Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή

Στην Ασφάλεια Υπολογιστών και Δικτύων

" Ανάπτυξη ενός μοντέλου για διαχείριση ταυτότητας στα διάχυτα δίκτυα μικρομεσαίων επιχειρήσεων"

Όνομα Επώνυμο: Παναγιώτης Πιερή

Επιβλέπουσα Καθηγήτρια :
Αδαμαντίνη Περατικού

Μήνας Έτος 12/2018

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Ασφάλεια Υπολογιστών και Δικτύων

Τίτλος : " Ανάπτυξη ενός μοντέλου για διαχείριση ταυτότητας στα διάχυτα δίκτυα μικρομεσαίων επιχειρήσεων"

Παναγιώτης Πιερή

Επιβλέπουσα Καθηγήτρια
Αδαμαντίνη Περατικού

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Δεκέμβριος 2018

Περίληψη

Η υιοθέτηση από τις κυπριακές μικρομεσαίες επιχειρήσεις IoT συσκευών, αποτελεί σημαντικό γεγονός, βοηθώντας τις να αντιμετωπίσουν τις αυξανόμενες απαιτήσεις των πελατών και την εξέλιξη των παρεχόμενων υπηρεσιών τους. Ωστόσο, η ταυτοποίηση των χρηστών για σύνδεσή τους στο εταιρικό δίκτυο είναι αναγκαία προϋπόθεση, για τη διασφάλιση του δικτύου, των δεδομένων και των πληροφοριών. Το κίνητρο για τη διεξαγωγή αυτής της έρευνας είναι η έλλειψη βιώσιμων, ευέλικτων λύσεων και μηχανισμών αναγνώρισής και ταυτοποίησης των IoT συσκευών γενικότερα στα εταιρικά δίκτυα .

Η παρούσα μελέτη έχει ως στόχο να ερευνήσει τις διαδικασίες και τις μεθόδους που εφαρμόζονται από τις κυπριακές μικρομεσαίες επιχειρήσεις, έχοντας ως δεδομένο την πολυπλοκότητα που παρουσιάζεται σε οποιοδήποτε εταιρικό δίκτυο, το οποίο φιλοξενεί IoT συσκευές λόγω των πολλαπλών παραγόντων που τις διέπουν, τους διαφαινόμενους περιορισμούς και τους επιπροσθέτους αυξανομένους κίνδυνους. Η συλλογή δεδομένων από τις μικρομεσαίες επιχειρήσεις έγινε με βάση ερωτηματολόγιο και η ανάλυση των αποτελεσμάτων, με τη χρήση στατιστικής ανάλυσης δεδομένων μέσω του SPSS. Επίσης, έχουν εξαχθεί συμπεράσματα, τα οποία έχουν αναδείξει την ανάγκη υλοποίησης και αξιολόγησης ενός η κάποιων συνδυασμών των προτεινομένων μοντέλων. Η διαχείριση ταυτοποίησης και πρόσβασης αποτελεί μια συνεχή πρόκληση για το δίκτυο της επιχείρησης. Ωστόσο η αναγκαιότητα επικαιροποίησης και αναβάθμισης αποτελεί βασικό κομμάτι, τόσο στην ασφάλεια του δικτύου και των πληροφοριών που διακινούνται σε αυτό, όσο και στην ιδιωτικότητα και την προστασία των προσωπικών δεδομένων των χρηστών.

Συμπερασματικά, η συνεχομένη εξέλιξη στον τομέα της ένταξης των IoT συσκευών στα εταιρικά δίκτυα ευνοεί την ανάγκη όλο και περισσοτέρων πεδίων έρευνας για διαχείριση ταυτοποίησης στα διάχυτα δίκτυα μικρομεσαίων επιχειρήσεων.

Summary

The adoption of the IoT devices by small and medium-sized enterprises in Cyprus is an important factor as it helps to cope with the increasing demands of customers and the development of their provided services. However, the user identification mechanism that allows the connection to the corporate network is a prerequisite for securing the network, data and information. The incentive for the conduct of this research is the lack of viable and flexible solutions that address some of the key factors in technology.

This study focuses in investigating the procedures and methods applied by the small and medium-sized enterprises in Cyprus which host the IoT devices as it leads to a complexity presented in any corporate network. This is an outcome due to the multiple factors that affect each network such as the apparent constraints and the additional increasing risks of using the IoT devices. The data collection method used was a survey which was provided to a number of small and medium-sized enterprises in Cyprus, the results were analysed through a statistical analysis with the use of SPSS software.

Conclusions have been drawn, which have shown the need to implement and evaluate a certain combination of the proposed models. The identification and access management is a constant challenge for the enterprise’s network since the necessity of updating and upgrading acts as the key factor in the network security, the information that flows in it, the privacy and the protection of the users' personal data.

In conclusion, the incessant development in the integration field of the IoT devices in the corporate networks favors the need for conducting further research in order to manage the identification in the diffuse networks of small and medium-sized enterprises.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά την καθηγήτρια μου κα Αδαμαντίνη Περατικού, τόσο για την προτροπή της να εντρυφήσω με το συγκεκριμένο θέμα, όσο και τη γενική στήριξη, καθοδήγηση και επίβλεψή της, καθ' όλη τη διάρκεια εκπόνησης της εργασίας μου. Επιπρόσθετα, ευχαριστώ την οικογένειά μου και ιδιαίτερα τη σύζυγό μου Αγάθη για τη συμπαράστασή της κατά τη διάρκεια του εν λόγω μεταπτυχιακού προγράμματος, καθώς και τα δύο μου παιδιά Ανδρέα και Δώρα για την κατανόησή τους, λόγω του περιορισμένου χρόνου που τους αφιέρωνα.

Περιεχόμενα

Περιεχόμενα - Εικόνες

Περιεχόμενα - Πίνακες

Περιεχόμενα - Διαγράμματα

Κεφάλαιο 1
Αναλυτικότερη πρόταση

1.1 Εισαγωγή

Η χρήση των συσκευών που χρησιμοποιούμε στην καθημερινότητα μας όπως είναι τα έξυπνα τηλεφωνά, έξυπνα ρολόγια, Tablets, φορητοί υπολογιστές, συστήματα αυτοκίνητων κλπ, φέρουν εφαρμογές οι οποίες έχουν κατασκευαστεί με σκοπό τη ψυχαγωγία, επικοινωνία, ανταλλαγή αρχείων. Οι συσκευές αυτές επιτρέπουν την εγκατάσταση εφαρμογών, οπού οι κατασκευαστές των εφαρμογών αυτών στις πλείστες περιπτώσεις δε δίνουν μεγάλη έμφαση στην ασφάλεια των δεδομένων και ορισμένες εφαρμογές επιτρέπουν ακόμη και απομακρυσμένο έλεγχο, τόσο των ιδίων των εφαρμογών , όσο και πλήρη πρόσβαση στις ιδίες τις συσκευές (Root Access). Έχουν εντοπιστεί εφαρμογές που φέρουν κακόβουλο κώδικα με αποτέλεσμα την υποκλοπή δεδομένων.

Με την τεράστια αύξηση των συσκευών - που χρησιμοποιούνται στην καθημερινότητα μας, όλο και περισσότεροι χρήστες είναι αυτοί που επιθυμούν τη χρήση τους στο εργασιακό τους χώρο, υπάρχουν επίσης εργοδοτούμενοι οι οποίοι θεωρούν

πως δεν υπάρχει διαχωρισμός της προσωπικής και επαγγελματικής τους ζωής. Σιγουρά υπάρχει μεγάλη εξάρτηση των χρηστών με τις συσκευές τους που τείνει αναπόφευκτά να αποτελεί αναπόσπαστο μέρος του εταιρικού δικτύου η χρήση αυτών των συσκευών μπορεί να φέρει θετικά αποτελέσματα όπως είναι η αυξημένη αποδοτικότητα των εργοδοτούμενων και η αμεσότητα σε πληροφορίες που χρειάζονται για διεκπεραίωση των εργασιών τους.

1.2 Σκοπός Έρευνας

Σκοπός της μελέτης είναι να διαπιστωθεί κατά ποσό υπάρχει στο δίκτυο των μικρομεσαίων επιχειρήσεων η απαραίτητη υποδομή για ταυτοποίηση, προσβασιμότητα, προστασία των πληροφοριών και των δεδομένων της από συσκευές που πιθανόν να αποκτούν διαδικτυακή πρόσβαση, είτε αυτοί είναι υπάλληλοι, είτε είναι φιλοξενούμενοι στην επιχείρηση μέσω των προσωπικών τους συσκευών.

Κυρίος στόχος αυτής της έρευνας είναι να προσδιορίσει και να προτείνει ένα πρότυπο για τη διαχείριση ταυτότητας των διάχυτων συστημάτων με διαδικτυακή πρόσβαση, σε ένα εταιρικό περιβάλλον. Το κίνητρο για τη διεξαγωγή αυτής της έρευνας είναι η έλλειψη βιώσιμων και ευέλικτων λύσεων που να αντιμετωπίζουν μερικούς από τους βασικούς παράγοντες της τεχνολογίας. Παρόλο που υπάρχουν διαθέσιμες λύσεις διαχείρισης ταυτότητας για τις συσκευές IoT, χρειάζονται βελτίωση. Το πλήρες δυναμικό του IoT είναι να προχωρήσει πέρα από τα enterprise centric συστήματα και να πορευτεί προς μια προσέγγιση με γνώμονα τον χρήστη (user centric).

Από τη μελέτη αυτή αναμένεται ότι κάποιες εταιρίες είτε δεν παρέχουν καθόλου πρόσβαση στο δίκτυο τους σε αυτές τις φιλοξενούμενές συσκευές , είτε κάποιες άλλες παρέχουν αντί το εταιρικό τους δίκτυο, οικιακή σύνδεση διαδικτύου, είτε προσφέρουν πρόσβαση στο εταιρικό τους δίκτυο χωρίς να εφαρμόζουν κάποιο ολοκληρωμένο σύστημα ταυτοποίησης του χρήστη που επιθυμεί να συνδέσει την προσωπική του συσκευή, με αποτέλεσμα να μην υπάρχει ασφάλεια στο εταιρικό τους δίκτυο και παράλληλα χωρίς να υπάρχει παρακολούθηση-monitoring για τα δεδομένα ή κάποιο σύστημα εντοπισμού επίθεσης.

1.3 Βασικά ερευνητικά ερωτήματα:

Τα ερευνητικά ερωτήματα της μελέτης βασίζονται σε μικρομεσαίες επιχειρήσεις στην Κύπρο.

1) Εφαρμόζεται κάποιο μοντέλο ταυτοποίησης, προσπέλασης και εξουσιοδότησης από εξωτερικές -φιλοξενούμενες συσκευές;
2) Πώς διασφαλίζεται η ταυτοποίηση του χρήστη μέσω τον προσωπικών του συσκευών;
3) Ο χρήστης που χρησιμοποιεί το εταιρικό δίκτυο από τον εταιρικό εξοπλισμό, έχει την ίδια ταυτοποίηση – Profile σε περίπτωση που θα αποκτούσε πρόσβαση από προσωπική του συσκευή;
4) Ο χρήστης που χρησιμοποιεί το εταιρικό δίκτυο από τον εταιρικό εξοπλισμό, έχει τα ίδια δικαιώματα και προσβασιμότητα στα δεδομένα της εταιρίας σε περίπτωση που χρησιμοποιεί προσωπικές του συσκευές;
5) Οι χρήστες που χρησιμοποιούν τις προσωπικές τους συσκευές έχουν την ίδια ταυτοποίηση, δηλαδή το ίδιο Profile;

1.4 Αναγκαιότητα και σπουδαιότητα της έρευνας:

"Ανάπτυξη ενός μοντέλου για διαχείριση ταυτότητας στα διάχυτα δίκτυα μικρομεσαίων επιχειρήσεων". Με την όλο και αυξανομένη χρήση των συσκευών και την ανάγκη των χρηστών για τη χρήση του διαδικτύου μέσω των προσωπικών τους συσκευών, γίνεται όλο και πιο επιτακτική η ανάγκη για προστασία του εταιρικού δικτύου, όσο και για ικανοποίηση της ανάγκης των χρηστών για πρόσβαση. Όλο και περισσότεροι εργοδοτούμενοι επιθυμούν τη χρήση των προσωπικών τους συσκευών, κυρίως επειδή τις θεωρούν πιο απλές και άμεσες για τη διεξαγωγή ακόμη και επαγγελματικών καθηκόντων τους, είναι αρκετά σημαντικό να υπάρχει ευελιξία σε αυτό το τομέα επειδή με αυτό το τρόπο εκσυγχρονίζονται και οι παρεχόμενες υπηρεσίες μιας επιχείρησης όπως είναι η επικοινωνία εκτός από φωνή, εικόνα και διαμερισμό αρχείων. Θα πρέπει ο διαχειριστής του δικτύου να είναι σε θέση να παρέχει και να έχει εξασφαλίσει την ταυτοποίηση του δικτύου είτε με λογισμικά-software είτε και υλικά -Hardware, ακόμη και με συνδυασμό των δυο λαμβάνοντας υπόψη τα διαφορά λειτουργικά συστήματα πχ. Android, iOS, Linux οπού έχει σαν αποτέλεσμα την αύξηση της πολυπλοκότητα του συστήματος καθώς και της ασυμβατότητας. Ένα άλλο σημαντικό πρόβλημα που προκύπτει, λόγω των διαφορετικών

λειτουργικών και εκδόσεων τους, είναι ότι το κάθε ένα έχει διαφορετικές ευπάθειες, διαφορετικούς ιούς και διαφορετικό τρόπο συμπεριφοράς στην κάθε πλατφόρμα. Εντοπίζεται πρόβλημα στο οποίο οι πλείστες συσκευές μετα από κάποιο χρονικό διάστημα, παύουν να έχουν οποιαδήποτε υποστήριξη από την κατασκευάστρια εταιρεία με αποτέλεσμα αυτές οι συσκευές να μένουν ευάλωτες και χωρίς οποιαδήποτε αναβάθμιση ασφάλειας ως προς τις αδυναμίες που συνεχώς εντοπίζονται και εκμεταλλεύονται κακόβουλα από άτομα. Επιπρόσθετα, υπάρχει η απαραίτητη υποδομή στο δίκτυο των επιχειρήσεων για εντοπισμό των ιών, σκουληκιών - warms, δουρείων ίππων - trojan horse, εξωτερικών επιθέσεων από τα λειτουργικά που εφαρμόζονται στις εξωτερικές συσκευές;. Υπάρχει τρόπος να εντοπιστεί από τα συστήματα άμυνας του δικτύου ώστε να μπορεί να ταυτοποίηση την εξωτερική συσκευή που στέλνει ή λαμβάνει δεδομένα ανά πασά στιγμή;. Θα πρέπει ο διαχειριστής του δικτύου να καθορίσει την προσβασιμότητα στα αρχεία του δικτύου της επιχείρησης από τέτοιες συσκευές καθώς θα πρέπει να διασφαλιστούν όλες οι ευαίσθητες πληροφορίες. Άλλη επίπτωση που πιθανό να παρουσιαστεί είναι η ανεξέλεγκτη διόγκωση του δικτύου από τη χρήση των προσωπικών συσκευών με αποτέλεσμα να μην μπορεί να διασφαλιστεί πλήρως η ασφάλεια του δικτύου.

Η ταυτοποίησή μπορεί να επιτευχθεί μέσω της εταιρικής ιστοσελίδας Intranet, ακολούθως με τη χρήση κωδίκων πρόσβασης. Άλλος τρόπος θα μπορούσε να είναι με τη χρήση κριτήριων που θα αφορά username, password, την τοποθεσία (GPS) και χρονική στιγμή (π.χ. ώρες εργασίας). Εναλλακτική μέθοδος θα μπορούσε να είναι αυτή της αναγνώρισης μέσω βιομετρικών συστημάτων, δηλαδή μέσω φωνητικής αναγνώρισης, δακτυλικού αποτυχόντος , αναγνώριση προσώπου και ίριδας του ματιού οπού είναι τεχνολογίες που ήδη υπάρχουν προ εγκατεστημένοι αισθητήρες στις σύγχρονες προσωπικές συσκευές. Επίσης, εναλλακτικός τρόπος ταυτοποίησης χρήστη που επιθυμεί να συνδεθεί από προσωπική του συσκευή στο δίκτυο της επιχειρήσεις είναι μέσω προγραμματισμού του access point σε RADIUS όπου θα απαιτείται από τη συσκευή που θα έχει σύνδεση WIFI εγκατάσταση αρχείου πιστοποίησης και θα υπάρχει ήδη ρυθμισμένο από τον IT της εταιρείας με καθορισμένο τα στοιχεία και τα δικαιώματα πρόσβασης του χρήστη για τα δεδομένα που βρίσκονται στο Server.

Κεφαλαίο 2
Βιβλιογραφική επισκόπηση

Εννοιολογική έννοια του Internet of Things (IoT).

Ο Kevin Ashton [01] είναι ο εμπνευστής του όρου Internet of Things όταν το 1999 ως συνιδρυτής της εταιρείας Auto-ID Center είχε ως στόχο τη χρήση της ετικέτας RFID σε συνδυασμό με αισθητήρες εγκατεστημένους σε αντικείμενα οι οποίοι θα επέτρεπαν την επικοινωνία και την αλληλεπίδραση μεταξύ των διάφορων συσκευών, μέσω της χρήσης του διαδικτύου.

Με τη συνεχομένη εξέλιξη και εξάπλωση του διαδικτύου, έχουν επίσης αναπτυχθεί με γρήγορους ρυθμούς και οι συσκευές που χρησιμοποιούμε στην καθημερινότητα μας, ώστε να υποστηρίζουν συνδεσιμότητα στο διαδίκτυο μέσω ethernet ή ασυρμάτου δικτύου, με τη χρήση των πρωτοκόλλων TCP, UDP και Point to Point, Bluetooth, Near Field Communication (NFC) και το πρωτόκολλο IEEE 802.15.4 από τη Zigbee. Επιπρόσθετα, οι συσκευές είναι εφοδιασμένες με διάφορους αισθητήρες (φωτός, υγρασίας, κίνησης, θερμότητας κλπ), ώστε να συλλέγουν δεδομένα σχετικά με τα περιβάλλοντα στα οποία εγκαθίσταται, καθώς και την κατάσταση της συσκευής, σε συνδυασμό με τη διαδικτυακή σύνδεση για να υπάρχει επικοινωνία με το χρήστη. Αυτό τις καθιστά ως έξυπνες αυτόνομες συσκευές με περιορισμένη νοημοσύνη. Ο απώτερος στόχος για τις IoT συσκευές δεν αφορά μόνο τις συσκευές επικοινωνίας, αλλά και

οποιοδήποτε φυσικό αντικείμενο να μπορεί να συνδεθεί και να ελέγχεται μέσω του διαδικτύου. Συγκεκριμένα,[02] η χρήση πολλών και διαφορετικών αντικείμενων με δυνατότητες επικοινωνίας, αλληλεπίδρασης και συνεργασίας μεταξύ τους για την επίτευξη ενός κοινού σκοπού. Ένα τέτοιο δίκτυο από αυτονόμους αισθητήρες και τη συγκέντρωση των δεδομένων τους σε συγκεκριμένη τοποθεσία ονομάζεται ασύρματο δίκτυο αισθητήρων WSN – Wireless Sensor Network

Έξυπνες συσκευές είναι αυτές με διαφορετικές δυνατότητες, όπου αποτελούνται από το λογισμικό, το μικροεπεξεργαστή, με δυνατότητα διασύνδεσης και ένα σύνολο αισθητήρων, που συλλέγουν πληροφορίες, οι οποίες πληροφορίες αποστέλλονται είτε σε προκαθορισμένο Cloud Server της κατασκευάστριας εταιρεία της IoT συσκευής όπου και αναλύονται, είτε μέσω του προγράμματος της εφαρμογής, όπου σε συνδυασμό του μικροεπεξεργαστή με το λογισμικό επιτυγχάνεται η επεξεργασία και ανάλογα με τον προγραμματισμό τους, εξάγουν αποτελέσματα.

Επίσης, θα πρέπει να αναφέρουμε ότι στις IoT συσκευές πρωταρχικό ρολό έχει ο χρήστης, διότι αυτός ορίζει τον προγραμματισμό με τη χρήση αυτοματοποιημένων ρυθμίσεων ,οι οποίες υπάρχουν προκαθορισμένες στην εφαρμογή της IoT συσκευής και αποκωδικοποιεί τον τρόπο που θα λειτουργεί η συσκευή. Ακολούθως αυτές οι ρυθμίσεις εκτελούνται και εφαρμόζονται με τη μορφή εντολών στους αισθητήρες της συσκευής.

Η ανάπτυξη των έξυπνων συσκευών με τη χρήση διάφορων αισθητήρων έχει όλο και πιο μεγάλη διείσδυση στη ανθρώπινή μας ύπαρξη, όπως είναι οι συσκευές wearable οι οποίες καταγράφουν τις καθημερινές μας δραστηριότητες, αναλύοντας τους παλμούς της καρδιάς, το χάσιμο των θερμίδων σε συνδυασμό με τις καιρικές συνθήκες, τη διαλυομένη απόσταση, το υψόμετρο κλπ. Με τα αποτελέσματα των διάφορων αισθητήρων, γίνεται ανάλυση των πληροφοριών που έχουν συλλεχθεί από τον κάθε αισθητήρα ξεχωριστά και δημιουργείται μια κατάσταση για την ανθρώπινή υγεία, δίνοντας στον ιατρό του χρήστη πληροφορίες σχετικές με την υγειά του πελάτη του, καθώς αποτελεί αναπόσπαστο μέρος της σύγχρονης ιατρικής, όπως είναι η τηλεϊατρική.

Στόχος των IoT συσκευών είναι να διευκολύνουν τη καθημερινότητά μας, παρέχοντας πληροφορίες μέσω των αισθητήρων και την αλληλεπίδραση τους μεταξύ μίας γκάμας διάφορων συμβατών συσκευών, σε ένα πιο γενικό πληροφοριακό σύστημα δημιουργώντας νέες κατηγορίες, που απορρέουν από τις έξυπνες συσκευές οδηγώντας μας σε ένα πιο εξελιγμένο και αυτοματοποιημένο περιβάλλον όπως είναι η δημιουργία των έξυπνων μηχανημάτων, τα έξυπνα σπίτια, οι έξυπνες πόλεις και τα έξυπνα

αυτοκίνητα. Ο έλεγχος των IoT συσκευών επιτυγχάνεται, είτε μέσω browser από υπολογιστή ή έξυπνο τηλέφωνο , είτε μέσω εφαρμογής από Android και IOS λειτουργικά τα οποία είναι και τα πιο διαδεδομένα λειτουργικά στα έξυπνα τηλεφωνά.

Η ένταξη IoT συσκευών σε μια εταιρία, μπορεί να διαδραματίσει ένα νέο ρολό στις επιχειρηματικές δραστηριότητες της. Για παράδειγμα η χρήση ετικετών αναγνώρισης με τη χρήση ραδιοσυχνοτήτων θα μπορούσε να παρέχει τις απαραίτητες πληροφορίες σχετικά με την παρακολούθηση τις τοποθεσίας των προϊόντων της, το διαθέσιμο απόθεμα στις αποθήκες των προϊόντων μιας επιχείρησης η οποία ασχολείται με το εμπόριο. Σε επιχείρηση κατασκευαστικού τομέα, η χρήση των αισθητήρων θα μπορεί να συλλεγεί πληροφορίες σχετικές με την κατάσταση και τη συντήρηση των μηχανήματων παραγωγής. Η χρήση των Ιό συσκευών μπορούν να συμβάλουν στη βελτίωση της ποιότητας στο εργασιακό περιβάλλον παρέχοντας πληροφορίες σχετικές με την θερμοκρασία και τη ποιότητα του αέρα, με αποτέλεσμα την καλύτερη υγειά τον εργαζομένων.

Η ραγδαία ανάπτυξη των IoT συσκευών διαφαίνεται μέσα από την έρευνα της Gartner [03], οπού μέσα στο 2017 θα χρησιμοποιούνται 8,4 δισεκατομμύρια συσκευές. Αύξηση 31% σε σύγκριση με το 2016 και αναμένεται ότι μέχρι το 2020 θα υπάρχουν ανάμεσά μας 20,4 δισεκατομμύρια. Η αύξηση των IoT συσκευών δεν οφείλεται μόνο στην ευκολία και αμεσότητα που προσφέρουν στους χρήστες τους, αλλά και στους μικροεπεξεργαστές με ελάχιστες απαιτήσεις, τόσο σε ενέργεια, όσο και σε ικανοποιητική απόδοση. Ως αποτέλεσμα το χαμηλό κόστος κατασκευής, αλλά και απόκτησής τους ,έχει συμβάλει τα μέγιστα στη ζήτηση των συσκευών αυτών.

IoT Units Installed Base by Category (Millions of Units)

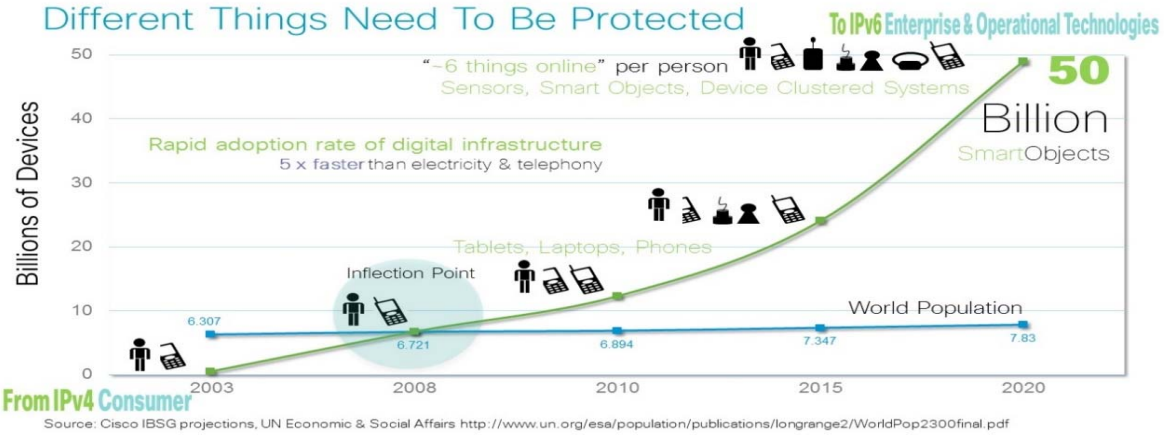
Εικόνα 1 - Εγκατεστημένες IoT συσκευές ανά κατηγορία.

Category	**2016**	**2017**	**2018**	**2020**
Consumer	3,963.0	5,244.3	7,036.3	12,863.0
Business: Cross-Industry	1,102.1	1,501.0	2,132.6	4,381.4
Business: Vertical-Specific	1,316.6	1,635.4	2,027.7	3,171.0
Grand Total	**6,381.8**	**8,380.6**	**11,196.6**	**20,415.4**

Source: Gartner (January 2017)

Σύμφωνα με την Cisco[04], με την αυξάνουσα ροή των IoT συσκευών μέχρι το 2020 θα υπάρχουν 50 δισεκατομμύρια συσκευές με αποτέλεσμα την εξάντληση των διευθύνσεων του IPv4 και την μετάβαση στο IPv6, ως εκ τούτου πρέπει να δοθεί έμφαση στο IPv6 σε σχέση με την ασφάλεια και της επιπτώσεις του.

Εικόνα 2 - Διάγραμμα αυξάνουσας ροής IoT συσκευών.



Source: cisco security-center

Η αποδοτικότητα και η αποτελεσματικότητα των IoT συσκευών [05] εξαρτώνται από την επιλογή εργαλείων ασφάλειας (IDS, ειδικού υλικού – hardware, επιπρόσθετες συσκευές κλπ), καθώς αλληλεπίδρασης που υπάρχει με άλλες συσκευές. Είναι πολύ σημαντικό να μπορεί να διασφαλιστεί η ακεραιότητα και η αξιοπιστία των ανταλλασσόμενων δεδομένων από πιθανές επιθέσεις λαμβάνοντας υπόψη τη διαφορετικότητα των συσκευών, των διαφορετικών εκδόσεων λογισμικών, των μικρό επεξεργαστών, με το κάθε ένα να έχει τις δικές του ευπάθειες. Πρόσφατη έρευνα της Kaspersky Lab[06], η οποία αφορά έξυπνες συσκευές που υπάρχουν σε ένα σπίτι, έχει διαπιστώσει ότι όσο περισσότερες έξυπνες συσκευές υπάρχουν, τόσο μεγαλύτερος είναι ο κίνδυνος διαρροής προσωπικών δεδομένων.

Απαράβατος κανόνας για την κάθε εταιρία είναι να μπορεί να ανταπεξέρχεται στις οποιεσδήποτε αλλαγές, εφαρμόζοντας νέες τεχνολογίες, οι οποίες θα είναι ικανές να τη βοηθήσουν να αυξάνει την παραγωγικότητα και την αποτελεσματικότητά της. Ο πιο σημαντικός παράγοντας στην εταιρία είναι το ανθρώπινο δυναμικό όπου, όλο και περισσότεροι εργοδοτούμενοι επιθυμούν τη χρήση των προσωπικών τους συσκευών, κυρίως επειδή τις θεωρούν πιο απλές και άμεσες για τη διεξαγωγή ακόμη και των επαγγελματικών σκοπών τους. Είναι αρκετά σημαντικό να υπάρχει ευελιξία σε αυτό τον

τομέα, επειδή με τον τρόπο αυτό εκσυγχρονίζονται και οι παρεχόμενες υπηρεσίες μιας επιχείρησης, όπως είναι η επικοινωνία εκτός από τη φωνή, την εικόνα και το διαμερισμό αρχείων.

Η ευκολία και η αμεσότητα που δίδεται στο χρήστη από τη χρήση των έξυπνων συσκευών, έχει καταστήσει στο άτομο θετική εξάρτηση με κύριο χαρακτηριστικό την εξοικονόμηση κόπου, χρόνου και παροχής άμεσης πληροφόρησης, χαρακτηριστικά που όλο και περισσότεροι χρήστες επιθυμούν να έχουν στον εργασιακό τους χώρο.

Υπάρχουν, επίσης, εργοδοτούμενοι, οι οποίοι θεωρούν πως δεν υπάρχει διαχωρισμός της προσωπικής και επαγγελματικής τους ζωής. Η μεγάλη εξάρτηση των χρηστών με τις συσκευές τους τείνει αναπόφευκτά να αποτελεί αναπόσπαστο μέρος του εταιρικού δικτύου. Η χρήση αυτών των συσκευών μπορεί να φέρει θετικά αποτελέσματα, όπως είναι η αυξημένη αποδοτικότητα των εργοδοτουμένων και η αμεσότητα σε πληροφορίες που χρειάζονται για διεκπεραίωση των εργασιών τους.

Επιπρόσθετα, [02]οι IoT συσκευές παρουσιάζουν προκλήσεις που θα πρέπει να επιλυθούν, με πιο σημαντική αυτή της ασφάλειας, της ιδιωτικότητας, τις προσωπικές ευαίσθητες πληροφορίες, την πληθώρα δεδομένων και την αρχιτεκτονική του δικτύου, σε συνδυασμό με την ενεργειακή απόδοση, των πρωτοκόλλων και της ποιότητας των υπηρεσιών. Οι συσκευές IoT θα πρέπει να ενισχυθούν σε σχέση με πιθανές επιθέσεις DoS και να μπορούν να κρυπτογραφούν τα δεδομένα, με τη χρήση κρυπτογραφημένων μπλοκ, ροής και ασύμμετρους μηχανισμούς.

Ένα μοντέλο που προτείνεται είναι το Risk-Adaptable Access Control (RAdAC) [7] σε συνδυασμό με τα παραδοσιακά δίκτυα Zero Trust Networking και το οποίο αφορά την προσβασιμότητα, με ένα σύστημα ελέγχου, που να μπορεί να μεταβάλλεται δυναμικά (Risk-Adaptable Access Control (RAdAC). Το RAdAC είναι ένα μοντέλο που σχεδιάστηκε για ιδιαίτερα μεταβλητά περιβάλλοντα, τα οποία απαιτούν μεγάλη ασφάλεια στο δίκτυο, είναι ανθεκτικό σε εξωτερικές επιθέσεις και η πρόσβαση που θα παρέχεται στην IoT συσκευή, θα είναι προσαρμοσμένη ανάλογα με το χρήστη και τη συσκευή, λαμβάνοντας υπόψη παράγοντες όπως είναι η τοποθεσία και το ιστορικό πρόσβασης. Η πρόταση και η σχεδίαση Framework είναι βασισμένη στο πλαίσιο ελέγχου πολιτικής πρόσβασης UCON [07] και χρήζει περεταίρω διερεύνησης, τόσο σε Zero Trust Networking, όσο και σε πιο σύγχρονα δίκτυα Cloud.

Έχει αναπτυχθεί το framework με την ονομασία Objective, Models, Architecture and Mechanisms (OM-AM)[08], το οποίο δίνει έμφαση στην εξουσιοδότηση. Το συγκεκριμένο

Framework εφαρμόζεται σε τέσσερα επίπεδα, όπως αυτά αναφέρονται στην ονομασία του. Objective – Υποκειμενικά, οτιδήποτε σχετίζεται με την ασφάλεια, τον έλεγχο και το επίπεδο της προσβασιμότητας. Authorization model – μοντέλο εξουσιοδότησης, το οποίο σε συνάρτηση με την πολιτική ασφάλειας που εφαρμόζεται, ανάλογα επιλέγεται το μοντέλο ή συνδυασμός μοντέλων εξουσιοδότησης και μηχανισμών ελέγχου πρόσβασης. Architecture – αρχιτεκτονική, που λαμβάνει υπόψη δυο παράγοντες την προσβασιμότητα και την πολιτική ασφάλειας. Mechanisms – μηχανισμοί, που είναι σχετικοί με λογισμικό και υλικό. Είναι τα εργαλεία, τα οποία εκτελούν μέσω ρυθμίσεων τις πολίτικες ελέγχου πρόσβασης, ασφάλειας και εξουσιοδότησης.

Η γνωστή εταιρεία Cisco[04], έχει σχεδιάσει ένα πλαίσιο ασφάλειας με ονομασία IoT/M2M που δίδει έμφαση σε τέσσερα επίπεδα: Authentication (πιστοποίηση), Authorization (εξουσιοδότηση), Network Enforced Policy (πολιτική δικτύωσης) και Secure Analytics: Visibility and Control (αναλυτικός έλεγχος: επίβλεψη και έλεγχος). Authentication (πιστοποίηση) μιας IoT συσκευής θα πρέπει να γίνεται αυτόματα από το δίκτυο με τη χρήση αναγνωριστικών, όπως είναι η αναγνώριση μέσω ραδιοσυχνοτήτων (RFID), shared secret, την πιστοποίηση X.509, την Mac διεύθυνση της συσκευής στο τελικό σημείο ή με άλλους τύπους ταυτοποίησης, βασιζόμενο σε μη εναλλασσόμενο hardware-υλικό, σε αντίθεση με την ταυτοποίηση που γίνεται σε άλλες συσκευές, με βάση την πιστοποίηση του χρήστη.

Η εξουσιοδότηση(Authorization), αφού επιτευχθεί πιστοποίηση της IoT συσκευής, τότε και μόνο δημιουργείται ένα αξιόπιστο κανάλι επικοινωνίας το οποίο θα επιτρέπει την ανταλλαγή πληροφοριών. Network Enforced Policy (πολιτική δικτύωσης) είναι η υποδομή και διαδρομή που μεταφέρονται τα δεδομένα. Secure Analytics: Visibility and Control (αναλυτικός έλεγχος: επίβλεψη και έλεγχος) όπου θα υπάρχει μια κεντρική πλατφόρμα - Massive Parallel Database (MPP) –η οποία θα συλλέγει μεγάλους όγκους δεδομένων, από όλες τις συνδεδεμένες συσκευές, με σκοπό την ανάλυση και τον έλεγχο των δεδομένων, καθώς και αναγνώριση και ανίχνευση απειλών.

Επιχειρηματικό δίκτυο [20] είναι ένα σύνολο συστημάτων και συσκευών τα οποία είναι σε θέση να επικοινωνούν μέσω πρωτοκόλλων επικοινωνίας, να παρέχουν και να ανακτούν πληροφορίες από τις βάσεις δεδομένων της εταιρείας. Επιπρόσθετα, όλα τα φυσικά συστήματα και συσκευές θα πρέπει να έχουν τη δυνατότητα να διατηρούν και να παρέχουν ικανοποιητικές επιδόσεις, αξιοπιστία και ασφάλεια. Ένα εταιρικό δίκτυο θα πρέπει να έχει ευέλικτη αρχιτεκτονική, [10] ώστε να μπορεί να προσαρμόζεται σε

αλλαγές και να δίνει δυνατότητες επεκτάσεις χωρίς να περιορίζει την ανάπτυξη και την ευημερία της επιχείρησης καθώς και την εξέλιξη της. Το σημαντικότερο χαρακτηριστικό που θα πρέπει να έχει το εταιρικό δίκτυο είναι η ασφάλεια του ιδίου του δικτύου, καθώς και η διαφύλαξη της ασφάλειας κατά τη χρήση του δικτύου. Οποιαδήποτε πληροφορία διακινείται στο δίκτυο θα πρέπει να χαρακτηρίζεται από την εμπιστευτικότητα (confidentiality), ακεραιότητα (Integrity) και διαθεσιμότητα (availability). Είναι κοινώς αποδεκτό ότι έξυπνες συσκευές πρέπει και θα αποτελέσουν μέρος του εταιρικού δικτύου, για αυτό θα πρέπει να εντοπιστούν οι κίνδυνοι ασφάλειας που θα επιβαρύνουν το δίκτυο και να βρεθούν λύσεις αντιμετώπισης τους. Υπάρχουν διαφορετικές προσεγγίσεις που αφορούν τα θέματα ασφάλειας στις IoT συσκευές σε [11] επίπεδα όπως είναι της της αρχιτεκτονικής, της ανταλλαγής δεδομένων, ζητήματα ασφάλειας σχετικά με καθορισμένα πρωτοκολλά που αφορούν της IoT, τα συστήματα διαχείρισης κλειδιών, τους αλγορίθμους κρυπτογραφίας, σε επίπεδο hardware, δικτύου και εφαρμογών ενώ άλλες προσεγγίσεις αναφέρονται στην ασφάλεια από άκρο σε άκρο. Εξάλλου, δημιουργούνται επιπρόσθετοι κίνδυνοι ασφάλειας που αφορούν το εταιρικό δίκτυο από την πολυπλοκότητα του δικτύου που θα πρέπει να διαχειριστεί διαφορά λειτουργικά με τις πιθανές ασυμβατότητες που θα υπάρξουν, επιπλέον η απρόβλεπτή διόγκωση του δικτύου είναι ικανή να δημιουργήσει προβλήματα ελέγχου ασφάλειας. Με την υιοθέτηση των IoT συσκευών, γίνονται ολοένα και πιο εύκολες οι παθητικές και ενεργητικές επιθέσεις στο εταιρικό δίκτυο. Για το οποιοδήποτε δίκτυο βασικός παράγοντας είναι να υπάρχει έγγραφο της πολιτικής ασφάλειας [12] πληροφοριών, η οποία είναι αυτή που θα θέτει το πλαίσιο, καθορίζει τις δομές, τις βασικές αρχές σχεδιασμού ενός ασφαλούς δικτύου και είναι αυτή που θα πρέπει να υποστηρίζεται πλήρως από τους χρήστες του εταιρικού δικτύου. Οποιαδήποτε εταιρεία επιτρέψει συνδεσιμότητα έξυπνων συσκευές στο δίκτυο της, είναι αναγκαίο να τροποποιήσει και την πολιτική ασφάλειας της, η οποία και θα απαιτεί την αλλαγή στη σχεδίαση του υφιστάμενου της δικτύου και τη διαδικασία που θα πρέπει να ακολουθούν οι χρήστες των συσκευών αυτών. Ακολούθως, για να επιτραπεί σε κάποια φιλοξενουμένη συσκευή να χρησιμοποιήσει το εταιρικό δίκτυο θα πρέπει το ίδιο το δίκτυο ,αυτοματοποιημένα, να μπορεί να ταυτοποιήσει την εν λόγω συσκευή, για να μπορέσει είτε να την αποδεκτεί και να της δοθεί η ανάλογη πρόσβαση στο δίκτυο είτε να την απορρίψει, μέσω αυτής της διαδικασίας. Η ταυτοποίηση των IoT συσκευών μπορεί να γίνει με τη χρήση του αλγορίθμου SHA-3 [13]. Ο SHA-3 θεωρείτε πιο ασφαλής σε σύγκριση με τον SHA-2,

καθώς οι δυο αλγόριθμοι έχουν διαφορά ακόμη και στη σχεδίαση τους. Συνεπώς δεν μπορεί να έχει τις ίδιες ευπάθειες ο SHA-2 με τον SHA-3. Επιπρόσθετα, ο SHA-3 έχει την ιδιότητα να τρέχει σε διαφορετικές υπολογιστικές συσκευές και κυρίως σε συσκευές που έχουν μικρή επεξεργαστική ισχύει και συνεπώς τις IoT συσκευές.

Δυστυχώς οι πλείστες IoT συσκευές δεν ενσωματώνουν οποιοδήποτε σύστημα ασφάλειας εξαιτίας του χαμηλού κόστους, της περιορισμένης μνήμης και της μικρής επεξεργαστικής δύναμης. Επιπλέον, η καθιέρωση ταυτοποίησης μέσω της πιστοποίησης X.509 [14] σε αρκετές από τις έξυπνες συσκευές δεν μπορεί να εφαρμοστεί λόγω των προαναφερθέντων, με αποτέλεσμα να μην μπορούν να επικυρώσουν την πιστοποίηση. Επίσης, με αφορμή τη διαφορετικότητα των συσκευών αυτών και της τεχνολογίας που φέρουν, δεν μπορεί να τεθεί σύστημα ταυτοποίησης μέσω βιομετρικών μηχανισμών, όπως είναι τα δακτυλικά αποτυπώματα, η ίριδα του ματιού, η αναγνώριση προσώπου κλπ.

Όπως οι υπολογιστές και αλλά συστήματα που χρησιμοποιούμε έχουν τις δίκες τους ευπάθειες, έτσι και οι έξυπνες συσκευές θεωρούνται πιο ευάλωτες. Οι πιθανές απειλές και τα τρωτά σημεία που έχουν οι έξυπνες συσκευές αφορούν την παραβίαση δεδομένων όταν αυτές συνδέονται σε μη αξιόπιστο δίκτυο, την αναμετάδοση απειλών , τις επιθέσεις DoS, καθιστώντας τους πόρους του δικτύου μη διαθέσιμους προς τους χρήστες του, κακόβουλος κώδικας που περιλαμβάνει ιούς, δουρείους ίππους και μηνύματα ανεπιθύμητης αλληλογραφίας, τα οποία ενδέχεται να προκαλέσουν αποτυχία λογισμικού. Ο απομακρυσμένος έλεγχος είναι ένα από τα χαρακτηριστικά που κάποιος επιτιθέμενος είναι σε θέση να αποκτήσει, όπως αυτό διαφάνηκε από την ερευνά της Kaspersky [06]. Θα αποτελούσε σοβαρή παράλειψη να μην αναφερθούν οι κίνδυνοι που εμπεριέχει η κλοπή μιας IoT συσκευής, αφενός για τα προσωπικά δεδομένα του ιδιοκτήτη της, αφετέρου για τα δεδομένα και τις πληροφορίες που θα μπορούν να υποκλαπούν από ένα εταιρικό δίκτυο μέσω μιας τέτοιας συσκευής.

Δεν πρέπει να αγνοήσουμε το το μοντέλο ARM οπού είναι μια κοινή προσπάθεια που γίνετε από την IoT – A [15] με όραμα της, την ανάπτυξη μιας κοινής αρχιτεκτονικής οπού στόχο έχει τη δια λειτουργικότητα σε επίπεδο επικοινωνίας το οποίο θα είναι ικανό να επεκταθεί σε άλλες διαφορετικές πλατφόρμες. Η αρχιτεκτονική που προκρίνετε περιγράφει βασικά δομικά στοιχεία, επιλογές σχεδιασμού για αντιμετώπιση αντικρουόμενων απαιτήσεων όσο αφορά τη λειτουργικότητα, την απόδοση, την ανάπτυξη και την ασφάλεια.

Η ταυτοποίηση και ακολούθως η πιστοποίηση είναι ο πρωταρχικός έλεγχος που γίνετε με στόχο το διαχωρισμό το εξουσιοδοτημένων χρηστών που θα έχουν πρόσβαση στο δίκτυο, από τους μη εξουσιοδοτημένος. Είναι, η πιο σημαντικότερη διαδικασία οπού ο εξουσιοδοτημένος χρήστης θα πρέπει να καταχωρήσει το προσωπικό του Username και αυτός να πιστοποιηθεί ακολούθως από το Password.

GDPR - Νομικό πλαίσιο προστασίας προσωπικών δεδομένων

Το νέο νομοθετικό πλαίσιο [16] αποτελεί Ευρωπαϊκό κανονισμός και συνεπώς νομοθεσία προς όλα τα ευρωπαϊκά κράτη, το οποίο έχει ψηφιστεί από το Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο στις 27 Απρίλιου του 2016. Έχει τεθεί σε εφαρμογή στις 25 Μάιου του 2018, με στόχο την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Τα αρχικά του προέρχονται από το General Data Protection Regulation. Όταν αναφερόμαστε σε προσωπικά δεδομένα εννοούμε για παράδειγμα το όνομα και επώνυμο ενός ατόμου, τη διεύθυνση κατοικίας του, τη διεύθυνση IP,την ηλεκτρονική του διεύθυνση κλπ. Η συγκατάθεση είναι απαραίτητη για τη συλλογή και επεξεργασία των προσωπικών δεδομένων, η οποία πρέπει να χαρακτηρίζεται ως ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επίγνωση ένδειξη βουλήσεως.

Η πορεία του νέου νομικού πλαισίου έχει άμεση σχέση με την ταυτοποίηση του χρήστη προς τα εταιρικά δίκτυα, λόγω της πρόσβασης σε προσωπικά δεδομένα που διακινούνται και αποθηκεύονται σε αυτά. Δεν πρέπει να αγνοήσουμε ότι η διακίνηση προσωπικών δεδομένων σε IoT συσκευές, οι οποίες δεν βρίσκονται σε ελεγχόμενο περιβάλλον, αυτόματα αυξάνει τους κίνδυνους για διαρροή των δεδομένων. Επιπρόσθετα, οι IoT συσκευές είναι εύκολα προσβάσιμες προς τρίτα άτομα, είτε αυτά είναι εξουσιοδοτημένα είτε όχι. Κλοπή οποιασδήποτε IoT συσκευής, θα αποτελούσε άμεσο κίνδυνο προς τα δεδομένα των πελατών και των προμηθευτών. Η σωστή μέθοδος ταυτοποίησης στο εταιρικό δίκτυο από τους χρήστες IoT συσκευών ικανοποιεί την αρχή της λογοδοσίας και διασφαλίζει την παρεμπόδιση μη εξουσιοδοτημένων χρηστών. Εντούτοις, η πρόσβαση σε προσωπικά δεδομένα από IoT συσκευές, θα πρέπει να δίνεται αυστηρά σε περιορισμένους χρήστες. Τροποποίηση αυτών των δεδομένων, από δυσαρεστημένο υπάλληλο είναι ένα ενδεχόμενο που θα πρέπει να λαμβάνεται υπόψιν.

Επίσης, η ύπαρξη περιστατικού παραβίασης ασφάλειας προϋποθέτει άμεση γνωστοποίηση προς τον Επίτροπο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, κοινοποιώντας στοιχεία που αφορούν το περιστατικό, όπως π.χ. αν βρίσκεται σε εξέλιξη, ποτέ έγινε αντιληπτό, αν αφορά παραβίαση ακεραιότητας ή και διαθεσιμότητας, καθώς και πληροφορίες για τα μέτρα που λαμβάνονται για μείωση των κίνδυνων από την εταιρεία, για προστασία των προσωπικών δεδομένων. Σύμφωνα με την έρευνα αναμένεται ότι οι κυπριακές μικρομεσαίες επιχειρήσεις, μετά από την εφαρμογή του νομοθετικού πλαισίου, καταγράφουν χαμηλά ποσοστά όσον αφορά την προστασία του εταιρικού δικτύου και κατά συνέπεια των προσωπικών δεδομένων.

Σύμφωνα με την Κυπριακή Νομοθεσία, οι ποινές επιβάλλονται σε χρηματικό ποσό από €10000 μέχρι €30000, ή φυλάκιση από 1 έτος μέχρι 3 έτη ή και τις δύο αυτές ποινές, ανάλογα με τα αδικήματα που έχουν διαπραχθεί.

Κεφάλαιο 3
Η Μεθοδολογία της Έρευνας

Η κατάλληλη ερευνητική μέθοδος επιλέχθηκε με βάση την βιβλιογραφική ανασκόπηση καθώς επίσης και για την εξυπηρέτηση των στόχων της έρευνας. Η παρούσα έρευνα πρωτογενών στοιχείων χαρακτηρίζεται ως ποσοτική και η διεξαγωγή της γίνεται με την χρήση ερωτηματολογίου, εργαλείο που χρησιμοποιείται κατά κόρων σε παρόμοιου είδους έρευνες [17].

Γενικός στόχος της έρευνας είναι η διερεύνηση του βαθμού στον οποίο εφαρμόζεται η ταυτοποίηση στα δίκτυα των μικρομεσαίων επιχειρήσεων από τη χρήση των διάχυτων συσκευών και του ΙΟΤ.

Επιπλέον, σχηματίστηκαν οι ακόλουθες ερωτήσεις ως συμπλήρωμα των ερευνητικών ερωτήσεων που αναγνωρίστηκαν στο κεφάλαιο 1:

- Ποιοι οι λόγοι χρησιμοποίησης του Internet of Things (IoT);
- Ποιες πρακτικές ακολουθούν οι μικρομεσαίες επιχειρήσεις στον Κυπριακό χώρο αναφορικά με την ασφάλεια των δικτύων τους;

- Ποιες εφαρμογές συμμετέχουν στο δίκτυο της επιχείρησης και συγκαταλέγονται στην γενικότερη κατηγορία του Internet of Things (IoT);
- Υπάρχει στατιστικά σημαντική διαφοροποίηση του βαθμού στον οποίο εφαρμόζεται η ταυτοποίηση στα δίκτυα των μικρομεσαίων επιχειρήσεων από τη χρήση των διάχυτων συσκευών και του IOT σε αναλογία με τα στοιχεία της επιχείρησης (είδος επιχείρησης, αριθμός εργαζομένων)

3.1. Το Ερευνητικό Εργαλείο

Στην παρούσα μεταπτυχιακή εργασία επιλέχθηκε το ερωτηματολόγιο, όπως αυτό αναφέρεται στο παράρτημα 1, ως το εργαλείο συλλογής των δεδομένων της έρευνας. Για τη συλλογή δεδομένων της έρευνας κατασκευάσθηκε πρωτότυπο ερωτηματολόγιο με βάση προηγούμενες έρευνες στο πεδίο της ταυτοποίησης στα δίκτυα των μικρομεσαίων επιχειρήσεων από τη χρήση των διάχυτων συσκευών και του IOT.

Το ερωτηματολόγιο περιλαμβάνει 42 ερωτήσεις. Αρχικά οι ερωτώμενοι καλούνται να απαντήσουν μία ερώτηση ελέγχου ώστε να εξακριβωθεί πως μπορούν να συμμετέχουν στην έρευνα. Συγκεκριμένα, οι συμμετέχοντες ερωτήθηκαν εάν έχουν καθήκοντα στο τμήμα πληροφορικής στον οργανισμό. Ακολούθως, ζητούνται τα δημογραφικά στοιχεία των ερωτώμενων (φύλο, ηλικία, μορφωτικό επίπεδο, έτη εργασιακής εμπειρίας) και τα στοιχεία της επιχείρησης (Είδος ιδιοκτησίας της επιχείρησης, αριθμός εργαζομένων). Στη συνέχεια παρατίθεται 35 ερωτήσεις αναφορικά με το αντικείμενο της έρευνας με τις απαντήσεις τους να δίνονται είτε σε διχοτομικές κλίμακες πολλαπλής επιλογής, είτε με μία κλίμακα τύπου Likert 5 σημείων όπου 1=διαφωνώ έντονα και 5=Συμφωνώ έντονα.

3.2. Ο Πληθυσμός και το Δείγμα της Έρευνας

Ο πληθυσμός της έρευνας αναφέρεται στο τμήμα του ευρύτερου πληθυσμού, που μπορεί να συμμετέχει στην έρευνα, δηλαδή τα υποψήφια στοιχεία, που μπορούν να επιλεγούν για τη δημιουργία του δείγματος [18]. Στην παρούσα έρευνα ο πληθυσμός στόχος είναι οι εργαζόμενοι στο τμήμα πληροφορικής μικρομεσαίων επιχειρήσεων και το τελικό δείγμα της έρευνας ήταν δείγμα ευχέρειας 26 επιχειρήσεων. Η επιλογή των ερωτώμενων έγινε τυχαία και για λόγους βολικότητας του ερευνητή. Βασικό κριτήριο συμμετοχής στην έρευνα ήταν εργασία σε τμήμα πληροφορικής μικρομεσαίων

επιχειρήσεων. Τέλος, γεωγραφικά η έρευνα πραγματοποιήθηκε με επιχειρήσεις από όλες τις περιοχές της Κύπρου με σκοπό την πρόσβαση σε όσο το δυνατόν μεγαλύτερο δείγμα.

3.3. Διεξαγωγή της Έρευνας

Πιλοτική φάση έρευνας

Πριν από την τελική διανομή των ερωτηματολογίων και την πραγματοποίηση της έρευνας, κρίθηκε καλό να γίνει μια πιλοτική φάση με στόχο να εξακριβωθεί η αποτελεσματικότητά του εργαλείου, να εντοπιστούν τα πιθανά λάθη και να γίνουν οι αναγκαίες διορθώσεις. Η συγκεκριμένη δοκιμαστική φάση έγινε την πρώτη εβδομάδα του Ιουνίου, σε δείγμα 3 ερωτώμενων / επιχειρήσεων. Η επιλογή των ατόμων έγινε με σκοπό την ομοιότητα τους με το τελικό δείγμα της έρευνας ενώ και τα άτομα αποκλείστηκαν στη συνέχεια από την διεξαγωγή της έρευνας. Η διαδικασία της συμπλήρωσής του δεν έδειξε ιδιαίτερα προβλήματα. Το ερωτηματολόγιο κρίθηκε πως έχει το κατάλληλο μέγεθος (πως δεν ήταν πολύ μεγάλο), πως είναι ευκολοδιάβαστο και το θέμα του αρκετά ενδιαφέρον για τους ερωτώμενους.

Η Διαδικασία της έρευνας

Όπως αναφέρθηκε στο κεφάλαιο της δειγματοληψίας, η έρευνα πραγματοποιήθηκε σε δείγμα μικρομεσαίων επιχειρήσεων της Κύπρου. Χρονικά η έρευνα πραγματοποιήθηκε από τις 10 Ιουνίου έως τις 30 του ίδιου μήνα και το ερωτηματολόγιο συμπληρώθηκε από 26 ερωτώμενους. Σαν ερευνητής είχα προηγούμενος επικοινωνία με τους ερωτωμένους για την συμπλήρωση του ερωτηματολογίου εξασφαλίζοντας την κατανόηση την απάντηση όλων των ερωτήσεων, αποφεύγοντας έτσι πιθανές παρερμηνείες και απώλεια δεδομένων κατά τη συμπλήρωση. Επίσης, ο ερευνητής επισήμανε στους ερωτώμενους πως τα ερωτηματολόγια είναι ανώνυμα και πως τα αποτελέσματα θα χρησιμοποιηθούν μόνο για ερευνητικούς σκοπούς.

Περιορισμοί

Όπως κάθε έρευνα, έτσι και η συγκεκριμένη υπόκειται σε κάποιους περιορισμούς, οι οποίοι πρέπει να αναφέρονται. Αρχικά, η έρευνα έπρεπε να διεξαχθεί σε συγκεκριμένο χρονικό διάστημα, οπότε υπήρχε ο χρονικός περιορισμός, οποίος υπάρχει σε κάθε έρευνα που διεξάγεται για ακαδημαϊκούς σκοπούς. Επιπλέον υπήρχε ο χωρικός περιορισμός, τον οποίο αν και προσπαθήσαμε να παρακάμψουμε με το ερωτηματολόγιο να προωθείται μέσω ηλεκτρονικού ταχυδρομείου ή με τη δημοσίευσή του στα μμέσα κοινωνικής δικτύωσης, σε άτομα που εργάζονται σε μικρομεσαίες επιχειρήσεις και έχουν καθήκοντα στον τομέα της πληροφορικής. Επίσης, λόγω του περιορισμένου χρόνου, για τον οποίο διεξήχθη η έρευνα, ήταν πολύ δύσκολη η προσέγγιση μμεγαλύτερου αριθμού συμμμετεχόντων.

3.4. Ανάλυση Δεδομένων

Η ανάλυση των δεδομένων που παρείχε η έρευνα πρωτογενών στοιχείων έγινε με τη χρήση του προγράμματος στατιστικής ανάλυσης SPSS 23.0[19]. Οι συμμετέχοντες που απάντησαν στις ερωτήσεις, αφορά το δείγμα μας που είναι N=26.

Για την ανάλυση των δεδομένων και την παρουσίαση των αποτελεσμάτων έγινε χρήση:

- Πινάκων συχνοτήτων και ραβδογραμμάτων.
- Συγκριτικής στατιστικής ανάλυσης για την διαπίστωση τυχόν στατιστικής σημαντικότητας στη συσχέτιση μεταξύ των μεταβλητών.

Η ανάλυση διακύμανσης (ANOVA) και το παραμετρικό τεστ Pearson correlation επιλέχθηκε για την εξακρίβωση των στατιστικά σημαντικών συσχετίσεων. Η επιλογή των τεστ έγινε με βάση το επίπεδο μέτρησης των μεταβλητών. Συγκεκριμένα η ανάλυση διακύμανσης ANOVA επιλέχθηκε για την συσχέτιση μεταξύ μίας ποσοτικής και μίας ποιοτικής μεταβλητής ενώ το παραμετρικό τεστ Pearson για τη συσχέτιση μεταξύ δύο ποιοτικών μεταβλητών. Η διαδικασία ελέγχου υπόθεσης χρησιμοποιήθηκε για την εξακρίβωση των συσχετίσεων και επαναλήφθηκε για κάθε ζευγάρι μεταβλητών.
Η διαδικασία ελέγχου-υπόθεσης που ακολουθήθηκε (με επίπεδο σημαντικότητας τέθηκε

0.05) ήταν η εξής:

- H_0 = Δεν υπάρχει συσχέτιση μεταξύ δύο μεταβλητών.
- H_1 = Υπάρχει συσχέτιση μεταξύ δύο μεταβλητών.

Κεφάλαιο 4
Ευρήματα της Έρευνας

Δομή Ερωτηματολογίου

Το ερωτηματολόγιο (ΠΑΡΑΡΤΗΜΑ 1) διαχωρίζεται σε 4 ενότητες:

Η **Πρώτη ενότητα** του ερωτηματολογίου , περιέχει ερωτήσεις που αφορούσαν δημογραφικά χαρακτηριστικά των συμμετεχόντων στην έρευνα, όπως Φύλο, Ηλικία, Εκπαίδευση, και Έτη εργασιακής εμπειρίας.

Στη **Δεύτερη ενότητα** υπήρχαν ερωτήσεις σχετικά με στοιχεία της επιχείρησης σε σχέση με το είδος ιδιοκτησίας της επιχείρησης και των αριθμό των εργαζομένων.

Στην **Τρίτη ενότητα** οι συμμετέχοντες ρωτήθηκαν για τους λόγους χρήσης του Internet of Things (IoT) στην επιχείρηση. Οι ερωτώμενοι είχαν να επιλέξουν μέσα από μια σειρά κλειστού τύπου απαντήσεων με τη χρήση πολλαπλών επιλόγων, για οτιδήποτε εφαρμόζεται στην επιχείρηση, καθώς επίσης και πεδίο ανοικτού τύπου απαντήσεων για επιπρόσθετες απαντήσεις, στις οποίες δεν υπήρχαν στις επιλογές.

Οι ερωτήσεις της **Τέταρτης Ενότητας** καλούσαν τους συμμετέχοντες να απαντήσουν σε διάφορες κατηγόριες, που αφορούν τα μετρά που εφαρμόζονται για την ασφάλεια του δικτύου της επιχείρησης.

Η τέταρτη ενότητα περιέχει εννιά υποκατηγορίες:

Η πρώτη υποκατηγορία αφορά τη διαχείριση των συστημάτων και των δεδομένων με τη χρήση πολλαπλών απαντήσεων και διατιμών, απαντήσεων μεταξύ του Ναι και του Όχι.

Η δεύτερη υποκατηγορία σχετίζεται με την ύπαρξη και εφαρμογή της πολιτική ασφάλειας - Security Policy της επιχείρησης. Οι απαντήσεις κωδικοποιήθηκαν ως εξής: Διαφωνώ απολυτά=1, Διαφωνώ=2, Ουδέτερο=3, Συμφωνώ=4, Συμφωνώ απολυτά=5, χρησιμοποιώντας 5- βαθμιαία κλίμακα Likert.

Στην τρίτη υποκατηγορία είναι η διαχείριση κίνδυνων - Risk management, οι συμμετέχοντες ρωτήθηκαν για τις διαδικασίες αξιολόγησης, μείωσης πιθανού ρίσκου, την ασφάλεια των δεδομένων και τον εντοπισμό νέων πρακτικών και δομών αναφορικά με την ασφάλεια των υπολογιστικών συστημάτων. Οι απαντήσεις κωδικοποιήθηκαν πάλι ως εξής: Διαφωνώ απολυτά=1, Διαφωνώ=2, Ουδέτερο=3, Συμφωνώ=4, Συμφωνώ απολυτά=5, χρησιμοποιώντας 5- βαθμιαία κλίμακα Likert.

Στην τέταρτη υποκατηγορία η Εκπαίδευση και ευαισθητοποίηση - Training and Awareness, οι συμμετέχοντες είχαν να επιλέξουν μεταξύ ερωτήσεων αναφορικά με την εκπαίδευση, την επεξήγηση και τις επιμορφωτικές ενημερώσεις για την εφαρμογή από μέρους των υπάλληλων. Χρησιμοποιήθηκε η ίδια κλίμακα όπως και στην προηγουμένη ενότητα.

Στην πέμπτη υποκατηγορία οι συμμετέχοντες καλούνται να απαντήσουν σε ερωτήσεις σχετικές με το παρελθόν των υπάλληλων - Background checks σε σχέση με πιθανή παραβατικότητά, σύμβαση εμπιστευτικότητας και εφαρμογή διαδικασίας απομάκρυνσης ή της μεταφοράς ενός εργαζομένου. Οι απαντήσεις κωδικοποιήθηκαν πάλι χρησιμοποιώντας 5- βαθμιαία κλίμακα Likert.

Στην έκτη υποκατηγορία είναι η Φυσική ασφάλεια - Physical Security, για πρόσβαση στις εγκαταστάσεις και γενικότερα η ύπαρξη οργανωμένου συστήματος ασφάλειας των εγκαταστάσεων. Οι απαντήσεις κωδικοποιήθηκαν πάλι χρησιμοποιώντας 5- βαθμιαία κλίμακα Likert..

Στην εβδόμη υποκατηγορία, η ασφάλεια δικτύου - Network security. Οι ερωτήσεις αναφέρονται στην ύπαρξη εξωτερικών συστημάτων από επιλογές πρόσβασης, η παράνομη πρόσβαση στο δίκτυο, ο εντοπισμός τρωτών σημείων στα συστήματα επικοινωνίας και στα πληροφοριακά συστήματα και γενικότερα η ύπαρξη συστημάτων προστασίας των δεδομένων, που διακινούνται στο εταιρικό δίκτυο. Οι απαντήσεις κωδικοποιήθηκαν πάλι ως εξής: Διαφωνώ απολυτά=1, Διαφωνώ=2, Ουδέτερο=3,

Συμφωνώ=4, Συμφωνώ απολυτά=5, χρησιμοποιώντας 5- βαθμιαία κλίμακα Likert και επιπρόσθετα για την μεταφορά ευαίσθητων πληροφορίων σε εξωτερικούς αποδέκτες με πεδίο ανοικτού τύπου απαντήσεων για επιπρόσθετες απαντήσεις πέραν του Ναι και του Όχι.

Στην ογδόη υποκατηγορία Λογικής πρόσβασης - Logical access, οι συμμετέχοντες είχαν να απαντήσουν μεταξύ Ναι και Όχι, σε ερωτήσεις σχετικά με την παροχή μοναδικής ταυτοποίησης και κωδικού, άδεια πρόσβασης με βάση τη θέση των εργαζομένων, την ύπαρξη λίστας υπάλληλων για πρόσβαση, πολυπλοκότητα κωδικού, λίστα με δέκτες κινητές συσκευές, αυτοματοποιημένη αποσύνδεση και ανιχνευσιμότητα της ταυτοποίησης των χρηστών. Οι απαντήσεις κωδικοποιήθηκαν ως εξής: Καθόλου Σημαντικό=1, Λιγότερο Σημαντικό=2, Ουδέτερο=3, Σημαντικό=4, Πολύ Σημαντικό=5, χρησιμοποιώντας 5-βάθμια κλίμακα Likert. Επιπρόσθετα, στο ερώτημα για τη διαχείριση λειτουργιών - Operations Management δίδονται πολλαπλές απαντήσεις σχετικές με την ύπαρξη antivirus και παρακολούθηση διαδικασιών για την προστασία των δεδομένων.

Στην ένατη υποκατηγορία Διαχείριση επιχειρηματικής συνέχειας -Business continuity management, ζητήθηκε από τους συμμετέχοντες να δηλώσουν κατά ποσό διαφυλάσσονται με τη χρήση Back up, οι πληροφορίες και τα ευαίσθητα δεδομένα. Οι απαντήσεις κωδικοποιήθηκαν ως εξής: Διαφωνώ απολυτά=1, Διαφωνώ=2, Ουδέτερο=3, Συμφωνώ=4, Συμφωνώ απολυτά=5, χρησιμοποιώντας 5- βαθμιαία κλίμακα Likert.

4.1. Περιγραφική Στατιστική Ανάλυση των Αποτελεσμάτων

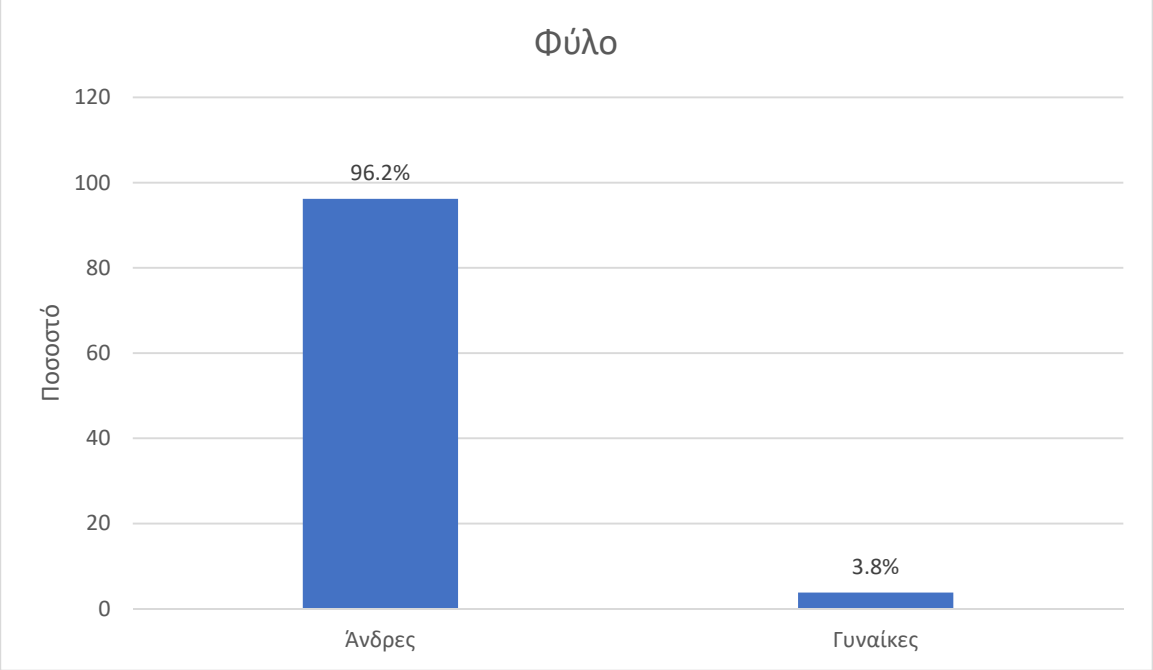
ΕΝΟΤΗΤΑ 1: Δημογραφικά Χαρακτηριστικά

- Φύλο

Ο Πίνακας 1 και το Διάγραμμα 1 παρουσιάζουν τις συχνότητες και το ποσοστό για κάθε φύλο που συμμετείχε στην έρευνα. Οι άνδρες αποτελούν το 96.2% των ερωτηθέντων ενώ οι γυναίκες μόλις το 3.8%.

Πίνακας 1: Φύλο

	Συχνότητα	Ποσοστό	Έγκυρο ποσοστό	Αθροιστικό ποσοστό
Άνδρες	25	96.2	96.2	96.2
Γυναίκες	1	3.8	3.8	100.0
Σύνολο	26	100.0	100.0	



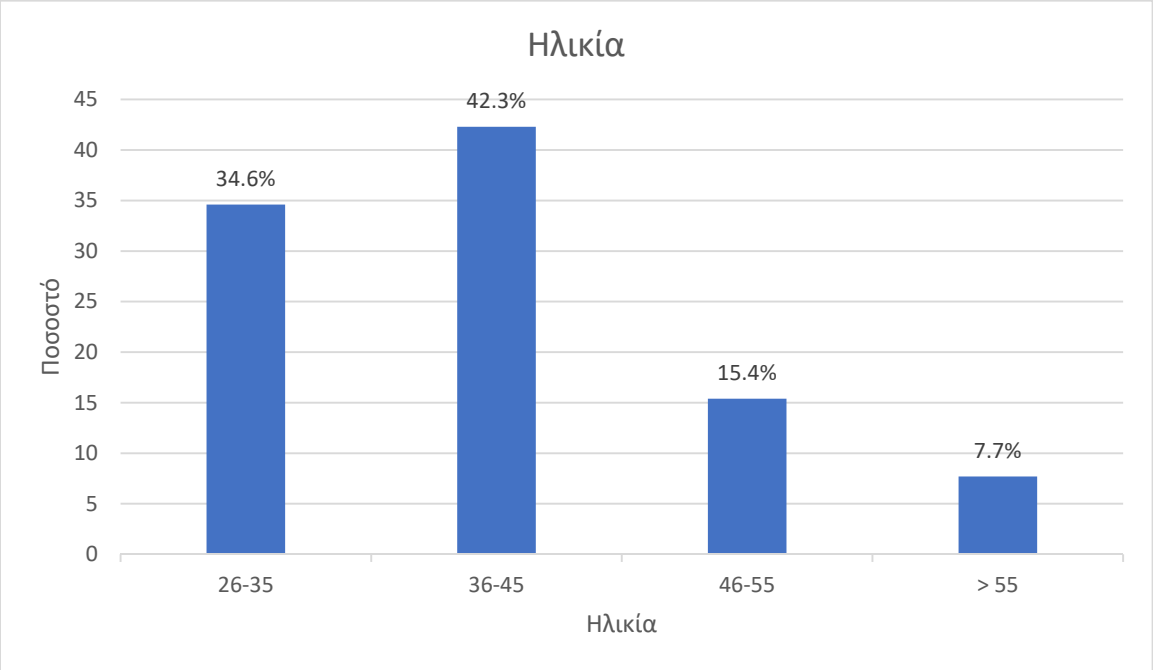
Διάγραμμα 1 - Φύλο

- Ηλικία

Το μεγαλύτερο ποσοστό των ερωτώμενων (42.3%) ηλικιακά ανήκει στην κατηγορία από 36 έως 45 ετών, και ακολουθούν οι ηλικιακές ομάδες «26-35» με ποσοστό 34.6%, «46-55 ετών» με ποσοστό 15.4% και τέλος πάνω από 55 ετών με ποσοστό 7.7% (Πίνακας 2, Διάγραμμα 2).

Πίνακας 2: Ηλικία

	Συχνότητα	Ποσοστό	Έγκυρο ποσοστό	Αθροιστικό ποσοστό
26-35	9	34.6	34.6	34.6
36-45	11	42.3	42.3	76.9
46-55	4	15.4	15.4	92.3
> 55	2	7.7	7.7	100.0
Σύνολο	26	100.0	100.0	



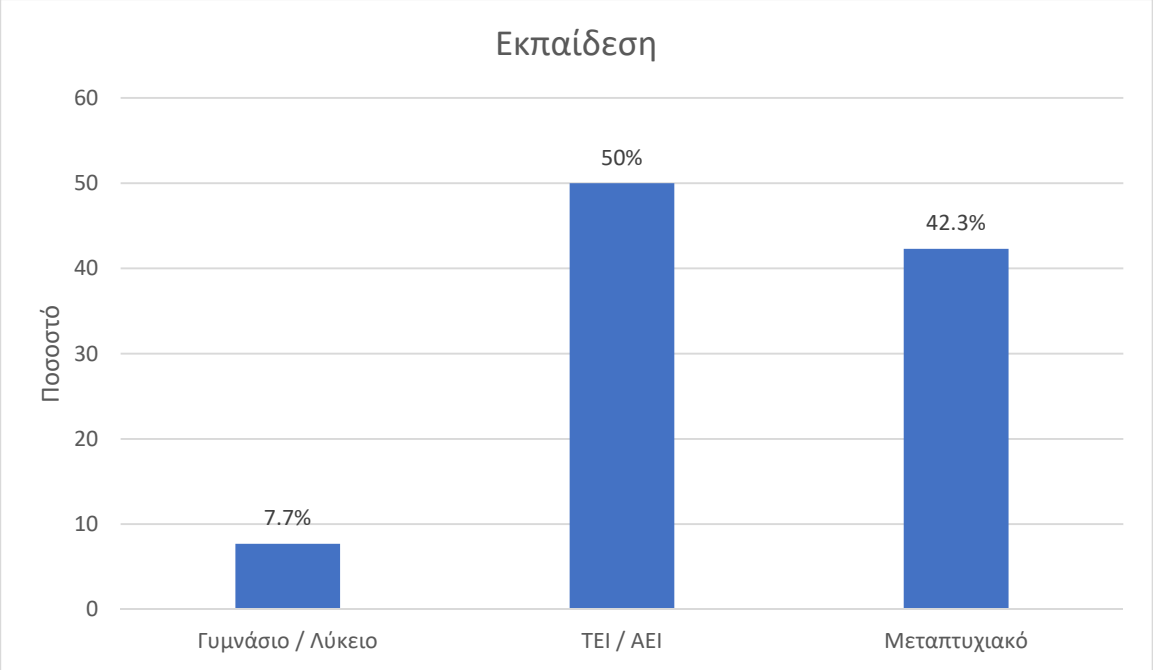
Διάγραμμα 2 – Ηλικία

- Εκπαίδευση

Σχετικά με το μορφωτικό επίπεδο των ερωτώμενων, το δείγμα αποτελείται κατά 50% από απόφοιτους ΤΕΙ ή ΑΕΙ, 42.3% έχουν ολοκληρώσει μεταπτυχιακές σπουδές και 7.7% ήταν απόφοιτοι γυμνασίου / Λυκείου (Πίνακας 3, Διάγραμμα 3).

Πίνακας 3: Εκπαίδευση

	Συχνότητα	Ποσοστό	Έγκυρο ποσοστό	Αθροιστικό ποσοστό
Γυμνάσιο / Λύκειο	2	7.7	7.7	7.7
ΤΕΙ / ΑΕΙ	13	50.0	50.0	57.7
Μεταπτυχιακό	11	42.3	42.3	100.0
Σύνολο	26	100.0	100.0	



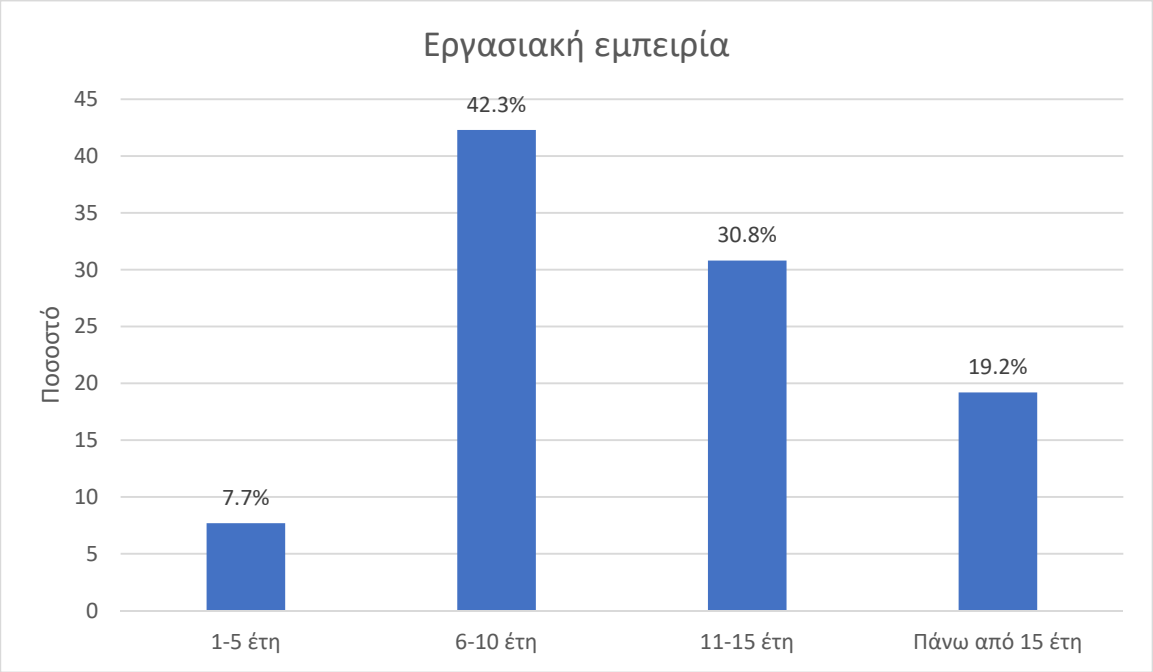
Διάγραμμα 3 - Εκπαίδευση

- Έτη εργασιακής εμπειρίας

Ο Πίνακας 4 και το Διάγραμμα 4 παρουσιάζουν τις συχνότητες και το ποσοστό σχετικά με τα έτη εργασιακής εμπειρίας των ερωτώμενων. Συγκεκριμένα, το 42.3% των ερωτηθέντων εργάζεται έχει από 6 έως 10 έτη εργασιακής εμπειρίας, και ακολούθως 30.85 από 11 έως 15 έτη, 19.2% πάνω από 15 έτη ενώ μόλις 7.7% έως 5 έτη υπηρεσίας.

Πίνακας 4: Έτη εργασιακής εμπειρίας

	Συχνότητα	Ποσοστό	Έγκυρο ποσοστό	Αθροιστικό ποσοστό
1-5 έτη	2	7.7	7.7	7.7
6-10 έτη	11	42.3	42.3	50.0
11-15 έτη	8	30.8	30.8	80.8
Πάνω από 15 έτη	5	19.2	19.2	100.0
Σύνολο	26	100.0	100.0	



Διάγραμμα 4 - Έτη εργασιακής εμπειρίας

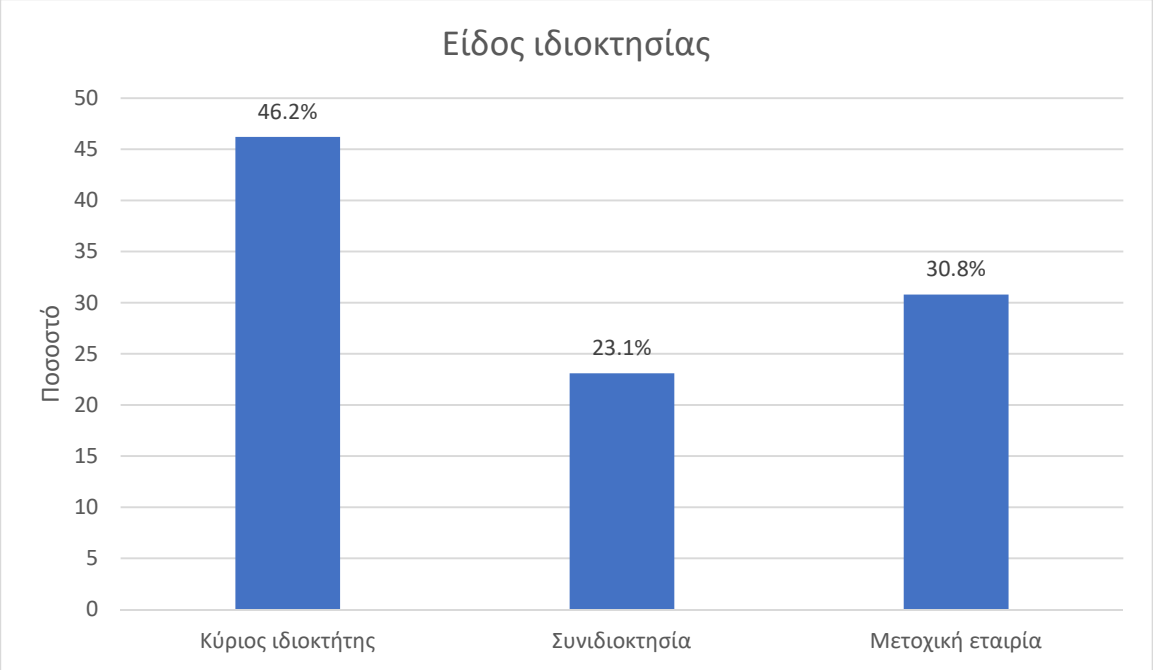
Ενότητα 2 Στοιχεία της επιχείρησης

- Είδος ιδιοκτησίας της επιχείρησης

Ο Πίνακας 5 και το Διάγραμμα 5 παρουσιάζουν τις συχνότητες και το ποσοστό σχετικά με το είδος ιδιοκτησίας της επιχείρησης. Συγκεκριμένα, το 46.2% των ερωτηθέντων ήταν κύριοι ιδιοκτήτες της επιχείρησης, 30.8% εργάζονται σε μετοχική εταιρίας, και 23/1% σε εταιρία με συνιδιοκτησία.

Πίνακας 5: Είδος ιδιοκτησίας

	Συχνότητα	Ποσοστό	Έγκυρο ποσοστό	Αθροιστικό ποσοστό
Κύριος ιδιοκτήτης	12	46.2	46.2	46.2
Συνιδιοκτησία	6	23.1	23.1	69.2
Μετοχική εταιρία	8	30.8	30.8	100.0
Σύνολο	26	100.0	100.0	



Διάγραμμα 5 - Είδος ιδιοκτησίας

- Αριθμός εργαζομένων

Ο Πίνακας 6 παρουσιάζει το μέσο όρο, την τυπική απόκλιση, την μέγιστη και ελάχιστη τιμή αναφορικά με τον αριθμό των εργαζομένων στην επιχείρηση. Ειδικότερα, ο μέσος αριθμός εργαζομένων στην επιχείρηση ήταν 52.3 (Τ.Α. = 40.65), με μέγιστο τους 150 και ελάχιστο τους 3 εργαζόμενους.

Πίνακας 6: Αριθμός εργαζομένων

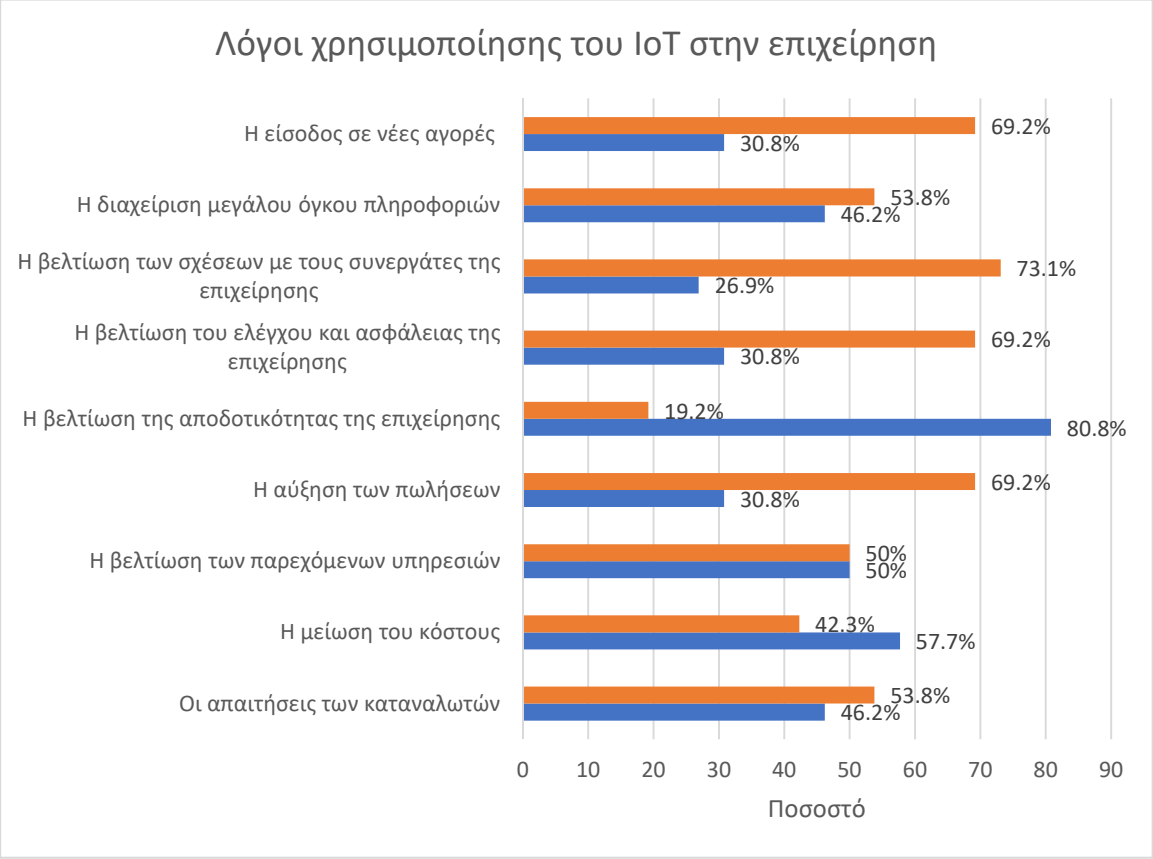
	N	Ελάχιστο	Μέγιστο	Μέσος όρος	Τυπική απόκλιση
Αριθμός εργαζομένων	26	3.00	150.00	52.3077	40.65737

Ενότητα 3 Λόγοι χρησιμοποίησης του Internet of Things (IoT) στην επιχείρηση

Ο Πίνακας 7 και το Διάγραμμα 6 παρουσιάζουν τις συχνότητες και τα ποσοστά των απαντήσεων των ερωτηθέντων σχετικά με τους παράγοντες που συντέλεσαν στην απόφαση να υιοθετήσουν τεχνολογίες που συγκαταλέγονται στην γενικότερη κατηγορία του Internet of Things (IoT) στην επιχείρηση τους. Συγκεκριμένα, οι ερωτώμενοι απάντησαν πως οι σημαντικότεροι παράγοντες που συντέλεσαν στην απόφαση να υιοθετήσουν τεχνολογίες που συγκαταλέγονται στην γενικότερη κατηγορία του Internet of Things (IoT) στην επιχείρηση που εργάζονται ήταν η βελτίωση της αποδοτικότητας της επιχείρησης (80.8%) και ακολούθως, η μείωση του κόστους (57.7%), η βελτίωση των παρεχόμενων υπηρεσιών (50%), η διαχείριση μεγάλου όγκου πληροφοριών (46.2%) και οι απαιτήσεις των καταναλωτών (46.2%). Αντιθέτως, μικρότερη επιρροή είχαν η βελτίωση των σχέσεων με τους συνεργάτες της επιχείρησης (26.9%) και η αύξηση των πωλήσεων (30.8%).

Πίνακας 7: Λόγοι χρησιμοποίησης του Internet of Things (IoT) στην επιχείρηση

	(1= Διαφωνώ έντονα, 5= Συμφωνώ έντονα)	ΝΑΙ	ΟΧΙ
1	Οι απαιτήσεις των καταναλωτών	46.2	53.8
2	Η μείωση του κόστους	57.7	42.3
3	Η βελτίωση των παρεχόμενων υπηρεσιών	50	50
4	Η αύξηση των πωλήσεων	30.8	69.2
5	Η βελτίωση της αποδοτικότητας της επιχείρησης	80.8	19.2
6	Η βελτίωση του ελέγχου και ασφάλειας της επιχείρησης	30.8	69.2
7	Η βελτίωση των σχέσεων με τους συνεργάτες της επιχείρησης	26.9	73.1
8	Η διαχείριση μεγάλου όγκου πληροφοριών	46.2	53.8
9	Η είσοδος σε νέες αγορές	30.8	69.2



Διάγραμμα 6 - Λόγοι χρησιμοποίησης του Internet of Things (IoT) στην επιχείρηση

Ενότητα 4 Ασφάλεια δικτύου

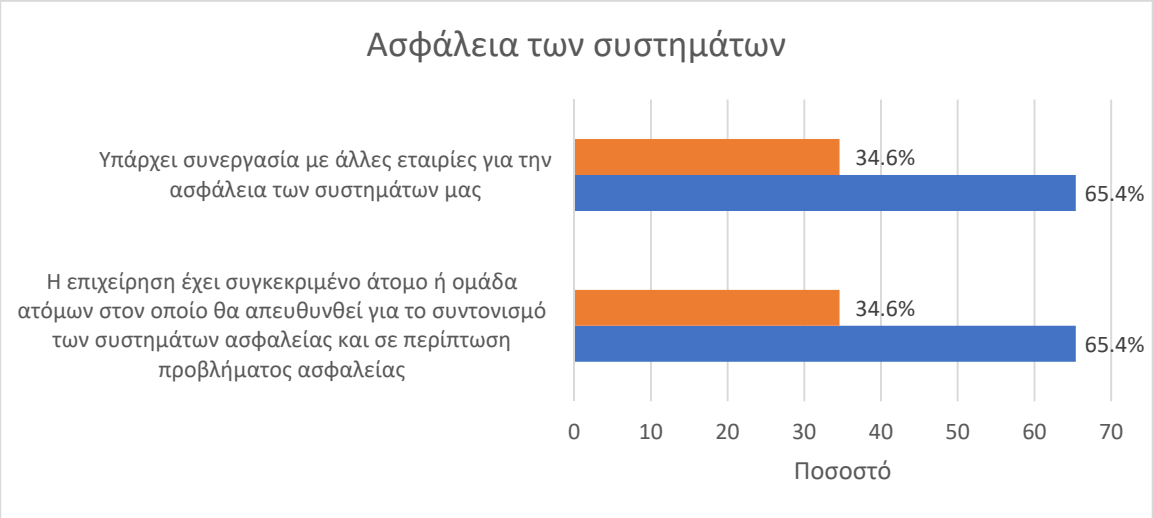
- Security program

10. Ασφάλεια των συστημάτων

Ο Πίνακας 8 και το Διάγραμμα 8 παρουσιάζουν τις συχνότητες και τα ποσοστά των απαντήσεων των ερωτηθέντων σχετικά με την ασφάλεια των συστημάτων. Συγκεκριμένα, τα 2/3 των ερωτώμενων απάντησαν πως η επιχείρηση έχει συγκεκριμένο άτομο ή ομάδα ατόμων στον οποίο θα απευθυνθεί για το συντονισμό των συστημάτων ασφαλείας και σε περίπτωση προβλήματος ασφαλείας καθώς επίσης πως υπάρχει συνεργασία με άλλες εταιρίες για την ασφάλεια των συστημάτων.

Πίνακας 8: Ασφάλεια των συστημάτων

		ΝΑΙ	ΟΧΙ
1	Η επιχείρηση έχει συγκεκριμένο άτομο ή ομάδα ατόμων στον οποίο θα απευθυνθεί για το συντονισμό των συστημάτων ασφαλείας και σε περίπτωση προβλήματος ασφαλείας	65.4	34.6
2	Υπάρχει συνεργασία με άλλες εταιρίες για την ασφάλεια των συστημάτων μας	65.4	34.6



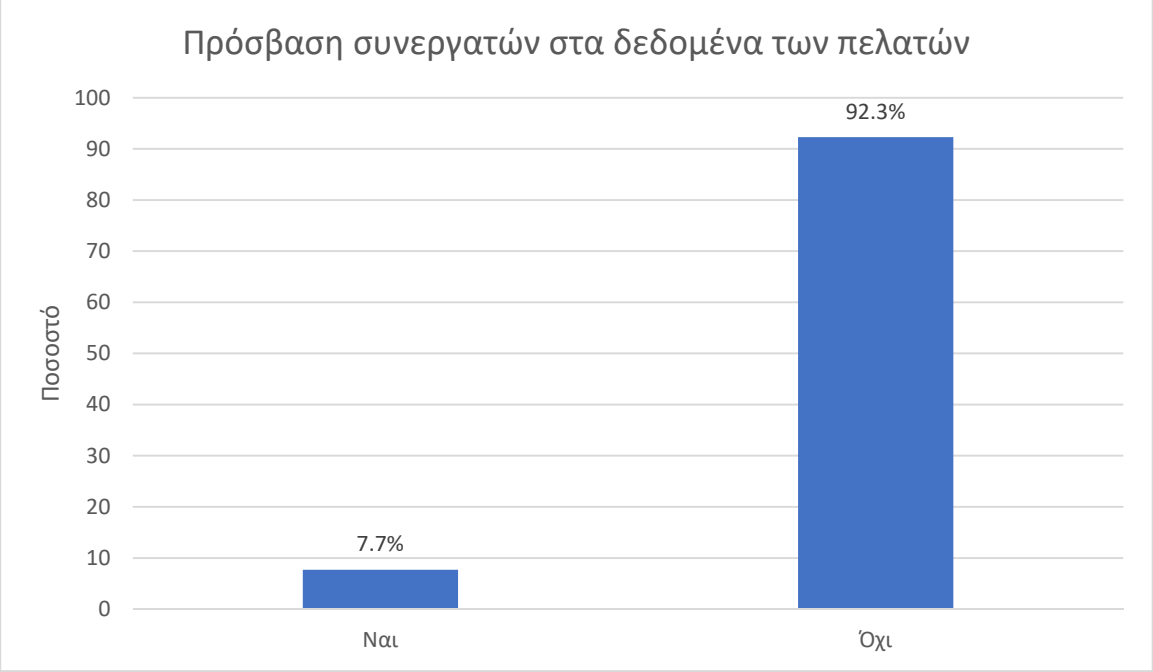
Διάγραμμα 7 - Ασφάλεια των συστημάτων

11. Οι συνεργάτες της εταιρίας έχουν πρόσβαση στα δεδομένα των πελατών μας

Ο Πίνακας 9 και το Διάγραμμα 9 παρουσιάζουν τις συχνότητες και τα ποσοστά των απαντήσεων των ερωτηθέντων σχετικά με το εάν οι συνεργάτες της εταιρίας έχουν πρόσβαση στα δεδομένα των πελατών. Συγκεκριμένα, στο 92.3% των περιπτώσεων οι συνεργάτες της εταιρίας δεν έχουν πρόσβαση στα δεδομένα των πελατών.

Πίνακας 9: Πρόσβαση συνεργατών στα δεδομένα των πελατών

	Συχνότητα	Ποσοστό	Έγκυρο ποσοστό	Αθροιστικό ποσοστό
Ναι	2	7.7	7.7	7.7
Όχι	24	92.3	92.3	100.0
Σύνολο	26	100.0	100.0	



Διάγραμμα 8 - Πρόσβαση συνεργατών στα δεδομένα των πελατών

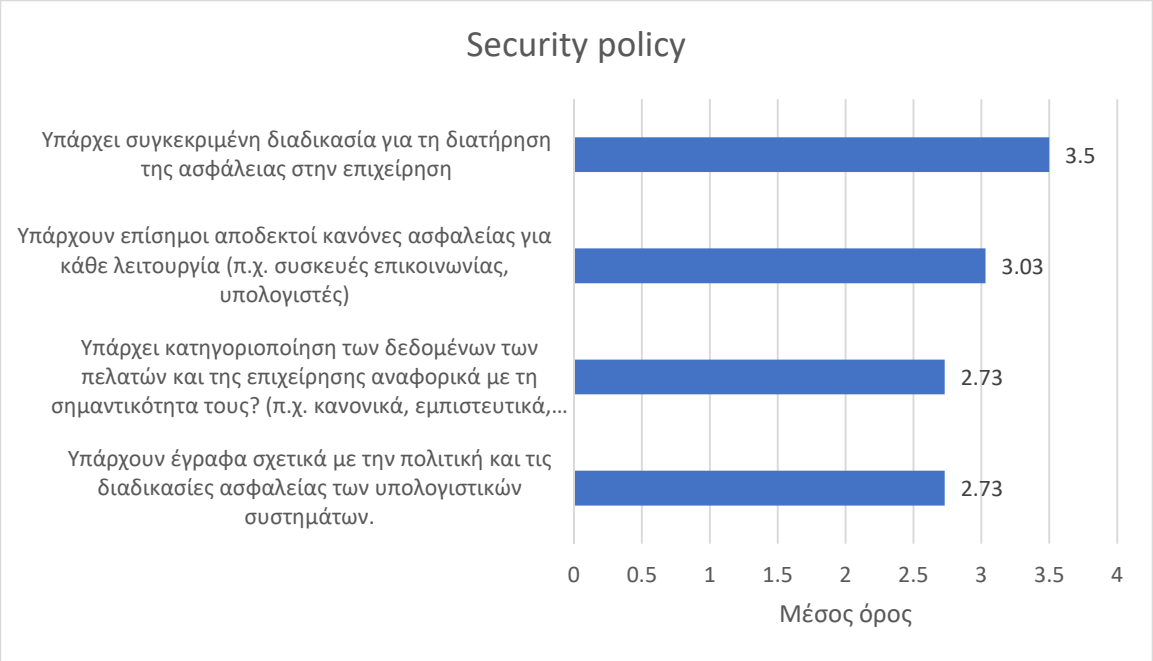
- Security Policy

Ο Πίνακας 10 και το Διάγραμμα 9 παρουσιάζουν τις συχνότητες και τα ποσοστά των απαντήσεων των ερωτηθέντων σχετικά με το Security Policy που ακολουθείται στην εταιρία που εργάζονται. Συγκεκριμένα, οι ερωτώμενοι δήλωσαν σε μεγαλύτερο βαθμό πως υπάρχει συγκεκριμένη διαδικασία για τη διατήρηση της ασφάλειας στην επιχείρηση

(M = 3.50) και ακολούθως πως υπάρχουν επίσημοι αποδεκτοί κανόνες ασφαλείας για κάθε λειτουργία (π.χ. συσκευές επικοινωνίας, υπολογιστές) (M = 3.03).

Πίνακας 10: Security policy

	1 = Καθόλου, 5 = Πάρα πολύ	1	2	3	4	5	Μέσος όρος
12	Υπάρχουν έγραφα σχετικά με την πολιτική και τις διαδικασίες ασφαλείας των υπολογιστικών συστημάτων.	34.6	15.4	7.7	26.9	15.4	2.73
13	Υπάρχει κατηγοριοποίηση των δεδομένων των πελατών και της επιχείρησης αναφορικά με τη σημαντικότητα τους? (π.χ. κανονικά, εμπιστευτικά, απόρρητα)	34.6	15.4	15.4	11.5	23.1	2.73
14	Υπάρχουν επίσημοι αποδεκτοί κανόνες ασφαλείας για κάθε λειτουργία (π.χ. συσκευές επικοινωνίας, υπολογιστές)	19.2	26.9	11.5	15.4	26.9	3.03
15	Υπάρχει συγκεκριμένη διαδικασία για τη διατήρηση της ασφάλειας στην επιχείρηση	-	33.3	12.5	25	29.2	3.50



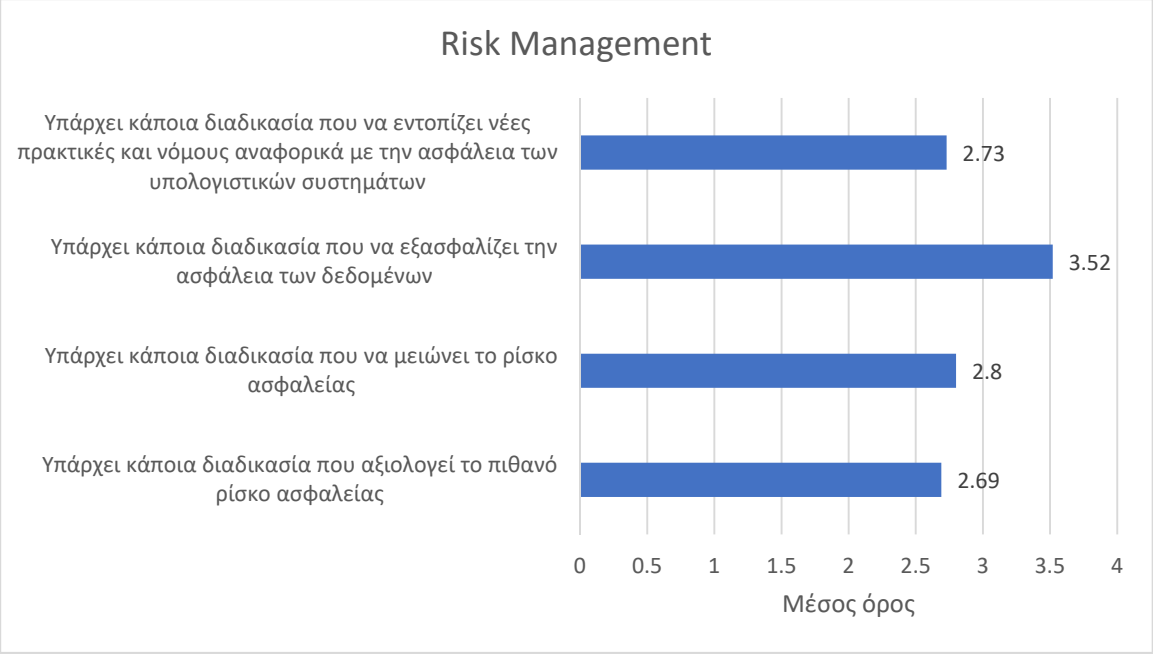
Διάγραμμα 9 - Security policy

- Risk Management

Ο Πίνακας 11 και το Διάγραμμα 10 παρουσιάζουν τις συχνότητες και τα ποσοστά των απαντήσεων των ερωτηθέντων σχετικά με το Risk Management που ακολουθείται στην εταιρία που εργάζονται. Συγκεκριμένα, οι ερωτώμενοι δήλωσαν σε μεγαλύτερο βαθμό πως υπάρχει κάποια διαδικασία που να εξασφαλίζει την ασφάλεια των δεδομένων (M = 3.52) και ακολούθως πως υπάρχει κάποια διαδικασία που να μειώνει το ρίσκο ασφαλείας (M = 2.80).

Πίνακας 11: Risk Management

	1 = Καθόλου, 5 = Πάρα πολύ	1	2	3	4	5	Μέσος όρος
16	Υπάρχει κάποια διαδικασία που αξιολογεί το πιθανό ρίσκο ασφαλείας	34.6	15.4	15.4	15.4	19.2	2.69
17	Υπάρχει κάποια διαδικασία που να μειώνει το ρίσκο ασφαλείας	23.1	23.1	19.2	19.2	15.4	2.80
18	Υπάρχει κάποια διαδικασία που να εξασφαλίζει την ασφάλεια των δεδομένων	4	24	16	28	28	3.52
19	Υπάρχει κάποια διαδικασία που να εντοπίζει νέες πρακτικές και νόμους αναφορικά με την ασφάλεια των υπολογιστικών συστημάτων	23.1	26.9	19.2	15.4	15.4	2.73



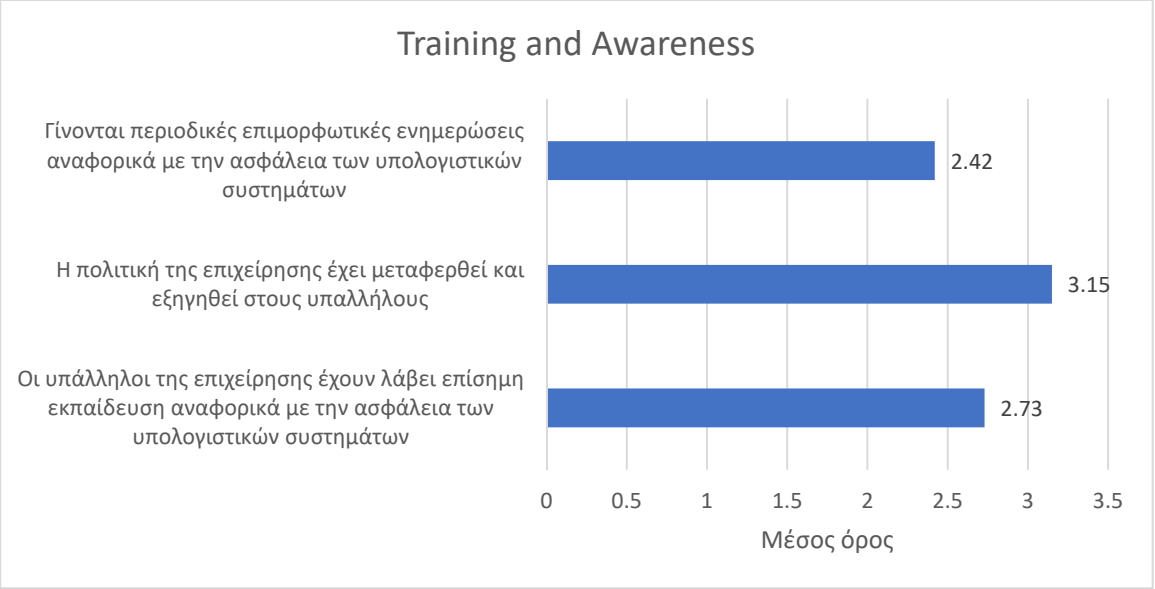
Διάγραμμα 10 - Risk Management

- Training and Awareness

Ο Πίνακας 12 και το Διάγραμμα 11 παρουσιάζουν τις συχνότητες και τα ποσοστά των απαντήσεων των ερωτηθέντων σχετικά με το Training and Awareness που ακολουθείται στην εταιρία που εργάζονται. Συγκεκριμένα, οι ερωτώμενοι δήλωσαν σε μεγαλύτερο βαθμό πως η πολιτική της επιχείρησης έχει μεταφερθεί και εξηγηθεί στους υπαλλήλους (M = 3.15).

Πίνακας 12: Training and Awareness

	1 = Καθόλου, 5 = Πάρα πολύ	1	2	3	4	5	Μέσος όρος
20	Οι υπάλληλοι της επιχείρησης έχουν λάβει επίσημη εκπαίδευση αναφορικά με την ασφάλεια των υπολογιστικών συστημάτων	11.5	30.8	38.5	11.5	7.7	2.73
21	Η πολιτική της επιχείρησης έχει μεταφερθεί και εξηγηθεί στους υπαλλήλους	3.8	34.6	19.2	26.9	15.4	3.15
22	Γίνονται περιοδικές επιμορφωτικές ενημερώσεις αναφορικά με την ασφάλεια των υπολογιστικών συστημάτων	23.1	34.6	26.9	7.7	7.7	2.42



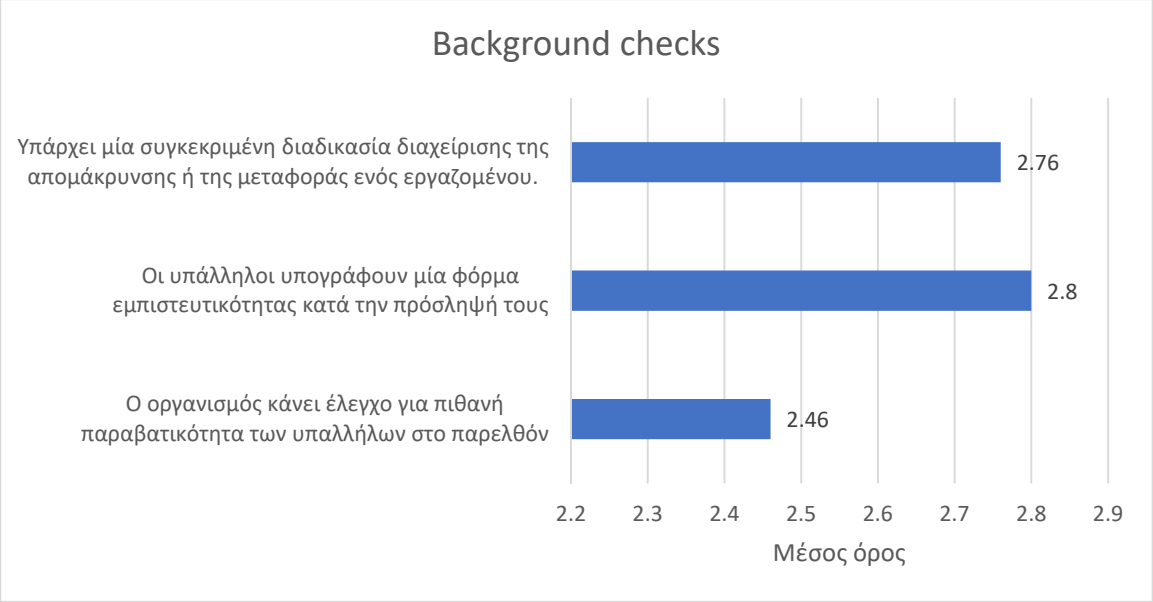
Διάγραμμα 11 - Training and Awareness

- Background checks

Ο Πίνακας 13 και το Διάγραμμα 12 παρουσιάζουν τις συχνότητες και τα ποσοστά των απαντήσεων των ερωτηθέντων σχετικά με το Background checks που ακολουθείται στην εταιρία που εργάζονται. Συγκεκριμένα, οι ερωτώμενοι δήλωσαν σε μεγαλύτερο βαθμό πως οι υπάλληλοι υπογράφουν μία φόρμα εμπιστευτικότητας κατά την πρόσληψή τους (M = 2.80).

Πίνακας 13: Background checks

	1 = Καθόλου, 5 = Πάρα πολύ	1	2	3	4	5	Μέσος όρος
23	Ο οργανισμός κάνει έλεγχο για πιθανή παραβατικότητα των υπαλλήλων στο παρελθόν	38.5	26.9	-	19.2	15.4	2.46
24	Οι υπάλληλοι υπογράφουν μία φόρμα εμπιστευτικότητας κατά την πρόσληψή τους	36	16	4	20	24	2.80
25	Υπάρχει μία συγκεκριμένη διαδικασία διαχείρισης της απομάκρυνσης ή της μεταφοράς ενός εργαζομένου.	34.6	15.4	7.7	23.1	19.2	2.76



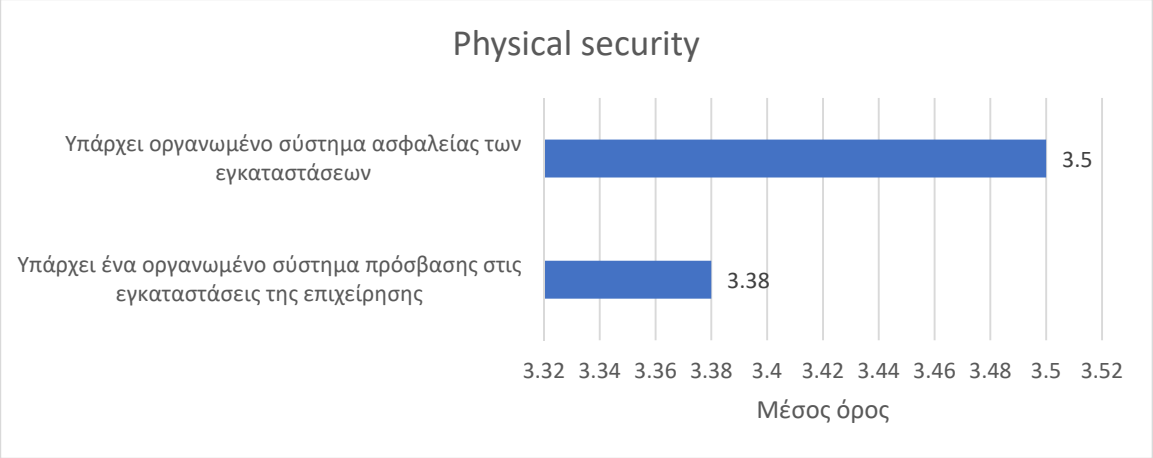
Διάγραμμα 12 - Background checks

- Physical security

Ο Πίνακας 14 και το Διάγραμμα 13 παρουσιάζουν τις συχνότητες και τα ποσοστά των απαντήσεων των ερωτηθέντων σχετικά με το Physical security που ακολουθείται στην εταιρία που εργάζονται. Συγκεκριμένα, οι ερωτώμενοι δήλωσαν σε μεγαλύτερο βαθμό πως υπάρχει οργανωμένο σύστημα ασφαλείας των εγκαταστάσεων (M = 3.50) καθώς επίσης σε μεγάλο βαθμό υπάρχει ένα οργανωμένο σύστημα πρόσβασης στις εγκαταστάσεις της επιχείρησης (M = 3.38).

Πίνακας 14: Physical security

	1 = Καθόλου, 5 = Πάρα πολύ	1	2	3	4	5	Μέσος όρος
26	Υπάρχει ένα οργανωμένο σύστημα πρόσβασης στις εγκαταστάσεις της επιχείρησης	7.7	19.2	23.1	26.9	23.1	3.38
27	Υπάρχει οργανωμένο σύστημα ασφαλείας των εγκαταστάσεων	7.7	15.4	23.1	26.9	26.9	3.50



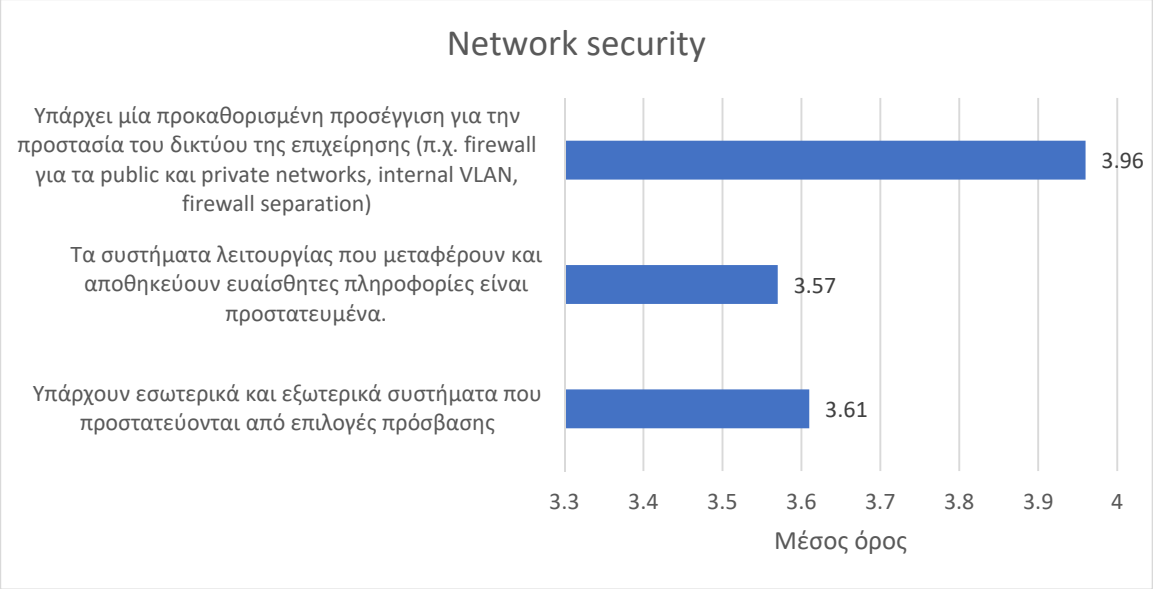
Διάγραμμα 13 - Physical security

- Network security

Ο Πίνακας 15 και το Διάγραμμα 14 παρουσιάζουν τις συχνότητες και τα ποσοστά των απαντήσεων των ερωτηθέντων σχετικά με το Network security που ακολουθείται στην εταιρία που εργάζονται. Συγκεκριμένα, οι ερωτώμενοι δήλωσαν σε μεγαλύτερο βαθμό πως υπάρχει μία προκαθορισμένη προσέγγιση για την προστασία του δικτύου της επιχείρησης (π.χ. firewall για τα public και private networks, internal VLAN, firewall separation) (M = 3.96).

Πίνακας 15: Network security

	1 = Καθόλου, 5 = Πάρα πολύ	1	2	3	4	5	Μέσος όρος
28	Υπάρχουν εσωτερικά και εξωτερικά συστήματα που προστατεύονται από επιλογές πρόσβασης	3.8	15.4	19.2	38.5	23.1	3.61
29	Τα συστήματα λειτουργίας που μεταφέρουν και αποθηκεύουν ευαίσθητες πληροφορίες είναι προστατευμένα.	3.8	15.4	26.9	26.9	26.9	3.57
30	Υπάρχει μία προκαθορισμένη προσέγγιση για την προστασία του δικτύου της επιχείρησης (π.χ. firewall για τα public και private networks, internal VLAN, firewall separation)	-	24	8	16	52	3.96



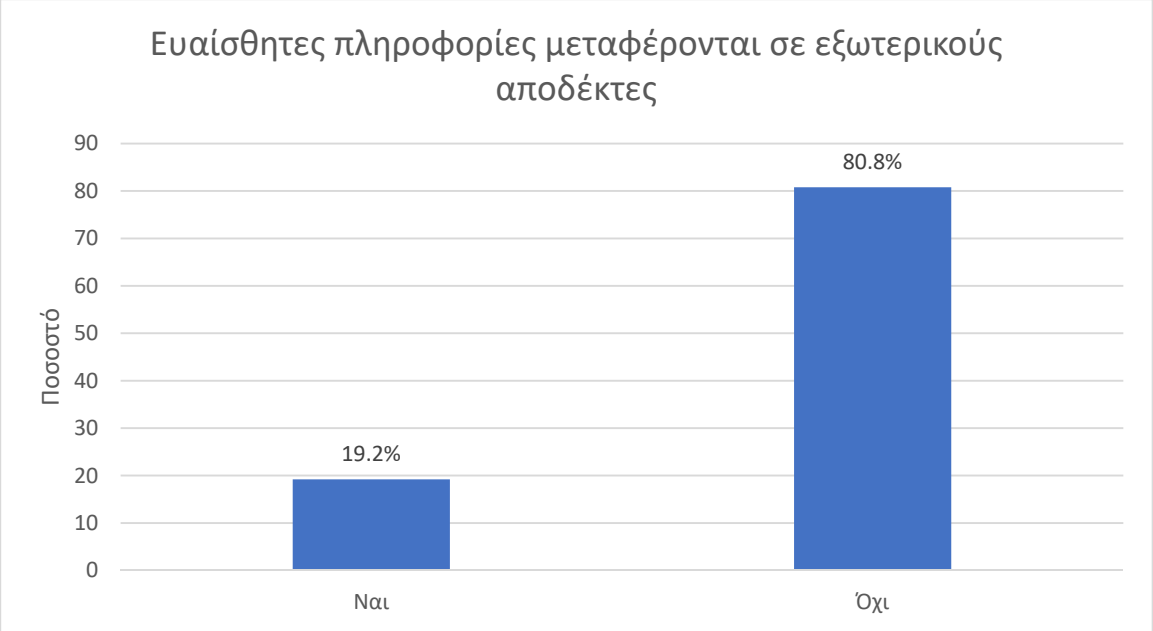
Διάγραμμα 14 - Network security

31. Ευαίσθητες πληροφορίες μεταφέρονται σε εξωτερικούς αποδέκτες

Όπως φαίνεται από τον Πίνακα 16 και το Διάγραμμα 15 παρουσιάζουν τις συχνότητες και τα ποσοστά των απαντήσεων των ερωτηθέντων σχετικά με το βαθμό στον οποίο οι ευαίσθητες πληροφορίες μεταφέρονται σε εξωτερικούς αποδέκτες. Συγκεκριμένα, οι ερωτώμενοι δήλωσαν σε ποσοστό 80.8% πως οι ευαίσθητες πληροφορίες δεν μεταφέρονται σε εξωτερικούς αποδέκτες.

Πίνακας 16: Ευαίσθητες πληροφορίες μεταφέρονται σε εξωτερικούς αποδέκτες

	Συχνότητα	Ποσοστό	Έγκυρο ποσοστό	Αθροιστικό ποσοστό
Ναι	5	19.2	19.2	19.2
Όχι	21	80.8	80.8	100.0
Σύνολο	26	100.0	100.0	

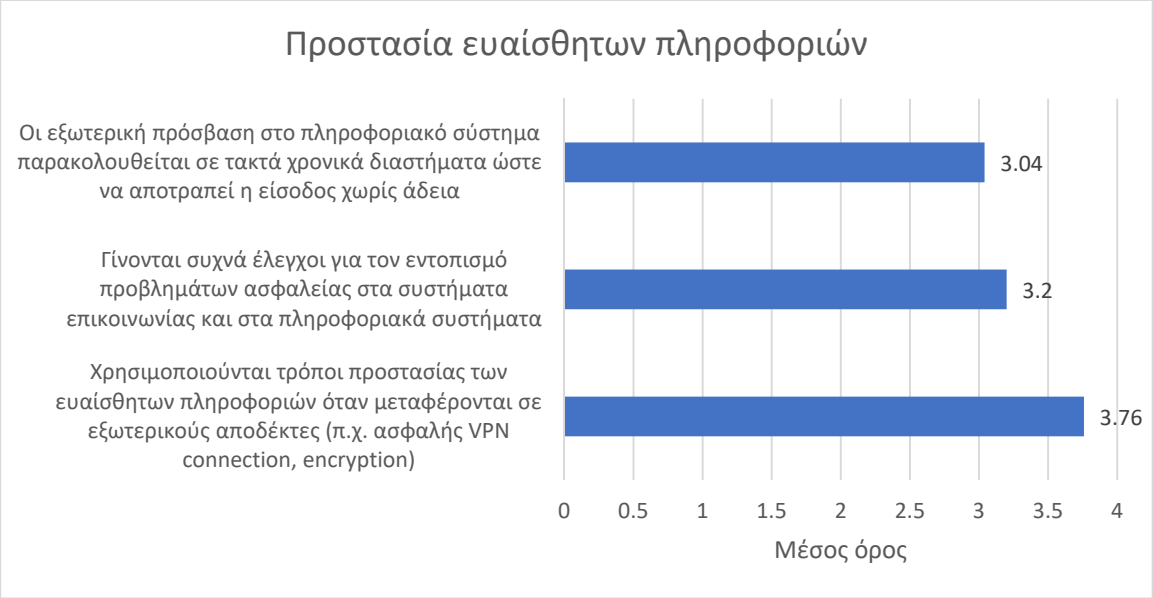


Διάγραμμα 15 - Ευαίσθητες πληροφορίες μεταφέρονται σε εξωτερικούς αποδέκτες

Επίσης, η επιχείρηση χρησιμοποιεί σε αρκετά μεγάλο βαθμό τρόπους προστασίας των ευαίσθητων πληροφοριών όταν μεταφέρονται σε εξωτερικούς αποδέκτες (π.χ. ασφαλής VPN connection, encryption) (M = 3.76).

Πίνακας 17: Προστασία ευαίσθητων πληροφοριών

	1 = Καθόλου, 5 = Πάρα πολύ	1	2	3	4	5	Μέσος όρος
32	Χρησιμοποιούνται τρόποι προστασίας των ευαίσθητων πληροφοριών όταν μεταφέρονται σε εξωτερικούς αποδέκτες (π.χ. ασφαλής VPN connection, encryption)	4	16	12	36	32	3.76
33	Γίνονται συχνά έλεγχοι για τον εντοπισμό προβλημάτων ασφαλείας στα συστήματα επικοινωνίας και στα πληροφοριακά συστήματα	8	32	16	20	24	3.20
34	Οι εξωτερική πρόσβαση στο πληροφοριακό σύστημα παρακολουθείται σε τακτά χρονικά διαστήματα ώστε να αποτραπεί η είσοδος χωρίς άδεια	16	28	12	24	20	3.04



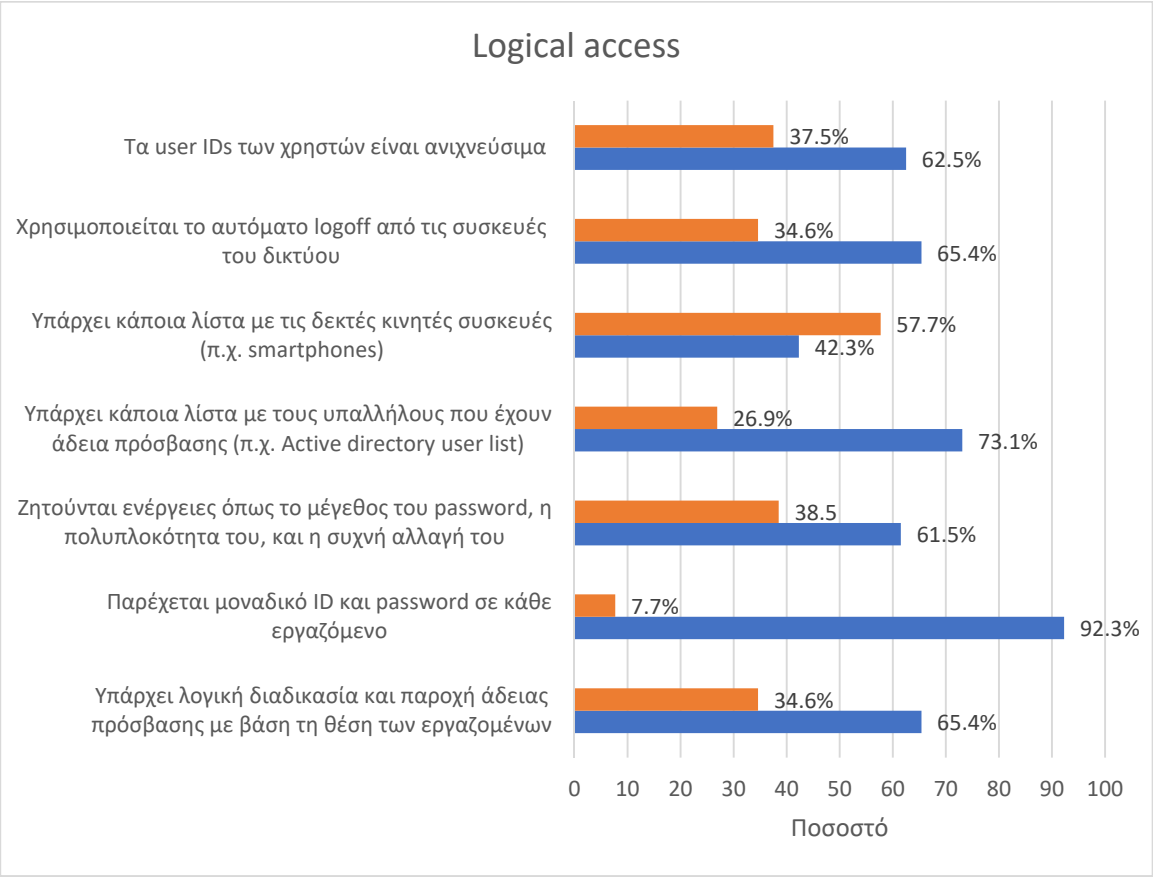
Διάγραμμα 16 - Προστασία ευαίσθητων πληροφοριών

- Logical access

Ο Πίνακας 18 και το Διάγραμμα 17 παρουσιάζουν τις συχνότητες και τα ποσοστά των απαντήσεων των ερωτηθέντων σχετικά με τις πρακτικές Logical access που ακολουθούνται στην εταιρία που εργάζονται. Συγκεκριμένα, οι ερωτώμενοι δήλωσαν σε μεγαλύτερο βαθμό πως παρέχεται μοναδικό ID και password σε κάθε εργαζόμενο (92.3%) και ακολούθως πως υπάρχει κάποια λίστα με τους υπαλλήλους που έχουν άδεια πρόσβασης (π.χ. Active directory user list) (73.1%), πως υπάρχει λογική διαδικασία και παροχή άδειας πρόσβασης με βάση τη θέση των εργαζομένων (65.4%) και πως χρησιμοποιείται το αυτόματο logoff από τις συσκευές του δικτύου (65.4%).

Πίνακας 18: Logical access

		ΝΑΙ	ΟΧΙ
35	Υπάρχει λογική διαδικασία και παροχή άδειας πρόσβασης με βάση τη θέση των εργαζομένων	65.4	34.6
36	Παρέχεται μοναδικό ID και password σε κάθε εργαζόμενο	92.3	7.7
37	Ζητούνται ενέργειες όπως το μέγεθος του password, η πολυπλοκότητα του, και η συχνή αλλαγή του	61.5	38.5
38	Υπάρχει κάποια λίστα με τους υπαλλήλους που έχουν άδεια πρόσβασης (π.χ. Active directory user list)	73.1	26.9
39	Υπάρχει κάποια λίστα με τις δεκτές κινητές συσκευές (π.χ. smartphones)	42.3	57.7
40	Χρησιμοποιείται το αυτόματο logoff από τις συσκευές του δικτύου	65.4	34.6
41	Τα user IDs των χρηστών είναι ανιχνεύσιμα	62.5	37.5



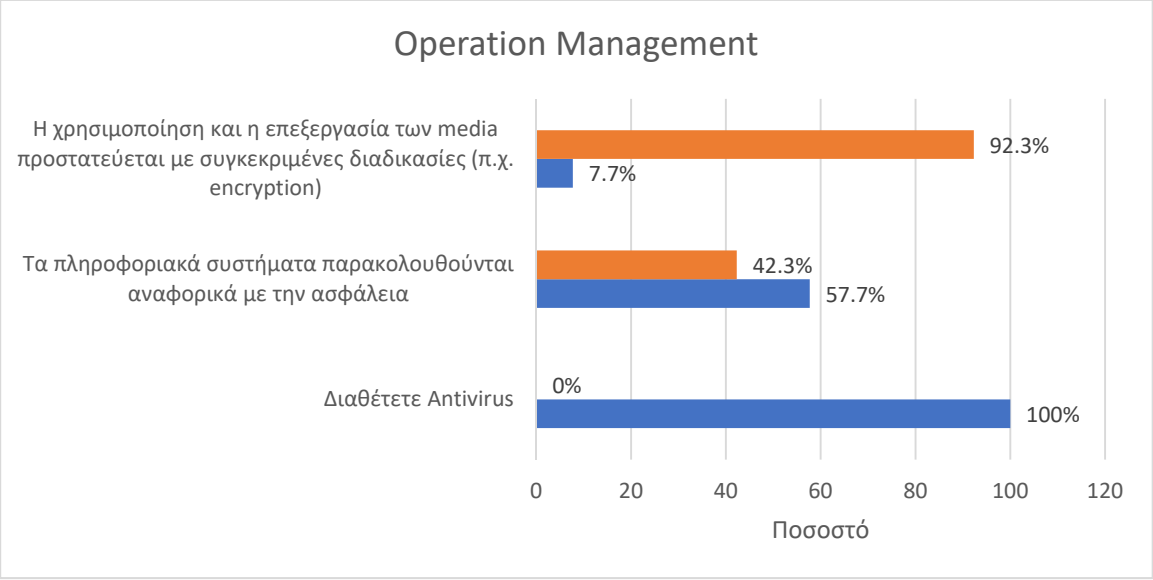
Διάγραμμα 17 - Logical access

42. Operation Management

Ο Πίνακας 19 και το Διάγραμμα 18 παρουσιάζει τα ποσοστά των απαντήσεων των ερωτηθέντων σχετικά με το Operation Management που ακολουθείται στην εταιρία που εργάζονται. Συγκεκριμένα, οι ερωτώμενοι δήλωσαν στο σύνολο τους πως η επιχείρηση στην οποία εργάζονται διαθέτει Antivirus και ακολούθως πως τα πληροφοριακά συστήματα παρακολουθούνται αναφορικά με την ασφάλεια (57.7%).

Πίνακας 19: Operation Management

	NAI	OXI
Διαθέτετε Antivirus	100	-
Τα πληροφοριακά συστήματα παρακολουθούνται αναφορικά με την ασφάλεια	57.7	42.3
Η χρησιμοποίηση και η επεξεργασία των media προστατεύεται με συγκεκριμένες διαδικασίες (π.χ. encryption)	7.7	92.3



Διάγραμμα 18 - Operation Management

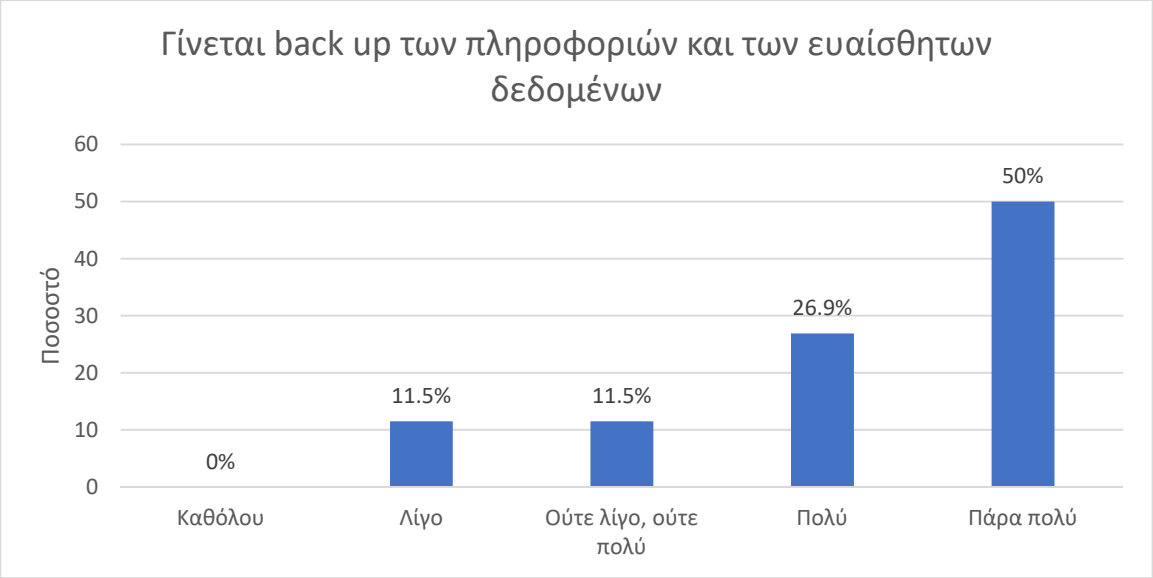
- Business continuity management

Ο Πίνακας 20 και το Διάγραμμα 19 παρουσιάζει τα ποσοστά των απαντήσεων των ερωτηθέντων σχετικά με το εάν γίνεται back up των πληροφοριών και των ευαίσθητων δεδομένων στην επιχείρηση στην οποία εργάζονται. Συγκεκριμένα, οι ερωτώμενοι

δήλωσαν πως σε πάρα πολύ μεγάλο βαθμό γίνεται back up των πληροφοριών και των ευαίσθητων δεδομένων που συγκεντρώνονται.

Πίνακας 20: Γίνεται back up των πληροφοριών και των ευαίσθητων δεδομένων

	Συχνότητα	Ποσοστό	Έγκυρο ποσοστό	Αθροιστικό ποσοστό
Λίγο	3	11.5	11.5	11.5
Ούτε λίγο, ούτε πολύ	3	11.5	11.5	23.1
Πολύ	7	26.9	26.9	50.0
Πάρα πολύ	13	50.0	50.0	100.0
Σύνολο	26	100.0	100.0	



Διάγραμμα 19 - Γίνεται back up των πληροφοριών και των ευαίσθητων δεδομένων

4.2. Συγκριτική Στατιστική Ανάλυση

Το παρόν κεφάλαιο παρουσιάζει την παρουσίαση των στατιστικών ευρημάτων μετά από τις συσχετίσεις μεταξύ των μεταβλητών. Υπενθυμίζεται πως όπως έχει αναφερθεί στο κεφάλαιο της μεθοδολογίας της έρευνας το επίπεδο σημαντικότητας είναι 0.05. Ακόμα, θα αναφερθούν μόνο οι συσχετίσεις που βρέθηκαν στατιστικά σημαντικές.

- Συσχέτιση του αριθμού των εργαζομένων της επιχείρησης με τις πρακτικές που ακολουθεί.

Όπως προκύπτει από το παραμετρικό τεστ Pearson υπάρχει στατιστικά σημαντική συσχέτιση του αριθμού των εργαζομένων με:

- Την ύπαρξη κατηγοριοποίησης των δεδομένων των πελατών και της επιχείρησης αναφορικά με τη σημαντικότητα τους (θετική μέτρια συσχέτιση, $r = .389$, $p < 0.05$)
- Το κατά πόσο ο οργανισμός κάνει έλεγχο για πιθανή παραβατικότητα των υπάλληλων στο παρελθόν (θετική μέτρια συσχέτιση, $r = .454$, $p < 0.05$)
- Την ύπαρξη εσωτερικών και εξωτερικών συστημάτων που προστατεύονται από επιλογές πρόσβασης (θετική μέτρια συσχέτιση, $r = .480$, $p < 0.05$)
- Το κατά πόσο τα συστήματα λειτουργιάς που μεταφέρουν και αποθηκεύουν ευαίσθητες πληροφορίες είναι προστατευμένα (θετική μέτρια συσχέτιση, $r = .401$, $p < 0.05$)
- Την ύπαρξη μίας προκαθορισμένης προσέγγισης για την προστασία του δικτυού της επιχείρησης (θετική μέτρια συσχέτιση, $r = .552$, $p < 0.001$)
- Το κατά πόσο χρησιμοποιούνται τρόποι προστασίας των ευαίσθητων πληροφοριών όταν μεταφέρονται σε εξωτερικούς αποδέκτες (θετική μέτρια συσχέτιση, $r = .515$, $p < 0.001$)
- Το κατά πόσο η εξωτερική πρόσβαση στο πληροφοριακό σύστημα παρακολουθείται σε τακτά χρονικά διαστήματα ώστε να αποτραπεί η είσοδος χωρίς άδεια (θετική μέτρια συσχέτιση, $r = .486$, $p < 0.05$)
- Το κατά πόσο γίνεται back up των πληροφοριών και των ευαίσθητων δεδομένων (θετική μέτρια συσχέτιση, $r = .398$, $p < 0.05$)

21. **Correlations**

		Αριθμός εργαζομένων	1	2	3	4	5	6	7	8
Αριθμός εργαζομένων	Pearson Correlation	1	.389*	.454*	.480*	.401*	.552**	.515**	.486*	.398*
1) Υπάρχει κατηγοριοποίηση των δεδομένων των πελατών και της επιχείρησης αναφορικά με τη σημαντικότητα τους?	Pearson Correlation		1	.673**	.837**	.783**	.769**	.703**	.709**	.475*
2) Ο οργανισμός κάνει έλεγχο για πιθανή παραβατικότητα των υπάλληλων στο παρελθόν	Pearson Correlation			1	.558**	.616**	.567**	.456*	.617**	.618**
3) Υπάρχουν εσωτερικά και εξωτερικά συστήματα που προστατεύονται από επιλογές πρόσβασης	Pearson Correlation				1	.836**	.899**	.740**	.818**	.557**
4) Τα συστήματα λειτουργιάς που μεταφέρουν και αποθηκεύουν ευαίσθητες πληροφορίες είναι προστατευμένα	Pearson Correlation					1	.841**	.738**	.767**	.707**
5) Υπάρχει μια προκαθορισμένη προσέγγιση για την προστασία του δικτυού της επιχείρησης	Pearson Correlation						1	.833**	.780**	.709**
6) Χρησιμοποιούνται τρόποι προστασίας των ευαίσθητων πληροφοριών όταν μεταφέρονται σε εξωτερικούς αποδέκτες	Pearson Correlation							1	.785**	.551**
7) Η εξωτερική πρόσβαση στο πληροφοριακό σύστημα παρακολουθείται σε τακτά χρονικά διαστήματα ώστε να αποτραπεί η είσοδος χωρίς άδεια	Pearson Correlation								1	.606**
8) Γίνεται back up των πληροφοριών και των ευαίσθητων δεδομένων	Pearson Correlation									1

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

- Είδος ιδιοκτησίας της επιχείρησης / Γίνεται back up των πληροφοριών και των ευαίσθητων δεδομένων

Όπως προκύπτει από την ανάλυση διασποράς (ANOVA) το p-value (0.048) είναι μικρότερο του a (0.05) επομένως συμπεραίνουμε πως υπάρχει στατιστικά σημαντική συσχέτιση και πως οι κλάσεις της μεταβλητής "Είδος ιδιοκτησίας της επιχείρησης" διαφέρουν σε σχέση με το κατά πόσο γίνεται back up των πληροφοριών και των ευαίσθητων δεδομένων.

22. **ANOVA**

Γίνεται back up των πληροφοριών και των ευαίσθητων δεδομένων

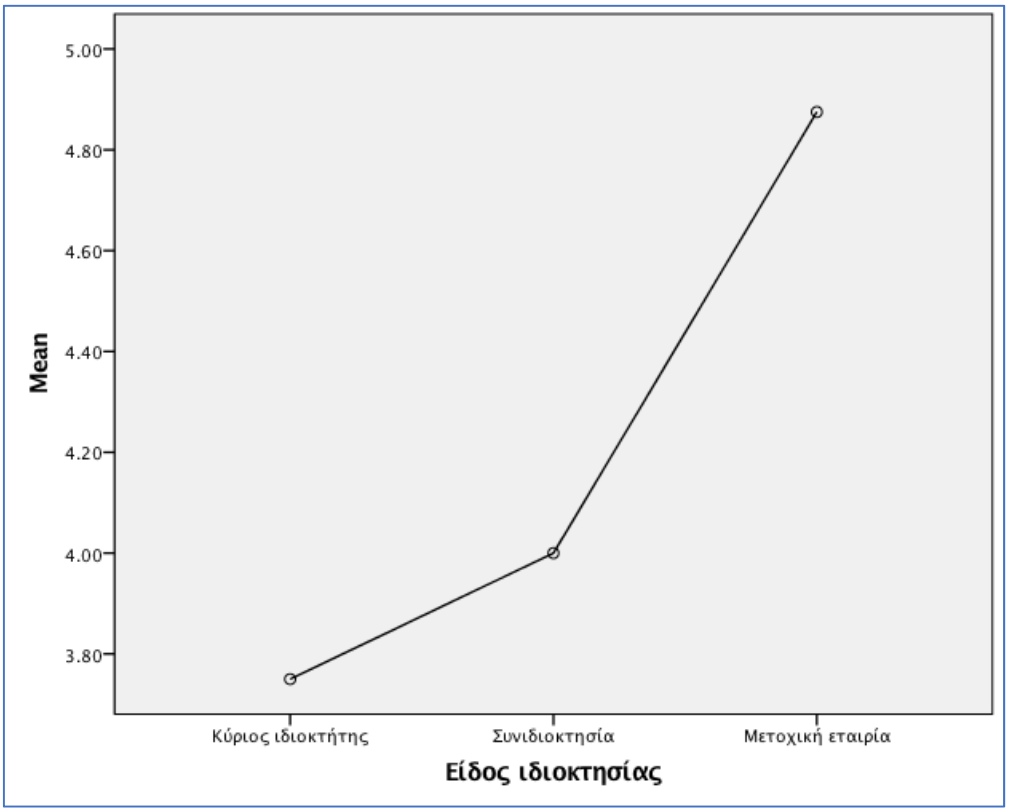
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	6.260	2	3.130	3.408	.048
Within Groups	21.125	23	.918		
Σύνολο	27.385	25			

Επίσης, όπως φαίνεται από τον παρακάτω πίνακα και διάγραμμα μέσων όρων στις επιχειρήσεις με μετοχική σύνθεση γίνεται σε μεγαλύτερο βαθμό back up των πληροφοριών και των ευαίσθητων δεδομένων (M = 4.87, T.A. = .353) και ακολούθως στις επιχειρήσεις με συνιδιοκτησία (M = 4.00, T.A. = 1.26).

*23.***Descriptives**

Γίνεται back up των πληροφοριών και των ευαίσθητων δεδομένων

	N	Μέσος όρος	Τυπική απόκλιση	Std. Error	95% Confidence Interval for Mean		Ελάχιστο	Μέγιστο
					Lower Bound	Upper Bound		
Κύριος ιδιοκτήτης	12	3.7500	1.05529	.30464	3.0795	4.4205	2.00	5.00
Συνιδιοκτησία	6	4.0000	1.26491	.51640	2.6726	5.3274	2.00	5.00
Μετοχική εταιρία	8	4.8750	.35355	.12500	4.5794	5.1706	4.00	5.00
Σύνολο	26	4.1538	1.04661	.20526	3.7311	4.5766	2.00	5.00



Διάγραμμα 20 - Descriptives. Γίνεται back up των πληροφοριών και των ευαίσθητων δεδομένων

- Είδος ιδιοκτησίας της επιχείρησης / Υπάρχει μια προκαθορισμένη προσέγγιση για την προστασία του δικτυού της επιχείρησης

Όπως προκύπτει από την ανάλυση διασποράς (ANOVA) το p-value (0.008) είναι μικρότερο του a (0.05) επομένως συμπεραίνουμε πως υπάρχει στατιστικά σημαντική συσχέτιση και πως οι κλάσεις της μεταβλητής "Είδος ιδιοκτησίας της επιχείρησης" διαφέρουν σε σχέση με την ύπαρξη μίας προκαθορισμένης προσέγγισης για την προστασία του δικτυού της επιχείρησης.

24.**ANOVA**

Υπάρχει μια προκαθορισμένη προσέγγιση για την προστασία του δικτυού της επιχείρησης

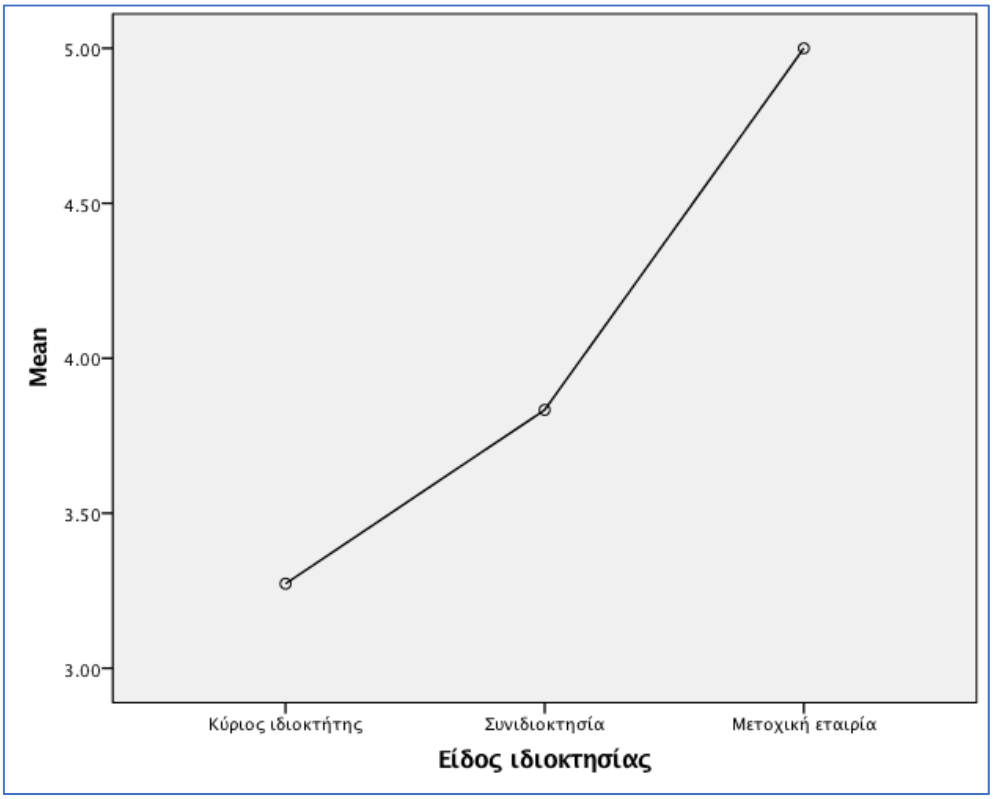
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	13.945	2	6.972	6.132	.008
Within Groups	25.015	22	1.137		
Σύνολο	38.960	24			

Επίσης, όπως φαίνεται από τον παρακάτω πίνακα και διάγραμμα μέσων όρων στις επιχειρήσεις με μετοχική σύνθεση υπάρχει σε μεγαλύτερο βαθμό μια προκαθορισμένη προσέγγιση για την προστασία του δικτυού της επιχείρησης (M = 5.00, T.A. = .000) και ακολούθως αυτό συμβαίνει στις επιχειρήσεις με συνιδιοκτησία (M = 3.83, T.A. = 1.47).

25.**Descriptives**

Υπάρχει μια προκαθορισμένη προσέγγιση για την προστασία του δικτυού της επιχείρησης

	N	Μέσος όρος	Τυπική απόκλιση	Std. Error	95% Confidence Interval for Mean		Ελάχιστο	Μέγιστο
					Lower Bound	Upper Bound		
Κύριος ιδιοκτήτης	11	3.2727	1.19087	.35906	2.4727	4.0728	2.00	5.00
Συνιδιοκτησία	6	3.8333	1.47196	.60093	2.2886	5.3781	2.00	5.00
Μετοχική εταιρία	8	5.0000	.00000	.00000	5.0000	5.0000	5.00	5.00
Σύνολο	25	3.9600	1.27410	.25482	3.4341	4.4859	2.00	5.00



Διάγραμμα 21 - Descriptives. Υπάρχει μια προκαθορισμένη προσέγγιση για την προστασία του δικτυού της επιχείρησης

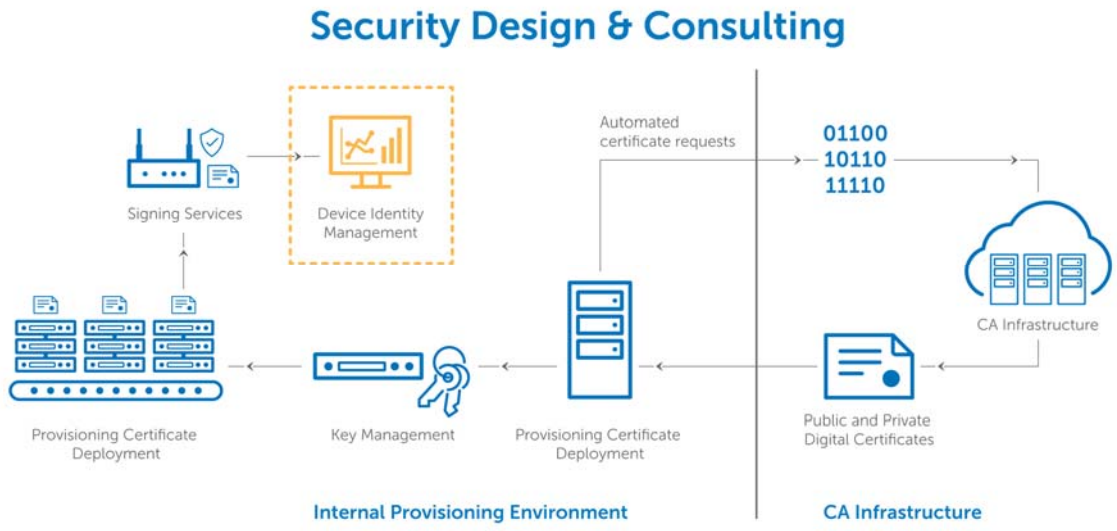
Κεφάλαιο 5
Μοντέλο Διαχείρισης Ταυτότητας

Η ασφάλεια του δικτύου προϋποθέτει την ταυτοποίηση των συσκευών και είναι αδιαμφισβήτητα σημαντικός παράγοντας για τη διασφάλισή των δεδομένων και τη λογοδοσία, η οποία είναι απαραίτητο συστατικό στην πολιτική ασφάλειας, ανεξάρτητα από το μέγεθος της επιχείρησης.

Η διαχείριση ταυτοποίησης και πρόσβασης αποτελεί μια συνεχή πρόκληση για το δίκτυο της επιχείρησης, η αναγκαιότητα επικαιροποίησης και αναβάθμισης αποτελεί βασικό κομμάτι τόσο στην ασφάλεια του δικτύου και των πληροφοριών που διακινούνται σε αυτά, όσο και για την ιδιωτικότητα και την προστασία των προσωπικών δεδομένων των χρηστών. Η δυσκολία που διαφαίνεται λόγω της διαφορετικότητας συσκευών και πρωτοκόλλων διαχείρισης από πολυάριθμους προμηθευτές, καθιστούν το ενιαίο μοντέλο ταυτοποίησης πολύπλοκο. Ως εκ τούτου, πολλά πρότυπα στον τομέα της πληροφορικής τροποποιούνται ή αξιοποιούνται για να παρουσιάσουν αρχιτεκτονικές αναφοράς και βέλτιστες πρακτικές ασφάλειας για την τις IoT συσκευές στο Διαδίκτυο. Κοινή μεταξύ αυτών των πλαισίων είναι η ανάγκη, για μια ισχυρή, μοναδική και

αμετάβλητη ταυτότητα για κάθε συσκευή IoT. Η διαχείριση ταυτότητας μπορεί να χωριστεί σε 3 κατηγορίες, κεντρική, απομονωμένη και ομοσπονδιακή-federated.

Παρόλο που υπάρχουν διάφοροι τρόποι για ταυτοποίηση IoT συσκευών [20], αναλυτές της βιομηχανίας, σημαντικοί προμηθευτές πλατφόρμας cloud και καινοτόμες εταιρείες συμφωνούν ότι η υποδομή δημόσιου κλειδιού (Public Key Infrastructure) θα αποτελέσει τον επιλεγμένο μηχανισμό, για το παρόν, αλλά και το μέλλον. Η χρήση του δημοσίου κλειδιού έχει αναβαθμιστεί και προσαρμοστεί τώρα στον 21ο αιώνα, με όλο και πιο αυξημένη υιοθέτηση, αλλά και ευρεία εφαρμογή σε ποικίλο αριθμό περιπτώσεων. Η χρήση του δημοσίου κλειδιού προϋποθέτει την ύπαρξη μιας Ανεξάρτητης Αρχής Πιστοποίησης, αξιόπιστες διαπιστευτήριες οντότητες, όπου εκδίδουν πιστοποιητικά και είναι σε θέση να επιβεβαιώσουν την ταυτότητά τους. Ως εκ τούτου, ένα ψηφιακό πιστοποιητικό που εκδίδεται από μια Αρχή πιστοποίησης είναι μια καθολικά αποδεκτή πιστοποίηση ταυτότητας στις περισσότερες ψηφιακές πλατφόρμες. Στο ενδιάμεσο της Αρχής Πιστοποίησης και στην οντότητα όπου ζητά την ταυτοποίηση υπάρχει η Αρχή Εγράφης. Ευθύνη της είναι ο έλεγχος και η διαχείριση κατά την επαλήθευση της ταυτότητας πριν από την έκδοση της και παράλληλα η πιστοποίηση ότι συγκεκριμένο δημόσιο κλειδί ανήκει στην οντότητα που ζητά το πιστοποιητικό.



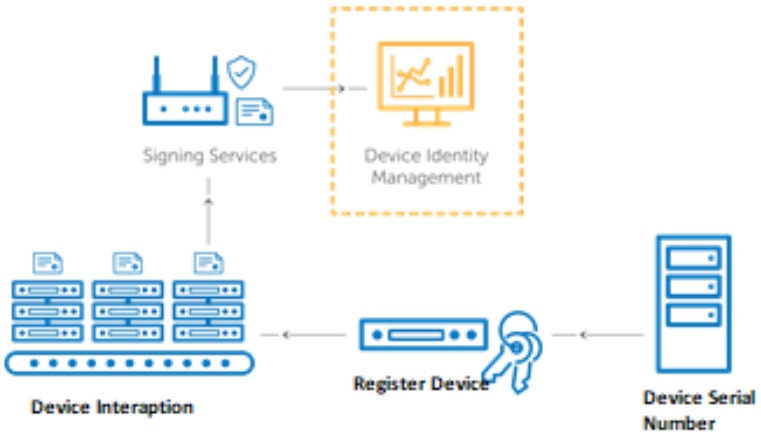
Εικόνα 3 -Γενικό Μοντέλο Διαχείρισης Ταυτότητας

[21]

Η υλοποίηση του πιο πάνω μοντέλου με βάση την ταυτοποίηση της συσκευής, πώς θα διαχωρίζεται η πρόσβαση και τα δικαιώματα στο εταιρικό δίκτυο, σε συνδυασμό με το χρήστη της συσκευής. Επίσης, η ύπαρξη πολυάριθμων IoT συσκευών σε διαφορετικά περιβάλλοντα, καθώς και η συμβατότητα, τόσο σε υφιστάμενες συσκευές, όσο και σε μελλοντικές συσκευές αποτελεί ένα σημαντικό πρόβλημα υλοποίησης. Η προσθήκη βοηθητικών στρωμάτων, για παράδειγμα μια μηχανή διαμόρφωσης και κανόνων, ομαδοποίηση και ταξινόμηση συσκευών σε συνδυασμό με τη δημιουργία τοπικών Αρχών Εγγραφής, θα μπορούσε να λύσει σε κάποιο βαθμό τα πιο πάνω προβλήματα. Η αυθεντικότητα της συσκευής σε σχέση με τη χρήση δημοσίου κλειδιού, θα μπορούσε να εφαρμοστεί με διάφορους τρόπους ή και σε συνδυασμό των πιο κάτω.

- Η χρήση του ενσωματωμένου αριθμού αναγνώρισης της συσκευής

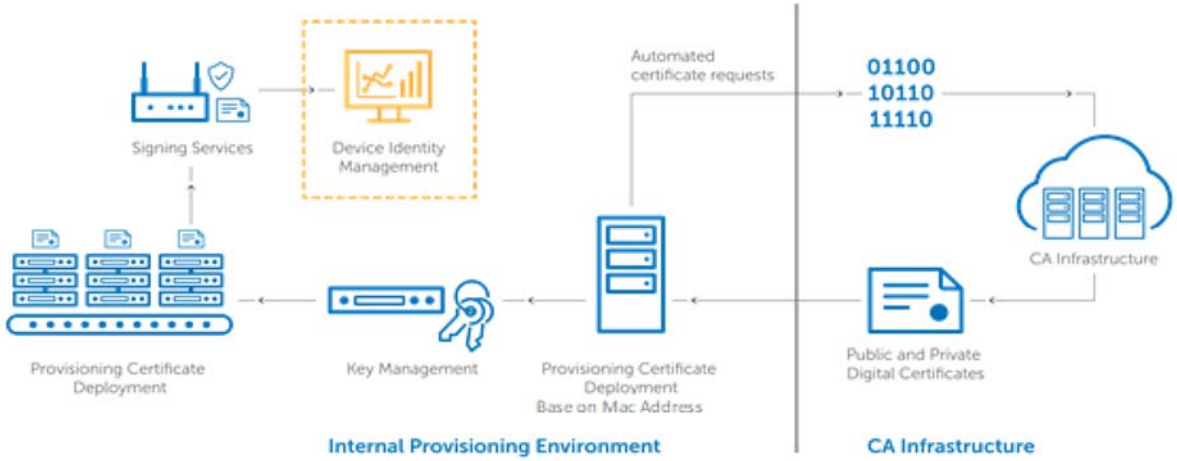
Το πλαίσιο, το οποίο φαίνεται να είναι ικανό να ανταπεξέλθει σε υφιστάμενες και μελλοντικές συσκευές IoT, έχει ως βάση τον αριθμό αναγνώρισης της συσκευή όπου ο κάθε κατασκευαστής χρησιμοποιεί κατά τη διαδικασία κατασκευής. Ο αριθμός αναγνώρισης θα μπορούσε να είναι ένα κοινόχρηστο μυστικό κλειδί, ένας μοναδικός αύξων αριθμός ή ένα άλλο πιστοποιητικό, που μερικές φορές ονομάζεται πιστοποιητικό γέννησης. Θα μπορούσαμε ,επίσης, να χρησιμοποιήσουμε ένα στοιχείο ασφαλείας υλικού, που είναι ενσωματωμένο στη συσκευή - μια μονάδα Trusted Platform Module (TPM) ή μια φυσική μη αποκλειστική λειτουργία - Physically Unclonable Function (PUF) βασισμένη σε υλικό.



Εικόνα 4- Μοντέλο Διαχείρισης Ταυτότητας. Χρήση ενσωματωμένου αριθμού αναγνώρισης

- Βάση λίστας εξουσιοδοτημένων συσκευών

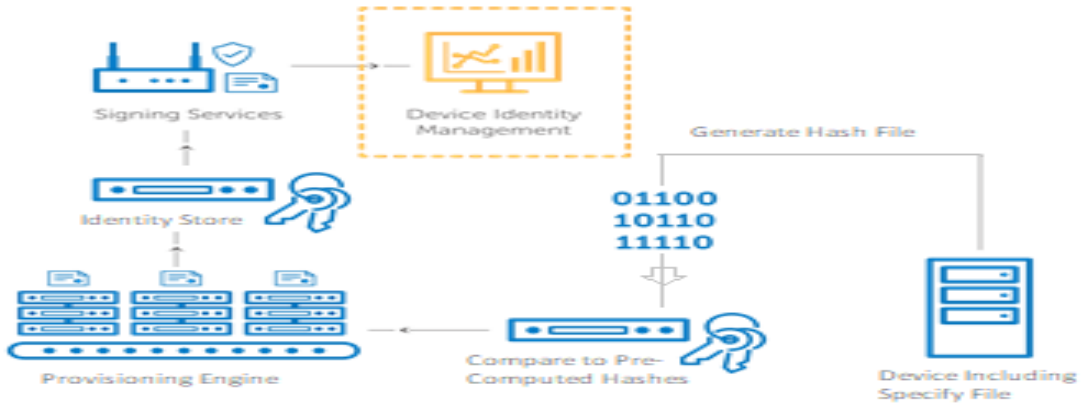
Η δημιουργία μιας λίστας επιτρεπόμενων συσκευών με τη χρήση μοναδικού χαρακτηριστικού, όπως είναι η διεύθυνση MAC Αρχή Εγγραφής θα είναι η αρμόδια αρχή, όπου θα εγκρίνει την εν λόγω λίστα. Για να έχει πρόσβαση η οποιαδήποτε εξουσιοδοτημένη συσκευή, η Αρχή Εγράφης θα μπορούσε να αποστέλλει πρόσκληση ανταπόκρισης προς την IoT συσκευή και ακολούθως η συσκευή θα παρήγαγε ένα δημόσιο κλειδί. Το παραγόμενο κλειδί θα ερχόταν σε αντιδιαστολή με βάση τη λίστα των εξουσιοδοτημένων συσκευών από την Αρχή Εγράφης και η ύπαρξή του, θα οδηγούσε στην αναγνώριση της συσκευής και στην έκδοση πιστοποιητικού.



Εικόνα 5 - Μοντέλο Διαχείρισης Ταυτότητας. Βάση λίστας εξουσιοδοτημένων συσκευών.

- Υπογραφή βάσει συμπεριφοράς των συσκευών.

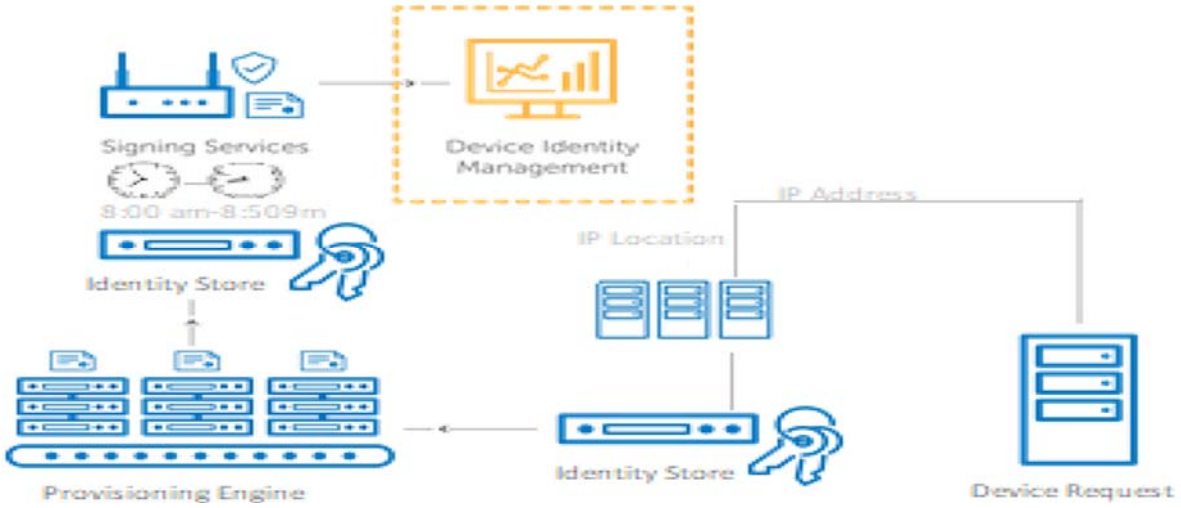
Σε περίπτωση συσκευών IoT που δεν ενσωματώνουν οποιοδήποτε αριθμό αναγνώρισης, τότε θα μπορούσε να υπάρξει αναγνώριση βάσει ορισμένων μοναδικών χαρακτηριστικών συμπεριφοράς της συσκευής. Ένας τρόπος προσδιορισμού αυτών των συσκευών, είναι η δημιουργία αρχείων κατακερματισμού όπου θα λειτουργούν ως ταυτότητα για τη συσκευή καθιστώντας ικανή την αναγνώριση της συσκευής, σε σχέση με τη μέθοδο αντιδιαστολής της λίστας εξουσιοδοτημένων συσκευών.



Εικόνα 6- Μοντέλο Διαχείρισης Ταυτότητας. Βάσει συμπεριφοράς συσκευών.

- Επαλήθευση της αυθεντικότητας με βάση τη γεωγραφικών χαρακτηριστικών.

Επαλήθευση της αυθεντικότητας με βάση τα γεωγραφικά χαρακτηριστικά είναι δυνατό να εφαρμοστεί από την τοποθεσία της IP διεύθυνσης, από την οποία θα προέρχεται το αίτημα προς την Αρχή Εγράφης, σε συνδυασμό με ένα χρονικό διάστημα κατά το οποίο οι συσκευές είναι πιθανό να συνδεθούν, με βάση προγραμματισμένα χρονοδιαγράμματά. Αυτή η μέθοδος επαλήθευσης δε θα μπορούσε να χαρακτηριστεί απολύτως ασφαλής, αλλά δεν παύει να αποτελεί μια αξιόλογη προσέγγιση.

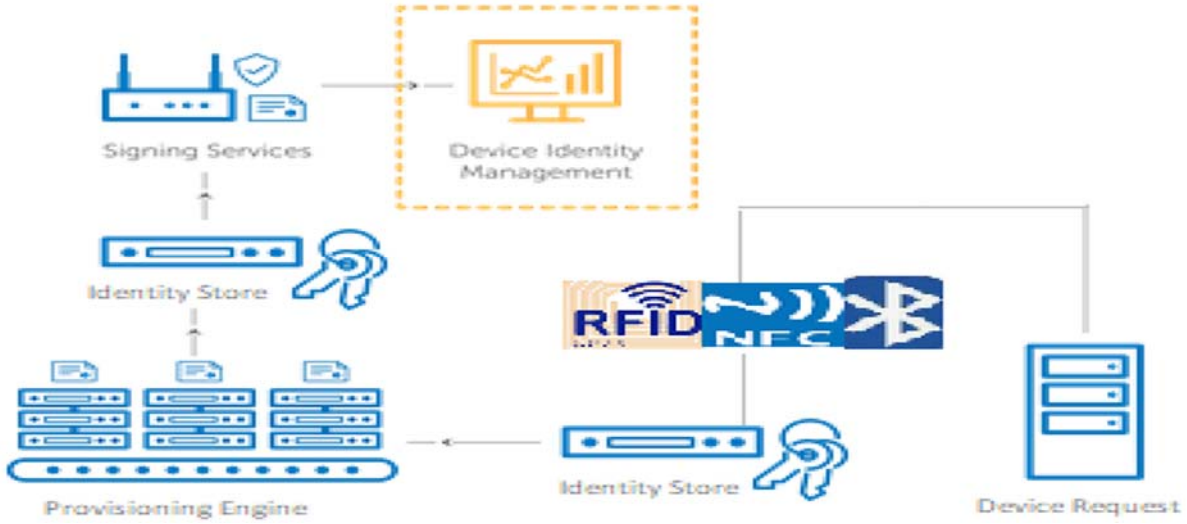


Εικόνα 7- Μοντέλο Διαχείρισης Ταυτότητας. Βάση γεωγραφικών χαρακτηριστικών.

- Συμβάν εμπιστοσύνης μιας φοράς

Αναγνώριση συσκευής με τη χρήση ενός συμβάντος εμπιστοσύνης μίας φοράς - βασικά θεωρούμε ότι μια συσκευή είναι αληθινή και αυθεντική μία φορά, ώστε να μπορεί να

πραγματοποιήσει εγγραφή συσκευής και την παροχή με ένα αρχικό Αναγνωριστικό συσκευής. Όσο πιο νωρίς και πιο κοντά γίνεται αυτή η διαδικασία στο στάδιο παραγωγής και εκτέλεσης του συμβάντος, τόσο το καλύτερο. Ωστόσο, αυτό μπορεί να γίνει και για συσκευές που είναι εγγυημένες, ότι αναπτυχθήκαν σε ασφαλές περιβάλλον. Για να μετριάσουμε τους κινδύνους, μπορούμε ακόμη και να δώσουμε ένα προσωρινό ή ένα κλειδί χρήσης, που δεν μπορεί να χρησιμοποιηθεί αν η συσκευή απομακρυνθεί και επιστρέψει στο περιβάλλον ή/και στο σύστημα.



Εικόνα 8- Μοντέλο Διαχείρισης Ταυτότητας. Συμβάν εμπιστοσύνης μιας φοράς.

Σε τυπικά επιχειρηματικά δίκτυα[22], τα τελικά σημεία μπορεί να αναγνωρίζονται από μια ανθρώπινη πιστοποίηση (π.χ. όνομα χρήστη και κωδικό πρόσβασης, κάρτα επικύρωσης ή βιομετρικά στοιχεία). Τα τελικά σημεία IoT / M2M πρέπει να επιβεβαιώνονται με μέσα που δεν απαιτούν ανθρώπινη αλληλεπίδραση. Τέτοια αναγνωριστικά περιλαμβάνουν την αναγνώριση ραδιοσυχνοτήτων (RFID), κοινό μυστικό κωδικό, τα πιστοποιητικά X.509, τη διεύθυνση MAC του τελικού σημείου ή κάποιο είδος αμετάβλητου στοιχείου εμπιστοσύνης που βασίζεται στο υλικό.

Η δημιουργία ταυτότητας μέσω πιστοποιητικών X.509 παρέχει ένα ισχυρό σύστημα ελέγχου ταυτότητας. Ωστόσο, στον τομέα του IoT, πολλές συσκευές ενδέχεται να μην έχουν αρκετή μνήμη για να αποθηκεύσουν ένα πιστοποιητικό ή μπορεί να μην έχουν ακόμη την απαιτούμενη ισχύ CPU για να εκτελέσουν τις κρυπτογραφικές διαδικασίες επικύρωσης των πιστοποιητικών X.509 (ή οποιουδήποτε τύπου λειτουργίας δημόσιου κλειδιού).

Τα υπάρχοντα πρωτοκολλά ελέγχου ταυτότητας, όπως το 802.1AR και τα πρωτόκολλα ελέγχου ταυτότητας, όπως ορίζονται από το IEEE 802.1X, μπορούν να αξιοποιηθούν για εκείνες τις συσκευές που μπορούν να διαχειριστούν, τόσο το φορτίο της επεξεργαστικής τους δυνατότητας, όσο και τη μνήμη για την αποθήκευση ισχυρών διαπιστευτηρίων. Ωστόσο, οι προκλήσεις των νέων μορφών παραγόντων, καθώς και οι νέες μορφές, δημιουργούν την ευκαιρία για περαιτέρω έρευνα στον καθορισμό των μικρότερων τύπων διαπιστευτηρίων αποτυπώματος και των κρυπτογραφικών κατασκευασμάτων και των πρωτόκολλων ελέγχου ταυτότητας που απαιτούν μικρότερη υπολογιστική ένταση.

Το πρότυπο το 802.1AR καθορίζει τα αναγνωριστικά ασφαλούς συσκευής (Secure Device Identifiers - DevIDs) που έχουν σχεδιαστεί για να χρησιμοποιούνται ως διαπιστευτήρια ελέγχου ταυτότητας ασφαλούς συσκευής, με επεκτάσιμο πρωτόκολλο ελέγχου ταυτότητας (Authentication Protocol - EAP) και άλλα πρωτόκολλα ελέγχου ταυτότητας βιομηχανικού προτύπου. Μια τυποποιημένη ταυτότητα συσκευών διευκολύνει τον διαλειτουργικό έλεγχο ταυτότητας συσκευών και απλοποιεί την ασφαλή ανάπτυξη και τη διαχείριση συσκευών.

Το πρότυπο IEEE 802.1X ορίζει ένα πρωτόκολλο ελέγχου πρόσβασης και ελέγχου ταυτότητας που βασίζεται σε υπολογιστή-χρήστη και διακομιστή, το οποίο περιορίζει τη σύνδεση μη εξουσιοδοτημένων χρηστών σε τοπικό δίκτυο υπολογιστών - LAN. Ο διακομιστής ελέγχου ταυτότητας επαληθεύει κάθε πελάτη συνδεδεμένο σε μια θύρα μεταγωγής και εκχωρεί τη θύρα σε ένα VLAN, πριν κάνει διαθέσιμες τις υπηρεσίες που παρέχει ο διακόπτης ή το LAN. Μέχρι την πιστοποίηση του χρήστη, ο έλεγχος πρόσβασης 802.1X επιτρέπει μόνο την επέκταση πρωτόκολλο ελέγχου ταυτότητας (Extensible Authentication Protocol) μέσω LAN (EAPOL) μέσω της θύρας στην οποία είναι συνδεδεμένος ο χρήστης. Αφού ο έλεγχος ταυτότητας είναι επιτυχής, η αποστολή και λήψη δεδομένων μπορεί να περάσει από τη θύρα.

Οι παρούσες τεχνικές κρυπτογράφησης και πιστοποίησης που βασίζονται στις σουίτες κρυπτογράφησης (AES) για την εμπιστευτική μεταφορά δεδομένων, Rivest-Shamir-Adleman (RSA) για ψηφιακή υπογραφή και διαδικασία ανταλλαγής κλειδιού και Diffie-Hellman (DH) για διαπραγμάτευση και διαχείριση κλειδιών (RSA). Παρόλο που χαρακτηρίζονται ως ισχυρά πρωτοκολλά, εντούτοις δεν μπορούν να αξιοποιηθούν από αρκετές IoT συσκευές λόγω των περιορισμών τους σε επεξεργαστική δύναμη και μνήμη. Επιπλέον, αρκετές από τις IoT συσκευές θα πρέπει να έχουν περιορισμένη πρόσβαση σε

ένα επιχειρηματικό δίκτυο. Για σκοπούς ασφάλειας θα πρέπει να παρεμβαίνει ο διαχειριστής του δικτύου, αλλάζοντας τις εργοστασιακές τους ρυθμίσεις, για προστασία από τυχόν παραβίασης, κλοπής η και άλλων μορφών επέμβασης από τρίτους, με σκοπό την προστασία του δικτύου και των δεδομένων.

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) επέλεξε πρόσφατα το πρότυπο του SHA-3 ως νέο αλγόριθμο για τις λεγόμενες "ενσωματωμένες" ή έξυπνες συσκευές που συνδέονται με ηλεκτρονικά δίκτυα, όπου απαιτεί λιγότερη επεξεργαστική δύναμη και μνήμη από τις συσκευές, παρέχοντας τους ισχυρή κρυπτογράφηση και αξιοπιστία

Αναγκαιότητα Ασφάλειας Πληροφοριακών Συστημάτων

Η ασφάλεια των πληροφοριακών συστημάτων έχει σκοπό τη διαφύλαξη των αγαθών από απειλές, οι οποίες μπορούν να εκμεταλλευθούν αδυναμίες ή ευπάθειες και να προξενήσουν ζημιές και επιπτώσεις.

Η σημαντικότητα της ασφάλειας έγκειται στο γεγονός της προστασίας της πληροφορίας. Με αυτή την έννοια η προστασία της πληροφορίας προϋποθέτει την ασφάλεια των υπολογιστών, των δικτυών, του διαδικτύου, την εφαρμογή πολιτικών ασφάλειας και τη διαχείριση ασφάλειας των πληροφοριών. Η αναγκαιότητα διαφύλαξης των πληροφοριών είναι πρωταρχικός παράγοντας για τη λειτουργία ενός πληροφοριακού συστήματος, έχοντας καθοριστικό ρολό για την ασφάλεια του οργανισμού το σύνολο του οποίου αποτελείται από τους ανθρώπους, τις διαδικασίες, το υλικό, το λογισμικό την υποδομή του δικτύου και τα δεδομένα. Υπάρχουν πολλά παραδείγματα που αφορούν οργανισμούς, οι οποίοι έχουν τεθεί εκτός λειτουργίας για κάποιο χρονικό διάστημα, με ανυπολόγιστο κόστος, τόσο σε χρήμα όσο και σε φήμη. Επιτυχημένη επίθεση από χάκερ θα έχει ως αποτέλεσμα την κλοπή πληροφοριών και συνεπώς ευαίσθητων προσωπικών δεδομένων. Επιπλέον, επιθέσεις εκ των έσω από δυσαρεστημένους εργαζομένους μπορούν να επιφέρουν αλλοίωση της οποιασδήποτε πληροφορίας ή και διαρροή με σκοπό να βλάψει τον οργανισμό.

Τα συστατικά ενός πληροφοριακού συστήματος, τα οποία χρειάζονται προστασία είναι τα αγαθά (assets) τα οποία έχουν αξία και πρέπει ως εκ τούτου να προστατεύονται. Τα αγαθά αυτά είναι το υλικό, το λογισμικό, τα δεδομένα, οι υποδομές του δικτύου, οι άνθρωποι και οι διαδικασίες.

Θεμελιώδεις απαιτήσεις ασφαλείας των πληροφοριακών συστημάτων

Η ασφάλεια των πληροφοριακών συστημάτων βασίζεται απαραίτητα σε τρεις βασικές θεμελιώδεις απαιτήσεις, το τρίγωνο C.I.A (Confidentiality, Integrity, Availability), οι οποίες είναι η Εμπιστευτικότητα, η Ακεραιότητα και η Διαθεσιμότητα.

Η Εμπιστευτικότητα, έχει ως στόχο να διασφαλίσει ότι η οποιαδήποτε πληροφορία θα μπορεί να αναγνωστεί μόνο από εξουσιοδοτημένα άτομα, καθώς επίσης και τον αποκλεισμό στην πληροφορία στους μη εξουσιοδοτημένους χρήστες. Επίσης, είναι σημαντικό να δοθεί ιδιαίτερη έμφαση, όσον αφορά πληροφορίες, οι οποίες θα υπάρχουν στο δίκτυο μιας εταιρίας και αφορούν προσωπικά δεδομένα, είτε αυτά αφορούν πελάτες, είτε υπάλληλους ή συνεργάτες.

Ακεραιότητα, είναι η διασφάλιση ότι τα δεδομένα δεν έχουν τροποποιηθεί, διαγραφεί ή αλλοιωθεί από οποιοδήποτε μη εξουσιοδοτημένο άτομο.

Διαθεσιμότητα, είναι η διασφάλιση ότι ο οποιοσδήποτε εξουσιοδοτημένος χρήστης θα μπορεί να έχει ομαλή προσπέλαση στα δεδομένα και στις υπηρεσίες του δικτύου. Υπό αυτή την έννοια, όλα τα δεδομένα και οι υπηρεσίες θα πρέπει να είναι διαθέσιμα, ακόμη και σε περιπτώσεις διακοπής του ηλεκτρικού, σε προβλήματα υλικού, σε πιθανά προβλήματα που θα δημιουργηθούν λόγω επιθέσεων άρνησης παροχής υπηρεσιών στο δίκτυο, καθώς επίσης σε κατάσταση οποιασδήποτε φυσικής καταστροφής. Ακόμη και σε αυτές τις περιπτώσεις οι εξουσιοδοτημένοι χρήστες θα πρέπει να έχουν στη διάθεση τους απαραίτητους πόρους στο δίκτυο.

Βασικές Πτυχές της ασφάλειας πληροφοριών.

Εκτός από το τρίγωνο της CIA, στην οποία περιγράφονται οι βασικοί πυλώνες της ασφάλειας των πληροφοριών, υπάρχουν και οι πιο κάτω επιμέρους πτυχές τις ασφάλειας οι οποίες είναι οι εξής:

Ιδιωτικότητα (privacy), η οποία προνοεί τη διασφάλιση όλων το προσωπικών δεδομένων, τα οποία θα πρέπει να εξυπηρετούν μόνο το σκοπό που έχουν συλλεχθεί, σύμφωνα με την έγκριση που έχει δοθεί από τον ιδιοκτήτη της πληροφορίας.

Ταυτοποίηση (Identification) είναι η διαδικασία στην οποία ο χρήστης θα πρέπει να παρουσιάσει την ταυτότητα προς το πληροφοριακό σύστημα.

Αυθεντικοποίηση (Authentication) είναι η επαλήθευση της ταυτότητας του χρήστη για να δοθεί πρόσβαση στο σύστημα.

Εξουσιοδότηση (Authorization), η οποία ανάλογα με την ταυτοποίηση του χρήστη στο σύστημα θα δοθεί και η προκαθορισμένη πρόσβαση και δικαιώματα, για αλλαγές σε πληροφορίες. Με στοιχεία ελέγχου ταυτότητας και εξουσιοδότησης, δημιουργείται μια σχέση εμπιστοσύνης μεταξύ των συσκευών για την ανταλλαγή κατάλληλων πληροφοριών.

Λογοδοσία (Non-Repudiation) είναι η ιδιότητα του συστήματος να μπορεί να καταγράψει τις ενέργειες του κάθε χρήστη και οτιδήποτε συμβεί στο σύστημα να μπορεί να αποδοθεί αποδεδειγμένα σε ποιο χρηστή οφείλεται το οποιοδήποτε συμβάν.

Μοντέλο ARM Αρχιτεκτονικής Ιντερνέτ των Πράγματων – IoT-A

Η IoT-ARM[23], αρχιτεκτονική των πράγματων είναι αποτέλεσμα μιας πολυετούς συζητήσεις, η οποία ξεκίνησε το 2009, μεταξύ ομάδας ερευνητών, περισσοτέρων από 20 βιομηχανικών οργανισμών και άλλων ερευνητικών ιδρυμάτων. Κοινή τους πεποίθηση για την ανάγκη για μιας κοινής αρχιτεκτονικής για το ίντερνετ των πράγματων, καθώς και μια κοινή γλώσσα επικοινωνίας. Η αρχιτεκτονική IoT-A έχει στηριχτεί από το έβδομο πρόγραμμα πλαίσιο της Ευρωπαϊκής Ένωσης για την Ερεύνα και την ανάπτυξη, με στόχο τη δημιουργία μιας αρχιτεκτονικής για το Ιντερνέτ των Πράγματων.

Στόχος των εταίρων του IoT-A είναι η αντιμετώπιση δυσκολίων που αφορούν τόσο από τεχνικής άποψης, στο γεγονός ότι IoT συσκευές θα επέτρεπε να είναι συμβατές μεταξύ τους, για να είναι σε θέση να επικοινωνούν και να αλληλοεπιδρούν μεταξύ τους, ώστε να μπορούν να εκτελούν διαφορετικές συνθέτες διεργασίες και να έχουν ένα αποτέλεσμα από το σύνολο αυτών των διεργασιών από τις συσκευές. Ωστόσο, επιπρόσθετα προβλήματα για τις IoT συσκευές αποτελούν η προστασία της ιδιωτικότητας και της ασφάλειας σε διαφορετικές αγορές οπού εφαρμόζετε ξεχωριστή νομοθεσία.

Λόγω της πολυπλοκότητας και της διαφορετικότητας των IoT συσκευών θα ήταν δύσκολο να εφαρμοστεί ένα και μόνο πρωτόκολλο επικοινωνίας μεταξύ των IoT συσκευών. Για αυτόν το λόγο, οι εταίροι κατέληξαν σε ένα γενικότερο αφηρημένο στρώμα, με την δημιουργία του αρχιτεκτονικού μοντέλου Αναφοράς (ARM), οπού θα έφερε ένα συμβατικό χαρακτηριστικό πλεονέκτημα της συμβατότητας με προηγουμένης γενιάς συσκευών IoT. Η δημιουργία της νέας αρχιτεκτονικής θα επέτρεπε να σχεδιαστεί και να αναπτυχθεί στον πραγματικό κόσμος, σε αντιθέσει με άλλες αρχιτεκτονικές οπού

σχεδιάζονται και εφαρμόζονται σε εργαστήριο, αυτή αποτέλεσε το επίκεντρο της νέας αρχιτεκτονικής. Για τον πιο πάνω λόγο ο σχεδιασμός της αρχιτεκτονικής IoT-A είχε α πευθυνθεί στη συμμετοχή των τελικών χρηστών εκτός των συμμετεχόντων οργανισμών για σχεδιασμό και ανάπτυξη αρχιτεκτονικής, με αποτέλεσμα να πρέπει να ικανοποιηθούν νέες απαιτήσεις για τη δημιουργία του νέου μοντέλου. Οι πληροφορίες και η ανατροφοδότηση από τους εξωτερικούς συνεργάτες για το μοντέλο αρχιτεκτονικής από διαφορετικούς τομείς, αποτέλεσε σημαντικό παράγοντα στη δομή και την ανάπτυξη το ARM με στόχο να ικανοποιήσει διαφορετικές απαιτήσεις και να επιτρέψει την ολιστική προσέγγιση του IoT-A. Επιπρόσθετα, χρησιμοποιήθηκαν περαιτέρω εργαστήρια και ερωτηματολόγια των ενδιαφερομένων μερών για την ανασκόπηση της εξέλιξης της ανάπτυξης του ARM και για τον ορισμό των εννοιών και του μοντέλου. Η βασική ιδέα είναι ότι η IoT-ARM να παρέχει μια κοινή διάρθρωση και κατευθυντήριες γραμμές για την αντιμετώπιση των βασικών πτυχών της ανάπτυξης, χρήσης και ανάλυσης συστημάτων Διασύνδεσης.

Πλεονεκτήματα χρήσης του μοντέλου ARM

- **Γνωστική Βοήθεια**, όπου προκύπτει από την ύπαρξη μιας κοινής γλώσσας κατά την ανάπτυξη του και την σχεδίαση του. Η ύπαρξη της κοινής γλώσσας βοηθά στην καθοδήγηση των συζητήσεων μεταξύ των συμμετεχόντων χρηστών , οι οποίοι προέρχονται από διαφορετικό γνωστικό πεδίο, επιτυγχάνοντας την σωστή επικοινωνία. το μοντέλο αρχιτεκτονικής του ARM αναφέρετε σε γενικότερους όρους, με αποτέλεσμά να βρίσκεις εφαρμογής σε διαφόρους τομίες δημιουργώντας καινούργια πεδία εκμαθήσεις. Εντούτοις, νέοι χρήστες είναι πιο εύκολο να κατανοήσουν, να αντιληφθούν τα ιδιαίτερα χαρακτηριστικά και την πολυπλοκότητα του IoT. Η εφαρμογής του μοντέλου σε όλο και περισσοτέρους τομίες, με διαφορετικές εκτελέσεις σε συνδυασμό με την ανατροφοδότηση από την κοινότητα, βοηθά στη συνεχομένη εξέλιξη και ανάπτυξη της αρχιτεκτονικής να βρίσκεις όλο και περισσότερη εφαρμογής σε ιδιαίτερα πολύπλοκα δίκτυα όπως αυτά των επιχειρήσεων.
- **Μοντέλο αναφοράς ως κοινή βάση,** η καθιέρωση του μοντέλου κοινής βάσης για το Διαδίκτυο περιλαμβάνει τα διαφορετικά πιθανά σημεία διασύνδεσης μεταξύ διαφορετικών συσκευών και ως εκ τούτου τη δημιουργία

αλληλεπιδράσης τους και τις σχέσεις που μπορούν να δημιουργηθούν μεταξύ των συσκευών.

- **Δημιουργία αρχιτεκτονικών,** αυτό επιτυγχάνεται λόγω των εργαλείων υποστήριξης που προσφέρουν αυτοματισμούς και τη δυνατότητα να εφαρμόζεται σε διαφορετικά περιβάλλοντα, δημιουργώντας νέες αρχιτεκτονικές που βρίσκουν εφαρμογής, σε αλλά εξειδικευμένα συστήματα. Αποτέλεσμα είναι η επέκταση και η αναβάθμιση γνωστικού πεδίου της αρχιτεκτονικής και η διαλειτουργικότητα σε καινούργιες αρχιτεκτονικές στα συστήματα IoT.
- **Προσδιορισμός των διαφορών στις παράγωγες αρχιτεκτονικές,** με χρήση των εργαλείων της αρχιτεκτονικής IoT ARM κατά την ανάπτυξη οποιασδήποτε αρχιτεκτονικής υποδεικνύει τις δυνατότητες , τις ιδιαιτερότητες της καθώς παρέχει τη δυνατότητα να προβλέπει τη πολυπλοκότητα της παραγόμενης αρχιτεκτονικής κατά την εφαρμογής της. Αυτό έχει σαν αποτέλεσμά την ικανοποίηση των ποιοτικών απαιτήσεων για τη σωστή λειτουργία του δικτύου. Επιπλέον, η χρήση εργαλείων της σουίτας είναι σε θέση να προβλέψει και να προσδιορίσει τις διάφορες μεταξύ δυο διαφορετικών αρχιτεκτονικών και το παραγόμενο αποτέλεσμά τους. Τέλος, υπάρχει η δυνατότητα σύγκρισης μιας υφιστάμενης αρχιτεκτονικής, με την υπόδειξη μεθόδων τροποποίησης της και ακολούθως προτεινομένους τρόπους μεταφοράς και συμβατότητας προς αυτή του IoT ARM.
- **Επίτευξη της δια λειτουργικότητας,** αναπόφευκτα αποτελεί μεγάλη πρόκληση η διαλειτουργηκότητα μεταξύ δυο διαφορετικών αρχιτεκτονικών. Δυστυχώς, η αρχιτεκτονική του ARM δεν είναι σε θέση να εγγυηθεί την επίτευξη διαλειτουργηκοτητας μεταξύ ανόμοιων αρχιτεκτονικών. Εν τούτης, κατά την σύγκλιση δυο αρχιτεκτονικών με βάση των προσδιορισμό των διαφορών αρχιτεκτονικών, υποδεικνύονται τα σημεία όπου θα πρέπει να ληφθούν μετρά για να υπάρχει διαλειτουργηκότητα κατά τη εφαρμογή των αρχιτεκτονικών. Η επίτευξη της δια λειτουργικότητας μπορεί να διεκπεραιωθεί είτε με την εφαρμογής ενός υποσυστήματος IoT σε ένα άλλο σύστημα, είτε με τη δημιουργία γέφυρας οπού θα συνδέονται η βασικές λειτουργίες αλλού συστήματος με αυτή του IoT. Ο επανασχεδιασμός αρχιτεκτονικής αποτελεί πιο πολύπλοκη διαδικασία, σε σύγκριση με την εναλλακτική λύση της γέφυρας μεταξύ συστημάτων.

- **Χάρτες πορείας συστήματος και ο κύκλος ζωής των προϊόντων,** όπως έχουμε αναφερθεί πιο πάνω για την επίτευξη της διαλειτουργηκότητας με τον εντοπισμό των διαφορών μεταξύ των δύο διαφορετικών αρχιτεκτονικών, η προσέγγιση αυτή μπορεί επίσης να χρησιμοποιηθεί για να καταγράψει την εξέλιξη νέων αρχιτεκτονικών προσφέροντας διαφορετικές σχεδιαστικές επιλογές που συνδέονται με ποιοτικές απαιτήσεις. Σε περιπτώσεις που κατά τη σχεδίαση για συνδυασμό διαλειτουργηκότητας δυο διαφορετικών αρχιτεκτονικών, δεν μπορεί να επιτευχθεί αυτό ή υπάρχουν περιορισμοί , τότε υπάρχει δυνατότητα μέσω αναφοράς από το χρήστη ώστε να ληφθεί υπόψη για σχεδιασμοί μελλοντικών συσκευών και να μπορεί να υποστηριχτεί κατά το σχεδιασμοί της επομένης γενιάς προϊόντων. Η προσέγγιση αυτή βοηθά επίσης τον σχεδιαστή να διαμορφώσει σαφείς και τυποποιημένες, απαιτήσεις με βάση το σκεπτικό για τη χαρτογράφηση του συστήματος που έχει επιλεγεί και το κύκλο ζωής του προϊόντος που προκύπτουν από το σχεδιασμοί του συστήματος.
- **Συγκριτική αξιολόγηση,** η αρχιτεκτονική αναφορά παρέχει τις ελάχιστες λειτουργικές απαιτητής του συστήματος για τα συστήματα – αρχιτεκτονικές. Αυτή η τυποποίηση και η οριοθέτηση των παραμέτρων του συστήματος παρέχει στο σχεδιαστή μια εικόνα αναμενομένου αποτελέσματος. Η πληροφορίες που παρέχονται αφορούν τον τρόπο αλληλεπίδρασης του συστήματος, την πολυπλοκότητα τόσο προς τη σύνθεση όσο προς τη δομή αλλά και ως προς την αλληλεπίδραση.

Κεφάλαιο 6
Συμπεράσματα της Έρευνας

Το δείγμα της έρευνας αποτελείται κατά 96.2% από άνδρες, 42.3% ηλικιακά ανήκει στην κατηγορία από 36 έως 45 ετών, 50% είναι απόφοιτοι ΤΕΙ ή ΑΕΙ και 42.3% έχουν ολοκληρώσει μεταπτυχιακές σπουδές, και 42.3% των ερωτηθέντων εργάζεται έχει από 6 έως 10 έτη εργασιακής εμπειρίας. Ακόμα, το 46.2% των ερωτηθέντων ήταν εργαζόμενοι σε επιχειρήσεις οπού υπάρχει απολυτή ιδιοκτησία από ένα άτομο – "κύριο ιδιοκτήτη", 30.8% εργάζονται σε μετοχική εταιρίας, και 23.1% σε εταιρία με συνιδιοκτησία, ενώ ο μέσος αριθμός εργαζομένων στην επιχείρηση ήταν 52.3 άτομα.

Σχετικά με τους παράγοντες που συντέλεσαν στην απόφαση να υιοθετήσουν τεχνολογίες που συγκαταλέγονται στην γενικότερη κατηγορία του Internet of Things (IoT) στην επιχείρηση τους, οι ερωτώμενοι απάντησαν πως οι σημαντικότεροι ήταν η βελτίωση της αποδοτικότητας της επιχείρησης (80.8%) και ακολούθως, η μείωση του κόστους (57.7%), η βελτίωση των παρεχόμενων υπηρεσιών (50%), η διαχείριση μεγάλου όγκου πληροφοριών (46.2%) και οι απαιτήσεις των καταναλωτών (46.2%). Αντιθέτως, μικρότερη επιρροή είχαν η βελτίωση των σχέσεων με τους συνεργάτες της επιχείρησης (26.9%) και η αύξηση των πωλήσεων (30.8%).

Αναφορικά με την ασφάλεια των συστημάτων βρέθηκε πως στα 2/3 του δείγματος, η επιχείρηση έχει συγκεκριμένο άτομο ή ομάδα ατόμων στον οποίο θα απευθυνθεί για το συντονισμό των συστημάτων ασφαλείας και σε περίπτωση προβλήματος ασφαλείας καθώς επίσης πως υπάρχει συνεργασία με άλλες εταιρίες για την ασφάλεια των συστημάτων.

Επίσης, βρέθηκε πως

- στο 92.3% των περιπτώσεων οι συνεργάτες της εταιρίας δεν έχουν πρόσβαση στα δεδομένα των πελατών.
- σε μεγάλο βαθμό υπάρχει συγκεκριμένη διαδικασία για τη διατήρηση της ασφάλειας στην επιχείρηση (M = 3.50) και ακολούθως πως υπάρχουν επίσημοι αποδεκτοί κανόνες ασφαλείας για κάθε λειτουργία (π.χ. συσκευές επικοινωνίας, υπολογιστές) (M = 3.03).
- σε μεγαλύτερο βαθμό πως υπάρχει κάποια διαδικασία που να εξασφαλίζει την ασφάλεια των δεδομένων (M = 3.52) και ακολούθως πως υπάρχει κάποια διαδικασία που να μειώνει το ρίσκο ασφαλείας (M = 2.80).
- σε μεγάλο βαθμό πως η πολιτική της επιχείρησης έχει μεταφερθεί και εξηγηθεί στους υπαλλήλους (M = 3.15).
- σε μεγάλο βαθμό πως οι υπάλληλοι υπογράφουν μία φόρμα εμπιστευτικότητας κατά την πρόσληψή τους (M = 2.80).
- σε μεγαλύτερο βαθμό πως υπάρχει οργανωμένο σύστημα ασφαλείας των εγκαταστάσεων (M = 3.50) καθώς επίσης σε μεγάλο βαθμό υπάρχει ένα οργανωμένο σύστημα πρόσβασης στις εγκαταστάσεις της επιχείρησης (M = 3.38).
- σε μεγαλύτερο βαθμό πως υπάρχει μία προκαθορισμένη προσέγγιση για την προστασία του δικτύου της επιχείρησης (π.χ. firewall για τα public και private networks, internal VLAN, firewall separation) (M = 3.96).
- σε ποσοστό 80.8% πως οι ευαίσθητες πληροφορίες δεν μεταφέρονται σε εξωτερικούς αποδέκτες.
- η επιχείρηση χρησιμοποιεί σε αρκετά μεγάλο βαθμό τρόπους προστασίας των ευαίσθητων πληροφοριών όταν μεταφέρονται σε εξωτερικούς αποδέκτες (π.χ. ασφαλής VPN connection, encryption) (M = 3.76).

- σε μεγαλύτερο βαθμό πως παρέχεται μοναδικό ID και password σε κάθε εργαζόμενο (92.3%) και ακολούθως πως υπάρχει κάποια λίστα με τους υπαλλήλους που έχουν άδεια πρόσβασης (π.χ. Active directory user list) (73.1%), πως υπάρχει λογική διαδικασία και παροχή άδειας πρόσβασης με βάση τη θέση των εργαζομένων (65.4%) και πως χρησιμοποιείται το αυτόματο logoff από τις συσκευές του δικτύου (65.4%).
- οι ερωτώμενοι δήλωσαν στο σύνολο τους πως η επιχείρηση στην οποία εργάζονται διαθέτει Antivirus και ακολούθως πως τα πληροφοριακά συστήματα παρακολουθούνται αναφορικά με την ασφάλεια (57.7%).
- οι ερωτώμενοι δήλωσαν πως σε πάρα πολύ μεγάλο βαθμό γίνεται back up των πληροφοριών και των ευαίσθητων δεδομένων που συγκεντρώνονται.

Ακόμα, από την συγκριτική στατιστική ανάλυση και προς απάντηση της 4ης ερευνητικής ερώτησης βρέθηκε πως όσο υψηλότερος ο αριθμός των εργαζομένων τόσο σε μεγαλύτερο βαθμό υπάρχει κατηγοριοποίηση των δεδομένων των πελατών και της επιχείρησης αναφορικά με τη σημαντικότητα τους, τόσο σε μεγαλύτερο βαθμό ο οργανισμός κάνει έλεγχο για πιθανή παραβατικότητα των υπάλληλων στο παρελθόν. Υπάρχουν εσωτερικά και εξωτερικά συστήματα που προστατεύονται από επιλογές πρόσβασης, τα συστήματα λειτουργιάς που μεταφέρουν και αποθηκεύουν ευαίσθητες πληροφορίες είναι προστατευμένα. Υπάρχει μία προκαθορισμένη προσέγγιση για την προστασία του δικτυού της επιχείρησης, χρησιμοποιούνται τρόποι προστασίας των ευαίσθητων πληροφοριών όταν μεταφέρονται σε εξωτερικούς αποδέκτες, η εξωτερική πρόσβαση στο πληροφοριακό σύστημα παρακολουθείται σε τακτά χρονικά διαστήματα ώστε να αποτραπεί η είσοδος χωρίς άδεια και γίνεται back up των πληροφοριών και των ευαίσθητων δεδομένων.

Τέλος, το είδος ιδιοκτησίας της επιχείρησης βρέθηκε να σχετίζεται με το κατά πόσο γίνεται back up των πληροφοριών και των ευαίσθητων δεδομένων. Ειδικότερα, στις επιχειρήσεις με μετοχική σύνθεση γίνεται σε μεγαλύτερο βαθμό back up των πληροφοριών και των ευαίσθητων δεδομένων ενώ το ίδιο συμβαίνει και με την ύπαρξη μιας προκαθορισμένης προσέγγισης για την προστασία του δικτυού της επιχείρησης.

Γενικά συμπεράσματα

Σε ένα συνεχές εξελισσόμενο περιβάλλον, με ταχύτατους ρυθμούς εξέλιξης στον τομέα των ηλεκτρονικών συσκευών, που βασίζονται στην αλληλεπίδραση είναι κοινώς αποδεκτό ότι η ένταξη των IoT συσκευών θα πρέπει να αποτελέσει αναπόσπαστο κομμάτι του εταιρικού δικτύου προσφέροντας πολλαπλά πλεονεκτήματα. Όπως διαφαίνεται από την ερευνά οι IoT συσκευές συνεισφέρουν σημαντικά σε πολλαπλούς τομείς της επιχειρήσεις όπως είναι η παραγωγικότητα, η μείωση του κόστους, τη βελτίωση των παρεχόμενων υπηρεσιών, στη διαχείριση των πληροφοριών, της εξυπηρετήσεις και στην αποδοτικότητα της επιχείρησης. Παράλληλα όμως, με τη χρήση των IoT συσκευών στο εταιρικό δίκτυο, η χρήση τεχνικών προστασίας που εφαρμόζονται από τις μικρομεσαίες επιχειρήσεις χαρακτηρίζετε σαν η απολυτός απαραίτητη. Ως κύριο μετρό προστασίας που χρησιμοποιείται από όλες τις μικρομεσαίες επιχειρήσεις είναι η χρήση Antivirus προγράμματος. Η χρήση Antivirus προγράμματος αποτελεί μέτρο αντιμετώπισης από ιούς , Δουρείους Ίππους, σκουλήκια και κακόβουλο λογισμικό, τα οποία μπορούν να επηρεάσουν, τόσο το υλικό, όσο και τα αρχεία. Επίσης, το αμέσως επόμενο διαδεδομένο μετρό προστασίας που εφαρμόζεται, είναι η χρήση Firewall, είτε αυτό εφαρμόζεται ως πρόγραμμα είτε ως υλικό, με σκοπό τον έλεγχο των εισερχομένων και εξερχομένων πακέτων δεδομένων. Επιπρόσθετα, η χρήση τοίχου ασφάλειας παρέχει ασφάλεια σε επίπεδο εφαρμογών, αφού υπάρχει η δυνατότητα να επεξεργάζονται πρωτοκολλά και εφαρμογές που ενδέχεται να δημιουργήσουν ανεπιθύμητες συνδέσεις. Ωστόσο, η προστασία ευαίσθητων πληροφοριών όταν μεταφέρονται σε εξωτερικούς αποδέκτες όπως αυτές εφαρμόζονται μέσω VPN, καθώς και με τη χρήση κρυπτογραφίας είναι ένας σημαντικός παράγοντας για τη διασφάλιση των πληροφοριών που διακινούνται από το εταιρικό δίκτυο, ώστε να αποτραπεί το ενδεχόμενο είτε να υποπέσουν πληροφορίες σε λάθος άτομο είτε να υπάρξει υποκλοπή των δεδομένων από επιθέσεις Man In the Middle.

Παρόλα αυτά, είναι ανησυχητικό το γεγονός ότι δεν υπάρχουν προκαθορισμένες διαδικασίες για αξιολόγηση μείωσης του ρίσκου ασφάλειας, σε συνδυασμό με τη μη διενέργεια συχνών ελέγχων για εντοπισμό προβλημάτων ασφάλειας, όσο και για πρόσβαση μη εξουσιοδοτημένων χρηστών στο εταιρικό δίκτυο. Η ύπαρξη και εφαρμογή πολιτικής ασφάλειας θα μπορεί να καθορίσει τη σωστή διαχείριση της ασφάλειας του δίκτυο. Η υλοποίηση εσωτερικών και εξωτερικών ελέγχων για εντοπισμό ευπαθειών,

κακόβουλων λογισμικών και ανεύρεση τρωτών σημείων θα πρέπει να εφαρμόζεται ανελλιπώς από τους διαχειριστές του δικτύου, για άμεση αντιμετώπιση των κίνδυνων, προτού εντοπιστούν και γίνουν εκμεταλλεύσιμοι από μη εξουσιοδοτημένα άτομα. Ωστόσο, το ενδεχόμενο να συμβεί οποιοδήποτε περιστατικό ασφάλειας χωρίς την ύπαρξη απαραίτητων ελέγχων για άμεσο εντοπισμό, εμπεριέχει κίνδυνους, τόσο σε οικονομικό επίπεδο, όσο και έλλειψη εμπιστοσύνης των πελατών και προμηθευτών της επιχείρησης. Ο μη έγκαιρος εντοπισμός μη εξουσιοδοτημένων χρηστών στο εταιρικό δίκτυο επιτρέπει στον κακόβουλο χρήστη να υποκλέψει, να διαγράψει και να τροποποιήσει αρχεία, καθώς επίσης και την απόκρυψη στοιχείων, που θα μπορούσαν να οδηγήσουν στον εντοπισμό του, είτε ακόμη και το σημείο πρόσβασής του. Επιπρόσθετα, δημιουργεί την προοπτική στον μη εξουσιοδοτημένο χρήστη, να έχει πρόσβαση στο εταιρικό δίκτυο οποιαδήποτε στιγμή, αφήνοντας «πίσω πόρτα» - Backdoor, εκμεταλλευόμενος ευπάθεια.

Δεν πρέπει να αγνοήσουμε το γεγονός ότι ένας μεγάλος αριθμός μικρομεσαίων επιχειρήσεων διατηρεί λίστα με τους υπαλλήλους, που έχουν άδεια πρόσβασης στο εταιρικό δίκτυο, αφού ο κάθε χρήστης για να διασφαλίσει την είσοδο του στο εταιρικό δίκτυο, θα πρέπει να ελεγχθούν τα διαπιστευτήρια του χρήστη. Συγχρόνως, η παροχή μοναδικού ID και password σε κάθε εργαζόμενο, αποτελεί απαραίτητο στοιχείο για την είσοδο εξουσιοδοτημένων χρηστών στο εταιρικό δίκτυο. Λαμβάνοντας υπόψιν την αναγκαιότητα διασφάλισης της ακεραιότητας των πληροφοριών και του εταιρικού δικτύου, είναι θετικό ότι στις περισσότερες επιχειρήσεις τα user IDs των χρηστών είναι ανιχνεύσιμα, όπου εξυπηρετείται ο στόχος της λογοδοσίας. Ωστόσο, η πολυπλοκότητα και η αλλαγή του κωδικού πρόσβασης ανά τακτά χρονικά διαστήματα θα μπορούσε να διασφαλίσει το εταιρικό δίκτυο από επίδοξους εισβολείς. Η ύπαρξη μεθόδων ανίχνευσης πιθανών κωδίκων για το χρήστη, σε συνδυασμό με τις πολλαπλές μεθόδους Phishing καθιστά ευάλωτο το εταιρικό δίκτυο. Επίσης, η ύπαρξη λογικής διαδικασίας και παροχής άδειας πρόσβασης με βάση τη θέση των εργαζομένων, καταλαμβάνει χαμηλό ποσοστό σύμφωνα με την ερευνά. Μπορεί να χαρακτηριστεί ως δικαιολογημένη αφού ορισμένες πολύ μικρές εταιρείες εργοδοτούν μικρό αριθμό εργαζομένων, όπου τα καθήκοντά τους σε αρκετές περιπτώσεις είναι ενιαία. Τέλος, για την ένταξη οποιασδήποτε IoT συσκευής στο εταιρικό δίκτυο, θα πρέπει να ικανοποιούνται ορισμένες ελάχιστες απαιτήσεις, ακολούθως να αξιολογούνται και να τροποποιούνται οι προκαθορισμένες ρυθμίσεις τους, με στόχο την διασφάλιση του εταιρικού δικτύου,

χωρίς να μπορεί κάποιος κακόβουλος να αποκτήσει πρόσβαση μέσω ευπαθειών ή τρωτών σημείων αυτής.

Κεφάλαιο 7
Επίλογος

Συμπεράσματα και Μελλοντική μελέτη

Η παρούσα εργασία είχε ως σκοπό να παρουσιάσει τις διαδικασίες που εφαρμόζονται από τις Κυπριακές μικρομεσαίες επιχειρήσεις, σχετικά με τη διαχείριση της ταυτοποίησης IoT συσκευών, στα διάχυτα δίκτυά τους.

Στην εργασία παρουσιάζετε μια ολοκληρωμένη ανασκόπηση της έννοιας της διατήρησης ταυτοποίησης IoT συσκευών, όπως αυτή εξετάζεται στη διεθνή βιβλιογραφία. Εν συνεχεία, καταγράφηκαν διαφορά πλαίσια – Frameworks, σχετικά με την ταυτοποίηση, είτε αυτά αναφέρονται σε θεωρητικό επίπεδο, είτε σε εμπειρικό. Ωστόσο θα πρέπει να ληφθεί υπόψιν ότι από τη διεθνή βιβλιογραφία, προκύπτει ότι η ταυτοποίηση IoT συσκευών στα εταιρικά δίκτυα, αποτελεί μια διαδικασία, η οποία χαρακτηρίζεται ως πολύπλοκη, καθώς είναι συνεχώς εναλλασσόμενη, τόσο όσον αφορά τις μεθόδους ταυτοποίησης των συσκευών, όσο και στον τρόπο που πρέπει να είναι δομημένο το εταιρικό δίκτυο για να υπάρχει ομαλή αλληλεπίδραση. Στη συνέχεια, έγινε καταγραφή ερωτήσεων με σκοπό την ανάδειξη των λόγων ένταξης των IoT συσκευών και την ύπαρξη πολιτικής ασφάλειας, τα οποία σχετίζονται με ζητήματα διασφάλισης των

πληροφοριών, την ένταξη και την απαραίτητη εκπαίδευση του προσωπικού και κυρίως τη χρήσης μηχανισμών ταυτοποίησης IoT συσκευών ,κατά τη σύνδεση τους στο εταιρικό δίκτυο. Ακολούθως, η εξαγωγή και η ανάλυση των αποτελεσμάτων έχει αναδείξει χρήσιμα αποτελέσματα, όπως το γεγονός ότι οι κυπριακές μικρομεσαίες εταιρίες, δεν έχουν εφαρμόσει οποιαδήποτε ολοκληρωμένη διαδικασία ταυτοποίησης IoT συσκευών στα εταιρικά δίκτυα και επιπρόσθετα ότι οι περισσότερες δεν έχουν υιοθετήσει νέες τεχνολογίες προς την κατεύθυνση αυτή. Επίσης, οι κυπριακές μικρομεσαίες επιχειρήσεις φαίνονται στο παρόν στάδιο να είναι ευάλωτες και να παρουσιάζουν περισσότερο ρίσκο στο δίκτυο τους, μετά την ένταξη IoT συσκευών.

Η ταυτοποίηση IoT συσκευών παραμένει φλέγον ζήτημα λόγω της ύπαρξης πολυάριθμων συσκευών, με διαφορετικά τεχνικά χαρακτηριστικά και λειτουργικά, τα οποία επιφέρουν τη δημιουργία ενός πολύπλοκου δικτύου. Αυτή η πολυπλοκότητα, όμως, αναδεικνύει την αδυναμία της χρήσης ενός κοινού πλαισίου συνδεσιμότητας στο εταιρικό δίκτυο, που οφείλεται σε περιορισμούς από τις IoT συσκευές, όσον αφορά το υλικό ή και το λειτουργικό, όπως είναι η διαθέσιμη μνήμη, η επεξεργαστική δύναμη ή και τα υποστηριζόμενα πρωτόκολλα επικοινωνίας.

Η μελέτη ολοκληρώνεται με προτεινόμενα μοντέλα, λαμβάνοντας υπόψιν τους πιο πάνω περιορισμούς που εμφανίζουν οι IoT συσκευές, τους κίνδυνους που ελλοχεύει η ένταξη τους στο εταιρικό δίκτυο, καθώς και τις διαφορετικές προσεγγίσεις μεθόδων ταυτοποίησης που υπάρχουν. Παρόλα αυτά, θεωρείται ότι θα πρέπει κάθε μικρομεσαία εταιρεία να εισάγει ένα είδος ελάχιστων προδιαγραφών για ένταξη IoT συσκευών, με σκοπό να μπορεί να εφαρμοστεί ένα υψηλό επίπεδο ασφάλειας. Το μοντέλο ταυτοποίησης με τη χρήση δημοσίου κλειδιού από την αρχή πιστοποίησης, στο παρόν στάδιο, διαφαίνεται το πιο διαδεδομένο από επιχειρήσεις στο εξωτερικό, εξασφαλίζοντας σε μεγάλο βαθμό ένα ασφαλή μηχανισμό ταυτοποίησης.

Εν κατακλείδι, η συνεχομένη εξέλιξη στο τομέα της ένταξης των IoT συσκευών στα εταιρικά δίκτυα ευνοεί την ανάγκη όλο και περισσοτέρων πεδίων ερευνάς, σε σχέση με την αναζήτηση νέων μεθόδων ταυτοποίησης των IoT συσκευών. Επίσης, θα ήταν πολύ χρήσιμο να διενεργηθεί μια αντίστοιχη έρευνα απευθυνόμενη σε μεγαλύτερο αριθμό μικρομεσαίων επιχειρήσεων, βασιζομένη στις υποδείξεις και στα ευρήματα της υφιστάμενης έρευνας. Επιπρόσθετα, η υλοποίηση και αξιολόγηση ενός η κάποιων συνδυασμών των προτεινομένων μοντέλων, θα μπορούσε να εξάγει σημαντικά

αποτελέσματα, καθώς θα βοηθούσε στην ανάπτυξη, βελτίωση και δημιουργία νέων μοντέλων ταυτοποίησης IoT συσκευών.

Βιβλιογραφία

[01] Tim Cole, “Interview with Kevin Ashton - inventor of IoT: Is driven by the users - SMART INDUSTRY,” 2018. [Online]. Available: https://www.smart-industry.net/interview-with-iot-inventor-kevin-ashton-iot-is-driven-by-the-users/. [Accessed: 22-Oct-2018].

[02] G. Marques, N. Garcia, and N. Pombo, “A Survey on IoT: Architectures, Elements, Applications, QoS, Platforms and Security Concepts,” *Adv. Mob. Cloud Comput. Big Data 5G Era*, vol. 22, pp. 115–130, 2017.

[03] Rob van der Meulen, “Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016,” 2017. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016. [Accessed: 01-Oct-2018].

[04] Cisco Security Research & Operations, “Securing the Internet of Things: A Proposed Framework - Cisco.” [Online]. Available: https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html#7. [Accessed: 10-Dec-2017].

[05] A. Rullo, D. Midi, E. Serra, and E. Bertino, “Strategic Security Resource Allocation for Internet of Things,” *Proc. - Int. Conf. Distrib. Comput. Syst.*, vol. 2016–Augus, no. 0, pp. 737–738, 2016.

[06] “How connected objects help to make lives more insecure – Kaspersky Lab official blog,” 2015. [Online]. Available: https://www.kaspersky.com/blog/surviving-iot/10480/. [Accessed: 11-Dec-2017].

[07] B. Lee, R. Vanickis, F. Rogelio, and P. Jacob, “Situational Awareness based Risk-adaptable Access Control in Enterprise Networks,” no. IoTBDS, pp. 400–405, 2017.

[08] A. A. O. Aafaf Ouaddah, Hajar Mousannif, Anas Abou Elkalam, “Access control in the Internet of Things: Big challenges and new opportunities,” *Comput. Networks*, vol. 112, no. 15 January 2017, pp. 237–262, 2016.

[09] “What is an Enterprise Network? - Definition from Techopedia.” [Online]. Available: https://www.techopedia.com/definition/7044/enterprise-network. [Accessed: 11-Dec-2017].

[10] Steve G. Belovich, “A Brief History of IT Security & Architecture,” 2010.

[11] M. A. Khan and K. Salah, “IoT security: Review, blockchain solutions, and open challenges,” *Futur. Gener. Comput. Syst.*, 2017.

[12] S. V. Flowerday and T. Tuyikeze, “Information security policy development and implementation: The what, how and who,” *Comput. Secur.*, vol. 61, pp. 169–183, 2016.

[13] “NIST Selects Winner of Secure Hash Algorithm (SHA-3) Competition | NIST,” 2012. [Online]. Available: https://www.nist.gov/news-events/news/2012/10/nist-selects-winner-secure-hash-algorithm-sha-3-competition. [Accessed: 10-Dec-2017].

[14] S. Li, *Security Architecture in the Internet of Things*. Elsevier Inc., 2017.

[15] M. Bauer, M. Boussard, N. Bui, and F. Carrez, “Final Architectural Reference Model for IoT,” no. 257521, pp. 53–59, 2013.

[16] “Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα,” 2018. [Online]. Available: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/4C942764EA123CDAC22582480036A204?OpenDocument. [Accessed: 30-Oct-2018].

[17] A. Bryman and E. C. N.-M. L. (HUB S. L.-G. floor H. . B. M. L. (STANDARD L.-2nd floor H. . B. Bell, *Business research methods*. 2007.

[18] B. Publishing Asia, S. Quine, Y. Wells, D. de Vaus, and H. Kendig, “When choice in retirement decisions is missing: Qualitative and quantitative findings of impact on well-being,” *Australas. J. Ageing*, vol. 26, pp. 173–179, 2007.

[19] *IBM SPSS statistics 23 brief guide*. 2015.

[20] Nisarg Desai, “Identifying the Internet of Things – one device at a time | Network World,” 2018. [Online]. Available: https://www.networkworld.com/article/3287927/internet-of-things/identifying-the-internet-of-things-one-device-at-a-time.html. [Accessed: 23-Sep-2018].

[21] “IoT Device Identity Management | DigiCert.com.” [Online]. Available: https://www.digicert.com/images/iot/DeviceIdentityManagement.png. [Accessed: 25-Oct-2018].

[22] Cisco, “Securing the internet of things: A proposed framework.,” *[Online]. Available: http://www.cisco.com/c/en/us/about/securitycenter/ secure-iot-proposed-*

framework.html. accessed: September 2, 2018, 2012. [Online]. Available: https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html#9a. [Accessed: 26-Sep-2018].

[23] T. Kramp, R. van Kranenburg, and S. Lange, *Introduction to the internet of things*. 2013.

Παραρτήματα

Παράρτημα 1 - Online Ερωτηματολόγιο

Χρήση διάχυτων συσκευών και του IOT
Το παρακάτω ερωτηματολόγιο περιλαμβάνει έναν αριθμό ερωτήσεων σχετικά με τον βαθμό στον οποίο εφαρμόζεται η ταυτοποίηση στα δίκτυα των μικρομεσαίων επιχειρήσεων από τη χρήση των διάχυτων συσκευών και του IOT. Οι πληροφορίες που θα δώσετε είναι εμπιστευτικές και θα χρησιμοποιηθούν μόνο για την εξαγωγή ερευνητικών συμπερασμάτων. Θα θέλαμε να σε ευχαριστήσουμε εκ των προτέρων για την υπομονή και τη συνεργασία σας. Το ερωτηματολόγιο είναι ανώνυμο και οι απαντήσεις είναι απολύτως εμπιστευτικές. Οι πληροφορίες, που θα προκύψουν, θα αναλυθούν στατιστικά, θα χρησιμοποιηθούν για καθαρά ερευνητικούς σκοπούς.

* Απαιτείται

1. **Διεύθυνση ηλεκτρονικού ταχυδρομείου** *

Δημογραφικά στοιχεία

2. **1. Έχετε καθήκοντα στο τμήμα πληροφορικής στον οργανισμό?**

* *Να επισημαίνεται μόνο μία έλλειψη.*

- ◯ Ναι - Αν ναι παρακαλώ συνεχίστε στις παρακάτω ερωτήσεις.
- ◯

Οχι *Μετά την τελευταία ερώτηση αυτής της ενότητας, σταματήστε να συμπληρώνετε αυτή τη φόρμα.*

3. **Φύλο**

Να επισημαίνεται μόνο μία έλλειψη.

- Άρρεν
- Θήλυ

4. **Ηλικία**

Να επισημαίνεται μόνο μία έλλειψη.

- 18-25
- 26-35
- 36-45
- 46-55 >55

5. **Εκπαίδευση**

Να επισημαίνεται μόνο μία έλλειψη.

- Γυμνάσιο / Λύκειο
- ΤΕΙ/ΑΕΙ
- Μεταπτυχιακό Άλλο: _____

6 **Έτη εργασιακής εμπειρίας** *Να επισημαίνεται μόνο μία έλλειψη.*

- 1-5 έτη
- 6-10 έτη
- 11-15 έτη
- Πάνω από 15 έτη

Στοιχεία της επιχείρησης

7. **Είδος ιδιοκτησίας της επιχείρησης** *Να επισημαίνεται μόνο μία έλλειψη.*

- Κύριος ιδιοκτήτης
- Συνιδιοκτησία
- Μετοχική Εταιρία

8. **Αριθμός εργαζομένων**

_____

Internet of Things (IoT) στην επιχείρηση

9. **1. Λόγοι χρησιμοποίησης του Internet of Things (IoT) στην επιχείρηση**
Επιλέξτε όλα όσα ισχύουν.

- [ ] Οι απαιτήσεις των καταναλωτών
- [ ] Η μείωση του κόστους
- [ ] Η βελτίωση των παρεχόμενων υπηρεσιών
- [ ] Η αύξηση των πωλήσεων
- [ ] Η βελτίωση της αποδοτικότητας της επιχείρησης
- [ ] Η βελτίωση ελέγχου και ασφαλειας της επιχείρησης
- [ ] Η βελτίωση των σχέσεων με τους συνεργάτες της επιχείρησης
- [ ] Η διαχείριση μεγάλου όγκου πληροφοριών
- [ ] Η είσοδος σε νέες αγορές

Ασφάλεια δικτύου

Security program

---

10. **1. Ασφάλεια των συστημάτων:** *Επιλέξτε όλα όσα ισχύουν.*

- [ ] Η επιχείρηση έχει συγκεκριμένο άτομο ή ομάδα ατόμων στον οποίο θα απευθυνθεί για το συντονισμό των συστημάτων ασφαλείας και σε περίπτωση προβλήματος ασφαλείας
- [ ] Υπάρχει συνεργασία με άλλες εταιρίες για την ασφάλεια των συστημάτων σας

11. **2. Οι συνεργάτες της εταιρίας έχουν πρόσβαση στα δεδομένα των πελατών μας** *Να επισημαίνεται μόνο μία έλλειψη.*

- ◯ Ναι
- ◯ Οχι

Security Policy

Ποιες από τις παρακάτω εφαρμογές συμμετέχουν στο δίκτυο της επιχείρησης και συγκαταλέγονται στην γενικότερη κατηγορία του Internet of Things (IoT)? Παρακαλώ απαντήστε στις παρακάτω ερωτήσεις σημειώνοντας τον συμμετοχής στο αντίστοιχο τετράγωνο (1= Καθόλου, 5= Πάρα πολύ)

12. **1. Υπάρχουν έγραφα σχετικά με την πολιτική και τις διαδικασίες ασφαλείας των υπολογιστικών συστημάτων.**
Να επισημαίνεται μόνο μία έλλειψη.

1	2	3	4	5
◯	◯	◯	◯	◯

13. **2. Υπάρχει κατηγοριοποίηση των δεδομένων των πελατών και της επιχείρησης αναφορικά με τη σημαντικότητα τους? (π.χ. κανονικά, εμπιστευτικά, απόρρητα)**
Να επισημαίνεται μόνο μία έλλειψη.

1	2	3	4	5
◯	◯	◯	◯	◯

14. **3. Υπάρχουν επίσημοι αποδεκτοί κανόνες ασφαλείας για κάθε λειτουργία (π.χ. συσκευές επικοινωνίας, υπολογιστές)**
Να επισημαίνεται μόνο μία έλλειψη.

1	2	3	4	5
◯	◯	◯	◯	◯

15. **4. Υπάρχει συγκεκριμένη διαδικασία για τη διατήρηση της ασφάλειας στην επιχείρηση** *Να επισημαίνεται μόνο μία έλλειψη.*

1	2	3	4	5
◯	◯	◯	◯	◯

Risk management

Ποιες από τις παρακάτω εφαρμογές συμμετέχουν στο δίκτυο της επιχείρησης και συγκαταλέγονται στην γενικότερη κατηγορία του Internet of Things (IoT)? Παρακαλώ απαντήστε στις παρακάτω ερωτήσεις σημειώνοντας τον συμμετοχής στο αντίστοιχο τετράγωνο (1= Καθόλου, 5= Πάρα πολύ)

16. **1. Υπάρχει κάποια διαδικασία που αξιολογεί το πιθανό ρίσκο ασφαλείας** *Να επισημαίνεται μόνο μία έλλειψη.*

1	2	3	4	5
◯	◯	◯	◯	◯

17. **2. Υπάρχει κάποια διαδικασία που να μειώνει το ρίσκο ασφαλείας**
Να επισημαίνεται μόνο μία έλλειψη.

1	2	3	4	5

◯	◯	◯	◯	◯

18 **3. Υπάρχει κάποια διαδικασία που να εξασφαλίζει την ασφάλεια των δεδομένων** *Να επισημαίνεται μόνο μία έλλειψη.*

1	2	3	4	5
◯	◯	◯	◯	◯

19. **4. Υπάρχει κάποια διαδικασία που να εντοπίζει νέες πρακτικές και νόμους αναφορικά με την ασφάλεια των υπολογιστικών συστημάτων** *Να επισημαίνεται μόνο μία έλλειψη.*

1	2	3	4	5
◯	◯	◯	◯	◯

Training and Awareness

Ποιες από τις παρακάτω εφαρμογές συμμετέχουν στο δίκτυο της επιχείρησης και συγκαταλέγονται στην γενικότερη κατηγορία του Internet of Things (IoT)? Παρακαλώ απαντήστε στις παρακάτω ερωτήσεις σημειώνοντας τον συμμετοχής στο αντίστοιχο τετράγωνο (1= Καθόλου, 5= Πάρα πολύ)

20. **1. Οι υπάλληλοι της επιχείρησης έχουν λάβει επίσημη εκπαίδευση αναφορικά με την ασφάλεια των υπολογιστικών συστημάτων** *Να επισημαίνεται μόνο μία έλλειψη.*

1	2	3	4	5
◯	◯	◯	◯	◯

21. **2. Η πολιτική της επιχείρησης έχει μεταφερθεί και εξηγηθεί στους υπαλλήλους** *Να επισημαίνεται μόνο μία έλλειψη.*

1	2	3	4	5
◯	◯	◯	◯	◯

22. **3. Γίνονται περιοδικές επιμορφωτικές ενημερώσεις αναφορικά με την ασφάλεια των υπολογιστικών συστημάτων**
Να επισημαίνεται μόνο μία έλλειψη.

1	2	3	4	5
◯	◯	◯	◯	◯

Background checks

Ποιες από τις παρακάτω εφαρμογές συμμετέχουν στο δίκτυο της επιχείρησης και συγκαταλέγονται στην γενικότερη κατηγορία του Internet of Things (IoT)? Παρακαλώ απαντήστε στις παρακάτω ερωτήσεις σημειώνοντας τον συμμετοχής στο αντίστοιχο τετράγωνο (1= Καθόλου, 5= Πάρα πολύ)

23. **1. Ο οργανισμός κάνει έλεγχο για πιθανή παραβατικότητα των υπαλλήλων στο παρελθόν** *Να επισημαίνεται μόνο μία έλλειψη.*

1	2	3	4	5
◯	◯	◯	◯	◯

24 **2. Οι υπάλληλοι υπογράφουν μία φόρμα εμπιστευτικότητας κατά την πρόσληψή τους** *Να επισημαίνεται μόνο μία έλλειψη.*

1	2	3	4	5
◯	◯	◯	◯	◯

25. **3. Υπάρχει μία συγκεκριμένη διαδικασία διαχείρισης της απομάκρυνσης ή της μεταφοράς ενός εργαζομένου.**
Να επισημαίνεται μόνο μία έλλειψη.

1	2	3	4	5
◯	◯	◯	◯	◯

Physical Security

Ποιες από τις παρακάτω εφαρμογές συμμετέχουν στο δίκτυο της επιχείρησης και συγκαταλέγονται στην γενικότερη κατηγορία του Internet of Things (IoT)? Παρακαλώ απαντήστε στις παρακάτω ερωτήσεις σημειώνοντας τον συμμετοχής στο αντίστοιχο τετράγωνο (1= Καθόλου, 5= Πάρα πολύ)

26. **1. Υπάρχει ένα οργανωμένο σύστημα πρόσβασης στις εγκαταστάσεις της επιχείρησης** *Να επισημαίνεται μόνο μία έλλειψη.*

1	2	3	4	5
◯	◯	◯	◯	◯

27. **2. Υπάρχει οργανωμένο σύστημα ασφαλείας των εγκαταστάσεων** *Να επισημαίνεται μόνο μία έλλειψη.*

1	2	3	4	5

Network security

Ποιες από τις παρακάτω εφαρμογές συμμετέχουν στο δίκτυο της επιχείρησης και συγκαταλέγονται στην γενικότερη κατηγορία του Internet of Things (IoT)? Παρακαλώ απαντήστε στις παρακάτω ερωτήσεις σημειώνοντας τον συμμετοχής στο αντίστοιχο τετράγωνο (1= Καθόλου, 5= Πάρα πολύ)

28. **1. Υπάρχουν εσωτερικά και εξωτερικά συστήματα που προστατεύονται από επιλογές πρόσβασης**
Να επισημαίνεται μόνο μία έλλειψη.

1	2	3	4	5
◯	◯	◯	◯	◯

29. **2. Τα συστήματα λειτουργίας που μεταφέρουν και αποθηκεύουν ευαίσθητες πληροφορίες είναι προστατευμένα.**
Να επισημαίνεται μόνο μία έλλειψη.

1	2	3	4	5
◯	◯	◯	◯	◯

30 **3. Υπάρχει μία προκαθορισμένη προσέγγιση για την προστασία του δικτύου της επιχείρησης**
(π.χ. firewall για τα public και private networks, internal VLAN, firewall separation) *Να επισημαίνεται μόνο μία έλλειψη.*

1	2	3	4	5
◯	◯	◯	◯	◯

31. **4. Ευαίσθητες πληροφορίες μεταφέρονται σε εξωτερικούς αποδέκτες** *Να επισημαίνεται μόνο μία έλλειψη.*

◯ Ναι Όχι
◯ Άλλο:
◯ _____

32. **5. Χρησιμοποιούνται τρόποι προστασίας των ευαίσθητων πληροφοριών όταν μεταφέρονται σε εξωτερικούς αποδέκτες (π.χ. ασφαλής VPN connection, encryption)** *Να επισημαίνεται μόνο μία έλλειψη.*

1	2	3	4	5
◯	◯	◯	◯	◯

33. **6. Γίνονται συχνά έλεγχοι για τον εντοπισμό προβλημάτων ασφαλείας στα συστήματα επικοινωνίας και στα πληροφοριακά συστήματα** *Να επισημαίνεται μόνο μία έλλειψη.*

1	2	3	4	5
◯	◯	◯	◯	◯

34. **7. Οι εξωτερική πρόσβαση στο πληροφοριακό σύστημα παρακολουθείται σε τακτά χρονικά διαστήματα ώστε να αποτραπεί η είσοδος χωρίς άδεια** *Να επισημαίνεται μόνο μία έλλειψη.*

1	2	3	4	5
◯	◯	◯	◯	◯

Logical access

Ποιες από τις παρακάτω εφαρμογές συμμετέχουν στο δίκτυο της επιχείρησης και συγκαταλέγονται στην γενικότερη κατηγορία του Internet of Things (IoT)? Παρακαλώ απαντήστε στις παρακάτω ερωτήσεις σημειώνοντας τον συμμετοχής στο αντίστοιχο τετράγωνο (1= Καθόλου, 5= Πάρα πολύ)

35. **1. Υπάρχει λογική διαδικασία και παροχή άδειας πρόσβασης με βάση τη θέση των εργαζομένων** *Να επισημαίνεται μόνο μία έλλειψη.*

- ◯ Ναι
- ◯ Όχι

36. **2. Παρέχεται μοναδικό ID και password σε κάθε εργαζόμενο** *Να επισημαίνεται μόνο μία έλλειψη.*

- ◯ Ναι
- ◯ Όχι

37 **3. Ζητούνται ενέργειες όπως το μέγεθος του password, η πολυπλοκότητα του, και η συχνή αλλαγή του**

Να επισημαίνεται μόνο μία έλλειψη.

- Ναι
- Όχι

38. **4. Υπάρχει κάποια λίστα με τους υπαλλήλους που έχουν άδεια πρόσβασης (π.χ. Active directory user list)**
Να επισημαίνεται μόνο μία έλλειψη.

- Ναι
- Όχι

39. **5. Υπάρχει κάποια λίστα με τις δεκτές κινητές συσκευές (π.χ. smartphones)** *Να επισημαίνεται μόνο μία έλλειψη.*

- Ναι
- Όχι

40. **6. Χρησιμοποιείται το αυτόματο logoff από τις συσκευές του δικτύου** *Να επισημαίνεται μόνο μία έλλειψη.*

- Ναι
- Όχι

41. **7. Τα user IDs των χρηστών είναι ανιχνεύσιμα** *Να επισημαίνεται μόνο μία έλλειψη.*

- Ναι
- Όχι

42. **8. Operations Management** *Επιλέξτε όλα όσα ισχύουν.*

- [ ] Διαθέτετε Antivirus
- [ ] Τα πληροφοριακά συστήματα παρακολουθούνται αναφορικά με την ασφάλεια
- [ ] Η χρησιμοποίηση και η επεξεργασία των media προστατεύεται με συγκεκριμένες διαδικασίες(π.χ. encryption)

Business continuity management

Ποιες από τις παρακάτω εφαρμογές συμμετέχουν στο δίκτυο της επιχείρησης και συγκαταλέγονται στην γενικότερη κατηγορία του Internet of Things (IoT)? Παρακαλώ απαντήστε στις παρακάτω ερωτήσεις σημειώνοντας τον συμμετοχής στο αντίστοιχο τετράγωνο (1= Καθόλου, 5= Πάρα πολύ)

43. **1. Γίνεται back up των πληροφοριών και των ευαίσθητων δεδομένων** *Να επισημαίνεται μόνο μία έλλειψη.*

1	2	3	4	5
⬭	⬭	⬭	⬭	⬭

Παράρτημα 2 - Συγκατάθεση

Έντυπο συγκατάθεσης
Καλησπέρα σας, ονομάζομαι Παναγιώτης Πιερή και θα σας παρακαλούσα όπως αφιερώσετε τον κατάλληλο χρόνο, για να λάβετε μέρος στην ακόλουθη έρευνα. Η έρευνα γίνεται με σκοπό να διαφανεί σε ποιο βαθμό εφαρμόζεται η ταυτοποίηση στα δίκτυα των μικρομεσαίων επιχειρήσεων, από τη χρήση των διάχυτων συσκευών και του IOT.

Η έρευνα διεξάγεται στα πλαίσια του μεταπτυχιακού προγράμματος «Ασφάλεια Υπολογιστών & Δικτύων» του Ανοικτού Πανεπιστήμιου Κύπρου. Τα στοιχεία σας δεν πρόκειται να χρησιμοποιηθούν ή να αποκαλυφθούν.
Για οποιαδήποτε διευκρίνηση θα είμαι στη διάθεση σας. Οι τρόποι επικοινωνίας είναι μέσω τηλεφωνικής επικοινωνίας στο 99979330 ή στο email: panayiotis.pieri@gmail.com

Δεν πρέπει να συμμετάσχετε, εάν δεν επιθυμείτε ή εάν έχετε οποιουσδήποτε ενδοιασμούς αφορούν τη συμμετοχή σας στην έρευνα.
Είστε ελεύθεροι να αποσύρετε οποιαδήποτε στιγμή εσείς επιθυμείτε τη συγκατάθεση, για τη συμμετοχή σας στην έρευνα.

Σύντομος Τίτλος της Έρευνας στην οποία καλείστε να συμμετάσχετε

Σε ποιο βαθμό εφαρμόζεται η ταυτοποίηση στα δίκτυα των μικρομεσαίων επιχειρήσεων από τη χρήση των διάχυτων συσκευών και του IOT.

* Απαιτείται

Διεύθυνση ηλεκτρονικού ταχυδρομείου *

_____

1. **Επιβεβαιώνω ότι έχω διαβάσει και καταλάβει τις πιο πάνω πληροφορίες**

☐ ΝΑΙ ☐ ΟΧΙ

2. **Δηλώνω τη συγκατάθεση μου για τη συμμετοχή μου.**

☐ ΝΑΙ ☐ ΟΧΙ

3. **Επίθετο:**

_____

4. **Όνομα:**

_____

5. **Υπογραφή:(ή Ονοματεπώνυμο ολογράφως αν το παρών έντυπο είναι ηλεκτρονικά)**

_____

6. **Ημερομηνία:**