια την εξαναγκάζει να πληρώσει ένα μεγάλο χρηματικό ποσό για να σταματήσει ή επίθεση - ζημία. Οι επιθέσεις DDoS βρίσκονται σε έξαρση, που ακόμα και κάποιοι από τους μεγαλύτερους κολοσσούς παγκοσμίως δεν μπορούν να μείνουν άτρωτοι από αυτές τις επιθέσεις. Η μεγαλύτερη DDoS επίθεση συνέβη τον Φεβρουάριο του 2020 στην εταιρεία Amazon Web Services (AWS). Οι συνέπειες μιας επίθεσης DDoS περιλαμβάνουν την πτώση της πελατειακής κίνησης, ζημία στην φήμη της εταιρείας ή της επιχείρησης κ.α.

Μια επίθεση DDoS εστιάζει στην υπερφόρτωση των συσκευών, των υπηρεσιών και του δικτύου του επιδιωκόμενου στόχου με ψεύτικη ροή δεδομένων, μετατρέποντας τα μη προσβάσιμα ή άχρηστα για τους νόμιμους χρήστες. Μια κατανεμημένη άρνηση εξυπηρέτησης επίθεση (DDoS) είναι μια υποκατηγορία της ευρύτερης επίθεσης άρνησης εξυπηρέτησης (DoS). Σε μια απλή επίθεση άρνησης εξυπηρέτησης, ο επιτιθέμενος χρησιμοποιεί απλά μια σύνδεση στο διαδίκτυο για να κατακλύσει έναν στόχο με ψεύτικα αιτήματα ή για να προσπαθήσει να εκμεταλλευτεί μια ευπάθεια της κυβερνοασφάλειας. Από την άλλη πλευρά, οι DDoS επιθέσεις είναι μεγαλύτερες σε κλίμακα και χρησιμοποιούν χιλιάδες ή ακόμα και εκατομμύρια συνδεδεμένες συσκευές, για να εκπληρώσουν τον στόχο τους. Η μεγάλη ποσότητα των συσκευών που χρησιμοποιούνται, καθιστούν τις DDoS επιθέσεις δύσκολες να αντιμετωπιστούν.

Όπως αναφέρθηκε και στο κεφάλαιο με τους ιούς bot, ο κύριος τρόπος για να πραγματοποιηθεί μια DDoS επίθεση είναι τα botnets. Ο επιτιθέμενος θα διεισδύσει σε υπολογιστές ή άλλες συσκευές και θα εγκαταστήσει ένα κακόβουλο κομμάτι κώδικα ή λογισμικό, το οποίο ονομάζεται “bot”. Όλοι μαζί οι υπολογιστές που έχουν μολυνθεί από αυτό το κακόβουλο λογισμικό (bot) ονομάζεται “botnet”. Στην συνέχεια ο επιτιθέμενος καθοδηγεί το botnet να κατακλύσει τον διακομιστή και τις συσκευές του θύματος, με περισσότερα αιτήματα σύνδεσης από αυτά που μπορούν να διαχειριστούν. Διαφορετικές επιθέσεις στοχεύουν διαφορετικά μέρη ενός δικτύου και κατηγοριοποιούνται σύμφωνα με τα επίπεδα του δικτύου που έχουν στοχεύσει. Μια σύνδεση δικτύου αποτελείται από επτά

διαφορετικά επίπεδα, όπως καθορίζονται από το μοντέλο OSI (Open Systems Interconnection) που έχει δημιουργηθεί από τον παγκόσμιο οργανισμό τυποποίησης. Το μοντέλο αυτό επιτρέπει διαφορετικοί υπολογιστές να μπορούν να επικοινωνούν μεταξύ τους. Συνεπώς, λαμβάνοντας όλα αυτά υπόψη οι τύποι DDoS επιθέσεων είναι οι εξής :

1. **Ογκομετρικές επιθέσεις.** Αυτός ο τύπος επίθεσης έχει ως στόχο να ελέγξει όλο το διαθέσιμο εύρος ζώνης (bandwidth) μεταξύ του θύματος και του διαδικτύου. Η αυξημένη ροή δεδομένων του ιεραρχικού συστήματος ονοματοδοσίας διαδικτύου (Domain Name System – DNS) είναι ένα παράδειγμα ογκομετρικής επίθεσης. Σε αυτή την περίπτωση, ο επιτιθέμενος πλαστογραφεί την διεύθυνση IP του στόχου του και στην συνέχεια στέλνει ένα αίτημα αναζήτησης ενός ονόματος DNS σε έναν DNS διακομιστή, χρησιμοποιώντας την διεύθυνση IP που έχει πλαστογραφήσει. Όταν ο DNS διακομιστής στείλει την ανταπόκριση με την DNS καταχώρηση, αυτή τελικά θα καταλήξει στον στόχο του επιτιθέμενου από τον οποίο έχει πλαστογραφήσει την διεύθυνση IP. Το αποτέλεσμα είναι ο στόχος να λάβει μια αυξημένη ροή δεδομένων που θα προέρχεται από το αρχικό ερώτημα του επιτιθέμενου.
2. **Επιθέσεις πρωτοκόλλου.** Οι επιθέσεις αυτές καταναλώνουν όλη την διαθεσιμότητα των δικτυακών διακομιστών ή άλλων πόρων, όπως για παράδειγμα τα “firewalls”. Εκθέτουν αδυναμίες στα επίπεδα 3 και 4 του πρωτοκόλλου OSI, καθιστώντας τον στόχο μη προσβάσιμο. Ένα παράδειγμα μιας επίθεσης πρωτοκόλλου είναι το λεγόμενο “SYN flood”, κατά το οποίο ο επιτιθέμενος στέλνει στον στόχο έναν συντριπτικό αριθμό αιτημάτων του πρωτοκόλλου ελέγχου μεταφοράς (Transmission Control Protocol – TCP), χρησιμοποιώντας τις διευθύνσεις IP (Internet Protocol addresses) που έχει πλαστογραφήσει από υπολογιστές που βρίσκονται υπό τον έλεγχό του. Ο διακομιστής του στόχου προσπαθεί να ανταποκριθεί σε κάθε ένα από τα αιτήματα σύνδεσης, αλλά το τελικό αίτημα ποτέ δεν ολοκληρώνεται αφού κατά την διαδικασία αυτή ο διακομιστής έχει ήδη πλημμυρίσει από μεγάλο αριθμό αιτημάτων σύνδεσης.
3. **Επιθέσεις επιπέδου εφαρμογής.** Αυτές οι επιθέσεις έχουν ως σκοπό να εξαντλήσουν ή να υπερφορτώσουν τους πόρους του στόχου αλλά είναι δύσκολο να επισημανθούν σαν κακόβουλες. Συχνά, αναφέρονται σαν DDoS επιθέσεις επιπέδου 7 του μοντέλου OSI και έχουν ως στόχο το επίπεδο κατά το οποίο, οι ιστοσελίδες αρχίζουν να εμφανίζονται σε έναν περιηγητή μέσω της ανταπόκρισης στα αιτήματα του πρωτοκόλλου μεταφοράς υπερκειμένου (Hypertext Transfer Protocol – HTTP). Ένας διακομιστής εκτελεί ερωτήματα βάσεων δεδομένων (databases’ queries), για να εμφανίσει μια ιστοσελίδα. Σε αυτή την μορφή επίθεσης, ο επιτιθέμενος εξαναγκάζει τον διακομιστή του θύματος, να διαχειριστεί περισσότερη πληροφορία από ότι διαχειρίζεται συνήθως. Μια πλημμύρα HTTP (HTTP flood) είναι ένας τύπος επίθεσης επιπέδου εφαρμογής και είναι παρόμοια με την συνεχόμενη ανανέωση καρτελών του περιηγητή σε διαφορετικούς υπολογιστές ταυτόχρονα. Με αυτόν τον τρόπο, ο υπερβολικός αριθμός των HTTP αιτημάτων κατακλύζει τον διακομιστή, έχοντας υλοποιήσει μια DDoS επίθεση[27].

2.3.1.α9 Λογικές βόμβες – Logic bombs

Είναι ένα από τα παλαιότερα είδη προγραμμάτων απειλής, προγενέστερο από τους ιούς (viruses) και τα ηλεκτρονικά σκουλήκια (worms). Οι λογικές βόμβες είναι ένα κομμάτι κώδικα, ο οποίος συνήθως είναι κομμάτι του κώδικα κάποιας νόμιμης εφαρμογής και παραμένει αδρανής μετά την εγκατάσταση της εφαρμογής. Ο κώδικας αυτός θα

ενεργοποιηθεί, όταν συμβούν κάποιες συγκεκριμένες προϋποθέσεις και συνθήκες, οι οποίες θα αποτελέσουν έναυσμα για την έναρξή του. Οι πιο συνηθισμένες λογικές βόμβες είναι οι βόμβες χρόνου. Κατά το παρελθόν οι λογικές βόμβες έχουν χρησιμοποιηθεί σε κυβερνοεπιθέσεις που στόχο έχουν υψηλά πρόσωπα. Σε μια βόμβα χρόνου, το κακόβουλο κομμάτι κώδικα παραμένει κρυμμένο και αδρανοποιημένο μέχρι μια συγκεκριμένη χρονική στιγμή. Σε αυτή την περίπτωση ο επιτιθέμενος μπορεί να τοποθετήσει κακόβουλο λογισμικό σε πολλά συστήματα, χωρίς να γίνουν αντιληπτά μέχρι μια συγκεκριμένη χρονική στιγμή, κατά την οποία «πυροδοτούνται» ηλεκτρονικά [28]. Κάποιες λογικές βόμβες χρησιμοποιούν άλλες αλληλεπιδράσεις του χρήστη ως συνθήκες ενεργοποίησής τους όπως για παράδειγμα η παρουσία ή η απουσία συγκεκριμένων αρχείων, η εκτέλεση μιας εφαρμογής από έναν συγκεκριμένο χρήστη και τέλος όπως ήδη έχουμε αναφέρει μια συγκεκριμένη χρονική στιγμή όπως μια συγκεκριμένη μέρα και ώρα της εβδομάδας. Με την πυροδότηση της, η βόμβα μπορεί να τροποποιήσει ή να διαγράψει δεδομένα ή ολόκληρα αρχεία, να προκαλέσει το «πάγωμα» ενός μηχανήματος, ή να προκαλέσει κάποια άλλη ζημιά. Ένα αξιοσημείωτο παράδειγμα χρήσης μιας λογικής βόμβας είναι η περίπτωση του Tim Lloyd, ο οποίος καταδικάστηκε για την τοποθέτηση μιας λογικής βόμβας στην εταιρεία στην οποία εργαζόταν και που της κόστισε 10 εκατομμύρια δολάρια. Της δημιούργησε χάος, την έβγαλε εκτός προγράμματος και στρατηγικών πλάνων και οδήγησε τελικά στην απόλυση 80 εργαζομένων [29].

2.3.1.α10 Bacteria – Ηλεκτρονικά βακτήρια

Τα ηλεκτρονικά βακτήρια (bacteria) γνωστά και ως ηλεκτρονικά κουνέλια (rabbits), είναι προγράμματα που δεν προκαλούν ζημιά σε κάποιο αρχείο του υπολογιστή. Ο μοναδικός τους στόχος είναι να πολλαπλασιάζονται. Ένα τυπικό ηλεκτρονικό βακτήριο ή ηλεκτρονικό κουνέλι ίσως να μην κάνει τίποτα περισσότερο από να εκτελέσει δύο αντίγραφα του εαυτού σε πολυπρογραμματισμένα συστήματα, ή ίσως να δημιουργήσει δύο νέα αρχεία, το καθένα από τα οποία είναι αντίγραφο από το πρωτότυπο αρχείο του ίδιου του βακτηρίου και τα δυο νέα αυτά αρχεία ίσως δημιουργήσουν με την σειρά του δυο διπλά αντίγραφα του εαυτού τους, και ούτω καθεξής. Τα ηλεκτρονικά βακτήρια αναπαράγονται με γρήγορους ρυθμούς και καταλήγουν στο να εξαντλούν όλη την ισχύ του επεξεργαστή ή τον χώρο της κύριας μνήμης και των δίσκων, μη επιτρέποντας στον χρήστη χρησιμοποιήσει αυτούς τους πόρους. Τα ηλεκτρονικά βακτήρια είναι ο πιο απλός τύπος ηλεκτρονικής απειλής. Οι χρήστες των πρώτων πολυεπεξεργαστικών μηχανών, έτρεχαν αυτά τα προγράμματα είτε για να βγάλουν εκτός λειτουργίας την μηχανή είτε για δουν τι θα συμβεί μετά την εκτέλεση ενός τέτοιου προγράμματος. Υπολογιστές χωρίς αναλογίες και όρια στην χρήση των πόρων τους είναι ευάλωτοι σε αυτού του τύπου επιθέσεις [30].

2.3.1.β Κακόβουλες εισβολές σε δίκτυα υπολογιστών

Μετά του ιούς που αναφέρθηκαν στο προηγούμενο κεφάλαιο, οι πιο διάσημες απειλές για την ασφάλεια ενός υπολογιστή είναι οι εισβολείς (intruders) που είναι ευρέως γνωστοί ως hackers ή crackers. Σε μια πρώιμη μελέτη για την κατανόηση των εισβολών και εισβολέων, ο Anderson προσδιόρισε 3 κατηγορίες εισβολέων :

1. **Μεταμφιεσμένος (masquerader).** Ένα άτομο που δεν έχει την εξουσιοδότηση να χρησιμοποιήσει έναν υπολογιστή, και το οποίο διαπερνά όλους τους ελέγχους πρόσβασης ενός συστήματος για να εκμεταλλευτεί τον λογαριασμό ενός νόμιμου χρήστη.

2. **Παράνομος (misfeasor).** Ένας νόμιμος χρήστης που προσπελάζει δεδομένα, προγράμματα, ή πόρους για τα οποία δεν έχει εξουσιοδότηση για τέτοιου είδους πρόσβαση, ή ο οποίος είναι εξουσιοδοτημένος αλλά κακομεταχειρίζεται τα προνόμιά του.
3. **Κρυφός χρήστης (clandestine user).** Ένα άτομο που αποκτά γενικό έλεγχο εποπτείας ενός συστήματος (supervisor), και τον χρησιμοποιεί για να αποφύγει την παρακολούθηση και τους ελέγχους πρόσβασης, ή για να εμποδίσει τη συλλογή δεδομένων παρακολούθησης.

Ο μεταμφιεσμένος πιθανόν να είναι κάποιος εξωτερικός παρείσακτος, ο παράνομος γενικά είναι κάποιος «εκ των έσω» και ο κρυφός χρήστης μπορεί να είναι και εξωτερικός και εσωτερικός παρείσακτος.

Οι επιθέσεις των εισβολέων ποικίλλουν από ήπιες έως πιο σοβαρές. Στις ήπιες μορφές επιθέσεων κατατάσσονται επιθέσεις που υλοποιούνται από άτομα που απλά θέλουν να εξερευνήσουν τον τομέα των δικτύων και να ανακαλύψουν τι υπάρχει εκεί. Στις σοβαρές επιθέσεις βρίσκονται επιθέσεις όπου ο επιτιθέμενος προσπαθεί να διαβάσει απόρρητα δεδομένα ή να τα τροποποιήσει χωρίς εξουσιοδότηση και να παραβιάσει κάποιο σύστημα [31]. Παρακάτω θα αναλυθεί εκτενώς τι είναι το hacking / cracking.

2.3.1.β1 Hacking

Ο πιο ευρέως αποδεκτός ορισμός για το τι είναι “hacking” ορίζει το hacking ως μια ενέργεια, που θέτει σε κίνδυνο ψηφιακές συσκευές και δίκτυα μέσω μιας μη εξουσιοδοτημένης πρόσβασης σε έναν λογαριασμό ή σε ένα σύστημα υπολογιστή. Το hacking δεν είναι πάντα κακόβουλη ενέργεια, αλλά τις περισσότερες φορές συνδέεται με παράνομη δραστηριότητα και με κλοπή δεδομένων από κυβερνοεγκληματίες. Το hacking αφορά την κατάχρηση των συσκευών όπως οι υπολογιστές, τα κινητά τηλέφωνα (smartphones), τα tablets και των δικτύων, για να προκαλέσουν ζημιά και να καταστρέψουν συστήματα, να κλέψουν και να συγκεντρώσουν πληροφορίες, δεδομένα και αρχεία χρηστών, ή να διακόψουν κάθε είδους δραστηριότητα που έχουν σχέση με δεδομένα.

Μια παραδοσιακή άποψη αυτούς που πραγματοποιούν επιθέσεις hacking, δηλαδή τους hackers, τους περιγράφει σαν μοναχικούς και πονηρούς προγραμματιστές, οι οποίοι έχουν εξαιρετικές δεξιότητες στον προγραμματισμό και στην τροποποίηση του λογισμικού των υπολογιστών και του υλικού των συστημάτων. Αλλά αυτή η περιορισμένη άποψη δεν καλύπτει την αληθινή φύση του hacking. Η εμπειρία των hackers, αυξάνεται ολοένα και περισσότερο, αφού χρησιμοποιούν όλο και πιο αόρατες μεθόδους επίθεσης, οι οποίες είναι σχεδιασμένες να περνούν απαρατήρητες από λογισμικά ασφάλειας και από ομάδες πληροφορικής (IT teams). Είναι επίσης αρκετά επιδέξιοι στο να δημιουργήσουν ένα διάνυσμα επίθεσης, το οποίο μπερδεύει τους χρήστες κάνοντας τους να ανοίξουν κακόβουλες επισυνάψεις ή συνδέσμους και με αυτόν τον τρόπο να δώσουν στους hackers ευαίσθητα προσωπικά δεδομένα. Το διάνυσμα επίθεσης (attack vector) είναι ένα μονοπάτι ή μέθοδος που χρησιμοποιεί ένας hacker για να αποκτήσει πρόσβαση σε έναν υπολογιστή ή ένα δίκτυο εκμεταλλευόμενος πιθανές ευπάθειες του συστήματος. Στη σύγχρονη εποχή το hacking δεν σχετίζεται μόνο με θυμωμένα παιδιά κλεισμένα στο δωμάτιό τους που το υλοποιούν. Αντιθέτως, έχει εξελιχθεί σε μια βιομηχανία πολλών εκατομμυρίων με αρκετά εξελιγμένες και επιτυχημένες τεχνικές [32].

Οι hackers χρησιμοποιούν μια ποικιλία τεχνικών για να επιτύχουν τους στόχους τους. Κάποιες από τις πιο συνηθισμένες μεθόδους είναι :

- **Social engineering – Κοινωνική μηχανική.** Είναι μια τεχνική χειραγώγησης που είναι έτσι σχεδιασμένη ώστε, να εκμεταλλεύεται ένα ανθρώπινο λάθος, για να αποκτηθεί πρόσβαση από τον επιτιθέμενο σε προσωπικές πληροφορίες του χρήστη. Χρησιμοποιώντας ο hacker ψεύτικη ταυτότητα και διάφορα ψυχολογικά κόλπα μπορεί να εξαπατήσει το θύμα αποκαλύπτοντάς του προσωπικές ή οικονομικές του πληροφορίες. Μπορεί ακόμα ο hacker να βασίζεται σε απάτες ηλεκτρονικού ψαρέματος (phishing scams), σε ανεπιθύμητα ηλεκτρονικά μηνύματα είτε ηλεκτρονικού ταχυδρομείου είτε εφαρμογών άμεσης συνομιλίας, ή ακόμα και σε ψεύτικες ιστοσελίδες.
- **Το «σπάσιμο» κωδικών πρόσβασης.** Οι hackers χρησιμοποιούν διάφορους τρόπους για να αποκτήσουν κωδικούς πρόσβασης κάποιου χρήστη. Μια από αυτές τις μεθόδους είναι η γνωστή μέθοδος της δοκιμής και του σφάλματος ή αλλιώς η εξαντλητική δοκιμή κλειδιών – κωδικών (brute force attack). Ο επιτιθέμενος προσπαθεί να μαντέψει κάθε πιθανό συνδυασμό για να μπορέσει να αποκτήσει πρόσβαση. Οι hackers μπορούν ακόμα να χρησιμοποιήσουν απλούς αλγόριθμους, για να παράξουν διαφορετικούς συνδυασμούς για γράμματα, νούμερα και σύμβολα, βοηθώντας έτσι να ταυτοποιήσουν συνδυασμούς κωδικών. Μια άλλη τεχνική που συγκαταλέγεται σε αυτή την κατηγορία είναι οι επιθέσεις λεξιλογίου (dictionary attacks), κατά τις οποίες ένα πρόγραμμα εισάγει συνηθισμένες λέξεις στα πεδία που απαιτούν κάποιο κωδικό πρόσβασης, βοηθώντας έτσι τους hackers να καταλάβουν εάν κάποια από αυτές τις λέξεις είναι η σωστή.
- **Μόλυνση συσκευών και υπολογιστών με κάποιο κακόβουλο λογισμικό.** Ένας hacker μπορεί να διεισδύσει μέσα σε μια συσκευή ενός χρήστη και να εγκαταστήσει κάποιο κακόβουλο λογισμικό. Το πιο πιθανό είναι να στοχεύσουν θύματα μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου ή εφαρμογών άμεσης αποστολής μηνυμάτων και μέσω ιστοσελίδων με περιεχόμενο προς λήψη ή P2P δικτύων.
- **Εκμετάλλευση των μη ασφαλών ασύρματων δικτύων.** Από το να χρησιμοποιήσει ένας hacker κάποιο κακόβουλο λογισμικό για να διεισδύσει στον υπολογιστή κάποιου χρήστη, πολλές φορές είναι προτιμότερο για αυτόν να εκμεταλλευτεί ένα ανοιχτό ασύρματο δίκτυο. Η διαδικασία προστασίας των routers δεν είναι κάτι που ακολουθείται από όλους και αυτό μπορεί να οδηγήσει σε εκμετάλλευση αυτής της κατάστασης από τους hackers, που ψάχνουν για ανοιχτές μη ασφαλείς ασύρματες συνδέσεις. Όταν ένας hacker συνδεθεί σε ένα μη ασφαλές δίκτυο, αποκτά πρόσβαση σε όλες τις συσκευές που είναι συνδεδεμένες σε αυτό το δίκτυο παρακάμπτοντας απλά την βασική ασφάλεια.
- **Πρόσβαση σε έναν υπολογιστή μέσω μιας κερκόπορτας – backdoor.** Οι hackers σε κάποιες περιπτώσεις, δημιουργούν λογισμικό που ψάχνει για απροστάτευτα μονοπάτια μέσα σε συστήματα δικτύων και υπολογιστές. Οι hackers αποκτούν πρόσβαση μέσω αυτών των ευπαθειών, μολύνοντας τον υπολογιστή ή το σύστημα με έναν δούρειο ίππο (trojan horse), ο οποίος δημιουργήθηκε από τους ίδιους τους hackers για να υποκλέψουν σημαντικά δεδομένα χωρίς το θύμα να το καταλάβει.
- **Κατασκοπεία στα μηνύματα ηλεκτρονικού ταχυδρομείου.** Οι hackers μπορούν να δημιουργήσουν κώδικα, ο οποίος τους επιτρέπει να υποκλέψουν και να διαβάσουν emails. Σήμερα, οι περισσότερες εφαρμογές ηλεκτρονικού ταχυδρομείου

χρησιμοποιούν τεχνικές κρυπτογράφησης έτσι ώστε, ακόμα και εάν κάποιος hacker υποκλέψει ένα μήνυμα, να μην μπορέσει να το διαβάσει.

- **Καταγραφή στην πληκτρολόγηση (Logging keystrokes).** Μερικά προγράμματα επιτρέπουν στον επιτιθέμενο να παρακολουθεί κάθε πάτημα στο πληκτρολόγιο που πραγματοποιεί ένας χρήστης. Μόλις ένα τέτοιο πρόγραμμα εγκατασταθεί σε έναν υπολογιστή, αρχίζει να καταγράφει κάθε πάτημα στο πληκτρολόγιο, δίνοντας έτσι στον hacker όλα όσα χρειάζεται για να διεισδύσει μέσα στο σύστημα ή να κλέψει την ταυτότητα του θύματος.
- **Δημιουργία zombies ή bots υπολογιστών.** Όπως αναφέρθηκε και στους ιούς bot αλλά και στις κατανεμημένες άρνησης εξυπηρέτησης επιθέσεις (DDoS), ένας υπολογιστής bot μπορεί να χρησιμοποιηθεί από τον επιτιθέμενο για να στείλει ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου ή να εξαπολύσει DDoS επιθέσεις. Μόλις το θύμα εκτελέσει έναν φαινομενικά αθώο κώδικα, θα δημιουργηθεί μια σύνδεση μεταξύ του υπολογιστή του θύματος και του συστήματος του hacker. Στην συνέχεια, ο hacker μπορεί να χρησιμοποιήσει μυστικά τον υπολογιστή του θύματος για να διαπράξει κάθε είδους ηλεκτρονικού εγκλήματος [33] .

Τυπικά υπάρχουν τέσσερα κίνητρα που οδηγούν έναν κακόβουλο φορέα να επιτεθεί – διεισδύσει σε ιστοσελίδες ή συστήματα :

1. Οικονομικό όφελος μέσω της κλοπής πληροφοριών πιστωτικών καρτών ή από κατάχρηση οικονομικών υπηρεσιών.
2. Εταιρική κατασκοπεία.
3. Η απόκτηση κακοφημίας και σεβασμού για τα ταλέντα του στο hacking.
4. Κρατικά χορηγούμενες επιθέσεις που στοχεύουν στην υποκλοπή επιχειρηματικών πληροφοριών και εθνικών μυστικών πληροφοριών.

Πέρα από αυτά, υπάρχουν πολιτικά παρακινημένοι hackers γνωστοί και ως hacktivists, που στοχεύουν να τραβήξουν την δημόσια προσοχή, διαρρέοντας ευαίσθητες πληροφορίες. Τέτοιοι φορείς είναι οι Anonymous, Lulzsec και WikiLeaks. Αρά σύμφωνα με τα κίνητρα αυτά οι hackers χωρίζονται σε τρεις κατηγορίες :

- **Black Hat Hackers :** Αυτοί είναι οι κακοί του hacking. Οι hackers αυτοί προσπαθούν να ανακαλύψουν ευπάθειες σε συστήματα υπολογιστών και σε λογισμικό, για να τις εκμεταλλευτούν για οικονομικό τους όφελος ή για πιο κακόβουλους σκοπούς όπως, η απόκτηση φήμης, η διεξαγωγή κατασκοπείας σε εταιρείες ή ακόμα και ως μέρος μιας κρατικά χορηγούμενης εκστρατείας hacking. Αυτές οι ενέργειες μπορούν να προκαλέσουν σοβαρές ζημιές και σε μεμονωμένους χρήστες και σε εταιρείες για τις οποίες εργάζονται.
- **White Hat Hackers.** Οι white hat hackers μπορούν να χαρακτηριστούν κατά μια έννοια οι καλοί που προσπαθούν να αποτρέψουν την επιτυχία των κακών hackers (black hat hackers), μέσω του προληπτικού hacking (proactive hacking). Χρησιμοποιούν τις τεχνικές δεξιότητες για να διεισδύσουν σε συστήματα για να αξιολογήσουν και να τεστάρουν το επίπεδο ασφάλειας του δικτύου. Αυτή η διαδικασία είναι γνωστή και ως ηθικό hacking (ethical hacking). Αυτό συνεισφέρει στο να εκτεθούν πιθανές ευπάθειες στα συστήματα πριν οι black hat hackers προλάβουν να τις εντοπίσουν και να τις εκμεταλλευτούν. Οι τεχνικές που χρησιμοποιούν οι white hat hackers είναι παρόμοιες ή ακόμα και ίδιες με τις τεχνικές που χρησιμοποιούν οι black hat hackers, αλλά η διαφορά τους είναι ότι οι white hat

hackers προσλαμβάνονται από εταιρείες ή οργανισμούς, για να τεστάρουν και να ανακαλύψουν ενδεχόμενες τρύπες στην ασφάλειά τους.

- **Gray Hat Hackers.** Βρίσκονται στην κλίμακα κάπου μεταξύ των black hat hackers και των white hat hackers. Σε αντίθεση με τους black hat hackers, οι gray hat hackers προσπαθούν να παραβιάσουν ήθη και αρχές χωρίς όμως να επιδιώξουν να βλάψουν κάποιον ή για να κερδίσουν χρήματα. Οι ενέργειές τους τυπικά υλοποιούνται για το κοινό καλό. Για παράδειγμα, μπορούν να εκμεταλλευτούν μια ευπάθεια για να ευαισθητοποιήσουν το κοινό για ένα ζήτημα, αλλά το κάνουν δημόσια και όχι ιδιωτικά όπως οι white hat hackers [32].

2.3.1.β2 Cracking

Το “cracking” πρακτικά είναι ακριβώς το ίδιο με το hacking καθώς και τα αποτελέσματά τους είναι τα ίδια. Το cracking συγκεκριμένα είναι η προσπάθεια της παράνομης πρόσβασης σε έναν υπολογιστή με στόχο την κλοπή, την καταστροφή ή την παράνομη προβολή δεδομένων. Τα μέσα ενημέρωσης θεωρούν όλες αυτές τις ενέργειες hacking, αλλά οι hackers έχοντας μια υπεροψία θεωρούν τους εαυτούς τους ειδικούς και ότι αποτελούν την αφρόκρεμα των προγραμματιστών, υποστηρίζοντας ότι μια τέτοια ενέργεια πρέπει να λέγεται cracking [34].

2.3.1.γ Phishing – Ηλεκτρονικό Ψάρεμα

Ηλεκτρονικό «ψάρεμα» (phishing) είναι όταν ένας κυβερνοεγκληματίας προσπαθεί να ξεγελάσει χρήστες στο να κάνουν κάποιες λάθος κινήσεις. Οι κινήσεις αυτές μπορεί να είναι το άνοιγμα ενός κακόβουλου συνδέσμου ο οποίος θα κατεβάσει στον υπολογιστή του χρήστη κάποιο κακόβουλο λογισμικό ή θα οδηγήσει τον χρήστη σε έναν επικίνδυνο ιστότοπο. Το ηλεκτρονικό «ψάρεμα» μπορεί να εκτελεστεί μέσω μηνυμάτων κειμένου, από τα μέσα κοινωνικής δικτύωσης, ή μέσω τηλεφώνου, αλλά ο όρος ηλεκτρονικό «ψάρεμα» χρησιμοποιείται κυρίως για να περιγράψει επιθέσεις εξαπάτησης μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου (emails). Τα emails ηλεκτρονικού ψαρέματος μπορούν να σταλούν σε εκατομμύρια χρήστες ταυτόχρονα, και κρύβονται ανάμεσα σε πάρα πολλά emails που λαμβάνει ένας πολυσύχολος χρήστης. Μέσω του ηλεκτρονικού «ψαρέματος» μπορεί να γίνει εγκατάσταση κάποιου άλλου είδους κακόβουλου λογισμικού στον υπολογιστή ενός χρήστη όπως ransomware, δολιοφθορά στο σύστημα ή ακόμα και να κλαπεί περιουσία πνευματικών δικαιωμάτων και χρήματα [35].

Σύμφωνα με την επίσημη ιστοσελίδα της Microsoft, οι επιθέσεις ηλεκτρονικού «ψαρέματος» αποσκοπούν στην υποκλοπή και την καταστροφή ευαίσθητων δεδομένων, μέσω της εξαπάτησης των θυμάτων ώστε να αποκαλύψουν προσωπικές τους πληροφορίες όπως κωδικούς πρόσβασης και αριθμούς πιστωτικών καρτών. Οι επιθέσεις ηλεκτρονικού «ψαρέματος» προέρχονται από απατεώνες, που είναι μεταμφιεσμένοι σε έμπιστες πηγές και μπορούν να διευκολύνουν την πρόσβαση σε όλους τους τύπους ευαίσθητων δεδομένων. Οι πιο διαδεδομένοι τύποι ηλεκτρονικού «ψαρέματος» είναι :

- **Ηλεκτρονικό "ψάρεμα" μέσω ηλεκτρονικού ταχυδρομείου.** Η πιο συνηθισμένη μορφή ηλεκτρονικού "ψαρέματος". Αυτός ο τύπος επίθεσης χρησιμοποιεί τακτικές, όπως ψεύτικες υπερ-συνδέσεις, για να παρασύρει τους παραλήπτες ηλεκτρονικού ταχυδρομείου να μοιραστούν τις προσωπικές τους πληροφορίες. Οι επιτιθέμενοι συχνά μεταμφιέζονται σε έναν μεγάλο πάροχο λογαριασμών, όπως η Microsoft ή η Google, ή ακόμη και σε έναν συνάδελφο.

- **Ηλεκτρονικό "ψάρεμα" με κακόβουλο λογισμικό.** Μια άλλη συχνά χρησιμοποιούμενη μορφή ηλεκτρονικού "ψαρέματος". Αυτός ο τύπος επίθεσης περιλαμβάνει την τοποθέτηση κακόβουλου λογισμικού μεταμφιεσμένου σε ένα αξιόπιστο και ασφαλές συνημμένο αρχείο (όπως ένα βιογραφικό σημείωμα ή μια τραπεζική δήλωση) σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου. Κάποιες φορές, το άνοιγμα και η εκτέλεση ενός συνημμένου κακόβουλου λογισμικού μπορεί να παραλύσει ολόκληρα συστήματα πληροφορικής.
- **Εστιασμένο ηλεκτρονικό «ψάρεμα».** Ενώ οι περισσότερες επιθέσεις ηλεκτρονικού «ψαρέματος» έχουν ως κύριο στόχο κάθε χρήστη ανεξαρτήτως, το εστιασμένο ηλεκτρονικό "ψάρεμα" στοχεύει σε συγκεκριμένα άτομα, αξιοποιώντας πληροφορίες που συλλέγονται μέσω έρευνας σχετικά με την εργασία και την κοινωνική τους ζωή. Αυτές οι επιθέσεις είναι ιδιαίτερα εξατομικευμένες, γεγονός που τις καθιστά ιδιαίτερα αποτελεσματικές στην παράκαμψη της βασικής ασφάλειας από απειλές στον κυβερνοχώρο.
- **Ηλεκτρονικό "ψάρεμα" λογαριασμών υψηλών προσώπων.** Πολλές φορές οι επιθέσεις ηλεκτρονικού ψαρέματος στοχεύουν υψηλά και σημαντικά πρόσωπα, όπως ένα στέλεχος επιχείρησης ή μια διασημότητα. Αυτό ονομάζεται ηλεκτρονικό "ψάρεμα" εξεχόντων λογαριασμών. Αυτοί του είδους οι επιτιθέμενοι συχνά πραγματοποιούν σημαντική έρευνα σχετικά με τους στόχους τους, έτσι ώστε να μπορέσουν να βρουν την κατάλληλη στιγμή για να κλέψουν τις ευαίσθητες τους πληροφορίες, τα στοιχεία σύνδεσης αριθμούς λογαριασμών τραπεζής κ.τ.λ.
- **Smishing (Ηλεκτρονικό "ψάρεμα" μέσω SMS).** Το smishing προέρχεται από την ένωση των λέξεων "SMS" και "phishing". Περιλαμβάνει την αποστολή μηνυμάτων κειμένου μεταμφιεσμένων σε αξιόπιστη επικοινωνία από επιχειρήσεις μεγάλου κύρους όπως η Amazon ή η FedEx. Οι άνθρωποι είναι ιδιαίτερα ευάλωτοι σε απάτες με SMS, καθώς τα μηνύματα κειμένου έχουν την μορφή απλού κειμένου και μοιάζουν πιο προσωπικά.
- **Φωνητικό "ψάρεμα" (Vishing).** Στις επιθέσεις vishing, οι επιτιθέμενοι, χρησιμοποιώντας ψεύτικα τηλεφωνικά κέντρα, επιχειρούν να παραπλανήσουν τους χρήστες ώστε να δώσουν ευαίσθητες πληροφορίες μέσω τηλεφώνου. Σε πολλές περιπτώσεις, αυτές οι απάτες χρησιμοποιούν κοινωνική μηχανική (social engineering) για να εξαπατήσουν τα θύματα ώστε να εγκαταστήσουν κακόβουλο λογισμικό στις συσκευές τους με τη μορφή μιας εφαρμογής [36].

2.3.1.δ Spamming – Ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου

Με τον όρο "Spamming" αναφερόμαστε σε μεταφορά και διάδοση ανεπιθύμητων μηνυμάτων. Ο όρος αυτός αναφέρεται συνήθως σε ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου (emails), αλλά μπορούν να συμπεριληφθούν και άλλοι τύποι επικοινωνιών όπως, τα μηνύματα κειμένου sms, μηνύματα εφαρμογών άμεσης ανταλλαγής μηνυμάτων, τα posts σε μέσα κοινωνικής δικτύωσης κ.α. Εκτός από την ενόχληση και τον εκνευρισμό, τα ανεπιθύμητα μηνύματα μπορούν να προκαλέσουν και άλλες σημαντικές ζημιές, όπως για παράδειγμα μπορούν να μολύνουν ολόκληρα υπολογιστικά συστήματα με κακόβουλο λογισμικό προκαλώντας τους μεγάλη ζημιά. Οι κυβερνοεγκληματίες που χρησιμοποιούν την μέθοδο των ανεπιθύμητων μηνυμάτων για να επιτεθούν σε ένα σύστημα ονομάζονται "spammers" και χαρακτηρίζονται από εφευρετικότητα και σκληράδα. Οι spammers προσπαθούν να δημιουργήσουν ένα δόλωμα ολοένα και πιο ελκυστικό έτσι ώστε να πείσουν όσους περισσότερους χρήστες μπορούν, να ανοίξουν τα μηνύματά τους που περιέχουν κάποιο κακόβουλο λογισμικό. Ακόμα προσπαθούν να βρίσκουν συνεχώς νέες διευθύνσεις

ηλεκτρονικού ταχυδρομείου και νέα μέσα επικοινωνίας από τα οποία θα διαδώσουν τα ανεπιθύμητα μηνύματά τους.

Οι επιθέσεις spamming εκμεταλλεύονται συνήθως αδυναμίες και ευπάθειες του πρωτοκόλλου SMTP (Simple Mail Transfer Protocol). Το SMTP είναι ένα βασικό πρωτόκολλο που χρησιμοποιείται για να μεταφερθούν μηνύματα μεταξύ δύο μέσων που βρίσκονται σε επικοινωνία, γνωστά και ως Message Transfer Agents (MTA). Ο MTA του αποστολέα δέχεται μηνύματα από τελικούς χρήστες και τα παραδίδει στον αντίστοιχο MTA του παραλήπτη, ο οποίος χρησιμοποιεί και αυτός το πρωτόκολλο SMTP. Παρ' όλα αυτά η χρήση του SMTP πρωτοκόλλου έχει και κάποιες αδυναμίες, τις οποίες εκμεταλλεύονται οι spammers τα μηνύματα αυτά. Η πιο σοβαρή αδυναμία που έχει το πρωτόκολλο SMTP είναι ότι δεν παρέχει κανέναν έλεγχο ταυτότητας του αποστολέα για να γίνει η επαλήθευση της αυθεντικότητάς του. Οι άλλες αδυναμίες που έχει αυτό το πρωτόκολλο και χρησιμοποιούνται από τους spammers και χρησιμοποιούνται από τους spammers είναι τα open relays και open proxies.

Ένας διακομιστής SMTP θεωρείται ότι είναι ενεργός με δυνατότητα αναμετάδοση ή αλλιώς “relay-enabled” εάν, δέχεται μηνύματα από οποιονδήποτε τομέα εκτός της καθορισμένης λίστας διευθύνσεων και τα προωθεί. Άρα, το SMTP χρησιμοποιείται από τους αποστολείς των ηλεκτρονικών μηνυμάτων για να επικοινωνήσουν με τον SMTP διακομιστή και αυτός στην συνέχεια προωθεί τα μηνύματα αυτά στους παραλήπτες. Πλέον, οι SMTP διακομιστές χρησιμοποιούν διάφορες δικλείδες ασφαλείας για εξακρίβωση της ταυτότητας των χρηστών που στέλνουν τα μηνύματα. Στην περίπτωση όμως που δεν υπάρχουν αυτές οι δικλείδες ασφαλείας για την επαλήθευση των αποστολέων στους SMTP διακομιστές και ο κάθε αποστολέας μπορεί να στείλει την αλληλογραφία του σε οποιονδήποτε χρήστη τότε, η αναμετάδοση του SMTP είναι ανοιχτή ή αλλιώς “relay-open”. Οι spammers μπορούν να χρησιμοποιήσουν το relay-open και στείλουν τα μηνύματά τους ανώνυμα, παρακάμπτοντας τα φίλτρα ανεπιθύμητης αλληλογραφίας καθώς δεν υπάρχουν περιορισμοί στην προώθηση μηνυμάτων ηλεκτρονικού ταχυδρομείου από τον ένα τομέα στον άλλον. Ωστόσο, αυτό το πρόβλημα ήταν συχνότερο στο παρελθόν αφού τα λογισμικά που χρησιμοποιούν SMTP περιέχουν πλέον αρκετούς μηχανισμούς ασφαλείας.

Αντίστοιχο με το “open relays” είναι και το “open proxies”. Ένας διακομιστής μεσολάβησης πρέπει να δέχεται μηνύματα και αιτήματα μόνο από τους δικούς του πελάτες, είτε χρησιμοποιώντας κάποιος έλεγχο ταυτότητας, είτε αναγκάζοντας τους να συνδεθούν με ένα συγκεκριμένο μέγεθος διεύθυνσης IP. Αν ο διακομιστής δεν λάβει αυτούς τους περιορισμούς για να περιορίσει την ομάδα πελατών του και επιτρέψει σε οποιονδήποτε πελάτη να τον χρησιμοποιήσει, τότε ονομάζεται ανοιχτός διακομιστής μεσολάβησης ή αλλιώς “open proxy server”. Ένας τέτοιος διακομιστής έχει την δυνατότητα να δέχεται συνδέσεις πελατών με οποιαδήποτε διεύθυνση IP και να του επιτρέπει να κάνει συνδέσεις σε οποιονδήποτε τομέα του διαδικτύου επιθυμεί. Άρα, γίνεται αντιληπτό ότι οι διακομιστές αυτοί λειτουργούν σαν τυφλοί ενδιάμεσοι προς άλλες διευθύνσεις IP, χωρίς να χρησιμοποιούν κάποιον έλεγχο ταυτότητας. Με αυτόν τον τρόπο τα “open proxies” χρησιμοποιούνται από τους spammers για να στείλουν μεγάλο αριθμό μηνυμάτων χρησιμοποιώντας πλαστές ταυτότητες, αλλά και για να συνδεθούν ανώνυμα σε έναν διακομιστή αλληλογραφίας. Το αποτέλεσμα είναι ότι οποιοδήποτε μήνυμα αποστέλλεται με αυτόν τον τρόπο, ο παραλήπτης βλέπει ότι προέρχεται από τον proxy server και όχι από την πραγματική διεύθυνση IP. Τέλος, ένας open proxy server μπορεί να χρησιμοποιηθεί και ως μέσο για να παρακαμφθούν διάφορα φίλτρα που εστιάζουν σε ονόματα τομέα (domain names) και σε IP διεύθυνση (IP address).

Αξιο αναφοράς είναι και το γεγονός ότι οι spammers πολλές φορές χρησιμοποιούν και τους υπολογιστές zombies για να διαμοιράσουν την ανεπιθύμητη αλληλογραφία τους. Σε αυτή την περίπτωση οι υπολογιστές αυτοί λέγονται “spam zombies” που έχουν ευρυζωνική σύνδεση και ελέγχονται απομακρυσμένα από τους spammers για να ξεκινήσουν μια μαζική αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου. Ο απομακρυσμένος αυτός έλεγχος επιτυγχάνεται μέσω του “Trojan Remote Access” (RAT).

Τα ανεπιθύμητα μηνύματα - spam μπορούν να κατηγοριοποιηθούν σε τέσσερις κατηγορίες :

1. **Spoofed Name** : Αυτή η εκδοχή είναι η συνηθέστερη και αντιπροσωπεύει το 75% των επιθέσεων. Χρησιμοποιείται το όνομα του πλαστογραφημένου - spoofed στελέχους στο πεδίο «from». Όμως η διεύθυνση του email προέρχεται από εξωτερική υπηρεσία, όπως το Hotmail, και ανήκει στον επιτιθέμενο.
2. **Reply-To Spoofing** : Αυτή η τεχνική χρησιμοποιεί το πραγματικό όνομα και email του αποστολέα που πλαστοπροσωπείται. Το όνομα στο «Reply-to» χρησιμοποιεί επίσης το όνομα του πλαστοπροσωποποιημένου αποστολέα. Όμως η διεύθυνση «απάντηση σε», όπου αποστέλλονται οι απαντήσεις, ανήκει στον επιτιθέμενο.
3. **Spoofed Sender (with No Reply-to address)** : Αυτή η μορφή απάτης μέσω email χρησιμοποιεί το όνομα και το email του spoofed στελέχους. Όμως το μήνυμα δεν περιλαμβάνει διεύθυνση «Απάντηση σε», οπότε είναι αδύνατη η αμφίδρομη αλληλογραφία. Το μήνυμα συχνά περιλαμβάνει οδηγίες μεταφοράς χρημάτων, που καταργούν την ανάγκη για περαιτέρω διευκρινήσεις.
4. **Lookalike Domain** : Σε αυτήν την μορφή απάτης μέσω email, η διεύθυνση «Από» του επιτιθέμενου έχει παρόμοια εμφάνιση με αυτή του πλαστοπροσωποποιημένου στελέχους. Το παρόμοιο domain μπορεί να διαφέρει μόνο προς ένα γράμμα από το πραγματικό. Για παράδειγμα, το metronlogistics.com μπορεί να γίνει metronlogstics.com [37].

2.3.1.ε Software Piracy - Πειρατεία Λογισμικού

Μια από τις καινοτομίες που έφερε η χρήση του διαδικτύου και των torrents, είναι η εύκολη πρόσβαση σε ταινίες, μουσικά κομμάτια και κάθε είδους λογισμικού δωρεάν. Η πειρατεία μέσω διαδικτύου έχει εξελιχθεί σε αναπόσπαστο κομμάτι της ζωής μας που, είτε εν αγνοία μας, είτε συνειδητά συμβάλλουμε όλοι. Αυτό έχει σαν αποτέλεσμα τα κέρδη των προγραμματιστών όταν πρόκειται για λογισμικό, ή των δημιουργών όταν πρόκειται για ταινίες, μουσική, βιβλία κ.τ.λ. να μειώνονται. Η πειρατεία λογισμικού δεν εστιάζει μόνο στην παράνομη χρήση πνευματικής ιδιοκτησίας, αλλά περιέχει και το κομμάτι της παράνομης διανομής αυτής της πνευματικής ιδιοκτησίας στερώντας ακόμα περισσότερα κέρδη από τον νόμιμο δημιουργό.

Η πειρατεία λογισμικού είναι η μη εξουσιοδοτημένη χρήση και διανομή λογισμικού υπολογιστή. Οι προγραμματιστές καταβάλουν μεγάλη προσπάθεια και κόπο για να αναπτύξουν αυτά τα λογισμικά και με την πειρατεία τα έσοδά τους μειώνονται και καθιστούν την συντήρηση των ήδη υπαρχόντων λογισμικών αλλά και την ανάπτυξη νέων ασύμφορη. Εκτός από αυτό, η πειρατεία λογισμικού επηρεάζει και την παγκόσμια οικονομία καθώς τα κεφάλαια μεταφέρονται από άλλους τομείς που οδηγούν σε λιγότερες επενδύσεις στο μάρκετινγκ και την έρευνα. Κάποιες από τις μορφές πειρατείας λογισμικού είναι :

- Μη εξουσιοδοτημένη φόρτωση λογισμικού στον υπολογιστή.

- Χρήση ενός λογισμικού σε πολλούς υπολογιστές χρησιμοποιώντας μόνο ένα κλειδί προϊόντος.
- Χρήση μιας γεννήτριας κλειδιών για την παράκαμψη της προστασίας αντιγραφής
- Διανομή αδειοδοτημένης ή μη αδειοδοτημένης («σπασμένης») έκδοσης λογισμικού μέσω διαδικτύου και εκτός.

Μια άλλη απειλή που πρέπει να αναφερθεί είναι η κλωνοποίηση. Κατά την κλωνοποίηση ο παραβάτης αντιγράφει την ιδέα πίσω από ένα λογισμικό και γράφει τον δικό του κώδικα. Αξίζει να σημειωθεί ότι οι ιδέες δεν προστατεύονται διαρκώς από αντιγραφή, ωστόσο δεν θεωρείται τελείως παράνομο. Τα λογισμικά “crack” είναι μια παράνομη ληφθείσα έκδοση ενός λογισμικού που είναι λειτουργικό, χωρίς να το επηρεάζει η κωδικοποίηση για την αποφυγή πιθανής αντιγραφής. Οι χρήστες πειρατικού λογισμικού μπορούν να χρησιμοποιήσουν μια γεννήτρια κλειδιών για να κατασκευάσουν έναν σειριακό αριθμό που ξεκλειδώνει μια έκδοση αξιολόγησης του λογισμικού, καταργώντας με αυτόν τον τρόπο τις δικλείδες ασφαλείας που έχει το λογισμικό για πιθανή αντιγραφή του. Το σπάσιμο του λογισμικού και η χρήση γεννήτριας μη εξουσιοδοτημένων κλειδιών είναι παράνομες πράξεις παραβίασης πνευματικών δικαιωμάτων.

Η χρήση πειρατικών αρχείων κρύβει και άλλους κινδύνους, εκτός της καταπάτησης πνευματικής ιδιοκτησίας. Τα πειρατικά αρχεία ιδίως τα πειρατικά λογισμικά μπορεί να περιέχουν κακόβουλα λογισμικά όλων των ειδών όπως ηλεκτρονικούς ιούς, trojans, worms κ.α., καθώς οι πειρατές σε πολλές περιπτώσεις μολύνουν τα λογισμικά αυτά με κακόβουλο κώδικα. Οι χρήστες πειρατικών προγραμμάτων έχουν κίνδυνο πιθανή τιμωρίας από τον νόμο για μη εξουσιοδοτημένη χρήση πνευματικής ιδιοκτησίας. Επιπροσθέτως, οι χρήστες δεν λαμβάνουν από τους προγραμματιστές υποστήριξη για το λογισμικό. Για να προστατεύσουν οι δημιουργοί τα λογισμικά τους από την πειρατεία, χρησιμοποιούν διάφορα μέτρα ασφαλείας. Σε πολλές περιπτώσεις η πώληση ενός λογισμικού γίνεται με την χρήση ψηφιακού αποτυπώματος, που βοηθά στον εντοπισμό πειρατικών αντιγράφων. Μια άλλη κοινή τεχνική είναι το να κλειδώσουν το λογισμικό. Με αυτόν τον τρόπο η άδεια χρήσης ή διαφορετικά το κλειδί προϊόντος (product key) κλειδώνεται για χρήση μόνο από έναν υπολογιστή, χωρίς να μπορεί άλλος υπολογιστής να το χρησιμοποιήσει. Παρ’όλα αυτά οι hackers βρίσκουν συνεχώς νέους τρόπους να παρακάμψουν ή να εξαλείψουν αυτές τις δικλείδες ασφαλείας [38].

2.3.2 Παραδοσιακά ηλεκτρονικά εγκλήματα

Τα παραδοσιακά ηλεκτρονικά εγκλήματα είναι τα εγκλήματα εκείνα τα οποία προϋπήρχαν πριν την εμφάνιση των ηλεκτρονικών υπολογιστών και του διαδικτύου. Ωστόσο, η ανάπτυξη της τεχνολογίας και την πρώτη εμφάνιση τόσο των ηλεκτρονικών υπολογιστών όσο και των δικτύων συνέβαλε σε μεγάλο βαθμό στην διάπραξη αυτού του είδους εγκλημάτων αλλά και στην ευκολία που απέκτησε ο εγκληματίας έχοντας ως μέσω το διαδίκτυο και ως εργαλείο πλέον τον ηλεκτρονικό υπολογιστή [19].

2.3.2.α Computer – Internet Fraud / Απάτη Μέσω Υπολογιστή - Διαδικτύου

Η συνεχής ανάπτυξη του διαδικτύου ευνόησε την εμφάνιση νέων μορφών εγκληματικότητας. Μια από αυτές είναι η απάτη μέσω διαδικτύου η οποία μπορεί και να χαρακτηριστεί ως μια ειδική περίπτωση οικονομικού εγκλήματος. Συγκεκριμένα, αυτό το είδος επιθέσεων ή για να είμαστε πιο σωστοί κυβερνοεγκλήματος, αναφέρεται στην πρόθεση

της παράνομης πρόκλησης απώλειας περιουσίας σε κάποιον άλλον μέσω α) οποιασδήποτε εισαγωγής, απώλειας, τροποποίησης ή απόκρυψης δεδομένων ηλεκτρονικού υπολογιστή, β) οποιασδήποτε επέμβαση στη λειτουργία ενός υπολογιστή ή συστήματος υπολογιστών με σκοπό να επιφέρει οικονομικό όφελος στον εαυτό του ή σε άλλον (Council of Europe, 2005). Οι πιο κοινές μορφές απάτης με υπολογιστή μέσω διαδικτύου είναι η απάτη με πιστωτική κάρτα απάτη με συναλλαγές μέσω ATM ή POS, η Νιγηριανή απάτη, τα πυραμιδικά συστήματα εργασίας, η απαλοιφή χρέους και οι ηλεκτρονικές δημοπρασίες. Παρακάτω θα αναλυθούν ορισμένα εξ αυτών.

Στην περίπτωση απάτης με πιστωτική κάρτα, ο απατεώνας προσπαθεί, μέσω των μηνυμάτων κυρίως ηλεκτρονικού ταχυδρομείου που στέλνει, να αποσπάσει από το θύμα του προσωπικά οικονομικά δεδομένα, όπως τα στοιχεία πιστωτικής κάρτας, τραπεζικού λογαριασμού κ.τ.λ. Αρχικά το θύμα δέχεται κάποιο email, που ως αποστολέας φαίνεται ότι είναι η τράπεζα του θύματος. Στο μήνυμα η τράπεζα φαινομενικά του ζητάει να επιβεβαιώσει το όνομα χρήστη χρησιμοποιεί και τον κωδικό πρόσβασης τα οποία χρησιμοποιεί για να έχει πρόσβαση στο e-banking του. Σαν αιτιολογίες για όλο αυτό, ο απατεώνας χρησιμοποιώντας την μάσκα της τράπεζας, αναφέρει κάποια υποτιθέμενα προβλήματα σε υπολογιστικά συστήματα της τράπεζας ή ότι υπάρχει πιθανή παραβίαση του λογαριασμού του θύματος και αν δεν γίνει επιβεβαίωση στοιχείων θα κλειδωθεί ο λογαριασμός. Επίσης, το email αυτό περιέχει κάποιο σύνδεσμο προς μια εικονική ιστοσελίδα της τράπεζας παρόμοια με την αυθεντική και βάζοντας τα στοιχεία του το θύμα σε αυτήν την ιστοσελίδα στέλνει απευθείας τα στοιχεία του στον απατεώνα.

Άλλη περίπτωση απάτης με πιστωτική κάρτα είναι οι dialers οι οποίοι μπορούν να θεωρηθούν και ως μια υποκατηγορία των κακόβουλων λογισμικών κατασκοπείας τα γνωστά και ως spyware. Τα spyware όπως έχει ήδη αναφερθεί, είναι σχεδιασμένα να υποκλέπτουν σημαντικές πληροφορίες του χρήστη όπως οι κωδικοί πρόσβασης, οι αριθμοί πιστωτικών καρτών, στοιχεία λογαριασμών χωρίς τη γνώση και έγκρισή του. Οι dialers αλλάζουν τις ρυθμίσεις του δικτύου και των routers μέσω τηλεφώνου, ώστε να υποχρεώσουν το χρήστη να καλεί έναν συγκεκριμένο άγνωστο αριθμό που συνήθως ο αριθμός αυτός είναι από άλλη χώρα πραγματοποιώντας έτσι διεθνής κλήση και να δημιουργηθεί υψηλό κόστος. Στη συνέχεια προχωρούν στη διαγραφή του αριθμού του παρόχου υπηρεσιών διαδικτύου (ISP) που χρησιμοποιεί ο χρήστης και τον αντικαθιστούν με τον δικό τους πάροχο. Με αυτόν τον τρόπο κάθε φορά που ο χρήστης συνδέεται στο διαδίκτυο χρησιμοποιεί τον αριθμό του dialer και όχι τον αριθμό του δικού του παρόχου υπηρεσιών διαδικτύου [39].

Στην περίπτωση της Νιγηριανής απάτης μηνύματα ηλεκτρονικού ταχυδρομείου αποστέλλονται σε ανυποψίαστα θύματα, μέσα από τα οποία περιγράφοντας οι απατεώνες πλασματικές ιστορίες και δελεάζοντας τα με μεγάλα κέρδη, προσπαθούν να τους αποσπάσουν μεγάλα χρηματικά ποσά. Οι απατεώνες συστήνονται στα θύματα ως έμπιστα πρόσωπα υψηλού κύρους της κυβέρνησης της Νιγηρίας και επικαλούμενοι κυρίως λόγους πολιτικής φύσεως, ζητάνε από τα θύματα την βοήθειά τους για την μεταφορά πολλών χρημάτων εκτός της χώρας (στην προκειμένη περίπτωση της Νιγηρίας). Συγκεκριμένα, το θύμα καλείται να διευκολύνει τον απατεώνα αποδέχοντας το χρηματικό ποσό και έτσι να γίνει δεκτή η μεταφορά των χρημάτων εκτός της χώρας. Για αυτή του την πράξη το θύμα θα εισπράξει ένα αρκετά μεγάλο χρηματικό ποσό. Όταν το χρηματικό ποσό μεταφερθεί στον τραπεζικό λογαριασμό του θύματος τότε υποτίθεται, με την είσπραξη μιας αρκετά μεγάλης προμήθειας, θα πρέπει μετά το θύμα να το παραχωρήσει στον αποστολέα του email. Σε πρώτη φάση αυτό που καλείται το θύμα να κάνει είναι να δώσει την συγκατάθεση του για

όλη αυτή την διαδικασία, αλλά και τις πληροφορίες του τραπεζικού του λογαριασμού. Μετά όταν κάποιο θύμα αποδεχτεί την πρόταση αυτή ξεκινάει μια διαδικασία συνεχών μηνυμάτων και επιστολών πιστεύοντας το θύμα ότι βρίσκεται πολύ κοντά στο να παραλάβει το μεγάλο χρηματικό ποσό. Πριν την τελική μεταβίβαση των χρημάτων όμως, εμφανίζεται από την μεριά του υψηλού προσώπου κάποιο προσωρινό πρόβλημα και ως εκ τούτου το υψηλό πρόσωπο προφασίζεται αδυναμία πληρωμής του ποσού λόγω του ότι έχει ήδη γίνει η μεταφορά χρημάτων με αποτέλεσμα να είναι δεσμευμένα μέχρι την στιγμή που θα λυθεί το πρόβλημα. Επίσης, στα πλαίσια συνεργασίας μεταξύ του υψηλού προσώπου και του θύματος, ζητείται στον δεύτερο να καταβάλει ένα ποσό το οποίο θα του αποπληρώσει το υψηλό πρόσωπο μόλις ολοκληρωθεί η συναλλαγή του μεγάλου χρηματικού ποσού. Αυτό βέβαια είναι η αρχή μιας μεγάλης αλυσίδας προβλημάτων που ισχυρίζεται ο δράστης, καταφέροντας έτσι να αποσπάσει από τα θύματά του ποσό που αγγίζει τις 500.000 €. Υπάρχουν βέβαια και περιπτώσεις που οι κυβερνοεγκληματίες πείθουν τα θύματά τους να ταξιδέψουν στο εξωτερικό, για να τους δείξουν τα λεφτά οδηγώντας τους σε τραπεζικές θυρίδες, ενώ εκείνοι έχουν ήδη καταλάβει ένα χρηματικό ποσό για την αποδέσμευση του κεφαλαίου [40].

2.3.2.β Πλαστογραφία – Forgery

Στην περίπτωση της πλαστογραφίας, οι εγκληματίες προσπαθούν με δόλιο τρόπο να εισάγουν, να διαγράψουν, να μεταβάλλουν και να τροποποιήσουν δεδομένα ενός ηλεκτρονικού υπολογιστή με τέτοιο τρόπο ώστε, τα ψεύτικα δεδομένα που δημιουργούνται μετά από αυτές τις ενέργειες να παρουσιάζονται και να χρησιμοποιούνται για νόμιμους σκοπούς. Με το αδίκημα αυτό μπορεί να τιμωρηθεί κάποιος μέχρι και με πέντε χρόνια φυλάκισης ή και με χρηματικό πρόστιμο.

Μία από τις σημαντικότερες ποινικές διατάξεις που αφορούν την ακεραιότητα και την ορθότητα της πληροφορίας είναι οι διατάξεις για την πλαστογραφία. Οι ποινικές αυτές διατάξεις εξασφαλίζουν την αυθεντικότητα ενός εγγράφου με την έννοια της εγγύησης του συντάκτη για το περιεχόμενο του εγγράφου. Σε ορισμένες νομοθεσίες απαιτείται υλική ενσωμάτωση του εγγράφου προκειμένου να υφίσταται η προστασία αυτή. Πολλές ευρωπαϊκές νομοθεσίες, μεταξύ των οποίων και η ελληνική, διεύρυναν την έννοια του παραδοσιακού έγγραφου ώστε αυτή να περιλαμβάνει όλα τα μέσα τα οποία χρησιμοποιούνται από υπολογιστή ή περιφερειακή μνήμη για την εγγραφή, αποθήκευση, παραγωγή και αναπαραγωγή πληροφοριακών στοιχείων με ηλεκτρονικό, μαγνητικό ή κοινό τρόπο. Σε αρκετές χώρες μελετάται η εισαγωγή νέας ειδικής νομοθεσίας για την προστασία από την πλαστογραφία νέων μορφών χρήματος όπως το πλαστικό χρήμα ή οι προπληρωμένες κάρτες κλπ [41].

Μια χαρακτηριστική περίπτωση πλαστογραφίας είναι η κλοπή ταυτότητας (identity theft). Η κλοπή ταυτότητας είναι η πράξη κατά την οποία κάποιος κακόβουλος χρήστης παίρνει τις προσωπικές πληροφορίες ενός άλλου ατόμου, με σκοπό να τις χρησιμοποιήσει για δικό του όφελος, ιδιαίτερα χωρίς την έγκριση του ατόμου στο οποίο ανήκουν οι πληροφορίες αυτές. Η κλοπή ταυτότητας μπορεί να πάρει πολλές μορφές, και κάθε μια από αυτές επηρεάζει το θύμα με διαφορετικούς τρόπους. Ανεξαρτήτως πως αντιλαμβάνεται ο καθένας μας την έννοια της κλοπής ταυτότητας, σε κάθε περίπτωση η οικονομική ασφάλεια, η φήμη και το οικονομικό μέλλον του θύματος βρίσκονται σε κίνδυνο. Επειδή υπάρχουν πολλοί τρόποι που ένας κυβερνοεγκληματίας μπορεί να κλέψει την ταυτότητα κάποιου θύματος, είναι ουσιαστικά αδύνατο να αποτρέψει κάποιος να γίνει στόχος. Ακόμα και στην περίπτωση

που κάποιος δεν έχει τόσα πολλά περιουσιακά στοιχεία, ή τόσα πολλά χρήματα στον τραπεζικό του λογαριασμό, ή πρόσβαση σε πολύτιμους στόχους, μπορεί ένας απατεώνας να βγάλει χρήματα με την ταυτότητά του. Σε πολλές περιπτώσεις, μόλις κλαπεί η ταυτότητα κάποιου θύματος, δεν έχει μεγάλες επιπτώσεις για αυτό. Παρ' όλα αυτά, ο απατεώνας μπορεί να βγάλει από λίγα μέχρι εκατοντάδες δολάρια πουλώντας την ταυτότητα και τις προσωπικές πληροφορίες του θύματος. Επομένως, οι κλέφτες ταυτότητας έχουν ως στόχο οποιονδήποτε χρήστη επειδή κάθε ταυτότητα έχει ξεχωριστή αξία στην μαύρη αγορά. Σε άλλες περιπτώσεις ο εγκληματίας σκοπεύει να εκμεταλλευτεί την ταυτότητα του θύματος και τότε μπορεί ο εγκληματίας να είναι πιο επιλεκτικός σχετικά με τα θύματα που θα επιλέξει. Οι πιο συνηθισμένοι τρόποι για να συμβεί μια κλοπή ταυτότητας είναι μέσω της μη ασφαλούς περιήγησης στο διαδίκτυο, με επιθέσεις ηλεκτρονικού «ψαρέματος» (phishing) και ανεπιθύμητης αλληλογραφίας (spamming) αλλά και μέσω κάποιου κακόβουλου λογισμικού.

Οι απάτες ταυτότητας (identity fraud) είναι παρόμοιες με τις κλοπές ταυτότητας και αυτές οι δύο έννοιες μπορούν να χρησιμοποιηθούν σε μερικές περιπτώσεις ισοδύναμα. Όμως, η απάτη ταυτότητας είναι διαφορετική από την κλοπή ταυτότητας γιατί, αναφέρεται συγκεκριμένα στον τρόπο χρήσης των κλεμμένων προσωπικών πληροφοριών ενός θύματος ενώ, η κλοπή ταυτότητας αναφέρεται μόνο στην πράξη της κλοπής και όχι στον μετέπειτα τρόπο χρήσης της από τον κλέφτη. Για τις απάτες ταυτότητας υπάρχουν διάφορες μορφές συμπεριλαμβανομένων σε αυτές η χρήση μιας πιστωτικής κάρτας, οι φόροι, η εργασία, οι λογαριασμοί κοινής ωφέλειας, οι πληροφορίες τραπεζικού λογαριασμού, ενοικιαστήρια ή δάνεια κ.α. Ανεξάρτητα από τον τύπο της απάτης, η εκτέλεση της επίθεσης είναι παρόμοια. Ο κλέφτης χρησιμοποιεί αριθμούς λογαριασμών, αριθμούς κοινωνικής ασφάλισης και άλλες προσωπικές πληροφορίες για να κάνει μια άλλη οντότητα να πιστέψει ότι είναι το θύμα και με αυτό τον τρόπο να βγάλει ή να πάρει χρήματα. Οι απάτες ταυτότητας μπορούν να θεωρηθούν και ως υποκατηγορία της κύριας κατηγορίας των απατών [42].

2.3.2.γ Cybersex Trafficking and Child Pornography – Διακίνηση Λευκής Σαρκός και Παιδικής Πορνογραφίας Μέσω Διαδικτύου

Η παιδική πορνογραφία είναι ένα από τα εγκλήματα που προϋπήρχαν της εμφάνισης των υπολογιστών και του διαδικτύου και ήταν πάντοτε ένα πολύ λεπτό και σκανδαλώδες έγκλημα. Με την εμφάνιση του διαδικτύου όμως, η ανάπτυξη και η διάδοση πορνογραφικού υλικού ανήλικων θυμάτων έγινε ευκολότερη και γρηγορότερη αλλά ταυτόχρονα κάνει και την σύλληψη αυτού του είδους κυβερνοεγκληματιών ακόμα πιο δύσκολη. Οι τρόποι διάδοσης της παιδικής πορνογραφίας στον κυβερνοχώρο είναι πολλοί. Για παράδειγμα, ένας παιδόφιλος ανεξάρτητα από το μέρος που βρίσκεται, μπορεί να κάνει εγγραφή σε ιστοσελίδες μέσα στις οποίες μπορεί να ανταλλάξει ή να αγοράσει υλικό παιδικής πορνογραφίας ανηλίκων, χωρίς να νιώθει ενοχές και ότι διαπράττει παράνομες πράξεις σε βάρος παιδιών. Μέσα από αυτές τις ιστοσελίδες δίνεται η δυνατότητα στον παιδόφιλο να έρθει σε επαφή με άλλα τέτοια άτομα και να ανταλλάξουν απόψεις δημιουργώντας τους έτσι ένα αίσθημα πως δεν παρανομούν με αυτόν τον τρόπο διακινώντας δηλαδή παιδικό πορνογραφικό υλικό. Κατά μια έννοια οι παιδόφιλοι αισθάνονται «ασφαλείς» ως μέλη τέτοιων διαδικτυακών κοινοτήτων και κατά αυτόν τον ενισχύεται και η αυτοπεποίθησή τους και το γόητρό τους.

Οι παιδόφιλοι εκμεταλλευόμενοι την ανωνυμία που προσφέρει το διαδίκτυο, μπορούν και εκφράζουν τα πιο βαθιές και διεστραμμένες επιθυμίες τους. Η ανωνυμία του κάνει να προβάλλουν όλες τις σεξουαλικές τους φαντασιώσεις με τέτοιο τρόπο, σαν να πιστεύουν πως είναι πανίσχυροι μέσα στον κόσμο του διαδικτύου, δοκιμάζοντας μάλιστα

κάθε φορά και νέες εμπειρίες, με το να υποδύονται διαφορετικά πρόσωπα ώστε να προσεγγίζουν τα θύματά τους πιο εύκολα. Επιπλέον, στις μέρες μας μπορεί οποιοςδήποτε να συλλέξει υλικό παιδικής πορνογραφίας, να μιλήσει ζωντανά είτε με ανήλικους είτε με ενήλικους που είναι και αυτοί παιδόφιλοι, αλλά και να παρακολουθήσει online υλικό με σεξουαλικές δραστηριότητες μεταξύ ενηλίκων και ανηλίκων. Βέβαια, δεν σταματούν εδώ οι παράνομες ενέργειες ενός παιδόφιλου, αλλά μπορούν να επεκταθούν και στον τομέα της παραγωγής τέτοιου είδους πορνογραφικού υλικού αφού ο καθένας μπορεί να γίνει παραγωγός παιδικής πορνογραφίας, ανεβάζοντας στο διαδίκτυο προσωπικό πορνογραφικό υλικό που έχει καταγράψει μέσα από τις σεξουαλικές του δραστηριότητες. Από την άλλη όταν κάποιος διαμοιράζει πορνογραφικό υλικό που διαθέτει για να βγάλει κάποιο χρηματικό ποσό τότε χαρακτηρίζεται ως έμπορος. Τα οικονομικά οφέλη από την εμπορία παιδικής πορνογραφίας υπολογίζονται ετησίως σε πολλά δισεκατομμύρια δολάρια, ενώ τα κυκλώματα και οι οργανώσεις είναι πάρα πολύ καλά οργανωμένα, κάνοντας την εξάρθρωσή τους πάρα πολύ δύσκολη.

Οι ιστοσελίδες που περιέχουν υλικό παιδικής πορνογραφίας δεν διαφημίζονται τόσο συχνά και έχουν το υλικό τους σε κοινή θέα έτσι ώστε να μπορούν όλοι όσοι ενδιαφέρονται να έχουν πρόσβαση σε αυτό. Οι ενδιαφερόμενοι χρήστες επικοινωνούν με τους διαχειριστές αυτών των ιστοσελίδων για να τους στείλουν υλικό παιδικής πορνογραφίας. Η αποστολή πραγματοποιείται μέσω email και η πληρωμή γίνεται συνήθως μέσω πιστωτικής κάρτας. Οι ιστοσελίδες αυτές όταν διαφημίζονται φαίνεται ότι έχουν απλώς νόμιμο υλικό πορνογραφίας, ενώ στην πραγματικότητα αυτό που δίνουν στους πελάτες τους είναι υλικό με πορνογραφία ανηλίκων. Το μειονέκτημα σε αυτό είναι ότι ο κάθε χρήστης πρέπει να γνωρίζει εκ των προτέρων τι υλικό πορνογραφίας διακινούν οι συγκεκριμένες σελίδες έτσι ώστε αν όντως δεν ενδιαφέρεται να μπορεί να τις αποφύγει.

Τέλος, πρέπει να αναφερθεί ότι και τα μέσα κοινωνικής δικτύωσης αλλά και τα διάφορα δωμάτια συνομιλιών (chat rooms), μπορούν να λειτουργήσουν ως μέσο επαφής και συνομιλίας των παιδόφιλων με πιθανά ανήλικα θύματά τους, κάνοντας πιο εύκολη την απόκτηση και ανταλλαγή υλικού παιδικής πορνογραφίας. Κάποιες φορές μάλιστα, ο παιδόφιλος επιδιώκει σε πραγματική επαφή με τα ανήλικα θύματά του, ώστε να επιτευχθεί σεξουαλική δραστηριότητα μεταξύ τους [43].

Ο όρος cybersex ουσιαστικά περιλαμβάνει κάθε χρήση του διαδικτύου με σκοπό την σεξουαλική ικανοποίηση. Δεν υπάρχει ομοφωνία μεταξύ των επιστημόνων και των ειδικών για το τι αποτελεί το «προβληματικό» cybersex. Η σχετική βιβλιογραφία πάνω στο θέμα του cybersex αναφέρει ότι, τα μόνα προβλήματα που υπάρχουν σε αυτή την δραστηριότητα είναι ο εθισμός ή προβλήματα δυσλειτουργίας και όχι παραβατικές και εγκληματικές συμπεριφορές σαν αυτές που είναι αναμεμιγμένες με τον ορισμό της εμπορίας λευκής σαρκός μέσω διαδικτύου, δηλαδή το γνωστό cybersex trafficking.

Με τον όρο cybersex trafficking αναφερόμαστε σε εγκληματικές ενέργειες όπως η πώληση παιδιών με σκοπό την ζωντανή βιντεοσκόπησή τους, ενώ βρίσκονται σε σεξουαλικές δραστηριότητες και την προβολή τους διαδικτυακά. Συχνά, αυτά τα παιδιά είναι θύματα λαθρεμπορίου ανθρώπων (human trafficking) και κρατούνται αιχμάλωτα για να παίρνουν μέρος σε αυτές τις σεξουαλικές εκπομπές στο διαδίκτυο, σε αντίθεση με τον πιο συνηθισμένο λόγω της παράνομης εμπορίας παιδιών για σεξουαλικούς σκοπούς, δηλαδή την πορνεία.

Εξαιτίας της έλλειψης επαρκούς βιβλιογραφίας για το ζήτημα του cybersex trafficking, δεν υπάρχει κάποιος ορισμός αυτού του συγκεκριμένου εγκλήματος που να είναι κοινά αποδεκτός. Για να γίνει περισσότερο κατανοητό όμως, θα παρατεθούν στοιχεία από τις Φιλιππίνες μιας και είναι η κοιτίδα τέτοιου είδους εγκλημάτων. Στις Φιλιππίνες το cybersex trafficking, γνωστό και ως παιδικός σεξουαλικός τουρισμός μέσω διαδικτύου, συνεπάγεται με την ζωντανή μετάδοση παραστάσεων σεξουαλικών δραστηριοτήτων ατόμων που δεν έχουν ή δεν μπορούν να δώσουν την συγκατάθεσή τους για όλο αυτό. Αυτό το υλικό με το σεξουαλικό περιεχόμενο μεταδίδεται και προβάλλεται μέσω ηλεκτρονικών συσκευών, όπως οι ηλεκτρονικοί υπολογιστές και τα κινητά τηλέφωνα. Τα θύματα αυτού του κυβερνοεγκλήματος στις Φιλιππίνες είναι πάντα παιδιά, παρότι και οι ενήλικες μπορούν να πέσουν θύματα αυτού του είδους εγκλήματος χωρίς εξαιρέσεις. Ο λόγος που γίνεται ένα τέτοιο έγκλημα είναι το κέρδος, αφού για να παρακολουθήσει κάποιος ενδιαφερόμενος πρέπει να πληρώσει ένα χρηματικό ποσό στο κυβερνογκληματία, που παρέχει τέτοιου είδους υπηρεσίες [44].

2.3.2.δ Online Harassment - Διαδικτυακή παρενόχληση

Η διαδικτυακή παρενόχληση μπορεί να οριστεί ως η χρήση τεχνολογιών πληροφορικής και τηλεπικοινωνιών, είτε από ένα άτομο, είτε από μια ομάδα ατόμων επανειλημμένα, με σκοπό να βλάψουν κάποιο άλλο άτομο. Είναι δηλαδή μια εσκεμμένη ενέργεια εκφοβισμού και παρενόχλησης, με την χρήση σύγχρονων τεχνολογιών και του διαδικτύου. Τις περισσότερες φορές, ο θύτης και το θύμα γνωρίζονται και συνήθως ανήκουν στην ηλικιακή ομάδα των παιδιών και των εφήβων.

Στην κατηγορία της διαδικτυακής παρενόχλησης εντάσσονται απειλές, αμυχανία ή ταπείνωση μέσω του περιβάλλοντος του διαδικτύου. Αυτό περιλαμβάνει εκφράσεις ή προκατειλημμένες συμπεριφορές και πεποιθήσεις όπως ο σεξισμός, ο ρατσισμός, η ξеноφοβία, η ομοφοβία, αλλά και οι προκατειλημμένες συμπεριφορές ως προς την εμφάνιση κάποιου ατόμου. Η διαδικτυακή παρενόχληση είναι γνωστή και ως κυβερνοεπιθετικότητα (cyberaggression), διαδικτυακός εκφοβισμός (cyberbullying), κυβερνοπαρενόχληση (cyber-harassment), κυβερνομίσος (cyberhate), κυβερνοθυματοποίηση (cybervictimisation) και αποκλίνουσα διαδικτυακή συμπεριφορά. Συνήθως, η διαδικτυακή παρενόχληση λαμβάνει χώρα σε πλαίσια όπως τα μέσα κοινωνικής δικτύωσης, τα μηνύματα απλού κειμένου SMS, σε μηνύματα εφαρμογών άμεσης ανταλλαγής μηνυμάτων και μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου. Συγκεκριμένα, οι μορφές που μπορεί να πάρει η διαδικτυακή παρενόχληση είναι :

- Παρενόχληση μέσω φωτογραφιών.
- Παρενόχληση μέσω βίντεο.
- Υποκίνηση τρίτων για διαδικτυακή παρενόχληση.
- Αποστολή πληροφοριών σε τρίτους.
- Μηνύματα παρενόχλησης στο κινητό ή στα μέσα κοινωνικής δικτύωσης.
- Παρενόχληση μέσω δημοσιεύσεων σε μέσα κοινωνικής δικτύωσης.
- Παρενόχληση μέσω ψεύτικων προφίλ στα μέσα κοινωνικής δικτύωσης.
- Παραβίαση των προσωπικών λογαριασμών ενός ατόμου, συνήθως για να αναρτηθούν δημοσιεύσεις που θα τον κάνουν να ταπεινωθεί.
- Η εσκεμμένη αποστολή ιών και άλλων κακόβουλων λογισμικών ώστε να μολυνθεί η συσκευή του θύματος [45] [46].

Μια άλλη σημαντική μορφή της διαδικτυακής παρενόχλησης είναι η παρακολούθηση στον κυβερνοχώρο (cyberstalking). Στη νέα αυτή μορφή κυβερνοεγκλήματος ένα άτομο παρακολουθείται συνεχώς. Ο καταδιώκτης, παρακολουθεί συνεχώς το θύμα του ακολουθώντας την διαδικτυακή του δραστηριότητα, συλλέγοντας έτσι πληροφορίες που θα τις χρησιμοποιήσει αργότερα για να απειλήσει ή να παρενοχλήσει το θύμα του μέσω λεκτικού εκφοβισμού. Αυτή η μορφή παραβατικής συμπεριφοράς μπορεί να θεωρηθεί και ως μια εισβολή στο διαδικτυακό απόρρητο κάποιου. Το κύριο χαρακτηριστικό της ηλεκτρονικής καταδίωξης είναι ότι εκμεταλλεύεται το διαδίκτυο ή οποιοδήποτε άλλο ηλεκτρονικό μέσο αλλά, πολλές φορές είναι συνοδευόμενη και από καταδίωξη ή παρακολούθηση του θύματος και στην κανονική του ζωή εκτός διαδικτύου. Συνήθως θύματα τέτοιων επιθέσεων είναι γυναίκες με τις οποίες έχουν πάθει εμμονή άντρες αλλά και παιδιά τα οποία παρακολουθούνται από παιδόφιλους. Ένας καταδιώκτης του κυβερνοχώρου μπορεί να είναι και γνωστό άτομο του θύματος αλλά μπορεί να είναι και κάποιος τελείως άγνωστος.

Οι διαδικτυακοί διώκτες παρακολουθούν τα θύματά τους μέσω του ηλεκτρονικού ταχυδρομείου, των μέσων κοινωνικής δικτύωσης, chat rooms, ιστοσελίδων, φόρουμ συζητήσεων και ανοικτών ιστότοπων δημοσίευσης (π.χ. blogs). Η εξέλιξη του διαδικτύου και ιδιαίτερα η αφθονία διαθεσιμότητας δωρεάν χώρου ηλεκτρονικού ταχυδρομείου / ιστότοπου, αλλά και η ανωνυμία που παρέχονται από τα δωμάτια συνομιλίας και τα φόρουμ συνέβαλαν στην αύξηση των περιστατικών παρακολούθησης στον κυβερνοχώρο. Ο καθένας πλέον έχει μια δικτυακή παρουσία χρησιμοποιώντας κάποια υπηρεσία ηλεκτρονικής αλληλογραφίας, έστω και αν δεν χρησιμοποιεί τα μέσα κοινωνικής δικτύωσης αφού πλέον είναι αναγκαία μια τέτοια υπηρεσία για διάφορες δραστηριότητες και εκτός του κόσμου του διαδικτύου. Συνεπώς, είναι πολύ εύκολο κάποιος που έχει ως στόχο το cyberstalking, με μια απλή αναζήτηση σε κάποια μηχανή αναζήτησης (Google, Bing κ.τ.λ.) να αποκτήσει το όνομα, το ψευδώνυμο, τον αριθμό επικοινωνίας και τη διεύθυνση του ενδιαφερόμενου θύματος. Καθώς ο ρόλος του διαδικτύου γίνεται όλο και πιο σημαντικός στην επαγγελματική και της προσωπικής του καθενός από εμάς, οι εγκληματίες του cyberstalking μπορούν να εκμεταλλευτούν την ευκολία επικοινωνίας αλλά και την μεγάλη διαθεσιμότητα και εύκολη πρόσβαση σε προσωπικές πληροφορίες οποιουδήποτε χρήστη. Η διαδικτυακή παρακολούθηση πραγματοποιείται με δύο τρόπους :

1. **Μέσω διαδικτύου.** Σε αυτήν την περίπτωση ο πιο συνηθισμένος τρόπος ένας κυβερνοεγκληματίας να απειλήσει τα θύματά του, είναι μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου αφού μπορεί να περιέχουν τόσο άσεμνο περιεχόμενο όσο και κάθε είδους κακόβουλο λογισμικό. Όμως η αποστολή τέτοιων ανεπιθύμητων μηνυμάτων δεν θεωρείται ενέργεια cyberstalking από μόνα τους, εκτός και αν αυτά αποστέλλονται συστηματικά με απώτερο σκοπό τον εκφοβισμό του θύματος. Βέβαια η καταδίωξη μέσω διαδικτύου δεν υλοποιείται μόνο μέσω των ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου, αλλά και μέσω κάθε χρήσης του διαδικτύου που έχει ως στόχο τον εκφοβισμό, την παρενόχληση και την συκοφαντία του θύματος.
2. **Μέσω υπολογιστή.** Αυτή την περίπτωση την επιλέγουν όσοι καταδιώκτες έχουν μεγάλες δεξιότητες στους υπολογιστές και στο hacking. Έχουν ως κύριο στόχο την μη εξουσιοδοτημένη πρόσβαση στον υπολογιστή του θύματος εκμεταλλευόμενοι τη λειτουργία του διαδικτύου και του λειτουργικού συστήματος των Windows. Αν και αυτό γίνεται συνήθως από άτομα με μεγάλες γνώσεις, οι οδηγίες για το πώς αυτό να πραγματοποιηθεί είναι εύκολα διαθέσιμες προς όλους στο διαδίκτυο.

Τέλος, πρέπει να σημειωθεί ότι τα μέσα κοινωνικής δικτύωσης έχουν γίνει κύριο εργαλείο για την πραγματοποίηση του cyberstalking. Όλοι πλέον μέσω αυτών δημοσιεύουν αλόγιστα μερικές από τις προσωπικές τους πληροφορίες στα προφίλ τους και δεδομένα όπως προσωπικές φωτογραφίες και κοινοποιήσεις παρουσίας τους σε διάφορα μέρη, είναι διαθέσιμα στο ευρύ κοινό. Η διαδικτυακή παρουσία του κάθε ατόμου παρέχει αρκετές πληροφορίες στους cyberstalkers, οι οποίοι στην συνέχεια αξιολογώντας αυτές τις πληροφορίες επιλέγουν τα επόμενα θύματά τους. Αν και οι τεχνολογίες της κοινωνικής δικτύωσης έχουν σαν κύριο στόχο την κοινωνικοποίηση των ανθρώπων μέσω του διαδικτύου, στο τέλος συμβάλουν άθελα τους σε κυβερνοεγκλήματα όπως αυτό της παρακολούθησης στον κυβερνοχώρο [47].

2.3.2.ε Drugs Trafficking – Λαθρεμπόριο Ναρκωτικών Μέσω Διαδικτύου

Τα τελευταία χρόνια εμφανίστηκαν νέες τεχνολογίες διαδικτύου που έχουν λειτουργήσει ως σημαντικοί διευκολυντές των διαδικτυακών αγορών φαρμάκων και ναρκωτικών ουσιών. Ιστορικά, οι παράνομες αγορές λιανικής πώλησης ναρκωτικών έχουν λειτουργήσει σε φυσικούς χώρους, με σχετικούς πρακτικούς περιορισμούς και όρια. Είτε λαμβάνει χώρα σε κεντρικό σημείο κάποιας πόλης είτε στον προσωπικό χώρο κάποιου αντιπροσώπου, το λαθρεμπόριο ναρκωτικών έχει συσχετιστεί με απτά πρόσωπα, μέρη και γεωγραφικούς χώρους. Οι νέες εξελίξεις επέτρεψαν την ανάπτυξη του διαδικτυακού χώρου εμπορίου σε εικονικές αγορές με παγκόσμια εμβέλεια. Αυτό έχει τη δυνατότητα να διευρύνει τα όρια της προμήθειας ναρκωτικών ουσιών και παρέχει περισσότερες ευκαιρίες σε αυτούς επιθυμούν να αγοράσουν ναρκωτικά. Οι διαδικτυακές αγορές ναρκωτικών ουσιών προσφέρουν στους συμμετέχοντες το πλεονέκτημα να αγοράζουν και να πωλούν τις ουσίες αυτές απομακρυσμένα, αποφεύγοντας με αυτό τον τρόπο τις συναντήσεις πρόσωπο με πρόσωπο, όπως συνηθίζεται με τις μαύρες αγορές εκτός διαδικτύου. αυτό μπορεί να προσφέρει έναν βαθμό ανωνυμίας και φυσική ασφάλεια στους εμπλεκόμενους που διαφορετικά θα ήταν δύσκολο να επιτευχθεί.

Η τεχνολογία ήταν πάντα συνδεδεμένη με αλλαγές στις αγορές ναρκωτικών. Ένα πρόσφατο παράδειγμα είναι η ευρεία χρήση των κινητών τηλεφώνων, που επέτρεψε την αγορά και πώληση ναρκωτικών αποφεύγοντας πιο ανοιχτά προσβάσιμους φυσικούς χώρους και καταλήγοντας σε κλειστά δίκτυα γνωστών επαφών. Η ανάπτυξη των εικονικών αγορών έχει αλλάξει τη δυναμική της διαδικασίας πώλησης και αγοράς περαιτέρω, αφού κατ' αυτόν τον τρόπο πραγματοποιήθηκε άνοιγμα της αγοράς σε ένα ευρύτερο κοινό, με συμμετέχοντες που μπορεί πλέον να είναι και άγνωστοι μεταξύ τους. Έτσι, μπορούμε να πούμε ότι αυτού του είδους οι διαδικτυακές αγορές είναι ανοιχτές αγορές οι οποίες λειτουργούν με μυστικό τρόπο. Στην πραγματικότητα, δεν μπορούν να πραγματοποιηθούν όλες οι πτυχές του λαθρεμπορίου ναρκωτικών μέσω διαδικτύου. Τόσο οι φάσεις της παραγωγής όσο και οι φάσεις της διανομής παραμένουν ίδιες με αυτές που γίνονται υπό συνθήκες εκτός διαδικτύου. Οι φυσικές συναλλαγές, που συχνά περιλαμβάνουν και παραδόσεις μέσω ταχυδρομείου είναι ακόμα αναγκαίες.

Πρόσφατα στοιχεία υποδηλώνουν ότι πρακτικά οποιοσδήποτε τύπος ναρκωτικού μπορεί να αγοραστεί στο διαδίκτυο. Οι αγορές ναρκωτικών που λειτουργούν στον επιφανειακό ή καθαρό ιστό φαίνεται να συνδέονται κυρίως με τη διανομή είτε μη ελεγχόμενων ουσιών είτε ουσιών για τις οποίες οι νομικοί έλεγχοι διαφέρουν μεταξύ χωρών και δικαιοδοσιών (φάρμακα, προϊόντα τρόπου ζωής, νέες ψυχοδραστικές ουσίες, πρόδρομες χημικές ουσίες). Τα διαδικτυακά φαρμακεία έχουν ανθίσει, διευρύνοντας τις προμήθειες τους

από προϊόντα lifestyle σε προϊόντα βελτίωσης της απόδοσης και συνταγογραφούμενα φάρμακα. Μια ταχεία επέκταση της διαδικτυακής αγοράς νέων ψυχοδραστικών ουσιών έχει παρατηρηθεί από το 2008, με αυτές τις ουσίες να πωλούνται τόσο ως «χημικά έρευνας» όσο και ως «νόμιμα ναρκωτικά» σε ηλεκτρονικά καταστήματα. Έχει επίσης εντοπιστεί μια αγορά για την προμήθεια πρόδρομων και πρόδρομων χημικών ουσιών. Παράλληλα με αυτές τις αγορές, η ανάπτυξη των μέσων κοινωνικής δικτύωσης έχει δει την εμφάνιση φόρουμ και εφαρμογών για κινητά όπου συζητούνται, διαφημίζονται και μερικές φορές πωλούνται τα ναρκωτικά. Έχει επίσης εντοπιστεί μια αγορά για την προμήθεια πρόδρομων και προ-πρόδρομων χημικών ουσιών. Παράλληλα με αυτές τις αγορές, η ανάπτυξη των μέσων κοινωνικής δικτύωσης υποδείξει την αναγκαιότητα για την δημιουργία φόρουμ και εφαρμογών για κινητά όπου συζητούνται, διαφημίζονται και μερικές φορές πωλούνται τα ναρκωτικά.

Πιο πρόσφατα, η προσοχή στράφηκε στην πώληση ναρκωτικών και άλλων παράνομων προϊόντων και υπηρεσιών σε αυτά που έχουν γίνει γνωστά ως dark net markets ή cryptomarkets, τα οποία υπάρχουν στην πραγματικότητα σε ένα «κρυφό» τμήμα του Διαδικτύου που δεν είναι προσβάσιμο μέσω τυπικών προγραμμάτων περιήγησης. Οι κρυπταγορές αντιπροσωπεύουν μια αξιοσημείωτη καινοτομία στο διαδικτυακό εμπόριο ναρκωτικών. Υπάρχουν επίσης λογισμικά που επιτρέπουν την ανωνυμοποίηση (π.χ. The Onion Router) ή την κρυπτογράφηση (π.χ. PGP) και τα κρυπτονομίσματα (π.χ. bitcoin) και παρέχουν υψηλό επίπεδο ανωνυμίας για αγοραστές και πωλητές και τα ναρκωτικά παραδίδονται μέσω του ταχυδρομείου, αποφεύγοντας την άμεση επαφή μεταξύ των εμπλεκόμενων. Αν και ορισμένοι σχολιαστές προτείνουν ότι αυτή η εικονικοποίηση του εμπορίου που σχετίζεται με τα ναρκωτικά, με φόρουμ που παρέχουν συμβουλές χρηστών και αξιολογήσεις για τους πωλητές και τα προϊόντα τους, μπορεί να μειώσει την εγκληματικότητα, τη βία και τον εκφοβισμό στις αγορές ναρκωτικών. Από την άλλη, η ταχύτητα με την οποία το Διαδίκτυο μεταμορφώνει τις αγορές ναρκωτικών αποτελεί μείζονα πρόκληση για την επιβολή του νόμου, τη δημόσια υγεία και τις υπηρεσίες έρευνας και παρακολούθησης [48].

2.3.2στ Cyberterrorism – Κυβερνοτρομοκρατία

Ο όρος της κυβερνοτρομοκρατίας (cyberterrorism) είναι ένας σύνθετος όρος. Δεν υπάρχει κάποιος εξειδικευμένος ορισμός της τρομοκρατίας που να είναι κοινά αποδεκτός παγκοσμίως. Συνήθως ο όρος κυβερνοτρομοκρατία χρησιμοποιείται για να περιγράψει επιθέσεις μέσω ηλεκτρονικών μέσων και τεχνολογιών, όπως για παράδειγμα τα δίκτυα υπολογιστών, οι ηλεκτρονικοί ιοί και άλλα κακόβουλα λογισμικά. Αυτές οι επιθέσεις αποβλέπουν στην διείσδυση και στην πρόκληση σοβαρής ζημιάς ή παρεμβολής σε σημαντικές υποδομές μιας χώρας. Οι υποδομές αυτές μπορεί να είναι εγκαταστάσεις, υπηρεσίες και δίκτυα τα οποία αν τεθούν εκτός λειτουργίας για μεγάλο χρονικό διάστημα μπορεί να προκαλέσουν σοβαρούς κινδύνους για την δημόσια υγεία, το περιβάλλον, την οικονομία, ακόμα και για την εθνική ασφάλεια ενός κράτους. Βέβαια και πάλι δεν μπορούμε να πούμε ότι αυτός είναι ένας ικανοποιητικός ορισμός για το τι είναι κυβερνοτρομοκρατία, αφού κάθε κράτος έχει δική του άποψη για το πότε μια κυβερνοεπίθεση μπορεί να χαρακτηριστεί κυβερνοτρομοκρατία. Όπως για παράδειγμα η Αυστραλία, η οποία υποστηρίζει ότι μια κυβερνοεπίθεση δεν χρειάζεται να επηρεάσει σημαντικές υποδομές μιας χώρας και να προκαλέσει σοβαρές ζημιές και δυσλειτουργίες για να χαρακτηριστεί ως κυβερνοτρομοκρατία, αλλά αρκεί μια κυβερνοεπίθεση να χαρακτηριστεί κατά αυτόν τον τρόπο, όταν παρέμβει σε ένα ηλεκτρονικό σύστημα με σκοπό τον εκφοβισμό είτε της

κυβέρνησης είτε των πολιτών. Σύμφωνα με την άποψη της Dorothy Denning, καθηγήτρια της Επιστήμης της Πληροφορικής « Η κυβερνοτρομοκρατία αποτελεί μία σύγκλιση, μία σύνθεση του κυβερνοχώρου και της τρομοκρατίας». Άρα γίνεται αντιληπτό ότι είναι αδύνατο να βρεθεί ένας κοινά αποδεκτός ορισμός για την κυβερνοτρομοκρατία, και αυτό επειδή η τρομοκρατία σαν έγκλημα φέρει διαφορετικά χαρακτηριστικά σε κάθε οργανωμένη κοινωνία.

Η καθηγήτρια Denning έδωσε επίσης ένα αρκετά σαφή ορισμό για το έγκλημα της κυβερνοτρομοκρατίας. Αυτός ο ορισμός αναφέρει ότι η κυβερνοτρομοκρατία είναι παράνομες επιθέσεις ή απειλές επιθέσεων που έχουν ως στόχο ηλεκτρονικούς υπολογιστές, δίκτυα ή πληροφορίες δικτύων, με σκοπό τον εκφοβισμό είτε της κυβέρνησης είτε των πολιτών ενός κράτους για να επιτευχθούν κάποιοι πολιτικοί ή κοινωνικοί στόχοι. Μια απειλή θεωρείται τρομοκρατική όταν γίνεται χρήση βίας σε ανθρώπους ή προκαλούνται ζημιές σε περιουσία και γενικά όταν προκαλείται τόσες ζημιές ώστε να προκαλούν φόβο. Επομένως, η κυβερνοτρομοκρατία εμπεριέχει δύο στοιχεία. Το ένα είναι ότι οποιοσδήποτε χρήστης του διαδικτύου μπορεί να πέσει θύμα κυβερνοτρομοκρατίας, αφού τα θύματα επιλέγονται τυχαία. Το άλλο είναι η δυσπιστία και η ανασφάλεια που υπάρχει με την χρήση του διαδικτύου και της τεχνολογίας. Παρά το γεγονός ότι η κυβερνοτρομοκρατία δεν περιέχει την άμεση άσκηση βίας, προκαλεί μεγάλες επιπτώσεις στο ψυχολογικό κομμάτι μπορούν να είναι πολύ ισχυρές όσο πι επιπτώσεις από την άσκηση άμεσης βίας. Τα χαρακτηριστικά της κυβερνοτρομοκρατίας είναι τα εξής :

- Αποτελεί οικονομικό τρόπο εκδήλωσης κυβερνοτρομοκρατικής επίθεσης, αφού οι κυβερνοτρομοκράτες δεν είναι αναγκαίο να αγοράσουν όπλα, εκρηκτικούς μηχανικούς κ.τ.λ. Αυτό που χρειάζονται είναι υπολογιστές και μια σύνδεση στο διαδίκτυο.
- Ο κυβερνοχώρος προσφέρει ανωνυμία, αφού είναι δύσκολο να ελεγχθεί και αν ελεγχθεί θα είναι ένα πολύ μικρό κομμάτι του, δεν μπορεί να υποβληθεί σε περιορισμούς και επίσης δίνει την δυνατότητα ελεύθερης πρόσβασης σε όποιον το επιθυμεί.
- Ο κυβερνοχώρος επίσης προσφέρει μεγάλη ποικιλία σε πιθανούς στόχους, που σημαίνει ότι οι κυβερνοτρομοκράτες μπορούν να στοχεύσουν σε ηλεκτρονικούς υπολογιστές και σε δίκτυα υπολογιστών μεμονωμένων ατόμων, κυβερνήσεων, δημόσιων υπηρεσιών κ.τ.λ. Χαρακτηριστικό παράδειγμα πιθανού στόχου μεγάλης σημασίας είναι οι πάροχοι ηλεκτρικού ρεύματος, γιατί είναι πιο ευάλωτοι επειδή κατέχουν περίπλοκα υπολογιστικά συστήματα, κάτι που σημαίνει ότι υπάρχουν και περισσότερες ευπάθειες που ίσως να μην έχουν ανακαλυφθεί από τους ίδιους τους παρόχους.
- Προσφέρει την δυνατότητα της υλοποίησης των επιθέσεων από απόσταση, χωρίς να απαιτείται η φυσική παρουσία των κυβερνοτρομοκρατών.
- Η αναγκαιότητα της σύγχρονης ανθρώπινης κοινωνίας για την εύρυθμη λειτουργία να χρησιμοποιεί υπολογιστικά συστήματα και δίκτυα, όπως για παράδειγμα τα συστήματα εθνικής άμυνας και τα συστήματα ελέγχου εναέριας κυκλοφορίας, την κάνει περισσότερο ευάλωτη και εκτεθειμένη σε κυβερνοτρομοκρατικές επιθέσεις [49].

Σύμφωνα με τα παραπάνω γίνεται αντιληπτό ότι οι κυβερνοτρομοκράτες αποτελούνται από τις εξής κοινωνικές κατηγορίες :

- ❖ Hackers με μεγάλες δεξιότητες και εμπειρία.

- ❖ Ομάδες ατόμων οι οποίοι έχουν εκπαιδευτεί από διάφορες κυβερνήσεις για διαπράττουν κάθε είδους ηλεκτρονικά εγκλήματα, μέσα σε αυτά και κυβερνοτρομοκρατικές επιθέσεις. Τις ομάδες αυτές αποτελούν συνήθως άτομα νεαρής ηλικίας.
- ❖ Τρομοκρατικές οργανώσεις.
- ❖ Κατάσκοποι που έχουν ως στόχο την υποκλοπή δεδομένων έχοντας κίνητρα ανταγωνισμού και οικονομικά συμφέροντα

Τέλος, πρέπει να αναφερθούν και οι μέθοδοι υλοποίησης επιθέσεων κυβερνοτρομοκρατίας, οι οποίες είναι :

- Μέσω κακόβουλου λογισμικού, δίνοντας στο επιτιθέμενο την δυνατότητα της απομακρυσμένης πρόσβασης σε ένα υπολογιστικό σύστημα ή κλειδώνοντας το σύστημα μέχρις ότου δοθεί από το θύμα το χρηματικό ποσό που αξιώνει ο επιτιθέμενος.
- Μέσω της μόλυνσης εφαρμογών που βρίσκονται στον υπολογιστή που βρίσκεται στο στόχαστρο του κυβερνοτρομοκράτη.
- Μέσω δικτύων botnets που αποτελούνται από υπολογιστές που έχουν μολυνθεί από κακόβουλα λογισμικά bots.
- Μέσω επιθέσεων άρνησης εξυπηρέτησης ή μέσω κατανεμημένων άρνησης εξυπηρέτησης επιθέσεων με στόχο να ρίξουν κάποιον διακομιστή όπως τον διακομιστή μιας κυβερνητικής ιστοσελίδας.
- Μέσω επιθέσεων ηλεκτρονικού «ψαρέματος» - phishing.
- Μέσω επιθέσεων ανεπιθύμητης αλληλογραφίας – spamming.
- Μέσω παραβιάσεων και υποκλοπών προσωπικών δεδομένων που βρίσκονται στο διαδίκτυο.
- Μέσω διαδικτυακής προπαγάνδας διαδίδοντας ψεύτικες ειδήσεις (fake news).
- Μέσω πλαστογραφίας / πλαστοπροσωπίας (identity theft).
- Μέσω διαρροής εμπιστευτικών δεδομένων.
- Μέσω ενδογενών παραγόντων που βρίσκονται στο εσωτερικό κάποιου οργανισμού είτε από λανθασμένες είτε από κακόβουλες ενέργειες κάποιου χρήστη [50].

Κεφάλαιο 3 Εμβάθυνση στον κυβερνοπόλεμο

Ο πόλεμος διαχρονικά υπήρξε ένας τρόπος επίδειξης δύναμης και ισχύος αρχικά μεταξύ φυλετικών ομάδων και αργότερα μεταξύ κρατών. Είναι η χρήση βίας και όπλων μεταξύ δύο ή περισσότερων κρατών και μπορούν να χαρακτηριστούν ως :

- Διακρατικοί πόλεμοι οι οποίοι υποδιαιρούνται σε επιθετικούς ή επεκτατικούς πολέμους και σε αμυντικούς
- Εσωτερικοί πόλεμοι που δεν περιλαμβάνουν εμπλοκή δυο κρατών (όχι άμεση τουλάχιστον) αλλά βρίσκονται στο εσωτερικό μόνο ενός κράτους όπως για παράδειγμα οι εμφύλιοι πόλεμοι.

Υπάρχουν και άλλες κατηγορίες πολέμων πιο εξειδικευμένες, όπως για παράδειγμα οι θρησκευτικοί πόλεμοι και οι δυναστικοί πόλεμοι μεταξύ δύο διαδόχων ενός βασιλείου, όμως και αυτοί μπορούν να θεωρηθούν ανάλογα με τα αίτια και τον τρόπο εκδήλωσής τους ως υποκατηγορίες είτε των διακρατικών είτε των εσωτερικών πολέμων [51].

Με την πάροδο των χρόνων και την εξέλιξη των επιστημών και της τεχνολογίας αλλά και τις αλλαγές που δημιουργήθηκαν στον τρόπο λειτουργίας των κρατών, προέκυψαν νέοι τρόποι, μέσα και τακτικές για την διεξαγωγή ή και την αντιμετώπιση ενός πολέμου. Ένα χαρακτηριστικό παράδειγμα, για κατανοηθεί επαρκώς για τι αλλαγές μιλάμε, είναι η εξέλιξη των όπλων. Από το ρόπαλο στο σπαθί και στην ασπίδα και από εκεί στο υγρό πυρ και την ανακάλυψη της πυρίτιδας, όπου σηματοδότησε την δημιουργία κάθε είδους πυροβόλου όπλου. Άρα, όπως γίνεται αντιληπτό, έτσι και η δημιουργία του διαδικτύου και του κυβερνοχώρου έφεραν την δημιουργία ενός νέου μέσου πολέμου που ονομάζεται «κυβερβοπόλεμος» (cyberwarfare) [52].

3.1Ο ορισμός του κυβερνοπόλεμου

Ο κυβερνοπόλεμος είναι ένα από τα «παραδοσιακά» ηλεκτρονικά εγκλήματα, αφού ο πόλεμος προϋπήρχε της πρώτης εμφάνισης των υπολογιστών και η οποία του έδωσε νέες διαστάσεις και μορφές. Ο κυβερνοπόλεμος είναι μια σύνθετη έννοια και υπάρχουν πολλοί ορισμοί που έχουν δοθεί από τους ειδικούς κατά καιρούς. Ο Lachow υποστηρίζει ότι ο κυβερνοπόλεμος είναι « η προετοιμασία και η διεξαγωγή στρατιωτικών επιχειρήσεων σύμφωνα με τις αρχές που σχετίζονται με πληροφορίες. Περιλαμβάνει διατάραξη, αν όχι ολική καταστροφή των συστημάτων πληροφοριών και επικοινωνιών με την ευρεία έννοια οριζόμενα να περιλαμβάνουν ακόμα και στρατιωτική κουλτούρα, στην οποία ο αντίπαλος στηρίζεται για να «γνωρίσει» από μόνος του ».

Ένας ακόμα ορισμός αναφέρει ότι κυβερνοπόλεμος αποτελεί έναν ανταγωνισμό ανάμεσα σε δύο αντίπαλες πλευρές, οι οποίες εκμεταλλεύονται διάφορες τεχνολογίες και μεθόδους δικτύων προκειμένου να επιτύχουν πλεονέκτημα στους τομείς της πληροφορικής, της πολιτικής, της οικονομίας, της στρατηγικής και της τεχνολογίας [53]. Αυτός ο ορισμός είναι παρόμοιος με τον ορισμό που έδωσε ο πρώην σύμβουλος ασφαλείας του Λευκού Οίκου, Richard Clarke, ο οποίος περιγράφει ότι «Ο κυβερνοπόλεμος είναι η καταστροφή, η αναστάτωση ή η πρόκληση ζημιάς σε συστήματα του πραγματικού κόσμου μέσω των επιθέσεων με συστήματα υπολογιστών, κάτι που συμβαίνει μόνο κατά τη διάρκεια κάποιου πολέμου ή, υποθέτω, κάποιας μυστικής δράσης. Άρα, πρόκειται να συμβεί όταν κράτη θα πάνε σε πόλεμο μεταξύ τους» [54]. Επομένως, ο κυβερνοπόλεμος μπορεί να θεωρηθεί ως ο

πέμπτος τομέας πολέμου μετά την στεριά, το νερό, τον αέρα και το διάστημα και ο οποίος περιλαμβάνει την χρήση της τεχνολογίας και κάθε είδους ηλεκτρονικού μέσου, ώστε πραγματοποιηθούν δυσλειτουργίες ακόμα και ολικές καταστροφές στις δραστηριότητες ενός κράτους, ειδικότερα οι επιθέσεις σε πληροφοριακά συστήματα και δίκτυα για στρατηγικούς και στρατιωτικούς σκοπούς [55].

Τέλος, οι ένοπλες δυνάμεις των Ηνωμένων Πολιτειών καθορίζουν τον κυβερνοπόλεμο ως κάθε στρατιωτική δράση που περιλαμβάνει την εκμετάλλευση ηλεκτρομαγνητικής και κατευθυνόμενης ενέργειας για τον έλεγχο του ηλεκτρομαγνητικού φάσματος ή για επίθεση κατά του εχθρού. και αποτελείται από τα εξής στοιχεία :

1. Η ηλεκτρονική προστασία περιλαμβάνει τόσο παθητικά όσο και ενεργά μέτρα για την προστασία του προσωπικού και του εξοπλισμού από εχθρικές ηλεκτρονικές απειλές.
2. Η ηλεκτρονική υποστήριξη που περιλαμβάνει την καταγραφή των ηλεκτρονικών εκπομπών του αντιπάλου για ενδεχόμενη εκμετάλλευση σε μεταγενέστερο στάδιο.
3. Η ηλεκτρονική επίθεση αντιστοιχεί σε επίθεση κατά ηλεκτρονικών υπολογιστών και αντίκειται στους κανόνες του διεθνούς δικαίου, δηλαδή, προκαλεί βλάβη σε δίκτυα Η/Υ χρησιμοποιώντας τους Η/Υ ως όπλα.

Ωστόσο, ο κυβερνοπόλεμος έχεις μεγάλες διαφορές με τον κανονικής μορφής πόλεμο. Μερικές από αυτές είναι :

- a. Δεν μπορεί να προσδιοριστεί γεωγραφικά όπως ο κανονικός πόλεμος
- b. Δεν χρειάζεται μεγάλα χρηματικά κονδύλια για να διεξαχθεί
- c. Είναι άμεσος και δεν χρειάζεται χρόνο για να διεξαχθεί
- d. Δεν χρειάζεται να ανακηρυχθεί όπως γίνεται στον κανονικό και για αυτό μπορεί να χαρακτηριστεί ως ακήρυχτος πόλεμος
- e. Είναι ένα είδος ασύμμετρου πολέμου αφού η ταυτότητα του επιτιθέμενου μπορεί να μείνει άγνωστη και μπορεί να είναι ιδιαίτερα καταστροφικός και απρόβλεπτος [52].

3.2 Χαρακτηριστικά και μορφές του κυβερνοπολέμου

Ο κυβερνοπόλεμος έχει κάποια ιδιαίτερα χαρακτηριστικά που τον κάνουν να διαφέρει από τον παραδοσιακό πόλεμο. Αυτά τα χαρακτηριστικά είναι τα παρακάτω :

- Ανυπαρξία δημόσιων, επιστημονικών και πολιτικών άποψεων σχετικά με τον τρόπο που θα μπορούσαμε να κάνουμε σωστή χρήση τέτοιων κυβερνοόπλων, τόσο σε πολιτικό επίπεδο όσο και από άποψη δεοντολογίας. Είναι σχεδόν αδύνατο να εντοπιστούν οι πηγές τέτοιων κυβερνοεπιθέσεων.
- Οι περισσότερες επιθέσεις κυβερνοπολέμου δεν έχουν τον ίδιο καταστροφικό αντίκτυπο και δεν μπορούν να προκαλέσουν απώλεια ανθρώπινων ζωών, όπως συμβαίνει με τα συμβατικά όπλα και τα πυρηνικά.
- Κάθε υπολογιστικό σύστημα και ηλεκτρονικός υπολογιστής μπορεί να χρησιμοποιηθεί ως πιθανό μέσο για τη διεξαγωγή μιας επίθεσης κυβερνοπολέμου, δηλαδή, μπορεί να αποτελέσει πιθανό κυβερνοόπλο. Επίσης, κάθε χρήστης στον τομέα της κυβερνοασφάλειας με εξαιρετικές προγραμματιστικές και τεχνολογικές δεξιότητες, και εκτενείς γνώσεις στον τομέα των πληροφοριακών συστημάτων, μπορεί να αποτελέσει πιθανό κυβερνοεγκληματία ή κυβερνοπολεμιστή.

- Η προστασία στον κυβερνοχώρο συνεπάγεται υψηλό κόστος και είναι ευάλωτη, όπως και η προστασία μέσω στρατιωτικών συστημάτων, ενώ η επίθεση είναι συνήθως οικονομικά προσιτή. Αυτό μπορεί να συγκριθεί με περιπτώσεις όπως η πυρηνική ασφάλεια και η αντιπυραυλική τεχνολογία και άλλες αντίστοιχες.
- Είναι αβέβαιο τι θα επακολουθήσει με μια κυβερνοεπίθεση ή σε έναν κυβερνοπόλεμο.
- Δεν είναι δυνατό να προβλεφθούν ακριβώς οι μακροπρόθεσμες δυσμενείς επιπτώσεις, όπως ασθένειες, οικονομικές κρίσεις και άλλα παρόμοια [54].

Ο κυβερνοπόλεμος μπορεί να έχει δύο κύριες μορφές. Η μια μορφή είναι ο «στρατηγικός» κυβερνοπόλεμος και η άλλη μορφή είναι ο «επιχειρησιακός» κυβερνοπόλεμος. Για τον στρατηγικό κυβερνοπόλεμο αναφέρεται ότι σε αυτή την μορφή εντάσσονται επιθέσεις οι οποίες στοχεύουν να επηρεάσουν αρνητικά την κυβερνητική πολιτική του αντιπάλου χρησιμοποιώντας μεθόδους εξαναγκασμού. Μια κυβερνοεπίθεση για να χαρακτηριστεί ως επίθεση στρατηγικού κυβερνοπόλεμου πρέπει να καλύπτει τρεις βασικές προϋποθέσεις :

1. Να μην υπάρχει άλλου είδους εχθροπραξιών ανάμεσα στις εμπλεκόμενες οντότητες – χώρες ή στην περίπτωση που υπάρχουν να μην είναι πρωτεύουσας σημασίας.
2. Εξαπόλυση κυβερνοεπιθέσεων από όλες τις εμπλεκόμενες χώρες – οντότητες.
3. Αδύνατη επίλυση της αντιπαράθεσης μέσω νομικών, διπλωματικών ή οικονομικών οδών και στην χρήση κυβερνοεπιθέσεων ως το μόνο μέσο επίλυσης.

Ωστόσο, ο στρατηγικός κυβερνοπόλεμος δεν εστιάζει μόνο στο να επηρεάσει αρνητικά την κυβερνητική πολιτική του αντιπάλου. Ο στρατηγικός κυβερνοπόλεμος επικεντρώνεται και στην διαχείριση της κυβερνοσύγκρουσης. Με πιο απλά λόγια έχει ως στόχο τον έλεγχο της κλιμάκωσής και της αποκλιμάκωσης ή της παύσης της σύγκρουσης, αλλά και τον περιορισμό του εύρους της. Αξίζει να σημειωθεί επίσης ότι ο στρατηγικός κυβερνοπόλεμος δεν είναι το υπέρτατο μέσο επίτευξης των στόχων που έχει θέσει ο επιτιθέμενος, καθώς έχει σαφείς και περιορισμένες δυνατότητες επιτυχίας. Έτσι γίνεται αντιληπτό ότι το αποτέλεσμα των αντικειμενικών στόχων, είναι σχετικό με το μέγεθος της επιρροής που επιφέρουν οι κυβερνοεπιθέσεις στο κράτος-στόχο. Αδιαμφισβήτητα, οι επιπτώσεις του στρατηγικού πολέμου είναι διαφορετικές σε μεγάλο βαθμό σε σχέση με αυτή του συμβατικού πολέμου. Ο βασικός λόγος είναι το γεγονός ότι η πίεση προς ένα κράτος σχετίζεται, αναλογικά, με τον αριθμό των ανθρώπινων απωλειών, οι οποίες προκαλούνται από μια σύγκρουση, πράγμα το οποίο δεν συμβαίνει με τον κυβερνοπόλεμο, επειδή η εκδήλωση αυτού του τύπου κυβερνοεπιθέσεων δεν έχει ως πρωτεύοντα στόχο την απώλεια ανθρώπινης ζωής. Επιπροσθέτως, τα αποτελέσματα του στρατηγικού κυβερνοπολέμου αποτελούν προσωρινά αποτελέσματα και ενθαρρύνουν την άποψη της κοινής γνώμης για απερίσκεπτη συμμετοχή στον εξαναγκασμό.

Με την ανάλυση της αντιπαραθετικής προσέγγισης όμως, συνολικά εκφράζεται ότι με τον στρατηγικό κυβερνοπόλεμο μπορεί να επιτευχθεί κάποια πίεση ή εξαναγκασμός του κράτους που είναι στο στόχαστρο του επιτιθέμενου, αν ακολουθούνται ορισμένες προϋποθέσεις. Η ιδέα αυτή προέρχεται από την κλασική "Τριάδα" του Clausewitz, που αποτελείται από το λαό, τις ένοπλες δυνάμεις και την κυβέρνηση, αλλά και το επίπεδο εξάρτησης κάθε μεμονωμένου στοιχείου της «Τριάδας» από τα συστήματα ηλεκτρονικών υπολογιστών. Αν σκεφτεί κάποιος την καθημερινότητά του και την καθημερινότητα των υπόλοιπων ατόμων, είναι εύκολο να καταλάβει ότι η ανθρώπινη ζωή είναι απευθείας

συνδεδεμένη με τα συστήματα ηλεκτρονικών υπολογιστών. Οι χρηματοοικονομικές συναλλαγές, οι τηλεπικοινωνίες και η υγεία είναι κάποιες από τις καθημερινές δραστηριότητες που το αποδεικνύουν. Επίσης, αξίζει να σημειωθεί ότι οι ένοπλες δυνάμεις των κρατών πλέον εξαρτώνται από την τεχνολογία της πληροφορικής και τον κυβερνοχώρο, με τους ηλεκτρονικούς υπολογιστές να χρησιμοποιούνται για ενέργειες όπως, η διαχείριση των συστημάτων διοίκησης και ελέγχου, η αποστολή και λήψη της στρατιωτικής αλληλογραφίας, η υλοποίηση των επικοινωνιών και η παρακολούθηση και η αναγνώριση της περιοχής που διεξάγεται ή που πρόκειται να διεξαχθεί μια μάχη. Ακόμα, η εποπτεία των αναγκών του λαού από την κυβερνητική ηγεσία ενός κράτους, ο έλεγχος για την υλοποίηση και την τήρηση των αποφάσεων της κυβέρνησης από τους πολίτες, αλλά και η επικοινωνία με τον λαό βασίζονται σε συστήματα υπολογιστών. Τέλος, μόνο στην περίπτωση συγχρονισμένης και μεγάλης κλίμακας κυβερνοεπίθεσης και στα τρία δομικά στοιχεία της «Τριάδας» θα υπάρξει κάποιο αποτέλεσμα έτσι ώστε, το κράτος που βρίσκεται στο στόχαστρο του επιτιθέμενου να καταλήξει σε στρατηγική παράλυση, αδυνατώντας να ανταποκριθεί αποτελεσματικά και τελικά να υποταχθεί στην βουλή του εχθρού – επιτιθέμενου.

Ο όρος «επιχειρησιακός κυβερνοπόλεμος» αναφέρεται στις κυβερνοεπίθεσεις οι οποίες εκδηλώνονται για να υποστηρίξουν έναν συμβατικό πόλεμο, με στόχο να πλήξουν στρατιωτικούς και μη στρατιωτικούς στόχους. Η επίθεση σε μη στρατιωτικούς στόχους είναι ιδιαίτερα σημαντική, αν σκεφτεί κανείς την πιθανή ζημία που μπορεί να προκληθεί στη διεξαγωγή στρατιωτικών επιχειρήσεων, όπως για παράδειγμα την επίθεση σε τηλεπικοινωνιακά δίκτυα ή σε εγκαταστάσεις.

Για να μπορέσει να χαρακτηριστεί μια κυβερνοεπίθεση ως «επιχειρησιακός κυβερνοπόλεμος» θα πρέπει να διευκρινιστούν τα παρακάτω :

- Οι δραστηριότητες συλλογής πληροφοριών από το κυβερνοχώρο (κυβερνοκατασκοπεία) δεν αποτελούν επιχειρησιακό πόλεμο.
- Η φυσική επίθεση στα δίκτυα ηλεκτρονικών υπολογιστών, η οποία επιφέρει την καταστροφή τους, δεν αντιπροσωπεύει επιχειρησιακό κυβερνοπόλεμο.
- Η εκτέλεση ψυχολογικών διαδικασιών ανήκει στον τομέα των πληροφοριακών επιχειρήσεων και όχι στην περίπτωση του επιχειρησιακού κυβερνοπολέμου.

Όπως ειπώθηκε και στον στρατηγικό κυβερνοπόλεμο τα αποτελέσματα δεν είναι μόνιμα και η χρήση των κυβερνοόπλων επικεντρώνεται στην υλοποίηση περιορισμένων στόχων. Ακριβέστερα, ο επιχειρησιακός κυβερνοπόλεμος έχει ως αποτέλεσμα την απροσδόκητη επίθεση κατά του αντιπάλου αιφνιδιαζόντάς τον. Στον κυβερνοχώρο, ο αιφνιδιασμός μπορεί να επιτευχθεί είτε πριν την έναρξη των συμβατικών επιχειρήσεων είτε κατά τη διάρκειά τους. Για τη διατήρηση του αιφνιδιασμού είναι απαραίτητο να διενεργείται πλήρης και ολοκληρωμένη κυβερνοκατασκοπεία, με στόχο να ανακαλυφθούν όλα τα σημεία αδυναμίας του αντιπάλου στον κυβερνοχώρο. Ακόμα, απαιτείται η διαθεσιμότητα μεγάλης γκάμας κυβερνοόπλων, καθώς η επαναλαμβανόμενη χρήση του ίδιου εργαλείου – κυβερνοόπλου δεν θα επιφέρει το επιδιωκόμενο αποτέλεσμα του αιφνιδιασμού.

Επίσης, το μεγαλύτερο κατόρθωμα του επιχειρησιακού κυβερνοπολέμου είναι η ικανότητα αποτροπής του αντιπάλου από την χρήση του κυβερνοχώρου για μια συγκεκριμένη χρονική περίοδο. Η παρεμπόδιση στον αντίπαλο να χρησιμοποιήσει τα υπολογιστικά συστήματα και δίκτυα, μπορεί να επιφέρει φόβο με αποτέλεσμα την απομόνωση, και αυτό

μπορεί να έχει αρνητικό επιχειρησιακό αντίκτυπο στην πραγματοποίηση των επιχειρήσεων και στη μεταφορά ζωτικής σημασίας πληροφοριών. Από την άλλη πλευρά, μέσω του επιχειρησιακού κυβερνοπολέμου δεν είναι δυνατό να επιτευχθεί νίκη σε μια στρατιωτική σύγκρουση ή να γίνει κατάληψη εδάφους. Εξαιτίας της προσωρινής διάρκειας των αποτελεσμάτων ενός επιχειρησιακού κυβερνοπολέμου, δεν μπορεί να οδηγηθεί με αυτόν τον τρόπο ένα σταθερό και ενωμένο κράτος στην εθελοντική παράδοσή του στον αντίπαλο. Επιπλέον, Ο επιχειρησιακός κυβερνοπόλεμος δεν μπορεί να εξασφαλίσει αποκλειστική υπεροχή στον κυβερνοχώρο, σε αντίθεση με την υπεροχή που επιτυγχάνεται μέσω συμβατικών συγκρούσεων στη ξηρά, τη θάλασσα και τον αέρα. Αυτό συμβαίνει διότι ο κυβερνοχώρος δεν αποτελεί μία ενιαία περιοχή, αλλά αποτελείται τουλάχιστον από ένα τμήμα σε κάθε αντίπαλη οντότητα [56].

Εκτός βέβαια από αυτές τις δύο κύριες μορφές, ο κυβερνοπόλεμος μπορεί να χωριστεί και σε πιο εξειδικευμένους τύπους ανάλογα με τον τρόπο που εκδηλώνεται. Οι τρόποι αυτοί είναι οι παρακάτω:

- **Κατασκοπεία (espionage).** Η κατασκοπεία αναφέρεται στο κατασκοπευτικό έργο σε άλλη χώρα για να κλαπούν μυστικά. Στον κυβερνοπόλεμο, αυτό μπορεί να συμπεριλάβει τη χρήση ενός botnet ή spear-fishing επίθεσης για να αποκτηθεί πρόσβαση σε έναν υπολογιστή πριν αποσπαστούν ευαίσθητες πληροφορίες.
- **Δολιοφθορά (sabotage).** Αφού αναγνωρίσουν τις ευαίσθητες πληροφορίες, οι οργανισμοί πρέπει να προσδιορίσουν τις πιθανές απειλές που αντιμετωπίζουν αυτά τα δεδομένα. Αυτό περιλαμβάνει τρίτα μέρη που ενδέχεται να επιθυμούν να κλέψουν τα δεδομένα, ανταγωνιστές που μπορούν να αποκομίσουν πλεονέκτημα με την κλοπή πληροφοριών, και εσωτερικές απειλές ή κακόβουλους εντός της επιχείρησης, όπως απογοητευμένους εργαζόμενους ή αμελείς εργαζόμενους.
- **Denial of Service attacks.** Μια επίθεση άρνησης εξυπηρέτησης (Denial-of-Service, DoS) εμπεριέχει την πλημμύρα (υπερφόρτωση) μιας ιστοσελίδας με ψεύτικα αιτήματα, αναγκάζοντας έτσι την ιστοσελίδα να επεξεργαστεί αυτά τα αιτήματα, και ως εκ τούτου να την καταστήσει μη διαθέσιμη για τους νόμιμους χρήστες.
- **Επιθέσεις στα δίκτυα ηλεκτρικής ενέργειας (electrical power grid attacks).** Η κακόβουλη διείσδυση στο ηλεκτρικό δίκτυο θα μπορούσε να δώσει στον επιτιθέμενο τη δυνατότητα να απενεργοποιήσει κρίσιμα συστήματα, παραλύοντας τη υποδομή και προκαλώντας τον θάνατο χιλιάδων ανθρώπων. Επιπλέον, μια επίθεση στο ηλεκτρικό δίκτυο θα μπορούσε να διακόψει τις επικοινωνίες, καθιστώντας αδύνατη τη χρήση υπηρεσιών όπως τα μηνύματα κειμένου ή η τηλεπικοινωνία.
- **Προπαγάνδα (propaganda).** Οι επιθέσεις προπαγάνδας περιλαμβάνουν την προσπάθεια ελέγχου των μυαλών ή των συναισθημάτων των ανθρώπων που ζουν ή πολεμούν για τη χώρα που βρίσκεται στο στόχαστρο επιθέσεων κυβερνοπολέμου. Η προπαγάνδα μπορεί να χρησιμοποιηθεί για να αποκαλύψει ενοχλητικές αλήθειες ή για να διαδώσει ψέματα που προκαλούν την απώλεια της εμπιστοσύνης των ανθρώπων στη χώρα τους, ή ακόμη και συμπάθεια προς τον εχθρό.
- **Αποδιοργάνωση στην οικονομία (economic disruption).** Τα περισσότερα σύγχρονα οικονομικά συστήματα εξαρτώνται από υπολογιστές για να λειτουργήσουν. Η επίθεση στα υπολογιστικά δίκτυα οικονομικών εγκαταστάσεων όπως τα χρηματιστήρια, τα συστήματα πληρωμών ή οι τράπεζες μπορεί να δώσει στους hackers πρόσβαση σε κεφάλαια ή να εμποδίσει τους στόχους τους από το να λάβουν

τα χρήματα που χρειάζονται για να ζήσουν ή να εμπλακούν σε κυβερνοπόλεμο ή άλλη μορφή πολέμου.

- **Αιφνίδια κυβερνοεπίθεση (surprise cyberattack).** Αυτά αναφέρονται στα είδη των κυβερνοεπιθέσεων που θα είχαν μια επίδραση παρόμοια με αυτή της επίθεσης στο Pearl Harbor ή της 11ης Σεπτεμβρίου - μαζικές επιθέσεις που πιάνουν τον εχθρό αδιάβαστο, αδυνατώντας τις αμυντικές τους δυνάμεις. Θα μπορούσαν να χρησιμοποιηθούν για να αποδυναμώσουν τον αντίπαλο προετοιμαζόμενοι για μια φυσική επίθεση ως μια μορφή υβριδικού πολέμου [57].

3.3 Στόχοι κυβερνοπολέμου

Σύμφωνα με την Υπηρεσία Κυβερνοασφάλειας και Ασφάλειας Υποδομών των Ηνωμένων Πολιτειών, υπάρχουν δεκαέξι κρίσιμοι τομείς υποδομών, των οποίων τα περιουσιακά στοιχεία, τα υπολογιστικά συστήματα και τα δίκτυα, είτε φυσικά είτε εικονικά, θεωρούνται ζωτικής σημασίας για την εύρυθμη λειτουργία του κράτους, ούτως ώστε μια πιθανή δυσλειτουργία ή καταστροφή μπορεί να προκαλέσει αποδυνάμωση για την ασφάλεια, την οικονομική ασφάλεια της χώρας, την εθνική δημόσια υγεία ή ασφάλεια, ή οποιοσδήποτε συνδυασμός αυτών. Οι πιθανοί στόχοι να πέσουν θύματα κυβερνοεπιθέσεων ενός κυβερνοπολέμου είναι οι εξής [58] :

- **Ο χημικός τομέας** ο οποίος είναι ένα αναπόσπαστο κομμάτι της κρατικής οικονομίας, ο οποίος κατασκευάζει, αποθηκεύει, χρησιμοποιεί και μεταφέρει δυνητικά επικίνδυνα χημικά που εξαρτώνται από μια ευρεία γκάμα άλλων κρίσιμων κλάδων υποδομής. Η ασφάλεια αυτών των χημικών έναντι των αυξανόμενων και εξελισσόμενων απειλών απαιτεί προσοχή τόσο από τον ιδιωτικό όσο και από τον δημόσιο τομέα. Εδώ εντάσσονται κάθε είδους χημική βιομηχανία, όπως οι φαρμακοβιομηχανίες, βιομηχανίες φυτοφαρμάκων και λιπασμάτων και βιομηχανίες καθαριστικών και απορρυπαντικών προϊόντων [59].
- **Ο τομέας επικοινωνιών** είναι σημαντικός παράγοντας για την ανάπτυξη της οικονομίας ενός κράτους αφού συνεισφέρει στην λειτουργία όλων των επιχειρήσεων, οργανισμών δημόσιας ασφάλειας και της κυβέρνησης. Θεωρείται ζωτικής σημασίας επειδή παρέχει μια λειτουργία διευκόλυνσης σε όλους τους κρίσιμους τομείς υποδομών. Τα τελευταία χρόνια ο τομέας των επικοινωνιών έχει εξελιχθεί από το να προσφέρει κυρίως φωνητικές υπηρεσίες σε μια ποικίλη, ανταγωνιστική και διασυνδεδεμένη βιομηχανία που χρησιμοποιεί συστήματα επίγειας, δορυφορικής και ασύρματης μετάδοσης. Η μετάδοση αυτών των υπηρεσιών έχει γίνει αλληλοεξαρτώμενη, όπου οι πάροχοι δορυφορικών, ασύρματων και ενσύρματων υπηρεσιών εξαρτώνται ο ένας από τον άλλο για τη μεταφορά και τη λήξη της κυκλοφορίας τους και οι εταιρείες συχνά μοιράζονται εγκαταστάσεις και τεχνολογία για να εξασφαλίσουν τη συμβατότητα μεταξύ τους [60].
- **Ο τομέας των εμπορικών εγκαταστάσεων** που περιλαμβάνει μια ποικιλία από τοποθεσίες που προσελκύουν μεγάλο αριθμό ανθρώπων για ψώνια, επιχειρηματικές δραστηριότητες, ψυχαγωγία ή διαμονή. Οι εγκαταστάσεις στον κλάδο αυτό λειτουργούν με βάση την αρχή της ανοικτής δημόσιας πρόσβασης, που σημαίνει ότι το γενικό κοινό μπορεί να κινηθεί ελεύθερα χωρίς τον αποτρεπτικό παράγοντα εμποδίων ασφαλείας. Η πλειοψηφία αυτών των εγκαταστάσεων είναι ιδιωτικής ιδιοκτησίας και λειτουργούν με ελάχιστη αλληλεπίδραση με την κυβέρνηση και άλλους ρυθμιστικούς φορείς [61].

- **Ο κατασκευαστικός τομέας** είναι κρίσιμης σημασίας για την οικονομική ευημερία και την ανάπτυξη ενός κράτους. Μια άμεση επίθεση ή διαταραχή στην λειτουργία της κατασκευαστικής βιομηχανίας θα μπορούσε να διακόψει τις βασικές λειτουργίες σε εθνικό επίπεδο και σε πολλούς κρίσιμους τομείς υποδομών. Παραδείγματα τέτοιων υποδομών είναι βιομηχανίες κατασκευής βασικής μεταλλουργίας όπως το σίδηρο το αλουμίνιο κ.τ.λ., βιομηχανίες κατασκευής μηχανημάτων, βιομηχανίες κατασκευής ηλεκτρονικού εξοπλισμού, συσκευών και εξαρτημάτων, βιομηχανίες κατασκευής εξοπλισμού μεταφοράς κ.α. [62].
- **Ο τομέας φραγμάτων νερού** παρέχει πολύ σημαντικές υπηρεσίες αποθήκευσης και ελέγχου υδάτων, όπως η παραγωγή υδροηλεκτρικής ενέργειας, η παροχή υδροδότησης τόσο σε δημοτικό επίπεδο όσο και σε βιομηχανικό, η άρδευση γεωργικών εκτάσεων, ο έλεγχος των πλημμυρών, η πλοήγηση στα ποτάμια για μαζική ναυτιλία, η διαχείριση βιομηχανικών αποβλήτων και η αναψυχή. Οι βασικές υπηρεσίες αυτού του τομέα υποστηρίζουν άλλους κρίσιμους τομείς υποδομών και βιομηχανίες [63].
- **Ο τομέας της βιομηχανίας άμυνας** αποτελεί το παγκόσμιο βιομηχανικό συγκρότημα που επιτρέπει την έρευνα και ανάπτυξη, καθώς και το σχεδιασμό, την παραγωγή, την παράδοση και τη συντήρηση συστημάτων όπλων, υποσυστημάτων και εξαρτημάτων ή μερών αυτών, για να ικανοποιηθούν οι απαιτήσεις των Ενόπλων Δυνάμεων ενός κράτους. Η βάση της βιομηχανίας άμυνας ενός κράτους συνεργάζεται με εκατοντάδες χιλιάδες εταιρείες που ασχολούνται με την αμυντική βιομηχανία και με τους υποπρομηθευτές τους όπου, τους εφοδιάζουν με όλα εκείνα τα απαραίτητα υλικά αλλά και με εγκαταστάσεις που ανήκουν στο κράτος και τις διαχειρίζονται είτε το ίδιο το κράτος, είτε κάποιοι εξωτερικοί συνεργάτες, με τους οποίους το κράτος έχει επισυνάψει σύμβαση. Οι εταιρείες της βιομηχανίας άμυνας αποτελούνται από εγχώριες και ξένες επιχειρήσεις, με εργοστάσια παραγωγής που βρίσκονται σε πολλές χώρες. Ο τομέας παρέχει προϊόντα και υπηρεσίες που είναι ουσιώδεις για την κινητοποίηση, την αποστολή και τη διατήρηση στρατιωτικών επιχειρήσεων. Παρ' όλα αυτά ο τομέας της βιομηχανίας άμυνας δεν περιλαμβάνει τις εμπορικές υποδομές των παρόχων υπηρεσιών όπως η ενέργεια, οι επικοινωνίες, η μεταφορά ή οι δημόσιες υπηρεσίες που χρησιμοποιεί το Υπουργείο Άμυνας για να καλύψει τις στρατιωτικές λειτουργικές ανάγκες του [64].
- **Ο τομέας επειγουσών υπηρεσιών** αποτελεί μια μεγάλη κοινότητα εξειδικευμένων και καταρτισμένων ατόμων, μαζί με τους φυσικούς και ηλεκτρονικούς πόρους, οι οποίοι παρέχουν μια ευρεία γκάμα πρόληψης, προετοιμασίας, αντίδρασης και αποκατάστασης κατά την διάρκεια της καθημερινής λειτουργίας και της ανταπόκρισης σε περιστατικά. Ο τομέας αυτός περιλαμβάνει γεωγραφικά κατανομημένες εγκαταστάσεις και εξοπλισμό, τόσο σε επί πληρωμή όσο και σε εθελοντικές ικανότητες, οργανωμένες κυρίως στα επίπεδα της ομοσπονδιακής, κρατικής, τοπικής και επικρατειακής διακυβέρνησης, όπως τμήματα αστυνομίας και πυροσβεστικοί σταθμοί, διάφορα τμήματα του Υπουργείου Άμυνας και τμήματα δημοτικών έργων των πόλεων. Περιλαμβάνει επίσης πόρους του ιδιωτικού τομέα, όπως βιομηχανικά τμήματα πυρόσβεσης, οργανώσεις ιδιωτικής ασφάλειας και παρόχους ιδιωτικών υπηρεσιών έκτακτης ανάγκης. Εδώ ανήκουν υπηρεσίες όπως η άμεση δράση της αστυνομίας, υπηρεσίες πυρκαγιών και έρευνας και διάσωσης κ.τ.λ. [65].
- **Ο τομέας της ενέργειας** έχει πολύ σημαντικό ρόλο για την οικονομία ενός κράτους τον 21^ο αιώνα. Πλέον χωρίς σταθερή ενεργειακή προμήθεια, η υγεία και η ευημερία κινδυνεύουν, και η οικονομία των περισσότερων αναπτυγμένων κρατών δεν μπορεί να λειτουργήσει. Ο ενεργειακός τομέας θεωρείται μοναδικά κρίσιμος, καθώς παρέχει μια

«ενεργοποιητική λειτουργία» σε όλους τους άλλους τομείς της κρίσιμης υποδομής. Στις περισσότερες χώρες σαν τις Η.Π.Α. το μεγαλύτερο ποσοστό των υποδομών ενέργειας ανήκουν στον ιδιωτικό τομέα, παρέχοντας καύσιμα στη βιομηχανία μεταφορών, ηλεκτρικό ρεύμα σε νοικοκυριά και επιχειρήσεις, και άλλες πηγές ενέργειας που είναι ουσιώδεις για την ανάπτυξη και την παραγωγή αυτών των χωρών [66].

- **Ο τομέας των χρηματοπιστωτικών υπηρεσιών** αντιπροσωπεύει ένα σημαντικό συστατικό της κρίσιμης υποδομής της χώρας μας. Μεγάλης κλίμακας διακοπές ρεύματος, πρόσφατες φυσικές καταστροφές και η αύξηση του αριθμού και της εξειδίκευσης των κυβερνοεπιθέσεων αποδεικνύουν το ευρύ φάσμα των δυνητικών κινδύνων που αντιμετωπίζει ο συγκεκριμένος τομέας. Ο τομέας των χρηματοπιστωτικών υπηρεσιών περιλαμβάνει χιλιάδες χρηματοπιστωτικά ιδρύματα, παρόχους επενδυτικών προϊόντων, ασφαλιστικές εταιρείες, άλλους οργανισμούς πίστωσης και χρηματοδότησης, και τους παρόχους των κρίσιμων χρηματοπιστωτικών υπηρεσιών και εργαλείων που υποστηρίζουν αυτές τις λειτουργίες. Τα χρηματοπιστωτικά ιδρύματα διαφέρουν σημαντικά σε μέγεθος και παρουσία, κυμαίνονται από μερικές από τις μεγαλύτερες εταιρείες στον κόσμο με χιλιάδες υπαλλήλους και πολλά δισεκατομμύρια δολάρια σε περιουσία, έως τις τοπικές τράπεζες και συνεταιριστικά καταστήματα με λίγους υπαλλήλους που εξυπηρετούν μεμονωμένες κοινότητες. Είτε πρόκειται για ένα ατομικό λογαριασμό αποταμίευσης, χρηματοπιστωτικά παράγωγα, πίστωση που παρέχεται σε μια μεγάλη επιχείρηση, είτε επενδύσεις που γίνονται σε ξένη χώρα, αυτά τα προϊόντα επιτρέπουν στους πελάτες :
 - Να καταθέτουν κεφάλαια και να πραγματοποιούν πληρωμές προς άλλους συμβαλλόμενους.
 - Να παρέχουν πίστωση και ρευστότητα στους πελάτες.
 - Να επενδύσουν κεφάλαια για μακροπρόθεσμα και βραχυπρόθεσμα χρονικά διαστήματα.
 - Να μεταφέρουν τα οικονομικά ρίσκα μεταξύ των πελατών[67].
- **Ο τομέας τροφίμων και γεωργίας** είναι σχεδόν πλήρως υπό ιδιωτική ιδιοκτησία και αποτελείται από αγροκτήματα, εστιατόρια και από εγγεγραμμένες μονάδες κατασκευής, επεξεργασίας και αποθήκευσης τροφίμων. Αυτός ο τομέας αποτελεί βασικό γρανάζι της οικονομίας μιας χώρας αφού συντελεί τον πρωτογενή της τομέα. Ο τομέας τροφίμων και γεωργίας συνεργάζεται με αρκετούς από τους υπόλοιπους βασικούς τομείς όπως :
 - Συστήματα ύδρευσης και αποχέτευσης, για καθαρή άρδευση και επεξεργασμένο νερό.
 - Συστήματα μεταφορών, για την μεταφορά αγροτικών και κτηνοτροφικών προϊόντων.
 - Με τον τομέα ενέργειας, για την παροχή ενέργειας στον εξοπλισμό που απαιτείται για τη γεωργική παραγωγή και την επεξεργασία τροφίμων.
 - Τον χημικό τομέα, για τα λιπάσματα και τα φυτοφάρμακα που χρησιμοποιούνται στην παραγωγή των καλλιεργειών [68].
- **Ο τομέας των κυβερνητικών εγκαταστάσεων** περιλαμβάνει μια μεγάλη ποικιλία κτιρίων, που βρίσκονται στο εσωτερικό του κράτους και στο εξωτερικό, τα οποία ιδιοκτησιακά ή επί πληρωμή κάποιου ενοικίου ανήκουν στη κυβέρνηση του κράτους. Πολλά κυβερνητικά κτίρια είναι ανοιχτά στο κοινό για επαγγελματικές δραστηριότητες, εμπορικές συναλλαγές ή ψυχαγωγικές δραστηριότητες, ενώ άλλα που δεν είναι ανοιχτά στο κοινό περιλαμβάνουν υψηλά ευαίσθητες πληροφορίες, υλικά, διαδικασίες και εξοπλισμό. Αυτές οι εγκαταστάσεις περιλαμβάνουν κτήρια γενικής χρήσης και ειδικής χρήσης, στρατιωτικών εγκαταστάσεων, πρεσβειών, δικαστηρίων, εθνικών εργαστηρίων και δομές που μπορεί να φιλοξενούν κρίσιμο εξοπλισμό, συστήματα, δίκτυα και

λειτουργίες. Εκτός από τις φυσικές δομές, ο τομέας περιλαμβάνει στοιχεία κυβερνοασφαλείας που συντελούν στην προστασία των περιουσιακών στοιχείων του τομέα (π.χ. συστήματα ελέγχου πρόσβασης και συστήματα κλειστού κυκλώματος τηλεόρασης), καθώς και άτομα που εκτελούν ουσιαστικές λειτουργίες ή διαθέτουν τακτική, λειτουργική ή στρατηγική γνώση [69].

- **Ο τομέας υγειονομικής περίθαλψης και δημόσιας υγείας** προστατεύει όλους τους τομείς της οικονομίας από κινδύνους όπως η τρομοκρατία, οι επιδημίες μολυσματικών ασθενειών και οι φυσικές καταστροφές. Επειδή η πλειοψηφία των περιουσιακών στοιχείων του τομέα είναι ιδιωτικά κατοχυρωμένα και λειτουργούν υπό αυτόνομη διαχείριση, η συνεργασία και η κοινοποίηση πληροφοριών ανάμεσα στον δημόσιο και τον ιδιωτικό τομέα είναι ουσιαστική για την αύξηση της ανθεκτικότητας της ιατροφαρμακευτικής περίθαλψης και της δημόσιας υγείας της κρίσιμης υποδομής της χώρας. Ο τομέας αυτός διαδραματίζει σημαντικό ρόλο στην ανταπόκριση και στην αποκατάσταση όλων των άλλων τομέων σε περίπτωση φυσικής ή ανθρωπογενούς καταστροφής. Ενώ η υγειονομική περίθαλψη συνήθως παρέχεται και διαχειρίζεται τοπικά, η δημόσια υγεία του κλάδου, που επικεντρώνεται κυρίως στη δημόσια υγεία του πληθυσμού, διαχειρίζεται από όλα τα επίπεδα της κυβέρνησης: εθνικό, περιφερειακό και τοπικό. Ο τομέας της υγειονομικής περίθαλψης και δημόσιας υγείας εξαρτάται σε μεγάλο βαθμό από τους συναπτομένους τομείς, για τη συνέχεια των λειτουργιών και την παροχή υπηρεσιών, συμπεριλαμβανομένων των επικοινωνιών, των υπηρεσιών έκτακτης ανάγκης, της ενέργειας, των τροφίμων και της γεωργίας, της τεχνολογίας πληροφοριών, των συστημάτων μεταφοράς και των συστημάτων ύδρευσης και αποχέτευσης [70].
- **Ο τομέας της πληροφορικής** είναι σημαντικός για την ασφάλεια, την οικονομία, τη δημόσια υγεία και ασφάλεια της χώρας καθώς οι επιχειρήσεις, οι κυβερνήσεις, οι ακαδημαϊκοί και οι ιδιώτες πολίτες εξαρτώνται όλο και περισσότερο από τις λειτουργίες του τομέα της πληροφορικής. Αυτές οι εικονικές και καταναμημένες λειτουργίες παράγουν και παρέχουν υλικό, λογισμικό καθώς και συστήματα και υπηρεσίες πληροφορικής ενώ, σε συνεργασία με τον τομέα επικοινωνιών, παρέχουν το διαδίκτυο. Το σύνθετο και δυναμικό περιβάλλον του τομέα καθιστά δύσκολη την αναγνώριση απειλών και την αξιολόγηση των ευπαθειών, και απαιτεί την αντιμετώπιση αυτών των καθηκόντων με συνεργατικό και δημιουργικό τρόπο. Οι λειτουργίες του τομέα της πληροφορικής πραγματοποιούνται από μια συνδυασμένη ομάδα οντοτήτων - συχνά ιδιοκτήτες και χειριστές και οι αντίστοιχοι σύλλογοι τους - που διατηρούν και ανασυγκροτούν το δίκτυο, συμπεριλαμβανομένου του διαδικτύου. Παρότι η υποδομή της πληροφορικής έχει ένα συγκεκριμένο επίπεδο ενσωματωμένης ανθεκτικότητας, η διεπαφή και η διασύνδεσή της με άλλες δομές δημιουργεί προκλήσεις, αλλά και ευκαιρίες για τον συντονισμό δραστηριοτήτων προετοιμασίας και προστασίας τόσο του δημόσιου όσο και του ιδιωτικού τομέα [71].
- **Ο τομέας πυρηνικών αντιδραστήρων, υλικών και αποβλήτων** είναι επίσης ένας από τους δεκαέξι σημαντικούς τομείς που είναι πιθανό να γίνει στόχος ενός κυβερνοπολέμου. Από τους πυρηνικούς αντιδραστήρες που παρέχουν ηλεκτρικό ρεύμα σε εκατομμύρια πολίτες, μέχρι τα ιατρικά ισότοπα που χρησιμοποιούνται για τη θεραπεία ασθενών με καρκίνο, ο τομέας πυρηνικών αντιδραστήρων, υλικών και αποβλήτων καλύπτει σχεδόν ολόκληρη την έκταση της αστικής πυρηνικής υποδομής ενός ανεπτυγμένου κράτους σαν αυτό των Ηνωμένων Πολιτειών. Ο τομέας αυτός ανήκει στο εκάστοτε υπουργείο εθνικής ασφάλειας του κάθε κράτους το οποίο είναι υπεύθυνο για τον συντονισμό της ασφάλειας και της ανθεκτικότητας του τομέα αυτού. Εδώ εντάσσονται ενεργοί πυρηνικοί

αντιδραστήρες είτε ενεργοί είτε αντιδραστήρες που έχουν βγει από λειτουργία για να αποσυρθεθούν αλλά και εγκαταστάσεις καυσίμων πυρηνικής καύσης. Τα ραδιενεργά υλικά έχουν και άλλες χρήσεις εκτός από πυρηνική σχάση και παραγωγή ενέργειας. Χρησιμοποιούνται για ιατρικές διαγνώσεις και θεραπεία σε νοσοκομεία, μετρήσεις βάθους σε σημεία διάτρησης πετρελαίου και φυσικού αερίου, για αποστείρωση σε εγκαταστάσεις παραγωγής τροφίμων, για έρευνα σε ακαδημαϊκά ιδρύματα και για ελέγχους ασφαλείας στα σημεία ελέγχου εμπορευματοκιβωτίων. Αυτός ο τομέας είναι αλληλοεξαρτώμενος και με άλλους σημαντικούς τομείς υποδομών όπως ο χημικός τομέας, ο τομέας επειγουσών υπηρεσιών για την αντιμετώπιση πιθανών πυρηνικών ατυχημάτων, με τον τομέα ενέργειας εφόσον οι πυρηνικοί αντιδραστήρες χρησιμοποιούνται κατά κόρον για την παραγωγή ηλεκτρικής ενέργειας, με τον τομέα υγειονομικής περίθαλψης και δημόσιας υγείας λόγω των ιατρικών χρήσεων των ραδιενεργών υλικών που αναφέρθηκαν πριν, με τον τομέα μεταφορών για την μεταφορά αυτών των ραδιενεργών υλικών σε οποιοδήποτε μέρος παγκοσμίως και με τον τομέα συστημάτων υδάτων και λυμάτων για την χρησιμοποίηση μεγάλων όγκων νερού για την ψύξη των πυρηνικών αντιδραστήρων [72].

- **Ο τομέας συστημάτων μεταφορών** είναι υπεύθυνος για την γρήγορη και ασφαλή μεταφορά τόσο των πολιτών όσο και των εμπορευμάτων εντός και εκτός συνόρων. Την ασφάλεια του τομέα αυτού την εξασφαλίζει και πάλι κάποιος κρατικός φορέας όπως το εκάστοτε υπουργείο εθνικής ασφάλειας κάθε χώρας. Ο τομέας αυτός εμπεριέχει την αεροπλοΐα και κάθε μέσο με το οποίο διενεργείται, τους αυτοκινητόδρομους, την ναυσιπλοΐα και όλα τα ναυτικά μέσα, τους επιβατικούς και οι εμπορικούς σιδηρόδρομους, τα συστήματα αγωγών για την μεταφορά καυσίμων όπως το φυσικό αέριο και τέλος το ταχυδρομικό δίκτυο [73].
- **Ο τομέας συστημάτων υδάτων και λυμάτων** Το ασφαλές πόσιμο νερό είναι προϋπόθεση για την προστασία της δημόσιας υγείας και της ανθρώπινης δραστηριότητας. Η κατάλληλη επεξεργασία λυμάτων είναι ζωτικής σημασίας για την πρόληψη ασθενειών και την προστασία του περιβάλλοντος. Έτσι, η διασφάλιση της προσφοράς πόσιμου νερού και της επεξεργασίας και υπηρεσιών λυμάτων είναι ουσιώδους σημασίας για τη σύγχρονη ζωή και την οικονομία της χώρας. Σε αυτόν τον τομέα ανήκουν τα συστήματα αγωγών υδροδότησης και υδραγωγεία, καθώς και αποχετευτικά συστήματα και συστήματα βιολογικής επεξεργασίας λυμάτων[74].

3.4 Κυβερνοόπλα

Τα κυβερνοόπλα μπορούν να ταξινομηθούν σε τουλάχιστον τρεις κατηγορίες : τα επιθετικά κυβερνοόπλα τα οποία χρησιμοποιούνται μόνο για επιθετικούς λόγους ή για να προκαλέσουν ζημιά, τα αμυντικά κυβερνοόπλα που χρησιμοποιούνται κυρίως για την προστασία από τέτοιου είδους κυβερνοεπιθέσεις και τα κυβερνοόπλα διπλής χρήσης τα οποία μπορούν να χρησιμοποιηθούν τόσο για επιθετικούς σκοπούς όσο και για αμυντικούς σκοπούς. Οι έλεγχοι των κυβερνοεπιθέσεων δεν χρειάζεται να εφαρμόζονται ή να εφαρμόζονται ομοιόμορφα για όλες τις τρεις κατηγορίες. Για παράδειγμα, θα μπορούσαν να εφαρμοστούν κυρίως ή αποκλειστικά σε όπλα μόνο για επιθέσεις που είναι επιζήμια χωρίς να προσφέρουν κανένα φανερό όφελος στα θύματά τους. Παρακάτω θα αναφερθούν ονομαστικά ποιοι ιοί ανήκουν σε κάθε κατηγορία χωρίς να αναλυθούν περεταίρω, αφού οι περισσότεροι έχουν αναλυθεί εκτενώς στο προηγούμενο κεφάλαιο.

3.4.1 Επιθετικά κυβερνοόπλα

Τα επιθετικά κυβερνοόπλα που χρησιμοποιούνται μόνο για επιθέσεις, περιλαμβάνουν κυρίως τα περισσότερα από τα ηλεκτρονικά σκουλήκια, τους ηλεκτρονικούς ιούς, τους δούρειους ίππους, τις βόμβες ηλεκτρονικού ταχυδρομείου, τα εργαλεία επιθέσεων άρνησης εξυπηρέτησης, τα scripts και προγράμματα που αξιοποιούν ή εκμεταλλεύονται ευπάθειες όπως η υπερχειλίση μιας ενδιάμεσης μνήμης (buffer overflow) αποκτώντας έτσι πρόσβαση ο επιτιθέμενος, τα rootkits με λειτουργίες παρόμοιες με αυτές των δούρειων ίπων, κερκόπορτες (backdoors), bots - botnets, και καθαριστές καταγραφών συστήματος (system log cleaners). Παρόλο που οι άνθρωποι έχουν υποθέσει τη δημιουργία ωφέλιμων ιών και στον εικονικό κόσμο, στην πραγματικότητα, ελάχιστοι ή κανένας δεν υπάρχουν, και ακόμη και οι μη κακόβουλοι ιοί θεωρούνται επιζήμιοι από τα θύματά τους.

3.4.2 Αμυντικά κυβερνοόπλα

Τα αμυντικά κυβερνοόπλα περιέχουν κρυπτογράφηση, αυθεντικοποίηση, έλεγχο πρόσβασης, τείχη προστασίας, αντικά λογισμικά, εργαλεία ελέγχου και ανίχνευσης εισβολής. Κάποια από αυτά, κυρίως η κρυπτογράφηση, μπορούν να υποβληθούν σε ελέγχους κατά την εξαγωγή τους από ένα κράτος, καθώς η χρήση τους από ξένες χώρες – αντιπάλους μπορεί να εμποδίσει τα κρατικά εγχειρήματα για την συλλογή πληροφοριών και να θεωρηθεί απειλή για το ίδιο το κράτος. Παρά το γεγονός ότι αυτοί οι περιορισμοί έχουν υποστεί σημαντική απελευθέρωση τα τελευταία χρόνια, παραμένουν ακόμα σταθερά σε ισχύ, ενώ δεν υπάρχουν σχεδόν καθόλου περιορισμοί στη χρήση επιθετικών κυβερνοεπιθέσεων που προκαλούν ζημιές. Το παράδοξο είναι ότι σε αρκετές χώρες, συμπεριλαμβανομένων και των Ηνωμένων Πολιτειών Αμερικής, είναι νόμιμο κάποιος να κατασκευάσει και να αναρτήσει δημόσια στο διαδίκτυο για ελεύθερη λήψη κάποιο κυβερνοόπλο το οποίο, μπορεί να προέρχεται από τρομοκρατικές ομάδες, προκαλώντας έτσι ζημιές στις κρίσιμες υποδομές μιας χώρας, ενώ είναι παράνομο να αναρτηθεί στο διαδίκτυο χωρίς περιορισμούς κάποιο λογισμικό κρυπτογράφησης.

3.4.3 Κυβερνοόπλα διπλής χρήσης

Τα κυβερνοόπλα διπλής χρήσης είναι αυτά που μπορούν να χρησιμοποιηθούν τόσο για να διευκολύνουν μια κυβερνοεπίθεση όσο και για να αμυνθούν κατά μιας επίθεσης. Χαρακτηριστικά παραδείγματα αυτής της κατηγορίας είναι τα “war dialers”, οι ανιχνευτές πακέτων (“sniffers”), αποκωδικοποιητές κωδικών (password crackers), οι σαρωτές θυρών και ευπαθειών και κάθε εργαλείο διαχείρισης και παρακολούθησης δικτύου. Τα war dialers και οι σαρωτές θυρών και ευπαθειών μπορούν να χρησιμοποιηθούν για την εύρεση (και διόρθωση) αδυναμιών στο δίκτυό μας ή για την εύρεση πιθανών στόχων επίθεσης. Τα κακόβουλα λογισμικά που σπάνε κωδικούς πρόσβασης ή αλλιώς οι password crackers μπορούν να χρησιμοποιηθούν για να διακυβέυσουν τους κωδικούς πρόσβασης κάποιου άλλου ή για να καθορίσουν εάν οι δικοί μας κωδικοί είναι επαρκείς. Μπορούν επίσης να χρησιμοποιηθούν για να ανακτήσουν κωδικούς που έχουν χαθεί ή ξεχαστεί. Ομοίως, τα “key crackers” μπορούν να χρησιμοποιηθούν για την μη εξουσιοδοτημένη πρόσβαση σε κρυπτογραφημένα δεδομένα κάποιου άλλου ή για την επαναφορά των δικών μας σε περίπτωση απώλειας ή καταστροφής των κλειδιών. Οι ανιχνευτές πακέτων δικτύου “sniffers” μπορούν να χρησιμοποιηθούν για την παρακολούθηση της απόδοσης του δικτύου και την ανίχνευση πιθανών εισβολών ή για τη συλλογή ονομάτων χρηστών και κωδικών πρόσβασης για

μελλοντική εκμετάλλευση. Τα εργαλεία διαχείρισης και παρακολούθησης δικτύου μπορούν να χρησιμοποιηθούν για τη διαχείριση του δικού μας δικτύου ή για να αποκτήσουν τον έλεγχο του υπολογιστή του θύματος και να κλέψουν ευαίσθητες πληροφορίες από αυτόν.

Σε ορισμένες περιπτώσεις, είναι δυνατό να διακρίνουμε διπλής χρήσης κυβερνοόπλα που χρησιμοποιούνται κυρίως για άμυνα από εκείνα που χρησιμοποιούνται για τη εξαπόλυση μιας κυβερνοεπίθεσης. Για παράδειγμα, ένα sniffer κωδικών πρόσβασης που σχεδιάστηκε αποκλειστικά για να κλέβει ονόματα χρηστών και κωδικούς πρόσβασης δεν έχει κανένα ρόλο στην άμυνα, ενώ ένα sniffer που χρησιμοποιείται για τον εντοπισμό διεισδύσεων έχει. Σε αυτήν την περίπτωση, το sniffer κωδικών πρόσβασης θα μπορούσε να θεωρηθεί ως επιθετικό όπλο. Η διάκριση ανάμεσα σε ωφέλιμα και επιβλαβή κυβερνοόπλα μπορεί να είναι δύσκολη σε μερικές περιπτώσεις. Για παράδειγμα, ένα εργαλείο άρνησης εξυπηρέτησης που πλημμυρίζει έναν στόχο με μηνύματα μπορεί να είναι χρήσιμο για τη δοκιμή της χωρητικότητας ενός δικτύου, προκειμένου να προσδιοριστούν οι τομείς όπου απαιτούνται επιπλέον πόροι. Ακόμη και αμυντικά όπλα όπως η κρυπτογράφηση μπορούν να χρησιμοποιηθούν από αντιπάλους για τη διευκόλυνση εγκληματικών δραστηριοτήτων. Τέλος, η διάκριση ανάμεσα στα καλά και στα κακά επίσης μπορεί να είναι αμφιλεγόμενη. Για παράδειγμα, ορισμένα εργαλεία διαχείρισης και παρακολούθησης δικτύου είναι φτιαγμένα από αναγνωρισμένες εταιρείες, ενώ άλλα προέρχονται από την κοινότητα του hacking. Σε απάντηση στη ζήτηση των πελατών, η βιομηχανία κατά των ηλεκτρονικών ιών συνήθως θα ελέγξει για εκείνα τα κακόβουλα λογισμικά που ανήκουν στη δεύτερη κατηγορία αλλά όχι για τα λογισμικά που δεν έχουν κακόβουλο σκοπό και τα οποία ανήκουν στην πρώτη. Αυτό έχει οδηγήσει σε παράπονα ότι η βιομηχανία κατά των ηλεκτρονικών ιών υποστηρίζει τις μεγάλες εταιρείες εις βάρος των μικρών. Εάν αυτού του είδους τα εργαλεία ελεγχόντουσαν, μια εναλλακτική προσέγγιση θα μπορούσε να είναι για ένα ανεξάρτητο όργανο να αποφασίζει ποια εργαλεία θα τοποθετηθούν στη λίστα ελεγχόμενων, με δυνατότητα έφεσης. Οι παραγωγοί των αντιικών προϊόντων θα μπορούσαν να ενθαρρυνθούν ή να υποχρεωθούν να ακολουθούν αυτήν τη λίστα [75].

3.5 Επιπτώσεις ενός κυβερνοπολέμου

Υπάρχουν πολλές επιπτώσεις που μπορεί να έχει ένας κυβερνοπόλεμος μέσω κυβερνοεπιθέσεων σε επιχειρήσεις όλων των μεγεθών ακόμα και στην ίδια την κοινωνία. Ας αναφερθούν αρχικά οι επιπτώσεις σε επιχειρήσεις :

1. **Οικονομικές απώλειες.** Σύμφωνα με εκτιμήσεις που έγιναν για το 2021, το κυβερνοεγκλημα όλων των τύπων και οι κυβερνοεπιθέσεις θα προκαλούσαν οικονομική ζημιά της τάξης 6 τρισεκατομμυρίων δολαρίων Ηνωμένων Πολιτειών, κάτι που αν μετρηθεί αυτό το ποσό ως ποσό κρατικών οικονομιών, τότε θα μπορούσε να είναι η τρίτη μεγαλύτερη οικονομία παγκοσμίως μετά την οικονομία των Ηνωμένων Πολιτειών και της Κίνας. Το επιστημονικό περιοδικό Cybersecurity Ventures, το οποίο ηγείται της έρευνας και ενημέρωσης για την παγκόσμια κυβερνοοικονομία, το οποίο είναι μια πολύ αξιόπιστη πηγή πληροφοριών για τα γεγονότα, τα νούμερα και τα στατιστικά της κυβερνοασφάλειας, αναφέρει ότι, αναμένεται το παγκόσμιο κόστος του κυβερνοεγκλήματος να αυξηθεί κατά 15% ετησίως τα επόμενα χρόνια, φτάνοντας 10,5 τρισεκατομμύρια δολάρια ετησίως το 2025 από 3 δισεκατομμύρια δολάρια που ήταν το 2015. Αυτό αντιπροσωπεύει τη μεγαλύτερη μεταφορά οικονομικού πλούτου στην ιστορία, απειλεί τα κίνητρα για καινοτομία και επένδυση, είναι εκθετικά μεγαλύτερο από τη ζημιά που προκαλείται

από φυσικές καταστροφές κατά μέσο όρο ετησίως και θα είναι πιο κερδοφόρο από τον παγκόσμιο εμπόριο όλων των κυριότερων παράνομων ναρκωτικών μαζί. Η εκτίμηση του κόστους ζημιάς βασίζεται σε ιστορικά στοιχεία κυβερνοεγκληματικότητας, συμπεριλαμβανομένης της πρόσφατης αύξησης ετήσιας ανάπτυξης, μιας δραματικής αύξησης στις εχθρικές δραστηριότητες των hackers που χρηματοδοτούνται από κράτη και οργανωμένες εγκληματικές ομάδες, καθώς και επιθέσεις κυβερνοχώρου που θα είναι μεγαλύτερου μεγέθους το 2025. Το κόστος του κυβερνοεγκλήματος περιλαμβάνει τη ζημία και καταστροφή δεδομένων, κλοπή χρημάτων, απώλεια παραγωγικότητας, κλοπή πνευματικής ιδιοκτησίας, κλοπή προσωπικών και οικονομικών δεδομένων, εξαπάτηση, απάτη, μετα-επιθετική αναταραχή της κανονικής εξέλιξης της επιχείρησης, εγκληματολογική διερεύνηση, αποκατάσταση και διαγραφή κλαπείσας πληροφορίας και συστημάτων, καθώς και βλάβη στο κύρος της επιχείρησης [76].

2. **Ζημιά στο κύρος και στην φήμη μιας επιχείρησης.** Η εμπιστοσύνη αποτελεί ένα ουσιαστικό στοιχείο της σχέσης μιας επιχείρησης με τους πελάτες της. Οι κυβερνοεπιθέσεις μπορούν να βλάψουν το κύρος μιας επιχείρησής και να υπονομεύσουν την εμπιστοσύνη που έχουν οι πελάτες για την επιχείρηση αυτή. Αυτό με τη σειρά του, μπορεί δυνητικά να οδηγήσει σε απώλεια πελατών και σε μειώσεις πωλήσεων και κερδών. Η επίδραση της ζημιάς της φήμης μπορεί ακόμα και να επηρεάσει τους προμηθευτές με τους οποίους συνεργάζεται μια επιχείρηση, ή να επηρεάσει τις σχέσεις που μπορεί να έχει με εταίρους, επενδυτές, και άλλα τρίτα μέρη που έχουν επενδυτικό ενδιαφέρον για την επιχείρησή [77].
3. **Νομικές και ρυθμιστικές συνέπειες.** Οι κυβερνοεπιθέσεις είναι μια πολύ σημαντική απειλή για την επιβίωση των επιχειρήσεων. Μια κυβερνοεπίθεση σε μια επιχείρηση που αποκαλύπτει προσωπικά ή εμπιστευτικά δεδομένα μπορεί να έχει αρκετές δυσάρεστες συνέπειες για την επιχείρησή αυτή, συμπεριλαμβανομένων εκτός από όλες αυτές τις συνέπειες που προαναφέρθηκαν, και χρηματικές απαιτήσεις που υποβάλλονται από πελάτες μιας επιχείρησης όπως για παράδειγμα, όταν μια επιχείρηση δεν έχει συμμορφωθεί με την πολιτική απορρήτου της. Επίσης, στις νομικές συνέπειες εντάσσονται οι χρηματικές απαιτήσεις για παραβίαση συμβολαίου εάν δεν εφαρμόζει μια επιχείρηση τις συμβατικές τους υποχρεώσεις για συμμόρφωση με την νομοθεσία περί προστασίας δεδομένων και πρόστιμα από τους αρμόδιους φορείς για μη συμμόρφωση με τον γενικό κανόνα προστασίας δεδομένων GDPR. Οι νέες και μικρότερες εταιρείες και επιχειρήσεις συχνά θεωρούνται στόχοι από κυβερνοεγκληματίες επειδή δεν διαθέτουν τους απαραίτητους πόρους πληροφορικής και τη νομική εμπειρογνωμοσύνη μεγαλύτερων επιχειρήσεων [78].
4. **Διακοπές στην λειτουργία τους.** Αναφορές για περιστατικά κυβερνοασφάλειας σε όλο τον κόσμο συχνά τονίζουν τις οικονομικές απώλειες και τη διαταραχή της λειτουργίας της επιχείρησης ως τον κύριο αντίκτυπο των κυβερνοεπιθέσεων. Οι τελευταίες εξελίξεις στον κυβερνοεγκληματικό κόσμο, ωστόσο, υπογραμμίζουν ότι ο λειτουργικός αντίκτυπος (operational disruption) μπορεί να είναι πολύ πιο σημαντικός από τις οικονομικές απώλειες (financial losses). Μια έρευνα από την KPMG και την Oracle έδειξε ότι δύο στους τρεις (66%) από τους ερωτηθέντες είχαν βιώσει ένα περιστατικό κυβερνοασφάλειας που επηρέασε τις επιχειρηματικές τους λειτουργίες τα τελευταία χρόνια. Αυτά τα αποτελέσματα περιλαμβάνουν διακοπές των τυπικών επιχειρηματικών λειτουργιών, διακοπές στη δυνατότητα παροχής υπηρεσιών, απώλεια παραγωγικότητας των υπαλλήλων και καθυστερήσεις σε έργα πληροφορικής (τα οποία μπορεί να επηρεάσουν τα μελλοντικά σχέδια και λειτουργίες

της εταιρείας). Ο λειτουργικός αντίκτυπος των κυβερνοεπιθέσεων (όπως οι επιθέσεις με ransomware) εκδηλώνεται σε τέτοιες ανησυχητικές καταστάσεις που επηρέασαν όχι μόνο την τεχνολογία, αλλά ακόμα και τους ανθρώπους (για παράδειγμα, οι οργανισμοί υγείας που είχαν μολυνθεί με κακόβουλο λογισμικό δεν μπορούσαν να παρέχουν άμεσα και κατάλληλη φροντίδα στους ασθενείς) [79].

5. **Παραβιάσεις δεδομένων.** Όπως αναφέρθηκε στην ζημιά του κύρους μιας επιχείρησης αλλά και στις νομικές συνέπειες, μια επιπλέον συνέπεια κυβερνοεπιθέσεων σε μια επιχείρηση είναι η παραβίαση δεδομένων (data breach). Σύμφωνα με την εταιρεία Malwarebytes, το 2018 ήταν η χρονιά στην οποία πραγματοποιήθηκαν οι περισσότερες παραβιάσεις δεδομένων. Η λίστα των εταιρειών που δέχτηκαν επίθεση από κυβερνοεγκληματίες εκλαμβάνεται σαν λίστα των μεγαλύτερων τεχνολογικών εταιρειών, καταστημάτων λιανικής και παρόχων φιλοξενίας παγκοσμίως και αυτό είναι μόνο το μέρος των διαρροών δεδομένων που έγιναν γνωστά. Σε πολλές περιπτώσεις, ένας οργανισμός ή μια εταιρεία δεν θα γνωρίζει καν ότι έχει υποστεί παραβίαση μέχρι χρόνια αργότερα. Σύμφωνα με τη μελέτη του Ινστιτούτου Ponemon για το Κόστος Ενός Παραβιασμού Δεδομένων του 2018, η παραβίαση δεδομένων παραμένει για μέσο όρο 197 ημέρες χωρίς να γίνει αντιληπτή και χρειάζεται επιπλέον 69 μέρες για την αντιμετώπισή της. Μέχρι να ανακαλυφθεί η αστοχία στην ασφάλεια και να διορθωθεί, η ζημιά έχει ήδη γίνει. Οι κυβερνοεγκληματίες που ευθύνονται για αυτό, θα έχουν επιτύχει ανεμπόδιστη πρόσβαση σε βάσεις δεδομένων που περιέχουν πολύτιμα δεδομένα εκατομμυρίων ατόμων, που είχαν την ατυχία να συνεργαστούν επιχειρηματικά και εμπορικά με εταιρείες που έπεσαν θύμα κυβερνοεπιθέσεων [80].

Για την κοινωνία οι επιπτώσεις είναι οι εξής :

1. **Ζημιές σε σημαντικές υποδομές μιας κοινωνίας.** Όπως αναφέραμε και σε προηγούμενο κεφάλαιο για τους πιθανούς στόχους ενός κυβερνοπολέμου και σύμφωνα με τον Οργανισμό Κυβερνοασφάλειας και Ασφάλειας Υποδομών των Η.Π.Α. (Cybersecurity & Infrastructure Security Agency), οι κρίσιμες υποδομές μιας χώρας μπορούν να υποστούν ζημιές στα συστήματα πληροφορικής που διαθέτουν. Αυτό έχει ως αποτέλεσμα την δυσλειτουργία των κρίσιμων αυτών υποδομών έχοντας και σημαντικό αντίκτυπο στην κοινωνία. Για παράδειγμα, αν ένα νοσοκομείο, το οποίο είναι μια από τις κρίσιμες υποδομές, δεχθεί μια κυβερνοεπίθεση τότε, θα αντιμετωπίσει δυσκολίες στην λειτουργία του και κατ' επέκταση στην εξυπηρέτηση των ασθενών που είναι μέρος της κοινωνίας [58].
2. **Κίνδυνοι στην δημόσια ασφάλεια.** Ο αριθμός των κυβερνοεπιθέσεων αυξάνεται εκθετικά κάθε χρόνο, με την αύξηση των εφαρμογών σε κινητά τηλέφωνα, των πλατφόρμων κοινωνικών μέσων και άλλων τεχνολογιών να λειτουργούν ως καταλύτης. Αυτή η τάση εμφανίζεται σε όλους τους τομείς, αλλά ένας τομέας ιδιαίτερης ανησυχίας είναι η δημόσια ασφάλεια. Ο αυξανόμενος αριθμός κυβερνοεπιθέσεων σε αρχές αποτελεί μια επικίνδυνη τάση με πραγματικές επιπτώσεις όχι μόνο για την προστασία της ιδιωτικότητας των πολιτών αλλά και για τη διαφύλαξη των κρίσιμων υποδομών. Για να προετοιμαστούν οι υπηρεσίες δημόσιας ασφαλείας για τις κυβερνοεπιθέσεις, είναι σημαντικό να κατανοούν τους τύπους των επιθέσεων και τις επιπτώσεις τους σε ευρύτερο επίπεδο. Μέχρι πρόσφατα, ο βασικός κίνδυνος αποτελούσε η κλοπή προσωπικών πληροφοριών από τους κυβερνοεγκληματίες. Αυτές οι επιθέσεις βάζουν σε κίνδυνο τα

ευαίσθητα δεδομένα μιας αρχής, όπως οι εγκληματικοί φάκελοι σε ένα αστυνομικό τμήμα. Ωστόσο, αυτή δεν είναι πλέον η μόνη απειλή. Ο κυβερνοακτιβισμός (cyberhacktivism) είναι μια αναδυόμενη τάση που δεν εκτελείται απαραίτητα για να κλαπεί πληροφορία, αλλά για να προωθηθεί μια πολιτική ατζέντα μέσω κυβερνοεπίθεσης. Δυστυχώς, οι αστυνομικές και άλλες κρίσιμες υπηρεσίες ασφαλείας συχνά βρίσκονται στόχο αυτών των ενεργειών. Η κυβερνοτρομοκρατία και ο κυβερνοπόλεμος αυξάνονται επίσης σημαντικά, καθώς οι επιπτώσεις τους υπερβαίνουν την παραβίαση ευαίσθητων δεδομένων και μπορεί να προκαλέσουν την «παράλυση» μιας κοινότητας ή ακόμη και μιας ολόκληρης περιοχής. Για παράδειγμα, εάν στοχευθεί κρίσιμη υποδομή, όπως μια δημόσια υπηρεσία, μπορεί να αναγκαστεί να κλείσει το δίκτυό της. Οι αρχές πρέπει να είναι προετοιμασμένες να αντιμετωπίσουν την πραγματικότητα της έλλειψης πρόσβασης στα συστήματα αλλά να παραμένουν σε ετοιμότητα να ανταποκριθούν στις φυσικές επιπτώσεις της κυβερνοεπίθεσης, καθώς και στις καθημερινές ανάγκες, όπως ιατρικές επείγουσες καταστάσεις. Τέλος, μια περιοχή που συχνά παραβλέπεται είναι η επίδραση της φυσικής ασφάλειας στις κυβερνοαπειλές. Εργαζόμενοι με ελλιπή εκπαίδευση ή μη εξουσιοδοτημένοι εισβολείς μπορούν να προκαλέσουν χάος στο δίκτυο μιας υπηρεσίας με ένα άκαρπο flash drive ή μια σειρά άλλων δυνητικών παραβιάσεων [81].

3. **Κοινωνικές ταραχές.** Οι κρίσιμες υποδομές μιας χώρας – κοινωνίας είναι πολύ σημαντικές για την ανθρώπινη ευημερία και χωρίζονται στις κατηγορίες που αναφέρθηκαν πριν. Η δυσλειτουργία των κρίσιμων αυτών υποδομών μπορεί να προκληθεί από αστοχίες του διαδικτύου, αν η λειτουργία της υποδομής είναι άμεσα συνδεδεμένη με εντολές που μεταφέρονται από υπηρεσίες πληροφορικής. Τέτοιες άμεσες επιπτώσεις στη λειτουργικότητα της υποδομής μπορεί να οφείλονται σε τεχνικές αποτυχίες, σε σφάλματα των χειριστών ή σε κακόβουλες ενέργειες, όπως η σαμποτάζ και η τρομοκρατία. Οι περισσότερες ευαίσθητες υποδομές έχουν επαρκή συστήματα για εφεδρικές υπηρεσίες εισαγωγής και προστασίας και είναι σε ετοιμότητα για την δρομολόγηση μιας πιθανής έκτακτης ανάγκης. Παρ' όλα αυτά υπάρχουν πολλά παραδείγματα τεχνικών αλλά και ανθρώπινων αποτυχιών που έχουν οδηγήσει σε μερική ή ολική αποτυχία των κρίσιμων υποδομών, έχοντας ως αποτέλεσμα την διαταραχή της κάλυψης των βασικών ανθρώπινων αναγκών. Συνεπώς, η κοινωνική αναταραχή είναι πιο πιθανή να προκληθεί όταν οι αστοχίες της πληροφορικής συνοδεύουν προβλήματα υποδομών παρά όταν τα προκαλούν. Εάν η πληροφορική και οι υπολογιστές είναι αιτία μιας διακοπής υπηρεσίας, η κοινωνική αναταραχή θα είναι πιθανότατα στραμμένη κατά της έλλειψης της υπηρεσίας και των εκπροσώπων της οργάνωσης. Ωστόσο, εάν μια αστοχία της πληροφορικής επιδεινώνει μια δεδομένη καταστροφή, για παράδειγμα αποκλείοντας όλα τα μέσα επικοινωνίας, η αναταραχή μπορεί να στραφεί κατά των παρόχων των υπηρεσιών επικοινωνίας και όσων πιστεύουν ότι εκπροσωπούν αυτές τις υπηρεσίες. Καθώς πρόκειται για υποθετικά γεγονότα, μπορούμε μόνο να υποθέσουμε ότι πολλοί θα εκφράσουν τη δυσαρέσκειά τους για μια κατάσταση αποτυχίας της τεχνολογίας χωρίς να παρέχουν προτάσεις για τη βελτίωση της κατάστασης. Η δυσαρέσκεια θα είναι σίγουρα παρούσα σε αυτήν την περίπτωση, αλλά θα είναι διασπαρμένη και όχι καλά οργανωμένη. Η δυσαρέσκεια μπορεί να εμφανιστεί σε περιπτώσεις όπου οι άνθρωποι αντιμετωπίζουν σοβαρές ζημιές, όπως η απώλεια συγγενικών ή φίλων ή όταν οι άνθρωποι δεν είναι

ικανοποιημένοι με τη διαχείριση κινδύνων. Αυτό μπορεί να συμβεί εάν οι άνθρωποι δεν υποστηρίζονται για μεγάλο χρονικό διάστημα με νερό, ενέργεια, τρόφιμα και άλλα αγαθά που είναι αναγκαία για τη ζωή. Σημαντική στις περιπτώσεις αυτές είναι επίσης η υπόθεση, ότι οι άνθρωποι πιστεύουν ότι οι αρχές διαχείρισης κινδύνου είναι ανίκανες και δεν είναι προετοιμασμένες να τους βοηθήσουν να βελτιώσουν την κατάστασή τους. Εάν αυτό δεν είναι περιστατικό αναταραχής, μπορεί να συμβεί αποσταθεροποίηση νωρίτερα ή σε περιπτώσεις όπου η βοήθεια δεν δίνεται πλήρως ή δίνεται μόνο σε λίγους, υπάρχει η κατηγορία για αδικία. Ένας άλλος σημαντικός παράγοντας είναι η κάλυψη των μέσων ενημέρωσης. Πληροφορίες που μεταδίδονται και αποδεικνύονται ότι δεν είναι αληθείς καταστρέφουν την εμπιστοσύνη και μπορεί να εξυπηρετήσουν ως καταλύτης για κοινωνική αναταραχή, όπως συνέβη κατά τη διάρκεια του τυφώνα Katrina. Τέλος, συμπεραίνουμε ότι τα αποτελέσματα αναταραχής σε περιπτώσεις κινδύνου που σχετίζονται με τον κυβερνοχώρο, είναι παρόμοια με τα αποτελέσματα άλλων κινδύνων ή διαταραχών που έχουν τη δυνατότητα να προκαλέσουν κοινωνική αναταραχή. Επομένως, μπορεί να μην είναι το πρόβλημα που σχετίζεται με την κυβερνοασφάλεια αυτό που θα οδηγήσει άμεσα σε κοινωνική αναταραχή αλλά οι μεταβλητές περιβάλλοντος στις οποίες μπορεί να ενταχθούν οι κυβερνοεπιθέσεις. Το κυβερνοπρόβλημα είναι πιθανό να λειτουργήσει ως προωθητής της σύγκρουσης που θα ενισχύσει την έντασή της [82].

4. **Οικονομική ζημιά.** Όπως αναφέραμε ήδη για τις οικονομικές απώλειες των επιχειρήσεων ως αποτέλεσμα των κυβερνοεπιθέσεων, αυτό έχει επίπτωση τόσο για την εγχώρια οικονομία όσο και για την παγκόσμια. Ήδη αναφέρθηκε ότι η οικονομική ζημιά που θα προκαλεί το κυβερνοέγκλημα ετησίως μέχρι το 2025 θα αγγίζει το ποσό των 10,5 τρισεκατομμυρίων δολαρίων, ποσό που είναι μεγαλύτερο από τις οικονομίες των κρατών εκτός των Η.Π.Α. και της Κίνας [76].
5. **Παγκόσμιες εντάσεις.** Για να γίνει περισσότερο κατανοητή αυτή η επίπτωση στην κοινωνία είναι συνετό να αναφερθεί η περίπτωση Ουκρανίας – Ρωσίας. Έναν χρόνο μετά την εισβολή της Ρωσίας στην Ουκρανία, το γεωπολιτικό πλαίσιο γίνεται όλο και πιο ταραγμένο και ασταθές. Ο κόσμος αντιμετωπίζει αρκετές σοβαρές κρίσεις σε αυτό που έχει χαρακτηριστεί ως «πολυ-κρίση», ένα συνδυασμό παγκόσμιων σοκ με επιβαρυντικές επιδράσεις. Η άθλια παγκόσμια οικονομική προοπτική σε συνδυασμό με την αύξηση του πληθωρισμού, της αναταραχής της αλυσίδας εφοδιασμού, των ενεργειακών σοκ, των ακραίων καιρικών φαινομένων και της γεωπολιτικής αστάθειας αυξάνει τον κίνδυνο πιθανών διακυμάνσεων στις κυβερνοεπιθέσεις. Οι γεωπολιτικές εντάσεις αυξάνουν τον κίνδυνο στον κυβερνοχώρο, ενώ οι κυβερνοεπιθέσεις επιδεινώνουν τις γεωπολιτικές δυναμικές. Ένα χαρακτηριστικό παράδειγμα αυτού του είδους επιπτώσεων είναι η κυβερνοεπίθεση που δέχθηκε ο πάροχος δορυφορικών επικοινωνιών Viasat τον Φεβρουάριο του 2022, προκαλώντας διακοπές σε ολόκληρη την Ευρώπη λίγες ώρες πριν η Ρωσία ξεκινήσει την εισβολή της στην Ουκρανία. Παρόλο που Ουκρανικός στρατός ήταν ο κύριος στόχος, η επίθεση επηρέασε επίσης τις υπηρεσίες internet για δεκάδες χιλιάδες πολίτες στην Ευρώπη και αποσυνδέθηκε η απομακρυσμένη πρόσβαση σε περίπου 5.800 ανεμογεννήτριες σε ολόκληρη τη Γερμανία. Την άνοιξη του 2022, η αρχή κυβερνοασφάλειας των Ηνωμένων Πολιτειών και άλλοι σύμμαχοι εξέδωσαν κοινό Συμβουλευτικό Επισήμανσης Κυβερνοασφάλειας που προειδοποιούσε ότι

κυβερνοεγκληματίες που συνδέονται με τη Μόσχα είχαν σχεδιάσει κυβερνοεπιθέσεις εναντίον κρίσιμων υποδομών. Λαμβάνοντας υπόψη την πιθανότητα ενός μακροχρόνιου πολέμου και μιας ανανεωμένης ρωσικής επίθεσης, αναμένονται κακόβουλες κυβερνοεπιθέσεις ως μέρος μιας συντονισμένης υβριδικής πολεμικής προσπάθειας [83].

3.6 Περιπτώσεις διεξαγωγής κυβερνοπολέμου

Αν και ο κυβερνοπόλεμος σαν μέθοδος διεξαγωγής πολέμου άρχισε να χρησιμοποιείται πρόσφατα, κυρίως στα τέλη της δεκαετίας του 1990 με αρχές του 2000, υπάρχουν πολλές περιπτώσεις που πρέπει να αναφερθούν. Παρακάτω θα γίνει περιγραφή στις πιο σημαντικές περιπτώσεις, αλλά και στην μέχρι πρόσφατη περίπτωση του πολέμου της Ρωσίας με την Ουκρανία, που εκτός από χερσαίες επιχειρήσεις, υπήρξαν και πολλές κυβερνοεπιθέσεις.

3.6.1 Η περίπτωση της Εσθονίας

Το 2007, η Εσθονία δέχθηκε, από αγνώστου ταυτότητας επιτιθέμενο, σκληρή και με διάρκεια κυβερνοεπίθεση επηρεάζοντας τις δημόσιες υπηρεσίες, τα μέσα ενημέρωσης και ιδιωτικούς φορείς και τις τράπεζες της χώρας. Παρόλο που δεν υπήρξαν ανθρώπινες απώλειες και δεν χύθηκε αίμα όπως στον συμβατικό πόλεμο, η κυβερνοεπίθεση που διεξήχθη ήταν σκληρή και μεγάλης κλίμακας, αποδεικνύοντας σε όλους ότι μια χώρα μπορεί να παραλύσει εντελώς, δεχόμενη μόνο επιθέσεις στον κυβερνοχώρο και το διαδίκτυο. Αργότερα, έγινε γνωστό ότι αυτή την κυβερνοεπίθεση την είχε εξαπολύσει η Ρωσία σε βάρος της Εσθονίας [84].

Το είδος της κυβερνοεπίθεσης που δέχθηκε η Εσθονία ήταν καταναεμημένη επίθεση άρνησης εξυπηρέτησης (DDoS attack). Μαζικά κύματα ανεπιθύμητων μηνυμάτων στάλθηκαν από botnets και τεράστιες ποσότητες αυτοματοποιημένων διαδικτυακών αιτημάτων πλημμύρισαν τους διακομιστές. Το αποτέλεσμα για τους Εσθονούς πολίτες ήταν ότι οι τραπεζικοί μηχανισμοί (ATM) και οι ηλεκτρονικές τραπεζικές υπηρεσίες στο διαδίκτυο ήταν εντελώς εκτός λειτουργίας ή ανέτοιμες να λειτουργήσουν, οι υπάλληλοι της κυβέρνησης δεν μπορούσαν να επικοινωνήσουν μεταξύ τους μέσω email, και οι εφημερίδες και οι ραδιοτηλεοπτικοί σταθμοί αντιμετώπισαν ξαφνικά πρόβλημα στην μετάδοση ειδήσεων [85]. Αμέσως μετά την επίθεση το NATO έστειλε ειδικούς σε θέματα κυβερνοασφάλειας για να βοηθήσουν την Εσθονία να αναδιοργανώσει την κυβερνοάμυνά της. Αφορμή για αυτήν την κυβερνοεπίθεση στάθηκε η καθαίρεση ενός σοβιετικού μνημείου από το κέντρο της πρωτεύουσας, τη Ταλίν. Για αυτόν τον λόγο όλες οι υποψίες έπεσαν στην Ρωσία, αν και η ίδια αρνήθηκε την εμπλοκή της σε αυτό το γεγονός.

Αρκετοί έχουν την άποψη ότι, αυτή η κυβερνοεπίθεση ήταν κομβικής σημασίας για τον κυβερνοπόλεμο, καθώς πέρασε από την θεωρία και όλα τα υποθετικά σενάρια στην πράξη. Άλλοι πάλι, όπως ο Αντρέους Παντάρ, δεν ενστερνίζονται αυτή την άποψη, αφού όπως λέει και ο ίδιος «Συχνά αναφέρεται ως ένας κυβερνοπόλεμος εναντίον της Εσθονίας αλλά τώρα αναγνωρίζουμε ότι πρόκειται περισσότερο για έναν οργανωμένο διαδικτυακό χουλιγκανισμό.» [86].

3.6.2 Η περίπτωση της Γεωργίας

Λίγες εβδομάδες πριν ξεκινήσει ο πόλεμος μεταξύ Γεωργίας και Ρωσίας, άρχισαν να γίνονται αντιληπτές κυβερνοεπιθέσεις εναντίον της Γεωργίας. Ο Jose Nazario της Arbor Networks στο Λέξινγκτον παρατήρησε μια ροή δεδομένων που κατευθυνόταν προς

ιστότοπους της γεωργιανής κυβέρνησης και περιείχε το μήνυμα: "win+love+in+Rusia". Άλλοι ειδικοί του διαδικτύου στις Ηνωμένες Πολιτείες ανέφεραν ότι οι επιθέσεις κατά της διαδικτυακής υποδομής της Γεωργίας ξεκίνησαν από τις 20 Ιουλίου, με συντονισμένες επιθέσεις εκατομμυρίων αιτημάτων - γνωστές ως καταναεμημένες επιθέσεις άρνησης εξυπηρέτησης (Distributed Denial of Service, ή DDoS.) - που υπερφόρτωσαν και έθεσαν εκτός λειτουργίας τους διακομιστές της Γεωργίας. Οι ερευνητές του Shadowserver, μιας εθελοντικής ομάδας που παρακολουθεί κακόβουλες δραστηριότητες στο δίκτυο, ανέφεραν ότι η ιστοσελίδα του προέδρου της Γεωργίας, Μιχαήλ Σαakasβίλι, έχει καταστεί μη λειτουργική για 24 ώρες λόγω πολλαπλών επιθέσεων DDoS. Ανέφεραν ότι ο διακομιστής διοίκησης και ελέγχου που κατευθύνει την επίθεση είχε βάση στις Ηνωμένες Πολιτείες και είχε ενεργοποιηθεί αρκετές εβδομάδες πριν από την έναρξη της επίθεσης.

Όπως αποδείχθηκε, η επίθεση του Ιουλίου μπορεί να ήταν μια πρόβα για μια πλήρη διεξαγωγή κυβερνοπολέμου όταν ξεκίνησαν οι συγκρούσεις μεταξύ Γεωργίας και Ρωσίας. Σύμφωνα με τεχνικούς εμπειρογνώμονες του διαδικτύου, ήταν η πρώτη φορά που μια γνωστή κυβερνοεπίθεση συνέπεσε με μια πολεμική σύγκρουση. Ωστόσο, όπως δήλωσε ο Bill Woodcock, ο ερευνητικός διευθυντής του Packet Clearing House, μια μη κερδοσκοπική οργάνωση που παρακολουθεί την κίνηση του διαδικτύου, πιθανότατα δεν θα είναι η τελευταία φορά που θα αντιμετωπίσει τέτοιου είδους κυβερνοεπιθέσεις, αφού είναι τόσο φθηνές και εύκολες να πραγματοποιηθούν, με λίγα αποτυπώματα, που σχεδόν σίγουρα θα παραμείνουν χαρακτηριστικό του σύγχρονου πολέμου. Επίσης, ο κ. Woodcock συμπλήρωσε ότι, κοστίζει 4 λεπτά (cents) ανά μηχανή και ότι μπορεί χρηματοδοτηθεί ολόκληρη εκστρατεία κυβερνοπολέμου με το κόστος μιας αντικατάστασης μιας χαλασμένης αλυσίδας τεθωρακισμένου, οπότε θα ήταν ανόητος κάποιος εάν δεν το έκανε.

Ωστόσο, αξίζει να σημειωθεί ότι και σε αυτή την περίπτωση δεν είναι ξεκάθαρο για το ποιός οφείλεται για αυτές τις κυβερνοεπιθέσεις. Η κυβέρνηση της Γεωργίας κατηγορήσε τη Ρωσία για τις επιθέσεις, αλλά η ρωσική κυβέρνηση δήλωσε ότι δεν είχε σχέση με αυτές. Τελικά, η Γεωργία, με μόλις 4,6 εκατομμύρια κατοίκους και ως ένας σχετικά καινούργιος παίκτης στο διαδίκτυο, δεν επηρεάστηκε σημαντικά πέρα από την αδυναμία πρόσβασης σε πολλούς κυβερνητικούς ιστότοπους της, τα οποία περιόρισαν την ικανότητα της κυβέρνησης να διαδίδει το μήνυμά της στο διαδίκτυο και να συνδεθεί με υποστηρικτές της παγκοσμίως κατά τη διάρκεια των συγκρούσεων με τη Ρωσία. Η Γεωργία, σύμφωνα με ερευνητές ασφαλείας, δέχθηκε κυβερνοεπιθέσεις επίσης, σε εταιρείες μέσω ενημέρωσης, επικοινωνιών και μεταφορών. Η Shadowserver παρατήρησε ότι η επίθεση κατά της Γεωργίας εξαπλώθηκε σε υπολογιστές σε ολόκληρη την κυβέρνηση μετά την είσοδο των ρωσικών στρατευμάτων στην επαρχία της Νότιας Οσετίας. Η ιστοσελίδα της Εθνικής Τράπεζας της Γεωργίας υπέστη επίθεση με αποτέλεσμα να παραβιαστεί. Εικόνες δικτατόρων του 20ου αιώνα, καθώς και μια εικόνα του προέδρου της Γεωργίας, κ. Σαakasβίλι, τοποθετήθηκαν στην ιστοσελίδα.

Επιπλέον, εκτός από τις επιθέσεις DDoS. που απείλησαν την περιορισμένη υποδομή του διαδικτύου της Γεωργίας, οι ερευνητές είπαν ότι υπήρχαν αποδείξεις ανακατεύθυνσης της κυκλοφορίας του Διαδικτύου μέσω ρωσικών τηλεπικοινωνιακών εταιρειών από το προηγούμενο Σαββατοκύριακο. Οι επιθέσεις συνεχίστηκαν την Τρίτη, ελεγχόμενες από προγράμματα λογισμικού που βρίσκονταν σε κέντρα εξυπηρέτησης (hosts centers) που ελέγχονταν από ρωσικές τηλεπικοινωνιακές εταιρείες. Ένας ιστότοπος στα ρωσικά, stor.georgia.ru, συνέχισε επίσης να λειτουργεί και να προσφέρει λογισμικό για λήψη που χρησιμοποιείται για επιθέσεις DDoS. Τέλος κατά το τριήμερο, αρκετοί αμερικανοί ερευνητές ασφαλείας υπολογιστών που παρακολουθούσαν κακόβουλα προγράμματα που εκτελούσαν

botnets, τα οποία έστελναν ροές αναξιόπιστων δεδομένων σε υπολογιστές της Γεωργίας, ανέφεραν ότι είδαν σαφείς ενδείξεις μιας σκιώδους εγκληματικής συμμορίας με έδρα την Αγία Πετρούπολη, γνωστή ως Ρωσικό Επιχειρηματικό Δίκτυο ή R.B.N [87].

3.6.3 Η περίπτωση του Ιράν

Το 2010 πραγματοποιήθηκε μια εκτεταμένη κυβερνοεπίθεση εναντίον του Ιράν από τις Η.Π.Α. με την βοήθεια του Ισραήλ. Αυτές οι δύο χώρες κατασκεύασαν ένα κακόβουλο ηλεκτρονικό σκουλήκι, το οποίο ονομάζεται Stuxnet. Το Stuxnet εντοπίστηκε για πρώτη φορά στον κυβερνοχώρο το 2010, προκαλώντας εκτεταμένα προβλήματα στα ηλεκτρονικά συστήματα των βιομηχανιών. Όπως ανέφερε και η εφημερίδα New York Times, ο λόγος που δημιουργήθηκε αυτό το κακόβουλο λογισμικό από τις Ηνωμένες Πολιτείες ήταν για γίνει σαμποτάζ στο πυρηνικό πρόγραμμα που είχε σχεδιάσει το Ιράν. Επίσης, το ίδιο μέσο ενημέρωσης ανέφερε ότι, αυτή η κυβερνοεπίθεση σχεδιάζόταν ήδη από το 2006 και την κυβέρνηση του Μπους και είχε ως κωδική ονομασία «Ολυμπιακοί Αγώνες».

Αυτή η κυβερνοεπίθεση, αν και πρωτόγνωρη και καινοτόμα για την δεδομένη χρονική στιγμή, είχε ως στόχο την αποτροπή μιας ενδεχόμενης έντασης στην περιοχή της Μέσης Ανατολής που θα λειτουργούσε σαν αφορμή μιας πολεμικής σύρραξης. Πριν από αυτό ωστόσο, η CIA προσπάθησε να σαμποτάρει το πυρηνικό σχέδιο του Ιράν, παρεμβαίνοντας στην διαδικασία προμήθειας απαραίτητων εξαρτημάτων αλλάζοντάς τα με ελαττωματικά, πράγμα το οποίο δεν είχε το επιθυμητό αποτέλεσμα.

Το ηλεκτρονικό σκουλήκι Stuxnet σχεδιάστηκε για να διεισδύει σε ηλεκτρονικά συστήματα βιομηχανιών, προκαλώντας πρόβλημα στην λειτουργία των φυγοκεντριστών, οι οποίοι έπρεπε να λειτουργούν σε μεγάλες ταχύτητες συνεχόμενα για μέρες. Το Stuxnet δυνάμωνε και χαμήλωνε την ταχύτητα αυτών των μηχανημάτων με αποτέλεσμα να διαλυθούν. Οι πρώτες επιθέσεις με αυτό το ηλεκτρονικό σκουλήκι ξεκίνησαν το 2008 με θετικά αποτελέσματα. Τελικώς, αυτή η μυστική επιχείρηση με το Stuxnet συνεχίστηκε από την κυβέρνηση του Ομπάμα. Με την νέα κυβέρνηση Ομπάμα που σχηματίστηκε, ο αριθμός αυτών των κυβερνοεπιθέσεων αυξήθηκε ραγδαία, και έγιναν πιο στοχευμένες. Όμως, το καλοκαίρι του 2010, αυτό το κακόβουλο ηλεκτρονικό σκουλήκι αφέθηκε ελεύθερο από λάθος στο διαδίκτυο, μολύνοντας με αυτόν τον τρόπο χιλιάδες υπολογιστές οι οποίοι δεν ήταν επιθυμητοί στόχοι. Όπως χαρακτηριστικά ανέφεραν τα μέσα ενημέρωσης στις Ηνωμένες Πολιτείες, ο πρόεδρος Ομπάμα μετά από αυτό το συμβάν είχε κάποιες επιφυλάξεις, ωστόσο πείστηκε από τους συμβούλους του να συνεχίσει την επιχείρηση με το Stuxnet, αν και το ηλεκτρονικό σκουλήκι είχε ήδη χαθεί από τον έλεγχό τους. Τελικά, το Stuxnet βρέθηκε από της εταιρείες που ασχολούνται με την κυβερνοασφάλεια, οι οποίες αμέσως μετά ξεκίνησαν να ψάχνουν για τα ίχνη του. Το αποτέλεσμα ήταν να μείνει πίσω χρονικά το πρόγραμμα για διάστημα 1,5 με 2 χρόνια, αν και κάποιοι θεωρούν ότι το διάστημα αυτό ήταν λιγότερο [88].

3.6.4 Η περίπτωση της Ουκρανίας

Η κρίση μεταξύ των κρατών Ρωσίας και Ουκρανίας κρατεί εδώ και αρκετά χρόνια. Το 2014, έναν μήνα μετά την προσάρτηση της Κριμαίας στο Ρωσικό κράτος, μια ομάδα από hackers που ονομάζεται Voodoo Bear, εξαπέλυσε μεγάλης κλίμακας κυβερνοεπίθεση στις ενεργειακές και μεταφορικές υποδομές της Ουκρανίας. Τον χειμώνα του επόμενου έτους, ένα κακόβουλο λογισμικό έπληξε αρκετές υποδομές παραγωγής ηλεκτρικής ενέργειας, με αποτέλεσμα 80.000 άτομα να μείνουν χωρίς ηλεκτρικό ρεύμα και κατ' επέκταση χωρίς θέρμανση. Αμέσως μετά ακολούθησε η κατηγορία της Ουκρανίας, ότι υπεύθυνος για αυτές

τις κυβερνοεπιθέσεις ήταν η Ρωσία, με την δεύτερη να διαψεύδει κάθε ανάμειξή της με αυτά τα συμβάντα.

Η ισπανική εφημερίδα El País ανέφερε χαρακτηριστικά ότι, παρόμοιου τύπου κυβερνοεπιθέσεις συνεχίστηκαν για τα επόμενα δύο χρόνια, με την εμφάνιση ενός εξελιγμένου κακόβουλου λογισμικού το 2017 που ονομάζεται NotPetya. Αυτό το κακόβουλο λογισμικό πάλι προκάλεσε δυσλειτουργίες σε υποδομές παραγωγής ηλεκτρικής ενέργειας, αλλά και καταστροφές ευαίσθητων κυβερνητικών δεδομένων και προβλήματα σε υπολογιστικά συστήματα ουκρανικών εταιρειών. Τελικά, αυτός ο ηλεκτρονικός ιός αποδείχθηκε ένας από τους πιο καταστροφικούς στην ιστορία του κυβερνοχώρου που ενώ αρχικά είχε ως στόχο να πλήξει οργανισμούς, ιδρύματα και κρίσιμες υποδομές της Ουκρανίας, στο τέλος κατέληξε να εξαπλωθεί παγκόσμια.

Εκτός από τον ηλεκτρονικό ιό NotPetya, το 2017 βρέθηκαν και άλλα κακόβουλα λογισμικά όπως ο FakeCry και ο BadRabbit, που είχαν ως πρωταρχικό στόχο να πλήξουν τα δίκτυα επικοινωνιών της Ουκρανίας. Αξίζει να σημειωθεί, ότι με αυτές τις επιθέσεις οι ειδικοί που παρακολουθούν διαχρονικά τις ενέργειες των Ρώσων hackers, όπως ο Adam Mayers, κατάλαβαν ότι έγινε προσπάθεια μίμησης κάποιων άλλων. Ένα τέτοιο παράδειγμα είναι η ομάδα hackers που ονομάζεται FSociety, έχοντας πάρει αυτό το όνομα από μια τηλεοπτική σειρά που ονομάζεται Mr. Robot.

Η κλιμάκωση του κυβερνοπολέμου αυτού που είχε ξεκινήσει από το 2014, έγινε 8 χρόνια μετά λίγες εβδομάδες πριν ξεκινήσει η εισβολή των ρωσικών στρατευμάτων στα ουκρανικά εδάφη. Η Ρωσία εξαπέλυσε μεγάλης κλίμακας κυβερνοεπιθέσεις στον Υπουργείο Άμυνας της Ουκρανίας και σε δύο κρατικούς τραπεζικούς οργανισμούς καθιστώντας αυτές τις κυβερνοεπιθέσεις ως τις χειρότερες που είχε βιώσει ποτέ η Ουκρανία. Αρκετοί ουκρανικοί κυβερνητικοί ιστότοποι είχαν δεχθεί κυβερνοεπιθέσεις τον Ιανουάριο, έναν μήνα πριν την εισβολή. Οι ιστότοποι των υπουργείων εξωτερικών, καταστροφών και έρευνας είχαν τεθεί εκτός λειτουργίας. Μάλιστα, ο ιστότοπος του υπουργείου εξωτερικών εμφάνιζε ένα μήνυμα σε ρωσικά, ουκρανικά και πολωνικά που έλεγε «Φοβόμαστε και περιμένουμε το χειρότερο».

Μια μέρα πριν την επίθεση της Ρωσίας στην Ουκρανία τον Φεβρουάριο του 2022, οι κρίσιμες υποδομές της Ουκρανίας είχαν γίνει στόχος κυβερνοεπιθέσεων, με τις ιστοσελίδες του υπουργείου εξωτερικών, της κυβέρνησης και του κοινοβουλίου να τίθενται εκτός λειτουργίας. Παράλληλα, οι hackers μόλυναν εκατοντάδες υπολογιστές με ένα κακόβουλο λογισμικό γνωστό και ως «υαλοκαθαριστήρες». Το λογισμικό αυτό δρα εξ αποστάσεως και προκαλεί μεγάλες ζημιές, αφού μπορεί να αναμορφώσει τους σκληρούς δίσκους των συστημάτων και να διαγράψει δεδομένα. Η υποψία βέβαια των ειδικών για αυτές τις κυβερνοεπιθέσεις ήταν ότι προκλήθηκαν από Ρώσους hackers ή hackers οι οποίοι χρηματοδοτούνται από την Ρωσική κυβέρνηση.

Η Ρωσία χρησιμοποίησε τεχνικές υβριδικού πολέμου, δηλαδή πόλεμο που περιέχει τόσο συμβατικό πόλεμο όσο και κυβερνοπόλεμο, όπως και στον πόλεμο με την Γεωργία. Η Ρωσία μέσω του κυβερνοπολέμου προσπάθησε να υπονομεύσει την εμπιστοσύνη των Ουκρανών πολιτών κατά της κυβέρνησής τους. Οι κυβερνητικές υπηρεσίες της Ουκρανίας ανέφεραν καθημερινά κυβερνοεπιθέσεις, οι οποίες προερχόντουσαν από Ρώσους hackers, με αποτέλεσμα να δημιουργείται ένα αίσθημα φόβου στους πολίτες. Άρα οι κυβερνοεπιθέσεις της Ρωσίας, είτε με κακόβουλα λογισμικά είτε με επιθέσεις άρνησης εξυπηρέτησης, δεν είχαν ως στόχο μόνο να πλήξουν κρίσιμες υποδομές όπως υποδομές παροχής ενέργειας ή νερού,

ούτε να διαγράψουν σημαντικά δεδομένα και να μπλοκάρει υπολογιστικά συστήματα. Είχε και ως στόχο την προσπάθεια χειραγώγησης των συναισθημάτων των Ουκρανών πολιτών [89].

Η πρώτη κυβερνοεπίθεση έλαβε χώρα στις 14 Ιανουαρίου πριν την έναρξη του Ρωσοουκρανικού πολέμου. Η Microsoft ενημέρωσε για την ύπαρξη ενός λογισμικού με την ονομασία WhisperGate, το οποίο στοχεύει συσκευές Windows. Αυτό το κακόβουλο λογισμικό καταστρέφει το χώρισμα που περιέχει Master Boot Record (MBR) και γενικότερα τον σκληρό δίσκο του ηλεκτρονικού υπολογιστή του θύματος. Σχεδιάστηκε έτσι ώστε να μοιάζει με ransomware αλλά δεν παρέχει μηχανισμό ανάκτησης λύτρων, πράγμα του οποίου καθιστά τη συσκευή μη επισκευάσιμη [90]. Φυσικά από τις κυβερνητικές υπηρεσίες και τις κρίσιμες υποδομές της Ουκρανίας που δέχθηκαν κυβερνοεπιθέσεις, δεν θα μπορούσε να λείπουν στρατιωτικά υπολογιστικά συστήματα και στρατιωτικές υποδομές της χώρας [89].

3.7 Η σχέση μεταξύ κυβερνοπολέμου και τρομοκρατίας

Στην σύγχρονη εποχή, οι τρομοκρατικές οργανώσεις εκμεταλλεύονται τον κυβερνοχώρο για να επικοινωνούν, να ανταλλάσσουν και να συλλέγουν πληροφορίες, να έρχονται σε επαφή με τους οπαδούς τους, να συγκεντρώνουν χρηματικά ποσά για τους σκοπούς τους, να οργανώνουν και να διαχειρίζονται τις επιχειρήσεις τους, να αποκτούν με παράνομο τρόπο διαβατήρια και βίζες και να προσελκύουν νέα μέλη. Το διαδίκτυο είναι ένα πολύτιμο εργαλείο για τις τρομοκρατικές οργανώσεις, καθώς διευκολύνει την επικοινωνία και την ανταλλαγή πληροφοριών μεταξύ τους. Οι κυβερνήσεις έχουν την δυνατότητα να εντοπίσουν και να μπλοκάρουν, εξειδικευμένες ιστοσελίδες που εξυπηρετούν τρομοκρατικούς σκοπούς, οι οποίες μόλις εντοπιστούν μπορούν να αντικατασταθούν από άλλες. Οι υποστηρικτές των οργανώσεων μπορούν να χρησιμοποιούν τις εν λόγω ιστοσελίδες για την ανταλλαγή μηνυμάτων ή την ενημέρωση σχετικά με τις εξελίξεις στις επιχειρήσεις τους στο Αφγανιστάν, το Πακιστάν, το Ιράκ και άλλες περιοχές. Στο διαδίκτυο είναι δυνατόν να βρεθούν πληροφορίες σχετικά με την τεχνολογία των όπλων και των οπλικών συστημάτων, την κατασκευή εκρηκτικών μηχανισμών, τον σχεδιασμό και την υλοποίηση επιθέσεων και άλλες τεχνικές που αξιοποιούνται από τρομοκρατικές οργανώσεις.

Από την άλλη πλευρά, το διαδίκτυο και ο κυβερνοχώρος είναι ένας χώρος δράσης των τρομοκρατικών οργανώσεων και των δυνάμεων ασφαλείας των χωρών. Παρ' όλα αυτά το διαδίκτυο δεν αποτελεί δυνητικό στόχο και μέχρι στιγμής δεν έχει γίνει φανερή κάποια πρόθεση από κάποια τρομοκρατική οργάνωση να πλήξει μέσω κυβερνοεπιθέσεων το ίδιο το διαδίκτυο και να προκαλέσει την καταστροφή του. Στο διαδίκτυο είναι δυνατόν να βρεθούν πληροφορίες σχετικά με την τεχνολογία των όπλων και των οπλικών συστημάτων, την κατασκευή εκρηκτικών μηχανισμών, τον σχεδιασμό και την υλοποίηση επιθέσεων και άλλες τεχνικές που αξιοποιούνται από τρομοκρατικές οργανώσεις. Υπάρχουν τρεις παράγοντες που μειώνουν την ελκυστικότητα των κυβερνοεπιθέσεων στο ίδιο το διαδίκτυο για τις τρομοκρατικές οργανώσεις :

1. Η αποτελεσματικότητα των κυβερνοεπιθέσεων είναι λιγότερη σε σχέση με άλλες επιθέσεις, καθώς δεν έχουν τις ίδιες συνέπειες όπως οι επιθέσεις που προκαλούν νεκρούς, και δεν έχουν την ίδια ψυχολογική ή πολιτική επίδραση.
2. Οι κυβερνοεπιθέσεις που στοχεύουν τις κρίσιμες υποδομές είναι πιο δύσκολες να πραγματοποιηθούν με επιτυχία λόγω της πολυπλοκότητάς τους.
3. Το διαδίκτυο είναι το μέσο για να υλοποιήσουν οι τρομοκράτες τους σκοπούς τους.

Με την εξέλιξη των τεχνικών και των τακτικών στον κυβερνοπόλεμο, η καταστροφή κρίσιμων υποδομών των χωρών γίνεται πιο εφικτή, γεγονός που ενδέχεται να οδηγήσει στη στρατολόγηση ειδικών στον τομέα αυτό από τρομοκρατικές οργανώσεις. Αυτό μπορεί να οδηγήσει σε χτυπήματα που δεν θα είναι τόσο εκτυφλωτικά όσο αυτό στους Δίδυμους Πύργους, αλλά που θα προκαλέσουν σημαντικές οικονομικές ζημιές [91].

Κεφάλαιο 4 Τρόποι πρόληψης στον κυβερνοχώρο

Υπάρχουν πολλοί τρόποι να προστατευτούν από τις κυβερνοεπιθέσεις τόσο οι δημόσιοι και οι ιδιωτικοί οργανισμοί, όσο και οι μικρές επιχειρήσεις και οι μεμονωμένοι χρήστες. Σε αυτό το κεφάλαιο θα εξεταστούν όλες οι ενέργειες, οι τεχνικές και οι τεχνολογίες, οι οποίες συμβάλλουν στην πρόληψη του ηλεκτρονικού εγκλήματος. Αρχικά, θα αναφερθούν τρόποι με τους οποίους ένα δίκτυο μπορεί να είναι ασφαλές και στην συνέχεια θα αναφερθούν και στις ενέργειες τις οποίες πρέπει να ακολουθήσει ένας μεμονωμένος χρήστης έτσι ώστε να παραμείνει ασφαλής στο διαδίκτυο και τον κυβερνοχώρο.

Λόγω της ευρείας διάδοσης του διαδικτύου και των πολλαπλών τρόπων χρήσης του στην καθημερινότητα μας, καθώς και των απειλών που συνδέονται με αυτό, είναι αναγκαίο να ληφθούν κάποια μέτρα πρόληψης για να διασφαλιστεί η ασφαλής χρήση των χρηστών. Σε αυτό το κεφάλαιο, παρουσιάζονται μέτρα και εργαλεία που βοηθούν στην πρόληψη εισβολών και επιθέσεων από κυβερνοεγκληματίες με σκοπό να προκαλέσουν ζημιές στα θύματά τους.

Είναι ήδη γνωστό από πολλούς ειδικούς σε θέματα κυβερνοασφάλειας ότι, ένα πληροφοριακό σύστημα για να είναι ασφαλές, θα πρέπει να περιέχει τα τρία παρακάτω χαρακτηριστικά : α) Διαθεσιμότητα, β) Εμπιστευτικότητα και γ) Ακεραιότητα. Με τον όρο διαθεσιμότητα, το πληροφοριακό σύστημα πρέπει να είναι πάντα διαθέσιμο προς χρήση χωρίς να αντιμετωπίζει προβλήματα ανταπόκρισης, με τον όρο εμπιστευτικότητα, το πληροφοριακό σύστημα δεν πρέπει να μοιράζεται τα δεδομένα των χρηστών με μη εξουσιοδοτημένες οντότητες και τέλος με τον όρο ακεραιότητα, το πληροφοριακό σύστημα πρέπει να προλαμβάνει μια μη εξουσιοδοτημένη εγγραφή ή διαγραφή, και την μη εξουσιοδοτημένη δημιουργία δεδομένων. Με την έλλειψη των τριών αυτών χαρακτηριστικών το πληροφοριακό σύστημα θεωρείται ανασφαλές, που είτε ηθελημένα είτε άθελα γίνεται μέσω διάπραξης ηλεκτρονικού εγκλήματος [92].

4.1 Αντιικά λογισμικά (antivirus)

Τα περισσότερα ηλεκτρονικά εγκλήματα διαπράττονται μέσω των κακόβουλων λογισμικών και των ηλεκτρονικών ιών. Ο πιο συνηθισμένος τρόπος να προστατευθεί ένας χρήστης του διαδικτύου από τα κακόβουλα λογισμικά είναι με την χρήση κάποιου αντιικού λογισμικού, γνωστό και ως antivirus. Ένα πρόγραμμα antivirus πρέπει να υλοποιεί τρεις βασικές λειτουργίες :

- Να μπορεί να αναγνωρίζει έναν ιό. Αυτό επιτυγχάνεται ή με αυτόματη σάρωση από το ίδιο το πρόγραμμα στο σύστημα και στα αποθηκευτικά μέσα που περιέχει ή με σάρωση μέσω εντολής από τον ίδιο τον χρήστη.
- Να μπορεί να ταυτοποιεί και να μπορεί να διακρίνει σε ποιο είδος από τα κακόβουλα λογισμικά που αναφέραμε στο κεφάλαιο 2, ανήκει ο ιός που έχει προσβάλει έναν ηλεκτρονικό υπολογιστή.
- Να μπορεί να αποβάλλει τον ιό από το σύστημα, επιδιορθώνοντας τα μολυσμένα αρχεία [93].

Ο όρος «αντικό λογισμικό» δεν αναφέρεται μόνο σε λογισμικά που δρουν κατά τον ηλεκτρονικών ιών, αντιθέτως αναφέρεται σε λογισμικά τα οποία αντιμετωπίζουν όλα τα είδη κακόβουλων λογισμικών (antimalware). Malware μπορεί να είναι επίσης τα εξής spyware, adware, trojans, worms και άλλα κακόβουλα λογισμικά που έχουν αναφερθεί στο κεφάλαιο 2.

Ο λόγος που έχει επικρατήσει ως γενική ονομασία «αντικό λογισμικό» είναι επειδή πριν μερικά χρόνια οι ηλεκτρονικοί ιοί (και σε μικρότερο βαθμό τα Trojans και τα ηλεκτρονικά σκουλήκια) μονοπωλούσαν στις ειδήσεις, οι εταιρείες ασφάλειας αποφάσισαν να επικεντρωθούν για λόγους marketing σε αυτούς δίνοντας τελικά μια γενική ονομασία για όλα τα λογισμικά κατά των κακόβουλων λογισμικών.

Για να περιγραφεί με σαφήνεια η λειτουργία των αντικών λογισμικών θα αναφερθεί η περίπτωση του Avast. Σύμφωνα με τον Jiri Sejtko, διευθυντή του εργαστηρίου ιών της Avast, «το λογισμικό της εταιρείας σκανάρει και προστατεύει τους πελάτες από όλα τα είδη κακόβουλο λογισμικού. Οι ιοί ήταν εξαιρετικά 'δημοφιλείς' τη δεκαετία του '90, που είναι και η εποχή που έγινε συνηθισμένος ο όρος 'Αντικό', αλλά σήμερα οι ιοί αποτελούν τη μειονότητα όταν πρόκειται για κακόβουλο λογισμικό. Υπάρχουν, ωστόσο, μερικοί ιοί που εξακολουθούν να εξελίσσονται και να εξαπλώνονται ακόμη, αυτοί περιλαμβάνουν τους 'Salinity' και 'Virus'. Πιο συνηθισμένα από τους ιούς είναι άλλα κακόβουλα λογισμικά όπως, Trojans, Worms, Backdoors, Exploits, Adware, and PUP (Potentially Unwanted Programs), τα οποία μπορεί να περιλαμβάνουν πελάτες επικοινωνίας, απομακρυσμένες επιφάνειες εργασίας και εργαλεία αποκάλυψης κωδικών. Η εστίαση των διαδικτυακών εγκληματιών έχει μετατοπιστεί, και συνεπώς το κακόβουλο λογισμικό έχει αλλάξει. Οι εγκληματίες βλέπουν τη σημερινή διαδικτυακή κοινωνία ως μια ευκαιρία για να κλέψουν προσωπικά δεδομένα, συμπεριλαμβανομένων των στοιχείων πιστωτικής κάρτας και τραπεζικών λογαριασμών, PINs και κωδικών πρόσβασης, καθώς και πληροφοριών, όπως διευθύνσεις οικιών, αριθμούς τηλεφώνων ακόμα και τα ονόματα από μέλη της οικογένειας. Οι εγκληματίες μπορούν, για παράδειγμα, να γράψουν κακόβουλο κώδικα και να τον διανέμουν ως trojan. Τα trojan μπορούν να συλλέξουν προσωπικά δεδομένα τα οποία μπορούν να πωληθούν σε εγκληματικές οργανώσεις, οι οποίες μπορούν στη συνέχεια να κλέψουν χρήματα απευθείας από τον τραπεζικό λογαριασμό των θυμάτων. Η τεράστια βάση χρηστών της Avast αποτελείται από περισσότερα από 184 εκατομμύρια άτομα παγκοσμίως, καθένα από τα οποία είναι συνδεδεμένο με το Avast Cloud. Αυτό επιτρέπει την ανάλυση κάθε εκτέλεσης αρχείου σε πραγματικό χρόνο στο διαδίκτυο. Μόλις ανιχνευθεί κακόβουλο λογισμικό μέσα στη βάση χρηστών, αποστέλλεται μια ενημέρωση σχεδόν σε πραγματικό χρόνο σε όλους τους χρήστες, προσφέροντας σχεδόν άμεση προστασία από όλο το νεότερο κακόβουλο λογισμικό.»

Συνεπώς, σύμφωνα με τα λεγόμενα του Sejtko το λογισμικό της Avast προστατεύει τον χρήστη από τις «κλασικές» απειλές όπως οι ιοί, Trojans, worms, αλλά επίσης προστατεύει και από adware, bots και άλλα κακόβουλα λογισμικά που εκμεταλλεύονται ευπάθειες [93.1].

4.2 Τείχη προστασίας (firewall)

Με τον όρο τείχος προστασίας ή “firewall” αναφερόμαστε σε κάποια ηλεκτρονική συσκευή ή λογισμικό που έχουν ως στόχο να ελέγχουν τα πακέτα που μεταφέρονται από ένα δίκτυο υπολογιστών σε ένα άλλο. Τα firewalls μπορούν να θεωρηθούν ως «συνοριακές» πύλες ή πύλες ελέγχου που διαχειρίζονται την κίνηση επιτρεπόμενων και απαγορευμένων δραστηριοτήτων στον ιδιωτικό δίκτυο. Γλωσσολογικά ο όρος προέρχεται από την έννοια των φυσικών τοίχων που είναι εμπόδια για να επιβραδύνουν τη διάδοση της φωτιάς μέχρι να μπορέσουν οι υπηρεσίες έκτακτης ανάγκης να την σβήσουν. Σε σύγκριση με αυτό, τα firewalls ασφάλειας δικτύου είναι για τη διαχείριση της κίνησης στον ιστό - συνήθως σχεδιασμένα για να επιβραδύνουν τη διάδοση των απειλών στον ιστό.

Τα firewalls δημιουργούν στενά σημεία (choke points) στα οποία θα κατευθύνουν την κυκλοφορία του ιστού και μέσω αυτών στη συνέχεια ελέγχεται η κυκλοφορία αυτή βάσει ενός συνόλου προγραμματισμένων παραμέτρων και ενεργούν αναλόγως. Ορισμένα firewalls παρακολουθούν επίσης την κυκλοφορία και τις συνδέσεις σε αρχεία καταγραφής ελέγχου για να αναφέρουν τι έχει επιτραπεί ή αποκλειστεί. Τα firewalls χρησιμοποιούνται συνήθως για να φυλάσσουν τα «σύνορα» μιας ιδιωτικής δικτύωσης ή των κατοχυρωμένων συσκευών της. Έτσι, τα firewalls αποτελούν ένα εργαλείο ασφαλείας στην ευρύτερη κατηγορία ελέγχου πρόσβασης χρήστη. Αυτοί οι φραγμοί συνήθως ρυθμίζονται σε δύο θέσεις - σε ειδικούς υπολογιστές στο δίκτυο ή στους υπολογιστές των χρηστών και άλλα τελικά σημεία (hosts).

Ένα τείχος προστασίας αποφασίζει ποια κίνηση δικτύου επιτρέπεται να περάσει και ποια κίνηση θεωρείται επικίνδυνη. Ουσιαστικά, λειτουργεί φιλτράροντας το καλό από το κακό, ή το αξιόπιστο από το μη αξιόπιστο. Ωστόσο, πριν εξετάσουμε λεπτομερώς, βοηθάει να κατανοήσουμε τη δομή των δικτύων βασισμένων στο web. Τα firewall προορίζονται για την ασφάλεια των ιδιωτικών δικτύων και των τερματικών συσκευών μέσα σε αυτά, γνωστές ως δικτυακοί οικοδεσπότες (network hosts). Οι δικτυακοί οικοδεσπότες είναι συσκευές που επικοινωνούν με άλλους οικοδεσπότες στο δίκτυο. Αποστέλλουν και λαμβάνουν δεδομένα μεταξύ εσωτερικών δικτύων, καθώς και εξερχόμενα και εισερχόμενα μεταξύ εξωτερικών δικτύων.

Οι υπολογιστές και άλλες συσκευές τερματικού σημείου χρησιμοποιούν δίκτυα για να έχουν πρόσβαση στο internet και μεταξύ τους. Ωστόσο, το internet είναι διαμερισμένο σε υποδίκτυα ή "subnets" για λόγους ασφαλείας και ιδιωτικότητας. Τα βασικά υποδίκτυα είναι τα εξής:

- Τα εξωτερικά δημόσιοι δίκτυα αναφέρονται συνήθως στο δημόσιο / παγκόσμιο διαδίκτυο ή σε διάφορα εξωτερικά δίκτυα (extranets).
- Το εσωτερικό ιδιωτικό δίκτυο καθορίζει ένα δίκτυο στο σπίτι, εταιρικά intranets και άλλα «κλειστά» δίκτυα.
- Τα περιμετρικά δίκτυα περιγράφουν τα σύνορα των δικτύων που αποτελούνται από προπύργιους hosts, δηλαδή σε ηλεκτρονικούς υπολογιστές εξειδικευμένοι με την σκληραγώγηση της ασφάλειας και που είναι έτοιμοι να αντέξουν μια εξωτερική επίθεση. Ως ασφαλής αντιμετώπιση μεταξύ εσωτερικών και εξωτερικών δικτύων, αυτά μπορούν επίσης να χρησιμοποιηθούν για να φιλοξενήσουν οποιεσδήποτε υπηρεσίες που παρέχονται από το εσωτερικό δίκτυο προς το εξωτερικό (δηλαδή, διακομιστές για ιστοσελίδες, ηλεκτρονικό ταχυδρομείο, FTP, VoIP, κλπ.). Είναι πιο ασφαλή από τα εξωτερικά δίκτυα αλλά λιγότερο ασφαλή από τα εσωτερικά. Δεν είναι πάντα παρόντα σε απλούστερα δίκτυα όπως τα οικιακά δίκτυα, αλλά συχνά χρησιμοποιούνται σε εταιρικά ή εθνικά εσωτερικά δίκτυα.

Οι δρομολογητές προστασίας (screening routers) είναι εξειδικευμένοι υπολογιστές-πύλες που τοποθετούνται σε ένα δίκτυο για να το διαχωρίσουν. Είναι γνωστοί ως οικιακά τείχη προστασίας σε επίπεδο δικτύου. Τα δύο πιο κοινά μοντέλα διαχωρισμού είναι ο διαχωρισμός με τείχος προστασίας εξυπηρετητή (host) και ο διαχωρισμός με τείχος προστασίας υποδικτύου :

- Οι διαχωρισμοί με τείχος προστασίας εξυπηρετητή χρησιμοποιούν έναν μόνο δρομολογητή διαμερισμού μεταξύ των εξωτερικών και των εσωτερικών δικτύων. Αυτά τα δίκτυα είναι τα δύο υποδίκτυα αυτού του μοντέλου.

- Οι διαχωρισμοί με τείχος προστασίας υποδικτύου χρησιμοποιούν δύο ειδικούς δρομολογητές - έναν που ονομάζεται access router (δρομολογητής πρόσβασης) μεταξύ του εξωτερικού και του περιμετρικού δικτύου και έναν ακόμη που ονομάζεται choke router (δρομολογητής περιορισμού) μεταξύ του περιμετρικού και του εσωτερικού δικτύου. Αυτό δημιουργεί τρία υποδίκτυα αντίστοιχα.

Τόσο η περιφέρεια του δικτύου όσο και οι ίδιοι οι υπολογιστές των οικοδεσποτών (hosts) μπορούν να φιλοξενούν ένα τείχος προστασίας. Για να επιτευχθεί αυτό, το τείχος προστασίας τοποθετείται μεταξύ ενός μεμονωμένου υπολογιστή και της σύνδεσής του με ένα ιδιωτικό δίκτυο.

- ❖ Τα τείχη προστασίας δικτύου (network firewalls) αφορούν την εφαρμογή ενός ή περισσότερων τοίχων προστασίας μεταξύ εξωτερικών δικτύων και εσωτερικών ιδιωτικών δικτύων. Αυτά ρυθμίζουν την εισερχόμενη και εξερχόμενη δικτυακή κυκλοφορία, διαχωρίζοντας τα εξωτερικά δημόσια δίκτυα - όπως το παγκόσμιο διαδίκτυο - από τα εσωτερικά δίκτυα, όπως τα ασύρματα δίκτυα στο σπίτι, τα εταιρικά intranet ή τα εθνικά intranet. Τα network firewalls μπορούν να λειτουργήσουν ως εξής: ως εξειδικευμένο υλικό (hardware), ως λογισμικό, ή ως εικονικό λογισμικό.
- ❖ Τα τείχη προστασίας των εξυπηρετητών - οικοδεσποτών (host firewalls) ή «λογισμικά τείχη προστασίας» αφορούν τη χρήση τοίχων προστασίας σε ξεχωριστές συσκευές χρηστών και άλλα άκρα ιδιωτικών δικτύων ως φραγμό μεταξύ των συσκευών εντός του δικτύου. Αυτές οι συσκευές, ή hosts, λαμβάνουν προσαρμοσμένη ρύθμιση της κίνησης προς και από συγκεκριμένες εφαρμογές υπολογιστών. Τα τοπικά τείχη προστασίας μπορούν να τρέχουν σε τοπικές συσκευές ως υπηρεσία λειτουργικού συστήματος ή ως εφαρμογή ασφαλείας άκρου. Τα τοπικά τείχη προστασίας μπορούν επίσης να εμβαθύνουν στην κίνηση του ιστού, φιλτράροντας βάσει του πρωτοκόλλου HTTP και άλλων πρωτοκόλλων δικτύωσης, επιτρέποντας τη διαχείριση του περιεχομένου που φτάνει στη συσκευή του χρήστη, αντί να αποφασίζει μόνο από πού προέρχεται.

Ένα network firewall απαιτεί ρύθμιση για μια ευρεία περιοχή συνδέσεων, ενώ ένα host firewall μπορεί να προσαρμοστεί για να ταιριάζει με τις ανάγκες κάθε μηχανής. Ωστόσο, τα firewall των υπολογιστών απαιτούν περισσότερη προσπάθεια για εξατομίκευση, που σημαίνει ότι τα βασισμένα σε δίκτυα είναι ιδανικά για μια σφαιρική λύση ελέγχου. Ωστόσο, η χρήση και των δύο τύπων firewall σε και τις δύο τοποθεσίες ταυτόχρονα είναι ιδανική για ένα πολυεπίπεδο σύστημα ασφαλείας.

Ο έλεγχος κίνησης μέσω ενός τείχους προστασίας χρησιμοποιεί προκαθορισμένους ή δυναμικά μαθημένους κανόνες για την επιτροπή ή απόρριψη προσπαθειών σύνδεσης. Αυτοί οι κανόνες είναι ο τρόπος με τον οποίο ένα τείχος προστασίας ρυθμίζει τη ροή κίνησης στο διαδίκτυο, μέσω του ιδιωτικού δικτύου και των προσωπικών υπολογιστών του χρήστη. Ανεξάρτητα από τον τύπο, όλα τα τείχη προστασίας μπορούν να φιλτράρουν με κάποιο συνδυασμό των ακόλουθων:

1. Πηγή: Από πού προσπαθεί να γίνει σύνδεση.
2. Προορισμός: Η τοποθεσία στην οποία η απόπειρα σύνδεσης έχει σκοπό να πάει.
3. Περιεχόμενα: Τι προσπαθεί να στείλει μια προσπάθεια σύνδεσης.

4. Πρωτόκολλα πακέτων: Σε ποια "γλώσσα" μιλάει μια προσπάθεια σύνδεσης για να μεταφέρει το μήνυμά της. Ανάμεσα στα πρωτόκολλα δικτύωσης που χρησιμοποιούν οι υπολογιστές για να "μιλήσουν" μεταξύ τους, τα πρωτόκολλα TCP/IP χρησιμοποιούνται κυρίως για την επικοινωνία στο internet και στα εντός δικτύων/υποδικτύων.
5. Πρωτόκολλα εφαρμογών: Συνήθη πρωτόκολλα περιλαμβάνουν τα HTTP, Telnet, FTP, DNS και SSH.

Η πηγή και ο προορισμός επικοινωνούν μέσω του πρωτοκόλλου internet protocol (IP) και θυρών (ports). Οι IP διευθύνσεις είναι μοναδικά ονόματα συσκευών για κάθε κόμβο δικτύου. Οι θύρες είναι ένα υποεπίπεδο κάθε πηγής και προορισμού συσκευής, παρόμοιο με γραφεία σε ένα μεγαλύτερο κτίριο. Συνήθως, οι θύρες ανατίθενται για συγκεκριμένους σκοπούς, έτσι ώστε αν ορισμένα πρωτόκολλα και διευθύνσεις IP που χρησιμοποιούν ασυνήθιστες θύρες ή απενεργοποιημένες θύρες μπορεί να αποτελέσουν ανησυχία. Χρησιμοποιώντας αυτά τα αναγνωριστικά χαρακτηριστικά, ένα τείχος προστασίας μπορεί να αποφασίσει αν ένα πακέτο δεδομένων που προσπαθεί να συνδεθεί πρέπει να απορριφθεί - αθόρυβα ή με απόρριψη κατά την επιστροφή σφάλματος στον αποστολέα - ή να προωθηθεί [94].

Η χρήση firewall συχνά συνδυάζεται με άλλες τεχνολογίες, κυρίως με τον δρομολογητή, και πολλές τεχνολογίες που συχνά συσχετίζονται με τα τείχη προστασίας αποτελούν μάλλον μέρος αυτών των άλλων τεχνολογιών. Για παράδειγμα, η μετάφραση διευθύνσεων δικτύου (NAT) θεωρείται μερικές φορές ως τεχνολογία προστατευτικού τείχους, αλλά στην πραγματικότητα αποτελεί τεχνολογία δρομολόγησης. Πολλά firewalls περιλαμβάνουν επίσης χαρακτηριστικά φιλτραρίσματος περιεχομένου, για την επιβολή πολιτικών της οργάνωσης που δεν σχετίζονται άμεσα με την ασφάλεια. Κάποια τείχη προστασίας περιλαμβάνουν επίσης τεχνολογίες συστημάτων πρόληψης διείσδυσης (IPS), τα οποία μπορούν να αντιδράσουν σε επιθέσεις που ανιχνεύουν για να αποτρέψουν τη ζημιά σε συστήματα που προστατεύονται από το firewall.

Τα firewalls τοποθετούνται συχνά στα περίχωρα ενός δικτύου. Ένα τέτοιο firewall μπορεί να έχει εξωτερική και εσωτερική διεπαφή, με την εξωτερική διεπαφή να βρίσκεται στο έξω μέρος του δικτύου. Αυτές οι δύο διεπαφές ονομάζονται μερικές φορές ανεπτυγμένη και προστατευμένη αντίστοιχα. Ωστόσο, να λέμε ότι κάτι είναι ή δεν είναι προστατευμένο συχνά δεν είναι κατάλληλο, διότι οι πολιτικές ενός τείχους προστασίας μπορούν να λειτουργούν και στις δύο κατευθύνσεις. Για παράδειγμα, μπορεί να υπάρχει μια πολιτική για τον περιορισμό του εκτελέσιμου κώδικα από το εσωτερικό της περιμέτρου προς το εξωτερικό μέρος της περιμέτρου.

4.2.1 Τείχη προστασίας φιλτραρίσματος πακέτων

Η κύρια λειτουργία ενός firewall είναι το φίλτρο πακέτων. Τα παλαιότερα τείχη προστασίας που ήταν μόνο φίλτρα πακέτων ήταν ουσιαστικά συσκευές δρομολόγησης που παρείχαν λειτουργικότητα ελέγχου πρόσβασης για τις διευθύνσεις των υπολογιστών και τις συνεδρίες επικοινωνίας. Αυτές οι συσκευές, γνωστές επίσης ως τείχη προστασίας χωρίς κατάσταση, δεν καταγράφουν την κατάσταση κάθε ροής κυκλοφορίας που περνά από το τείχος. Αυτό σημαίνει, για παράδειγμα, ότι δεν μπορούν να συσχετίσουν πολλαπλά αιτήματα εντός μίας μόνο συνεδρίας μεταξύ τους. Το φιλτράρισμα πακέτων βρίσκεται στον πυρήνα των περισσότερων σύγχρονων firewalls, αλλά στις μέρες μας υπάρχουν λίγα τείχη προστασίας που ασχολούνται μόνο με το φιλτράρισμα ανιθαγενών πακέτων. Ανόμοια από πιο προηγμένα φίλτρα, τα φίλτρα πακέτων δεν ενδιαφέρονται για το περιεχόμενο των πακέτων. Η

λειτουργικότητά τους για τον έλεγχο πρόσβασης διέπεται από ένα σύνολο οδηγιών που αναφέρονται ως κανόνες. Οι δυνατότητες φιλτραρίσματος πακέτων είναι ενσωματωμένες σε περισσότερα λειτουργικά συστήματα και σε συσκευές που υποστηρίζουν τη δρομολόγηση. Το πιο κοινό παράδειγμα μιας συσκευής που ασχολείται αποκλειστικά με το φιλτράρισμα πακέτων είναι ένα δρομολογητής δικτύου που χρησιμοποιεί λίστες ελέγχου πρόσβασης.

Στην πιο βασική τους μορφή, τα firewalls με φίλτρα πακέτων λειτουργούν στο επίπεδο δικτύου. Αυτό παρέχει έλεγχο πρόσβασης στο δίκτυο βασισμένο σε διάφορες πληροφορίες που περιέχονται σε ένα πακέτο, συμπεριλαμβανομένων :

- Η πηγαία διεύθυνση IP του πακέτου - η διεύθυνση του υπολογιστή από τον οποίο προήλθε το πακέτο (όπως το 192.168.1.1)
- Η διεύθυνση προορισμού του πακέτου - η διεύθυνση του υπολογιστή προς τον οποίο επιχειρεί να φτάσει το πακέτο (π.χ. 192.168.2.1)
- Το δίκτυο ή το πρωτόκολλο μεταφοράς που χρησιμοποιείται για την επικοινωνία μεταξύ των υπολογιστών πηγής και προορισμού, όπως TCP, UDP ή ICMP.
- Πιθανώς κάποια χαρακτηριστικά των συνεδριών επικοινωνίας στο επίπεδο μεταφοράς, όπως οι θύρες πηγής και προορισμού της συνεδρίας (π.χ., TCP 80 για τη θύρα προορισμού που ανήκει σε έναν διακομιστή ιστού, TCP 1320 για τη θύρα πηγής που ανήκει σε έναν προσωπικό υπολογιστή που αποκτά πρόσβαση στο διακομιστή).
- Η διεπαφή που διασχίζεται από το πακέτο και η κατεύθυνσή του (εισερχόμενο ή εξερχόμενο).

Το φιλτράρισμα της εισερχόμενης κυκλοφορίας είναι γνωστό ως φιλτράρισμα εισόδου. Η εξερχόμενη κυκλοφορία μπορεί επίσης να φιλτράρεται, διαδικασία που αναφέρεται ως φιλτράρισμα εξόδου. Εδώ, οι οργανισμοί μπορούν να επιβάλλουν περιορισμούς στην εσωτερική τους κυκλοφορία, όπως το φραγμό της χρήσης εξωτερικών διακομιστών πρωτοκόλλου μεταφοράς αρχείων (FTP) ή τον περιορισμό της εκτέλεσης επιθέσεων απόρριψης υπηρεσίας (DoS) από το εσωτερικό του οργανισμού εναντίον εξωτερικών φορέων. Οι οργανισμοί πρέπει να επιτρέπουν μόνο την εξερχόμενη κυκλοφορία που χρησιμοποιεί τις διευθύνσεις IP πηγής που χρησιμοποιούνται από τον ίδιο τον οργανισμό - μια διαδικασία που βοηθά στο να αποτραπεί η διαρροή κυκλοφορίας με ψευδείς διευθύνσεις σε άλλα δίκτυα. Οι ψευδείς διευθύνσεις μπορεί να προκληθούν από κακόβουλα γεγονότα, όπως μολυσμένο λογισμικό ή διακριθείσες υπολογιστικές μονάδες που χρησιμοποιούνται για επιθέσεις, ή από ακούσιες λανθασμένες ρυθμίσεις.

Τα φίλτρα πακέτων χωρίς κατάσταση είναι γενικά ευάλωτα σε επιθέσεις και εκμετάλλευση προβλημάτων εντός της προδιαγραφής TCP/IP και του πρωτοκόλλου. Για παράδειγμα, πολλά φίλτρα πακέτων είναι ανίκανα να ανιχνεύσουν όταν οι πληροφορίες διεύθυνσης του δικτύου σε ένα πακέτο στο οποίο έχουν παραποιηθεί ή αλλοιωθεί με κάποιον τρόπο, ή όταν χρησιμοποιεί επιλογές που επιτρέπονται από τα πρότυπα αλλά χρησιμοποιούνται γενικά για κακόβουλους σκοπούς, όπως η δρομολόγηση πηγής IP. Οι επιθέσεις με παραποίηση, όπως η χρήση εσφαλμένων διευθύνσεων στις κεφαλίδες των πακέτων, χρησιμοποιούνται γενικά από εισβολείς για να παρακάμψουν τους ελέγχους ασφαλείας που εφαρμόζονται σε μια πλατφόρμα προστατευτικού φράγματος. Τα τείχη προστασίας που λειτουργούν σε υψηλότερα επίπεδα μπορούν να αποτρέψουν ορισμένες επιθέσεις παραποίησης ελέγχοντας ότι μια συνεδρία είναι εδραιωμένη, ή ελέγχοντας την αυθεντικότητα των χρηστών πριν επιτρέψουν την διέλευση της κυκλοφορίας. Εξαιτίας αυτού,

τα περισσότερα τείχη προστασίας που χρησιμοποιούν φίλτρα πακέτων διατηρούν επίσης κάποιες πληροφορίες κατάστασης για τα πακέτα που διασχίζουν το firewall.

Ορισμένα φίλτρα πακέτων μπορούν να φιλτράρουν ειδικά πακέτα που έχουν κατακερματιστεί. Η διάσπαση των πακέτων επιτρέπεται από τις προδιαγραφές TCP/IP και προωθείται σε καταστάσεις όπου απαιτείται. Ωστόσο, η διάσπαση πακέτων έχει χρησιμοποιηθεί για να καταστήσει ορισμένες επιθέσεις δυσκολότερο να ανιχνευθούν (τοποθετώντας τις μέσα σε κατακερματισμένα πακέτα), και η ασυνήθιστη διάσπαση έχει χρησιμοποιηθεί επίσης ως μορφή επίθεσης. Για παράδειγμα, ορισμένες επιθέσεις βασισμένες στο δίκτυο έχουν χρησιμοποιήσει πακέτα που δεν θα έπρεπε να υπάρχουν σε κανονικές επικοινωνίες, όπως η αποστολή ορισμένων αποσπασμάτων ενός πακέτου αλλά όχι το πρώτο απόσπασμα, ή η αποστολή αποσπασμάτων πακέτων που επικαλύπτονται μεταξύ τους. Για να αποτραπεί η χρήση κατακερματισμένων πακέτων σε επιθέσεις, ορισμένα τείχη προστασίας έχουν ρυθμιστεί για να μπλοκάρουν τα κατακερματισμένα πακέτα.

Τα κατακερματισμένα πακέτα στο Διαδίκτυο συχνά συμβαίνουν όχι λόγω επιθέσεων, αλλά λόγω τεχνολογιών εικονικών ιδιωτικών δικτύων (VPN) που ενθυλακώνουν πακέτα μέσα σε άλλα πακέτα. Εάν η ενθυλάκωση ενός πακέτου θα οδηγούσε το νέο πακέτο να υπερβεί το μέγιστο επιτρεπόμενο μέγεθος για το μέσο μετάδοσης στο οποίο θα μεταδοθεί, το πακέτο πρέπει να κατακερματιστεί. Η φραγή κατακερματισμένων πακέτων από προστατευτικά φράγματα αποτελεί συνηθισμένο αίτιο προβλημάτων συμβατότητας VPN.

Ορισμένα firewalls μπορούν να επανασυναρμολογήσουν τα κατακερματισμένα αποσπάσματα πριν τα περάσουν στο εσωτερικό δίκτυο, αν και αυτό απαιτεί επιπλέον πόρους του τείχους προστασίας, ειδικά μνήμη. Τα firewalls που έχουν αυτή τη δυνατότητα επανασυναρμολόγησης πρέπει να την υλοποιήσουν προσεκτικά, διαφορετικά κάποιος μπορεί εύκολα να εκτελέσει επίθεση αρνήσης υπηρεσίας. Η επιλογή εάν θα μπλοκαριστούν, επανασυναρμολογηθούν ή θα περάσουν τα κατακερματισμένα πακέτα αποτελεί έναν συμβιβασμό μεταξύ της συνολικής δικτυακής συμβατότητας και της πλήρους ασφάλειας του συστήματος. Δεδομένου αυτού, δεν συνιστάται η αυτόματη φραγή όλων των κατακερματισμένων πακέτων λόγω των νόμιμων και απαραίτητων χρήσεων της διάσπασης στο Διαδίκτυο."

4.2.2 Τείχη προστασίας επιθεώρησης κατάστασης

Η εποπτεία με κατάσταση βελτιώνει τις λειτουργίες των φίλτρων πακέτων παρακολουθώντας την κατάσταση των συνδέσεων και φράζοντας πακέτα που αποκλίνουν από την αναμενόμενη κατάσταση. Αυτό επιτυγχάνεται με την ενσωμάτωση μεγαλύτερης επίγνωσης στο επίπεδο μεταφοράς. Όπως και με το φιλτράρισμα πακέτων, η εποπτεία με κατάσταση παρεμβαίνει στα πακέτα στο επίπεδο δικτύου και τα επιθεωρεί για να δει αν επιτρέπονται από έναν υπάρχον κανόνα του τείχους προστασίας, αλλά αντίθετα με το φιλτράρισμα πακέτων, η εποπτεία με κατάσταση παρακολουθεί κάθε σύνδεση σε έναν πίνακα κατάστασης. Ενώ οι λεπτομέρειες των καταχωρήσεων στον πίνακα κατάστασης ποικίλλουν ανάλογα με το προϊόν του τείχους προστασίας, συνήθως περιλαμβάνουν τη διεύθυνση IP πηγής, τη διεύθυνση IP προορισμού, τους αριθμούς θυρών και πληροφορίες για την κατάσταση της σύνδεσης.

Τρεις κύριες καταστάσεις υπάρχουν για την κυκλοφορία TCP - η δημιουργία σύνδεσης, η χρήση και ο τερματισμός (που αναφέρεται τόσο σε ένα άκρο που ζητά τον τερματισμό μιας σύνδεσης όσο και σε μια σύνδεση με μεγάλη περίοδο αδράνειας.) Η

εποπτεία με κατάσταση σε ένα τείχος προστασίας εξετάζει ορισμένες τιμές στις κεφαλίδες TCP για να παρακολουθεί την κατάσταση κάθε σύνδεσης. Κάθε νέο πακέτο συγκρίνεται από το firewall με τον πίνακα κατάστασης του, για να καθοριστεί εάν η κατάσταση του πακέτου αντιφάσκει με την αναμενόμενη κατάσταση. Για παράδειγμα, ένας εισβολέας θα μπορούσε να δημιουργήσει ένα πακέτο με μια κεφαλίδα που υποδηλώνει ότι είναι μέρος μιας κατάστασης που έχει ήδη δημιουργηθεί, με την ελπίδα ότι θα περάσει από ένα firewall. Εάν το firewall χρησιμοποιεί εποπτεία με κατάσταση, θα ελέγξει πρώτα αν το πακέτο ανήκει σε μια ήδη δημιουργημένη σύνδεση που αναφέρεται στον πίνακα κατάστασης.

Στην απλούστερη περίπτωση, ένα firewall θα επιτρέψει τη διέλευση οποιουδήποτε πακέτου που φαίνεται να ανήκει σε μια ανοιχτή σύνδεση (ή ακόμη και σε μια σύνδεση που δεν έχει ακόμα δημιουργηθεί πλήρως). Ωστόσο, πολλά firewalls γνωρίζουν καλύτερα τις μηχανές κατάστασης για πρωτόκολλα όπως το TCP και το UDP, και θα φράξουν πακέτα που δεν συμμορφώνονται αυστηρά με την κατάλληλη μηχανή κατάστασης. Για παράδειγμα, είναι συνηθισμένο για τα firewalls να ελέγχουν χαρακτηριστικά όπως, οι αριθμοί ακολουθίας TCP και να απορρίπτουν πακέτα που είναι εκτός ακολουθίας. Όταν ένα προστατευτικό φράγμα παρέχει υπηρεσίες NAT, συχνά συμπεριλαμβάνει πληροφορίες NAT στον πίνακα κατάστασης του.

Επειδή ορισμένα πρωτόκολλα, κυρίως το UDP, είναι χωρίς σύνδεση και δεν διαθέτουν μια επίσημη διαδικασία για την αρχικοποίηση, τη δημιουργία και την τερματισμό μιας σύνδεσης, η κατάστασή τους δεν μπορεί να διαμορφωθεί στο επίπεδο μεταφοράς όπως για το TCP. Για αυτά τα πρωτόκολλα, τα περισσότερα τείχη προστασίας με εποπτεία κατάστασης είναι σε θέση να παρακολουθούν μόνο τις διευθύνσεις IP πηγής και προορισμού καθώς και τις θύρες. Τα πακέτα UDP πρέπει να αντιστοιχούν ακόμα σε μια καταχώριση στον πίνακα κατάστασης με βάση τις πληροφορίες διεύθυνσης IP πηγής και προορισμού και τις θύρες για να επιτραπεί η διέλευσή τους - για παράδειγμα, μια απάντηση DNS από μια εξωτερική πηγή θα επιτρεπόταν να περάσει μόνο αν το firewall είχε δει προηγουμένως μια αντίστοιχη ερώτηση DNS από μια εσωτερική πηγή. Δεδομένου ότι το firewall δεν είναι σε θέση να καθορίσει πότε έχει λήξει μια συνεδρία, η καταχώριση αφαιρείται από τον πίνακα κατάστασης μετά από ένα προπρογραμματισμένο χρονικό όριο που έχει οριστεί. Τα firewalls σε επίπεδο εφαρμογής που είναι σε θέση να αναγνωρίσουν το DNS μέσω του UDP θα τερματίσουν μια συνεδρία μετά την λήψη μιας απάντησης DNS, και μπορεί να ενεργήσουν παρόμοια με το πρωτόκολλο Network Time Protocol (NTP).

4.2.3 Τείχη προστασίας εφαρμογών

Μια πιο πρόσφατη τάση στην εποπτεία με κατάσταση είναι η προσθήκη μιας ικανότητας ανάλυσης πρωτοκόλλου με κατάσταση, που ορισμένοι προμηθευτές αναφέρουν ως βαθιά ανάλυση πακέτων. Η ανάλυση πρωτοκόλλου με κατάσταση βελτιώνει την τυπική εποπτεία με κατάσταση, προσθέτοντας τεχνολογία ανίχνευσης εισβολών - έναν μηχανισμό εποπτείας που αναλύει πρωτόκολλα στο επίπεδο εφαρμογής, για να συγκρίνει τα ανεπτυγμένα από τον προμηθευτή προφίλ της αγνής δραστηριότητας του πρωτοκόλλου με τα παρατηρούμενα γεγονότα, για την ανίχνευση αποκλίσεων. Αυτό επιτρέπει σε ένα τείχος προστασίας να επιτρέπει ή να αρνείται την πρόσβαση με βάση τον τρόπο με τον οποίο μια εφαρμογή λειτουργεί στο δίκτυο. Για παράδειγμα, ένα τείχος προστασίας εφαρμογής μπορεί να καθορίσει αν ένα μήνυμα ηλεκτρονικού ταχυδρομείου περιέχει έναν τύπο συνημμένου που ο οργανισμός δεν επιτρέπει (όπως ένα εκτελέσιμο αρχείο) ή αν χρησιμοποιείται άμεση ανταλλαγή μηνυμάτων (IM) μέσω της θύρας 80 (η οποία χρησιμοποιείται συνήθως για το

HTTP). Μια άλλη δυνατότητα είναι ότι μπορεί να αποκλείσει συνδέσεις στις οποίες εκτελούνται συγκεκριμένες ενέργειες (για παράδειγμα, οι χρήστες μπορεί να εμποδιστούν από τη χρήση της εντολής FTP "put," που επιτρέπει στους χρήστες να γράφουν αρχεία στο διακομιστή FTP). Αυτή η δυνατότητα μπορεί επίσης να χρησιμοποιηθεί για να επιτρέψει ή να απαγορεύσει ιστοσελίδες που περιέχουν συγκεκριμένους τύπους ενεργού περιεχομένου, όπως Java ή ActiveX, ή που διαθέτουν πιστοποιητικά SSL που έχουν υπογραφεί από συγκεκριμένη αρχή πιστοποίησης (CA), όπως μια αρχή πιστοποίησης με προβλήματα ή ανακλημένη.

Τα firewalls εφαρμογής μπορούν να επιτρέψουν την αναγνώριση απροσδόκητων ακολουθιών εντολών, όπως η επανάληψη της ίδιας εντολής ή η εκτέλεση μιας εντολής που δεν προηγήθηκε από άλλη εντολή από την οποία εξαρτάται. Αυτές οι ύποπτες εντολές προέρχονται συχνά από επιθέσεις buffer overflow, επιθέσεις DoS, κακόβουλο λογισμικό και άλλες μορφές επίθεσης που πραγματοποιούνται εντός πρωτοκόλλων εφαρμογής όπως το HTTP. Μια άλλη κοινή δυνατότητα είναι ο έλεγχος εισόδου για τις μεμονωμένες εντολές, όπως ελάχιστα και μέγιστα μήκη για τα ορίσματα. Για παράδειγμα, ένα όρισμα ονόματος χρήστη μήκους 1000 χαρακτήρων είναι ύποπτο - ακόμη περισσότερο αν περιέχει δυαδικά δεδομένα. Τα firewalls εφαρμογής είναι διαθέσιμα για πολλά κοινά πρωτόκολλα, συμπεριλαμβανομένων του HTTP, των βάσεων δεδομένων (όπως το SQL), των ηλεκτρονικών ταχυδρομείων (SMTP, Πρωτόκολλο Ταχυδρομείου [POP] και Πρωτόκολλο Πρόσβασης σε Μηνύματα στο Διαδίκτυο [IMAP]), της τηλεφωνίας μέσω διαδικτύου (VoIP) και της Επεκτάσιμης Σημαντικής Γλώσσας (XML).

Μια άλλη δυνατότητα που βρίσκεται σε ορισμένα firewalls εφαρμογής περιλαμβάνει την επιβολή μηχανών κατάστασης της εφαρμογής, οι οποίες είναι ουσιαστικά έλεγχοι της συμμόρφωσης της κίνησης με το πρότυπο για το εκάστοτε πρωτόκολλο. Αυτός ο έλεγχος συμμόρφωσης, ονομάζεται μερικές φορές "συμμόρφωση με το RFC" επειδή τα περισσότερα πρωτόκολλα καθορίζονται σε RFC που εκδίδονται από την Ομάδα Εργασίας για την Μηχανική του Διαδικτύου (IETF), μπορεί να είναι ένα αμφιλεγόμενο χαρακτηριστικό. Πολλά προϊόντα υλοποιούν πρωτόκολλα με τρόπους που πρακτικά, αλλά όχι εντελώς, ταιριάζουν με την προδιαγραφή, γι' αυτό συνήθως είναι απαραίτητο να επιτραπεί σε τέτοιες υλοποιήσεις να επικοινωνούν μέσω του firewall. Ο έλεγχος συμμόρφωσης είναι χρήσιμος μόνο όταν ανιχνεύει και αποκλείει επικοινωνίες που μπορεί να είναι επιβλαβείς για τα προστατευόμενα συστήματα.

Τα τείχη προστασίας που διαθέτουν τόσο ικανότητες εποπτείας με κατάσταση όσο και ανάλυσης πρωτοκόλλου με κατάσταση δεν είναι πλήρη συστήματα ανίχνευσης και πρόληψης εισβολών (IDPS), τα οποία συνήθως προσφέρουν πολύ πιο εκτεταμένες ικανότητες ανίχνευσης και πρόληψης επιθέσεων. Για παράδειγμα, τα IDPS χρησιμοποιούν επίσης ανάλυση βασισμένη σε υπογραφές και/ή ανωμαλίες για την ανίχνευση επιπρόσθετων προβλημάτων στην κυκλοφορία του δικτύου.

4.2.4 Πύλες πληρεξούσιων εφαρμογών

Ένα τείχος προστασίας εφαρμογής είναι μια δυνατότητα των προηγμένων τειχών προστασίας που συνδυάζει τον έλεγχο πρόσβασης σε χαμηλότερα επίπεδα με τη λειτουργικότητα σε υψηλότερα επίπεδα. Αυτά τα τείχη προστασίας περιέχουν ένα πράκτορα προξενητή που λειτουργεί ως μεσολαβητής μεταξύ δύο υπολογιστών που επιθυμούν να επικοινωνήσουν μεταξύ τους και δεν επιτρέπει ποτέ μια άμεση σύνδεση μεταξύ τους. Κάθε επιτυχημένη προσπάθεια σύνδεσης ουσιαστικά οδηγεί στη δημιουργία δύο ξεχωριστών συνδέσεων - μία μεταξύ του πελάτη και του διακομιστή προξενητή και μια άλλη μεταξύ του

διακομιστή προξενητή και του πραγματικού προορισμού. Ο προξενητής προορίζεται να είναι διαφανής για τους δύο υπολογιστές - από την άποψη τους υπάρχει μια άμεση σύνδεση. Επειδή οι εξωτερικοί υπολογιστές επικοινωνούν μόνο με τον πράκτορα προξενητή, οι εσωτερικές διευθύνσεις IP δεν είναι ορατές στον εξωτερικό κόσμο. Ο πράκτορας προξενητής διασυνδέεται απευθείας με τον σύνολο κανόνων του firewall για να καθορίσει εάν ένα συγκεκριμένο πακέτο δικτύου πρέπει να επιτραπεί να διασχίσει το firewall.

Εκτός από το σύνολο κανόνων, ορισμένοι πράκτορες προξενητή έχουν τη δυνατότητα να απαιτούν την ταυτοποίηση κάθε μεμονωμένου χρήστη δικτύου. Αυτή η ταυτοποίηση μπορεί να παίρνει πολλές μορφές, συμπεριλαμβανομένου του αναγνωριστικού χρήστη και του κωδικού πρόσβασης, του υλικού ή λογισμικού διακριτικού, της διεύθυνσης πηγής και της βιομετρίας.

Όπως και τα firewalls εφαρμογής, το proxy gateway λειτουργεί στο επίπεδο της εφαρμογής και μπορεί να επιθεωρήσει το πραγματικό περιεχόμενο της κυκλοφορίας. Αυτές οι πύλες πραγματοποιούν επίσης την αρχική χειραψία TCP με το σύστημα προέλευσης και μπορούν να προστατεύσουν από εκμεταλλεύσεις σε κάθε βήμα της επικοινωνίας. Επιπλέον, οι πύλες μπορούν να λαμβάνουν αποφάσεις για την έγκριση ή την απόρριψη της κυκλοφορίας με βάση πληροφορίες στις κεφαλίδες του πρωτοκόλλου εφαρμογής ή τα φορτία δεδομένων. Αφού η πύλη καθορίσει ότι τα δεδομένα πρέπει να επιτραπούν, αυτά προωθούνται προς τον προορισμό.

4.2.5 Εξειδικευμένοι διακομιστές μεσολάβησης

Οι εξειδικευμένοι διακομιστές μεσολάβησης διαφέρουν από τις προξενητικές πύλες εφαρμογής στο γεγονός ότι ενώ διατηρούν τον προξενητικό έλεγχο της κυκλοφορίας, συνήθως έχουν πολύ περιορισμένες δυνατότητες σαν ένα τείχος προστασίας. Περιγράφονται σε αυτήν την ενότητα λόγω της στενής σχέσης τους με τα τείχη προστασίας πληρεξούσιας εφαρμογής. Πολλοί εξειδικευμένοι διακομιστές προξενητή είναι ειδικοί σε εφαρμογές και ορισμένοι πραγματικά πραγματοποιούν ανάλυση και επικύρωση των συνηθισμένων πρωτοκόλλων εφαρμογής, όπως το HTTP. Επειδή αυτοί οι διακομιστές έχουν περιορισμένες δυνατότητες προστατευτικού φραγμού, όπως απλώς τον αποκλεισμό της κυκλοφορίας με βάση την πηγή ή τον προορισμό της, συνήθως τοποθετούνται πίσω από παραδοσιακά τείχη προστασίας. Συνήθως, ένα κύριο τείχος προστασίας θα μπορούσε να δέχεται εισερχόμενη κυκλοφορία, να καθορίζει ποια εφαρμογή στοχεύεται και να παραδίδει την κυκλοφορία στον κατάλληλο αφιερωμένο διακομιστή προξενητή (π.χ., διακομιστής ηλεκτρονικού ταχυδρομείου). Αυτός ο διακομιστής θα πραγματοποιούσε λειτουργίες φιλτραρίσματος ή καταγραφής στην κυκλοφορία, και στη συνέχεια θα την προωθούσε στα εσωτερικά συστήματα. Ένας διακομιστής προξενητής θα μπορούσε επίσης να δέχεται εξερχόμενη κυκλοφορία απευθείας από τα εσωτερικά συστήματα, να φιλτράρει ή να καταγράφει την κυκλοφορία και να την προωθεί στο τείχος προστασίας για εξερχόμενη παράδοση. Ένα παράδειγμα αυτού είναι ένας προξενητικός διακομιστής HTTP που τοποθετείται πίσω από το firewall - οι χρήστες θα χρειαζόταν να συνδεθούν σε αυτόν τον προξενητικό διακομιστή προτού συνδεθούν με εξωτερικούς διακομιστές ιστού. Οι αφιερωμένοι διακομιστές προξενητή χρησιμοποιούνται συνήθως για να μειώσουν το φόρτο εργασίας του προστατευτικού φράγματος και να πραγματοποιήσουν εξειδικευμένο φιλτράρισμα και καταγραφή που ενδέχεται να είναι δύσκολο να πραγματοποιηθεί απευθείας στο προστατευτικό φράγμα.

Τα τελευταία χρόνια, η χρήση των εισερχόμενων διακομιστών προζενιτή έχει μειωθεί δραματικά. Αυτό συμβαίνει επειδή ένας εισερχόμενος διακομιστής προζενιτή πρέπει να μιμείται τις δυνατότητες του πραγματικού διακομιστή που προστατεύει, κάτι που γίνεται σχεδόν αδύνατο όταν πρέπει να προστατεύσει ένα διακομιστή με πολλά χαρακτηριστικά. Η χρήση ενός διακομιστή προζενιτή με λιγότερες δυνατότητες από τον διακομιστή που προστατεύει καθιστά τις μη ταιριαστές δυνατότητες άχρηστες. Επιπλέον, τα βασικά χαρακτηριστικά που θα έπρεπε να έχουν οι εισερχόμενοι διακομιστές προζενιτή (καταγραφή, έλεγχος πρόσβασης κλπ.) συνήθως είναι ενσωματωμένα στους πραγματικούς διακομιστές. Οι περισσότεροι διακομιστές προζενιτή που χρησιμοποιούνται τώρα είναι εξερχόμενοι διακομιστές προζενιτή, με τους πιο συνηθισμένους να είναι οι προζενιτές HTTP.

4.2.6 Εικονικά ιδιωτικά δίκτυα - VPN

Οι συσκευές firewall στα όρια ενός δικτύου καλούνται ενίοτε να πραγματοποιούν περισσότερες ενέργειες εκτός από τον αποκλεισμό ανεπιθύμητης κυκλοφορίας. Ένα κοινό αίτημα για αυτά τα προστατευτικά φράγματα είναι η κρυπτογράφηση και αποκρυπτογράφηση συγκεκριμένων ροών κυκλοφορίας δικτύου μεταξύ του προστατευμένου δικτύου και των εξωτερικών δικτύων. Αυτό σχεδόν πάντα περιλαμβάνει εικονικά ιδιωτικά δίκτυα (VPN), τα οποία χρησιμοποιούν επιπρόσθετα πρωτόκολλα για την κρυπτογράφηση της κυκλοφορίας και την παροχή αυθεντικοποίησης χρηστών και ελέγχου ακεραιότητας. Τα VPN χρησιμοποιούνται συνήθως για την παροχή ασφαλών επικοινωνιών δικτύου σε μη αξιόπιστα δίκτυα. Για παράδειγμα, η τεχνολογία VPN χρησιμοποιείται ευρέως για την επέκταση του προστατευμένου δικτύου ενός οργανισμού με πολλαπλές τοποθεσίες μέσω του Internet και, πρόσθετα, για την παροχή ασφαλούς απομακρυσμένης πρόσβασης χρηστών στα εσωτερικά οργανωτικά δίκτυα μέσω του Internet. Δύο συνηθισμένες επιλογές για ασφαλή VPN είναι το IPsec και το Secure Sockets Layer (SSL)/Transport Layer Security (TLS).

Οι δύο πιο συνηθισμένες αρχιτεκτονικές VPN είναι η αρχιτεκτονική από πύλη σε πύλη και η αρχιτεκτονική από υπολογιστή σε πύλη. Η αρχιτεκτονική από πύλη σε πύλη συνδέει πολλές σταθερές τοποθεσίες μέσω δημόσιων γραμμών χρησιμοποιώντας τύλες VPN - για παράδειγμα, για να συνδέσει γραφεία υποκαταστημάτων με το κεντρικό γραφείο ενός οργανισμού. Μια πύλη VPN είναι συνήθως μέρος ενός άλλου δικτυακού εξοπλισμού, όπως ενός τείχους προστασίας ή ενός δρομολογητή. Όταν εδραιώνεται μια σύνδεση VPN μεταξύ των δύο πυλών, οι χρήστες στις τοποθεσίες υποκαταστημάτων δεν γνωρίζουν τη σύνδεση και δεν απαιτούν ειδικές ρυθμίσεις στους υπολογιστές τους. Ο δεύτερος τύπος αρχιτεκτονικής, από υπολογιστή σε πύλη, παρέχει ασφαλή σύνδεση στο δίκτυο για ατομικούς χρήστες, συνήθως ονομάζονται απομακρυσμένοι χρήστες, οι οποίοι βρίσκονται έξω από τον οργανισμό (στο σπίτι, σε ένα ξενοδοχείο κλπ). Εδώ, ένας πελάτης στον υπολογιστή του χρήστη διαπραγματεύεται την ασφαλή σύνδεση με την πύλη VPN του οργανισμού. Για τις αρχιτεκτονικές VPN από πύλη σε πύλη και από υπολογιστή σε πύλη, η λειτουργικότητα του VPN είναι συχνά μέρος του firewall του ίδιου. Τοποθετώντας το πίσω από το firewall θα απαιτούσε τη διέλευση της κυκλοφορίας του VPN μέσα από το προστατευτικό φράγμα ενώ είναι κρυπτογραφημένη, εμποδίζοντας το firewall από τον έλεγχο της κυκλοφορίας.

Όλες οι απομακρυσμένες συνδέσεις (από υπολογιστή σε πύλη) VPN επιτρέπουν στον διαχειριστή του firewall να αποφασίσει ποιοι χρήστες έχουν πρόσβαση σε ποιους πόρους του δικτύου. Ο έλεγχος αυτής της πρόσβασης είναι συνήθως διαθέσιμος ανά χρήστη και ανά ομάδα· δηλαδή, η πολιτική VPN μπορεί να καθορίσει ποιοι χρήστες και ομάδες είναι εξουσιοδοτημένοι να έχουν πρόσβαση σε ποιους πόρους, αν ένας οργανισμός χρειάζεται αυτό

το επίπεδο λεπτομέρειας. Οι VPN βασίζονται συνήθως σε πρωτόκολλα πιστοποίησης όπως το Remote Authentication Dial In User Service (RADIUS). Το RADIUS χρησιμοποιεί διάφορα είδη διαπιστευτηρίων πιστοποίησης, με τα πιο συνηθισμένα παραδείγματα να είναι το όνομα χρήστη και ο κωδικός πρόσβασης, ψηφιακές υπογραφές και υλικά tokens. Ένα άλλο πρωτόκολλο πιστοποίησης που χρησιμοποιείται συχνά από τα VPN είναι το Lightweight Directory Access Protocol (LDAP)· είναι ιδιαίτερα χρήσιμο για τη λήψη αποφάσεων πρόσβασης για τους ατομικούς χρήστες και τις ομάδες.

Για να εκτελεστεί η λειτουργία VPN σε ένα τείχος προστασίας απαιτούνται επιπλέον πόροι που εξαρτώνται από τον όγκο της κυκλοφορίας που περνά μέσω του VPN και τον τύπο κρυπτογράφησης που χρησιμοποιείται. Για ορισμένα περιβάλλοντα, η επιπλέον κυκλοφορία που σχετίζεται με τα VPN μπορεί να απαιτήσει επιπλέον σχεδιασμό χωρητικότητας και πόρων. Επιπλέον, απαιτείται σχεδιασμός για τον καθορισμό του τύπου του VPN (από πύλη σε πύλη και/ή από υπολογιστή σε πύλη) που πρέπει να συμπεριληφθεί στο προστατευτικό φράγμα. Πολλά τείχη προστασίας περιλαμβάνουν υλικό επιτάχυνσης για την κρυπτογράφηση προκειμένου να ελαχιστοποιήσουν τον αντίκτυπο των υπηρεσιών VPN.

4.2.7 Έλεγχος πρόσβασης δικτύου

Άλλη μια συνηθισμένη απαίτηση για τα τείχη προστασίας στο όριο ενός δικτύου είναι να πραγματοποιούν ελέγχους πελατών για εισερχόμενες συνδέσεις από απομακρυσμένους χρήστες και να επιτρέπουν ή να απαγορεύουν την πρόσβαση με βάση αυτούς τους ελέγχους. Αυτός ο έλεγχος, που συνήθως ονομάζεται Έλεγχος Πρόσβασης Δικτύου (NAC) ή Προστασία Πρόσβασης Δικτύου (NAP), επιτρέπει την πρόσβαση με βάση τα διαπιστευτήρια του χρήστη και τα αποτελέσματα από την πραγματοποίηση "ελέγχων υγείας" στον υπολογιστή του χρήστη. Οι έλεγχοι υγείας συνήθως αποτελούνται από τον έλεγχο ότι ένας ή περισσότεροι από τους ακόλουθους συμμορφώνονται με την πολιτική του οργανισμού:

- Τελευταίες ενημερώσεις στο λογισμικό antimalware και προσωπικού τείχους προστασίας.
- Ρυθμίσεις διαμόρφωσης για το λογισμικό antimalware και για το λογισμικό προσωπικού τείχους προστασίας.
- Χρόνος που έχει παρέλθει από τον προηγούμενο έλεγχο για κακόβουλο λογισμικό.
- Επίπεδο ενημέρωσης του λειτουργικού συστήματος και επιλεγμένων εφαρμογών.
- Διαμόρφωση της ασφάλειας του λειτουργικού συστήματος και των επιλεγμένων εφαρμογών.

Αυτοί οι έλεγχοι υγείας απαιτούν λογισμικό στο σύστημα του χρήστη που ελέγχεται από το προστατευτικό φράγμα. Αν ο χρήστης έχει αποδεκτά διαπιστευτήρια αλλά η συσκευή δεν περνά τον έλεγχο υγείας, ο χρήστης και η συσκευή ενδέχεται να έχουν μόνο περιορισμένη πρόσβαση στο εσωτερικό δίκτυο για σκοπούς αποκατάστασης.

4.2.8 Ενοποιημένη διαχείριση απειλών (UTM)

Πολλά τείχη προστασίας συνδυάζουν πολλά χαρακτηριστικά σε ένα μόνο σύστημα, με την ιδέα ότι είναι πιο εύκολο να ορίσουν και να διατηρήσουν πολιτικές σε ένα μόνο σύστημα αντί σε πολλά συστήματα που είναι εγκατεστημένα στον ίδιο τόπο ενός δικτύου. Ένα τυπικό σύστημα ενοποιημένης διαχείρισης απειλών (UTM) διαθέτει ένα προστατευτικό

φράγμα, ανίχνευση και εξάλειψη κακόβουλου λογισμικού, ανίχνευση και αποκοπή ύποπτων δικτυακών εξερευνήσεων και άλλα. Υπάρχουν πλεονεκτήματα και ανεπιθύμητες πλευρές στο να συγχωνεύονται πολλές λειτουργίες που δεν είναι εντελώς συσχετισμένες σε ένα μόνο σύστημα. Για παράδειγμα, η υλοποίηση ενός UTM μειώνει την πολυπλοκότητα καθιστώντας ένα μόνο σύστημα υπεύθυνο για πολλούς στόχους ασφαλείας, αλλά απαιτεί επίσης από το UTM να διαθέτει όλα τα επιθυμητά χαρακτηριστικά για την εκπλήρωση κάθε στόχου. Άλλος συμβιβασμός αφορά την απόδοση: ένα μόνο σύστημα που αντιμετωπίζει πολλές εργασίες πρέπει να έχει αρκετούς πόρους, όπως ταχύτητα CPU και μνήμη, για να αντιμετωπίσει κάθε εργασία που του ανατίθεται. Ορισμένοι οργανισμοί θα βρουν την ισορροπημένη εύνοια ενός UTM, ενώ άλλοι οργανισμοί θα χρησιμοποιούν πολλά προστατευτικά τείχη στον ίδιο τόπο στο δίκτυό τους.

4.2.9 Τείχη προστασίας εφαρμογών ιστού

Το πρωτόκολλο HTTP που χρησιμοποιείται στους διακομιστές ιστού έχει εκμεταλλευτεί από επιτιθέμενους με διάφορους τρόπους, όπως τοποθέτηση κακόβουλου λογισμικού στον υπολογιστή ενός χρήστη περιήγησης στον ιστό, ή τον αποκλεισμό κάποιου ώστε να αποκαλύψει ιδιωτικές πληροφορίες που ίσως δεν θα έκανε αλλιώς. Πολλές από αυτές τις εκμεταλλεύσεις μπορούν να ανιχνευθούν από εξειδικευμένα τείχη προστασίας εφαρμογών που ονομάζονται προστατευτικά τείχη εφαρμογών ιστού που βρίσκονται μπροστά από τον διακομιστή ιστού.

Τα τείχη προστασίας εφαρμογών ιστού είναι μια σχετικά νέα τεχνολογία σε σύγκριση με άλλες τεχνολογίες προστατευτικών τειχών, και οι τύποι απειλών που αντιμετωπίζουν αλλάζουν συχνά. Διότι τοποθετούνται μπροστά από τους διακομιστές ιστού για να αποτρέψουν επιθέσεις στο διακομιστή, συχνά θεωρούνται πολύ διαφορετικά από τα παραδοσιακά τείχη προστασίας.

4.2.10 Τείχη προστασίας για εικονικές δομές

Πολλές λύσεις εικονικοποίησης επιτρέπουν την ταυτόχρονη λειτουργία περισσότερων από ενός λειτουργικών συστημάτων σε έναν μόνο υπολογιστή, καθένα από αυτά φαίνεται ως να ήταν ένας πραγματικός υπολογιστής. Αυτό έχει γίνει δημοφιλές πρόσφατα, καθώς επιτρέπει στους οργανισμούς να κάνουν πιο αποδοτική χρήση του υλικού υπολογιστή. Οι περισσότεροι από αυτούς τους τύπους εικονικοποίησης περιλαμβάνουν εικονικά δίκτυα, τα οποία επιτρέπουν τα πολλαπλά λειτουργικά συστήματα να επικοινωνούν ως να ήταν σε ένα τυπικό Ethernet, παρόλο που δεν υπάρχει πραγματικό υλικό δικτύωσης.

Δραστηριότητες δικτύου που διέρχονται απευθείας μεταξύ εικονικών λειτουργικών συστημάτων εντός ενός κεντρικού υπολογιστή δεν μπορούν να παρακολουθηθούν από ένα εξωτερικό τείχος προστασίας. Ωστόσο, ορισμένα συστήματα εικονικοποίησης προσφέρουν ενσωματωμένα τείχη προστασίας ή επιτρέπουν την προσθήκη τειχών προστασίας λογισμικού από τρίτους ως πρόσθετα. Η χρήση firewalls για την παρακολούθηση των εικονικών δικτύων αποτελεί ένα σχετικά νέο πεδίο της τεχνολογίας firewalls και πιθανόν να αλλάξει σημαντικά καθώς η χρήση της εικονικοποίησης συνεχίζει να αυξάνεται [94.1].

4.3 Αυθεντικοποίηση – ταυτοποίηση χρήστη και τεχνικές

Ένας τρόπος για να εξασφαλιστεί η ασφάλεια των υπολογιστικών συστημάτων είναι η αυθεντικοποίηση και η ταυτοποίηση του χρήστη. Με τον όρο ταυτοποίηση ενός χρήστη (user identification) αναφερόμαστε στην μέθοδο στην οποία, ένα υπολογιστικό σύστημα ζητά από τον χρήστη κάποιες πληροφορίες που μόνο ο συγκεκριμένος χρήστης γνωρίζει, έτσι ώστε

να επιτραπεί στον χρήστη να χρησιμοποιήσει αυτό το υπολογιστικό σύστημα. Συνήθως οι πληροφορίες που ζητούνται από έναν χρήστη κατά την ταυτοποίησή του είναι κάποιος μοναδικός κωδικός (pin) ή κάποιος κωδικός πρόσβασης. Αυθεντικοποίηση είναι η μέθοδος που ο χρήστης χρειάζεται να παρέχει συμπληρωματικές πληροφορίες στο υπολογιστικό σύστημα, με τις οποίες θα εξεταστεί η αυθεντικότητα της ταυτοποίησής του. Πλέον, η χρήση κωδικών πρόσβασης για την ταυτοποίηση των χρηστών είναι αναπόσπαστο κομμάτι των υπολογιστικών συστημάτων λόγω της απλότητάς τους αλλά και της μεγάλης ασφάλειας που παρέχουν [93][95].

Οι τεχνικές αυθεντικοποίησης χωρίζονται με βάση τα εξής χαρακτηριστικά :

- **Κάτι που ο χρήστης γνωρίζει (Something You Know).** Εδώ εντάσσονται κωδικοί πρόσβασης (passwords), κωδικοί PIN(Personal Identification Number), κρυπτογραφικό κλειδί, μοτίβα αφής κ.α. Αυτά τα τεκμήρια αυθεντικοποίησης μπορούν εύκολα να τροποποιηθούν αλλά δεν χάνονται και δεν κλέβονται. Παρά την απλή και εύκολη χρήση τους, ο συνδυασμός των γραμμάτων και των αριθμών είναι πολύ πιθανό να είναι μοναδικός, οπότε είναι δύσκολη η αποκάλυψή τους.
- **Κάτι που ο χρήστης κατέχει (Something You Have).** Εδώ εντάσσονται οι συσκευές PDA, μνήμες USB flash που περιέχουν ψηφιακές υπογραφές, έξυπνες κάρτες, ψηφιακά πιστοποιητικά κ.α. Επειδή πρόκειται για αντικείμενα σε αυτή την περίπτωση, η αντιγραφή τους είναι αδύνατο να πραγματοποιηθεί. Αυτό συμβαίνει επειδή η κατασκευή τους γίνεται με ειδικά υλικά τα οποία δεν είναι ευρέως διαθέσιμα. Παρ' όλα αυτά επειδή το κόστος αυτών των αντικειμένων είναι μεγάλο, είναι πολύ πιθανό να χαθούν και να κλαπούν.
- **Κάτι που είναι ο χρήστης (Something You Are).** Εδώ εντάσσονται χαρακτηριστικά βιομετρικής φύσης όπως δακτυλικά αποτυπώματα, διαστάσεις παλάμης – χεριού, χαρακτηριστικά προσώπου, χαρακτηριστικά ματιού όπως οι διαστάσεις ίριδας σάρωση αμφιβληστροειδή χιτώνα και γεωμετρία φλεβών. Επίσης εδώ εντάσσονται τα φωνητικά χαρακτηριστικά όπως η συχνότητα ταλάντωσης των φωνητικών χορδών αλλά και ο γραφικός χαρακτήρας καθώς ο κάθε άνθρωπος έχει ξεχωριστό γραφικό χαρακτήρα.
- **Κάπου που είναι ο χρήστης.** Εδώ εντάσσονται χαρακτηριστικά τοποθεσίας που βρίσκεται ο χρήστης όπως η διεύθυνση IP.
- **Συνδυασμός όλων των παραπάνω τεχνικών** [95][96][97].

Οι μηχανισμοί αυθεντικοποίησης αποτελούν έναν κύριο στόχο για κάθε επιτιθέμενο, διότι η παραβίασή τους οδηγεί στην κλοπή ταυτότητας και την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε πολύτιμους πόρους του οργανισμού. Υπάρχουν ποικίλοι τρόποι με τους οποίους κάποιος μπορεί να αποκτήσει τα διαπιστευτήρια για έναν λογαριασμό χρήστη:

- Αδύναμοι κωδικοί πρόσβασης. Οι περισσότεροι χρήστες χρησιμοποιούν εύκολα θυμώμενες λέξεις ως συνθηματικά (passwords), τα οποία μπορούν να αποκτηθούν εύκολα μέσω λεξικογραφικής επίθεσης (dictionary attack).
- Ο χρήστης να αποθηκεύει τους κωδικούς του με ανεπαρκή ασφάλεια.
- Χρήση μη ασφαλών μεθόδων κρυπτογράφησης για τη φύλαξη των κωδικών στα συστήματα.
- Κλοπή του συνθηματικού από τον προσωπικό λογαριασμό ενός χρήστη, το οποίο ωστόσο χρησιμοποιεί το ίδιο συνθηματικό σε έναν επαγγελματικό λογαριασμό.

- Εξαπάτηση του χρήστη μέσω της τεχνικής της κοινωνικής μηχανικής, με στόχο να τον πείσει να αποκαλύψει τα στοιχεία πρόσβασης του, για παράδειγμα, μέσω μιας πλαστής online φόρμας στην οποία ανακατευθύνεται ο χρήστης μέσω ενός συνδέσμου που του έχει σταλεί μέσω phishing email.
- Χρήση κακόβουλου λογισμικού (malware) που εξάγει κωδικούς πρόσβασης από τη μνήμη του υπολογιστή ή το δίκτυο.

Η χρήση διπλής αυθεντικοποίησης αναμφίβολα αυξάνει την ασφάλεια, καθώς προσθέτει έναν επιπρόσθετο παράγοντα, μαζί με τον κωδικό πρόσβασης, κατά την επαλήθευση της ταυτότητας ενός χρήστη. Ωστόσο, η αποστολή κειμένου μέσω SMS είναι πλέον ευαίσθητη σε διάφορα είδη επιθέσεων, με την πιο γνωστή μορφή να είναι η μεθοδολογία του SIM swapping. Πολύ πιο ασφαλής εναλλακτική είναι η χρήση μιας κινητής εφαρμογής που δημιουργεί μιας χρήσης κωδικούς πρόσβασης (one-time passwords) στη συσκευή του χρήστη, χωρίς να χρειάζεται να μεταδοθεί κάτι μέσω του δικτύου και τους κινδύνους που αυτό συνεπάγεται. Παραδείγματα γνωστών εφαρμογών με αυτή τη λειτουργία περιλαμβάνουν το Google Authenticator, το LastPass, το Authy και άλλες [97.1].

Η διπλή αυθεντικοποίηση – 2 factors authentication (2FA) προσφέρει πολλά πλεονεκτήματα σε άτομα και οργανισμούς που επιδιώκουν να προστατεύσουν τα ευαίσθητα δεδομένα και τους λογαριασμούς τους από κυβερνοεπιθέσεις. Παρακάτω αναφέρονται ορισμένα από τα κύρια πλεονεκτήματα της 2FA:

1. Ενισχυμένη ασφάλεια: Η 2FA μέθοδος παρέχει ένα επιπλέον επίπεδο ασφάλειας πέραν του απλού συνδυασμού χρήστη και κωδικού πρόσβασης, καθιστώντας πολύ πιο δύσκολο για χάκερς ή κυβερνοεγκληματίες να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στον λογαριασμό ή τη συσκευή ενός χρήστη.
2. Προστασία από κλοπή κωδικού πρόσβασης: Ακόμη κι αν ένας χάκερ καταφέρει να αποκτήσει τον κωδικό πρόσβασης ενός χρήστη, θα χρειαστεί ακόμη τον δεύτερο παράγοντα αυθεντικοποίησης για να αποκτήσει πρόσβαση στον λογαριασμό. Αυτό καθιστά πολύ πιο δύσκολο για τους χάκερς να χρησιμοποιήσουν κλεμμένους κωδικούς πρόσβασης για να αποκτήσουν πρόσβαση σε λογαριασμούς χρηστών.
3. Εύκολη χρήση: Πολλές μέθοδοι 2FA είναι εύκολες στη χρήση και απαιτούν ελάχιστη προσπάθεια από τους χρήστες, όπως η λήψη ενός κωδικού μιας χρήσης μέσω μηνύματος κειμένου ή τη χρήση αναγνώστη αποτυπωμάτων.
4. Συμβατή με πολλές συσκευές: Η 2FA μπορεί να χρησιμοποιηθεί με πολλές συσκευές, συμπεριλαμβανομένων smartphones, tablets και υπολογιστών, καθιστώντας την μια ευέλικτη και ευρέως διαθέσιμη λύση ασφαλείας.
5. Συμμόρφωση με τους κανονισμούς: Σε ορισμένες βιομηχανίες και οργανισμούς επιβάλλεται από το νόμο η υλοποίηση επιπλέον μέτρων ασφαλείας για την προστασία ευαίσθητων δεδομένων. Η 2FA μπορεί να συμβάλει στην εκπλήρωση αυτών των κανονιστικών απαιτήσεων.
6. Μείωση απάτης και μη εξουσιοδοτημένης πρόσβασης: Η 2FA μπορεί να συμβάλει στην πρόληψη πολλών τύπων κυβερνοεπιθέσεων, συμπεριλαμβανομένων αποπειρών απάτης μέσω ψαρέματος (phishing), επιθέσεων με κακόβουλο λογισμικό (malware) και επιθέσεων man-in-the-middle, μειώνοντας τον κίνδυνο απάτης και μη εξουσιοδοτημένης πρόσβασης σε ευαίσθητα δεδομένα [97.2].

Η ταυτοποίηση χρήστη είναι ένας τρόπος για να επιβεβαιώσουμε την ταυτότητα ενός ατόμου και να διασφαλίσουμε ότι οι πληροφορίες που λαμβάνουμε από αυτόν είναι

αξιόπιστες. Η ταυτοποίηση μπορεί να βοηθήσει στην αποτροπή κυβερνοεπιθέσεων, καθώς μπορεί να διασφαλίσει ότι οι πληροφορίες που λαμβάνουμε δεν προέρχονται από κακόβουλους χρήστες. Επιπλέον, η ταυτοποίηση μπορεί να βοηθήσει στη διαχείριση των δικαιωμάτων πρόσβασης, και να διασφαλίσει ότι μόνο εξουσιοδοτημένα άτομα έχουν πρόσβαση σε ευαίσθητες πληροφορίες [97.3] [97.4] [97.5].

4.4 Κρυπτογραφία

Η κρυπτογραφία είναι από τους σημαντικότερους πυλώνες της ασφάλειας ενός υπολογιστικού συστήματος. Από πολύ νωρίς ο άνθρωπος αναγνώρισε την αξία που έχει μια πληροφορία και προσπάθησε από την αρχαιότητα να βρει τρόπους με τους οποίους να κρύψει την πληροφορία ακόμα και αν αυτή έπεφτε σε χέρια ανεπιθύμητων. Από την αρχαιότητα μέχρι σήμερα, η σημαντικότητα της κρυπτογραφίας είναι τόσο μεγάλη που πλέον η κρυπτογραφία είναι μια επιστήμη από μόνη που βασίζεται στα μαθηματικά και χρησιμοποιείται στην επιστήμη της πληροφορικής και των τηλεπικοινωνιών. Για παράδειγμα, ένας χρήστης μιας εφαρμογής άμεσης αποστολής μηνυμάτων, όταν στέλνει ένα μήνυμα δεν γνωρίζει ότι το μήνυμά του κρυπτογραφείται από την ίδια την συσκευή από την οποία το στέλνει, έτσι ώστε να μην γίνει αντιληπτό το μήνυμα από κάποιον άλλο παρά μόνο από τον συνομιλητή του.

Η λέξη κρυπτογραφία είναι σύνθεση των λέξεων, «κρυπτός» + «γράφω» και είναι ο επιστημονικός τομέας εκείνος, που προσπαθεί να βρει μεθόδους και τεχνικές για την απόκρυψη των πληροφοριών, όπως αναφέραμε και παραπάνω το περιεχόμενο ενός μηνύματος. Η κρυπτογραφία είναι ένας από τους δύο επιστημονικούς τομείς της ευρύτερης επιστήμης της κρυπτολογίας. Ο άλλος τομέας της κρυπτολογίας που μπορεί να θεωρηθεί το αντίθετο της κρυπτογραφίας είναι η κρυπτανάλυση, η οποία ασχολείται με μεθόδους και τεχνικές με τις οποίες θα μπορούσε να αποκρυπτογραφηθεί η κρυπτογραφημένη πληροφορία. Η κρυπτογραφία παρέχει τέσσερις λειτουργίες ασφαλείας :

1. **Εμπιστευτικότητα (confidentiality).** Η πληροφορία που μεταδίδεται είναι προσβάσιμη μόνο από εξουσιοδοτημένα μέλη, ενώ όταν πέσει σε χέρια μη εξουσιοδοτημένου ατόμου δεν είναι δυνατή η κατανόησή της.
2. **Ακεραιότητα (integrity).** Η πληροφορία μπορεί να τροποποιηθεί μόνο από τα εξουσιοδοτημένα μέλη και αν αυτή τροποποιηθεί είναι εμφανείς οι αλλαγές.
3. **Αυθεντικοποίηση / πιστοποίηση (authentication).** Όλα τα μέλη που παίρνουν μέρος στην επικοινωνία, δηλαδή και ο αποστολέας ενός μηνύματος και ο παραλήπτης, θα πρέπει να μπορούν να επιβεβαιώσουν τις ταυτότητές τους και ότι δεν είναι πλαστές, αλλά και από πού προέρχεται και που πρέπει να πάει το μήνυμα που περιέχει την πληροφορία.
4. **Αδυναμία αποποίησης – μη απάρνηση (non-repudiation).** Τα μέλη που συμμετέχουν στην επικοινωνία, είτε ο αποστολέας της πληροφορίας, είτε ο παραλήπτης, δεν έχουν την δυνατότητα να αρνηθούν την αυθεντικότητα της μετάδοσης της πληροφορίας ή την αυθεντικότητα της δημιουργίας της.

Η ιστορία της κρυπτογραφίας χωρίζεται σε τρεις χρονικές περιόδους. Η πρώτη και η μεγαλύτερη περίοδος είναι μεταξύ του 1900 π.Χ και 1900 μ.Χ, όπου σε αυτή την περίοδο οι διαδικασίες της κρυπτογράφησης γινόντουσαν αποκλειστικά με χαρτί και μελάνι. Οι διαδικασίες αυτές επικεντρώνονταν στην αντικατάσταση και στην αναδιάταξη των γραμμάτων του αλφαβήτου. Η δεύτερη περίοδος είναι από το 1900 μ.Χ έως το 1950 μ.Χ, στην οποία γίνεται χρήση κρυπτογραφικών μηχανών, κυρίως κατά την διάρκεια του Β΄

παγκοσμίου πολέμου, με χαρακτηριστικό παράδειγμα η κρυπτογραφική μηχανή που χρησιμοποιούσαν οι Γερμανοί με την ονομασία Enigma. Η τρίτη και τελευταία περίοδος της κρυπτογραφίας είναι από το 1950 μ.Χ έως και σήμερα. Η τελευταία αυτή περίοδος χαρακτηρίζεται από την εξέλιξη της κρυπτογραφίας, ως αποτέλεσμα της εξέλιξης των μαθηματικών και της εμφάνισης των υπολογιστών οι οποίοι επέτρεψαν την χρήση πιο περίπλοκων αλγορίθμων κρυπτογράφησης.

Η σημερινή μορφή που έχουν τα κρυπτογραφικά συστήματα οφείλεται κυρίως σε δύο πρόσωπα που ασχολήθηκαν με έρευνες στον τομέα της κρυπτογραφίας, ο Kerckhoff και ο Shannon. Ο Kerckhoff ανέφερε τα πρότυπα σχεδίασης που πρέπει να έχει ένα κρυπτογραφικό σύστημα και που από τότε κάθε κρυπτογραφικό σύστημα ακολουθεί πιστά. Τα πρότυπα αυτά ανέφεραν ότι η ασφάλεια ενός συστήματος πρέπει να εξαρτάται μόνο στην μυστικότητα του κλειδιού και δεν πρέπει να εξαρτάται στην μυστικότητα του αλγορίθμου που χρησιμοποιείται για την κρυπτογράφηση. Η δεύτερη έρευνα που ανήκει στον πατέρα της επιστήμης της Θεωρίας της Πληροφορίας, Shannon, έθεσε την κρυπτογραφία ως ξεχωριστή επιστήμη και βοήθησε στην γρήγορη εξέλιξή της από τα μέσα του 20^{ου} αιώνα και μετά. Στον Shannon και στην έρευνά του βασίστηκαν όλοι οι σύγχρονοι κρυπτογραφικοί αλγόριθμοι. Στην σύγχρονη περίοδο της κρυπτογραφίας σημαντική στιγμή υπήρξε η έρευνα των Diffie – Hellman το 1976, οι οποίοι πρότειναν την κρυπτογράφηση δημοσίου κλειδιού ως μια νέα μέθοδος κρυπτογράφησης. Αυτή η μέθοδος κάνει προβλήματα όπως η ασφαλή ανταλλαγή κλειδιού και η πιστοποίηση ταυτότητας των χρηστών να ξεπεραστούν. Επίσης, καθορίστηκαν και οι παρακάτω ιδιότητες που θα πρέπει να έχει ένα κρυπτοσύστημα :

- Το κρυπτοσύστημα θα πρέπει να χρησιμοποιεί αποδοτικούς αλγόριθμους για την κρυπτογράφηση και την αποκρυπτογράφηση.
- Το κρυπτοσύστημα πρέπει να είναι εύκολο ως προς την χρήση του.
- Η προστασία που παρέχει το κρυπτοσύστημα θα πρέπει να βασίζεται μόνο στην μυστικότητα του κλειδιού και όχι στην μυστικότητα των αλγορίθμων κρυπτογράφησης που χρησιμοποιεί το κρυπτοσύστημα (αρχή Kerckhoff).

Η διαδικασία μετατροπής ενός αρχικού κειμένου εισόδου (plaintext) σε κρυπτογραφημένο κείμενο (ciphertext) ονομάζεται κρυπτογράφηση (encryption), ενώ η διαδικασία μετατροπής του κρυπτογραφημένου κειμένου σε απλό κείμενο ονομάζεται αποκρυπτογράφηση (decryption). Οι διαδικασίες της κρυπτογράφησης και της αποκρυπτογράφησης γίνονται μέσω ειδικών αλγορίθμων και των κατάλληλων κλειδιών που χρειάζονται. Ένα κρυπτογραφικό σύστημα αποτελείται από έναν αλγόριθμο κρυπτογράφησης και έναν αλγόριθμο αποκρυπτογράφησης και μια τεχνική κατασκευής κλειδιού. Η κρυπτογραφία αποτελείται από δύο είδη κρυπτογράφησης. Το ένα είδος ονομάζεται συμβατική ή συμμετρική κρυπτογράφηση και το άλλο είδος ονομάζεται ασύμμετρη κρυπτογράφηση ή κρυπτογράφηση δημοσίου κλειδιού. Επιπλέον, κατά την κρυπτογράφηση χρησιμοποιούνται συναρτήσεις κατακερματισμού (hash function), οι οποίες δέχονται ως είσοδο δεδομένα μεταβλητού μεγέθους και παράγει μια ως έξοδο σύννοψη των δεδομένων που δέχτηκε ως είσοδο. Η τιμές εξόδου που παράγει μια συνάρτηση hash ονομάζονται και τιμές hash. Η συνάρτηση κατακερματισμού hash χρησιμοποιείται για την αυθεντικοποίηση του μηνύματος, αφού είναι αδύνατο για κάποιον που γνωρίζει την τιμή hash και τον αλγόριθμο της συνάρτησης hash να βρει το περιεχόμενο του αρχικού μηνύματος.

Στη συμμετρική κρυπτογράφηση χρησιμοποιούνται αλγόριθμοι οι οποίοι χρησιμοποιούν το ίδιο κλειδί και για την διαδικασία της κρυπτογράφησης και για την

διαδικασία της αποκρυπτογράφησης. Το κλειδί σε αυτή την περίπτωση πρέπει να είναι μυστικό και να το γνωρίζουν τα εξουσιοδοτημένα μέλη για την επικοινωνία. Η συμμετρική κρυπτογράφηση περιέχει τεχνικές όπως ο αλγόριθμος του Καίσαρα, ο αλγόριθμος Vigenere και ο αλγόριθμος DES και η εξελιγμένη μορφή του ο αλγόριθμος AES.

Στην κρυπτογράφηση δημοσίου κλειδιού χρησιμοποιούνται αλγόριθμοι οι οποίοι χρησιμοποιούν διαφορετικά κλειδιά, ένα για την κρυπτογράφηση και ένα άλλο διαφορετικό για την αποκρυπτογράφηση. Ένα κλειδί από αυτά είναι το δημόσιο και το άλλο είναι το ιδιωτικό. Στην ασύμμετρη κρυπτογράφηση το αρχικό μήνυμα μετατρέπεται σε κρυπτοκείμενο χρησιμοποιώντας το ένα από τα δύο κλειδιά μαζί με τον αλγόριθμο κρυπτογράφησης. Για την αποκρυπτογράφηση του κρυπτοκειμένου χρησιμοποιείται το έτερο, δηλαδή το δεύτερο κλειδί μαζί με έναν αλγόριθμο αποκρυπτογράφησης. Η ασύμμετρη κρυπτογράφηση μπορεί να παρέχει και αυθεντικοποίηση και εμπιστευτικότητα. Ο πιο γνωστός αλγόριθμος για την κρυπτογράφηση δημοσίου κλειδιού είναι ο RSA και η ασφάλειά του έγκειται στην δυσκολία να βρεθούν οι πρώτοι παράγοντες ενός σύνθετου αριθμού και η ανταλλαγή κλειδιού μεταξύ των οντοτήτων γίνεται με τον αλγόριθμο Diffie – Hellman[95][98][99].

4.5 Ενέργειες που πρέπει να ακολουθήσει ο χρήστης για να παραμείνει ασφαλής από ηλεκτρονικά εγκλήματα

Εκτός από τα τεχνολογικά μέσα που βοηθούν κάποιον χρήστη του διαδικτύου να παραμείνει ασφαλής από κακόβουλες ενέργειες, υπάρχουν και κάποιες καλές τακτικές που προσφέρουν στον χρήστη μια ασφαλής περιήγηση στον κυβερνοχώρο. Σύμφωνα με την εταιρεία Norton, που ασχολείται με την ανάπτυξη αντικών λογισμικών και τον Οργανισμό Κυβερνοασφάλειας και Ασφάλειας Υποδομών των Ηνωμένων Πολιτειών (CISA), οι τακτικές αυτές είναι :

- **Χρήση κάποιου αντικού λογισμικού (antivirus software).** Όπως έχει ήδη αναφερθεί ένα τέτοιο λογισμικό βοηθά στην προστασία της συσκευής του χρήστη αλλά και στην προστασία της ιδιωτικότητας, της ταυτότητας και των οικονομικών του πληροφοριών όταν ο χρήστης βρίσκεται στον χώρο του διαδικτύου.
- **Η χρήση ισχυρών κωδικών πρόσβασης (passwords).** Ο χρήστης δεν πρέπει να επαναλαμβάνει την χρήση του ίδιου κωδικού πρόσβασης σε πολλούς διαφορετικούς ιστότοπους. Ο χρήστης ακόμα πρέπει να αλλάζει τους κωδικούς πρόσβασής του τακτικά και να τους κάνει όσο πιο περίπλοκους γίνεται, χρησιμοποιώντας πάνω από δέκα χαρακτήρες που αποτελούνται από γράμματα, νούμερα και σύμβολα. Υπάρχουν εφαρμογές διαχείρισης κωδικών που βοηθούν τους χρήστες να διατηρήσουν τους κωδικούς τους ασφαλείς.
- **Η συνεχής ενημέρωση του λογισμικού.** Τα λειτουργικά συστήματα και τα λογισμικά ασφαλείας πρέπει να είναι ενημερωμένα. Οι κυβερνοεγκληματίες συχνά χρησιμοποιούν γνωστές ευπάθειες ή ελαττώματα στο λογισμικό, για να αποκτήσουν πρόσβαση στο σύστημα κάποιου χρήστη. Η επιδιόρθωση αυτών των ευπαθειών μέσα από τις συχνές ενημερώσεις του λογισμικού, μπορεί να καταστήσει λιγότερο πιθανό να γίνει ένας χρήστης στόχος κυβερνοεπιθέσεων.
- **Η καλή διαχείριση των ρυθμίσεων των μέσων κοινωνικής δικτύωσης.** Οι χρήστες μέσων κοινωνικής δικτύωσης πρέπει να κρατάνε τις προσωπικές και ιδιωτικές τους πληροφορίες κλειδωμένες. Οι κυβερνοεγκληματίες συχνά χρησιμοποιώντας τεχνικές κοινωνικής μηχανικής και χειραγώγησης, μπορούν να αποκτήσουν τις προσωπικές

πληροφορίες των χρηστών, μόνο με μερικά στοιχεία δεδομένων. Για αυτόν τον λόγο όσο λιγότερα στοιχεία αποκαλύψει ένας χρήστης δημόσιας, τόσο το καλύτερο.

- **Ενίσχυση του οικιακού δικτύου.** Είναι καλό ένας χρήστης να χρησιμοποιεί έναν ισχυρό κωδικό κρυπτογράφησης, καθώς και ένα εικονικό ιδιωτικό δίκτυο (virtual private network VPN). Το VPN μπορεί να καταγράψει όλη την εξερχόμενη κίνηση πακέτων από την συσκευή ενός χρήστη μέχρι αυτά τα πακέτα να φτάσουν στον προορισμό τους. Εάν ένας κυβερνοεγκληματίας καταφέρει να διεισδύσει σε αυτή την γραμμή επικοινωνίας, το πόνο που θα καταφέρει να δει είναι τα κρυπτογραφημένα δεδομένα. Η σύνδεση με την χρήση VPN είναι καλή τακτική όταν χρήστης συνδέεται από δημόσια δίκτυα Wi-Fi όπως τα δίκτυα καφετεριών, αεροδρομίων κ.τ.λ.
- **Ενημέρωση των παιδιών για τον διαδίκτυο και τον κυβερνοχώρο.** Τα παιδιά μπορούν να διδαχθούν είτε από το οικογενειακό τους, είτε από τους δασκάλους τους για την αποδεκτή χρήση του διαδικτύου και τους κινδύνους που εγκυμονεί το διαδίκτυο για κάποιον που δεν είναι προσεκτικός.
- **Συστηματική ενημέρωση των χρηστών σχετικά με τις παραβιάσεις ασφαλείας.** Εάν κάποια ιστοσελίδα, στην οποία ένας χρήστης έχει λογαριασμό, παραβιαστεί τότε ο χρήστης πρέπει να ενημερωθεί αμέσως σχετικά με το ποιές προσωπικές του πληροφορίες διέρρευσαν στους hackers και αμέσως μετά πρέπει να αλλάξει τον κωδικό πρόσβασης.
- **Λήψη μέτρων που θα προστατέψουν τον χρήστη από το να κλαπεί η ταυτότητά του.** Η κλοπή ταυτότητας συμβαίνει όταν κάποιος αποκτά παράνομα τα προσωπικά δεδομένα κάποιου χρήστη με απάτη ή δόλο, συνήθως για οικονομικό κέρδος. Αυτό γίνεται μέσω της εξαπάτησης του χρήστη από την κακόβουλη οντότητα, δίνοντας προσωπικές πληροφορίες στο διαδίκτυο, για παράδειγμα, ή να κλέψει την ηλεκτρονική αλληλογραφία του για να αποκτήσει πρόσβαση σε πληροφορίες λογαριασμών. Γι' αυτό είναι σημαντικό να φυλάει κάθε χρήστης του διαδικτύου τα προσωπικά του δεδομένα. Ένα σύστημα VPN μπορεί επίσης να βοηθήσει στην προστασία των δεδομένων που αποστέλλονται και λαμβάνονται από έναν χρήστη στο διαδίκτυο, ειδικά η σύνδεση στο διαδίκτυο γίνεται μέσω δημόσιων δικτύων Wi-Fi.
- **Να είναι ο χρήστης ενημερωμένος σχετικά με την κλοπή ταυτότητας που είναι πιθανό να του συμβεί παντού.** Είναι καλή τακτική επίσης ένας χρήστης να προστατεύει την ταυτότητά του ακόμα και όταν ταξιδεύει. Υπάρχουν πολλά πράγματα που μπορεί να κάνει ένας χρήστης, για να αποτρέψει κυβερνοεγκληματίες να αποκτήσουν τα προσωπικά του δεδομένα κατά την διάρκεια ταξιδιών. Μερικά από αυτά είναι να μην δημοσιεύει πληροφορίες σχετικά με το ταξίδι σε μέσα κοινωνικής δικτύωσης και όταν συνδέεται στο διαδίκτυο μέσω δημόσιων δικτύων τότε καλό θα ήταν να το κάνει με χρήση VPN.
- **Τα παιδιά πρέπει να παρακολουθούνται τακτικά σχετικά με τις δραστηριότητές τους στο διαδίκτυο.** Οι κλέφτες ταυτοτήτων συχνά στοχεύουν τα παιδιά επειδή οι αριθμοί Κοινωνικής Ασφάλισης και το ιστορικό οικονομικών στοιχείων τους είναι καθαρά. Οι γονείς μπορούν να προστατεύσουν τα παιδιά τους από κλοπές ταυτότητας όταν είναι προσεκτικοί τις φορές που μοιράζονται τα στοιχεία των παιδιών τους. Επίσης, οι γονείς πρέπει να είναι σε θέση να γνωρίζουν πότε η ταυτότητα των παιδιών τους έχει παραβιαστεί.
- **Ο χρήστης πρέπει να γνωρίζει τι πρέπει να κάνει σε περίπτωση που πέσει θύμα κυβερνοεγκλήματος.** Εάν ο χρήστης υποψιαστεί ότι έχει πέσει θύμα κυβερνοεγκλήματος τότε, πρέπει να ενημερώσει τις αρμόδιες αρχές όπως το τοπικό αστυνομικό τμήμα, και σε κάποιες περιπτώσεις την γενική αστυνομική διεύθυνση της χώρας. Αυτή η ενέργεια είναι πολύ σημαντική ακόμα και αν το κυβερνοεγκλήμα που έχει διαπραχθεί είναι πολύ μικρής

σημασίας. Η αναφορά που θα κάνει το θύμα θα βοηθήσει να αποτραπούν κυβερνοεγκληματίες από το να εκμεταλλευτούν άλλους ανθρώπους στο μέλλον. Αν κάποιος χρήστης έχει την υποψία ότι κυβερνοεγκληματίες έχουν κλέψει την ταυτότητά του, αυτά είναι μερικά από τα βήματα που πρέπει να ακολουθήσει :

- Να επικοινωνήσει με τις εταιρείες και τις τράπεζες όπου έγινε γνωστή ή απάτη.
- Να τοποθετήσει ειδοποιήσεις απάτης και να λαμβάνει το ιστορικό της τραπεζικής του κάρτας.
- **Να έχει ενεργοποιήσει ο χρήστης την πολυπαραγοντική ταυτοποίηση.** Παράδειγμα αυτής της τεχνικής είναι όταν ο χρήστης πραγματοποιεί μέσω e-banking μια χρηματική συναλλαγή και για την ολοκλήρωσή της του έρχεται με στο προσωπικό του τηλεφωνικό νούμερο ένα μήνυμα με έναν κωδικό τον οποίο χρειάζεται να γράψει για να ολοκληρωθεί η συναλλαγή.
- **Να ελέγχει την διεύθυνση μιας ιστοσελίδας.** Κάθε χρήστης πρέπει να ελέγχει την διεύθυνση μιας ιστοσελίδας και αν παρατηρεί κάτι περίεργο και δεν μοιάζει όπως μια διεύθυνση μιας αξιόπιστης ιστοσελίδας τότε να μην προχωράει σε άλλες ενέργειες που θα μοιραστεί προσωπικά του στοιχεία.
- **Να πραγματοποιεί αγορές μόνο μέσω έμπιστων διαδικτυακών μαγαζιών.** Μια περίπτωση απάτης είναι η αγορά προϊόντων μέσω ψεύτικων ηλεκτρονικών μαγαζιών. Αυτό συνεπάγεται ότι κακόβουλες οντότητες μαθαίνουν για τα στοιχεία τραπεζικής ενός χρήστη προκαλώντας περεταίρω προβλήματα.
- **Κάθε φορά που ένας χρήστης κλείνει μια ιστοσελίδα πρέπει να θυμάται να κάνει πάντα αποσύνδεση από τον λογαριασμό του στην συγκεκριμένη ιστοσελίδα.**[100][101]

4.6 Ενέργειες που πρέπει να ακολουθήσει ένας οργανισμός και τα μεγάλα στελέχη του για να παραμείνουν ασφαλείς από ηλεκτρονικά εγκλήματα

Όλοι οι οργανισμοί και οι εταιρείες, ανεξαρτήτως μεγέθους, πρέπει να έχουν μια σοβαρή στάση όσον αφορά την κυβερνοασφάλεια και την προστασία των πιο κρίσιμων περιουσιακών τους στοιχείων. Οι συνιστώμενες ενέργειες περιλαμβάνουν :

- **Μείωση της πιθανότητας μιας επιζήμιας κυβερνοεπίθεσης.**
 - Ένας οργανισμός πρέπει να έχει βεβαιωθεί ότι όλη η απομακρυσμένη πρόσβαση στο ιδιωτικό του δίκτυο και η πρόσβαση σε προνομιακά ή διαχειριστικά δικαιώματα απαιτεί πολυπαραγοντική ταυτοποίηση.
 - Ο οργανισμός πρέπει να ελέγχει συχνά ότι το λογισμικό είναι ενημερωμένο, δίνοντας προτεραιότητα σε ενημερώσεις που αντιμετωπίζουν γνωστά εκμεταλλευόμενα ευπαθή σημεία που έχουν αναγνωριστεί από τις σχετικές αρχές
 - Οι υπεύθυνοι του τμήματος Πληροφορικής της εταιρείας - επιχείρησης (IT&T department) πρέπει να είναι βέβαιοι ότι έχουν απενεργοποιήσει όλες τις θύρες και πρωτόκολλα που δεν είναι απαραίτητα για τους σκοπούς της εταιρείας - επιχείρησης.
 - Εάν ο οργανισμός χρησιμοποιεί υπηρεσίες cloud, το προσωπικό του τμήματος Πληροφορικής έχει εξετάσει και έχει εφαρμόσει ισχυρούς ελέγχους που αναφέρονται στις οδηγίες που έχουν θεσπίσει οι αρμόδιοι οργανισμοί κυβερνοασφάλειας.
- **Μέτρα για τον γρήγορο εντοπισμό μιας δυνητικής επίθεσης.**
 - Το προσωπικό του τμήματος κυβερνοασφάλειας/Πληροφορικής πρέπει να επικεντρώνεται στον εντοπισμό και τη γρήγορη αξιολόγηση οποιασδήποτε

απροσδόκητης ή ασυνήθιστης συμπεριφοράς στο δίκτυο. Επίσης, πρέπει να εφαρμόζεται η καταγραφή για καλύτερη διερεύνηση θεμάτων ή συμβάντων.

- Επιβεβαίωση του οργανισμού ότι ολόκληρο το δίκτυο του προστατεύεται από αντικό λογισμικό και ότι οι υπογραφές σε αυτά τα εργαλεία ενημερώνονται.
- Λόγω του πολέμου μεταξύ Ρωσίας – Ουκρανίας, ένας οργανισμός που συνεργάζεται με οργανισμούς από την Ουκρανία πρέπει να παρακολουθεί, να επιθεωρεί και να απομονώνει την κίνηση από αυτούς τους οργανισμούς. Πρέπει να ελέγχει προσεκτικά τους ελέγχους πρόσβασης για τέτοιες κινήσεις.
- **Ετοιμότητα ενός οργανισμού, σε περίπτωση παράνομης διείσδυσης ή άλλης κυβερνοεπίθεσης, να αντιδράσει.**
 - Κάθε οργανισμός πρέπει να συγκροτήσει μια ομάδα ανταπόκρισης σε κρίσεις με κύρια σημεία επαφής για ύποπτα περιστατικά κυβερνοασφάλειας και ρόλους / ευθύνες εντός του οργανισμού, συμπεριλαμβανομένων τεχνολογίας, επικοινωνιών, νομικής και επιχειρησιακής εξέλιξης.
 - Το κλειδί του αρμόδιου προσωπικού πρέπει να είναι διαθέσιμο. Η ταυτοποίηση σημαίνει αυξημένη υποστήριξη, ως ανταπόκριση σε ένα περιστατικό
 - Ασκήσεις ελέγχου έτσι ώστε να διασφαλιστεί ότι όλοι οι συμμετέχοντες κατανοούν τους ρόλους τους κατά τη διάρκεια μιας παραβίασης ασφαλείας.
- **Μεγιστοποίηση της ανθεκτικότητας του οργανισμού σε μια καταστροφική κυβερνοεπίθεση.**
 - Έλεγχος στις διαδικασίες αντιγράφων ασφαλείας για να διασφαλιστεί ότι τα κρίσιμα δεδομένα μπορούν να αποκατασταθούν γρήγορα αν οργανισμός επηρεαστεί από ransomware ή μια καταστροφική κυβερνοεπίθεση. Επιβεβαίωση ότι τα αντίγραφα ασφαλείας είναι απομονωμένα από τις δικτυακές συνδέσεις.
 - Εάν γίνεται χρήση συστημάτων ελέγχου βιομηχανικής ή λειτουργικής τεχνολογίας, πρέπει να πραγματοποιηθεί έλεγχος των μη αυτοματοποιημένων ελέγχων για να εξασφαλίσετε ότι οι κρίσιμες λειτουργίες παραμένουν λειτουργικές εάν ο δικτυακός τύπος του οργανισμού είναι μη διαθέσιμος ή μη αξιόπιστος.

Εάν ένας οργανισμός ή μια εταιρεία ακολουθήσει τα παραπάνω βήματα μπορούν να σημειώσουν πρόοδο στην βελτίωση της κυβερνοασφάλειας και της ανθεκτικότητάς τους [102].

Κεφάλαιο 5 Ανίχνευση επιθέσεων και η αντιμετώπισή τους

5.1 Εισαγωγή στα συστήματα ανίχνευσης επιθέσεων

Η σύνδεση ενός χρήστη στο διαδίκτυο και στον κυβερνοχώρο, εγκυμονεί πολλούς κινδύνους. Οι κίνδυνοι αυτοί είναι αποτελέσματα από πολλά σφάλματα (bugs) και κενά ή ευπάθειες στην ασφάλεια του υλικού (hardware) και του λογισμικού (software). Όποτε γίνεται αντιληπτή η ανάγκη για εγκατάσταση μηχανισμών ασφαλείας, οι οποίοι θα αποτρέπουν κάθε μη εξουσιοδοτημένη πρόσβαση σε πόρους του υπολογιστικού συστήματος ή σε δεδομένα που περιέχει το σύστημα αυτό. Όμως είναι ανέφικτη η πλήρης επιτυχία για την προστασία από όλα τα προβλήματα ασφαλείας.

Αυτό που μπορεί να γίνει είναι να αναγνωριστούν αυτές οι επιθέσεις και οι εισβολές αλλά και οι απόπειρες, ακόμα και αν δεν πλήξουν το υπολογιστικό σύστημα, όσο πιο γρήγορα γίνεται. Αν ανιχνευτούν πολύ νωρίς, οι ζημιές που θα έχουν επιφέρει αυτές οι κακόβουλες ενέργειες παραβίασης της ασφάλειας θα είναι λιγότερες. Όταν τα μέτρα πρόληψης αποτύχουν στο να προστατεύσουν το σύστημα, τότε η ασφάλεια θα πρέπει να βασιστεί σε τεχνικές ανίχνευσης, που θα βοηθήσουν στον γρήγορο εντοπισμό των επιθέσεων αποτρέποντας τις και επιδιορθώνοντας τυχόν ζημιές. Η ραγδαία αύξηση των κυβερνοεπιθέσεων τα τελευταία χρόνια, έχει καταστήσει τα συστήματα ανίχνευσης απαραίτητα για την διασφάλιση της ασφάλειας στον κυβερνοχώρο των οργανισμών και των εταιρειών. Είναι απαραίτητες οι τεχνικές ανίχνευσης επιθέσεων καθώς δεν μπορεί να εξασφαλιστεί πότε στο 100% η ασφάλεια ενός συστήματος.

Σύμφωνα με την Dorothy E. Denning, το μοντέλο ανίχνευσης επιθέσεων βασίζεται στην υπόθεση, ότι η εκμετάλλευση των ευπαθειών ενός συστήματος εμπεριέχει ασυνήθιστη χρήση του υπολογιστικού συστήματος. Επομένως, οι παραβιάσεις της ασφάλειας θα

μπορούσαν να εντοπιστούν μέσα από μη φυσιολογική χρήση του συστήματος. Η μη φυσιολογική χρήση ενός συστήματος μπορεί να περιέχει τα παρακάτω :

- **Η απόπειρα διάρρηξης.** Είναι η προσπάθεια εισβολής σε ένα σύστημα, η οποία μπορεί να οδηγήσει σε αποτυχίες των κωδικών πρόσβασης, είτε σε έναν μεμονωμένο λογαριασμό, είτε στο σύστημα ως σύνολο.
- **Η παραπλανητική ή επιτυχής διάρρηξη.** Συμβαίνει όταν κάποιος καταφέρνει να συνδεθεί σε ένα σύστημα χρησιμοποιώντας έναν μη εξουσιοδοτημένο λογαριασμό και κωδικό. Σε αυτή την περίπτωση, ο εισβολέας μπορεί να έχει διαφορετικό χρόνο εισόδου, τοποθεσία ή είδος σύνδεσης από τον νόμιμο χρήστη. Επιπλέον, η συμπεριφορά του εισβολέα μπορεί να διαφέρει πολύ από αυτήν του νόμιμου χρήστη.
- **Εισβολή από εξουσιοδοτημένο χρήστη.** Ένας χρήστης με εξουσιοδότηση πρόσβασης στο σύστημα μπορεί να προσπαθήσει να παρακάμψει τα μέτρα ασφαλείας του συστήματος και να αποκτήσει πρόσβαση σε αρχεία και προγράμματα για τα οποία δεν έχει εξουσιοδότηση. Αν επιτύχει στο να παρακάμψει τα μέτρα ασφαλείας, θα έχει πρόσβαση σε εντολές και αρχεία που υπό κανονικές συνθήκες δεν θα είχε πρόσβαση.
- **Διαρροή από νόμιμο χρήστη.** Όταν ένας χρήστης προσπαθεί να διαρρεύσει ευαίσθητα αρχεία, μπορεί να χρησιμοποιήσει το σύστημα σε ασυνήθιστες ώρες ή να στείλει δεδομένα σε εκτυπωτές που δεν χρησιμοποιούνται, προκαλώντας μια διαρροή δεδομένων που μπορεί να έχει σοβαρές συνέπειες.

- **Δούρειος Ίππος (Trojan horse).** Η συμπεριφορά ενός κακόβουλου λογισμικού μπορεί να διαφέρει από το αντίστοιχο νόμιμο πρόγραμμα, καθώς μπορεί να εκτελεί μυστικές λειτουργίες ή να προκαλέσει ζημιά στο σύστημα, ενώ το νόμιμο πρόγραμμα θα λειτουργούσε σύμφωνα με τις προδιαγραφές του.
- **Ηλεκτρονικός ιός (virus).** Ένας ιός που τοποθετείται σε ένα σύστημα μπορεί να προκαλέσει αύξηση στη συχνότητα επανεγγραφής εκτελέσιμων αρχείων, τη χρήση αποθηκευτικού χώρου από εκτελέσιμα αρχεία ή την εκτέλεση ενός συγκεκριμένου προγράμματος καθώς ο ιός εξαπλώνεται.
- **Η άρνηση εξυπηρέτησης.** Αναφέρεται σε μια επίθεση όπου ένας εισβολέας μπορεί να καταλαμβάνει μια πηγή, όπως ένα δίκτυο ή έναν διακομιστή, και να προκαλέσει ανεπιθύμητες επιπτώσεις σε άλλους χρήστες. Ο εισβολέας μπορεί να προκαλέσει ασυνήθιστα υψηλό επίπεδο δραστηριότητας στην πηγή, ενώ οι υπόλοιποι χρήστες έχουν πρόσβαση σε αφύσικα χαμηλά επίπεδα υπηρεσίας.

Τα υπολογιστικά συστήματα που δέχονται κάποια κυβερνοεπίθεση δεν ακολουθούν τουλάχιστον μια από τις παρακάτω προϋποθέσεις :

1. Η συνολική συμπεριφορά των χρηστών και των διεργασιών μπορεί να ακολουθεί ένα προβλέψιμο στατιστικό μοτίβο. Παραδείγματα περιλαμβάνουν περιπτώσεις όπου επιτρέπεται η πρόσβαση σε δίκτυα από διευθύνσεις που παλαιότερα ήταν απαγορευμένες ή η εκτέλεση συγκεκριμένων εντολών από έναν χρήστη που πριν δεν εκτελούνταν.
2. Οι ενέργειες των χρηστών και των διεργασιών δεν πρέπει να περιλαμβάνουν εντολές που θα παραβιάζουν την πολιτική ασφάλειας του συστήματος, αλλά στην πραγματικότητα, υπάρχουν γνωστές ακολουθίες εντολών που μπορούν να χρησιμοποιηθούν από εισβολείς για να υπονομεύσουν την ασφάλεια του συστήματος και οι οποίες μπορούν να ανιχνευτούν. Για παράδειγμα, κατά την επίθεση ενός εισβολέα που επιδιώκει να αποκτήσει δικαιώματα root σε ένα σύστημα, μπορεί να χρησιμοποιηθούν συγκεκριμένες τεχνικές και ακολουθίες εντολών που θα χρησιμοποιηθούν για να παραβιάσουν την ασφάλεια του συστήματος.
3. Οι διεργασίες εκτελούν ενέργειες που συμμορφώνονται με ένα σύνολο προδιαγραφών, το οποίο καθορίζει ποιες ενέργειες είναι επιτρεπτές.

Το Σύστημα Ανίχνευσης Εισβολής (ΣΑΕ ή στα αγγλικά Intrusion Detection System, IDS) είναι ένα σύστημα παρακολούθησης και ανάλυσης των συμβάντων που συμβαίνουν σε ηλεκτρονικούς υπολογιστές και δίκτυα υπολογιστών. Το σύστημα αυτό ανιχνεύει και αναφέρει επιθέσεις και κακόβουλες ενέργειες που εκτελούνται από εξωτερικούς εισβολείς ή εσωτερικούς χρήστες που παραβιάζουν την ασφάλεια του συστήματος. Δηλαδή, η αποστολή ενός Συστήματος Ανίχνευσης Εισβολής (ΣΑΕ) είναι να εντοπίζει σημάδια πιθανών επιθέσεων, κατά τις οποίες μπορεί να εντοπιστούν συχνά αποδείξεις παραβίασης της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των πληροφοριακών πόρων. Απλούστερα, ένα σύστημα IDS εξετάζει τα αρχεία καταγραφής και ελέγχου του συστήματος (logging and audit), για να ανιχνεύσει στοιχεία που υποδεικνύουν ότι έχει γίνει μια επίθεση ή παρουσιάζονται άλλα σημάδια που σχετίζονται με γνωστές επιθέσεις. Το προσωπικό (host-based) λογισμικό IDS εντοπίζει ύποπτες δραστηριότητες που σχετίζονται με τον υπολογιστή που προστατεύει, όπως εγγραφές στο μητρώο, απόπειρες εισόδου, port scans, δυσλειτουργίες ή τροποποιήσεις προγραμμάτων και απόπειρες DOS. Από την άλλη, το δικτυακό (NIDS)

λογισμικό IDS συνεργάζεται συνήθως με ένα σύστημα firewall ή εγκαθίσταται σε σημαντικής σημασίας σημεία εντός του δικτύου της επιχείρησης και εντοπίζει την κίνηση του δικτύου για γνωστές ανωμαλίες, όπως port scans, συγχρονισμένες επιθέσεις DOS κ.λπ.

5.2 Λόγοι χρήσης συστημάτων ανίχνευσης εισβολών

Οι λόγοι για τους οποίους ένας οργανισμός ή επιχείρηση θα ήταν επιθυμητό να χρησιμοποιήσει ένα σύστημα ανίχνευσης εισβολής είναι πάρα πολλοί. Θα αναφερθούν παρακάτω οι πιο σημαντικοί :

1. Πρόληψη προβλημάτων. Η χρήση συστημάτων ανίχνευσης εισβολών συμβάλλει στην πρόληψη προβλημάτων σε δύο επίπεδα. Αρχικά, μπορεί να ανιχνεύσει τις προσπάθειες εισβολής σε πολύ αρχικό στάδιο και να παρθούν άμεσα μέτρα για την αντιμετώπισή τους, πριν προκληθεί μεγάλη ζημιά. Σε δεύτερο επίπεδο, η ύπαρξη ενός τέτοιου συστήματος μπορεί να αποτρέψει τους επιτιθέμενους να προσπαθήσουν να εισβάλλουν, καθώς γνωρίζουν ότι υπάρχει περίπτωση να αποκαλυφθούν και να τιμωρηθούν.
2. Ανίχνευση επιθέσεων και παραβιάσεων που είναι αδύνατον να ανιχνευτούν με άλλα μέσα. Για παράδειγμα, τα σχήματα εξακρίβωσης ταυτότητας και ελέγχου πρόσβασης δεν μπορούν να αντιμετωπίσουν τις καταχρήσεις δικαιωμάτων από εσωτερικούς χρήστες γιατί δεν έχουν σχεδιαστεί για να αντιμετωπίζουν τέτοιου είδους θέματα.
3. Εντοπισμός και αντιμετώπιση προσπαθειών ανίχνευσης. Συνήθως, μια επίθεση σε πληροφοριακά συστήματα ακολουθεί ένα τυπικό σχέδιο που αποτελείται από τρεις βασικές φάσεις. Η πρώτη φάση είναι η ανίχνευση του πληροφοριακού συστήματος, κατά την οποία διαπιστώνεται η δομή και οι διαθέσιμες υπηρεσίες του συστήματος. Στην επόμενη φάση, εξετάζονται «βιβλιοθήκες» τεχνικών που είναι πιθανό να χρησιμοποιηθούν για να παραβιαστεί η ασφάλεια του συστήματος και, τέλος, εφαρμόζονται αυτές οι τεχνικές. Ενώ άλλα μέτρα ασφάλειας, όπως οι firewalls, ο έλεγχος πρόσβασης και οι εφαρμογές επιδιόρθωσης, αναλαμβάνουν να προστατεύσουν το σύστημα από επιθέσεις στην τελική τους φάση, τα συστήματα ανίχνευσης εισβολών μπορούν να ανιχνεύσουν τις προσπάθειες εισβολής και να εμποδίσουν τους εισβολείς ή να ειδοποιήσουν τους διαχειριστές για να ληφθούν κατάλληλα μέτρα. Αντιδρώντας άμεσα σε παρόμοια περιστατικά, το σύστημα ενισχύεται και γίνεται πιο ανθεκτικό στις επιθέσεις, ενώ ταυτόχρονα αποθαρρύνονται οι πιθανοί εισβολείς από την επανάληψη των επιθέσεων.
4. Τεκμηρίωση υπαρκτών απειλών. Τα συστήματα ανίχνευσης εισβολών έχουν τη δυνατότητα να εντοπίσουν την ύπαρξη απειλών στο πληροφοριακό σύστημα πριν αυτές προκαλέσουν σοβαρές ζημιές. Μία τεκμηρίωση που αποδεικνύει την ύπαρξη απειλών στο πληροφοριακό σύστημα είναι πολύτιμη για πολλούς λόγους αφού (1) πείθει τη διοίκηση του οργανισμού ή της εταιρείας για την κατανομή πόρων στα συστήματα ασφαλείας, (2) συμβάλει στον προσδιορισμό των πιο κατάλληλων μέτρων ασφαλείας για το σύστημα διότι η φύση των απειλών καθορίζει σε μεγάλο βαθμό τα αντίμετρα που πρέπει να ληφθούν και (3) βοηθά στην αποδοτικότερη κατανομή των πόρων ασφαλείας στις διάφορες τομές του πληροφοριακού συστήματος, λαμβάνοντας υπόψη τις απειλές που αντιμετωπίζει καθένα από αυτά και τη σημασία του για τον οργανισμό.
5. Έλεγχος ποιότητας για το σχεδιασμό ασφαλείας και τη διαχείριση. Είναι πιθανόν να υπάρχουν ατέλειες τόσο στο σχέδιο ασφαλείας του οργανισμού όσο και στην υλοποίηση του από τους υπεύθυνους ασφαλείας και τα συστήματα. Για αυτόν τον

λόγο, είναι απαραίτητος ο έλεγχος ποιότητας ώστε να διασφαλιστεί η ασφάλεια του οργανισμού. Με τη χρήση συστημάτων ανίχνευσης εισβολών, είναι δυνατόν να εντοπιστούν ατέλειες στο σύστημα ασφαλείας και να αντιμετωπιστούν πριν προκαλέσουν πραγματικό κίνδυνο.

6. Τα συστήματα ανίχνευσης εισβολών μπορούν να παρέχουν πληροφορίες για τις επιτυχημένες επιθέσεις, βοηθώντας έτσι στο να αξιολογηθεί το μέγεθος της ζημιάς, στον σχεδιασμό και την εφαρμογή των απαραίτητων ενεργειών για την ανάκαμψη και στη διαμόρφωση μιας λίστας με προληπτικά μέτρα για την αποτροπή μελλοντικών παρόμοιων περιστατικών.
7. Θωράκιση παλαιών συστημάτων. Η αναβάθμιση παλαιών συστημάτων αποτελεί συχνά αναγκαιότητα καθώς αυτά γίνονται ευάλωτα σε επιθέσεις και δεν λαμβάνουν πλέον υποστήριξη από τους κατασκευαστές τους. Ωστόσο, η θωράκισή τους με συστήματα ανίχνευσης εισβολών μπορεί να βοηθήσει στην προστασία τους και στη διατήρησή τους σε λειτουργία.
8. Συμπλήρωση των διαδικασιών εγκατάστασης επιδιορθωτικών προγραμμάτων. Ακόμα και αν οι κατασκευαστές των συστημάτων του οργανισμού συνεχίζουν να παρέχουν υποστήριξη και υπάρχουν διαθέσιμα επιδιορθωτικά προγράμματα, η διαθεσιμότητά τους δεν είναι πάντα άμεση, ενώ για πολύπλοκα περιβάλλοντα η εγκατάστασή τους μπορεί να καθυστερεί λόγω διάφορων παραγόντων.
9. Αναγκαιότητα ύπαρξης ευπαθών υπηρεσιών. Παρ'όλο που κάποιες υπηρεσίες έχουν γνωστά προβλήματα ασφαλείας, οι χρήστες ή οι διαχειριστές των οργανισμών επιμένουν να τις χρησιμοποιούν καθώς θεωρούν ότι είναι πιο εύχρηστες και συμβάλλουν στην αύξηση της παραγωγικότητας. Η υπηρεσία FTP είναι ένα κλασικό παράδειγμα μιας προβληματικής υπηρεσίας, καθώς δεν κρυπτογραφεί τα συνθηματικά κατά τη διακίνησή τους. Παρόλα αυτά, η χρήση ενός ασφαλούς πρωτοκόλλου μεταφοράς αρχείων είναι πιο ασφαλές, αλλά συνήθως πιο δύσχρηστο για τους χρήστες. Τα συστήματα ανίχνευσης εισβολών έχουν τη δυνατότητα να ελέγχουν τις επιβλαβείς υπηρεσίες και να εντοπίζουν περιστατικά όπου αυτές δημιουργούν αυξημένους κινδύνους.
10. Αξιολόγηση των ενεργειών των χρηστών ή των διαχειριστών. Οι χρήστες και οι διαχειριστές μπορεί να μην χρησιμοποιούν ορθά τους μηχανισμούς ασφαλείας που προσφέρονται από το σύστημα. Η χρήση ενός συστήματος ανίχνευσης εισβολών μπορεί να βοηθήσει στην εντοπισμό των αδυναμιών αυτών των μηχανισμών και στην επισήμανση των δυνατοτήτων βελτίωσης.
11. Έλεγχος συνέπειας μεταξύ πολιτικής ασφάλειας και κανόνων πρόσβασης. Ενδέχεται η πολιτική ασφάλειας που εφαρμόζεται στον οργανισμό να μην τηρείται πλήρως από τους διαχειριστές στα θέματα πρόσβασης στο σύστημα. Ωστόσο, με τη χρήση αρχείων καταγραφής που διατηρούνται από τα συστήματα ανίχνευσης εισβολών, μπορούν να ανακαλυφθούν τυχόν ασυνέπειες και να διορθωθούν ανάλογα.

5.3 Διαχείριση των εισβολών από ένα Σύστημα Διαχείρισης Εισβολών – IDS

Η διαδικασία διαχείρισης μιας εισβολής από ένα IDS, μπορεί να χωριστεί σε έξι βήματα – ενέργειες.

- 1) Αρχικά, πραγματοποιείται η προετοιμασία για μια επίθεση, μια διαδικασία που προηγείται της ανίχνευσης οποιασδήποτε επίθεσης. Κατά τη διάρκεια αυτής της φάσης, γίνεται η υλοποίηση των διαδικασιών και μηχανισμών που χρησιμοποιούνται για την ανίχνευση και την αντίδραση σε επιθέσεις.

- 2) Μετά την προετοιμασία για μια επίθεση, το επόμενο σημαντικό βήμα είναι η ταυτοποίησή της. Η διαδικασία αυτή είναι καθοριστική γιατί βοηθά να καθοριστούν οι επόμενες κινήσεις που θα ακολουθήσουν οι διαχειριστές ή οι μηχανικοί ασφάλειας, προκειμένου να αντιμετωπίσουν την επίθεση με τον καλύτερο δυνατό τρόπο.
- 3) Στη συνέχεια, λαμβάνονται μέτρα για τον περιορισμό της επίθεσης. Με αυτόν τον τρόπο, περιορίζεται η πρόσβαση στο σύστημα, προκειμένου να αποτραπεί η επέκταση των ζημιών. Ωστόσο, η επίθεση παρακολουθείται παθητικά και καταγράφονται πλήρως οι ενέργειες του επιτιθέμενου για μελλοντική ανάλυση.
- 4) Στο τέταρτο βήμα, πραγματοποιείται η εξουδετέρωση της επίθεσης, κατά την οποία η επίθεση διακόπτεται και το σύστημα επανέρχεται στη λειτουργία του.
- 5) Μετά την εξουδετέρωση της επίθεσης, ακολουθεί η φάση της αποκατάστασης, κατά την οποία το σύστημα επαναφέρεται σε μια ασφαλή κατάσταση σύμφωνα με τις πολιτικές ασφαλείας που έχουν καθοριστεί.
- 6) Στο τελευταίο βήμα, γίνεται συνεχής παρακολούθηση της επίθεσης προκειμένου να ληφθούν μέτρα κατά του επιτιθέμενου. Ταυτόχρονα, καταγράφονται τυχόν προβλήματα κατά τη διάρκεια της αντιμετώπισης της επίθεσης και σημαντικές εμπειρίες που αποκτήθηκαν για μελλοντική αντιμετώπιση ανάλογων προβλημάτων.

5.4 Κατηγοριοποίηση Συστημάτων Ανίχνευσης Εισβολών – IDS και χρονισμός της ανάλυσης

Η κατηγοριοποίηση των Συστημάτων Ανίχνευσης Εισβολών γίνεται με βάση τριών μοντέλων :

- 1) **Σύστημα Ανίχνευσης Υπογραφής (Signature based Detection System or Misused based Detection System).** Η συγκεκριμένη μέθοδος ανίχνευσης αποδεικνύεται αποτελεσματική εναντίον γνωστών επιθέσεων, ωστόσο απαιτεί συνεχείς ενημερώσεις για να παραμένει αποτελεσματική και δεν μπορεί να ανιχνεύσει προηγούμενες άγνωστες απειλές ή νέες μορφές επιθέσεων.
- 2) **Σύστημα Ανίχνευσης Ανωμαλιών (Anomaly based Detection System).** Αυτός ο τύπος ανίχνευσης επαρκεί για την αναγνώριση των γνωστών απειλών στο σύστημα μέσω της διαχωριστικής κατηγοριοποίησης του σε φυσιολογικό και μη φυσιολογικό, βασιζόμενος σε κανόνες ή ευρετική λειτουργία, αντί για σχέδια ή υπογραφές. Για να εφαρμοστεί αυτό το σύστημα, χρειάζεται να γνωρίζουμε την φυσιολογική συμπεριφορά του δικτύου. Το σύστημα αυτό μπορεί επίσης να ανιχνεύσει άγνωστες απειλές που δεν έχουν καταγραφεί προηγουμένως, σε αντίθεση με το σύστημα ανίχνευσης υπογραφής.
- 3) **Σύστημα Ανίχνευσης Προδιαγραφών (Specification based detection system).** Ο συγκεκριμένος τύπος ανίχνευσης αναλαμβάνει τον έλεγχο των διαδικασιών και των πραγματικών δεδομένων σε σχέση με το πρόγραμμα, με στόχο να ανιχνεύει αφυσικές συμπεριφορές και να εκδίδει συναγερμούς σε αυτή την περίπτωση. Προκειμένου να είναι αποτελεσματικό, απαιτείται η συντήρηση και η ενημέρωση του συστήματος για οποιαδήποτε αλλαγή στα προγράμματα παρακολούθησης, έτσι ώστε να είναι σε θέση να ανιχνεύσει προηγούμενες επιθέσεις.

Οι πληροφορίες που συλλέγουν τα Συστήματα Ανίχνευσης Εισβολών μπορούν να αναλυθούν με δύο τρόπους :

1. Ανάλυση που πραγματοποιείται σε πραγματικό χρόνο. Οι πληροφορίες που συλλέγονται αναλύονται αμέσως μόλις παραλαμβάνονται, αλλά αυτό απαιτεί δίκτυα με υψηλές ταχύτητες και ισχυρούς υπολογιστές, επειδή η ταχύτητα επεξεργασίας και ανάλυσης των πληροφοριών πρέπει να είναι μεγαλύτερη από το ρυθμό με τον οποίο παράγονται. Αυτή η προσέγγιση επιτρέπει την άμεση αντίδραση σε πιθανές απειλές.
2. Περιοδική ή μαζική ανάλυση. Οι πληροφορίες που συλλέγονται αποθηκεύονται σε αρχεία καταγραφής και αναλύονται σε μαζικές περιόδους που θεωρούνται πιο κατάλληλες, όπως περίοδοι με ελαττωμένο υπολογιστικό ή δικτυακό φόρτο. Η προσέγγιση αυτή είναι ευνοϊκή στην περίπτωση που η οντότητα που παρακολουθείται και το σύστημα ανίχνευσης εισβολών λειτουργούν στο ίδιο υπολογιστικό περιβάλλον, καθώς η ανάλυση σε πραγματικό χρόνο μπορεί να επηρεάσει αρνητικά την απόδοση του συστήματος. Ωστόσο, αυτή η προσέγγιση επιβραδύνει τη δυνατότητα άμεσης αντίδρασης στις πιθανές εισβολές.

5.5 Κατηγοριοποίηση των Συστημάτων Ανίχνευσης Εισβολών σύμφωνα με την πηγή πληροφοριών

Η πηγή συλλογής των πληροφοριών είναι το πιο συνηθισμένο κριτήριο για να πραγματοποιηθεί η ταξινόμηση των συστημάτων ανίχνευσης εισβολών. Οι πληροφορίες μπορεί να προέρχονται από τη δικτυακή κυκλοφορία, τα συμβάντα που σχετίζονται με έναν υπολογιστή ή τις δραστηριότητες ορισμένων εφαρμογών. Τα συστήματα ανίχνευσης εισβολών μπορούν να ταξινομηθούν σε τρεις κατηγορίες :

1. **Συστήματα ανίχνευσης επιθέσεων host based.** Σε αυτόν τον τύπο συστήματος, τοποθετείται συνήθως σε έναν server, όπου γίνεται η τοπική ανάλυση των δεδομένων στη συσκευή και συλλέγονται από διαφορετικές πηγές. Ένα HIDS μπορεί να χρησιμοποιήσει εξίσου και ένα σύστημα ανίχνευσης ανωμαλιών αλλά και ένα σύστημα ανίχνευσης υπογραφής.
2. **Συστήματα ανίχνευσης επιθέσεων network based.** Χρησιμοποιείται σε σημεία της υποδομής του δικτύου που έχουν στρατηγική σημασία. Έχει την δυνατότητα να αποθηκεύσει και να εξετάσει δεδομένα για μπορέσει να ανιχνεύσει επιθέσεις συγκρίνοντας σχέδια ή υπογραφές στη βάση δεδομένων. Επίσης, μπορεί και να ανιχνεύσει μη φυσιολογικές λειτουργίες με σάρωση της κυκλοφορίας δεδομένων. Αυτό το είδος συστημάτων ανάλυσης δεδομένων είναι γνωστό και ως "packet-sniffers".
3. **Συστήματα ανίχνευσης επιθέσεων hybrid based.** Πρόκειται για μια πρακτική που αναφέρεται στη διαχείριση και προειδοποίηση από HIDS και NIDS, η οποία συμπληρώνει τη διαχείριση των δύο αυτών τύπων, εξαιτίας των μειονεκτημάτων που παρουσιάζουν.

5.6 Πιθανές αντιδράσεις των Συστημάτων Ανίχνευσης Εισβολών

Όταν εντοπιστεί μια επίθεση σε ένα υπολογιστικό σύστημα, τα συστήματα ανίχνευσης εισβολών τα οποία έχουν εντοπίσει την επίθεση αυτή, αντιδρούν ακολουθώντας μια σειρά από ενέργειες οι οποίες είναι των ρυθμίσεων που έχουν πραγματοποιηθεί στα συστήματα αυτά. Οι αντιδράσεις αυτές χωρίζονται σε ενεργητικές και παθητικές.

Ένα σύστημα ανίχνευσης εισβολών το οποίο αντιδρά ενεργητικά, εμπεριέχει λειτουργίες οι οποίες αντιμετωπίζουν μια επίθεση ή κάποια ανωμαλία – δυσλειτουργία. Παραδείγματος χάριν, συνεργαζόμενο με το firewall, ένα ενεργητικό σύστημα ανίχνευσης εισβολών μπορεί να εκκινήσει την διαδικασία φιλτραρίσματος προκειμένου να μπλοκάρει

την είσοδο πιθανώς επικίνδυνων πακέτων στο σύστημα. Στο πλαίσιο αυτού του παραδείγματος, το λογισμικό IDS αποκαλείται και ως σύστημα πρόληψης εισβολών (Intrusion Prevention System / IPS). Εκτός όμως από αυτή την βασική λειτουργία, έναν ενεργητικό σύστημα ανίχνευσης εισβολών μπορεί να πραγματοποιήσει και τις παρακάτω λειτουργίες :

1. **Συλλογή πληροφοριών** για την βέλτιστη αξιολόγηση της επίθεσης στο υπολογιστικό σύστημα αλλά και για την χρήση τους σε νομικές ενέργειες. Για την επίτευξη του στόχου αυτού, μπορεί να αυξηθεί η ευαισθησία των "αισθητήρων", όπως για παράδειγμα των αρχείων καταγραφής ή των πακέτων δικτύου που αναλύονται. Επιπλέον, μπορεί να χρησιμοποιηθούν "ερωτήσεις" προς το σύστημα από το οποίο πραγματοποιείται η επίθεση, με σκοπό τη αναγνώριση ποιοι χρήστες είναι συνδεδεμένοι και άλλες αντίστοιχες πληροφορίες.
2. **Τροποποίηση του περιβάλλοντος.** Με την λειτουργία αυτή στοχεύει ένα ενεργητικό σύστημα ανίχνευσης εισβολών να καταστήσει μια εισβολή ανεφάρμοστη, αποτρέποντάς την. Αυτό υλοποιείται με πολλούς τρόπους, όπως η αποστολή πακέτων τερματισμού σύνδεσης που να φαίνεται ότι προέρχονται από το υπό επίθεση σύστημα, με επαναρύθμιση των συσκευών ελέγχου πακέτων όπως τα firewalls και οι δρομολογητές και τέλος την εφαρμογή απαγορεύσεων για συγκεκριμένες διευθύνσεις IP, θύρες, πρωτόκολλα, υπηρεσίες και φυσικές συνδέσεις.
3. **Αντεπίθεση,** με την οποία γίνεται η χρήση διαφόρων τεχνικών που στοχεύουν στο μπλοκάρισμα του επιτιθέμενου, αδρανοποιώντας τον, και την συλλογή δεδομένων που τον αφορούν. Χαρακτηριστικά παραδείγματα είναι, η αποστολή μεγάλου αριθμού πακέτων προς το σύστημα από το οποίο προέρχεται η επίθεση και η εξάπολυση επιθέσεων για να πληγούν υπηρεσίες που πιθανόν να προσφέρει ο επιτιθέμενος.

Από την άλλη πλευρά, τα παθητικά συστήματα ανίχνευσης εισβολών δεν περιλαμβάνουν ενεργητικές ενέργειες όπως η αποτροπή επιθέσεων, αντιθέτως εστιάζουν μόνο σε ενέργειες ενημερωτικού χαρακτήρα ανιχνεύοντας κάθε είδους επιθέσεις και παράνομης ενέργειας και τις οποίες στην συνέχεια τις καταγράφει. Αυτός ο τύπος συστημάτων ανίχνευσης εισβολών συνήθως ενεργοποιεί κάποιου είδους συναγερμό, για την ειδοποίηση των διαχειριστών του συστήματος ότι κάποια επίθεση βρίσκεται σε εξέλιξη. Για την αναφορά των προβλημάτων μπορεί χρησιμοποιείται ευρέως το δικτυακό πρωτόκολλο SNMP. Αυτό το πρωτόκολλο δίνει το πλεονέκτημα στο δίκτυο να ολοκληρωθεί μέσω συστήματα διαχείρισης δικτύου, εκμεταλλευόμενο μια δαπανηρή υποδομή λογισμικού και επικοινωνίας, και επιτρέποντας την ολοκλήρωση των λειτουργιών διαχείρισης. Ωστόσο, οι παθητικές ενέργειες των συστημάτων ανίχνευσης εισβολών σε σχέση με της ενεργητικές, δεσμεύουν λιγότερους από τους πόρους του υπολογιστικού συστήματος.

5.7 Αντιμετώπιση πιθανών καταστροφών από επιθέσεις στον κυβερνοχώρο

Σε περίπτωση που όταν τα μέτρα ασφαλείας δεν λειτουργήσουν και η ανίχνευση και η αντιμετώπιση των απειλών δεν γίνει άμεσα τότε, πρέπει να υπάρχει σχέδιο αντιμετώπισης των καταστροφών που θα έχουν επιφέρει οι επιθέσεις στο σύστημα. Αυτό επιτυγχάνεται κυρίως μέσω της διαδικασίας λήψης αντιγράφων ασφαλείας (backup).

Κατά την διαδικασία λήψης αντιγράφων ασφαλείας, αποθηκεύονται σε ασφαλή μέσα διάφοροι πληροφοριακοί πόροι ενός υπολογιστικού συστήματος, οι οποίοι είναι κρίσιμης σημασίας για έναν χρήστη ή έναν οργανισμό. Οι πόροι αυτοί μπορεί να είναι

αρχεία, βάσεις δεδομένων και προγράμματα. Αυτά τα αντίγραφα (backup data) σε περίπτωση κυβερνοεπίθεσης, μπορούν να ανακτηθούν έτσι ώστε ο αντίκτυπος της επίθεσης να περιοριστεί και να μην προκαλέσει ολοκληρωτική καταστροφή και την μόνιμη διαγραφή των πόρων αυτών.

Στον τομέα των υπολογιστών, η ανάγκη για αντίγραφα ασφαλείας σχετίζεται με :

- Την ανάκτηση ενός ολόκληρου συστήματος, συμπεριλαμβανομένου του λειτουργικού συστήματος, των δεδομένων και των προγραμμάτων, σε περίπτωση που το σύστημα παρουσιάζει δυσλειτουργίες ή καταστραφεί, όπως για παράδειγμα απώλεια ή κλοπή σκληρού δίσκου, αλλοίωση αρχείων συστήματος, κακόβουλο λογισμικό με καταστροφικές συνέπειες, εισβολή (hacking) και καταστροφή αρχείων, δεδομένων ή εφαρμογών (cracking).
- Την ανάγκη για επαναφορά συγκεκριμένων αρχείων και δεδομένων που πηγάζει από την απώλεια, καταστροφή, αλλοίωση ή κλοπή αυτών των αρχείων, καθώς και από τη μη διαθεσιμότητά τους για οποιονδήποτε άλλο λόγο, όπως η διαγραφή τους από λάθος του χρήστη.

Συνήθως, ένα αντίγραφο ασφαλείας αποθηκεύεται σε μαγνητικά ή οπτικά μέσα, όπως σκληρούς δίσκους ή CD/DVD. Ωστόσο, η αύξηση των ταχυτήτων δικτύωσης σε τοπικά δίκτυα και στις ευρυζωνικές συνδέσεις, έχει δώσει τη δυνατότητα για απομακρυσμένη λήψη αντιγράφων ασφαλείας (remote backup) [95][103].

Κεφάλαιο 6 Συμπεράσματα και προτάσεις βελτίωσης.

Παρατηρώντας με προσοχή τα παραπάνω, βλέπουμε ότι η ραγδαία εξέλιξη των ηλεκτρονικών υπολογιστών και των δικτύων, επέφεραν και ταχύτατη εξέλιξη των μορφών και των τρόπων υλοποίησης των ηλεκτρονικών εγκλημάτων. Τα ηλεκτρονικά εγκλήματα με την σειρά τους δημιούργησαν νέες τεχνικές για την διεξαγωγή ήδη υπάρχοντων μορφών εγκλήματος όπως η τρομοκρατία και ο πόλεμος.

Η ηλεκτρονική μορφή του πολέμου, ο κυβερνοπόλεμος, ιδιαίτερα από την αρχή του 21^{ου} αιώνα, έχει γνωρίσει μεγάλη δημοφιλία και αποτελεί πλέον έναν από τους πιο χρησιμοποιούμενους και προτιμότερους τρόπους διεξαγωγής ενός πολέμου. Ιδιαίτερα πριν από την έναρξη των χερσαίων πολεμικών επιχειρήσεων, εκτελούνται διάφορες ενέργειες στον κυβερνοχώρο με την διάδοση κακόβουλων λογισμικών ή με την προσπάθεια αναγνώρισης διάφορων ευπαθειών στα υπολογιστικά συστήματα του αντιπάλου, έτσι ώστε να προκληθεί σύγχυση και να είναι πιο εύκολο για τον επιτιθέμενο να επιτεθεί και ο αμυνόμενος να μην προλάβει να οργανωθεί.

Ο κυβερνοπόλεμος έχει αποκτήσει μεγάλη δημοτικότητα και λόγω της μικρής χρηματικής απαίτησης που έχει για την διεξαγωγή του και λόγω της μεγαλύτερης ευκολίας που έχει. Σε σύγκριση με της χερσαίες επιχειρήσεις πολέμου, ο κυβερνοπόλεμος δεν χρειάζεται ανθρώπινο δυναμικό (στρατιώτες) για τις μάχες, παρά μόνο ολιγομελείς ομάδες εξειδικευμένων hackers, ο οποίοι θα κληθούν να πάρουν την θέση των στρατιωτών, αλλά στον κυβερνοχώρο και όχι στα αληθινά πεδία μαχών. Με αυτόν τον τρόπο ο επιτιθέμενος έχει την δυνατότητα να μην υποστεί την παραμικρή ανθρώπινη απώλεια αλλά και ταυτόχρονα η δυσκολία που έχει ένας πραγματικός πόλεμος στον πραγματικό χώρο ελαχιστοποιείται, όταν συνδυάζεται μαζί με κυβερνοεπιθέσεις.

Εκτός από όλα αυτά, το κύριο πλεονέκτημα του κυβερνοπολέμου είναι ότι είναι απρόβλεπτος, συνδυάζοντας πολλές τεχνικές και μορφές άλλων ηλεκτρονικών εγκλημάτων. Ο κύριος τρόπος είναι μέσω κακόβουλων λογισμικών όπως οι ηλεκτρονικοί ιοί, τα spyware, τα κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου τους δούρειους ίππους, τις επιθέσεις άρνησης εξυπηρέτησης και τα botnets. Αυτό κάνει τον κυβερνοπόλεμο να μην μπορεί να αντιμετωπιστεί πλήρως σε μια ενδεχόμενη διακρατική κυβερνοεπίθεση, και η αντιμετώπισή του από τον αμυνόμενο δεν γίνεται έγκαιρα.

Αρα η ανάγκη για τεχνολογική εκπαίδευση του ανθρώπου στην σύγχρονη εποχή είναι αυξημένη. Οι περισσότερες επιθέσεις στον κυβερνοχώρο ξεκινούν μέσω της λάθους εκτίμησης της κατάστασης από τον ίδιο τον χρήστη. Για παράδειγμα, ένας χρήστης ενός οργανισμού μετά από άγνοιά του μπορεί να ανοίξει ένα spam email που περιέχει κάποιο κακόβουλο υπερσύνδεσμο ή κάποιο κακόβουλο λογισμικό και με αυτό τον τρόπο να ξεκινήσει μια εκτεταμένη κυβερνοεπίθεση στα συστήματα του οργανισμού ή της εταιρείας, μολύνοντας με αυτόν τον τρόπο όλα τα υπολογιστικά συστήματα του οργανισμού που βρίσκονται συνδεδεμένα στο ιδιωτικό δίκτυο. Οι περισσότερες εταιρείες σήμερα, έχουν δημιουργήσει εξειδικευμένα τμήματα πληροφορικής, που ασχολούνται αποκλειστικά με την κυβερνοασφάλεια (cybersecurity), με την διατήρηση των υπολογιστικών συστημάτων της εταιρείας ασφαλή αλλά και την αντιμετώπιση πιθανών κυβερνοεπιθέσεων σε περίπτωση που συμβούν.

Τέλος, βλέποντας κράτη σαν την Ελλάδα τα οποία δεν έχουν δώσει την πρέπουσα σημασία στην τεχνολογική εκπαίδευση των πολιτών και ιδιαίτερα στα σχολεία όπου τα μαθήματα πληροφορικής αντιμετωπίζονται σαν δευτερευούσης σημασίας, πρέπει να αρχίσουν να θεωρούν την τεχνολογική εκπαίδευση το ίδιο σημαντική με την εκπαίδευση που λαμβάνει ένα παιδί και για τις άλλες εξίσου σημαντικές επιστήμες. Αυτό είναι πολύ σημαντικό όχι μόνο για την μελλοντική επαγγελματική σταδιοδρομία του ατόμου, αλλά και γιατί με αυτόν τον τρόπο το άτομο αυτό θα μπορέσει να παραμείνει ασφαλές από κάθε είδους ηλεκτρονικού εγκλήματος στον κυβερνοχώρο.

Βιβλιογραφία

- [1] – Παναγιώτης Τσόπελας, Σεπτέμβριος 2005 [Διατριβή: Ορισμός και εφαρμογή δεικτών αξιοπιστίας σε πληροφοριακά δίκτυα και ανάπτυξη λογισμικού υποστήριξης - Κωδικός: 34838 \(ekt.gr\)](#)
- [2] – Larry L. Peterson & Bruce S. Davie “ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ ΜΙΑ ΠΡΟΣΕΓΓΙΣΗ ΑΠΟ ΤΗΝ ΑΠΟ ΤΗ ΣΚΟΠΙΑ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ” Εκδόσεις Κλειδάριθμος σελ. 34-35
- [3] - Larry L. Peterson & Bruce S. Davie “ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ ΜΙΑ ΠΡΟΣΕΓΓΙΣΗ ΑΠΟ ΤΗΝ ΑΠΟ ΤΗ ΣΚΟΠΙΑ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ” Εκδόσεις Κλειδάριθμος σελ. 359
- [4] – Παναγιώτης Μυλωνάς, Θεσσαλονίκη 2009 «Διαδίκτυο Και Εξάρτηση» [ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ \(uom.gr\)](#)
- [5] – Διονυσία Γούργαρη, Σεπτέμβριος 2021 «Τα ανθρώπινα δικαιώματα στον κυβερνοχώρο υπό το πρίσμα του διεθνούς δικαίου » [Microsoft Word - Διπλωματική εργασία.docx \(unipi.gr\)](#) σελ. 6&7
- [6] - «Κατανόηση του Ηλεκτρονικού Εγκλήματος και Στρατηγικές Πρόληψης και Αντιμετώπισής του, σε Εθνικό και Προσωπικό Επίπεδο», διπλωματική εργασία Αθανασίου Ζαννιά, Δημήτριος Τσιμπούκας Τμήμα Μηχανικών και Πληροφοριακών Συστημάτων Πανεπιστήμιο Αιγαίου Σάμος, Σεπτέμβριος 2017 [---icsd09032-icsd09145.pdf \(aegean.gr\)](#) σελ.20
- [7] - Κανονιστικό Πλαίσιο της Κοινωνίας της Πληροφορίας – Θέμα Παράδοσης 9: Παραβατικότητα και Ποινικό Δίκαιο στην Κοινωνία της Πληροφορίας -1 Πανεπιστήμιο Αιγαίου ΛΙΑΙΑΝ ΜΗΤΡΟΥ [διαθέσιμο στο διαδίκτυο] [714097945.doc \(live.com\)](#) σελ.3-4
- [8] - «Κατανόηση του Ηλεκτρονικού Εγκλήματος και Στρατηγικές Πρόληψης και Αντιμετώπισής του, σε Εθνικό και Προσωπικό Επίπεδο», διπλωματική εργασία Αθανασίου Ζαννιά, Δημήτριος Τσιμπούκας Τμήμα Μηχανικών και Πληροφοριακών Συστημάτων Πανεπιστήμιο Αιγαίου Σάμος, Σεπτέμβριος 2017 [---icsd09032-icsd09145.pdf \(aegean.gr\)](#) σελ.21
- [9] – Επίσημη σελίδα της εταιρείας Kaspersky [What is Cybercrime? Cybercrime Prevention & Cybercrime Security \(kaspersky.com\)](#)
- [10] - Κανονιστικό Πλαίσιο της Κοινωνίας της Πληροφορίας – Θέμα Παράδοσης 9: Παραβατικότητα και Ποινικό Δίκαιο στην Κοινωνία της Πληροφορίας -1 Πανεπιστήμιο Αιγαίου ΛΙΑΙΑΝ ΜΗΤΡΟΥ [διαθέσιμο στο διαδίκτυο] [714097945.doc \(live.com\)](#) σελ.4-5
- [11] - Carter David L., Ph. D. (1995 σε άρθρο που δημοσιεύτηκε τον Ιούλιο του 1995) Computer Crime Categories: How Techno-Criminals Operate, στο FBI Magazine [διαθέσιμο στο διαδίκτυο] [Computer Crime: How Techno-Criminals Operate \(upcounsel.com\)](#)
- [12] - [Κυβερνοέγκλημα & Ασφάλεια :: CyberInsuranceGreece.com](#)

- [13] – Επίσημη σελίδα Οργανισμού Ηνωμένων Εθνών [index \(unodc.org\)](https://www.unodc.org/)
- [14] - [Η Νομική Αντιμετώπιση των Επιθέσεων κατά Συστημάτων Πληροφοριών - Law and Tech](#)
- [15] - [The Novelty of ‘Cybercrime’ An Assessment in Light of Routine Activity Theory \(researchgate.net\)](#) σελ. 409
- [16] – Σημειώσεις από μάθημα ασφάλειας του Καποδιστριακού Πανεπιστημίου Αθηνών [Microsoft PowerPoint - 01-intro.ppt \(uoa.gr\)](#)
- [17] – William Stallings «Βασικές Αρχές Ασφάλειας δικτύων», τρίτη Αμερικανική έκδοση, Εκδόσεις Κλειδάριθμος σελ 24-29
- [18] – «Ηλεκτρονικό Έγκλημα: Μορφές Και Αντιμετώπιση» διπλωματική εργασία Αγγελάκη Χρήστου, Ιωσηφέλλη Ασπασία, Τμήμα Διοίκησης Επιχειρήσεων ΤΕΙ Δυτικής Ελλάδας, Μεσολόγγι 2018 σελ.14&15
[<4D6963726F736F667420576F7264202D20D0D4D5D7C9C1CAC720C5D1C3C1D3C9C120C7CBC5CAD4CFD1CDC9CACF20C5C3CACBC7CCC120CCCFD1D6C5D320CAC1C920C1CDD4C9CCC5D4D9D0C9D3C7> \(teiwest.gr\)](#)
- [19] - «Κατανόηση του Ηλεκτρονικού Εγκλήματος και Στρατηγικές Πρόληψης και Αντιμετώπισής του, σε Εθνικό και Προσωπικό Επίπεδο», διπλωματική εργασία Αθανασίου Ζαννιά, Δημήτριος Τσιμπούκας Τμήμα Μηχανικών και Πληροφοριακών Συστημάτων Πανεπιστήμιο Αιγαίου Σάμος, Σεπτέμβριος 2017 [- - icsd09032-icsd09145.pdf \(aegean.gr\)](#) σελ. 28&29&43
- [20] - [Malware - τι είναι, και πώς λειτουργεί η προστασία από το κακόβουλο λογισμικό | ESET](#)
- [21] – Επίσημη ιστοσελίδα της εταιρείας Fortinet. Τι είναι ένας δούρειος ίππος; [What Is a Trojan Horse? Trojan Virus and Malware Explained | Fortinet](#)
- [22] - Επίσημη ιστοσελίδα της εταιρείας Fortinet. Τι είναι ένας ηλεκτρονικός ιός ; [What are Computer Viruses? | Definition & Types of Computer Viruses \(fortinet.com\)](#)
- [23] – Επίσημη ιστοσελίδα της εταιρείας Fortinet. Τι είναι ένα ηλεκτρονικό σκουλήκι; [What Is a Worm Virus \(Computer Worm\)? | Fortinet](#)
- [24] – Επίσημη ιστοσελίδα της εταιρείας Fortinet. Τι είναι το λογισμικό κατασκοπείας; [What Is Spyware? Definition, Types And Protection | Fortinet](#)
- [25] – Επίσημη ιστοσελίδα της εταιρείας Fortinet. Τι είναι το λογισμικό rootkit; [What Is a Rootkit? How to Defend and Stop Them? | Fortinet](#)
- [26] - Επίσημη ιστοσελίδα της εταιρείας Fortinet. Τι είναι το λογισμικό ransomware; [What Is Ransomware? How to Prevent Ransomware Attacks? | Fortinet](#)
- [27] - Επίσημη ιστοσελίδα της εταιρείας Fortinet. Τι είναι DDoS επιθέσεις; [What is a DDoS Attack? DDoS Meaning, Definition & Types | Fortinet](#)

- [28] – Επίσημο αρχείο της εταιρείας Fortinet. Advanced Threats, Advanced Solutions: Integrating a Sandbox Into Your Infrastructure [Integrating a Sandbox Into Your Infrastructure \(fortinet.com\)](https://www.fortinet.com)
- [29] - William Stallings «Βασικές Αρχές Ασφάλειας δικτύων», τρίτη Αμερικανική έκδοση, Εκδόσεις Κλειδάριθμος σελ.440 & 441
- [30] - Simson Garfinkel & Gene Spafford, «Practical UNIX & Internet Security», δεύτερη έκδοση, εκδόσεις O'Reilly & Associates, Κεφάλαιο 11.1.7. [\[Chapter 11\] Protecting Against Programmed Threats \(deu.edu.tr\)](https://www.deu.edu.tr/~gspafford/UNIX/Chapter11.htm)
- [31] - William Stallings «Βασικές Αρχές Ασφάλειας δικτύων», τρίτη Αμερικανική έκδοση, Εκδόσεις Κλειδάριθμος σελ.397
- [32] – Επίσημη ιστοσελίδα της εταιρείας Fortinet. Τι είναι το hacking; [What Is Hacking? Types of Hacking & More | Fortinet](https://www.fortinet.com/resources/white-papers/what-is-hacking.html)
- [33] - Επίσημη σελίδα της εταιρείας Kaspersky. [What is hacking and how does hacking work? \(kaspersky.com\)](https://www.kaspersky.com/resources/what-is-hacking)
- [34] – Επίσημη ιστοσελίδα του South African portal for resources and information on Cybercrime. [Cracking Definition | Cybercrime.org.za | Safety & Security Guide](https://www.cybercrime.org.za/)
- [35] – Επίσημη ιστοσελίδα του κέντρου εθνικής κυβερνοασφάλειας του Ηνωμένου Βασιλείου. [Phishing attacks: defending your organisation - NCSC.GOV.UK](https://www.ncsc.gov.uk/infrastructure/phishing-attacks)
- [36] – Επίσημη ιστοσελίδα της εταιρείας Microsoft. Τι είναι το ηλεκτρονικό «ψάρεμα» - phishing; [Τι είναι το ηλεκτρονικό "ψάρεμα"; | Ασφάλεια της Microsoft](https://www.microsoft.com/en-us/security/default?cid=11111111-1111-1111-1111-111111111111)
- [37] – «ΑΝΕΠΙΘΥΜΗΤΑ ΗΛΕΚΤΡΟΝΙΚΑ ΜΗΝΥΜΑΤΑ: ΕΠΙΠΤΩΣΕΙΣ ΚΑΙ ΑΝΤΙΜΕΤΡΑ», διπλωματική εργασία του Νικόλαου Βελιμαχίτη, Τμήμα Μηχανικών και Πληροφοριακών Συστημάτων Πανεπιστήμιο Αιγαίου Σάμος, Μάρτιος 2020 [Ανεπιθύμητα ηλεκτρονικά μηνύματα: επιπτώσεις και αντίμετρα \(aegean.gr\)](https://www.aegean.gr/~/media/Files/Εργασίες/Διπλωματικές/2020/Ανεπιθύμητα_ηλεκτρονικά_μηνύματα_επιπτώσεις_και_αντίμετρα/Ανεπιθύμητα_ηλεκτρονικά_μηνύματα_επιπτώσεις_και_αντίμετρα.pdf) σελ. 8-10
- [38] – «Ηλεκτρονικό Έγκλημα», πτυχιακή εργασία της Σαρτέρη Βερόνικας, Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών Πανεπιστήμιο Δυτικής Αττικής [cse 41789.pdf \(uniwa.gr\)](https://www.uniwa.gr/~/media/Files/Πτυχιακές/2018/Σαρτέρη_Βερόνικα/Ηλεκτρονικό_Έγκλημα.pdf) σελ. 24&25
- [39] – «Ηλεκτρονικό Έγκλημα : Μορφές και Αντιμετώπιση», πτυχιακή εργασία Αγγελάκη Χρήστου και Ιωσηφέλλη Ασπασία, Τμήμα Διοίκησης Επιχειρήσεων ΤΕΙ Δυτικής Ελλάδας, Μεσολόγγι 2018
[<4D6963726F736F667420576F7264202D20D0D4D5D7C9C1CAC720C5D1C3C1D3C9C120C7CBC5CAD4CFD1CDC9CACF20C5C3CACBC7CCC120CCCFD1D6C5D320CAC1C920C1CDD4C9CCC5D4D9D0C9D3C7> \(teiwest.gr\)](https://www.teiwest.gr/~/media/Files/Πτυχιακές/2018/Αγγελάκης_Χρήστος_και_Ιωσηφέλλη_Ασπασία/Ηλεκτρονικό_Έγκλημα_Μορφές_και_Αντιμετώπιση.pdf) σελ.26-28
- [40] – Επίσημη σελίδα του τμήματος Δίωξης Ηλεκτρονικού Εγκλήματος. Τι είναι οι Νιγηριανές επιστολές; [Νιγηριανή Απάτη – CYBERALERT](https://www.cyberalert.gr/)
- [41] - «Ηλεκτρονικό Έγκλημα : Μορφές και Αντιμετώπιση», πτυχιακή εργασία Αγγελάκη Χρήστου και Ιωσηφέλλη Ασπασία, Τμήμα Διοίκησης Επιχειρήσεων ΤΕΙ Δυτικής Ελλάδας, Μεσολόγγι 2018

<4D6963726F736F667420576F7264202D20D0D4D5D7C9C1CAC720C5D1C3C1D3C9C12
0C7CBC5CAD4CFD1CDC9CACF20C5C3CACBC7CCC120CCCFD1D6C5D320CAC1C92
0C1CDD4C9CCC5D4D9D0C9D3C7> (teiwest.gr) σελ.24

[42] - Επίσημη ιστοσελίδα της εταιρείας Fortinet. Διαφορές μεταξύ κλοπής ταυτότητας και απάτης ταυτότητας. [What Is Identity Theft? Identity Fraud vs. Identity Theft | Fortinet](#)

[43] – Άρθρο του εγκληματολόγου κ. Δημήτρη Μπισιούκη για την παιδική πορνογραφία στο «Διεθνές Ινστιτούτο Κυβερνοασφάλειας» [Η παιδική πορνογραφία στο διαδίκτυο. Πώς λειτουργεί και τι πρέπει να γνωρίζουμε - CSI - Cyber Security International Institute](#)

[44] –Επιστημονική αναφορά «CRIMINAL LAW BULLETIN Volume 54, Number 1 : CYBERSEX TRAFFICKING: TOWARD A MORE EFFECTIVE PROSECUTORIAL RESPONSE Joshua T. Carback, [Cybersex Trafficking: Toward a More Effective Prosecutorial Response by Joshua Carback :: SSRN](#) σελ. 99 & 100 / pdf σελ .38 & 39

[45] – Επίσημη ιστοσελίδα για την αναφορά περιπτώσεων διαδικτυακής παρενόχλησης του πανεπιστημίου του Durham. [What is online harassment? - Report + Support - Durham University](#)

[46] – Επίσημη ιστοσελίδα της εταιρείας bitdefender. Ο ορισμός για τον διαδικτυακό εκφοβισμό. [Διαδικτυακή Παρενόχληση: Ενημερωθείτε κατάλληλα | Bitdefender](#)

[47] - «Ηλεκτρονικό Έγκλημα», πτυχιακή εργασία της Σαρτέρη Βερόνικας, Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών Πανεπιστήμιο Δυτικής Αττικής [cse_41789.pdf \(uniwa.gr\)](#) σελ. 21 & 22

[48] – «The internet and drug markets», επιστημονική αναφορά του Ευρωπαϊκού Κέντρου Παρακολούθησης Ναρκωτικών και Τοξικομανίας, [TDXD16001ENN_FINAL.pdf \(soton.ac.uk\)](#) σελ. 13-14

[49] – «Κυβερνοτρομοκρατία : εννοιολογική προσέγγιση μίας πραγματικής απειλής», διπλωματική εργασία Βουλκίδη Κωνσταντίνου, τμήμα νομικής του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης, Θεσσαλονίκη, Σεπτέμβριος 2018 [GRI-2019-23303.pdf \(auth.gr\)](#) σελ. 36-39

[50] – «ΚΥΒΕΡΝΟΤΡΟΜΟΚΡΑΤΙΑ ΚΑΙ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΕ ΠΑΓΚΟΣΜΙΟ ΚΑΙ ΕΘΝΙΚΟ ΕΠΙΠΕΔΟ - ΟΙ ΠΡΟΚΛΗΣΕΙΣ ΚΑΙ ΤΑ ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ -», διπλωματική εργασία της Θάλειας Δερμεντζή για το διδρυματικό μεταπτυχιακό πρόγραμμα σπουδών του Πανεπιστημίου Μακεδονίας – τμήμα εφαρμοσμένης πληροφορικής και του Αριστοτελείου Πανεπιστημίου – τμήμα νομικής, Φεβρουάριος 2022 Θεσσαλονίκη [DermentziThaliaMsc2022.pdf \(uom.gr\)](#) σελ. 15 & 16

[51] – «Ο Πόλεμος», Ηρακλείδης Αλέξιος, προπτυχιακό εγχειρίδιο σπουδών για θέματα διεθνών σχέσεων και διεθνών πολιτικών για σχολές πολιτικών επιστημών [01_chapter_5.pdf \(kallipos.gr\)](#) σελ.93

[52] – «ΚΥΒΕΡΝΟΠΟΛΕΜΟΣ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗ ΑΠΕΙΛΩΝ. ΣΥΓΚΡΙΤΙΚΗ ΑΝΑΛΥΣΗ ΚΑΙ ΣΤΡΑΤΗΓΙΚΗ ΓΙΑ ΤΗΝ ΕΛΛΑΔΑ», διπλωματική εργασία Νικόλαου Τερεζί για το διδρυματικό μεταπτυχιακό πρόγραμμα σπουδών του Πανεπιστημίου Μακεδονίας – τμήμα Διεθνών και Ευρωπαϊκών Σπουδών τμήμα Βαλκανικών, Σλαβικών και

Ανατολικών σπουδών και της Ανώτατης Διακλαδικής Σχολής Πολέμου, Δεκέμβριος 2018
[4D6963726F736F667420576F7264202D20C4C9D0CBD9CCC1D4C9CAC720C5D1C3C1D3C9C1](https://www.uom.gr/4D6963726F736F667420576F7264202D20C4C9D0CBD9CCC1D4C9CAC720C5D1C3C1D3C9C1) > (uom.gr) σελ. 19 & 20

[53] – «Κυβερνοπόλεμος Και Επιθέσεις Στο Διαδίκτυο», διπλωματική εργασία της Σίμους Φλώρας, τμήμα Μηχανικών και Πληροφοριακών Συστημάτων Πανεπιστήμιο Αιγαίου Σάμος, Οκτώβρης 2016 [Κυβερνοπόλεμος και επιθέσεις στο διαδίκτυο \(aegean.gr\)](https://www.aegean.gr/kybernopolemos-kei-epitheseis-sto-diadiktyo) σελ.10

[54] – «Κυβερνοπόλεμος και Ελληνικές ΕΔ: παρούσα κατάσταση, μελλοντικές προοπτικές», διπλωματική εργασία του Στέργιου Αναστασιάδη, τμήμα Διεθνών, Ευρωπαϊκών και Περιφερειακών σπουδών του Πάντειο Πανεπιστήμιο, Αθήνα, 2019 [Pandemos - Digital Library, Panteion University](https://panteion.gr/pandemos-digital-library) σελ.30 & 31

[55] – «Η Πολιτική Ασφαλείας Της Κίνας Στον Κυβερνοχώρο», διπλωματική εργασία της Δημητρακοπούλου Μαρίας, τμήμα Τμήμα Διεθνών και Ευρωπαϊκών Σπουδών Πανεπιστήμιο Πειραιώς 2018. [Πανεπιστήμιο Πειραιώς \(unipi.gr\)](https://www.unipi.gr/pανεπιστημιο-πειραιως) σελ. 19

[56] – «Ο ΚΥΒΕΡΝΟΠΟΛΕΜΟΣ ΩΣ ΠΟΛΥΔΙΑΣΤΑΣΤΟ ΣΤΡΑΤΗΓΙΚΟ ΕΡΓΑΛΕΙΟ ΚΑΙ Η ΕΦΑΡΜΟΓΗ ΤΟΥ ΣΕ ΚΡΙΣΙΜΕΣ ΣΤΡΑΤΙΩΤΙΚΕΣ ΚΑΙ ΜΗ ΥΠΟΔΟΜΕΣ», μεταπτυχιακή διατριβή του Τατσούλη Περικλή για το διδρυματικό μεταπτυχιακό πρόγραμμα σπουδών του Πολυτεχνείου Κρήτης – τμήμα Μηχανιών Παραγωγής και Διοίκησης και της Στρατιωτικής Σχολής Ευελπίδων – τμήμα Στρατιωτικών Επιστημών. Μάιος 2019 [Tsatsoulis Periklis MSc 2019 \(2\).pdf](https://www.tsatsoulis-periklis-msc-2019-2.pdf) σελ. 33-36

[57] - Επίσημη ιστοσελίδα της εταιρείας Fortinet. Τι είναι ο κυβερνοπόλεμος; [What Is Cyber Warfare? | Fortinet](https://www.fortinet.com/what-is-cyber-warfare)

[58] – Επίσημη ιστοσελίδα του Οργανισμού Κυβερνοασφάλειας και Ασφάλειας Υποδομών των Η.Π.Α. [Critical Infrastructure Sectors | CISA](https://www.cisa.gov/critical-infrastructure-sectors)

[59] - Επίσημη ιστοσελίδα του Οργανισμού Κυβερνοασφάλειας και Ασφάλειας Υποδομών των Η.Π.Α. Τομέας χημικών υποδομών. [Chemical Sector | CISA](https://www.cisa.gov/chemical-sector)

[60] - Επίσημη ιστοσελίδα του Οργανισμού Κυβερνοασφάλειας και Ασφάλειας Υποδομών των Η.Π.Α. Τομέας επικοινωνιών [Communications Sector | CISA](https://www.cisa.gov/communications-sector)

[61] - Επίσημη ιστοσελίδα του Οργανισμού Κυβερνοασφάλειας και Ασφάλειας Υποδομών των Η.Π.Α. Τομέας εμπορικών εγκαταστάσεων. [Commercial Facilities Sector | CISA](https://www.cisa.gov/commercial-facilities-sector)

[62] - Επίσημη ιστοσελίδα του Οργανισμού Κυβερνοασφάλειας και Ασφάλειας Υποδομών των Η.Π.Α. Κατασκευαστικός τομέας. [Critical Manufacturing Sector | CISA](https://www.cisa.gov/critical-manufacturing-sector)

[63] – Επίσημη ιστοσελίδα του Οργανισμού Κυβερνοασφάλειας και Ασφάλειας Υποδομών των Η.Π.Α. Τομέας φραγμάτων νερού. [Dams Sector | CISA](https://www.cisa.gov/dams-sector)

[64] - Επίσημη ιστοσελίδα του Οργανισμού Κυβερνοασφάλειας και Ασφάλειας Υποδομών των Η.Π.Α. Τομέας βιομηχανίας άμυνας. [Defense Industrial Base Sector | CISA](https://www.cisa.gov/defense-industrial-base-sector)

[65] - Επίσημη ιστοσελίδα του Οργανισμού Κυβερνοασφάλειας και Ασφάλειας Υποδομών των Η.Π.Α. Τομέας επειγουσών υπηρεσιών. [Emergency Services Sector | CISA](https://www.cisa.gov/emergency-services-sector)

- [66] - Επίσημη ιστοσελίδα του Οργανισμού Κυβερνοασφάλειας και Ασφάλειας Υποδομών των Η.Π.Α. Τομέας ενέργειας. [Energy Sector | CISA](#)
- [67] - Επίσημη ιστοσελίδα του Οργανισμού Κυβερνοασφάλειας και Ασφάλειας Υποδομών των Η.Π.Α. Τομέας χρηματοπιστωτικών υπηρεσιών. [Financial Services Sector | CISA](#)
- [68] - Επίσημη ιστοσελίδα του Οργανισμού Κυβερνοασφάλειας και Ασφάλειας Υποδομών των Η.Π.Α. Τομέας τροφίμων και γεωργίας. [Food and Agriculture Sector | CISA](#)
- [69] - Επίσημη ιστοσελίδα του Οργανισμού Κυβερνοασφάλειας και Ασφάλειας Υποδομών των Η.Π.Α. Τομέας κυβερνητικών εγκαταστάσεων. [Government Facilities Sector | CISA](#)
- [70] - Επίσημη ιστοσελίδα του Οργανισμού Κυβερνοασφάλειας και Ασφάλειας Υποδομών των Η.Π.Α. Τομέας υγειονομικής περίθαλψης και δημόσιας υγείας. [Healthcare and Public Health Sector | CISA](#)
- [71] - Επίσημη ιστοσελίδα του Οργανισμού Κυβερνοασφάλειας και Ασφάλειας Υποδομών των Η.Π.Α. Τομέας πληροφορικής. [Information Technology Sector | CISA](#)
- [72] - Επίσημη ιστοσελίδα του Οργανισμού Κυβερνοασφάλειας και Ασφάλειας Υποδομών των Η.Π.Α. Τομέας πυρηνικών αντιδραστήρων, υλικών και αποβλήτων. [Nuclear Reactors, Materials, and Waste Sector | CISA](#)
- [73] - Επίσημη ιστοσελίδα του Οργανισμού Κυβερνοασφάλειας και Ασφάλειας Υποδομών των Η.Π.Α. Τομέας συστημάτων μεταφορών. [Transportation Systems Sector | CISA](#)
- [74] - Επίσημη ιστοσελίδα του Οργανισμού Κυβερνοασφάλειας και Ασφάλειας Υποδομών των Η.Π.Α. Τομέας συστημάτων υδάτων και λυμάτων. [Water and Wastewater Systems Sector | CISA](#)
- [75] - Επιστημονικό άρθρο με τίτλο «Reflections on Cyberweapons Controls» , της Dorothy Denning για το Computer Security Journal το έτος 2000. [Reflections on Cyberweapons Controls \(nps.edu\)](#) σελ. 4-6
- [76] – Επιστημονικό άρθρο με τίτλο «Cybercrime To Cost The World \$10.5 Trillion Annually By 2025», του Steve Morgan για το επιστημονικό περιοδικό Cybersecurity Ventures το έτος 2021. [Cybercrime To Cost The World \\$10.5 Trillion Annually By 2025 \(cybersecurityventures.com\)](#)
- [77] - Στοιχεία που αντλήθηκαν από το nibusinessinfo.co.uk, μια δωρεάν υπηρεσία που προσφέρεται από το Invest Northern Ireland, το επίσημο διαδικτυακό κανάλι για επιχειρηματικές συμβουλές και καθοδήγηση στη Βόρεια Ιρλανδία. [Impact of cyber attack on your business | nibusinessinfo.co.uk](#)
- [78] – Στοιχεία που αντλήθηκαν από επιστημονικό άρθρο με τίτλο «Legal consequences of a cyber attack», του δικηγόρου και υπεύθυνου προστασίας δεδομένων και απορρήτου Clive Mackintosh, εκ μέρους της εταιρείας παροχής νομικών υπηρεσιών Harper James. [Cyber attack: Legal consequences of data privacy breaches \(harperjames.co.uk\)](#)
- [79] – Επιστημονικό άρθρο στο LinkedIn με τίτλο «Disruptions To Business Operations Become More Frequent Outcomes Of Cyber Attacks Than Financial Losses», του διευθυντή

κυβερνοασφάλειας της εταιρείας KMPG στην Ρουμανία Gheorghe Vlad. [Disruptions to business operations become more frequent outcomes of cyber attacks than financial losses | LinkedIn](#)

[80] – Επίσημη ιστοσελίδα της εταιρείας Malwarebytes που ασχολείται με την αποτροπή και την αντιμετώπιση κακόβουλων λογισμικών. Τι είναι η παραβίαση δεδομένων (data breach); [What is a Data Breach? | Malwarebytes](#)

[81] – Στοιχεία που αντλήθηκαν από άρθρο για το περιοδικό Security Magazine, του Bill Campbell Αντιπρόεδρος της Βόρειας Αμερικής στην Υποδομή Ασφαλείας και Γεωχωρικής διαίρεσης της Hexagon. [The time to improve public safety cybersecurity is now | Security Magazine](#)

[82] – Στοιχεία που αντλήθηκαν από την επιστημονική αναφορά των Ortwin Renn, Aleksandar Jovanovic και Regina Schröter, ως συνεισφορά για το επιστημονικό έργο “Future Global Shocks” του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης (OECD), Ιανουάριος 2011. [Social Unrest \(draft V 1 \(oecd.org\)](#) σελ. 10&11

[83] – Στοιχεία που αντλήθηκαν από το επιστημονικό άρθρο του Παγκόσμιου Οικονομικού Φόρουμ με τίτλο “Cybersecurity in this era of polycrisis”, των Giulia Moschetta ειδικός Έρευνας και Ανάλυσης στο Κέντρο Κυβερνοασφάλειας, Παγκόσμιο Οικονομικό Φόρουμ, Filipe Beato υπεύθυνος στο Κέντρο Κυβερνοασφάλειας, Παγκόσμιο Οικονομικό Φόρουμ και Akshay Joshi επικεφαλής Βιομηχανίας και Συνεργασιών, Κέντρο Κυβερνοασφάλειας, Παγκόσμιο Οικονομικό Φόρουμ, 24 Φεβρουαρίου 2023 [Cybersecurity must be tightened up in this era of polycrisis | World Economic Forum \(weforum.org\)](#)

[84] – Στοιχεία που αντλήθηκαν από το ενημερωτικό φυλλάδιο του Ευρωκοινοβουλίου με τίτλο «Κυβερνοπόλεμος: από επιστημονική φαντασία, πραγματικότητα;», σχετικά με την μεταφορά του κυβερνοπολέμου από την θεωρία στην πράξη [03A-DV-PRESSE STO\(2010\)10-25\(89965\) EL.pdf \(europa.eu\)](#)

[85] – Άρθρο του βρετανικού μέσου ενημέρωσης BBC με τίτλο “How a cyber attack transformed Estonia”, γραμμένο από τον Damien McGuinness τον Απρίλιο του 2017. [How a cyber attack transformed Estonia - BBC News](#)

[86] – Άρθρο του κ. Χρήστου Δήμτσα για τον κυβερνοπόλεμο στο Διεθνές Ινστιτούτο Κυβερνοασφάλειας (CSLi), με τίτλο «Από τα τουφέκια στα πληκτρολόγια». [Από τα τουφέκια στα πληκτρολόγια - CSLi - Cyber Security International Institute](#)

[87] – Άρθρο του John Markoff για την Αμερικάνικη εφημερίδα New York Times με τίτλο “Before the Gunfire, Cyberattacks”, Αύγουστος 2008. [Before the Gunfire, Cyberattacks - The New York Times \(nytimes.com\)](#)

[88] – Στοιχεία που αντλήθηκαν από το μέσο ενημέρωσης TV χωρίς σύνορα (tvxs), Ιούνιος 2012. [Stuxnet, το «σκουλήκι» των ΗΠΑ για κυβερνοπόλεμο στο Ιράν \(tvxs.gr\)](#)

[89] – Άρθρο του Μιχάλη Ψύλου για την εφημερίδα Ναυτεμπορική με τίτλο «Ο ατέλειωτος κυβερνοπόλεμος της Ρωσίας κατά της Ουκρανίας», Φεβρουάριος 2022. [Ο ατέλειωτος κυβερνοπόλεμος της Ρωσίας κατά της Ουκρανίας \(naftemporiki.gr\)](#)

- [90] – Επίσημη αναφορά από την εταιρεία Microsoft σχετικά με τα κακόβουλα λογισμικά που στοχεύουν τους Ουκρανικούς οργανισμούς με τίτλο “Destructive malware targeting Ukrainian organizations”. [Destructive malware targeting Ukrainian organizations - Microsoft Security Blog](#)
- [91] - «Ο ΚΥΒΕΡΝΟΠΟΛΕΜΟΣ ΩΣ ΠΟΛΥΔΙΑΣΤΑΣΤΟ ΣΤΡΑΤΗΓΙΚΟ ΕΡΓΑΛΕΙΟ ΚΑΙ Η ΕΦΑΡΜΟΓΗ ΤΟΥ ΣΕ ΚΡΙΣΙΜΕΣ ΣΤΡΑΤΙΩΤΙΚΕΣ ΚΑΙ ΜΗ ΥΠΟΔΟΜΕΣ», μεταπτυχιακή διατριβή του Τατσούλη Περικλή για το διδρυματικό μεταπτυχιακό πρόγραμμα σπουδών του Πολυτεχνείου Κρήτης – τμήμα Μηχανιών Παραγωγής και Διοίκησης και της Στρατιωτικής Σχολής Ευελπίδων – τμήμα Στρατιωτικών Επιστημών. Μάιος 2019 [Ο κυβερνοπόλεμος ως πολυδιάστατο στρατηγικό εργαλείο και η εφαρμογή του σε κρίσιμες στρατιωτικές και μη υποδομές - Ιδρυματικό Αποθετήριο \(tuc.gr\)](#) σελ.37
- [92] - «Κατανόηση του Ηλεκτρονικού Εγκλήματος και Στρατηγικές Πρόληψης και Αντιμετώπισής του, σε Εθνικό και Προσωπικό Επίπεδο», διπλωματική εργασία Αθανασίου Ζαννιά, Δημήτριος Τσιμπούκας Τμήμα Μηχανικών και Πληροφοριακών Συστημάτων Πανεπιστήμιο Αιγαίου Σάμος, Σεπτέμβριος 2017 [-- -icsd09032-icsd09145.pdf \(aegean.gr\)](#) σελ. 59
- [93] – «ΗΛΕΚΤΡΟΝΙΚΑ – ΔΙΑΔΙΚΤΙΑΚΑ ΕΓΚΛΗΜΑΤΑ : ΚΑΤΗΓΟΡΙΕΣ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗ ΑΥΤΩΝ», διπλωματική εργασία του Γιώργου Αλεξάκη, τμήμα Ψηφιακών Συστημάτων Πανεπιστήμιο Πειραιά, [ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ \(unipi.gr\)](#) σελ.23 & 24
- [93.1] – Άρθρο του Alan Henry στην ιστοσελίδα lifehacker με τίτλο “The Difference Between Antivirus and Anti-Malware (and Which to Use)”, Αύγουστος 2013 [The Difference Between Antivirus and Anti-Malware \(and Which to Use\) \(lifehacker.com\)](#)
- [94] – Επίσημη ιστοσελίδα της εταιρείας Kaspersky. Τι είναι το τείχος προστασίας – firewall. [What is a Firewall? How Firewalls Work & Types of Firewalls \(kaspersky.com\)](#)
- [94.1] – National Institute of Standards and Security (NIST) «Οδηγίες για τα firewalls και για τις πολιτικές των firewalls» Karen Scarfone, Paul Hoffman, Σεπτέμβριος 2009, [Wayback Machine \(archive.org\)](#) σελ.2-1 έως 2-9
- [95] - «Κατανόηση του Ηλεκτρονικού Εγκλήματος και Στρατηγικές Πρόληψης και Αντιμετώπισής του, σε Εθνικό και Προσωπικό Επίπεδο», διπλωματική εργασία Αθανασίου Ζαννιά, Δημήτριος Τσιμπούκας Τμήμα Μηχανικών και Πληροφοριακών Συστημάτων Πανεπιστήμιο Αιγαίου Σάμος, Σεπτέμβριος 2017 [-- -icsd09032-icsd09145.pdf \(aegean.gr\)](#) σελ. 65-90
- [96] – «ΤΕΧΝΟΛΟΓΙΕΣ ΤΑΥΤΟΠΟΙΗΣΗΣ ΧΡΗΣΤΩΝ ΜΕ ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ», πτυχιακή εργασία του Νικόλαου Γάσπαρη και του Αναστάσιου Μαστροκώστα, σχολή Οικονομικών Επιστημών και Διοίκησης Επιχειρήσεων, τμήμα Διοίκησης Τουρισμού Πανεπιστήμιο Πατρών, Ιούλιος 2020. [<4D6963726F736F667420576F7264202D20C3C1D3D0C1D1C7D32D20CCC1D3D4D1CFCAD9D3D4C1D3> \(teimes.gr\)](#) σελ. 20
- [97] - «Μέθοδοι Δημιουργίας Συνθηματικών», διπλωματική εργασία του Παναγιώτη Ταγματάρχη, τμήμα Μηχανικών και Πληροφοριακών Συστημάτων Πανεπιστήμιο Αιγαίου Σάμος, Μάιος 2021. [Microsoft Word - ÎœÎ \(aegean.gr\)](#) σελ. 4

- [97.1] – «Εγχειρίδιο Κυβερνοασφάλειας - Cybersecurity Handbook» Υπουργείο Ψηφιακής Διακυβέρνησης, Ιούνιος 2021, [Εγχειρίδιο-Κυβερνοασφάλειας.pdf \(mindigital.gr\)](#) σελ 20 & 21
- [97.2] – Άρθρο στο LinkedIn με τίτλο “The Importance of Two-Factor Authentication in Preventing Cyber attacks”, του Ritik Shrivastava, Μάρτιος 2023, [\(1\) The Importance of Two-Factor Authentication in Preventing Cyber attacks | LinkedIn](#)
- [97.3] – «Συχνές Ερωτήσεις - Απαντήσεις για το Ε.Μ.Επ.», Υπουργείο Ψηφιακής Διακυβέρνησης, [Συχνές Ερωτήσεις - Απαντήσεις για το Ε.Μ.Επ. | Γενική Γραμματεία Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης \(gsis.gr\)](#)
- [97.4] – «Επιβεβαίωση της ταυτότητας των χρηστών gov.gr μέσω TaxisNet ή e-banking», Οδηγός του Πολίτη, Απρίλιος 2020, [Επιβεβαίωση της ταυτότητας των χρηστών gov.gr μέσω TaxisNet ή e-banking \(odigostoupoliti.eu\)](#)
- [97.5] – «Επιβεβαίωση ταυτότητας των χρηστών gov.gr μέσω TaxisNet, e-banking, ηλεκτρονικής υπογραφής», Οδηγός του Πολίτη, Σεπτέμβριος 2020, [Επιβεβαίωση ταυτότητας των χρηστών gov.gr μέσω TaxisNet, e-banking, ηλεκτρονικής υπογραφής \(odigostoupoliti.eu\)](#)
- [98] – «Κρυπτογραφία και κρυπτανάλυση από την αρχαιότητα μέχρι σήμερα», διπλωματική εργασία των Καραμολέγκου Άννα-Νεφέλη και Κρδονούρη Αλεξάνδρα, Σχολή Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών, Εθνικό Μετσόβειο Πολυτεχνείο Νοέμβριος 2011. [Κρυπτογραφία και κρυπτανάλυση από την αρχαιότητα μέχρι σήμερα \(ntua.gr\)](#) σελ. 3&4
- [99] - William Stallings «Κρυπτογραφία και Ασφάλεια Δικτύων», πρώτη Ελληνική έκδοση, Εκδόσεις Ίων σελ. 16-21 & 32-39 & 284-291
- [100] – Επίσημη ιστοσελίδα της εταιρείας Norton. “Eleven ways to help protect yourself against cybercrime”, συγγραφέας Alison Grace Johansen, Αύγουστος 2020. [11 Ways to Help Protect Yourself From Cybercrime | Norton](#)
- [101] - Επίσημη ιστοσελίδα του Οργανισμού Κυβερνοασφάλειας και Ασφάλειας Υποδομών των Η.Π.Α. Οδηγός ασφάλειας στον κυβερνοχώρο. [Shields Up | CISA](#)
- [102] - Επίσημη ιστοσελίδα του Οργανισμού Κυβερνοασφάλειας και Ασφάλειας Υποδομών των Η.Π.Α. Οδηγός ασφάλειας στον κυβερνοχώρο για τους οργανισμούς και τις εταιρείες. [Shields Up: Guidance for Organizations | CISA](#)
- [103] – Σημειώσεις μαθήματος «Προστασία και Ασφάλεια Υπολογιστικών Συστημάτων», διδάσκων Κ.Βασιλάκης, Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών, [Microsoft Word - notes.doc \(uoa.gr\)](#) Κεφάλαιο 10 «Συστήματα Ανίχνευσης Εισβολών»

