ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ
ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ - ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ ΚΑΙ ΑΝΙΧΝΕΥΣΗ ΕΙΣΒΟΛΩΝ ΣΕ ΕΞΥΠΝΕΣ ΣΥΣΚΕΥΕΣ

ΑΛΕΞΑΝΔΡΗΣ ΡΑΦΑΗΛ ΑΛΕΞΑΝΔΡΟΣ

ΠΤΥΧΑΚΗ ΕΡΓΑΣΙΑ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ

Παναγιώτης Βαρζάκας
Δρ. Μέλος ΔΕΠ, Καθηγητής Α βαθμίδας
Τμήμα Πληροφορικής και Τηλεπικοινωνιών

ΣΥΝΕΠΙΒΛΕΠΟΥΣΑ
Μαρία Κοζύρη

Λαμία, Οκτώβριος 2020

UNIVERSITY OF
THESSALY

SCHOOL OF SCIENCE

DEAPRTMENT OF COMPUTER SCIENCE &
TELECOMMUNICATIONS

CYBERCRIME – MALICIOUS SOFTWARE AND INTRUSION DETECTION ON SMART DEVICES

ALEXANDRIS RAFAIL ALEXANDROS

FINAL THESIS

ADVISOR

Dr.Panagiotis Varzakas
Department of Computer Science
and Telecommunications

CO ADVISOR
Maria Koziri

Lamia, October 2020

«Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις [1], που προβλέπονται από της διατάξεις της παρ. 6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι:

*1. Δεν παραθέτω κομμάτια βιβλίων ή άρθρων ή εργασιών άλλων αυτολεξεί **χωρίς να τα περικλείω σε εισαγωγικά** και χωρίς να αναφέρω το συγγραφέα, τη χρονολογία, τη σελίδα. Η αυτολεξεί παράθεση χωρίς εισαγωγικά χωρίς αναφορά στην πηγή, είναι λογοκλοπή. Πέραν της αυτολεξεί παράθεσης, λογοκλοπή θεωρείται και η παράφραση εδαφίων από έργα άλλων, συμπεριλαμβανομένων και έργων συμφοιτητών μου, καθώς και η παράθεση στοιχείων που άλλοι συνέλεξαν ή επεξεργάσθηκαν, χωρίς αναφορά στην πηγή. Αναφέρω πάντοτε με πληρότητα την πηγή κάτω από τον πίνακα ή σχέδιο, όπως στα παραθέματα.*

*2. Δέχομαι ότι η αυτολεξεί **παράθεση χωρίς εισαγωγικά**, ακόμα κι αν συνοδεύεται από αναφορά στην πηγή σε κάποιο άλλο σημείο του κειμένου ή στο τέλος του, είναι αντιγραφή. Η αναφορά στην πηγή στο τέλος π.χ. μιας παραγράφου ή μιας σελίδας, δεν δικαιολογεί συρραφή εδαφίων έργου άλλου συγγραφέα, έστω και παραφρασμένων, και παρουσίασή τους ως δική μου εργασία.*

3. Δέχομαι ότι υπάρχει επίσης περιορισμός στο μέγεθος και στη συχνότητα των παραθεμάτων που μπορώ να εντάξω στην εργασία μου εντός εισαγωγικών. Κάθε μεγάλο παράθεμα (π.χ. σε πίνακα ή πλαίσιο, κλπ), προϋποθέτει ειδικές ρυθμίσεις, και όταν δημοσιεύεται προϋποθέτει την άδεια του συγγραφέα ή του εκδότη. Το ίδιο και οι πίνακες και τα σχέδια

4. Δέχομαι όλες τις συνέπειες σε περίπτωση λογοκλοπής ή αντιγραφής.

Ημερομηνία: 16/10/2020

Ο Δηλών

Αλεξανδρής Ραφαήλ Αλέξανδρος

(1) «Όποιος εν γνώσει του δηλώνει ψευδή γεγονότα ή αρνείται ή αποκρύπτει τα αληθινά με έγγραφη υπεύθυνη δήλωση
του άρθρου 8 παρ. 4 Ν. 1599/1986 τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Εάν ο υπαίτιος αυτών των πράξεων
σκόπευε να προσπορίσει στον εαυτόν του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον, τιμωρείται με κάθειρξη μέχρι 10 ετών.»

Περίληψη

Τα τελευταία χρόνια, μηχανισμοί εντοπισμού κακόβουλου λογισμικού αναπτύσσονται σε συστήματα φορητών έξυπνων συσκευών και συγκεντρώνονται από ερευνητές. Με τη γρήγορη επέκταση των κακόβουλων λογισμικών που βρίσκονται σε έξυπνες συσκευές, παραβιάζοντας το απόρρητο των χρηστών αυτών των συσκευών, είναι εξαιρετικά επιτακτικοί και απαραίτητοι οι μηχανισμοί αυτοί. Τα συστήματα ανίχνευσης είναι συσκευές προγραμματισμού που κατά συνέπεια συγκεντρώνουν πληροφορίες, τις τεμαχίζουν και αναγνωρίζουν τέτοια περιστατικά, σε μια προσπάθεια να περιοριστούν τα φαινόμενα του ηλεκτρονικού εγκλήματος.

Η ακρίβεια παίζει σημαντικό ρόλο στην εισβολή. Γι' αυτό είναι απαραίτητη η αναφορά στα συστήματα ανίχνευσης και η αποτελεσματικότητα των μεθόδων βάσει μιας μέτρησης αξιολόγησης. Σε αυτή την διπλωματική γίνεται λόγος για το ηλεκτρονικό έγκλημα και τα είδη κακόβουλου λογισμικού που μπορούν να προσβάλουν τις έξυπνες συσκευές. Επιπλέον δίνονται και σενάρια με τρόπους ανίχνευσης και αντιμετώπισης κακόβουλων λογισμικών. Ενώ, τέλος, γίνεται εκτενή αναφορά στο IoT, όπως επίσης στις περιπτώσεις των έξυπνων σπιτιών και πως αυτά μπορούν να επηρεαστούν από την ύπαρξη τέτοιων κακόβουλων λογισμικών.

(Λέξεις Κλειδιά)

Κακόβουλο λογισμικό, Αφαίρεση κακόβουλου λογισμικού, Ιός, Trojan, Συστήματα ανίχνευσης εισβολών, Έξυπνες Συσκευές, Επιθέσεις ασφαλείας, IoT.

Abstract

In recent years, malware detection mechanisms have been developed on mobile smart systems and assembled by researchers. With the rapid spread of malware on smart devices, violating the privacy of users of these devices, these mechanisms are extremely urgent and necessary. Detection systems are programming devices that collect information, segment it, and detect such incidents, in an effort to contain these acts of cyber crime.

Accuracy plays an important role in the invasion. That is why it is necessary to refer to the detection systems and the effectiveness of the methods based on an evaluation measurement. This dissertation discusses cybercrime and the types of malware that can infect smart devices. Moreover, some scenarios are given with ways to detect and deal with malware. And, finally, there is an extensive report about IoT and also the cases of smart homes and how they can be affected by the existence of such malware.

Keywords: Malicious Software, Malware Removal, Virus, Trojan, Intrusion Detection, Smart Devices, Security Attacks, IoT.

ΕΥΧΑΡΙΣΤΙΕΣ

Σε αυτό το σημείο θα ήθελα να ευχαριστήσω όλους όσους συνέβαλαν στην ολοκλήρωση αυτού του μεγάλου προσωπικού έργου.

Τον Δρ. Παναγιώτη Βαρζάκα ο οποίος με καθοδήγησε καθ'όλη τη διάρκεια εκπόνησης της παρούσας εργασίας, καθοδηγώντας με σε όλα τα αναγκαία στάδια υλοποίησης της, με τις εύστοχες παρατηρήσεις του και την εμπειρογνωμοσύνη του.

Τέλος, φυσικά θέλω να ευχαριστήσω από τα βάθη της καρδιάς μου τους γονείς μου για την συνεχή στήριξη και κατανόηση που έδειξαν σε όλη τη διάρκεια της φοίτησης μου, με την αμέριστη ψυχολογική και όχι μόνο υποστήριξη που πάντα μου παρείχαν.

Περιεχόμενα

Εισαγωγή

Στο κεφάλαιο αυτό γίνεται αναφορά στο πεδίο εφαρμογής της διπλωματικής εργασίας, καθώς επίσης στο αντικείμενο και στη διάρθρωσή της. Το πεδίο εφαρμογής της διπλωματικής εργασίας είναι οι έξυπνες συσκευές (Smart Devices) και ειδικότερα το ηλεκτρονικό έγκλημα και οι εφαρμογές κακόβουλου λογισμικού που στοχεύουν σε αυτές. Το αντικείμενο της διπλωματικής εργασίας είναι καταρχήν, η βιβλιογραφική καταγραφή των κυριότερων έως σήμερα, κατηγοριών κακόβουλου λογισμικού σε έξυπνες συσκευές, καθώς επίσης και η περιγραφή των μεθοδολογιών δράσης τέτοιου λογισμικού αλλά συγχρόνως και τρόποι ανίχνευσής του, με βάση το λειτουργικό τους σύστημα.

Οι έξυπνες συσκευές εμφανίζονται γρήγορα ως δημοφιλείς συσκευές με όλο και πιο ισχυρές δυνατότητες πληροφορικής, δικτύωσης και ανίχνευσης. Ίσως τα πιο επιτυχημένα παραδείγματα τέτοιων συσκευών μέχρι στιγμής είναι τα smartphones και τα tablets, τα οποία στην τρέχουσα γενιά τους είναι πολύ πιο ισχυρά από τους πρώτους προσωπικούς υπολογιστές. Η βασική διαφορά μεταξύ τέτοιων "έξυπνων" συσκευών και παραδοσιακών "μη έξυπνων" συσκευών είναι ότι προσφέρουν τη δυνατότητα εύκολης ενσωμάτωσης εφαρμογών τρίτων μέσω διαδικτυακών αγορών. Η δημοτικότητα των έξυπνων συσκευών, που σχετίζονται στενά με την άνοδο των προτύπων υπολογιστικού νέφους που παρέχουν συμπληρωματικές υπηρεσίες αποθήκευσης και πληροφορικής, υποστηρίζεται από πρόσφατες εμπορικές έρευνες, που δείχνουν ότι πολύ σύντομα θα ξεπουλήσουν τον αριθμό των υπολογιστών σε όλο τον κόσμο [1]. Για παράδειγμα, ο αριθμός των χρηστών smartphone έχει αυξηθεί ραγδαία τα τελευταία χρόνια. Το 2011, οι παγκόσμιες αποστολές κινητών συσκευών έφτασαν τα 1,6 δισεκατομμύρια σε μονάδες [2] και οι συνολικές πωλήσεις smartphone ανήλθαν σε 472 εκατομμύρια μονάδες (58% τοις εκατό όλων των πωλήσεων κινητών συσκευών σε σχέση με το 2010) [3].

Στην πραγματικότητα, ο αριθμός των χρηστών android και IOS μόνο αυξήθηκε από 38 σε 84 εκατομμύρια μεταξύ 2011 και 2012, σύμφωνα με μια έκθεση της Nielsen [4]. Η ίδια έκθεση αναφέρει επίσης ότι ο μέσος αριθμός εφαρμογών ανά συσκευή αυξήθηκε από 32 σε 41 και το ποσοστό του χρόνου που αφιερώνουν οι χρήστες σε εφαρμογές smartphone σχεδόν ισούται με το χρόνο που αφιερώνεται στο Διαδίκτυο (73% έναντι 81%). Επιπλέον, ο αριθμός των παγκόσμιων πωλήσεων smartphone σημείωσε ρεκόρ 207,7 εκατομμυρίων μονάδων κατά τη διάρκεια του 2012, σημειώνοντας αύξηση 38,3% σε σχέση με την ίδια περίοδο του προηγούμενου έτους [5]. Συγκεκριμένα, το μερίδιο αγοράς του παγκόσμιου λειτουργικού

συστήματος κινητής τηλεφωνίας (OS) δείχνει ότι το ANDROID OS έφτασε το 69,7% στις αρχές του 2013, σε σχέση με τα παλαιότερα SYMBIAN OS, BLACKBERRY OS και IOS . Νέες έξυπνες συσκευές εμφανίζονται με σταθερό ρυθμό, συμπεριλαμβανομένων των τηλεοράσεων, των ρολογιών, των γυαλιών , των ρούχων και των αυτοκινήτων [6]. Αυτό δεν διαδραματίζει μόνο βασικό ρόλο στην ανάδειξη πολυσυζητημένων προτύπων, όπως η wearable-computing ή το Internet of Things, αλλά και στην εύρεση καινοτόμων και πολύ ελκυστικών εφαρμογών σε κρίσιμους τομείς, όπως, για παράδειγμα, η παιδεία και η υγειονομική περίθαλψη. Επομένως, αποκτά ιδιαίτερη σημασία η έγκαιρη και αξιόπιστη αντιμετώπιση κακόβουλου λογισμικού με τρόπους που θα μπορούσαν να ολοκληρωθούν σε ένα ενιαίο πρότυπο, με σκοπό το πρότυπο αυτό να ενσωματωθεί σε όλες τις μελλοντικές, έξυπνες συσκευές.

Ίσως οι πιο επικίνδυνοι τύποι δημιουργών κακόβουλων προγραμμάτων είναι οι χάκερ και οι ομάδες χάκερ που δημιουργούν κακόβουλα προγράμματα λογισμικού σε μια προσπάθεια να επιτύχουν τους δικούς τους συγκεκριμένους εγκληματικούς στόχους. Αυτοί οι εγκληματίες στον κυβερνοχώρο δημιουργούν ιούς υπολογιστών και Trojan προγράμματα που μπορούν:

- Κλέψουν κωδικούς πρόσβασης σε τραπεζικούς λογαριασμούς
- Διαφημίσουν προϊόντα ή υπηρεσίες στον υπολογιστή του θύματος
- Χρησιμοποιήσουν παράνομα πόρους ενός μολυσμένου υπολογιστή - για να αναπτύξουν και να εκτελέσουν:
    - Καμπάνιες ανεπιθύμητων προϊόντων
    - Κατανεμημένες επιθέσεις δικτύου (DDoS)
    - Λειτουργίες εκβιασμού

Σκοπός αυτής της εργασίας είναι να δοθεί ώθηση προς τη βελτίωση της ανίχνευσης κακόβουλου λογισμικού για έξυπνες συσκευές και την αντιμετώπισή της. Επίσης, στόχος της παρούσας εργασίας είναι η μελέτη των προαναφερόμενων απειλών και του λογισμικού προστασίας από αυτές, τόσο με χρήση και αξιοποίηση του υπάρχοντος λογισμικού όσο και με τη δημιουργία προτάσεων για την αύξηση της ασφάλειας τόσο των δεδομένων που

ανταλλάσσονται μεταξύ χρηστών και εταιρειών όσο και αυτών που αποθηκεύονται. Υπάρχουν διαφορετικές τεχνικές που μπορούν ναι χρησιμοποιηθούν στην ανίχνευση εισβολών και μία από τις προτεραιότητες της συγκεκριμένης εργασίας είναι η μελέτη και ανάδειξη τους.

Τέλος για την επίτευξη των στόχων της συγκεκριμένης εργασίας χρησιμοποιήθηκε η ερευνητική μέθοδος της συστηματικής ανασκόπησης, της διεθνούς, ευρωπαϊκής και εγχώριας βιβλιογραφίας. Για την αναζήτηση των περισσότερων πληροφοριών έγινε η περιήγηση στα άρθρα του Scholar Google.

Βιβλιογραφικές Αναφορές – Παράρτημα εικόνων: Στις Βιβλιογραφικές αναφορές αναφέρονται δημοσιεύσεις (papers), βιβλία και πηγές του διαδικτύου και εικόνες που χρησιμοποιήθηκαν για την εκπόνηση της παρούσας διπλωματικής εργασίας, και μπορούν να χρησιμοποιηθούν για περαιτέρω μελέτη.

Κεφάλαιο 1

1.1 Περιεχόμενο και Διακρίσεις Ηλεκτρονικού Εγκλήματος

Στο κεφάλαιο αυτό θα γίνει προσπάθεια να προσδιοριστεί το ηλεκτρονικό έγκλημα ανάλογα με τη συχνότητα, την ιδιαιτερότητα και την πολυπλοκότητα του, καθώς αποτελεί την πιο σύγχρονη μορφή εγκληματικότητας στις εξορμήσεις στο διαδίκτυο. Στη συνέχεια θα γίνει προσπάθεια να παρουσιαστεί το περιεχόμενο του και οι κατηγορίες στις οποίες χωρίζεται με τα βασικά χαρακτηριστικά της κάθε μίας από αυτές, όπως έχουν διαμορφωθεί σύμφωνα με τον κανονιστικό πλαίσιο και τη σύγχρονη ηλεκτρονική πραγματικότητα.

Πριν ξεκινήσουμε την εν τω βάθει αποκωδικοποίηση του ηλεκτρονικού εγκλήματος, πριν αναλύσουμε τις μορφές εμφάνισής του αλλά και τα μέσα που είναι απαραίτητα για την διεξαγωγή ενός τέτοιου εγκλήματος, θα πρέπει να δώσουμε ένα βασικό ορισμό που θα περιγράφει την ουσία του όρου "ηλεκτρονικό έγκλημα". Ένας από τους πρώτους γενικούς ορισμούς δόθηκε από τους Forester και Morrison το 1994, με τον οποίο το ηλεκτρονικό έγκλημα προσδιοριζόταν ως «μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσής της», κυριότερο αλλά όχι απαραίτητα μοναδικό, ιδίως σκεπτόμενοι το πόσες άλλες έξυπνες συσκευές είναι ευάλωτες σε επιθέσεις.

Όπως αναφέραμε, βασικό στοιχείο για την διεξαγωγή του εν λόγω εγκλήματος έχει ο ηλεκτρονικός υπολογιστής ή κάποια άλλη έξυπνη συσκευή με παρόμοια χαρακτηριστικά και δυνατότητες. Υπάρχουν τρία σενάρια για τον ρόλο που μπορεί να διαδραματίσει ο ηλεκτρονικός υπολογιστής.

1)Να είναι ο βασικός στόχος κάποιας επίθεσης.

2)Να συμβάλει ως ένα βοηθητικό μέσο για τη διάπραξη του εγκλήματος, π.χ. να αποθηκεύονται σε αυτόν στοιχεία ή πληροφορίες που αφορούν άτομα τα οποία συμμετέχουν σε παράνομες δραστηριότητες ή σχετίζονται με αυτές με ποικίλους τρόπους.

3)Να αποτελεί το ίδιο το μέσο διάπραξης κάποιας επίθεσης, δηλαδή το όργανο με το οποίο ο παραβάτης διεξάγει την εγκληματική πράξη. (Shinder, 2002)

Το ηλεκτρονικό έγκλημα είναι ένα δευτερεύον προϊόν της ανάπτυξης του Διαδικτύου. Σε σύγκριση με το συμβατικό έγκλημα, το έγκλημα στον κυβερνοχώρο είναι νέο. Ωστόσο, η καταστροφή που έχει κοστίσει το έγκλημα στον κυβερνοχώρο δεν είναι μικρότερη από το συμβατικό έγκλημα. Ωστόσο, το πρώτο ηλεκτρονικό έγκλημα έχει τεκμηριωθεί στις αρχές του 1820. Μια ομάδα υπαλλήλων του Joseph-Marie Jacquard προσπάθησε να σαμποτάρει τον αργαλειό Jacquard που εφευρέθηκε, έχοντας το φόβο ότι θα χάσουν τη δουλειά τους από τη συσκευή. Ωστόσο, αυτό είναι ένα παράδειγμα που είναι αρκετά διαφορετικό από το έγκλημα στον κυβερνοχώρο που υπάρχει σήμερα. [7] Το έγκλημα στον κυβερνοχώρο που γνωρίζουμε συνήθως εξαρτάται από το δίκτυο και το σύγχρονο υπολογιστή, ενώ για πρώτη φορά βρέθηκε μετά την ανάπτυξη του σύγχρονου υπολογιστή και του Arpanet. Το πρώτο κακόβουλο πρόγραμμα ηλεκτρονικού εγκλήματος που εμφανίστηκε ονομάζεται Creeper το 1971 από τον Bob Thomas, ο οποίος δεν είχε καμία πρόθεση να διεξάγει οποιεσδήποτε εγκληματικές δραστηριότητες. [8] Από τότε, έχει δημιουργηθεί αμέτρητο κακόβουλο λογισμικό, το οποίο γίνεται όλο και πιο περίπλοκο και οι κύριες λειτουργίες και οι σκοποί του συνεχώς αλλάζουν. Καθώς μπήκαμε στην Εποχή της Πληροφορίας, η κοινωνία εξαρτάται όλο και περισσότερο από τον υπολογιστή και το Διαδίκτυο. Παρόλο που η ουσία του κακόβουλου λογισμικού δεν έχει αλλάξει πολύ, το πεδίο εξάσκησης έχει διευρυνθεί ευρέως.

Είναι η εξέλιξη της κοινωνίας μας που κάνει το έγκλημα στον κυβερνοχώρο να ευδοκιμεί. Εκτός από αυτό, το συμβατικό έγκλημα σύμφωνα με το ρεύμα της εποχής της πληροφορίας προσαρμόζεται στον κόσμο μας με την ψηφιοποίηση. Το εμπόριο παράνομων ουσιών, το παράνομο εμπόριο όπλων και άλλες συμβατικές εγκληματικές δραστηριότητες άρχισαν να προσφέρουν ηλεκτρονικές υπηρεσίες που μειώνουν την πιθανότητα σύλληψης. Η κοινή παρανόηση του εγκλήματος στον κυβερνοχώρο είναι ότι το έγκλημα στον κυβερνοχώρο πρέπει να περιλαμβάνει τον υπολογιστή ή το διαδίκτυο σε κάθε βήμα. Ωστόσο, δεν πραγματοποιούνται όλα τα βήματα σε ολόκληρο τον υπολογιστή ή το Internet. Μια άλλη κοινή παρεξήγηση είναι ότι ο υπολογιστής είναι πάντα αναγκαίος για τη διάπραξη ενός εγκλήματος..

Σε περίπτωση που παρατηρήσουμε μια δυσλειτουργία ή κάποια ανωμαλία στη στο σύστημα, ποιες είναι οι ακόλουθες ενέργειες μας; Αν ένας μηχανικός προσπαθήσει να αντιμετωπίσει μια δυσλειτουργία της συσκευής, πρώτα θα εντοπίσει το πρόβλημα και τότε θα προσπαθήσει να το λύσει. Αν αντιμετωπίσει πάρα πολλά εμπόδια, θα τα σπάσει σε

μικρότερα προβλήματα, και θα τα επιλύσει ένα προς ένα. Για τον έλεγχο ή την επίλυση ενός εγκλήματος στον κυβερνοχώρο, πρώτα πρέπει να καταλάβουμε τι χαρακτηριστικό έχει, τι κίνητρο έχει ένας εισβολέας, και τι δυσκολίες αντιμετωπίζουμε. Τα ηλεκτρονικά εγκλήματα, ως ένα νέο είδος εγκλήματος, έχουν πολλά χαρακτηριστικά που είναι πιο ισχυρά από τα συμβατικά εγκλήματα. Αυτά τα χαρακτηριστικά τα καθιστούν πιο περίπλοκα για την επιβολή του νόμου από τα συμβατικά εγκλήματα. Σε σύγκριση με τα συμβατικά εγκλήματα, το έγκλημα στον κυβερνοχώρο είναι πολύ ταχύτερο και πιο ισχυρό από το πρώτο. Για παράδειγμα, η διακίνηση παράνομων ουσιών μεταξύ χωρών θα πάρει ημέρες, και ο λαθρέμπορος θα είχε τεράστιο κίνδυνο να πιαστεί κατά τη διάρκεια της μεταφοράς. Αντίθετα, ένας χάκερ θα μπορούσε να χακάρει τον τραπεζικό λογαριασμό κάποιου, η χώρα του οποίου μπορεί να βρίσκεται στην άλλη πλευρά της γης σε λίγα λεπτά, και ο κίνδυνος να πιαστεί σε δράση είναι σχεδόν μηδενικός. Εξάλλου, χωρίς το κατάλληλο διεθνές δίκαιο, οι χάκερ θα μπορούσαν να φύγουν ελεύθεροι μετά τη διεξαγωγή εγκλήματος. Σε ορισμένες περιπτώσεις, ένας χάκερ με κάποια γνώση του διεθνούς περιβάλλοντος θα μπορούσε να χρησιμοποιήσει τη σχέση μεταξύ των χωρών ως ασπίδα. [8]

Για αυτό το λόγο προέκυψε η ανάγκη μιας κοινής νομοθεσίας μεταξύ των χωρών για την παγκόσμια κάλυψη νομοθεσίας για ηλεκτρονικά εγκλήματα που ίσως εξελίχθηκαν σε παραπάνω από μια χώρες ή οι παραβάτες έχουν διαφορετικοί εθνικότητα από την χώρα στην οποία διέπραξαν κάποιο έγκλημα. Σε μια προσπάθεια να δημιουργηθούν οι απαραίτητες νομοθεσίες και μηχανισμοί κατανόησης και κατηγοριοποίησης των διαφορετικών ειδών εγκλήματος και παραβάσεων έγινε το πρώτο Συνέδριο για το Ηλεκτρονικό Έγκλημα στη Βουδαπέστη το 2001 (Budapest Convention on Cybercrime). Οι μεγάλες ανάγκες που κλήθηκε να καλύψει το Συνέδριο ήταν το γεγονός πως πολλές χώρες δεν είχαν κάποιο επιβεβλημένο νομοθετικό σύστημα για την καταπολέμηση του ηλεκτρονικού εγκλήματος καθώς και οι χώρες που είχαν κάποια μορφή νομοθεσίας βρισκόταν σε πολύ πρώιμο στάδιο και δεν κάλυπτε όλες τις πτυχές και κατηγορίες του. Επιπλέον ένα μεγάλο εμπόδιο στο Συνέδριο ήταν η από κοινού διακρατική συμφωνία για ένα θέμα το οποίο ήταν πρωτοεμφανιζόμενο και δεν υπήρχε κοινή βάση και πορεία πλεύσης. Ακόμα, πολύ σημαντική παράμετρος που ακολουθήθηκε στο Συνέδριο ήταν η δημιουργία μιας συλλογικής αντί εγκληματικής πολιτικής που θα δημιουργούσε μια σφαίρα προστασίας και νομοθεσιών με κύριο παράγοντα την διασφάλιση και τον σεβασμό των θεμελιωδών ανθρώπινων δικαιωμάτων. Δικαιώματα όπως η ελευθερία του λόγου, το δικαίωμα σεβασμού απορρήτου, ελευθερία έκφρασης και αναζήτησης-διανομής πληροφοριών μεταξύ πολλών άλλων είχαν

σημαντικό ρόλο στην οριοθέτηση μεταξύ ελευθερίας άσκησης βασικών ανθρώπινων δικαιωμάτων και εγκληματικής ενέργειας. Βασικά συμπεράσματα που προέκυψαν κατά την συνέλευση του Συνεδρίου ήταν η ανάγκη για την από κοινού διεθνή συνεργασία μεταξύ των εθνών για την καταπολέμηση του ηλεκτρονικού εγκλήματος καθώς και την απαραίτητη συνεργασία μεταξύ ιδιωτικού και δημοσίου τομέα σε εθνικό επίπεδο προκείμενου να διασφαλιστούν οι κατάλληλες επιθυμητές ισορροπίες. Στις 23/11/2001, 26 υπουργοί ευρωπαϊκών κρατών, περιλαμβανομένης και της Ελλάδας, υπέγραψαν από κοινού συμφωνία με σκοπό την αντιμετώπιση του ηλεκτρονικού εγκλήματος.[9][10]

Επιστρέφοντας στην ουσία του ηλεκτρονικού εγκλήματος στον κυβερνοχώρο, είναι απαραίτητο να τονίσουμε πως χρειάζεται ορισμένες δεξιότητες όπως κάθε άλλο έγκλημα. Ωστόσο, σε αντίθεση με ορισμένα εγκλήματα, μέρος του εγκλήματος στον κυβερνοχώρο απαιτεί εκτεταμένη γνώση της επιστήμης των υπολογιστών. Εκτός από αυτό, ορισμένοι εγκληματίες πρέπει να είναι σε θέση να αναγνωρίσουν το αδύναμο σημείο σε ένα μεγάλο ποσοστό των κωδικών. Πρέπει να καλύψουν το ψηφιακό τους αποτύπωμα σχολαστικά, ώστε να μην αφήσουν τα ίχνη τους. Πρέπει να κάνουν σχέδια για τις επιθέσεις τους. Όλα αυτά τα χαρακτηριστικά καθιστούν ακόμα πιο δύσκολο να συλληφθούν από την επιβολή του νόμου σε όλο τον κόσμο. Επιπροσθέτως, οι ταυτότητες των χρηστών του διαδικτύου δεν είναι παρά μια σειρά αριθμών και γραμμάτων. Αυτές οι ταυτότητες μπορούν εύκολα να συγκαλυφθούν και να τροποποιηθούν. Αυτό το χαρακτηριστικό δίνει στους ανθρώπους το θάρρος να κάνουν ό, τι φοβούνται να κάνουν στην πραγματική ζωή. Εκείνοι που εκφοβίζονται στην πραγματική ζωή είναι πιο πιθανό να διεξάγουν διαφορετική συμπεριφορά στον κυβερνοχώρο. Οι ταυτότητες δίνουν στους ανθρώπους μια ευθύνη για τη συμπεριφορά τους. [11] Εντούτοις, μόλις κρυφτεί η ταυτότητα, η αίσθηση της ευθύνης πέφτει, και οι άνθρωποι είναι σε θέση να ασκήσουν τη συμπεριφορά που τους κρατά υπεύθυνους στην πραγματική ζωή. Το χαρακτηριστικό παράδειγμα είναι ο διαδικτυακός ρατσισμός. Μπορούμε να βρούμε πολλά σχόλια των ρατσιστών σε απευθείας σύνδεση στα μέσα ενημέρωσης, αλλά σπάνια στην πραγματική ζωή. Επειδή οι άνθρωποι φοβούνται να χάσουν τη φήμη και την ευημερία τους στην πραγματική ζωή. Το όνομά μας είναι συνυφασμένο με τη φήμη μας. Κάποια συμπεριφορά όπως ο ρατσισμός θα το βλάψει αυτό. Ωστόσο, από τη στιγμή που η συμπεριφορά μας δεν συνδέεται πλέον με την ταυτότητά μας ή με το ποιοι είμαστε, γινόμαστε πολύ πιο τολμηροί.

Ιδιαίτερη οργάνωση με την ανάπτυξη της ασφάλειας των δικτύων πραγματοποιείται με στόχο να δυσκολεύεται η διεξαγωγή του εγκλήματος στον κυβερνοχώρο. Έτσι, αντί να εργάζονται μόνοι και να λαμβάνουν όλο το φόρτο εργασίας, οι εγκληματίες του κυβερνοχώρου αποφασίζουν να συνεργαστούν και να διαιρέσουν την εργασία. Ο καταμερισμός της εργασίας καθιστά το έγκλημα στον κυβερνοχώρο πιο αποτελεσματικό και κερδοφόρο. Γενικά, αυτές οι ομάδες συναντώνται σε απευθείας σύνδεση φόρουμ. Επικοινωνούν μέσω των κοινωνικών μέσων μαζικής ενημέρωσης ή τα dark-net-chatroom. Δεν γνωρίζουν φυσικά τις πραγματικές ταυτότητες των άλλων. Αυτή η δομή του εγκλήματος κάνει για τις αρχές, ακόμα πιο δύσκολο να συλλάβουν ολόκληρη την οργάνωση. Ταυτόχρονα έχει διαπιστωθεί ότι τα υψηλά κέρδη του εγκλήματος στον κυβερνοχώρο είναι προσοδοφόρα. Οι άνθρωποι μπορούν να φανταστούν τους εγκληματίες του κυβερνοχώρου ως επιστήμονες των υπολογιστών, γνώστες και προγραμματιστές. Αντιθέτως, οι περισσότεροι από τους εγκληματίες του κυβερνοχώρου δεν είναι. Χρησιμοποιούν απλώς το λογισμικό που αποκτούν, ως μέσο το οποίο θα τους αποφέρει κάποιο οικονομικό κέρδος. [12]

Σε άλλες χώρες, το κόστος για τη διεξαγωγή του εγκλήματος στον κυβερνοχώρο είναι διαφορετικό, αλλά το κέρδος είναι παρόμοιο ή και ακόμη μεγαλύτερο [13]. Κάτω από το ζοφερό οικονομικό περιβάλλον σε όλο τον κόσμο, αυτή η βιομηχανία υψηλού κέρδους και αμελητέου κινδύνου προσελκύει εκατοντάδες και χιλιάδες ανθρώπους. Αυτό πιστεύεται ότι είναι ο λόγος της αύξησης του εγκλήματος στον κυβερνοχώρο σε όλο τον κόσμο. Εκτός από αυτό, πολλές ομάδες από εγκληματίες του κυβερνοχώρου χρηματοδοτούνται καλά. Προσλαμβάνονται για να επιτεθούν στους αντιπάλους του εργοδότη τους, να αποσπάσουν πολύτιμες πληροφορίες και να διεξάγουν άλλες παράνομες συμπεριφορές. Αν και μια ακριβής τιμή δεν μπορούσε να βρεθεί για τη διαφορετική υπηρεσία, οι ακριβείς υπηρεσίες βρέθηκαν κατά τη διάρκεια της έρευνας. Ορισμένοι χάκερ για ενοικίαση προσφέρουν μόνο νομική υπηρεσία που σημαίνει ότι διεξάγουν μόνο ηθικά hacking για τα άτομα ή τις εταιρείες για να εντοπίσουν την πιθανή παραβίαση της ασφάλειας τους ή να βρουν τον χαμένο κωδικό πρόσβασής τους. Ωστόσο, υπάρχουν επίσης πολλοί χάκερ που προσφέρουν παράνομες υπηρεσίες.

Όπως αναφέρθηκε πριν, οι ομάδες κυβερνο-εγκληματιών χρηματοδοτούνται καλά. Σε ορισμένες περιπτώσεις, οι χρηματοδότες είναι κυβερνήσεις. Καθώς η τεχνολογία μας φέρνει ένα βολικό και αποτελεσματικό τρόπο ζωής, μας φέρνει επίσης πιθανές απειλές. Κυβερνήσεις σε όλο τον κόσμο, εκσυγχρονίζουν το σύστημά τους με την τεχνολογία.

Ωστόσο, αυτό καθιστά το κυβερνητικό σύστημα πιο ευάλωτο από πριν. Αμέτρητες ευαίσθητες κυβερνητικές πληροφορίες ψηφιοποιούνται και γίνονται στόχος για χάκερ που εργάζονται για άλλες κυβερνήσεις. Το πιο διαβόητο περιστατικό είναι γνωστό ως έργο PRISM. Η αμερικανική κυβερνητική υπηρεσία NSA (National Security Agency) διεξήγαγε (μπορεί ακόμα να διεξάγει) παράνομη επιτήρηση σε παγκόσμια κλίμακα στο όνομα της αντιτρομοκρατίας. Σύμφωνα με τους ισχυρισμούς, πολλές αμερικανικές επιχειρήσεις εμπλέκονται σε αυτό το έργο που εργάζονται με την NSA. Αν και αρνήθηκαν τη συμμετοχή αυτού του προγράμματος PRISM, ο πρώην ανάδοχος της NSA Edward Snowden παρουσίασε μάλλον πειστικά αποδεικτικά στοιχεία. Η κυβέρνηση των ΗΠΑ συλλέγει ένα μεγάλο όγκο προσωπικών δεδομένων ανθρώπων ανά τον κόσμο συμπεριλαμβανομένων υψηλόβαθμους κυβερνητικούς αξιωματούχους σε όλο τον κόσμο. Οι ΗΠΑ έχουν ήδη χτίσει το δικό τους στρατό για τον πόλεμο στον κυβερνοχώρο που ονομάζεται Cyber Command. [14] Εντούτοις, το ερώτημα είναι «εάν αυτό το είδος στρατιωτικών δραστηριοτήτων ανιχνεύθηκε σε άλλες χώρες, πρέπει να θεωρηθεί ως πράξη πολέμου;» [15], δεδομένου ότι ο παραδοσιακός πόλεμος πρέπει να ακολουθήσει το αυστηρό διεθνές δίκαιο και τη συνθήκη. Αυτό το είδος της συμπεριφοράς επίσης πρέπει να υπακούσει στο νόμο και τη συνθήκη; Θα υπάρχουν στόχοι που προστατεύονται από το νόμο και τη συνθήκη;

Σε ορισμένες περιπτώσεις, οι κυβερνήσεις απευθύνονται σε κυβερνο-εγκληματίες, ακόμη και "τρομοκράτες" στον κυβερνοχώρο. Προσφέρουν πολιτικό άσυλο για τέτοιου είδους οργανώσεις. Με αυτόν τον τρόπο, θα μπορούσαν να επιτύχουν πολιτικό όφελος μέσω αυτών. Επίσης, υπάρχουν πολλές χώρες που εργάζονται για τη δημιουργία "όπλων" στον κυβερνοχώρο. Σύμφωνα με τους ισχυρισμούς, το πρόσφατο ξέσπασμα κακόβουλου λογισμικού - ransomware είναι ένα από αυτά τα μέσα - όπλο στον κυβερνοχώρο από την NSA ή τη Βόρεια Κορέα. Αν και διαφορετικές ειδήσεις αναφέρονται από διαφορετικό πρακτορείο ειδήσεων, η ίδια θεωρία είναι ότι είναι ένα όπλο στον κυβερνοχώρο που αναπτύχθηκε από την κυβέρνηση. Ένα άλλο πρόσφατο περιστατικό είναι οι φήμες για τη ρωσική συμμετοχή στην προεκλογική εκστρατεία του Προέδρου των ΗΠΑ. Η κατηγορία είναι ότι οι Ρώσοι χάκερ παραποίησαν τα εκλογικά δεδομένα για να διασφαλίσουν ότι ο Ντόναλντ Τράμπ θα κερδίσει τις εκλογές. Χωρίς αδιάσειστα στοιχεία, αυτή η κατηγορία δεν μπορεί να σταθεί. Ωστόσο, μόνο η ύπαρξη αυτής της φήμης εφιστά την προσοχή στην ασφάλεια στον κυβερνοχώρο και σκιαγραφεί τα υψηλά επίπεδα επιρροής που μπορεί να έχει το ηλεκτρονικό έγκλημα, δεδομένου ότι τα ψηφιακά δεδομένα είναι ευάλωτα και αναλώσιμα. [16]

1.2 Κατηγορίες Ηλεκτρονικού Εγκλήματος

Ακολουθούν δώδεκα τρόποι με τους οποίους ένα έγκλημα στον κυβερνοχώρο μπορεί να πραγματοποιηθεί, και θα πρέπει να γίνουν γνωστοί. Για να προστατευθεί κάποιος πρέπει να γνωρίζει τους διαφορετικούς τρόπους με τους οποίους ο υπολογιστής, ένα δίκτυο και τοίχοι ασφαλείας μπορούν να παραβιαστούν. Σε αυτή την ενότητα, αναφέρονται μερικά κοινά εργαλεία και τεχνικές που χρησιμοποιούνται από τους εγκληματίες του κυβερνοχώρου. Αυτό δεν είναι ένας εξαντλητικός κατάλογος με οποιοδήποτε μέσο, αλλά θα δώσει μια περιεκτική ιδέα των κενών ασφαλείας που υπάρχουν στα δίκτυα και τα συστήματα ασφαλείας, τα οποία μπορούν να αξιοποιηθούν από τους επιτιθέμενους, καθώς και τα πιθανά κίνητρά τους για να το πράξουν.

1.2.1 Hacking

Με απλά λόγια, hacking είναι μια πράξη που διαπράχθηκε από έναν εισβολέα με την πρόσβαση στο σύστημα του υπολογιστή χωρίς την άδειά του ιδιοκτήτη. Hackers (οι άνθρωποι που εμπλέκονται στη διαδικασία του «hacking») είναι κατά κύριο λόγο προγραμματιστές υπολογιστών, οι οποίοι έχουν μια προηγμένη κατανόηση των υπολογιστών και συνήθως καταχρώνται αυτή τη γνώση για δόλιους σκοπούς. Είναι συνήθως λάτρεις της τεχνολογίας, που έχουν δεξιότητες σε επίπεδο εμπειρογνωμόνων σε ένα συγκεκριμένο πρόγραμμα λογισμικού ή γλώσσα. Όσο για τα κίνητρα, θα μπορούσαν να υπάρχουν αρκετά, αλλά το πιο κοινό είναι αρκετά απλό και μπορεί να εξηγηθεί από μια ανθρώπινη τάση, όπως η απληστία, η φήμη, η δύναμη, κλπ. Μερικοί άνθρωποι το κάνουν καθαρά για να αναδείξουν την εμπειρία τους - που κυμαίνεται από σχετικά αβλαβείς δραστηριότητες, όπως η τροποποίηση του λογισμικού (και ακόμη και του υλικού) για την εκτέλεση εργασιών που είναι εκτός της πρόθεσης του δημιουργού, άλλοι απλά θέλουν να προκαλέσουν καταστροφή.[16]

Η ταυτότητα ενός χάκερ

Πολλοί μπορεί να είναι οι λόγοι που θα προκαλέσουν έναν χάκερ να σπάσει τις ασφάλειες των συστημάτων για να κλέψει προσωπικές τραπεζικές πληροφορίες, τα οικονομικά στοιχεία μιας εταιρείας, κλπ. Προσπαθούν επίσης και να τροποποιήσουν τα συστήματα, ώστε να μπορούν να εκτελέσουν εργασίες ανάλογα με τις ιδιοτροπίες τους. Η λέξη χάκερ (hacker) αρχικά είχε χρήση για να υποδηλώσει την μεγάλη και εκτενή γνώση

κάποιου στον χειρισμό των λειτουργιών ενός ηλεκτρονικού υπολογιστή, τις ικανότητες του στον προγραμματισμό και σε ένα γενικό πλαίσιο την άριστη ικανότητα διαχείρισης όλων των πτυχών ενός δικτύου. Παρεμφερή ονομασία ενός χάκερ είναι και κράκερ (cracker) που προέρχεται από την αγγλική λέξη crack που σημαίνει 'σπάω' υπονοώντας την ικανότητα του συγκεκριμένου προσώπου να σπάσει και να παραβιάσει δικλείδες ασφαλείας κερδίζοντας έτσι πρόσβαση πέρα από την δικαιοδοσία του. Η φύση ενός χάκερ είναι τέτοια ώστε να θεωρεί κάθε ευκαιρία να αποδείξει τις δυνατότητες του ως προσωπική δοκιμασία με πολύ σοβαρό ύφος. Ένας σημερινός επιδέξιος χάκερ εκτός από βαθιές γνώσεις υπολογιστών και δικτύων πρέπει να διαθέτει και κατάλληλο εξοπλισμό ο οποίος βέβαια προκύπτει από το πόσο μεγάλο θα είναι το χακάρισμα το οποίο θα επιχειρήσει. Πολλοί σημερινοί χάκερ είναι λογικό να έχουν πρόσβαση σε υπολογιστές με μεγάλη επεξεργαστική ισχύ, ασφαλή προσωπικά δίκτυα - VPN - συνδρομή σε πάροχο πρόσβασης. Κατά κύριο λόγο υπάρχουν δύο πτυχές ενός χάκερ. Σαν βασική αρχή ένας χάκερ προσπαθεί να εκμεταλλευτεί και να βρεί ρωγμές στην ασφάλεια των συστημάτων που επιχειρεί να διεισδύσει, να βρεί ελαττώματα στις δομές του λογισμικού και γενικά την πιο μικρή πτυχή η οποία θα τον βοηθήσει στο έργο του. Όμως ποιος είναι ο σκοπός του χάκερ εκτός από την προσωπική ικανοποίηση και επιβεβαίωση των ικανοτήτων του; Από την μια πλευρά υπάρχουν χάκερ οι οποίοι έχουν ως σκοπό το προσωπικό οικονομικό όφελος και εξαπολύουν επιθέσεις με κύριο στόχο μικρές επιχειρήσεις, ή προσωπικά τραπεζικά στοιχεία ανυποψίαστων χρηστών. Σε άλλη περίπτωση κακόβουλου χακαρίσματος περιλαμβάνεται και κάποια επίθεση η οποία γίνεται με μοναδικό σκοπό την αποδιοργάνωση ενός δικτύου και τη υποκλοπή πληροφοριών προκείμενου να ικανοποιηθούν οι προσωπικές επιδιώξεις του εκάστοτε χάκερ. Στον αντίποδα υπάρχει και το activism hacking το οποίο ουσιαστικά περιγράφει ένα είδος επίθεσης που γίνεται με καλή πρόθεση και για σημαντικό σκοπό. Τέτοια παραδείγματα είναι ή προσπάθεια προσπέλασης ενός συστήματος ασφαλείας, προκειμένου να βρεθούν αδύναμα σημεία και ελλείψεις στην δομή που υπάρχει, έτσι ώστε με την κατάλληλη ανατροφοδότηση από τον χάκερ, οι υπεύθυνοι του συστήματος να επιδιορθώσουν και ενισχύσουν τα αδύναμα σημεία. Είναι σύνηθες φαινόμενο καινούργιες εταιρίες να διεξάγουν ένα είδος διαγωνισμού όπου ζητάνε από επίδοξους χάκερ να προσπαθήσουν να βρουν κενά ασφαλείας και να τα αναφέρουν πίσω στην εταιρεία προκειμένου αυτή να αξιοποιήσει αυτή την ανατροφοδότηση πληροφορίας και να ενισχύσει το σύστημα της. Πολλές φορές οι εταιρείες αυτές πληρώνουν αδρά για τέτοιου είδους υπηρεσίες που μελλοντικά μπορεί να τους κοστίσουν όχι μόνο σε χρήματα αλλά και σε αξιοπιστία στο τομέα της αγοράς. Μέσω μιας πληθώρας από penetration testing ένας

χάκερ μπορεί να εντοπίσει όλες τις αδυναμίες που μπορεί να παρουσιάσει ένα σύστημα ασφαλείας. Με πιο απλά λόγια θα μπορούσαμε να πούμε ότι οι «ευγενικοί» χάκερς προσπαθούν να προστατέψουν σημαντικά συστήματα από κακόβουλους χάκερς, ψάχνοντας να βρούνε bugs και αδυναμίες πριν προλάβει κάποιος να τις εκμεταλλευτεί. Επιπλέον μορφές ακτιβιστικού χάκινγκ είναι προσπάθειες από χάκερς να ρίξουν – τερματίσουν την λειτουργία ιστοσελίδων που προάγουν ιδέες οι οποίες αποκλίνουν από τα προσωπικά πιστεύω των ιδίων. Σελίδες που μπορεί να προάγουν βία, ρατσισμό κοκ. Χάκερ οι οποίοι έχουν ως σκοπό την ενίσχυση και ενδυνάμωση των συστημάτων ασφαλείας και προάγουν την θετική χρήση των δυνατοτήτων τους χαρακτηρίζονται ως χάκερ με «λευκό καπέλο» και είναι ένας από τους πιο διαδεδομένους όρους και πιθανούς χαρακτηρισμούς που καθορίζει άμεσα την φύση ενός χάκερ. Φυσικά στον αντίποδα όσοι χαρακτηρίζονται με «μαύρο καπέλο» είναι αυτοί που έχουν δόλιες βλέψεις, ενώ υπάρχει και ένας τρίτος χαρακτηρισμός για όσους χάκερ οι οποίοι αυτόβουλα χωρίς κάποια έγκριση χακάρουν σε συστήματα και βάσεις δεδομένων έχοντας όμως καλό σκοπό, σε αυτούς απονέμεται ο χαρακτηρισμός του «γκρι καπέλου». [17]

Εικόνα 1: Ηλεκτρονικό Έγκλημα στον κυβερνοχώρο

Μερικές από τις πιο διάσημες ιδιοφυίες υπολογιστών ήταν κάποτε χάκερ που θέλησαν να χρησιμοποιήσουν τις ικανότητές τους για την εποικοδομητική τεχνολογική ανάπτυξη. Ο Dennis Ritchie και ο Ken Thompson, οι δημιουργοί του λειτουργικού συστήματος UNIX (προκάτοχος του Linux), ήταν δύο από αυτούς. Ο Shawn Fanning, ο κύριος του έργου του

Napster, ο MarkZuckerberg του Facebook, αποτελούν κάποια από τα πιθανά παραδείγματα. Το πρώτο βήμα προς την πρόληψη απόκτησης πρόσβασης από ένα χάκερ στο σύστημα μας, είναι να γίνει αποδεκτή η ύπαρξη του hacking. Φυσικά είναι πέρα από το πεδίο εφαρμογής αυτής τη έρευνας, αλλά θα καλύψει τις διάφορες τεχνικές που χρησιμοποιούνται από τους χάκερ για να φτάσουν στους ιδιοκτήτες μέσω του διαδικτύου.[18]

Διαδεδομένες πρακτικές hacking μεταξύ άλλων περιλαμβάνουν:

α. SQL Ενέσεις: Μια ένεση SQL είναι μια τεχνική που επιτρέπει στους χάκερ να παίξουν με τα τρωτά σημεία ασφαλείας του λογισμικού που χρησιμοποιεί μια ιστοσελίδα. Μπορεί να χρησιμοποιηθεί για να επιτεθεί σε οποιονδήποτε τύπο μη προστατευμένης ή εσφαλμένα προστατευμένης βάσης δεδομένων SQL. Αυτή η διαδικασία περιλαμβάνει την εισαγωγή τμημάτων κώδικα SQL σε ένα πεδίο καταχώρησης φόρμας web (πιο συχνά ονόματα χρήστη και κωδικούς πρόσβασης) για να δώσει στον χάκερ περαιτέρω πρόσβαση στο back-end-site, ή σε ένα συγκεκριμένο λογαριασμό του χρήστη. Όταν εισάγετε πληροφορίες σύνδεσης σε πεδία εισόδου, αυτές οι πληροφορίες συνήθως μετατρέπονται σε εντολή SQL. Αυτή η εντολή ελέγχει τα δεδομένα που εισάγει ο χρήστης στην προσπάθεια του να συνδεθεί, σε σχέση με τον σχετικό πίνακα στη βάση δεδομένων.

Εάν τα δεδομένα εισόδου ταιριάζουν με τα δεδομένα στον πίνακα, έχει εκχωρηθεί πρόσβαση, αν όχι, ο χρήστης λαμβάνει το είδος του σφάλματος που θα είχε όπως όταν θα τοποθετούσε λάθος κωδικό πρόσβασης. Μια ένεση SQL είναι συνήθως μια πρόσθετη εντολή που όταν εισάγεται στη φόρμα web, προσπαθεί να αλλάξει το περιεχόμενο της βάσης δεδομένων για να αντικατοπτρίζει μια επιτυχημένη σύνδεση. Μπορεί επίσης να χρησιμοποιηθεί για την ανάκτηση πληροφοριών, όπως αριθμούς πιστωτικών καρτών ή κωδικούς πρόσβασης από μη προστατευμένους ιστότοπους.[19][21]

β. Κλοπή κωδικών πρόσβασης FTP (File Transfer Protocol): Αυτός είναι ένας άλλος πολύ κοινός τρόπος για να παραποιηθούν οι ιστοσελίδες με κωδικό πρόσβασης. Αυτή εκμεταλλεύεται το γεγονός ότι πολλοί διαχειριστές ιστοσελίδων (webmasters) αποθηκεύουν στην ιστοσελίδα τους πληροφορίες σύνδεσης σε υπολογιστές με χαμηλά επίπεδα προστασίας και ασφάλειας. Ο υποψήφιος χάκερ ψάχνει το σύστημα του θύματος για FTP στοιχεία σύνδεσης, και στη συνέχεια τα αναμεταδίδει στο δικό του απομακρυσμένο υπολογιστή. Στη συνέχεια συνδέεται στην ιστοσελίδα μέσω του απομακρυσμένου υπολογιστή και με την

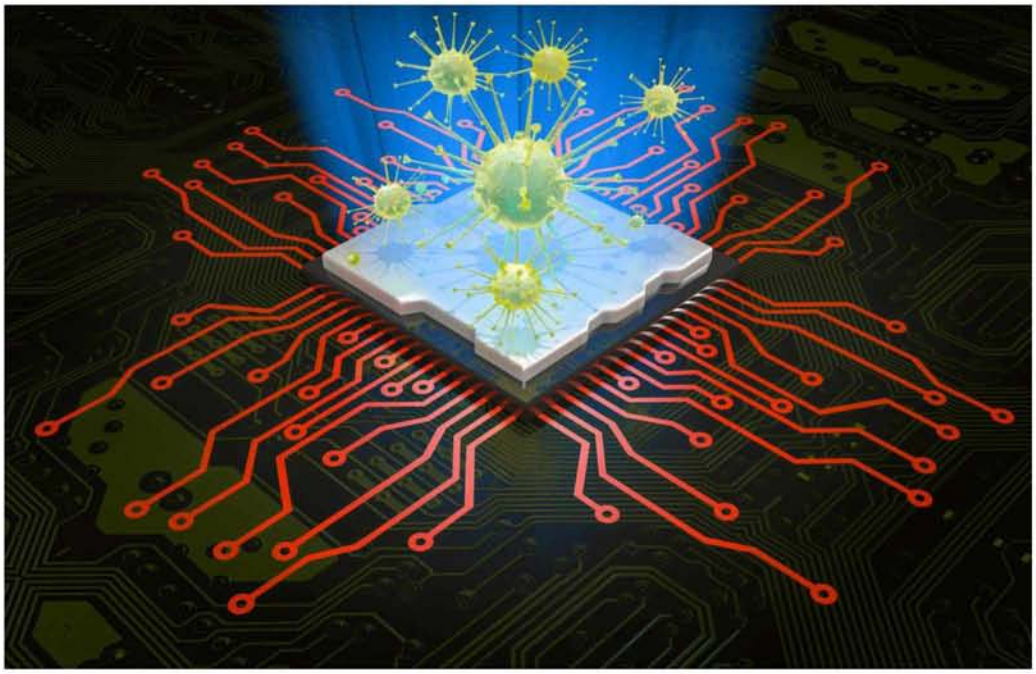
πρόσβαση στους κωδικούς που απέκτησε μπορεί να προχωρήσει στην τροποποίηση των ιστοσελίδων κατά τη θέληση του.

γ. Δέσμες ενεργειών μεταξύ τοποθεσιών: Επίσης γνωστό ως XSS (πρώην CSS - Cross-Site Scripting, αλλά μετονομάστηκε λόγω σύγχυσης με επικαλυπτόμενα φύλλα στυλ), είναι ένας πολύ εύκολος τρόπος για την παράκαμψη ενός συστήματος ασφαλείας. Σε μια τυπική επίθεση XSS, ο χάκερ μολύνει μια ιστοσελίδα με ένα κακόβουλο πρόγραμμα από την πλευρά του πελάτη. Όταν επισκέπτεται αυτήν την ιστοσελίδα, η δέσμη ενεργειών λαμβάνεται αυτόματα στο πρόγραμμα περιήγησης και εκτελείται. Συνήθως, οι εισβολείς εισάγουν HTML, JavaScript, VBScript, ActiveX ή Flash σε μια ευάλωτη εφαρμογή για να εξαπατήσουν και να συλλέξουν εμπιστευτικές πληροφορίες. Το βασικό και πιο απλό μέτρο προστασίας του υπολογιστή από κακόβουλους χάκερ, είναι η επένδυση σε ένα καλό τείχος προστασίας που θα παρέχει την απαραίτητη ασφάλεια κατά την διάρκεια και όχι μόνο, σύνδεσης του υπολογιστή στο διαδίκτυο. Το Hacking γίνεται μέσω ενός δικτύου, γι 'αυτό είναι πολύ σημαντικό να παραμένει κάποιος ασφαλείς, ενώ το χρησιμοποιεί. [20] [22]

Η κύρια διαφορά μεταξύ μιας επίθεσης έγχυσης SQL και XSS είναι ότι οι επιθέσεις SQL χρησιμοποιούνται για την κλοπή πληροφοριών από βάσεις δεδομένων, ενώ οι επιθέσεις XSS χρησιμοποιούνται για την ανακατεύθυνση χρηστών σε ιστότοπους όπου οι εισβολείς μπορούν να κλέψουν δεδομένα από αυτούς. Το SQL injection επικεντρώνεται στη βάση δεδομένων, ενώ το XSS προσανατολίζεται επιθετικά στους τελικούς χρήστες.

1.2.2 Διάδοση Ιού

Οι ιοί είναι προγράμματα υπολογιστών που συνδέονται ή μολύνουν ένα σύστημα ή αρχεία και έχουν την ικανότητα να μεταδίδονται σε άλλους υπολογιστές σε ένα δίκτυο. Διαταράσσουν τη λειτουργία του υπολογιστή και επηρεάζουν τα δεδομένα που αποθηκεύονται - είτε τροποποιώντας τα είτε διαγράφοντας τα εντελώς. [23] Τα "Worms" σε αντίθεση με τους ιούς δεν χρειάζονται έναν οικοδεσπότη για να προσκολλώνται. Αναπαράγονται μόνο μέχρι να επεκταθούν και αχρηστεύσουν όλη τη διαθέσιμη μνήμη στο σύστημα. Ο όρος "σκουλήκι" χρησιμοποιείται μερικές φορές για να σημάνει την αυτόνομη παραγωγή του "κακόβουλο λογισμικό" (MALicioussoftWARE). Οι όροι αυτοί χρησιμοποιούνται συχνά εναλλακτικά στο πλαίσιο των υβριδικών ιών / worms που κυριαρχούν.[24]

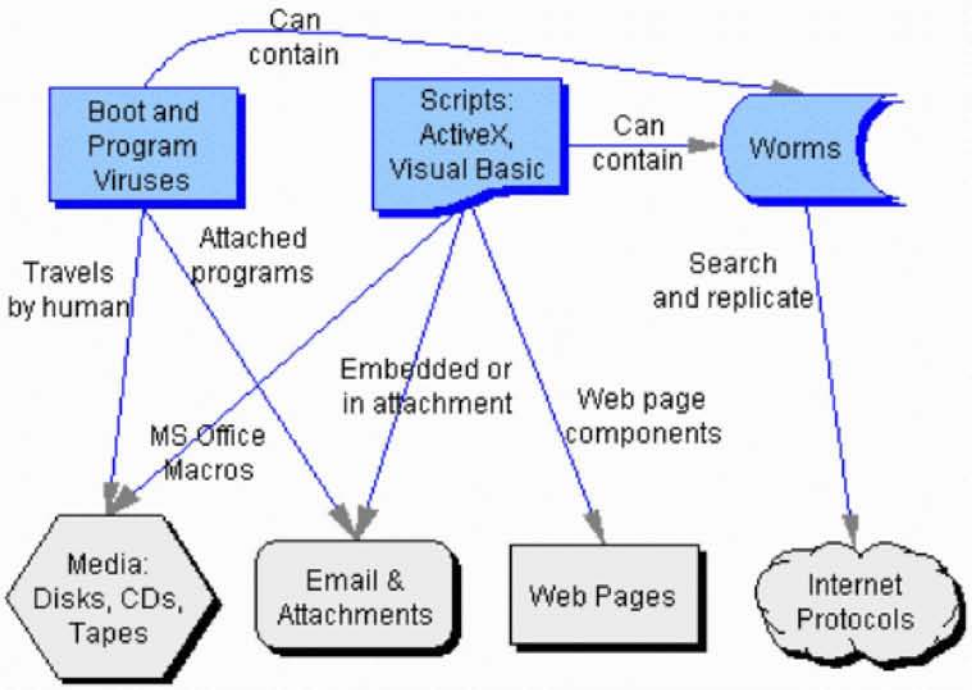


Εικόνα 2: Μετάδοση ιού σε ένα σύστημα

Μπορεί να αποτελεί την καλύτερη εφεύρεση της ανθρωπότητας, αλλά το διαδίκτυο εξακολουθεί να είναι ένα ναρκοπέδιο απειλών, επιπλέον από τα προ αναφερθέντα υπάρχει και η απειλή του Δούρειου ίππου – Trojan. Οι "Δούρειοι ίπποι" είναι διαφορετικοί από τους ιούς στον τρόπο διάδοσης τους. Μεταμφιέζονται ως νόμιμο αρχείο, όπως ένα συνημμένο ηλεκτρονικού ταχυδρομείου από έναν υποτιθέμενο φίλο με ένα πολύ πιστευτό όνομα, και σε πρώτη ματιά πείθουν ως τυπική εισερχόμενη ηλεκτρονική αλληλογραφία χωρίς να προδίδουν την κακόβουλη φύση τους. Ο χρήστης εν αγνοία του βρίσκεται σε κίνδυνο να εγκαταστήσει ένα trojan-μολυσμένο πρόγραμμα μέσω drive-by λήψης όταν ανοίγει ένα mail, επισκεπτόμενος μια ιστοσελίδα, παίζοντας online παιχνίδια ή χρησιμοποιώντας internet-drive εφαρμογές. Ένας δούρειος ίππος μπορεί να προκαλέσει ζημιά παρόμοια με άλλους ιούς, όπως η κλοπή πληροφοριών ή η παρεμπόδιση/διακοπή της λειτουργίας των συστημάτων υπολογιστών.[25]

Πώς γίνεται αυτό; Ο κακόβουλος κώδικας ή ιός εισάγεται στην αλυσίδα της διοίκησης, έτσι ώστε όταν το μολυσμένο πρόγραμμα εκτελείται, ο ιογενής κώδικας εκτελείται επίσης (ή σε ορισμένες περιπτώσεις, τρέχει αντί του νόμιμου προγράμματος). Οι ιοί θεωρούνται συνήθως ως εξωγενής κώδικας που επισυνάπτεται σε ένα πρόγραμμα υποδοχής, αλλά αυτό δεν συμβαίνει πάντα. Μερικές φορές, το περιβάλλον χειραγωγείται έτσι ώστε καλώντας ένα νόμιμο μη μολυσμένο πρόγραμμα καλεί το πρόγραμμα ιού. Το ιογενές πρόγραμμα μπορεί επίσης να εκτελεστεί πριν από οποιοδήποτε άλλο πρόγραμμα. Αυτό μπορεί να μολύνει

ουσιαστικά κάθε εκτελέσιμο αρχείο στον υπολογιστή, ακόμα κι αν κανένας από αυτούς τους κώδικες αρχείων δεν ήταν πραγματικά αλλοιωμένος. Οι ιοί που ακολουθούν αυτόν τον τρόπο λειτουργίας περιλαμβάνουν ιούς "cluster" ή "FAT" (File Allocation Table, Πίνακας Εκχώρησης Αρχείων), οι οποίοι ανακατευθύνουν τους δείκτες συστήματος σε μολυσμένα αρχεία, συσχετίζουν ιούς που τροποποιούν τις καταχωρήσεις καταλόγου μητρώου των Windows, έτσι ώστε ο δικός τους κώδικας να εκτελείται πριν από οποιοδήποτε άλλο νόμιμο πρόγραμμα.[26]



Εικόνα 3: Τρόποι διείσδυσης και μετάδοση κακόβουλου λογισμικού

Οι ιοί υπολογιστών συνήθως μεταδίδονται μέσω αφαιρούμενων μέσων ή του Διαδικτύου. Ένας δίσκος flash, ένα CD-ROM, ή άλλη συσκευή αποθήκευσης που βρίσκεται σε έναν μολυσμένο υπολογιστή έχει τη δυνατότητα να μολύνει όλους τους μελλοντικούς υπολογιστές στους οποίους χρησιμοποιείται. Ένας υπολογιστής μπορεί επίσης να συνάψει ιό από απειλητικά συνημμένα ηλεκτρονικού ταχυδρομείου, μολυσμένες ιστοσελίδες ή μολυσμένο λογισμικό, ο οποίος μπορεί να διαδοθεί σε κάθε άλλο υπολογιστή που μοιράζεται το ίδιο δίκτυο με τον αρχικά μολυσμένο υπολογιστή.[27]

Όλοι οι ιοί υπολογιστών προκαλούν άμεσες ή έμμεσες οικονομικές ζημίες. Με βάση αυτό, υπάρχουν δύο κατηγορίες ιών:

1) Εκείνοι που διαδίδουν μόνο και δεν προκαλούν τη σκόπιμη ζημία

2) Αυτά που είναι προγραμματισμένοι να προκαλέσουν ζημιά.

Ωστόσο, ακόμη και με τη διάδοση, καταλαμβάνουν άφθονο χώρο μνήμης, καθώς και το χρόνο και τους πόρους που δαπανώνται απλά και μόνο με την ανενεργή τους ύπαρξη στο σύστημα. Άμεσες επιβαρύνσεις προκαλούνται όταν οι ιοί αλλάζουν τις πληροφορίες κατά τη διάρκεια της ψηφιακής μετάδοσης. Σημαντικές δαπάνες πραγματοποιούνται από ιδιώτες, επιχειρήσεις και αρχές για την ανάπτυξη και την εφαρμογή των εργαλείων κατά των ιών για την προστασία των συστημάτων πληροφορικής.[28]

1.2.3 Λογικές Χρονο-Βόμβες

Μια χρονο-βόμβα, είναι ένα κακόβουλο κομμάτι κώδικα που εισάγεται σκόπιμα στο λογισμικό για να εκτελέσει μια κακόβουλη εργασία όταν ενεργοποιείται από ένα συγκεκριμένο γεγονός. Δεν είναι ιός, αν και συνήθως συμπεριφέρεται με παρόμοιο τρόπο. Κρυφά εισάγεται στο πρόγραμμα όπου βρίσκεται αδρανής μέχρι να πληρούνται οι καθορισμένες προϋποθέσεις. Το κακόβουλο λογισμικό, όπως οι ιοί και οι ιοί τύπου worm, συχνά περιέχουν τέτοιες βόμβες που ενεργοποιούνται σε ένα συγκεκριμένο ωφέλιμο φορτίο ή σε προκαθορισμένο χρόνο. Το ωφέλιμο φορτίο μιας βόμβας είναι άγνωστο στο χρήστη του λογισμικού και η εργασία που εκτελεί είναι ανεπιθύμητη. Οι κωδικοί προγραμμάτων που έχουν προγραμματιστεί να εκτελεστούν σε μια συγκεκριμένη χρονική στιγμή είναι γνωστοί ως χρονο-βόμβες. Για παράδειγμα, ο διαβόητος ιός "Παρασκευή 13" ο οποίος ενεργοποιούταν μονάχα εάν η ημερομηνία του συστήματος στην οποία βρισκόταν εγκατεστημένος ήταν η 13η μέρα του μήνα και συγχρόνως η ημέρα αυτή ήταν Παρασκευή προκαλώντας έτσι επιβράδυνση του συστήματος στην προκαθορισμένη χρονική στιγμή.[29]

Έχει παρατηρηθεί πως οι βόμβες αυτές χρησιμοποιούνται συνήθως από δυσαρεστημένους υπαλλήλους που εργάζονται στον τομέα της πληροφορικής. Πολλές φορές έχει γίνει λόγος για "το σύνδρομο των δυσαρεστημένων εργαζομένων" όπου θυμωμένοι εργαζόμενοι που έχουν απολυθεί χρησιμοποιούν βόμβες για να διαγράψουν τις βάσεις δεδομένων των εργοδοτών τους, απενεργοποιούν το δίκτυο για μια στιγμή ή ακόμη φτάνουν στο σημείο να κάνουν εμπιστευτικές συναλλαγές. Τα εναύσματα που σχετίζονται με την εκτέλεση βομβών μπορεί να είναι μια συγκεκριμένη ημερομηνία και ώρα, μια καταχώρηση

που λείπει από μια βάση δεδομένων ή να μην τοποθετεί μια εντολή τη συνηθισμένη ώρα, που σημαίνει ότι το άτομο δεν εργάζεται εκεί πια. Οι περισσότερες βόμβες παραμένουν μόνο στο δίκτυο στο οποίο απασχολούνταν. Έτσι, στις περισσότερες περιπτώσεις, είναι μια δουλειά εμπιστευτικών πληροφοριών. Αυτό τις καθιστά ευκολότερες στο σχεδιασμό και την εκτέλεση από έναν ιό. Δεν χρειάζεται να αναπαραχθεί, κάτι που είναι μια πιο περίπλοκη δουλειά. Για να διατηρηθεί το δίκτυό προστατευμένο από τις βόμβες, χρειάζεται συνεχής παρακολούθηση των δεδομένων και αποτελεσματικό λογισμικό προστασίας από ιούς σε κάθε έναν από τους υπολογιστές του δικτύου. [29]

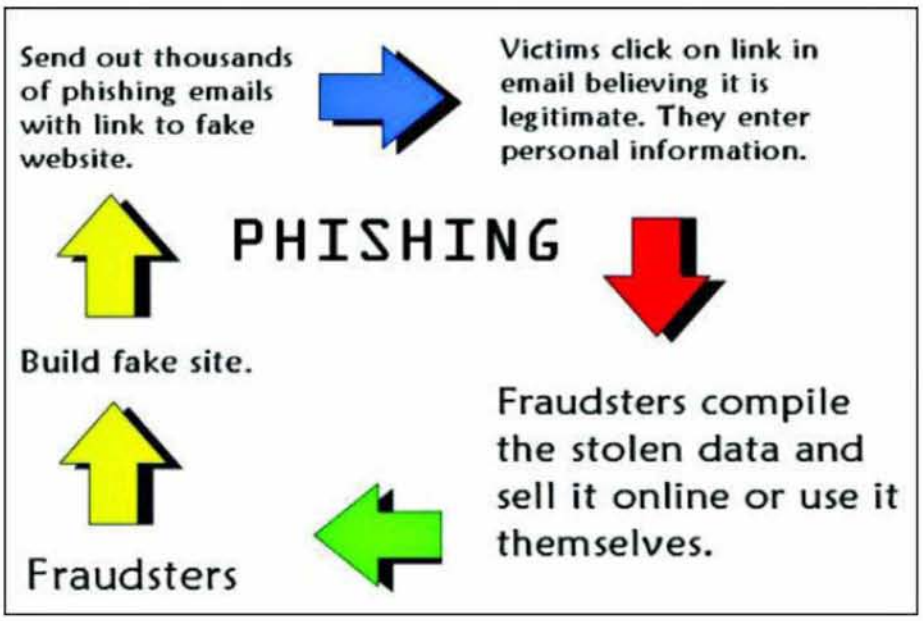
1.2.4 Επίθεση Άρνησης Υπηρεσίας

Μια επίθεση άρνησης υπηρεσίας DoS (Denial of Service) είναι μια ρητή προσπάθεια των επιτιθέμενων να αρνηθούν την υπηρεσία σε προβλεπόμενους χρήστες αυτής της υπηρεσίας. Περιλαμβάνει την υπέρ φόρτωση ενός πόρου υπολογιστή με περισσότερες αιτήσεις από ό, τι μπορεί να χειριστεί καταναλώνοντας το διαθέσιμο εύρος ζώνης του, το οποίο έχει ως αποτέλεσμα την υπερφόρτωση του διακομιστή. Αυτό προκαλεί τη διακοπή λειτουργίας ή την επιβράδυνση του πόρου (π.χ. διακομιστή web), ώστε να μην έχει κανείς πρόσβαση σε αυτόν. Χρησιμοποιώντας αυτήν την τεχνική, ο εισβολέας μπορεί να καταστήσει μια τοποθεσία Web μη λειτουργική στέλνοντας τεράστιες ποσότητες κυκλοφορίας στην τοποθεσία προορισμού. Μια τοποθεσία μπορεί να παρουσιάσει προσωρινά πλήρη δυσλειτουργία ή αιφνίδια διακοπή λειτουργίας, σε κάθε περίπτωση με αποτέλεσμα την αδυναμία του συστήματος να επικοινωνήσει επαρκώς. Οι επιθέσεις DoS παραβιάζουν τις αποδεκτές πολιτικές χρήσης σχεδόν όλων των παρόχων υπηρεσιών Διαδικτύου.[30]

Μια άλλη παραλλαγή σε μια επίθεση άρνησης υπηρεσίας είναι γνωστή ως "Κατανεμημένη άρνηση υπηρεσίας" (DDoS - Distributed Denial of Service) επίθεση όπου μια σειρά όπου δράστες πλημμυρίζουν την κυκλοφορία του δικτύου. Οι επιθέσεις άρνησης υπηρεσίας στοχεύουν συνήθως διακομιστές τοποθεσίας Web υψηλού προφίλ που ανήκουν σε τράπεζες και σε σελίδες που έχουν άμεση σχέση με την αγοροπωλησία. Ιστοσελίδες εταιρειών όπως η Amazon, CNN, Yahoo, Twitter και eBay έχουν γίνει θύμα τέτοιων επιθέσεων.[30]

1.2.5 Ηλεκτρονικό Ψάρεμα – Phishing

Αυτή είναι μια τεχνική εξαγωγής εμπιστευτικών πληροφοριών, όπως αριθμούς πιστωτικών καρτών, κωδικούς πρόσβασης χρήστη κοκ. Το ηλεκτρονικό ψάρεμα συνήθως πραγματοποιείται μέσω πλαστογράφησης και την κοινή χρήση του ηλεκτρονικού ταχυδρομείου. Πιθανώς μεγάλο ποσοστό χρηστών έχει λάβει μηνύματα ηλεκτρονικού ταχυδρομείου που περιέχουν συνδέσμους σε νόμιμες ιστοσελίδες που εμφανίζονται. [31]



Εικόνα 4: Τρόπος λειτουργίας phishing

Το κακόβουλο λογισμικό θα είχε εγκατασταθεί στον υπολογιστή υποκλέβοντας ιδιωτικές πληροφορίες. Οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν την κοινωνική μηχανική για να ξεγελάσουν τους χρήστες έτσι ώστε να κατεβάσουν κακόβουλο λογισμικό από το διαδίκτυο ή να συμπληρώσουν τα προσωπικά τους στοιχεία με ψευδείς προφάσεις. Μια απάτη ηλεκτρονικού "ψαρέματος" σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου μπορεί να αποφευχθεί, έχοντας κατά νου ορισμένα πράγματα.

- Αναζήτηση ορθογραφικών λαθών στο κείμενο.
- Τοποθέτηση του δείκτη του ποντικιού επάνω από τη διεύθυνση URL με υπερ-συνδέσεις, αλλά χωρίς κλικ. Έλεγχος αν η διεύθυνση ταιριάζει με αυτήν που αναγράφεται στο μήνυμα.
- Αξιολόγηση περιεχομένου για ψεύτικες απειλές.

- Οι επιτιθέμενοι χρησιμοποιούν τα ονόματα και τα λογότυπα γνωστών ιστοσελίδων για να εξαπατήσουν. Τα γραφικά και οι διευθύνσεις ιστού που χρησιμοποιούνται στο μήνυμα ηλεκτρονικού ταχυδρομείου είναι εντυπωσιακά παρόμοια με τα νόμιμα, αλλά οδηγούν σε ψεύτικες τοποθεσίες.[31]

Δεν γίνεται όλο το ηλεκτρονικό ψάρεμα μέσω ηλεκτρονικού ταχυδρομείου ή ιστοσελίδων. Το Vishing (voice-phishing) περιλαμβάνει κλήσεις σε θύματα χρησιμοποιώντας ψεύτικη ταυτότητα που ξεγελά τους χρήστες και θεωρούν ότι η κλήση είναι από έναν αξιόπιστο οργανισμό. Μπορεί να ισχυρίζονται ότι προέρχονται από μια τράπεζα ζητώντας να καλέσει ο χρήστης έναν αριθμό (που παρέχεται από την υπηρεσία VoIP - Voice over IP και ανήκει στον εισβολέα) και να εισάγει τα στοιχεία του λογαριασμού του. Μόλις το κάνει αυτό, η ασφάλεια του λογαριασμού του έχει παραβιαστεί. Για την αντιμετώπιση όλων των αυτόκλητων τηλεφωνικών κλήσεων χρειάζεται σκεπτικισμός και άρνηση παροχής προσωπικών πληροφοριών. Πολλές τράπεζες έχουν εκδώσει προληπτικές προειδοποιήσεις ενημερώνοντας τους χρήστες τους για απάτες ηλεκτρονικού "ψαρέματος" με τις ενέργειες και τις συναλλαγές σχετικά με τα στοιχεία του λογαριασμού. Έχει επίσης αναφερθεί ένας ακόμη τρόπος με τον οποίο χακάρονται λογαριασμοί gmail άλλων ανθρώπων με την αποστολή ενός μηνύματος ηλεκτρονικού ταχυδρομείου σε ένα λογαριασμό που αποτελείται με το όνομα χρήστη και τον κωδικό πρόσβασής, αυτό είναι το ψάρεμα.[32]

1.2.6 Βομβαρδισμός Ηλεκτρονικού Ταχυδρομείου και Spamming

Ο βομβαρδισμός μέσω ηλεκτρονικού ταχυδρομείου χαρακτηρίζεται από έναν κακοποιό που στέλνει τεράστιους όγκους ηλεκτρονικού ταχυδρομείου σε μια διεύθυνση στόχο με αποτέλεσμα τη συντριβή του λογαριασμού ηλεκτρονικού ταχυδρομείου ή των διακομιστών αλληλογραφίας του θύματος. Το μήνυμα δεν έχει νόημα και είναι υπερβολικά μεγάλο προκειμένου να καταναλωθούν πόροι δικτύου. Εάν είναι στοχευμένοι πολλοί λογαριασμοί ενός διακομιστή αλληλογραφίας, ενδέχεται να έχει αντίκτυπο στην άρνηση υπηρεσίας. Τέτοια αλληλογραφία που φθάνει συχνά στα εισερχόμενά μπορεί εύκολα να ανιχνευθεί από φίλτρα spam. Ο βομβαρδισμός ηλεκτρονικού ταχυδρομείου πραγματοποιείται συνήθως χρησιμοποιώντας botnets (ιδιωτικοί συνδεδεμένοι στο διαδίκτυο υπολογιστές των οποίων η ασφάλεια έχει παραβιαστεί από κακόβουλο λογισμικό και βρίσκονται υπό τον έλεγχο του εισβολέα) ως επίθεση DDoS. [33]

Αυτός ο τύπος επίθεσης είναι πιο δύσκολο να ελεγχθεί λόγω πολλαπλών διευθύνσεων προέλευσης και των bots που έχουν προγραμματιστεί να στέλνουν διαφορετικά μηνύματα για να νικήσουν τα φίλτρα ανεπιθύμητης αλληλογραφίας. Το "Spamming" είναι μια παραλλαγή της βομβιστικής επίθεσης ηλεκτρονικού ταχυδρομείου. Εδώ τα αυτόκλητα μαζικά μηνύματα αποστέλλονται σε μεγάλο αριθμό χρηστών, αδιακρίτως. Το άνοιγμα συνδέσμων που δίνονται σε ανεπιθύμητα μηνύματα μπορεί να οδηγήσει σε ιστοσελίδες ηλεκτρονικού "ψαρέματος" που φιλοξενούν κακόβουλο λογισμικό. Η ανεπιθύμητη αλληλογραφία μπορεί επίσης να έχει μολυσμένα αρχεία ως συνημμένα. Η ανεπιθύμητη αλληλογραφία επιδεινώνεται όταν ο παραλήπτης απαντά στο μήνυμα ηλεκτρονικού ταχυδρομείου προκαλώντας τη λήψη της απάντησης από όλους τους αρχικούς παραλήπτες. Οι αποστολείς ανεπιθύμητης αλληλογραφίας συλλέγουν διευθύνσεις ηλεκτρονικού ταχυδρομείου από λίστες πελατών, ομάδες συζήτησης, chat-rooms, ιστοσελίδες και ιούς που συλλέγουν βιβλία διευθύνσεων χρηστών και τις πωλούν και σε άλλους αποστολείς ανεπιθύμητης αλληλογραφίας. Ένα μεγάλο ποσό ανεπιθύμητης αλληλογραφίας αποστέλλεται σε μη έγκυρες διευθύνσεις ηλεκτρονικού ταχυδρομείου.[33]

Εικόνα 5 : Το ηλεκτρονικό ταχυδρομείο φιλτράρει την ανεπιθύμητη αλληλογραφία

Η αποστολή ανεπιθύμητων μηνυμάτων παραβιάζει την αποδεκτή πολιτική χρήσης (AUP - Acceptable Use Policy) σχεδόν όλων των παρόχων υπηρεσιών Διαδικτύου. Εάν το σύστημά ξαφνικά γίνεται υποτονικό (το ηλεκτρονικό ταχυδρομείο φορτώνει αργά ή δεν φαίνεται να αποστέλλει ή να λαμβάνει), ο λόγος μπορεί να είναι ότι η πλατφόρμα που χρησιμοποιούμε επεξεργάζεται μεγάλο αριθμό μηνυμάτων. Δυστυχώς, αυτή τη στιγμή, δεν υπάρχει τρόπος να αποφευχθεί εντελώς η βομβιστική επίθεση ηλεκτρονικού ταχυδρομείου

και spam μηνυμάτων, καθώς είναι αδύνατο να προβλεφθεί η προέλευση της επόμενης επίθεσης. Ωστόσο, αυτό που μπορούν οι χρήστες να κάνουν είναι να προσδιορίσουν την πηγή των spam μηνυμάτων και να ρυθμίσουν το δρομολογητή τους ώστε να αποκλείει τυχόν εισερχόμενα πακέτα από αυτήν τη διεύθυνση.[34]

1.2.7 Web Jacking

Το Web jacking οφείλει το όνομά του στην "πειρατεία". Εδώ, ο χάκερ παίρνει τον έλεγχο μιας ιστοσελίδας δόλια. Μπορεί να αλλάξει το περιεχόμενο της αρχικής ιστοσελίδας ή ακόμη και να ανακατευθύνει το χρήστη σε ένα μια άλλη ψεύτικη παρόμοια σελίδα αναζήτησης που ελέγχεται από αυτόν. Ο ιδιοκτήτης της ιστοσελίδας δεν έχει πλέον τον έλεγχο και ο εισβολέας μπορεί να χρησιμοποιήσει την ιστοσελίδα για τα δικά του εγωιστικά συμφέροντα.

Η επίθεση μεθόδου υποδοχής ιστού μπορεί να χρησιμοποιηθεί για να δημιουργήσει έναν κλώνο της ιστοσελίδας, και να παρουσιάσει το θύμα με τη νέα σύνδεση λέγοντας ότι η περιοχή έχει μετακινηθεί. Σε αντίθεση με τις συνήθεις μεθόδους ηλεκτρονικού "ψαρέματος", όταν τοποθετείται ο δείκτης του ποντικιού πάνω από τη σύνδεση που παρέχεται, η διεύθυνση URL που παρουσιάζεται θα είναι η αρχική και όχι η τοποθεσία του εισβολέα. Αλλά όταν γίνεται η επιλογή στο νέο σύνδεσμο, ανοίγει και αντικαθίσταται γρήγορα με το κακόβουλο διακομιστή web. Το όνομα στη γραμμή διευθύνσεων θα είναι ελαφρώς διαφορετικό από την αρχική ιστοσελίδα που μπορεί να ξεγελάσει το χρήστη να νομίζει ότι είναι μια νόμιμη τοποθεσία. Για παράδειγμα, το "gmail" μπορεί να κατευθύνει στο "**gmai1**". [35]

Το Web jacking μπορεί επίσης να γίνει με την αποστολή ενός πλαστού μηνύματος στο καταχωρητή που ελέγχει την καταχώριση ονόματος τομέα, με μια ψευδή ταυτότητα ζητώντας του να συνδέσει ένα όνομα τομέα με τη διεύθυνση IP του webjacker, στέλνοντας έτσι στους ανύποπτους καταναλωτές που εισάγουν το συγκεκριμένο όνομα τομέα σε μια ιστοσελίδα που ελέγχεται από το webjacker. Ο σκοπός αυτής της επίθεσης είναι να προσπαθήσει να συγκομίσει τα διαπιστευτήρια, τα ονόματα χρήστη, τους κωδικούς πρόσβασης και τους αριθμούς λογαριασμών των χρηστών, χρησιμοποιώντας μια ψεύτικη ιστοσελίδα με μια έγκυρη σύνδεση που ανοίγει όταν ο χρήστης ανακατευθύνεται σε αυτό μετά το άνοιγμα της νόμιμης ιστοσελίδας.[35]

1.2.8 Παρακολούθηση στον Κυβερνοχώρο

Η Cyberstalking είναι μια νέα μορφή του εγκλήματος στο διαδίκτυο στην κοινωνία μας, όταν ένα άτομο επιδιώκεται ή ακολουθείται σε απευθείας σύνδεση. Ένας κυνηγός στον κυβερνοχώρο δεν ακολουθεί σωματικά το θύμα του. Το κάνει ουσιαστικά με την ακολουθία, της σε απευθείας σύνδεση δραστηριότητάς του για να συγκομίσει τις πληροφορίες για τη παρακολούθηση και να παρενοχλήσει τον χρήστη και να κάνει τις απειλές χρησιμοποιώντας τον λεκτικό εκφοβισμό. Κοινώς, παραβίαση της ιδιωτικής ζωής κάποιου στο διαδίκτυο.[36]

Η Cyber παρακολούθηση χρησιμοποιεί το διαδίκτυο ή οποιοδήποτε άλλο ηλεκτρονικό μέσο και είναι διαφορετική από την offline παρακολούθηση, ενώ μερικές φορές μπορεί να συνοδεύεται και από αυτή. Οι Cyberstalkers ευδοκιμούν σε άπειρους χρήστες του διαδικτύου που δεν γνωρίζουν καλά το δίκτυο και τους κανόνες της ασφάλειας στο διαδίκτυο. Ένας κυνηγός στον κυβερνοχώρο μπορεί να είναι ένας ξένος, αλλά θα μπορούσε εξίσου εύκολα να είναι κάποιος που γνωρίζει το θύμα.[36]

Οι κυνηγοί του κυβερνοχώρου παρενοχλούν τα θύματά τους μέσω ηλεκτρονικού ταχυδρομείου, chatrooms, ιστοσελίδων, φόρουμ συζητήσεων και ανοικτών ιστοσελίδων δημοσίευσης (π.χ. ιστολόγια). Η διαθεσιμότητα του δωρεάν ηλεκτρονικού ταχυδρομείου / website χώρο και η ανωνυμία που παρέχεται από chatrooms και φόρουμ έχει συμβάλει στην αύξηση των περιστατικών παρακολούθησης στον κυβερνοχώρο. Ο καθένας έχει μια σε απευθείας σύνδεση παρουσία στις μέρες μας, και είναι πραγματικά εύκολο να κάνει μια αναζήτηση Google και να πάρει το όνομα κάποιου, ψευδώνυμο, τον αριθμό επικοινωνίας και τη διεύθυνση, συμβάλλοντας στην απειλή που είναι η παρακολούθηση στον κυβερνοχώρο. Δεδομένου ότι το διαδίκτυο γίνεται όλο και περισσότερο αναπόσπαστο μέρος της προσωπικής και επαγγελματικής ζωής μας, οι stalkers μπορούν να επωφεληθούν από την ευκολία των επικοινωνιών και τη διαθεσιμότητα των προσωπικών πληροφοριών μόνο με μερικά κλικ του ποντικιού μακριά. Επιπλέον, ο ανώνυμος και μη συγκρουσιακός χαρακτήρας των διαδικτυακών επικοινωνιών αφαιρεί περαιτέρω τυχόν αντικίνητρα με τον τρόπο της παρακολούθησης στον κυβερνοχώρο. Η παρακολούθηση στον κυβερνοχώρο γίνεται με δύο πρωταρχικούς τρόπους:[37]

- **Παρακολούθηση στο διαδίκτυο:** Εδώ ο παραβάτης παρενοχλεί το θύμα μέσω του διαδικτύου. Αυτόκλητα μηνύματα ηλεκτρονικού ταχυδρομείου είναι ο πιο συνηθισμένος τρόπος για να απειλεί κάποιον, και ο παραβάτης μπορεί ακόμη και να

στείλει ιούς μέσω ηλεκτρονικού ταχυδρομείου. Ωστόσο, οι ιοί και τα ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου από μόνα τους δεν συνιστούν παρακολούθηση στον κυβερνοχώρο. Αλλά εάν μηνύματα στέλνονται από το ηλεκτρονικό ταχυδρομείο επανειλημμένα σε μια προσπάθεια να εκφοβίσει τον παραλήπτη, μπορούν να θεωρηθούν ως καταδίωξη. Η παρακολούθηση του Διαδικτύου δεν περιορίζεται στο ηλεκτρονικό ταχυδρομείο. Οι stalkers μπορούν να χρησιμοποιήσουν πιο ολοκληρωμένα το διαδίκτυο για να παρενοχλούν τα θύματα. Οποιοδήποτε άλλο έγκλημα στον κυβερνοχώρο που έχουμε ήδη διαβάσει, αν γίνει με την πρόθεση να απειλήσει, να παρενοχλήσει ή να συκοφαντήσει το θύμα μπορεί να ισοδυναμεί με παρακολούθηση στον κυβερνοχώρο.

- **Παρακολούθηση υπολογιστών:** Οι πιο τεχνολογικά προηγμένοι διώκτες εφαρμόζουν τις δεξιότητες των υπολογιστών τους για να τους βοηθήσουν με το έγκλημα. Αποκτούν μη εξουσιοδοτημένο έλεγχο του υπολογιστή του θύματος με την εκμετάλλευση της λειτουργίας του διαδικτύου και του λειτουργικού συστήματος των Windows. Αν και αυτό γίνεται συνήθως από τους πιο ικανούς χρήστες υπολογιστών, οι οδηγίες για το πώς να επιτευχθεί αυτό είναι εύκολα διαθέσιμες στο διαδίκτυο.[37]

Η Cyber καταδίωξη έχει πλέον ανοίξει τα φτερά της στην κοινωνική δικτύωση. Με την αυξημένη χρήση των μέσων κοινωνικής δικτύωσης, όπως το Facebook, το Twitter, το Flickr και το YouTube, το προφίλ , οι φωτογραφίες και οι ενημερώσεις κατάστασης είναι για να τα δει ο κόσμος. Η Online παρουσία παρέχει αρκετές πληροφορίες για να γίνει κάποιος ένα πιθανό θύμα της καταδίωξης χωρίς καν να γνωρίζει τον κίνδυνο. Με τα "check-ins", τα "γεγονότα ζωής", τις εφαρμογές που έχουν πρόσβαση στις προσωπικές πληροφορίες και την ανάγκη να παρουσιάζονται σχεδόν όλα όσα κάνει και πού το κάνει ο χρήστης, δεν αφήνει πραγματικά τίποτα για τους διώκτες να καταλάβουν για τον εαυτό του. Η τεχνολογία κοινωνικής δικτύωσης παρέχει μια κοινωνική και συνεργατική πλατφόρμα για τους χρήστες του διαδικτύου να αλληλεπιδρούν, να εκφράζουν τις σκέψεις τους και να μοιράζονται σχεδόν τα πάντα για τη ζωή τους. Αν και προωθεί την κοινωνικοποίηση μεταξύ των ανθρώπων, στην πορεία συμβάλλει στην αύξηση των παραβιάσεων του διαδικτύου.[37]

1.2.9 Data Diddling

Το Data Diddling είναι μη εξουσιοδοτημένη τροποποίηση πληροφοριών καθώς εισάγονται σε ένα σύστημα υπολογιστή. Χρησιμοποιώντας αυτήν την τεχνική, ο εισβολέας μπορεί να τροποποιήσει την αναμενόμενη έξοδο και είναι δύσκολο να εντοπιστεί. Με άλλα λόγια, οι αρχικές πληροφορίες που πρέπει να εισαχθούν αλλάζουν, είτε από ένα άτομο που πληκτρολογεί τα δεδομένα, έναν ιό που έχει προγραμματιστεί να αλλάξει τα δεδομένα, τον προγραμματιστή της βάσης δεδομένων ή της εφαρμογής, ή οποιονδήποτε άλλο εμπλέκεται στη διαδικασία δημιουργίας, εγγραφής, κωδικοποίησης, εξέτασης, ελέγχου, μετατροπής ή μετάδοσης δεδομένων.[38]

Αυτή είναι μια από τις απλούστερες μεθόδους για τη διάπραξη ενός ηλεκτρονικού εγκλήματος που σχετίζεται με αυτό, επειδή ακόμη και ένας ερασιτέχνης στους υπολογιστές μπορεί να το κάνει. Παρά το γεγονός ότι αυτό είναι ένα αβίαστο έργο, μπορεί να έχει αρνητικές επιπτώσεις. Για παράδειγμα, ένα άτομο που είναι υπεύθυνο για τη λογιστική πτυχή μιας εταιρίας μπορεί να αλλάξει δεδομένα σχετικά με τον εαυτό του ή έναν φίλο ή συγγενή που δείχνει ότι πληρώνεται πλήρως. Τροποποιώντας κατάλληλα τα ευαίσθητα δεδοένα μπορεί να εισαγάγουν πληροφορίες και στην συνέχεια να κλέψουν από την επιχείρηση.

1.2.10 Κλοπή Ταυτότητας και Απάτη Πιστωτικών Καρτών

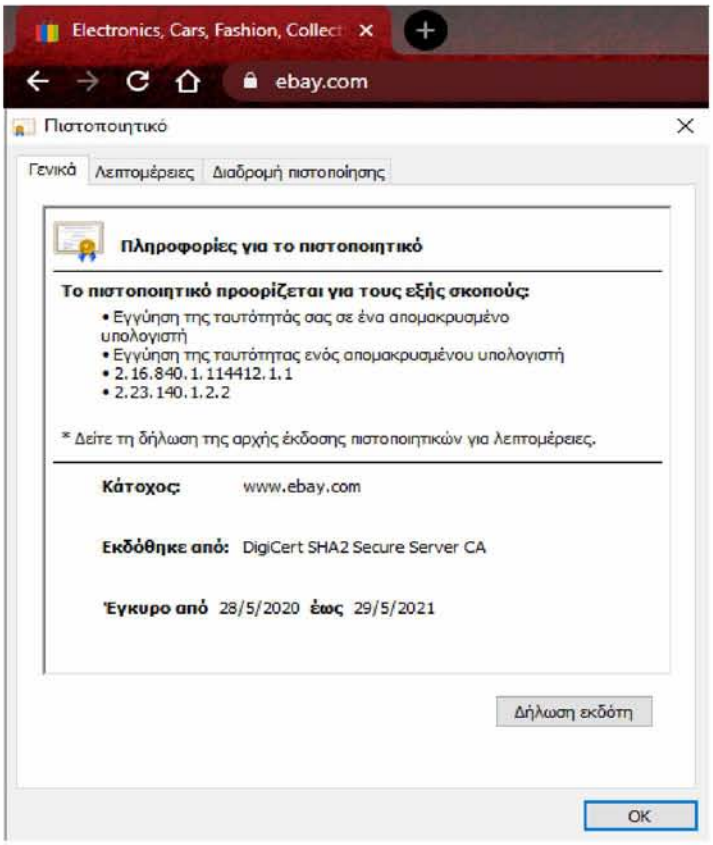
Η κλοπή ταυτότητας συμβαίνει όταν κάποιος κλέβει την ταυτότητά του χρήστη και προσποιείται ότι είναι αυτός για να αποκτήσει πρόσβαση σε πόρους όπως πιστωτικές κάρτες, τραπεζικούς λογαριασμούς και άλλα οφέλη στο όνομά του. Ο απατεώνας μπορεί επίσης να χρησιμοποιήσει την ταυτότητά για να διαπράξει άλλα εγκλήματα. Η "Απάτη πιστωτικών καρτών" χαρακτηρίζει ένα ευρύ χρονικό διάστημα για τα εγκλήματα που αφορούν την κλοπή ταυτότητας, όπου ο εγκληματίας χρησιμοποιεί την πιστωτική κάρτα για τη χρηματοδότηση των συναλλαγών του. Η απάτη πιστωτικών καρτών είναι κλοπή ταυτότητας στην απλούστερη μορφή της. Η πιο συνηθισμένη περίπτωση απάτης με πιστωτικές κάρτες είναι η προέγκριση κάρτας που πέφτει στα χέρια κάποιου άλλου.[39]

Εικόνα 6 : Η απάτη της πιστωτικής κάρτας είναι ο πιο κοινός τρόπος για τους χάκερ να κλέψουν χρήματα

Μπορεί να τη χρησιμοποιήσει για να αγοράσει οτιδήποτε μέχρι οι πράξεις του να γίνουν εμφανείς και να μπλοκάρει την κάρτα του χρήστη. Το μόνο μέτρο ασφαλείας στις αγορές πιστωτικών καρτών είναι η υπογραφή στην απόδειξη, αλλά αυτό μπορεί πολύ εύκολα να πλαστογραφηθεί. Ωστόσο, σε ορισμένες χώρες ο έμπορος μπορεί ακόμη και να ζητήσει ένα αναγνωριστικό ή ένα PIN, ως επιπλέον μέτρο ασφαλείας και διασφάλισης της αληθής ταυτότητας του κατόχου της εν λόγω κάρτας. Ορισμένες εταιρείες πιστωτικών καρτών έχουν λογισμικό για να εκτιμήσουν την πιθανότητα απάτης. Εάν πραγματοποιηθεί μια ασυνήθιστα μεγάλη συναλλαγή, ο εκδότης μπορεί ακόμη και να καλέσει για επαλήθευση τον κάτοχο της κάρτας. [39]

Συχνά οι άνθρωποι ξεχνούν να συλλέξουν το αντίγραφο της απόδειξης της πιστωτικής κάρτας. Αυτές οι αποδείξεις έχουν τον αριθμό της πιστωτικής μας κάρτας και την υπογραφή μας για οποιονδήποτε θελήσει να τη δει και να τη χρησιμοποιήσει. Με μόνο αυτές τις πληροφορίες, κάποιος μπορεί να κάνει αγορές online ή μέσω τηλεφώνου και ο κάτοχος δεν θα το παρατηρήσει μέχρι να γίνει προσωπικός έλεγχος των χρηματικών κινήσεων. Είναι απαραίτητο να βεβαιώνεται ο καθένας ότι ο ιστότοπος είναι αξιόπιστος και ασφαλής όταν πραγματοποιεί ηλεκτρονικές αγορές. Ορισμένοι χάκερ ενδέχεται να αποκτήσουν τον αριθμό της πιστωτικής κάρτας χρησιμοποιώντας τεχνικές ηλεκτρονικού "ψαρέματος". Μερικές φορές εμφανίζεται ένα μικροσκοπικό εικονίδιο λουκέτου στην αριστερή γωνία της οθόνης της γραμμής διευθύνσεων στο πρόγραμμα περιήγησής, το οποίο παρέχει υψηλότερο επίπεδο ασφάλειας για τη μετάδοση δεδομένων. Εάν κάνει κάποιος κλικ σε αυτό, φαίνεται επίσης το λογισμικό κρυπτογράφησης που χρησιμοποιεί η σελίδα που επισκεπτόμαστε.[39]

Μια πιο σοβαρή ανησυχία είναι η χρήση των προσωπικών πληροφοριών με τη βοήθεια κλεμμένων ή πλαστών εγγράφων είναι το άνοιγμα λογαριασμών (ή ακόμα χειρότερα, χρησιμοποιώντας τον υπάρχοντα λογαριασμό ενός χρήστη) για να πάρει κάποιος ένα δάνειο στο όνομά του. Οι επίδοξοι εγκληματίες, μπορούν να συλλέξουν τα προσωπικά στοιχεία κάποιου από το γραμματοκιβώτιό ή τον κάδο απορριμμάτων. Αν αναλογιστεί κάποιος όλες τις σημαντικές λεπτομέρειες που αναγράφονται σε αποδείξεις, τα αποκόμματα πληρωμής θα ήταν σημαντικό να τεμαχίζονται όλα τα ευαίσθητα έγγραφα κατά το πέρας της χρήσης τους. [40]



Εικόνα 7 : Πιστοποίηση ασφάλειας ιστοσελίδας

Με τις αυξανόμενες περιπτώσεις απάτης πιστωτικών καρτών, πολλά χρηματοπιστωτικά ιδρύματα έχουν παρέμβει με λύσεις λογισμικού για την παρακολούθηση της πιστωτικής και τη φύλαξη της ταυτότητάς των χρηστών. Η ασφάλεια κλοπής ταυτότητας μπορεί να ληφθεί για να ανακτήσει τους χαμένους μισθούς και να αποκαταστήσει την πιστωτική κάρτα. Αλλά για να μην ξοδέψει κάποιος μια περιουσία σε αυτές τις υπηρεσίες, πρέπει να εφαρμόσει τα χωρίς κόστος, μέτρα κοινής λογικής για να αποτρέψει ένα τέτοιο έγκλημα.[40]

1.2.11 Salami Επίθεση με Τεμαχισμό

Μια "επίθεση με τεμαχισμό" ή "απάτη σαλάμι" είναι μια τεχνική με την οποία οι εγκληματίες του κυβερνοχώρου κλέβουν χρήματα ή πόρους κομμάτι κομμάτι κάθε φορά, έτσι ώστε να μην υπάρχει αισθητή διαφορά στο συνολικό μέγεθος. Ο δράστης ξεφεύγει με αυτά τα μικρά κομμάτια από ένα μεγάλο αριθμό πόρων και έτσι συσσωρεύει ένα σημαντικό ποσό κατά τη διάρκεια μιας χρονικής περιόδου. Η ουσία αυτής της μεθόδου είναι η αποτυχία ανίχνευσης της υπεξαίρεσης. Η πιο κλασική προσέγγιση είναι η τεχνική "collect-the-roundoff". Οι περισσότεροι υπολογισμοί πραγματοποιούνται σε ένα συγκεκριμένο νόμισμα στρογγυλοποιούνται προς τα πάνω στον πλησιέστερο αριθμό περίπου το ήμισυ του χρόνου και κάτω από το υπόλοιπο του χρόνου. Εάν ένας προγραμματιστής αποφασίσει να συλλέξει αυτά τα περιττά κλάσματα σε ξεχωριστό λογαριασμό, καμία καθαρή απώλεια για το σύστημα δεν φαίνεται εμφανής. Αυτό γίνεται με τη προσεκτική μεταφορά των κεφαλαίων στο λογαριασμό του δράστη.[39]

Οι εισβολείς εισάγουν ένα πρόγραμμα στο σύστημα για την αυτόματη εκτέλεση της εργασίας. Οι λογικές βόμβες μπορούν επίσης να χρησιμοποιηθούν από ανικανοποίητους άπληστους υπαλλήλους που εκμεταλλεύονται την τεχνογνωσία τους για το δίκτυο ή/και την προνομιακή πρόσβαση στο σύστημα. Σε αυτήν την τεχνική, τα εγκληματικά προγράμματα λειτουργούν ως αριθμητικές αριθμομηχανές για την αυτόματη τροποποίηση δεδομένων, όπως στους υπολογισμούς τόκων. [39]

Η κλοπή χρημάτων ηλεκτρονικά είναι η πιο κοινή χρήση της τεχνικής τεμαχισμού σαλάμι, αλλά δεν περιορίζεται στο ξέπλυμα χρήματος. Αυτή η τεχνική μπορεί επίσης να εφαρμοστεί για τη συλλογή μικρών κομματιών πληροφοριών σε μια χρονική περίοδο για να συμπεράνει μια συνολική εικόνα ενός οργανισμού. Αυτή η πράξη κατανεμημένης συλλογής πληροφοριών μπορεί να πλήττει άτομο ή οργανισμό. Τα δεδομένα μπορούν να συλλεχθούν από ιστοσελίδες, διαφημίσεις, έγγραφα που συλλέγονται από κάδους απορριμμάτων, και άλλα παρόμοια και σταδιακά να οδηγήσουν στη δημιουργία μιας ολόκληρης βάσης δεδομένων των πραγματικών πληροφοριών σχετικά με το στόχο.

Δεδομένου ότι το ποσό της υπεξαίρεσης είναι ακριβώς κάτω από το όριο της αντίληψης, πρέπει να είναι όλοι πιο προσεκτικοί. Η προσεκτική εξέταση των περιουσιακών στοιχείων, των συναλλαγών και κάθε άλλης συναλλαγής, συμπεριλαμβανομένης της ανταλλαγής

εμπιστευτικών πληροφοριών με άλλους, μπορεί να βοηθήσει στη μείωση των πιθανοτήτων επίθεσης με αυτή τη μέθοδο.[39]

1.2.12 Πειρατεία Λογισμικού

Χάρη στο διαδίκτυο και τα torrents, ο καθένας μπορεί να βρει σχεδόν οποιαδήποτε ταινία, λογισμικό ή τραγούδι από οποιαδήποτε προέλευση δωρεάν. Η πειρατεία στο Διαδίκτυο αποτελεί αναπόσπαστο μέρος της ζωής μας, στο οποίο εν γνώσει ή εν αγνοία μας όλοι συμβάλλουμε. Με αυτόν τον τρόπο, τα κέρδη των προγραμματιστών μειώνονται. Δεν είναι μόνο για την καταπάτηση της πνευματικής ιδιοκτησίας κάποιου άλλου παράνομα, αλλά και τη μεταβίβασή της στους φίλους του με περαιτέρω μείωση των εσόδων που τους αξίζουν.

Η πειρατεία είναι ανεξέλεγκτη ανά τον κόσμο, αλλά γνωστό επίσης είναι ότι η πειρατεία λογισμικού είναι η μη εξουσιοδοτημένη χρήση και διανομή λογισμικού υπολογιστών. Οι προγραμματιστές λογισμικού εργάζονται σκληρά για την ανάπτυξη αυτών των προγραμμάτων και η πειρατεία περιορίζει την ικανότητά τους να παράγουν αρκετά έσοδα για να διατηρήσουν την ανάπτυξη εφαρμογών. Αυτό επηρεάζει ολόκληρη την παγκόσμια οικονομία, καθώς τα κεφάλαια αναμεταδίδονται από άλλους τομείς, γεγονός που οδηγεί σε λιγότερες επενδύσεις στο μάρκετινγκ και την έρευνα.[38]

Τα ακόλουθα αποτελούν πειρατεία λογισμικού:

- Φόρτωση λογισμικού χωρίς άδεια χρήσης στον υπολογιστή
- Χρήση λογισμικού με μία άδεια χρήσης σε πολλούς υπολογιστές
- Χρήση μιας βασικής γεννήτριας για την παράκαμψη της προστασίας αντιγραφής
- Διανομή μιας έκδοσης λογισμικού με άδεια χρήσης ή χωρίς άδεια χρήσης ("σπασμένη") μέσω internet και χωρίς σύνδεση[38]

Η "Κλωνοποίηση" είναι μια άλλη απειλή. Συμβαίνει όταν κάποιος αντιγράφει την ιδέα πίσω από το λογισμικό κάποιου και γράφει το δικό του κώδικα. Δεδομένου ότι οι ιδέες που δεν αποτελούν αντιγραφή προστατεύονται, αυτό δεν είναι αυστηρά παράνομο. Ένα λογισμικό "σπασμένο" είναι παράνομο και η λήψη της έκδοσης του λογισμικού αυτού λειτουργεί γύρω από την κωδικοποιημένη πρόληψη του αντίγραφου. Οι χρήστες του

πειρατικού λογισμικού μπορούν να χρησιμοποιήσουν μια βασική γεννήτρια για να παραγάγουν έναν «αύξοντα» αριθμό που ξεκλειδώνει μια έκδοση αξιολόγησης του λογισμικού, νικώντας κατά συνέπεια την προστασία αντιγράφων. Το σπάσιμο λογισμικού και η χρήση μη εξουσιοδοτημένων κλειδιών είναι παράνομες πράξεις παραβίασης πνευματικών δικαιωμάτων.[38]

Η χρήση πειρατικού υλικού συνοδεύεται από τους δικούς της κινδύνους. Το πειρατικό λογισμικό μπορεί να περιέχει Trojans, ιούς, σκουλήκια και άλλο κακόβουλο λογισμικό, δεδομένου ότι οι πειρατές θα μολύνουν συχνά το λογισμικό με κακόβουλο κώδικα. Οι χρήστες πειρατικού λογισμικού μπορούν να τιμωρηθούν από το νόμο για παράνομη χρήση υλικού που προστατεύεται από πνευματικά δικαιώματα. Ενώ όπως είναι φυσικό, πλέον δεν θα μπορούν οι χρήστες να έχουν την υποστήριξη λογισμικού που παρέχεται από τους προγραμματιστές.[39]

Για να προστατεύσει κάποιος το λογισμικό του από την πειρατεία, αν είναι προγραμματιστής, θα πρέπει να εφαρμόσει ισχυρές διασφαλίσεις. Ορισμένοι ιστότοποι πωλούν λογισμικό με ένα "ψηφιακό αποτύπωμα" που βοηθά στον εντοπισμό των πειρατικών αντιγράφων στην πηγή. Μια άλλη κοινή μέθοδος είναι το κλείδωμα υλικού. Χρησιμοποιώντας αυτό, η άδεια χρήσης λογισμικού είναι κλειδωμένη σε ένα συγκεκριμένο υλικό υπολογιστή, έτσι ώστε να εκτελείται μόνο σε αυτόν τον υπολογιστή. Δυστυχώς, οι χάκερ συνεχίζουν να βρίσκουν το δρόμο τους γύρω από αυτά τα μέτρα.[38]

Μέχρι στιγμής έχει γίνει συζήτηση για τις ειδικές μεθόδους διάπραξης εγκλημάτων στον κυβερνοχώρο. Εν συντομία, κάθε αδίκημα που διαπράττεται με τη χρήση ηλεκτρονικών μέσων, όπως ο καθαρός εκβιασμός, ο εκφοβισμός στον κυβερνοχώρο, και η απάτη στο διαδίκτυο, ονομάζεται έγκλημα στον κυβερνοχώρο. Το διαδίκτυο είναι ένα τεράστιο γόνιμο έδαφος για πληθώρα παραβάσεων, οι οποίες όμως υπόκεινται σε διαφορετικές βαθμίδες σημαντικότητας, βάσει των πολιτιστικών θέσεων και πεποιθήσεων που της εκάστοτε χώρας και νομοθεσίας καθώς αυτό που μπορεί να θεωρηθεί άσεμνο σε μια χώρα, μπορεί να μην θεωρηθεί με τον ίδιο τρόπο σε άλλες χώρες.[39]

1.3. Στοιχεία ηλεκτρονικού εγκλήματος

- Η χρήση malware ευθύνεται στο μεγαλύτερο ποσοστό στις διαδικτυακές επιθέσεις

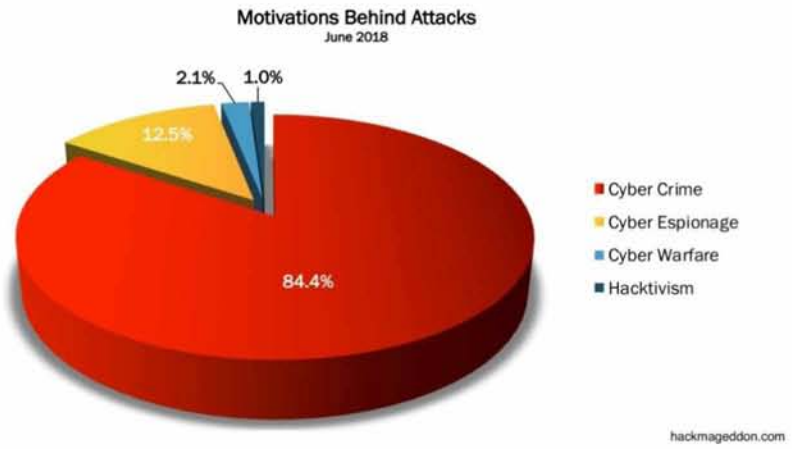
Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	⊃	1. Malware	⊃	→
2. Web Based Attacks	∩	2. Web Based Attacks	∩	→
3. Web Application Attacks	∩	3. Web Application Attacks	⊃	→
4. Phishing	∩	4. Phishing	∩	→
5. Spam	∩	5. Denial of Service	∩	↑
6. Denial of Service	∩	6. Spam	⊃	↓
7. Ransomware	∩	7. Botnets	∩	↑
8. Botnets	∩	8. Data Breaches	∩	↑
9. Insider threat	⊃	9. Insider Threat	∪	→
10. Physical manipulation/ damage/ theft/loss	⊃	10. Physical manipulation/ damage/ theft/loss	⊃	→
11. Data Breaches	∩	11. Information Leakage	∩	↑
12. Identity Theft	∩	12. Identity Theft	∩	→
13. Information Leakage	∩	13. Cryptojacking	∩	NEW
14. Exploit Kits	∪	14. Ransomware	∪	↓
15. Cyber Espionage	∩	15. Cyber Espionage	∪	→

Legend: Trends: ∪ Declining, ⊃ Stable, ∩ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Εικόνα 8 : Σύγκριση απειλών 2017-2018

- Η χρήση κακόβουλου λογισμικού είναι η υπεύθυνη για την μεγαλύτερη οικονομική ζημιά σε οργανισμούς. Και πάνω από το ένα τέταρτο αυτών είχαν έως στόχο κάποιο τραπεζικό σύστημα.

- Κατά το έτος 2018 το ηλεκτρονικό έγκλημα απέδωσε κατά προσέγγιση 1.5 τρις εκατομμύρια δολάρια.
- Ο χρόνος που μένει ανενεργή μια ιστοσελίδα μιας μεγάλης επιχείρησης αγοροπωλησιών της κοστίζει 24 φορές το ποσό που ζητούνται ως λύτρα για την επαναφορά της.
- Το 2018 το 84.4% του κινήτρου πίσω από μια επίθεση κακόβουλης εισόδου ήταν το ηλεκτρονικό έγκλημα. Με μόλις 1% να πρόκειται για ακτιβιστικούς λόγους.



Εικόνα 9 : Στατιστικά κινήτρου επίθεσης

- Τα τελευταία 6 χρόνια παραπάνω από 1.3 δις εκατομμύρια προφίλ σε πλατφόρμες κοινωνικής δικτύωσης είχαν πέσει θύμα υποκλοπής των στοιχείων τους.

- Εκτιμάτε μια άνοδος της τάξης του 70% σε παραβιάσεις ασφαλείας από διαδικτυακές επιθέσεις έως το 2024.

- Κατά μέσο όρο μια επίθεση hacker σε οποιοδήποτε επίπεδο προκύπτει κάθε 40 δευτερόλεπτα.

- Το 2018, το μεγαλύτερο ποσοστό – το ένα πέμπτο των επιθέσεων που έγιναν είχαν ατομικούς στόχους.

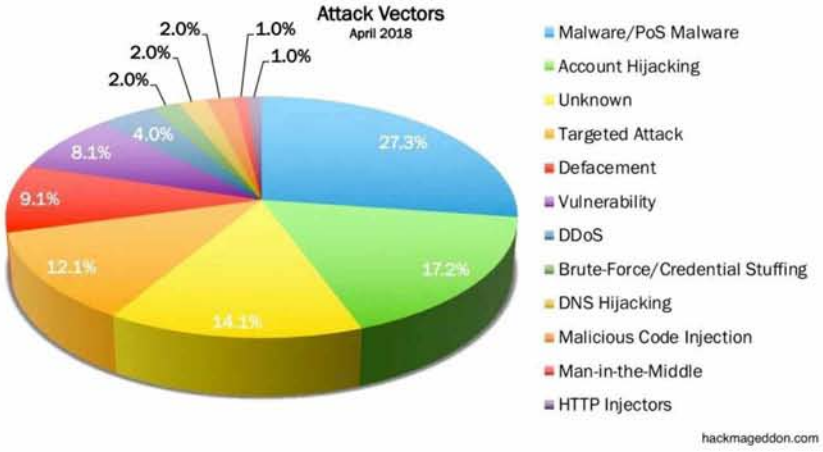
- Παραπάνω από 24.000 εφαρμογές κινητών που έχουν ως σκοπό την υποκλοπή πληροφοριών του χρήστη μαρκάρονται και μπλοκάρονται από τους αντίστοιχους παροχείς εφαρμογών

Εικόνα 10 : Στόχος επιθέσεων

- Τα μεγαλύτερα ποσοστά επιθέσεων διακρίνονται σε χώρες όπως την Κίνα και τις Ηνωμένες Πολιτείες της Αμερικής ενώ το χαμηλότερο αντίστοιχο ποσοστό στην Ολλανδία.

- Ένα σημαντικό ατού στο οποίο βασίζονται πολύ παραβάτες είναι η αίσθηση ανωνυμίας που έχουν με την χρήση ψευδών στοιχείων και της ασφάλειας της απομακρυσμένης αλληλεπίδρασης που τους παρέχει η χρήση του υπολογιστή.

- Ένα ηλεκτρονικό έγκλημα μπορεί να είναι δύσκολο να εντοπιστεί και να συνδεθεί με τον πραγματικό παραβάτη ο οποίος μπορεί να χρησιμοποιεί ποικίλους τρόπους για να καλύψει τα ίχνη του και να κάνει τον εντοπισμό του πολύ δύσκολο.



Εικόνα 11 : Τρόποι επίθεσης

- Σε περίπτωση που διαφορετικά στοιχεία ενοχοποίησης όπως ένας ηλεκτρονικός υπολογιστής με σημαντικά ενοχοποιητικά στοιχεία ή η πιθανή τοποθεσία του παραβάτη βρεθούν σε διαφορετικές χώρες είναι απαραίτητη ή συνεργασία όλων των κρατών που φέρονται να έχουν εμπλέκονται με τον ένα ή τον άλλο τρόπο, όπως και προσδιορίζεται από το συνέδριο της Βουδαπέστης.

IoT

- Από το 2016 στο 2017 παρουσιάστηκε άνοδος 600% σε επιθέσεις ενάντια σε συσκευές συνδεδεμένες με το Internet of Things.
- Ο αριθμός των συσκευών που περιέχονται στο IoT αναμένεται να αυξηθεί στα 35 δισεκατομμύρια στο 2021 και στα 75 δισεκατομμύρια μέχρι το 2025.

- Η οικονομία που περιστρέφεται γύρω από την ασφάλεια των εφαρμογών που ανήκει στο IoT αυξάνεται με ετήσιο ρυθμό 44% υπολογίζοντας πως θα φτάσει τα 4.4 δισεκατομμύρια δολάρια έως το 2022.
- 69% των επιχειρήσεων έχουν δίκτυα τα οποία αποτελούνται από περισσότερες συσκευές που ανήκουν στο IoT από ότι υπολογιστές.
- 84% των ειδικών στον τομέα της τεχνολογίας θεωρούν πως οι υπολογιστές παρέχουν περισσότεροι προστασία από τις υπόλοιπες συσκευές IoT
- 48% των επιχειρήσεων δεν μπορούν να εντοπίσουν με βεβαιότητα κάποια παραβίαση συστήματος

1.4 Διακρίσεις Ηλεκτρονικού Εγκλήματος

Στην βιβλιογραφία γίνεται η διάκριση των εγκλημάτων στον κυβερνοχώρο τα οποία χωρίζονται αρχικά σε γνήσια ηλεκτρονικά εγκλήματα. Τα συγκεκριμένα εγκλήματα είναι αποτέλεσμα της χρήσης και της εμφάνισης των υπολογιστών και του διαδικτύου, καθώς η εκτέλεση τους χρειάζεται οπωσδήποτε τη χρήση ψηφιακής τεχνολογίας όπως και τη διερεύνησή τους. Τέτοια εγκλήματα συνήθως χαρακτηρίζονται εκείνα εναντίον της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας στα δεδομένα των ηλεκτρονικών υπολογιστών όπως έχουν αναληφθεί. Η διάκριση των ηλεκτρονικών εγκλημάτων έχει ορίσει ως δεύτερη κατηγορία διάκρισης τα παραδοσιακά ή συμβατικά εγκλήματα ως εκείνη τη μορφή η οποία προηγείται του χρόνου εμφάνισης των ηλεκτρονικών υπολογιστών και του διαδικτύου, δηλαδή αυτά που πλέον μπορεί να εμπλέκουν την χρήση υπολογιστή αλλά στην αρχική τους μορφή αυτό δεν ήταν απαραίτητο. Όπως για παράδειγμα, το ξέπλυμα βρώμικου χρήματος. Με αυτές τις μεταβλητές και το κακόβουλο λογισμικό διευκολύνεται η τέλεση συμβατικών εγκλημάτων ενισχύοντας τη συχνότητά τους και το καταστροφικό τους έργο. Αυτά τα εγκλήματα γίνονται και εξιχνιάζονται με ή και χωρίς την υποστήριξη της ψηφιακής τεχνολογίας. Αυτού του τύπου η ηλεκτρονική παραβατικότητα συμπεριλαμβάνει εγκλήματα που σχετίζονται με τους ηλεκτρονικούς υπολογιστές, το περιεχόμενο και τα πνευματικά δικαιώματα, την κατασκοπεία και την υποκλοπή σε τηλεφωνικές συνομιλίες με την παραβίαση του απορρήτου της επικοινωνίας.[41]

Ταυτόχρονα ανάλογα με τον τόπο στον οποίο εκτελούνται τα ηλεκτρονικά εγκλήματα διακρίνονται σε εγκλήματα που έχουν διαπραχθεί σε κοινό τόπο, δηλαδή

εγκλήματα που έχουν πραγματοποιηθεί σε ένα συμβατικό ηλεκτρονικό περιβάλλον, με παραδείγματα τέτοιων να αποτελούν η αποστολή ενός μηνύματος ηλεκτρονικού ταχυδρομείου προσβλητικό ή δυσφημιστικό υλικό, η μεταφορά πνευματικού δικαιώματος όπως η αντιγραφή κινηματογραφικής ταινίας ή ενός τραγουδιού. Αν το συγκεκριμένο έγκλημα έχει διαπραχθεί σε διαδικτυακό περιβάλλον με τη χρήση ενός ή περισσότερων ηλεκτρονικών υπολογιστών τότε θεωρείται ότι έχει σχέση με τον κυβερνοχώρο ή ότι η εκτέλεση του έγινε με τη συνδρομή του κυβερνοχώρου. Επίσης διακρίνονται σε εγκλήματα που έχουν διαπραχθεί σε περιβάλλον ηλεκτρονικών υπολογιστών τα οποία διαπράττονται μόνο σε υπολογιστές χωρίς τη συνδρομή ή τη συμμετοχή του διαδικτύου. Τέτοια παραδείγματα αποτελούν η αντιγραφή της ταινίας, ενός τραγουδιού ή ενός λογισμικού σε φορητή μονάδα αποθήκευσης δεδομένων όπως είναι ένα USB. Τέλος, είναι τα εγκλήματα που έχουν διαπραχθεί στον κυβερνοχώρο. Σε αυτά συμπεριλαμβάνονται εγκλήματα τα οποία έχουν διαπραχθεί αποκλειστικά στο διαδίκτυο και αποτελούν ειδικότερη μορφή του ηλεκτρονικού εγκλήματος. Για να πραγματοποιηθεί ένα τέτοιο έγκλημα στον κυβερνοχώρο θα πρέπει να χρησιμοποιηθεί ηλεκτρονικός υπολογιστής και να συνδέεται αυτός στο διαδίκτυο. Παραδείγματα τέτοιων εγκλημάτων περιγράφονται στα άρθρα 2 έως 10 της σύμβασης της Βουδαπέστης όπως είναι η παράνομη είσοδος ή πρόσβαση σε έναν υπολογιστή.[41]

Κεφάλαιο 2

2.1 Ασφάλεια

Όπως έχουμε ήδη αναφέρει, ένα πολύ σημαντικό κομμάτι του ηλεκτρονικού εγκλήματος βασίζεται στην ικανότητα που έχουν επιδέξιοι χάκερ να ξεπερνάνε την ασφάλεια των πληροφοριακών συστημάτων που κατέχει ο χρήστης- θύμα. Η εισβολή αυτή μπορεί να επιτευχθεί με ποικίλους τρόπους, συνηθέστερος αυτών όντας η χρήση κάποιου κακόβουλου λογισμικού. Μπορούμε να καταλάβουμε με αυτό τον τρόπο την πολύ μεγάλη αναγκαιότητα που υπάρχει να προστατεύουμε την ιδιωτικότητα των προσωπικών μας συσκευών και δεδομένων.

Με τον όρο ασφάλεια των πληροφοριακών συστημάτων ή ασφάλεια υπολογιστών, αναφερόμαστε στον κλάδο της επιστήμης της πληροφορικής που έχει ως κύριο σκοπό την προστασία των υπολογιστών, των δεδομένων σε αυτά τα συστήματα και των δικτύων που τους συνδέουν, αποτρέποντας τη μη εξουσιοδοτημένη χρήση ή πρόσβαση τους (υποκλοπή). Ακόμα ως προστασία των πληροφοριακών συστημάτων θεωρούμε και την βεβαίωση πως δεν υπάρχει εσφαλμένη χρήση των υπηρεσιών που αυτά παρέχουν.

Στην τρέχουσα εποχή αυτός ο κλάδος της επιστήμης αποκτά όλο και μεγαλύτερη υπόσταση και αξία στον κόσμο του διαδικτύου λόγω της αυξημένης εξάρτησης από τα συστήματα υπολογιστών, της συνεχούς εξέλιξης του Internet, όλων των τεχνολογιών-προτύπων που επιτρέπουν την απομακρυσμένη ασύρματη σύνδεση δικτύου όπως Wi-Fi και Bluetooth. Καθώς και της ίδιας της εξέλιξης στις ικανότητες μιας έξυπνης συσκευής (tablet, smartTV) που αποτελούν το «Διαδίκτυο των Πραγμάτων» (IoT-InternetofThings)[11]

2.1.1 Βασικές Αρχές Ασφαλείας

Μπορούμε να μαζέψουμε την ουσία της ασφάλειας συστημάτων και να την κατατάξουμε στις τρεις βασικές αρχές στις οποίες βασίζεται και οι οποίες είναι απαραίτητες για την σωστή λειτουργία των υπολογιστικών συστημάτων. Αυτές είναι η ακεραιότητα, η εμπιστευτικότητα και η διαθεσιμότητα.

Ακεραιότητα (Integrity): Με τον όρο «ακεραιότητα» χαρακτηρίζουμε την ανάγκη του συστήματος μας να είναι άτρωτο σε μη εξουσιοδοτημένες προσβάσεις και εισβολείς που έχουν ως σκοπό την χρήσης των υπολογιστών και δικτύων του συστήματος από άτομα χωρίς άδεια. Επιπλέον μέσα στον όρο αυτό συμπεριλαμβάνεται και η διατήρηση των δεδομένων μιας έξυπνης συσκευής σε μια γνωστή κατάσταση χωρίς ανεπιθύμητες τροποποιήσεις, αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα.

Εμπιστευτικότητα (Confidentiality): Η έννοια της εμπιστευτικότητας αναφέρεται στις ευαίσθητες πληροφορίες οι οποίες δεν θα πρέπει να είναι προσβάσιμες από άτομα χωρίς την κατάλληλη εξουσιοδότηση. Αυτή η βασική αρχή ασφάλειας μπορεί να παρακαμφθεί όχι μόνο μέσω ψηφιακών μέσων, αλλά και με την φυσική κλοπή κάποιας φορητής έξυπνης συσκευής η οποία περιέχει προσωπικές και ευαίσθητες πληροφορίες του εκάστοτε χρήστη.

Διαθεσιμότητα (Availability): Ως διαθεσιμότητα δεδομένων και υπολογιστικών πόρων ή πληροφοριών ορίζεται η ικανότητα άμεσης παροχής του δικτύου και των δεδομένων που αυτό περιέχει στους χρήστες οι οποίοι αιτούνται την χρήση αυτών. Στην περίπτωση απώλειας πληροφοριών του δικτύου μπορούμε να έχουμε άμεση ανατροφοδότηση των πληροφοριών αυτών δεδομένου της ύπαρξης και συντήρησης εφεδρικών αντιγράφων. Πιο κατανοητή μπορεί να γίνει η έννοια της διαθεσιμότητας με την παράθεση κάποιων παραδειγμάτων επίθεσης, όπως είναι για παράδειγμα η άρνηση υπηρεσιών (DOSattack), ως DOSattack ορίζονται γενικά «οι επιθέσεις εναντίον ενός υπολογιστή, ή μιας υπηρεσίας που παρέχεται, οι οποίες έχουν ως σκοπό να καταστήσουν τον υπολογιστή ή την υπηρεσία ανίκανη να δεχτεί άλλες συνδέσεις και έτσι να μην μπορεί να εξυπηρετήσει άλλους πιθανούς πελάτες». Ένας τρόπος επίτευξης αυτής της επίθεσης είναι την μέθοδο Slashdot, όπου μια ιστοσελίδα με χαμηλή κίνηση και χαμηλό όριο φόρτου εργασίας συνδέεται με κάποια ιστοσελίδα στην οποία υπάρχει μεγάλο πλήθος χρηστών με συνέπεια αυτοί να υπερφορτώσουν τη σύνδεση της αναφερομένης ιστοσελίδας με αποτέλεσμα να επιβραδύνουν σε σημαντικό βαθμό όλες τις συνδέσεις ή στην χειρότερη περίπτωση να θέσουν την ιστοσελίδα σε μια προσωρινή κατάσταση αδράνειας. [42]

Εικόνα 12 : Βασικά στοιχεία ασφαλείας

2.1.2 Μέθοδοι Ασφαλείας – Μέτρα Ασφαλείας

Υπάρχουν τέσσερις βασικές κατηγορίες μεθόδων ασφαλείας – προστασίας που βασίζονται στις βασικές αρχές. Μέσω αυτών μπορούμε να εντοπίσουμε κινδύνους στο σύστημα μας και να διασφαλίσουμε την φυσιολογική λειτουργία του.

Οι τέσσερις κατηγορίες χωρίζονται ως εξής:

Πρόληψη: Γενικά μέτρα και μηχανισμοί προστασίας που έχουν ως σκοπό να μειώσουν τους εξωτερικούς κινδύνους που μπορούν να επηρεάσουν το σύστημα μας.

Διασφάλιση: Εργαλεία, έλεγχοι και στρατηγικές που διασφαλίζουν την συνεχή αποτελεσματικότητα των εν ενεργεία δικλείδων ασφαλείας.

Ανίχνευση: Προγράμματα και τεχνικές αντιμετώπισης εισβολών. Που έχουν ως σκοπό τον εντοπισμό, και την αντιμετώπιση περιστατικών παραβίασης ασφαλείας.

Επαναφορά: Η διαδικασία που ακολουθείτε προκειμένου το σύστημα μας να επαναφέρει τον εαυτό του σε μια παρελθοντική ασφαλή κατάσταση (safestate), δηλαδή σε μια κατάσταση όπου όλες οι παράμετροι λειτουργούν κανονικά και δεν υπάρχει η υποψία κάποιας παραβίασης. [43]

Προκειμένου να εξασφαλιστεί η σωστή λειτουργία τις άνωθεν μεθόδους ασφαλείας είναι βασικό να διατηρούμε τις τελευταίες ενημερώσεις για τις εν λόγω λειτουργίες που έχουν ως σκοπό την διασφάλιση της κανονικής λειτουργίας του συστήματος. Ακόμα θα πρέπει να υπάρχουν σχέδια έκτακτης ανάγκης, τα οποία είναι εξουσιοδοτημένα για σημαντικές λειτουργίες όπως η «ανάκαμψη από καταστροφή» (disaster recovery plan), καθώς και το πλάνο «αποκατάστασης λειτουργίας» (contingency action plan). Επιπλέον μέτρα περιλαμβάνουν:

Διαχωρισμός του δικτύου

Ένα βασικό μέρος της ασφάλειας δικτύου είναι η διαίρεση του σε ζώνες βάσει των απαιτήσεων ασφαλείας. Αυτό μπορεί να γίνει χρησιμοποιώντας υποδίκτυα στο ίδιο δίκτυο ή δημιουργώντας εικονικά τοπικά δίκτυα (VLAN), καθένα από τα οποία συμπεριφέρεται σαν ένα ολοκληρωμένο ξεχωριστό δίκτυο. Η τμηματοποίηση περιορίζει τον πιθανό αντίκτυπο μιας επίθεσης σε μία ζώνη και απαιτεί από τους εισβολείς να λάβουν ειδικά μέτρα για να διεισδύσουν και να αποκτήσουν πρόσβαση σε άλλες ζώνες δικτύου.

Ρύθμιση της πρόσβασης στο Διαδίκτυο μέσω διακομιστή μεσολάβησης

Δεν πρέπει να επιτρέπεται στους χρήστες του δικτύου να έχουν πρόσβαση στο Internet χωρίς έλεγχο. Όλα τα αιτήματα θα πρέπει να περνούν από έλεγχο μέσω ενός διαφανούς διακομιστή μεσολάβησης και να χρησιμοποιούνται για τον έλεγχο και την παρακολούθηση της συμπεριφοράς των χρηστών. Είναι σημαντικό να υπάρχει βεβαίωση ότι οι εξερχόμενες συνδέσεις πραγματοποιούνται πραγματικά από άνθρωπο και όχι από bot ή άλλο αυτοματοποιημένο μηχανισμό. Επιτρέπεται η πρόσβαση σε τομείς που επιτρέπουν στους εταιρικούς χρήστες να έχουν πρόσβαση μόνο σε ιστότοπους που έχουν εγκριθεί ρητά.

Σωστή τοποθέτηση των συσκευών ασφαλείας

Θα πρέπει να τοποθετείται σωστά ένα τείχος προστασίας σε κάθε διασταύρωση των ζωνών δικτύου, όχι μόνο στην άκρη του δικτύου. Εάν δεν είναι δυνατή η πλήρης ανάπτυξη τειχών προστασίας παντού, θα πρέπει να χρησιμοποιείται η ενσωματωμένη λειτουργία τείχους προστασίας των διακοπτών και των δρομολογητών. Επίσης θα πρέπει να αναπτύσσονται συσκευές anti-DDoS ή υπηρεσίες cloud του δικτύου. Πρέπει προσεκτικά να τοποθετούνται στρατηγικές συσκευές, όπως εξισορροπητές φορτίων.

Χρήση Μετάφρασης Διεύθυνσης Δικτύου

Η Μετάφραση Διεύθυνσης Δικτύου NAT (Network Address Translation) επιτρέπει τη μετάφραση εσωτερικών διευθύνσεων IP σε διευθύνσεις προσβάσιμες σε δημόσια δίκτυα. Μπορεί να χρησιμοποιείται για τη σύνδεση πολλών υπολογιστών στο Διαδίκτυο χρησιμοποιώντας μία μόνο διεύθυνση IP. Αυτό παρέχει ένα επιπλέον επίπεδο ασφάλειας, επειδή οποιαδήποτε εισερχόμενη ή εξερχόμενη κίνηση πρέπει να περάσει από μια συσκευή

NAT και υπάρχουν λιγότερες διευθύνσεις IP που καθιστούν δύσκολο για τους εισβολείς να κατανοήσουν σε ποιον κεντρικό υπολογιστή συνδέονται.

Παρακολούθηση της κυκλοφορίας δικτύου

Θα πρέπει να υπάρχει πλήρης ορατότητα της εισερχόμενης, εξερχόμενης και εσωτερικής κίνησης δικτύου, με τη δυνατότητα αυτόματου εντοπισμού απειλών και κατανόησης του πλαισίου και του αντίκτυπου τους. Θα πρέπει να συνδυάζονται δεδομένα από διαφορετικά εργαλεία ασφαλείας για τη λήψη μιας σαφούς εικόνας του τι συμβαίνει στο δίκτυο, αναγνωρίζοντας ότι πολλές επιθέσεις καλύπτουν πολλά συστήματα πληροφορικής, λογαριασμούς χρηστών και διανύσματα απειλών. Η επίτευξη αυτού του επιπέδου ορατότητας μπορεί να είναι δύσκολη με τα παραδοσιακά εργαλεία ασφάλειας.

Συγκεντρωτικά ακολουθούν δέκα βέλτιστες πρακτικές για την καταπολέμηση κακόβουλου λογισμικού.

1. Χρήση εργαλείων πρώτης γραμμής άμυνας που μπορούν να κλιμακωθούν, όπως πλατφόρμες ασφάλειας cloud
2. Συμμόρφωση με πολιτικές και πρακτικές για επιδιόρθωση εφαρμογών, συστήματος και συσκευών
3. Χρησιμοποίηση τμηματοποίησης δικτύου για τη μείωση των εκθέσεων εστιών
4. Υιοθέτηση εργαλείων παρακολούθησης διαδικασίας επόμενης γενιάς
5. Πρόσβαση σε έγκαιρα, ακριβή δεδομένα και διαδικασίες πληροφοριών σχετικά με την απειλή που επιτρέπουν την ενσωμάτωση αυτών των δεδομένων στην παρακολούθηση και την εκδήλωση ασφάλειας
6. Απόδοση βαθύτερων και πιο προηγμένων αναλυτικών στοιχείων
7. Επανεξέταση και εφαρμογή διαδικασιών απόκρισης ασφαλείας
8. Συστηματική δημιουργία αντιγράφων ασφαλείας δεδομένων και δοκιμές διαδικασιών αποκατάστασης - διαδικασίες που είναι κρίσιμες σε έναν κόσμο ταχέων, δικτυακών σκουληκιών ransomware που βασίζονται σε δίκτυο και καταστροφικών όπλων στον κυβερνοχώρο
9. Διεξαγωγή σάρωσης ασφαλείας
10. Επανεξέταση συστημάτων ασφαλείας και διερεύνηση της χρήσης αναλυτικών στοιχείων SSL και, εάν είναι δυνατόν, αποκρυπτογράφησης SSL[47]

2.2 Απειλές για Έξυπνες Συσκευές

Οι ιοί, τα worms, τα Trojans και τα bots αποτελούν μέρος μιας κατηγορίας λογισμικού που ονομάζεται "κακόβουλο λογισμικό". Το κακόβουλο λογισμικό είναι, επίσης γνωστό ως κακόβουλος κώδικας. Είναι κώδικας ή λογισμικό που έχει σχεδιαστεί ειδικά για να προκαλέσει ζημιά, να διακόψει, να κλέψει ή γενικά να προκαλέσει κάποια άλλη «κακή» ή παράνομη ενέργεια σε δεδομένα, κεντρικούς υπολογιστές ή δίκτυα.

Υπάρχουν πολλές διαφορετικές κατηγορίες κακόβουλου λογισμικού που έχουν διαφορετικούς τρόπους μόλυνσης συστημάτων και διάδοσης. Το κακόβουλο λογισμικό μπορεί να μολύνει τα συστήματα συνδυαζόμενα με άλλα προγράμματα ή προσαρτημένα ως μακροεντολές σε αρχεία. Άλλα εγκαθίστανται εκμεταλλευόμενα μια γνωστή ευπάθεια σε ένα λειτουργικό σύστημα, μια συσκευή δικτύου ή άλλο λογισμικό, όπως μια τρύπα σε ένα πρόγραμμα περιήγησης που το μόνο που απαιτεί από τους χρήστες είναι απλά να επισκέπτονται έναν ιστότοπο για να μολύνουν τους υπολογιστές τους. Η συντριπτική πλειοψηφία, ωστόσο, εγκαθίσταται από κάποια ενέργεια από έναν χρήστη, όπως κάνοντας κλικ σε ένα συνημμένο email ή λήψη ενός αρχείου από το Διαδίκτυο.

Μερικοί από τους πιο γνωστούς τύπους κακόβουλου λογισμικού είναι ιοί, τα worms, οι Trojans, τα bots, το ransomware, οι backdoors, το spyware και το adware. Η ζημιά από κακόβουλο λογισμικό ποικίλλει από την πρόκληση μικρού ερεθισμού (όπως αναδυόμενες διαφημίσεις προγράμματος περιήγησης), την κλοπή εμπιστευτικών πληροφοριών ή χρημάτων, την καταστροφή δεδομένων και την παραβίαση ή / και την απενεργοποίηση των συστημάτων και δικτύων.[44]

Εκτός από την καταστροφή δεδομένων και λογισμικού που βρίσκονται σε εξοπλισμό, το κακόβουλο λογισμικό έχει εξελιχθεί για να στοχεύσει το φυσικό υλικό αυτών των συστημάτων. Το κακόβουλο λογισμικό δεν πρέπει επίσης να συγχέεται με το ελαττωματικό λογισμικό.

Κατηγορίες απειλών - Κακόβουλου λογισμικού

Δύο από τους πιο συνηθισμένους τύπους κακόβουλου λογισμικού είναι οι ιοί και τα worms. Αυτοί οι τύποι προγραμμάτων είναι σε θέση να αυτό-αντιγράφονται και μπορούν να

διαδώσουν αντίγραφα από μόνα τους, τα οποία μπορεί ακόμη και να είναι τροποποιημένα αντίγραφα. Για να ταξινομηθεί ως ιός ή σκουλήκι, το κακόβουλο λογισμικό πρέπει να έχει τη δυνατότητα διάδοσης. Η διαφορά είναι ότι ένα worm λειτουργεί περισσότερο ανεξάρτητα από άλλα αρχεία, ενώ ένας ιός εξαρτάται από ένα πρόγραμμα υποδοχής για να εξαπλωθεί. Αυτές και άλλες κατηγορίες κακόβουλου λογισμικού περιγράφονται παρακάτω.

Ransomware

Το Ransomware είναι ένας τύπος κακόβουλου λογισμικού που απειλεί να δημοσιεύσει τα δεδομένα του θύματος ή να αποκλείσει διαρκώς την πρόσβαση σε αυτό, εκτός εάν καταβληθεί χρηματικό ποσό. Ενώ μερικά ransomware απλά ενδέχεται να κλειδώσουν το σύστημα με τρόπο που δεν είναι δύσκολο για έναν έμπειρο άτομο να αντιστρέψει. Το κακόβουλο λογισμικό κλειδώνει τα αρχεία του μολυσμένου χρήστη καθώς χρησιμοποιεί μια τεχνική που ονομάζεται κρυπτοϊική εκβίαση, η οποία κρυπτογραφεί όλα τα αρχεία του θύματος, καθιστώντας τα απρόσιτα και απαιτεί πληρωμή λύτρων για να τα αποκρυπτογραφήσει. [45]

Ιοί

Ο ιός του υπολογιστή είναι ένας τύπος κακόβουλου λογισμικού που διαδίδεται εισάγοντας ένα αντίγραφο του εαυτού του και γίνεται μέρος ενός άλλου προγράμματος. Απλώνεται από τον έναν υπολογιστή στον άλλο, αφήνοντας λοιμώξεις καθώς ταξιδεύει. Οι ιοί μπορεί να κυμαίνονται σε σοβαρότητα από την πρόκληση ελαφρώς ενοχλητικών αποτελεσμάτων έως την καταστροφή δεδομένων ή λογισμικού και την πρόκληση συνθηκών άρνησης υπηρεσίας (DoS). Σχεδόν όλοι οι ιοί είναι συνδεδεμένοι σε ένα εκτελέσιμο αρχείο, που σημαίνει ότι ο ιός μπορεί να υπάρχει σε ένα σύστημα, αλλά δεν θα είναι ενεργός ή δεν μπορεί να εξαπλωθεί έως ότου ένας χρήστης εκτελέσει ή ανοίξει το κακόβουλο αρχείο ή πρόγραμμα. Όταν εκτελείται ο κεντρικός κώδικας, εκτελείται επίσης ο κώδικας του ιού. Κανονικά, το πρόγραμμα υποδοχής συνεχίζει να λειτουργεί αφού μολυνθεί από τον ιό. Ωστόσο, ορισμένοι ιοί αντικαθιστούν άλλα προγράμματα με αντίγραφα τους. Οι ιοί εξαπλώνονται όταν το λογισμικό ή το έγγραφο στο οποίο συνδέονται μεταφέρεται από έναν υπολογιστή σε έναν άλλο χρησιμοποιώντας το δίκτυο, έναν δίσκο, μια κοινή χρήση αρχείων ή μολυσμένα συνημμένα email.[27]

Σκουλήκια

Τα υπολογιστικά σκουλήκια είναι παρόμοια με ιούς, καθώς αναπαράγουν λειτουργικά αντίγραφα και μπορούν να προκαλέσουν τον ίδιο τύπο ζημιάς. Σε αντίθεση με τους ιούς, οι οποίοι απαιτούν την εξάπλωση ενός μολυσμένου αρχείου κεντρικού υπολογιστή, τα worms είναι αυτόνομο λογισμικό και δεν απαιτούν πρόγραμμα υποδοχής ή ανθρώπινη βοήθεια για τη διάδοση. Για να εξαπλωθούν, τα worms είτε εκμεταλλεύονται μια ευπάθεια στο σύστημα προορισμού είτε χρησιμοποιούν κάποιο είδος κοινωνικής μηχανικής για να εξαπατήσουν τους χρήστες να τα εκτελέσουν. Ένα worm που εισέρχεται στο σύστημα εκμεταλλεύεται τις δυνατότητες μεταφοράς αρχείων ή μεταφοράς πληροφοριών στο σύστημα, επιτρέποντάς του να ταξιδεύει χωρίς βοήθεια. Τα πιο προηγμένα worms αξιοποιούν κρυπτογράφηση και τεχνολογίες ransomware για να βλάψουν τους στόχους τους.[24]

Δούρειος ίππος

Το Trojan είναι ένας άλλος τύπος κακόβουλου λογισμικού που πήρε το όνομά του από το ξύλινο άλογο που οι Έλληνες χρησιμοποιούσαν για να διεισδύσουν στην Τροία. Είναι ένα επιβλαβές λογισμικό που φαίνεται νόμιμο. Οι χρήστες συνήθως ξεγελιούνται για να το φορτώσουν και να το εκτελέσουν στα συστήματά τους. Μετά την ενεργοποίησή του, μπορεί να επιτύχει οποιονδήποτε αριθμό επιθέσεων στον κεντρικό υπολογιστή, από ενόχληση του χρήστη (αναδυόμενα παράθυρα ή αλλαγή επιτραπέζιων υπολογιστών) έως καταστροφή του κεντρικού υπολογιστή (διαγραφή αρχείων, κλοπή δεδομένων ή ενεργοποίηση και διάδοση άλλων κακόβουλων προγραμμάτων, όπως ιοί). Είναι επίσης γνωστοί ότι δημιουργούν backdoors για να παρέχουν στους κακόβουλους χρήστες πρόσβαση στο σύστημα. Σε αντίθεση με τους ιούς και τους ιούς τύπου worm, οι Trojans δεν αναπαράγονται μολύνοντας άλλα αρχεία ούτε αυτό-αναπαράγονται. Οι Trojans πρέπει να εξαπλωθούν μέσω της αλληλεπίδρασης των χρηστών, όπως το άνοιγμα ενός συνημμένου email ή η λήψη και η εκτέλεση ενός αρχείου από το Διαδίκτυο.[46]

Bots

Το "Bot" προέλευση της λέξης “robot” και είναι μια αυτοματοποιημένη διαδικασία που αλληλοεπιδρά με άλλες υπηρεσίες δικτύου. Τα Bots αυτοματοποιούν συχνά εργασίες και παρέχουν πληροφορίες ή υπηρεσίες που διαφορετικά θα διεξάγονταν από έναν

άνθρωπο. Μια τυπική χρήση των bots είναι η συλλογή πληροφοριών, όπως τα προγράμματα ανίχνευσης ιστού ή η αυτόματη αλληλεπίδραση με Instant Messaging (IM) , Internet Relay Chat (IRC) ή άλλες διεπαφές ιστού. Μπορούν επίσης να χρησιμοποιηθούν για να αλληλεπιδρούν δυναμικά με ιστότοπους.[47] Τα bots μπορούν να χρησιμοποιηθούν είτε για καλή ή κακόβουλη πρόθεση. Ένα κακόβουλο bot, είναι αυτόνομο κακόβουλο λογισμικό που έχει σχεδιαστεί για να μολύνει έναν κεντρικό υπολογιστή και να επιστρέφει σε έναν κεντρικό διακομιστή ή διακομιστές που λειτουργούν ως κέντρο εντολών και ελέγχου για ένα ολόκληρο δίκτυο παραβιασμένων συσκευών ή "botnet". Με ένα botnet, οι εισβολείς μπορούν να ξεκινήσουν ευρείας βάσης, "τηλεχειριστήριο", επιθέσεις εναντίον των στόχων τους. Εκτός από την ικανότητα που μοιάζει με σκουλήκι και μπορεί να αυτο-πολλαπλασιαστεί, τα bots μπορούν να περιλαμβάνουν τη δυνατότητα καταγραφής πληκτρολογίων, συλλογής κωδικών πρόσβασης, λήψης και ανάλυσης πακέτων, συλλογή οικονομικών πληροφοριών, εκκίνηση επιθέσεων Denial of Service (DOS) και αναμετάδοσης spam. Τα bots έχουν όλα τα πλεονεκτήματα των worm, αλλά είναι γενικά πολύ πιο ευπροσάρμοστα στον φορέα μόλυνσης και συχνά τροποποιούνται εντός ωρών από τη δημοσίευση ενός νέου exploit (ρήγματος στη ζώνη προστασίας της ασφάλειας). Είναι γνωστό επίσης ότι εκμεταλλεύονται ανοιχτούς χώρους που έχουν δημιουργηθεί από σκουλήκια και ιούς. Τα bots σπάνια ανακοινώνουν την παρουσία τους με υψηλούς ρυθμούς σάρωσης που καταστρέφουν την υποδομή του δικτύου. Αντίθετα, μολύνουν δίκτυα με τρόπο που ξεφεύγει από την άμεση ειδοποίηση.

Τα προηγμένα botnets ενδέχεται να επωφεληθούν από κοινές συσκευές διαδικτύου πραγμάτων (IOT), όπως οικιακά ηλεκτρονικά αντικείμενα και συσκευές για την αύξηση των αυτοματοποιημένων επιθέσεων. Η εξόρυξη κρυπτογράφησης είναι μια κοινή χρήση αυτών των bots για κακόβουλους σκοπούς.

Κανάλια διανομής για κακόβουλο λογισμικό

Το προηγμένο κακόβουλο λογισμικό έρχεται συνήθως μέσω των ακόλουθων καναλιών διανομής σε υπολογιστή ή δίκτυο:

- Λήψη Drive-by — Αθέλητη λήψη λογισμικού υπολογιστή από το Διαδίκτυο
- Ανεπιθύμητο email - Ανεπιθύμητα συνημμένα ή ενσωματωμένοι σύνδεσμοι σε ηλεκτρονικό ταχυδρομείο
- Φυσικά μέσα — (Π.χ. USB)

- Αυτοδιάδοση - Ικανότητα κακόβουλου λογισμικού να μετακινείται από υπολογιστή σε υπολογιστή ή δίκτυο σε δίκτυο μέσω συστημάτων που βρίσκονται μέσα στον προγραμματισμό του.

Στη συνέχεια παραθέτονται διάφορες κατηγορίες περιπτώσεων κακόβουλων λογισμικών, βάση του τελικού αποτελέσματος που θέλουν να πετύχουν αλλά και του τρόπου που λειτουργούν:

Adware

Λογισμικό που δημιουργεί έσοδα για τον προγραμματιστή του δημιουργώντας αυτόματα διαδικτυακές διαφημίσεις στη διεπαφή χρήστη του λογισμικού ή σε οθόνη που παρουσιάζεται στον χρήστη κατά τη διαδικασία εγκατάστασης. Το λογισμικό μπορεί να αποφέρει δύο τύπους εσόδων: το ένα είναι για την προβολή της διαφήμισης και ένα άλλο με βάση την "πληρωμή ανά κλικ" εάν ο χρήστης κάνει κλικ στη διαφήμιση.

Backdoors

Ένας μη τεκμηριωμένος τρόπος πρόσβασης σε ένα σύστημα, παρακάμπτοντας τους κανονικούς μηχανισμούς ελέγχου ταυτότητας. Ορισμένα backdoors τοποθετούνται στο λογισμικό από τον αρχικό προγραμματιστή και άλλα τοποθετούνται σε συστήματα μέσω ενός συμβιβασμού συστήματος, όπως ένας ιός ή ένα worm. Συνήθως, οι επιτιθέμενοι χρησιμοποιούν backdoors για ευκολότερη και συνεχή πρόσβαση σε ένα σύστημα αφού έχει παραβιαστεί.

Bootkit

Μια παραλλαγή κακόβουλου λογισμικού που τροποποιεί τους τομείς εκκίνησης ενός σκληρού δίσκου, όπως το Master Boot Record (MBR) και το Volume Boot Record (VBR). Οι εχθροί μπορούν να χρησιμοποιήσουν πακέτα εκκίνησης για να παραμείνουν σε συστήματα σε ένα επίπεδο κάτω από το λειτουργικό σύστημα, κάτι που μπορεί να δυσκολεύει την πλήρη αποκατάσταση του συστήματος σε μια ασφαλή κατάσταση.

Browser Hijacker

Λογισμικό που τροποποιεί τις ρυθμίσεις ενός προγράμματος περιήγησης ιστού χωρίς την άδεια ενός χρήστη, ώστε να εισάγει ανεπιθύμητες διαφημίσεις στο πρόγραμμα

περιήγησης του χρήστη. Ένας Hijacker προγράμματος περιήγησης μπορεί να αντικαταστήσει την υπάρχουσα αρχική σελίδα, τη σελίδα σφάλματος ή τη μηχανή αναζήτησης με τη δική του. Αυτή η χρήση γίνεται γενικά για την επιβολή επισκέψεων σε έναν συγκεκριμένο ιστότοπο, αυξάνοντας τα έσοδα από διαφημίσεις. Αυτό το λογισμικό έρχεται συχνά με τη μορφή γραμμής εργαλείων του προγράμματος περιήγησης και λαμβάνεται μέσω συνημμένου email ή λήψης αρχείου.

Crimeware

Μια κατηγορία κακόβουλου λογισμικού ειδικά σχεδιασμένη για την αυτοματοποίηση του εγκλήματος στον κυβερνοχώρο. Το Crimeware (διαφορετικό από το spyware και το adware) έχει σχεδιαστεί για να διαπράττει κλοπή ταυτότητας μέσω κοινωνικής μηχανικής ή τεχνικής μυστικότητας, προκειμένου να έχει πρόσβαση στους οικονομικούς και λιανικούς λογαριασμούς ενός χρήστη υπολογιστή με σκοπό τη λήψη χρημάτων από αυτούς τους λογαριασμούς ή την ολοκλήρωση μη εξουσιοδοτημένων συναλλαγών που εμπλουτίζουν τον κυβερνοχώρο. Εναλλακτικά, το crimeware μπορεί να κλέψει εμπιστευτικές ή ευαίσθητες εταιρικές πληροφορίες.

Exploit

Ένα κομμάτι λογισμικού, μια εντολή ή μια μεθοδολογία που επιτίθεται σε μια συγκεκριμένη αδυναμία ασφαλείας. Οι εκμεταλλεύσεις δεν είναι πάντα κακόβουλες στην πρόθεση - μερικές φορές χρησιμοποιούνται μόνο ως τρόπος απόδειξης ότι υπάρχει αδυναμία. Ωστόσο, είναι ένα κοινό συστατικό του κακόβουλου λογισμικού.

Keyloggers

Η ενέργεια της καταγραφής των πλήκτρων που "χτυπήθηκαν" σε ένα πληκτρολόγιο, συνήθως κρυφά, έτσι ώστε το άτομο που χρησιμοποιεί το πληκτρολόγιο να μην γνωρίζει ότι οι ενέργειές του παρακολουθούνται. Στη συνέχεια, τα δεδομένα μπορούν να ανακτηθούν από το άτομο που χειρίζεται το πρόγραμμα καταγραφής. Ένα keylogger μπορεί να είναι είτε λογισμικό είτε υλικό.

Κακόβουλα Crypto Miners

Λογισμικό που χρησιμοποιεί πόρους συστήματος για την επίλυση μεγάλων μαθηματικών υπολογισμών που έχουν ως αποτέλεσμα την απόδοση ορισμένου ποσού κρυπτογράφησης στους λύτες. Το λογισμικό εξόρυξης βασίζεται τόσο στους πόρους της CPU όσο και στην ηλεκτρική ενέργεια. Μόλις ένα σύστημα ρίξει έναν miner σε αυτό και ξεκινά την εξόρυξη, δεν χρειάζεται τίποτα άλλο. Ο miner δημιουργεί έσοδα με συνέπεια μέχρι να αφαιρεθεί. Πρακτικά είναι η χρήση ξένων μονάδων επεξεργαστών, από συσκευές που έχουν μολυνθεί, για την παραγωγή κρυπτονομισμάτων που επιστρέφουν στην κατοχή του δημιουργού του λογισμικού.

Κακόβουλο λογισμικό σημείου πώλησης (POS)

Ένας τύπος κακόβουλου λογισμικού που χρησιμοποιείται από εγκληματίες του κυβερνοχώρου για να στοχεύσει στα τερματικά σημείου πώλησης (POS) με σκοπό την απόκτηση πληροφοριών πιστωτικής κάρτας και χρεωστικής κάρτας διαβάζοντας τη μνήμη της συσκευής από το σύστημα πωλήσεων λιανικής πώλησης. Το κακόβουλο λογισμικό POS κυκλοφορεί από τους χάκερ για την επεξεργασία και την κλοπή δεδομένων πληρωμής συναλλαγών. Τα στοιχεία της κάρτας, καταγράφονται, υποκλέπτονται και στέλνονται στον εγκληματία στον κυβερνοχώρο.

Wipers

Ένας τύπος καταστροφικού κακόβουλου λογισμικού που περιέχει έναν μηχανισμό διαγραφής δίσκων, όπως η ικανότητα να μολύνει την κύρια εγγραφή εκκίνησης με ένα ωφέλιμο φορτίο που κρυπτογραφεί τον εσωτερικό πίνακα αρχείων. Οι wipers καθιστούν τη διαδικασία επίθεσης ή το στοιχείο άχρηστο στον τελικό χρήστη.

Root kit

Προγράμματα που αποκρύπτουν την ύπαρξη κακόβουλου λογισμικού παρεμποδίζοντας και τροποποιώντας κλήσεις API (Application Programming Interface) λειτουργικού συστήματος που παρέχουν πληροφορίες συστήματος. Η λειτουργία ενεργοποίησης Rootkits ή rootkit ενδέχεται να βρίσκεται σε επίπεδο χρήστη ή πυρήνα στο λειτουργικό σύστημα ή χαμηλότερη ώστε να περιλαμβάνει έναν επόπτη, μια κύρια εγγραφή εκκίνησης ή το υλικο λογισμικό του συστήματος. Οι αντίπαλοι χρήστες μπορούν να χρησιμοποιούν rootkit για να αποκρύψουν την παρουσία προγραμμάτων, αρχείων,

συνδέσεων δικτύου, υπηρεσιών, προγραμμάτων οδήγησης και άλλων στοιχείων του συστήματος.

Δυνητικά ανεπιθύμητα προγράμματα ή εφαρμογές

Λογισμικό που ένας χρήστης μπορεί να αντιληφθεί ως ανεπιθύμητο. Σε αυτά ενδέχεται να περιλαμβάνονται προγράμματα κατασκοπίας adware, spyware ή browser. Τέτοιο λογισμικό μπορεί να χρησιμοποιεί μια εφαρμογή που μπορεί να θέσει σε κίνδυνο το απόρρητο ή να αποδυναμώσει την ασφάλεια της μολυσμένης συσκευής. Οι εταιρείες συχνά συνδυάζουν μια επιθυμητή λήψη προγράμματος με μια εφαρμογή "περιτυλίγματος" η οποία συνήθως προτείνεται προς εγκατάσταση μαζί με το αρχικό πρόγραμμα. Με αυτό τον τρόπο γίνεται πιο εύκολο να εγκαταστήσουν μια ανεπιθύμητη εφαρμογή, σε ορισμένες περιπτώσεις χωρίς να παρέχουν μια σαφή μέθοδο εξαίρεσης επιλογής της εν λόγω εφαρμογής.

Λογισμικό υποκλοπής

Λογισμικό που στοχεύει στη συλλογή πληροφοριών σχετικά με ένα άτομο ή έναν οργανισμό χωρίς να το γνωρίζει, το οποίο μπορεί να στείλει τέτοιες πληροφορίες σε άλλη οντότητα χωρίς τη συγκατάθεση του καταναλωτή ή που ισχυρίζεται ότι ελέγχει μια συσκευή χωρίς να το γνωρίζει ο καταναλωτής.

Ανιχνευτές ιστού

Προγράμματα που περιηγούνται συστηματικά στο Διαδίκτυο και ευρετήριο δεδομένων, συμπεριλαμβανομένου περιεχομένου σελίδας και συνδέσμων. Αυτά τα προγράμματα ανίχνευσης ιστού βοηθούν στην επικύρωση κώδικα HTML και ερωτημάτων μηχανών αναζήτησης για τον εντοπισμό νέων ιστοσελίδων ή νεκρών συνδέσμων. [48],[49],[50],[51],[52]

2.3 Flash Player Trojan Scam

'Οπως αναφέραμε στην αρχή οι νέες γενιές έξυπνων κινητών και τάμπλετ έχουν φτάσει σε πολύ υψηλά επίπεδα, ξεπερνώντας σε υπολογιστικές ικανότητες και σε αξία υλικού υπολογιστές παλαιότερων γενεών. Πολλά από τα κακόβουλα λογισμικά που αναφέρονται σε αυτή την πτυχιακή έχουν το σκοπό να διεισδύσουν στις έξυπνες συσκευές της γενιάς μας, ανεξαρτήτως εάν αυτές είναι ένα λάπτοπ, ένα κινητό τηλέφωνο, ένα ρούτερ, ένα τάμπλετ, οτιδήποτε έχει την ικανότητα να συνδεθεί στο διαδίκτυο διατρέχει τον κίνδυνο μόλυνσης από λογισμικό που έχει φτιαχτεί για το σκοπό αυτό. 'Ενα ηλεκτρονικό μήνυμα που περιέχει ένα κακόβουλο λινκ ή μια SQL μολυσμένη ιστοσελίδα ή απλά αποτελεί spam καταλήγει στον ίδιο χρήστη που είχε ως στόχο ανεξάρτητα από τη συσκευή που θα χρησιμοποιήσει για να επεξεργαστεί το μήνυμα αυτό. Ένα καλοφτιαγμένο κακόβουλο λογισμικό έχει την ικανότητα να επηρεάσει την συσκευή στην οποία βρίσκεται ανεξάρτητα από το υλικό της, εάν έχει μεγάλη ή μικρή RAM πολλούς ή λίγους πυρήνες.

Όμως αυτό δεν σημαίνει ότι δεν υπάρχουν εξατομικευμένα κακόβουλα λογισμικά που είναι φτιαγμένα κατά κύριο λόγο μόνο για υπολογιστές, και άλλοι μόνο για έξυπνες συσκευές που ανήκουν στην ευρύτερη κατηγορία των smartphone.

Ένα τέτοιο παράδειγμα αποτελεί ένα Trojan λογισμικό που εξαπλώνεται ως απομίμηση της εφαρμογής Flash Player ανακαλύφθηκε και μελετήθηκε από τους επιστήμονες και ερευνητές της ESET (Σλοβακικής προέλευσης εταιρεία στον τομέα της ασφάλειας). Η λειτουργία της εν λόγω εφαρμογής είχε ως εξής, έπειτα από την λήψη και της εγκατάσταση της, η εφαρμογή ζητάει πρόσβαση στα δικαιώματα διαχείρισης της συσκευής, σε μια προσπάθεια να προστατευθεί από την εύκολη απεγκατάστασή της. Στο επόμενο βήμα το κακόβουλο λογισμικό ελέγχει για την ύπαρξη συγκεκριμένων τραπεζικώς εφαρμογών και εάν αυτές είναι επίσης εγκατεστημένες στην συσκευή που βρίσκεται, εάν τις εντοπίσει, λαμβάνει ψεύτικες οθόνες σύνδεσης για κάθε τραπεζική εφαρμογή από τον command & control server. Με αυτό το τρόπο μόλις το θύμα χρησιμοποιήσει μια τραπεζική εφαρμογή, η οποία έχει γίνει στόχος από το Trojan λογισμικό, εμφανίζεται μία ψεύτικη οθόνη σύνδεσης πάνω από την κορυφή της νόμιμης εφαρμογής, αφήνοντας την οθόνη κλειδωμένη μέχρι το θύμα να εισάγει τα προσωπικά του στοιχεία πρόσβασης. [53]

Οι κυβερνοεγκληματίες είχαν με αυτό τον τρόπο την δυνατότητα να συνδεθούν στο λογαριασμό του θύματος από απόσταση και να μεταφέρουν χρηματικά ποσά σε προσωπικούς

τους λογαριασμούς. Ενώ είχαν επίσης τρόπο μέσω της εφαρμογής την ικανότητα να συλλέξουν όλα τα μηνύματα κειμένου SMS που έχουν ληφθεί στη μολυσμένη συσκευή, καθώς και να τα διαγράψουν.

Το κακόβουλο λογισμικό, εμφανίζεται ως Android/Spy.Agent.SI, και παρακάτω φαίνονται συναρτήσεις από τις εντολές που μπορεί να εκτελεί όσο βρίσκεται στη συσκευή.

- login user names for certain applications/services
- login passwords for certain applications/services
- device model
- IMEI number
- language settings
- SDK version
- information about the operating system and system settings
- the list of installed software
- download files from a remote computer and/or the Internet
- monitor incomming SMS messages
- send SMS messages
- delete SMS
- send gathered information

Εικόνα 13 : Το κακόβουλο λογισμικό εμφανιζόμενο ως Flash Player κατέχει δικαιώματα administrator

2.4 PIN Skimmer

Σε παρόμοια περίπτωση αλλά με ευγενικό σκοπό και σε πιο απλή μορφή ερευνητές από το Πανεπιστήμιο του Cambridge δημιούργησαν μια εφαρμογή ονόματι PIN Skimmer, θέλοντας να τραβήξει την απαραίτητη προσοχή στα θέματα ασφάλειας που υπάρχουν στα smartphones, καθώς στο ενδεχόμενο που μία συσκευή μολυνθεί με κάποιο malware ή ιό, με παρόμοιες δυνατότητες του PIN Skimmer, θα βρίσκονται σε κίνδυνο να υποκλαπεί το PIN του κινητού τηλεφώνου και στη συνέχεια όπως είδαμε παραπάνω, να εντοπιστεί το PIN που χρησιμοποιούμε στις όλες τις χρηματικές συναλλαγές.

Πως όμως λειτουργεί το λογισμικό αυτό; Βασικό ρόλο έχουν η κάμερα και το μικρόφωνο. Το μικρόφωνο για να καταγράφει τον ήχο που ακούγεται πατώντας τα νούμερα, και την κάμερα για να ανιχνεύει τις κινήσεις του προσώπου, καθώς το θύμα κοιτάει προς το κινητό κατά την εισαγωγή του PIN.

Όπως κάθε κακόβουλο λογισμικό έτσι και αυτό έπρεπε να αποκρύψει την ύπαρξη του στη συσκευή μειώνοντας την πιθανότητα να ανακαλυφθεί. Πως έγινε αυτό;

- Όλοι οι αλγόριθμοι επεξεργασίας εικόνας γινόντουσαν σε απομακρυσμένα επεξεργαστές με σκοπό να ελαχιστοποιηθεί η κατανάλωση της μπαταρίας, γεγονός που ενδεχομένως να βάλει τον χρήστη σε υποψίες. Για τον ίδιο λόγο όλα τα βίντεο και φωτογραφίες που τραβούσε το λογισμικό δεν ξεπερνούσαν τα 2.5MB φοβούμενοι την απότομη έλλειψη αποθηκευτικού χώρου της συσκευής (Σημαντικό είναι να σημειωθεί πως κατά κύριο λόγω όλες οι κακόβουλες εφαρμογές με αυτό τον τρόπο δράσης θα είχαν ως σκοπό την άμεση αποστολή των αρχείων αυτών σε μια απομακρυσμένη πλατφόρμα αφήνοντας μηδενικά αποτυπώματα στη συσκευή του χρήστη)
- Πάνω σε αυτό, ένα άλλο πρόβλημα που οι ερευνητές κλίθηκαν να λύσουν, ήταν η μεταφορά των παραπάνω αρχείων. Οι πρόσθετες χρεώσεις δικτύου είναι ένα θέμα που συνδέεται με τη μετάδοση δεδομένων. Οι περισσότεροι χρήστες smartphone χρησιμοποιούν προγράμματα για να γνωρίζουν τις χρώσεις αλλά και για να είναι σίγουροι ότι δεν θα χρησιμοποιήσουν τα δεδομένα πέρα από κάποιο συγκεκριμένο όριο. Για αυτό το λόγο, προσπαθώντας πάλι να αποκρύψει την ύπαρξη του το PIN Skimmer θα ξεκινούσε την μετάδοση των δεδομένων μόλις το κινητό συνδεόταν σε κάποιο δίκτυο WiFi.

- Επιπλέον έγινε η χρήση ενός API εκτεθειμένο από το λειτουργικό σύστημα Android για να απενεργοποιήσει το LED που ανάβει σε ορισμένες συσκευές, όταν η κάμερα είναι σε χρήση.

Μια ερώτηση που τέθηκε σε αυτή την έρευνα ήταν κατά πόσο το μήκος του κωδικού PIN, μπορεί να επηρεάσει τις πιθανότητες το κακόβουλο λογισμικό να ανακαλύψει τον κωδικό. Τα ευρήματα δείχνουν πως ένα μεγάλου μήκους PIN είναι ευκολότερο να σπάσει από ένα μικρότερο καθώς τα πιο μακροσκελή PIN έδωσαν στο πρόγραμμα περισσότερες πληροφορίες προς επεξεργασία αυξάνοντας την ακρίβειά του.

Από μια δοκιμασία με 50 τετραψήφιους κωδικούς, το PIN Skimmer βρήκε περισσότερο από το 30% των κωδικών PIN μετά από 2 προσπάθειες, και πάνω από το 50% των κωδικών μετά από 5 προσπάθειες Από ένα σύνολο 200 οκταψήφιων PINs, το πρόγραμμα των ερευνητών ανακάλυψε περίπου το 45% των κωδικών PIN μετά από 5 προσπάθειες και το 60% εξ' αυτών μετά από 10 προσπάθειες. [54][55]

2.5 Επιθέσεις στην Ασφάλεια Δικτύου

Μια επίθεση στο δίκτυο είναι μια προσπάθεια απόκτησης μη εξουσιοδοτημένης πρόσβασης στο δίκτυο ενός οργανισμού, με στόχο την κλοπή δεδομένων ή την εκτέλεση άλλων κακόβουλων δραστηριοτήτων. Υπάρχουν δύο βασικοί τύποι επιθέσεων δικτύου:

- **Παθητική:** Οι εισβολείς αποκτούν πρόσβαση σε ένα δίκτυο και μπορούν να παρακολουθούν ή να κλέβουν ευαίσθητες πληροφορίες, αλλά χωρίς να κάνουν καμία αλλαγή στα δεδομένα, αφήνοντάς τα ανέπαφα.
- **Ενεργητική:** Οι επιτιθέμενοι όχι μόνο αποκτούν μη εξουσιοδοτημένη πρόσβαση αλλά και τροποποιούν δεδομένα, είτε διαγράφοντας, κρυπτογραφώντας ή γενικότερα κάνοντάς τα άχρηστα προς χρήση.

Διακρίνονται οι επιθέσεις δικτύου από πολλούς άλλους τύπους επιθέσεων:

- **Επιθέσεις τελικού σημείου** — απόκτηση μη εξουσιοδοτημένης πρόσβασης σε συσκευές χρηστών, διακομιστές ή άλλα τελικά σημεία, που συνήθως διακυβεύονται μολύνοντάς τα με κακόβουλο λογισμικό.

- **Επιθέσεις κακόβουλου λογισμικού** — μόλυνση πόρων πληροφορικής με κακόβουλο λογισμικό, επιτρέποντας στους εισβολείς να θέσουν σε κίνδυνο συστήματα, να κλέψουν δεδομένα και να κάνουν ζημιά. Αυτές περιλαμβάνουν επίσης επιθέσεις ransomware.
- **Αδυναμίες, εκμεταλλεύσεις και επιθέσεις** - αξιοποίηση αδυναμιών σε λογισμικό που χρησιμοποιείται στον οργανισμό, για την απόκτηση μη εξουσιοδοτημένης πρόσβασης, συμβιβασμού ή σαμποτάζ.
- **Προηγμένες επίμονες απειλές** - αυτές είναι πολύπλοκες απειλές πολλαπλών επιπέδων, οι οποίες περιλαμβάνουν επιθέσεις δικτύου αλλά και άλλους τύπους επιθέσεων.[56]

Σε επιθέσεις δικτύου, οι εισβολείς επικεντρώνονται στη διείσδυση της περιμέτρου του εταιρικού δικτύου και στην πρόσβαση σε εσωτερικά συστήματα. Πολύ συχνά, οι επιτιθέμενοι θα συνδυάσουν άλλους τύπους επιθέσεων, για παράδειγμα συμβιβασμό ενός τελικού σημείου, διάδοση κακόβουλου λογισμικού ή εκμετάλλευση μιας αδυναμίας σε ένα σύστημα εντός του δικτύου.

Ακολουθούν συνηθισμένοι φορείς απειλής που μπορούν να χρησιμοποιήσουν οι εισβολείς για να διεισδύσουν στο δίκτυό.[56]

1. Μη εξουσιοδοτημένη πρόσβαση

Η μη εξουσιοδοτημένη πρόσβαση αναφέρεται σε εισβολείς που έχουν πρόσβαση σε ένα δίκτυο χωρίς να λάβουν άδεια. Μεταξύ των αιτιών των μη εξουσιοδοτημένων επιθέσεων πρόσβασης είναι οι αδύναμοι κωδικοί πρόσβασης, η έλλειψη προστασίας έναντι της κοινωνικής μηχανικής, οι λογαριασμοί που είχαν προηγουμένως παραβιαστεί και οι απειλές εσωτερικού.

2. Επιθέσεις με κατανεμημένη άρνηση υπηρεσίας (DDoS)

Οι επιτιθέμενοι δημιουργούν botnets, μεγάλους στόλους παραβιασμένων συσκευών και τα χρησιμοποιούν για να κατευθύνουν εσφαλμένη κίνηση στο δίκτυο ή τους διακομιστές. Το DDoS μπορεί να συμβεί σε επίπεδο δικτύου, για παράδειγμα στέλνοντας τεράστιους όγκους πακέτων SYN / ACC (κομμάτι " χειραψίας" τριπλής διαδρομής μεταξύ δύο συνεργατών επικοινωνίας που συχρονίζονται μεταξύ τους κατά τη διάρκεια της σύνδεσης)

που μπορούν να κατακλύσουν έναν διακομιστή ή σε επίπεδο εφαρμογής, για παράδειγμα εκτελώντας σύνθετα ερωτήματα SQL που φέρνουν μια βάση δεδομένων στα όρια της.

3. Επίθεση από man in the middle

Η επίθεση man in the midle περιλαμβάνει επιτιθέμενους που παρεμποδίζουν την κυκλοφορία, είτε μεταξύ του δικτύου και των εξωτερικών ιστότοπων είτε εντός του δικτύου. Εάν τα πρωτόκολλα επικοινωνίας δεν είναι ασφαλή ή οι εισβολείς βρουν έναν τρόπο να παρακάμψουν αυτήν την ασφάλεια, μπορούν να κλέψουν δεδομένα που μεταδίδονται, να αποκτήσουν διαπιστευτήρια χρήστη και να εισβάλουν στις συνεδρίες τους.

4. Επιθέσεις με έγχυση κώδικα και SQL

Πολλοί ιστότοποι δέχονται εισόδους χρήστη και δεν επικυρώνουν-ασφαλίζουν ικανοποιητικά αυτές τις εισόδους. Οι εισβολείς μπορούν στη συνέχεια να συμπληρώσουν μια φόρμα ή να κάνουν μια κλήση API, (Application Programming Interface) -διασύνδεση προγραμματισμού εφαρμογών- περνώντας κακόβουλο κώδικα αντί για τις αναμενόμενες τιμές δεδομένων. Ο κώδικας εκτελείται στον διακομιστή και επιτρέπει στους εισβολείς να τον θέσουν σε κίνδυνο.

5. Κλιμάκωση προνομίων

Μόλις οι εισβολείς διεισδύσουν στο δίκτυό, οι επίδοξοι χάκερ, μπορούν να χρησιμοποιήσουν την κλιμάκωση προνομίων για να επεκτείνουν την εμβέλεια τους. Η οριζόντια κλιμάκωση προνομίων περιλαμβάνει τους επιτιθέμενους να αποκτήσουν πρόσβαση σε επιπλέον, παρακείμενα συστήματα και κάθετη κλιμάκωση, που σημαίνει ότι οι εισβολείς αποκτούν υψηλότερο επίπεδο προνομίων για τα ίδια συστήματα. Έχοντας έτσι την δυνατότητα τροποποίησης του συστήματος και τον αρχείων που περιλαμβάνονται σε αυτό.

6. Απειλές εσωτερικών πληροφοριών

Ένα δίκτυο είναι ιδιαίτερα ευάλωτο σε κακόβουλα άτομα, τα οποία έχουν ήδη προνομιακή πρόσβαση σε οργανωτικά συστήματα. Οι απειλές του εσωτερικού μπορεί να είναι δύσκολο να εντοπιστούν και να προστατευθούν, επειδή οι παραβάτες δεν χρειάζεται να διεισδύσουν στο δίκτυο για να κάνουν κακό, καθώς βάση της θέσης τους έχουν ήδη

πρόσβαση σε ότι χρειάζονται αποφεύγοντας έτσι κάθε κίνδυνο και τοίχος προστασίας που θα έβρισκαν αλλιώς στο δρόμο τους. Από έρευνες προκύπτει πως σε ποσοστό κοντά στο 60% φθάνουν οι εκ των έσω επιθέσεις. Χαρακτηριστικά τέτοιων επιθέσεων και κίνητρα αυτών συχνά είναι ένας δυσαρεστημένος υπάλληλος της εταιρείας ο οποίος καταχράται τα επίπεδα εξουσιοδότησης που έχει προκειμένου να βλάψει την εταιρεία υποκλέπτει στοιχεία, ή τροποποιεί στοιχεία ή στο πλαίσιο της βιομηχανικής κατασκοπείας να διαρρέει εμπιστευτικές πληροφορίες σε αντίπαλες πλευρές οι οποίες ενδιαφέρονται στην κλοπή προτύπων κατασκευαστικών μεθόδων ή νέων καινοτομιών. Πολλές φορές κάποιο ανάλογο φαινόμενο διαρροής μπορεί να γίνει και ως αποτέλεσμα άγνοιας και κακής χρήσης υλικού από την πλευρά του χρήστη. Καταλήγουμε όμως στο γεγονός πως ενώ οι περισσότεροι επόπτες συστήματος προσπαθούν να ασφαλίσουν τα συστήματα τους από εξωτερικούς παράγοντες και απειλές, ξεχνούν να τα προστατέψουν από εσωτερικούς κινδύνους.

Χαρακτηριστικά δεν είναι λίγες οι περιπτώσεις όπου κωδικοί ασφαλείας πρώην εργαζομένων να μην διαγράφονται ποτέ από τις βάσεις δεδομένων μιας εταιρείας, παραμένοντας έγκυροι και μετά την απομάκρυνση του εργαζομένου από τον οργανισμό, επιτρέποντας στον χρήστη πρόσβαση σε ευαίσθητα δεδομένα της εταιρείας. Οι νέες τεχνολογίες όπως το User and Even Behavioral Analytics (UEBA) μπορούν να βοηθήσουν στον εντοπισμό ύποπτης ή ανώμαλης συμπεριφοράς από εσωτερικούς χρήστες, οι οποίες εν συνεχεία μπορούν να βοηθήσουν στον εντοπισμό επιθέσεων εσωτερικού.

2.6 Συστήματα Ανίχνευσης Επιθέσεων / IDS

Ένα σύστημα εντοπισμού εισβολών IDS (Intrusion Detection System) είναι μια συσκευή ή εφαρμογή λογισμικού που παρακολουθεί ένα δίκτυο ή συστήματα για κακόβουλη δραστηριότητα ή παραβιάσεις πολιτικής. Οποιαδήποτε δραστηριότητα εισβολής ή παραβίαση αναφέρεται συνήθως είτε σε διαχειριστή είτε συλλέγεται κεντρικά χρησιμοποιώντας ένα σύστημα πληροφοριών ασφαλείας και διαχείρισης συμβάντων SIEM (Security Information and Event Management). Ένα σύστημα SIEM συνδυάζει εξόδους από πολλές πηγές και χρησιμοποιεί τεχνικές φιλτραρίσματος συναγερμών για να διακρίνει την κακόβουλη δραστηριότητα από ψευδείς συναγερμούς. [57]

Οι τύποι IDS κυμαίνονται από έναν υπολογιστή σε μεγάλα δίκτυα. [58] Οι πιο συνηθισμένες ταξινομήσεις είναι τα συστήματα ανίχνευσης εισβολής

δικτύου NIDS (Network Intrusion Detection System) και τα συστήματα ανίχνευσης εισβολής που βασίζονται σε ξενιστές HIDS (Host-Based Intrusion Detection). Ένα σύστημα που παρακολουθεί σημαντικά αρχεία λειτουργικού συστήματος είναι ένα παράδειγμα HIDS, ενώ ένα σύστημα που αναλύει την εισερχόμενη κίνηση δικτύου είναι ένα παράδειγμα NIDS. Είναι επίσης δυνατό να ταξινομηθεί το IDS με προσέγγιση ανίχνευσης. Οι πιο γνωστές παραλλαγές είναι η ανίχνευση βάσει υπογραφής (αναγνώριση κακών μοτίβων, όπως το κακόβουλο λογισμικό) και η ανίχνευση βάσει ανωμαλιών (εντοπισμός αποκλίσεων από ένα μοντέλο "καλής" επισκεψιμότητας, το οποίο συχνά βασίζεται σε μηχανική εκμάθηση). Μια άλλη κοινή παραλλαγή είναι η ανίχνευση βάσει φήμης (αναγνωρίζοντας την πιθανή απειλή σύμφωνα με τις βαθμολογίες φήμης). Ορισμένα προϊόντα IDS έχουν τη δυνατότητα να ανταποκρίνονται σε εντοπισμένες εισβολές. Τα συστήματα με δυνατότητες απόκρισης αναφέρονται συνήθως ως σύστημα πρόληψης εισβολής . [59] Τα συστήματα ανίχνευσης εισβολής μπορούν επίσης να εξυπηρετήσουν συγκεκριμένους σκοπούς, αυξάνοντάς τα με προσαρμοσμένα εργαλεία, όπως η χρήση honeypot για την προσέλκυση και αποτροπή κακόβουλης κίνησης.

Παρόλο που και οι δύο σχετίζονται με την ασφάλεια του δικτύου, ένα IDS διαφέρει από ένα τείχος προστασίας στο ότι ένα παραδοσιακό τείχος προστασίας δικτύου χρησιμοποιεί ένα στατικό σύνολο κανόνων για να επιτρέπει ή να απορρίπτει συνδέσεις δικτύου. Αποτρέπει σιωπηρά τις εισβολές, υποθέτοντας ότι έχουν καθοριστεί από ένα κατάλληλο σύνολο κανόνων. Ουσιαστικά, τα τείχη προστασίας περιορίζουν την πρόσβαση μεταξύ δικτύων για να αποτρέψουν την εισβολή και να μην σηματοδοτούν επίθεση από το εσωτερικό του δικτύου. Ένα IDS εντοπίζει μια υποψία εισβολής μόλις πραγματοποιηθεί και σηματοδοτήσει έναν συναγερμό. Ένα IDS παρακολουθεί επίσης επιθέσεις που προέρχονται από ένα σύστημα. Αυτό επιτυγχάνεται παραδοσιακά εξετάζοντας τις επικοινωνίες δικτύου, εντοπίζοντας ευρετικές και μοτίβα (συχνά γνωστά ως υπογραφές) κοινών επιθέσεων σε υπολογιστές και ανάληψη δράσης για την ειδοποίηση των χειριστών. Ένα σύστημα που τερματίζει τις συνδέσεις ονομάζεται σύστημα πρόληψης εισβολής και εκτελεί έλεγχο πρόσβασης όπως ένα τείχος προστασίας επιπέδου εφαρμογής. [60]

Τα IDS μπορούν να ταξινομηθούν ανάλογα με το που πραγματοποιείται η ανίχνευση (δίκτυο ή κεντρικός υπολογιστής) ή με τη μέθοδο ανίχνευσης που χρησιμοποιείται (υπογραφή ή με βάση την ανωμαλία).

Συστήματα ανίχνευσης εισβολής δικτύου

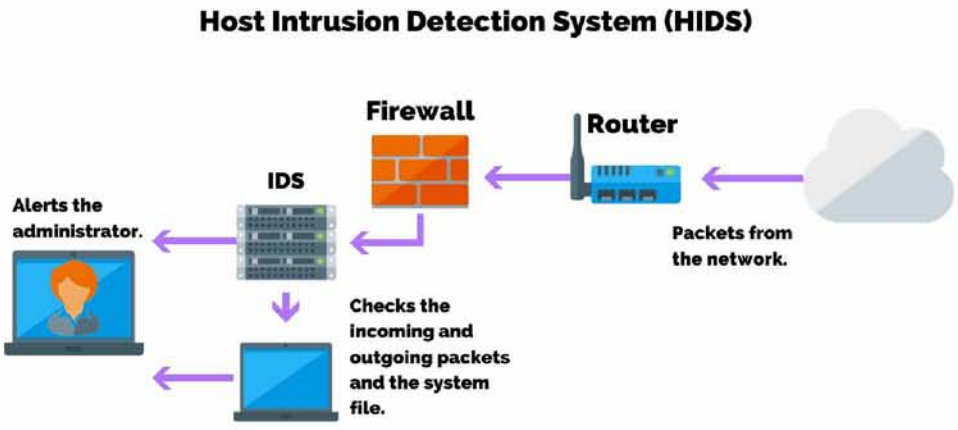
Τα συστήματα ανίχνευσης εισβολής δικτύου (NIDS) τοποθετούνται σε στρατηγικό σημείο ή σημεία εντός του δικτύου για την παρακολούθηση της κυκλοφορίας από και προς όλες τις συσκευές του δικτύου. Εκτελεί μια ανάλυση της μετάδοσης κίνησης σε ολόκληρο το υποδίκτυο, και ταιριάζει με την κίνηση που μεταφέρεται στα υποδίκτυα στη βιβλιοθήκη γνωστών επιθέσεων. Μόλις εντοπιστεί μια επίθεση ή ανιχνευθεί μη φυσιολογική συμπεριφορά, η ειδοποίηση μπορεί να σταλεί στον διαχειριστή. Ένα παράδειγμα ενός NIDS θα ήταν να το εγκαταστήσουμε στο υποδίκτυο όπου βρίσκονται τα τείχη προστασίας για να παρατηρήσουμε αν κάποιος προσπαθεί να εισέλθει στο τείχος προστασίας. Στην ιδανική περίπτωση αυτό θα σαρώσει όλη την εισερχόμενη και εξερχόμενη κίνηση, ωστόσο κάτι τέτοιο θα μπορούσε να δημιουργήσει ένα σημείο συμφόρησης που θα μπορούσε να επηρεάσει τη συνολική ταχύτητα του δικτύου. Το OPNET και το NetSim χρησιμοποιούνται συνήθως ως εργαλεία για την προσομοίωση συστημάτων ανίχνευσης εισβολής δικτύου. Τα συστήματα NID είναι επίσης ικανά να συγκρίνουν υπογραφές για παρόμοια πακέτα, για σύνδεση και απόθεση επιβλαβών πακέτων που έχουν εντοπιστεί και έχουν υπογραφή που ταιριάζει με τις εγγραφές στο NIDS. Όταν ταξινομούμε το σχεδιασμό του NIDS σύμφωνα με την ιδιότητα διαδραστικότητας του συστήματος, υπάρχουν δύο τύποι: NIDS on-line και off-line, που συχνά αναφέρονται ως λειτουργία inline και tap. Τα διαδικτυακά NIDS ασχολούνται με το δίκτυο σε πραγματικό χρόνο. Αναλύουν τα πακέτα Ethernet και εφαρμόζουν ορισμένους κανόνες, για να αποφασίσουν εάν είναι επίθεση ή όχι. Το NIDS εκτός σύνδεσης ασχολείται με τα αποθηκευμένα δεδομένα και τα περνά μέσω ορισμένων διαδικασιών για να αποφασίσει εάν πρόκειται για επίθεση ή όχι.

Το NIDS μπορεί επίσης να συνδυαστεί με άλλες τεχνολογίες για την αύξηση των ποσοστών ανίχνευσης και πρόβλεψης. Τα τεχνητά νευρωνικά δίκτυα IDS είναι ικανά να αναλύουν τεράστιους όγκους δεδομένων, με έξυπνο τρόπο, λόγω της αυτό-οργανωμένης δομής που επιτρέπει στο IDS να αναγνωρίζει αποτελεσματικότερα μοτίβα εισβολής. Τα νευρικά δίκτυα βοηθούν τους IDS στην πρόβλεψη επιθέσεων μαθαίνοντας από λάθη. Το IDS συμβάλλει στην ανάπτυξη ενός συστήματος έγκαιρης προειδοποίησης, που βασίζεται σε δύο επίπεδα. Το πρώτο επίπεδο δέχεται μεμονωμένες τιμές, ενώ το δεύτερο επίπεδο παίρνει την έξοδο των πρώτων ως είσοδο. Ο κύκλος επαναλαμβάνεται και επιτρέπει στο σύστημα να αναγνωρίζει αυτόματα νέα απρόβλεπτα μοτίβα στο δίκτυο. [61] Αυτό το σύστημα μπορεί να

ανιχνεύσει κατά μέσο όρο το 99,9% και το ποσοστό ταξινόμησης, με βάση τα αποτελέσματα έρευνας 24 επιθέσεων δικτύου, χωρισμένα σε τέσσερις κατηγορίες: DOS, Probe, Remote-to-Local και user-to-root. [62]

Συστήματα ανίχνευσης εισβολής κεντρικού υπολογιστή

Τα συστήματα ανίχνευσης εισβολής κεντρικού υπολογιστή (HIDS) εκτελούνται σε μεμονωμένους κεντρικούς υπολογιστές ή συσκευές στο δίκτυο. Το HIDS παρακολουθεί τα εισερχόμενα και εξερχόμενα πακέτα μόνο από τη συσκευή και θα ειδοποιεί τον χρήστη ή τον διαχειριστή εάν εντοπιστεί ύποπτη δραστηριότητα. Παίρνει ένα στιγμιότυπο των υπαρχόντων αρχείων συστήματος και το ταιριάζει με το προηγούμενο στιγμιότυπο. Εάν τα κρίσιμα αρχεία συστήματος τροποποιήθηκαν ή διαγράφηκαν, αποστέλλεται μια ειδοποίηση στον διαχειριστή για διερεύνηση. Εκτός από τη δυναμική επιθεώρηση των πακέτων του δικτύου που απευθύνονται στο συγκεκριμένο υπολογιστή, ένα HIDS έχει την ικανότητα να ανιχνεύσει οποιοδήποτε πρόγραμμα αποκτά πρόσβαση και σε ποιους συγκεκριμένους πόρους ελέγχοντας έτσι ύποπτες κινήσεις. Με τον ίδιο τρόπο ένα HIDS μπορεί να εξετάσει την κατάσταση ενός συστήματος, την αποθηκευμένη πληροφορία του στη μνήμη RAM, στα αρχεία καταγραφής συμβάντων και να ελέγξει εάν το περιεχόμενο αυτών εμφανίζεται έτσι όπως αναμενόταν, δηλαδή δεν έχει αλλάξει από εισβολείς. Ένα παράδειγμα της χρήσης HIDS μπορεί να δει κανείς σε μηχανήματα κρίσιμης αποστολής, τα οποία δεν αναμένεται να αλλάξουν τις διαμορφώσεις τους. [63],[64]



Εικόνα 14 : Έλεγχος πακέτων και ανίχνευση εισβολής στο δίκτυο

Με βάση την υπογραφή

Το IDS βάσει υπογραφής αναφέρεται στον εντοπισμό επιθέσεων αναζητώντας συγκεκριμένα μοτίβα, όπως ακολουθίες byte στην κίνηση δικτύου ή γνωστές κακόβουλες ακολουθίες εντολών που χρησιμοποιούνται από κακόβουλο λογισμικό.[65] Αυτή η ορολογία προέρχεται από λογισμικό προστασίας από ιούς , το οποίο αναφέρεται σε αυτά τα μοτίβα που έχουν εντοπιστεί ως υπογραφές. Παρόλο που το IDS βάσει υπογραφής μπορεί εύκολα να εντοπίσει γνωστές επιθέσεις, είναι δύσκολο να εντοπιστούν νέες επιθέσεις, για τις οποίες δεν υπάρχει διαθέσιμο μοτίβο. [66]

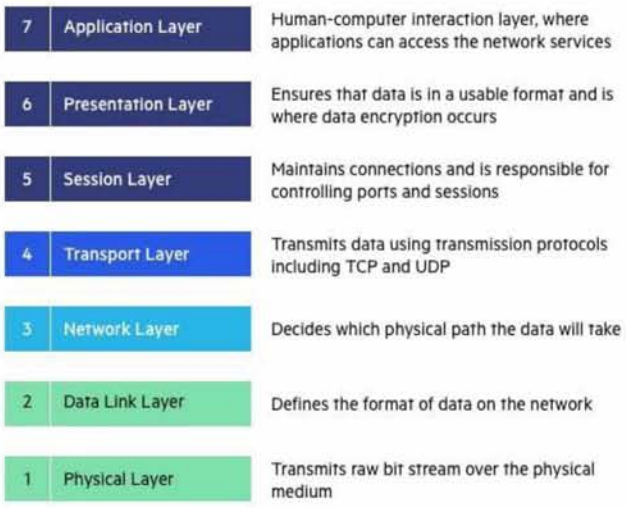
Βάση ανωμαλιών

Τα συστήματα ανίχνευσης εισβολής που βασίζονται σε ανωμαλίες εισήχθησαν κυρίως για την ανίχνευση άγνωστων επιθέσεων, εν μέρει λόγω της ταχείας ανάπτυξης κακόβουλου λογισμικού. Η βασική προσέγγιση είναι η χρήση της μηχανικής μάθησης για να δημιουργήσουμε ένα μοντέλο αξιόπιστης δραστηριότητας και, στη συνέχεια, να συγκρίνουμε τη νέα συμπεριφορά με αυτό το μοντέλο. Δεδομένου ότι αυτά τα μοντέλα μπορούν να εκπαιδευτούν σύμφωνα με τις εφαρμογές και τις διαμορφώσεις υλικού, η μέθοδος που βασίζεται στη μηχανική μάθηση έχει μια καλύτερη γενικευμένη ιδιότητα σε σύγκριση με τα παραδοσιακά IDS με βάση την υπογραφή. Τα περισσότερα από τα υπάρχοντα IDS υποφέρουν από τη χρονοβόρα διαδικασία ανίχνευσης που υποβαθμίζει την απόδοση των IDS. Ο αποτελεσματικός αλγόριθμος επιλογής χαρακτηριστικών καθιστά τη διαδικασία ταξινόμησης που χρησιμοποιείται στην ανίχνευση πιο αξιόπιστη. [6]

Η τοποθέτηση συστημάτων ανίχνευσης εισβολής είναι κρίσιμη και ποικίλλει ανάλογα με το δίκτυο. Η πιο συνηθισμένη τοποθέτηση βρίσκεται πίσω από το τείχος προστασίας στην άκρη ενός δικτύου. Αυτή η πρακτική παρέχει στο IDS υψηλή ορατότητα της κυκλοφορίας που εισέρχεται στο δίκτυό και δεν θα λαμβάνει καμία κίνηση μεταξύ των χρηστών στο δίκτυο. Το άκρο του δικτύου είναι το σημείο στο οποίο ένα δίκτυο συνδέεται με το extranet. Μια άλλη πρακτική που μπορεί να επιτευχθεί εάν υπάρχουν περισσότεροι πόροι είναι μια στρατηγική όπου ένας τεχνικός θα τοποθετήσει το πρώτο IDS στο σημείο της υψηλότερης ορατότητας και ανάλογα με τη διαθεσιμότητα πόρων θα τοποθετήσει ένα άλλο στο επόμενο υψηλότερο σημείο, συνεχίζοντας τη διαδικασία μέχρι όλα τα σημεία του καλύπτονται δίκτυο. [73]

Εάν ένα IDS τοποθετηθεί πέρα από το τείχος προστασίας ενός δικτύου, ο κύριος σκοπός του θα ήταν να υπερασπιστεί τον θόρυβο από το Διαδίκτυο. Ένα IDS σε αυτήν τη θέση θα παρακολουθούσε τα επίπεδα 4 έως 7 του μοντέλου OSI και θα βασίζονταν σε υπογραφές. Αυτή είναι μια πολύ χρήσιμη πρακτική, επειδή το IDS σε αυτήν τη θέση βοηθά επίσης στη μείωση του χρόνου που χρειάζεται για να ανακαλυφθούν επιτυχημένες επιθέσεις εναντίον ενός δικτύου. [74]

Μερικές φορές ένα IDS με πιο προηγμένες δυνατότητες θα ενσωματωθεί σε ένα τείχος προστασίας, ώστε να μπορεί να παρακολουθεί εξελιγμένες επιθέσεις που εισέρχονται στο δίκτυο. Παραδείγματα προηγμένων λειτουργιών θα περιλαμβάνουν πολλαπλά περιβάλλοντα ασφαλείας στο επίπεδο δρομολόγησης και τη λειτουργία γεφύρωσης. Όλα αυτά με τη σειρά τους μειώνουν δυνητικά το κόστος και τη λειτουργική πολυπλοκότητα.



Εικόνα 15 : Εφτά επίπεδα OSI

Μια άλλη επιλογή για τοποθέτηση IDS βρίσκεται στο πραγματικό δίκτυο. Αυτά θα αποκαλύψουν επιθέσεις ή ύποπτη δραστηριότητα εντός του δικτύου. Η παράβλεψη της ασφάλειας σε ένα δίκτυο μπορεί να προκαλέσει πολλά προβλήματα, είτε θα επιτρέψει στους χρήστες να προκαλέσουν κινδύνους ασφαλείας είτε να επιτρέψουν σε έναν εισβολέα που έχει ήδη εισέλθει στο δίκτυο να περιπλανηθεί ελεύθερα. Η έντονη ασφάλεια του intranet δυσκολεύει τους hackers στο δίκτυο να κάνουν ελιγμούς και να κλιμακώσουν τα προνόμιά τους. [74]

Περιορισμοί

- Ο θόρυβος μπορεί να περιορίσει σοβαρά την αποτελεσματικότητα ενός συστήματος ανίχνευσης εισβολής. Κακά πακέτα που δημιουργούνται από σφάλματα λογισμικού, κατεστραμμένα δεδομένα DNS και τοπικά πακέτα που διέφυγαν μπορούν να δημιουργήσουν σημαντικά υψηλό ρυθμό ψευδούς συναγερμού. [75]
- Δεν είναι ασυνήθιστο ο αριθμός των πραγματικών επιθέσεων να είναι πολύ χαμηλότερος από τον αριθμό των ψευδών συναγερμών, με αποτέλεσμα οι πραγματικές επιθέσεις συχνά παραλείπονται και να αγνοούνται.
- Πολλές επιθέσεις προορίζονται για συγκεκριμένες εκδόσεις λογισμικού που είναι συνήθως ξεπερασμένες. Απαιτείται μια συνεχώς μεταβαλλόμενη βιβλιοθήκη υπογραφών για τον μετριασμό των απειλών. Οι ξεπερασμένες βάσεις δεδομένων υπογραφής μπορούν να αφήσουν το IDS ευάλωτο σε νεότερες στρατηγικές. [75]
- Για IDS βάσει υπογραφής, θα υπάρχει διαφορά μεταξύ μιας νέας ανακάλυψης απειλής και της υπογραφής της που εφαρμόζεται στο IDS. Κατά τη διάρκεια αυτού του χρόνου καθυστέρησης, το IDS δεν θα είναι σε θέση να εντοπίσει την απειλή. [74]
- Δεν μπορεί να αντισταθμίσει τους αδύναμους μηχανισμούς αναγνώρισης και ελέγχου ταυτότητας ή αδυναμίες στα πρωτόκολλα δικτύου. Όταν ένας εισβολέας αποκτά πρόσβαση λόγω αδύναμων μηχανισμών ελέγχου ταυτότητας, τότε το IDS δεν μπορεί να αποτρέψει τον αντίπαλο από κακή πρακτική.
- Τα κρυπτογραφημένα πακέτα δεν υποβάλλονται σε επεξεργασία από τις περισσότερες συσκευές ανίχνευσης εισβολής. Επομένως, το κρυπτογραφημένο πακέτο μπορεί να επιτρέψει την εισβολή στο δίκτυο που δεν ανακαλύπτεται έως ότου έχουν πραγματοποιηθεί πιο σημαντικές εισβολές δικτύου.
- Το λογισμικό ανίχνευσης εισβολής παρέχει πληροφορίες με βάση τη διεύθυνση δικτύου που σχετίζεται με το πακέτο IP που αποστέλλεται στο δίκτυο. Αυτό είναι ευεργετικό εάν η διεύθυνση δικτύου που περιέχεται στο πακέτο IP είναι ακριβής. Ωστόσο, η διεύθυνση που περιέχεται στο πακέτο IP θα μπορούσε να είναι πλαστή ή αναμεμιγμένη.
- Λόγω της φύσης των συστημάτων NIDS και της ανάγκης τους να αναλύουν πρωτόκολλα καθώς συλλαμβάνονται, τα συστήματα NIDS μπορεί να είναι ευαίσθητα στις ίδιες επιθέσεις που βασίζονται σε πρωτόκολλα στις οποίες οι κεντρικοί υπολογιστές δικτύου

ενδέχεται να είναι ευάλωτοι. Τα μη έγκυρα δεδομένα και οι επιθέσεις στοίβας TCP / IP ενδέχεται να προκαλέσουν διακοπή λειτουργίας του NIDS. [76]

Τεχνικές αποφυγής

Υπάρχουν πολλές τεχνικές που χρησιμοποιούν οι εισβολείς, τα ακόλουθα θεωρούνται «απλά» μέτρα που μπορούν να ληφθούν για να αποφύγουν το IDS:

- Κατακερματισμός: στέλνοντας κατακερματισμένα πακέτα, ο εισβολέας θα βρίσκεται κάτω από το ραντάρ και μπορεί εύκολα να παρακάμψει την ικανότητα ανίχνευσης του συστήματος να ανιχνεύει την υπογραφή της επίθεσης.
- Αποφυγή προεπιλογών: Η θύρα TCP (Transmission Control Protocol) που χρησιμοποιείται από ένα πρωτόκολλο δεν παρέχει πάντα ένδειξη για το πρωτόκολλο που μεταφέρεται. Για παράδειγμα, ένα IDS μπορεί να αναμένει να εντοπίσει ένα trojan στη θύρα 12345. Εάν ένας εισβολέας είχε διαμορφώσει εκ νέου για να χρησιμοποιήσει μια διαφορετική θύρα, το IDS ενδέχεται να μην είναι σε θέση να εντοπίσει την παρουσία του trojan.
- Συντονισμένες επιθέσεις με χαμηλό εύρος ζώνης: ο συντονισμός μιας σάρωσης μεταξύ πολλών εισβολέων (ή πρακτόρων) και η κατανομή διαφορετικών θυρών ή κεντρικών υπολογιστών σε διαφορετικούς επιτιθέμενους δυσκολεύει το IDS να συσχετίσει τα πακέτα που έχουν συλληφθεί και να συμπεράνει ότι μια σάρωση δικτύου βρίσκεται σε εξέλιξη.
- Διεύθυνση πλαστογράφησης / διακομιστή μεσολάβησης: οι εισβολείς μπορούν να αυξήσουν τη δυσκολία της ικανότητας των Διαχειριστών ασφαλείας να προσδιορίσουν την πηγή της επίθεσης, χρησιμοποιώντας διακομιστές μεσολάβησης με κακή ασφάλεια ή λανθασμένη διαμόρφωση για να αναπηδήσουν μια επίθεση. Εάν η πηγή πλαστογραφηθεί και αναπηδήσει από έναν διακομιστή, καθιστά πολύ δύσκολο για το IDS να εντοπίσει την προέλευση της επίθεσης.
- Διαφυγή αλλαγής προτύπων: Το IDS βασίζεται γενικά στο «μοτίβο αντιστοίχισης» για να εντοπίσει μια επίθεση. Αλλάζοντας ελαφρά τα δεδομένα που χρησιμοποιήθηκαν στην επίθεση, είναι δυνατόν να αποφύγει την ανίχνευση. Για παράδειγμα, ένας διακομιστής πρωτοκόλλου πρόσβασης μηνύματος Διαδικτύου IMAP (Internet Message Access Protocol) ενδέχεται να είναι ευάλωτος σε υπερχείλιση buffer και ένα

IDS είναι σε θέση να εντοπίσει την υπογραφή επίθεσης 10 κοινών εργαλείων επίθεσης. Τροποποιώντας το ωφέλιμο φορτίο που αποστέλλεται από το εργαλείο, έτσι ώστε να μην μοιάζει με τα δεδομένα που αναμένει το IDS, αποφεύγοντας πιθανή ανίχνευση.

Ανάπτυξη - Ιστορικά

Η πρώτη ιδέα IDS οριοθετήθηκε το 1980 από τον James Anderson στην Υπηρεσία Εθνικής Ασφάλειας των ΗΠΑ και αποτελούταν από ένα σύνολο εργαλείων που προορίζονταν να βοηθήσουν τους διαχειριστές να ελέγξουν τα ίχνη ελέγχου. Τα αρχεία καταγραφής πρόσβασης χρήστη, τα αρχεία καταγραφής πρόσβασης αρχείων και τα αρχεία καταγραφής συμβάντων συστήματος είναι παραδείγματα διαδρομών ελέγχου. Ο Fred Cohen σημείωσε το 1987 ότι είναι αδύνατο να εντοπιστεί μια εισβολή σε κάθε περίπτωση, και ότι οι πόροι που απαιτούνται για την ανίχνευση των εισβολών αυξάνονται με το ποσό της χρήσης. [77]

Η Dorothy E. Denning, επικουρούμενη από τον Peter G. Neumann, δημοσίευσε ένα μοντέλο IDS το 1986 που αποτέλεσε τη βάση για πολλά συστήματα σήμερα. Το μοντέλο της χρησιμοποίησε στατιστικά στοιχεία για την ανίχνευση ανωμαλιών και οδήγησε σε ένα πρώιμο IDS στο SRI International που ονομάστηκε IDES (Intrusion Detection Expert System), το οποίο έτρεχε σε σταθμούς εργασίας της Sun και μπορούσε να λάβει υπόψη δεδομένα επιπέδου χρήστη και δικτύου.Το IDES είχε μια διπλή προσέγγιση με ένα σύστημα εμπειρογνωμόνων βασισμένο σε κανόνες για την ανίχνευση γνωστών τύπων παρεμβολών συν ένα στοιχείο ανίχνευσης στατιστικής ανωμαλίας που βασίζεται σε προφίλ χρηστών, συστημάτων κεντρικών υπολογιστών και συστημάτων στόχων. [78]

Το σύστημα εντοπισμού και ειδοποίησης εισβολής Multics (MIDAS), ένα εξειδικευμένο σύστημα που χρησιμοποιεί P-BEST και Lisp , αναπτύχθηκε το 1988 με βάση το έργο των Denning και Neumann. Το Haystack αναπτύχθηκε επίσης εκείνο το έτος χρησιμοποιώντας στατιστικά στοιχεία για τη μείωση των διαδρομών ελέγχου. Το 1986 η Εθνική Υπηρεσία Ασφαλείας των ΗΠΑ ξεκίνησε ένα πρόγραμμα μεταφοράς έρευνας IDS υπό την Rebecca Bace. Η οποία δημοσίευσε αργότερα το κείμενο σχετικά με το θέμα, *Intrusion Detection*, το 2000. [79]

Το Wisdom&Sense (W&S) ήταν ένας ανιχνευτής ανωμαλιών συστήματος βάσει στατιστικών που αναπτύχθηκε το 1989 στο Εθνικό Εργαστήριο LosAlamos. Δημιούργησε κανόνες βάσει στατιστικής ανάλυσης και στη συνέχεια χρησιμοποίησε αυτούς τους κανόνες για ανίχνευση ανωμαλιών. Το 1990, το Time-based Inductive Machine (TIM) έκανε ανίχνευση ανωμαλιών χρησιμοποιώντας επαγωγική εκμάθηση διαδοχικών μοτίβων χρήστη στο Common Lisp σε έναν υπολογιστή VAX 3500. [76] Το Network Security Monitor (NSM) πραγματοποίησε κάλυψη σε πίνακες πρόσβασης για ανίχνευση ανωμαλιών σε σταθμό εργασίας Sun-3/50. Ο Βοηθός Αξιωματούχου Ασφάλειας Πληροφοριών (ISOA) ήταν ένα πρωτότυπο του 1990 που εξέτασε μια ποικιλία δεδομένων, όπως στατιστικά στοιχεία, ελεγκτής προφίλ και σύστημα εμπειρογνωμόνων. [81]

Στη συνέχεια, το 1991, ερευνητές στο Πανεπιστήμιο της Καλιφόρνια, δημιούργησαν ένα πρωτότυπο Κατανεμημένο Σύστημα Ανίχνευσης Εισβολής (DIDS). Το Network Anomaly Detection and Intrusion Reporter (NADIR), επίσης, το 1991, ήταν ένα πρωτότυπο IDS που αναπτύχθηκε στο Ολοκληρωμένο Δίκτυο Πληροφοριών του Εθνικού Εργαστηρίου Los Alamos (ICN) και επηρεάστηκε σε μεγάλο βαθμό από το έργο του Denning και του Lunt. Το Εθνικό Εργαστήριο Lawrence Berkeley ανακοίνωσε το σύστημα Bro (Big Brother) το 1998, το οποίο χρησιμοποίησε τη δική του γλώσσα για ανάλυση πακέτων από δεδομένα libpcap.

Το APE αναπτύχθηκε ως πακέτο sniffer, χρησιμοποιώντας επίσης libpcap, το Νοέμβριο του 1998, και μετονομάστηκε Snort ένα μήνα αργότερα. Το Snort έγινε από τότε το μεγαλύτερο χρησιμοποιημένο σύστημα IDS / IPS στον κόσμο με περισσότερους από 300.000 ενεργούς χρήστες. Μπορεί να παρακολουθεί τόσο τα τοπικά συστήματα όσο και τα απομακρυσμένα σημεία λήψης.

Το IDS Ανάλυσης Δεδομένων Ελέγχου και Εξόρυξης (ADAM) το 2001 χρησιμοποίησε το tcpdump για να δημιουργήσει προφίλ κανόνων για ταξινομήσεις. Το 2003, οι Yongguang Zhang και Wenke Lee υποστηρίζουν τη σημασία του IDS σε δίκτυα με κινητούς κόμβους.

Το 2015, ο Viegas και οι συνεργάτες του πρότειναν μια μηχανή ανίχνευσης εισβολής που βασίζεται σε ανωμαλίες, με στόχο το System-on-Chip (SoC) για εφαρμογές στο Internet of Things (IoT), για παράδειγμα. Η πρόταση εφαρμόζει μηχανική εκμάθηση για ανίχνευση ανωμαλιών, παρέχοντας ενεργειακή απόδοση σε μια εφαρμογή ταξινόμησης απόφασης Tree, Naive-Bayes και k-NearestNeighbour. Αυτή ήταν η πρώτη εργασία που εφαρμόζει κάθε

ταξινομητή ισοδύναμα σε λογισμικό και υλικό και μετρά την κατανάλωση ενέργειας και στα δύο. Επιπλέον, ήταν η πρώτη φορά που μετρήθηκε η κατανάλωση ενέργειας για την εξαγωγή κάθε δυνατότητας που χρησιμοποιήθηκε για την ταξινόμηση πακέτων δικτύου, που εφαρμόστηκε σε λογισμικό και υλικό.[82]

2.7 Ασφάλεια Συστημάτων Έξυπνων Συσκευών και Μέτρα Ασφάλειας

Ορισμένα συστήματα ενδέχεται να προσπαθήσουν να σταματήσουν μια προσπάθεια εισβολής αλλά αυτό δεν απαιτείται ούτε αναμένεται από ένα σύστημα παρακολούθησης. Τα συστήματα ανίχνευσης και πρόληψης εισβολής (IDPS) επικεντρώνονται κυρίως στον εντοπισμό πιθανών συμβάντων, την καταγραφή πληροφοριών σχετικά με αυτά και την απόπειρα αναφοράς. Επιπλέον, οι οργανισμοί χρησιμοποιούν IDPS για άλλους σκοπούς, όπως τον εντοπισμό προβλημάτων με τις πολιτικές ασφαλείας, την τεκμηρίωση των υπαρχουσών απειλών και την αποτροπή των ατόμων από την παραβίαση των πολιτικών ασφαλείας. Οι IDPS έχουν γίνει απαραίτητη προσθήκη στην υποδομή ασφαλείας σχεδόν κάθε οργανισμού. [69]

Οι IDPS καταγράφουν συνήθως πληροφορίες που σχετίζονται με συμβάντα που παρατηρούνται, ειδοποιούν τους διαχειριστές ασφαλείας για σημαντικά συμβάντα που παρατηρούνται και συντάσσουν αναφορές. Πολλοί IDPS μπορούν επίσης να ανταποκριθούν σε μια απειλή που εντοπίστηκε προσπαθώντας να την αποτρέψουν από την επιτυχία. Χρησιμοποιούν πολλές τεχνικές απόκρισης, οι οποίες περιλαμβάνουν το IDPS να σταματήσει την ίδια την επίθεση, να αλλάξει το περιβάλλον ασφαλείας (π.χ. αναδιάταξη ενός τείχους προστασίας) ή να αλλάξει το περιεχόμενο της επίθεσης. [69]

Τα συστήματα πρόληψης εισβολής (IPS), επίσης γνωστά ως συστήματα ανίχνευσης και πρόληψης εισβολής (IDPS), είναι συσκευές ασφάλειας δικτύου που παρακολουθούν δραστηριότητες δικτύου ή συστήματος για κακόβουλη δραστηριότητα. Οι κύριες λειτουργίες των συστημάτων πρόληψης εισβολής είναι ο εντοπισμός κακόβουλης δραστηριότητας, η καταγραφή πληροφοριών σχετικά με αυτήν τη δραστηριότητα, η αναφορά της και η απόπειρα αποκλεισμού ή διακοπής της. [70].

Τα συστήματα πρόληψης εισβολών θεωρούνται επεκτάσεις συστημάτων ανίχνευσης εισβολών επειδή παρακολουθούν και οι δύο την κυκλοφορία του δικτύου ή / και τις δραστηριότητες του συστήματος για κακόβουλη δραστηριότητα. Οι κύριες διαφορές είναι, σε αντίθεση με τα συστήματα ανίχνευσης εισβολής, τα συστήματα πρόληψης εισβολών είναι σε θέση να αποτρέψουν ενεργά ή να μπλοκάρουν τις εισβολές που εντοπίζονται.[71] Το IPS μπορεί να προβεί σε ενέργειες όπως η αποστολή συναγερμού, η απόρριψη εντοπισμένων κακόβουλων πακέτων, η επαναφορά μιας σύνδεσης ή ο αποκλεισμός της κίνησης από την προσβλητική διεύθυνση IP. Ένα IPS μπορεί επίσης να διορθώσει σφάλματα κυκλικού ελέγχου πλεονασμού – CRC (Cyclic Redundancy Code), ροές πακέτων ανασυγκρότησης, να μετριάσει τα προβλήματα αλληλουχίας TCP. [71]

Ταξινόμηση

Τα συστήματα πρόληψης εισβολής μπορούν να ταξινομηθούν σε τέσσερις διαφορετικούς τύπους:[72]

1. **Σύστημα πρόληψης εισβολής βάσει δικτύου (NIPS- Network Intrusion Prevention System)** : παρακολουθεί ολόκληρο το δίκτυο για ύποπτη κίνηση, αναλύοντας τη δραστηριότητα του πρωτοκόλλου.
2. **Σύστημα πρόληψης ασύρματων εισβολών (WIPS – Wireless Intrusion Prevention System)** : παρακολούθηση ασύρματου δικτύου για ύποπτη κίνηση, αναλύοντας πρωτόκολλα ασύρματης δικτύωσης.
3. **Ανάλυση συμπεριφοράς δικτύου (NBA – Network Behavioral Analysis)** : εξετάζει την κυκλοφορία δικτύου για τον εντοπισμό απειλών που δημιουργούν ασυνήθιστες ροές επισκεψιμότητας, όπως επιθέσεις κατανεμημένης άρνησης υπηρεσίας (DDoS), συγκεκριμένες μορφές κακόβουλου λογισμικού και παραβιάσεις πολιτικής.
4. **Σύστημα πρόληψης εισβολής βάσει κεντρικού υπολογιστή (HIPS - Host Intrusion Prevention System)** : ένα εγκατεστημένο πακέτο λογισμικού που παρακολουθεί έναν μόνο κεντρικό υπολογιστή για ύποπτη δραστηριότητα, αναλύοντας συμβάντα που συμβαίνουν εντός αυτού του κεντρικού υπολογιστή.

2.8 Τρόποι Αντιμετώπισης Απειλών

Τις τελευταίες δύο δεκαετίες, το Διαδίκτυο έχει εξελιχθεί από καινοτομία σε ένα εργαλείο στο οποίο οι περισσότεροι από εμάς βασιζόμαστε σε μεγάλο βαθμό κάθε μέρα. Το Διαδίκτυο έχει αλλάξει εντελώς τον τρόπο που κάνουμε τα πράγματα, από τον τρόπο που εργαζόμαστε, τον τρόπο που επικοινωνούμε, ψωνίζουμε και μαθαίνουμε. Όταν σκεφτόμαστε πόσο εξαρτάται από το Διαδίκτυο η καθημερινή μας ζωή, είναι δύσκολο να φανταστεί κανείς τη ζωή χωρίς αυτό. Όμως, όσο το Διαδίκτυο είναι ένα απαραίτητο εργαλείο, η χρήση του μας αφήνει ευάλωτους σε κακόβουλες απειλές. Υπάρχει μια αφθονία από Δούρειους ίππους, bots, adware, ransomware, macroviruses, rogueware, spyware, worms και phishing επιθέσεις που στοχεύουν χρήστες του διαδικτύου καθημερινά. Οι επιθέσεις εγκληματικών προγραμμάτων και η απάτη ταυτότητας μπορούν να συμβούν σε οποιονδήποτε ανά πάσα στιγμή και όσο περισσότερο χρησιμοποιούμε το Διαδίκτυο, τόσο πιο ευάλωτοι είμαστε σε απειλές.

Υπάρχουν πολλά μέτρα ασφαλείας που μπορούν να εφαρμόσουν οι χρήστες του Διαδικτύου για να ελαχιστοποιηθεί ο κίνδυνος από κακόβουλες επιθέσεις. Εάν κάποιος είναι θύμα μιας επίθεσης, θα πρέπει να ελέγξει τα βήματα που μπορεί να λάβει ως απάντηση στο συμβάν.

Εάν κάποιος είναι θύμα μιας επίθεσης με λογισμικό, θα πρέπει να αποσυνδεθεί αμέσως από το Διαδίκτυο. Εάν είναι συνδεδεμένος μέσω Wi-Fi, τηλεφώνου ή καλωδίου Ethernet, πρέπει να απενεργοποιήσει τη σύνδεση το συντομότερο δυνατό για να αποτρέψει τη μετάδοση δεδομένων στον εγκληματία. Η διακοπή της σύνδεσης δικτύου είναι ο καλύτερος τρόπος για να σταματήσει αμέσως την επίθεση. Μπορεί να διακόψει τη σύνδεση στο Διαδίκτυο αποσυνδέοντας φυσικά από το δρομολογητή ή τη σύνδεση δικτύου και επίσης απενεργοποιώντας τη σύνδεση στη συσκευή ακολουθώντας το απλό μονοπάτι Έναρξη->Ρυθμίσεις->Συνδέσεις Δικτύου->Απενεργοποίηση. (για Windows)

Σε περιπτώσεις επίθεσης σε δίκτυα εταιριών, θα πρέπει να υπάρχει άμεση επικοινωνία με το τμήμα πληροφορικής. Η ομάδα πληροφορικής της εταιρείας πρέπει να γνωρίζει σχετικά με τη μόλυνση για να την εμποδίσει να διαδώσει ή να θέσει σε κίνδυνο τα ευαίσθητα δεδομένα που βρίσκονται στον μολυσμένο σύστημα. Στη συνέχεια, το τμήμα πληροφορικής θα μπορεί να λάβει τα σωστά μέτρα για την αποκατάσταση της ζημιάς που προκλήθηκε. Εάν πραγματοποιηθεί επίθεση σε προσωπική συσκευή, θα πρέπει να επικοινωνήσει με τον πάροχο υπηρεσιών διαδικτύου (ISP).

Είναι καλή πρακτική να έχει κάποιος εγκατεστημένο και ενημερωμένο λογισμικό προστασίας από ιούς, σε περίπτωση που συμβεί αυτό το είδος συμβάντος. Το λογισμικό προστασίας από ιούς και antispyware είναι τα καλύτερα εργαλεία για την προστασία από το ηλεκτρονικό έγκλημα. Είναι απαραίτητο να γίνονται περιοδικές διαγνωστικές σαρώσεις με το λογισμικό. Επίσης να ρυθμίζονται αυτόματες σαρώσεις σε τακτά χρονικά διαστήματα για να προστατεύεται περαιτέρω η συσκευή.

Δημιουργία αντίγραφου ασφαλείας

Είναι καλή πρακτική να δημιουργούνται τακτικά αντίγραφα ασφαλείας των αρχείων και των φακέλων. Ενώ ο στόχος του ηλεκτρονικού εγκλήματος είναι σε μεγάλο βαθμό η κλοπή πληροφοριών ή δεδομένων, υπάρχει μεγάλη πιθανότητα τα αρχεία να χαθούν ή να καταστραφούν κατά τη διαδικασία ανάκτησης. Μπορεί να δημιουργηθούν αντίγραφα ασφαλείας χρησιμοποιώντας λογισμικό δημιουργίας αντιγράφων ασφαλείας, χρησιμοποιώντας έναν άλλο σκληρό δίσκο ή αφαιρούμενο μέσο όπως CD, DVD ή μονάδα flash ή όπως γίνεται πιο συχνά σε εφαρμογές cloud.

Επανεγκατάσταση στο λειτουργικό σύστημα

Ανάλογα με τη σοβαρότητα της επίθεσης, ίσως χρειαστεί επανεγκατάσταση το λειτουργικό σύστημα του υπολογιστή. Ορισμένες απειλές είναι πολύ περίπλοκες και μπορεί να κρύβονται βαθιά στο σύστημα χρησιμοποιώντας τεχνικές rootkit, πράγμα που σημαίνει ότι θα περάσουν απαρατήρητες από το λογισμικό προστασίας.

Το λογισμικό μπορεί να επαναφέρει το σύστημα στην τελευταία του σταθερή κατάσταση πριν από τη μόλυνση. Σε άλλες περιπτώσεις, η ημερομηνία μόλυνσης ενδέχεται να μην είναι γνωστή και ενδέχεται να τεθούν σε κίνδυνο πιο ευαίσθητα δεδομένα. Σε αυτήν την περίπτωση, η ασφαλέστερη επιλογή μπορεί να είναι η ανάκτηση των αρχείων και η επανεγκατάσταση του λειτουργικού συστήματος.[83]

Κρυπτογράφηση

Ως κρυπτογράφηση ορίζουμε την μετατροπή ανάλυσης των δεδομένων σε καινούργια κωδικοποιημένη μορφή που να είναι αδύνατον να διαβαστεί χωρίς τη γνώση της σωστής ακολουθίας bit που οδηγεί στη αντίστροφη κωδικοποίηση – αποκωδικοποίηση. Το κλειδί ή αλλιώς η ακολουθία bit κωδικοποίησης χρησιμοποιείται σε συνδυασμό με την κατάλληλη συνάρτηση-αλγόριθμο. ‘Ενας αλγόριθμος θεωρείται ασφαλής όταν μόνο οι

εξουσιοδοτημένοι χρήστες μπορούν να προβούν στην άμεση αποκρυπτογράφηση του χρησιμοποιώντας το κλειδί τους. Η αντίστροφη διαδικασία είναι η αποκρυπτογράφηση και απαιτεί γνώση του κλειδιού. Βασικά στοιχεία της κρυπτογράφησης είναι ο τρόπος που δημιουργούνται τα κλειδιά ασφαλείας τι ρόλο παίζουν αυτά για τον κάθε χρήστη.

Εικόνα 16 : Η κρυπτογράφηση ως μέσο προστασίας δεδομένων

Ένας αλγόριθμος θεωρείται ασφαλής αν κανείς άλλος εκτός των εξουσιοδοτημένων, δεν μπορεί να υπολογίσει οποιαδήποτε συνάρτηση του αρχικού κειμένου.

Ασύμμετρη κρυπτογράφηση περιλαμβάνει τους κρυπτογραφικούς αλγόριθμους στους οποίους χρησιμοποιούνται δύο διαφορετικά κλειδιά ένα για την κρυπτογράφηση ενώ το άλλο για την αποκρυπτογράφηση των δεδομένων. Το κλειδί κρυπτογράφησης γνωστοποιείται συνήθως μέσω ψηφιακού πιστοποιητικού σε τρίτους και λέγεται δημόσιο κλειδί ενώ το κλειδί αποκρυπτογράφησης είναι γνωστό μόνο στον κάτοχό του και λέγεται ιδιωτικό. Η κρυπτογράφηση δημοσίου κλειδιού μπορεί να χρησιμοποιηθεί και για τη δημιουργία και επαλήθευση ψηφιακής υπογραφής. [84]

Χαρακτηριστικό αυτής της κατηγορίας αλγορίθμων αποτελεί το μεγάλο μήκος κλειδιού και η αργή τους ταχύτητα.

Η Συμμετρική Κρυπτογράφηση περιλαμβάνει τους κρυπτογραφικούς αλγόριθμους στους οποίους χρησιμοποιείται το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων. Στη συμμετρική κρυπτογράφηση το κλειδί κρυπτογράφησης/αποκρυπτογράφησης είναι εξ ορισμού μυστικό κλειδί, γνωστό μόνο στους εξουσιοδοτημένους κατόχους. [85]

Κεφάλαιο 3

3.1. IoT

«Το Διαδίκτυο των πραγμάτων ή Ίντερνετ των πραγμάτων (αγγλικά: Internet of things) αποτελεί το δίκτυο επικοινωνίας πληθώρας συσκευών, οικιακών συσκευών, αυτοκινήτων καθώς και κάθε αντικειμένου που ενσωματώνει ηλεκτρονικά μέσα, λογισμικό, αισθητήρες και συνδεσιμότητα σε δίκτυο ώστε να επιτρέπεται η σύνδεση και η ανταλλαγή δεδομένων. Απλούστερα, η φιλοσοφία του IoT είναι η σύνδεση όλων των ηλεκτρονικών συσκευών μεταξύ τους (τοπικό δίκτυο) ή με δυνατότητα σύνδεσης στο διαδίκτυο (παγκόσμιο ιστό).» [87]

Το να ζεις σε έναν «έξυπνο» κόσμο σημαίνει ότι υπάρχει ένα ταχέως αναπτυσσόμενο δίκτυο συνδεδεμένων συσκευών που συλλέγουν και μοιράζονται δεδομένα. Χάρη στο Διαδίκτυο των πραγμάτων (IoT), υπάρχουν έξυπνες συσκευές όπως θερμοστάτες, όργανα γυμναστικής και ακόμη και ψυγεία. Στην πραγματικότητα, αναμένεται να εγκατασταθούν πάνω από 20 δισεκατομμύρια μονάδες IoT έως το τέλος του 2020. Αυτό αντιπροσωπεύει μια σημαντική επιχειρηματική ευκαιρία για τους κατασκευαστές.

Ως αποτέλεσμα της διευρυμένης αγοράς IoT, οι κατασκευαστές σε όλο τον κόσμο ανταγωνίζονται για την ανάπτυξη της τελευταίας συσκευής και τη θέτουν στα χέρια των καταναλωτών. Το IoT είναι αυτό που επιτρέπει την αλληλεπίδραση σε πραγματικό χρόνο μεταξύ αντικειμένων, ανεξάρτητα από τη φυσική απόσταση. Για παράδειγμα, μπορεί ο χρήστης ελέγξει την θερμοκρασία του σπιτιού ελέγχοντας το θερμοστάτη του σπιτιού του μέσω μιας εγφαρμογής, ενώ βρίσκεται στην άλλη πλευρά της χώρας περιμένοντας την πτήση από ένα επαγγελματικό ταξίδι ή μπορεί να λάβει δεδομένα υγείας απευθείας στο τηλέφωνό σχετικά με την προπόνηση που μόλις ολοκλήρωσε.

Τα δεδομένα είναι αυτά που επιτρέπουν την πραγματοποίηση αυτών των αλληλεπιδράσεων, ώστε να πιστεύουμε ότι η ασφάλεια και το απόρρητο των δεδομένων αποτελούν κορυφαίες ανησυχίες για τους κατασκευαστές IoT και τους χρήστες.

Εικόνα 17 : Cloud – Συνδεσιμότητα

Όμως, αυτό το κύμα νέων έξυπνων συσκευών έχει κόστος: η γρήγορη ταχύτητα ανάπτυξης προϊόντων δεν επιτρέπει πάντα αρκετό χρόνο για λόγους ασφαλείας. Και, με τόσα δεδομένα που ρέουν μέσα και έξω από όλες αυτές τις συσκευές IoT, υπάρχει μια σημαντική ευκαιρία για τα δεδομένα να καταλήξουν σε λάθος χέρια.[86]

Δεδομένων των δισεκατομμυρίων συσκευών που χρησιμοποιούνται σε καθημερινή βάση, οι επενδύσεις στην εξασφάλιση υποδομής, ασφάλειας του IoT θα πρέπει να αποτελούν κορυφαία προτεραιότητα για τους κατασκευαστές, αλλά στην πραγματικότητα αυτό δεν συμβαίνει. Αντ' αυτού, η ασφάλεια δεδομένων και το απόρρητο είναι τα μεγαλύτερα ζητήματα στον σύγχρονο έξυπνο κόσμο. Τα δεδομένα μεταδίδονται, υποβάλλονται σε επεξεργασία και αποθηκεύονται συνεχώς από οργανισμούς και ιδιώτες, χρησιμοποιώντας μια ποικιλία συσκευών IoT - από έξυπνες τηλεοράσεις έως αυτοκίνητα με δυνατότητα Wi-Fi και όλα τα ενδιάμεσα. Τα δεδομένα προέρχονται από τη συσκευή και στη συνέχεια αποθηκεύονται στο cloud. Από εκεί, τα δεδομένα χρησιμοποιούνται για την ανάπτυξη αναλυτικών στοιχείων που στη συνέχεια παραδίδονται σε μια ποικιλία χρηστών. Το μεγαλύτερο ζήτημα το οποίο προκύπτει είναι ότι αυτά τα δεδομένα αποστέλλονται συχνά χωρίς καμία κρυπτογράφηση, θέτοντάς τα σε κίνδυνο έκθεσης, κλοπής ή παραβίασης. Για να το διευκρινιστεί αυτό, εξετάζονται αυτές οι κοινές εφαρμογές IoT:

- **Ασφάλεια σπιτιού:** Εάν υπάρχει μια συσκευή ασφαλείας βίντεο στην μπροστινή πόρτα, χρησιμοποιεί το IoT για να στείλει στιγμιότυπα οποιουδήποτε ατόμου χτυπάει το κουδούνι, απευθείας στην εφαρμογή στο smartphone. Εάν η οικιακή συσκευή ασφαλείας δεν κρυπτογραφήσει αυτά τα δεδομένα, ένα τρίτο μέρος - όπως η αστυνομία - θα μπορούσε να αποκτήσει πρόσβαση στο "αρχείο καταγραφής επισκεπτών" χωρίς να το γνωρίζει ο χρήστης. Με κρυπτογράφηση, τα στιγμιότυπα / βίντεο δεν θα ήταν προσβάσιμα από τον κατασκευαστή και, επομένως, όλα τα μη εξουσιοδοτημένα τρίτα μέρη, δεν θα μπορέσουν, τελικά να θέσουν τον έλεγχο αυτών των ευαίσθητων δεδομένων στα χέρια τους.
- **Φορητές συσκευές γυμναστικής:** Η φορητή τεχνολογία - όπως τα smartwatches ή fitnesstrackers - είναι μια από τις πιο γνωστές εφαρμογές του IoT. Αυτά τα gadget συλλέγουν μεγάλες ποσότητες δεδομένων από τον χρήστη, όπως καρδιακό ρυθμό, αρτηριακή πίεση, επίπεδα οξυγόνου στο αίμα και πολλά άλλα. Αυτά τα δεδομένα έχουν αποδειχθεί πολύτιμα για τη βιομηχανία υγειονομικής περίθαλψης επειδή μπορούν να χρησιμοποιηθούν για την πρόληψη ασθενειών και για γενική έρευνα. Παρά αυτά τα οφέλη για τη βιομηχανία υγειονομικής περίθαλψης και για τους χρήστες, πολλές συσκευές γυμναστικής έρχονται επίσης με σημαντική έλλειψη ασφάλειας και απορρήτου δεδομένων χρήστη. Εάν αυτές οι συσκευές χρησιμοποιούσαν κρυπτογράφηση, οι κατασκευαστές θα μπορούσαν να διασφαλίσουν ότι τα δεδομένα χρήστη είναι προσβάσιμα μόνο για εξουσιοδοτημένους χρήστες.
- **GPS Trackers:** Η παρακολούθηση των τοποθεσιών των παιδιών, των κατοικίδιων ζώων ή ακόμα και των ηλικιωμένων είναι δυνατή από το IoT. Οι ιχνηλάτες GPS που στέλνουν τις ακριβείς συντεταγμένες θέσης πίσω στη συνδεδεμένη συσκευή, δίνουν ηρεμία για την ασφάλεια των αγαπημένων προσώπων. Αλλά, ένα σημαντικό ελάττωμα ασφαλείας μπορεί να έχει ως αποτέλεσμα να προσπελαστούν από τρίτους, χιλιάδες ή ακόμα εκατομμύρια τέτοιες συσκευές, τα δεδομένα των οποίων (συσκευών) αποστέλλονται χωρίς κρυπτογράφηση από τις συσκευές στο cloud. Αυτό σημαίνει ότι αυτές οι συσκευές είναι ένας εύκολος στόχος για χάκερ που βρίσκεται σε θέση να ελέγχει την τοποθεσία που αναμεταδίδει η συσκευή GPS ανά πάσα στιγμή. Αν η κρυπτογράφηση είχε τοποθετηθεί στην ασφάλεια αυτών των συσκευών από την αρχή, οι κάτοχοι συσκευών θα μπορούσαν να ελέγχουν ποιος έχει πρόσβαση στα δεδομένα τοποθεσίας των αγαπημένων τους.

Από πλευράς απορρήτου, αυτά τα παραδείγματα είναι ανησυχητικά επειδή τα δεδομένα των ατόμων κοινοποιούνται - και συχνά πωλούνται σε - διάφορους οργανισμούς χωρίς τη γνώση του χρήστη. Για να λάβουμε υπόψη τους οργανισμούς των οποίων η δραστηριότητα είναι η πώληση ή η ανάλυση δεδομένων που δημιουργούνται από συσκευές IoT, απαιτούνται κανόνες και κανονισμοί απορρήτου για την ανωνυμοποίηση ευαίσθητων δεδομένων που μπορούν να αναγνωρίσουν προσωπικά άτομα. Καθώς εισάγονται περισσότεροι κανονισμοί απορρήτου, όπως ο νόμος περί απορρήτου των καταναλωτών της Καλιφόρνια (CCPA).Οι κατασκευαστές IoT θα πρέπει να θεωρήσουν την κρυπτογράφηση ως τρόπο όχι μόνο για τη διατήρηση του απορρήτου των δεδομένων, αλλά και για τη μελλοντική απόδειξη της επιχείρησής τους και την τήρηση των κανονιστικών προτύπων. Για απόλυτη ασφάλεια, κάθε σημείο δεδομένων πρέπει να προστατεύεται με κρυπτογράφηση που βασίζεται σε δεδομένα και στοιχεία ελέγχου απορρήτου που ταξιδεύουν με τα δεδομένα από τη στιγμή που δημιουργούνται από τη συσκευή IoT. Η κρυπτογράφηση προστατεύει και απομονώνει την πρόσβαση στα δεδομένα μεταξύ χρηστών, εταιρειών και τρίτων. Η κρυπτογράφηση βοηθά επίσης τους οργανισμούς να οικοδομήσουν εμπιστοσύνη με τους χρήστες όσον αφορά την κοινή χρήση ευαίσθητων πληροφοριών με τα σωστά άτομα.

Προχωρώντας προς τα εμπρός, οι οργανισμοί πρέπει να δώσουν προσοχή και να προτεραιότητα στους τρόπους με τους οποίους η κρυπτογράφηση του IoT μπορεί να τροφοδοτήσει με ασφάλεια την επόμενη γενιά συσκευών. Όπως φαίνεται, η μεγαλύτερη απειλή για το μέλλον του IoT είναι η έλλειψη προστασίας δεδομένων. Ευτυχώς, υπάρχει μια λύση. Με κρυπτογράφηση με επίκεντρο τα δεδομένα, τα δεδομένα IoT προστατεύονται από τη στιγμή που δημιουργούνται, ανεξάρτητα από το πού κοινοποιούνται.

Προκειμένου να πετύχει στο μέλλον, καθώς η αγορά του IoT γίνεται ακόμη πιο ανταγωνιστική - και καθώς οι κανονισμοί απορρήτου σφίγγονται - οι πάροχοι λύσεων πρέπει να διασφαλίζουν καλύτερη προστασία δεδομένων με κεντρική ασφάλεια δεδομένων. Όμως, για μικρές εταιρείες με περιορισμένους προϋπολογισμούς και πόρους, η ασφαλής ανάπτυξη εφαρμογών για κινητά ή εφαρμογών IoT που είναι έτοιμες για web μπορεί να είναι αρκετά δύσκολη.

Για να διατηρηθεί ένας γρήγορος ρυθμός καινοτομίας διασφαλίζοντας ότι οι νέες εξελίξεις IoT είναι ασφαλείς, οι πάροχοι λύσεων μπορούν να βασίζονται σε λογισμικά κρυπτογράφησης για να ενσωματώσουν την προστασία δεδομένων στην εφαρμογή τους, χωρίς να απαιτείται καμία κρυπτογραφική εμπειρογνωμοσύνη. Η προστασία των δεδομένων με επίμονη κρυπτογράφηση και διαχείριση κλειδιών που έχουν δοκιμαστεί από τον

κλάδο είναι πλέον δυνατή με την πλατφόρμα προστασίας δεδομένων που είναι ενσωματωμένη στις εφαρμογές IoT.

3.2 Μελέτη περίπτωσης έξυπνων σπιτιών

Ένα όλο και πιο πολύ αυξανόμενο φαινόμενο, που πλέον αποτελεί το σύνηθες σε πολλές από τις λεγόμενες ανεπτυγμένες χώρες, είναι η ύπαρξη των έξυπνων σπιτιών (smart home). Τι είναι όμως ένα έξυπνο σπίτι και γιατί έχει κάνει την εμφάνιση του;

Ξεκινώντας από την δεύτερη ερώτηση η απάντηση μπορεί να είναι όσο απλή όσο λέγοντας πως η εξέλιξη της τεχνολογίας μας επίτρεψε την δημιουργία του έξυπνου σπιτιού και οι ευκολίες και παροχές που έρχονται με αυτό έχουν ξεκινήσει να μπαίνουν στη ζωή μας από τις αρχές τις χιλιετίας. Η ιδέα και η υλοποίηση του έξυπνου σπιτιού είναι η επιτομή του Internet of Things.

Ένα έξυπνο ή αλλιώς αυτόματο σπίτι έχει ως κύριο χαρακτηριστικό την συνδεσιμότητα των συσκευών οι οποίες περιέχονται σε αυτό. Η σύνδεση αυτή μεταξύ των συσκευών γίνεται κυρίως με τη χρήση ενός κοινού τοπικού δικτύου (LAN). Πως όμως λειτουργεί στην πραγματικότητα; Αρχικά, έχουμε μια σειρά από αισθητήρες που έχουν εγκατασταθεί στο σπίτι και μπορούν να παρακολουθούν τη συμπεριφορά του κατοίκου και την αλληλεπίδρασή του με τις οικιακές συσκευές. Δεύτερον, οι συσκευές υποστήριξης μπορούν να πραγματοποιήσουν το είδος των δράσεων που ένας κατοίκον φροντιστής θα μπορούσε να εκτελέσει, όπως να ανάψουν και να κλείσουν τα φώτα ή να χειριστούν την κουζίνα. Τρίτον, έχουν ένα δίκτυο επικοινωνίας που συνδέει όλους τους αισθητήρες και τις συσκευές υποστήριξης. Το δίκτυο έχει ενσωματωμένα υπολογιστικά εργαλεία που μπορούν να εφαρμόζουν αλγορίθμους που χρησιμοποιούν τα δεδομένα του αισθητήρα για να λάβει μια απόφαση για το πώς πρέπει να αντιδράσει

Συσκευές που μπορούν να βρεθούν σε ένα αυτόματο σπίτι είναι συνήθως ασύρματα συστήματα αναπαραγωγής ήχου, κάμερες ασφαλείας, συστήματα πυρασφάλειας, θερμοστάτες, ψυγεία, φωτορυθμικά, αυτόματες ηλεκτρονικές κλειδαριές, και άλλες έξυπνες οικιακές συσκευές όπως Alexa της Amazon και το Google Home.

Αυτό που επιτυγχάνουμε με την συνδεσιμότητα όλων αυτών των συσκευών είναι η ικανότητα διαχείρισης αυτών με την χρήση μιας και μόνο εφαρμογής μέσω ενός smartphone από την οποία ελέγχεται και ρυθμίζεται κάθε πιθανή παράμετρος των συνδεδεμένων

συσκευών, επιτρέποντας στον χρήστη να έχει πλήρη απομακρυσμένο έλεγχο του σπιτιού του. Μερικές από τις λειτουργίες που μπορεί να παρέχει το έξυπνο σπίτι είναι οι παρακάτω : το έξυπνο ψυγείο το οποίο θα στείλει ενημέρωση στην εφαρμογή όταν η ποσότητα προμηθειών θα μειωθεί, η κατάλληλη ρύθμιση του θερμοστάτη για εξοικονόμηση ενέργειας, η αυτόματη λειτουργία της καφετιέρας κάθε πρωί στην προκαθορισμένη ώρα που έχει επιλέξει ο χρήστης, δίνει τον απόλυτο έλεγχο σε συστήματα ασφάλειας, θέρμανσης, φωτισμού, ηλεκτρικών συσκευών, περιεχομένων multimedia και χιλιάδες άλλες επιλογές που ξεδιπλώνονται όσο οι κατασκευή των συσκευών γίνεται εξυπνότερη και πιο ευρηματική προκειμένου να καλύψει όλες τις καθημερινές μας ανάγκες.

Επιπλέον, για μεγαλύτερη άνεση και ευκολία μπορούν να προγραμματιστούν πιθανά σενάρια τα οποία εφαρμόζονται με το πάτημα ενός πλήκτρου στο κινητό ή με την λειτουργία έναν διακόπτη. Πιθανά σενάρια μπορεί να είναι:

- Διακοπές: Όταν ο χρήστης σκοπεύει να είναι μακριά από το σπίτι του για εκτεταμένο χρονικό διάστημα με αυτή την επιλογή θα μπορεί να θέτει σε λειτουργία τον φωτισμό στο σπίτι ή την άμεση μετάδοση εικόνας από τις κάμερες ασφαλείας του σπιτιού
- Απενεργοποίηση: Καθώς ο χρήστης φεύγει από το σπίτι δεν θα χρειάζεται να ελέγχει εκτενώς τις ηλεκτρικές του συσκευές, έναντι, με ένα πάτημα του κουπιού έχει ήδη καθορίσει ποιες συσκευές θα απενεργοποιούνται αυτόματα, ποια φώτα θα σβήσουν και ποια θα ανοίξουν
- Επιστροφή: Κατά την επιστροφή του στο σπίτι με αυτή την επιλογή έχει ήδη ρυθμίσει πως θέλει να ενημερώνεται στην εφαρμογή του για τα διαθέσιμα προϊόντα μέσα στο "έξυπνο" ψυγείο του και να προκύπτει μια λίστα με τις ελλείψεις που υπάρχουν, ενώ συγχρόνως θα ενεργοποιείται η εσωτερική θέρμανση του σπιτιού στη επιθυμητή θερμοκρασία.

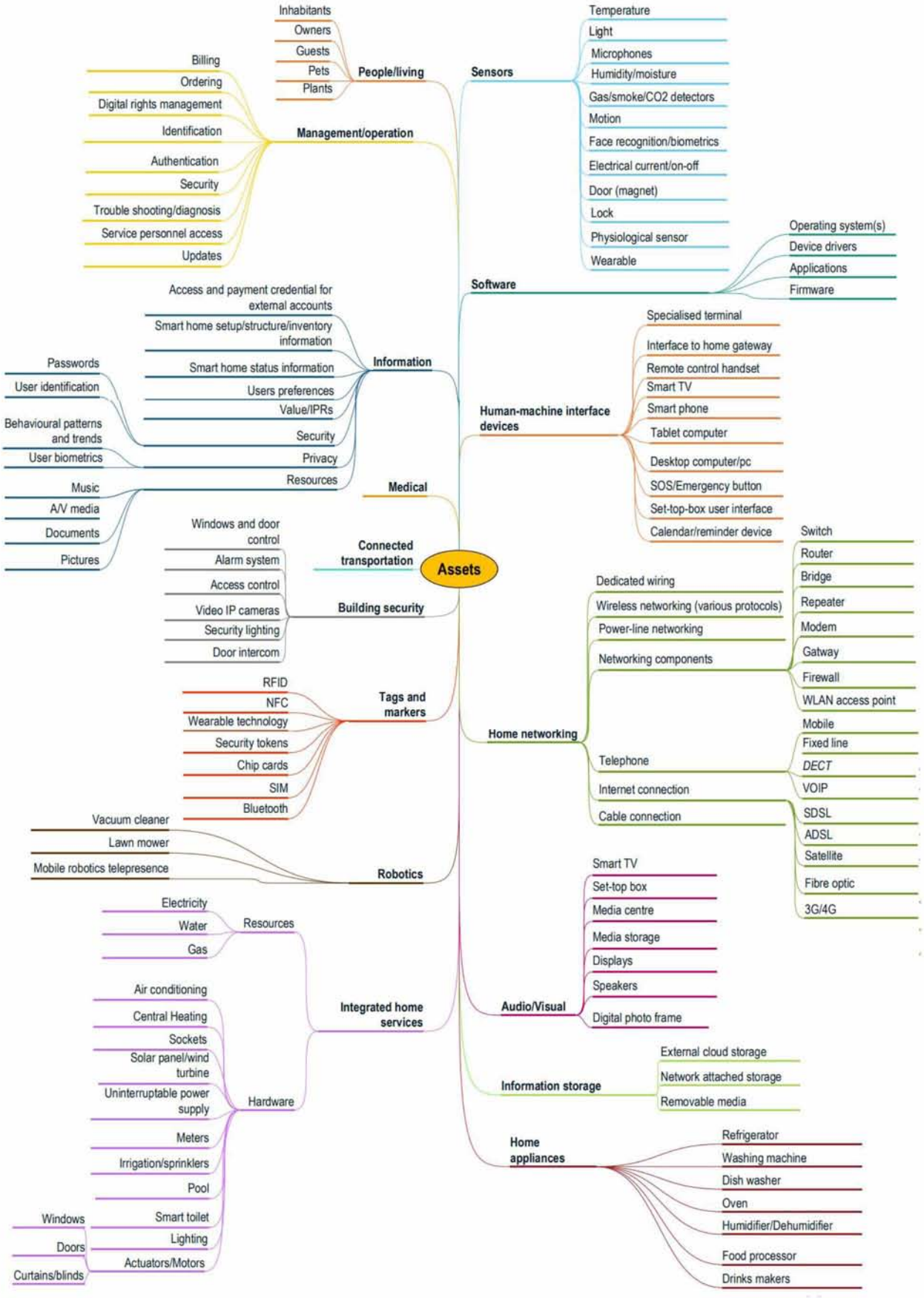
Ένα έξυπνο σπίτι προσφέρει πλήθος λειτουργιών οι οποίες κατοχυρώνουν μεγαλύτερη ασφάλεια και προστασία της ιδιοκτησίας σας με εξελιγμένους τρόπους που προηγουμένως ήταν ανέφικτοι. Για παράδειγμα με τα συστήματα ασφαλείας οι ένοικοι μπορούν:

- Να ειδοποιηθούν ότι επιχειρείται διάρρηξη και παράλληλα να προκληθεί πανικός στους επίδοξους διαρρήκτες ενεργοποιώντας την σειρήνα και τον φωτισμό σε ολόκληρο το σπίτι. Το σύστημα μπορεί να ειδοποιήσει τον ιδιοκτήτη στο κινητό του τηλέφωνο, το Κέντρο Λήψεων Σημάτων και εφόσον έχει γίνει η σχετική ρύθμιση ειδοποιείται αυτόματα και η αστυνομία.
- Αν αντιληφθούν ύποπτες κινήσεις και θορύβους κατά την διάρκεια της νύχτας, να πραγματοποιήσουν φωταψία σε ολόκληρη την οικία με το πάτημα ενός διακόπτη.
- Να ειδοποιηθούν από το σύστημα για πλημμύρα, πυρκαγιά, ακραία καιρικά φαινόμενα, βλάβες του ηλεκτρομηχανολογικού εξοπλισμού κ.α.
- Να έχουν οπτική αναπαράσταση της οικίας τους μέσω εγκατάστασης μίας ή περισσότερων καμερών οι οποίες θα μεταφέρουν την εικόνα του σπιτιού στον υπολογιστή ή στο κινητό.

3.2.1 Assets – Στοιχεία έξυπνου σπιτιού

Το παρακάτω σχεδιάγραμμα (Εικόνα 17) παρέχει μια επισκόπηση των έξυπνων οικιακών στοιχείων που συντελούν το έξυπνο σπίτι και άρα απαιτούν προστασία. Αυτή η κατηγοριοποίηση επομένως χρησιμεύει για να χτιστεί ένα ευρύ πλάνο της τοπολογίας και της πιθανής συνδεσμολογίας υλικών μέσα σε ένα σπίτι. Πολλά από αυτά τα στοιχεία θα μπορούσαν να αποσυντεθούν περαιτέρω σε στοιχεία και υπο-διεργασίες, αλλά δεν κρίνεται σκόπιμο, καθώς η κατηγοριοποίηση εδώ προσπαθεί να επιτύχει μια ισορροπία μεταξύ βασικές σημαντικές κατηγορίες και σχετικές λεπτομέρειες. Κάθε ένα κομμάτι της παρακάτω συνδεσμολογίας μπορεί να αποτελέσει στόχο εισβολής από κακόβουλους χρήστες και στη συνέχεια να οδηγήσει στη περεταίρω επέκταση σε ολόκληρο το σύστημα. Σε αυτή την τοπολογία απειλών έχουν εντοπιστεί οι ακόλουθες ομάδες στοιχείων: Αισθητήρες, λογισμικό, συσκευές διεπαφής, οικιακή δικτύωση, οπτικοακουστικό, αποθήκευση πληροφοριών, οικιακές συσκευές, ολοκληρωμένες οικιακές υπηρεσίες, ρομποτική, ετικέτες και δείκτες, ασφάλεια κτιρίων, συνδεδεμένες μεταφορές, πληροφορίες, διοίκηση / διεργασία και άνθρωποι / διαβίωση. Πάνω σε αυτές τις κατηγορίες γίνεται η τμηματοποίηση επιπλέον στοιχείων-υποκατηγορίες. Π.χ., στην ομάδα στοιχείων των αισθητήρων, περιλαμβάνουμε στοιχεία όπως η θερμοκρασία, τα φώτα, τα μικρόφωνα κ.λπ. Αυτός ο κατάλογος στοιχείων έχει αναπτυχθεί από μια εξέταση κοινών μοντέλων πραγματικών και δυνατοτήτων στα

έξυπνα σπίτια, καθοδηγούμενοι από της εξέλιξη των συσκευών που περιλαμβάνονται στο IoT. Είναι λογικό πως το παρακάτω σχεδιάγραμμα αποτελεί μια όσο δυνατόν πιο πλήρη εικόνα όλων των πιθανών πτυχών που μπορούν να υπάρχουν σε ένα έξυπνο σπίτι, χωρίς φυσικά αυτό να σημαίνει πως τα έξυπνα σπίτια θα περιέχουν απαραίτητα όλα αυτά τα στοιχεία. Ανεξάρτητα από τις διαφορετικές κατηγορίες στοιχείων σε κάθε σπίτι, αυτές οδηγούν σε περίπλοκα περιβάλλοντα ακόμη και μέσα ένα ενιαίο σπίτι, δεδομένου ότι παράγονται από διαφορετικούς κατασκευαστές, κάνοντας την εναρμόνισή της και την προστασία της μια μεγάλη διαδικασία. Η έξυπνη οικιακή τεχνολογία, εξακολουθεί να αναπτύσσεται, και να αναπτύσσονται νέες εφαρμογές μαζί με την εξέλιξη του IoT γεγονός που συνέχεια οδηγεί στην αλλαγή των δεδομένων. [86]



Εικόνα 18 : Επισκόπηση των έξυπνων οικιακών στοιχείων και πολυμέσων

3.2.2 Threats – Απειλές έξυπνου σπιτιού

Όλες αυτές οι παροχές φαίνονται ιδανικές, αλλά, υπάρχει μια μεγάλη απειλή και αρνητική μεταβλητή στην προκειμένη περίπτωση και αυτή είναι η ευρεία συνδεσιμότητα που υπάρχει μεταξύ των συσκευών. Το μεγαλύτερο ατού ενός έξυπνου σπιτιού είναι και το μεγαλύτερο αρνητικό που παρουσιάζεται ενόψει μιας επερχόμενης επίθεσης. Για τους απεικόνιση του εύρους απειλών για ένα έξυπνο σπίτι, αναπτύχθηκε το παρακάτω σχεδιάγραμμα (Εικόνα 18). Οι απειλές που περιλαμβάνονται σε αυτήν τη συλλογή ισχύουν για τα έξυπνα οικιακά στοιχεία που παρουσιάζονται προηγουμένως. Η παρουσιαζόμενη ταξινόμηση καλύπτει κυρίως απειλές για την ασφάλεια στον κυβερνοχώρο, δηλαδή, απειλές που ισχύουν για τα στοιχεία τεχνολογίας πληροφοριών και επικοινωνιών. Μερικές επιπλέον απειλές εκτός από αυτές που περιλαμβάνονται στον τομέα της πληροφορικής υπάρχουν σε αυτή τη λίστα, όπως πχ φυσικές καταστροφές. Σε αυτό το σχεδιάγραμμα απειλών μπορούν να εντοπιστούν οι ακόλουθες κατηγορίες: Φυσικές επιθέσεις, αθέλητη ζημιά, καταστροφές, ζημιές / απώλειες στα υλικά πληροφορικής, δυσλειτουργίες, υποκλοπές / πειρατεία, δόλια δραστηριότητα / κατάχρηση κτλ. Οι αναγνωρισμένες απειλές και οι υπο-απειλές κατηγοριοποιούνται και παρατίθενται σε αυτές τις ομάδες απειλών. Πιο αναλυτικά έχουμε:

DoS: Η παραδοσιακή άρνηση υπηρεσίας και οι κατανεμημένες επιθέσεις άρνησης υπηρεσίας σε συστήματα πληροφοριών μπορεί να είναι απειλές για το έξυπνο σπίτι, δεδομένου ότι όλες οι οικιακές συσκευές συνδέονται με το διαδίκτυο. Τέτοιες επιθέσεις μπορεί να είναι το πρώτο βήμα για την αφαίρεση ενός έξυπνου σπιτιού από ένα δίκτυο, προκειμένου να εκμεταλλευτεί μια ευπάθεια των συσκευών του συστήματος ενώ αυτό βρίσκεται σε αποσυνδεδεμένη κατάσταση.

Φυσικές απειλές: Η πλειονότητα των έξυπνων οικιακών asset είναι αντικείμενα που μπορεί να υποστούν φυσική ζημιά, και πολλά έχουν αυξημένη οικονομική αξία παρακινώντας στην κλοπή τους. Αυτά τα έξυπνα οικιακά assets είναι επομένως ευάλωτα σε φυσικές επιθέσεις, οι οποίες ενδέχεται να τα αφαιρέσουν από τον κάτοχό τους (κλοπή) ή να τα καταστρέψουν, υποβιβάζοντας ή αποτρέποντάς τους λειτουργικότητα. Οι φυσικές επιθέσεις μπορούν να διαταράξουν τις επικοινωνίες μεταξύ των διαφόρων στοιχείων ενός έξυπνου σπιτιού. Ορισμένα αντικείμενα, κύριας σημασία για τη λειτουργικότητα της όλης δομής όπως τηλέφωνα, tablet, αφαιρούμενα μέσα αποθήκευσης και υπολογιστές, μπορεί να κινηθούν φυσικά μέσα και έξω από το σπίτι, καθιστώντας τα πιο ευάλωτα στους εξωτερικούς χώρους.

Αθέλητες απειλές: Πολλά στοιχεία ενός έξυπνου σπιτιού χρησιμοποιούν machine learning και AI προκειμένου να αναλύσουν τις επιθυμείς και συνήθειες του χρήστη ώστε μελλοντικά να βελτιώσουν τις αποδόσεις τους. Εδώ προκύπτει το πρόβλημα πως πολλοί διαφορετικοί χρήστες αλλά και επισκέπτες μπορεί να υπερτροφοδοτήσουν το πρόγραμμα με περισσότερες πληροφορίες από όσες αναμένει τυπικά το σύστημα. Επίσης ο ανεπαρκής σχεδιασμός είναι βασικό ζήτημα για τα έξυπνα σπίτια, καθώς μπορούν να προκαλέσουν προβλήματα στην ασφάλεια και ιδιωτικότητα. Ανεπαρκής σχεδιασμός μπορεί να συμβεί σε επίπεδο εξαρτημάτων και υπηρεσιών έξυπνου σπιτιού όπως και στο το επίπεδο της γενικής εγκατάστασης και ολοκλήρωσης του έξυπνου σπιτιού στο σύνολό του. Σε επίπεδο υλικού, ο κακός σχεδιασμός ασφάλειας μπορεί να κυμαίνεται από έλλειψη μεθόδων ασφαλείας έως ανεπαρκή εφαρμογή της ασφάλειας.

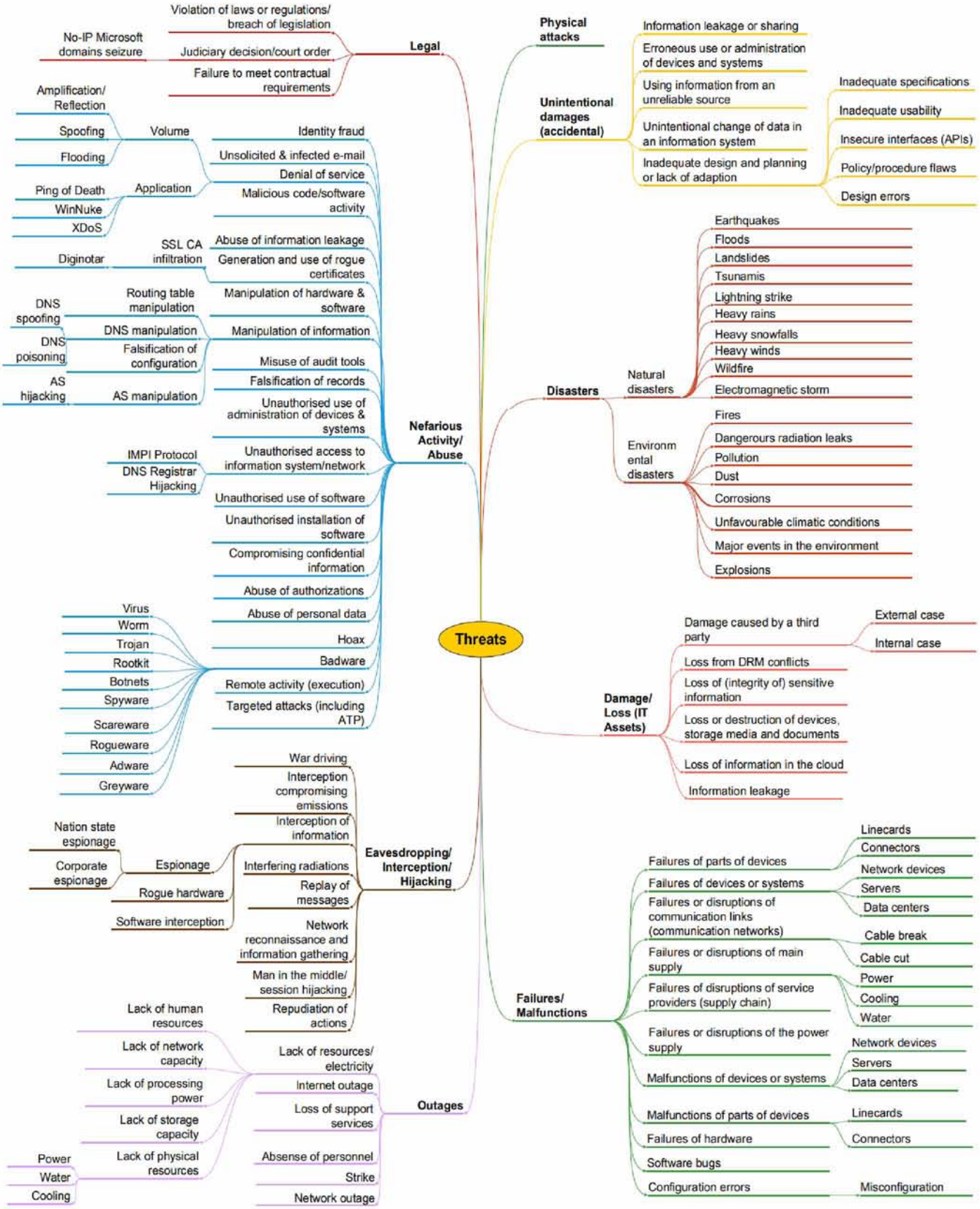
Απειλές από αστοχίες και δυσλειτουργίες: Τα έξυπνα σπίτια και οι συσκευές τους είναι σύνθετα συστήματα, που βασίζονται σε διαφορετικές εισόδους και είναι ευάλωτες σε αστοχίες και δυσλειτουργίες. Σε πολλές περιπτώσεις η αποτυχία ή η δυσλειτουργία έχει ως αποτέλεσμα η έξυπνη οικιακή υπηρεσία να μην είναι πλέον διαθέσιμη. Σε ορισμένες περιπτώσεις αυτό θα είναι μια μικρή ενόχληση, για παράδειγμα, η αδυναμία πρόσβασης στο δίκτυο, αλλά σε άλλες περιπτώσεις μπορεί να οδηγήσει σε δαπανηρή ζημία, για παράδειγμα πόρτες που έχουν κλειδώσει και δεν μπορούν να ανοίξουν χωρίς επισκευή. Η ανάκτηση από αστοχία μπορεί να περιπλέκεται από το σχεδιασμό του συστήματος. Για παράδειγμα, μια συσκευή ενδέχεται να πρέπει να επαναφερθεί φυσικά ή να επανεκκινηθεί από τον χρήστη, ο οποίος μπορεί να βρίσκεται σε απομακρυσμένη τοποθεσία.

Απειλές υποκλοπής: Πολλές έξυπνες οικιακές συσκευές δεν διαθέτουν αποκλειστικό λογισμικό ασφαλείας και ασφαλείς κρυπτογραφημένες επικοινωνίες (λόγω έλλειψης επεξεργακτικής ισχύς ή ηλεκτρικής ισχύος, το πρόσθετο κόστος και μειωμένη ευκολία προσθήκης κρυπτογράφησης). Αυτό αυξάνει την πιθανότητα διαρροής πληροφοριών. Η υποκλοπή, η παρακολούθηση και η "πειρατεία" είναι βασικές απειλές για τα έξυπνα σπίτια. Τα έξυπνα σπίτια διαθέτουν υψηλά επίπεδα επικοινωνίας μεταξύ διαφορετικών συσκευές σε μια σειρά πρωτοκόλλων και τεχνολογιών. Αυτά περιλαμβάνουν ασύρματα πρωτόκολλα όπως όπως Wi-Fi, Zigbee, Bluetooth και άλλα. Οι τελικές συσκευές δεν διαθέτουν ισχύ επεξεργασίας για κρυπτογράφηση στο σπίτι, που τις καθιστά πολύ ευάλωτες σε δίαφορα είδη επιθέσεων όπως για παράδειγμα man in the middle που αναφε\έρθηκε πιο πάνω. και τον έλεγχο τα gadget όταν βρίσκονται σε φυσική γειτνίαση. Επιπλέον, πολλές έξυπνες οικιακές

συσκευές από διαφορετικούς κατασκευαστές, χρησιμοποιούν διαφορετική ασύρματη επικοινωνία. Τα πρωτόκολλα ενδέχεται να αλληλεπιδρούν μεταξύ τους ή να ανταγωνίζονται για το ίδιο εύρος ζώνης λειτουργίας. Πολλαπλά έξυπνα σπίτια σε κοντινή απόσταση μπορεί να αντιμετωπίσουν παρεμβολές μεταξύ Wi-Fi στο ίδιο κανάλι προκαλώντας υποβάθμιση της ποιότητας του σήματος γεγονός που διευκολύνει την διαδικασία της ανυποψίαστης υποκλοπής δεδομένων.

Συνεχίζοντας στο κομμάτι των υποκλοπών κρίνεται σκόπιμο να γίνει μια μικρή αναφορά στο πως λειτουργεί μια επίθεση "man in the middle" Οι επιθέσεις man-in-the-middle περιλαμβάνουν έναν εισβολέα που κάνει ανεξάρτητες συνδέσεις με δύο μέρη ή συσκευές και αναμεταδίδει τις επικοινωνιών μεταξύ τους. Αυτό επιτρέπει στον εισβολέα να παρακολουθεί την επικοινωνία των συστημάτων και να ελέγχει άλλα στοιχεία της επικοινωνίας. Όπως αναφέρθηκε οι συσκευές που δεν διαθέτουν σωστά εφαρμοσμένες κρυπτογραφημένες επικοινωνίες και έλεγχος ταυτότητας τελικού σημείου, είναι ευάλωτες σε τέτοιες επιθέσεις . Τέτοιες αδυναμίες που θα μπορούσαν να επιτρέψουν την υλοποίηση μιας τέτοιας επίθεσης έχουν εντοπιστεί στα πρωτόκολλα ZigBee. [86]

Κλοπή ταυτότητας: Τα συστήματα έξυπνων σπιτιών μπορούν να αποθηκεύουν και να διαχειρίζονται πιστοποιητικά για διάφορες λειτουργίες και υπηρεσίες τις οποίες το σπίτι παρέχει και χρησιμοποιεί. Αυτά τα πιστοποιητικά μπορεί να προορίζονται για εσωτερική χρήση (λογαριασμοί χρηστών, δικαιώματα, προτιμήσεις και ρυθμίσεις ή δεδομένα πρόσβασης) ή εξωτερική (λογαριασμοί πολυμέσων, cloud αποθήκευση, αγορές και παράδοση στο σπίτι, συναγερμοί ασφαλείας). Αυτά τα πιστοποιητικά ενδέχεται να περιλαμβάνουν στοιχεία πληρωμής (πιστωτική κάρτα ή αριθμούς λογαριασμού) που είναι στόχοι για εγκληματίες στον κυβερνοχώρο με οικονομικά κίνητρα. Πληροφορίες σχετικά με τη συμπεριφορά των χρηστών, τις προτιμήσεις, συνήθειες, ταξίδια, χρήση πολυμέσων κ.λπ., που συλλέγονται και αποθηκεύονται στο έξυπνο σπίτι, μπορεί να βοηθήσουν διάφορες μορφές απάτης πλαστοπροσωπίας. Η πιο απλή, τοπική, μορφή απάτης ταυτότητας μπορεί να περιλαμβάνει τη μη εξουσιοδοτημένη χρήση λογαριασμών έξυπνων οικιακών χρηστών που ανήκουν σε άλλους κατοίκους.



Εικόνα 19 : Επισκόπηση απειλών προς τις έξυπνες συσκευές – έξυπνο σπίτι

Η μη εξουσιοδοτημένη πρόσβαση στο σύστημα πληροφοριών στο πλαίσιο του έξυπνου σπιτιού επιτρέπει την εξαγωγή πληροφοριών σχετικά με τους κατοίκους, συμπεριλαμβανομένων των συμπεριφορών, των προτιμήσεων και των πιστοποιητικών τους. Αυτό επιτρέπει στον εισβολέα να αλλάξει ρυθμίσεις και να εγκαταστήσει ή να χειριστεί λογισμικό. Η μη εξουσιοδοτημένη πρόσβαση επιτρέπει στον δράστη να αναπαραγάγει όλη τη δραστηριότητα που είναι διαθέσιμη στον νόμιμο χρήστη, και ως εκ τούτου για να ενεργεί σαν ένας κάτοικος. Στη συνέχεια, ο δράστης μπορεί να έχει πρόσβαση σε πολυμέσα και άλλες πληροφορίες και μπορεί να εξουσιοδοτήσει λήψεις αρχείων, αγορές κ.λπ. Μπορεί επίσης να τροφοδοτήσει με εσφαλμένες πληροφορίες τους αισθητήρες του σπιτιού. Ανάλογα με το βαθμό στον οποίο το έξυπνο σπίτι έχει πρόσβαση σε διαφορετικούς λογαριασμούς και υπηρεσίες αναλόγως εξαρτάται και ο βαθμός διείσδυσης που μπορεί να έχει ο κυβερνοεγκληματίας. [86]

3.2.3 Καλές πρακτικές στο σχεδιασμό ενός έξυπνου σπιτιού

Αρκετές καλές πρακτικές για μέτρα ασφαλείας περιλαμβάνουν τη λήψη καλών επιλογών και αποφάσεων στο επίπεδο του σχεδιασμού του έξυπνου σπιτιού ως σύστημα, συμπεριλαμβανομένου του πώς θα ενσωματωθούν μαζί οι διάφορες συσκευές. Αυτές οι καλές πρακτικές προτείνουν τρόπους με τους οποίους μπορεί να σχεδιαστεί το έξυπνο σπίτι προκειμένου να αυξηθεί η ασφάλεια και να μειωθούν οι επικείμενοι κίνδυνοι.

Οι σχεδιαστικές σκέψεις περιλαμβάνουν:

1. Προσεκτική εξέταση της ασφάλειας του έξυπνου σπιτιού που βασίζεται σε αποθήκευση στο cloud, και μεγιστοποίηση του βαθμού στον οποίο η αυτοματοποίηση και η αποθήκευση δεδομένων μπορούν να παραμείνουν στον έλεγχο του ιδιοκτήτη
2. Μείωση του αριθμού των εξωτερικών υπηρεσιών που χρησιμοποιούνται στο έξυπνο σπίτι ο σχεδιασμός των οποίων μπορεί να μειώσει τις επιλογές επίθεσης, χρησιμοποιώντας δηλαδή όσο το δυνατόν, λιγότερες και αξιόπιστες συσκευές. Αυτό διότι η χρήση ενός μόνο τύπου έξυπνης οικιακής τεχνολογίας μπορεί να ελαχιστοποιήσει τα σημεία ευπάθειας που προκύπτουν από την ανάμειξη πολλαπλών τεχνολογιών και πρωτοκόλλων
3. Επιλογή πρωτοκόλλων Open Source έναντι κλειστών ή ιδιόκτητων πρωτοκόλλων έτσι ώστε το η κάθε εφαρμογή να μπορεί να επιθεωρηθεί και να κατανοηθεί.

4. Καλύτερος σχεδιασμός έτσι ώστε οι οικιακοί χρήστες να μπορούν να κατανοήσουν καλύτερα τη λειτουργία των συσκευών τους και να ασκήσουν καλύτερα έλεγχο της δραστηριότητάς τους.

Καλές πρακτικές στη σχεδίαση συστημάτων

Αυτά τα μέτρα απευθύνονται στους κατασκευαστές συσκευών, αλλά μπορούν επίσης να καθοδηγήσουν την επιλογή συσκευών από έξυπνους σχεδιαστές και ιδιοκτήτες έξυπνων σπιτιών.

1. Αποφυγή προεπιλεγμένων (default) κωδικών πρόσβασης
2. Χρήση κωδικοποιημένης επικοινωνίας
3. Διασφάλιση προστασίας πυλών IP
4. End-to-end αυθεντικοποίηση και πρόσβαση μετά από έλεγχο
5. Συνεχές ενημερώσεις λογισμικού με καινούργια μέτρα προστασίας

Εικόνα 20 : Διαχείριση έξυπνου σπιτιού με μια εφαρμογή

Συμπεράσματα

Η ευρεία διάδοση των έξυπνων συσκευών πέρα από το ότι διευκολύνει την καθημερινότητα των σύγχρονων ανθρώπων τραβάει επίσης και την προσοχή επίδοξων κακόβουλων χρηστών οι οποίοι μέσα από αυτές βλέπουν έναν χώρο, ο οποίος ανοίγεται μπροστά τους με στόχο τη δημιουργία καινούργιων κακόβουλων λογισμικών. Αυτά τα λογισμικά εξελίσσονται σε μεγάλο βαθμό και είναι ικανά να προκαλούν μεγάλο αριθμό προβλημάτων στους χρήστες, από υποκλοπές προσωπικών πληροφοριών μέχρι και χρηματικές ζημιές. Κατά συνέπεια απαιτείται ιδιαίτερη προσοχή από τους κατόχους έξυπνων συσκευών με στόχο την έγκαιρη αντιμετώπιση των λογισμικών πριν κατορθώσουν να διεισδύσουν στις συσκευές τους, καθώς μετά από αυτό είναι εξαιρετικά δύσκολος ο εντοπισμός στην πλειοψηφία τους, δεδομένου ότι δημιουργούν μηχανισμούς απόκρυψης της ύπαρξης τους. Επίσης θα πρέπει να δημιουργηθούν λειτουργικά συστήματα βελτίωσης της ασφάλειας των προϊόντων με στόχο να προστατευτούν οι χρήστες.

Μέσα από την εκτέλεση εφαρμογής ανίχνευσης κακόβουλου λογισμικού μπορεί να αναδειχθεί με πρακτικό τρόπο η σημασία καθορισμένων δικλείδων ασφαλείας οι οποίες αποτελούν και την εύκολη πύλη εισόδου με στόχο να προβληθεί μία έξυπνη συσκευή. Επιπλέον, θα πρέπει να επισημανθεί ότι οι περισσότεροι επίδοξοι εισβολείς που πράττουν ηλεκτρονικά εγκλήματα στον κυβερνοχώρο επιλέγουν να κάνουν χρήση αποτελεσματικότερων τρόπων προσβολής έξυπνων συσκευών όχι απλά μέσω της απλής πρόσβασης στη συσκευή, αλλά ταυτόχρονα με την προσπάθεια να εκμεταλλευτούν μία ενδεχόμενη απροσεξία κάποιων χρηστών κατά τη διάρκεια της χρήσης. Για αυτό θα πρέπει οι χρήστες να είναι ιδιαίτερα προσεκτικοί όσον αφορά τη χρήση εφαρμογών και του διαδικτύου.

Καλή πρακτική θα είναι να εκτελούνται συχνά έλεγχοι για την επικαιροποίηση των εκδόσεων ασφαλείας στα συστήματα πού χρησιμοποιούνται εξασφαλίζοντας περισσότερες δυνατότητες ρυθμίσεων ασφαλείας για τη συσκευή. Ακόμα, θα πρέπει να προστατεύονται προσωπικά και ευαίσθητα δεδομένα, να θωρακίζεται με ασφάλεια οποιαδήποτε συσκευή με ειδικά προγράμματα και να χρησιμοποιούνται απαραίτητα ολοκληρωμένα και επώνυμα αντιικά προγράμματα προστασίας τα οποία προσφέρουν την ανίχνευση ενός κακόβουλου λογισμικού και έλεγχο στις ρυθμίσεις της συσκευής. Καθίσταται λοιπόν πλέον επιτακτική ανάγκη ευαισθητοποίησης των χρηστών έξυπνων συσκευών, έτσι ώστε να μπορούν να τηρούν την απαραίτητη εμπιστευτικότητα και να μην έχουν τη λάθος αντίληψη ότι η έκθεσή

τους στους επίδοξους εγκληματίες του κυβερνοχώρου προέρχεται μόνο από τη χρήση του υπολογιστή τους. Η χρήση της ασφάλειας που παρέχεται σήμερα από την τεχνολογία των έξυπνων συσκευών σε συνδυασμό με τη χρήση ολοκληρωμένων και αξιόπιστων λογισμικό προστασίας από κακόβουλα λογισμικά θα πρέπει να θεωρείται απαραίτητη. Τέλος απαραίτητη είναι και η απόκτηση επιμέρους κουλτούρας ασφαλείας από τους χρήστες με γνώμονα την αξιοπιστία και την ασφάλεια των προσωπικών τους δεδομένων τόσο κατά την εγκατάσταση όσο και κατά τη χρήση των λογισμικών στην έξυπνη συσκευή τους. Η ανάπτυξη κακόβουλου λογισμικού και η ασφάλεια συστημάτων είναι δύο ποσά ανάλογα που εξελίσσονται μέρα με τη μέρα και είναι δύσκολο να προβλέψουμε την πορεία τους, μπορούμε μόνο να μιλήσουμε για το παρόν τους και πως μας επηρεάζουν άμεσα σήμερα.

Αναφορές

1. Brechbuhl, H., Bruce, R., Dynes, S., & Johnson, E. (2010, January) Protecting Critical Information Infrastructure: Devloping Cybersecurity Policy, Information Technology for Development, 16(1), pp. 83-91,
2. Harknett, R., &Stever, J. (2011) The New Policy World of Cybersecurity, (N. Roberts, Ed.), Public Administration Review, pp. 455-460,
3. Favell, A. (Ed.) (2011, November 2) 96 Percent of Smartphones and Tablets Lack Necessary Security Software. Why It Matters to Your Business - A Lot, from MobiThinking: http://mobithinking.com/blog/mobile-security-business-implications,
4. Canalys (2011, October 04) Mobile Security Investment to Climb 44% Each Year Through 2015, from MobiThinking: http://mobithinking.com/blog/mobile-security-business-implications,
5. 2012 Best Mobile Security Software Comparisons and Reviews (2012), from Top Ten Reviews: http://mobile-security-software-review.toptenreviews.com/
6. McLaughlin, S., Enck, W. & McDaniel, P. (2009) Semantically rich, applicationcentric security in Android, Retrieved from Proceedings of teh 25th Annual Computer Security Applciations Conference (ACSAC '09): http://dl.acm.org,
7. Introduction to Cyber Crime http://www.inf.tsu.ru/WebDesign/libra3.nsf/161d3ebc95608f55c62571f5003467e9/3b47f7a6821 452fdc62572040016d843/$FILE/cybercrime.pdf,
8. Yuri Ilyin. 2014. Cybercrime, Inc.: how profitable is the business?. [BLOG] Kaspersky Available at: https://blog.kaspersky.com/cybercrime-inc-how-profitable-is-the-business/15034/ ,
9. "The History of Cyber Crime." *Le VPN*, 23 July 2020, www.le-vpn.com/history-cyber-crime-origin-evolution/,
10. "Convention on Cybercrime." *Wikipedia*, Wikimedia Foundation, 27 Jan. 2020, en.wikipedia.org/wiki/Convention_on_Cybercrime,
11. Ayala, Karissa, "Cybercrime" (2004). *LLM Theses and Essays*. 59. https://digitalcommons.law.uga.edu/stu_llm/59,
12. Adams, Jo-Ann M. 'Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet', Computer and High Technology Law, 12 (1996): 403-434,
13. Aldesco, Albert I. 'The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime', Loyola of Los Angeles Entertainment Law Review, vol. 23(2002): 81-123,
14. Brenner, Susan W. 'U.S. Cybercrime Law: Defining Offences', Information Systems Frontiers, 6(2004): 115-132,
15. Yar M (2005). The novelty of cybercrime: An assessment in light of routine activity theory. Eur. J. Criminol. 2 (4): 407- 427,
16. Wall DS (2001). Maintaining order and law on the internet. In: Wall DS (Ed.), Crime and the internet. London: Routledgepp. 167-183,
17. "White Hat (Computer Security)." *Wikipedia*, Wikimedia Foundation, 2 Oct. 2020, en.wikipedia.org/wiki/White_hat_(computer_security),
18. Yagoda, Ben. (2015). "A Short History of "Hack"". *The New Yorker*,

19. DuBois, Shelley.(2011). "A who's who of hackers". *Reporter*. Fortune Magazine,
20. Taylor, Paul A. (1999). *Hackers: Crime in the Digital Sublime*. Routledge,
21. Sean Michael Kerner (November 25, 2013). "How Was SQL Injection Discovered? The researcher once known as Rain Forrest Puppy explains how he discovered the first SQL injection more than 15 years ago",
22. «Viruslist.com». Αρχειοθετήθηκε από το πρωτότυπο στις 16 Οκτωβρίου 2006,
23. TechTarget.com, Wikipedia,
24. «What is a computer worm». , Wikipedia,
25. «What is the difference between a computer virus and a computer worm» (PDF). Αρχειοθετήθηκε από το πρωτότυπο (PDF) στις 10 Σεπτεμβρίου 2019,
26. https://bitdefender.gr/blog/ti_einai_o_ios_upologisth/,
27. About.com γιατουςιούς,Wikipedia,
28. «Computer Knowledge». Αρχειοθετήθηκε από το πρωτότυπο στις 6 Μαρτίου 2008,
29. Βασικές Αρχές Ασφάλειας Δικτύων: Εφαρμογές και Πρότυπα, WilliamStallings,
30. «Understanding Denial-of-Service Attacks»,Wikipedia,
31. «Internet PhishingAlert». Αρχειοθετήθηκε από το πρωτότυπο στις 10 Οκτωβρίου 2018,
32. Ramzan, Zulfikar (2010). «Phishing attacks and countermeasures». Στο: Stamp, Mark &Stavroulakis, Peter. *Handbook of Information and Communication Security*. Springer,
33. Gupta, Arushi; Kaushal, Rishabh (2015). "Improving spam detection in Online Social Networks". *2015 International Conference on Cognitive Computing and Information Processing(CCIP). www.ieee.org*. IEEE. pp. 1–6,
34. *Dan Tynan (3 April 2012). "Social spam is taking over the Internet". ITworld,*
35. https://fraudfighting.org/wp-content/uploads/2017/12/Web-Jacking.pdf,
36. Spitzberg, Brian H.; Hoobler, Gregory (February 2002). "Cyberstalking and the technologies of interpersonal terrorism" (PDF). *New Media & Society*. 1. **4**: 71–92. doi:10.1177/14614440222226271. S2CID 27102356,
37. Moore, Alexis A. "What is cyberstalking?". About.com,
38. *"The 12 types of Cyber Crime". Digit,*
39. Silverbug. "10 Types Of Cyber Crimes... And Another 10 You've Never Heard Of". *www.silverbug.it,*
40. Hébert, Monique; Pilon, Marilyn (1991). *Computer Crime*. Law and GovernmentDivision, Library of Parliament,
41. «Μορφές ηλεκτρονικών εγκλημάτων», ανακτήθηκε στις 16-10-2008 από τη διεύθυνση: http://www.elesme.gr/elesmegr/periodika/t19/t19 03.htm,
42. "Computer Security." *Wikipedia*, Wikimedia Foundation, 8 Oct. 2020, en.wikipedia.org/wiki/Computer_security,
43. "Ασφάλεια Πληροφοριακών Συστημάτων." *Wikipedia*, Wikimedia Foundation, 16 July 2020, el.wikipedia.org/wiki/ Ασφάλεια_πληροφοριακών_συστημάτων,

44. Βασιλακάκος, Δ. (2015). Κινητικότητα, Εξόρυξη Δεδομένων και Ιδιωτικότητα, Διπλωματική Εργασία, ΜΠΣ Σχεδίαση και Ανάπτυξη Διάχυτων Συστημάτων Υπολογισμού, Ελληνικό Ανοικτό Πανεπιστήμιο,
45. Μάγκος, Ε. (2013). Ασφάλεια Υπολογιστών και Προστασία Δεδομένων, Πανεπιστημιακές Σημειώσεις, Ιόνιο Πανεπιστήμιο,
46. *"What is Trojan horse? – Definition from Whatis.com"*,
47. Dunham, Ken; Melnick, Jim (2047). *Malicious Bots: An Inside Look into the Cyber-Criminal Underground of the Internet*. CRC Press,
48. Cisco 2018 Annual Cybersecurity Report,
49. http://www.sans.org/resources/glossary.php,
50. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf,
51. https://attack.mitre.org/wiki/Technique/T1067,
52. https://attack.mitre.org/wiki/Initial_Access,
53. "Android/Spy.Agent.SI [Threat Name] Go to Threat." *Android/Spy.Agent.SI | ESET Virusradar*, www.virusradar.com/en/Android_Spy.Agent.SI/description,
54. "Department of Computer Science and Technology." Department of Computer Science and Technology: The Computer Laboratory, www.cl.cam.ac.uk/,
55. nssbackend, |By. "Κακόβουλο Λογισμικό Κλέβει PIN Από Κινητά, Χρησιμοποιώντας Την Κάμερα Και Το Μικρόφωνο." *NSS*, 17 July 2018, www.nss.gr/el/news/470-smartphone-pins-skimmed-with-microphone-and-camera/,
56. Hughes, Larry J., (1961). Actually useful Internet security techniques,Indianapolis, Ind. : New Riders Pub,
57. Martellini, Maurizio; Malizia, Andrea (2017-10-30). *Cyber and Chemical, Biological, Radiological, Nuclear, Explosives Challenges: Threats and Counter Efforts*. Springer,
58. Axelsson, S (2000). "Intrusion Detection Systems: A Survey and Taxonomy",
59. *Vacca, John R. (2013-08-26). Network and System Security. Elsevier,*
60. Newman, Robert (2009-06-23). *Computer Security: Protecting Digital Resources*. Jones&BartlettLearning,
61. Vilela, Douglas W. F. L.; Lotufo, Anna Diva P.; Santos, Carlos R. (2018). *Fuzzy ARTMAP Neural Network IDS Evaluation applied for real IEEE 802.11w data base. 2018 International Joint Conference on NeuralNetworks (IJCNN),*
62. *Inc, IDG Network World (2003-09-15). Network World. IDG Network World Inc,*
63. Groom, Frank M.; Groom, Kevin; Jones, Stephan S. (2016-08-19). *Network and Data Security for Non-Engineers*. CRC Press,
64. Brandon Lokesak (December 4, 2008). "A Comparison Between Signature Based and Anomaly Based Intrusion Detection Systems",
65. *Douligeris, Christos; Serpanos, Dimitrios N. (2007-02-09). NetworkSecurity: Current Status and FutureDirections. JohnWiley& Sons,*
66. Rowayda, A. Sadek; M Sami, Soliman; Hagar, S Elsayed (November 2013). "Effective anomaly intrusion detection system based on neural network with indicator variable and rough set reduction". *International Journal of Computer ScienceIssues (IJCSI)*. **10** (6),

67. *"Gartner report: Market Guide for User and Entity Behavior Analytics"*
68. *"Gartner: Hype Cycle for Infrastructure Protection, 2016"*,
69. ^ *"Gartner: Defining Intrusion Detection and Prevention Systems"*,
70. ^ Jump up to:[a] [b] *Scarfone, Karen; Mell, Peter (February 2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)"(PDF). Computer Security Resource Center (800–94). Archivedfrom the original (PDF) on 1 June 2010,*
71. ^ Jump up to:[a] [b] *"NIST – Guide to Intrusion Detection and Prevention Systems (IDPS)" (PDF). February 2007,*
72. ^ Jump up to:[a] [b] *Robert C. Newman (19 February 2009). Computer Security: Protecting Digital Resources. Jones & Bartlett Learning. ISBN 978-0-7637-5994-0,*
73. ^ Jump up to:[a] [b] [c] *Michael E. Whitman; Herbert J. Mattord (2009). Principles of Information Security. Cengage Learning EMEA. ISBN 978-1-4239-0177-8,*
74. "IDS Best Practices". cybersecurity.att.com,
75. Richardson, Stephen (2020-02-24). "IDS Placement - CCIE Security" CiscoCertifiedExpert,
76. Anderson, Ross (2001). Security Engineering: A Guide to Building Dependable Distributed Systems. NewYork: JohnWiley& Sons. pp. 387–388. ISBN 978-0-471-38922-4,
77. http://www.giac.org/paper/gsec/235/limitations-network-intrusion-detection/100739,
78. Denning, Dorothy E., "An Intrusion Detection Model," Proceedings of the Seventh IEEE Symposium on Security and Privacy, May 1986, pages 119–131,
79. Lunt, Teresa F., "Detecting Intruders in Computer Systems," 1993 Conference on Auditing and Computer Technology, SRI International,
80. Sebring, Michael M., and Whitehurst, R. Alan., "Expert Systems in Intrusion Detection: A Case Study," The 11th National Computer Security Conference, October, 1988,
81. Smaha, Stephen E., "Haystack: An Intrusion Detection System," The Fourth Aerospace Computer Security Applications Conference, Orlando, FL, December, 1988,
82. McGraw, Gary (May 2007). "Silver Bullet Talks with Becky Bace" (PDF). IEEE Security & Privacy Magazine. 5 (3): 6–9. doi:10.1109/MSP.2007.70. Archived from the original (PDF) on 19 April 2017,
83. Intrusion Detection Techniques for Mobile Wireless Networks, ACM WINET 2003 <http://www.cc.gatech.edu/~wenke/papers/winet03.pdf,
84. "Ασύμμετρη Κρυπτογράφηση." *Ασύμμετρη Κρυπτογράφηση - Βικιβιβλία*, el.wikibooks.org/wiki/Ασύμμετρη_Κρυπτογράφηση,
85. "Συμμετρική Κρυπτογράφηση." *Συμμετρική Κρυπτογράφηση - Βικιβιβλία*, el.wikibooks.org/wiki/Συμμετρική_Κρυπτογράφηση,
86. "Threat Landscape for Smart Home and Media Convergence." *ENISA*, 9 Feb. 2015, www.enisa.europa.eu/publications/threat-landscape-for-smart-home-and-media-convergence,

87. "Διαδίκτυο Των Πραγμάτων." *Wikipedia*, Wikimedia Foundation, 12 Oct. 2020, el.wikipedia.org/wiki/Διαδίκτυο_των_πραγμάτων.

Παράρτημα Εικόνων

1. "Στο Σύστημα Της 'Σύμβασης Για Το Έγκλημα Στον Κυβερνοχώρο' Εντάχθηκε η Ελλάδα." *Thepressroom.gr*, 25 Jan. 2017, www.thepressroom.gr/politiki/sto-systima-tis-symvasis-gia-egklima-ston,
2. Fruhlinger, Josh. "What Is a Computer Worm? How This Self-Spreading Malware Wreaks Havoc." *CSO Online*, CSO, 6 Aug. 2019, www.csoonline.com/article/3429569/what-is-a-computer-worm-how-this-self-spreading-malware-wreaks-havoc.html,
3. "Mini Info On The Computer Virus - Lessons - Tes Teach." *Tes Teach with Blendspace*, www.tes.com/lessons/bGYWXzX79ibW0Q/mini-info-on-the-computer-virus,
4. Suryavanshi, Nirmala. "[PDF] A Review of Various Techniques for Detection and Prevention for Phishing Attack A Review of Various Techniques for Detection and Prevention for Phishing Attack: Semantic Scholar." *[PDF] A Review of Various Techniques for Detection and Prevention for Phishing Attack A Review of Various Techniques for Detection and Prevention for Phishing Attack | Semantic Scholar*, 1 Jan. 1970, www.semanticscholar.org/paper/A-Review-of-Various-Techniques-for-Detection-and-A-Suryavanshi/692b6a3e22b97497d64b1bc3b2184d629a702173,
5. Frink, Lyle, et al. "Spam-Support Site Leaves 800 Million Email Addresses - and More - out in the Open." *Avira Blog*, 3 Apr. 2019, www.avira.com/en/blog/800-million-emails-dropped-real-source-unknown.
6. "SSOCircle." *SSOCircle RSS2*, www.ssocircle.com/en/2153/banks-ignore-crypto-checks-in-credit-card-transactions-standards-are-not-enough/,
7. Screenshot1,
8. says:, Crown H, et al. "300 Terrifying Cybercrime & Cybersecurity Statistics [2020 EDITION]." *Comparitech*, 29 July 2020, www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/.
9. Passeri, Paolo. "June 2018 Cyber Attacks Statistics." *HACKMAGEDDON*, 30 Dec. 2018, www.hackmageddon.com/2018/07/23/june-2018-cyber-attacks-statistics/,
10. Passeri, Paolo. "June 2018 Cyber Attacks Statistics." *HACKMAGEDDON*, 30 Dec. 2018, www.hackmageddon.com/2018/07/23/june-2018-cyber-attacks-statistics/,
11. Passeri, Paolo. "June 2018 Cyber Attacks Statistics." *HACKMAGEDDON*, 30 Dec. 2018, www.hackmageddon.com/2018/07/23/june-2018-cyber-attacks-statistics/,
12. Posted by hayro On August 27, 2019. "The Three Goals of Cyber Security-CIA Triad Defined." *Preferred IT Group, LLC*, www.preferreditgroup.com/2019/08/27/the-three-goals-of-cyber-security-cia-triad-defined/,
13. "Android/Spy.Agent.SI [Threat Name] Go to Threat." *Android/Spy.Agent.SI | ESET Virusradar*, www.virusradar.com/en/Android_Spy.Agent.SI/description,
14. Swanagan, Michael, and Michael Swanagan. "What Is The Difference Between IDS And IPS?" *PurpleSec*, 8 Oct. 2020, purplesec.us/intrusion-detection-vs-intrusion-prevention-systems/,
15. "What Is OSI Model: 7 Layers Explained: Imperva." *Learning Center*, Imperva, 10 June 2020, www.imperva.com/learn/application-security/osi-model/,

16. Atlastugce. "How Does Cryptography Work?" *Logsign*, 30 Mar. 2020, blog.logsign.com/how-does-cryptography-work/,
17. Nyambi, Walters. "The IoT Revolution: Challenges and Opportunities." *Geneva Business News | Actualités: Emploi, RH, Économie, Entreprises, Genève, Suisse.*, 23 Sept. 2019, www.gbnews.ch/the-iot-revolution/,
18. "Threat Landscape for Smart Home and Media Convergence." *ENISA*, 9 Feb. 2015, www.enisa.europa.eu/publications/threat-landscape-for-smart-home-and-media-convergence,
19. "Threat Landscape for Smart Home and Media Convergence." *ENISA*, 9 Feb. 2015, www.enisa.europa.eu/publications/threat-landscape-for-smart-home-and-media-convergence,
20. "Hvad Skal Du Bruge Til Dit Smart Home?" *Somfy Shop DK*, 5 Nov. 2018, shop.somfy.dk/blog/hvad-skal-du-bruge-til-dit-smart-home/.