ΤΙΤΛΟΣ ΕΡΕΥΝΗΤΙΚΗΣ ΕΚΘΕΣΗΣ

Internet of Things

Υπόθεμα : «Προβληματισμός»

ΤΑ ΜΕΛΗ ΤΗΣ ΟΜΑΔΑΣ

Χαραλαμπάκη Γεωργία

Χατζηγεωργίου Κατερίνα

Χατζηπαντσούδη Χρύσα

Χρηστίδου Κλειώ

Χριστοδουλίδου Αναστασία

Επιβλέπουσα καθηγήτρια : Καλλιόπη Μαγδαληνού, ΠΕ19

ΠΡΟΒΛΗΜΑΤΙΣΜΟΙ ΤΟΥ INTERNET OF THINGS

Εισαγωγή

Ζούμε σε μία εποχή όπου τα πάντα κινούνται γύρω μας με ασύλληπτους πλέον ρυθμούς. Τα νέα επιτεύγματα της τεχνολογίας μεταβάλλουν καθημερινά το περιβάλλον στο οποίο ζούμε, με αποτέλεσμα να κατακλυζόμαστε διαρκώς από πληθώρα πληροφοριών, κυρίως λόγω της διάδοσης των τεχνολογιών της πληροφορικής και των επικοινωνιών. Οι τεχνολογίες αυτές έχουν εκμηδενίσει το χώρο και το χρόνο, φέρνοντας πιο κοντά ανθρώπους από κάθε γωνιά της γης.

Ευρήματα

Τρεις από τις κύριες ανησυχίες που συνοδεύουν το Ίντερνετ των πραγμάτων είναι η παραβίαση της ιδιωτικής ζωής, η υπερβολική εξάρτηση από την τεχνολογία, και η απώλεια θέσεων εργασίας. Όταν κάτι έχει τεθεί στο διαδίκτυο θα είναι πάντα εκεί. Φυσικά υπάρχουν και τα μέτρα ασφαλείας που λαμβάνονται για την προστασία των πληροφοριών, αλλά υπάρχει πάντα η δυνατότητα οι χάκερς να σπάσουν το σύστημα και να κλέψουν τα δεδομένα. Για παράδειγμα, Ανώνυμος είναι μια ομάδα ατόμων που χακάρουν ομοσπονδιακούς χώρους και κυκλοφορούν εμπιστευτικές πληροφορίες στο κοινό.

Ένα άλλο επιχείρημα κατά του IoT είναι η υπερβολική εξάρτηση από την τεχνολογία. Δεδομένου ότι οι εποχές έχουν αλλάξει, η σημερινή γενιά μας έχει μεγαλώσει με την άμεση διαθεσιμότητα του Διαδικτύου και της τεχνολογίας γενικότερα. Ωστόσο, στηριζόμενη στην τεχνολογία σε καθημερινή βάση, η λήψη αποφάσεων από τις πληροφορίες που δίνει μπορεί να οδηγήσει μέχρι και σε καταστροφή. Κανένα σύστημα δεν είναι ισχυρό και απρόσκοπτο. Βλέπουμε δυσλειτουργίες που συμβαίνουν συνεχώς στην τεχνολογία, ειδικά στο διαδίκτυο. Ανάλογα με το ποσό που επικαλείται ο ιδιώτης στις πληροφορίες που παρέχονται θα μπορούσε να ζημιώνεται αν το σύστημα καταρρέει. Όσο περισσότερο εμπιστευόμαστε τόσο πιο εξαρτημένοι είμαστε στο Διαδίκτυο.

Τέλος, η σύνδεση των όλο και περισσότερων συσκευών με το Διαδίκτυο θα έχει ως αποτέλεσμα την απώλεια θέσεων εργασίας. Η αυτοματοποίηση του IoT "θα έχει καταστροφικές συνέπειες για τις προοπτικές απασχόλησης των λιγότερο μορφωμένων εργαζομένων» (Schumpeter, 2010). Για παράδειγμα, οι άνθρωποι που την αποτίμηση των αποθεμάτων θα χάσουν τη δουλειά τους, επειδή οι συσκευές μπορούν όχι μόνο να επικοινωνούν μεταξύ τους, αλλά και να διαβιβάζουν τις πληροφορίες για τον ιδιοκτήτη. Τα μειονεκτήματα αυτά μπορεί να είναι σε μεγάλο βαθμό καταστροφικά για την κοινωνία στο σύνολό της, καθώς και για τα άτομα και τους καταναλωτές.

Σύμφωνα με την έρευνα της Ομοσπονδιακής Επιτροπής Εμπορίου (FTC)**, η έλλειψη διαθέσιμων ενημερώσεων και patches ασφαλείας.** Η έκθεση αναφέρει ότι, οι επιχειρήσεις μπορεί να μην έχουν κίνητρο να στηρίξουν ενημερώσεις λογισμικού για

όλη την ωφέλιμη διάρκεια ζωής των συσκευών αυτών, ενδεχομένως αφήνοντας τους καταναλωτές με ευάλωτες συσκευές. Επιπλέον, μπορεί να είναι δύσκολο ή αδύνατο να εφαρμοστούν ανανεωμένες εκδόσεις σε ορισμένες συσκευές.

Συσκευές με σκληρό-κωδικοποιημένες κωδικούς πρόσβασης. "Καθώς οι συσκευές IoT προσφέρουν νέες ευκαιρίες για τους καταναλωτές να παρακολουθούν τις καθημερινές δραστηριότητές τους, πρόσβαση σε περιεχόμενο, και να αλληλεπιδρούν με τον κόσμο, αυτές οι συσκευές δημιουργούν επίσης νέες ευκαιρίες για μη εξουσιοδοτημένα άτομα να εκμεταλλεύονται τα τρωτά σημεία που μπορούν να διευκολύνουν την κλοπή ταυτότητας ή απάτης», λέει η FTC.

Διευκόλυνση επιθέσεις σε άλλα συστήματα . Η FTC ανησυχεί ότι IoT συνδεδεμένες συσκευές μπορούν να χρησιμοποιηθούν κακόβουλα εναντίον του καταναλωτή σε μια έναρξη επίθεση άρνησης υπηρεσίας (DDoS) ή ηλεκτρονικού ταχυδρομείου phising.

Υποκλοπές συσκευή . Η FTC τόνισε επίσης ανησυχίες ότι ένας κατασκευαστής ή ένας εισβολέας θα μπορούσε να σας ακούσει από απόσταση μέσα στο δικό σας σπίτι. Αυτό αποτελεί κυρίως μεγάλη ανησυχία για συσκευές με ένα μικρόφωνο και τις συσκευές που διαθέτουν κάμερα.

Τρόποι για να προστατεύσουμε τις συσκευές μας

1. Κωδικοί πρόσβασης: Νούμερο ένα tip για την εξασφάλιση IoT αντικείμενα είναι η προστασία με μοναδικούς και σύνθετους κωδικούς πρόσβασης . Αν δεν το έχετε ήδη κάνει, φροντίστε να προστατεύσετε με κωδικό πρόσβασης τις ρυθμίσεις του δρομολογητή σας, καθώς και τα Wi-Fi της σύνδεσης. Χρησιμοποιήστε ισχυρούς κωδικούς πρόσβασης για όλες τις Internet-συνδεδεμένες συσκευές, συμπεριλαμβανομένων συσκευές παρακολούθησης μωρού, καφετιέρες και κάμερες. Θα πρέπει να γνωρίζετε ότι πολλά αντικείμενα IoT ξεκινήσει υπηρεσία με γενική προεπιλογή κωδικούς πρόσβασης που οι ιδιοκτήτες θα πρέπει να αλλάξετε με το χέρι πριν από την τοποθέτηση των αντικειμένων σε χρήση. Default κωδικούς πρόσβασης συχνά γράφονται στον πηγαίο κώδικα ενός αντικειμένου IoT και μπορεί να ληφθεί εύκολα από τους χάκερ.

2. Εγκαταστήστε τον κωδικό πρόσβασης λογισμικό διαχείρισης, όπως το **Dashlane** , σε υπολογιστές, ταμπλέτες και smartphones για την αποθήκευση και εύκολη πρόσβαση σε κωδικούς πρόσβασης σε προγράμματα περιήγησης, εφαρμογές και online τραπεζικές συναλλαγές. Το Dashlane έχει αξιολογηθεί ως ο καλύτερος password manager. Μπορεί να συγχρονίσει τα διαπιστευτήριά σας σε όλες αυτές τις συσκευές, αλλά και να συμβάλει στη δημιουργία ισχυρών κωδικών πρόσβασης.

3. Εγκαταστήστε antivirus και anti-malware λογισμικό για υπολογιστές και φορητές συσκευές.

4. Συχνά ελέγξετε για ενημερώσεις ασφαλείας λογισμικού.

5. Ρυθμίστε τις συνδέσεις Bluetooth για φορητούς υπολογιστές και κινητά τηλέφωνα για να "μην εντοπιστούν", όταν είναι σε πολυσύχναστα μέρη, όπως αεροδρόμια, καφετέριες και άλλους δημόσιους χώρους όπου υπάρχει κίνδυνος, άλλος αντίστοιχος χρήστης με τη συσκευή σας να το hackαρει για πληροφορίες. Καλύτερα ακόμα, όταν δεν βρίσκονται σε χρήση, απενεργοποιήστε συνδέσεις Bluetooth στις συσκευές σας.

Σύνοψη - Συμπεράσματα

Για την δημιουργία της εργασίας μας, αρχικά ψάξαμε πληροφορίες για τον προβληματισμό του Internet of Things και βρήκαμε εικόνες. Ύστερα, με τις πληροφορίες που βρήκαμε γράψαμε την έκθεση της εργασίας και μετά φτιάξαμε το Power Point.

Ιστογραφία :
https://dspace.lib.uom.gr/bitstream/2159/14896/6/PapageorgiouIoannaMsc2012.pdf

ΠΑΡΑΡΤΗΜΑ Α

ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ Β6

1) Γνωρίζετε τι είναι το IOT (Internet Of Things);
☐ Ναι ☐ Όχι ☐ Δεν Ξέρω

2) Πιστεύετε ότι θα βοηθήσει στην εξέλιξη της τεχνολογίας ;
☐ Ναι ☐ Όχι ☐ Δεν Ξέρω

3) Γνωρίζετε αν υπάρχουν οικιακές συσκευές που συνδέονται στο Διαδίκτυο;
☐ Ναι ☐ Όχι ☐ Δεν Ξέρω

4) Γνωρίζετε τι είναι Smart Cities ;
☐ Ναι ☐ Όχι ☐ Δεν Ξέρω

5) Μπορεί το IOT να είναι επικίνδυνο για τα προσωπικά μας δεδομένα;
☐ Ναι ☐ Όχι ☐ Δεν Ξέρω

6) Είναι αρκετά αξιόπιστο;
☐ Ναι ☐ Όχι ☐ Δεν Ξέρω

7) Θεωρείτε ότι είναι ασφαλές;
☐ Ναι ☐ Όχι ☐ Δεν Ξέρω

8) Γνωρίζετε αν υπάρχουν gadgets που να λειτουργούν με σύνδεση στο διαδίκτυο ;
☐ Ναι ☐ Όχι ☐ Δεν Ξέρω

9) Γνωρίζετε τι είναι το Smart Home;
☐ Ναι ☐ Όχι ☐ Δεν Ξέρω

11) Πρόσφατα η Bosch δημιούργησε ένα ψυγείο που ζυγίζει το βάρος των προϊόντων της. Αν λείπει κάτι, κάνει αυτόματα παραγγελία . Θεωρείτε ότι μπορεί να ζημιώσει αυτό τον καταναλωτή;
☐ Ναι ☐ Όχι ☐ Δεν Ξέρω

12) Θεωρείτε ότι το διαδίκτυο με αυτή την λειτουργία μπορεί πραγματικά να μας βοηθήσει;
☐ Ναι ☐ Όχι ☐ Δεν Ξέρω