ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Επιμόρφωση γενικού πληθυσμού σε θέματα ασφάλειας σε οικιακές συσκευές και συστήματα»

Της φοιτήτριας
Κεγκέρογλου Άρτεμις
Αρ. Μητρώου: 2019067

Επιβλέπων
Δρ. Ηλιούδης Χρήστος
Καθηγητής

6 Σεπτεμβρίου 2024

Επιμόρφωση γενικού πληθυσμού σε θέματα ασφάλειας σε οικιακές συσκευές και συστήματα
Κωδικός Δ.Ε. 24160
Κεγκέρογλου Άρτεμις
Ηλιούδης Χρήστος
Ημερομηνία ανάληψης Δ.Ε. 20/03/2024
Ημερομηνία περάτωσης Δ.Ε. 06/09/2024

Βεβαιώνω ότι είμαι η συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

Η έγκριση της διπλωματικής εργασίας από το Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του Διεθνούς Πανεπιστημίου της Ελλάδος, δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων της συγγραφέα, εκ μέρους του Τμήματος.

«Σε όσους προσπαθούν πολύ για τα όνειρά τους»

1. Πρόλογος

Το ενδιαφέρον μου για μάθηση και ανάλυση της ασφάλειας που υπάρχει σε ένα δίκτυο καθώς και το γεγονός ότι υπάρχει ελλιπής ενημέρωση του γενικού πληθυσμού όσον αφορά την προστασία των συσκευών και συστημάτων του είναι οι κύριοι λόγοι για τους οποίους επέλεξα την εκπόνηση του συγκεκριμένου θέματος ως διπλωματική μου εργασία. Όσον αφορά τις έξυπνες οικιακές συσκευές και συστήματα, υπάρχει η αντίληψη, από τους περισσότερους χρήστες, ότι είναι και αδιαμφισβήτητα ασφαλείς. Ωστόσο σε κάθε τέτοια συσκευή και κατ' επέκταση και σύστημα υπάρχουν πολλά αδύναμα σημεία ασφάλειας και λόγω των εξαιρετικά ευαίσθητων δεδομένων που διαχειρίζονται, χρειάζονται περισσότερη διερεύνηση και πιθανές βελτιώσεις. Επομένως, κύριος στόχος της εργασίας είναι να αναλυθεί το βάθος και η φύση του προβλήματος, τα πρότυπα και οι απαιτήσεις ασφάλειας έξυπνων συσκευών, και να παρουσιαστούν καλές πρακτικές που μπορούν να χρησιμοποιηθούν από οργανισμούς στην εγκατάσταση και χρήση έξυπνων συσκευών και με αυτόν τον τρόπο να γίνει πιο εύκολη η διαδικασία εκπαίδευσης και ενημέρωσης του κοινού. Στην μετάδοση της πληροφορίας αυτής μπορούν να συνεισφέρουν ενεργά τα συστήματα Επαυξημένης Πραγματικότητας (Augmented reality - AR). Μέσα από την έρευνα αυτή, καλλιεργήθηκε σημαντικά η συνδυαστική μου σκέψη και απέκτησα πληθώρα γνώσεων σχετικά με θέματα ασφάλειας σε έξυπνες συσκευές.

2. Περίληψη

Η διπλωματική εργασία πραγματεύεται ευπάθειες ασφάλειες και γενικότερα όλη την διαδικασία από την σκέψη, σχεδίαση, κατανόηση των πρακτικών ασφάλειας και υλοποίηση μιας έξυπνης οικιακής συσκευής. Αρχικά, παρουσιάστηκαν συχνές και μη επιθέσεις σε έξυπνες συσκευές, ομαδοποιημένες ανά επίπεδο IoT. Δόθηκαν τρόποι μετρίασης αυτών των επιθέσεων καθώς διασαφηνίστηκαν και κάποιοι τρόποι με τους οποίους μπορούν οι χρήστες να επιμορφωθούν σχετικά με την ασφάλεια των συσκευών τους. Στην συνέχεια, διακρίθηκαν πρότυπα και πρωτόκολλα ασφάλειας, παρουσιάστηκαν κάποιες έξυπνες οικιακές συσκευές με τις διαθέσιμες λειτουργίες τους και συγκεντρώθηκαν και αναφέρθηκαν κάποιες βέλτιστες πρακτικές ασφάλειας των συσκευών. Κλείνοντας, προτάθηκαν τακτικές που βοηθούν στην ασφάλιση των συσκευών και παρουσιάστηκε έρευνα η οποία είχε σκοπό την ευαισθητοποίηση των χρηστών σχετικά με την ασφάλεια των έξυπνων οικιακών συσκευών τους.

«Education on safety issues related to smart home appliances and systems»

«Kegkeroglou Artemis»

3. Abstract

This paper deals with security vulnerabilities and, in general, the entire process from the conception, design, and understanding of security practices to the implementation of a smart home device. Initially, common as well as unusual attacks on smart devices were presented, grouped by IoT level. Mitigation methods for these attacks were provided, and ways in which users can educate themselves about the security of their devices were clarified. Subsequently, security standards and protocols were distinguished, some smart home devices with their available functions were presented, and also best security practices for devices were mentioned. Finally, tactics that help secure devices were proposed, and research – aimed at raising user awareness about the security of their smart home devices – was presented.

4. Ευχαριστίες

Θέλω να ευχαριστήσω όλους όσους βοήθησαν και συνέβαλλαν με τον τρόπο τους στην δημιουργία και ανάπτυξη της Διπλωματικής μου εργασίας και του ερωτηματολογίου που βοήθησε πολύ στην έρευνα και την εξαγωγή σημαντικών συμπερασμάτων. Πιο συγκεκριμένα, θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή της εργασίας μου, τον κύριο Ηλιούδη Χρήστο, ο οποίος οριοθετούσε τις πολλές ιδέες που είχα και με κατεύθυνε σε ένα, αρκετά άγνωστο σε εμένα, γνωστικό πλαίσιο που περιλάμβανε η θεματική της Διπλωματικής μου. Ακόμη, θα ήθελα να ευχαριστήσω κάθε έναν ξεχωριστά από εκείνους που συμπλήρωσαν το ερωτηματολόγιο και συνέβαλλαν τόσο στην ολοκλήρωση της έρευνας, έκαναν την μελέτη πιο ευχάριστη και για εμένα γιατί ήταν ένας διαδραστικός τρόπος να πάρω τις πληροφορίες που χρειαζόμουν και να διαπιστώσω και μόνη μου συνήθειες και μοτίβα συμπεριφοράς των χρηστών σχετικά με την χρήση των έξυπνων οικιακών συσκευών τους. Τέλος, δεν θα μπορούσα να μην ευχαριστήσω τα άτομα που πιστεύουν πάντα σε εμένα, ακόμα και όταν εγώ δεν το κάνω. Δεν θα ήταν ίδια η προσπάθεια και ο κόπος που κατέβαλα χωρίς αυτά.

5. Περιεχόμενα

6. Κατάλογος Εικόνων

Κεφάλαιο 1ο: Εισαγωγή

1.1 Περιγραφή θέματος

Στη σύγχρονη εποχή που ζούμε, όλων των ειδών τα έξυπνα συστήματα βρίσκονται στο κέντρο της προσοχής. Από έξυπνο ποτιστικό μέχρι έξυπνο αυτοκίνητο, όλες οι έξυπνες συσκευές και εγκαταστάσεις, μονοπωλούν το ενδιαφέρον και μας φέρνουν όλο και πιο κοντά στο μέλλον.

Αρχικά, ενδιέφεραν ιδιαίτερα οι συσκευές και τα συστήματα που χρησιμοποιούνταν για κάποιου είδους εργασία. Πιο συγκεκριμένα, οι κλάδοι της γεωργίας, της ιατρικής, της παραγωγής και της μεταφοράς είναι μερικοί τομείς που ενδιέφεραν περισσότερο κατά την δημιουργία των έξυπνων συσκευών, με σκοπό να βοηθήσουν αλλά και να κάνουν εργασίες με μεγαλύτερη ακρίβεια και ταχύτητα από ότι παλαιότερα.

Αργότερα όμως, οι έξυπνες συσκευές άρχισαν να μπαίνουν στην καθημερινότητα, να χρησιμοποιούνται πολύ συχνά και να φέρουν πολλαπλή λειτουργικότητα και χρηστικότητα, κάτι που δεν είχαμε φανταστεί ότι θα μπορούσε να συμβεί. Με αυτόν τον τρόπο, οι συσκευές αυτές άρχισαν να αντικαθιστούν τις οικιακές συσκευές, καθιστώντας έτσι και τον όρο έξυπνο σπίτι πραγματικότητα. Με τον καιρό βέβαια, όλο και βελτιώνονται τέτοιου είδους έξυπνες συσκευές, όσον αφορά την εμφάνιση, την λειτουργία, την δομή τους ίσως και τον τρόπο επικοινωνίας με τον χρήστη. Το πιο σημαντικό όμως που χρειάζεται τακτικά ενημέρωση και βελτιστοποίηση, είναι τα αδύνατα σημεία ασφάλειας που έχει κάθε συσκευή και σύστημα. Η συχνή βελτίωση και η ευαισθητοποίηση των χρηστών σε θέματα ασφάλειας κρίνεται τόσο σημαντική λόγω της ευαισθησίας των δεδομένων που συλλέγονται και διαχειρίζονται αλλά και των εργασιών που φέρνουν εις πέρας αυτές. Ακόμη, είναι γεγονός ότι δεν είναι τόσο διαδεδομένη και εύκολη η εκπαίδευση των “οικιακών χρηστών” σε ζητήματα ασφάλειας. Επομένως, όλα αυτά επηρεάζουν αποθαρρυντικά όσον αφορά την ενημέρωση των χρηστών για τις οικιακές τους συσκευές, που από την φύση τους θα έπρεπε να είναι προστατευμένες και να παρέχονται με επαρκή εκπαίδευση.

Η ενημέρωση αυτή θα μπορούσε να υλοποιηθεί με την χρήση συστημάτων Επαυξημένης Πραγματικότητας. Συνεπώς, ενσωματώνοντας τον εικονικό στον πραγματικό κόσμο, προσφέρεται μία διαδραστική εμπειρία για τον χρήστη, ο οποίος καταλαβαίνει πιο εύκολα τους δύσκολους όρους που υπάρχουν στην ασφάλεια των συσκευών και συστημάτων.

1.2 Οργάνωση ενοτήτων

Η εργασία αποτελείται από οκτώ κεφάλαια. Το πρώτο κεφάλαιο, πραγματεύεται το βάθος και την φύση του προβλήματος ευαισθητοποίησης των χρηστών σε θέματα ασφάλειας όσον αφορά τις έξυπνες οικιακές συσκευές. Παρουσιάζονται οι ενότητες και το περιεχόμενό τους, καθώς επίσης και οι επιθυμητοί στόχοι της έρευνας.

Στο δεύτερο κεφάλαιο, ομαδοποιούνται και παρουσιάζονται είδη επιθέσεων και λύσεις μετριασμού αυτών, ανά επίπεδο IoT, καθώς επίσης παρατίθενται κάποιες τεχνολογίες εκπαίδευσης που υπάρχουν έως και σήμερα.

Στο τρίτο κεφάλαιο, σχολιάζονται οι απαιτήσεις ασφάλειας και τα πρότυπα ασφάλειας που υλοποιούνται σε έξυπνες συσκευές. Με τα πρότυπα ασφάλειας καθορίζονται κάποια κριτήρια σύμφωνα με τα οποία κάθε οργανισμός μπορεί να προστατέψει τα απόρρητα και σημαντικά δεδομένα που

διαχειρίζεται. Οι απαιτήσεις ασφάλειας σχετίζονται με το ποιος έχει πρόσβαση και μπορεί να τροποποιήσει τα δεδομένα, την χρονική στιγμή που το κάνει, πιθανούς κινδύνους και ευαλωτότητες που έχει το σύστημα και πως θα μπορούσαν να αποφευχθούν. Οι απαιτήσεις ασφάλειας συμβάλλουν στην ακεραιότητα, εμπιστευτικότητα και διαθεσιμότητα των δεδομένων.

Στο τέταρτο κεφάλαιο, γίνεται συνοπτική παρουσίαση κάποιων έξυπνων συσκευών και συστημάτων, διακρίνονται ομαδοποιημένες λειτουργίες που έχουν και ζητήματα ασφάλειας που υπάρχουν τα οποία και αυτά ομαδοποιούνται ανάλογα την περιοχή επίδρασής τους.

Στο πέμπτο κεφάλαιο, εξετάζονται καλές πρακτικές που μπορούν να χρησιμοποιηθούν από οργανισμούς για βελτίωση στην εγκατάσταση και χρήση των έξυπνων οικιακών συσκευών. Διακρίνονται καλές και βέλτιστες πρακτικές ανάλογα το στάδιο εφαρμογής τους και αξιολογούνται σε ευκολία εφαρμογής και αποτελεσματικότητα. Οι καλές και βέλτιστες πρακτικές απευθύνονται και στον κατασκευαστή και στον χρήστη και προτείνουν με πρακτικό και εύκολο τρόπο μεθόδους ασφάλισης των έξυπνων οικιακών συσκευών και συστημάτων τους, καθώς στην συνέχεια προτείνονται καλές πρακτικές και προς οργανισμούς και επιχειρήσεις.

Στο έκτο κεφάλαιο, προτείνονται, από μέχρι στιγμής έρευνα και γνώσεις επί του θέματος, κάποιες τακτικές που αποσκοπούν στην βελτίωση της ασφάλειας στις έξυπνες συσκευές. Προτείνονται οδηγοί προς χρήστες και κατασκευαστές καθώς και συνδυαστικοί οδηγοί οι οποίοι θα ενισχύσουν την ασφάλεια και περιορίσουν τις ευπάθειες των έξυπνων οικιακών συσκευών.

Στο έβδομο κεφάλαιο παρουσιάζεται ένα ερωτηματολόγιο που πραγματοποιήθηκε στο πλαίσιο ευαισθητοποίησης και εγρήγορσης των χρηστών σχετικά με την εκπαίδευσή τους σε θέματα ασφάλειας. Στην συνέχεια, παρουσιάζονται όλες οι μέθοδοι που βοηθούν στον παραπάνω σκοπό και αναλύονται τα αποτελέσματα τα οποία παρουσιάζονται και σε μορφή γραφήματος για καλύτερη κατανόηση.

Στο όγδοο και τελευταίο κεφάλαιο, διακρίνονται και επεξηγούνται τα αποτελέσματα και συμπεράσματα από τα θέματα που έχουν αναφερθεί παραπάνω και πιθανές προτάσεις για περαιτέρω έρευνα. Στο συγκεκριμένο κεφάλαιο παρουσιάζονται συμπεράσματα που έχουν βγει από την, μέχρι στιγμής, έρευνα.

Τέλος, στο παράρτημα Α’ αναλύονται και επεξηγούνται εκτενέστερα οι ερωτήσεις, τα ποσοστά απαντήσεών τους και τα σχετικά βίντεο που θεάθηκαν κατά την συμπλήρωση του ερωτηματολογίου.

1.3 Στόχοι έρευνας

Στόχοι της παρούσας διπλωματικής είναι, αρχικά, να αναλυθούν με μεγάλη σαφήνεια και ακρίβεια όλα τα κεφάλαια που παρουσιάστηκαν παραπάνω με την αντίστοιχη θεματολογία τους. Επιπρόσθετοι στόχοι είναι η μελέτη πάνω στις ευπάθειες που φέρουν οι έξυπνες οικιακές συσκευές, καθώς επίσης και η αξιολόγηση των διαθέσιμων τρόπων και μέσων βασικής εκπαίδευσης χρήσης και αξιοποίησης αυτών των συσκευών. Τέλος, αξιολογείται η μέχρι στιγμής γνώση, αντίληψη και ευαισθητοποίηση των χρηστών με παραστατικό τρόπο μέσω ενός ερωτηματολογίου που είχε πολλούς σημαντικούς στόχους. Μερικοί από αυτούς ήταν οι σύντομες ερωτήσεις και βίντεο με σκοπό την συμπλήρωση του ερωτηματολογίου σε συγκεκριμένο χρόνο, λόγω και του περιορισμένου χρόνου των χρηστών, η παρουσίαση σύντομων και εύστοχων βίντεο και στην συνέχεια η παρουσίαση των αποτελεσμάτων και μέσω γραφημάτων.

1.4 Επίλογος

Στο πρώτο κεφάλαιο έγινε αναφορά στο θέμα που θα πραγματευτεί η Διπλωματική εργασία. Στην συνέχεια διακρίθηκε και οργανώθηκε, ανά κεφάλαιο, η θεματολογία που θα αναλυθεί, στόχους και σκοπιμότητα αναφοράς των συγκεκριμένων θεμάτων. Τέλος, παρουσιάστηκαν και διασαφηνίστηκαν οι επιθυμητοί στόχοι εκπλήρωσης κατά την ολοκλήρωση συγγραφής της εργασίας.

Κεφάλαιο 2ο: Επιθέσεις και παραδοσιακές μέθοδοι εκπαίδευσης χρηστών

2.1 Εισαγωγή

Στο δεύτερο κεφάλαιο γίνεται αναφορά στατιστικών σχετικά με επιθέσεις από προηγούμενα έτη αλλά και τι αναμένεται. Παρουσιάζονται οι κύριοι λόγοι που πετυχαίνουν οι επιθέσεις αυτές, οι τεχνολογίες που βοήθησαν στην περαιτέρω εξάπλωση των έξυπνων συσκευών και κατά συνέπεια στην αύξηση των διαθέσιμων "ευάλωτων" συσκευών. Περιγράφεται η έννοια του έξυπνου σπιτιού και πως συνδυάζοντας τις τεχνολογίες Επαυξημένη και Εικονική πραγματικότητα ενισχύεται περαιτέρω η έννοια αυτή. Στην συνέχεια, καταγράφονται και ομαδοποιούνται συχνές επιθέσεις σε έξυπνες οικιακές συσκευές καθώς και οι στόχοι των επιτιθέμενων σε αυτές. Διασαφηνίζονται τεχνικές και μέτρα για αποτροπή και αντιμετώπιση των επιθέσεων αυτών. Τέλος, αναλύονται παραδοσιακές τεχνικές όσον αφορά την ασφάλεια σε έξυπνες οικιακές συσκευές καθώς και τα προβλήματα που αντιμετωπίζουν στην υλοποίησή τους.

2.2 Στατιστικά επιθέσεων

Τα στατιστικά των τελευταίων έξι χρόνων αναφέρουν ότι το διαδικτυακό έγκλημα αυξάνεται ανησυχητικά πολύ, αναφέροντας 515.612 περιστατικά το 2020, ενώ τα 162.091 από αυτά καταγράφηκαν πρόσφατα. Το 2021, το ηλεκτρονικό "ψάρεμα" και παρόμοιου είδους κυβερνοεπιθέσεις, που στόχευαν σε εταιρικά email και μετάδοση κακόβουλου λογισμικού ήταν οι κύριες πηγές παραβάσεων σε δεδομένα. Αναφορικά με πρόσφατες μελέτες, το 2022, οι επιθέσεις ransomware ξεπέρασαν το ηλεκτρονικό ψάρεμα κυρίως διότι βασικός στόχος των επιτιθέμενων είναι οι ευαίσθητες πληροφορίες του εκάστοτε φορέα. Επομένως, το θέμα είναι να μπορεί να προβλεφθεί το ψεύτικο και παραπλανητικό περιεχόμενο και να καταγραφεί σαν επίθεση. Έρευνα της IBM που πραγματοποιήθηκε το 2022, έδειξε ότι το 25% των παραβάσεων ασφαλείας σε βιομηχανικούς οργανισμούς, συνέβησαν λόγω ανθρώπινων λαθών. Πιο συγκεκριμένα, η έλλειψη εκπαίδευσης των εργαζομένων σε ζητήματα ασφάλειας είναι ο κύριος λόγος που πετύχαιναν αυτές οι επιθέσεις. [1]

Πρόσφατες τεχνολογίες όπως το Διαδίκτυο των Πραγμάτων (Internet of Things - IOT) έχουν φέρει την προσωπική ζωή καθενός όλο και πιο κοντά στον κυβερνοχώρο. Αναπτυσσόμενες τεχνολογίες όπως η Εικονική Πραγματικότητα (Virtual Reality) και η Επαυξημένη Πραγματικότητα (Augmented Reality), φέρνουν τον κυβερνοχώρο πιο κοντά στον άνθρωπο και ούτω καθεξής. Αυτή η υπερέκθεση των δεδομένων των χρηστών μπορεί να επηρεάσει όχι μόνο την ιδιωτικότητα τους αλλά και την προσωπική τους ασφάλεια. Κύρια απώλεια που υφίστανται τέτοιου είδους mixed-reality εφαρμογές είναι η διαρροή των προσωπικών δεδομένων με συνέπεια την έλλειψη εμπιστοσύνης στην εφαρμογή και κακή φήμη για την εταιρεία, ίσως και σωματική και ψυχική ζημιά. [2]

Τα έξυπνα σπίτια είναι μια σημαντική IoT εφαρμογή που χρησιμοποιείται για να διευκολύνει σε θέματα καθημερινότητας. Έξυπνες συσκευές όπως κουδούνι, θερμοστάτης, κλειδαριά πόρτας, έξυπνος φούρνος, φώτα και ψυγείο, εγκαθίστανται και ρυθμίζονται στο smart home. Μπορούν εύκολα να ελεγχθούν από τους χρήστες του σπιτιού μέσω φιλικών στο χρήστη διεπαφών, όπως εφαρμογές ή προγράμματα περιήγησης. Η αλληλεπίδραση σε ένα έξυπνο σπίτι μπορεί να γίνει μέσω μηχανών ή μέσω ανθρώπου - μηχανής. Ένα παράδειγμα για επικοινωνία μηχανών είναι όταν υπάρχει ανίχνευση κίνησης κοντά στο σπίτι να φωτογραφίζει και να στέλνει την φωτογραφία μέσω ειδοποίησης στον χρήστη. Στην

επικοινωνία ανθρώπου - μηχανής ανήκει κάθε αλληλεπίδραση του ανθρώπου μέσω της εφαρμογής ή κάποιου προγράμματος περιήγησης για να πραγματοποιήσει κάποια λειτουργία στο σπίτι, όπως για παράδειγμα να ανοίξει τα φώτα. [3]

Στο 2 παρουσιάζεται η άποψη ότι σε ένα έξυπνο σπίτι που χρησιμοποιούνται AR και VR (mixed-reality) εφαρμογές, αναπτύσσεται η εμπειρία του χρήστη όσον αφορά την ιατροφαρμακευτική περίθαλψη, την διαχείριση της ενέργειας και την ψυχαγωγία του. Ωστόσο, ένα πρόσφατο πείραμα με ψεύτικο smart home έδειξε ότι συνέβησαν περισσότερα από 12 χιλιάδες σκαναρίσματα ή προσπάθειες να εισέλθουν στο σύστημα κακόβουλοι χρήστες, σε διάστημα μιας εβδομάδας. Επιπρόσθετα, οι χρήστες smart home προβλέπεται ότι θα ξεπεράσουν τους 77 εκατομμύρια μέχρι το 2025. Ακόμη, η αγορά των smart home αναπτύσσεται με επιταχυνόμενο ρυθμό και υπολογίζεται ότι μέχρι το 2027 θα αξίζει 222,90 δισεκατομμύρια δολάρια, με 672,60 εκατομμύρια ενεργούς χρήστες [4]. Επομένως, η αύξηση των χρηστών έξυπνων σπιτιών θα αυξήσει δραματικά και τα θύματα, σε περίπτωση που οι χρήστες δεν είναι ευαισθητοποιημένοι σχετικά με την ασφάλεια των συσκευών και συστημάτων τους, και δεν γνωρίζουν μεθόδους αποτροπής των κακόβουλων χρηστών από το να εισέλθουν στο σύστημά τους. Όμως, το υψηλό χρηματικό κόστος, ο χρόνος, και τα μέσα που απαιτούνται από έναν χρήστη για να λάβει μέρος σε επιμορφωτικά προγράμματα κυβερνοασφάλειας, αποτελούν αποτρεπτικούς παράγοντες για τους χρήστες. Όπως προτείνεται και από τον Lu [5] κάποιου είδους ανταμοιβές θα έδιναν επιπλέον κίνητρο στους χρήστες να υιοθετήσουν κανόνες ασφάλειας των συστημάτων τους. Οι ανταμοιβές αυτές σίγουρα διαφέρουν από χρήστη σε χρήστη, όμως σύμφωνα με το [6] τα κίνητρα που σχετίζονται με κοινωνικούς ‘κανόνες’ και όχι τόσο τα χρηματικά ποσά, φαίνεται να έχουν μεγαλύτερο αντίκτυπο στις συμπεριφορές στα νοικοκυριά.

2.3 Συχνές Επιθέσεις σε έξυπνες οικιακές συσκευές

Το ISO 27005 όρισε ως επίθεση την ικανότητα να εκμεταλλευτεί κάποιος τις αδυναμίες μιας εγκατάστασης και να οδηγήσει τον οργανισμό σε μεγάλη απώλεια. [7] Παρουσιάζοντας μια ενδεικτική εικόνα για τις επιθέσεις στον κυβερνοχώρο, εκείνες που στοχεύουν σε έξυπνα σπίτια χωρίζονται σε τρεις βασικές κατηγορίες. Η πρώτη αποτελεί τις “παραδοσιακές” επιθέσεις δικτύου, όπως οι Distributed Denial of Service επιθέσεις (DDoS) στις οποίες ο επιτιθέμενος δημιουργεί πολύ μεγάλη κίνηση ψεύτικων δεδομένων, οι Man-In-The-Middle επιθέσεις (MITM) στις οποίες ο επιτιθέμενος βρίσκεται ενδιάμεσα δύο μερών και παρεμποδίζει την επικοινωνία τους, και οι επιθέσεις eavesdropping στις οποίες ο επιτιθέμενος υποκλέπτει, διαγράφει ή τροποποιεί τα δεδομένα που ανταλλάσσονται μεταξύ δύο συσκευών (γνωστή και ως snooping ή sniffing). Στη δεύτερη κατηγορία ανήκουν οι επιθέσεις στις οποίες στόχος είναι οι έξυπνες συσκευές και πως θα μπορέσει ο επιτιθέμενος να εκμεταλλευτεί ευαλωτότητες που μπορεί να έχουν. Η τρίτη κατηγορία απευθύνεται στον ανθρώπινο παράγοντα, μελετώντας καλά το περιβάλλον και τα ενδιαφέροντα του χρήστη, οι επιτιθέμενοι προσπαθούν να υποκλέψουν προσωπικά δεδομένα ή να εισέλθουν στο σύστημα. [7][4]

2.4 Επίπεδα IoT

Πριν γίνει αναφορά στα είδη επιθέσεων ανά επίπεδο, κρίνεται σημαντικό να αναφερθούν αυτά τα επίπεδα. Η δομή των επιπέδων του IoT περιβάλλοντος αποτελείται από τα επίπεδα Application, Physical, Network και Perception. [7]

Όλες οι εφαρμογές και υπηρεσίες που προσφέρει το IoT, όπως έξυπνα σπίτια, πόλεις, νοσοκομεία ανήκουν στο Application layer. Λειτουργεί σαν διεπαφή μεταξύ του δικτύου και των IoT συσκευών. Αυτό το επίπεδο έχει την ευθύνη να ελέγχει τις υπηρεσίες κάθε εφαρμογής και να δίνει διαφορετικές υπηρεσίες σε διαφορετικές εφαρμογές σύμφωνα με πληροφορίες που λαμβάνει από τους αισθητήρες. Κύριο ζήτημα σε αυτό το επίπεδο είναι η ασφάλεια. [7]

Στην συνέχεια, στο φυσικό επίπεδο περιλαμβάνονται όλες οι συσκευές ή εξαρτήματα όπως μετασχηματιστές, smartphones και οικιακές συσκευές. Αυτό το επίπεδο συνίσταται από αισθητήρες που συλλέγουν πληροφορίες από το περιβάλλον. Ακόμη, κάθε συσκευή επικοινωνεί με τις υπόλοιπες για να πραγματοποιηθεί μια εργασία. [7]

Το επίπεδο δικτύου αποτελείται από λογισμικό επικοινωνίας δικτύου και συσκευές δικτύου, που επιτρέπουν σε διαφορετικού είδους συσκευές να επικοινωνούν μεταξύ τους. Το βασικό χαρακτηριστικό αυτού του επιπέδου είναι η αποστολή δεδομένων σε end devices και στις συσκευές ανάμεσα στους τελικούς κόμβους (end nodes). Σημαντική δυσκολία είναι η αποστολή δεδομένων σε μεγάλες αποστάσεις. Λειτουργεί δηλαδή σαν γέφυρα στην οποία μεταφέρονται δεδομένα στους αισθητήρες. Το μέσο μετάδοσης μπορεί να είναι ενσύρματο ή η επικοινωνία να γίνεται ασύρματα, και σε αυτό το επίπεδο συσχετίζονται τα δίκτυα με τις δικτυακές συσκευές μεταξύ τους. [7]

Τέλος, το Perception layer αποτελείται από διαφορετικές συσκευές και τεχνολογίες που λαμβάνουν κάποια είσοδο από το περιβάλλον. Αυτές οι συσκευές και τεχνολογίες θα μπορούσαν να είναι αισθητήρες πίεσης, καπνού, δόνησης και RFID αισθητήρες. Κύριος στόχος του επιπέδου αυτού είναι να ενώνει πληροφορίες από διεργασίες. Και τέλος το βασικό πρόβλημα που χρήζει επίλυσης σε αυτό το επίπεδο, είναι η συλλογή και η αποθήκευση των πληροφοριών. [7]

2.5 Επιθέσεις ανά επίπεδο IoT

Για να βελτιωθεί η ασφάλεια γύρω από τις έξυπνες οικιακές συσκευές, απαιτείται η μελέτη κάθε επιπέδου και τι είδους επιθέσεις προτιμώνται σε κάθε ένα από αυτά. Στη συνέχεια, με πιο ουσιαστική κατανόηση των ευπαθειών, μπορεί να ασφαλιστεί κάθε επίπεδο σύμφωνα και με τα αδύναμα σημεία που μπορούν οι επιτιθέμενοι να εκμεταλλευτούν σε αυτό.

2.5.1 Επίπεδο εφαρμογών

Στο επίπεδο εφαρμογών οι επιθέσεις που πραγματοποιούνται σχετίζονται με προγραμματιστικά λάθη ή παραλείψεις. Αποτέλεσμα αυτών των επιθέσεων είναι η δημιουργία σφαλμάτων στο πρόγραμμα της εφαρμογής που οδηγεί σε ασυνήθιστη λειτουργία της. [7] Παρακάτω παρουσιάζονται οι κύριες επιθέσεις σε αυτό το επίπεδο.

Όπως αναφέρθηκε και προηγουμένως, το ηλεκτρονικό “ψάρεμα” αποτελεί μια συνηθισμένη επίθεση. Ανήκει στο επίπεδο εφαρμογών και σχετίζεται με παραπλανητικές πληροφορίες ή προτάσεις που ο κακόβουλος χρήστης στέλνει στο θύμα, με σκοπό την απόσπαση σημαντικών πληροφοριών ή την αποστολή του θύματος σε ένα “ασφαλές” περιβάλλον, για να αποσπάσει χρηματικά ποσά.

Ακόμη μια πολύ συνηθισμένη μέθοδος επίθεσης είναι η μετάδοση κακόβουλου λογισμικού. Αυτό μπορεί να πραγματοποιηθεί με πολλούς τρόπους, όπως με ένα computer worm. Στην συγκεκριμένη επίθεση ο επιτιθέμενος έχοντας μολύνει έναν υπολογιστή του δικτύου, προσπαθεί να μολύνει και τους υπόλοιπους του δικτύου αυτού. Χωρίζοντας τις επιθέσεις αυτές σε τρεις βασικές κατηγορίες, σύμφωνα

με το [8] αυτές είναι οι επιθέσεις Botnet Mirai, Ransomware και εκείνες που σχετίζονται με τον φυσικό εξοπλισμό (hardware) ή τον χειρισμό αισθητήρων. Στις Botnet Mirai επιθέσεις οι επιτιθέμενοι παρακολουθούν την δραστηριότητα του δικτύου, την καταγράφουν και έχουν ως σκοπό να χειρίζονται από απόσταση τις έξυπνες συσκευές ως bot, που όλες μαζί αποτελούν ένα botnet. [7] Οι Ransomware επιθέσεις χωρίζονται σε δύο είδη, locker ransomware και crypto-ransomware. Στο πρώτο είδος δεν παρέχεται πρόσβαση του χρήστη στον υπολογιστή ή την συσκευή του ενώ στο δεύτερο αποκλείεται η πρόσβαση σε αρχεία ή δεδομένα. Και στις δύο κατηγορίες όμως το κοινό είναι ότι παρεμποδίζεται ο χρήστης να κάνει κάτι και ως αντάλλαγμα ζητείται πληρωμή για να παραχωρηθεί πρόσβαση. [9]

Το επόμενο είδος επίθεσης, αφορά στην εξάπλωση κακόβουλου λογισμικού σε εφαρμογές του χρήστη και επιπλέον εγκατάσταση rootkits για να εξασφαλίσουν οι επιτιθέμενοι την παραμονή τους ως διαχειριστή κρυφά. Ακόμη, το tampering αναφέρεται και ως φυσική προσαρμογή του εξοπλισμού των συσκευών. Ως αποτέλεσμα του λοιπόν, έχει την υποκλοπή προσωπικών στοιχείων του χρήστη ή την αλλαγή των εξαρτημάτων της συσκευής. [7]

Η επίθεση στο σύστημα διαχείρισης πρόσβασης είναι εξίσου συνήθης. Η διαχείριση πρόσβασης έχει ως σκοπό να διαφυλάξει ότι μόνο ο έννομος χρήστης έχει πρόσβαση σε δεδομένα. Οι access control επιθέσεις συμβαίνουν όταν μια αυθεντικοποιημένη διαδικασία ελέγχου πρόσβασης παραβιαστεί. Όταν παραβιαστεί η διαχείρισης ασφάλειας, όλο το σύστημα καθίσταται ευπαθές σε επιτιθέμενους. [7]

Ακόμη, το γεγονός ότι κάποια συστήματα ή εφαρμογές δεν δέχονται καθόλου ή συχνά ενημερώσεις και το είδος των ενημερώσεων διαμοιράζεται ή πραγματοποιείται χωρίς κρυπτογράφηση, μπορεί να οδηγήσει σε άλλα είδη επιθέσεων όπως hijacking attacks. [7]

Επιπρόσθετα, οι επιθέσεις σε smart meters/grids είναι συχνό φαινόμενο καθώς στέλνοντας την ενεργειακή κατανάλωση και άλλες ζητούμενες πληροφορίες χωρίς κρυπτογράφηση στα αρμόδια συστήματα μπορεί να υποκλαπούν και να παρατηρηθεί από επιτιθέμενους η διαθεσιμότητα του χρήστη στο σπίτι του, βασιζόμενοι στην ενεργειακή κατανάλωση του χρήστη. [7]

Τέλος, οι Social Engineering επιθέσεις είναι ακόμα ένα είδος επιθέσεων στο οποίο ο επιτιθέμενος μέσω χειρισμού του θύματος καταφέρνει να αποσπάσει ευαίσθητα δεδομένα, χρήματα ή υπηρεσία από αυτό. Βασιζόμενος σε ηλικιακό προφίλ, ενδιαφέροντα και αδυναμίες, επικοινωνεί με το θύμα είτε διαδικτυακά είτε δια ζώσης προσπαθώντας να αποσπάσει σημαντικές πληροφορίες για να επιτεθεί σε κάποιο σύστημα ή δίκτυο ή να εισέλθει στο δίκτυο εκμεταλλευόμενος πληροφορίες που γνωρίζει. Χωρίζεται σε αρκετές κατηγορίες παραπλάνησης του θύματος. Ένα απλό παράδειγμα μιας από αυτές τις κατηγορίες της μεθόδου είναι η είσοδος του επιτιθέμενου σε εταιρικό δίκτυο που υπάρχει έλεγχος πρόσβασης, προσποιούμενος ότι είναι το συνεργείο καθαρισμού. Δηλαδή με πληροφορίες που έχει αποσπάσει ο επιτιθέμενος προσπαθεί να εκμεταλλευτεί ανθρώπινες αδυναμίες και να εισέλθει στο δίκτυο. Οι Social Engineering επιθέσεις συμβαίνουν μέσω τηλεφωνικών κλήσεων, emails, αλλά και κατ' ιδίαν επικοινωνία. [10]

2.5.2 Perception layer

Οι περισσότερες επιθέσεις στο perception layer βασίζονται στις συσκευές - κόμβους που μεταδίδουν τα δεδομένα. Αλλάζοντας το λογισμικό των συσκευών αυτών, οι επιτιθέμενοι μπορούν να πάρουν τον έλεγχο και να βλέπουν τις πληροφορίες για εκείνη την συσκευή - κόμβο καθώς και την επικοινωνία με άλλες. Συνεπώς, κατά κύριο λόγο οι επιθέσεις αυτές συμβαίνουν από απόσταση και οι αισθητήρες

κόμβοι παίζουν σημαντικό ρόλο στο αν θα πετύχουν οι επιθέσεις αυτές. Παρακάτω αναφέρονται και επεξηγούνται κάποια βασικά είδη επιθέσεων σε αυτό το επίπεδο.

Οι eavesdropping επιθέσεις, στις οποίες έχει γίνει ήδη μια αναφορά, πραγματοποιούνται σε αυτό το επίπεδο και αφορούν σε τροποποίηση, διαγραφή και ανάγνωση των δεδομένων που ανταλλάσσονται μεταξύ δύο συσκευών. Αυτό πραγματοποιείται όταν ο επιτιθέμενος βρει κάποια συσκευή στο οικιακό έξυπνο σπίτι αφύλακτη, κάτι αρκετά συχνό καθώς δεν ασφαλίζονται επαρκώς αυτές οι συσκευές και στην συνέχεια στέλνοντας ειδοποιήσεις ή αιτήματα, μπορεί να υποκλέψει ευαίσθητα δεδομένα του χρήστη. Στο άρθρο 4, καλείται και ως sniffing ή snooping επίθεση, ενώ στο 6 διαφοροποιούνται οι όροι. [4][7]

Ακόμη ένα είδος επιθέσεων που πραγματοποιούνται σε αυτό το επίπεδο είναι οι booting attacks. Οι επιθέσεις αυτές εφαρμόζονται στο ξεκίνημα του συστήματος όταν οι συσκευές προετοιμάζονται για επικοινωνία, ή οι αλγόριθμοι ασφάλειας δεν έχουν ακόμη εγκατασταθεί. Σε αυτό το σημείο οι επιτιθέμενοι εκμεταλλεύονται τις "ευάλωτες" συσκευές, παίρνοντας τον έλεγχο. [7]

Οι επιθέσεις side-channel πραγματοποιούνται επίσης σε αυτό το επίπεδο, σχετίζονται με φυσικά παρατηρήσιμα φαινόμενα που προκαλούνται από εκτέλεση υπολογιστικών διεργασιών στις υπάρχουσες μικρουπολογιστικές συσκευές. Υπάρχουν πολλές πληροφορίες που διαρρέονται από την επικοινωνία των υπολογιστών για την σωστή λειτουργία των συστημάτων οι οποίες μπορεί να διαρεύσουν σε κακόβουλους χρήστες. Μερικές από αυτές είναι η ενεργειακή κατανάλωση, τα ηλεκτρομαγνητικά κύματα, ενέργεια, θόρυβος του μικροεπεξεργαστή και ο χρόνος που απαιτείται για την ολοκλήρωση κάθε διεργασίας. [11]

Τέλος, τα άσχετα δεδομένα που αποστέλλονται σε έξυπνες συσκευές, μπορεί να οδηγήσουν τις συσκευές αυτές σε ανεπιθύμητες ή λανθασμένες ενέργειες και καθυστέρηση στο δίκτυο. Επιπρόσθετα, λόγω των μεγάλων αποστάσεων που στέλνονται τα δεδομένα, καθώς και το γεγονός ότι χρησιμοποιείται ασύρματη επικοινωνία, δημιουργούν πολλές πιθανότητες οι πληροφορίες να φτάνουν ατελείς, λανθασμένες και μη χρήσιμες για τον τελικό αποδέκτη. [7]

2.5.3 Network layer

Το επίπεδο δικτύου είναι υπεύθυνο για την μεταφορά των πληροφοριών μεταξύ των συσκευών. Συνεπώς, σε αυτό το επίπεδο βασικά προβλήματα που προκύπτουν είναι η "συμφόρηση" των δεδομένων και η ακεραιότητα και επαλήθευση γνησιότητας των δεδομένων που στέλνονται στον παραλήπτη. [7] Παρακάτω παρουσιάζονται επιθέσεις που σχετίζονται με αυτό το επίπεδο.

Αρχικά, οι denial of service attacks προκαλούν συμφόρηση στην σύνδεση επικοινωνίας, και μπορούν να προκληθούν σε αυτό το επίπεδο. Σε αυτού του είδους την επίθεση, ο κακόβουλος χρήστης εκμεταλλεύεται την σύνδεση στο Internet που προσφέρει πολλών ειδών υπηρεσίες και κάνει τεράστιο αριθμό από αιτήσεις στο θύμα. [12] Ακόμη, σύμφωνα με το άρθρο 13 οι γνωστές επιθέσεις DoS γενικά στοχεύουν και κυριαρχούν το θύμα τους εξαντλώντας τους πόρους του οι οποίοι μπορεί να είναι οτιδήποτε σχετικό με το υπολογιστικό δίκτυο, την απόδοση των υπηρεσιών, όπως link bandwidth, TCP connection buffers, application/service αποθηκευτικές μνήμες και κύκλοι CPU. [13] Όταν συμβεί μια τέτοια επίθεση, μπορεί να προκαλέσει διακοπή λειτουργίας του δικτύου, και η πρόσβαση του χρήστη να αποκλειστεί. [7] Εξελιγμένα εργαλεία επίθεσης είναι διαθέσιμα στο διαδίκτυο και προσφέρουν αυτοματισμό στην διαδικασία εκμετάλλευσης του θύματος με οδηγίες που ακόμη και κάποιος ερασιτέχνης μπορεί να ακολουθήσει. [12] Έτσι, εγκαθιστώντας εργαλεία από το διαδίκτυο, ακόμη και

απλοί χρήστες υπολογιστή μπορούν να γίνουν DoS attackers. Οι επιθέσεις αυτές συμβαίνουν για διάφορους σκοπούς. Κάποιοι οργανισμοί τις χρησιμοποιούν για να "ρίξουν" τα δίκτυα των αντιπάλων τους και να αποκτήσουν περισσότερους πελάτες. Άλλοι στοχεύουν σε οργανισμούς που φέρουν διαφορετικές πολιτικές. Τέλος, επειδή είναι δύσκολο να πραγματοποιηθεί αυτή η επίθεση με μόνο έναν υπολογιστή, πολλές DoS attacks χρησιμοποιούν τεράστιο αριθμό από απομακρυσμένους υπολογιστές στο διαδίκτυο που έχουν ήδη "μολύνει" και υπερφορτώνουν τον στόχο πολύ πιο γρήγορα. Τέτοιου είδους επιθέσεις ονομάζονται Distributed Denial of Service (DDoS) attacks. [13]

Επιπρόσθετα, στην gateway attack στόχος είναι το link που επιτρέπει την επικοινωνία ενός τοπικού δικτύου με το διαδίκτυο. Θα μπορούσε να είναι μια DoS ή routing επίθεση στο gateway που θα στέλνονται από το διαδίκτυο άκυρες ή λανθασμένες πληροφορίες στις έξυπνες οικιακές συσκευές, όπως αισθητήρες, ενεργοποιητές και κόμβοι καθυστερώντας ή και διακόπτοντας την λειτουργία τους για κάποιο χρονικό διάστημα. [7]

Ακόμη, ένα είδος επιθέσεων λεγόμενο Storage attacks σχετίζεται με την ακεραιότητα των δεδομένων του νόμιμου χρήστη στον αποθηκευτικό χώρο του υπολογιστή του ή στο cloud. Αυτές οι επιθέσεις στοχεύουν στην απώλεια ή καταστροφή των αρχικών δεδομένων. [7]

Οι Man-In-The-Middle (MITM) επιθέσεις, πραγματοποιούνται και αυτές σε αυτό το επίπεδο και είναι πολύ συχνές και γνωστές επιθέσεις. Πρόκειται για ένα είδος επίθεσης στο οποίο ο επιτιθέμενος παίρνει τον έλεγχο στην ανταλλαγή των δεδομένων δύο έννομων χρηστών οι οποίοι επικοινωνούν. Το όνομα της επίθεσης αυτής (Man-In-The-Middle) προέρχεται από τον χώρο του μπάσκετ. Όταν δύο συμπαίκτες θέλουν να περάσουν την μπάλα ο ένας στον άλλον και υπάρχει κάποιος τρίτος παίκτης ανάμεσά τους που προσπαθεί να αρπάξει την μπάλα καλείται Man-In-The-Middle. Πρόκειται για ένα είδος επίθεσης, στο οποίο ένα κακόβουλο τρίτο μέρος κρυφά παίρνει τον έλεγχο επικοινωνίας του καναλιού μεταξύ δύο ή περισσότερων endpoints. Ο επιτιθέμενος έχει την δυνατότητα να υποκλέψει, τροποποιήσει, ή αντικαταστήσει τα δεδομένα των χρηστών. Συνεπώς, επηρεάζεται η εμπιστευτικότητα των δεδομένων καθώς ο επιτιθέμενος παίρνει τα δεδομένα που ανταλλάσσουν τα δύο ή περισσότερα μέρη που επικοινωνούν. Επηρεάζεται ακόμη η ακεραιότητα των δεδομένων καθώς μπορεί να τροποποιηθούν τα μηνύματα και η διαθεσιμότητα των δεδομένων εφόσον μπορεί να προκληθεί τερματισμός της επικοινωνίας αυτής. Τρεις βασικές κατηγορίες της MITM επίθεσης είναι αυτή που βασίζεται στην τεχνική της πλαστοπροσωπίας στην οποία ο επιτιθέμενος προσπαθεί να πείσει τα θύματα ότι είναι έγκυρο endpoint. Στην δεύτερη κατηγορία ανήκουν οι επιθέσεις MITM που βασίζονται στο μέσο επικοινωνίας στο οποίο πραγματοποιείται η επίθεση. Στην τρίτη κατηγορία ανήκουν οι επιθέσεις που βασίζονται στην γεωγραφική τοποθεσία του χρήστη και στοχεύεται το δίκτυο. Οι MITM επιθέσεις είναι γνωστές επίσης και ως Monkey-in-the middle attack, Session hijacking, TCP hijacking, TCP session hijacking. Περισσότερα σχετικά με αυτές τις επιθέσεις θα βρείτε στο 14. [14]

Άλλες επιθέσεις που σχετίζονται με την μετάδοση "ψεύτικων" μηνυμάτων στους κόμβους, για να παραστήσουν μια γειτονική συσκευή τους και να αποσπάσουν πληροφορίες του δικτύου ή επιθέσεις που σχετίζονται με την παρεμπόδιση της δρομολόγησης των πακέτων εντάσσονται σε αυτό το επίπεδο και περισσότερες σχετικές πληροφορίες παρουσιάζονται στο 7.

2.5.4 Physical layer

Στο Physical layer ανήκει κάθε είδος φυσικής καταστροφής του εξοπλισμού, των ενδιάμεσων κόμβων, αισθητήρων, ενεργοποιητών και των τελικών συσκευών που χρησιμοποιεί ο χρήστης και συμβαίνει από περιβαλλοντικό ή ανθρώπινο παράγοντα. Αφορά την αλλαγή συμπεριφοράς των συσκευών με

αποτέλεσμα να χάνουν την λειτουργικότητά τους. Περιβαλλοντικοί παράγοντες επηρεάζουν επίσης την ακεραιότητα έξυπνων οικιακών συστημάτων και συσκευών και αφορούν φυσικές καταστροφές όπως βροχή, χιόνι και καταιγίδες. [7]

Ακόμη, η απώλεια ρεύματος μπορεί επίσης να προκαλέσει πρόβλημα, σε συσκευές που δεν διαθέτουν εφεδρική πηγή ενέργειας και συνεπώς σε μια τέτοια περίπτωση θα μπουν σε λειτουργία εξοικονόμησης ενέργειας. Στην συνέχεια, μπορεί να μην λειτουργήσουν όπως αναμένεται ή και καθόλου. [7]

Μια εξίσου γνωστή επίθεση είναι το jamming. Κατά την επίθεση αυτή, τεράστια ποσότητα ραδιοκυμάτων στέλνονται στο δίκτυο ή συσκευή θύμα με συνέπεια να καταναλώνεται πολύ γρήγορα η μπαταρία της συσκευής και να παρεμποδίζεται η συσκευή ή το δίκτυο να στείλει δεδομένα. Χαρακτηρίζεται ως η συχνότερη επίθεση σε δίκτυα IoT ασύρματων αισθητήρων (WSN). [7]

Τέλος, παρεμβολή μπορεί να προκληθεί και στην λειτουργία του RFID. Όταν σταλούν τεράστιες ποσότητες σημάτων μέσω ραδιοσυχνοτήτων, η λειτουργία του RFID καθίσταται αδύνατη. [7]

2.6 Λύσεις σε επιθέσεις ανά επίπεδο IoT

Παρακάτω, σύμφωνα και με τις επιθέσεις που αναφέρθηκαν σε κάθε επίπεδο, προτείνονται λύσεις και μέτρα ασφαλείας, που καλό θα ήταν να ακολουθούνται.

2.6.1 Επίπεδο εφαρμογών

Στο επίπεδο εφαρμογών αναφέρθηκαν αρκετές επιθέσεις. Στις περισσότερες παρουσιάζονται μέτρα πρόληψης και αντιμετώπισης. Αρχικά, σχετικά με την επίθεση phishing, η αποτροπή αυτής της επίθεσης βασίζεται στην πρόληψη και την ανίχνευση. Όσον αφορά την ανίχνευση, χωρίζεται σε δύο βασικές κατηγορίες · την αντίληψη του χρήστη και την ανίχνευση του εισβολέα από λογισμικό. Υπάρχει παραδοσιακή και αυτόματη μέθοδος ανίχνευσης από λογισμικό. Η αυτόματη μέθοδος χωρίζεται επιπλέον σε δύο υποκατηγορίες, την public phishing detection toolbars και academic phishing detection / classification schemes. Παρακάτω αναλύονται περαιτέρω οι δύο βασικές μέθοδοι αποτροπής του ηλεκτρονικού “ψαρέματος”. [15]

Αναφορικά με την πρόληψη της επίθεσης αυτής, παρέχεται επιπλέον επίπεδο ασφάλειας όταν ο χρήστης συνδέεται στην συσκευή ή ιστοσελίδα. Το έξτρα επίπεδο ασφάλειας πραγματοποιείται με επιβεβαίωση γνησιότητας δύο παραγόντων (two-factor authentication), που είναι μια διαδικασία επαλήθευσης της ταυτότητας του χρήστη πριν του δοθεί πρόσβαση εισόδου στον λογαριασμό. Η διαδικασία έχει ως εξής, ο χρήστης συνδέεται με username, password στην ιστοσελίδα, και στην συνέχεια με κάποια δεύτερη ενέργεια, όπως μήνυμα στο κινητό, του στέλνεται κωδικός επιβεβαίωσης σύνδεσης στην ιστοσελίδα έγκαιρα και εισέρχεται στον λογαριασμό του. Ο κωδικός αυτός ισχύει για μερικά λεπτά. Με αυτόν τον τρόπο γίνεται πολύ πιο δύσκολο κάποιος να εισέλθει στον συγκεκριμένο λογαριασμό, καθώς χρειάζεται πρόσβαση σε ακόμα μία συσκευή, την συσκευή του χρήστη. [15]

Όσον αφορά την ανίχνευση, χωρίζεται στην επαγρύπνηση του χρήστη και στην ανίχνευση από λογισμικό, όπως ήδη αναφέρθηκε. Σχετικά με τον χρήστη, είναι σημαντικό να γνωρίζει μεθόδους απόσπασης πληροφοριών ώστε να είναι σε θέση να αναγνωρίσει μια προσπάθεια “ψαρέματος”. Πιο συγκεκριμένα, να μην εισάγει προσωπικά του δεδομένα σε ιστοσελίδες που του αποστέλλονται μέσω

SMS ή email αλλά να πληκτρολογεί ο ίδιος την ιστοσελίδα που θέλει να εισέλθει και να ελέγχει το URL πρώτα. [15]

Η ανίχνευση μέσω λογισμικού, προσπαθεί να προσδιορίσει αν η ιστοσελίδα είναι η έγκυρη ή όχι. Σύμφωνα με την παραδοσιακή μέθοδο, δημιουργείται μία blacklist στην οποία εισάγονται phishing ιστοσελίδες και ενημερώνονται ανά τακτά χρονικά διαστήματα. Το κύριο μειονέκτημα της μεθόδου αυτής είναι ότι υπάρχουν αρκετές σελίδες οι οποίες είναι παραπλανητικές και δεν ανήκουν ακόμα σε αυτή τη λίστα, δηλαδή δεν έχουν εισαχθεί ακόμα, όπως σε περιπτώσεις που οι ιστοσελίδες δημιουργούνται με μικρή διάρκεια ζωής ή αλλάζουν διεύθυνση ip ή domain name πολύ συχνά, με αποτέλεσμα να μην είναι προστατευμένος ο χρήστης σε όλες αυτές τις περιπτώσεις. Από την άλλη πλευρά, πλεονέκτημα αποτελεί το γεγονός ότι έχει μεγάλη ακρίβεια στις ιστοσελίδες που χαρακτηρίζει ως κακόβουλες. [15]

Η αυτόματη μέθοδος, συνδυάζει την blacklist προσέγγιση με μέθοδο αυτοεκπαίδευσης. Συγκεκριμένα, σύμφωνα με τα περιεχόμενα της ιστοσελίδας, προσπαθεί να προβλέψει, από τα περιεχόμενα των ιστοσελίδων της blacklist, αν και η συγκεκριμένη ιστοσελίδα είναι παραπλανητική. Αυτό πραγματοποιείται εξετάζοντας την διάταξη της ιστοσελίδας, το λεξιλόγιο που περιέχει καθώς επίσης και το URL αυτής. Ακόμη σε αυτή τη μέθοδο το λογισμικό ανιχνεύει και μπλοκάρει τις ιστοσελίδες, είτε με παθητική προειδοποίηση στην οποία απλά ενημερώνει τον χρήστη, είτε με ενεργητική προειδοποίηση στην οποία διακόπτει την φόρτωση της ιστοσελίδας και δεν επιτρέπει στον χρήστη να δει τα περιεχόμενα αυτής. [15]

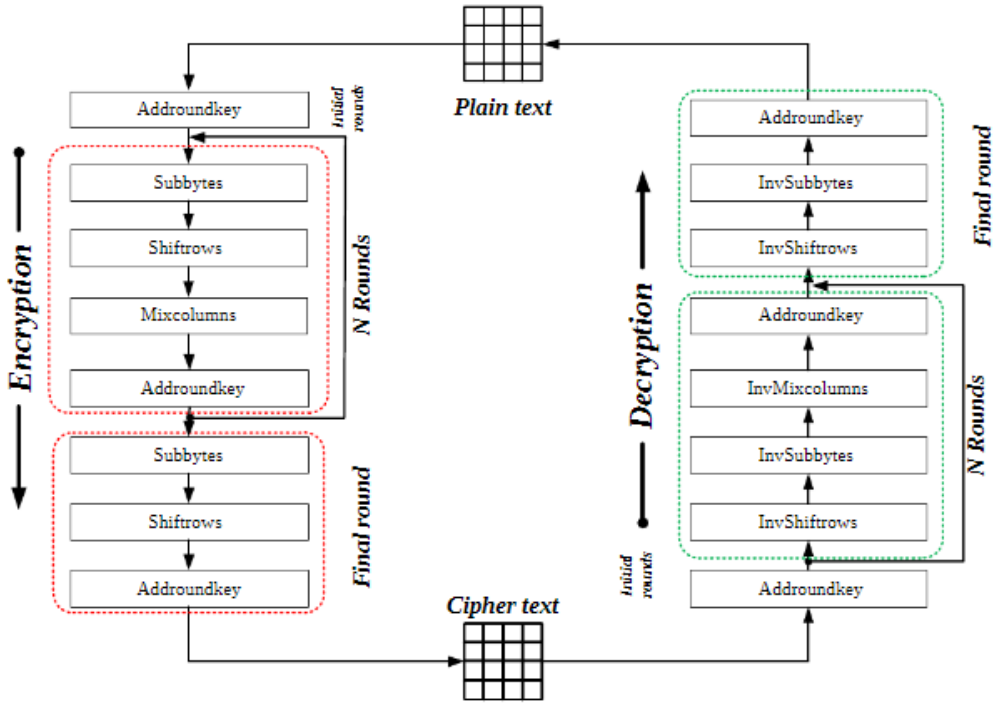
Ακόμη μια συχνή επίθεση στο επίπεδο εφαρμογών είναι η επίθεση Ransomware. Αρχικά, η συμπεριφορά των χρηστών αποτελεί σημαντικό ρόλο στην αποτροπή των επιθέσεων αυτών. Οι μικροί, επαναλαμβανόμενοι κωδικοί και ο διαμοιρασμός των προφίλ ή η σύνδεση του χρήστη σε διαφορετικό δίκτυο αποτελούν τους κύριους λόγους που πετυχαίνουν οι επιθέσεις αυτές. Καλή πρακτική από τον χρήστη είναι να μην εισέρχεται σε ιστοσελίδες που του κοινοποιούνται και να πραγματοποιούνται τακτικά αντίγραφα ασφαλείας των αρχείων που υπάρχουν στην εκάστοτε συσκευή. Ακόμη, σε περίπτωση που έχει πραγματοποιηθεί η επίθεση, προτείνεται να αποσυνδέεται η συσκευή από το ρεύμα όσο το δυνατόν νωρίτερα και στην διαδικασία backup να εξακριβωθεί ότι το αντίγραφο ασφαλείας δεν συνδέεται κάπως με την “μολυσμένη” συσκευή. Ακόμη, προτείνεται η απομόνωση της συσκευής αυτής από το δίκτυο το συντομότερο δυνατό, διότι πρόκειται για μια ταχεία μεταδιδόμενη επίθεση. Τέλος, συστήνεται ο χρήστης να μην πληρώνει το αντίτιμο που θέτει ο επιτιθέμενος για να του δώσει πίσω τα δεδομένα του. [16]

2.6.2 Perception layer

Στο Perception layer κύριο πρόβλημα αποτελεί η μεταφορά των δεδομένων και κατά πόσο αυτά είναι φανερά σε τρίτους. Συνεπώς, κρίνεται σημαντικό να αναφερθούν κάποιοι αλγόριθμοι κρυπτογράφησης. Μερικοί από αυτούς είναι οι DES, AES, RC6, RC2, IDEA και RSA, ECC, EES οι οποίοι είναι συμμετρικοί ή ασύμμετροι. Παρακάτω, παρουσιάζονται συνοπτικά τρεις αλγόριθμοι κρυπτογράφησης · ο AES, ο DES και ο RSA.

Ο αλγόριθμος Advanced Encryption Standard (AES), κατά την διαδικασία της κρυπτογράφησης κωδικοποιεί δέκα κύκλους, για κλειδιά μεγέθους 128 bits, δώδεκα κύκλους για κλειδιά 192 bits και δεκατέσσερις κύκλους για κλειδιά των 256 bits. Ο AES αφήνει 128 bits μέγεθος πληροφορίας, το οποίο μπορεί να χωριστεί σε τέσσερα κύρια ενεργά μπλοκ. Αυτά τα μέρη διαχειρίζονται σαν μια γραμμή από

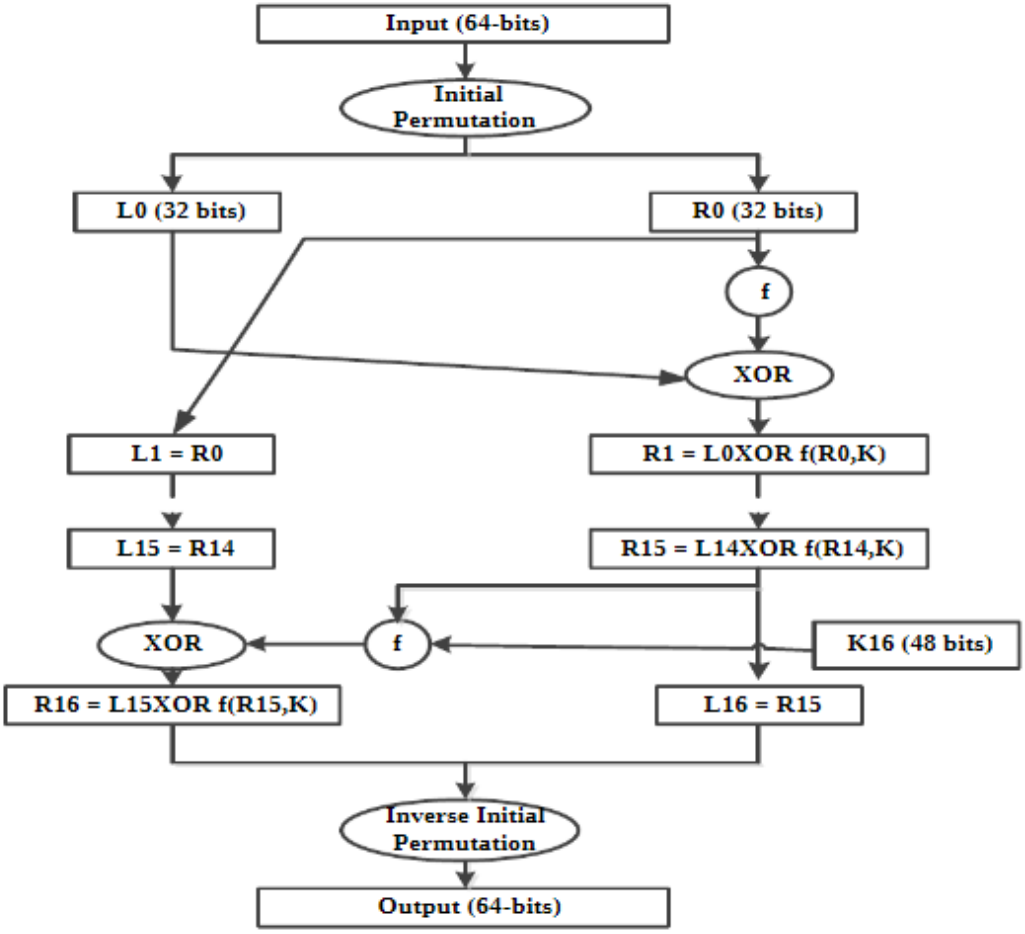
byte και συνδυάζουν έναν πίνακα τέσσερα επί τέσσερα ονομαζόμενο “state”. Η διαδικασία έχει ως εξής, στην κρυπτογράφηση και αποκρυπτογράφηση η κωδικοποίηση ξεκινά με μία διαδικασία “Στάδιο προσθήκης κυκλικού κλειδιού”. Χρησιμοποιείται δηλαδή το ίδιο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση. Στην συνέχεια, για εννιά φορές επαναλαμβάνει τις διαδικασίες Sub-bytes, Shift-rows, Mix-columns και Add round Key. Οι διαδικασίες αυτές ισχυροποιούν την ασφάλεια του αρχικού κειμένου. Στην δέκατη και τελευταία επανάληψη η διαδικασία mix-columns transformation δεν είναι πλέον διαθέσιμη ενώ οι υπόλοιπες πραγματοποιούνται κανονικά. Τέλος, στην αποκρυπτογράφηση πραγματοποιούνται οι ίδιες διαδικασίες απλά αντίστροφα. Παρακάτω παρουσιάζονται σε μορφή σχεδιαγράμματος οι προαναφερθείσες διεργασίες. [17]



Εικόνα 1. Advanced Encryption Standard process [17]

Αναφορικά με τον DES αλγόριθμο, οι οδηγίες κωδικοποίησης είναι ότι λαμβάνει δεδομένα μήκους 64 bits και 56 bits κλειδί και καταλήγει με μπλοκ μήκους 64 bits. Το μπλοκ απλού κειμένου χρειάζεται να μετατραπεί σε bits. Το αναγνώσιμο μήνυμα και το κλειδί παράγονται από τις παρακάτω διαδικασίες. Το κλειδί χωρίζεται στην μέση (28 bits - 28 bits). Κάθε μισό εναλλάσσεται με ένα ή δύο bits, ανάλογα τον γύρο. Τα δύο μέρη ξανά ενώνονται και υποβάλλονται σε έναν κύκλο μείωσης του κλειδιού από 56 σε 48 bits. Αυτά τα συμπιεσμένα κλειδιά χρησιμοποιούνται για την κρυπτογράφηση του μπλοκ απλού κειμένου. [17]

Στην κρυπτογράφηση του απλού κειμένου απαιτείται το κλειδί στην φάση που έχει χωριστεί στην μέση και το κάθε μισό έχει εναλλαχθεί με bits. Τα μπλοκ δεδομένων χωρίζονται και αυτά σε δύο μέρη των 32 bits το καθένα. Το ένα μέρος θα υποβληθεί σε διαδικασία αύξησης του μεγέθους του κατά 16 bits (μπλοκ μεγέθους 48 bits). Στην συνέχεια πραγματοποιείται η λογική πράξη OR ανάμεσα στο κλειδί και το μπλοκ δεδομένων των 48 bits, το αποτέλεσμα θα υποβληθεί σε s-box, στο οποίο αντικαθίστανται τα bits του κλειδιού και μειώνεται το μήκος αυτού που θα προκύψει σε 32 bits. Και τέλος, το αποτέλεσμα αυτό υποβάλλεται σε p-box και στην συνέχεια πραγματοποιείται η λογική πράξη αποκλειστικό OR. Παρακάτω παρουσιάζεται το διάγραμμα ροής του αλγορίθμου για καλύτερη κατανόηση. [17]



Εικόνα 2. Διάγραμμα ροής αλγορίθμου DES [17]

Κλείνοντας, ο αλγόριθμος RSA εφαρμόζει μπλοκ διαφορετικού μεγέθους κρυπτογράφησης και μεταβλητού μεγέθους κλειδί. Πρόκειται για ένα ασύμμετρο σύστημα κωδικοποίησης που βασίζεται σε αριθμητική σύνθεση. Χρησιμοποιεί δύο βασικούς αριθμούς για να προκύψει το δημόσιο και ιδιωτικό κλειδί. Ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του και το μήνυμα αποστέλλεται στον παραλήπτη. Ο παραλήπτης στην συνέχεια το αποκρυπτογραφεί χρησιμοποιώντας το ιδιωτικό του κλειδί. Ο συγκεκριμένος αλγόριθμος έχει τρία βασικά βήματα τα οποία είναι η παραγωγή του κλειδιού, η κρυπτογράφηση και η αποκρυπτογράφηση. Περισσότερες πληροφορίες σχετικά με τους αλγόριθμους κρυπτογράφησης αναλύονται στο [17]. [17]

2.6.3 Network layer

Στο επίπεδο δικτύου περιγράφονται τρόποι και μέθοδοι αποτροπής και αντιμετώπισης δύο βασικών επιθέσεων που πραγματοποιούνται σε αυτό το επίπεδο · Denial of Service επιθέσεις και Man-In-The-middle επιθέσεις. Ξεκινώντας με τις επιθέσεις DoS και DDos, όπως έχει ήδη αναφερθεί ο επιτιθέμενος στοχεύει στους υπολογιστικούς πόρους του θύματος, όπως CPU, μνήμη, αλλά και bandwidth και υποδομή δικτύου. Λόγω της φύσης της επίθεσης αυτής, η οποία στοχεύει στην άρνηση εξυπηρέτησης του θύματος σε κάποιο πόρο, διεργασία ή υπηρεσία, σίγουρα προτιμάται η αποτροπή της επίθεσης παρά η αντιμετώπισής της όταν έχει υλοποιηθεί. Επομένως, παρακάτω παρουσιάζονται κάποιοι τρόποι προφύλαξης των χρηστών και στην συνέχεια αναλύονται τρόποι ανίχνευσης της επίθεσης Dos, DDos. [18]

Αρχικά, προτείνεται η χρήση φίλτρων κατά την διακίνηση των δεδομένων, ώστε να αποκλείεται κακόβουλη κυκλοφορία από ή προς το δίκτυο. Με αυτόν τον τρόπο, προστατεύεται ο χρήστης και από την επίθεση και από το να γίνει η συσκευή του κακόβουλη προς άλλες, χωρίς να το γνωρίζει. Οι τεχνικές στην χρήση φίλτρων είναι αρκετές και παρέχουν σε μικρό ή μεγαλύτερο βαθμό προστασίας στον χρήστη. [18]

Μια πολύ γνωστή μέθοδος φιλτραρίσματος δεδομένων είναι εκείνη που ελέγχει εισερχόμενα και εξερχόμενα δεδομένα στο δίκτυο. Αυτή η τεχνική αποτρέπει από το να μπουν δεδομένα με "ψεύτικη" IP σε ένα προστατευμένο δίκτυο. Κατά την εξαγωγή δεδομένων από το δίκτυο, ελέγχεται αν η IP ανήκει στο δίκτυο αυτό και αν όχι απλά απορρίπτεται από το δρομολογητή. Ακόμη, όσον αφορά στα δεδομένα που εισέρχονται στο δίκτυο, η μέθοδος αυτή παρουσιάζει μεγάλη επιτυχία στην εύρεση των κακόβουλων πακέτων με "spoofed IPs". Ωστόσο, σε επίθεση DDos στην οποία η IP του αποστολέα ανήκει σε κάποιο ανυποψίαστο θύμα και δεν είναι ψεύτικη, η τεχνική αυτή δεν μπορεί να ανιχνεύσει τον κακόβουλο, επιτρέποντας κανονικά στα δεδομένα να εισέλθουν στο δίκτυο, όμως μπορεί να περιοριστεί ο αριθμός των πακέτων που δέχεται μια συσκευή ανά δευτερόλεπτο με σκοπό την σωστή λειτουργία της. [18]

Ακόμη μια τεχνική αποτροπής κακόβουλων δεδομένων στο δίκτυο είναι εκείνη που βασίζεται στην διαδρομή του πακέτου (Route-based packet filtering). Πιο συγκεκριμένα, προσθέτοντας κάποιες επιπλέον ρυθμίσεις στο κεντρικό (ή κεντρικά) router, εκείνο δέχεται δεδομένα από συγκεκριμένες source IPs που γνωρίζει. Αυτή η μέθοδος απαιτεί συγκεκριμένη διαδρομή των δεδομένων ώστε να περνούν όλα από κάποιο/α router που διαθέτουν αυτές τις ρυθμίσεις οπότε απαιτεί πληροφορίες του Border Gateway Protocol (BGP) για την τοπολογία της δρομολόγησης. Τέλος, οι ρυθμίσεις αυτές στους δρομολογητές πρέπει να ενημερώνονται τακτικά, και η μέθοδος αυτή είναι αναποτελεσματική, στην περίπτωση που κάποιος επιτιθέμενος υποκλέψει BGP sessions και μάθει πληροφορίες σχετικά με τις IPs που δέχεται το δίκτυο, και χρησιμοποιήσει αυτές. [18]

Άλλες τεχνικές που βασίζονται στην διαδρομή των δεδομένων, τον αριθμό των δρομολογητών που πέρασαν τα δεδομένα αλλά και την πιθανότητα ένα πακέτο να προέρχεται από έννομο χρήστη, βάση των χαρακτηριστικών του, παρουσιάζονται στο [18].

Μια ακόμη μέθοδος αποτροπής επιθέσεων DDos η οποία προστατεύει ένα υποδίκτυο είναι η Secure overlay. Βασίζεται στην ιδέα της δημιουργίας ενός δικτύου το οποίο θα "καλύπτει" το πραγματικό και κάθε εξωτερική διακίνηση δεδομένων θα φτάνει πρώτα εκεί και στην συνέχεια αυτό το δίκτυο θα επικοινωνεί με ασφάλεια με το πραγματικό. Θεωρείται ότι η απομόνωση του δικτύου γίνεται κρύβοντας τις IP διευθύνσεις του ή χρησιμοποιώντας ένα διανεμημένο τείχος προστασίας (firewall). Ωστόσο, αυτή η μέθοδος μπορεί να εφαρμοστεί με επιτυχία κυρίως σε ιδιωτικά δίκτυα και όχι σε δημόσιους εξυπηρετητές (servers). [18]

Μια όχι και τόσο γνωστή μέθοδος αποτροπής επιθέσεων DDos είναι η Honeypots/Honeynets. Πρόκειται για ένα μέρος του δικτύου που αποτελείται από συσκευές οι οποίες είναι λιγότερο ασφαλείς και όταν τους επιτεθούν, ανιχνεύουν, αναλύουν και εμποδίζουν τις επιθέσεις από το να εξαπλωθούν στο δίκτυο. [19] Με αυτόν τον τρόπο, μπορούν να εξαχθούν χρήσιμες πληροφορίες για την επίθεση σχετικά με τις τεχνικές του επιτιθέμενου, το λογισμικό και άλλα εργαλεία που χρησιμοποίησε καθώς επίσης την δραστηριότητά του στην συσκευή. Κύρια μειονεκτήματα του μηχανισμού αυτού είναι ότι μπορεί ο επιτιθέμενος να ανακαλύψει ότι δεν πρόκειται για πραγματική συσκευή, και τα honeypots μπορεί να μην ανιχνεύσουν την επίθεση και τα πακέτα του επιτιθέμενου να προωθηθούν στο δίκτυο. [18]

Επίσης, μια προσέγγιση που προσπαθεί να ισορροπήσει την επιβάρυνση κάθε συσκευής ώστε καμία να μην υπερφορτώνεται, ονομάζεται load balancing. Η τεχνική αυτή βοηθάει στην ταχύτητα δρομολόγησης των πακέτων. Επομένως, σε μια περίπτωση DDos επίθεσης σε κάποια συσκευή με αποτέλεσμα την υπερφόρτωση της, φροντίζεται η διαδρομή για τα υπόλοιπα πακέτα να περνάει από άλλες συσκευές για να προωθηθούν και γρηγορότερα, βοηθώντας έτσι το δίκτυο να μείνει σχεδόν ή και ολοκληρωτικά ανεπηρέαστο. [18]

Τέλος, πρακτικές όπως αλλαγή IP διευθύνσεων των συσκευών, απενεργοποίηση αχρησιμοποίητων υπηρεσιών, συχνή αλλαγή των κωδικών στις έξυπνες συσκευές και η τακτική ενημέρωση του συστήματος αποτελούν κάποιες απλές τακτικές που μπορεί να εφαρμόσει κάθε χρήστης και να βοηθήσει στην αποτροπή τέτοιου είδους επιθέσεων. [18]

Αναφορικά με την ανίχνευση επιθέσεων DoS, DDoS είναι πολύ απλή κυρίως γιατί μετά από μια τέτοια επίθεση οι λειτουργίες του συστήματος υποβαθμίζονται δραματικά. Το βασικό ζήτημα παραμένει στο πως μπορεί να ανιχνευτεί το κακόβουλο από το νόμιμο traffic και έτσι υπάρχουν δύο κατηγορίες που διαφοροποιούν αυτά τα δύο διαφορετικά είδη δεδομένων που διακινούνται στο δίκτυο. Αυτά είναι η ανίχνευση με βάση την ψηφιακή υπογραφή και η ανίχνευση με βάση ανωμαλίες του συστήματος. [18]

Η ανίχνευση με βάση την ψηφιακή υπογραφή, ουσιαστικά βασίζεται στις γνωστές επιθέσεις DDoS με σκοπό να ταυτοποιήσει τις υπογραφές της επίθεσης και να διαφοροποιήσει τα δύο προαναφερθέντα είδη δεδομένων. Κάποια εργαλεία ανίχνευσης είναι τα Management information base traffic variable correlation (MIB), Bro, SNORT. Στο MIB αναλύονται δεδομένα που αφορούν στην διαχείριση του συστήματος, το Bro είναι ένα σύστημα ανίχνευσης εισβολής σε δίκτυο, σε πραγματικό χρόνο, ενώ το SNORT είναι και αυτό ένα εργαλείο ανίχνευσης. [18]

Στον μηχανισμό ανίχνευσης με βάση ανωμαλίες μπορούν να διαχειριστούν επιθέσεις με καινούργιες υπογραφές, καθώς εμφανίζονται συχνά νέες επιθέσεις. Το βασικό θέμα σε αυτόν τον μηχανισμό είναι η διαφοροποίηση των δεδομένων καθώς δεν είναι γνωστές οι επιθέσεις και οι υπογραφές αυτές. Μερικά παραδείγματα τέτοιων μεθόδων είναι τα MULTOPS και DWARD. Το Multi-Level Tree for Online Packet Statistics (MULTOPS) είναι μία τεχνική ανίχνευσης επιθέσεων που στοχεύουν στο bandwidth της συσκευής. Και το DWARD είναι μία τεχνική ανίχνευσης και περιορισμού του ρυθμού λειτουργίας που χρησιμοποιείται κοντά στην πηγή της επίθεσης. Περισσότερα σχετικά με τις μεθόδους ανίχνευσης στις Dos, DDos επιθέσεις περιγράφονται στο [18]. [18]

Οι επιθέσεις MITM χωρίζονται σε τέσσερις βασικές κατηγορίες και αντίστοιχα αντιμετωπίζεται κάθε μία από αυτές. Χωρίζονται στις Spoofing-based MITM, SSL/TLS MITM, BGP MITM και False Base Station based (FBS-based) MITM. [14]

Οι spoofing attacks χωρίζονται σε ARP, DNS, DHCP, IP spoofing-based MITM επιθέσεις. Σε όλα τα προηγούμενα είδη, οι επιτιθέμενοι εκμεταλλεύονται τις αδυναμίες των αντίστοιχων πρωτοκόλλων με κύρια την έλλειψη εξακρίβωσης αυθεντικότητας των μηνυμάτων αποστολέα και παραλήπτη. Στις spoofing επιθέσεις ο επιτιθέμενος μιμείται μία συσκευή ή χρήστη του δικτύου. Περιγράφεται από κάποια άρθρα ως το πρώτο βήμα ή ένα από τα πρώτα βήματα για την εκτέλεση της MITM επίθεσης, ενώ άλλοι το αναφέρουν ως μία κατηγορία της επίθεσης αυτής. Στο συγκεκριμένο είδος επίθεσης, ο επιτιθέμενος παρεμβάλλεται ανάμεσα στους χρήστες και διαμορφώνει τα δεδομένα της επικοινωνίας τους χωρίς εκείνοι να το γνωρίζουν. Στις ARP Spoofing επιθέσεις, σύμφωνα και με την διαδικασία που ακολουθείται στο ARP, ο επιτιθέμενος στέλνει λανθασμένη φυσική διεύθυνση στους υπόλοιπους χρήστες, οι οποίοι ενημερώνουν την ARP cache τους και όταν χρειαστεί να στείλουν σε αυτή τη διεύθυνση κάποιο μήνυμα, το στέλνουν στον επιτιθέμενο. Επομένως, ο επιτιθέμενος μπορεί να

προσποιηθεί κάποιο χρήστη στο εσωτερικό του δικτύου ή την default gateway. [14] Στο 14 προτείνονται αρκετά εργαλεία και προγράμματα που βοηθούν στην ανίχνευση τέτοιων επιθέσεων, αν και πολλά από αυτά ακόμα δεν είναι ολοκληρωτικά διαθέσιμα και δεν είναι πάντοτε αποτελεσματικά. Ωστόσο λειτουργούν σε πολλές περιπτώσεις και κάποια με μειωμένο κόστος. Τα υπόλοιπα είδη επιθέσεων spoofing παρουσιάζονται στο 14 και είναι παρόμοια στην αντιμετώπιση με τις ARP spoofing επιθέσεις.

Η SSL/TLS MITM επίθεση βασίζεται στην επαλήθευση του πιστοποιητικού. Συνεπώς οι επιτιθέμενοι στοχεύουν στην δημιουργία, την υποκλοπή του πιστοποιητικού, ή την υποκλοπή ιδιωτικού κλειδιού από έναν πραγματικό εξυπηρετητή (server). Με αυτόν τον τρόπο, ο επιτιθέμενος μπαίνει ανάμεσα στην επικοινωνία client - server, και διαμοιράζει στον client το πιστοποιητικό που έκλεψε ή δημιούργησε και δημιουργεί επικοινωνία με τον client. Στην συνέχεια φτιάχνει μια επικοινωνία με έναν εξυπηρετητή και έτσι μπορεί να ελέγχει την επικοινωνία των δύο μερών. Η ανίχνευση μιας τέτοιας επίθεσης βασίζεται στην αναγνώριση αυθεντικότητας του πιστοποιητικού, όμως στην περίπτωση υποκλοπής του αυθεντικού, αυτός ο τρόπος είναι αναποτελεσματικός. [14]

Η BGP MITM επίθεση βασίζεται στην υποκλοπή της IP διεύθυνσης. Αυτό συμβαίνει όταν ένας κακώς διαμορφωμένος speaker BGP, στέλνει μηνύματα στους ομότιμούς του στα οποία αναφέρει το prefix ενός υποδικτύου με αποτέλεσμα να δίνει πληροφορίες σε επιτιθέμενους αν αυτοί παρακολουθούν την «συζήτηση». Η αποτροπή μιας τέτοιας επίθεσης βασίζεται στην κρυπτογραφία, την παρατήρηση και μετρίαση των ανωμαλιών σχετικά με την υποκλοπή IPs. Περισσότερες πληροφορίες σχετικά με τις επιθέσεις MITM βρίσκονται στο 14. [14]

2.6.4 Physical layer

Στο φυσικό επίπεδο όπως ήδη αναφέρθηκε πραγματοποιούνται φυσικές καταστροφές στον εξοπλισμό και τις συσκευές, από ανθρώπινο ή περιβαλλοντικό παράγοντα. Ακόμη σε αυτό το επίπεδο ανήκουν και οι επιθέσεις στις οποίες ο επιτιθέμενος έχει πρόσβαση στην συσκευή με φυσικό τρόπο. Επομένως, η προστασία των συσκευών και η φύλαξη τους σε ειδικά διαμορφωμένο χώρο μπορεί να βοηθήσει στην προστασία τους. Επίσης, η απόκτηση εφεδρικής πηγής ενέργειας θα βοηθήσει στην περίπτωση απώλειας ρεύματος στις συσκευές.

Τέλος, αναφορικά με τις jamming επιθέσεις κάποιοι τρόποι ανίχνευσής τους είναι αρχικά η παρακολούθηση της ποιότητας του link και άλλων παραμέτρων απόδοσης. Για παράδειγμα η μέτρηση του packet delivery ratio και packet send ratio, στην πλευρά του πομπού, είναι πολύ σχετικές τιμές με την επίθεση jamming. Το packet delivery ratio είναι η αναλογία των πακέτων που θα φτάσουν επιτυχώς στον προορισμό προς το σύνολο των πακέτων που στάλθηκαν, ενώ το packet send ratio είναι το σύνολο των πακέτων που στάλθηκαν προς το σύνολο των πακέτων που προοριζόταν να σταλούν σε συγκεκριμένο χρονικό διάστημα. Άλλες εξίσου χρήσιμες μετρικές είναι η ενεργειακή κατανάλωση και το bad packet ratio. Το bad packet ratio ορίζεται ως το πλήθος των πακέτων που στάλθηκαν ανεπιτυχώς προς το συνολικό πλήθος των πακέτων που έφτασαν στον προορισμό. Για περισσότερες πληροφορίες σχετικά με τεχνικές anti jamming προτείνεται το 20. [20]

2.7 Παραδοσιακές τεχνικές εκπαίδευσης

Παρακάτω κρίνεται σημαντικό να αναφερθούν κάποιες παραδοσιακές τεχνικές εκπαίδευσης των χρηστών για την αποφυγή επιθέσεων. Μια τεχνική επιμόρφωσης βασίζεται στις διαλέξεις σε μια ομάδα ενδιαφερόμενων. Πραγματοποιούνται από έναν καθηγητή, είναι διαδραστικός τρόπος μάθησης όμως βασίζεται στο ενδιαφέρον και την επιμονή του "μαθητή" διαφορετικά δεν θα έχει τα επιθυμητά αποτελέσματα. [1]

Ακόμη μερικές μέθοδοι επιμόρφωσης είναι εκείνες που βασίζονται στον γραπτό λόγο ή σε βιντεοδιαλέξεις. Και οι δύο τεχνικές μπορούν να πραγματοποιηθούν όποτε το επιθυμεί ο χρήστης, απλά είναι πιο αποδοτική η εκμάθηση μέσω βιντεοδιαλέξεων λόγω της διαδραστικότητας. [1]

Επιπρόσθετα, η μέθοδος που συνδυάζει τις δύο προαναφερθείσες μεθόδους (text-based, video-based training) και την εκπαίδευση μέσω παιχνιδιών (game-based training) είναι πολύ αποτελεσματική γιατί προσφέρει στον χρήστη ευελιξία να επιμορφώνεται όποτε αυτός το επιθυμεί και για όσο μπορεί και αλληλεπίδραση μέσω των βίντεο και παιχνιδιών. Ακόμη, η μέθοδος εκπαίδευσης με προσομοίωση μοιάζει αρκετά στην προηγούμενη μέθοδο με κύριο μειονέκτημα την καθυστέρηση που μπορεί να υπάρχει στις εφαρμογές προσομοίωσης και το γεγονός ότι δεν προσφέρεται ανάδραση μεταξύ του εκπαιδευτή και του εκπαιδευόμενου. [1]

Οι τελευταίες μέθοδοι βασίζονται στην από απόσταση εκπαίδευση. Πρόκειται για την game-based μέθοδο, στην οποία μέσω των παιχνιδιών κυβερνοασφάλειας οι χρήστες ακολουθούν μία σειρά από κανόνες και επιλογές που τους δίνονται ολοκληρώνοντας έτσι κάθε εργασία (task) που τους ανατίθεται. Μία άλλη μέθοδος βασίζεται στην μάθηση μέσω ρυθμίσεων και δοκιμών που κάνουν οι χρήστες σε εικονικά περιβάλλοντα, ώστε και να μην υπάρχει το άγχος για βλάβη στο σύστημα και με πρακτικό τρόπο οι χρήστες να εξοικειωθούν με τις δύσκολες έννοιες της ασφάλειας. Τέλος, μια εξίσου διαδραστική τεχνική εκπαίδευσης είναι εκείνη που βασίζεται στις διαλέξεις με καθηγητή και εξάσκηση του πρακτικού μέρους σε περιβάλλον. Με αυτόν τον τρόπο, επιτρέπεται στους εκπαιδευόμενους να μαθαίνουν τόσο το θεωρητικό όσο και το πρακτικό μέρος της ύλης. [1]

2.8 Προβλήματα μεθόδων εκπαίδευσης

Κρίνεται χρήσιμο να παρουσιαστούν και μερικά προβλήματα αυτών των μεθόδων επιμόρφωσης σε θέματα ασφάλειας έξυπνων οικιακών συσκευών, για να γίνει αντιληπτή και η δυσκολία πραγματοποίησής τους.

Μερικά από τα προβλήματα που αντιμετωπίζουν οι παραδοσιακές τεχνικές εκπαίδευσης είναι προσωπικοί και οικονομικοί περιορισμοί. Ο περιορισμένος χρόνος των χρηστών, η άγνοια αναφορικά στις επιθέσεις και τα θέματα ασφάλειας αλλά και τα αναποτελεσματικά προγράμματα εκπαίδευσης είναι ακόμα μερικοί λόγοι που οι παραδοσιακές μέθοδοι δεν λειτουργούν. Επίσης, απαιτείται πολλή προσήλωση από τους εκπαιδευόμενους για την κατανόηση των δύσκολων πρακτικών και εννοιών για την ασφάλεια των έξυπνων οικιακών συσκευών, κάτι το οποίο είναι αρκετά δύσκολο λόγω των αυξημένων υποχρεώσεων της σύγχρονης εποχής. [1]

Στους προσωπικούς και οικονομικούς λόγους αποστροφής των χρηστών από την εκπαίδευσή τους δεν ανήκει μόνο το κόστος της εκπαίδευσης αλλά και η έλλειψη ενδιαφέροντος και κινήτρου που πιθανώς έχουν πολλοί χρήστες.

2.9 Επίλογος

Το δεύτερο κεφάλαιο αναφέρθηκε στις επιθέσεις και τις μεθόδους εκπαίδευσης των χρηστών καθώς και σε κάποιες μεθόδους αποτροπής των επιθέσεων. Αρχικά, παρουσιάστηκαν σημαντικά στατιστικά επιθέσεων τα τελευταία χρόνια, πρόσφατες τεχνολογίες και τον ρόλο τους στις επιθέσεις. Οι τεχνολογίες που παρουσιάστηκαν ήταν το Διαδίκτυο των Πραγμάτων, η Εικονική Πραγματικότητα και η Επαυξημένη Πραγματικότητα. Επίσης παρουσιάστηκε ο όρος έξυπνο σπίτι με κάποιες βασικές τεχνολογίες που χρησιμοποιούνται στην λειτουργία του. Στην συνέχεια, αναλύθηκαν συχνές επιθέσεις σε έξυπνες οικιακές συσκευές ανά επίπεδο IoT και λύσεις στις επιθέσεις αυτές πάλι ανά επίπεδο. Διασαφηνίστηκαν μέτρα και μέθοδοι που μπορούν να αξιοποιηθούν για την αντιμετώπιση ή την ανίχνευση των επιθέσεων αυτών. Και τέλος, έγινε αναφορά σε παραδοσιακές τεχνικές εκπαίδευσης των χρηστών σε ζητήματα ασφάλειας σε έξυπνες οικιακές συσκευές καθώς και προβλήματα που φέρουν αυτές οι τεχνικές.

Κεφάλαιο 3ο: Πρότυπα και απαιτήσεις ασφάλειας

3.1 Εισαγωγή

Στο τρίτο κεφάλαιο αρχικά διευκρινίζονται οι απαιτήσεις που πρέπει να λαμβάνονται υπόψιν κατά την διαδικασία υλοποίησης έξυπνων οικιακών συσκευών. Στην συνέχεια, παρουσιάζονται κάποια πρωτόκολλα και πρότυπα ασφάλειας που χρησιμοποιούνται σε τέτοιου είδους συσκευές, καθώς καταγράφονται και κάποιοι οργανισμοί που βοηθούν στην περαιτέρω ανάπτυξη των προτύπων ασφάλειας. Τέλος, αξιολογούνται τα πρότυπα σύμφωνα με την χρήση τους σε ένα smart home.

3.2 Απαιτήσεις Ασφάλειας

Από τα πρώτα στάδια της σχεδίασης έξυπνων οικιακών συσκευών και συστημάτων είναι απαραίτητο να μελετώνται και να λαμβάνονται υπόψιν βασικές απαιτήσεις που πρέπει να εξυπηρετούνται από τις συσκευές αυτές. Με σκοπό την διασφάλιση εξακρίβωσης του αποστολέα, την επίτευξη εμπιστευτικότητας και ακεραιότητας των δεδομένων που ανταλλάσσουν οι συσκευές αυτές μεταξύ τους καθώς επίσης και την ασφαλή αποθήκευση και επεξεργασία των πληροφοριών αυτών από τους κατασκευαστές. Η διασφάλιση εξακρίβωσης του αποστολέα σχετίζεται με την σιγουριά ότι αυτός που στέλνει το μήνυμα είναι και αυτός που υπογράφει σαν αποστολέας σε αυτό. Η εμπιστευτικότητα βασίζεται στην βεβαιότητα ότι μόνο ο έννομος παραλήπτης μπορεί να διαβάσει το περιεχόμενο του μηνύματος και η ακεραιότητα βεβαιώνει ότι το μήνυμα δεν τροποποιήθηκε από τρίτους παρά μόνο από τον αποστολέα.

Η ασφάλεια και προστασία των δεδομένων που συλλέγονται από τους οικιακούς αισθητήρες αποτελεί μια σημαντική ανησυχία. Τα δεδομένα αποθηκεύονται σε εξυπηρετητές στο cloud, fog ή ακόμη και τοπικά δίκτυα. Σύμφωνα με το World Economic Forum, το 92,1% του παγκόσμιου πληθυσμού βασίζεται στο 10% αυτών που συνδέονται στο διαδίκτυο. [21]

Παρακάτω παρουσιάζονται βασικές απαιτήσεις ασφάλειας έξυπνων συσκευών οι οποίες προφυλάσσουν το σύστημα από ανεπιθύμητους εισβολείς.

Οι απαιτήσεις ασφάλειας σε έξυπνα οικιακά συστήματα μπορούν να χωριστούν σε δύο βασικές κατηγορίες · τις απαιτήσεις που στοχεύουν στην αποφυγή εξωτερικών απειλών και σε αυτές που προέρχονται από το εσωτερικό του συστήματος.

Στην πρώτη κατηγορία απαιτήσεων ανήκει η κρυπτογράφηση των δεδομένων, η παρακολούθηση του δικτύου και η αυθεντικοποίηση του χρήστη. [22]

Η κρυπτογράφηση αποτελεί μια από τις πιο σημαντικές απαιτήσεις ασφάλειας σε συστήματα smart home τα οποία κατά κύριο λόγο διαχειρίζονται από smartphones. Καθώς, η επικοινωνία του συστήματος με το τηλέφωνο πραγματοποιείται μέσω του internet, αρχίζουν να υπάρχουν πολλά προβλήματα κυβερνοασφάλειας. Όπως έχει ήδη αναφερθεί πολλές επιθέσεις ελέγχουν, παρακολουθούν και επηρεάζουν την επικοινωνία μεταξύ των συσκευών. Επομένως, με την κρυπτογράφηση των δεδομένων αυτές οι επιθέσεις περιορίζονται. Ο πιο συχνά χρησιμοποιούμενος συμμετρικός αλγόριθμος κρυπτογράφησης είναι ο AES, λίγα λόγια για τον οποίο αναφέρονται στο κεφάλαιο δύο. Ενώ σχετικά με τους ασύμμετρους χρησιμοποιούνται περισσότερο οι RSA, SHA, ECC, DH. Όλοι αυτοί οι

αλγόριθμοι είναι πολύ χρήσιμοι και αρκετά αξιόπιστοι, όμως λόγω και της ετερογενούς φύσης των smart home συστημάτων απαιτείται ένας συνδυασμός τους, που δεν έχει ακόμη δημιουργηθεί. [22]

Λόγω των πολλών συσκευών που χρειάζεται να επικοινωνήσουν σε ένα έξυπνο οικιακό δίκτυο, και των πολλών πρωτοκόλλων επικοινωνίας που χρησιμοποιούνται σε αυτό, κρίνεται σημαντική η διαδικασία παρακολούθησης του traffic του δικτύου για καλύτερη ασφάλειά του. Στο 23, οι συγγραφείς προτείνουν ένα framework που αποσκοπεί στην ασφάλεια συστημάτων έξυπνου σπιτιού. Στο συγκεκριμένο framework αναλύονται τα δεδομένα που ανταλλάσσονται στο δίκτυο με συστήματα Intrusion Detection (IDS) και χρησιμοποιείται ένα έξυπνο gateway με τείχος προστασίας εσωτερικά και εξωτερικά του (πριν εισέλθουν ή εξέλθουν τα δεδομένα από το δίκτυο). [22]

Για την επικοινωνία ανάμεσα στο smartphone και τις έξυπνες συσκευές του συστήματος που ελέγχονται από αυτό, απαιτείται μια εφαρμογή. Επομένως, είναι σημαντικό να ελέγχεται η πρόσβαση στην εφαρμογή και η εμπιστευτικότητα των δεδομένων που ανταλλάσσονται από αυτή. Αρχικά, αναφορικά με την αυθεντικοποίηση του χρήστη προτείνονται μέθοδοι όπως χρήση κωδικού, δακτυλικού αποτυπώματος ή αναγνώρισης προσώπου. Συνήθως, η διαδικασία αυθεντικοποίησης βασίζεται σε μία hash function. [22]

Στην δεύτερη κατηγορία απαιτήσεων ανήκουν η φυσική προστασία, η διαθεσιμότητα των συσκευών και η εξακρίβωση αυθεντικότητας των συσκευών. Αναφορικά με την φυσική προστασία των συσκευών, απαιτείται η φύλαξή τους σε ειδικά διαμορφωμένους χώρους οι οποίοι φυλάσσονται και παρακολουθούνται. Η διαθεσιμότητα αναφέρεται στην δυνατότητα πρόσβασης σε δεδομένα και υπηρεσίες της συσκευής όλη την ώρα, ακόμα και μετά από ενημερώσεις. Η διαθεσιμότητα εξασφαλίζει ακόμη και να μην χαθούν δεδομένα όταν η μετάδοσή τους γίνεται κάποια στιγμή μη λειτουργίας της συσκευής. Τέλος, η αυθεντικοποίηση των συσκευών βοηθάει στην αντιμετώπιση επιθέσεων όπως οι Denial of Service, καθώς βεβαιώνεται η γνησιότητα για τις συνδεδεμένες συσκευές. Ωστόσο λόγω της ετερογενούς φύσης και του αριθμού όλων αυτών των συσκευών που απαρτίζουν ένα έξυπνο σπίτι, αποτελεί πρόκληση η αυθεντικοποίησή τους. [22]

Επιπρόσθετα, η μη άρνηση υπηρεσιών και η επικαιρότητα των δεδομένων αποτελούν δύο πολύ σημαντικές απαιτήσεις έξυπνων οικιακών συστημάτων. Η μη άρνηση υπηρεσιών αφορά την βεβαίωση ότι όλες οι συσκευές στο σύστημα δέχονται τις υπηρεσίες που τους ζητούνται και τις πραγματοποιούν. Ουσιαστικά, αυτή η απαίτηση βασίζεται στο ότι δεν μπορεί ο χρήστης να αρνηθεί την αυθεντικότητα της ψηφιακής υπογραφής σε ένα μήνυμα που του στέλνεται. Ενώ η επικαιρότητα των δεδομένων διασφαλίζει ότι τα δεδομένα δεν ξανά στέλνονται σε μελλοντικές επικοινωνίες και αυτό πραγματοποιείται με την βοήθεια timestamps. [23]

Σύμφωνα με το 25, οι απαιτήσεις ασφάλειας στην κατασκευή έξυπνων οικιακών συσκευών χωρίζονται σε δύο κατηγορίες · τις λειτουργικές απαιτήσεις και τις απαιτήσεις επιπέδου πρόσβασης.

Οι λειτουργικές απαιτήσεις περιλαμβάνουν την διαθεσιμότητα, την αυτοοργάνωση, την ανθεκτικότητα και την διαχείριση αντιθέσεων. Η διαθεσιμότητα προδιαθέτει την λειτουργία των συσκευών του δικτύου και των υπηρεσιών του, σε εξουσιοδοτημένους χρήστες μόνο. Ακόμη, παρέχει κάποιο ελάχιστο επίπεδο υπηρεσιών, στην περίπτωση απώλειας ρεύματος ή κάποιας υπερφόρτωσης του δικτύου. Η αυτοοργάνωση εξυπηρετεί το δίκτυο, καθώς σε περίπτωση απώλειας ενέργειας ή ενημερώσεων πρέπει κάποιες συσκευές να μπορούν να αυτοοργανωθούν με σκοπό την διατήρηση ενός επιπέδου ασφάλειας. Η ανθεκτικότητα βασίζεται στην δημιουργία και διατήρηση ενός σχεδίου ασφάλειας, που θα προστατεύει το δίκτυο ακόμη και αν αρκετές συσκευές έχουν επηρεαστεί από κάποια επίθεση. Η ανθεκτικότητα σχετίζεται και με την απομόνωση των πιο σημαντικών συσκευών του δικτύου από τις

υπόλοιπες, με σκοπό σε κάθε περίπτωση να μην επηρεαστεί ολόκληρο το δίκτυο από επιθέσεις. Τέλος, η διαχείριση εξαιρέσεων αναφέρεται στην διατήρηση των υπηρεσιών που προσφέρει ένα δίκτυο σε μη φυσιολογικές συνθήκες. Αυτές οι συνθήκες μπορεί να είναι λανθασμένη ρύθμιση συσκευών, ασυμβατότητα λειτουργικών συστημάτων, κακώς σχεδιασμένος εξοπλισμός, κακόβουλες συσκευές ή μη λειτουργία συσκευών. [25]

3.3 Πρωτόκολλα ασφάλειας

Μερικά πρωτόκολλα ασφαλείας που χρησιμοποιούνται σε έξυπνες συσκευές για την μεταφορά των δεδομένων είναι το SSL/TLS (Secure Sockets Layer/Transport Layer Security) και το WPA2/WPA3 (Wi-Fi Protected Access 2/3).

Αναφορικά με το SSL/TLS, είναι ένα πρωτόκολλο ασφάλειας, το οποίο χρησιμοποιώντας κρυπτογράφηση, πιστοποιητικά και ψηφιακές υπογραφές, προσφέρει εμπιστευτικότητα, ακεραιότητα των μηνυμάτων και επιβεβαίωση γνησιότητας στον παραλήπτη. Το SSL παρέχει ένα ασφαλές κανάλι μεταξύ δύο μηχανών, που ονομάζονται πρόγραμμα-πελάτης (client) και εξυπηρετητής (server). Το κανάλι αυτό παρέχει ωστόσο και διαφάνεια, δηλαδή μέσω κρυπτογράφησης τα δεδομένα μεταφέρονται αμετάβλητα από τον αποστολέα στον παραλήπτη. Το SSL αποτελείται από τέσσερα υπο-πρωτόκολλα τα οποία λειτουργούν στο TCP/IP (το SSL Record Protocol στο επίπεδο δικτύου και τα SSL Handshake Protocol, SSL ChangeCipherSpec Protocol και το SSL Alert Protocol στο application layer). [26]

Στο SSL ακολουθείται μια διαδικασία κρυπτογράφησης, κατά την οποία απλό κείμενο, μετατρέπεται σε κρυπτογραφημένο χρησιμοποιώντας ένα ειδικό κλειδί, συνήθως ένα τυχαίο αλφαριθμητικό σύμβολο μήκους 8-24 bytes. Το αποτέλεσμα είναι η δημιουργία κωδικοποιημένου μηνύματος που μοιάζει με τυχαία δεδομένα χωρίς χρήσιμη πληροφορία. Οπότε για την αποκρυπτογράφηση απαιτείται το κλειδί ή τα κλειδιά που χρησιμοποιήθηκαν για την κρυπτογράφηση ενώ δεν είναι απαραίτητα κρυφός ο αλγόριθμος που ακολουθήθηκε, μιας και μόνο με αυτόν δεν γίνεται να φτάσουμε στο αρχικό μήνυμα. [25]

Ακόμα ένα πρωτόκολλο ασφάλειας είναι το WPA2 που παρέχει ασφαλή επικοινωνία σε ασύρματα δίκτυα. Σύμφωνα με το IEEE 802.11 standard που ορίζει το πρωτόκολλο WPA2, επιτρέπει σε έναν client να δημιουργεί κλειδιά κρυπτογράφησης με ένα access point, με σκοπό την κρυπτογράφηση των μηνυμάτων που ανταλλάσσονται σε ένα δίκτυο. Το συγκεκριμένο πρωτόκολλο έχει ως βασική λειτουργία την δημιουργία pairwise transient key (PTK) και group temporal key (GTK). Για την δημιουργία αυτών των κλειδιών πραγματοποιείται ανταλλαγή μηνυμάτων με καθορισμένο τρόπο μεταξύ client - access point, το οποίο είναι γνωστό ως four-way handshake. Στην συγκεκριμένη "χειραψία" οι access point - client μοιράζονται τα pairwise transient κλειδιά τους, αφού πρώτα σταλεί ο pairwise master key (PMK), που θα μπορούσε να είναι ο κωδικός που βάζουμε όταν συνδεόμαστε σε ένα ασύρματο δίκτυο. Στην συνέχεια, το access point μοιράζεται το δικό του GTK και τέλος, ο client εγκαθιστά το κλειδί και μπορεί να κρυπτογραφεί μηνύματα με αυτό. [27]

3.4 Πρότυπα Ασφάλειας

Ένα framework για διαχείριση κινδύνων κυβερνοασφάλειας, είναι μία καλά δομημένη προσέγγιση που βασίζεται σε ένα σετ αρχών καθοδήγησης και ταιριάζει το γενικό πλαίσιο με το πως μπορούν να αποκαλυφθούν και να διαχειριστούν από έναν οργανισμό οι απειλές, καθώς επίσης να παρέχεται

υποστήριξη σε ζητήματα όπως ο σχεδιασμός, η υλοποίηση και η αξιολόγηση της διαχείρισης των κινδύνων στον κυβερνοχώρο. [27]

Παρακάτω αναλύονται τα βασικά σημεία από διαφορετικά πρότυπα και framework ασφάλειας που υπάρχουν. Συζητούνται τα κύρια χαρακτηριστικά και λειτουργίες τους καθώς και τα οφέλη των προτύπων στην δημιουργία συσκευών και συστημάτων.

3.4.1 NIST Cybersecurity Framework

Το NIST framework (National Institute of Standards and Technology) δημιουργήθηκε βασισμένο σε ένα σετ βιομηχανικών προτύπων και βέλτιστων πρακτικών με σκοπό να βοηθήσει οργανισμούς να διαχειριστούν τις σημαντικές υποδομές των ζητημάτων ασφάλειας. Αυτό το framework μπορεί να χρησιμοποιηθεί και σε IoT έξυπνα περιβάλλοντα, ενώ αποτελείται από μία συλλογή από δραστηριότητες, πορίσματα και ενημερωτικές πληροφορίες σχετικά με την ασφάλεια προσφέροντας λεπτομερή καθοδήγηση ανάπτυξης οργάνωσης ατομικών προφίλ. Ειδικότερα, το NIST χωρίζεται σε πέντε κύριες λειτουργίες διαχείρισης κινδύνων αναφορικά με δεδομένα και πληροφορίες ασφάλειας. Αυτές οι λειτουργίες είναι η αναγνώριση, προστασία, ανίχνευση, απάντηση και "ανάρρωση". [27]

Η αναγνώριση βοηθάει τους οργανισμούς να αντιληφθούν πως να διαχειρίζονται κίνδυνοι ασφάλειας που σχετίζονται με συστήματα, ανθρώπους, δεδομένα, περιουσιακά στοιχεία και ικανότητες όπως διαχείριση επιχειρησιακού περιβάλλοντος, μέσω διαδικασιών διαχείρισης και αξιολόγησης. Η προστασία βασίζεται στην ανάπτυξη και εφαρμογή μέτρων ασφάλειας που εξασφαλίζουν την παράδοση σημαντικών υπηρεσιών καθώς επίσης καθορίζονται έλεγχοι ασφάλειας για προστασία των δεδομένων και πληροφοριών των συστημάτων. Στην ανίχνευση πραγματοποιούνται ανάλογες δραστηριότητες που αφορούν στον προσδιορισμό των συμβάντων κυβερνοασφάλειας καθώς προσφέρεται καθοδήγηση στην ανίχνευση ανωμαλιών ασφάλειας, σε συστήματα παρακολούθησης και δίκτυα ώστε να αποκαλυφθούν αντίστοιχα περιστατικά. Η λειτουργία απάντηση σχετίζεται με τις δραστηριότητες που πραγματοποιούνται μετά την ανίχνευση κάποιου περιστατικού κυβερνοασφάλειας. Επίσης περιέχει συστάσεις αντιμετώπισης επόμενων πιθανών περιστατικών. Τέλος, η αποκατάσταση αφορά σε δημιουργία και διατήρηση σχεδίων δράσης για επαναφορά των συστημάτων ή υπηρεσιών μετά από κάποιο περιστατικό κυβερνοασφάλειας. [29]

3.4.2 NIST Risk Management Framework (RMF)

Το NIST RMF framework παρέχει μια εύκολη, επαναλαμβανόμενη διαδικασία επτά βημάτων που μπορεί να ακολουθήσει κάθε οργανισμός για να διαχειριστεί κινδύνους που σχετίζονται με ιδιωτικότητα και ασφάλεια πληροφοριών. Αυτά τα πέντε βήματα αφορούν στις διαδικασίες που ασχολούνται με την προετοιμασία, κατηγοριοποίηση, διαλογή, εφαρμογή, αξιολόγηση, έγκριση και παρακολούθηση. Η κατηγοριοποίηση σχετίζεται με τις ενέργειες διαφοροποίησης του συστήματος και των πληροφοριών που διαχειρίζονται, αποθηκεύονται και μεταδίδονται. Στην διαλογή επιλέγεται το σετ των NISP SP 800-53 που ελέγχουν την προστασία του συστήματος που βασίζεται στην αξιολόγηση του κινδύνου. Τέλος, η εφαρμογή βοηθάει τους οργανισμούς να επιβάλλουν ελέγχους και να τεκμηριώσουν πως αυτοί θα αξιοποιηθούν. Τα υπόλοιπα βήματα έχουν προφανή λειτουργία. [29]

3.4.3 NIST Privacy Framework

Το NIST privacy framework αναπτύχθηκε για να βοηθήσει στον εντοπισμό και στη διαχείριση κινδύνων ιδιωτικότητας. Οι βασικές λειτουργίες του framework είναι η αναγνώριση, η διακυβέρνηση, ο έλεγχος, η επικοινωνία και η ασφάλεια. Η αναγνώριση βοηθάει τους οργανισμούς να καταλάβουν πως να

διαχειρίζονται κίνδυνοι ιδιωτικότητας, η διακυβέρνηση βοηθάει στην εφαρμογή και ανάπτυξη της δομής διαχείρισης επιχειρηματικών κινδύνων και προτεραιοτήτων. Ο έλεγχος σχετίζεται με την σωστή διαχείριση των δεδομένων ώστε να είναι επαρκώς ασφαλισμένα. Τέλος, η επικοινωνία βοηθάει τους οργανισμούς να αντιληφθούν την συσχέτιση των δεδομένων και την επεξεργασία τους και η προστασία θέτει κανόνες ασφαλείας για την επεξεργασία των δεδομένων. [29]

3.4.4 NIST SP 800-53, 800-30, 800-37, 800-39, 800-12, 800-14, 800-53R1

Αυτή η ειδική έκδοση, NIST SP 800-53, σε θέματα ασφάλειας και ιδιωτικότητας παρέχει έλεγχο δεδομένων σε συστήματα και οργανισμούς. Παρέχει ακόμη προστασία περιουσιακών στοιχείων και άλλων οργανισμών από ανθρώπινα λάθη και παραλείψεις, φυσικές καταστροφές και δομικά λάθη που συμβαίνουν. Στην NIST SP 800-30 έκδοση, παρέχεται καθοδήγηση σε οργανισμούς σχετικά με την δημιουργία συστημάτων πληροφοριών που αξιολογούν την επικινδυνότητα. Ακόμη, η έκδοση NIST SP 800-37 διευκρινίζει την εφαρμογή RMF στα συστήματα πληροφοριών και τους οργανισμούς. Η ειδική έκδοση NIST SP 800-39 αναπτύχθηκε για να συνεισφέρει στις λειτουργίες των οργανισμών αναφορικά με τους κινδύνους ασφάλειας. Επιπρόσθετα, η έκδοση NIST SP 800-12 σχεδιάστηκε για ομοσπονδιακούς και κρατικούς οργανισμούς, ωστόσο μπορεί να χρησιμοποιηθεί και από άλλους οργανισμούς που επικεντρώνονται στον έλεγχο και την ασφάλεια υπολογιστών γενικότερα. Η NIST SP 800-14 δημιουργήθηκε με σκοπό να παρέχει γενικές περιγραφές κοινώς χρησιμοποιούμενων αρχών ασφαλείας, ώστε να βοηθήσει τους οργανισμούς να κατανοήσουν τις πολιτικές της κυβερνοασφάλειας. Τέλος, η έκδοση NIST SP 800-31R1 σχεδιάστηκε με σκοπό να διασφαλίζει εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα του συστήματος και των πληροφοριών του. [29]

3.4.5 Health Insurance Portability and Accounting Act (HIPAA)

Το HIPAA αναπτύχθηκε για να προσφέρει σχέδια υγείας και παροχών ιατρικής περίθαλψης για εφαρμογή ελέγχων ασφάλειας υπαλλήλων και πελατών, και να προστατεύονται ευαίσθητες ιατρικές πληροφορίες. Το συγκεκριμένο framework μπορεί να χρησιμοποιηθεί και σε IoT έξυπνα συστήματα υγείας. [29]

3.4.6 IEC 61850 and GB/T22239 Security Classified Protection Standards

Το συγκεκριμένο πρότυπο ασχολείται με την ηλεκτρική αυτοματοποίηση, συνίσταται από τα IEC 61850-1 μέχρι IEC 61850-9. Τα IEC 61850 χαρακτηριστικά περιλαμβάνουν data modeling, αναφορά σχημάτων, γρήγορη μεταφορά συμβάντων, ρύθμιση ομάδων, μεταφορά δειγμάτων δεδομένων, εντολών και αποθήκευση δεδομένων. [30]

3.4.7 IEC 62351 on Smart Grid Security

Το IEC 62351 χρησιμοποιείται σε συστήματα ενεργειακής διαχείρισης και σχετίζεται με την ανταλλαγή δεδομένων. Το IEC 62351-1 χρησιμοποιείται για επικοινωνία δικτύων και συστημάτων ασφαλείας κάνοντας μια εισαγωγή σε θέματα ασφάλειας. Το IEC 62351-2 περιέχει το αντίστοιχο λεξιλόγιο και όρους. Χρησιμοποιείται ακόμη μία σειρά από πρωτόκολλα όπως το IEC 62351-3, IEC 62351-4, IEC 62351-5, IEC 62351-6, IEC 62351-7 και IEC 62351-8 ώστε να εκπληρώνονται οι στόχοι του προτύπου οι οποίοι αφορούν στην επαλήθευση γνησιότητας των δεδομένων που μεταφέρονται μέσω ψηφιακών υπογραφών, επιτρέποντας μόνο εξουσιοδοτημένη πρόσβαση, αποτρέποντας με αυτόν τον τρόπο πολλά είδη επιθέσεων. [30]

3.4.8 ISO/IEC 15408

Το ISO/IEC 15408 δημιουργήθηκε με σκοπό να προσφέρει τεχνικές εύρεσης βέλτιστων τρόπων αξιολόγησης και αντιμετώπισης κινδύνων. Συγκεκριμένα το ISO/IEC 15408-1 αποτελείται από τρία μέρη που σχετίζονται με την εισαγωγή και γενικό μοντέλο, λειτουργικές απαιτήσεις ασφάλειας και απαιτήσεις διασφάλισης ασφάλειας. [30]

3.4.9 American National Standards Institute (ANSI)/International Society of Automation (ISA) (ANSI/ISA 62443)

Το ANSI/ISA 62443 πρότυπο το οποίο είναι μέρος του IEC 62443 International Series of Standards on Industrial communication networks, δημιουργήθηκε από την ανάπτυξη των ANSI και ISA και παρέχει διαδικασίες, τεχνικές και απαιτήσεις για βιομηχανικούς αυτοματισμούς και συστήματα ελέγχου (Industrial Automation and Control Systems - IACS). Ακόμη, περιέχονται ασφαλή πακέτα ανάπτυξης απαιτήσεων τα οποία βοηθούν στην δημιουργία και διατήρηση ασφαλών προϊόντων. Και αυτό το πρότυπο ενδείκνυται για IoT συσκευές και συστήματα. [29]

3.4.10 General Data Protection Regulation (GDPR)

Το GDPR σχεδιάστηκε για την Ευρωπαϊκή Ένωση και επιβάλλει ιδιωτικότητα δεδομένων και δεσμεύσεις ασφάλειας σε οργανισμούς που εδρεύουν οπουδήποτε στον κόσμο εφόσον χρησιμοποιούν ή συλλέγουν δεδομένα από ανθρώπους που ζουν σε κράτος της Ευρωπαϊκής Ένωσης. Θα μπορούσε να εφαρμοστεί σε ειδικά περιβάλλοντα στα οποία IoT συσκευές χρησιμοποιούν και διαμοιράζονται δεδομένα σχετικά με τον χρήστη. [29]

3.4.11 Systems and Organizations Controls (SOC2)

Το SOC2 δημιουργήθηκε από το American Institute of CPAs (AICPA). Επιτρέπει σε οργανισμούς να συλλέγουν και να αποθηκεύουν προσωπικά δεδομένα πελατών χρησιμοποιώντας υπηρεσίες cloud για την διατήρηση ασφάλειας καθώς και απαιτήσεων ασφαλείας σε προμηθευτές και εξωτερικούς συνεργάτες οι οποίοι πρέπει να συμμορφώνονται. Επίσης, οι αναφορές του SOC2 σχεδιάστηκαν με σκοπό να προστατεύουν τις ανάγκες των χρηστών απαιτώντας λεπτομερείς πληροφορίες και εγγύηση για ελέγχους υπηρεσιών των οργανισμών, σχετικά με την ασφάλεια, διαθεσιμότητα και ακεραιότητα των διαδικασιών των συστημάτων που χρησιμοποιούνται από τους οργανισμούς για επεξεργασία των δεδομένων καθώς και την εμπιστευτικότητα των πληροφοριών. [29]

3.4.12 Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)

Το OCTAVE αναπτύχθηκε από το Software Engineering Institute με σκοπό να βοηθήσει στην αναγνώριση και διαχείριση κινδύνων ασφάλειας των δεδομένων. Βασίζεται σε τρεις βασικές πρακτικές · την δημιουργία προφίλ επιθέσεων ανάλογα τα κέρδη που πέτυχαν, την αναγνώριση ευπαθών σημείων της υποδομής και την σχεδίαση μεθόδων και στρατηγικών ασφάλειας. Το OCTAVE προσφέρει μεθόδους με τις οποίες βοηθάει οργανισμούς να εντοπίσουν και αξιολογήσουν τις πληροφορίες που διαχειρίζονται και κατά πόσο σημαντικές είναι ανάλογα την θεματολογία και την χρήση τους. Με αυτόν τον τρόπο, οι οργανισμοί είναι σε θέση να προστατέψουν επιπλέον τις πιο σημαντικές πληροφορίες οι οποίες πιθανόν να βρίσκονται σε κίνδυνο. [31]

3.4.13 Information Assurance for Small and Medium Enterprises (IASME) Governance

Το IASME πρότυπο δημιουργήθηκε με στόχο την εκπαίδευση πάνω σε ζητήματα κυβερνοασφάλειας και την απόδοση των επιχειρήσεων. Περιέχει μεθόδους διαχείρισης, αξιολόγησης κινδύνων, εκπαίδευσης, παρακολούθησης και διαχείρισης ανθρώπινου δυναμικού. Ακόμη, βοηθάει ενεργά τους οργανισμούς στην διατήρηση της συνέχειάς τους προσφέροντας τεχνικές "απάντησης" σε διαφορετικά περιστατικά και προτροπή για τακτικά αντίγραφα ασφαλείας. Εφαρμόζεται και σε IoT συσκευές δίνοντας μία σημαντική ελάχιστη βάση για το επίπεδο ασφάλειας της επιχείρησης, ενισχύοντας παράλληλα και τις γνώσεις και δεξιότητες των υπαλλήλων αυτής. [29]

3.4.14 Technical Committee on Cyber Security (TC CYBER) Framework

Το TC CYBER ανέπτυξε ένα framework το οποίο προτείνει ένα σετ απαιτήσεων βελτίωσης της επαγρύπνησης των ατόμων και οργανισμών καθώς επίσης συνεισφέρει στα πρότυπα τηλεπικοινωνιών που χρησιμοποιούνται μεταξύ χωρών της Ευρωπαϊκής Ένωσης. Οι στόχοι του TC CYBER χωρίζονται σε εννιά κύριες περιοχές · την κατανόηση του οικοσυστήματος της κυβερνοασφάλειας, την προστασία των προσωπικών δεδομένων και επικοινωνίας, την επιβολή ασφάλειας και ιδιωτικότητας σε IoT συστήματα, την ασφάλεια δικτύων, την εύρεση και χρήση εργαλείων και οδηγών, την υποστήριξη της νομοθεσίας της Ευρωπαϊκής Ένωσης και την ενίσχυση της κρυπτογραφίας. [29]

3.4.15 10 steps to Cybersecurity

Το 10 steps to Cybersecurity αποτελεί μία εξέλιξη του National Cyber Security Centre (NCSC) το οποίο παρέχει γενικές οδηγίες οι οποίες αφορούν την προστασία των οργανισμών στον κυβερνοχώρο, και περιγράφεται σε δέκα στάδια. [29]

3.4.16 Information Security Management System (ISMS) Framework

Παρέχει πολιτικές, διαδικασίες και πηγές σχετικά με την σχεδίαση, υλοποίηση, παρακολούθηση, αξιολόγηση και διατήρηση ενός Information Security Management System. Αυτά πραγματοποιούνται με γνώμονα τις ανάγκες και στόχους που έχει κάθε οργανισμός και μπορεί να αφορά σε διαφορετικές λειτουργίες. [27]

3.4.17 Factor Analysis of Information Risk (FAIR) Framework

Πρόκειται για ένα framework που ασχολείται με την μεταφορά και μετάδοση της πληροφορίας και συνεπώς τους κινδύνους που φέρουν αυτά. Εξετάζονται οι παράγοντες κινδύνου απώλειας ή παρεμβολής της μετάδοσης των δεδομένων. Αναλύονται μέθοδοι υπολογισμού των παραγόντων κινδύνου και μελετάται υπολογιστική μηχανή για τον υπολογισμό κινδύνων με μοντέλο προσομοίωσης για την δημιουργία και περεταίρω ανάλυση περιπτώσεων κινδύνων. [27]

3.4.18 Cyber Resiliency Engineering Framework

Περιέχει στοιχεία σχετικά με την επίτευξη στόχων και πρακτικών, ομαδοποίηση κινδύνων, τομείς που χρήζουν περισσότερης ασφάλειας καθώς και κόστη και μελέτες σχετικά με τις παραπάνω διαδικασίες. [27]

3.4.19 Cybersecurity Risk Management Reporting Framework

Συνίσταται από τρία δομικά στοιχεία · περιγραφή κριτηρίων για διαχείριση των απειλών, έλεγχος και αξιολόγηση της αποδοτικότητας των μεθόδων ελέγχου ασφάλειας. [27]

3.4.20 Information Technology Infrastructure Library (ITIL) version 3

Πρόκειται για ένα framework διαχείρισης υπηρεσιών IT. Παρέχει πέντε κύριες εκδόσεις οι οποίες βασίζονται στις υπηρεσίες στρατηγικής, σχεδιασμού, μετάβασης, λειτουργίας και συνεχής εξέλιξης και περιέχει είκοσι έξι διαδικασίες διευκόλυνσης παράδοσης και διαχείρισης υπηρεσιών IT υψηλής ποιότητας. [27]

3.4.21 ETSI Standards

Το European Telecommunications Standards Institute (ETSI) είναι ένας μη κερδοσκοπικός οργανισμός ο οποίος στοχεύει στην παραγωγή προτύπων τηλεπικοινωνίας, τα οποία χρησιμοποιούνται στην Ευρώπη. Ωστόσο, αναπτύσσει ακόμη και πρότυπα από διαφορετικά τμήματα της κυβερνοασφάλειας και του Διαδικτύου των Πραγμάτων (IoT). [29] Στο 29 βρίσκονται επιπλέον πληροφορίες σχετικά με τα πολλά πρότυπα που έχουν αναπτυχθεί από το ETSI, τους κύριους στόχους τους και την περιοχή που μελετούν, είτε σχετίζεται με το Διαδίκτυο των Πραγμάτων όπως έξυπνες πόλεις, έξυπνα σπίτια, είτε ασχολείται με την κυβερνοασφάλεια. [29]

3.4.22 Control Objectives for Information and Related Technology (COBIT) version 5

Πρόκειται για ένα framework που ασχολείται με την διακυβέρνηση και διαχείριση. Βασίζεται σε πέντε θεμελιώδεις αρχές · να εκπληρώνονται οι ανάγκες των ενδιαφερόμενων, να εφαρμόζεται ένα μόνο ενσωματωμένο framework, να διευκολύνεται μια ολιστική προσέγγιση και να διαχωρίζεται η διακυβέρνηση από την διαχείριση. Συνίσταται από ελέγχους υψηλού επιπέδου, οι οποίοι ομαδοποιούνται σε τέσσερις κατηγορίες: σχεδιασμό και οργάνωση, απόκτηση και υλοποίηση, παράδοση και υποστήριξη, παρακολούθηση και αξιολόγηση. [27]

3.4.23 Risk IT Framework

Παρέχει ένα μοντέλο end-to-end με τρεις τομείς με σκοπό την αποδοτική διαχείριση των κινδύνων στην τεχνολογία πληροφοριών (IT) που βασίζονται σε αρκετές αρχές καθοδήγησης και καλές πρακτικές. Αυτοί οι τρεις τομείς είναι διακυβέρνηση απειλών, αξιολόγηση και απάντηση σε αυτές. [27]

3.5 Οργανισμοί που βοηθούν στην ανάπτυξη προτύπων και framework

Όπως έχει ήδη αναφερθεί, πολλοί οργανισμοί βοηθούν στην ανάπτυξη προτύπων και framework κυβερνοασφάλειας, με σκοπό την βελτίωση στην κατασκευή έξυπνων συσκευών και γενικότερα στην εξασφάλιση κάποιου ελάχιστου επιπέδου μέτρων ασφαλείας στον κυβερνοχώρο. Παρακάτω, παρουσιάζονται σχετικές πληροφορίες για κάποιους από τους οργανισμούς που δημιούργησαν τα ανωτέρω πρότυπα και framework.

Αρχικά, ο οργανισμός National Institute of Standards and Technology (NIST) ιδρύθηκε το 1901 και πλέον είναι τμήμα του U.S. Department of Commerce. Επικεντρώνεται σε τέσσερις κύριες λειτουργίες. Αναλύει πρακτικές διαχείρισης δεδομένων σε NIST οργανωτικές μονάδες, τεκμηριώνει διαδικασίες και δημιουργεί προσαρμόσιμα και επεκτάσιμα εργαλεία για την υποστήριξη πλάνων διαχείρισης

δεδομένων. Δημιουργεί framework διαχείρισης δεδομένων για δεδομένα όλων των επιπέδων εργασίας. Και τέλος, επιταχύνει τις διαδικασίες αναγνώρισης, αξιολόγησης, εξουσιοδότησης και υλοποίησης εργαλείων λογισμικού ευρείας χρήσης που υποστηρίζουν ανταλλαγή δεδομένων και έρευνα συνεργασίας. [32]

Αναφορικά με το International Electrotechnical Commission (IEC) αναγνωρίστηκε το 1906 με βασικό σκοπό την εδραίωση ορολογίας και αξιολόγηση των παγκόσμιων ηλεκτρικών συσκευών. [33]

Το 1918, το American Engineering Standards Committee (AESC και αργότερα ANSI) εδραίωσε το μοντέλο του, με πολιτική της χρήση εθελοντικής, ομόφωνης προσέγγισης στην δημιουργία βιομηχανικών Αμερικανικών προτύπων. [33]

Το ISO δημιουργήθηκε μετά και το τέλος του δεύτερου παγκοσμίου πολέμου, καθώς οι εθνικές επιτροπές προτύπων (National Standards communities) επιθυμούσαν μία παγκόσμια συνεργασία όπως παρόμοια μοντέλα που είχαν ήδη δημιουργηθεί. [33]

Τέλος, το European Telecommunications Standards Institute (ETSI) είναι ένας οργανισμός Ευρωπαϊκών προτύπων που δημιουργήθηκε το 1988 από το European Conference of Postal and Telecommunications Administrations (CEPT) ως απάντηση στις προτάσεις της Ευρωπαϊκής Commission. Περισσότερες πληροφορίες σχετικά με τα επιτεύγματα του οργανισμού από την δημιουργία του μέχρι τώρα, μπορείτε να βρείτε στην ιστοσελίδα του. [34]

3.6 Αξιολόγηση Προτύπων και framework

Συνοψίζοντας τα πρότυπα και framework που έχουν αναφερθεί, παρουσιάζονται τα πιο απαραίτητα στην υλοποίηση ενός έξυπνου περιβάλλοντος. Μία συλλογή από framework και πρότυπα τα οποία βοηθούν στην σχεδίαση, υλοποίηση και αξιολόγηση έξυπνων οικιακών συσκευών είναι το NIST Cybersecurity Framework, το IEC 62351 on Smart Grid Security, το American National Standards Institute (ANSI)/International Society of Automation (ISA) (ANSI/ISA 62443), το Systems and Organizations Controls (SOC2), το Technical Committee on Cyber Security (TC CYBER) Framework, το Factor Analysis of Information Risk (FAIR) Framework και το ETSI Standards. Σύμφωνα με αυτά, παρέχεται ασφάλεια δεδομένων κατά την μεταφορά τους, την εξέταση κινδύνων καθόλη την διάρκεια λειτουργίας και υλοποίησης των συσκευών, με κύριο στόχο την διασφάλιση ακεραιότητας, διαθεσιμότητας και εμπιστευτικότητας της πληροφορίας.

3.7 Επίλογος

Το δεύτερο κεφάλαιο επικεντρώθηκε στην παρουσίαση και αναφορά προτύπων και framework ασφάλειας. Αρχικά, αναλύθηκαν κάποιες βασικές απαιτήσεις ασφάλειας που πρέπει να εξυπηρετούνται κατά την υλοποίηση έξυπνων συσκευών και συστημάτων σε οικιακό περιβάλλον. Στην συνέχεια, σύμφωνα και με τις απαιτήσεις ασφάλειας παρουσιάστηκαν συνοπτικά κάποια πρωτόκολλα ασφάλειας και πιο αναλυτικά κάποια πρότυπα και framework. Τέλος, αξιολογήθηκαν οι οργανισμοί που συμβάλλουν πιο ενεργά στην κατασκευή και ασφάλιση έξυπνων συσκευών smart home καθώς επίσης συνοψίστηκαν τα πιο σημαντικά πρότυπα στην κατασκευή και διασφάλισή τους.

Κεφάλαιο 4ο: Έξυπνες οικιακές συσκευές και συστήματα

4.1 Εισαγωγή

Στο τέταρτο κεφάλαιο αρχικά αναλύεται συνοπτικά ένα σύστημα έξυπνου σπιτιού, λειτουργίες και υπηρεσίες που προσφέρει κάθε λειτουργία και σκοπιμότητά της. Παρουσιάζονται συνοπτικά κάποιες συσκευές για smart home, καθώς επίσης διακρίνεται η λειτουργία τους και τα θέματα ασφάλειας που προκύπτουν.

4.2 Λειτουργίες Smart Home που στοχεύουν στην άνεση του χρήστη

Ένας από τους κύριους στόχους κατά το στάδιο της έρευνας σχετικά με το έξυπνο σπίτι είναι η διευκόλυνση της ζωής του χρήστη, αυξάνοντας την άνεση στην εξυπηρέτησή του. Αυτό πραγματοποιείται με δύο τρόπους · την αυθεντικοποίηση και αυτοματισμό των λειτουργιών από απόσταση και την διαχείριση του σπιτιού από απόσταση. Παρακάτω παρουσιάζονται projects που βοηθούν την αυτοματοποίηση των έξυπνων οικιακών συσκευών, χρησιμοποιώντας την ανθρώπινη δραστηριότητα και συμπεριφορά. Με αυτόν τον τρόπο μπορεί να μειωθεί η ενεργειακή κατανάλωση καθώς δεν χρησιμοποιούνται όλες οι υπηρεσίες των συσκευών ούτε όλες οι συσκευές συνέχεια. [35]

Αρχικά, σχετικά με την δραστηριότητα αυθεντικοποίησης και αυτοματοποίησης εργασιών, ένα smart home καθώς είναι σχεδιασμένο με ευφυία μπορεί να διακρίνει τοποθεσία, ταυτότητα χρήστη, δραστηριότητες και χρόνο. Πιο συγκεκριμένα, μαθαίνει από την συμπεριφορά του χρήστη και προσαρμόζει αυτοματοποιημένες λειτουργίες σύμφωνα με αυτήν, καθώς επίσης εντοπίζει την τοποθεσία του χρήστη και την ταυτότητά του. Σχετικά με τις παραπάνω λειτουργίες, υπάρχουν πολλά project τα οποία βασίζονται σε αυτές. Το managing an adaptive versatile home (MavHome) project που αναπτύχθηκε από το Πανεπιστήμιο Arlington, χρησιμοποιεί ένα συνδυασμό από διεπιστημονικές τεχνολογίες όπως Τεχνητή Νοημοσύνη, multimedia τεχνολογία, mobile computing και ρομποτική. Η αρχιτεκτονική του χωρίζεται σε τέσσερα επίπεδα · φυσικό επίπεδο, επικοινωνίας, πληροφορίας και απόφασης. Χρησιμοποιεί το πρωτόκολλο X10 για έλεγχο και παρακολούθηση περισσότερων από εξήντα συσκευών συνδεδεμένων στο σύστημα. Διαθέτει αλγορίθμους για λήψη αποφάσεων, υπολογισμό πιθανοτήτων να συμβεί κάτι και χρησιμοποιείται για πρόβλεψη ενεργειών για έναν χρήστη. Περισσότερα projects σχετικά με παρόμοιες λειτουργίες βρίσκονται στο 35. [35]

Ακόμη μία λειτουργία ενός καλά σχεδιασμένου έξυπνου σπιτιού είναι η απομακρυσμένη πρόσβαση και έλεγχος. Αυτό σχετίζεται και με την παρακολούθηση του χώρου. Παρακάτω παρουσιάζονται δύο project που αναφέρονται στον απομακρυσμένο έλεγχο του smart home, το οποίο μπορεί να γίνει με ευκολία αν χρησιμοποιηθεί μια πλατφόρμα για αυτές τις λειτουργίες. [35]

Στο Πανεπιστήμιο της Μαλαισίας, το Institute of Advanced Technology, παρουσιάστηκε ο σχεδιασμός και η υλοποίηση ενός Simple Object Access Protocol (SOAP)-based έξυπνου σπιτιού. Το συγκεκριμένο project βασίζεται στην διαλειτουργία πολλών οικιακών συσκευών του σπιτιού. Με τον όρο διαλειτουργία, εννοείται η λειτουργία δύο ή περισσότερων συσκευών του συστήματος. Ακόμη, έχει συμπεριληφθεί η περίπτωση διακοπής λειτουργίας του server, καθώς και μέσω μηνύματος μπορεί να ελεγχθεί το σύστημα και οι συσκευές του από απόσταση. Τέλος, παρέχει έλεγχο δύο κατευθύνσεων σε πραγματικό χρόνο, και παρακολούθηση του smart home. [35]

Ακόμη, ένα IoT project που υλοποιήθηκε με την πλατφόρμα BTDisplay, η οποία είναι μια πλατφόρμα IoT που επιτρέπει την σύνδεση πολλών hardware συσκευών στο cloud, την σχεδίαση εφαρμογών και τον έλεγχο φωτισμού του σπιτιού δίνοντας οδηγίες μέσω της εφαρμογής από το τηλέφωνο. Κύριος στόχος του project είναι η εξοικονόμηση ενεργειακής κατανάλωσης. Έτσι, προτείνεται η αυτοματοποίηση του συστήματος, η οποία πραγματοποιείται καθώς στέλνονται οι απαιτούμενες πληροφορίες στον χρήστη ώστε να μπορεί να διαχειριστεί ασύρματα τις λειτουργίες του σπιτιού του. [36]

Σχετικά με την μηχανική σχεδίαση του συστήματος, εκμεταλλευόμενο τις τεχνολογίες όπως το Internet of Things, μειώνει την ενεργειακή κατανάλωση στο σπίτι. Χρησιμοποιεί Arduino Uno που συνδέεται με ασύρματη μονάδα, μονάδα Bluetooth και άλλα δομικά συστατικά για την σωστή λειτουργία του συστήματος. Η συγκεκριμένη σχεδίαση έχει γίνει για ένα σύστημα ελέγχου που μπορεί να χρησιμοποιηθεί και στον φωτισμό του σπιτιού. Επίσης, ο κώδικας που εκτελείται από το Arduino Uno δημιουργήθηκε από το λογισμικό Proteus, και η επικοινωνία του μικροελεγκτή με τον χρήστη πραγματοποιείται μέσω της εφαρμογής BTDisplay. Μέσω σύνδεσης Bluetooth, η εφαρμογή αυτή χειρίζεται τις οικιακές συσκευές από απόσταση, και οι εντολές ή μηνύματα του μικροελεγκτή εμφανίζονται άμεσα στην εφαρμογή καθώς υπάρχει και μεταξύ τους επικοινωνία. Η εφαρμογή επιτρέπει και φωνητικές εντολές έχοντας επιλέξει την κατάλληλη γλώσσα και δίνοντας συγκεκριμένες εντολές οι οποίες αποστέλλονται κατευθείαν στον μικροελεγκτή. Περισσότερες πληροφορίες όπως η ακριβής συνδεσμολογία, ο κώδικας καθώς και μελλοντικές προεκτάσεις και ελλείψεις του συστήματος δίνονται από το 36. [36]

4.3 Λειτουργίες Smart Home σχετικά με την υγεία του χρήστη

Τα έξυπνα σπίτια παρέχουν λειτουργίες και υπηρεσίες ασφάλειας στους χρήστες τους, ειδικά σε ηλικιωμένα άτομα, ή άτομα με προβλήματα υγείας που σίγουρα χρειάζονται βοηθήματα για να βεβαιώνονται για την υγεία τους ανά τακτά χρονικά διαστήματα. Καθώς είναι πολύ σημαντικό να υπάρχει μέτρηση και παρακολούθηση από απόσταση αλλά και ειδοποίηση των χρηστών. Παρακάτω παρουσιάζονται projects που υλοποιούν με αποτελεσματικό τρόπο την ιατρική υποστήριξη ασθενών ή μη σε οικιακά περιβάλλοντα.

Πολλά οικιακά συστήματα προσφέρουν εδώ και καιρό, υπηρεσίες παρακολούθησης της υγείας του χρήστη οι οποίες εξετάζουν τις συνθήκες, παρέχουν υποστηρικτικές υπηρεσίες και παράγουν και αποστέλλουν μηνύματα ή ειδοποιήσεις όταν χρειάζεται. Ένα σύστημα όπως αυτό που παρουσιάζεται στο [35] απαιτεί αισθητήρες και switches επικοινωνίας για να παρακολουθούνται οι δραστηριότητες του κατοίκου και οι πληροφορίες που μεταδίδονται μέσω ενός controller area δικτύου (CAN) στον τοπικό υπολογιστή. Διακρίνονται ακόμα πληροφορίες όπως δεδομένα μέτρησης πίεσης αίματος, καρδιακού παλμού και βάρους. Η μεθοδολογία βασίζεται σε εικοσιτετράωρο κιρκάδιο ρυθμό ο οποίος χωρίζεται σε παρακολούθηση κάθε μία ώρα. Μέθοδοι στατιστικού μέσου και απόκλισης εφαρμόζονται με σκοπό την κατάλληλη ειδοποίηση κάθε μία ώρα σε φυσιολογικές συνθήκες υγείας του χρήστη. [35]

Μια ακόμα σχετική έρευνα και υλοποίηση συστήματος υγείας το οποίο μετράει κιρκάδιο ρυθμό, HomeCare System και προτείνεται στο 37. Πιο συγκεκριμένα έχουν παρατηρηθεί δύο κατηγορίες παρέκκλισης κιρκάδιου ρυθμού, οι οποίες είναι η “short-term” και “long-term” παρεκκλίσεις. Η πρώτη αφορά την ανίχνευση επείγουσων αλλαγών κιρκάδιου ρυθμού που συνήθως συμβαίνουν από κάποιο ατύχημα. Αυτή η ανίχνευση βοηθάει στην αναγνώριση ξαφνικών και επείγοντων προβλημάτων υγείας.

Η δεύτερη κατηγορία περιλαμβάνει τις περιπτώσεις στις οποίες οι αλλαγές στον κιρκάδιο ρυθμό συμβαίνουν σταδιακά. Τον βαθμό παθολογίας του ασθενούς τον ορίζει ο γιατρός και στην συνέχεια αυτή η γνώση μπορεί να προστεθεί στο προσαρμόσιμο σύστημα το οποίο αυτο-εκπαιδεύεται. Κατά την υλοποίηση του συστήματος αυτού, υλοποιήθηκαν δύο βασικές μέθοδοι παρακολούθησης των ασθενών. Η πρώτη σχεδιάστηκε χρησιμοποιώντας PIR αισθητήρες. Η επικοινωνία πραγματοποιήθηκε με ZigBee τεχνολογία, και η απεικόνιση στον υπολογιστή υλοποιήθηκε στο Labview. Τα θετικά της μεθόδου αυτής είναι ότι ο υλικός εξοπλισμός ξεκινάει την λειτουργία του μόνο με μια CR μπαταρία. Δεν χρειάζεται καλώδια για την μετάδοση της πληροφορίας και ο αισθητήρας μπορεί να λειτουργεί για πολλή ώρα. Το κύριο μειονέκτημα της μεθόδου αυτής είναι ότι μπορεί να ανιχνευτεί ένα μεγαλόσωμο κατοικίδιο σαν να είναι ο χρήστης και η τοποθεσία του χρήστη δεν ήταν η ακριβής. Δηλαδή βρίσκει την περιοχή στην οποία βρίσκεται ο χρήστης αλλά όχι την ακριβή του τοποθεσία. [37]

Η δεύτερη μέθοδος χρησιμοποιεί την Location Engine λύση του Texas Instruments. Αυτή η μηχανή περιέχει ένα ZigBee chip με όνομα CC2431. Ο αλγόριθμος τοποθεσίας που χρησιμοποιείται στη συγκεκριμένη μηχανή βασίζεται στις μεταβλητές Received Signal Strength Indicator (RSSI) και η τιμή του RSSI μειώνεται καθώς αυξάνεται η απόσταση του χρήστη από τους κόμβους. Ο χώρος του διαμερίσματος αρχικά έχει χωριστεί σε τέσσερις κόμβους και ειδικά ρολόγια βοηθούν το chip στην μέτρηση της τοποθεσίας. Βασικό πλεονέκτημα είναι ότι σε αυτή τη μέθοδο η τοποθεσία του χρήστη είναι ακριβής και ότι δεν γίνεται παρανόηση του χρήστη με κάποιο κατοικίδιο. Κύριο μειονέκτημα όμως αποτελεί το γεγονός ότι ο χρήστης πρέπει να φοράει μια ενεργή ZigBee συσκευή · κάτι που ειδικά οι ηλικιωμένοι δεν είναι εύκολο να συνηθίσουν. [37]

Για την καλύτερη προσέγγιση, χρησιμοποιείται ένας συνδυασμός των δύο παραπάνω τεχνολογιών στο HomeCare σύστημα για τον καλύτερο προσδιορισμό του ατόμου. Ωστόσο, κατά τις βραδινές ώρες η θέση του χρήστη δεν είναι τόσο ακριβής. Λόγω του ότι οι πληροφορίες σχετικά με την τοποθεσία παίρνονται από PIR αισθητήρες, μπορούν να επηρεαστούν από πολλά σφάλματα. [37]

Σχετικά με την απομακρυσμένη παρακολούθηση αναφορικά με θέματα υγείας, προτείνεται ακόμη η ενημέρωση καταρτισμένου κοντινού κέντρου που μπορεί να προσφέρει ιατρική υποστήριξη του ασθενή και αυτή η ενημέρωση συμβαίνει αυτόματα από τις μετρήσεις των αισθητήρων εάν δοθεί κάποιο σημάδι ζωτικής σημασίας. Αυτή η προσέγγιση αφορά σε άμεση επέμβαση προσωπικού από απόσταση ή και από κοντά αν ο χρήστης δεν μπορεί. [35]

Ακόμη ένα σύστημα παρακολούθησης καθημερινότητας σε οικιακό περιβάλλον παρουσιάζεται στο 35. Πρόκειται για ένα σύστημα που ανιχνεύει κίνηση του κατοίκου από IR αισθητήρες, χρησιμοποιεί ακόμη αισθητήρα θερμοκρασίας στα κύρια σημεία του σπιτιού, για να μετράει την θερμοκρασία. Υλοποιείται επίσης ένα σύστημα ενεργοποίησης συναγερμού, το οποίο εφόσον ανιχνευτούν ασυνήθιστες συμπεριφορές, επικοινωνεί με απομακρυσμένο κέντρο βοήθειας. Το συγκεκριμένο σύστημα τηλεϊατρικής ανιχνεύει ασυνήθιστη διάρκεια ύπνου, μη αναμενόμενη ακινησία για μεγάλο χρονικό διάστημα, αλλαγές θερμοκρασίας διαμερίσματος και βλάβη ψυγείου. Τέλος, χρησιμοποιείται ένα ειδικό πρωτόκολλο τηλεπικοινωνίας το οποίο ονομάζεται “No Ring Calling”, το οποίο παρέχει μια πιο οικονομική λύση συλλογής δεδομένων των χρηστών, χρησιμοποιώντας την υπάρχουσα τηλεφωνική γραμμή. Ωστόσο, έχει χαμηλότερη προτεραιότητα από το κανονικό τηλέφωνο και έτσι σε περίπτωση εισερχόμενων ή εξερχόμενων κλήσεων, η επικοινωνία ακυρώνεται. [35]

4.4 Λειτουργίες που αφορούν την ασφάλεια του Smart Home

Τα έξυπνα σπίτια είναι ευάλωτα σε απειλές κυρίως δύο ειδών · αυτές που σχετίζονται με την αδύναμη αυθεντικοποίηση του χρήστη ή συσκευής. Οι επιθέσεις ασφάλειας πραγματοποιούνται τοπικά ή απομακρυσμένα. Παρακάτω παρουσιάζονται projects ασφάλειας που ασχολούνται με θέματα ασφάλειας σε έξυπνα σπίτια. [35]

Ένα μοντέλο ασφάλειας για έξυπνες οικιακές συσκευές, το οποίο βασίζεται στα προϊόντα, παρουσιάζεται στο 38. Το συγκεκριμένο μοντέλο προτείνει την ανάμειξη ενός τρίτου μέρους χειριστή στο δίκτυο με σκοπό την υλοποίηση μέτρων ασφάλειας που σχετίζονται με προϊόντα πολλών κατασκευαστών. Χρησιμοποιεί ένα οικιακό gateway σαν συστατικό κλειδί για την επιβολή χαρακτηριστικών ασφάλειας. Ο κύριος στόχος του gateway είναι να υλοποιήσει ένα σύστημα αυθεντικοποίησης του χρήστη. Μπορεί να εμποδίσει την πρόσβαση χρήστη και τις πληροφορίες του λογαριασμού βασιζόμενο στον έλεγχο εξακρίβωσης χρήστη κατά την είσοδό του. Περιέχει firewall και λογισμικό προστασίας από ιούς, ενώ ένα σημαντικό μέρος του άρθρου αποτελεί η ταξινόμηση παρόμοιων απειλών ασφάλειας σύμφωνα με την λειτουργικότητα των προϊόντων. Αυτή η κατηγοριοποίηση των απειλών προκύπτει από την εμπειρία των συγγραφέων πάνω στην ασφάλεια δικτύων υπολογιστών και μερικές από τις κατηγοριοποιήσεις είναι η προσποίηση χρήστη ή συσκευής, διακοπή υπηρεσίας, αλλαγή δεδομένων, worm ή ιοί, ηλεκτρονικό ψάρεμα, υποκλοπή δεδομένων και ευαλωτότητες του λειτουργικού συστήματος. Σύμφωνα με τους συγγραφείς όλες οι έξυπνες οικιακές συσκευές χρησιμοποιούν το διαδίκτυο και για αυτόν τον λόγο το μοντέλο που συζητείται εφαρμόζεται μόνο σε δίκτυα υπολογιστών. Δεν περιέχονται δηλαδή λύσεις σε άλλα πρωτόκολλα όπως το ZigBee που και αυτό χρησιμοποιείται αρκετά σε έξυπνα περιβάλλοντα. [35] [38]

Ακόμα ένα έξυπνο σύστημα για ασφάλεια και αυτοματοποίηση του οικιακού περιβάλλοντος παρουσιάζεται στο 39. Στο άρθρο αναλύονται τα βασικά συστατικά και ο τρόπος ένωσης του φυσικού εξοπλισμού του συστήματος, ενώ διακρίνονται ο τρόπος λειτουργίας και σχετικά πλεονεκτήματα του συστήματος αυτού. Κατά την υλοποίηση του συστήματος, χρησιμοποιούνται PIR αισθητήρες κίνησης στην είσοδο του σπιτιού. Μόλις ανιχνευτεί κίνηση, στέλνεται σήμα στον μικροεπεξεργαστή και στην συνέχεια καλείται ο ιδιοκτήτης του σπιτιού. Αν αυτός επιθυμεί να ανοίξει τα φώτα και να ηχήσει η σειρήνα παραβίασης πληκτρολογεί “1” στο πληκτρολόγιο του τηλεφώνου του. Δίνεται η δυνατότητα κλήσης σε κοντινό αστυνομικό τμήμα αν ο ιδιοκτήτης κρίνει ότι το σπίτι βρίσκεται σε κίνδυνο και τέλος τα φώτα σβήνουν και η σειρήνα σταματά μετά από ορισμένο χρονικό διάστημα. Ωστόσο, το σύστημα αυτό περιλαμβάνει και αυτοματισμούς όπως άνοιγμα πόρτας, λειτουργία θέρμανσης – ψύξης και βιντεοκλήση κάθε φορά που κάποιος έρχεται ή φεύγει από το σπίτι. Κύρια πλεονεκτήματα του συστήματος αυτού είναι το χαμηλό κόστος υλοποίησης, το γεγονός ότι δεν χρησιμοποιείται συγκεκριμένη εφαρμογή για την λειτουργία του, παρά μόνο την πληκτρολόγηση ψηφίων στο τηλέφωνο. Με αυτόν τον τρόπο, αποφεύγει και ζητήματα ασφάλειας που πιθανόν έχει μια εφαρμογή, καθώς επίσης επιτρέπει σε πολλούς χρήστες με διαφορετικές συσκευές και λειτουργικά να το χρησιμοποιήσουν. Επιπρόσθετα, δεν απαιτεί δεδομένα κινητής τηλεφωνίας και λειτουργεί κανονικά και με wifi. Τέλος, σημαντικό πλεονέκτημα του συστήματος αποτελεί το γεγονός ότι η σήμανση κινδύνου μπορεί να καλείται από το χρήστη, όμως αναλύεται και από το σύστημα γιατί πολλές φορές ο χρήστης δεν κρίνει σωστά την κατάσταση. [39]

Αναφορικά με την έξυπνη οικιακή ασφάλεια, αναλύεται ένα τελευταίο σύστημα, το οποίο περιγράφεται στο 40. Το συγκεκριμένο σύστημα προσφέρει και αυτό αυτοματισμό σε λειτουργίες και ασφάλεια στο smart home ενώ χρησιμοποιεί Raspberry Pi και αισθητήρες. Το Raspberry Pi είναι ένας μικρού μεγέθους υπολογιστής, ο οποίος κατασκευάστηκε με δυνατότητα μεταφοράς. Η συσκευή αυτή σχεδιάστηκε με

σκοπό να είναι μικρή και προσιτή για να βοηθήσει στην ανάπτυξη του προγραμματισμού και την κατανόηση του υλικού εξοπλισμού. Χρησιμοποιεί λειτουργικό σύστημα Linux και όλες οι λειτουργίες του πραγματοποιούνται με μειωμένη ενεργειακή κατανάλωση. Σχετικά με τους αισθητήρες, το σύστημα λειτουργεί με PIR αισθητήρες κίνησης οι οποίοι χρησιμοποιούνται σε κάθε πόρτα ή παράθυρο του σπιτιού. Οι αισθητήρες αυτοί με την χρήση υπέρυθρων ακτίνων, ανιχνεύουν οποιαδήποτε μορφή κίνησης. Ακόμη, το σύστημα ανιχνεύει την ύπαρξη επικίνδυνων αερίων όπως καπνό, διοξείδιο του άνθρακα ή προπάνιο. Για τον έλεγχο της θερμοκρασίας και της υγρασίας στο σπίτι, υπάρχουν πολλοί αισθητήρες όπως οι ψηφιακοί αισθητήρες DHT22 οι οποίοι είναι πιο ακριβείς στις μετρήσεις και στην μετάδοση των πληροφοριών. Τέλος, το σύστημα περιλαμβάνει και κάμερα για την επιτήρηση δραστηριότητας και ασφάλεια του χώρου. [40]

Το προκείμενο σύστημα περιλαμβάνει την δική του εφαρμογή για έλεγχο των πολλών και διαφορετικών συσκευών και για να παρέχει τα απαιτούμενα χαρακτηριστικά ασφάλειας. Η εφαρμογή είναι φιλική στον χρήστη και τον ενημερώνει με σχετικά μηνύματα αν υπάρχουν προσπάθειες παραβίασης, ασυνήθιστης συμπεριφοράς στο σπίτι ή σε περιπτώσεις φυσικής καταστροφής όπως φωτιά. Ακόμη, η εφαρμογή εφαρμόζει πολιτικές ασφάλειας τόσο των συσκευών όσο και των δεδομένων που μεταφέρονται και αναλύονται από τον έναν κόμβο στον άλλο. Για την ασφάλιση των δεδομένων χρησιμοποιείται ο αλγόριθμος AES. Συγκεκριμένα, κατά την είσοδο στην εφαρμογή απαιτούνται πιστοποιητικά αυθεντικοποίησης του χρήστη και ο διαχειριστής μπορεί εύκολα να αφαιρέσει ή προσθέσει χρήστη καθώς και να αλλάξει διαπιστευτήρια. Ο αλγόριθμος κρυπτογράφησης AES χρησιμοποιείται για περεταίρω ασφάλεια στο δίκτυο, ενώ οι διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης πραγματοποιούνται στον server (Raspberry Pi). Για επιπλέον ανάλυση των λειτουργιών του συστήματος και της διαδικασίας μεταφοράς των δεδομένων προτείνεται το 40. [40]

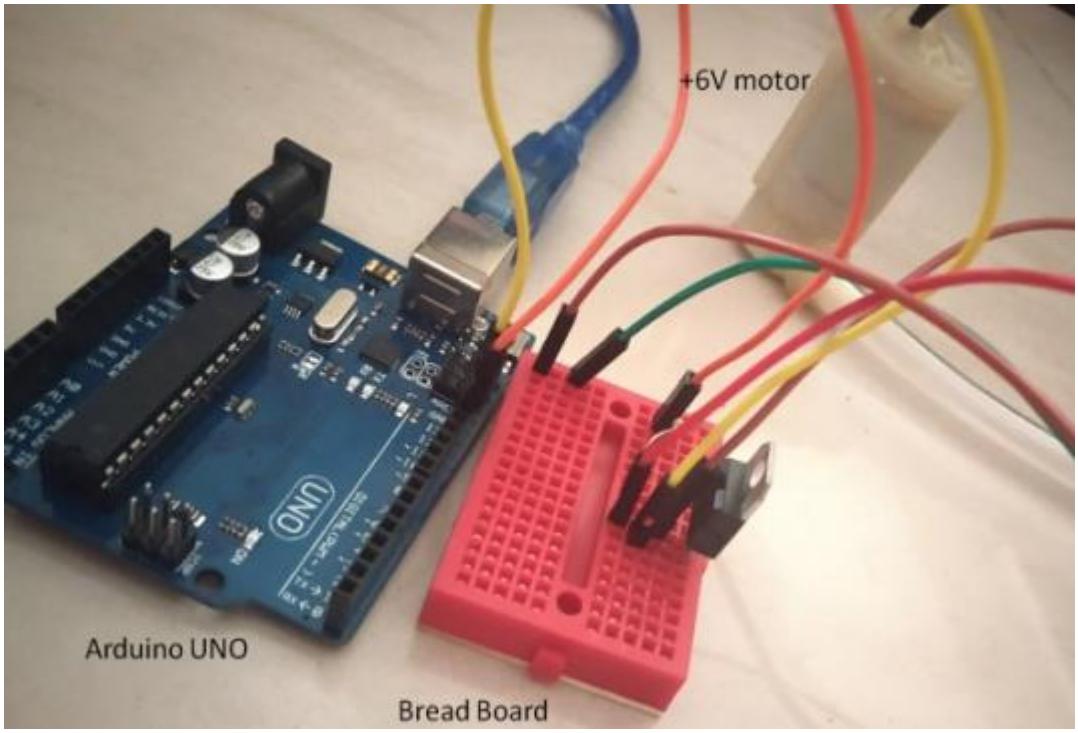
4.5 Έξυπνες οικιακές συσκευές

Παρακάτω, παρουσιάζονται μερικές έξυπνες συσκευές που λειτουργούν σε έξυπνα σπίτια, διακρίνεται η σχεδίαση και η υλοποίησή τους καθώς και διάφορες λειτουργίες τους που εξυπηρετούν το έξυπνο σπίτι.

4.5.1 Smart alarm clock

Το συγκεκριμένο έξυπνο ξυπνητήρι που παρουσιάζεται στο 41 υλοποιεί τέσσερις προσομοιώσεις ανάλογα τις διαφορετικές καταστάσεις στις οποίες πρέπει να ειδοποιεί τον χρήστη. Αρχικά, μία από τις καταστάσεις προσομοίωσης είναι η προσομοίωση ηλιοβασιλέματος. Για την ακρίβεια, το alarm clock βασίζεται στην δημιουργία τέτοιας έντασης φωτός ανάλογα με την ώρα και με τον φυσικό φωτισμό του ήλιου από μία συγκεκριμένη ώρα και μετά. Με τη χρήση ενός Arduino Uno R3 καθίσταται δυνατός ο καθορισμός έντασης του φωτός ανάλογα το ηλιακό φως και μισή ώρα πριν την ώρα που έχει ορίσει ο χρήστης για αφύπνιση, αρχίζει να αυξάνεται η φωτεινότητα. Την ώρα αφύπνισης φτάνει στην μέγιστη φωτεινότητα. Η επόμενη προσομοίωση ονομάζεται aroma alarm και λειτουργεί από την έξοδο που παίρνει από το alarm clock που ήδη αναφέρθηκε. Ουσιαστικά, με την συγκεκριμένη προσομοίωση παράγεται μυρωδιά καφέ την στιγμή που αφυπνείται ο χρήστης. Αυτό συμβαίνει διότι ο καφές έχει πλούσια μυρωδιά και κατά την έκχυσή του μπορεί να βοηθήσει στην διαδικασία αφύπνισης του εγκεφάλου. Η διαδικασία ξεκινάει από το προηγούμενο βράδυ, που ο χρήστης προσθέτει σκόνη καφέ σε ένα θερμό φιαλίδιο. Στην συνέχεια, ένας σωλήνας συνδέει το θερμό αυτό φιαλίδιο που περιέχει σκόνη καφέ με ένα άλλο φιαλίδιο που περιέχει νερό και όταν η φωτεινότητα φτάσει στην μέγιστη

έντασή της, τότε το Arduino ξεκινάει την λειτουργία σε ένα μοτέρ 6V που συνδέεται σε αυτό. Ένα transistor χρησιμοποιείται για να ενισχύσει την έξοδο που λαμβάνει από το Arduino και το μοτέρ ξεκινάει να περιστρέφεται και έτσι το νερό από το ένα φιαλίδιο πάει στο άλλο και παράγεται το χαρακτηριστικό άρωμα καφέ. Στην επόμενη προσομοίωση το ξυπνητήρι χρησιμοποιείται για να ειδοποιήσει τον χρήστη για συναντήσεις, ραντεβού και εργασίες που έχουν συγκεκριμένο χρόνο υλοποίησης με την χρήση του Arduino Uno. Η φυσική συνδεσμολογία περιγράφεται στο 41 ενώ παρουσιάζεται και στην παρακάτω εικόνα, και σχετικά με τις software ρυθμίσεις απαιτείται ο χρήστης να έχει λογαριασμό Temboo, και εφόσον έχει γίνει αυθεντικοποίηση του χρήστη, συνδέεται ο λογαριασμός του με το Google Calendar και ειδοποιείται για τις συναντήσεις και υποχρεώσεις του. Τέλος, αν σταλεί email στον χρήστη με περιεχόμενο “WAKE UP” ενεργοποιείται πάλι το alarm clock. Τελευταία λειτουργία αποτελεί η μέτρηση και ένδειξη θερμοκρασίας, υγρασίας και καιρικών φαινομένων που συχνά ενδιαφέρουν τους χρήστες λίγο πριν βγουν από το σπίτι. [41]



Εικόνα 3. Circuit using Arduino and motor [41]

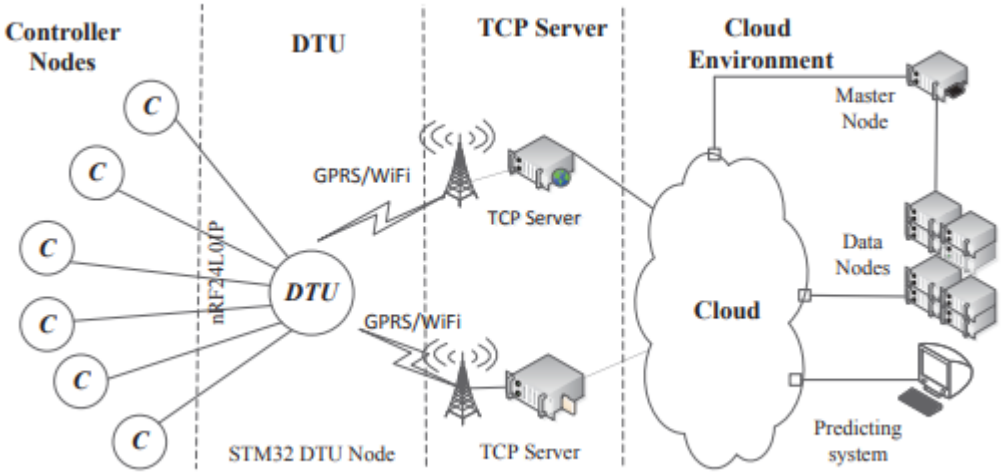
4.5.2 Έξυπνο ψυγείο

Το έξυπνο ψυγείο που περιγράφεται στο 42 αποτελείται από αισθητήρες οι οποίοι υπολογίζουν την ποσότητα γάλακτος και γενικά υγρών ποτών που υπάρχουν στο ψυγείο και άρα μπορεί να ειδοποιηθεί ο χρήστης πότε τελειώνει κάποιο τρόφιμο. Ακόμη, καταμετρείται ο αριθμός αυγών ή και λαχανικών που υπάρχουν και ανάλογα με τις προτιμήσεις του χρήστη να δημιουργείται λίστα με τα ψώνια που πρέπει να γίνουν. Σε αυτό το ψυγείο τα τρόφιμα έχουν συγκεκριμένη θέση. Τα μπουκάλια ή οποιοδήποτε υγρό ρόφημα μπαίνει σε θέση που υπάρχει ειδικός αισθητήρας για να υπολογίζει πότε τελειώνει. Σε περίπτωση που κάποιες θέσεις είναι κενές υπάρχει σχετική ένδειξη. Οι αισθητήρες που υπάρχουν σε αυτό το έξυπνο ψυγείο είναι αισθητήρες θερμοκρασίας, αερίων και proximity sensors. Ο αισθητήρας θερμοκρασίας χρησιμοποιείται για την μέτρηση και διατήρηση της σωστής θερμοκρασίας και ψύξης ενώ ακόμη χρησιμοποιείται και για την σύγκριση της θερμοκρασίας δωματίου με αυτήν της

αυτόματης απενεργοποίησης του ψυγείου. Ο αισθητήρας αερίων χρησιμοποιείται για λόγους ασφαλείας και ελέγχει την ύπαρξη αερίων στην ατμόσφαιρα που μπορεί να προέρχονται από λαχανικά ή φωτιά. Και το τελευταίο είδος αισθητήρα αξιοποιείται στην ανίχνευση ύπαρξης αντικειμένων, εν προκειμένω τροφίμων, και να υπολογίζεται η θέση τους αλλά και η ποσότητά τους. Κύριες λειτουργίες του ψυγείου είναι η λειτουργία ελέγχου ON/OFF από το κινητό τηλέφωνο, η αποστολή μηνύματος με λίστα προϊόντων που τελειώνουν ή τελείωσαν, η αποστολή ειδοποίησης σε περίπτωση που κάποια οσμή ξεπεράσει τα επιτρεπτά όρια. Ακόμη, ανιχνεύει την ποσότητα υγρού σε ροφήματα, στέλνει ειδοποιήσεις όταν θερμά αντικείμενα μπουν στο ψυγείο ή όταν κάποια τρόφιμα λήξουν, εξοικονομεί ενέργεια διακρίνοντας την θερμοκρασία περιβάλλοντος και ειδοποιεί τον χρήστη να κλείσει την πόρτα του ψυγείου μετά από κάποια δευτερόλεπτα. [42]

4.5.3 Smart Electric Heating Control System

Στο άρθρο 43 παρουσιάζεται ένα έξυπνο ηλεκτρικό σύστημα θέρμανσης. Αυτό το σύστημα βασίζεται σε έναν έξυπνο controller, του οποίου η φυσική ένωση με τον υπόλοιπο εξοπλισμό φαίνεται και περιγράφεται αναλυτικά στο άρθρο. Η σχεδίαση έγινε με βάση την εξοικονόμηση ενέργειας του συστήματος και του εξοπλισμού και η υλοποίηση του λογισμικού πραγματοποιήθηκε με FreeRTOS. Χρησιμοποιείται DTU το οποίο επιτρέπει την επικοινωνία μεταξύ του internet και του controller και το λογισμικό που τρέχει στο DTU πραγματοποιεί τέσσερις κύριες λειτουργίες. Η πρώτη αφορά την USART διεργασία δεδομένων, που αφορά την αποστολή και λήψη δεδομένων και άλλες λειτουργίες επικοινωνίας. Σε αυτό το σημείο τα δεδομένα από τις εντολές μεταφέρονται και συλλέγονται. Η δεύτερη λειτουργία πραγματοποιεί τον έλεγχο και ενημέρωση του συστήματος αποστέλλοντας μήνυμα στο κινητό τηλέφωνο του χρήστη με αντίστοιχα μηνύματα. Στην τρίτη λειτουργία προσφέρεται η δημιουργία TCP/IP συνδέσεων μεταξύ του DTU και του TCP server. Και στην τελευταία λειτουργία συλλέγονται δεδομένα από τον smart heater και αξιοποιούνται κατάλληλα. Παρακάτω διαφαίνεται και η αρχιτεκτονική του συστήματος ελέγχου του έξυπνου ηλεκτρικού συστήματος θέρμανσης. Περισσότερες πληροφορίες σχετικά με την συνδεσμολογία και τις λειτουργίες των server βρίσκονται στο 43. [43]



Εικόνα 4. The Smart Electric Heating Control System Architecture [43]

4.6 Διερεύνηση ευάλωτων σημείων στις έξυπνες οικιακές συσκευές

Στον οικιακό χώρο τα δεδομένα που ανταλλάσσονται είναι αρκετά προσωπικά καθώς αφορούν σε ήχο, εικόνα και βίντεο του χρήστη και συμπληρωματικά και με το γεγονός ότι οι έξυπνες συσκευές πρέπει να είναι διαθέσιμες για απομακρυσμένη διαχείριση και επικοινωνία μέσω του διαδικτύου δημιουργούνται πολλά «κενά» ασφάλειας, τα οποία χρήζουν εξέταση. Παρακάτω, αναφέρονται συνοπτικά κάποια ζητήματα ασφάλειας αυτών των συσκευών που σχετίζονται με την συσκευή, την επικοινωνία και τις υπηρεσίες που παρέχονται.

4.6.1 Ζητήματα ασφάλειας σχετικά με την συσκευή

Πολλές συσκευές είναι χαμηλής ενεργειακής κατανάλωσης με χαμηλό clock rate και throughput δεδομένων, επομένως δημιουργούν δυσκολίες στην προσθήκη κρυπτογράφησης των δεδομένων καθώς είναι μια διαδικασία που χρειάζεται πόρους για να πραγματοποιηθεί. Ακόμη, σε περίπτωση που δεν χρησιμοποιείται κάποιο πληκτρολόγιο, ποντίκι ή οθόνη για την διαχείριση της συσκευής, διαδικασίες όπως συναίνεση σε διάφορες πολιτικές μπορεί να είναι μια πρόκληση για τους χρήστες καθώς πρέπει να ενημερωθούν κατά κύριο λόγο από το smartphone. Τέλος, οι οικιακές συσκευές είναι τις περισσότερες φορές αφύλακτες ή ακόμα και μετά από κάποια ενημέρωση ή συντήρηση του συστήματος μπορεί να καταστούν ευάλωτες. Αυτό συμβαίνει καθώς αν τροποποιηθούν λειτουργίες για μείωση της ενεργειακής κατανάλωσης μπορεί να παρουσιαστούν κενά ασφάλειας και επίσης η ενημέρωση μπορεί να πραγματοποιηθεί από κακόβουλους σε περίπτωση που οι χρήστες δεν γνωρίζουν πως να το κάνουν, και βασιστούν σε κάποιον ειδικό. [44]

4.6.2 Ζητήματα ασφάλειας σχετικά με την επικοινωνία

Η ετερογένεια του συστήματος αποτελεί ευπάθειά του. Συσκευές από διαφορετικούς κατασκευαστές με διαφορετικά πρότυπα δικτύου και διαφορετικές δυνατότητες ενημέρωσης και το γεγονός ότι συνήθως δεν δίνονται εγχειρίδια χρήσης ή δεν είναι περιεκτικά, καθιστούν το σύστημα ευάλωτο και τους χρήστες ανυποψίαστους σχετικά με αυτό. Ακόμη, πολλές wearable συσκευές εισέρχονται και εξέρχονται από το οικιακό δίκτυο με μεγάλη ευκολία και διαχειρίζονται και απομακρυσμένα. Συνεπώς, η παρακολούθηση και διαχείριση συσκευών από κακόβουλους εισάγοντας συσκευές τους στο δίκτυο μπορεί να είναι εξίσου εύκολη. [45] [44]

4.6.3 Ζητήματα ασφάλειας σχετικά με τις υπηρεσίες

Η διαρκής άμβλυνση των ευπαθειών του συστήματος απαιτεί συνεχείς ενημερώσεις και επαναπρογραμματισμό από απόσταση. Αν κάποιες συσκευές δεν μπορούν να ακολουθήσουν αυτές τις ενημερώσεις λόγω του λειτουργικού συστήματος, του firmware ή του protocol stack που διαθέτουν, τότε δεν είναι ασφαλές να βρίσκονται στο δίκτυο. [44]

4.6.4 Ζητήματα ασφάλειας σχετικά με την φύση των έξυπνων IoT συσκευών

Λόγω της χρηστικότητας των έξυπνων οικιακών συσκευών, δηλαδή το γεγονός ότι πρέπει να είναι μικρές σε κατασκευή, χαμηλού βάρους και ενεργειακής κατανάλωσης, υψηλής απόδοσης καθώς και να διαχειρίζονται μεγάλο όγκο πληροφοριών, κάποιες διαδικασίες ασφάλειας όπως η κρυπτογραφία δεν είναι εύκολες στην υλοποίησή τους διότι χρειάζονται αρκετούς πόρους όπως bandwidth, ενεργειακή κατανάλωση και αποθηκευτικό χώρο. Για αυτόν τον λόγο, προτείνεται η χρήση “lightweight

cryptography" (LWC) με σκοπό να εξοικονομείται ενέργεια, υπολογισμοί, αποθήκευση και επικοινωνία άρα και ενεργειακή κατανάλωση που θα χρησιμοποιείται σε άλλου είδους εργασίες. Ωστόσο, όλοι οι αλγόριθμοι LWC μέχρι στιγμής βασίζονται στην συμμετρική κρυπτογράφηση και συνεπώς απαιτείται ο διαμοιρασμός πολλών συμμετρικών κλειδιών σε κάθε μία από τις έξυπνες αυτές συσκευές. Ακόμη, πρόκληση αποτελεί η διασφάλιση ψηφιακής υπογραφής για κάθε δημόσιο κλειδί ώστε να εξασφαλίζεται η αυθεντικοποίηση. [46] [47]

4.7 Επίλογος

Στο τέταρτο κεφάλαιο παρουσιάστηκαν και αναλύθηκαν κάποιες βασικές λειτουργίες του έξυπνου σπιτιού, που περιλαμβάνουν την άνεση, την υγεία του χρήστη και την ασφάλεια του συστήματος. Διασαφηνίστηκαν μερικά projects που υλοποιούν τις συγκεκριμένες λειτουργίες. Στην συνέχεια, διακρίθηκαν κάποιες έξυπνες συσκευές που απαρτίζουν το έξυπνο σπίτι, ο τρόπος λειτουργίας τους, η σχεδίαση και οι στόχοι των κατασκευαστών για αυτές τις συσκευές. Τέλος, διερευνήθηκαν ευπάθειες των έξυπνων συσκευών που σχετίζονται με τον σχεδιασμό τους, την επικοινωνία τους ή τις υπηρεσίες που μπορούν να προφέρουν.

Κεφάλαιο 5ο: Καλές πρακτικές προστασίας των συσκευών

5.1 Εισαγωγή

Στο πέμπτο κεφάλαιο διακρίνονται καλές πρακτικές ασφάλειας έξυπνων συσκευών που αφορούν σε κάθε στάδιο υλοποίησής τους, από την σχεδίαση μέχρι και την παραγωγή και υλοποίησή τους, την εξέλιξη και την συνεργασία με άλλες συσκευές. Αρχικά, διασαφηνίζεται η έννοια της καλής πρακτικής, πως συμβάλλει στην διαδικασία πραγματοποίησης έξυπνων συσκευών, καθώς επίσης αναφέρονται σχετικοί όροι για καλύτερη κατανόηση. Στην συνέχεια, αναλύονται καλές πρακτικές ανάλογα και το στάδιο υλοποίησης της συσκευής. Ακόμη, ομαδοποιούνται, παρουσιάζονται και εξετάζονται δεκατρείς οδηγοί – πρακτικές που προτείνει το UK Department for Culture, Media and Sport για την ασφάλιση των έξυπνων IoT συσκευών. Και τέλος, διακρίνονται βέλτιστες πρακτικές που χρειάζεται να ακολουθήσουν οι οργανισμοί με σκοπό την προστασία των συσκευών και συστημάτων που παράγουν.

Σχετικά με τον όρο πρακτική, σύμφωνα με το άρθρο 48, η καλή πρακτική έχει πρόθεση να πετύχει μετά από πολλή σκέψη ένα συγκεκριμένο αποτέλεσμα. Είναι κάτι που μπορεί να εξασκηθεί όπως μια πράξη και όχι κάτι που πρέπει απλά να πραγματοποιηθεί. Πρακτικά είναι αδύνατον να καθορίσεις ένα σκοπό σαν βέλτιστη πρακτική, καθώς το βέλτιστο διαφέρει ανάλογα το περιβάλλον, τις εφαρμογές και τους χρήστες που εξυπηρετούνται. Ο καθορισμός ενός στόχου ως βέλτιστη πρακτική απαιτεί γνώση όχι μόνο των υπόλοιπων πρακτικών και την σύγκρισή τους για να μετρηθεί κάπως η αξία του σε σχέση με τις υπόλοιπες αλλά και μία πρακτική one-size-fits-all που ταιριάζει δηλαδή σε όλες τις περιστάσεις. Σε κοινωνικό επίπεδο, "βέλτιστη πρακτική" συνήθως καλείται ο πιο κοινότυπος τρόπος (όχι απαραίτητα ο καλύτερος) για να κάνεις κάτι. Ακόμη, η διατύπωση και το αποτέλεσμα αυτής της πρακτικής πρέπει να είναι κατανοητά και από την σημασιολογική τους πλευρά και από την τεχνική τους πλευρά, και οι πρακτικές πρέπει να περιέχουν μόνο διαθέσιμες υπάρχουσες τεχνικές υλοποίησης. Κάποια αποτελέσματα συστήνουν πιο ξεκάθαρα τις πράξεις πραγματοποίησής τους από άλλα. Έτσι στο σύγγραμμα 48 διακρίνονται δύο βασικές κατηγορίες αποτελεσμάτων · αυτά τύπου V (από το Vague), τα οποία είναι πιο ασαφή στην πραγματοποίησή τους, και τα τύπου S (από το Specific), τα οποία απαιτούν συγκεκριμένες ενέργειες για να υλοποιηθούν. [48]

Όμως ακόμα και οι πρακτικές ανάλογα την ποιότητά τους και την αναγνώρισή τους χωρίζονται σε τρεις βασικές κατηγορίες · τις "Uber Practices", τις "Best Practices" και τις "Good Practices". Το πρώτο είδος αναφέρεται στις πρακτικές οι οποίες είναι υψηλού επιπέδου τεχνικά, όμως και υλοποιήσιμες σε μικρότερο βαθμό. Στο δεύτερο είδος περιλαμβάνονται οι πρακτικές στις οποίες λαμβάνεται υπόψιν η ποιότητά τους σε τέτοιο βαθμό ώστε να είναι οι πιο διαθέσιμες και ευρέως χρησιμοποιούμενες. Και τέλος, στην τρίτη κατηγορία ανήκουν εκείνες οι οποίες είτε δεν έχουν κοινή αποδοχή, είτε δεν χρησιμοποιούνται τόσο, είτε δεν έχουν μελετηθεί τόσο επειδή επιδιώκουν την ευκολία και το άμεσο όφελος. Τέλος, οι απαιτήσεις ανάλογα και το κάθε είδος πρακτικής ποικίλουν, όμως δεν καθορίζουν την ποιότητα της πρακτικής αλλά έχουν οριστεί ως απαιτήσεις από κάποια κυβερνητική οντότητα ή γενική απαίτηση. Οι απαιτήσεις περιέχουν πρακτικές επιπέδου αναφοράς αλλά και μια επίσημη αναγνώριση από οντότητες. [48]

5.2 Πρακτικές ασφάλειας

Η εφαρμογή ασφάλειας σε κάθε στάδιο υλοποίησης και χρήσης των συσκευών, αποτελεί την καλύτερη λύση για εξασφάλιση προστασίας των συσκευών. Παρακάτω παρουσιάζονται βέλτιστες πρακτικές για τα στάδια σχεδίασης και παραγωγής των συσκευών καθώς επίσης και για την διαχείριση, την επικοινωνία μεταξύ των συσκευών, την πρόσβαση σε αυτές, τις απαιτήσεις δικτύου, την διαχείριση των δεδομένων και ευαισθητοποίηση των χρηστών σχετικά με την διατήρηση της ασφάλειας στις IoT συσκευές.

5.2.1 Πρακτικές ασφάλισης συσκευών στο στάδιο σχεδίασης και υλοποίησης

Αρχικά, σε όλη την εξέλιξη του κύκλου ζωής των συσκευών πρέπει να λαμβάνεται υπόψιν η ασφάλειά τους. Αυτά τα στάδια είναι από την αρχική σχεδίαση και το πρωτότυπο, μέχρι το στάδιο ελέγχου και την ανάπτυξη της συσκευής. Κατά την υλοποίηση λοιπόν του hardware προτείνεται η χρήση λειτουργιών ασφάλειας όπως Trusted Platform Modules (TPMs) ή Hardware Security Modules (HSMs), τα οποία μπορούν να παρέχουν ασφαλή αποθήκευση κλειδιών κρυπτογράφησης κατά την διαδικασία κρυπτογράφησης, αποκρυπτογράφησης και αυθεντικοποίησης των συσκευών στο IoT δίκτυο και έτσι διευκολύνονται αυτές οι πολύ χρήσιμες, για την ασφάλεια, διαδικασίες. Ακόμη, στα πλαίσια μείωσης των ευπαθειών, υποδεικνύεται η ελαχιστοποίηση των διαθέσιμων πορτών των συσκευών, η απενεργοποίηση των μη χρησιμοποιούμενων υπηρεσιών και ο περιορισμός της χρήσης ευάλωτων πρωτοκόλλων επικοινωνίας. Επίσης, η χρήση ψηφιακών υπογραφών και κρυπτογραφικών hashes μπορούν να χρησιμοποιηθούν για να εξακριβωθεί η ακεραιότητα των firmware ενημερώσεων που πραγματοποιούνται κατά την διαδικασία εκκίνησης των IoT συσκευών. Αναφορικά με τους κατασκευαστές των συσκευών απαιτείται να υιοθετούν ασφαλείς πρακτικές ανάπτυξης λογισμικού, όπως χρήση στατικών και δυναμικών εργαλείων ανάλυσης κώδικα και πραγματοποίηση συχνών ελέγχων ασφάλειας. Πολύ σημαντική είναι και η συμβολή των ελέγχων ασφάλειας όπως penetration testing και αξιολόγηση των ευπαθειών κατά την διαδικασία ανάπτυξης των συσκευών με σκοπό την αναγνώριση πιθανών αδυναμιών ασφάλειας. Και τέλος, η συνεχής θέληση και προσπάθεια των οργανισμών για ευαισθητοποίηση και ενημέρωση των εργαζομένων τους, ενισχύει την ασφάλιση των συσκευών κατά το στάδιο σχεδίασης και παραγωγής των συσκευών. [49]

5.2.2 Πρακτικές ασφάλισης συσκευών κατά το στάδιο της ανάπτυξής τους

Όσον αφορά τις ενημερώσεις firmware των συσκευών προτείνεται η χρήση τους έγκαιρα, αναφορικά και με τις γνωστές ευπάθειες ασφάλειας, αλλά και να δίνεται η δυνατότητα αυτόματων ενημερώσεων ώστε να μην απαιτείται η παρέμβαση του χρήστη και να μένουν οι συσκευές ενήμερες σύμφωνα με τα πρόσφατα patches ασφάλειας. Ακόμη, η δυνατότητα ταυτοποίησης της τρέχουσας έκδοσης και η επιστροφή σε κάποια προηγούμενη έκδοση θα βοηθήσει τους χρήστες να επιστρέψουν σε κάποια προηγούμενη έκδοση αν υπάρχει κάποια ασυμβατότητα ή θέματα στην καινούργια. Αλλά και η ακριβής ενημέρωση των χρηστών σχετικά με τις ευπάθειες που πραγματεύεται η συγκεκριμένη ενημέρωση και η λειτουργικότητά της, θα διευκολύνει τους χρήστες να κατανοήσουν την σημασία και την αναγκαιότητά της. Τέλος, είναι απαραίτητο να υπάρχει δυνατότητα ενημέρωσης και των παλιότερων συσκευών, ίσως με την συμβολή άλλων παρόχων ή την χρήση firmware ανοιχτού κώδικα για την διατήρηση και συντήρηση και αυτών των συσκευών. [49]

5.2.3 Πρακτικές που βοηθούν στην αυθεντικοποίηση και έλεγχο των συσκευών

Η χρήση μοναδικών διαπιστευτηρίων κατά την είσοδο στην συσκευή και η συχνή αλλαγή τους πρέπει να προτείνεται στους χρήστες μέσω των συσκευών αλλά και η χρήση αυθεντικοποίησης πολλών παραγόντων βοηθάει στο να αποφεύγεται η εύκολη πρόσβαση από κακόβουλους μέσω γνωστών προεπιλεγμένων διαπιστευτηρίων και μέσω διείσδυσης σε μία μόνο συσκευή. Επιπρόσθετα, η διάκριση ρόλων των χρηστών ανάλογα και τις γνώσεις τους μπορεί να περιορίσει ανεπιθύμητες ενέργειες από μη γνώστες και η χρήση ασφαλών πρωτοκόλλων ασφάλειας όπως TLS, SSH ενισχύουν την ακεραιότητα και εμπιστευτικότητα των δεδομένων που ανταλλάσσονται μεταξύ των IoT συσκευών και των σχετικών δικτύων τους. Τέλος, η συνεχής παρακολούθηση των ενεργειών των χρηστών της συσκευής μπορεί να οδηγήσει σε ανίχνευση ασυνήθιστης συμπεριφοράς και να περιορίσει τις άδειες και ενέργειες του χρήστη αυτού. [49]

5.2.4 Πρακτικές ασφάλισης των δεδομένων

Με σκοπό την διασφάλιση των δεδομένων που διαχειρίζονται οι συσκευές, απαιτείται η κρυπτογράφησή τους. Πιο συγκεκριμένα, τα δεδομένα τα οποία αποθηκεύονται στις IoT συσκευές, όπως διαπιστευτήρια χρήστη, ρυθμίσεις και ευαίσθητα λειτουργικά δεδομένα της συσκευής, μπορούν να προστατευτούν μέσω αλγορίθμων κρυπτογράφησης όπως ο Advanced Encryption Standard (AES). Ωστόσο, για τα δεδομένα που ανταλλάσσουν οι συσκευές, χρειάζονται ασφαλή πρωτόκολλα επικοινωνίας καθώς τα δεδομένα περνούν από δίκτυα και υπηρεσίες cloud και μπορούν εύκολα να υποκλαπούν από τρίτους. Ακόμη, κατά την κρυπτογράφηση απαιτείται η υποδομή από τις συσκευές για αποθήκευση και διαχείριση των κρυπτογραφικών κλειδιών και προτείνεται η χρήση αλγορίθμων κρυπτογράφησης οι οποίοι είναι πολύ δοκιμασμένοι και ευρέως αποδεκτοί από την κοινότητα της κυβερνοασφάλειας, όπως οι AES, RSA, ECC. Επίσης, συστήνεται η κρυπτογράφηση end-to-end δηλαδή από τον αποστολέα στον παραλήπτη και υποδεικνύονται ασφαλείς μηχανισμοί κατά την ανταλλαγή των κρυπτογραφικών κλειδιών όπως οι Diffie-Hellman key exchange και Elliptic Curve Diffie-Hellman (ECDH). Τέλος, η πραγματοποίηση συχνών αξιολογήσεων και ενημερώσεων σχετικά με κρυπτογραφικές μεθόδους ενισχύουν στην αναγνώριση πιθανόν αδυναμιών άρα και προστασία από αυτές. [49]

5.2.5 Πρακτικές ασφάλισης δικτύου

Αναφορικά με την ασφάλιση του δικτύου που ανήκουν οι συσκευές, αποτελεί καλή πρακτική να χωρίζονται οι συσκευές IoT από το υπόλοιπο δίκτυο με την δημιουργία network segments ή virtual local area networks (VLANs). Αυτός ο κατακερματισμός του δικτύου βοηθάει τον περιορισμό εξάπλωσης μιας πιθανής επίθεσης σε συσκευές που διαχειρίζονται ευαίσθητα προσωπικά δεδομένα όπως είναι οι έξυπνες οικιακές συσκευές. Επιπρόσθετα, η χρήση firewall και intrusion detection and prevention systems (IDPS) στο δίκτυο για έλεγχο και περιορισμό δεδομένων που εισέρχονται ή εξέρχονται από αυτό αλλά και ανίχνευση ενδείξεων παραβατικής συμπεριφοράς, βοηθούν στην προστασία τόσο από εξωτερικούς όσο και από εσωτερικούς επιτιθέμενους και στην αναγνώριση μιας επίθεσης σε πραγματικό χρόνο. Στο ίδιο πλαίσιο, προτείνεται η εφαρμογή συστημάτων network access control (NAC) για διαχείριση και εφαρμογή πολιτικών σχετικά με την πρόσβαση των συσκευών στο δίκτυο. Με αυτόν τον τρόπο, μόνο εξουσιοδοτημένες συσκευές θα μπορούν να συνδεθούν στο δίκτυο. Και τέλος, με προσθήκη επιπλέον ασφάλειας στις gateway συσκευές αλλά και με καταγραφή ενεργειών κάθε συσκευής για παρατήρηση ασυνήθιστων ενεργειών προφυλάσσεται επιπλέον το κάθε δίκτυο που απαρτίζεται από έξυπνες IoT συσκευές. [49]

5.2.6 Πρακτικές ευαισθητοποίησης και εκπαίδευσης των χρηστών

Οι χρήστες των έξυπνων οικιακών συσκευών αποτελούν και τους άμεσα ενδιαφερόμενους σχετικά με την ασφάλεια και την προστασία του δικτύου και των συσκευών τους. Με τις ενέργειές τους μπορούν να περιορίσουν ή να επιδεινώσουν πιθανά ζητήματα ασφάλειας που υπάρχουν, επομένως κρίνεται σημαντική η επίγνωσή τους και να γίνεται, όσο το δυνατόν ευκολότερη, η διαδικασία επιμόρφωσής τους σε σχετικά θέματα. Αυτή η επιμόρφωση μπορεί να γίνεται σε κάποιο τακτικό πρόγραμμα, με σκοπό να γνωρίζουν τις επερχόμενες απειλές, τις βέλτιστες πρακτικές και τις υποχρεώσεις τους όσον αφορά την διατήρηση της ασφάλειας στις συσκευές τους. Ακόμη, πολύ χρήσιμο θα ήταν να υπάρχει συγκεκριμένο υλικό για τις ανάγκες και τα ζητήματα ασφάλειας κάθε συσκευής και οργανισμού, και έτσι σε λιγότερο χρόνο να μπορεί ο χρήστης να αποκτήσει συναφείς πληροφορίες σχετικά με τις συσκευές του εκάστοτε κατασκευαστή που διαθέτει. Επίσης, η δημιουργία κατανοητού υλικού και η μετάδοσή του σε πολλές μορφές όπως βίντεο ή ακόμα και παιχνίδι αλλά και η προσφορά κινήτρων όπως έπαθλα, σίγουρα θα εντείνει το ενδιαφέρον των χρηστών για περαιτέρω ενασχόληση με το αντικείμενο. Τέλος, η ανατροφοδότηση και αξιολόγηση της απόδοσης και ευαισθητοποίησης των χρηστών καθώς επίσης και συγκεκριμένες οδηγίες σε περιπτώσεις ανάγκης όπως αρχικά βήματα ανά περίσταση και άμεση επικοινωνία με κάποιο κέντρο βοηθείας μπορούν να κατατοπίσουν πλήρως τους χρήστες αναφορικά με τις βέλτιστες πρακτικές που χρειάζεται να ακολουθούν. [49]

5.3 UK’s 13 guidelines

Παρακάτω παρουσιάζονται δεκατρείς οδηγοί – πρακτικές που προτείνονται από σχετική ανάλυση του UK Department for Culture, Media and Sport (DCMS) για βελτίωση της ασφάλειας στις IoT συσκευές. Αυτοί οι οδηγοί χωρίζονται σε τέσσερα είδη σύμφωνα με το άρθρο 48, και το πρώτο είδος αφορά τις πρακτικές οι οποίες είναι εύκολες στην εφαρμογή, απαιτούν ελάχιστες έξτρα υπηρεσίες, προσφέρουν υψηλή αποτελεσματικότητα και θα έπρεπε ήδη να εφαρμόζονται με σκοπό την βελτίωση της ασφάλειας των συσκευών. Η πρώτη πρακτική πρόκειται για την εισαγωγή ενός κωδικού πρόσβασης στις συσκευές ο οποίος να είναι αρκετά μεγάλος ώστε να είναι σχετικά αδύνατο να τον «μαντέψει» κάποιος κακόβουλος, αλλά αρκετά εύκολος στην απομνημόνευση για να τον χρησιμοποιεί ο χρήστης. Σύμφωνα με το NIST ένας κωδικός με έξι τυχαία ψηφία επιλεγμένα για PIN μπορεί να βοηθήσει στην προστασία από ηλεκτρονικές απάτες εφόσον χρησιμοποιούνται φυσικά και άλλες μέθοδοι προστασίας. Ακόμη, κατά την αποθήκευση των δεδομένων στις συσκευές πρέπει να παρέχεται ασφάλεια. Τέτοια δεδομένα μπορεί να είναι πιστοποιητικά χρήστη όπως κωδικοί, PINs και πληροφορίες εισόδου όπως κλειδιά κρυπτογράφησης που χρησιμοποιούνται για ασφαλή επικοινωνία με άλλες συσκευές ή ευαίσθητα καταγεγραμμένα δεδομένα του χρήστη. Η υποκλοπή αυτών των δεδομένων μπορεί να συμβεί είτε από δια ζώσης παράβαση είτε από απομακρυσμένη επίθεση. Ακόμα μία πιο γνωστή πρακτική είναι η διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της αυθεντικοποίησης στις επικοινωνίες από και προς τις συσκευές και υπηρεσίες. Αφορά στις δυνατότητες που φέρει κάθε συσκευή και στις ενέργειες που μπορεί να πραγματοποιήσει, όπως διαδικασίες κρυπτογράφησης. Ο υπολογιστικός χρόνος που απαιτείται για αυτές τις διαδικασίες αλλά και η ενεργειακή κατανάλωση θα πρέπει να λαμβάνονται υπόψιν. Επίσης, επισημαίνεται ότι θα έπρεπε να είναι αναμενόμενο, ειδικά στις συσκευές οι οποίες είναι διαθέσιμες παγκοσμίως, να απενεργοποιούνται όλες οι μη χρησιμοποιούμενες υπηρεσίες και πρωτόκολλα. Αυτό αποτρέπει από την χρήση αυτών των υπηρεσιών από κακόβουλους με σκοπό να υποκλέψουν δεδομένα για την συσκευή ή το δίκτυο στο οποίο ανήκει, ή να εγκατασταθεί καινούργιο λογισμικό με επιπρόσθετες δυνατότητες που θα εξυπηρετεί τον επιτιθέμενο. Η απενεργοποίηση αυτών

των λειτουργιών μπορεί να είναι δύσκολη ειδικά για χρήστες που δεν ασχολούνται, έτσι θα πρέπει να προτείνονται από τους κατασκευαστές συντομεύσεις σε αυτού του είδους τις λειτουργίες, οι οποίες θα γνωστοποιούνται και στους αγοραστές των συσκευών. Τέλος, σχετικά με το πρώτο είδος πρακτικών ανήκει ακόμα και η προστασία των δεδομένων που αποθηκεύονται και διαχειρίζονται οι εξυπηρετητές. Τα δεδομένα που μεταφέρονται από μία συσκευή σε μία άλλη ακολουθούν τις ίδιες απαιτήσεις ασφαλείας με τα δεδομένα που αποθηκεύονται και χρησιμοποιούνται τοπικά και μάλιστα τα πρώτα «απειλούνται» από πολλούς περισσότερους κινδύνους, επομένως πρέπει να εξακριβώνονται και να αυθεντικοποιούνται πρώτα αυτά τα συμβαλλόμενα μέρη. [50]

Σχετικά με την δεύτερη κατηγορία απαιτήσεων, πρόκειται για πρακτικές οι οποίες έχουν εύκολη εφαρμογή, μικρή αποτελεσματικότητα στην προστασία ευπαθειών, θα έπρεπε να πραγματοποιηθούν όμως με χαμηλότερη προτεραιότητα. Αποκαλούνται “optional” πρακτικές, αν και μια βέλτιστη πρακτική ασφάλειας δεν θα έπρεπε να είναι προαιρετική, στην πραγματικότητα λόγω και του κόστους κα του χρόνου υλοποίησής τους, δεν μπορούν να πραγματοποιηθούν όλες οι πρακτικές και οι προτροπές ασφάλειας. Η πρώτη λοιπόν πρακτική απευθύνεται στους κατασκευαστές των συσκευών και αφορά στην ανάπτυξη πολιτικών σε περίπτωση εύρεσης ευπαθειών στο προϊόν, μέσω testing που γίνονται. Η ενημέρωση ότι κάτι δεν λειτουργεί όπως αναμένεται στο προϊόν, δίνει το κίνητρο για συνεχή εξέλιξη και διόρθωση λαθών σε όποιο στάδιο και αν ανήκουν και εξελίσσουν την ομάδα και το προϊόν. Αν και η δημιουργία μιας φόρμας ή διεύθυνσης διαθέσιμης στο ευρύ κοινό (όπως χρήστες ή ερευνητές) είναι κάτι εύκολο στην πραγματοποίησή του, ωστόσο από μόνη της δεν αποτελεί μια πρακτική η οποία θα βελτιώσει απαραίτητα την ασφάλεια του προϊόντος. Επίσης, προτείνεται η σχεδίαση συσκευών (φυσική σχεδίαση και user interface) να υλοποιείται με βάση την ευκολία χρήσης των χρηστών και να διευκολύνονται διαδικασίες όπως εγκατάσταση και συντήρηση. Καθώς ένα από τα χαρακτηριστικά των IoT συσκευών είναι ότι δεν έχουν μια συγκεκριμένη εμφάνιση, user interface, οθόνη, πληκτρολόγιο, και βασίζονται σε τεχνικές απομακρυσμένης επικοινωνίας για την λειτουργία τους, πολλές φορές είναι τόσο δύσκολη η εγκατάστασή τους στο δίκτυο που παραβλέπονται άλλα ζητήματα όπως οι ρυθμίσεις ασφαλείας τους. Με αυτόν τον τρόπο οι συσκευές λειτουργούν με τις προεπιλεγμένες ρυθμίσεις και έτσι αυτή η πρακτική σχετίζεται και με την ασφαλή σχεδίαση της συσκευής, δηλαδή την χρήση ασφαλών προτύπων κατά την διαδικασία της σχεδίασης και εφαρμογής ρυθμίσεων. [50]

Στην τρίτη κατηγορία πρακτικών ανήκουν εκείνες που έχουν δύσκολη εφαρμογή, χαμηλή αποτελεσματικότητα και δεν πραγματοποιούνται τόσο συχνά. Πρόκειται για πρακτικές οι οποίες έχουν υψηλό βαθμό συντήρησης, λιγότερη χρήση από τους χρήστες και δεν παρέχουν σημαντικά οφέλη στην ασφάλεια των συσκευών ώστε να αξίζουν το κόστος. Η υλοποίησή τους εξαρτάται από την εταιρία που κατασκευάζει τις έξυπνες αυτές συσκευές και τον διαθέσιμο οικονομικό προϋπολογισμό που διαθέτει για την ασφάλισή τους. Σε αυτού του είδους τις πρακτικές ανήκει η διαμόρφωση, η υλοποίηση και ο έλεγχος πλάνων για την διαχείριση και αντιμετώπιση περιπτώσεων διακοπής λειτουργίας της συσκευής και κατά πόσο σε αυτή την κατάσταση είναι ασφαλής. Είναι αρκετά σημαντικό η συσκευή να διαθέτει ένα ελάχιστο επίπεδο ρυθμίσεων με το οποίο θα μπορεί να λειτουργεί ανεξάρτητα από τις διαθέσιμες συνδέσεις που υπάρχουν για να είναι σε θέση να μεταδίδει δεδομένα συνέχεια, όπως προβλέπεται και από την φύση των συσκευών αυτών. Σχετικά με αυτό, απαιτείται να λαμβάνεται υπόψιν και το ποσοστό μπαταρίας που εξαντλείται για να πραγματοποιηθούν οι ενέργειες κάτω από αυτές τις συνθήκες. [50]

Στην τέταρτη και τελευταία ομαδοποίηση πρακτικών ανήκουν εκείνες που είναι δύσκολες στην υλοποίηση, φέρουν υψηλού επιπέδου αποτελεσματικότητα στην ασφάλεια και ακόμη ερευνώνται. Αυτό το είδος πρακτικών περιέχει την υλοποίηση αυτόματης και ασφαλής παροχής και εγκατάστασης ενημερώσεων ασφάλειας λογισμικού. Ενώ ο περιορισμός των ευπαθειών μιας συσκευής είναι μια πολύ

συχνά πραγματοποιήσιμη διαδικασία, η αυτοματοποίηση αυτών των ενημερώσεων δεν είναι. Ακόμη, η αποδοχή ότι ο χρήστης έχει την ευθύνη και θα κάνει τακτικά ενημέρωση στις συσκευές του είναι περισσότερο ουτοπικό παρά συμβατό με την πραγματικότητα. Ωστόσο, οι διαδικασίες αυτοματοποίησης της ακεραιότητας μιας ενημέρωσης, καθώς και η συνέχιση των ενημερώσεων σε παλαιότερες συσκευές ή από κατασκευαστές οι οποίοι δεν δραστηριοποιούνται πια, κάνουν ακόμη πιο δύσκολη την διεκπεραίωση του έργου αυτού, εφόσον όλα τα πιθανά σενάρια χρειάζεται να εξεταστούν. Επιπρόσθετα, η παροχή τρόπων ανίχνευσης και πιθανής ανάκτησης από παραβιάσεις ακεραιότητας λογισμικού αποτελούν ακόμα μια πρακτική. Αφορά στην επαναφορά της συσκευής σε μια «υγιή» κατάσταση, στην οποία μπορεί να έρθει μέσω του hardware ή με την δημιουργία προληπτικών λειτουργιών στο λογισμικό. Ακόμη προτείνεται η χρήση εργαλείου παρακολούθησης ενεργειών που πραγματοποιούνται μέσω της συσκευής, αν και αυτό δημιουργεί επιπλέον ζητήματα ασφάλειας καθώς τα δεδομένα θα πρέπει να μεταφέρονται και να αποθηκεύονται εκτός της συσκευής. Διαφορετικά, με την χρήση συστημάτων όπως Intrusion Detection System (IDS) μπορούν και τοπικά να προστατευτούν οι IoT συσκευές, όμως αυτό απαιτεί είτε ένα IDS στο κάθε δίκτυο είτε να τρέχει σε κάθε host του δικτύου. Ωστόσο κάτι τέτοιο σε IoT συσκευές αποτελεί πρόκληση και προβλέπεται να εφαρμοστεί στο μέλλον. Επίσης, χρειάζεται να δίνετε η δυνατότητα στους χρήστες να διαχειρίζονται και να διαγράφουν, εάν το επιθυμούν, τα προσωπικά τους δεδομένα τα οποία χρησιμοποιούνται από τις συσκευές. Αυτό φέρει δυσκολία κυρίως λόγω της εμφάνισης των συσκευών, οι οποίες κατά κύριο λόγο δεν έχουν κάποια οθόνη ή και αν έχουν είναι μικρή και δεν έγκειται για χρήση παρά μόνο για ανάγνωση χρήσιμων πληροφοριών. Οι περισσότερες IoT συσκευές χρησιμοποιούν υπολογιστή ή smartphone για να αλληλεπιδράσουν με τον χρήστη, ωστόσο σε αυτήν την περίπτωση τα δεδομένα με τις αντίστοιχες εντολές χρήσης τους διαχειρίζονται μέσω κάποιας εφαρμογής και η αποθήκευσή τους εντείνει επιπλέον τον βαθμό δυσκολίας. Τέλος, απαιτείται διασφάλιση των εντολών που εισάγονται στις συσκευές και κατά πόσο προέρχονται όντως από τον χρήστη. Καθώς οι εντολές μπορεί να προέρχονται από φωνητικές εντολές, γραπτές εντολές ή από πατήματα στην οθόνη, πρέπει με κάποιο τρόπο να φιλτράρονται και να βεβαιώνεται η γνησιότητα του χρήστη. [50]

5.4 Οδηγοί για πιο λειτουργική κυβερνοασφάλεια σε οργανισμούς

Στο σύγγραμμα 51 αναφέρονται βασικές κατευθυντήριες γραμμές για την διαχείριση και προστασία συστημάτων και συσκευών, σύμφωνα με σχετική έρευνα που έγινε. Σε αυτήν την έρευνα διαπιστώθηκε ότι η κυβερνοασφάλεια θα έπρεπε να λαμβάνεται υπόψιν από την σχεδίαση κιόλας της συσκευής καθώς και η λειτουργικότητά της να είναι τόσο ευέλικτη ώστε να μπορεί να προσαρμοστεί σε κάθε χρήστη. Ακόμη, συστήνεται η χρήση ανατροφοδότησης με σκοπό την κατανοητή και απλή ανάδραση του χρήστη με την συσκευή καθώς του δίνονται συμβουλές ανάλογα τις ενέργειες που πραγματοποιεί. Επίσης, η αποτροπή λαθών και η επαναφορά του συστήματος σε προηγούμενη κατάσταση είναι πολύ χρήσιμο εργαλείο καθώς μαζί με την περιγραφή της κατάστασης ασφάλειας της συσκευής σε κάθε ενέργεια που πραγματοποιεί ο χρήστης, προσφέρεται η αίσθηση ότι τίποτα δεν μπορεί να πάει λάθος και διορθώνονται πιθανώς λάθος ενέργειες. Έχει αποδειχτεί ότι οι χρήστες προτιμούν συσκευές οι οποίες παρέχουν ευκολία χρήσης καθώς επίσης δεν απαιτούν ιδιαίτερη μνήμη για να γίνουν οι λειτουργίες. Αυτό συμβαίνει διότι δεν μπορούν να διαθέσουν πολύ χρόνο και προσπάθεια στην αλληλεπίδρασή τους με τις συσκευές τους. Με βάση αυτό, είναι απαραίτητο να μένει στον χρήστη μια ευχάριστη εντύπωση κατά την χρήση της συσκευής. Δηλαδή, οι εντολές που δίνονται στην συσκευή να είναι αρκετά κατανοητές και όσο το δυνατόν πιο μικρές ώστε να δίνουν στον χρήστη μια ευχάριστη εμπειρία εφόσον θα είναι εύκολο και γρήγορο να πραγματοποιήσει το επιθυμητό αποτέλεσμα. Ακόμα

και η εμφάνιση αλλά και η ικανότητα μάθησης μέσω της συσκευής αποτελούν τακτικές για καλύτερη εντύπωση και εμπειρία που μένει στον χρήστη. [51]

Στο άρθρο 52, παρουσιάζονται βασικές τακτικές και βέλτιστες πρακτικές κυβερνοασφάλειας που πρέπει να εφαρμόζεται από κάθε οργανισμό με σκοπό την καλύτερη προστασία των συσκευών. Αρχικά, διασαφηνίζει ότι δεν υπάρχουν συγκεκριμένοι νόμοι κυβερνοασφάλειας όμως πρέπει κάθε οργανισμός σύμφωνα και με την κρίση του να ακολουθεί συγκεκριμένες πρακτικές από άλλους φορείς και διακεκριμένους οργανισμούς με σκοπό τον καθορισμό προγράμματος διαχείρισης πιθανού κινδύνου κυβερνοασφάλειας. Επιπρόσθετα, προτείνεται η αξιολόγηση και αποτίμηση των ευπαθειών που φέρει κάθε οργανισμός ή επιχείρηση, με σκοπό την αναγνώριση τρόπων εισβολής επιτιθέμενων στο σύστημα. Ακόμα, σε αυτό το πλαίσιο πολλές φορές τα δεδομένα του οργανισμού φέρουν και εσωτερικούς κινδύνους. Στην περίπτωση του bring-your-own-device (“BYOD”) κατά την οποία ο εργαζόμενος φέρνει δική του συσκευή για να εργαστεί, μεταφέρει δεδομένα του οργανισμού στην συσκευή του και αν η συσκευή του είναι μολυσμένη μπορεί να υποκλαπούν τα ευαίσθητα δεδομένα αυτής της επιχείρησης. Ακόμη, και στο οικιακό δίκτυο τα δεδομένα που διαχειρίζονται οι έξυπνες συσκευές είναι ευαίσθητα και οι χρήστες συνήθως δεν γνωρίζουν τι άδειες και δεδομένα τους χρησιμοποιούνται και πως μπορεί να λειτουργεί η συσκευή τους όταν δεν βρίσκεται σε δική τους χρήση. Δεδομένα όπως αν βρίσκονται αυτήν την χρονική στιγμή στο σπίτι μπορεί να διαρρεύσουν σε κακόβουλους, Αυτό μπορεί να συμβεί μέσω του συστήματος φωτός, θέρμανσης ή ψύξης ή ακόμα και η μη χρήση των συσκευών για πολλές ώρες μπορεί να υποδηλώσει τις ενέργειες του χρήστη. Κάτι που είναι πολύ γνωστό, ωστόσο είναι τόσο γνωστό λόγω της σημαντικότητάς του, είναι το να γίνονται πολύ τακτικά οι απαραίτητες ενημερώσεις στα συστήματα και τις συσκευές που χρησιμοποιούνται σε κάθε οργανισμό, καθώς ευαλωτότητες και αδυναμίες του λογισμικού που έχουν ληφθεί υπόψιν από τους προγραμματιστές, είναι πολύ χρήσιμες και πρέπει να καλύπτονται από τις ενημερώσεις αυτές. Επίσης, πολλοί οργανισμοί συνεργάζονται με άλλους, οπότε πρέπει να είναι σε θέση να εμπιστευτούν τον εκάστοτε άλλο οργανισμό και να γνωρίζουν πως ακριβώς οι υπηρεσίες που προσφέρονται από αυτούς, επηρεάζουν την ασφάλεια του δικού τους οργανισμού. Στο 52 προτείνονται συγκεκριμένες ερωτήσεις που βοηθούν επιχειρήσεις και οργανισμούς να εξετάσουν αν είναι όντως μια ασφαλής συνεργασία αυτή, ή αν αποτελεί μελλοντικό κίνδυνο, και αφορούν το ελάχιστο επίπεδο ασφάλειας που χρειάζεται να έχει κάποιος οργανισμός για να συνεργαστεί μαζί του κάποιος άλλος, τον τρόπο διαχείρισης και προστασίας των δεδομένων του και τι ενέργειες μπορεί να επιφέρει ο ένας οργανισμός στον άλλο. Ακόμη, προτείνεται η χρήση ενός πλάνου διαχείρισης και ελέγχου της πρόσβασης στα δεδομένα από όπου και αν προέρχεται. Πάλι παρέχονται κατατοπιστικές ερωτήσεις σχετικές με την δημιουργία του πλάνου αυτού και αφορούν την κατάλληλη στιγμή να ζητείται πρόσβαση από τον χρήστη, για πόσο χρονικό διάστημα θα δίνεται, σε ποια αρχεία πρέπει η πρόσβαση να αποκλείεται, αν υπάρχουν τέτοια αρχεία, ποιοι εργαζόμενοι μπορούν να έχουν πρόσβαση και σε τι είδους δεδομένα και τέλος αν μπορούν να κρυπτογραφηθούν οικονομικά και προσωπικά στοιχεία της επιχείρησης για να μην υποκλαπούν. Φυσικά και η εκπαίδευση των εργαζομένων και η κατάρτισή τους σχετικά με τους κανόνες της επιχείρησης δεν μπορεί να λείπει από τις τακτικές για καλύτερη ασφάλεια. Η επικοινωνία, οι μέθοδοι που ακολουθούνται ανά περίπτωση, η αναφορά περιστατικών και ο έλεγχος των εργαζομένων σχετικά με την κατανόηση και τήρηση των αρχών ασφάλειας της επιχείρησης περικλείουν την εκπαίδευση αυτή των εργαζομένων. Τέλος, πολύ σημαντικό είναι να καθοριστεί και πλάνο δράσης σε κάθε περίπτωση παραβίασης της ασφάλειας ώστε να είναι προετοιμασμένοι και οργανωμένοι και οι εργαζόμενοι. Αυτό το σχέδιο δράσης χρειάζεται συχνά επανεκτίμηση και επικαιροποίηση ανάλογα και τις τεχνολογίες που χρησιμοποιεί η επιχείρηση και ίσως η υλοποίησή του δοκιμαστικά για καλύτερη εξοικείωση και εύρεση πιθανών παραλήψεων ή και λαθών. [52]

5.5 Επίλογος

Στο πέμπτο κεφάλαιο παρουσιάστηκαν και αναλύθηκαν κάποιες καλές πρακτικές προστασίας έξυπνων IoT συσκευών. Αρχικά, διασαφηνίστηκε η σημασία του όρου πρακτική καθώς διακρίθηκαν και οι βασικές κατηγορίες πρακτικών. Στην συνέχεια, αναφέρθηκαν οι πρακτικές ασφάλειας των συσκευών στα στάδια σχεδίασης και υλοποίησης, ανάπτυξής τους, κατά τον έλεγχο και αυθεντικοποίηση των συσκευών και κατά την ασφάλιση των δεδομένων και του δικτύου. Επίσης, παρουσιάστηκαν πρακτικές ευαισθητοποίησης και εκπαίδευσης των χρηστών, καθώς επίσης αναλύθηκαν οι δεκατρείς πρακτικές που προτείνει το Department for Culture, Media and Sport (DCMS) και κατηγοριοποιήθηκαν οι πρακτικές αυτές ανάλογα τον βαθμό δυσκολίας υλοποίησής τους, την αποτελεσματικότητά τους στην ασφάλεια των συσκευών και κατά πόσο εφαρμόζονται από οργανισμούς και εταιρείες. Τέλος, προτάθηκαν βέλτιστες πρακτικές και οδηγοί προς τους οργανισμούς για διασφάλιση της προστασίας των συσκευών και συστημάτων τους.

Κεφάλαιο 6ο: Προτάσεις για βελτίωση της ασφάλειας στις έξυπνες οικιακές συσκευές

6.1 Εισαγωγή

Σύμφωνα με την μελέτη των προηγούμενων κεφαλαίων, ιδίως των κεφαλαίων τέσσερα και πέντε στα οποία παρουσιάζεται ο τρόπος λειτουργίας έξυπνων συσκευών αλλά και καλές πρακτικές που βοηθούν στην βελτίωση της προστασίας των συσκευών από επιτιθέμενους, προτείνονται βασικές οδηγίες προς χρήστες και κατασκευαστές, καθώς ομαδοποιούνται ανάλογα την λειτουργία και την σκοπιμότητά τους, με σκοπό την καλυτέρευση της προστασίας των συσκευών αυτών.

6.2 Οδηγοί προς τον χρήστη για βελτίωση της ασφάλειας των έξυπνων συσκευών

Αρχικά σε επίπεδο χρήστη, ανάλογα το φύλο, την ηλικία, την εξοικείωση με έξυπνες συσκευές, τον χρόνο που διαθέτει ο χρήστης, την εκπαίδευσή του και την διαύγειά του εκείνη την στιγμή, έχει άλλο επίπεδο ικανοτήτων και μπορεί να χειριστεί σε διαφορετικό βαθμό μια έξυπνη συσκευή που διαθέτει. Επικεντρώνοντας τις οδηγίες σε ένα μέσο επίπεδο μόρφωσης του χρήστη και μέσο βαθμό εξοικείωσης με τις συσκευές, παρακάτω δίνονται κάποιες κατευθυντήριες γραμμές συμπεριφοράς, απάντησης ή δράσης των χρηστών ανάλογα την περίσταση ή και ανεξάρτητα από κάθε περίσταση, για καθολικές πρακτικές που χρειάζεται να ακολουθούνται από τους χρήστες με σκοπό την προστασία των δεδομένων και της ιδιωτικότητάς τους. Οι χρήστες είναι εκείνοι οι οποίοι πρέπει να υιοθετήσουν τακτικές και πρακτικές με σκοπό την διατήρηση της ασφάλειας των συσκευών τους, αλλά και την γρήγορη αντίληψη ασυνήθιστων ενεργειών ή ενεργειών που δεν πραγματοποίησαν οι ίδιοι και να γνωρίζουν πως να αντιδράσουν σε κάθε περιστατικό αλλά και που να απευθυνθούν σε περίπτωση που δεν γνωρίζουν τι πρέπει να κάνουν. Παρακάτω παρουσιάζονται ομαδοποιημένες οδηγίες και προτροπές προς τους χρήστες ανάλογα την λειτουργία και την σκοπιμότητα που έχουν. Πιο συγκεκριμένα, διακρίθηκαν τέσσερις κατηγορίες οι οποίες βοηθούν στην διασφάλιση της πρόσβασης στις έξυπνες συσκευές, την ασφάλιση του δικτύου και της σύνδεσης των συσκευών σε αυτό, το τείχος προστασίας και μεθόδους παρακολούθησης του δικτύου και των συσκευών και τέλος την επιμόρφωση των χρηστών σχετικά με αυτά τα σημαντικά ζητήματα ασφάλειας.

Στην πρώτη κατηγορία ανήκουν οι οδηγίες που στοχεύουν στο να κάνουν την εισβολή του επιτιθέμενου στην συσκευή πολύ πιο δύσκολη. Αρχικά, προτείνεται η χρήση ισχυρών κωδικών πρόσβασης που περιλαμβάνουν συνδυασμό από γράμματα, αριθμούς και μοναδικούς χαρακτήρες. Πιο συγκεκριμένα, ισχυρός καλείται ο κωδικός που περιέχει τουλάχιστον δώδεκα χαρακτήρες, συνδυάζει κεφαλαία με πεζά γράμματα, αριθμούς και σύμβολα. Ακόμα, συστήνεται η αποφυγή χρήσης του ίδιου κωδικού σε πολλές συσκευές και η χρήση κωδικού ο οποίος περιέχει λέξεις που βρίσκονται στο λεξικό ή αποτελούν κάποιο όνομα, επωνυμία ή προϊόν. Ο κωδικός πρέπει να είναι αρκετά εύκολος για τον χρήστη ώστε να τον θυμάται και αρκετά δύσκολος από τον επιτιθέμενο να τον βρει. Κάθε χρήστης ο οποίος διαθέτει πολλούς κωδικούς που πρέπει να θυμάται, μπορεί να χρησιμοποιεί ένα διαχειριστή κωδικών (password manager) για να αποθηκεύει και να διαχειρίζεται εκεί τους κωδικούς του με ασφάλεια. Επιπρόσθετα, συστήνεται η ενεργοποίηση ταυτοποίησης δύο ή περισσότερων παραγόντων σε όλες τις συσκευές του χρήστη. Στην ταυτοποίηση δύο παραγόντων (two-factor-authentication - 2FA) προστίθεται ένα επιπλέον επίπεδο αυθεντικοποίησης, απαιτώντας από τον χρήστη που συνδέεται να αποδείξει ποιος είναι και με έναν

δεύτερο τρόπο. Συνήθως αυτό γίνεται με κάποιο μήνυμα στο κινητό του χρήστη το οποίο έχει ισχύ για λίγα λεπτά και μετά λήγει και δεν μπορεί να χρησιμοποιηθεί. Ο χρήστης πρέπει να συμπληρώσει τον κωδικό αυτό που του στάλθηκε στην συσκευή στην οποία πραγματοποιεί την σύνδεση. Ακόμη ένα παράδειγμα 2FA είναι η χρήση βιομετρικών χαρακτηριστικών όπως δακτυλικό αποτύπωμα, αναγνωριστικό προσώπου ή ίριδας με σκοπό την επαλήθευση του χρήστη. Φυσικά, η τακτική ενημέρωσης λογισμικού των συσκευών και η αυτοματοποίηση των ενημερώσεων, σε όποια συσκευή δίνεται η δυνατότητα αυτή, είναι από τα πιο σημαντικά και απλά πράγματα που μπορεί να κάνει ο χρήστης για να βοηθήσει στην προστασία της συσκευής του.

Στην δεύτερη κατηγορία ανήκουν οι προτροπές που βοηθούν στην ασφάλιση του δικτύου και των συνδέσεων των συσκευών. Αρχικώς, επιδεικνύεται η αλλαγή των προεπιλεγμένων (default) ρυθμίσεων που υπάρχουν από την κατασκευή των συσκευών και η αλλαγή του κωδικού πρόσβασης στην συσκευής καθώς και η ασφάλιση του, οικιακού στην προκειμένη περίπτωση, δικτύου στο οποίο ανήκει η συσκευή. Η γνώση της συσκευής και των υπηρεσιών που διαθέτει είναι απαραίτητο για την ασφάλειά της, καθώς με την απενεργοποίηση αχρησιμοποίητων δυνατοτήτων, πορτών που δέχεται αιτήματα, ή και υπηρεσιών που δεν χρειάζονται εκείνη την στιγμή ή ποτέ, περιορίζονται οι ευπάθειες που μπορεί να εκμεταλλευτεί ένας επιτιθέμενος. Σχετικά με αυτό, η αποσύνδεση και των αχρησιμοποίητων συσκευών που βρίσκονται στο δίκτυο, βοηθάει στην μείωση πιθανοτήτων εισβολής. Η χρήση ισχυρού κωδικού πρόσβασης στο δίκτυο, η απόκρυψη του δικτύου αν είναι δυνατόν ή η απομόνωση των έξυπνων συσκευών από το οικιακό δίκτυο μέσω Virtual Local Area Networks (VLANs), αποτελούν χρήσιμες πρακτικές στην ασφάλιση του δικτύου. Συστήνεται η αλλαγή του ονόματος του δικτύου σε όνομα που δεν παραπέμπει σε πληροφορίες του δικτύου, του κατασκευαστή ή του τύπου συσκευής. Ακόμη, αν δίνεται η δυνατότητα χρήσης ασφαλών και εξελιγμένων προτύπων για ασύρματη σύνδεση των συσκευών όπως το WPA3 να ενεργοποιείται από τον χρήστη. Στα πλαίσια της ασφαλής σύνδεσης της συσκευής στο δίκτυο, ανήκει και η ασφαλής απομακρυσμένη διαχείριση της συσκευής η οποία μπορεί να πραγματοποιηθεί μέσω Virtual Private Network (VPN). Με VPN η επικοινωνία πραγματοποιείται χρησιμοποιώντας κρυπτογράφηση, εξασφαλίζοντας ότι τα δεδομένα από τον αποστολέα στον παραλήπτη δεν μπορούν να διαβαστούν ή να τροποποιηθούν από τρίτο, καθώς τα κλειδιά αυτής της κρυπτογράφησης τα γνωρίζουν μόνο η συσκευή του αποστολέα και ο VPN εξυπηρετητής. Με αυτόν τον τρόπο, εξασφαλίζεται η εμπιστευτικότητα και η ακεραιότητα των δεδομένων.

Στην κατηγορία ανήκουν οι οδηγίες που έχουν ως στόχο την παρακολούθηση και αξιολόγηση ενεργειών στο δίκτυο. Η παρακολούθηση των δραστηριοτήτων που πραγματοποιούνται στο δίκτυο είναι αναγκαία διότι μπορεί να ανιχνευτεί και να αποτραπεί ασυνήθιστη συμπεριφορά από συσκευές στο δίκτυο και να ειδοποιηθεί ο χρήστης. Αυτό μπορεί να γίνει με την χρήση εργαλείων παρακολούθησης δικτύου και firewall τα οποία ελέγχουν το εισερχόμενο και εξερχόμενο traffic για μη εξουσιοδοτημένη πρόσβαση σε υπηρεσίες και δεδομένα και ανάλογα μπλοκάρει ή όχι την εισαγωγή/εξαγωγή τους. Επίσης, για τον έλεγχο του δικτύου προτείνεται η χρήση συστήματος Intrusion Prevention System (IPS) το οποίο παρακολουθεί την εισβολή εισερχόμενου και εξερχόμενου traffic καθώς ελέγχει σε πραγματικό χρόνο την γνησιότητα των υπογραφών των μηνυμάτων που στέλνονται. Στο ίδιο πλαίσιο, η ασφάλιση του φυσικού χώρου στον οποίο ανήκουν οι συσκευές, θα βοηθήσει σημαντικά στην επιτήρηση και έλεγχο του δικτύου, καθώς δεν θα είναι προσβάσιμο σε μη εξουσιοδοτημένα μέλη. Για λόγους ευχρηστίας και ασφάλειας ενδείκνυται η δημιουργία ασφαλών λογαριασμών για όλα τα μέλη που χειρίζονται τις έξυπνες συσκευές με σκοπό να μπορούν να εντοπιστούν πιθανά σφάλματα σε περίπτωση παραβίασης κάποιου από αυτούς τους λογαριασμούς. Ακόμη, καλό είναι να αποφεύγεται η αποθήκευση σημαντικών και ευαίσθητων δεδομένων στις έξυπνες συσκευές, όπως και οι κωδικοί, γιατί σε περίπτωση παραβίασης μπορεί να χαθούν ή ακόμα και να υποκλαπούν αυτά τα κρίσιμα δεδομένα.

Στην τέταρτη και τελευταία κατηγορία οδηγιών ανήκει η ευαισθητοποίηση και εκπαίδευση των χρηστών. Πρόκειται για κάτι πολύ σημαντικό και σχετικά απλό (ειδικά με την βοήθεια των κατασκευαστών) που μπορούν να κάνουν οι χρήστες με σκοπό την ασφάλεια των οικιακών συσκευών τους. Η εκπαίδευση και συνεχής ενημέρωση σχετικά με τις τελευταίες εξελίξεις και ζητήματα που προκύπτουν καθώς και η επιμόρφωση των μελών που χρησιμοποιούν τις συσκευές σχετικά με τις βέλτιστες πρακτικές που απαιτείται να υιοθετήσουν συμβάλει ενεργά στην διατήρηση ασφαλών συστημάτων και αντίστοιχων συνηθειών. Σύμφωνα με αυτό συστήνεται ο έλεγχος δικαιωμάτων και δεδομένων που διαχειρίζονται οι συσκευές, με σκοπό τον περιορισμό δικαιωμάτων που δεν είναι απαραίτητα και οριοθέτηση της συλλογής δεδομένων από τις ρυθμίσεις απορρήτου. Τέλος, η επιμόρφωση ενισχύει και την καλύτερη αντιμετώπιση και δράση του χρήστη σε επιθέσεις ή υπόνοια επίθεσης ανάλογα και τα στοιχεία που υπάρχουν.

Σύμφωνα με τις παραπάνω προτάσεις οι χρήστες δύνανται να αξιοποιήσουν πλήρως τις δυνατότητες που έχουν σχετικά και με τις διαθέσιμες ενέργειες που μπορούν να πραγματοποιήσουν και να προστατεύσουν τις συσκευές τους.

6.3 Οδηγοί προς τους κατασκευαστές για βελτίωση της ασφάλειας των έξυπνων συσκευών

Η συνεισφορά των κατασκευαστών στην ασφάλιση των έξυπνων οικιακών συσκευών είναι εξίσου σημαντική με αυτή των χρηστών. Με την ενασχόλησή τους μπορούν να ενισχύσουν την ασφάλεια των έξυπνων οικιακών συσκευών τους και να προστατεύσουν καλύτερα τους χρήστες από πιθανούς κινδύνους, κακόβουλες επιθέσεις και παραβιάσεις δεδομένων. Όπως έχουν ήδη αναφερθεί, ευπάθειες και πιθανές επιθέσεις μπορούν να πραγματοποιηθούν σε κάθε στάδιο από την σχεδίαση μέχρι και την υλοποίηση και λειτουργία των συσκευών, επομένως κρίνεται σημαντικό να ενσωματώνονται εργαλεία, πρωτόκολλα και μέτρα ασφάλειας ανάλογα το εκάστοτε επίπεδο λειτουργίας ή στάδιο κατασκευής ώστε να προλαμβάνονται τυχόν αδυναμίες του συστήματος.

Σύμφωνα και με τα σχετικά άρθρα που έχουν ήδη αναλυθεί στο πέμπτο κεφάλαιο, το οποίο ασχολήθηκε με την έρευνα και επεξήγηση καλών και βέλτιστων πρακτικών που προτείνονται από φορείς και οργανισμούς, προστίθενται ακόμα και μερικές προτάσεις που αφορούν τους κατασκευαστές των συσκευών και στοχεύουν στην προστασία αυτών των συσκευών. Αυτές οι προτάσεις χωρίζονται ανάλογα την θεματολογία τους και την εφαρμογή τους. Οι θεματολογίες αυτές αφορούν την ενσωμάτωση ασφάλειας κατά την σχεδίαση της συσκευής με όλες τις σχετικές ενέργειες και τακτικές που αποσκοπούν σε καλύτερη συνεργασία και λειτουργία των συσκευών. Η δεύτερη κατηγορία αφορά στην αλληλεπίδραση των κατασκευαστών μεταξύ τους με στόχο την ισχυροποίηση των προτύπων και την ενοποίηση λειτουργιών ασφάλειας σε όλες τις συσκευές. Ενώ στην τρίτη και τελευταία κατηγορία ανήκει η εκπαίδευση και ευαισθητοποίηση των χρηστών μέσω παροχής σχετικού και περιεκτικού υλικού στους χρήστες.

Η πρώτη κατηγορία σχετίζεται τόσο με την σχεδίαση και υλοποίηση των έξυπνων συσκευών, όσο και με την υιοθέτηση ασφαλών πρακτικών και τακτικών με στόχο την ομαλή και ασφαλή επικοινωνία και συνύπαρξη συσκευών από διαφορετικούς κατασκευαστές. Απαιτείται ακόμα και η ασφάλιση του προϊόντος κατά την διαδικασία ανάπτυξης και μεταφοράς του λογισμικού με σκοπό την αποτροπή εισβολής κακόβουλου λογισμικού σε αυτό. Αυτά ενισχύονται με την εισαγωγή ισχυρών και μοναδικών προεπιλεγμένων κωδικών πρόσβασης στις έξυπνες συσκευές, την χρήση ασφαλών προεπιλεγμένων

ρυθμίσεων και την δημιουργία εξοπλισμού που μπορεί να πραγματοποιήσει σύνθετες και απαραίτητες διαδικασίες, όπως η κρυπτογράφηση, η αποθήκευση των κλειδιών κρυπτογράφησης και η ταυτοποίηση δύο παραγόντων. Ακόμα, κατά τον σχεδιασμό των συσκευών, απαιτείται η εφαρμογή τακτικών ελέγχων ασφαλείας σε κάθε στάδιο υλοποίησης με σκοπό την αξιολόγηση πιθανών ευπαθειών και κινδύνων σε κάθε στάδιο και την διόρθωσή τους. Επιπρόσθετα η παροχή επεξήγησης κάθε ενημέρωσης και η δημιουργία αυτόματων ενημερώσεων κάνει την διαδικασία μιας τόσο σημαντικής διαδικασίας πιο εύκολη στους χρήστες, άρα και υλοποιήσιμη και βοηθάει στην όσο πιο σύντομη διόρθωση ευπαθειών του συστήματος. Ωστόσο, και η διαχείριση και αποθήκευση των δεδομένων αποτελεί ακόμα ένα ζήτημα στην ασφάλεια. Προτείνεται η ενσωμάτωση κρυπτογράφησης σε μεταφορά και αποθήκευση και ο έλεγχος συλλογής δεδομένων των χρηστών με σκοπό την ελαχιστοποίηση των απαιτούμενων δεδομένων για λειτουργία των συσκευών ώστε να ενισχύεται η ιδιωτικότητα των χρηστών. Σχετικά με αυτό, συστήνεται η εφαρμογή ασφαλών μεθόδων αποθήκευσης και διαχείρισης των απαιτούμενων, για την χρήση των συσκευών, δεδομένων. Ακόμη, η ανάπτυξη εργαλείων και περαιτέρω προτύπων για την ασφαλή κατάργηση προσωπικών δεδομένων των χρηστών ανά πάσα στιγμή το θελήσουν, βοηθάει την εδραίωση εμπιστοσύνης των χρηστών στις συσκευές και στις υπηρεσίες που παρέχονται. Επίσης, οι τακτικοί έλεγχοι και αξιολογήσεις ασφάλειας από τρίτους αλλά και η συνεχής διόρθωση ευάλωτων σημείων των συσκευών και μετά την κυκλοφορία τους αποτελούν ίσως τις πιο χρήσιμες πρακτικές ασφάλειας. Τέλος, σε αυτή την κατηγορία μπορεί να προστεθεί και η εφαρμογή zero trust αρχιτεκτονικής κατά την σχεδίαση και υλοποίηση των συσκευών και υπηρεσιών που προσφέρουν. Η αρχιτεκτονική zero trust βασίζεται σε αρχές που σχετίζονται με την επαλήθευση όλων των χρηστών, την εφαρμογή συγκεκριμένων και περιορισμένων δικαιωμάτων χρήστη και τον περιορισμό του σε συγκεκριμένες ενέργειες. Με αυτόν τον τρόπο, προωθείται η αυθεντικοποίηση του χρήστη καθώς επίσης εξετάζονται πληροφορίες όπως ο τύπος συσκευής και η τοποθεσία σύνδεσης με σκοπό την ανίχνευση κάποιας ασυνήθιστης συμπεριφοράς και την διακοπή πρόσβασης. Ακόμη, εφαρμόζονται περιορισμένες δυνατές ενέργειες που μπορεί να πραγματοποιήσει ο εκάστοτε χρήστης, και έτσι περιορίζεται σε ένα τμήμα του δικτύου, άρα και πιθανές παραβάσεις θα επηρεάσουν μόνο αυτό το τμήμα του δικτύου. Τέλος, καταγράφονται οι ενέργειες που κάνει με σκοπό να διευκρινιστούν αιτίες πιθανής εισβολής κακόβουλου στο δίκτυο αλλά και να αποδοθούν ευθύνες όταν και σε όποιον χρειάζεται.

Στην δεύτερη κατηγορία προτάσεων στους κατασκευαστές των έξυπνων συσκευών για καλύτερη ασφάλεια ανήκει η υιοθέτηση κοινών πρακτικών και κανόνων κατά την διαδικασία σχεδίασης και υλοποίησης των συσκευών με σκοπό να αλληλεπιδρούν σωστά και να λειτουργούν με παρόμοιο τρόπο όμοιες συσκευές και να διευκολύνεται η χρήση τους από τους χρήστες. Η συμμόρφωση με τα πρότυπα ασφάλειας και η κοινή πολιτική των κατασκευαστών είναι απαραίτητη για την λειτουργία των συσκευών και κάνει πιο εύκολη την χρήση τους καθώς δεν θα διαφέρουν στον τρόπο υλοποίησης των ενεργειών τους. Ακόμα, εξίσου σημαντική είναι η δημιουργία προγραμμάτων ανταμοιβής σχετικά με την ανίχνευση ευπαθειών ή bug που υπάρχουν στο σύστημα και η αναφορά τους στον εκάστοτε οργανισμό. Η δημιουργία ανοιχτής επικοινωνίας για λήψη αναφορών από την κοινότητα της ασφάλειας είναι σαφέστατα καλύτερο από την ατομική προσπάθεια μόνο ορισμένων μελών που εργάζονται εσωτερικά του οργανισμού και μπορεί να παραλείψουν ή να μην εντοπίσουν τυχόν θέματα. Αυτή η ανάπτυξη κοινότητας ανοιχτού κώδικα επιτρέπει όχι μόνο εσωτερικά της επιχείρησης αλλά και σε εξωτερικούς ειδικούς, να γίνουν συνεργάτες και να αξιολογούν και βελτιώνουν την ασφάλεια των συστημάτων και συσκευών συνεχώς.

Στην τρίτη και τελευταία κατηγορία ανήκουν οι σχετικές ενέργειες και δράσεις που αφορούν στην οργάνωση και κοινοποίηση υλικού που να είναι εύκολο στην κατανόηση και αρκετά περιεκτικό με

σκοπό να ευαισθητοποιήσει και να ενημερώσει συγχρόνως τους χρήστες ανεξάρτητα από το μορφωτικό επίπεδο και το επίπεδο εξοικείωσης του χρήστη με έξυπνες συσκευές. Είναι αναγκαίο για την σωστή και λειτουργική χρήση των συσκευών, να παρέχονται οδηγίες και εκπαιδευτικό υλικό με την αγορά κάθε έξυπνης συσκευής με στόχο και την καλύτερη ρύθμιση και ασφάλεια των συσκευών αυτών. Ακόμη, και η στελέχωση και επιμόρφωση μιας ομάδας της επιχείρησης ως υποστήριξη πελατών ειδικά σε ζητήματα ασφάλειας της συσκευής, αποτελεί μια πολύ καλή ιδέα στην ενίσχυση της εμπιστοσύνης και του αισθήματος ασφάλειας που θα νιώθουν οι χρήστες που χρησιμοποιούν τις συσκευές. Τέλος, σχετικά με τις βοηθητικές ενέργειες με σκοπό την ασφάλεια των έξυπνων συσκευών από την μεριά των κατασκευαστών, δεν μπορεί να λείπει η έμπρακτη υποστήριξη σε παλαιότερες συσκευές, η σύσταση ενημερώσεων και αναβαθμίσεων και αν αυτό δεν είναι εφικτό πια, η παροχή προγραμμάτων αντικατάστασης αυτών των συσκευών. Αυτό θα γίνεται με τον σχεδιασμό απόσυρσης της συσκευής από την δημιουργία ή στην πορεία την ανάπτυξής της από τον κατασκευαστή, ώστε και ο χρήστης να γνωρίζει τις δυνατότητες που έχει η εκάστοτε συσκευή του καθόλη τη διάρκεια «ζωής» της.

Με αυτές τις προτροπές και οδηγίες οι κατασκευαστές μπορούν να ενισχύσουν την ασφάλεια των έξυπνων συσκευών που αναπτύσσουν και να προστατεύσουν καλύτερα τους χρήστες οι οποίοι θα εμπιστεύονται τις συσκευές αυτές.

6.4 Οδηγοί προς κατασκευαστές και χρήστες για καλύτερη ασφάλεια των έξυπνων συσκευών

Η βελτίωση της ασφάλειας στις έξυπνες οικιακές συσκευές, εξαρτάται από πολλούς παράγοντες και σίγουρα δεν είναι κάτι το οποίο πραγματοποιείται αποκλειστικά και μόνο με την δράση των χρηστών ή των κατασκευαστών. Ο συνδυασμός και η συνεργασία και των δύο σχετικά με την προσπάθεια που καταβάλλουν είναι καταλυτικής σημασίας. Αρχικά, πρέπει και οι δύο να είναι ενήμεροι σχετικά με το κατά πόσο είναι δυνατή η ενσωμάτωση συγκεκριμένων συσκευών στο έξυπνο οικιακό σύστημα, που μπορεί να προϋπάρχει. Δηλαδή αν οι συσκευές αυτές είναι συμβατές με τις σύγχρονες τεχνολογίες ασφάλειας τις οποίες υποστηρίζει το υπόλοιπο δίκτυο. Επίσης, η χορήγηση προγραμμάτων επιβράβευσης, από τους οργανισμούς, αναφορικά με ευπάθειες ή προβλήματα που αντιμετώπισαν οι χρήστες σίγουρα θα εντείνει την ενασχόληση και το ενδιαφέρον και των ίδιων των χρηστών και ειδικών ασφάλειας, να αντιμετωπίζουν και αξιολογούν ευάλωτα σημεία ασφάλειας της συσκευής. Σχετικά με αυτό, είναι πολύ θετικό να δίνεται η δυνατότητα προτάσεων για βελτιώσεις στον τρόπο λειτουργίας των συσκευών σύμφωνα και με την ευκολότερη κατανόηση πραγματοποίησης συγκεκριμένων διεργασιών που θέλουν να εκτελέσουν οι χρήστες. Έτσι, ενισχύεται η λειτουργικότητα των συσκευών. Ακόμη, σε περιστατικά υπόνοιας παραβίασης της συσκευής, να δίνεται η δυνατότητα στους χρήστες να χρησιμοποιήσουν απομακρυσμένη επαναφορά και απενεργοποίηση των συσκευών τους με σκοπό να τις προφυλάξουν ή να τις επαναφέρουν εάν χρειάζεται. Επιπρόσθετα, θα μπορούσαν να δίνονται και κάποια μέτρα ασφάλειας και οδηγίες από τους κατασκευαστές με την αγορά των συσκευών τα οποία να αφορούν στον τρόπο υλοποίησης απομόνωσης συγκεκριμένων συσκευών από το δίκτυο, ενσωμάτωση τείχους ασφαλείας ή εφαρμογών που βοηθούν στην ασφάλεια της συσκευής, εγκατάσταση εφαρμογών εντοπισμού συσκευής σε περίπτωση απώλειάς της, καθώς επίσης και μεθόδους αλλαγής συγκεκριμένων απαιτούμενων ρυθμίσεων. Τέλος, από την πλευρά των κατασκευαστών είναι ωφέλιμο να υποστηρίζονται και να οργανώνονται ομάδες και οργανισμοί που προάγουν την ανάπτυξη και τήρηση διεθνών προτύπων ασφάλειας και από την πλευρά τους οι χρήστες να προτιμούν συσκευές οι οποίες σχεδιάζονται σύμφωνα με αυτά τα πρότυπα.

Όπως έχει ήδη γίνει αντιληπτό, η συνεισφορά χρηστών και κατασκευαστών ολοκληρώνει την επίβλεψη και τα μέτρα που μπορούν να πραγματοποιηθούν σχετικά με την προστασία των έξυπνων οικιακών συσκευών, αν και σίγουρα υπάρχουν και άλλα μέτρα τα οποία δεν αναφέρθηκαν στα πλαίσια της έρευνας αυτής.

6.5 Επίλογος

Στο έκτο κεφάλαιο αναφέρθηκαν και αναλύθηκαν οδηγίες και προτάσεις για βελτίωση της ασφάλειας των συσκευών. Σύμφωνα με την έρευνα που έγινε στο πλαίσιο συγγραφής της εργασίας, διευρύνθηκαν οι γνώσεις επί του θέματος και προτάθηκαν συγκεκριμένοι και ομαδοποιημένοι οδηγοί ασφάλειας έξυπνων οικιακών συσκευών προς χρήστες και κατασκευαστές καθώς επίσης διασαφηνίστηκαν και συνδυαστικά μέτρα, για χρήστες και κατασκευαστές, τα οποία εξυπηρετούν τον ίδιο σκοπό · την περαιτέρω υποστήριξη της ασφάλειας στις έξυπνες αυτές συσκευές.

Κεφάλαιο 7ο: Έρευνα για την ευαισθητοποίηση των χρηστών σχετικά με την ασφάλεια των συσκευών τους

7.1 Εισαγωγή

Στο έβδομο κεφάλαιο παρουσιάζονται τα αποτελέσματα έρευνας, η οποία διεξήχθη με σκοπό την ευαισθητοποίηση των χρηστών σχετικά με την ασφάλεια των έξυπνων οικιακών συσκευών τους. Αρχικά, η έρευνα πραγματοποιήθηκε σε ένα μικρό τυχαίο δείγμα πενήντα περίπου ατόμων και σε αυτό έγιναν κάποιες ερωτήσεις σχετικά με το είδος έξυπνων συσκευών που έχουν, την εξοικείωσή τους με αυτές, αν και κατά πόσο χρησιμοποιούν ασφαλείς τρόπους προστασίας της εισόδου στη συσκευή, αν πραγματοποιούν τακτικές ενημερώσεις λογισμικού, αν έχουν διαβάσει τα δεδομένα που συλλέγει η κάθε συσκευή και άλλες παρόμοιες ερωτήσεις. Στην συνέχεια, μέσω ενός βίντεο παρουσιάστηκε ένας εύκολος τρόπος δημιουργίας ισχυρών κωδικών και μέσω ενός δεύτερου βίντεο παρουσιάστηκαν αληθινά περιστατικά εισβολής κακόβουλου σε έξυπνη οικιακή συσκευή, καθώς επίσης διασαφηνίστηκαν μερικά μέτρα για την προστασία των συσκευών. Αργότερα ξανά ζητήθηκαν οι ίδιες ερωτήσεις οι οποίες δόθηκαν αρχικά με σκοπό την αξιολόγηση της ευαισθητοποίησης και της ετοιμότητας η οποία προήλθε από τις σχετικές αφηγήσεις στα βίντεο. Παρακάτω παρουσιάζονται αρχικώς οι ερωτήσεις που έγιναν και τον σκοπό που αυτές είχαν. Στην συνέχεια, διακρίνονται τα βίντεο που χρησιμοποιήθηκαν και η σκοπιμότητά τους. Τέλος, αναλύονται τα αποτελέσματα της έρευνας καθώς εμφανίζονται και σε σχετικά διαγράμματα για καλύτερη κατανόησή τους. Το σχετικό form βρίσκεται στον σύνδεσμο https://forms.gle/2WGyQN4bpvLYBJXt9.

7.2 Ερωτήσεις και σκοπιμότητά τους

Στο ερωτηματολόγιο παρατέθηκαν ερωτήσεις μέσα από τις οποίες θα έβγαιναν χρήσιμα συμπεράσματα σχετικά με την προστασία των έξυπνων οικιακών από τους χρήστες, τις γνώσεις που αυτοί διαθέτουν, την διάθεσή τους για εκπαίδευση και διερεύνηση άγνωστων γνωστικών περιοχών και τον βαθμό ευαισθητοποίησης πριν και μετά τις ερωτήσεις και τα σχετικά βίντεο. Οι ερωτήσεις σχεδιάστηκαν με σκοπό την σύντομη απάντησή τους και την όσο το δυνατόν προσήλωση των ερωτηθέντων καθόλη την διάρκεια της συμπλήρωσης των απαντήσεων, επομένως είναι λίγες σε αριθμό, σύντομες και περιεκτικές. Πολλές από τις δυνατές απαντήσεις για λόγους ευκολίας και ταχύτητας συμπλήρωσης έγιναν με αρίθμηση από το 1 έως το 5 με σχετική διασαφήνιση τι σημαίνει καθένα από αυτά. Επίσης, οι ερωτήσεις χωρίστηκαν σε δύο σετ ερωτήσεων οι οποίες και αυτές νοητά χωρίστηκαν σε ομάδες ανάλογα τις πληροφορίες που συλλέγονται από τις απαντήσεις τους. Το πρώτο σετ ασχολήθηκε από την μέχρι τώρα γνώση και ασχολία των χρηστών σε θέματα ασφάλειας των συσκευών τους, ενώ στο δεύτερο σετ μετά και την παρουσίαση των βίντεο, ζητήθηκαν ξανά κάποιες καίριες ερωτήσεις με σκοπό την διεξαγωγή συμπερασμάτων από την σύντομη παρουσίαση βασικών πληροφοριών ασφάλειας στους χρήστες.

Η πρώτη ομάδα ασχολήθηκε με πληροφορίες σχετικές με τον χρήστη όπως το φύλο, η ηλικιακή ομάδα που ανήκει, η εξοικείωση του ατόμου με τις έξυπνες συσκευές του και τα είδη των έξυπνων συσκευών που διαθέτει. Στην ερώτηση για τις έξυπνες οικιακές συσκευές που διαθέτει ο χρήστης, υπήρχε και πεδίο συμπλήρωσης σε περίπτωση που ο χρήστης είχε συσκευή που δεν αναφέρθηκε στις δυνατές απαντήσεις.

Η δεύτερη ομάδα αναφέρθηκε στην ασφάλιση της εισόδου στην συσκευή και πιο συγκεκριμένα ζητήθηκε να αξιολογηθεί από τους χρήστες η ανθεκτικότητα των κωδικών που πληκτρολογούν κατά την είσοδό τους στις συσκευές τους και στην συνέχεια παρουσιάστηκε σχετικό βίντεο. Ακόμη, σε αυτή την κατηγορία ανήκει και η επιπλέον αυθεντικοποίηση του χρήστη, η οποία μπορεί να πραγματοποιηθεί με χρήση βιομετρικών χαρακτηριστικών, και έτσι ερωτήθηκε κατά πόσο χρησιμοποιούν αυτή τη μέθοδο οι χρήστες στις συσκευές τους.

Η τρίτη ομάδα ερωτήσεων αφορούσε την ανησυχία που έχουν ήδη οι χρήστες σχετικά με την ασφάλεια των οικιακών συσκευών τους και κατά πόσο ενημερώνονται για τις άδειες και δεδομένα που χρησιμοποιεί κάθε συσκευή. Για την ακρίβεια, ερωτήθηκε η συχνότητα ενημέρωσης του λογισμικού των συσκευών τους, εάν έχει γίνει έλεγχος των αδειών και δεδομένων που συλλέγονται και χρησιμοποιούνται από τις συσκευές αυτές και εάν γνωρίζουν την πολιτική απορρήτου των συσκευών.

Στην τέταρτη κατηγορία ερωτήσεων ανήκουν εκείνες οι οποίες δείχνουν την μέχρι τώρα ευαισθητοποίηση των χρηστών σχετικά με την ασφάλεια των συσκευών τους και τις δράσεις που κάνουν σχετικά με αυτό. Επομένως, ζητήθηκε από τους χρήστες εάν έχουν κάνει αλλαγές στις προεπιλεγμένες ρυθμίσεις ασφαλείας των συσκευών τους και πόσο ανησυχούν με την ασφάλεια που διαθέτουν οι έξυπνες αυτές συσκευές τους. Στην συνέχεια, παρουσιάστηκε σχετικό βίντεο, το οποίο θα συζητηθεί αργότερα.

Και τέλος, στο δεύτερο σετ ερωτήσεων ερωτήθηκε ξανά εάν οι χρήστες έχουν σκοπό να δημιουργούν ισχυρούς κωδικούς στις συσκευές τους (εάν δεν το έκαναν μέχρι στιγμής) και εάν θα χρησιμοποιήσουν αυθεντικοποίηση σε αυτές με κάποια ακόμη μέθοδο όπως με την χρήση βιομετρικών χαρακτηριστικών. Ερωτήθηκε κατά πόσο θεωρούν σημαντικές τις συχνές ενημερώσεις της συσκευής τους και την αλλαγή των προεπιλεγμένων ρυθμίσεων ασφάλειας αυτής. Και τέλος, ζητήθηκε εάν πιστεύουν ότι θα έπρεπε να γνωρίζουν τις σχετικές άδειες και δεδομένα που συλλέγει η συσκευή τους.

7.3 Παρουσίαση βίντεο και σκοπιμότητά τους

Με σκοπό την ευαισθητοποίηση και επαγρύπνηση των χρηστών, θεωρήθηκε καλύτερο να παρουσιαστούν βίντεο τα οποία σχετίζονται με τις ερωτήσεις που γίνονται και πραγματεύονται τις σωστές πρακτικές που πρέπει να ακολουθήσει ο χρήστης στην προστασία των συσκευών του, με διαδραστικό και ευχάριστο τρόπο. Τα βίντεο που παρουσιάζονται πέρασαν από κάποια βασικά κριτήρια όπως να μην διαφημίζουν κάποιο προϊόν ή εταιρεία για πολύ χρόνο, να είναι σύντομα σε διάρκεια και περιεκτικά ώστε να τα παρατηρήσει ο χρήστης και να πάρει κάποιες απαιτούμενες πληροφορίες και τέλος, να περιέχουν ωραία αισθητικά γραφικά ή καλή ποιότητα εικόνας ώστε να είναι ευχάριστη η παρακολούθηση από τον χρήστη. Παρουσιάστηκαν δύο βίντεο, ενώ αρχικά είχαν βρεθεί πολλά περισσότερα, γιατί δεν πληρούσαν τα παραπάνω απαιτούμενα κριτήρια. Η ενσωμάτωση των βίντεο στο form και όχι η εισαγωγή ενός συνδέσμου που να παραπέμπει σε αυτά, έγινε με σκοπό την παραμονή του χρήστη στο form και την ολοκλήρωση απάντησης του ερωτηματολογίου. Τέλος, σχετικά με την θεματολογία των βίντεο, το πρώτο περιέχει καλές πρακτικές δημιουργίας ενός ισχυρού κωδικού οι οποίες παρουσιάζονται με απλό τρόπο και δίνονται παραδείγματα, κάτι που το κάνει ιδανικό για κατανόηση ακόμα και σε άτομα που δεν έχουν καθόλου γνώσεις επί του θέματος. Και το δεύτερο βίντεο αρχικά παρουσιάζει κάποιες έξυπνες οικιακές συσκευές και στην συνέχεια δείχνει τρεις περιπτώσεις στις οποίες μπορεί να επιφέρουν σημαντικές απώλειες αυτές οι συσκευές αν δεν προστατευτούν. Περιγράφει αληθινά περιστατικά τα οποία συνέβησαν σε μη φυλαγμένες έξυπνες οικιακές συσκευές

και με αυτόν τον τρόπο κρίνεται ότι κινητοποιεί και τους πιο επιφυλακτικούς σχετικά με την εφαρμογή μέτρων ασφάλειας. Στην συνέχεια, παρουσιάζει τους λόγους που δεν είναι αρκετά προστατευμένες οι IoT συσκευές στις μέρες μας, καθώς επίσης παραθέτει στατιστικά σχετικά για να επιδείξει την κρισιμότητα και την άγνοια των περισσότερων χρηστών σχετικά με την ασφάλεια των συσκευών τους. Τέλος, παρουσιάζει πέντε βήματα με σκοπό την βελτίωση προστασίας αυτών των συσκευών.

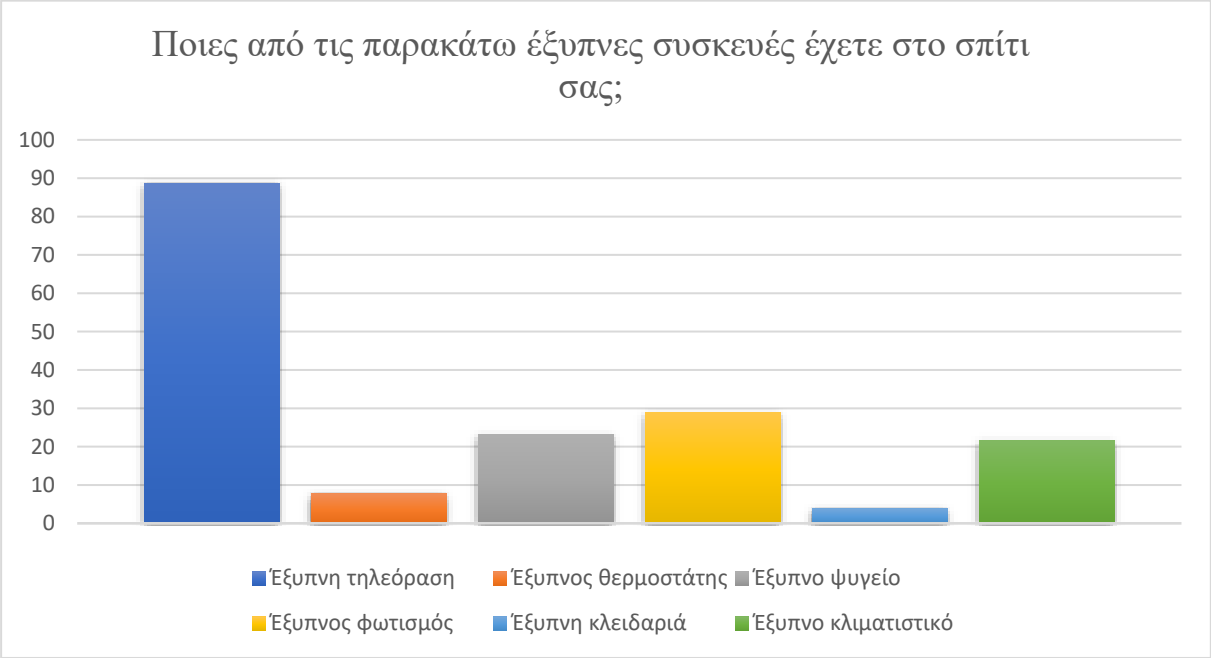
7.4 Αποτελέσματα έρευνας

Τα αποτελέσματα της έρευνας αρχικά παρουσιάζονται με στατιστικά και στην συνέχεια κάποια από αυτά διακρίνονται και σε διαγράμματα. Ξεκινώντας με το πρώτο σετ ερωτήσεων και από την πρώτη ομάδα, δηλαδή τις αναγνωριστικές ερωτήσεις προς τον χρήστη, από τις 52 απαντήσεις που δόθηκαν το 55,8% ήταν γυναίκες και το 44,2% ήταν άντρες.

Σχετικά με την ηλικιακή ομάδα που ανήκουν, το 36,5% είναι ηλικίας μικρότερης ή ίσης των είκοσι πέντε ετών. Αμέσως μετά, στην ηλικιακή ομάδα είκοσι έξι – τριάντα πέντε ετών άνηκε το ποσοστό των 26,9%, ενώ στην αμέσως επόμενη ομάδα, τριάντα πέντε – πενήντα πέντε ετών, άνηκε το 25%. Και τέλος, το 11,5% των ερωτηθέντων ήταν ηλικίας μεγαλύτερης από πενήντα πέντε ετών.

Αναφορικά με το επίπεδο εξοικείωσης των χρηστών με έξυπνες οικιακές συσκευές και σύμφωνα με την διαβάθμιση από ένα έως πέντε, για ευκολία συμπλήρωσης του ερωτηματολογίου, το 7,7% δεν είναι καθόλου εξοικειωμένοι με αυτές, το 19,2% έχουν την αμέσως επόμενη βαθμίδα εξοικείωσης. Το 28,8% έχει μία μέση εξοικείωση, το 32,7% έχει ακόμα καλύτερη εξοικείωση, ενώ το υπόλοιπο 11,5% έχει την μέγιστη εξοικείωση με τις οικιακές συσκευές τους.

Η τελευταία αναγνωριστική ερώτηση σχετικά με τους χρήστες είναι να απαντηθούν τα είδη έξυπνων συσκευών, γιατί μπορεί να έχουν περισσότερες από μία, στο οικιακό τους περιβάλλον. Διευκρινίζεται ότι πριν την συμπλήρωση του ερωτηματολογίου απαραίτητη προϋπόθεση των χρηστών ήταν να διαθέτουν έστω μία έξυπνη συσκευή στο σπίτι τους για να έχουν νόημα και οι απαντήσεις τους και να βγουν σχετικά συμπεράσματα για την ευαισθητοποίησή τους σχετικά με αυτές. Ξεκινώντας λοιπόν από την μεγαλύτερη σε ποσοστό απάντηση έως την μικρότερη, με 88,5% εμφανίζεται η έξυπνη τηλεόραση, αμέσως μετά με ποσοστό 28,8% βρίσκεται ο έξυπνος φωτισμός. Στην συνέχεια, το 23,1% διαθέτει έξυπνο ψυγείο ενώ το 11,5% διαθέτει έξυπνο κλιματιστικό. Τέλος, σε ποσοστό 7,7% βρίσκεται ο έξυπνος θερμοστάτης ενώ με 3,8% η έξυπνη κλειδαριά. Στον έξυπνο φωτισμό διευκρινίστηκε κατά την συμπλήρωση του ερωτηματολογίου, ότι δεν ανήκει αποκλειστικά κάθε σύστημα που περιλαμβάνει ολόκληρο το σπίτι, αλλά μπορεί και ένα μέρος αυτού να καλύπτεται από το σύστημα. Ομοίως, για λόγους ευκολίας στην παρουσίαση των αποτελεσμάτων κάθε έξυπνος μηχανισμός ή συσκευή που χρησιμοποιείται στο χώρο του ψυγείου, ενσωματώθηκε στην απάντηση έξυπνο ψυγείο. Και τέλος, όπως φαίνεται στις διαθέσιμες προς συμπλήρωση απαντήσεις, οι ερωτηθέντες πρόσθεσαν το έξυπνο κλιματιστικό. Παρακάτω φαίνεται και το σχετικό γράφημα που αντιπροσωπεύει τα ποσοστά των απαντήσεων αυτής της ερώτησης.

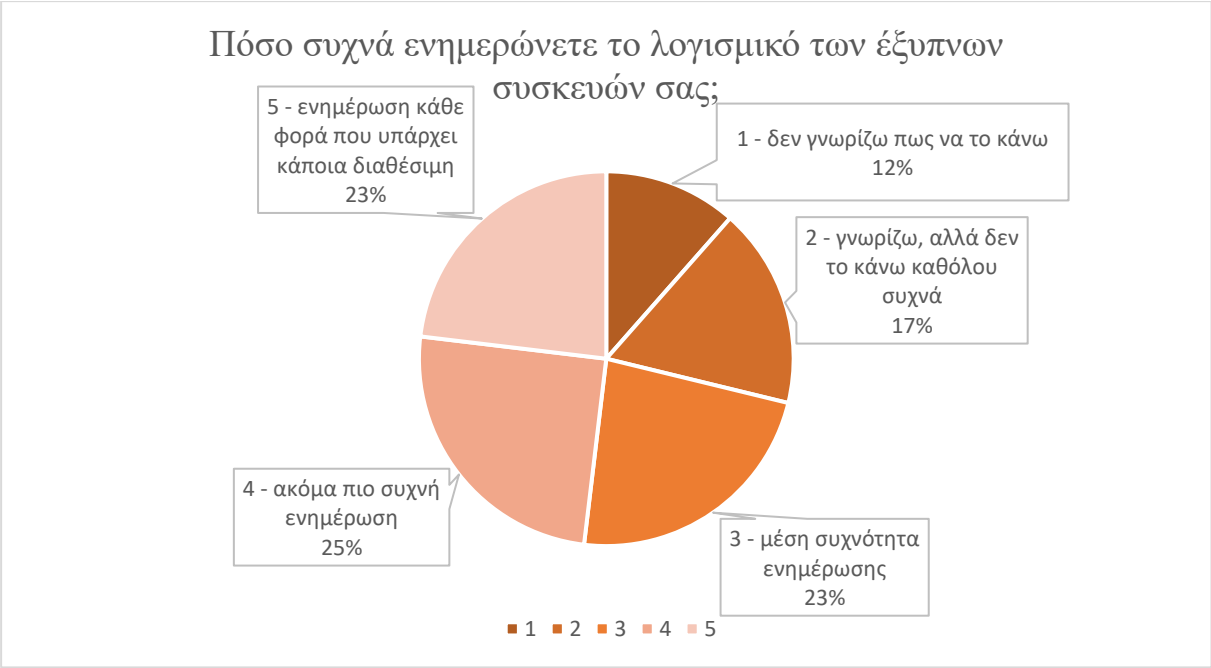


Εικόνα 5. Ποικιλομορφία έξυπνων οικιακών συσκευών

Σχετικά με την δεύτερη ομάδα ερωτήσεων, στις οποίες άνηκαν εκείνες που αφορούσαν την ασφάλιση των συσκευών κατά την είσοδό τους σε αυτές και πιο συγκεκριμένα στην ερώτηση αν χρησιμοποιούν ισχυρούς κωδικούς πρόσβασης στις έξυπνες συσκευές τους, σύμφωνα πάντα με την δική τους κρίση και με διαβάθμιση από το ένα – δεν χρησιμοποιούν ποτέ ισχυρούς κωδικούς έως το πέντε – χρησιμοποιούν πάντα. Το 9,6% απάντησε ότι δεν χρησιμοποιεί ποτέ ισχυρούς κωδικούς, στην αμέσως επόμενη κλίμακα ανήκει το 21,2%, ενώ στην επόμενη η οποία αφορά σε μία μέση χρήση ισχυρών κωδικών ανήκει το ποσοστό των 25%. Τέλος, ακόμα πιο συχνή χρήση ισχυρών κωδικών κάνει το 26,9%, ενώ το 17,3% χρησιμοποιεί πάντοτε ισχυρούς κωδικούς πρόσβασης στις συσκευές τους.

Στην επόμενη ερώτηση, η οποία αφορούσε αν οι χρήστες έχουν χρησιμοποιήσει βιομετρικά χαρακτηριστικά για αυθεντικοποίηση έστω σε μία συσκευή τους. Και πάλι σε κλίμακα από το ένα – δεν γνωρίζουν τι είναι, έως το πέντε – χρησιμοποιούν σε όλες τις συσκευές τους. Το ποσοστό των 15,4% απάντησε ότι δεν γνωρίζει τι είναι η αυθεντικοποίηση με χρήση βιομετρικών χαρακτηριστικών, το 25% ανήκει στην αμέσως επόμενη διαβάθμιση σχετικά με την χρήση αυτής της μεθόδου αυθεντικοποίησης, ενώ το 30,8% απάντησε ότι κάνει μια μέση χρήση αυτής της μεθόδου στις έξυπνες οικιακές συσκευές τους. Τέλος, το 19,2% απάντησε ότι την χρησιμοποιεί ακόμα πιο τακτικά ενώ το 9,6% χρησιμοποιεί αυτή τη μέθοδο σε όλες τις έξυπνες οικιακές συσκευές που διαθέτουν.

Στην ερώτηση η οποία αναφερόταν στην συχνότητα ενημέρωσης του λογισμικού των έξυπνων αυτών συσκευών, και πάλι σε διαβάθμιση από το ένα – δεν γνωρίζουν πως να το κάνουν έως το πέντε – πραγματοποιούν κάθε ενημέρωση μόλις είναι διαθέσιμη. Το ποσοστό 11,5% απάντησε ότι δεν γνωρίζει πως να κάνει ενημέρωση λογισμικού στις συσκευές τους ενώ στην αμέσως επόμενη διαβάθμιση ανήκει το 17,3%. Με μία μέση συχνότητα πραγματοποιεί ενημερώσεις λογισμικού το 23,1% ενώ το 25% ακόμα πιο συχνά. Τέλος, το 23,1% πραγματοποιεί τις ενημερώσεις μόλις αυτές είναι διαθέσιμες. Τα αποτελέσματα αυτά παρουσιάζονται και παρακάτω στο γράφημα.



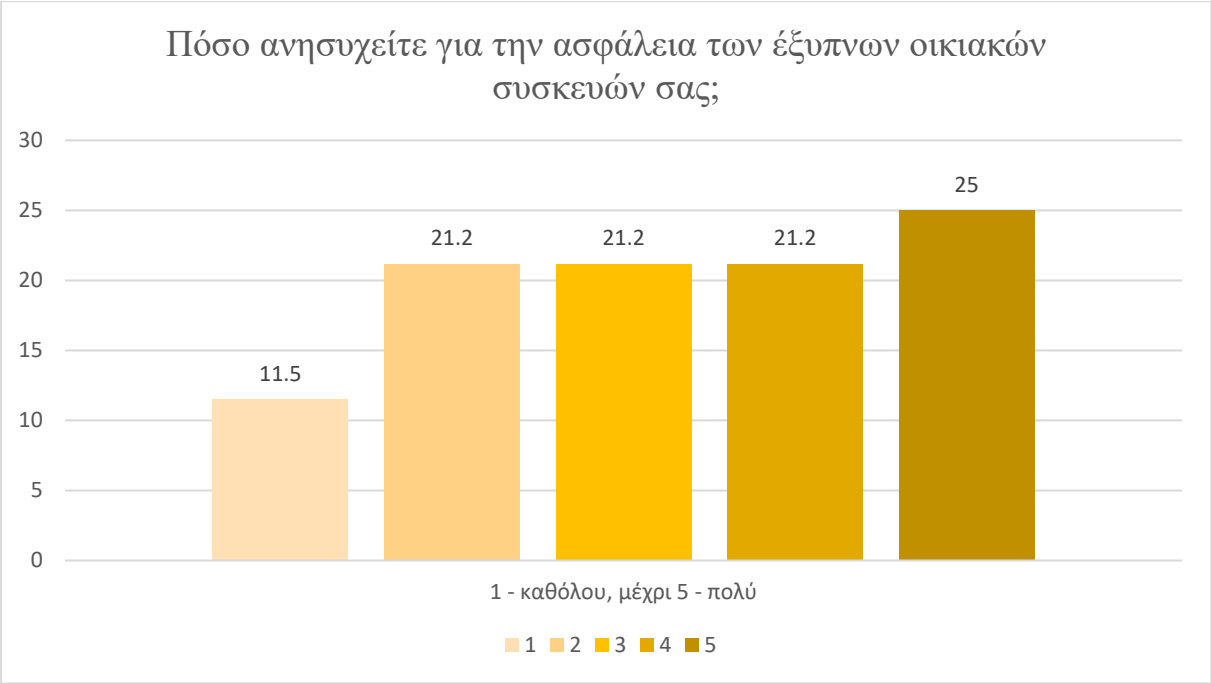
Εικόνα 6. Συχνότητα ενημέρωσης λογισμικού των έξυπνων συσκευών

Στην επόμενη ερώτηση που αναφέρεται στον έλεγχο των χρηστών σχετικά με τις άδειες και τα δεδομένα που συλλέγουν οι έξυπνες συσκευές τους, σε διαβάθμιση από το ένα – δεν ελέγχουν ποτέ, έως το πέντε – ελέγχουν σε όλες τις συσκευές τους. Το 34,6% απάντησε ότι δεν έχει ελέγξει ποτέ τις άδειες και τα δεδομένα που διαχειρίζεται η συσκευή τους, ενώ πιο συχνά ελέγχει το 15,4%. Σε μία μέση συχνότητα ελέγχου βρίσκεται το 30,8% ενώ το 13,5% ελέγχει ακόμα πιο τακτικά. Τέλος, το 5,8% απάντησε ότι ελέγχει πάντα τις άδειες και τα δεδομένα που χρειάζονται για την λειτουργία όποιας έξυπνης συσκευής διαθέτει.

Αναφορικά με την πολιτική απορρήτου των συσκευών, στην ερώτηση αν την έχουν διαβάσει, το 63,5% απάντησε ότι δεν την έχει διαβάσει ποτέ και σε καμία έξυπνη οικιακή συσκευή που διαθέτουν. Αμέσως μετά το 30,8% έχει διαβάσει την πολιτική απορρήτου σε κάποιες από τις συσκευές τους αλλά όχι προσεκτικά, ενώ το ποσοστό των 5,8% την διαβάζει προσεκτικά και σε όλες τις συσκευές που διαθέτουν.

Στην ερώτηση αν οι χρήστες έχουν αλλάξει ποτέ τις προεπιλεγμένες ρυθμίσεις ασφαλείας στις συσκευές τους, το 7,7% απάντησε ότι δεν γνωρίζει πως να το κάνει, το ποσοστό των 65,4% απάντησε ότι δεν τις έχει αλλάξει ποτέ, ενώ το 15,4% απάντησε ότι τις άλλαξε αλλά αργότερα, μετά την εγκατάσταση της συσκευής. Τέλος, το 11,5% των ερωτηθέντων απάντησε ότι άλλαξε τις ρυθμίσεις ασφάλειας αμέσως μόλις εγκαταστάθηκαν οι συσκευές.

Στην τελευταία ερώτηση του πρώτου σετ ερωτήσεων ανήκει το ποσοστό ανησυχίας των χρηστών σχετικά με την ασφάλεια των οικιακών έξυπνων συσκευών τους. Σε αυτήν την ερώτηση υπήρχε επίσης διαβάθμιση από το ένα – δεν ανησυχούν καθόλου, έως το πέντε – ανησυχούν πολύ. Το ποσοστό των 11,5% δεν ανησυχεί καθόλου για την ασφάλεια των συσκευών τους ενώ αμέσως μετά το ποσοστό των 21,2% ανησυχεί λίγο περισσότερο. Σε μία μέση ανησυχία βρίσκονται το 21,2% των ερωτηθέντων, ενώ το 21,2% ανησυχεί ακόμα περισσότερο. Τέλος, το υπόλοιπο 25% ανησυχεί πολύ για την ασφάλεια των συσκευών που διαθέτουν. Παρακάτω, διαφαίνεται το ποσοστό ανησυχίας των χρηστών και σε γράφημα.



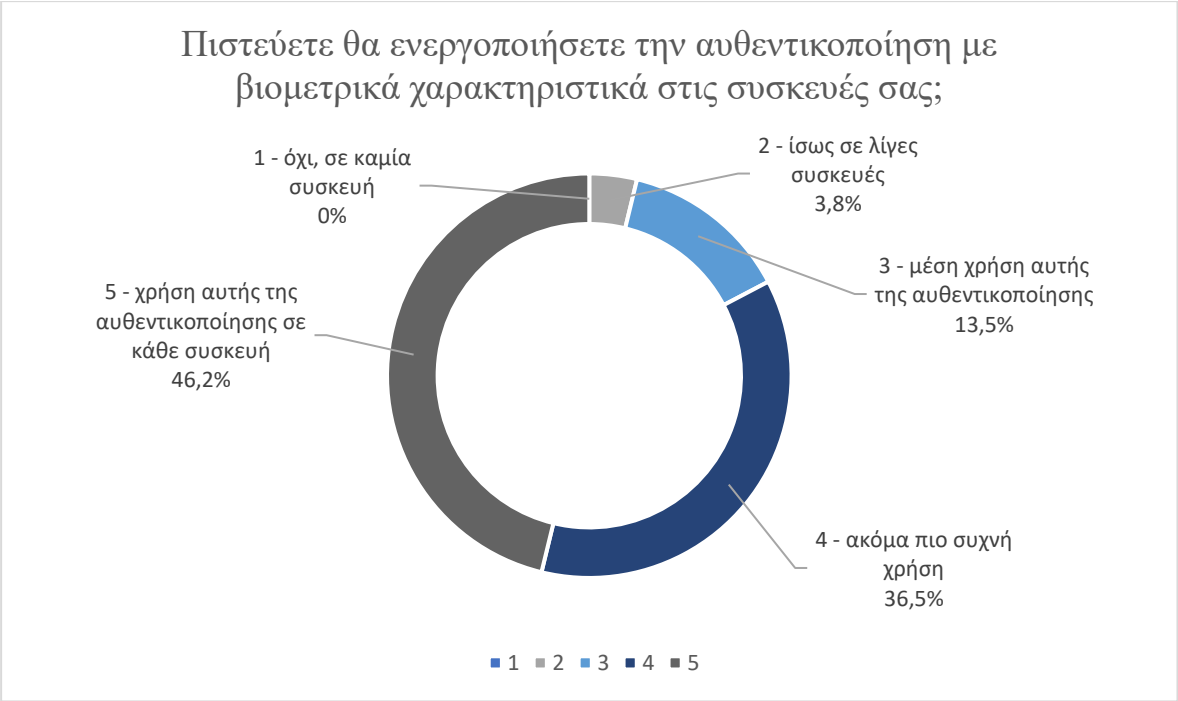
Εικόνα 7. Ανησυχία για την ασφάλεια των έξυπνων οικιακών συσκευών

Στην συνέχεια, μετά και την προβολή των σχετικών βίντεο που ήδη αναφέρθηκε το περιεχόμενό τους, ζητήθηκε από τους ερωτηθέντες να απαντήσουν σε τέσσερις ακόμα περιεκτικές ερωτήσεις με σκοπό να αντληθεί η βοήθεια που εξέλαβαν από το υλικό που τους δόθηκε. Στην πρώτη ερώτηση ανήκει η χρήση ισχυρών κωδικών από εδώ και πέρα. Και πάλι με διαβάθμιση από το ένα – δεν θα χρησιμοποιούσαν σε καμία συσκευή, έως το πέντε – θα χρησιμοποιούν σε όλες τις έξυπνες οικιακές συσκευές τους. Το 9,6% απάντησε ότι θα χρησιμοποιεί σε έναν μέσο βαθμό ισχυρούς κωδικούς στις συσκευές τους, το 40,4% απάντησε ότι θα χρησιμοποιεί ακόμα πιο συχνά ισχυρούς κωδικούς, ενώ το υπόλοιπο 50% απάντησε ότι θα χρησιμοποιεί πάντοτε ισχυρούς κωδικούς.

Στην επόμενη ερώτηση η οποία φορά την ενεργοποίηση αυθεντικοποίησης με την χρήση βιομετρικών χαρακτηριστικών, και σε κλίμακα από το ένα – δεν θα το χρησιμοποιούσαν σε καμία συσκευή τους, έως το πέντε – θα το χρησιμοποιούν σε κάθε συσκευή τους. Με ποσοστό 0% εμφανίστηκε η απάντηση ότι δεν θα χρησιμοποιούσαν αυτή την μέθοδο σε καμία συσκευή τους. Το 3,8% απάντησε ότι θα το χρησιμοποιεί σε κάποιες συσκευές, στην αμέσως επόμενη βαθμίδα με μία μέση χρήση ανήκει το 13,4%. Ενώ το 36,5% θα χρησιμοποιούν ακόμα πιο συχνά αυτή τη μέθοδο αυθεντικοποίησης και το 46,2% θα το χρησιμοποιεί σε όλες τις συσκευές του. Παρακάτω, παρουσιάζεται σχετικό γράφημα για καλύτερη κατανόηση των αποτελεσμάτων.

Στην ερώτηση σχετικά με την σημασία των ενημερώσεων του λογισμικού των συσκευών και την αλλαγή των προεπιλεγμένων ρυθμίσεων, το 5,8% απάντησε ότι κρίνει σημαντική μόνο την τακτική ενημέρωση λογισμικού των συσκευών τους ενώ το υπόλοιπο 94,2% απάντησε ότι είναι σημαντικά και τα δύο. Οι διαθέσιμες απαντήσεις οι οποίες δεν συγκέντρωσαν ποσοστό ήταν ότι δεν θεωρείται σημαντικό τίποτα από τα δύο (ενημερώσεις και αλλαγή προεπιλεγμένων ρυθμίσεων) και ότι θεωρείται σημαντική μόνο η αλλαγή των προεπιλεγμένων ρυθμίσεων.

Η τελευταία ερώτηση πραγματευόταν την σημασία γνώσης των αδειών και δεδομένων που συλλέγει και διαχειρίζεται κάθε έξυπνη συσκευή, με το ποσοστό των 3,8% να απαντά ότι δεν πιστεύει ότι θα έπρεπε να τα γνωρίζει, ενώ το υπόλοιπο 96,2% απάντησε ότι θα έπρεπε να τα γνωρίζει.



Εικόνα 8. Χρήση αυθεντικοποίησης με βιομετρικά χαρακτηριστικά

7.5 Επίλογος

Στο έβδομο κεφάλαιο αναλύθηκαν τα αποτελέσματα έρευνας που πραγματοποιήθηκε με σκοπό την ευαισθητοποίηση και επαγρύπνηση των χρηστών σχετικά με την ασφάλεια των έξυπνων οικιακών συσκευών τους. Αρχικά, παρουσιάστηκαν οι ερωτήσεις που έγιναν στο ερωτηματολόγιο που δημιουργήθηκε για τον σκοπό αυτό. Οι ερωτήσεις αυτές ομαδοποιήθηκαν ανάλογα την σκοπιμότητά τους, καθώς επίσης στο ερωτηματολόγιο παρουσιάστηκαν και σχετικά βίντεο για καλύτερη κατανόηση και διάδραση με τον χρήστη. Στην συνέχεια δόθηκαν ξανά ερωτήσεις, με σκοπό να γίνει αντιληπτό κατά πόσο βοήθησε το ερωτηματολόγιο στην ευαισθητοποίηση των χρηστών. Και τέλος, διασαφηνίστηκαν τα αποτελέσματα της έρευνας αυτής και δημιουργήθηκαν γραφήματα για κάποιες σημαντικές ερωτήσεις ώστε να παρουσιαστούν με πιο παραστατικό τρόπο οι απαντήσεις τους.

Κεφάλαιο 8ο: Συμπεράσματα και μελλοντικές επεκτάσεις

8.1 Εισαγωγή

Στο όγδοο κεφάλαιο διατυπώνονται και συζητιούνται τα συμπεράσματα της έρευνας που πραγματοποιήθηκε στα προηγούμενα κεφάλαια. Αναλύονται οι πηγές που βρέθηκαν και αξιολογούνται ανά κεφάλαιο σε βαθμό επάρκειας και πληρότητας, καθώς επίσης αναφέρεται και πιθανή μελέτη ή αναγκαία συνεισφορά που χρειάζεται σε κάθε τομέα που διαπραγματεύθηκε η κάθε ενότητα και υποενότητα της εργασίας. Στην συνέχεια, διασαφηνίζονται τυχόν τροποποιήσεις που έγιναν στην διπλωματική κατά την διαδικασία εκπόνησής της. Πιο συγκεκριμένα, στο έκτο και έβδομο κεφάλαιο πραγματοποιήθηκαν κάποιες τροποποιήσεις ή και ολοκληρωτικές αλλαγές οι οποίες αναλύονται παρακάτω. Και τέλος, διακρίνονται πιθανές βελτιώσεις, παραλήψεις και προτάσεις για περαιτέρω ανάπτυξη της μέχρι τώρα έρευνας της παρούσας εργασίας.

8.2 Συμπεράσματα

Καθώς το πρώτο κεφάλαιο είναι καθαρά εισαγωγικό και πραγματεύεται τα περιεχόμενα των υπόλοιπων ενοτήτων, ξεκινώντας από το αμέσως επόμενο, το δεύτερο κεφάλαιο, παρατηρήθηκαν τα παρακάτω. Κατά την έρευνα βρέθηκε μεγάλος αριθμός στατιστικών στοιχείων σχετικά με επιθέσεις που πραγματοποιούνται στον κυβερνοχώρο, με την πεποίθηση των περισσότερων χρηστών να είναι ότι δεν κινδυνεύουν οι συσκευές τους, χωρίς να γνωρίζουν και πολλά για τους τρόπους που μπορούν να τις προστατέψουν. Αναπτύχθηκαν οι τεχνολογίες Εικονική και Επαυξημένη Πραγματικότητα και ο όρος έξυπνος σπίτι, καθώς αναφέρθηκαν και περιστατικά παραβίασης που συμβαίνουν σε αυτό. Στην συνέχεια, παρατηρήθηκαν επιθέσεις που πραγματοποιούν οι επιτιθέμενοι, εκμεταλλευόμενοι τις ευπάθειες κάθε επιπέδου IoT. Αναφέρθηκαν γνωστές και μη επιθέσεις και διαπιστώθηκε ότι στα κατώτερα επίπεδα πραγματοποιούνται περισσότερες επιθέσεις ίσως γιατί υπάρχουν περισσότερες ευαλωτότητες σε αυτά και συνήθως οι συσκευές που λειτουργούν σε αυτά τα επίπεδα είναι κατασκευασμένες για να πραγματοποιούν συγκεκριμένο - μικρό αριθμό λειτουργιών.

Κατά την συγγραφή του τρίτου κεφαλαίου, προτάθηκαν απαιτήσεις και πρότυπα ασφάλειας που βοηθούν στον σχεδιασμό και ανάπτυξη των έξυπνων οικιακών συσκευών. Διαπιστώθηκε ότι σε πολλά άρθρα μπερδεύεται ο όρος πρωτόκολλο με πρότυπο ασφάλειας, και κατά την περιγραφή προτύπων ασφάλειας βρέθηκαν και αναφέρθηκαν αρκετά, τα περισσότερα όμως που βρέθηκαν αφορούσαν κυρίως επιχειρήσεις και οργανισμούς και όχι έξυπνα σπίτια.

Στο τέταρτο κεφάλαιο αναπτύχθηκαν έξυπνες οικιακές συσκευές και συστήματα. Για την ακρίβεια, παρουσιάστηκε ο τρόπος λειτουργίας και υπηρεσίες που προσφέρονται. Έγινε ομαδοποίηση λειτουργιών σχετικά με την προσφορά και την σκοπιμότητά τους, ενώ έγινε και αναφορά σε συγκεκριμένες έξυπνες συσκευές που χρησιμοποιούνται στο οικιακό σύστημα. Στην συνέχεια, διακρίθηκαν κάποια ευάλωτα σημεία των έξυπνων αυτών συσκευών καθώς επίσης αυτά ομαδοποιηθήκαν ανάλογα την περιοχή ευπάθειας τους και βγήκε το συμπέρασμα ότι και λόγω της χρήσης τους οι συσκευές αυτές έχουν ευπάθειες. Δηλαδή λόγω της μικρής κατασκευής, υψηλής απόδοσης και χαμηλής ενεργειακής κατανάλωσης που πρέπει να έχουν δημιουργούνται ζητήματα ασφάλειας. Παρατηρήθηκε ακόμα ότι το παραπάνω σημαντικό συμπέρασμα δεν αναφέρεται σε πολλά

άρθρα ενώ είναι ίσως το αρχικό χαρακτηριστικό που δίνει και την δυνατή λειτουργικότητα που έχει κάθε τέτοια συσκευή και συνεπώς επηρεάζει και τα «κενά» ασφάλειας που μπορεί να φέρει.

Κατά την ανάπτυξη του πέμπτου κεφαλαίου προσδιορίστηκε ο όρος πρακτική καθώς διακρίθηκαν και οι τρείς βασικές κατηγορίες ανάλογα την χρησιμότητα, την αναγνώριση και την ευκολία εφαρμογής τους. Παρατηρήθηκαν και αναπτύχθηκαν πρακτικές ανάλογα την εφαρμογή τους, το στάδιο υλοποίησης των συσκευών που αυτές εφαρμόζονται καθώς αναφέρθηκαν και δεκατρείς οδηγοί του Department for Culture, Media and Sport (DCMS). Υπήρξαν πολλές πηγές οι οποίες πραγματευόταν πρακτικές όμως κάποιες φορές επαναλαμβανόταν οι ίδιες πρακτικές ή δεν ήταν τόσο χρήσιμες σχετικά με την ασφάλεια των έξυπνων οικιακών συσκευών. Τέλος, προτάθηκαν πρακτικές προς τους οργανισμούς με σκοπό την βελτίωση της ασφάλειας των συσκευών που σχεδιάζουν και υλοποιούν ενώ βγήκε το συμπέρασμα ότι ένας συνδυασμός εφαρμογής πολλών πρακτικών από αυτές είναι ο ιδανικός για την αποτροπή εισβολής στις συσκευές και τον περιορισμό, όσο είναι δυνατόν, των ευπαθειών των συστημάτων.

Στο έκτο κεφάλαιο διακρίνονται, από την μέχρι στιγμής έρευνα επί του θέματος, σημαντικές μελλοντικές επεκτάσεις της ασφάλειας έξυπνων οικιακών συσκευών καθώς χωρίζονται και σε τρεις κατηγορίες · αυτές που πραγματοποιούνται από την μεριά των χρηστών, προτροπές προς τους κατασκευαστές και συνδυαστικές προτάσεις οι οποίες χρειάζονται την συνεισφορά και χρηστών και κατασκευαστών. Κύριο συμπέρασμα είναι ότι για την καλύτερη προστασία των συσκευών χρειάζονται πρακτικές που θα ακολουθούνται όχι μόνο στα πλαίσια ενός οργανισμού αλλά και από τους χρήστες των συσκευών αυτών. Ομαδοποιήθηκαν όμως και συγκεκριμένες προτροπές σε κάθε κατηγορία ανάλογα την περιοχή που ενισχύουν με την εφαρμογή τους και τις σχετικές δράσεις προς την εφαρμογή τους. Το έκτο κεφάλαιο αρχικά είχε σχεδιαστεί να αναφερθεί στη δομή συστημάτων που χρησιμοποιούν τεχνολογίες όπως η Επαυξημένη Πραγματικότητα και το Διαδίκτυο των Πραγμάτων καθώς και να παρουσιάσει τρόπους εκμάθησης και ευαισθητοποίησης των χρηστών σε θέματα ασφάλειας, όμως στην πορεία εκπόνησης της εργασίας διαπιστώθηκε ότι είναι καλύτερο να γίνει μια μικρή έρευνα, η οποία παρουσιάζεται στο έβδομο κεφάλαιο, και αφορά την μελέτη συμπεριφοράς και τακτικών που ακολουθούν οι χρήστες σχετικά με την προστασία των έξυπνων συσκευών τους. Αυτό συνέβη με παρουσίαση σχετικών βοηθητικών βίντεο για πιο διαδραστική προσέγγιση ευαισθητοποίησής τους. Συνεπώς στο έκτο κεφάλαιο, κρίθηκε σκόπιμο να διασαφηνιστούν οι πιο σημαντικές προτάσεις από την έρευνα που διεξήχθη στα προηγούμενα κεφάλαια και τις μέχρι τώρα γνώσεις επί του θέματος.

Στο έβδομο κεφάλαιο, αναλύθηκε η έρευνα που πραγματοποιήθηκε σε χρήστες με σκοπό την ευαισθητοποίηση και την εγρήγορσή τους σε θέματα ασφάλειας των έξυπνων οικιακών συσκευών τους. Η ύπαρξη του συγκεκριμένου κεφαλαίου προέκυψε κατά την συγγραφή της εργασίας. Αρχικά, παρουσιάστηκαν οι ερωτήσεις του ερωτηματολογίου, οι οποίες χωρίστηκαν σε σετ και ομάδες ανάλογα την ομοιότητά τους. Στην συνέχεια, αναφέρθηκε η σκοπιμότητα των βίντεο και αναλύθηκαν περαιτέρω. Τέλος, διακρίθηκαν τα αποτελέσματα της έρευνας καθώς παρουσιάστηκαν και τα αντίστοιχα γραφήματα για καλύτερη κατανόηση.

8.3 Μελλοντικές προεκτάσεις

Ξεκινώντας από το δεύτερο κεφάλαιο, μιας και στο πρώτο έγινε μια περίληψη των ενοτήτων της διπλωματικής, προτείνονται οι ακόλουθες μελλοντικές προεκτάσεις. Πιο συγκεκριμένα, στην ομαδοποίηση των επιθέσεων ανά επίπεδο IoT βρέθηκαν λίγες πηγές, κάτι που έκανε αρκετά δύσκολη την έρευνα και την ανάπτυξή της. Θεωρείται σκόπιμο να αναπτυχθούν παρόμοια άρθρα τα οποία θα

ομαδοποιούν επιθέσεις και «κενά» ασφάλειας σε κάθε επίπεδο IoT, τόσο για την κατανόηση των αναγνωστών, όσο και για την καλύτερη παρουσίαση ζητημάτων ασφάλειας σε ενδιαφερόμενους και συνεπώς την ευρύτερη γνώση σχετικά με το θέμα. Στην συνέχεια στο υποκεφάλαιο 2.6 στο οποίο διακρίνονται λύσεις για τις επιθέσεις που αναφέρθηκαν σε κάθε επίπεδο, βρέθηκαν ακόμα πιο λίγες πηγές αναφοράς, με γνωστές πηγές να μην αναφέρονται διότι δεν βρέθηκε το αντίστοιχο υλικό το οποίο να καταγράφει λύσεις που υπάρχουν με σκοπό την αντιμετώπισή τους. Κύριες επιθέσεις οι οποίες είχαν αρκετό διαθέσιμο υλικό ήταν οι MITM, DOS – DDOS και phishing επιθέσεις. Στην υποενότητα 2.7 αναλύθηκαν παραδοσιακές μέθοδοι εκπαίδευσης και αργότερα τα προβλήματα των μεθόδων αυτών. Συμπερασματικά, στο δεύτερο κεφάλαιο, προτείνεται περαιτέρω μελέτη και συγγραφή σχετικά με επιθέσεις και προτάσεις διαχείρισης αυτών των επιθέσεων σε συσκευές IoT.

Κατά την συγγραφή του τρίτου κεφαλαίου, προτάθηκαν απαιτήσεις και πρότυπα ασφάλειας που βοηθούν στον σχεδιασμό και ανάπτυξη των έξυπνων οικιακών συσκευών. Κατά την έρευνα και συγγραφή των προτύπων ασφάλειας βρέθηκαν και αναφέρθηκαν αρκετά, τα περισσότερα όμως που βρέθηκαν αφορούσαν κυρίως επιχειρήσεις και οργανισμούς και όχι έξυπνα σπίτια. Επομένως προτείνεται η περαιτέρω ανάπτυξη συγγραμμάτων τα οποία θα αναφέρονται σε πρότυπα ασφάλειας που χρησιμοποιούνται σε οικιακά συστήματα, ακόμα και η ανάπτυξη προτύπων ασφάλειας για αυτά τα συστήματα.

Σχετικά με το τέταρτο κεφάλαιο, παρουσιάστηκαν κάποιες λειτουργίες έξυπνων οικιακών συσκευών. Η συλλογή πληροφορίων ήταν αρκετά απαιτητική καθώς δεν υπήρχαν επαρκείς πηγές και αναφορές σε λειτουργίες έξυπνων συστημάτων χωρίς να προωθούνται κάποιες συγκεκριμένες εταιρείες ή προϊόντα. Είναι λογικό και θεμιτό μία εταιρία ή οργανισμός με την ανάπτυξη μιας έξυπνης συσκευής να επικεντρώνεται και στην περαιτέρω προώθηση του εκάστοτε οργανισμού, όμως παρατηρήθηκε ότι επικεντρώνονται πολύ περισσότερο στην διαφήμιση του προϊόντος παρά στις λειτουργίες, λύσεις που πιθανόν να δίνει το συγκεκριμένο προϊόν, στην αναφορά των πρωτοκόλλων που χρησιμοποιούν οι συσκευές ή ακόμα και στις τεχνολογίες που υποστηρίζουν. Επομένως, συστήνεται η δημιουργία συγγραμμάτων τα οποία θα περιέχουν περιεκτικές και χρήσιμες πληροφορίες για τον χρήστη, με σκοπό να μπορεί εύκολα να αντλήσει τις απαιτούμενες πληροφορίες που αναζητά. Επίσης, αναφορικά με την εμφάνιση και χρηστικότητα των συσκευών, διαπιστώθηκε ότι δημιουργούνται ζητήματα ασφάλειας. Η παραπάνω διαπίστωση βρέθηκε σε ένα άρθρο μόνο, μετά από αρκετή μελέτη και έρευνα. Αυτό το συμπέρασμα είναι πολύ αξιόλογο και συστήνεται θερμά να αναπτυχθεί και σε άλλα κείμενα, καθώς αποτελεί τον πρωταρχικό λόγο για τον οποίο όλες αυτές οι συσκευές έχουν περιορισμένες δυνατότητες ασφάλειας.

Κατά την ανάπτυξη του πέμπτου κεφαλαίου διακρίθηκαν κάποιες σημαντικές πρακτικές ασφάλειας των συσκευών. Με την έρευνα διαπιστώθηκε ότι ενώ υπήρξαν πολλές πηγές οι οποίες πραγματευόταν πρακτικές, οι περισσότερες είτε επαναλάμβαναν τις ίδιες πρακτικές είτε δεν ήταν τόσο χρήσιμες σχετικά με την ασφάλεια των έξυπνων οικιακών συσκευών. Οι περισσότερες πηγές επικεντρώνονταν σε καλές πρακτικές που μπορεί να πραγματοποιήσει μία εταιρία και όχι κάθε χρήστης μεμονωμένα. Συνεπώς, κρίνεται σημαντικό να διατυπωθούν σχετικά άρθρα για τις οικιακές συσκευές και συστήματα.

Στο έκτο κεφάλαιο διακρίνονται, από την μέχρι στιγμής έρευνα επί του θέματος, σημαντικές μελλοντικές επεκτάσεις της ασφάλειας έξυπνων οικιακών συσκευών καθώς χωρίζονται και σε τρεις κατηγορίες · αυτές που πραγματοποιούνται από την μεριά των χρηστών, προτροπές προς τους κατασκευαστές και συνδυαστικές προτάσεις οι οποίες χρειάζονται την συνεισφορά και χρηστών και κατασκευαστών. Η συλλογή των μελλοντικών προεκτάσεων ήταν απαιτητική καθώς ενώ βρέθηκαν αρκετές πηγές που αναφέρονταν επί του θέματος, ήταν αρκετά περιορισμένες οι προτροπές που

πρότεινε κάθε πηγή. Προτείνεται η συλλογή και αναφορά περισσότερων προτροπών σε κάθε άρθρο, καθώς και αυτό είναι ένα σημαντικό κομμάτι για περαιτέρω βελτίωση στην συγγραφή αντίστοιχων κειμένων.

Τέλος, στο έβδομο κεφάλαιο παρουσιάστηκαν οι απαντήσεις και τα συμπεράσματα ενός ερωτηματολογίου σχετικού με την ασφάλεια των έξυπνων οικιακών συσκευών και τα μοτίβα συμπεριφοράς των χρηστών σε θέματα ασφάλειας. Πιθανή βελτίωση της συγκεκριμένης έρευνας θα ήταν η συγκέντρωση μεγαλύτερου κοινού ώστε να είναι πιο συμπεριληπτικά τα αποτελέσματα, καθώς ο χρόνος συγγραφής και εκπόνησης μιας διπλωματικής εργασίας είναι σχετικά περιορισμένος.

8.4 Επίλογος

Στο όγδοο κεφάλαιο αναλύθηκαν ανά κεφάλαιο τα συμπεράσματα και οι μελλοντικές προεκτάσεις που μπορούν να πραγματοποιηθούν. Αναφέρθηκαν περιορισμοί οι οποίοι υπήρχαν κατά την συγγραφή της εργασίας ανά κεφάλαιο καθώς επίσης και τα κυριότερα στοιχεία και χαρακτηριστικά κάθε κεφαλαίου ενώ έγιναν σχετικές διευκρινήσεις.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Abdullah M. Alnajim, Shabana Habib, Muhammad Islam, Hazim Saleh AlRawashdeh and Muhammad Wasim, “Exploring Cybersecurity Education and Training Techniques: A Comprehensive Review of Traditional, Virtual Reality, and Augmented Reality Approaches,” MDPI, τόμος 15, έκδοση 12, 7 Δεκεμβρίου 2023, διαθέσιμο: https://www.mdpi.com/2073-8994/15/12/2175.

2. Douha, N.Y.-R., Renaud, K., Taenaka, Y. and Kadobayashi, Y. (2023), “Smart home cybersecurity awareness and behavioral incentives,” Information and Computer Security, τόμος 31, έκδοση 5, σελίδες 545-575, διαθέσιμο: https://doi.org/10.1108/ICS-03-2023-0032.
3. Ziarmal Nazar Mohammad, Fadi Farha, Adnan O.M Abuassba, Shunkun Yang, and Fang Zhou, “Access Control and Authorization in Smart Homes: A Survey,” Tsinghua Science and Technology, τόμος 26, έκδοση 6, σελίδες 906-917, Δεκέμβριος 2021.

4. N'guessan Yves-Roland Douha, “Human-Centered Cybersecurity Strategies and Behavioral Incentives for Secure Smart Home,” Nara Institute of Science and Technology, 15 Σεπτεμβρίου 2023.

5. Y. Lu, “Cybersecurity research: A review of current research topics,” Journal of Industrial Integration and Management, τόμος 3, νούμερο 04, 2018, διαθέσιμο: https:// doi.org/10.1142/S2424862218500148.

6. A.Lindbeck, “Incentives and Social Norms in Household Behavior,” The American Economic Review, τόμος 87, νούμερο 2, σελίδες 370 – 377, 1997, διαθέσιμο : http://www.jstor.org/stable/2950948.

7. Touqeer, Hussain, Zaman, Amin, Fadi Al-Turjman, Muhammad Bilal, “Smart home security: challenges, issues and solutions at different IoT layers,” τόμος 77, σελίδες 14053–14089, 10 Μαΐου 2021.

8. D. Wei and X. Qiu, “Status-based Detection of malicious code in Internet of Things (IoT) devices,” 2018 IEEE Conference on Communications and Network Security (CNS), Beijing, China, 2018, σελίδες. 1-7, διαθέσιμο: 10.1109/CNS.2018.8433183.

9. Neha Sharma, Amlan Chakrabarti, Valentina Emilia Balas. “Data Management, Analytics and Innovation,” Advances in Intelligent Systems and Computing, Springer Singapore, τόμος 1, έκδοση 1, σελίδες 740, 25 Οκρωβρίου 2019, διαθέσιμο: https://doi.org/10.1007/978-981-32-9949-8.

10. W. Syafitri, Z. Shukur, U. A. Mokhtar, R. Sulaiman and M. A. Ibrahim, “Social Engineering Attacks Prevention: A Systematic Literature Review,” IEEE Access, τόμος 10, σελίδες 39325-39343, 2022, διαθέσιμο: 10.1109/ACCESS.2022.3162594.

11. Ingrid M.R. Verbauwhede, “Secure Integrated Circuits and Systems,” Integrated Circuits and Systems, Springer New York, έκδοση 1, σελίδες 246, 5 Απριλίου 2010, διαθέσιμο: https://doi.org/10.1007/978-0-387-71829-3.

12. Alefiya Hussain, John Heidemann, Christos Papadopoulos, “A Framework for Classifying Denial of Service Attacks,” SIGCOMM '03: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications, σελίδες 99 - 110, Αύγουστος 2003, διαθέσιμο: 10.1145/863955.863968.

13. Gu, Qijun & Liu, Peng, “Denial of Service Attacks,” Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications, τόμος 3, σελίδες 454 - 468, Ιανουάριος 2012, διαθέσιμο: 10.1002/9781118256107.ch29.

14. M. Conti, N. Dragoni and V. Lesyk, “A Survey of Man In The Middle Attacks,” IEEE Communications Surveys & Tutorials, τόμος 18, έκδοση 3, σελίδες 2027-2051, thirdquarter 2016, διαθέσιμο: 10.1109/COMST.2016.2548426.

15. Apandi, Siti & Sallim, Jamaludin & Sidek, Roslina, “Types of anti-phishing solutions for phishing attack,” IOP Conference Series: Materials Science and Engineering, Ιούνιος 2020, διαθέσιμο: 012072. 10.1088/1757-899X/769/1/012072.

16. Tiu, Yan & Zolkipli, Mohamad, “Study on Prevention and Solution of Ransomware Attack”, Journal of IT in Asia, τόμος 9, έκδοση 1, σελίδες 133-139, Δεκέμβριος 2021, διαθέσιμο: 10.33736/jita.3402.2021.

17. Abood, Omar & Guirguis, Shawkat, “A Survey on Cryptography Algorithms,” International Journal of Scientific and Research Publications, σελίδες 495-516, Ιούλιος 2018, διαθέσιμο: 10.29322/IJSRP.8.7.2018.p7978.

18. Tasnuva Mahjabin, Yang Xiao, Guang Sun, Wangdong Jiang, “A survey of distributed denial-of-service attack, prevention, and mitigation techniques,” International Journal of Distributed Sensor Networks, τόμος 13, έκδοση 12, Δεκέμβριος 2017, διαθέσιμο: 10.1177/1550147717741463.

19. A. Huseinović, S. Mrdović, K. Bicakci and S. Uludag, “A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid,” IEEE Access, τόμος 8, σελίδες 177447-177470, Σεπτέμβριος 2020, διαθέσιμο: 10.1109/ACCESS.2020.3026923.

20. Mohamed A. Aref, Sudharman K. Jayaweera, Esteban Yepez, “Survey on cognitive anti-jamming communications,” IET Communications, τόμος 14, έκδοση 18, σελίδες 3087-3302, Ιούνιος 2020, διαθέσιμο: 10.1049/iet-com.2020.0024.

21. Noshina Tariq, Farrukh Aslam Khan, Muhammad Asim, “Security Challenges and Requirements for Smart Internet of Things Applications: A Comprehensive Analysis,” Procedia Computer Science, τόμος 191, σελίδες 425-430, 2021, διαθέσιμο: https://doi.org/10.1016/j.procs.2021.07.053.

22. K. Karimi and S. Krit, “Smart home-Smartphone Systems: Threats, Security Requirements and Open research Challenges,” 2019 International Conference of Computer Science and

Renewable Energies (ICCSRE), σελίδες 1-5, Αύγουστος 2019, διαθέσιμο: 10.1109/ICCSRE.2019.8807756.

23. T.Pecorella, L.Pierucci, F.Nizzi, ""Network Sentiment" Framework to Improve Security and Privacy for Smart Home," Future Internet 10, έκδοση 12, Δεκέμβριος 2018, διαθέσιμο: https://doi.org/10.3390/fi10120125.

24. Jangirala Srinivas, Ashok Kumar Das, Neeraj Kumar, "Government regulations in cyber security: Framework, standards and recommendations," Future Generation Computer Systems, τόμος 92, σελίδες 178-188, 2019, διαθέσιμο: https://doi.org/10.1016/j.future.2018.09.063.

25. M. M. Hossain, M. Fotouhi and R. Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things," 2015 IEEE World Congress on Services, σελίδες 21-28, Αύγουστος 2015, διαθέσιμο: 10.1109/SERVICES.2015.12.

26. Michael Hayoz, "Introducing SSL The Secure Sockets Layer Protocol," Department of Informatics University of Freiburg, 16 Ιουνίου 2003.

27. Cas Cremers, Benjamin Kiesl, Niklas Medinger, "A Formal Analysis of IEEE 802.11's WPA2: Countering the Kracks Caused by Cracking the Counters," 29th USENIX Security Symposium, 12-14 Αυγούστου 2020, διαθέσιμο: https://www.usenix.org/conference/usenixsecurity20/presentation/cremers.

28. Giuca, O., Popescu, T.M., Popescu, A.M., Prostean, G., Popescu, D.E., "A Survey of Cybersecurity Risk Management Frameworks," Advances in Intelligent Systems and Computing, Springer, τόμος 1221, Αύγουστος 2020, διαθέσιμο :https://doi.org/10.1007/978-3-030-51992-6_20.

29. N. M. Karie, N. M. Sahri, W. Yang, C. Valli and V. R. Kebande, "A Review of Security Standards and Frameworks for IoT-Based Smart Environments," IEEE Access, τόμος 9, σελίδες 121975-121995, Σεπτέμβριος 2021, διαθέσιμο: 10.1109/ACCESS.2021.3109886.

30. Y. Wang et al., "Analysis of Smart Grid security standards," 2011 IEEE International Conference on Computer Science and Automation Engineering, Ιούλιος 2011, σελίδες 697-701, διαθέσιμο: 10.1109/CSAE.2011.5952941.

31. C. J. Alberts, S. G. Behrens, R. D. Pethia, and W. R. Wilson, "Operationally critical threat, asset, and vulnerability evaluation (OCTAVE) framework, version 1.0," Carnegie Mellon University, 2018.

32. "National Institute of Standards and Technology (NIST)," NIST Public Access, διαθέσιμο: https://www.nist.gov/.

33. Yates, JoAnne and Murphy, Craig N., "Coordinating International Standards: The Formation of the ISO," MIT Sloan Research, σύγγραμμα 4638-07, Ιανουάριος 2007, διαθέσιμο: https://ssrn.com/abstract=962455 or http://dx.doi.org/10.2139/ssrn.962455.

34. About us, ETSI, διαθέσιμο: https://www.etsi.org/about.

35. M. R. Alam, M. B. I. Reaz and M. A. M. Ali, "A Review of Smart Homes—Past, Present, and Future," IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), τόμος 42, νούμερο 6, σελίδες 1190-1203, Νοέμβριος 2012, διαθέσιμο: 10.1109/TSMCC.2012.2189204.

36. Mahyuzie Jenal, Athira Nabilla Omar, Muhammad Azizi Aswad Hisham, Wan Najmi Wan Mohd Noh, Zul Adib Izzuddin Razali, "Smart Home Controlling System," Journal of Electronic Voltage and Application, τόμος 3, νούμερο 1, σελίδες 92-104, Ιούλιος 2022.

37. M. Cerny, M. Penhaker, "Circadian Rhythm Monitoring in HomeCare Systems," 13th International Conference on Biomedical Engineering, Springer, τόμος 23, σελίδες 950-953, διαθέσιμο: https://doi.org/10.1007/978-3-540-92841-6_235.

38. D. Pishva and K. Takeda, "A product based security model for smart home appliances," Proc. 40th Annu. IEEE Int. Carnahan Conf. Security Technol., σελίδες 234–242, 2006.

39. R. K. Kodali, V. Jain, S. Bose and L. Boppana, "IoT based smart security and home automation system," 2016 International Conference on Computing, Communication and Automation (ICCCA), σελίδες 1286-1289, 2016, διαθέσιμο: 10.1109/CCAA.2016.7813916.

40. S. Somani, P. Solunke, S. Oke, P. Medhi and P. P. Laturkar, "IoT Based Smart Security and Home Automation," 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), σελίδες 1-4, 2016, διαθέσιμο: 10.1109/ICCUBEA.2018.8697610.

41. Kumar Sitaraa, Dhiraj Divya, Cibi Christina, Sowmya, Sabitha, "Smart Alarm Clock," 2018 3rd International Conference on Communication and Electronics Systems (ICCES), Οκτώβριος 2018, διαθέσιμο: 999-1001. 10.1109/CESYS.2018.8724024.

42. Mukesh P. Mahajan, Rohit R. Nikam, Vivek P. Patil, Rahul D. Dond, "Smart Refrigerator Using IOT," International Journal of Latest Engineering Research and Applications (IJLERA), τόμος 2, έκδοση 3, σελίδες 86-91, Μάρτιος 2017.

43. I. Ganchev, Z. Ji and M. O'Droma, "An IoT-based smart electric heating control system: Design and implementation," 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), σελίδες 760-762, Ιούλιος 2017, διαθέσιμο: 10.1109/ICUFN.2017.7993895.

44. J. Bugeja, A. Jacobsson and P. Davidsson, "On Privacy and Security Challenges in Smart Connected Homes," 2016 European Intelligence and Security Informatics Conference (EISIC), σελίδες 172-175, 2016, διαθέσιμο: 10.1109/EISIC.2016.044.

45. Huichen Lin, Neil W. Bergmann, "IoT Privacy and Security Challenges for Smart Home Environments," IoT Privacy and Security Challenges for Smart Home Environments, τόμος 7, έκδοση 3, Ιούλιος 2016, διαθέσιμο: https://doi.org/10.3390/info7030044.

46. S. Al Salami, J. Baek, K. Salah, E. Damiani, "Lightweight Encryption for Smart Home," 2016 11th International Conference on Availability, Reliability and Security (ARES), σελίδες 382-388, Σεπτέμβριος 2016, διαθέσιμο: 10.1109/ARES.2016.40.

47. V. Vakhter, B. Soysal, P. Schaumont, U. Guler, “Threat Modeling and Risk Analysis for Miniaturized Wireless Biomedical Devices,” IEEE Internet of Things Journal, τόμος 9, νούμερο 15, σελίδες 13338-13352, Αύγουστος 2022, διαθέσιμο: 10.1109/JIOT.2022.3144130.

48. Christopher Bellman and Paul C. van Oorschot, “Best Practices for IoT Security: What Does That Even Mean?,” arXiv preprint, 2020, διαθέσιμο: arXiv:2004.12179.

49. Mughal, Arif Ali, “Cybersecurity Hygiene in the Era of Internet of Things (IoT): Best Practices and Challenges,” Applied Research in Artificial Intelligence and Cloud Computing, τόμος 2, έκδοση 1, σελίδες 1-31, Ιανουάριος 2019, διαθέσιμο: https://researchberg.com/index.php/araic/article/view/113.

50. Christopher Bellman, Paul C. van Oorschot, “Best Practices for IoT Security: What Does That Even Mean?,” arXiv, Απρίλιος 2020, διαθέσιμο: arXiv:2004.12179.

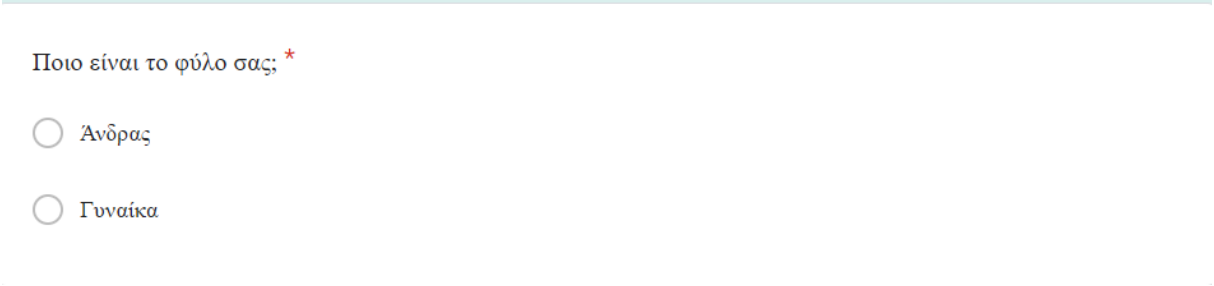
51. Nurse Jason, Creese Sadie, Goldsmith Michael, Lamberts Koen, “Guidelines for usable cybersecurity: Past and present,” Proceedings - 2011 3rd International Workshop on Cyberspace Safety and Security, Οκτώβριος 2011, διαθέσιμο: 10.1109/CSS.2011.6058566.

52. Mandy Stanton, George Ernst, Anton L. Janik, “Cybersecurity Best Practices,” The Arkansas Lawyer, τόμος 51, νούμερο 4, 2016.

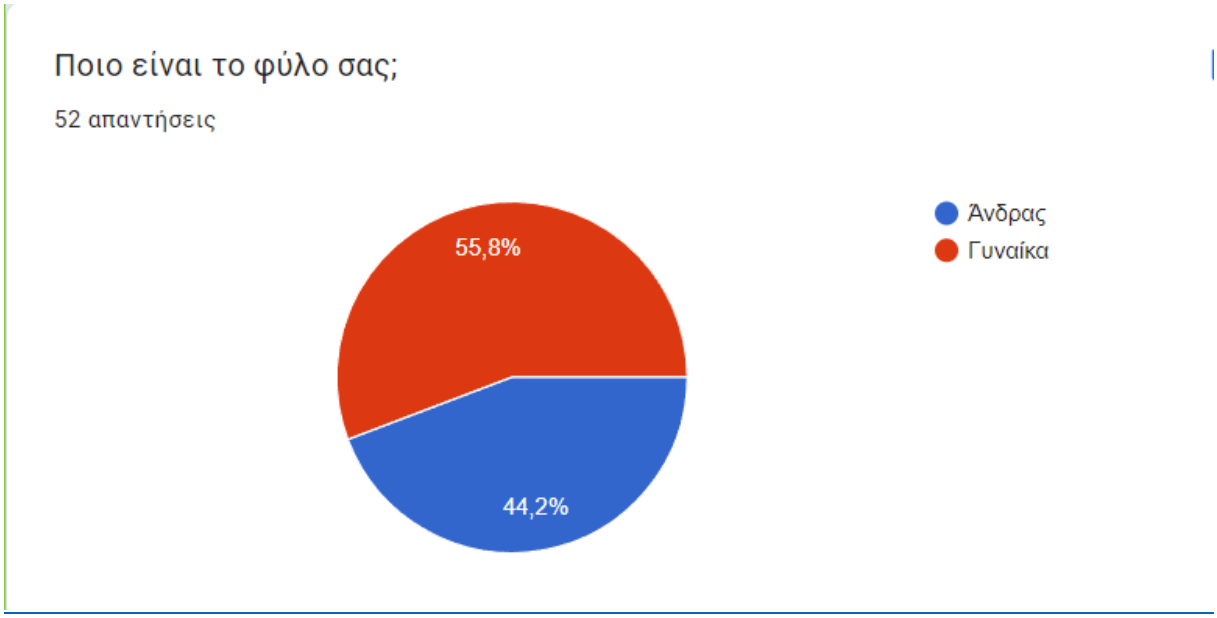
ΠΑΡΑΡΤΗΜΑ Α : ΠΑΡΟΥΣΙΑΣΗ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟΥ

Στο προκείμενο παράρτημα παρουσιάζονται πληροφορίες σχετικά με τις ερωτήσεις του ερωτηματολογίου που πραγματοποιήθηκε με σκοπό την ευαισθητοποίηση και επαγρύπνηση των χρηστών σε ζητήματα και τεχνικές ασφάλειας των έξυπνων οικιακών συσκευών τους. Παρακάτω διαφαίνονται στιγμιότυπα των ερωτήσεων που ζητήθηκαν, μια σχετική περιγραφή τους και τα αποτελέσματα που βγήκαν καθώς και τα αντίστοιχα συμπεράσματα.

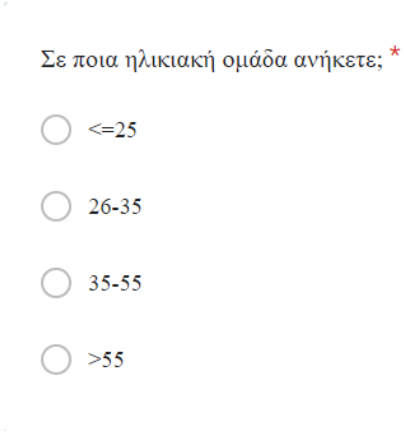
Αρχικά, με σκοπό την δημιουργία ενός ερωτηματολογίου με σαφή και επαρκή αποτελέσματα, επικεντρώθηκα στο είδος των ερωτήσεων που ήθελα να κάνω ώστε να λάβω και τις πληροφορίες που χρειαζόμουν. Επομένως, οι ερωτήσεις ομαδοποιηθήκαν σε κατηγορίες ώστε να καλύπτουν τις απαιτούμενες πληροφορίες που ήταν αναγκαίο να ληφθούν. Οι πρώτες ερωτήσεις ήταν αναγνωριστικές και ζητήθηκε το φύλο, η ηλικιακή ομάδα που ανήκουν οι χρήστες, η εξοικείωσή τους με τις έξυπνες συσκευές τους και τα είδη των έξυπνων συσκευών που αυτοί διαθέτουν. Παρουσιάζονται και παρακάτω οι σχετικές ερωτήσεις με τα ποσοστά κάθε απάντησης. Αξίζει να σημειωθεί ότι στην ερώτηση που σχετίζεται με τις έξυπνες οικιακές συσκευές που διαθέτουν οι ερωτηθέντες, υπήρχε δυνατότητα συμπλήρωσης κάποιας συσκευής που δεν υπήρχε στις απαντήσεις, και προστέθηκε το έξυπνο κλιματιστικό. Ακόμη, στην ερώτηση που αφορά την ηλικιακή ομάδα του χρήστη, οι απαντήσεις <=25 και <25 συμπτύχθηκαν καθώς κατά την συμπλήρωση του ερωτηματολογίου διαπιστώθηκε ότι η ηλικία 25 ετών δεν υπήρχε σαν απάντηση.



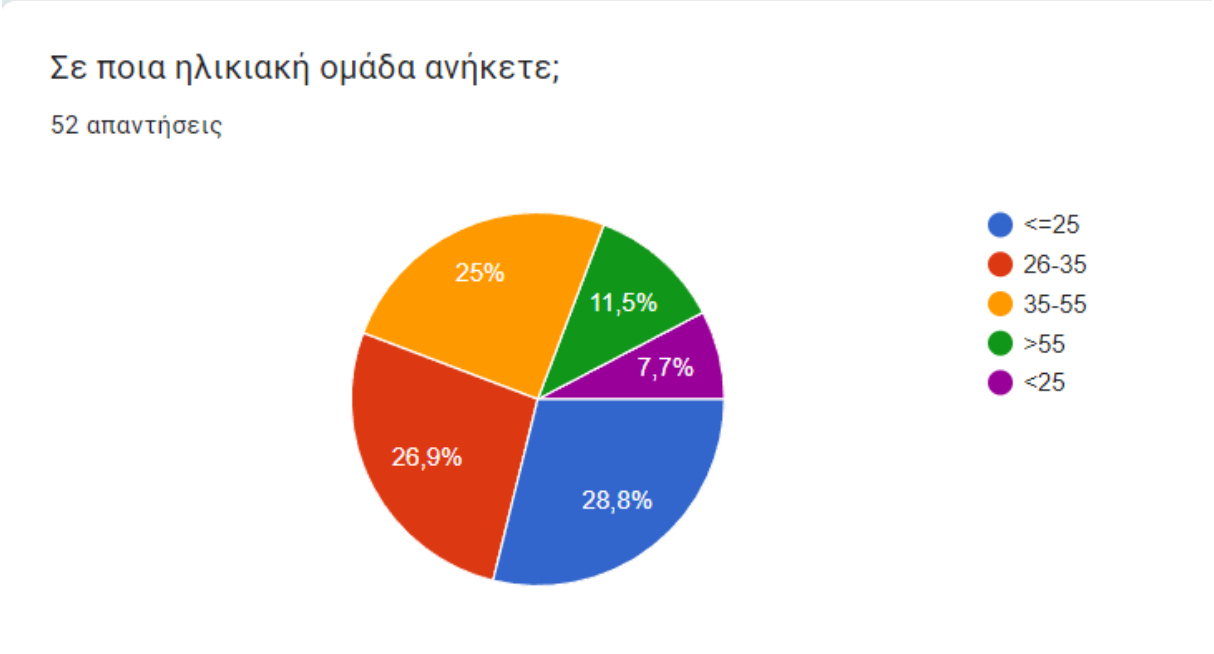
Εικόνα 9. Πρώτη ερώτηση, σχετίζεται με το φύλο του χρήστη



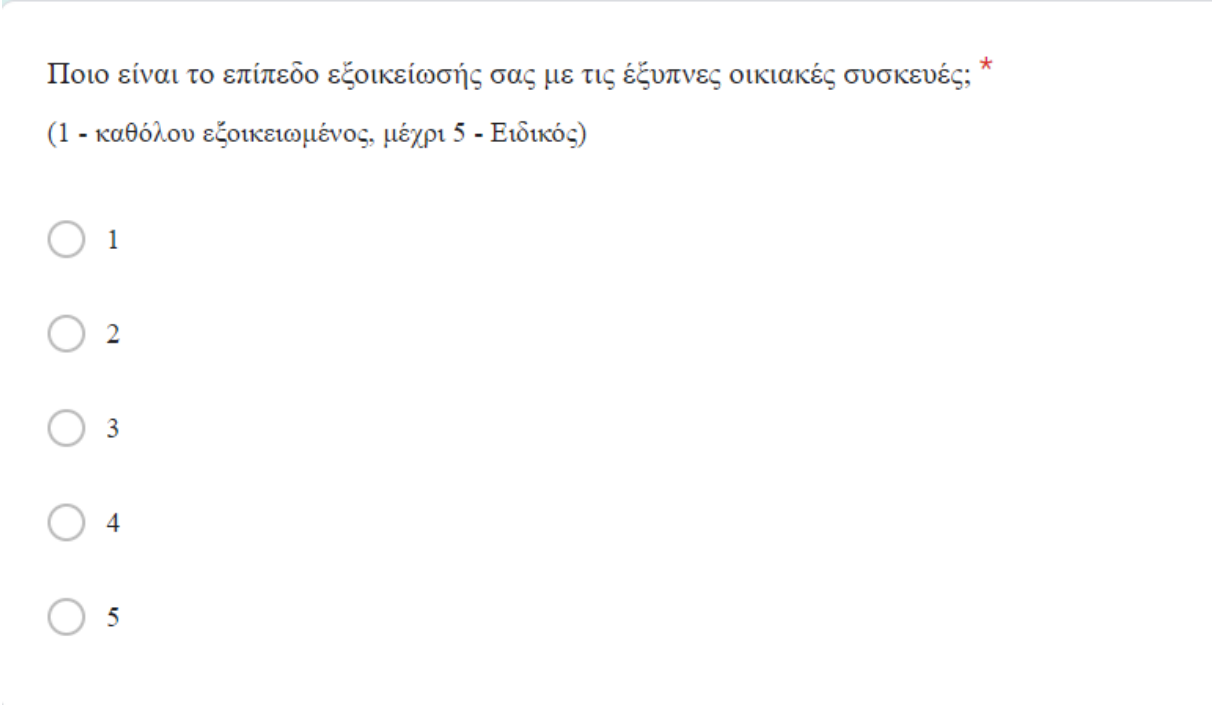
Εικόνα 10. Ποσοστά απαντήσεων πρώτης ερώτησης



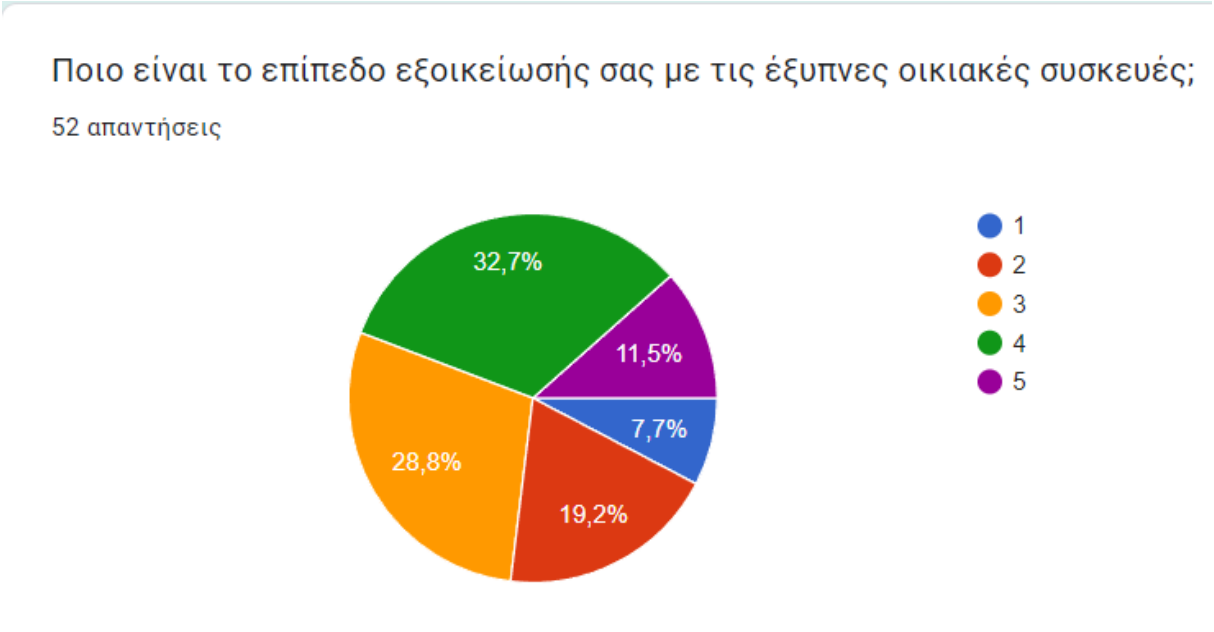
Εικόνα 11. Δεύτερη ερώτηση, σχετίζεται με την ηλικία του χρήστη



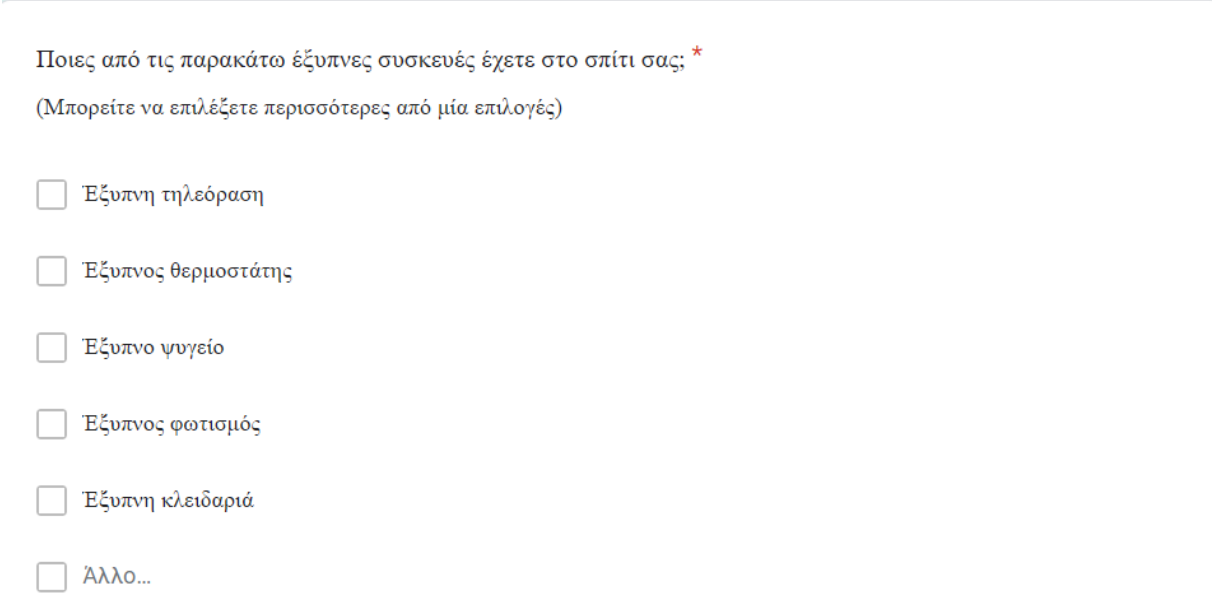
Εικόνα 12. Ποσοστά απαντήσεων δεύτερης ερώτησης



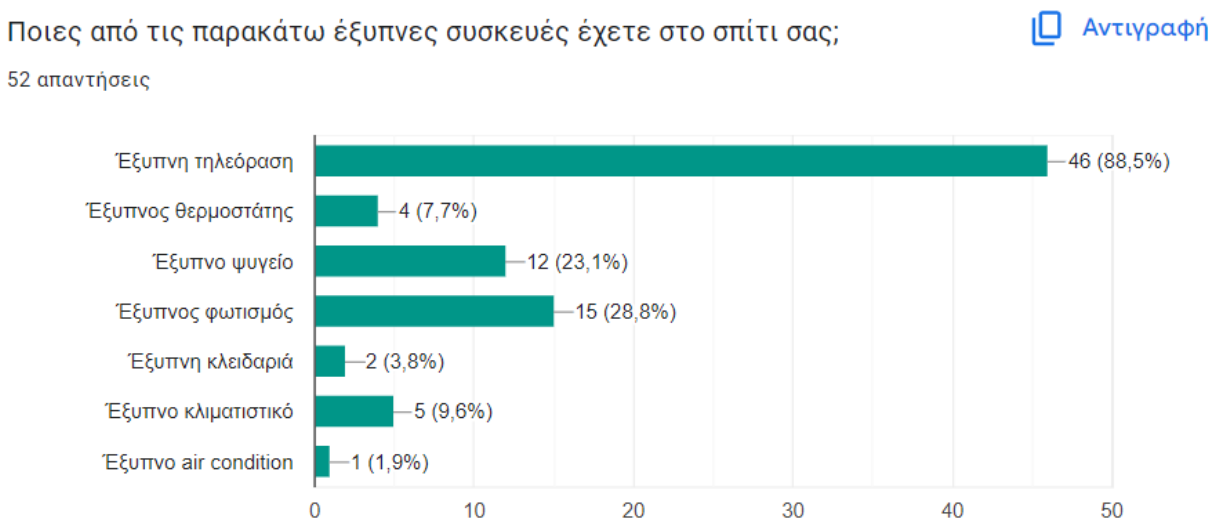
Εικόνα 13. Τρίτη ερώτηση, αφορά στο ποσοστό εξοικείωσης του χρήστη με τις συσκευές του



Εικόνα 14. Ποσοστά απαντήσεων τρίτης ερώτησης

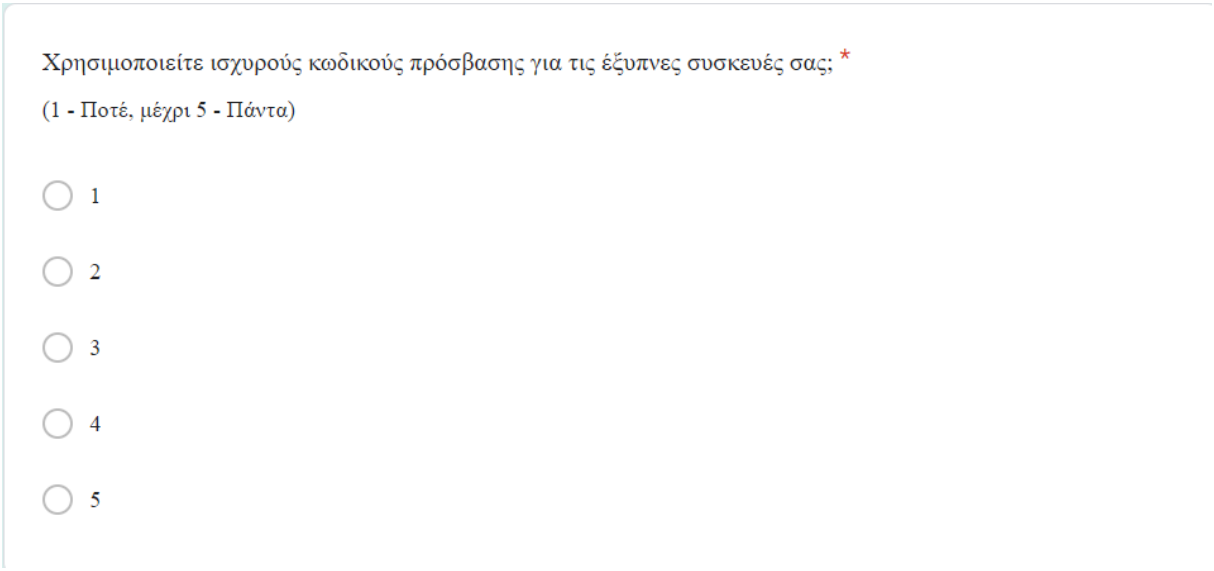


Εικόνα 15. Τέταρτη ερώτηση, καταγράφονται οι έξυπνες συσκευές του χρήστη



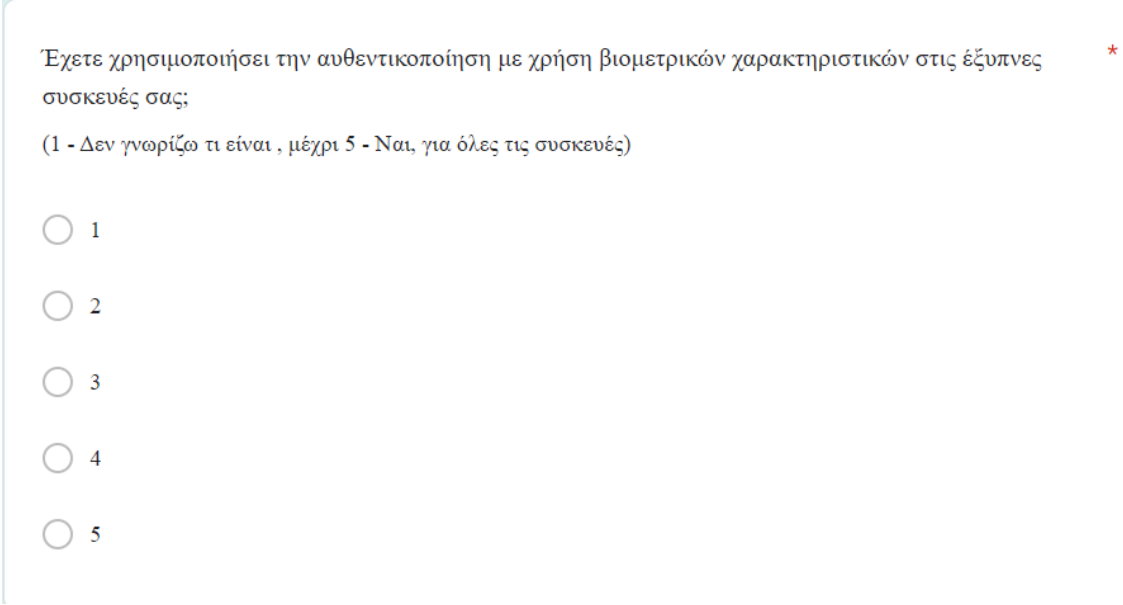
Εικόνα 16. Ποσοστά απαντήσεων τέταρτης ερώτησης

Στην συνέχεια, οι ερωτήσεις της δεύτερης κατηγορίας ασχολούνταν με το κατά πόσο οι χρήστες ασφαλίζουν τις έξυπνες συσκευές τους και ζητήθηκε να αξιολογηθεί από τους χρήστες η ανθεκτικότητα των κωδικών που χρησιμοποιούν κατά την είσοδό τους στις συσκευές τους και αργότερα παρουσιάστηκε σχετικό βίντεο. Ακόμη, οι χρήστες ρωτήθηκαν αν χρησιμοποιούν επιπλέον αυθεντικοποίηση στις συσκευές τους, και συγκεκριμένα με χρήση βιομετρικών χαρακτηριστικών. Παρακάτω διαφαίνονται οι δύο αυτές ερωτήσεις με τις απαντήσεις και τα ποσοστά τους.

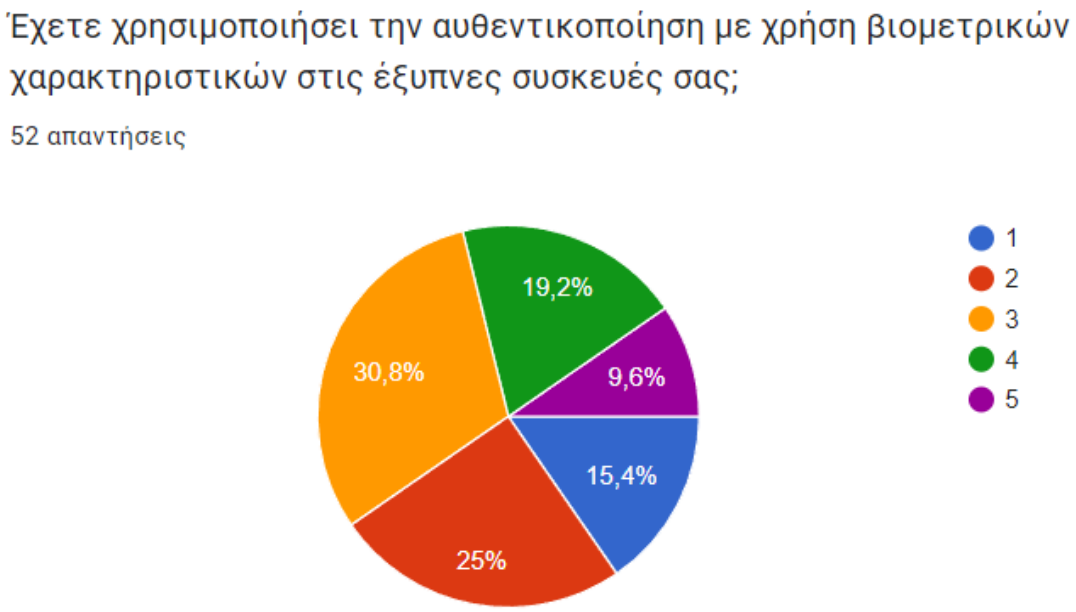


Εικόνα 17. Πέμπτη ερώτηση, σχετική με την χρήση ισχυρών κωδικών πρόσβασης στις συσκευές

Εικόνα 18. Ποσοστά απαντήσεων πέμπτης ερώτησης

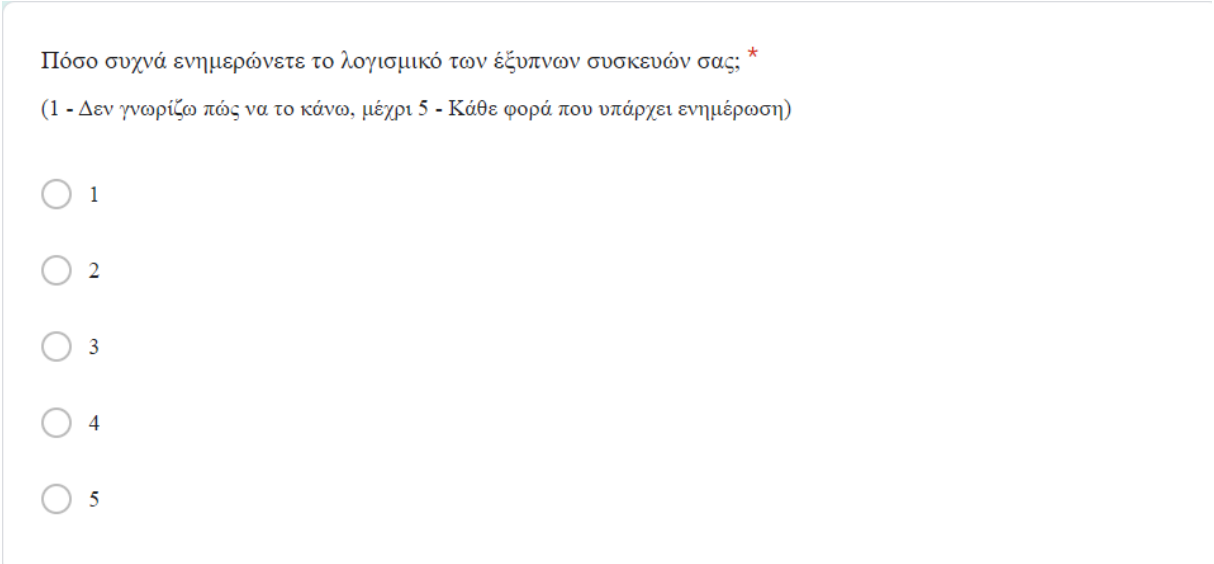


Εικόνα 19. Έκτη ερώτηση, αφορά στην χρήση αυθεντικοποίησης με βιομετρικά χαρακτηριστικά

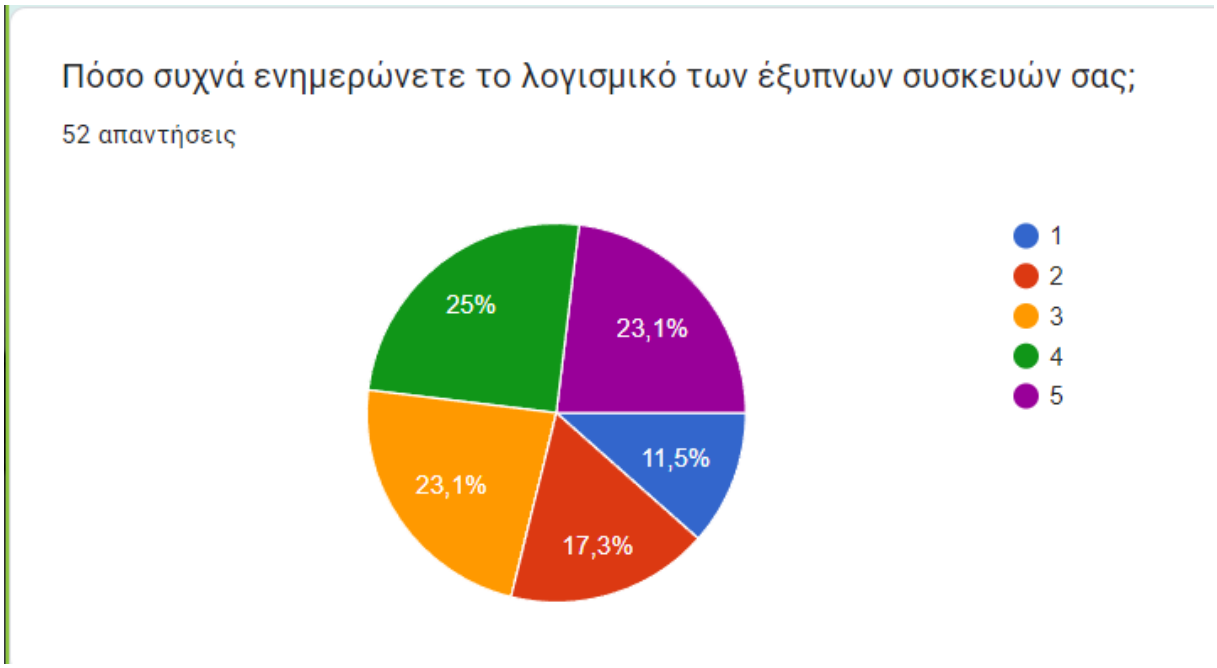


Εικόνα 20. Ποσοστά απαντήσεων έκτης ερώτησης

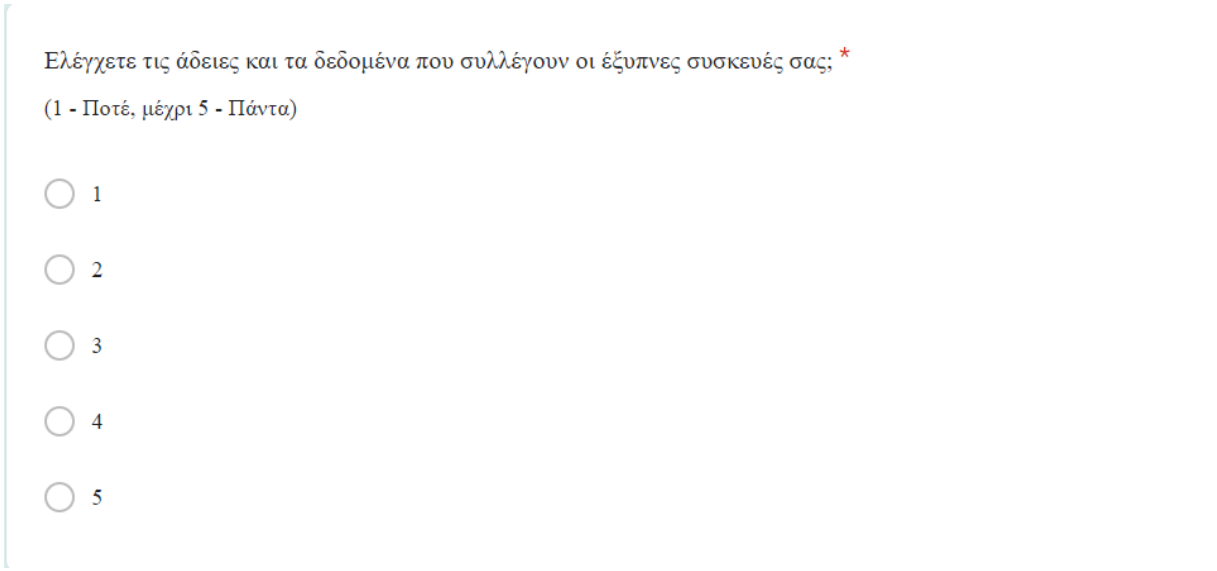
Επιπρόσθετα, στην επόμενη κατηγορία διευκρινίστηκε η συχνότητα με την οποία οι χρήστες ενημερώνουν τις έξυπνες οικιακές συσκευές τους, αν ενημερώνονται για τις σχετικές άδειες και δεδομένα που συλλέγονται από αυτές, καθώς επίσης αν έχουν διαβάσει την πολιτική απορρήτου των συσκευών τους. Παρακάτω παρουσιάζονται οι αντίστοιχες ερωτήσεις και τα ποσοστά των απαντήσεών τους.



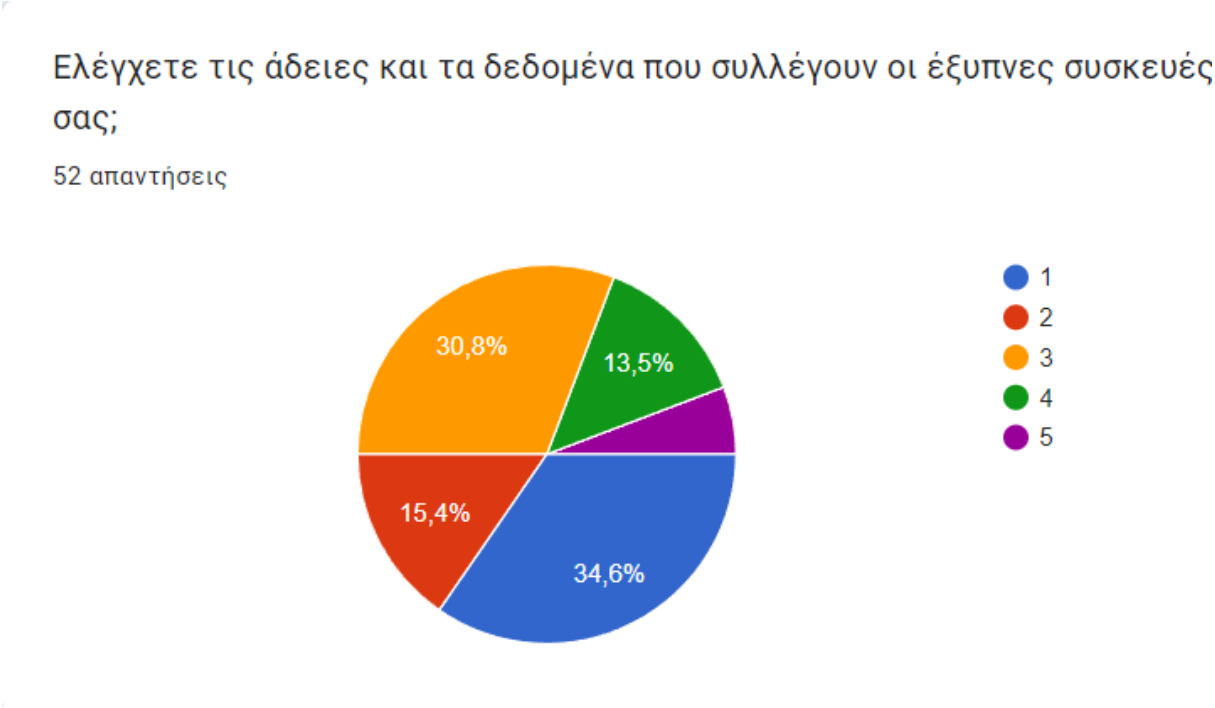
Εικόνα 21. Έβδομη ερώτηση, σχετίζεται με την συχνότητα ενημέρωσης λογισμικού



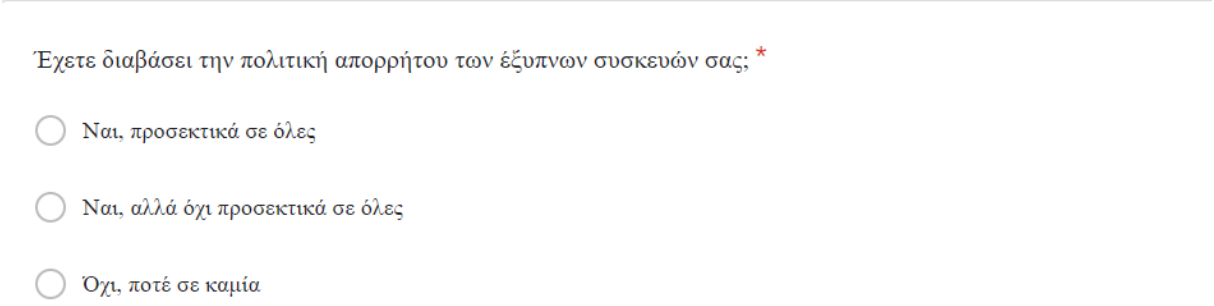
Εικόνα 22. Ποσοστά απαντήσεων έβδομης ερώτησης



Εικόνα 23. Όγδοη ερώτηση, αναφέρεται στον έλεγχο αδειών και δεδομένων που διαχειρίζονται οι συσκευές



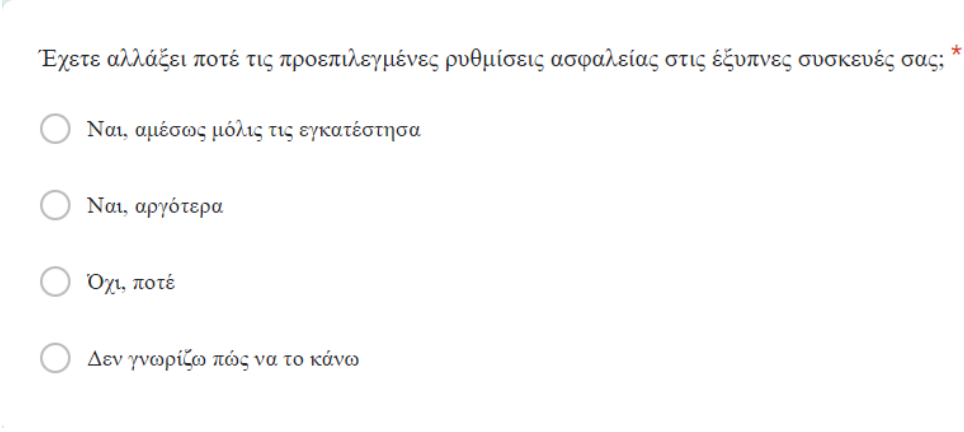
Εικόνα 24. Ποσοστά απαντήσεων όγδοης ερώτησης



Εικόνα 25. Ένατη ερώτηση, σχετική με την ανάγνωση της πολιτικής απορρήτου των συσκευών

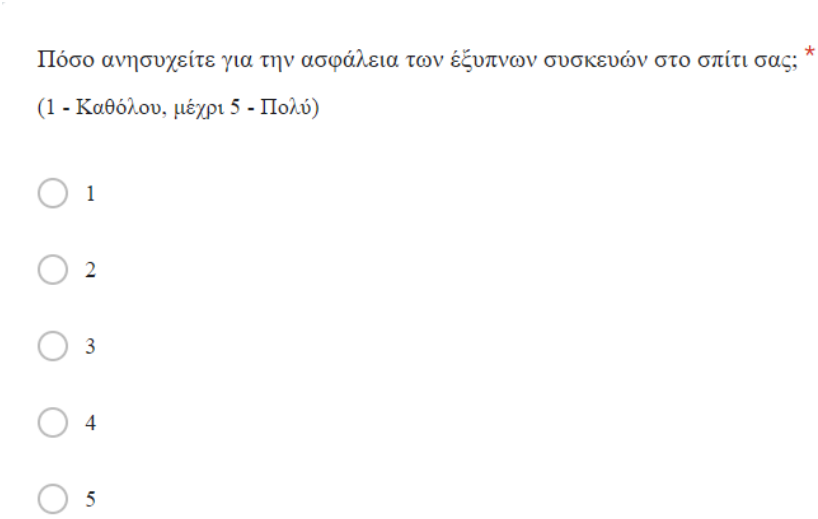
Εικόνα 26. Ποσοστά απαντήσεων ένατης ερώτησης

Επίσης, η επόμενη κατηγορία περιείχε δύο ερωτήσεις, οι οποίες αποσκοπούσαν στην άντληση πληροφοριών για την μέχρι τώρα ευαισθητοποίηση των χρηστών σχετικά με την ασφάλεια των συσκευών τους. Επομένως ζητήθηκε από τους χρήστες να απαντήσουν αν έχουν αλλάξει τις προεπιλεγμένες ρυθμίσεις κάθε συσκευής τους και κατά πόσο ανησυχούν για την ασφάλεια των συσκευών τους. Στην συνέχεια, παρουσιάστηκε σχετικό βίντεο που έχει αναλυθεί και παραπάνω, και είχε σκοπό την ευαισθητοποίηση των χρηστών με ένα πιο διαδραστικό και άμεσο τρόπο.



Εικόνα 27. Δέκατη ερώτηση, σχετική με την αλλαγή των προεπιλεγμένων ρυθμίσεων των συσκευών

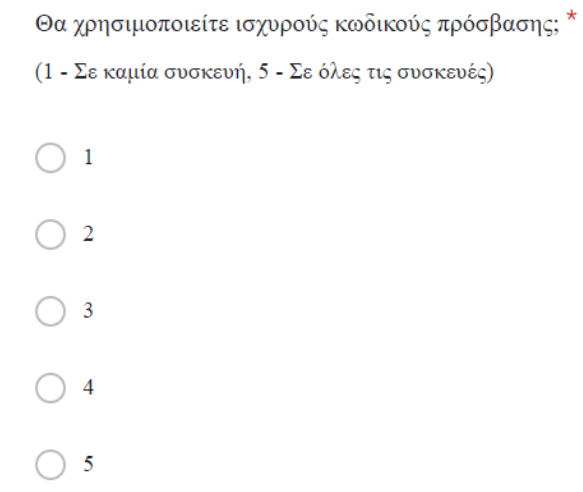
Εικόνα 28. Ποσοστά απαντήσεων δέκατης ερώτησης



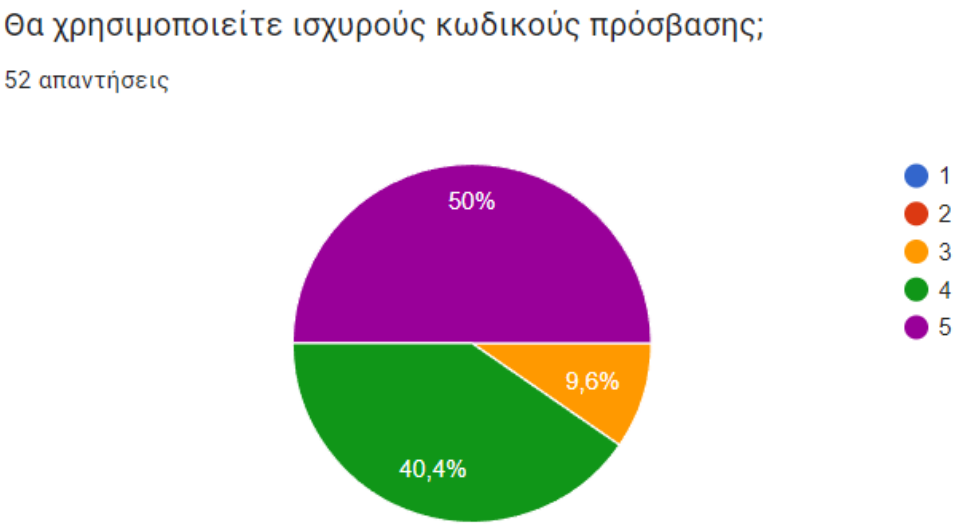
Εικόνα 29. Ενδέκατη ερώτηση, σχετίζεται με το ποσοστό ανησυχίας σχετικά με την ασφάλεια των έξυπνων οικιακών συσκευών

Εικόνα 30. Ποσοστά απαντήσεων ενδέκατης ερώτησης

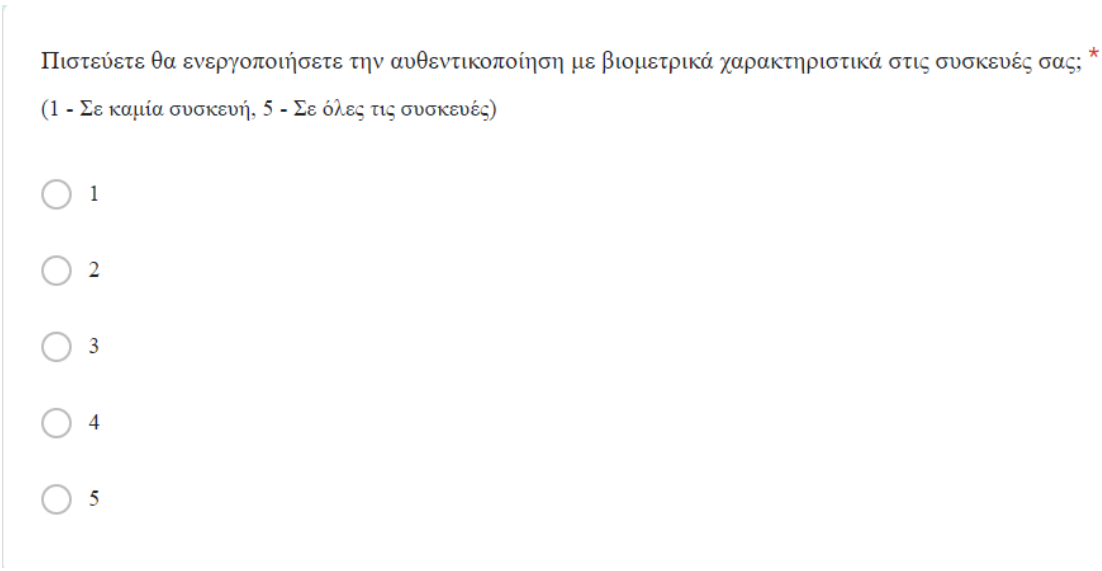
Τέλος, το επόμενο σετ ερωτήσεων αποτελείται από ερωτήσεις που είχαν γίνει και νωρίτερα και αποσκοπεί στην άντληση συμπερασμάτων σχετικά με την ευαισθητοποίησή τους μετά και την παρουσίαση των βίντεο και των ερωτήσεων που έγιναν νωρίτερα στο ερωτηματολόγιο. Οι ερωτήσεις ήταν σχετικές με το κατά πόσο οι χρήστες θα χρησιμοποιούσαν ισχυρούς κωδικούς (εάν δεν το έκαναν μέχρι στιγμής), εάν θα χρησιμοποιούσαν κάποια ακόμα μέθοδο αυθεντικοποίησης όπως με την χρήση βιομετρικών χαρακτηριστικών. Ακόμα, ερωτήθηκε εάν θεωρούν τις συχνές ενημερώσεις της συσκευής τους και την αλλαγή των προεπιλεγμένων ρυθμίσεων σημαντικές. Και τέλος, αν θεωρούν ότι είναι αναγκαίο να γνωρίζουν τις άδειες και δεδομένα που χρησιμοποιεί η συσκευή τους.



Εικόνα 31. Δωδέκατη ερώτηση, σχετική με την χρήση ισχυρών κωδικών πρόσβασης στις συσκευές

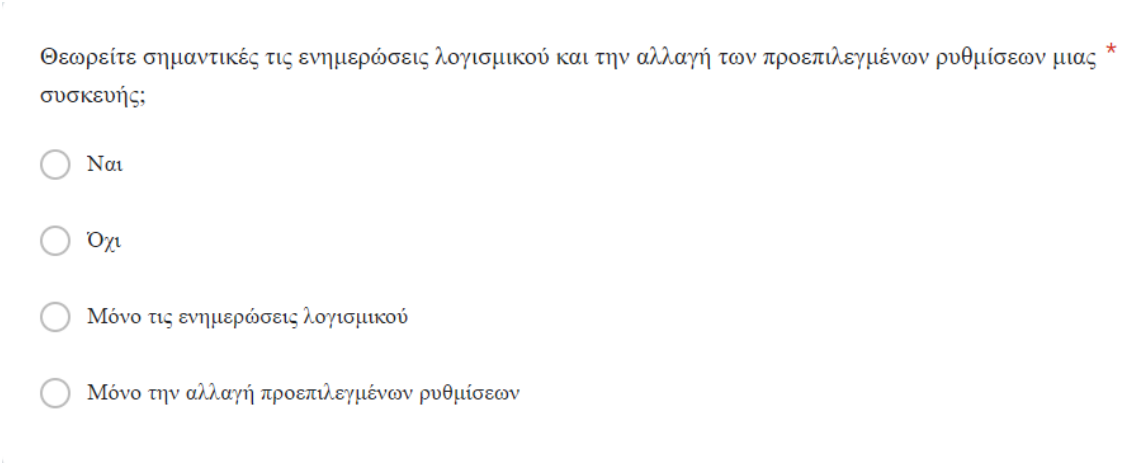


Εικόνα 32. Ποσοστά απαντήσεων δωδέκατης ερώτησης



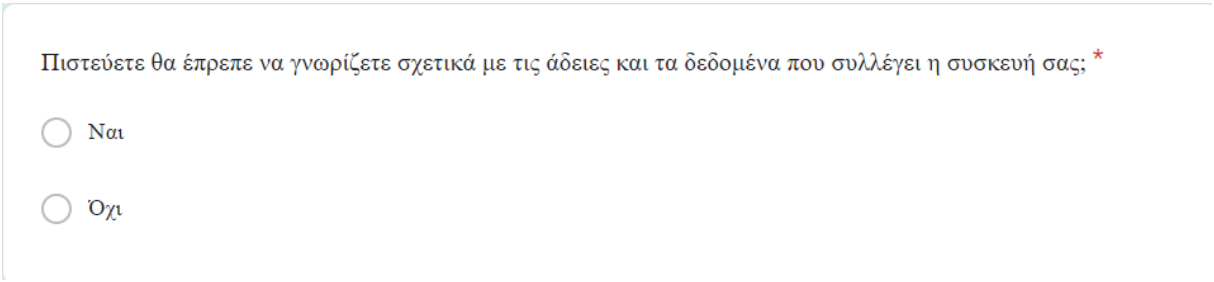
Εικόνα 33. Δέκατη τρίτη ερώτηση, σχετική με την αυθεντικοποίηση με χρήση βιομετρικών χαρακτηριστικών

Εικόνα 34. Ποσοστά απαντήσεων δέκατης τρίτης ερώτησης



Εικόνα 35. Δέκατη τέταρτη ερώτηση, σχετίζεται με την σημαντικότητα ενημερώσεων και αλλαγή των προεπιλεγμένων ρυθμίσεων των συσκευών

Εικόνα 36. Ποσοστά απαντήσεων δέκατης τέταρτης ερώτησης



Εικόνα 37. Δέκατη πέμπτη ερώτηση, σχετική με την σημαντικότητα γνώσης των αδειών και των δεδομένων που διαχειρίζεται κάθε συσκευή

Εικόνα 38. Ποσοστά απαντήσεων δέκατης πέμπτης ερώτησης

Κατά την συμπλήρωση των ερωτήσεων του ερωτηματολογίου, οι χρήστες έβλεπαν και σχετικά βίντεο για την επιπλέον ενημέρωση και ευαισθητοποίησή τους επί του θέματος. Δίνονται οι σχετικοί σύνδεσμοι των βίντεο, τα οποία πληρούσαν τα παρακάτω κριτήρια ώστε να επιλεχθούν. Αρχικά, δεν θα έπρεπε κατά την θέαση του βίντεο να διαφημίζεται κάποια εταιρία ή προϊόν για μεγάλο χρονικό διάστημα. Ακόμα, χρειαζόταν να ήταν σύντομα σε διάρκεια και περιεκτικά για να το παρακολουθήσει ολόκληρο ο ερωτηθέντας, και να αποκομίσει κάτι από αυτό. Τέλος, ένα από τα κριτήρια επιλογής ήταν η καλή ποιότητα εικόνας με σκοπό να είναι ευχάριστη η θέαση του βίντεο. Στο πρώτο βίντεο που παρουσιάστηκε, με σύνδεσμο https://youtu.be/q5DYkzOrz_I?si=GwFAs-kQ-TYIqDoY, περιέχονται πληροφορίες για την δημιουργία ισχυρών κωδικών πρόσβασης στις συσκευές, καθώς επιδεικνύονται και παραδείγματα, κάνοντας πιο διαδραστικό, ευχάριστο και περιεκτικό το περιεχόμενό του. Στο δεύτερο βίντεο, με σύνδεσμο https://youtu.be/3C7GoGRUCgw?si=yYke1IPA0kVpVrr8, παρουσιάζονται κάποιες έξυπνες οικιακές συσκευές και σημαντικές παραβιάσεις που μπορεί να πραγματοποιηθούν αν δεν προστατευτούν. Περιγράφονται περιστατικά που συνέβησαν σε αφύλακτες έξυπνες συσκευές καθώς και κάποιους λόγους για τους οποίους πολλές συσκευές δεν προστατεύονται. Παραθέτονται σχετικά στατιστικά που επιδεικνύουν την σοβαρότητα του θέματος και τέλος, παρουσιάζονται πέντε απλά βήματα που αποσκοπούν στην βελτίωση της ασφάλειας των έξυπνων οικιακών συσκευών.