Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια Υπολογιστών και Δικτύων*

Μεταπτυχιακή Διατριβή

Ασφάλεια και προστασία δεδομένων σε IoT τεχνολογίες – Μελέτη περίπτωσης

Βασίλειος Βασίλογλου

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Δεκέμβριος 2020

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια Υπολογιστών και Δικτύων*

Μεταπτυχιακή Διατριβή

Ασφάλεια και προστασία δεδομένων σε IoT τεχνολογίες – Μελέτη περίπτωσης

Βασίλειος Βασίλογλου

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

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 2020

Περίληψη

Η παρούσα διατριβή πραγματεύεται την λεπτομερή ανάλυση των θεμάτων ασφαλείας που διέπουν την IoT τεχνολογία με σκοπό να ενταχθούν κατάλληλα στο πλαίσιο μίας εκτίμησης αντικτύπου ως προς την προστασία προσωπικών δεδομένων. Στο θεωρητικό μέρος υλοποιείται μια προσέγγιση των ζητημάτων που αφορούν τις τεχνολογίες IOT, όπως η αρχιτεκτονική τους, οι εφαρμογές τους, καθώς και η τεχνολογία τους. Ακολούθως, μελετώνται τα ενδεχόμενα προβλήματα ασφαλείας που απορρέουν από την εφαρμογή τους, ενώ αναλύονται οι κίνδυνοι που υφίστανται από τις πιθανές επιθέσεις. Επιπρόσθετα, αναφέρονται οι απαιτήσεις και οι τεχνικές ασφαλείας, ώστε να είναι σε θέση να χρησιμοποιηθούν οι τεχνολογίες IoT, με όφελος προς τους χρήστες. Περαιτέρω, διερευνώνται και θέματα ιδιωτικότητας που ανακύπτουν, υπό το φως του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων.

Ως μελέτη περίπτωσης, εκπονείται στο πειραματικό μέρος μία εκτίμηση αντικτύπου ως προς την προστασία προσωπικών δεδομένων σε μια συγκεκριμένη κατηγορία της τεχνολογίας Διαδικτύου των Πραγμάτων (Internet of Things), το «Έξυπνο Σπίτι» (Smart Home). Η μελέτη αυτή γίνεται με τη χρήση ενός κατάλληλου εργαλείου λογισμικού γενικής χρήσης για Data Protection Impact Assessment (DPIA) που έχει αναπτυχθεί από εποπτική Αρχή Προστασίας Δεδομένων, ενώ περαιτέρω, ειδικά για την αναγνώριση κινδύνων ασφάλειας σε IoT εφαρμογές, αξιοποιείται σχετική πληροφόρηση από τον Ευρωπαϊκό Οργανισμό Κυβερνοασφάλειας. Μέσα από τη διαδικασία αυτή εξάγονται τ' ανάλογα συμπεράσματα για τη χρησιμότητα της μεθόδου.

Summary

This thesis deals with the detailed analysis of the security issues governing IoT technology with a view to being properly integrated into an impact assessment on personal data protection. In the theoretical part, an approach to IoT technologies, such as their architecture, applications and technology, is implemented. The possible security issues arising from their implementation are then examined, and the risks arising from the possible attacks are analysed. In addition, security requirements and techniques are mentioned to enable the use of IoT technologies, with the benefit of the users. Furthermore, privacy issues arising are also investigated in the light of the General Regulation on Protection of Personal Data.

As a case study, a privacy impact assessment is carried out in the experimental part on a specific category of Internet of Things, Smart Home. This study is conducted using a suitable generic software tool for Data Protection Impact Assessment (DPIA) developed by a Supervisory Data Protection Authority, and further, specifically for the recognition of security risks in IoT applications, relevant information is used by the European Cyber Security Agency. This procedure draws similar conclusions on the usefulness of the method.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω από καρδιάς τον καθηγητή μου κ. Κωνσταντίνο Λιμνιώτη για την αμέριστη βοήθεια και καθοδήγησή του. Επίσης, θα ήθελα να ευχαριστήσω την οικογένειά μου, αλλά και τη σύντροφό μου Ιωάννα που με στήριξαν και κατάφερα να φέρω εις πέρας το όλο εγχείρημα. Χωρίς τη συμπαράσταση όλων, δεν θα είχα καταφέρει να ολοκληρώσω την Μεταπτυχιακή μου Διατριβή.

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Καθώς οι καθημερινές απαιτήσεις της ζωής συνεχώς αυξάνονται, δεν θα μπορούσε και η τεχνολογία να παραμείνει στάσιμη. Η απαίτηση για περισσότερη αυτοματοποίηση οδήγησε στην ανάπτυξη νέων τεχνολογιών, όπως οι έξυπνες πόλεις (smart cities), έξυπνα σπίτια (smart homes) κ.λπ., οι οποίες χρησιμοποιούν μία γκάμα από έξυπνες συσκευές (smart devices) που επικοινωνούν μεταξύ τους με τη χρήση του διαδικτύου και συγκεκριμένων πρωτοκόλλων και αισθητήρων, καθώς και συλλέγουν/αποστέλλουν συνεχώς δεδομένα, ώστε με τη βοήθεια της τεχνητής νοημοσύνης να δημιουργούν διάφορα προφίλ της καθημερινότητας και να βοηθούν τους ανθρώπους να απλοποιήσουν τη ζωή τους και να την κάνουν πιο ευέλικτη. Το σύνολο όλων αυτών των τεχνολογιών βρίσκονται κάτω από το φάσμα ενός ραγδαία αναπτυσσόμενου τομέα που ονομάζεται Διαδίκτυο των Πραγμάτων (Internet of Things).

Από τη στιγμή που όλες αυτές οι έξυπνες συσκευές συλλέγουν δεδομένα από την καθημερινότητα των ανθρώπων, αλλά και ευαίσθητα προσωπικά τους δεδομένα, αυξάνεται παράλληλα και η ανάγκη για περισσότερη ασφάλεια και ιδιωτικότητα. Κρίνεται ιδιαίτερα σημαντικό ζήτημα, λοιπόν, η διαφύλαξη της ιδιωτικής ζωής, εξαιτίας της ευαισθησίας των προσωπικών δεδομένων και των device-centric δεδομένων. Στην αντίθετη περίπτωση όπου δε θα συμβεί και θα διαπιστωθεί διαρροή των δεδομένων, ακόμα και σε μικρό βαθμό, ελλοχεύει ο κίνδυνος εμφάνισης δυσμενών επιπτώσεων. Τα στοιχεία προστασίας των δεδομένων στο συγκεκριμένο επίπεδο καθίστανται αναγκαία με σκοπό τη διασφάλιση της ιδιωτικότητας, παρέχοντας την ικανότητα στους αλγόριθμους να προστατεύουν τα δεδομένα και ταυτόχρονα να εισάγουν τα στοιχεία ανωνυμίας. Ωστόσο, για την επίτευξη του παραπάνω σκοπού προβάλλει αναγκαία η προσβασιμότητά τους στο πέμπτο επίπεδο.

1.1 Σκοπός έρευνας

Σκοπός της διατριβής είναι ν' αναλυθούν λεπτομερώς και με συστηματικό τρόπο τα θέματα ασφάλειας που διέπουν την IoT τεχνολογία, με απώτερο σκοπό να ενταχθούν κατάλληλα στο πλαίσιο μίας εκτίμησης αντικτύπου ως προς την προστασία προσωπικών δεδομένων. Ειδικότερα, η διατριβή θα εστιάσει στην προσέγγιση των ζητημάτων που αφορούν τις τεχνολογίες IoT, όπως την αρχιτεκτονική τους, τις εφαρμογές τους, καθώς και τις συναφείς τεχνολογίες, δίνοντας έμφαση στα ενδεχόμενα προβλήματα ασφαλείας όπου απορρέουν από την εφαρμογή τους, αναλύοντας τους κινδύνους που υφίστανται από τις πιθανές επιθέσεις. Επιπρόσθετα, θα μελετηθούν οι συναφείς απαιτήσεις και οι τεχνικές ασφαλείας, ώστε να είναι σε θέση να χρησιμοποιηθούν οι τεχνολογίες IoT με όφελος προς τους χρήστες, καθώς επίσης και οι σχετικές νομικές απαιτήσεις ως προς την προστασία προσωπικών δεδομένων. Ακολούθως τα ανωτέρω θα ενταχθούν κατάλληλα σε μία εκτίμηση αντικτύπου ως προς την προστασία προσωπικών δεδομένων (Data Protection Impact Assessment – DPIA), για την ειδική περίπτωση IoT τεχνολογιών σε περιβάλλον «έξυπνου σπιτιού» (smart home), η οποία θα ενσωματώσει όχι μόνο ζητήματα ασφάλειας αλλά και ιδιωτικότητας.

1.2 Μεθοδολογία έρευνας

Η υλοποίηση των παραπάνω στόχων θα προέλθει πρώτα μέσα από βιβλιογραφική και συγκριτική μελέτη επιστημονικών άρθρων και βιβλίων πάνω στα ζητήματα αυτά. Η μελέτη αυτή θα επιτρέψει στη συνέχεια την υλοποίηση της μεθοδολογίας DPIA για το Έξυπνο Σπίτι μέσα από το ομώνυμο εργαλείο. Συγκεκριμένα, θα αξιοποιηθούν κατάλληλα εργαλεία λογισμικού τόσο για την ανάλυση κινδύνων ασφάλειας σε IoT περιβάλλοντα (βλ. ενδεικτικώς, το σχετικό εργαλείο λογισμικού του Ευρωπαϊκού Οργανισμού Κυβερνοασφάλειας (ENISA)), όσο και για την εκτίμηση αντικτύπου (βλ. σχετικώς το εργαλείο λογισμικού της Αρχής Προστασίας Δεδομένων της Γαλλίας).

1.3 Βασικά ερευνητικά ερωτήματα

Τα ερευνητικά ερωτήματα που διερευνώνται σε αυτή τη διατριβή είναι:

α) Κατηγοριοποίηση ζητημάτων ασφάλειας σε μελέτη περίπτωσης IoT εφαρμογής.

β) Πώς αντιμετωπίζονται ζητήματα ιδιωτικότητας και προστασίας προσωπικών δεδομένων σε περιβάλλοντα IoT τα οποία ανακύπτουν λόγω τεχνολογικών λύσεων που υιοθετούνται για την αντιμετώπιση ζητημάτων ασφάλειας;

γ) Πόσο πλήρης και αποτελεσματική είναι η μεθοδολογία DPIA ως προς την επιλογή των βέλτιστων τεχνολογικών λύσεων σε μία περίπτωση «έξυπνου» σπιτιού;

δ) Πώς αξιολογείται από την άποψη της ασφάλειας δεδομένων και ιδιωτικότητας η εφαρμογή IoT Έξυπνο Σπίτι, ως μια από τις πλέον τεχνολογικά προηγμένες εφαρμογές Διαδικτύου των Πραγμάτων;

1.4 Αναγκαιότητα και σπουδαιότητα έρευνας

Η εφαρμογή «Έξυπνο Σπίτι» (Smart Home) συνιστά μια από τις πιο σύγχρονες αλλά και αμφιλεγόμενες εφαρμογές του Διαδικτύου των Πραγμάτων. Πρόκειται για μια εφαρμογή που παρέχει σημαντικές υπηρεσίες μεν στο χρήστη της, αλλά θέτει την ασφάλεια και την ιδιωτικότητα προσωπικών δεδομένων υψηλής ευαισθησίας σε μεγάλη διακινδύνευση. Εάν οι κίνδυνοι αυτοί είναι αποδεκτοί θα πρέπει εντέλει να αποφασιστεί από το χρήστη, αλλά η επιστημονική έρευνα οφείλει να εξετάσει το ζήτημα λεπτομερώς ως προς την υιοθέτηση των βέλτιστων τεχνολογικών λύσεων, συγκεράζοντας τις απαιτήσεις ασφάλειας και ιδιωτικότητας.

Παράλληλα, η εκπόνηση εκτίμησης αντικτύπου ως προς την προστασία προσωπικών δεδομένων είναι μια νέα υποχρέωση για όσους επεξεργάζονται προσωπικά δεδομένα υψηλού κινδύνου, η οποία είναι σε ισχύ από το 2018. Λόγω του σχετικά πρόσφατου χαρακτήρα της, δεν έχουν ακόμη παγιωθεί συγκεκριμένες μεθοδολογίες για την εκπόνησή της. Ειδικά για τόσο κρίσιμες επεξεργασίες, όπως το «έξυπνο» σπίτι, δεν είναι γνωστές επίσημες καταγραφές εκτιμήσεων αντικτύπου, οι οποίες να δίνουν με συστηματικό τρόπο απαντήσεις στα ερωτήματα του κατά πόσον αντιμετωπίζονται επαρκώς οι κίνδυνοι ασφάλειας και ιδιωτικότητας.

1.5 Μεθοδολογία της έρευνας

Η παρούσα διατριβή εστίασε κατ' αρχάς στην καταγραφή ζητημάτων ασφάλειας που υπάρχουν σε εφαρμογές IoT, παρουσιάζοντας μία εμπεριστατωμένη μελέτη γνωστών απειλών. Μελετά, επίσης, τις βασικές υποχρεώσεις για τη νόμιμη επεξεργασία προσωπικών δεδομένων, οι οποίες ανακύπτουν από το Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR).

Ως μελέτη περίπτωσης, επελέγη ένα ιδεατό σενάριο «έξυπνου» σπιτιού, προκειμένου να εκπονηθεί μια εκτίμηση αντικτύπου ως προς την προστασία προσωπικών δεδομένων. Για την εκπόνηση αυτή, στηριχτήκαμε στους εξής δύο πυλώνες:

1. Αξιοποίηση ενός ειδικού εργαλείου λογισμικού που έχει αναπτυχθεί από αρμόδια εποπτική Αρχή Προστασίας Προσωπικών Δεδομένων, το οποίο υποβοηθά στην απάντηση ερωτημάτων που άπτονται της εκτίμησης αντικτύπου. Το εργαλείο είναι γενικό, για κάθε είδους επεξεργασία, οπότε διερευνήθηκε η αποτελεσματικότητά του για μια σύνθετη περίπτωση, όπως αυτή του «έξυπνου» σπιτιού.

2. Αξιοποίηση καταγεγραμμένων απειλών που έχει προδιαγράψει ο Ευρωπαϊκός Οργανισμός για την κυβερνοασφάλεια (ENISA) αναφορικά με εφαρμογές IoT. Οι απειλές αυτές λήφθηκαν κατάλληλα υπόψη κατά την εκτίμηση αντικτύπου.

Το παράδειγμά μας, αν και ρεαλιστικό, είναι υποθετικό. Γι' αυτό και έγιναν διάφορες παραδοχές τόσο ως προς τις παρεχόμενες υπηρεσίες, όσο και ως προς τις διαθέσιμες τεχνολογίες. Σε κάθε περίπτωση, ωστόσο, αποτυπώνει την αποτελεσματικότητα και χρησιμότητα που μπορεί να έχει μια ορθά εκπονηθείσα εκτίμηση αντικτύπου για περιπτώσεις επεξεργασίας προσωπικών δεδομένων μέσω IoT εφαρμογών.

1.6 Δομή της διατριβής

Η παρούσα διατριβή αποτελείται από πέντε κεφάλαια. Στο πρώτο κεφάλαιο «Διαδίκτυο των Πραγμάτων» γίνεται μια γενική εισαγωγή στην τεχνολογία του Internet of Things, όπου δίνονται διάφοροι ορισμοί, αναλύεται η αρχιτεκτονική του και περιγράφονται οι εφαρμογές και γενικότερα η τεχνολογία του. Στο δεύτερο κεφάλαιο «Ασφάλεια στο Διαδίκτυο των Πραγμάτων» αναλύονται οι διάφοροι κίνδυνοι και ευπάθειες που διέπουν την τεχνολογία του Internet of Things, καθώς και οι επιθέσεις ενάντια στην ασφάλειά του. Γίνεται ιδιαίτερη μνεία στις απαιτήσεις, αλλά και στις τεχνικές ασφάλειας και διαχείρισης κινδύνου της τεχνολογίας και δεν θα μπορούσε να παραλειφθεί η αναφορά στον κύριο στόχο της τεχνολογίας που αφορά την προστασία των προσωπικών δεδομένων.

Το τρίτο κεφάλαιο «Ιδιωτικότητα και προστασία των προσωπικών δεδομένων» περιγράφει τι είναι προσωπικά δεδομένα, γιατί είναι σημαντική η προστασία τους, αλλά και ποιο είναι το κύριο νομικό πλαίσιο στην Ευρώπη (GDPR) που επιβάλλει την μέριμνα για την προστασία τους. Στο τέταρτο κεφάλαιο «Μελέτη περίπτωσης: Εκτίμηση αντικτύπου προστασίας δεδομένων σε «έξυπνο» σπίτι» γίνεται μελέτη του εργαλείου PIA (Privacy Impact Assessment) και πραγματοποιείται εφαρμογή της μεθοδολογίας Αξιολόγησης Αντικτύπου Προστασίας Δεδομένων (DPIA) με το εργαλείο αυτό για την τεχνολογία του έξυπνου σπιτιού (Smart Home). Πρόκειται για εργαλείο που παρέχει όλες τις αναγκαίες κατηγορίες αξιολόγησης, που μας επιτρέπουν να υλοποιούμαι μια εμπεριστατωμένη και πλήρη αποτίμηση της ιδιωτικότητας μιας εφαρμογής.

Στο πέμπτο και τελευταίο κεφάλαιο «Συμπεράσματα», διεξάγονται τα διάφορα συμπεράσματα που απορρέουν από την έρευνα που πραγματοποιήθηκε.

Κεφάλαιο 2

Διαδίκτυο των πραγμάτων

Το διαδίκτυο των Πραγμάτων (IoT) αποτελεί τον καθρέφτη της βιομηχανικής και της τεχνολογικής εξέλιξης. Η παρουσία του στον κλάδο της επιστήμης και της τεχνολογίας, έχει επιφέρει μία καινοτόμα προσέγγιση σχετικά με την αλληλεπίδραση και τη διασύνδεση των αντικειμένων, προς τη δημιουργία έξυπνων υπηρεσιών και εφαρμογών, δίχως την ανθρώπινη επιρροή.

Αποτελεί ένα δίκτυο φυσικών αντικειμένων και συσκευών όπου εμπεριέχουν ενσωματωμένα ηλεκτρονικά συστήματα, λογισμικά και αισθητήρες για τη συλλογή και την ανταλλαγή δεδομένων. Η ιδέα γύρω από τη τεχνολογία του Internet of Things (IoT), αποτελεί η σύνδεση όλων των ηλεκτρονικών συσκευών μεταξύ τους, αλλά και με το διαδίκτυο.

Ωστόσο για την εφαρμογή της συγκεκριμένης τεχνολογίας, απαραίτητη προϋπόθεση αποτελεί η χρήση και η σύνδεση με το διαδίκτυο, γεγονός που επιφέρει ερωτήματα σχετικά με την προστασία των προσωπικών δεδομένων. Το διαδίκτυο των πραγμάτων έχει εισχωρήσει με γοργό ρυθμό στην καθημερινότητα των ανθρώπων, με συνέπεια ο κίνδυνος από τις επιθέσεις να παρουσιάζει ανοδικές τάσεις. Επομένως, το ζήτημα που απασχολεί την επιστημονική κοινότητα, όσον αφορά τη χρήση του IoT, αποτελεί η εύρεση τρόπων επίλυσης προς τις επιθέσεις, ώστε η εφαρμογή του διαδικτύου των πραγμάτων να αποδίδει πλεονεκτήματα στην ποιότητα ζωής των χρηστών, ενώ ταυτόχρονα να αισθάνονται εμπιστοσύνη και ασφάλεια.

Εικόνα 1. Τεχνολογία Internet of Things (IoT) (https://www.cybercureme.com/end-to-end-cyber-security-for-iot-ecosystems-to-protect-iot-devices-from-cyber-threats/)

2.1 Ορισμός Internet of Things (IOT)

Ορισμένοι εννοιολογικοί προσδιορισμοί έχουν αποδοθεί στην τεχνολογία του διαδικτύου των πραγμάτων (IoT). Οι πρώτοι ορισμοί που αποδόθηκαν είχαν σχέση με την ταυτοποίηση μέσω ραδιοσυχνοτήτων (RFID), από το ερευνητικό εργαστήριο του Τεχνολογικού Ινστιτούτου της Μασαχουσέτης (MIT) στην Αμερική.

Ένας ορισμός για το διαδίκτυο των πραγμάτων αποτελεί "*Η βασική ιδέα αυτής της έννοιας είναι η συνεχής παρουσία γύρω μας μιας ποικιλίας πραγμάτων ή αντικειμένων (things) - όπως ετικέτες (tags) ταυτοποίησης μέσω ραδιοσυχνοτήτων (RFID tags), αισθητήρες, ενεργοποιητές, κινητά τηλέφωνα, τα οποία μέσω μοναδικών συστημάτων διευθυνσιοδότησης, είναι σε θέση ν' αλληλοεπιδρούν μεταξύ τους και να συνεργάζονται με γειτονικά τους για να επιτύχουν κοινούς στόχους* " (Atzori et al., 2010).

Ένας δεύτερος εννοιολογικός προσδιορισμός δόθηκε από το Ευρωπαϊκό Ινστιτούτο Έρευνας (IERC) και αναρτήθηκε στην επίσημη ιστοσελίδα του, όπου αναφέρει: *"Μια διαδραστική υποδομή ενός παγκόσμιου δικτύου με δυνατότητες αυτοπροσαρμογής βασισμένο σε προτυποποιημένα για διαλειτουργικά πρωτόκολλα επικοινωνίας, όπου φυσικά και εικονικά αντικείμενα (Things) έχουν ταυτότητες, φυσικά χαρακτηριστικά και εικονικές προσωπικότητες και χρησιμοποιούν έξυπνες διεπαφές και ενσωματώνονται αδιάληπτα στο δίκτυο πληροφοριών."*

Ένας άλλος εννοιολογικός προσδιορισμός είναι ο διαχωρισμός της έννοιας σε δύο κατηγορίες, εκ των οποίων στην πρώτη αναφέρεται το διαδίκτυο των πραγμάτων ως μια ιδέα, ενώ στη δεύτερη ως μια υποδομή. Ο προσδιορισμός αποτελεί μία σύμπτυξη των δύο κατηγοριών και αναφέρεται ως εξής: *"Ένα ευρέως αναπτυγμένο σύνολο εφαρμογών πληροφορικής/επικοινωνιών και/ή συστήματος εφαρμογής-κατανάλωσης, το οποίο αναπτύσσεται σε τοπικό (L-IoT), μητροπολιτικό (M-IoT), περιφερειακό (R-IoT) , ή παγκόσμιο (G-IoT) επίπεδο, (α) που αποτελείται από κατανεμημένα όργανα μέτρησης (Things) με ενσωματωμένες επικοινωνίες μονόδρομης ή αμφίδρομης επικοινωνίας και ορισμένες (ή, κατά καιρούς, όχι) υπολογιστικές δυνατότητες, (β) όπου αντικείμενα είναι προσβάσιμα μέσω μιας πληθώρας ασύρματων ή ενσύρματων τοπικών και/ή οικουμενικών δικτύων, (γ) των οποίων τα εισερχόμενα δεδομένα και/ή εξερχόμενες εντολές διοχετεύονται ή εκδίδονται από ένα σύστημα (ή εφαρμογή) με (υψηλό) βαθμό (ανθρώπινη ή υπολογιστική) νοημοσύνης* (Minoli, 2013).

2.2 Αρχιτεκτονική IoT

Στη σύγχρονη εποχή, οι ηλεκτρονικοί υπολογιστές αλλά και οι υπολογιστικές δυνατότητες εφαρμόζονται σε συντριπτική πλειοψηφία στον βιομηχανικό τομέα. Το μοντέλο του διαδικτύου των πραγμάτων (IoT), διαχωρίζεται σε τέσσερα βασικά στρώματα, όπως αποτυπώνεται στο παρακάτω σχήμα, τα οποία αποτελούν:

- ✓ Στρώμα αισθητήρα (Sensor Layer).
- ✓ Στρώμα δικτύου (Network Layer).
- ✓ Στρώμα υπηρεσιών (Service Layer).
- ✓ Στρώμα εφαρμογής (Application Layer).

Εικόνα 2. Διαχωρισμός στρωμάτων (IoT)

Το στρώμα αισθητήρα εντοπίζεται στο κάτω μέρος στη διάταξη και αποτελείται από διάφορα είδη κόμβων και αισθητήρων, όπως για παράδειγμα είναι η συσκευή που χρησιμοποιεί ηλεκτρομαγνητικά πεδία με σκοπό τη μεταφορά των δεδομένων (RFID), καθώς και ετικέτες γραμμωτού κώδικα, ενεργοποιητές και έξυπνες συσκευές ανίχνευσης. Η χρήση των αισθητήρων αποσκοπεί στην ανίχνευση των αντικειμένων, αλλά και για τη μεταβίβαση των δεδομένων που ελήφθησαν στο επόμενο στρώμα. Η συλλογή των δεδομένων και η μεταφορά τους στο επίπεδο δικτύου με άμεσο ή έμμεσο τρόπο πραγματοποιείται διαμέσου των συσκευών (Παπαζώης, 2019).

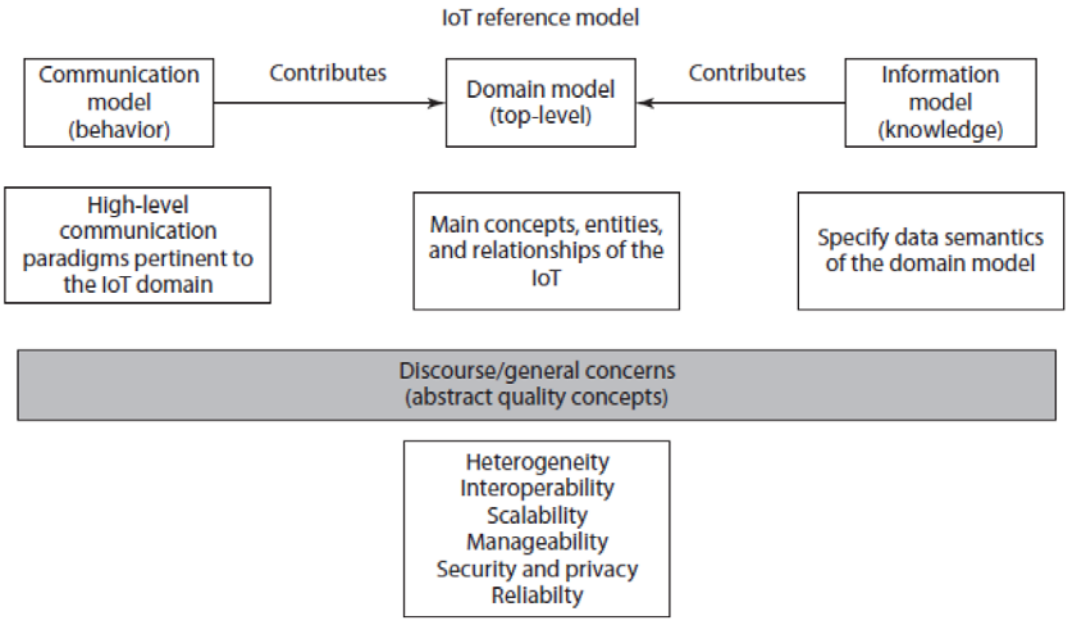
Προς την κατεύθυνση της ορθής αξιοποίησης της τεχνολογίας του Internet of Things (IoT) με στόχο την επίτευξη μεγαλύτερης απόδοσης της βιομηχανικής παραγωγής, αναπτύχθηκαν δύο πρότυπα για την αρχιτεκτονική των μοντέλων, εκ των οποίων το πρώτο αποτελεί το Industrial Internet Reference Architecture (IIRA) και το δεύτερο αντιστοιχεί στο Reference Architecture Model for Industries 4.0 (RAMI 4.0). Παράλληλα, η αρχιτεκτονική αναφοράς αισθητήρων δικτύου, διαθέτει μια γενική εικόνα τόσο των χαρακτηριστικών ενός δικτύου αισθητήρων, όσο και της οργάνωσης των στοιχείων τα οποία περιλαμβάνουν το συγκεκριμένο δίκτυο. Επιπρόσθετα, αναλύονται οι γενικές απαιτήσεις οι οποίες αναφέρονται στα δίκτυα των αισθητήρων, τα οποία έχουν σχέση με τα συστήματα του διαδικτύου των πραγμάτων, λόγω του γεγονότος πως αξιοποιούν τα δίκτυα αισθητήρων για τη συλλογή των δεδομένων.

Αξίζει να επισημανθεί πως έχει συσταθεί μία ερευνητική ομάδα από το διεθνή οργανισμό τυποποίησης - διεθνής ηλεκτροτεχνικής επιτροπής (ISO/IEC), σε συνεργασία με τον βιομηχανικό και εμπορικό κλάδο, την πολιτεία, αλλά και ακαδημαϊκών και ερευνητικών οργανισμών, με σκοπό την ανάπτυξη μιας αρχιτεκτονικής αναφοράς (IoT, RA-IoT Reference Architecture). Κύριο μέλημα αποτελεί η περιγραφή τόσο των χαρακτηριστικών και των πτυχών των συστημάτων του διαδικτύου των πραγμάτων, όσο και των συστημάτων RM που αναφέρονται σε Internet of Thinking συστήματα, καθώς και της διαλειτουργικότητας των φορέων του διαδικτύου. Ταυτόχρονα στις αρμοδιότητες της ερευνητικής ομάδας εντάσσεται ο καθορισμός των τομέων Internet of Thinking.

Η συνεργασία ανάμεσα σε βιομηχανικούς και πανεπιστημιακούς φορείς, απέφερε τη δημιουργία ενός αρχιτεκτονικού μοντέλου αναφοράς (ARM) για το διαδίκτυο των πραγμάτων, το οποίο ονομάστηκε IoT-A. Υπήρξε η πεποίθηση ανάμεσα στους φορείς πως η επίτευξη διαλειτουργικότητας ανάμεσα στα προϊόντα σε διάφορες πλατφόρμες θα είναι σε θέση να εξασφαλιστεί διαμέσου της διαλειτουργικότητας αποκλειστικά, σε επίπεδο επικοινωνίας και υπηρεσιών. Άξιο αναφοράς αποτελεί το γεγονός πως το IoT-A χρησιμοποιείται ως πρότυπο με στόχο την ανάπτυξη άλλων αρχιτεκτονικών, όπως το IoT RA. Όσον αφορά το μοντέλο ARM του IoT-A, δημιουργήθηκε για να είναι εφικτή η διαλειτουργικότητα ανάμεσα σε διάφορα συστήματα. Το μοντέλο ARM του Internet of Things αποτελείται από ένα RM και μια RA, ενώ προσδιορίζεται με σαφή και απλουστευμένο τρόπο, προκειμένου να είναι δυνατή η εφαρμογή του ως αναφορά για τη δημιουργία περίπλοκων αρχιτεκτονικών συστημάτων.

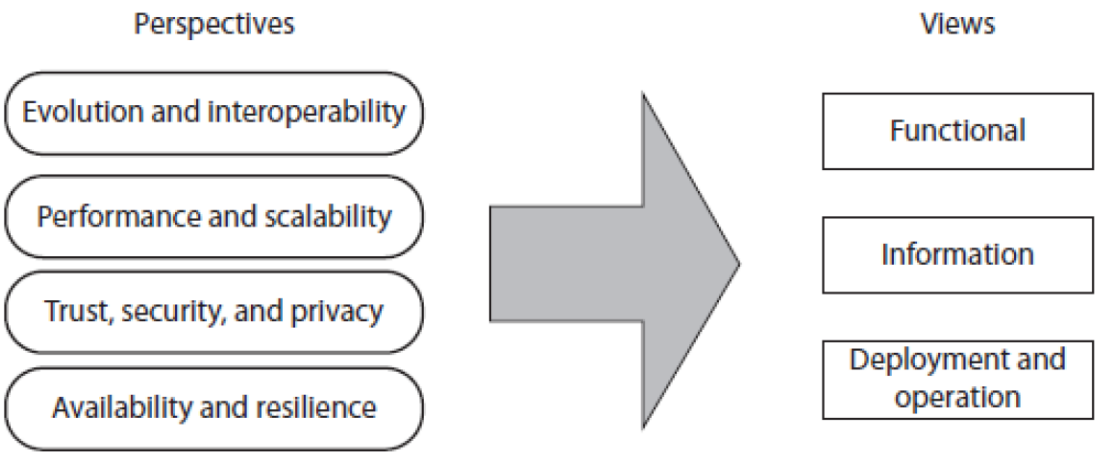
Στην εικόνα 3, αναπαρίσταται η περιγραφή του μοντέλου RM αναλυτικά, Το μοντέλο τομέα (Domain Model) προσδιορίζει μια ανώτατη περιγραφή των εννοιών και των οντοτήτων (φυσικές οντότητες, συσκευές, πόροι και υπηρεσίες) όπου αντιπροσωπεύουν ορισμένες πτυχές του τομέα του Internet of Things, ενώ ταυτόχρονα επιδρά καταλυτικά στις σχέσεις τους. Συνεπώς, είναι δυνατή η εφαρμογή του μοντέλου τομέα ως ταξινόμηση του διαδικτύου των πραγμάτων. Το μοντέλο πληροφοριών (Information Model), αναλύει τα χαρακτηριστικά των δεδομένων του μοντέλου τομέα και ειδικότερα περιγράφει τον τύπο των πληροφοριών, για τις οποίες είναι υπεύθυνες οι οντότητες. Το μοντέλο επικοινωνίας (Information Model) αναφέρεται στα κύρια πρωτόκολλα επικοινωνίας, όπου κρίνονται αναγκαία για τη σύνδεση των οντοτήτων, προκειμένου να εξασφαλιστεί η διαλειτουργικότητα ανάμεσα σε ετερογενή δίκτυα. Το

προτεινόμενο μοντέλο επικοινωνίας αποτελείται από ένα πλαίσιο επτά κατηγοριών και προσδιορίζει τον τρόπο διαχείρισης της επικοινωνίας της κατηγορίας σε ατομικό επίπεδο, με απώτερο στόχο την επίτευξη των χαρακτηριστικών διαλειτουργικότητας, τα οποία προβάλλουν ως προτεραιότητες στο διαδίκτυο των πραγμάτων. Παράλληλα, αναλύει τα επικοινωνούντα στοιχεία, καθώς και το κανάλι μετάδοσης για επικοινωνία στο σύστημα Internet of Things (Bassi et al., 2013).



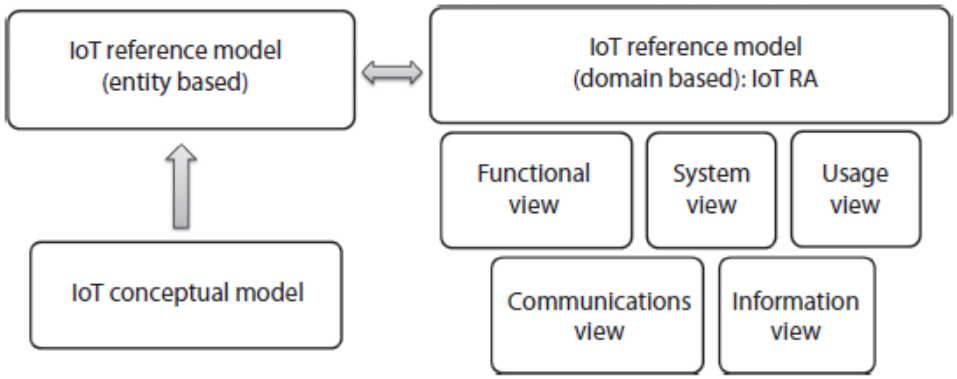
Εικόνα 3. Προτεινόμενο μοντέλο αναφοράς από την IoT-A.

Η RA του IoT-A σχηματίζεται βασικά από απόψεις (views) και προοπτικές (perspectives), όπου διαφοροποιούνται βάσει των απαιτήσεων των εφαρμογών σε ατομικό επίπεδο. Στην εικόνα 4, αποτυπώνεται η αλληλεπίδραση των προθέσεων και των προοπτικών. Στις προοπτικές "εξέλιξη και διαλειτουργικότητα", "απόδοση και κλιμάκωση", "εμπιστοσύνη, ασφάλεια και προστασία των προσωπικών δεδομένων" και "διαθεσιμότητα και ανθεκτικότητα", εφαρμόζονται συνολικά οι απόψεις: "λειτουργικότητα", "πληροφορία" και "ανάπτυξη και λειτουργία", αντίστοιχα. Αξίζει να επισημανθεί πως ο βαθμός και ο τρόπος επιρροής των απόψεων από τις προοπτικές δεν είναι ομοιογενής. Ένα παράδειγμα αποτελεί ο μεγαλύτερος βαθμός επιρροής, στην περίπτωση της εφαρμογής προοπτικών της άποψης “λειτουργία” (Bassi et al., 2013).



Εικόνα 4. Οι προοπτικές και οι προθέσεις της IoT-A.

Η IoT RA, που αναπτύχθηκε από τον διεθνή οργανισμό τυποποίησης - διεθνής ηλεκτροτεχνικής επιτροπής (ISO/IEC), προβλέπει τη δημιουργία ενός συστήματος IoT, το οποίο στηρίζεται σ' ένα γενικό εννοιολογικό πρότυπο IoT (CM), όπου εμπεριέχει τα βασικότερα χαρακτηριστικά και τους τομείς του Internet of Things. Ακολούθως εφαρμόζει ως πρότυπο το CM, με απώτερο στόχο την επίτευξη ενός υψηλού επιπέδου συστήματος βασισμένο σε RM. Το συγκεκριμένο μοντέλο αναφοράς, είναι δομημένο σε πέντε αρχιτεκτονικούς τομείς (λειτουργίας, συστήματος, χρήστη, πληροφοριών και επικοινωνιών) από διαφορετικές οπτικές γωνίες, οι οποίες συνθέτουν την RA.

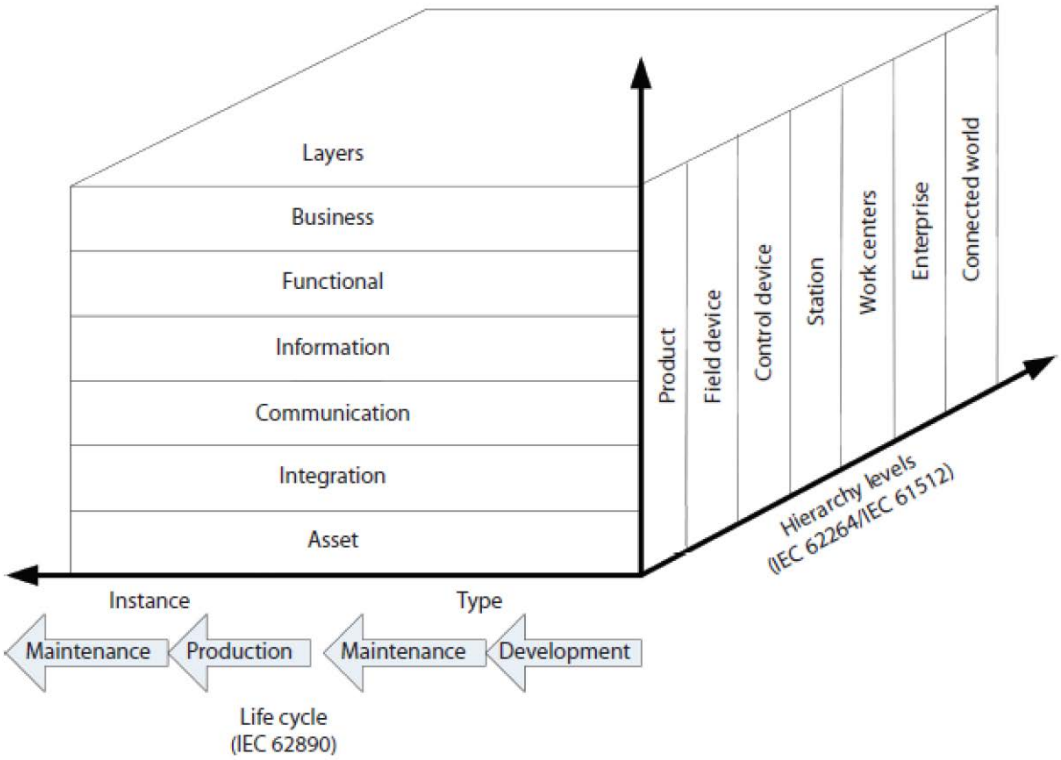


Εικόνα 5. Η σχέση ανάμεσα σε CM, RM, RA.

Παράλληλα, ένα άλλο μοντέλο αρχιτεκτονικής αποτελεί το RAMI 4.0, το οποίο εστιάζει στη βελτιστοποίηση της βιομηχανικής έρευνας και παραγωγής, καθώς και του

εφοδιασμού και των υπηρεσιών. Στο παρακάτω σχήμα, αναπαρίσταται το τρισδιάστατο μοντέλο αρχιτεκτονικής RAMI 4.0, όπου ο οριζόντιος άξονας αντιπροσωπεύει τον κύκλο ζωής των συστημάτων ή των προϊόντων, διαχωρίζοντας τον "τύπο" (type) από το "γεγονός" (instance). Ο τύπος αναφέρεται στον κύκλο ζωής ενός προϊόντος από την έναρξη μέχρι και την τελική διάθεση, διαμέσου του σχεδιασμού, της ανάπτυξης και της δοκιμής (Adolphs et al., 2015).

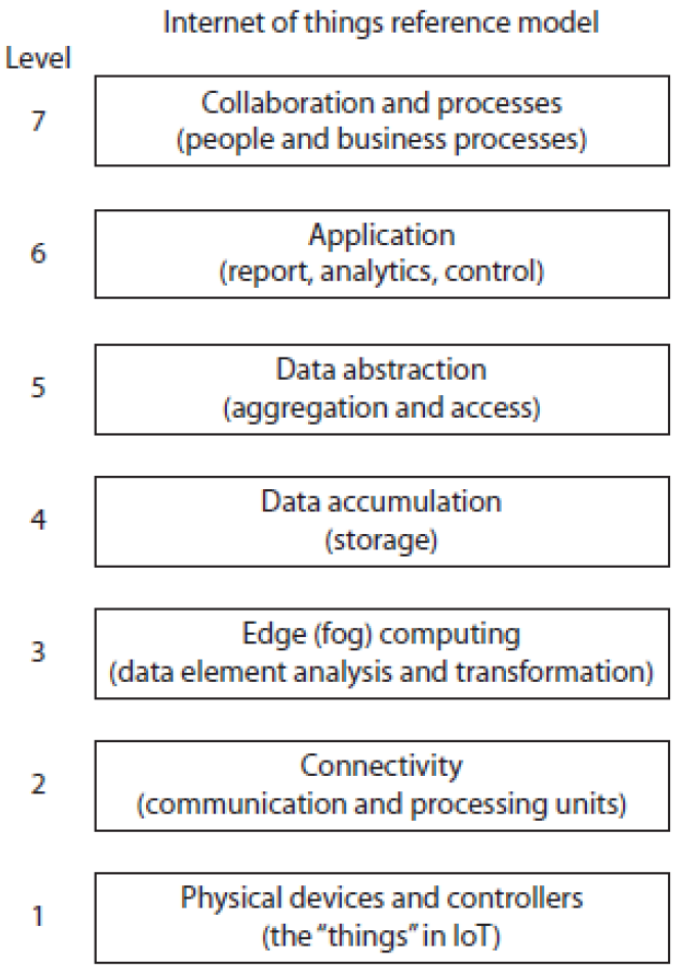
Από την άλλη πλευρά, το γεγονός αντιπροσωπεύει την παραγωγή ενός τύπου, με τον κύκλο ζωής του να διαπερνά από τα στάδια της κατασκευής, της πώλησης και της διάθεσης στον καταναλωτή, ώστε να εγκατασταθεί σε ένα ορισμένο σύστημα. Ο κάθετος άξονας περιλαμβάνει έξι στρώματα και αντιστοιχεί στην προοπτική του IT ενός τομέα του I4.0, γεγονός που σημαίνει πως διαχωρίζει σύνθετα έργα σε μικρότερα τμήματα, όπως επιχειρηματικές και λειτουργικές διαδικασίες, στοιχεία επικοινωνίας κ.λπ. Επιπρόσθετα, ο τρίτος άξονας αντιπροσωπεύει μια λειτουργική ιεραρχία, η οποία αντιστοιχεί στην ομαδοποίηση λειτουργιών και ευθυνών εντός των βιομηχανικών μονάδων. Περιέχει βασικές πτυχές του I4.0, όπως η συσκευή πεδίου και ελέγχου, ο σταθμός, οι μονάδες εργασίας και η εταιρεία.



Εικόνα 6. Το μοντέλο αρχιτεκτονικής RAMI 4.0.

Η Cisco πρότεινε ένα μοντέλο RM επτά επιπέδων, όπου τα τρία κατώτερα επίπεδα αντιστοιχούν σε λειτουργική τεχνολογία, ενώ τα επόμενα επίπεδα αφορούν την τεχνολογία πληροφοριών (IT). Το χαμηλότερο επίπεδο στην τεχνολογία πληροφοριών, αποτελεί η αποθήκευση και ακολούθως ανεβαίνοντας επίπεδα εντοπίζονται διαδοχικά οι εφαρμογές, οι διαδικασίες και οι εταιρικές συνεργασίες.

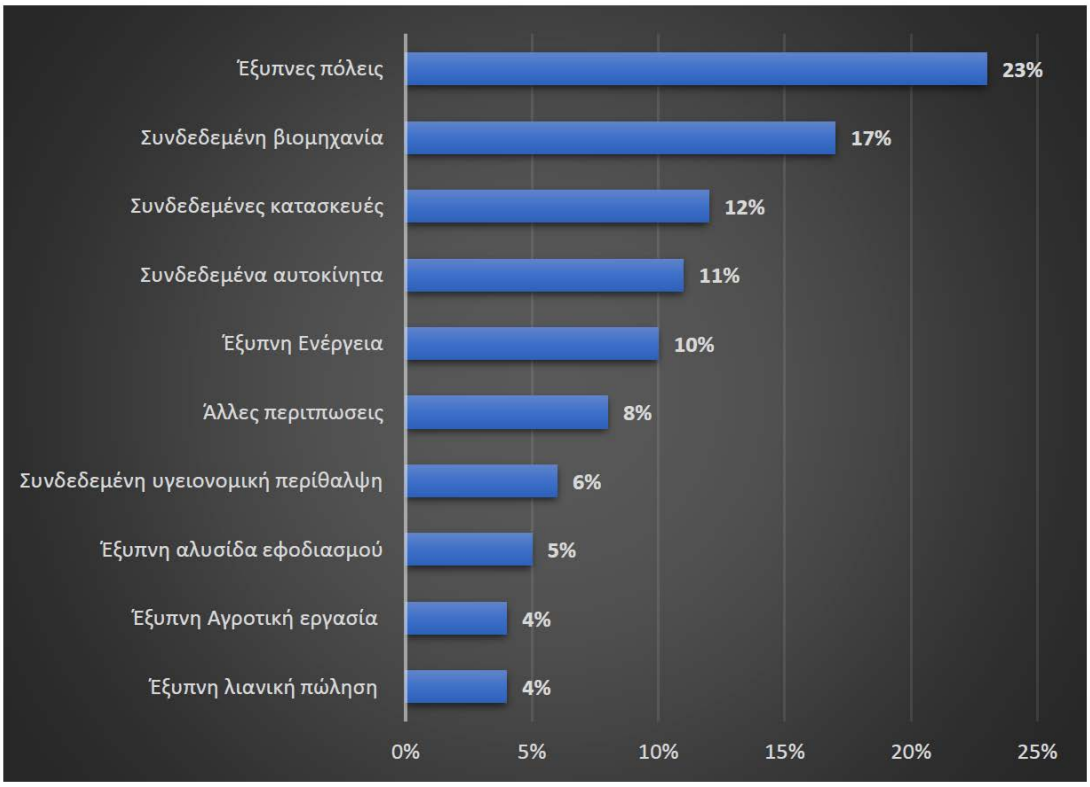
Το κατώτατο στρώμα περιλαμβάνει τις φυσικές συσκευές και τους ελεγκτές. Ανεβαίνοντας επίπεδο ακολουθεί η συνδεσιμότητα, και πιο πάνω εντοπίζεται το στρώμα στο οποίο είναι δυνατή η αρχική επεξεργασία των δεδομένων, όπως για παράδειγμα η συσσωμάτωση και η απαλοιφή της αλληλοεπικάλυψης. Στην εικόνα 7, αναπαρίσταται το προτεινόμενο μοντέλο της Cisco.



Εικόνα 7. Το μοντέλο IoT RM της Cisco.

2.3 Εφαρμογές IoT

Το διαδίκτυο των πραγμάτων (Internet of Things), βρίσκει αρκετές εφαρμογές, ενώ είναι δυνατό να αξιοποιηθεί αρκετά και στο μέλλον. Βάσει των στατιστικών δεδομένων, βρίσκει ευρεία εφαρμογή στις έξυπνες πόλεις, όπου η χρήση του αποσκοπεί στην επίλυση των δυσκολιών που αντιμετωπίζουν σε καθημερινή βάση οι κάτοικοι των μεγάλων αστικών κέντρων. Ωστόσο, το διαδίκτυο των πραγμάτων χρησιμοποιείται εκτεταμένα στον κλάδο της βιομηχανίας, των κατασκευών, της αυτοκινητοβιομηχανίας, αλλά και στον ενεργειακό και στον αγροτικό τομέα, όπως αποτυπώνεται στην παρακάτω εικόνα (Shanhong Liu, 2018).

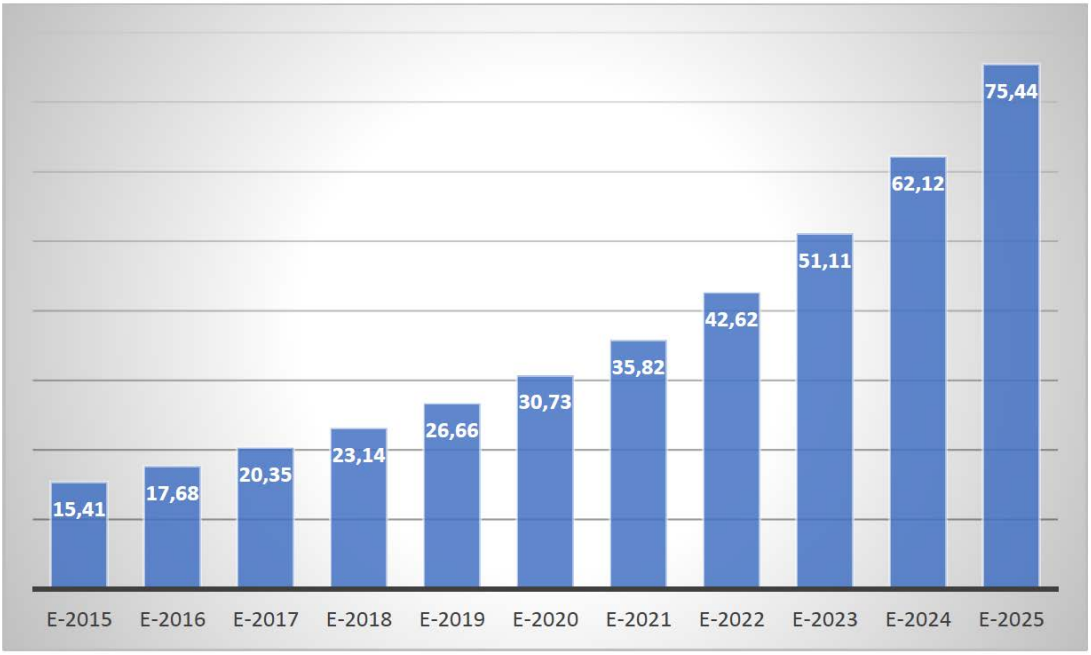


Εικόνα 8. Κατανομή των έργων του διαδικτύου των πραγμάτων (IoT) σε όλο τον κόσμο από τον Ιανουάριο του 2018, κατά τομέα.

Σε παγκόσμια κλίμακα το μεγαλύτερο ποσοστό των εφαρμογών των τεχνολογιών IoT, εντοπίζεται πάνω στις έξυπνες πόλεις. Πάντως, άξιο αναφοράς αποτελεί το γεγονός πως οι περισσότεροι τομείς όπου χρησιμοποιούν τη συγκεκριμένη τεχνολογία, έχουν

αλληλεπίδραση μεταξύ τους. Ένα παράδειγμα αποτελεί το γεγονός ότι η τεχνολογία IoT για την ενέργεια εξυπηρετεί ταυτόχρονα τις έξυπνες πόλεις και τη βιομηχανία (Statista Research Department, 2019).

Στην εικόνα 9, αποτυπώνονται τα στατιστικά δεδομένα, όπου διαπιστώνεται ο αριθμός των συνδεδεμένων συσκευών (Internet of Things), σε διεθνή κλίμακα, το χρονικό διάστημα από το 2015 έως το 2025. Η πρόβλεψη για το τρέχων ημερολογιακό έτος αποτελεί η αύξηση των συσκευών της τεχνολογίας IoT, κατά τριάντα ένα (31) δισεκατομμύρια σε διεθνές επίπεδο προσεγγιστικά.



Εικόνα 9. Συνδεδεμένες συσκευές IoT, όπου εγκαθίστανται σε παγκόσμιο επίπεδο από το 2015 έως το 2025, σε δισεκατομμύρια.

Η τεχνολογία Internet of Things, χρησιμοποιείται στα δικτυακά οχήματα, όπου στόχος αποτελεί η ευκολότερη και ασφαλέστερη μεταφορά των μόνιμων πολιτών και των τουριστών μιας πόλης. Η βασική ιδέα του Smart Mobility ή των έξυπνων μεταφορών θέτει ως σκοπό να ικανοποιήσει τρεις βασικές ανάγκες των πολιτών, όπου αποτελούν η ασφάλεια, η κινητικότητα και η άνεση. Όσον αφορά το ζήτημα της ασφάλειας συμπεριλαμβάνεται η ασφάλεια των δικτύων, της επικοινωνίας ανάμεσα στα οχήματα, αλλά και της επικοινωνίας του οχήματος με την υποδομή. Οι έξυπνοι αισθητήρες θα

παρέχουν μετακινήσεις των οχημάτων, όπου το χαρακτηριστικό τους θ' αποτελεί η φιλικότητα προς το περιβάλλον. Επιπρόσθετα, τα έξυπνα οχήματα θα έχουν τη δυνατότητα της αυτόματης παρακολούθησης και της αναγνώρισης των κρίσιμων σφαλμάτων του συστήματος, ενώ θα διαθέτουν σήμανση αναγνώρισης της επικινδυνότητας των οδών κυκλοφορίας (NIST, 2013).

Η εφαρμογή της τεχνολογίας IoT στα έξυπνα σπίτια, εστιάζεται στην άνεση, την ποιοτικότερη διαβίωση και την παρακολούθηση του περιβάλλοντος. Διαμέσου της εφαρμογής smart home, θα παρέχεται η δυνατότητα να μεταβάλλουν και να ελέγχουν περιβαλλοντικά δεδομένα εντός του σπιτιού, όπως η θερμοκρασία, ο φωτισμός και η υγρασία. Τα άτομα θα είναι σε θέση να μεταβάλλουν τις λεπτομέρειες της εφαρμογής smart home, διαμέσου μίας ηλεκτρονικής συσκευής, όπως είναι ο φορητός ή ο επιτραπέζιος υπολογιστής (NIST, 2013).

Εικόνα 10. Τεχνολογία smart home, για έξυπνα οικιακά σπίτια.

Οι συσκευές τεχνολογίας Internet of Things (IoT), έχουν τη δυνατότητα ελέγχου ανθρώπων που βρίσκονται σε μακρινή απόσταση από τα κέντρα υγειονομικής περίθαλψης. Ορισμένες συσκευές, όπως τα έξυπνα ρολόγια, ή οι έξυπνες συσκευές τόσο της υγειονομικής περίθαλψης, όσο και της παρακολούθησης της φυσικής κατάστασης παρέχουν τη δυνατότητα λήψης δεδομένων από τους αισθητήρες. Προϋπόθεση για την εφαρμογή των έξυπνων συσκευών στον τομέα της υγείας αποτελούν να διαθέτουν χαρακτηριστικά, όπως για παράδειγμα η χαμηλή ισχύς, η εξαιρετική αντοχή, η ακρίβεια, η αξιοπιστία, καθώς και η ασφάλεια για την προστασία του ιδιωτικού απόρρητου. (Vermesan & Friess, 2013).

Εικόνα 11. Τεχνολογία IOT, με εφαρμογή στον τομέα της υγείας.

2.4 Η τεχνολογία Internet of Things (IoT)

Το Διαδίκτυο των πραγμάτων (Internet of Things) παράγει, αποθηκεύει και κατευθύνει δεδομένα με αδιάκοπο ρυθμό. Η ροή των δεδομένων αποτελεί ένα συντελεστή ο οποίος κατέχει σημαντική θέση στην ανάπτυξη των αρχιτεκτονικών πληροφοριών, καθώς και των εφαρμογών λογισμικού. Η ταχεία αύξηση της ζήτησης για τη σύνδεση των συσκευών με το διαδίκτυο, δημιουργεί διαρκώς μεγάλες απαιτήσεις ως προς τη συλλογή, την αποθήκευση και τη διαχείριση των δεδομένων. Επομένως, κρίνεται αναγκαία η αναζήτηση και εύρεση λύσεων ως προς την ανάπτυξη εφαρμογών και

υπηρεσιών, ώστε να είναι εφικτή η ορθή διαχείριση και ταχεία ροή των δεδομένων, με απώτερο στόχο να βελτιωθεί σε ικανοποιητικό βαθμό η ικανότητα της λήψης των αποφάσεων και της πρόβλεψης.

Άξιο αναφοράς αποτελεί το γεγονός της ευκολίας της επεξεργασίας και της αυξημένης διαθεσιμότητας των δεδομένων του διαδικτύου των πραγμάτων, σε συνδυασμό με τη διαχείριση τους, βάσει μεταφοράς πακέτων. Απαραίτητη προϋπόθεση να καταστεί εφικτή η αυτόματη ροή των δεδομένων σε πραγματικό χρόνο, αποτελεί η ικανότητα διαρκούς ροής στις υποδομές τους. Όσον αφορά τις ροές των δεδομένων σε πραγματικό χρόνο, διαφέρουν ως προς την ευαισθησία στο χρόνο, το μέγεθος της χωρητικότητας, αλλά και τη μακροπρόθεσμη αξία αφού επεξεργαστούν, σε σύγκριση με τις παραδοσιακές ροές, όπου το χαρακτηριστικό τους αποτελεί η φόρτωση των δεδομένων σε προγραμματισμένη βάση. Αρκετές περιοχές δεδομένων μιας εταιρείας, συμπεριλαμβανομένων των μονάδων της όπου διαμοιράζονται τα δεδομένα με την εφαρμογή των αισθητήρων, ή των συστημάτων υπολογιστών ή τα κοινωνικά δίκτυα, αποτελούν πιθανές πηγές της ροής τους σε πραγματικό χρόνο (Kale, 2018).

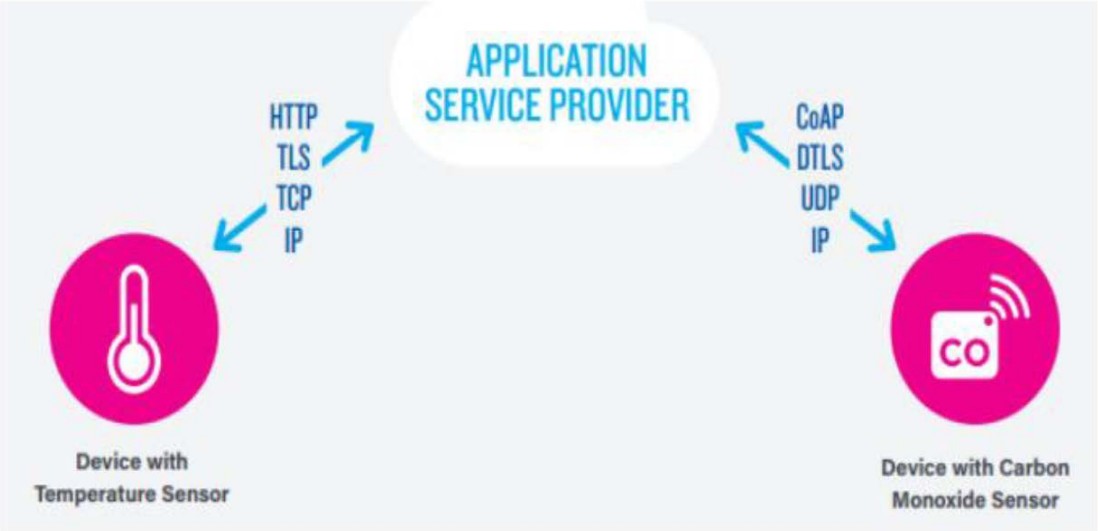
Το συμβούλιο αρχιτεκτονικής του διαδικτύου, δημοσίευσε ένα πρότυπο οδηγό σχετικά με τη διασύνδεση των έξυπνων συσκευών, όπου εμπεριέχει το γενικό πλαίσιο της αρχιτεκτονικής μοντέλων επικοινωνίας, το οποίο εφαρμόζεται στις συσκευές Internet of Things. Αναλυτικά, τα κύρια χαρακτηριστικά του κάθε μοντέλου περιγράφονται και διακρίνονται τέσσερις υποκατηγορίες.

Α. Μοντέλο Device-to-Device. Το συγκεκριμένο μοντέλο αφορά στην άμεση σύνδεση και επικοινωνία μεταξύ δύο συσκευών, δίχως την παρέμβαση ενός ενδιάμεσου διακομιστή εφαρμογών (Server). Αξιοποιούν ορισμένα πρωτόκολλα, όπως για παράδειγμα το Bluetooth. Η επικοινωνία των συσκευών επιτυγχάνεται διαμέσου αρκετών τύπων IP δικτύων ή το διαδίκτυο. Τα δίκτυα επικοινωνίας Device-to-Device ακολουθούν συγκεκριμένα πρωτόκολλα, ενώ απαραίτητη προϋπόθεση για την καλή λειτουργία τους, αποτελεί η ανταλλαγή μηνυμάτων. Το μοντέλο Device-to-Device αξιοποιείται βασικά σε χρήσεις οικιακού αυτοματισμού, όπου χαρακτηριστικό αποτελεί ο αργός ρυθμός μετάδοσης των δεδομένων. Ορισμένα παραδείγματα συσκευών αποτελούν οι λαμπτήρες και οι θερμοστάτες. Η άμεση σχέση επικοινωνίας τους παρέχει τη δυνατότητα όχι μόνο να διαθέτουν ενσωματωμένους μηχανισμούς ασφάλειας και

πιστοποίησης στοιχείων, αλλά και να αξιοποιούν τα μοντέλα δεδομένων, στενά συνδεδεμένα με την οικογένεια των συσκευών (Tschofenig et. al., 2015).

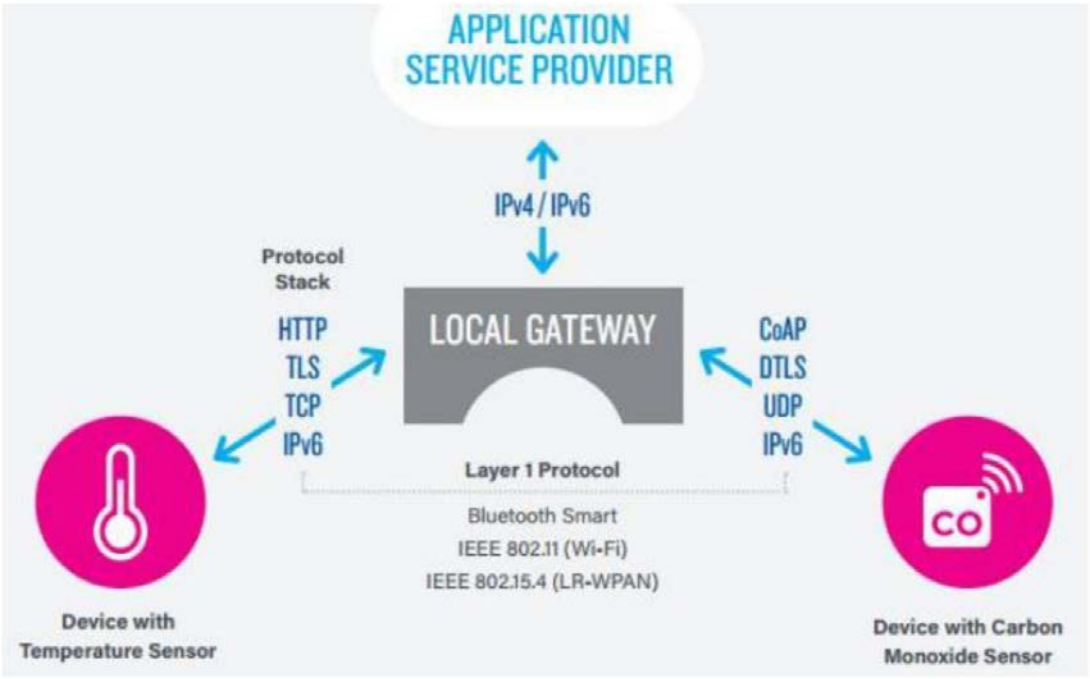
Εικόνα 12. Μοντέλο επικοινωνίας Device-to-Device

Β. Μοντέλο Device-to-Cloud. Παρέχει τη δυνατότητα της σύνδεσης των συσκευών Internet of Things, διαμέσου μιας διαδικτυακής υπηρεσίας Cloud. Η συγκεκριμένη υπηρεσία έχει εποπτικό ρόλο στην ανταλλαγή των δεδομένων, καθώς και της ροής των μηνυμάτων. Γενικότερα, αξιοποιούνται ορισμένα πρωτόκολλα επικοινωνίας, όπως το wi-fi, προκειμένου να εγκαταστήσει μία σύνδεση ανάμεσα στη συσκευή και του IP δικτύου, το οποίο συνδέεται ακολούθως με την Cloud υπηρεσία. Ένα παράδειγμα εφαρμογής Internet of Things, αποτελεί η Smart TV. Η συγκεκριμένη συσκευή αξιοποιεί μα διαδικτυακή σύνδεση, με σκοπό τη μεταβίβαση πληροφοριών, καθώς και την ενεργοποίηση διαδραστικών εφαρμογών, όπως για παράδειγμα η αναγνώριση ομιλίας.



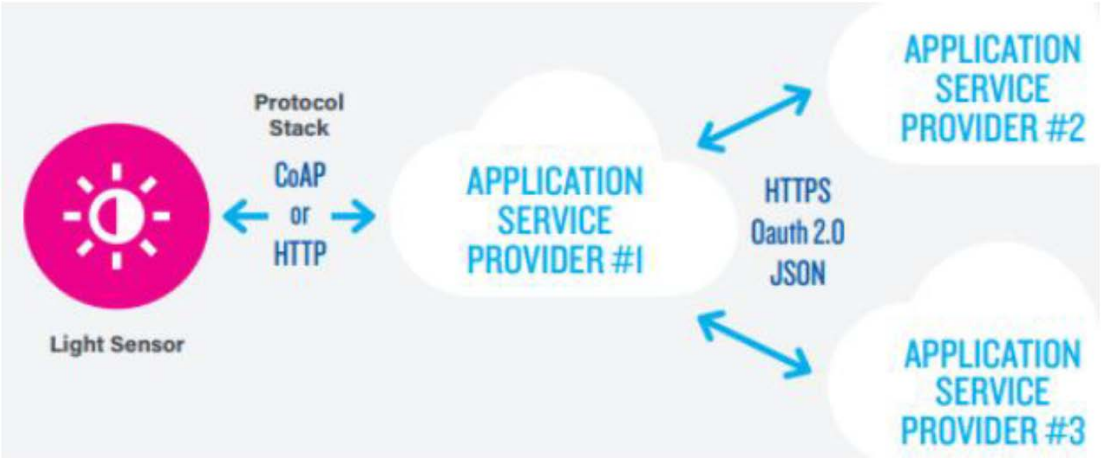
Εικόνα 13: Μοντέλο επικοινωνίας Device-to-Cloud

Γ. Μοντέλο Device-to-Gateway. Οι συσκευές Internet of Things, συνδέονται σε μια ενδιάμεση συσκευή, ώστε να έχουν τη δυνατότητα πρόσβασης σε μια Cloud υπηρεσία. Συνήθως, εμπεριέχει το λογισμικό της εφαρμογής που τρέχει σε μια τοπική πύλη, όπου έχει το ρόλο του ενδιάμεσου, ανάμεσα στις συσκευές και της Cloud υπηρεσίας. Η συγκεκριμένη πύλη-συσκευή διαθέτει την ικανότητα διαφόρων λειτουργιών, όπως της παροχής ασφάλειας, καθώς και της μετάφρασης δεδομένων και των πρωτοκόλλων. Παράλληλα, η εφαρμογή του μοντέλου δίνει τη δυνατότητα εισαγωγής νέων έξυπνων συσκευών, σε μία ήδη υπάρχουσα τοπική πύλη δικτύου, με συνέπεια να επιμηκύνονται οι εφαρμογές του διαδικτύου των πραγμάτων (Duffy Marsan, 2015).



Εικόνα 14. Μοντέλο επικοινωνίας Device-to-Gateway

Δ. Μοντέλο Back-End Data Sharing. Το συγκεκριμένο μοντέλο επικοινωνίας έχει ως κύρια λειτουργία την επιμήκυνση της Device-to-Cloud επικοινωνίας, προκειμένου να υπάρχει η δυνατότητα διαχείρισης των δεδομένων αποκλειστικά για έναν πάροχο υπηρεσιών εφαρμογής, διαμέσου των συσκευών Internet of Things. Οι χρήστες είναι σε θέση να εξάγουν και να διαχειρίζονται δεδομένα έξυπνων αντικειμένων διαμέσου μιας Cloud υπηρεσίας, σε συνδυασμό με δεδομένα από άλλες πηγές (Kulkarni & Kulkarni, 2017).



Εικόνα 15. Μοντέλο επικοινωνίας Backend-Data-Sharing

Κεφάλαιο 3

Ασφάλεια στο Διαδίκτυο των πραγμάτων

Η αύξηση του αριθμού των συσκευών Internet of Things, εγείρει ερωτήματα όσον αφορά την ασφάλεια και την προστασία των προσωπικών δεδομένων, ενώ διαπιστώνεται περισσότερη ανησυχία στην περίπτωση λειτουργίας τους σε κινητές συσκευές (Jayaraman et al., 2017) .

Παράλληλα, τα στοιχεία της ανάλυσης στο τέλος της συσκευής παράγουν ευαίσθητες πληροφορίες, εφόσον έχει διεκπεραιωθεί η επεξεργασία των ακατέργαστων ροών δεδομένων. Πάντως, τα στοιχεία ασφαλείας πέμπτου επιπέδου παρέχουν τη δυνατότητα ασφαλούς μεταβίβασης των ροών των δεδομένων τόσο σε συσκευές Internet of Things, όσο και ανάμεσα σε συσκευές Internet of Things και Cloud Data Centers (Daghighi et al., 2015).

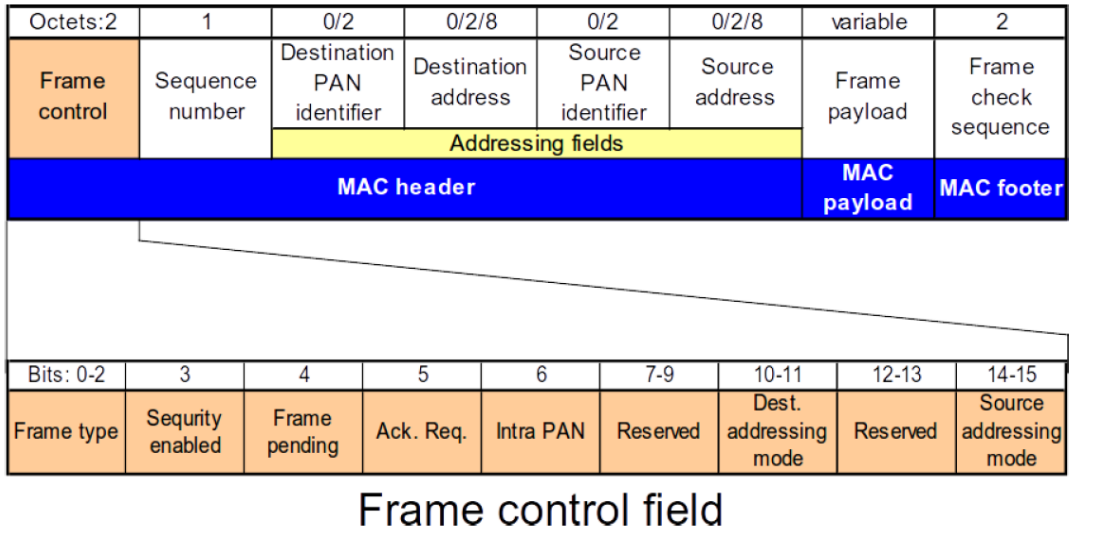
Αξίζει να επισημανθεί πως κρίνεται ιδιαίτερα σημαντικό ζήτημα η διαφύλαξη της ιδιωτικής ζωής, εξαιτίας της ευαισθησίας των προσωπικών δεδομένων και των device-centric δεδομένων. Στην αντίθετη περίπτωση όπου δε θα συμβεί και θα διαπιστωθεί διαρροή των δεδομένων, ακόμα και σε μικρό βαθμό, ελλοχεύει ο κίνδυνος εμφάνισης δυσμενών επιπτώσεων. Τα στοιχεία προστασίας των δεδομένων στο συγκεκριμένο επίπεδο καθίστανται αναγκαία με σκοπό τη διασφάλιση της ιδιωτικότητας, παρέχοντας την ικανότητα στους αλγόριθμους να προστατεύουν τα δεδομένα και ταυτόχρονα να εισάγουν τα στοιχεία ανωνυμίας. Ωστόσο, για την επίτευξη του παραπάνω σκοπού προβάλλει αναγκαία η προσβασιμότητά τους στο πέμπτο επίπεδο.

3.1 Προβλήματα και επιθέσεις ασφάλειας

Σημεία αναφοράς αποτελεί το πρώτο επίπεδο του OSI, το Physical Layer στο ZigBee. Στην περίπτωση του IEEE 802.15.4, αποτελεί το μικροκυματικό φάσμα των 868.0–868.6 MHz για την Ευρώπη, χωρισμένο σε ένα κανάλι, ενώ για τη Βόρεια Αμερική αντιστοιχεί σε 902–930 MHz, χωρισμένο σε 10 κανάλια. Όσον αφορά σε παγκόσμιο επίπεδο αντιστοιχεί σε 2400–2483.5 MHz, χωρισμένο σε 16 κανάλια (Hsing Yen & Ting Tsai, 2010).

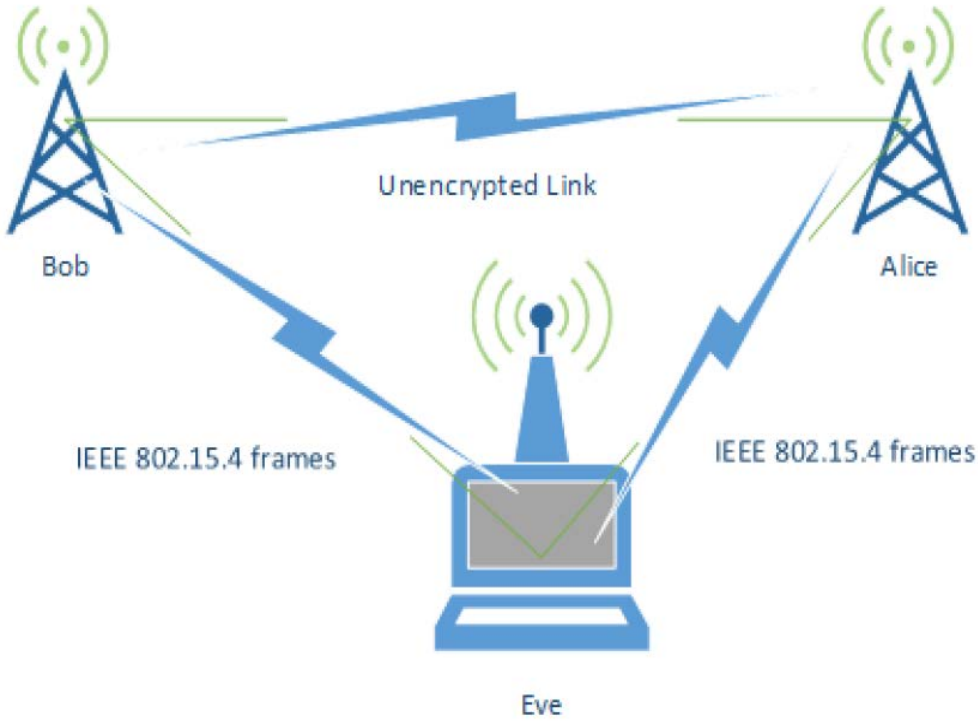
I. ΦΥΣΙΚΟ ΕΠΙΠΕΔΟ ΚΑΙ ΕΠΙΠΕΔΟ ΖΕΥΞΗΣ ΔΕΔΟΜΕΝΩΝ (IEEE 802.15.4)

Οι επιθέσεις που είναι σε θέση να πραγματοποιηθούν στο επίπεδο του Physical Layer, αντιστοιχούν σε καθαρά επιθέσεις ωτακουστή με συσκευές οι οποίες λειτουργούν στο ίδιο φάσμα με τις συσκευές στόχους. Ουσιαστικά, εφόσον ο χρήστης διαθέτει μία συσκευή όπου είναι σε θέση να εκπέμψει και να λάβει σήματα στο ίδιο φάσμα στο οποίο επικοινωνούν οι στόχοι, τότε ελλοχεύει ο κίνδυνος υποκλοπής των σημάτων, εφόσον εντοπίζεται στο βεληνεκές των στόχων. Ακολούθως, υπάρχει το επίπεδο Ζεύξης Δεδομένων το οποίο στα πλαίσια του IEEE 802.15.4, αναφέρεται ως MAC (Media Access Control) Layer. Στα όρια του συγκεκριμένου στρώματος διαπιστώνεται η διαμόρφωση των πλαισίων, όπου ανταλλάσσονται μεταξύ δύο IEEE 802.15.4 κόμβους οι οποίοι επικοινωνούν μεταξύ τους. Στην εικόνα 16, αναπαρίσταται η μορφή ενός πλαισίου IEEE 802.15.4 (Gutierrez et al., 2001).

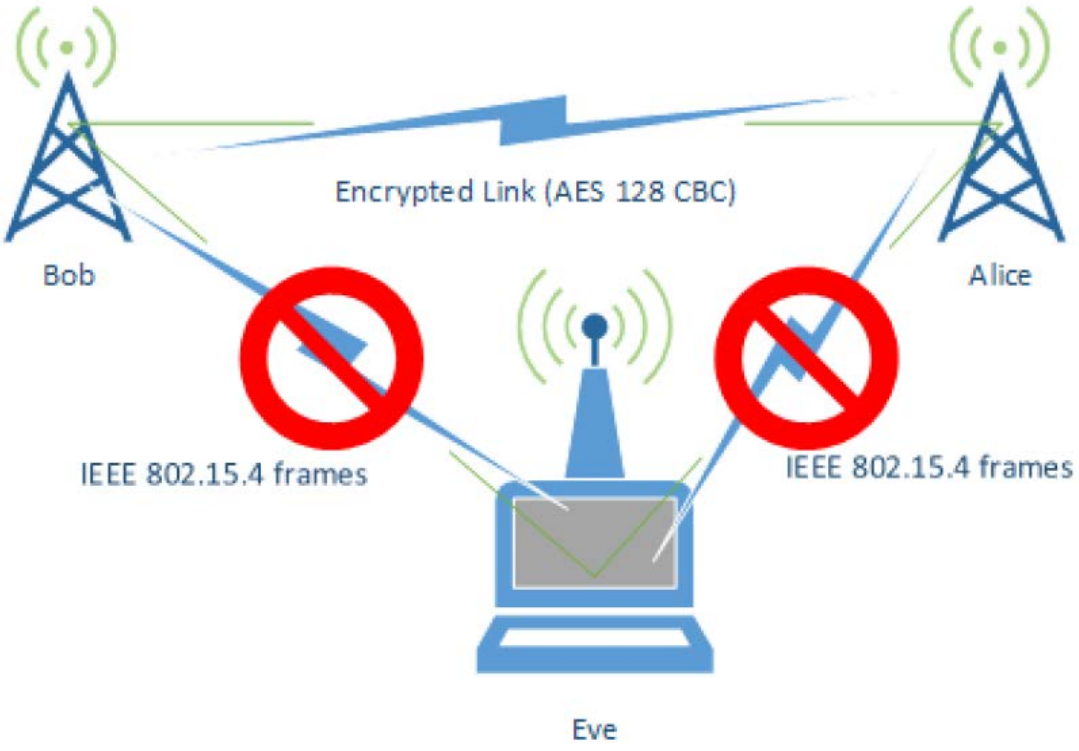


Εικόνα 16. IEEE 802.15.4 MAC layer frame

Οι επιθέσεις ωτακουστή ή Man-in-the-Middle attack αναπαρίστανται στις εικόνες 17, 18, όπου ο επιτιθέμενος (Eve) εντοπίζεται εντός του βεληνεκούς της ασύρματης επικοινωνίας των κανονικών κόμβων IEEE 802.15.4. Αν οι κόμβοι δεν αξιοποιούν μία ορισμένη κρυπτογράφηση κατά την επικοινωνία, επακόλουθο είναι ο επιτιθέμενος να είναι σε θέση να «υποκλέψει» καταγράφοντας τα IEEE 802.15.4 πλαίσια, δίχως ιδιαίτερη δυσκολία. Παράλληλα, είναι πιθανό να υλοποιήσει μια Man-in-the-Middle επίθεση αλλάζοντας την MAC διεύθυνση του, στην αντίστοιχη του κόμβου 1, όταν έρχεται σε επαφή με τον κόμβο 2 και αντίστροφα.



Εικόνα 17. Αναπαράσταση επίθεσης σε κόμβους

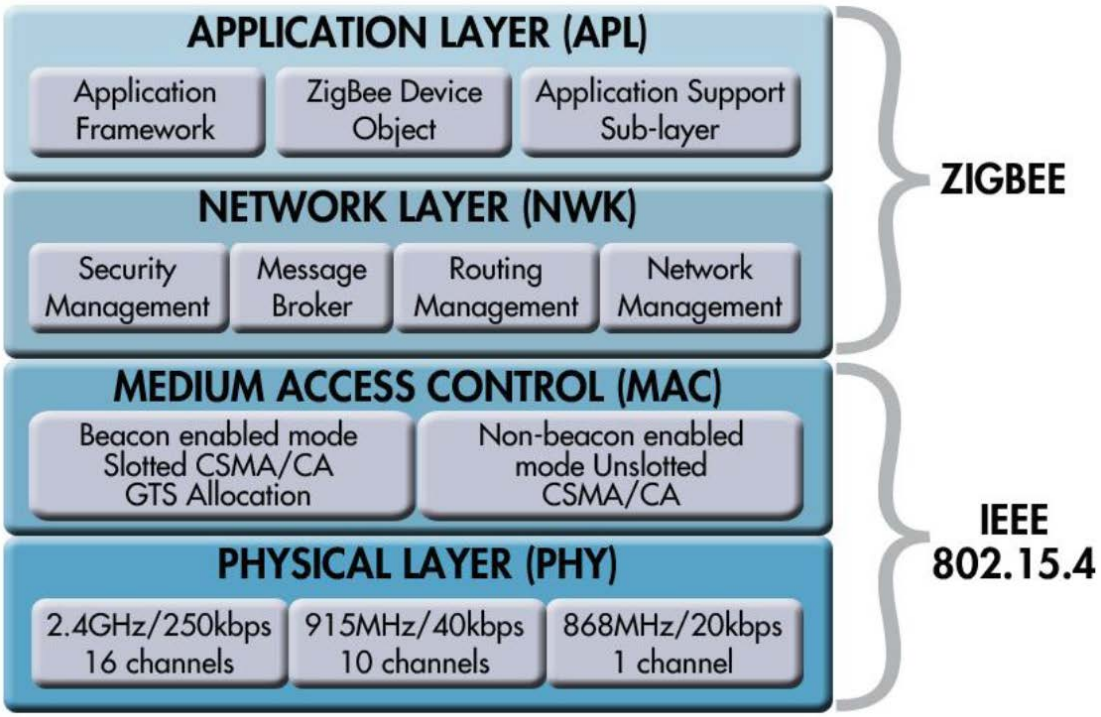


Εικόνα 18. Μπλοκάρισμα επίθεσης στους κόμβους

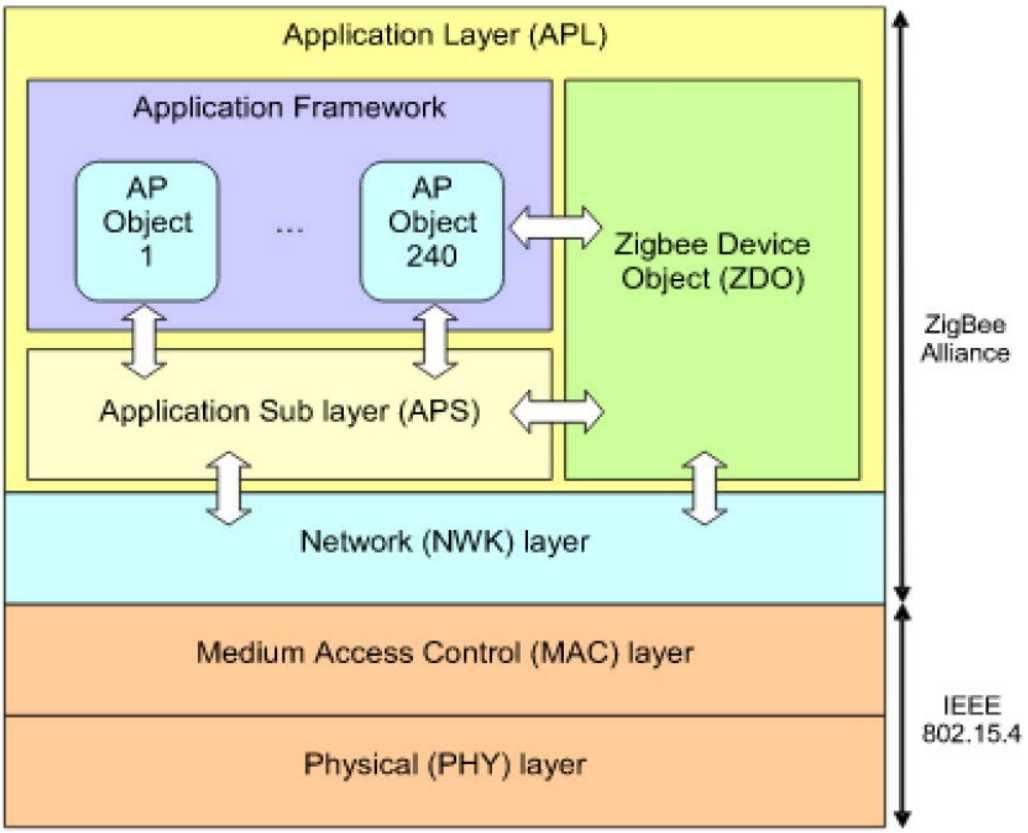
II. ΕΠΙΠΕΔΟ ΔΙΚΤΥΟΥ (ZigBee)

Αξίζει να επισημανθεί πως το επίπεδο δικτύου, δεν καθορίζεται σαφώς από το πρότυπο IEEE 802.15.4, ωστόσο υλοποιείται ορισμένη μορφή του επιπέδου δικτύου. Στην περίπτωση όπου χρησιμοποιούνται μονάδες ZigBee της Digi, όπου τις αναφέρει ως XBee, υλοποιείται ένα επίπεδο δικτύου. Στις παρακάτω εικόνες δίνεται η δυνατότητα παρατήρησης της διαστρωμάτωσης του ZigBee και IEEE 802.15.4 των επιπέδων του OSI, ενώ ταυτόχρονα διαπιστώνεται το σημείο παύσης του προτύπου IEEE 802.15.4 και το σημείο έναρξης του τεχνολογικού προτύπου του ZigBee (Baronti et al., 2006).

Διαπιστώνεται πως το ZigBee εισάγει ένα επίπεδο δικτύου πάνω από το IEEE 802.15.4 MAC επίπεδο, το οποίο φέρει την ευθύνη για τη διαχείριση του δικτύου, τον τρόπο επικοινωνίας των επιμέρους δικτύων, την ανάπτυξη μεγαλύτερων δικτύων (routing), καθώς και τη μεταβίβαση και την ασφάλεια των μηνυμάτων ανωτέρων επιπέδων.



Εικόνα 19. IEEE 802.15.4 και επίπεδα στοίβας δικτύου ZigBee

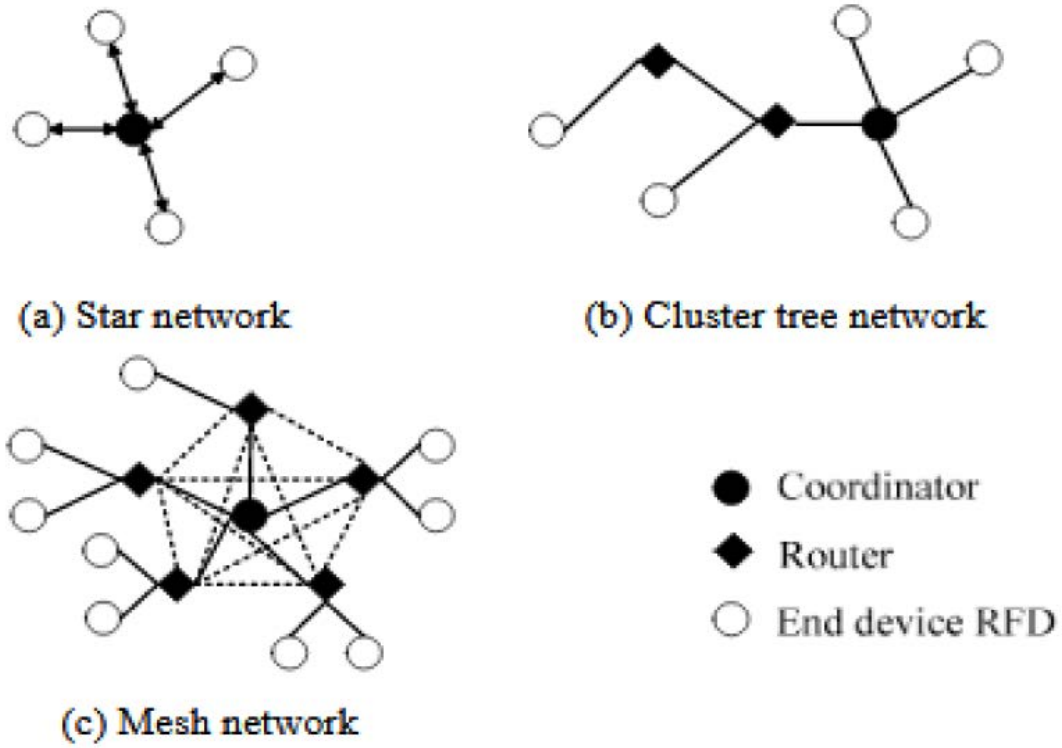


Εικόνα 20. Αρχιτεκτονική διαστρωμάτωση ZigBee

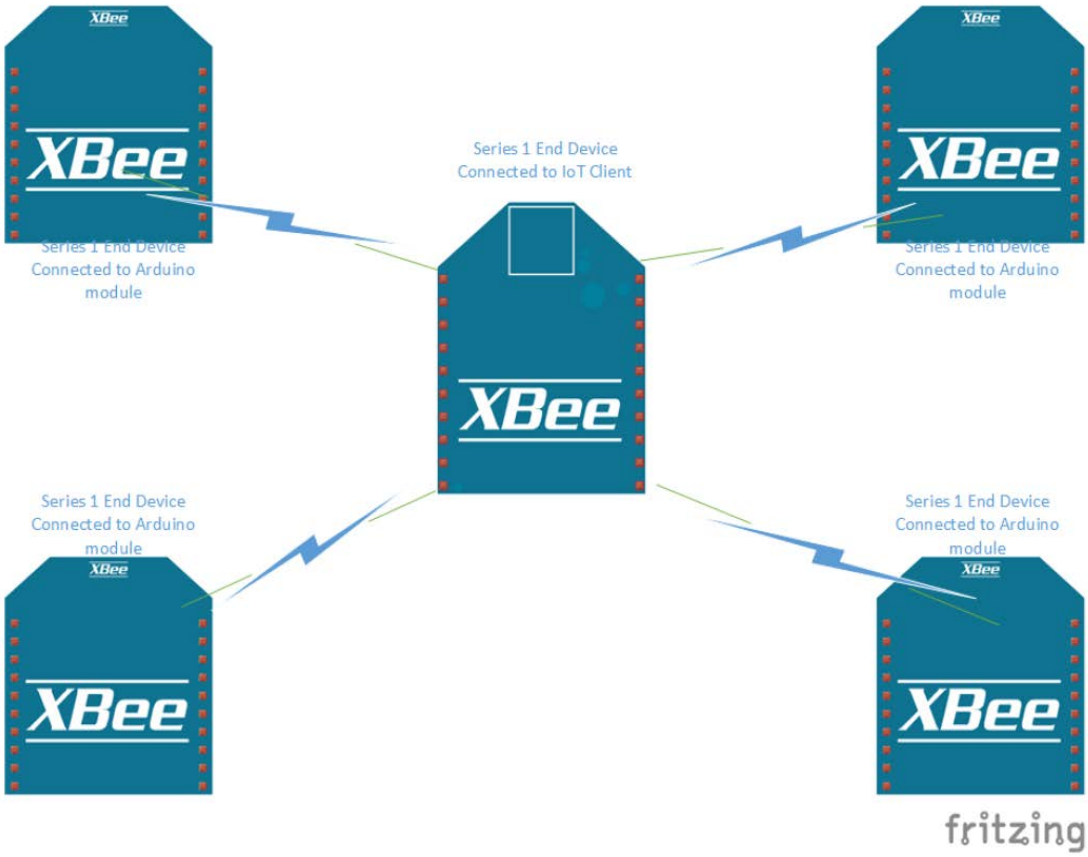
Σχετικά με την τοπολογία Δικτύου ZigBee, ταξινομούνται σε τέσσερις κατηγορίες, όπως αναπαρίστανται στο παρακάτω σχήμα. Οι κατηγορίες αποτελούν:

- Αστέρα (Star).
- Αδόμητη (Mesh).
- Δένδρο Συστάδων (Cluster Tree).
- Ζεύγος (Pair).

Στην περίπτωση του αστέρα υπάρχει ένας κεντρικός συντονιστής (Coordinator) και διάφορες τελικές συσκευές (End Devices) στην περιφέρεια του. Υπάρχει η δυνατότητα επικοινωνίας όλων των συσκευών διαμέσου του συντονιστή. Στην περίπτωση της αδόμητης τοπολογίας, υπάρχει μια ασαφής δομή, όπου σε ορισμένο σημείο στο κέντρο, εντοπίζεται ο συντονιστής, ο οποίος περιφέρεται από τελικές συσκευές και δρομολογητές (routers) που συνδέονται μεταξύ τους. Παρόμοια στη δομή του δέντρου συστάδων, εντοπίζεται ένας κεντρικός συντονιστής σαν ρίζα του δέντρου, και επιμέρους κλαδιά που βασίζονται σε routers, ενώ τα φύλλα αποτελούν οι τελικές συσκευές. Όσον αφορά το ζεύγος, υπάρχει ο κεντρικός συντονιστής σε συνδυασμό με ένα router ή μία τελική συσκευή (Jianpo et al., 2010).



Εικόνα 21. Τοπολογία δικτύου ZigBee



Εικόνα 22. Τοπολογία δικτύου αστέρα ZigBee

Οι επιθέσεις που είναι δυνατό να παρουσιαστούν στο επίπεδο δικτύου είναι πολλαπλές. Ένα παράδειγμα αποτελεί η υποκλοπή δεδομένων από χρήστη, ο οποίος είχε υποδυθεί το συντονιστή, ανάμεσα στη σύνδεση των τελικών συσκευών και των δρομολογητών. Ένα άλλο παράδειγμα ενδεχόμενης επίθεσης αποτελεί η σύνδεση ενός κακόβουλου χρήστη σ' ένα δίκτυο ZigBee, υποδυόμενος είτε τον δρομολογητή (router) προκειμένου να αναμεταδίδει δεδομένα, πιθανώς αλλοιώνοντας τα, είτε την τελική συσκευή μεταβιβάζοντας λανθασμένα δεδομένα.

III. ΕΥΠΑΘΕΙΣ ΕΦΑΡΜΟΓΕΣ

Στις επιθέσεις πρέπει να λαμβάνονται υπόψη οι εφαρμογές του διαδικτύου των πραγμάτων και ποιες επιπτώσεις επιφέρει μία ενέργεια η οποία θα παραβιάσει ευαίσθητες πληροφορίες. Ένα παράδειγμα αποτελεί μία Internet of Things εφαρμογή υγείας (e-health), όπου χρησιμοποιούνται ασύρματοι κόμβοι (wireless nodes), οι οποίοι υλοποιούν το IEEE 802.15.4/ZigBee stack. Δυστυχώς, ένας χρήστης είναι σε θέση να

υποκλέψει προσωπικά ιατρικά δεδομένα, διαμέσου ενός κόμβου ZigBee σε ορισμένο κεντρικό σύστημα που είναι συνδεδεμένος επάνω του ο συντονιστής. Έτσι για παράδειγμα, είναι σε θέση να υποκλέψει ιατρικά δεδομένα που αποστέλνονται από έναν αισθητήρα, για τη μέτρηση του επιπέδου του σακχάρου σε παθόντα.

Σε άλλο παράδειγμα αναφέρεται η περίπτωση της επίθεσης στο σύστημα smart IoT λαμπτήρων "Hue" της εταιρείας Philips. Στην συγκεκριμένη περίπτωση, η Smart Hub λύση της Philips που χρησιμοποιούσε μη κρυπτογραφημένη επικοινωνία ανάμεσα σε Series 1 XBee με ενεργοποιημένο το Over-The-Air (OTG) Update ήταν επιρρεπής σε εξαναγκασμένη αναβάθμιση του δικτύου με μολυσμένο firmware, το οποίο έδινε εντολή στους κόμβους να βρίσκονται υπό τον έλεγχο του επιτιθέμενου, δίχως την ικανότητα επανορθωτικής ενέργειας (Ανδριτσάκης, 2018).

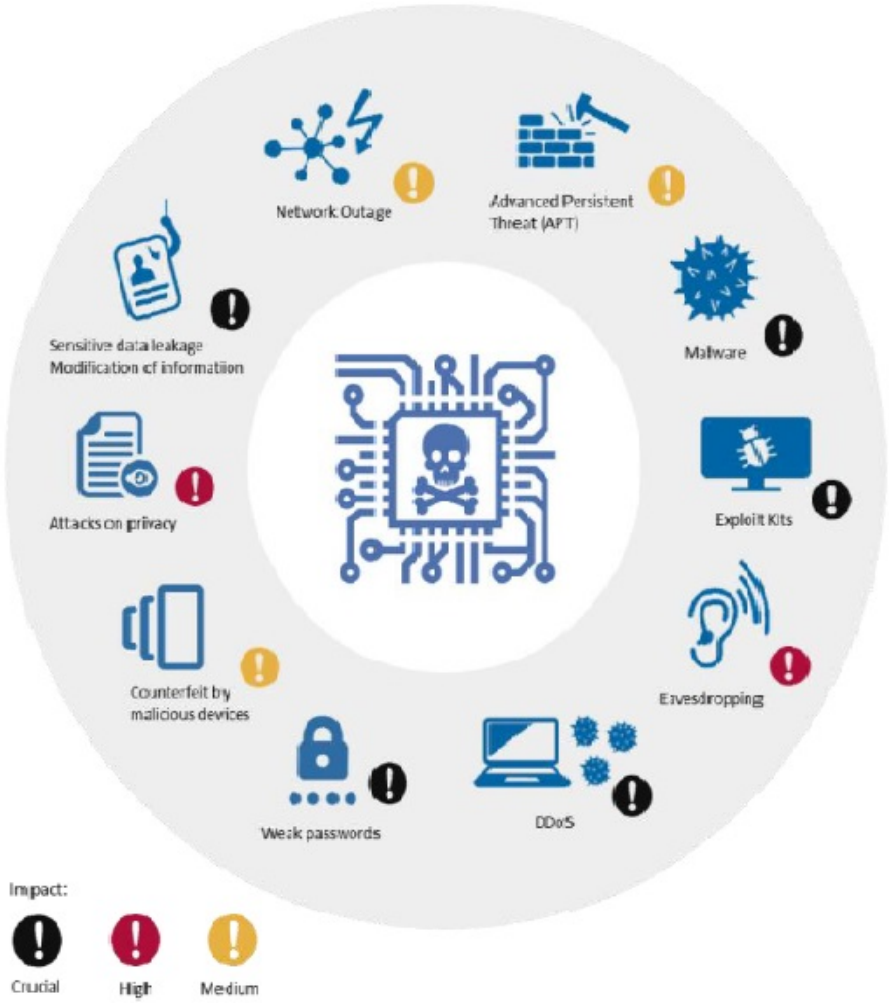
3.2 Ανάλυση και ταξινόμηση απειλών στο IoT

Κύριος στόχος της ενότητας αυτής είναι να καθορίσει και να απαριθμήσει τις απειλές για την ασφάλεια, τα τρωτά σημεία και τους παράγοντες κινδύνου που επηρεάζουν τις συσκευές και τα δίκτυα στο Διαδίκτυο των Πραγμάτων, λαμβάνοντας υπόψιν τα διάφορα επίπεδα σπουδαιότητας και κρισιμότητας όπως αναλύονται από τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Ασφάλεια στον Κυβερνοχώρο (European Union Agency for Cybersecurity - ENISA).

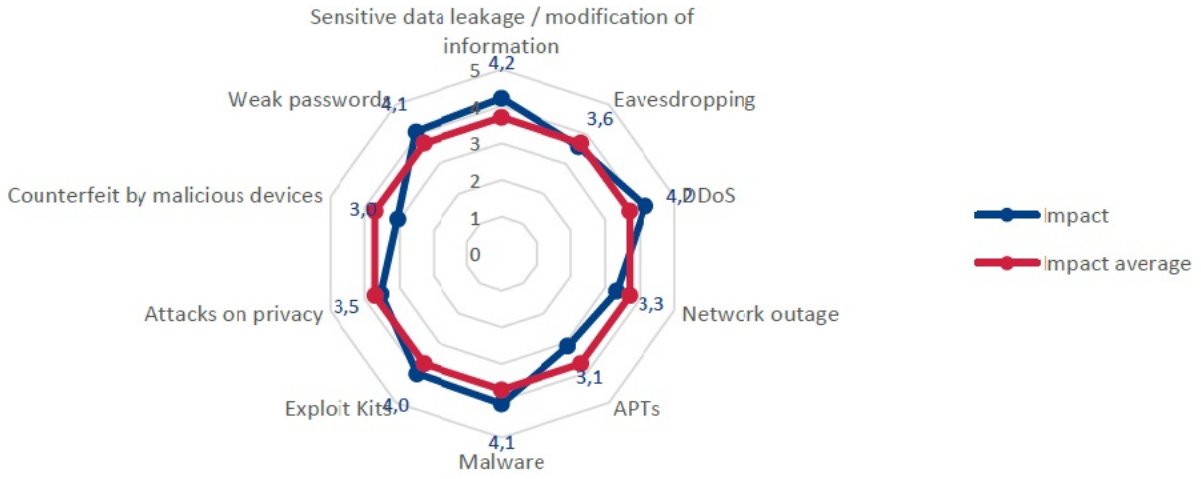
Τα τελευταία χρόνια ο αριθμός των απειλών ασφαλείας ολοένα και αυξάνεται. Η ευρύτερη διείσδυση του Διαδικτύου των Πραγμάτων σε ολόκληρο το φάσμα των καθημερινών δραστηριοτήτων και των κρίσιμων υποδομών, οδηγεί στην αυξητική τάση της εμφάνισης συμβάντων στην κυβερνοασφάλεια. Οι επιθέσεις στην πλειοψηφία τους σχετίζονται με συσκευές που έχουν παραβιαστεί ή με συστήματα που έχουν υποστεί βλάβη, αυξάνοντας ταυτόχρονα και τον αριθμό των κινδύνων που πρέπει να αντιμετωπιστούν στο Διαδίκτυο των Πραγμάτων. Οι απειλές και οι κίνδυνοι αυτοί θα μπορούσαν να χρησιμοποιηθούν από τους δράστες για να προκαλέσουν διαδοχικές επιπτώσεις και περαιτέρω ζημίες στα διαφορετικά επίπεδα της υποδομής.

Οι διάφορες απειλές έχουν διαφορετικές πιθανές επιπτώσεις, καθώς ποικίλλουν ανάλογα με τα σενάρια χρήσης. Ο αντίκτυπος κάθε απειλής, σύμφωνα με τον Οργανισμό

της Ευρωπαϊκής Ένωσης για την Ασφάλεια στον Κυβερνοχώρο (ENISA), προσδιορίστηκε με τον υπολογισμό ενός σταθμισμένου μέσου όρου των απαντήσεων από εμπειρογνώμονες, οι οποίοι βασίστηκαν σε μια κλίμακα πέντε βημάτων που κυμαινόταν από καμία σημασία έως κρίσιμη σημασία και απεικονίζονται στις εικόνες 23 και 24 (ENISA, 2017).



Εικόνα 23. Αντίκτυπος απειλών IoT



Εικόνα 24. Σταθμισμένος μέσος όρος επίπτωσης κάθε απειλής

Τέλος, ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια στον Κυβερνοχώρο (ENISA) παραθέτει στην έκθεσή του έναν συγκεντρωτικό πίνακα όλων των απειλών, ο οποίος περιλαμβάνει την κατηγορία της απειλής, την περιγραφή της και ποια αγαθά επηρεάζει η κάθε απειλή. Τις απειλές αυτές θα τις λάβουμε μεταγενέστερα υπόψιν στην παρούσα έρευνα όταν και θα εκπονήσουμε, για ένα υποθετικό σενάριο, μία εκτίμηση αντικτύπου ως προς την προστασία δεδομένων.

Κατηγορία	**Απειλή**	**Περιγραφή**	**Αγαθά που επηρεάζει**
Επικίνδυνη δραστηριότητα/ Κατάχρηση	Λογισμικό κακόβουλης λειτουργίας (Malware)	Πρόγραμμα λογισμικού που έχει σχεδιαστεί για την εκτέλεση ανεπιθύμητων και μη εξουσιοδοτημένων ενεργειών, με αποτέλεσμα την καταστροφή ή την κλοπή πληροφοριών. Ο αντίκτυπός της μπορεί να είναι υψηλός.	- Συσκευές IoT - Πλατφόρμα και σύστημα υποστήριξης
	Επίθεση άρνησης εξυπηρέτησης (DDoS attack)	Συστήματα που επιτίθενται σε έναν στόχο, ώστε να τον κάνουν να καταρρεύσει. Αυτό μπορεί να γίνει κάνοντας πολλές συνδέσεις, πλημμυρίζοντας ένα κανάλι επικοινωνίας ή επαναλαμβάνοντας την ίδια επικοινωνία.	- Συσκευές IoT - Πλατφόρμα και σύστημα υποστήριξης - Υποδομή

	Επιθέσεις στην προστασία προσωπικών δεδομένων	Η απειλή αυτή επηρεάζει τόσο την ιδιωτικότητα του χρήστη όσο και την έκθεση των στοιχείων του δικτύου σε μη εξουσιοδοτημένο πρόσωπα.	- Συσκευές IoT - Πλατφόρμα και σύστημα υποστήριξης - Υποδομή - Πληροφορίες
	Τροποποίηση πληροφοριών	Στην περίπτωση αυτή, στόχος δεν είναι να καταστραφούν οι συσκευές, αλλά να γίνει χειρισμός των πληροφοριών για να προκληθεί χάος.	- Συσκευές IoT - Πλατφόρμα και σύστημα υποστήριξης - Πληροφορίες
Υποκλοπή/Διακοπή/Πειρατεία	Επίθεση Man-in-the-Middle	Ενεργή επίθεση υποκλοπής, στην οποία ο εισβολέας μεταδίδει μηνύματα από το ένα θύμα στο άλλο, προκειμένου να τους κάνει να πιστέψουν ότι μιλούν απευθείας μεταξύ τους.	- Πληροφορίες - Δίκτυο επικοινωνίας - Συσκευές IoT
	Παρακολούθηση πληροφοριών	Μη εξουσιοδοτημένη παρακολούθηση (και μερικές φορές τροποποίηση) μιας ιδιωτικής επικοινωνίας, όπως τηλεφωνικές κλήσεις, άμεσα μηνύματα, επικοινωνίες μέσω ηλεκτρονικού ταχυδρομείου.	- Πληροφορίες - Δίκτυο επικοινωνίας - Συσκευές IoT
	Παραβίαση συνεδρίας (session hijacking)	Κλοπή της σύνδεσης δεδομένων ενεργώντας ως νόμιμος κόμβος με σκοπό την κλοπή, τροποποίηση ή τη διαγραφή δεδομένων.	- Πληροφορίες - Δίκτυο επικοινωνίας - Συσκευές IoT

	Συλλογή πληροφοριών	Παθητική λήψη εσωτερικών πληροφοριών που αφορούν το δίκτυο: συνδεδεμένες συσκευές, πρωτόκολλο κ.λπ.	- Πληροφορίες - Δίκτυο επικοινωνίας - Συσκευές IoT
Διακοπές	Αποτυχία συσκευών	Κίνδυνος βλάβης ή δυσλειτουργίας των συσκευών υλικού.	- Συσκευές IoT
	Αποτυχία Συστήματος	Κίνδυνος βλάβης των υπηρεσιών ή των εφαρμογών λογισμικού.	- Συσκευές IoT - Πλατφόρμα και σύστημα υποστήριξης
	Απώλεια υπηρεσιών υποστήριξης	Μη διαθέσιμες υπηρεσίες υποστήριξης, που απαιτούνται για την ορθή λειτουργία του συστήματος πληροφοριών.	Όλοι οι πόροι
Ζημία / Απώλεια Πόρων	Διαρροή δεδομένων / ευαίσθητων πληροφοριών	Τα ευαίσθητα δεδομένα αποκαλύπτονται, σκόπιμα ή όχι, σε μη εξουσιοδοτημένα μέρη. Η σημασία αυτής της απειλής μπορεί να ποικίλλει σημαντικά, ανάλογα με το είδος των δεδομένων που διαρρέουν.	- Συσκευές IoT - Πλατφόρμα και σύστημα υποστήριξης - Πληροφορίες
Αποτυχίες / Δυσλειτουργίες	Αδυναμίες λογισμικού	Οι πιο συνηθισμένες συσκευές IoT είναι συχνά ευάλωτες λόγω αδύναμων/προεπιλεγμένων κωδικών πρόσβασης, σφαλμάτων λογισμικού και σφαλμάτων διαμόρφωσης, που θέτουν σε κίνδυνο το δίκτυο.	- Συσκευές IoT - Πλατφόρμα και σύστημα υποστήριξης - Υποδομή - Εφαρμογές και υπηρεσίες
	Αδυναμίες τρίτων μερών	Σφάλματα σε ένα ενεργό στοιχείο του δικτύου που προκλήθηκαν από την εσφαλμένη ρύθμιση παραμέτρων ενός άλλου στοιχείου που έχει άμεση σχέση με αυτό.	- Συσκευές IoT - Πλατφόρμα και σύστημα υποστήριξης - Υποδομή -Εφαρμογές και υπηρεσίες
	Φυσική	Αυτά περιλαμβάνουν συμβάντα όπως πλημμύρες,	- Συσκευές IoT

Καταστροφή	καταστροφή	ισχυρούς ανέμους, και άλλες φυσικές καταστροφές, οι οποίες θα μπορούσαν να βλάψουν φυσικά τις συσκευές.	- Πλατφόρμα και σύστημα υποστήριξης - Υποδομή
	Περιβαλλοντική καταστροφή	Καταστροφές στα περιβάλλοντα υλοποίησης του εξοπλισμού IoT και πρόκληση της αδυναμίας λειτουργίας τους.	- Πλατφόρμα και σύστημα υποστήριξης - Υποδομή
Φυσικές επιθέσεις	Τροποποίηση συσκευής	Παραβίαση μιας συσκευής, όπως για παράδειγμα εκμετάλλευση εσφαλμένης διαμόρφωσης θυρών που παραμένουν ανοικτές.	- Δίκτυο επικοινωνίας - Συσκευές IoT
	Καταστροφή συσκευής	Περιστατικά όπως κλοπή συσκευών, βομβιστικές επιθέσεις, βανδαλισμός ή δολιοφθορά.	- Συσκευές IoT - Πλατφόρμα και σύστημα υποστήριξης - Υποδομή

Πίνακας 1. Ταξινόμηση απειλών σύμφωνα με τον ENISA

3.3 Απαιτήσεις ασφάλειας IoT

Τα βασικά ζητήματα ασφάλειας στο σύστημα Internet of Things προϋποθέτουν την ύπαρξη των μηχανισμών ελέγχου της ταυτότητας, καθώς και την προστασία της εμπιστευτικότητας των δεδομένων. Οι τρεις βασικές αρχές αποτελούν η διαθεσιμότητα των δεδομένων, η εμπιστευτικότητα και η ακεραιότητα. Σε περίπτωση που δεν εφαρμοστούν πιστά οι αρχές ασφαλείας ενδέχεται να επέλθουν σοβαρές επιπτώσεις στο Internet of Things. Συνεπώς, κάθε ένα από τα τέσσερα στρώματα του συστήματος δικτύου Internet of Things, οφείλει να πληροί τις συγκεκριμένες ελάχιστες απαιτήσεις. Στην εικόνα 23 αναπαρίσταται το τρίγωνο των αρχών ασφαλείας (Παπαζώης, 2019).

Εικόνα 25. Τριγωνική αναπαράσταση των αρχών ασφαλείας

3.4 Τεχνικές ασφάλειας και διαχείριση κινδύνων

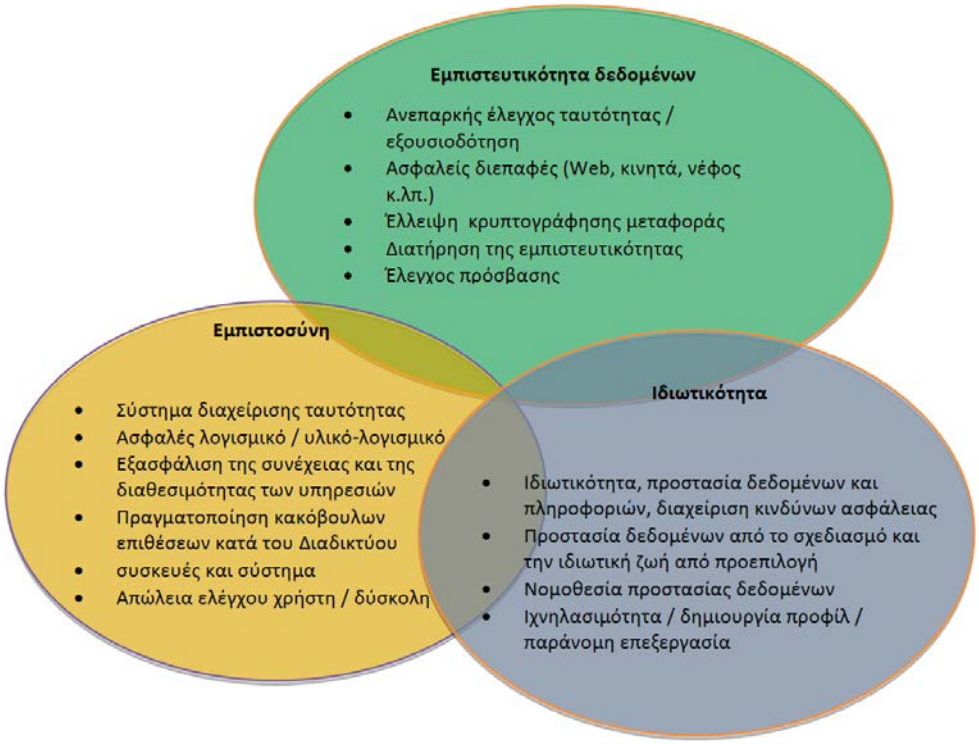
Στο σύστημα Internet of Things, κάθε συνδεδεμένη συσκευή αποτελεί κίνδυνο για παραβίαση των προσωπικών δεδομένων. Παράλληλα οι δυνητικοί κίνδυνοι οι οποίοι ελλοχεύουν από τη χρήση του διαδικτύου θα φθάσουν σε νέα επίπεδα, εφόσον η διαλειτουργικότητα και η αυτόνομη λήψη των αποφάσεων ξεκινάνε να ενσωματώνουν την πολυπλοκότητα, τα κενά ασφαλείας και την ενδεχόμενη ευπάθεια των συστημάτων. Η εμφάνιση κινδύνων ιδιωτικού απορρήτου καθίσταται εφικτή στο διαδίκτυο, καθώς η πολυπλοκότητα είναι σε θέση να προκαλέσει μεγαλύτερου βαθμού ευπάθεια όσον αφορά την προσφορά υπηρεσιών.

Σε μεγάλο μέρος των χρηστών, αρκετές πληροφορίες συνδέονται με τα προσωπικά τους στοιχεία, όπως για παράδειγμα τα στοιχεία ταυτότητας, η τοποθεσία μόνιμης διαμονής, αλλά και οικονομικά στοιχεία. Η συγκεκριμένη διάσταση της ογκώδους ποσότητας των δεδομένων επιφέρει προβλήματα και έτσι τα επαγγέλματα ασφάλειας οφείλουν να διασφαλίσουν τον τρόπο σκέψης τους διαμέσου των δυνητικών κινδύνων προστασίας της ιδιωτικής ζωής με ολόκληρο το σύνολο των δεδομένων. Το σύστημα Internet of Things οφείλει να εφαρμόζεται υπό νόμιμες και δημοκρατικές διαδικασίες, ενώ ταυτόχρονα να δίνεται έμφαση στις προκλήσεις που απορρέουν σε νομικό, τεχνικό και επιχειρηματικό επίπεδο (Li & Xu, 2017).

Οι βασικές ερευνητικές προκλήσεις στο Internet of Things εμπεριέχουν το απόρρητο των δεδομένων, την ιδιωτικότητα και την εμπιστοσύνη, όπως φαίνεται στο παρακάτω

σχήμα. Κύριο μέλημα αποτελεί η διασφάλιση των δεδομένων σε όλες τις φάσεις διεξαγωγής του έργου στο διαδίκτυο των πραγμάτων από τον αρχικό σχεδιασμό για τις υπηρεσίες οι οποίες εκτελούνται.

Αξίζει να επισημανθεί πως στο διαδίκτυο των πραγμάτων, εντοπίζονται τέσσερα επίπεδα ελέγχου ασφαλείας (ανίχνευσης, δικτύου, υπηρεσιών και διεπαφής εφαρμογής). Κάθε επίπεδο είναι σε θέση να παρέχει αντίστοιχα στοιχεία ασφαλείας, όπως για παράδειγμα ο έλεγχος πρόσβασης, ο έλεγχος ταυτότητας των συσκευών, η ακεραιότητα των δεδομένων και η εμπιστευτικότητα στη μετάδοση, η διαθεσιμότητα και η ικανότητα αντιμετώπισης κακόβουλου λογισμικού ή επιθέσεων.



Εικόνα 26. Η αντιμετώπιση των κυρίων προκλήσεων στο Internet of Things.

I. Ασφάλεια στο επίπεδο ανίχνευσης

Το συγκεκριμένο επίπεδο χαρακτηρίζεται ως η τομή ανάμεσα στους χρήστες, τους τόπους και τα πράγματα, τα οποία αποτελούν είτε απλές συσκευές, όπως για παράδειγμα τα συνδεδεμένα θερμόμετρα και οι λαμπτήρες, είτε σύνθετες συσκευές όπως για παράδειγμα τα ιατρικά εργαλεία και ο εξοπλισμός παραγωγής. Προς την κατεύθυνση εξασφάλισης της εμπιστοσύνης στους χρήστες, κρίνεται αναγκαία η σχεδίαση και η ενσωμάτωση στις ίδιες τις συσκευές. Συνεπώς, οι συσκευές του Internet of Things πρέπει να έχουν την ικανότητα απόδειξης της ταυτότητά τους, με απώτερο στόχο τη διασφάλιση της αυθεντικότητας, αλλά και της ακεραιότητας τους διαμέσου της κρυπτογράφησης των δεδομένων τους. Παράλληλα, θα πρέπει να διαθέτουν την ικανότητα ελάττωσης των τοπικών αποθηκευμένων δεδομένων με σκοπό την προάσπιση της ιδιωτικής ζωής.

Το μοντέλο ασφαλείας για συσκευές οφείλει να θέτει περιορισμούς, ώστε να μην επιτρέπεται η μη εξουσιοδοτημένη χρήση, ενώ ταυτόχρονα να παρέχει ευελιξία προκειμένου να υποστηρίζει ασφαλείς αλληλεπιδράσεις με τους χρήστες και άλλες συσκευές σε βραχυπρόθεσμη βάση. Επιπρόσθετα, κρίνεται αναγκαία η φυσική ασφάλεια, λόγω της παρουσίας των συσκευών στην ολότητα του συστήματος. Επομένως, απαραίτητη προϋπόθεση αποτελεί ο σχεδιασμός ανθεκτικότητας σε παραβιάσεις σε συσκευές, προκειμένου να παρουσιάζονται δυσκολίες κατά την εξαγωγή ευαίσθητων πληροφοριών, όπως για παράδειγμα προσωπικά δεδομένα, κωδικοί πρόσβασης κ.λπ. Άξιο αναφοράς αποτελεί το γεγονός της αναβάθμισης του λογισμικού των συσκευών του διαδικτύου των πραγμάτων, ώστε να διαθέτουν καλή λειτουργικότητα, εφόσον αναμένεται να έχουν μεγάλη διάρκεια ζωής (Li & Xu, 2017).

II. Ασφάλεια στο επίπεδο δικτύου

Το συγκεκριμένο επίπεδο του πλαισίου του διαδικτύου των πραγμάτων αντιπροσωπεύει τη συνδεσιμότητα, καθώς και τη μεταβίβαση των μηνυμάτων ανάμεσα στις συσκευές και Cloud υπηρεσιών. Οι επικοινωνίες στο διαδίκτυο συχνά αποτελούν συνδυασμό ιδιωτικών και δημόσιων δικτύων, συνεπώς η διασφάλιση της κυκλοφορίας καθίσταται σπουδαία. Σημαντικές κρίνονται για την ασφάλεια τεχνολογίες, όπως για παράδειγμα αποτελεί η κρυπτογράφηση TLS / SSL. Ωστόσο, η βασική δυσκολία δημιουργείται στην περίπτωση όπου απαιτούνται διαδικασίες κρυπτογράφησης σε

συσκευές με περιορισμένους πόρους, όπως μικρό-ελεγκτές 8 bit με περιορισμένη μνήμη RAM. Παράλληλα, ζήτημα ασφάλειας όσον αφορά το επίπεδο του δικτύου προκύπτει από το γεγονός πως η επικοινωνία αρκετών συσκευών Internet of Things διεξάγεται διαμέσου πρωτοκόλλων, διαφορετικών από το wi-fi. Επομένως, η πύλη Internet of Things φέρει την ευθύνη για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας κατά τη μετάφραση ανάμεσα σε διαφορετικά ασύρματα πρωτοκόλλα, όπως για παράδειγμα το Z-Wave ή το ZigBee στο wi-fi.

III. Ασφάλεια στο επίπεδο υπηρεσιών

Το συγκεκριμένο επίπεδο του πλαισίου αντιπροσωπεύει το σύστημα διαχείρισης του διαδικτύου και φέρει την αποκλειστική ευθύνη για την διαχείριση των συσκευών και των χρηστών, την εφαρμογή πολιτικών και κανόνων και το συντονισμό της αυτοματοποίησης σε όλες τις συσκευές. Ο έλεγχος πρόσβασης βάσει ρόλων με στόχο τη διαχείριση της ταυτότητας των χρηστών και των συσκευών, καθώς και οι ενέργειες στις οποίες έχουν εξουσιοδοτηθεί να υλοποιηθούν, κρίνονται εξαιρετικά σημαντικές. Προς την κατεύθυνση αποφυγής της αναδημοσίευσης, είναι σημαντικό να διατηρηθεί ένα ίχνος ελέγχου των αλλαγών οι οποίες υλοποιούνται από κάθε χρήστη και συσκευή, προκειμένου να μην είναι εφικτό ν' αντικρούονται οι ενέργειες που διεκπεραιώνονται στο σύστημα. Παράλληλα τα δεδομένα παρακολούθησης θα αποτελούσαν ένα μέσο για τον εντοπισμό ενδεχομένων συμβιβαζόμενων συσκευών, στην περίπτωση όπου ανιχνεύεται μη φυσιολογική συμπεριφορά (Li & Xu, 2017).

IV. Ασφάλεια στο επίπεδο διεπαφής

Η ισχυρή ασφάλεια συνδέεται με την ενσωμάτωσή της στις ίδιες τις συσκευές, όπου θα πρέπει να δίνεται έμφαση στην εφαρμογή κρυπτογραφίας σε όλες, ανεξαρτήτου μεγέθους. Άξιο αναφοράς αποτελεί η δημιουργία ενός συνόλου απαιτήσεων ασφάλειας, οι οποίες συνδέονται με την προάσπιση της ιδιωτικής ζωής, όπως για παράδειγμα η γνωστοποίηση σαφούς χρήσης δεδομένων, προκειμένου οι χρήστες να διαθέτουν αντίληψη των δεδομένων που αποστέλλονται και αποθηκεύονται στην cloud υπηρεσία, διαχωρισμένα ή κρυπτογραφημένα με κωδικούς πρόσβασης. Απαραίτητη προϋπόθεση κρίνεται η ανωνυμία των δεδομένων κατά την ανάλυσή τους.

Μια κρίσιμη απαίτηση του συστήματος Internet of Things αποτελεί η αλληλοσύνδεση των συσκευών, γεγονός που παρέχει ικανότητα επεξεργασίας των δεδομένων. Το

διαδίκτυο των πραγμάτων διαθέτει τη δυνατότητα παραλαβής, μεταβίβασης και επεξεργασίας πληροφοριών από κόμβους, όπως οι πύλες και οι συσκευές RFID, διαμέσου του δικτύου για την υλοποίηση πολύπλοκων εργασιών. Επομένως, κρίνεται αναγκαίο το διαδίκτυο των πραγμάτων να διαθέτει την ικανότητα παροχής εφαρμογών με μεγάλη προστασία ασφάλειας, όπως παράδειγμα κατά τη διαδικασία ηλεκτρονικών πληρωμών, απαιτείται η διασφάλιση των δεδομένων (Li & Xu, 2017).

3.5 Σύγχρονες τάσεις στην ασφάλεια του IoT

Η ραγδαία εξέλιξη της τεχνολογίας οδηγεί την αυτήν του Διαδικτύου των Πραγμάτων στη δημιουργία ενός δικτύου αυτόνομων συσκευών που επικοινωνούν και αλληλεπιδρούν μεταξύ τους, λαμβάνοντας έξυπνες αποφάσεις με τη χρήση της τεχνητής νοημοσύνης (δηλαδή χωρίς την ανθρώπινη παρέμβαση). Η δημιουργία του δικτύου αυτών των αυτόνομων συσκευών εισάγει με τη σειρά της νέες τάσεις στις τεχνολογίες ασφάλειας που διέπουν το IoT. Μια τέτοια τεχνολογία είναι και το blockchain (Nicholas Kolokotronis, Konstantinos Limniotis, Stavros Shiaeles, Romain Griffiths, 2019).

Πρόκειται για μια δομή δεδομένων που παρέχει μια επαληθεύσιμη διαδικασία αποθήκευσης συναλλαγών ή ψηφιακών περιουσιακών στοιχείων σ' ένα αμετάβλητο κοινόχρηστο καθολικό (ledger) με τέτοιο τρόπο ώστε να υπάρχει διαφάνεια, ασφάλεια και κύρος. Κάθε συναλλαγή που πραγματοποιείται μεταξύ των κόμβων του δικτύου συνοδεύεται από μια έγκυρη επαληθεύσιμη απόδειξη που είναι αποδεκτή από όλους τους κόμβους. Η χρήση της τεχνολογίας blockchain στο Διαδίκτυο των Πραγμάτων (Internet of Things), η οποία ονομάζεται αλλιώς και Distributed Ledger Technology (DLT), επιτρέπει στις συσκευές του οικοσυστήματος να ενεργούν αυτόνομα και να εκτελούν συναλλαγές με τη χρήση έξυπνων συμβάσεων.

Καθώς η ανάπτυξη του blockchain βρίσκεται ακόμη σε πρώιμο στάδιο, η προστασία της ιδιωτικότητας παραμένει μείζον πρόβλημα που επιζητά λύσεις, αφού όλοι οι κόμβοι του οικοσυστήματος έχουν άμεση πρόσβαση στα δεδομένα των άλλων, αλλά επίσης και οι συναλλαγές είναι ορατές σε όσους έχουν άμεση πρόσβαση στη διαδικασία του blockchain. Έτσι η τεχνολογική αυτή εξέλιξη φέρνει μαζί της και νέες μορφές απειλών και επιθέσεων που εκμεταλλεύονται την πολυπλοκότητα και την ετερογένεια του

οικοσυστήματος του IoT. Συμπεραίνουμε, λοιπόν, ότι η ασφάλεια συγκαταλέγεται στις σημαντικότερες πτυχές κατά την χρήση μιας τέτοιας τεχνολογίας.

Εικόνα 27. Blockchain & IoT (https://hackernoon.com/when-iot-meets-blockchain-%EF%B8%8F-892fecdaf00c)

Καθώς το IoT εξελίσσεται υπάρχουν αρκετοί αναδυόμενοι τομείς του, όπως σύγχρονα δίκτυα αισθητήρων, κατανεμημένα συστήματα ελέγχου κ.λπ., στους οποίους τομείς διασυνδέονται συσκευές με αρκετούς περιορισμούς που συνεργάζονται για την εκπλήρωση ορισμένων καθηκόντων επικοινωνώντας μεταξύ τους κυρίως ασύρματα. Επομένως, η επικοινωνία τους για να είναι ασφαλής θα πρέπει να χρησιμοποιηθούν ισχυροί κρυπτογραφικοί αλγόριθμοι.

Στην πλειονότητά τους οι τρέχοντες κρυπτογραφικοί αλγόριθμοι έχουν σχεδιαστεί για περιβάλλοντα κυρίως επιτραπέζιων υπολογιστών ή διακομιστών (Servers) με αποτέλεσμα οι περισσότεροι να μην μπορούν να ενσωματωθούν σε ένα δίκτυο περιορισμένων συσκευών.

Για το λόγο αυτό, το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology – NIST) διεξάγει διαγωνισμούς για την αναζήτηση, αξιολόγηση και τυποποίηση ελαφρών κρυπτογραφικών αλγορίθμων (lightweight cryptographic algorithms), η απόδοση των οποίων θα είναι κατάλληλη για χρήση σε

περιορισμένες συσκευές. Κύριο πεδίο εφαρμογής των αλγορίθμων αυτών είναι και το Διαδίκτυο των Πραγμάτων (https://csrc.nist.gov/projects/lightweight-cryptography).

3.6 Εμπιστευτικότητα προσωπικών δεδομένων

Η προστασία των προσωπικών δεδομένων (δηλαδή δεδομένων που αφορούν φυσικά πρόσωπα) προβάλλει ως πρωταρχικός παράγοντας κατά τη δημιουργία υπηρεσιών του συστήματος IoT. Θα πρέπει να δίνεται έμφαση στην ασφάλεια με απώτερο στόχο να αυξάνεται η εμπιστοσύνη των χρηστών, διαφορετικά θα σταματήσουν να το χρησιμοποιούν, ώστε να διασφαλίσουν την προστασία των προσωπικών τους δεδομένων. Ο διαρκής πολλαπλασιασμός του δικτύου Internet of Things, θα παρέχει τη δυνατότητα πρόσβασης σε ευαίσθητες πληροφορίες για οποιοδήποτε περιβάλλον.

Επομένως, ο κίνδυνος της διάθεσης τόσο των προσωπικών δεδομένων όσο και των δεδομένων που είναι σε θέση να δημιουργήσουν διάφορα προφίλ των καταναλωτών, όπως για παράδειγμα αποτελούν οι προτιμήσεις ενός χρήστη σχετικά με τα ταξίδια, είναι εφικτός. Επιπρόσθετα, ο συνδυασμός των διάφορων δεδομένων και η επεξεργασία τους, εγείρει έντονα την ανησυχία των καταναλωτών, διότι ελλοχεύει ο κίνδυνος μετάδοσης πληροφοριών, όπου δε θα ήταν επιθυμητό να δημοσιευτούν και να γίνουν αντικείμενο ενημέρωσης σε άλλους χρήστες του διαδικτύου (Τζιούφα, 2019).

Το απόρρητο δεν είναι εγγενές στο Internet of Things, επομένως όπου εντοπίζεται ένα σύστημα ή μια υπηρεσία του, δε συνεπάγεται την ενδεχόμενη παραβίαση των προσωπικών δεδομένων. Ωστόσο, η ογκώδης ποσότητα δεδομένων, η οποία υφίσταται στο σύνολο του διαδικτύου των πραγμάτων, σε όλα τα στοιχεία και τις υπηρεσίες του, ανεξάρτητα από τη διαφορά ιδιοκτησίας και διαχείρισης του, καθώς και της αποθήκευσης του, καθιστά αδιαμφισβήτητο το γεγονός πως το Internet of Things, αποτελεί εν δυνάμει μια αρκετά μεγάλη και μαζική πηγή δεδομένων, όπου συνήθως σημαντικό ποσοστό κατέχουν τα προσωπικά δεδομένα (Macaulay, 2017).

Εν κατακλείδι, ο κίνδυνος που απορρέει από τη ροή προσωπικών δεδομένων στο διαδίκτυο, οφείλει να είναι αντιληπτός από τους χρήστες, στα όρια των απαιτήσεων οι οποίες προκύπτουν βάσει της ρύθμισης του νόμου σε συνδυασμό με τη λειτουργικότητα του Internet of Things.

Θα πρέπει να επισημανθεί ότι για την προστασία των προσωπικών δεδομένων υπάρχει ένα στέρεο νομικό πλαίσιο, το οποίο περιγράφει υποχρεώσεις όσων επεξεργάζονται προσωπικά δεδομένα, αλλά και δικαιώματα των προσώπων των οποίων τα δεδομένα υφίστανται επεξεργασία. Το εν λόγω νομικό πλαίσιο καλύπτει όχι μόνο θέματα ασφάλειας, αλλά και θέματα που σχετίζονται με την ιδιωτικότητα του ατόμου (π.χ. διαφανή συλλογή και περαιτέρω επεξεργασία των προσωπικών δεδομένων, όχι χρήστη των δεδομένων για άλλο σκοπό πέραν από αυτόν για τον οποίο συλλέχτηκαν, όχι συλλογή υπέρμετρων προσωπικών δεδομένων σε σχέση με το σκοπό επεξεργασίας, ύπαρξη κατάλληλης νομικής βάσης για να είναι επιτρεπτή η επεξεργασία κτλ.). Μια γενική σύνοψη του εν λόγω νομικού πλαισίου παρατίθεται στο επόμενο κεφάλαιο.

Κεφάλαιο 4

Ιδιωτικότητα και προστασία προσωπικών δεδομένων

4.1. Εισαγωγή

Πριν την διερεύνηση, μέσω πρακτικής εφαρμογής, των κινδύνων προστασίας προσωπικών δεδομένων σε περιβάλλον IoT, θα γίνει λόγος στην εργασία αυτή για ορισμένες έννοιες οι οποίες είναι βασικές για την κατανόηση του σχετικού νομικού πλαισίου αυτού. Πρόκειται ειδικότερα για τις έννοιες:

Α) Ιδιωτικότητα

Β) Προστασία προσωπικών δεδομένων

Αν και υπάρχει μία στενή σύνδεση των δύο ανωτέρω εννοιών, δεν ταυτίζονται.

Επιπλέον, θα υλοποιηθεί μια σύντομη ανάλυση σχετικά με το νέο Γενικό Κανονισμό Προστασίας Δεδομένων (General Data Protection Regulation- GDPR), το βασικό νομικό κείμενο που διέπει την επεξεργασία προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση (αλλά και εκτός αυτής, εάν η επεξεργασία αφορά σε πολίτες εντός της Ένωσης). Πρέπει εδώ να αναφερθεί συγκεκριμένα ότι ο Γενικός Κανονισμός αυτός είναι εξαιρετικής σημασίας, αφού σε αυτόν βασίζεται η μεθοδολογία Αξιολόγησης Αντίκτυπου Προστασίας Δεδομένων, η οποία υλοποιείται μέσω του εργαλείου PIA στο επόμενο κεφάλαιο της εργασίας. Η επόμενη παράγραφος αφορά την ιδιωτικότητα.

4.2. Ιδιωτικότητα και προστασία προσωπικών δεδομένων

Η έννοια της ιδιωτικότητας (privacy) είναι μια έννοια αρκετά διαδεδομένη, από το χώρο της φιλοσοφίας (Ludwig Wittgenstein) μέχρι το χώρο της πληροφορικής και της νομικής, επιστήμες που, όταν συνδυάζονται, έχουμε το δίκαιο πληροφορικής, στο οποίο ο σχετικός προβληματισμός είναι ιδιαίτερα ανεπτυγμένος.

Στη συγκεκριμένη μεταπτυχιακή διατριβή θα γίνει χρήση ενός απλούστερου ορισμού, ο οποίος προέρχεται από σχετικούς οργανισμούς. Έτσι, σύμφωνα με τον ορισμό που δίνει ένας από τους μεγαλύτερους παγκοσμίως οργανισμούς ιδιωτικότητας, ο IAPP (International Association of Privacy Professionals), πρόκειται για:

α) Το δικαίωμα του να είναι κανείς μόνος (με κάποιον ή κάποιους άλλους),

β) Την ελευθερία από παρεμβάσεις ή εισβολές.

Ειδικότερη έννοια από την ιδιωτικότητα είναι η έννοια της ιδιωτικότητας των πληροφοριών. Πρόκειται για το δικαίωμα του ελέγχου πάνω στα δεδομένα κάθε ατόμου. Συγκεκριμένα, αυτός ο έλεγχος εκδηλώνεται ως εξής:

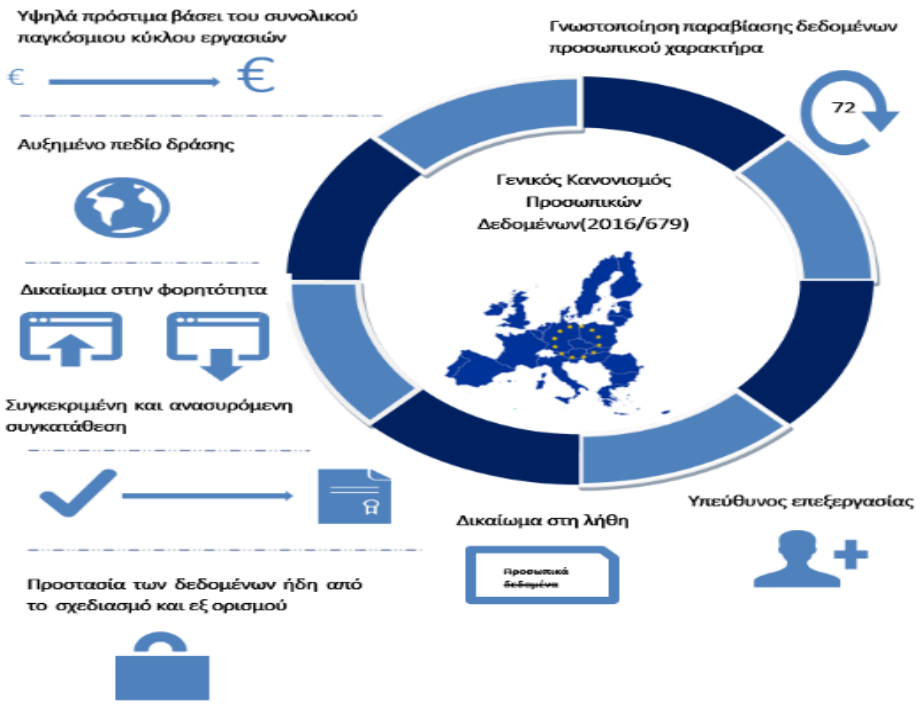
- Δικαίωμα συλλογής προσωπικών πληροφοριών.
- Δικαίωμα χρήσης προσωπικών πληροφοριών.

Από τα παραπάνω προκύπτει ότι υπάρχει μια στενή σχέση αφενός μεταξύ της έννοιας της ιδιωτικότητας και από την άλλη της προστασίας των προσωπικών πληροφοριών. Αυτό μπορεί κανείς να το επαληθεύσει και με άλλους τρόπους. Ένα παράδειγμα είναι ότι συχνά στην έρευνα οι δύο όροι, ιδιωτικότητα και προστασία προσωπικών δεδομένων, χρησιμοποιούνται εναλλάξ (Safari, 2017).

Γενικότερα, ο Γενικός Κανονισμός Προστασίας Δεδομένων είναι ο κανονισμός της Ευρωπαϊκής Ένωσης που τέθηκε σε ισχύ εδώ και τεσσεράμισι περίπου χρόνια, αντικαθιστώντας τον προηγούμενο κανονισμό 95/46/ΕΚ. επιφέρει μια σειρά αλλαγών. Αυτό είναι το αντικείμενο της επόμενης παραγράφου.

4.3. Ο Κανονισμός GDPR

Ο Κανονισμός GDPR είναι σε ισχύ από τις 27 Απριλίου 2016, τέθηκε σε εφαρμογή από τις 25 Μαΐου 2018, και στα πλαίσιά του πραγματοποιείται μια σειρά από αλλαγές, σε σχέση με το προηγούμενο νομικό πλαίσιο. Σχηματικά οι αλλαγές αυτές δίνονται στο διάγραμμα της Εικόνας 26, που προέρχεται από ιστοσελίδα του επίσημου φορέα της χώρας μας.



Εικόνα 28. Βασικά χαρακτηριστικά και δικαιώματα του GDPR (https://www.gdprgreece.com/article/5/gdpr)

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR- 2016/679) συνιστά μια πολύ μεγάλης κλίμακας αλλαγή για τη νομοθεσία της Ευρωπαϊκής Ένωσης. Είναι χαρακτηριστικό ότι η συγκεκριμένη νομοθεσία, ως Κανονισμός της Ευρωπαϊκής Ένωσης, τέθηκε σε άμεση εφαρμογή, χωρίς τον όρο ενσωμάτωσής της δηλαδή στην εθνική νομοθεσία (GDPR Greece - Τι είναι το GDPR και πως επηρεάζει τις επιχειρήσεις;).

Σκοπός του GDPR υπήρξε μεταξύ άλλων η δημιουργία ενός ενιαίου ευρωενωσιακού νομικού πλαισίου καθώς και η ενίσχυση ορισμένων δικαιωμάτων προστασίας

δεδομένων των πολιτών, τα οποία σχετίζονται με την προστασία των προσωπικών τους δεδομένων. Σημειώνεται επίσης ότι όλες οι επιχειρήσεις αλλά και οι αντίστοιχοι δημόσιοι οργανισμοί, σύλλογοι και λοιποί φορείς που επεξεργάζονται προσωπικά δεδομένα πολιτών της Ευρωπαϊκής Ένωσης οφείλουν να συμμορφώνονται με τον GDPR. Για επιχειρήσεις που δραστηριοποιούνται, για παράδειγμα, αποκλειστικά στις Ηνωμένες Πολιτείες, υφίστανται άλλοι κανονισμοί για ευαίσθητα προσωπικά δεδομένα (ACTA, HIPAA κ.ά.).

Κάποιες βασικές πτυχές του GDPR είναι οι εξής:

- Ο έλεγχος της εφαρμογής του σε ένα Κράτος Μέλος ανατίθεται σε αρμόδια ανεξάρτητη εποπτική Αρχή. Στην Κύπρο, αρμόδιο είναι το Γραφείο Επιτρόπου Προστασίας Προσωπικών Δεδομένων Προσωπικού Χαρακτήρα (http://www.dataprotection.gov.cy), ενώ στην Ελλάδα είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (www.dpa.gr). Η εποπτική Αρχή μπορεί να επιβάλλει διοικητικές κυρώσεις, οι οποίες μπορούν να είναι και επιβολή προστίμου, ανώτατου ύψους μέχρι και 10 ή 20 εκατομμύρια ευρώ (αναλόγως την περίπτωση).

- Ο φορέας/οργανισμός ο οποίος καθορίζει το σκοπό και τα μέσα της επεξεργασίας και είναι υποχρεωμένος να πληροί τις υποχρεώσεις του GDPR, είναι ο *«Υπεύθυνος Επεξεργασίας»* (data controller).

- Ο GDPR ενισχύει τα δικαιώματα όσων τα δεδομένα υφίστανται επεξεργασία με έμφαση στα μικρά παιδιά που θεωρούνται «ευάλωτα φυσικά πρόσωπα»

- Σε περίπτωση παραβίασης, ο Υπεύθυνος Επεξεργασίας πρέπει εντός 72 ωρών να ενημερώσει την αρμόδια Αρχή καθώς και –σε ορισμένες περιπτώσεις- και το υποκείμενο

- Τα δεδομένα πρέπει να προστατεύονται ήδη από τη στιγμή του καθορισμού των μέσων επεξεργασίας των δεδομένων καθώς και κατά τη στιγμή της επεξεργασίας

- Η συγκατάθεση των υποκειμένων των δεδομένων (δηλαδή των προσώπων των οποίων τα δεδομένα υφίστανται επεξεργασία) πρέπει πάντοτε να είναι ρητή και κατ' επίγνωση και επίσης να υπόκειται σε ανάκληση[1]

- Σε περίπτωση που η επεξεργασία είναι υψηλού κινδύνου για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, πρέπει να διενεργείται Εκτίμηση Αντικτύπου Προστασίας Δεδομένων (DPIA)

Επίσης, τα βασικά δικαιώματα των υποκειμένων που αναφέρονται στην επεξεργασία των δεδομένων που ορίζονται στον GDPR είναι τα ακόλουθα:

- Δικαίωμα ανάκλησης (σε ήδη δοσμένη συναίνεση για επεξεργασία).

- Δικαίωμα πρόσβασης στα δεδομένα (αίτηση για παραλαβή αντιγράφου).

- Δικαίωμα διόρθωσης ή/και διαγραφής δεδομένων (που κρατούνται από τον οργανισμό που τα επεξεργάζεται).

- Δικαίωμα περιορισμού της επεξεργασίας των δεδομένων (στις περιπτώσεις που είναι παράνομη, δεν είναι απαραίτητη κ.ά.).

- Δικαίωμα στη φορητότητα (λήψη προσωπικών δεδομένων προς διαβίβαση).

- Δικαίωμα εναντίωσης στην επεξεργασία δεδομένων (ασκείται υπό την προϋπόθεση ότι ο Υπεύθυνος Επεξεργασίας δεν μπορεί να αποδείξει υπέρτερο έννομο συμφέρον-απαίτηση).

Όλα τα παραπάνω συνοψίζουν τις βασικές αλλαγές που επέφερε ο GDPR, καθώς και τα βασικά δικαιώματα που αναγνωρίζονται στα υποκείμενα των δικαιωμάτων. Στην πράξη, αυτά τα δικαιώματα θα δειχθεί πώς θα προστατευθούν μέσα από την υλοποίηση της Εκτίμησης Αντικτύπου Προστασίας Δεδομένων.

[1] Αυτό ισχύει βέβαια όταν η νομική βάση για την επεξεργασία είναι η συγκατάθεση, διότι υπάρχουν και άλλες νομικές βάσεις που δεν εναπόκεινται στη συγκατάθεση (όπως η ύπαρξη έννομης υποχρέωσης, η εκτέλεση σύμβασης κ.α.)

Κεφάλαιο 5

Μελέτη περίπτωσης: Εκτίμηση αντικτύπου προστασίας δεδομένων σε «έξυπνο» σπίτι

5.1 Εισαγωγή

Στο τμήμα αυτό της εργασίας, θα μελετήσουμε μια συγκεκριμένη εφαρμογή στο Internet of Things (Διαδίκτυο των Πραγμάτων). Συγκεκριμένα, η εφαρμογή αυτή είναι η εφαρμογή smart home, δηλαδή το σύνολο των «πραγμάτων» μέσα στο σπίτι, από το φωτισμό έως ειδικούς αισθητήρες στον κήπο (https://www.iot-now.com/2020/06/10/98753-iot-home-automation-future-holds/), οι οποίοι μπορούν ν' ανήκουν στην κατηγορία αυτή. Αυτό που είναι εκ προοιμίου βέβαιο είναι ότι η συγκεκριμένη εφαρμογή θα πρέπει να έχει συγκεκριμένες προϋποθέσεις ασφάλειας και κατά συνέπεια ότι θα πρέπει να διερευνηθούν προσεκτικά τα ζητήματα ασφάλειας και ιδιωτικότητας. Λέγοντας ζητήματα ασφάλειας και ιδιωτικότητας, εννοούνται τα ζητήματα προστασίας των προσωπικών δεδομένων υψηλής ευαισθησίας, εφόσον οι εφαρμογές αυτές εισέρχονται μέσα στο χώρο της προσωπικής ζωής του ανθρώπου. Έτσι, τα συγκεκριμένα ζητήματα θα μελετηθούν μέσω ενός συγκεκριμένου εργαλείου, μέσω του οποίου μπορούν να καταχωρηθούν με κατάλληλο τρόπο. Το εργαλείο που θα χρησιμοποιηθεί για τα ζητήματα ιδιωτικότητας θα υλοποιήσει μελέτη τύπου *Data Protection Impact Assessment* (DPIA) και είναι εργαλείο που έχει αναπτυχθεί για το σκοπό αυτό, από την Αρχή Προστασίας Προσωπικών Δεδομένων της Γαλλίας.

Αναφορικά με τη δομή του συγκεκριμένου μέρους, επισημαίνεται εδώ ότι αρχικά θα πραγματοποιηθεί μια σύντομη παρουσίαση τριών θεμελιωδών θεμάτων για τη συνέχεια. Τα θέματα αυτά είναι:

1. Χαρακτηριστικά του *«Έξυπνου Σπιτιού»* (smart home)
2. Χαρακτηριστικά του εργαλείου που ονομάζεται *«PIA»* (και διεξάγει Protection Impact Assessment)

Εικόνα 29. Απεικόνιση προϊόντος Έξυπνου Σπιτιού (Smart Home)

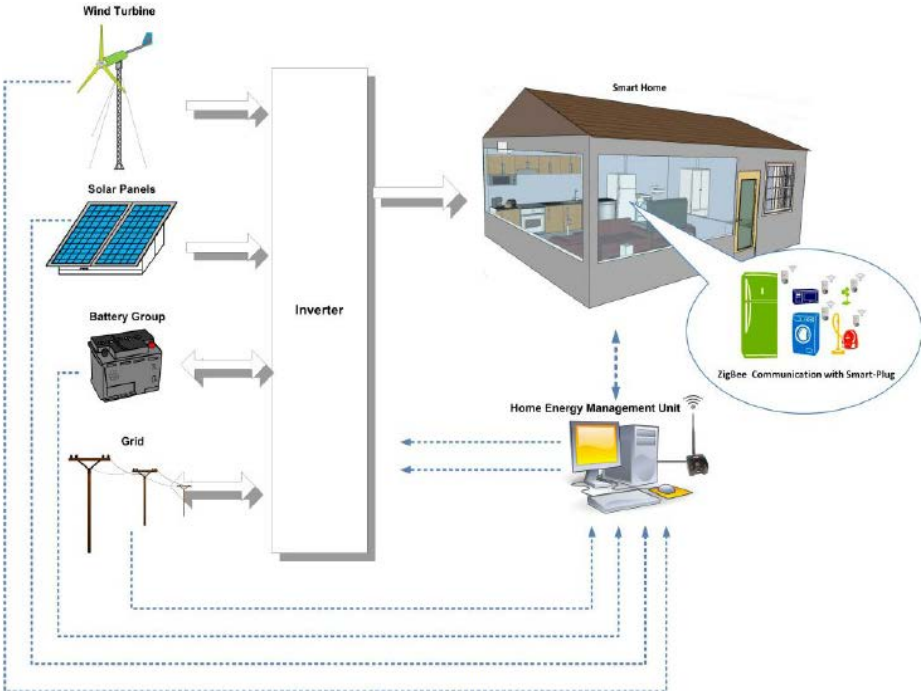
5.2 Έξυπνο Σπίτι

Οι εφαρμογές smart home για το Διαδίκτυο των Πραγμάτων είναι τα τελευταία χρόνια και στη χώρα μας μια γρήγορα αναπτυσσόμενη πραγματικότητα. Αν αναζητήσει κανείς σε κάποια μηχανή αναζήτησης, θα συναντήσει μια σειρά άρθρων σε ιστοσελίδες ενημερωτικού ή άλλου χαρακτήρα πολύ πρόσφατα και εκτεινόμενα συνολικά στα τρία τελευταία χρόνια σχετικά με την τεχνολογία του Έξυπνου Σπιτιού. Τίθεται ωστόσο το ερώτημα ποια είναι αυτά τα αντικείμενα, στα οποία μπορούμε να εφαρμόσουμε σύνδεση στο Διαδίκτυο και τα οποία συνιστούν τις εφαρμογές Smart Home.

Μια εμπεριστατωμένη και πλήρη παρουσίαση πραγματοποιεί ο (Αντωνάτος, 2018), ο οποίος απαριθμεί και τα παρακάτω στοιχεία:

1. **Σύστημα Διαχείρισης Ενέργειας**

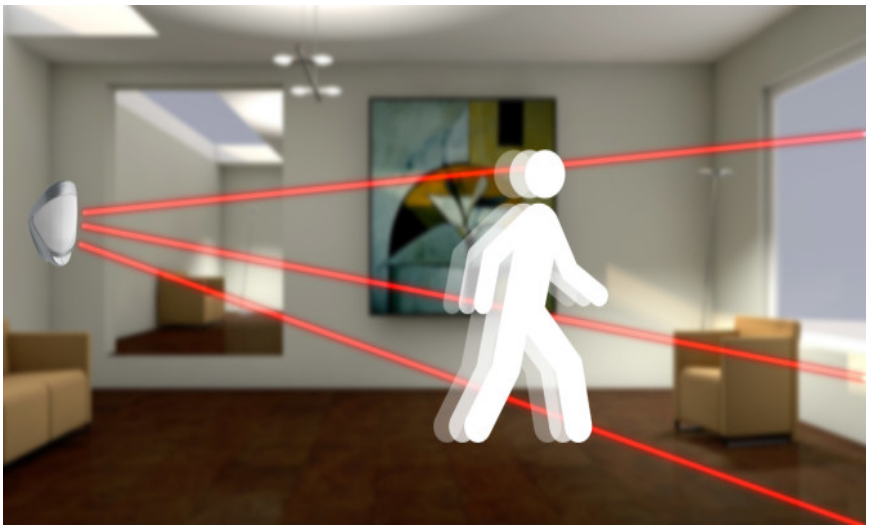
Πρόκειται για ένα σύστημα Διαχείρισης Ενέργειας Έξυπνου Σπιτιού, το οποίο πραγματοποιεί επίβλεψη και απόκτηση δεδομένων (Pau, Colotta, Ruano and Qin, 2017).



Εικόνα 30. Απεικόνιση Συστήματος Διαχείρισης Ενέργειας μέσα σε Έξυπνο Σπίτι (https://www.researchgate.net/figure/Smart-Home-Energy-Management-System-SHEMS-Concept_fig1_263220840)

2. **Ανίχνευση ανθρώπινης κίνησης-δραστηριότητας**

Πρόκειται για εφαρμογές, οι οποίες έχουν να κάνουν με την ανθρώπινη κίνηση εντός του χώρου του έξυπνου σπιτιού. Υπάρχουν ειδικοί αισθητήρες, οι οποίοι μπορούν να ανιχνεύσουν εάν υπάρχει είσοδος ή έξοδος από κάποιο δωμάτιο του σπιτιού ή κίνηση μέσα σε αυτό (βλ. Εικόνα 31), καθώς επίσης και την κατάσταση μιας πόρτας μέσα στο σπίτι (ανοιχτή ή κλειστή). Αυτοί οι δύο αισθητήρες μπορούν και συχνά μάλιστα στην πράξη όντως να λειτουργούν σε συνδυασμό.



Εικόνα 31. Ανίχνευση κίνησης εντός σπιτιού με ειδικό αισθητήρα (http://getsmarthomedevices.com/top-10-smart-home-motion-detectors)

3. **Έξυπνο ψυγείο**

Μια τρίτη εφαρμογή είναι αυτή του έξυπνου ψυγείου. Και πάλι εδώ έχουμε λειτουργία της συσκευής με έξυπνο τρόπο που μπορεί να είναι και ενεργειακά αποτελεσματικός. Συγκεκριμένα, ο χρήστης χειρίζεται μια οθόνη αφής στην πόρτα του ψυγείου. Έτσι, έχει δύο τρόπους χειρισμού του έξυπνου ψυγείου:

- Γραφική Διεπιφάνεια Χρήστη
- Φωνητικά μηνύματα Χρήστη

Εικόνα 32. Έξυπνο ψυγείο του εμπορίου (https://internetofbusiness.com/smart-appliance-market-set-for-growth/)

4. **Έξυπνο πλυντήριο ρούχων**

Το έξυπνο πλυντήριο ρούχων είναι μια ακόμη συσκευή που σχετίζεται με το Έξυπνο Σπίτι. Πρόκειται για πλυντήριο που, όπως όλα τ' άλλα σχετικά αντικείμενα, συνδέονται σε ασύρματο δίκτυο. Ειδικότερα, κανείς μπορεί να τα χειριστεί μέσω ενός κινητού τηλεφώνου τύπου smartphone, με τις αντίστοιχες εφαρμογές, όπως είναι η Alexa ή Google Assistant (Harding, n.d.).

Εικόνα 33. Έξυπνο πλυντήριο ρούχων και χειρισμός μέσω εφαρμογής κινητού τηλεφώνου

5. **Έξυπνα έπιπλα**

Η συγκεκριμένη τεχνολογία είναι από τις πλέον καινοτομικές που υπάρχουν και μπορεί να αφορά είτε σε πολυθρόνες που διαθέτουν κάποιο μηχανισμό που τους επιτρέπει την αυτόματη κίνηση είτε και καναπέδες σαλονιών, όπως παρατηρείται στην Εικόνα 34.

Εικόνα 34. Έξυπνος καναπές smart home (https://www.tallwallbed.com/uploadfile/201701/20/b1ec99281df01a23e51e018df4bc4196_medium.jpg)

6. **Έξυπνος θερμοστάτης**

Ένας θερμοστάτης μπορεί επίσης να είναι "*έξυπνος*", δηλαδή να εντάσσεται σε ένα Έξυπνο Σπίτι. Τέτοιες εφαρμογές IoT έχουν τη δυνατότητα να ρυθμίζουν δύο στοιχεία: θερμοκρασία και εξαερισμό, έτσι ώστε να επιτυγχάνεται το βέλτιστο αποτέλεσμα. Όπως παρατηρείται στην εικόνα 35, τέτοιες εφαρμογές τις χειρίζεται ο χρήστης μέσω κατάλληλης εφαρμογής στο κινητό.

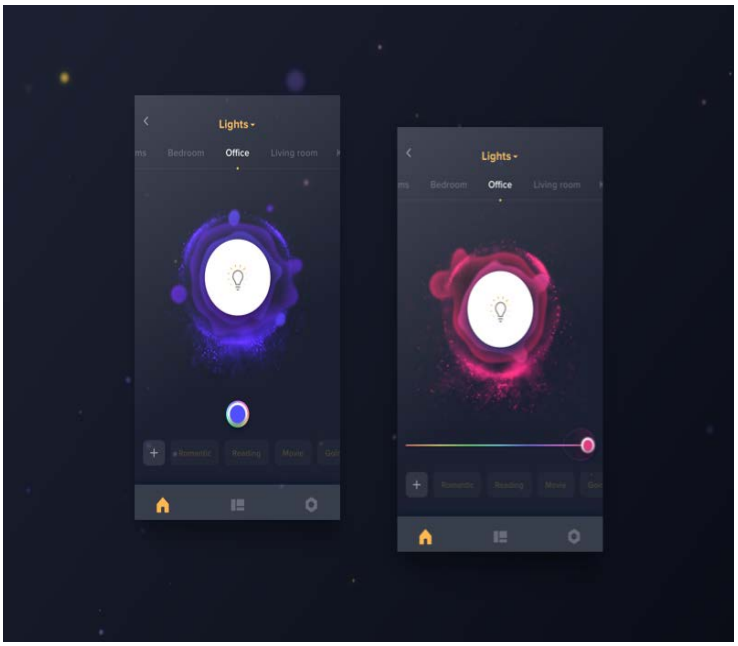
Εικόνα 35. Έξυπνος θερμοστάτης (https://www.smart-tech.gr/powertech-eksupnos-thermostatis-kalorifer-pt-782-wifi-touch-screen)

7. **Έξυπνος φωτισμός**

Η συγκεκριμένη εφαρμογή θεωρείται από τις πιο ενδιαφέρουσες που υπάρχουν στο Έξυπνο Σπίτι και τις επιδεχόμενες μεγαλύτερης εξέλιξης. Υπάρχουν δύο τρόποι ελέγχου και ρύθμισης του φωτισμού:

- Μέσω των επικοινωνιακών πρωτοκόλλων NFC.
- Μέσω των μετεωρολογικών φαινομένων και δεδομένων: στην προκειμένη περίπτωση, λαμβάνονται στοιχεία από τα νέφη και τον ουρανό

Οι εφαρμογές αυτές υπάρχουν σε συσκευές κινητών τηλεφώνων με Λειτουργικό Σύστημα Android και διακρίνονται στην παρακάτω εικόνα (Εικόνα 36).



Εικόνα 36. Έξυπνος φωτισμός (https://dribbble.com/shots/3432777-Smart-home-Lights-Control)

5.3 Αξιολόγηση Αντίκτυπου Προστασίας Δεδομένων (Data Protection Impact Assessment-DPIA)

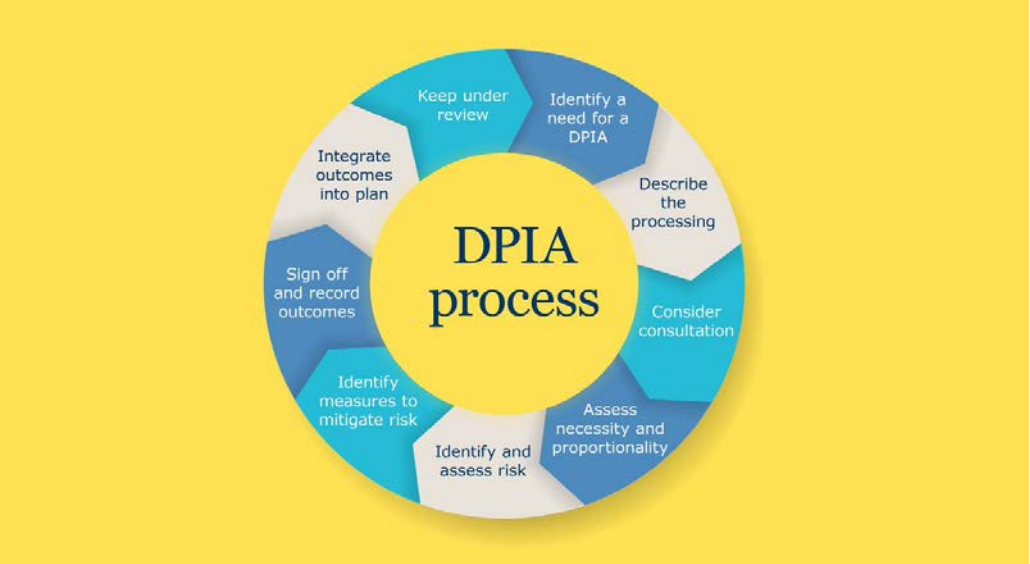
Στην παράγραφο αυτή, θα αναλυθεί η διαδικασία DPIA, η οποία και θα εφαρμοστεί στη συνέχεια στην εφαρμογή του Έξυπνου Σπιτιού, όπως περιεγράφηκε στα παραπάνω.

Η διαδικασία της Αξιολόγησης Αντίκτυπου Προστασίας Δεδομένων είναι μια διαδικασία που στοχεύει στην διασφάλιση των προσωπικών δεδομένων, τα οποία υπόκεινται σε επεξεργασία. Ένα τέτοιο είδος επεξεργασίας, το οποίο εγείρει κινδύνους προστασίας των προσωπικών δεδομένων, είναι σαφώς η επεξεργασία μέσω των εφαρμογών του Διαδικτύου των Πραγμάτων, όπως είναι το Έξυπνο Σπίτι.

Η εκτίμηση αντικτύπου ως προς την προστασία δεδομένων είναι μια μεθοδολογία που έχει τα ακόλουθα χαρακτηριστικά:

- Είναι δέουσα πρακτική η συγκεκριμένη μεθοδολογία, όταν υπάρχει έργο μεγάλης κλίμακας, στο οποίο πραγματοποιείται επεξεργασία προσωπικών δεδομένων υψηλής ευαισθησίας.

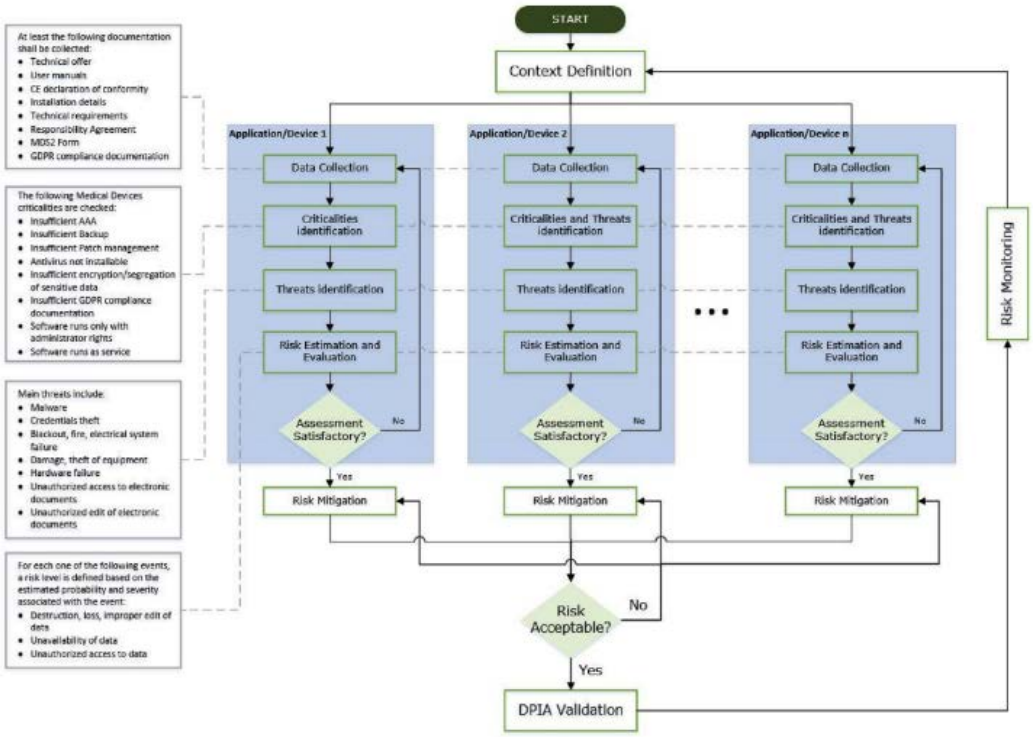
- Περιγράφεται στο έγγραφο ο χαρακτήρας, το εύρος, το συγκείμενο και οι στοχοθεσίες.
- Πρέπει στο πλαίσιο της μεθοδολογίας αυτής να γίνει αξιολόγηση της αναγκαιότητας και της αναλογικότητας των προτεινόμενων μέτρων καθώς και της συμμόρφωσης με τους νόμους και το κανονιστικό πλαίσιο.
- Η μεθοδολογία DPIA στοχεύει τόσο στην αναγνώριση και στην περιστολή σε ελάχιστο βαθμό των διάφορων κινδύνων που συνεπιφέρει ένα έργο σε ό,τι αφορά τα δεδομένα που εμπλέκονται με αυτό.
- Απαραίτητη κρίνεται η εφαρμογή της μεθοδολογίας αυτής σε περίπτωση πιθανότητας σημαντικής παραβίασης της προστασίας προσωπικών δεδομένων που συνεπιφέρουν ορισμένοι τύποι επεξεργασίας δεδομένων- με συνδυασμούς πιθανότητας και σοβαρότητας όπως: υψηλή πιθανότητα περιορισμένης ζημίας είτε και μικρότερη πιθανότητα πολύ αυξημένης ζημίας στα προσωπικά δεδομένα.
- Εφόσον υπάρχει σχετικός αξιωματούχος μέσα στα στελέχη που είναι εξειδικευμένος στην προστασία των δεδομένων (DPO – Data Protection Officer) θα πρέπει να λαμβάνεται και η δική του συμβουλή, καθώς και εάν χρειαστεί, από τρίτα μέρη εξειδικευμένα, καθώς και όσους θα επιφορτιστούν με την επεξεργασία των δεδομένων- αυτά ισχύουν ιδιαίτερα σε περίπτωση εκτίμησης υψηλού κινδύνου κατά μια ορισμένη μορφή επεξεργασίας.



Εικόνα 37. Διεργασία DPIA: διαδοχικά βήματα
(https://twitter.com/iconews/status/1103222464103006208)

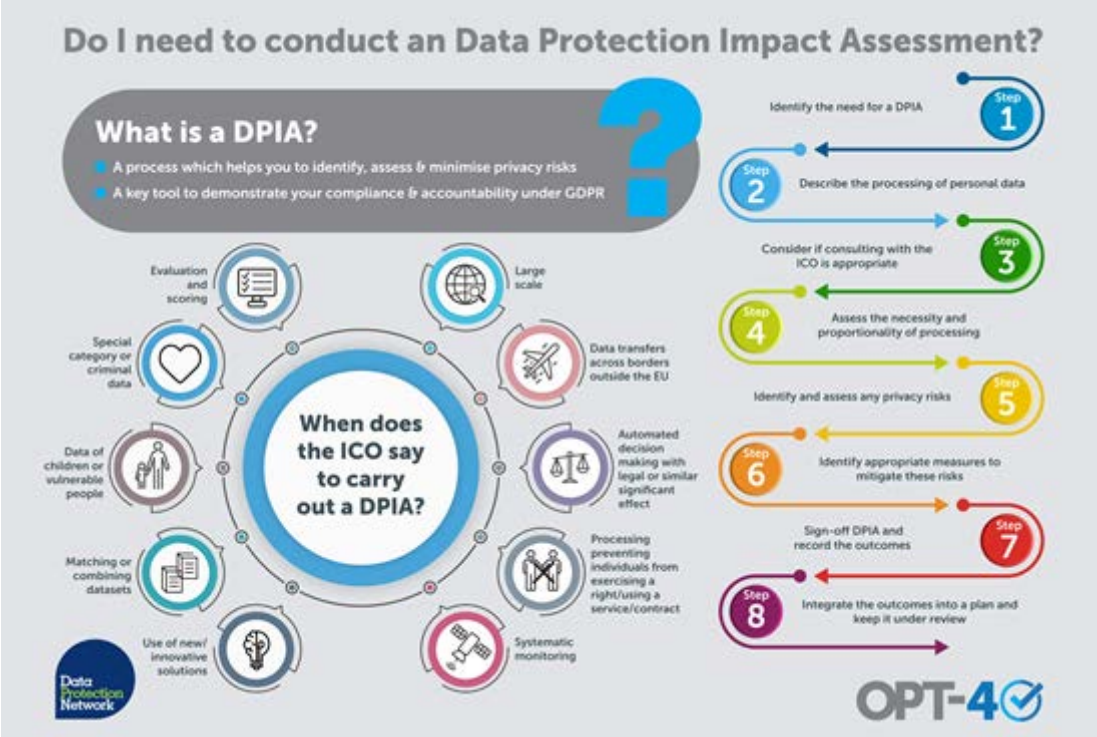
Συνολικά, αφού περατωθεί η εφαρμογή της συγκεκριμένης μεθοδολογίας, θα πρέπει να ληφθεί μια απόφαση, μετά από την αξιολόγηση που θα πραγματοποιήσει πιθανόν και το σχετικό επικεφαλής διοικητικό στέλεχος. Έτσι, μπορεί να υπάρχει η ακόλουθη έκβαση:

1. Να επιτραπεί η επεξεργασία των δεδομένων.
2. Να δοθεί επίσημη προειδοποίηση σχετικά με την επεξεργασία (μέρους ή της ολότητας) των δεδομένων.
3. Να απαγορευθεί εξολοκλήρου η επεξεργασία των δεδομένων.



Εικόνα 38. Εφαρμογή μεθοδολογίας DPIA σε πληροφοριακά συστήματα υγειονομικού ενδιαφέροντος (διάγραμμα ροής)

Η μεθοδολογία αυτή θα εφαρμοστεί, όπως ήδη αναφέρθηκε παραπάνω, στην εφαρμογή IoT του *Έξυπνου Σπιτιού*. Εισαγωγικά, χρήσιμη μπορεί να είναι για την κατανόηση της μεθοδολογίας αυτής πριν την τελική εφαρμογή της στην επιλεγμένη συσκευή IoT η παρακολούθηση ενός παραδείγματος εφαρμογής της σε μια άλλη περίπτωση. Σε μια πολύ πρόσφατη εργασία των (M. Todde et al., 2020), έχουμε μια ανάλυση που αφορά τα ιδρύματα που σχετίζονται με ιατρική περίθαλψη.



Εικόνα 39. Ορισμός και προϋποθέσεις διεξαγωγής της Αξιολόγησης Αντικτύπου Προστασίας Δεδομένων (https://dpnetwork.org.uk/wp-content/uploads/2019/08/bbb-2.jpg)

Κρίσιμα στοιχεία για την εφαρμογή της μεθοδολογίας σε ένα ίδρυμα που έχει να κάνει με ιατρική περίθαλψη και που επομένως σχετίζεται με την επεξεργασία πληροφορίας υψηλής ευαισθησίας είναι τα ακόλουθα στοιχεία:

1) Αρχικά, καθορίζεται το συνολικό πρότυπο ασφαλείας το οποίο ακολουθείται από το ίδρυμα υγειονομικού ενδιαφέροντος.
2) Χρειάζεται, επομένως, να υπάρξει συμμόρφωση με διάφορες προϋποθέσεις, οι οποίες μπορεί να είναι τεχνολογικού, νομικού ή οργανωτικού χαρακτήρα και με αυτόν τον τρόπο να καθοριστεί το συνολικό πλαίσιο.

3) Στη συνέχεια, χρειάζεται να πραγματοποιηθεί μια ανάλυση κινδύνου για κάθε επιμέρους εφαρμογή και συσκευή που εμπεριέχεται στο σύστημα. Ειδικότερα, απαιτείται η συλλογή όλης της τεκμηρίωσης που είναι συναφής με κάθε παράγοντα κινδύνου στο πλαίσιο του συνολικού πληροφοριακού συστήματος.
4) Οριοθετείται ο βαθμός κινδύνου για κάθε παράγοντα ευπάθειας όσον αφορά την ασφάλεια των δεδομένων, που συνίσταται στη γνωστή τριάδα της ασφάλειας: Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα (C.I.A.) των δεδομένων, υπό την έννοια να προστατεύονται τα δικαιώματα και ελευθερίες των πολιτών που ορίζονται από το νόμο.
5) Τελικά, πραγματοποιείται μια συνολική αξιολόγηση, η οποία, εφόσον κριθεί ικανοποιητική, υπάρχει προχώρημα προς τα μέτρα αντιμετώπισης των απειλών ασφάλειας.

Τα παραπάνω συνοψίζουν τη διαδικασία. Κάτι που έχει ιδιαίτερη αξία είναι το πώς προσδιορίζεται η επεξεργασία των δεδομένων. Στην περίπτωση μιας υγειονομικού χαρακτήρα εφαρμογής, η επεξεργασία μπορεί να αφορά, π.χ. τα εξής:

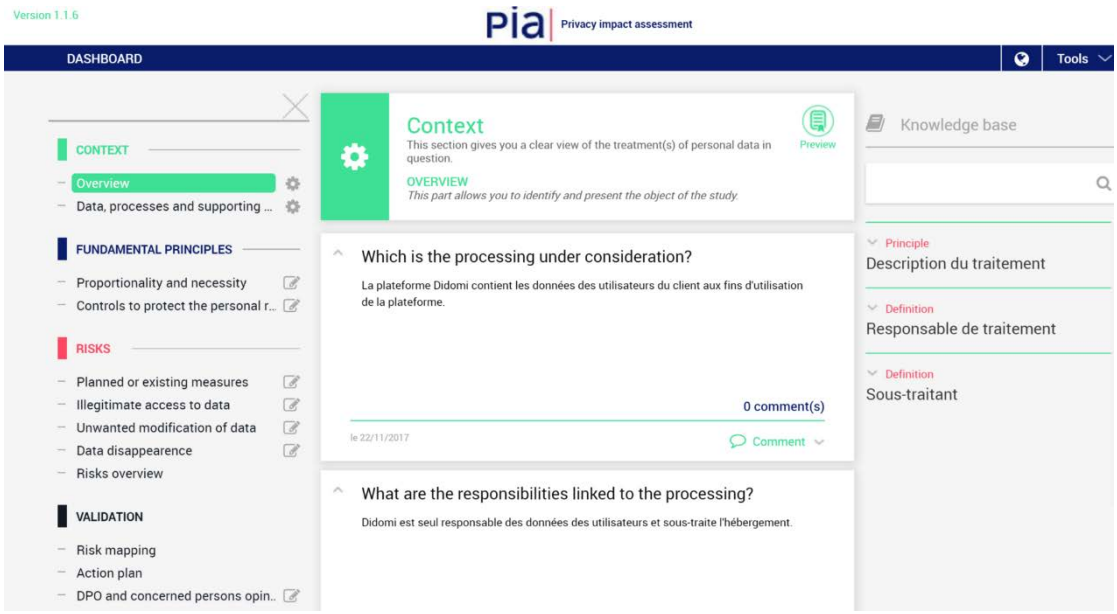
- Τη δρομολόγηση μιας συγκεκριμένης επιλογής περίθαλψης/φροντίδας υγείας.
- Τις διαδικασίες μιας περίθαλψης εκτός των εγκαταστάσεων της υγειονομικού ενδιαφέροντος μονάδας.
- Μια συγκεκριμένη διαγνωστική εξέταση που πραγματοποιείται για έναν ασθενή.

Πρέπει να επισημανθεί ότι η εκτίμηση αντικτύπου αποτελεί, κατά κάποιο τρόπο, κάτι ευρύτερο από μία διαχείριση κινδύνων ασφάλειας (security risk management): και αυτό γιατί εξετάζονται όχι μόνο κίνδυνοι ασφάλειας προσωπικών δεδομένων, αλλά και κίνδυνοι που άπτονται της ιδιωτικότητας και των νομικών απαιτήσεων του GDPR (όπως, π.χ. η διαφάνεια των σκοπών επεξεργασίας, αν είναι εφικτή η ικανοποίηση των δικαιωμάτων των χρηστών κ.λπ.).

5.4 Το εργαλείο PIA

Το εργαλείο PIA (Privacy Impact Assessment), το οποίο αξιοποιήθηκε στην έρευνά μας, είναι ένα εργαλείο δωρεάν και ανοιχτού κώδικα (open source/free software). Πρόκειται για ένα εργαλείο στο οποίο πολύ συστηματικά μπορούν να καταγραφούν όλα τα στοιχεία, οι προϋποθέσεις και τα χαρακτηριστικά της εφαρμογής, για την οποία

ενδιαφέρεται ο χρήστης της εφαρμογής να πραγματοποιήσει την αξιολόγηση. Ο σκοπός αυτού του μέρους της εργασίας είναι να υλοποιηθεί μια όσο γίνεται πλήρης και ενημερωμένη, βάσει αξιόπιστων πηγών και βιβλιογραφίας, καταγραφή των παραπάνω στοιχείων τα οποία είναι απαραίτητα για τη διεξαγωγή της αξιολόγησης. Στην παράγραφο αυτή, πραγματοποιείται μια σύντομη παρουσίαση του εργαλείου PIA, το οποίο έχει αναπτυχθεί, όπως προαναφέρθηκε, από την Αρχή Προστασίας Δεδομένων της Γαλλίας (βλ. https://www.cnil.fr/en/privacy-impact-assessment-pia).



Εικόνα 40. Dashboard του εργαλείου PIA

Το υπό μελέτη εργαλείο PIA έχει τα ακόλουθα βασικά χαρακτηριστικά.

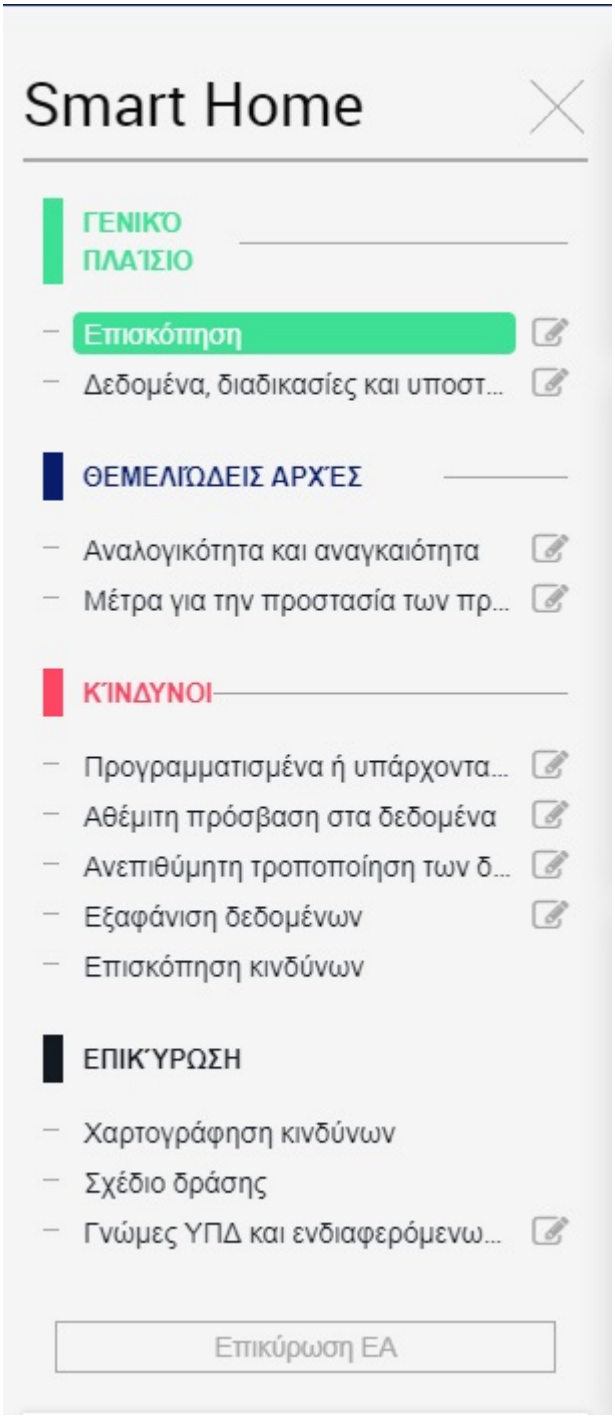
- Πρόκειται για μια διεπαφή που αναπτύχθηκε από την *Αρχή Προστασίας Δεδομένων* της Γαλλίας και επιτρέπει να υλοποιούνται οι *Αξιολογήσεις Αντικτύπου Ιδιωτικότητας* και να γίνεται η διαχείρισή τους με ένα απλό τρόπο. Το PIA παρέχει σειρά ειδικότερων εργαλείων μέσα από το interface του για να βοηθήσει στην καλύτερη κατανόηση των κινδύνων ιδιωτικότητας.
- Το εργαλείο είναι προσαρμοσμένο στην τρέχουσα πραγματικότητα σε ό,τι αφορά το νομικό πλαίσιο και την τεχνολογία. Έτσι, διασφαλίζεται η συμμόρφωση με το νομικό πλαίσιο και προστατεύονται αποτελεσματικά τα δικαιώματα όσων τα δεδομένα γίνονται αντικείμενο επεξεργασίας μέσα στην εφαρμογή που αξιολογείται. Ειδικότερα, μεταξύ άλλων ενσωματώνεται η

μεθοδολογία DPIA, καθώς βέβαια και η νέα Οδηγία της Ευρωπαϊκής Ένωσης GDPR (*General Data Protection Regulation*).

Το εργαλείο έχει μια σπονδυλωτή δομή. Ειδικότερα, επιτρέπει με ευελιξία τις ρυθμίσεις που θα εξυπηρετήσουν την κάθε διαφορετική περίπτωση, δηλαδή την εφαρμογή που θέλει να αξιολογήσει κάποιος.

5.5 Εφαρμογή Εκτίμησης Αντίκτυπου Προστασίας Δεδομένων (Data Protection Impact Assessment-DPIA)

Στη συγκεκριμένη παράγραφο, καταλήγει το τμήμα αυτό της εργασίας, που είναι η αμιγώς πρακτική εφαρμογή. Θα πρέπει να πραγματοποιηθεί ουσιαστικά η εφαρμογή της μεθοδολογίας Αξιολόγησης Αντικτύπου Προστασίας Δεδομένων (DPIA) στο αντίστοιχο εργαλείο, το οποίο μελετήθηκε στις παραπάνω σελίδες. Πρόκειται για το εργαλείο PIA, το οποίο παρέχει όλες τις αναγκαίες κατηγορίες αξιολόγησης οι οποίες επιτρέπουν την υλοποίηση μιας εμπεριστατωμένης και πλήρους αποτίμησης της ιδιωτικότητας της εφαρμογής smart home, η οποία πραγματοποιείται για λογαριασμό μιας φανταστικής, υποθετικής εταιρείας που υλοποιεί την αξιολόγηση για τους πελάτες της και για την προστασία της ιδιωτικότητας τους. Η αξιολόγηση που πραγματοποιείται σε αυτή την παράγραφο έχει ονομαστεί *"Smart Home"*. Στην εικόνα 41, διακρίνεται το σύνολο των βασικών κατηγοριών της αξιολόγησης. Αυτή ξεκινάει με την υπερκατηγορία *«Γενικό Πλαίσιο»* και την υποκατηγορία αυτής *«Επισκόπηση»*.



Εικόνα 41. Σύνολο βασικών Υπερκατηγοριών και Υποκατηγοριών, όπως πραγματοποιούνται στο εργαλείο PIA

Προκειμένου να πραγματοποιηθεί κατά το δυνατόν σωστότερο τρόπο η συμπλήρωση των πεδίων που αντιστοιχούν στη μεθοδολογία DPIA, χρειάζονται μια σειρά από διακριτά στοιχεία. Ορισμένα από αυτά ήταν το αντικείμενο των προηγούμενων παραγράφων και έχουν να κάνουν τόσο με τη γνώση της μεθοδολογίας που θα εφαρμοστεί όσο παράλληλα και με το εργαλείο PIA και τον τρόπο που αυτό το υλοποιεί.

Ένα ακόμη στοιχείο είναι οπωσδήποτε οι εφαρμογές του Έξυπνου Σπιτιού, κάτι που επίσης διερευνήθηκε στις προηγούμενες παραγράφους. Ταυτόχρονα, όμως, χρειάζεται μια γνώση του τρόπου που η εφαρμογή IoT του Έξυπνου Σπιτιού μπορεί να αξιολογηθεί μέσα από τη μεθοδολογία της Αξιολόγησης Αντικτύπου Ιδιωτικότητας. Για την προσέγγιση μιας τέτοιας προσπάθειας εντοπίστηκαν άρθρα και μελέτες δύο ειδών:

- Η πρώτη αξιολογεί με γενικότερο τρόπο την ιδιωτικότητα των εφαρμογών που απαρτίζουν το Smart Home (Basarudin, Yeon and Yusoff, 2018).
- Η δεύτερη είναι κατά πολύ πιο δυσεύρετη, εφόσον εισάγει ακόμη ένα κριτήριο: την υλοποίηση από το συντάκτη του άρθρου της μεθοδολογίας DPIA και μάλιστα στο Έξυπνο Σπίτι- τέτοιο άρθρο εντοπίστηκε στη διατριβή του (Tarekegn, 2016).

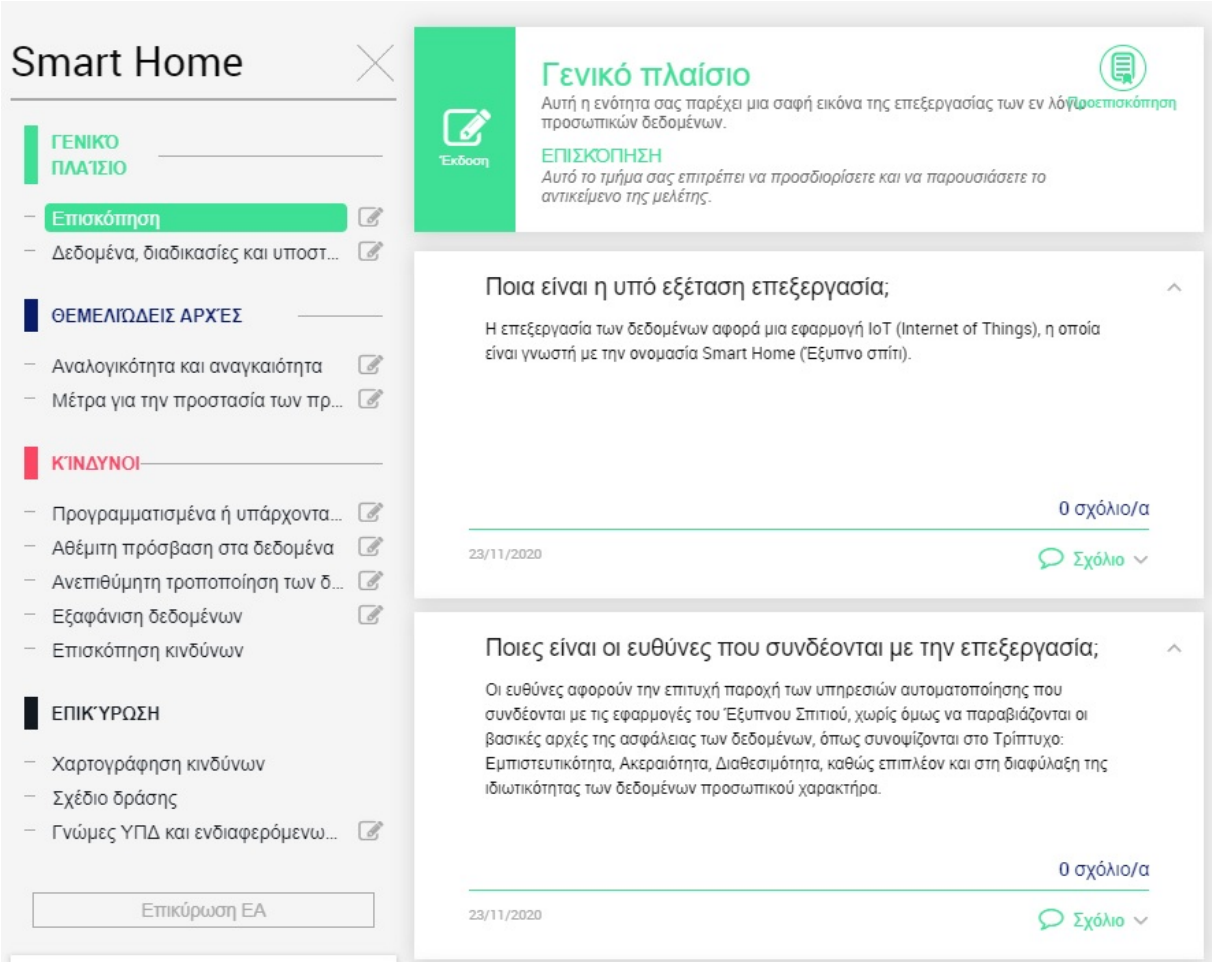
Στην εικόνα 42 διακρίνονται οι συμπληρώσεις των δύο πρώτων πεδίων του Γενικού Πλαισίου, όπου εξηγείται ποια είναι η επεξεργασία που είναι επιθυμητή (δηλαδή επεξεργασία δεδομένων), καθώς επίσης και ποιες είναι οι ευθύνες της επιχείρησης (που υποθετικά παρέχει υπηρεσίες *Έξυπνου Σπιτιού* για το IoT).

Έτσι, η απάντηση στην πρώτη ερώτηση είναι η ακόλουθη:

Η επεξεργασία των δεδομένων αφορά μια εφαρμογή IoT (Internet of Things), η οποία είναι γνωστή με την ονομασία Smart Home (Έξυπνο σπίτι).

Και η απάντηση στη δεύτερη ερώτηση είναι η εξής:

Οι ευθύνες αφορούν την επιτυχή παροχή των υπηρεσιών αυτοματοποίησης που συνδέονται με τις εφαρμογές του Έξυπνου Σπιτιού, χωρίς όμως να παραβιάζονται οι βασικές αρχές της ασφάλειας των δεδομένων, όπως συνοψίζονται στο Τρίπτυχο: Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα, καθώς επιπλέον και στη διαφύλαξη της ιδιωτικότητας των δεδομένων προσωπικού χαρακτήρα.

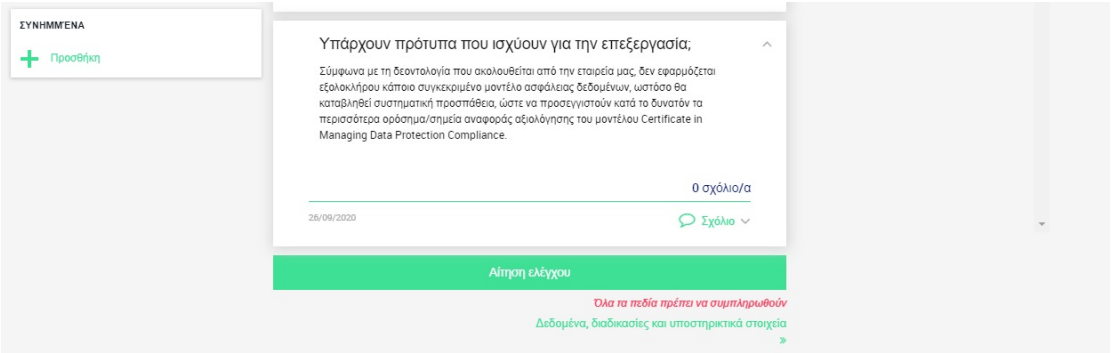


Εικόνα 42. Συμπλήρωση πρώτων στοιχείων Επισκόπησης Γενικού Πλαισίου για την PIA (Privacy Impact Assessment)

Τέλος, στο τρίτο πεδίο της Επισκόπησης, συμπληρώνεται το ακόλουθο κείμενο:

Σύμφωνα με τη δεοντολογία που ακολουθείται από την εταιρεία μας, δεν εφαρμόζεται εξολοκλήρου κάποιο συγκεκριμένο μοντέλο ασφάλειας δεδομένων, ωστόσο θα καταβληθεί συστηματική προσπάθεια, ώστε να προσεγγιστούν κατά το δυνατόν τα περισσότερα ορόσημα/σημεία αναφοράς αξιολόγησης του μοντέλου Certificate in Managing Data Protection Compliance.

Στη συνέχεια, διακρίνεται η αντίστοιχη εικόνα από το εργαλείο PIA.



Εικόνα 43. Συμπλήρωση τελικού στοιχείου Επισκόπησης στο εργαλείο PIA

Στην Υπερκατηγορία και πάλι *«Γενικό πλαίσιο»*, συνεχίζουμε με το δεύτερο πεδίο με τον τίτλο *«Δεδομένα, διαδικασίες και υποστηρικτικά στοιχεία»*. Στο πεδίο αυτό, πρέπει να συλλεγούν τα δεδομένα τα οποία υπόκεινται σε συλλογή, προκειμένου να υποστούν επεξεργασία.

Η επόμενη υποκατηγορία συμπληρώνεται με κείμενο και σε οπτικό πλαίσιο που διακρίνεται παρακάτω.

Τα δεδομένα που υφίστανται επεξεργασία είναι δεδομένα που απαιτούνται για τη λειτουργία της κάθε έξυπνης συσκευής, όπως περιγράφονται στη συνέχεια.

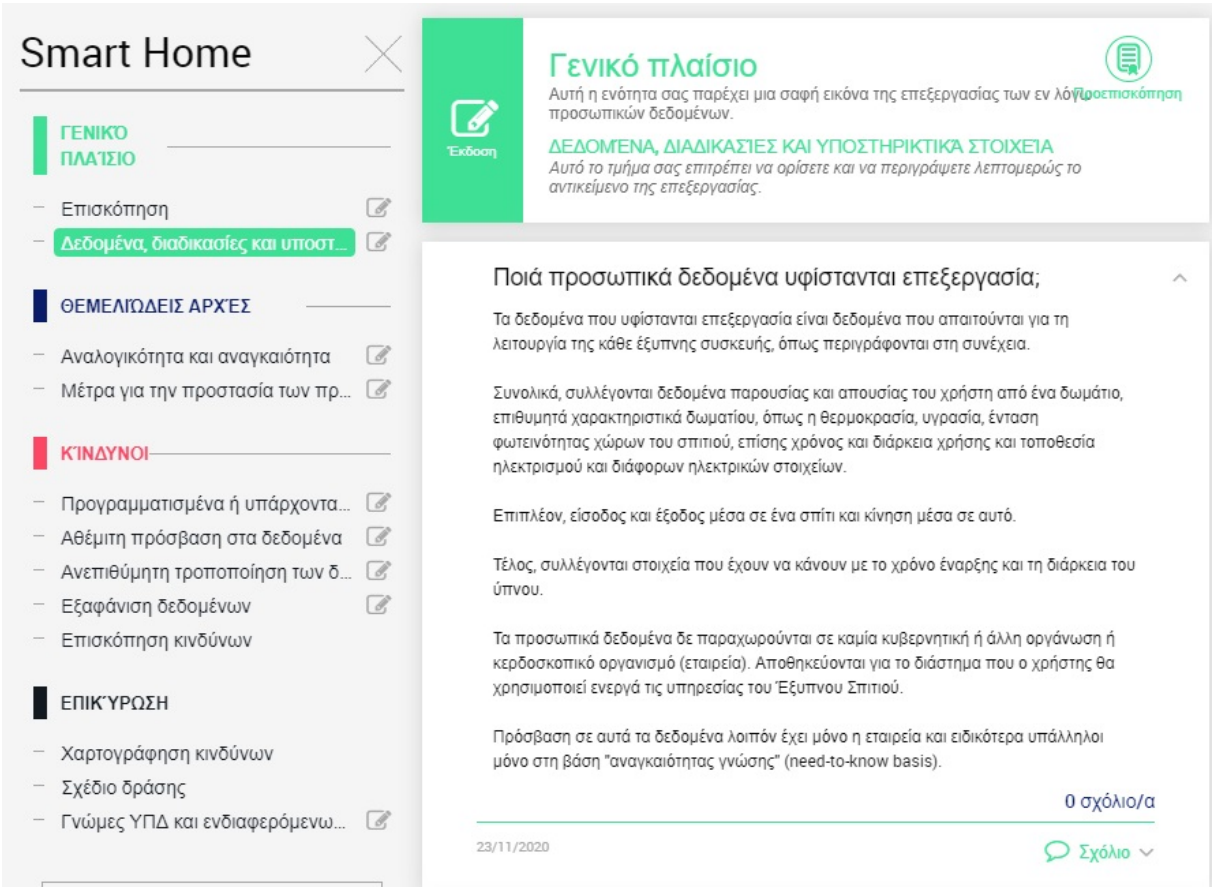
Συνολικά, συλλέγονται δεδομένα παρουσίας και απουσίας του χρήστη από ένα δωμάτιο, επιθυμητά χαρακτηριστικά δωματίου, όπως η θερμοκρασία, υγρασία, ένταση φωτεινότητας χώρων του σπιτιού, επίσης χρόνος και διάρκεια χρήσης και τοποθεσία ηλεκτρισμού και διάφορων ηλεκτρικών στοιχείων.

Επιπλέον, είσοδος και έξοδος μέσα σε ένα σπίτι και κίνηση μέσα σε αυτό.

Τέλος, συλλέγονται στοιχεία που έχουν να κάνουν με το χρόνο έναρξης και τη διάρκεια του ύπνου.

Τα προσωπικά δεδομένα δε παραχωρούνται σε καμία κυβερνητική ή άλλη οργάνωση ή κερδοσκοπικό οργανισμό (εταιρεία). Αποθηκεύονται για το διάστημα που ο χρήστης θα χρησιμοποιεί ενεργά τις υπηρεσίας του Έξυπνου Σπιτιού.

Πρόσβαση σε αυτά τα δεδομένα λοιπόν έχει μόνο η εταιρεία και ειδικότερα υπάλληλοι μόνο στη βάση "αναγκαιότητας γνώσης" (need-to-know basis).



Εικόνα 44. Προσωπικά δεδομένα που υφίστανται επεξεργασία- απεικόνιση

Η επόμενη ερώτηση έχει να κάνει με τον κύκλο ζωής των δεδομένων και διαδικασιών (data lifecycle). Η απάντηση, όπως και το σχετικό στιγμιότυπο οθόνης, δίνεται παρακάτω.

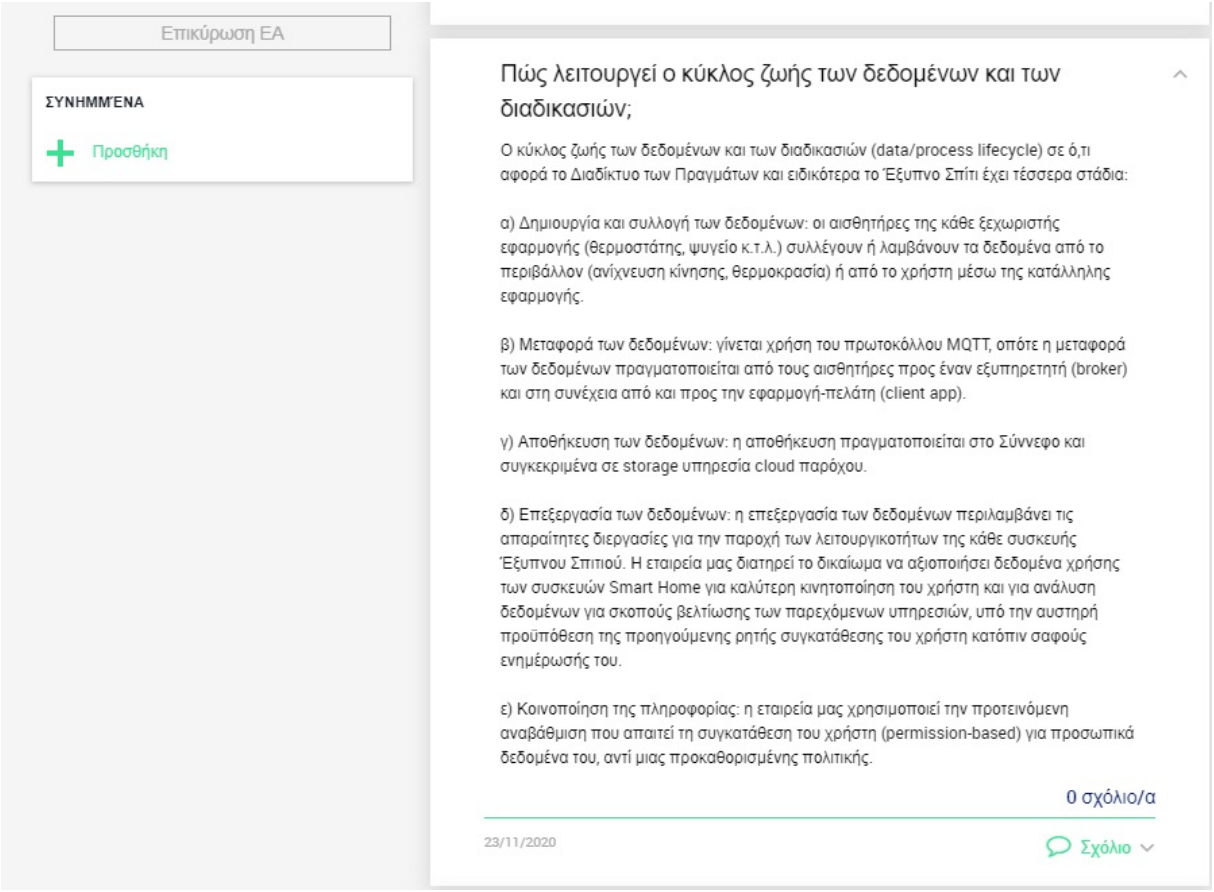
Ο κύκλος ζωής των δεδομένων και των διαδικασιών (data/process lifecycle) σε ό,τι αφορά το Διαδίκτυο των Πραγμάτων και ειδικότερα το Έξυπνο Σπίτι έχει τέσσερα στάδια: α) δημιουργία και συλλογή των δεδομένων: οι αισθητήρες της κάθε ξεχωριστής εφαρμογής (θερμοστάτης, ψυγείο κ.τ.λ.) συλλέγουν ή λαμβάνουν τα δεδομένα από το περιβάλλον (ανίχνευση κίνησης, θερμοκρασία) ή από το χρήστη μέσω της κατάλληλης εφαρμογής

β) μεταφορά των δεδομένων: γίνεται χρήση του πρωτοκόλλου MQTT, οπότε η μεταφορά των δεδομένων πραγματοποιείται από τους αισθητήρες προς έναν εξυπηρετητή (broker) και στη συνέχεια από και προς την εφαρμογή-πελάτη (client app)

γ) αποθήκευση των δεδομένων: η αποθήκευση πραγματοποιείται στο Σύννεφο και συγκεκριμένα σε storage υπηρεσία cloud παρόχου.

δ) επεξεργασία των δεδομένων: η επεξεργασία των δεδομένων περιλαμβάνει τις απαραίτητες διεργασίες για την παροχή των λειτουργικοτήτων της κάθε συσκευής Έξυπνου Σπιτιού. Η εταιρεία μας διατηρεί το δικαίωμα να αξιοποιήσει δεδομένα χρήσης των συσκευών Smart Home για καλύτερη κινητοποίηση του χρήστη και για ανάλυση δεδομένων για σκοπούς βελτίωσης των παρεχόμενων υπηρεσιών, υπό την αυστηρή προϋπόθεση της προηγούμενης ρητής συγκατάθεσης του χρήστη κατόπιν σαφούς ενημέρωσής του.

ε) κοινοποίηση της πληροφορίας: η εταιρεία μας χρησιμοποιεί την προτεινόμενη αναβάθμιση που απαιτεί τη συγκατάθεση του χρήστη (permission-based) για προσωπικά δεδομένα του, αντί μιας προκαθορισμένης πολιτικής



Εικόνα 45. Κύκλος ζωής Δεδομένων/Διαδικασιών

Τέλος, σε ό,τι αφορά αυτή την κατηγορία, ζητούνται και καταχωρούνται τα στοιχεία υποστήριξης που αφορούν τα δεδομένα, από πρωτόκολλα έως επιχειρηματικές εφαρμογές. Το στιγμιότυπο οθόνης του PIA και η σχετική καταχώρηση δίνονται στη συνέχεια.

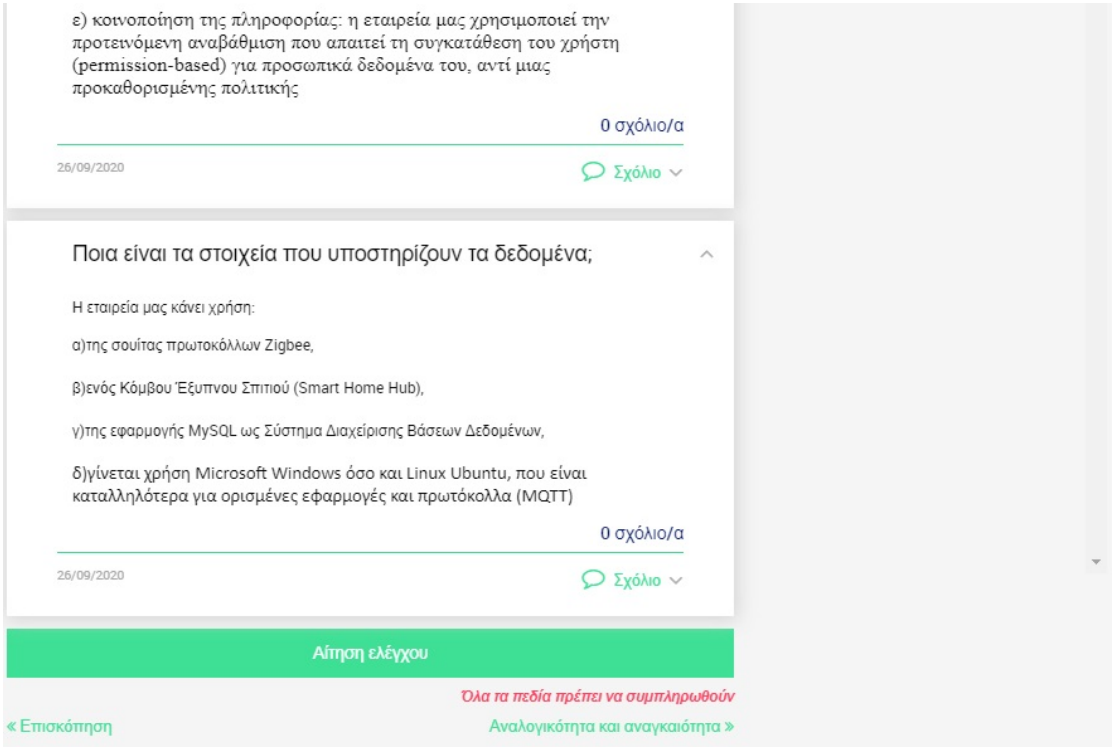
Η εταιρεία μας κάνει χρήση:

α) της σουίτας πρωτοκόλλων Zigbee,

β) ενός Κόμβου Έξυπνου Σπιτιού (Smart Home Hub),

γ) της εφαρμογής MySQL ως Σύστημα Διαχείρισης Βάσεων Δεδομένων,

δ) γίνεται χρήση Microsoft Windows όσο και Linux Ubuntu, που είναι καταλληλότερα για ορισμένες εφαρμογές και πρωτόκολλα (MQTT)



Εικόνα 46. Στοιχεία υποστήριξης Δεδομένων

Αφού ολοκληρώθηκε το Γενικό Πλαίσιο, στη συνέχεια συμπληρώνονται οι ***Θεμελιώδεις Αρχές***. Πρώτη αρχή είναι η ***Αναλογικότητα και Αναγκαιότητα***.

Στη συνέχεια δίνονται το στιγμιότυπο οθόνης του PIA για τα δύο πρώτα πεδία και οι αντίστοιχες καταχωρήσεις.

Είναι σαφείς, ρητοί και νόμιμοι οι σκοποί επεξεργασίας;

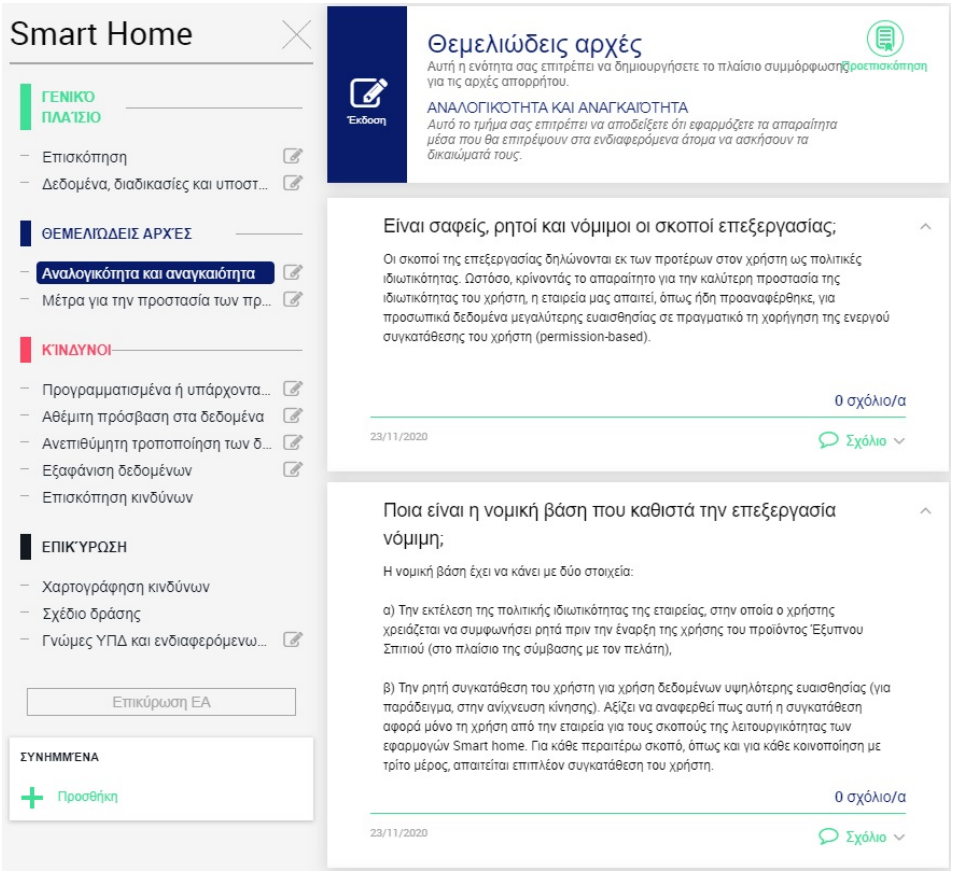
Οι σκοποί της επεξεργασίας δηλώνονται εκ των προτέρων στον χρήστη ως πολιτικές ιδιωτικότητας. Ωστόσο, κρίνοντάς το απαραίτητο για την καλύτερη προστασία της ιδιωτικότητας του χρήστη, η εταιρεία μας απαιτεί, όπως ήδη προαναφέρθηκε, για προσωπικά δεδομένα μεγαλύτερης ευαισθησίας σε πραγματικό τη χορήγηση της ενεργού συγκατάθεσης του χρήστη (permission-based).

Ποια είναι η νομική βάση που καθιστά την επεξεργασία νόμιμη;

Η νομική βάση έχει να κάνει με δύο στοιχεία:

α) την εκτέλεση της ***πολιτικής ιδιωτικότητας*** *της εταιρείας, στην οποία ο χρήστης χρειάζεται να συμφωνήσει ρητά πριν την έναρξη της χρήσης του προϊόντος Έξυπνου Σπιτιού (στο πλαίσιο της σύμβασης με τον πελάτη),*

β) την ***ρητή συγκατάθεση*** *του χρήστη για χρήση δεδομένων υψηλότερης ευαισθησίας (για παράδειγμα, στην ανίχνευση κίνησης). Αξίζει να αναφερθεί πως αυτή η συγκατάθεση αφορά μόνο τη χρήση από την εταιρεία για τους σκοπούς της λειτουργικότητας των εφαρμογών Smart home. Για κάθε περαιτέρω σκοπό, όπως και για κάθε κοινοποίηση με τρίτο μέρος, απαιτείται επιπλέον συγκατάθεση του χρήστη.*



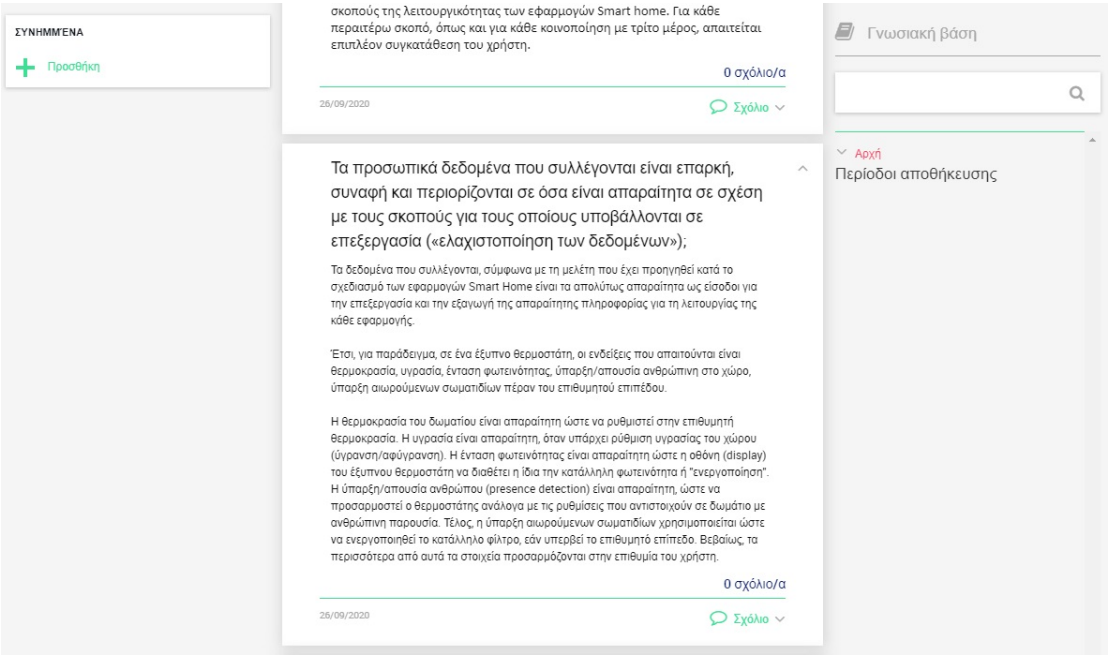
Εικόνα 47. Αναλογικότητα και Αναγκαιότητα- 1

Τα προσωπικά δεδομένα που συλλέγονται είναι επαρκή, συναφή και περιορίζονται σε όσα είναι απαραίτητα σε σχέση με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»);

Τα δεδομένα που συλλέγονται, σύμφωνα με τη μελέτη που έχει προηγηθεί κατά το σχεδιασμό των εφαρμογών Smart Home είναι τα απολύτως απαραίτητα ως είσοδοι για την επεξεργασία και την εξαγωγή της απαραίτητης πληροφορίας για τη λειτουργίας της κάθε εφαρμογής.

Έτσι, για παράδειγμα, σε ένα έξυπνο θερμοστάτη, οι ενδείξεις που απαιτούνται είναι θερμοκρασία, υγρασία, ένταση φωτεινότητας, ύπαρξη/απουσία ανθρώπινη στο χώρο, ύπαρξη αιωρούμενων σωματιδίων πέραν του επιθυμητού επιπέδου.

*Η **θερμοκρασία** του δωματίου είναι απαραίτητη ώστε να ρυθμιστεί στην επιθυμητή θερμοκρασία. Η **υγρασία** είναι απαραίτητη, όταν υπάρχει ρύθμιση υγρασίας του χώρου (ύγρανση/αφύγρανση). Η **ένταση φωτεινότητας** είναι απαραίτητη ώστε η οθόνη (display) του έξυπνου θερμοστάτη να διαθέτει η ίδια την κατάλληλη φωτεινότητα ή "ενεργοποίηση". Η **ύπαρξη/απουσία ανθρώπου (presence detection)** είναι απαραίτητη, ώστε να προσαρμοστεί ο θερμοστάτης ανάλογα με τις ρυθμίσεις που αντιστοιχούν σε δωμάτιο με ανθρώπινη παρουσία. Τέλος, η **ύπαρξη αιωρούμενων σωματιδίων** χρησιμοποιείται ώστε να ενεργοποιηθεί το κατάλληλο φίλτρο, εάν υπερβεί το επιθυμητό επίπεδο. Βεβαίως, τα περισσότερα από αυτά τα στοιχεία προσαρμόζονται στην επιθυμία του χρήστη.*



Εικόνα 48. Ελαχιστοποίηση των Δεδομένων

Όλα τ' ανωτέρω δεδομένα είναι συσχετισμένα με τον κάθε πελάτη (χρήστη υπηρεσιών) προσωποποιημένα, βάσει των στοιχείων του που τηρούνται με τη σύμβασή του.

Τα δεδομένα είναι ακριβή και ενημερωμένα;

Η ακρίβεια και η ενημέρωση των δεδομένων είναι συνιστώσες της ποιότητας των δεδομένων (data quality), για τη διασφάλιση της οποίας η εταιρεία μας κάνει χρήση μεθόδους καθαρισμού των δεδομένων (data cleaning). Αυτές οι μέθοδοι εξαλείφουν σε μεγάλο βαθμό τις ασυνέπειες, τις ακραίες τιμές (outliers) και διασφαλίζουν την ταχύτητα της ενημέρωσης και την ακρίβεια των παρουσιαζόμενων ενδείξεων προς το χρήστη.

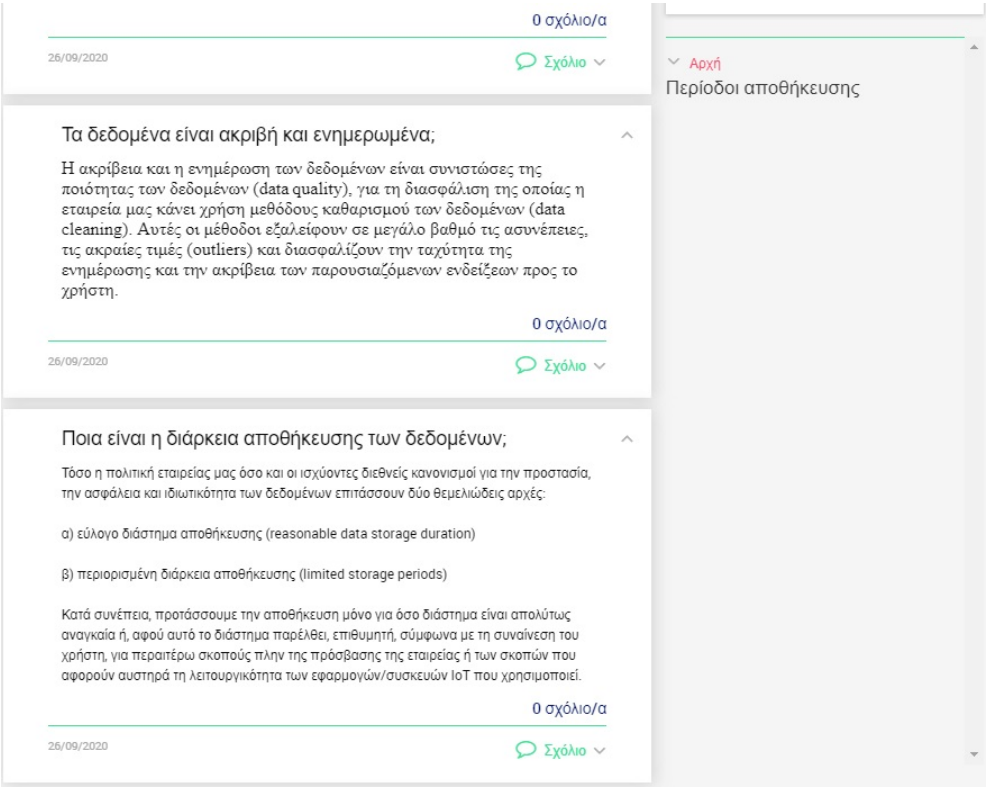
Ποια είναι η διάρκεια αποθήκευσης των δεδομένων;

Τόσο η πολιτική εταιρείας μας όσο και οι ισχύοντες διεθνείς κανονισμοί για την προστασία, την ασφάλεια και ιδιωτικότητα των δεδομένων επιτάσσουν δύο θεμελιώδεις αρχές:

α) εύλογο διάστημα αποθήκευσης (reasonable data storage duration)

β) περιορισμένη διάρκεια αποθήκευσης (limited storage periods)

Κατά συνέπεια, προτάσσουμε την αποθήκευση μόνο για όσο διάστημα είναι απολύτως αναγκαία ή, αφού αυτό το διάστημα παρέλθει, επιθυμητή, σύμφωνα με τη συναίνεση του χρήστη, για περαιτέρω σκοπούς πλην της πρόσβασης της εταιρείας ή των σκοπών που αφορούν αυστηρά τη λειτουργικότητα των εφαρμογών/συσκευών IoT που χρησιμοποιεί.



Εικόνα 49. Ποιότητα Δεδομένων και Διάρκεια Αποθήκευσης Δεδομένων

Εν συνεχεία, περνάμε στη δεύτερη Θεμελιώδη Αρχή, που είναι τα *«Μέτρα για την προστασία των προσωπικών δικαιωμάτων των υποκειμένων των δεδομένων»*.

Τα πρώτα δύο μέτρα έχουν να κάνουν με την ενημέρωση των υποκειμένων των δεδομένων καθώς και την επίτευξη της συγκατάθεσής τους για την επεξεργασία.

Πώς ενημερώνονται τα υποκείμενα των δεδομένων σχετικά με την επεξεργασία;

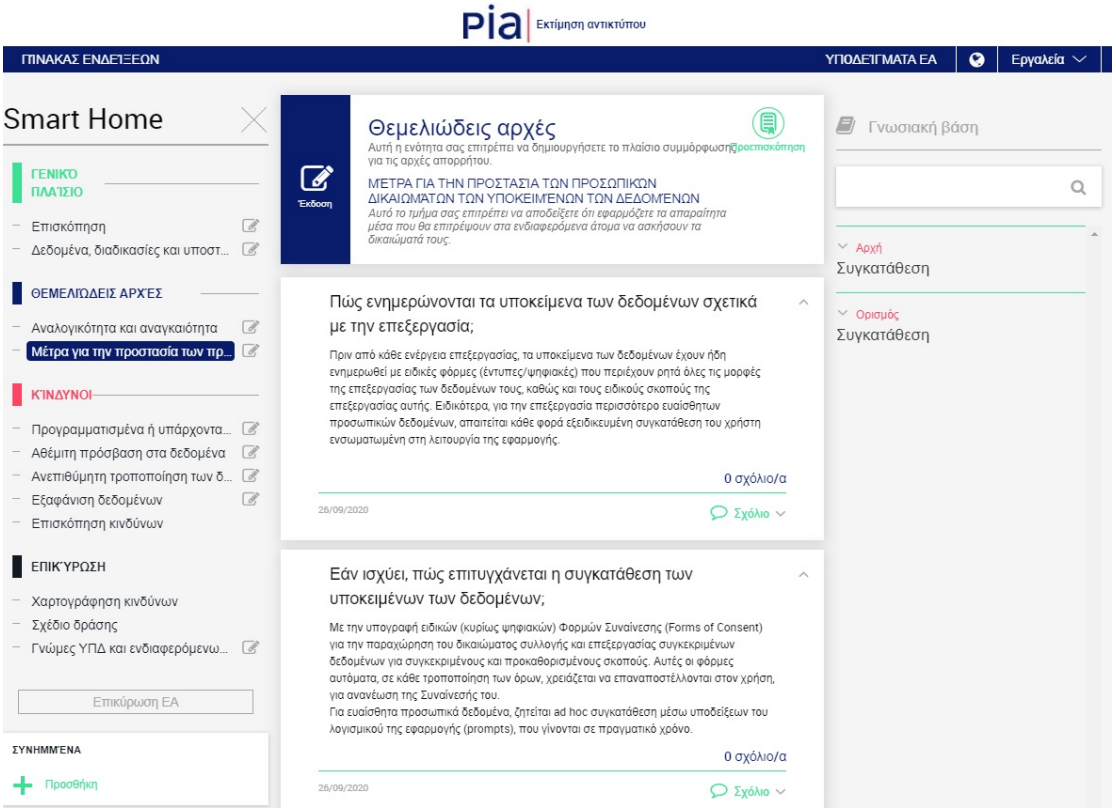
Πριν από κάθε ενέργεια επεξεργασίας, τα υποκείμενα των δεδομένων έχουν ήδη ενημερωθεί με ειδικές φόρμες (έντυπες/ψηφιακές) που περιέχουν ρητά όλες τις μορφές της επεξεργασίας των δεδομένων τους, καθώς και τους ειδικούς σκοπούς της επεξεργασίας αυτής. Ειδικότερα, για την επεξεργασία περισσότερο ευαίσθητων προσωπικών δεδομένων, απαιτείται κάθε φορά εξειδικευμένη συγκατάθεση του χρήστη ενσωματωμένη στη λειτουργία της εφαρμογής.

Εάν ισχύει, πώς επιτυγχάνεται η συγκατάθεση των υποκειμένων των δεδομένων;

Με την υπογραφή ειδικών (κυρίως ψηφιακών) Φορμών Συναίνεσης (Forms of Consent) για την παραχώρηση του δικαιώματος συλλογής και επεξεργασίας συγκεκριμένων δεδομένων για συγκεκριμένους και προκαθορισμένους σκοπούς. Αυτές οι φόρμες

αυτόματα, σε κάθε τροποποίηση των όρων, χρειάζεται να επαναποστέλλονται στον χρήση, για ανανέωση της Συναίνεσής του.

Για ευαίσθητα προσωπικά δεδομένα, ζητείται ad hoc συγκατάθεση μέσω υποδείξεων του λογισμικού της εφαρμογής (prompts), που γίνονται σε πραγματικό χρόνο.



Εικόνα 50. Ενημέρωση Υποκειμένων Δεδομένων και Επίτευξη Συγκατάθεσης Υποκειμένων Δεδομένων

Πώς μπορούν τα υποκείμενα δεδομένων να ασκήσουν τα δικαιώματά τους πρόσβασης και φορητότητας προσωπικών δεδομένων;

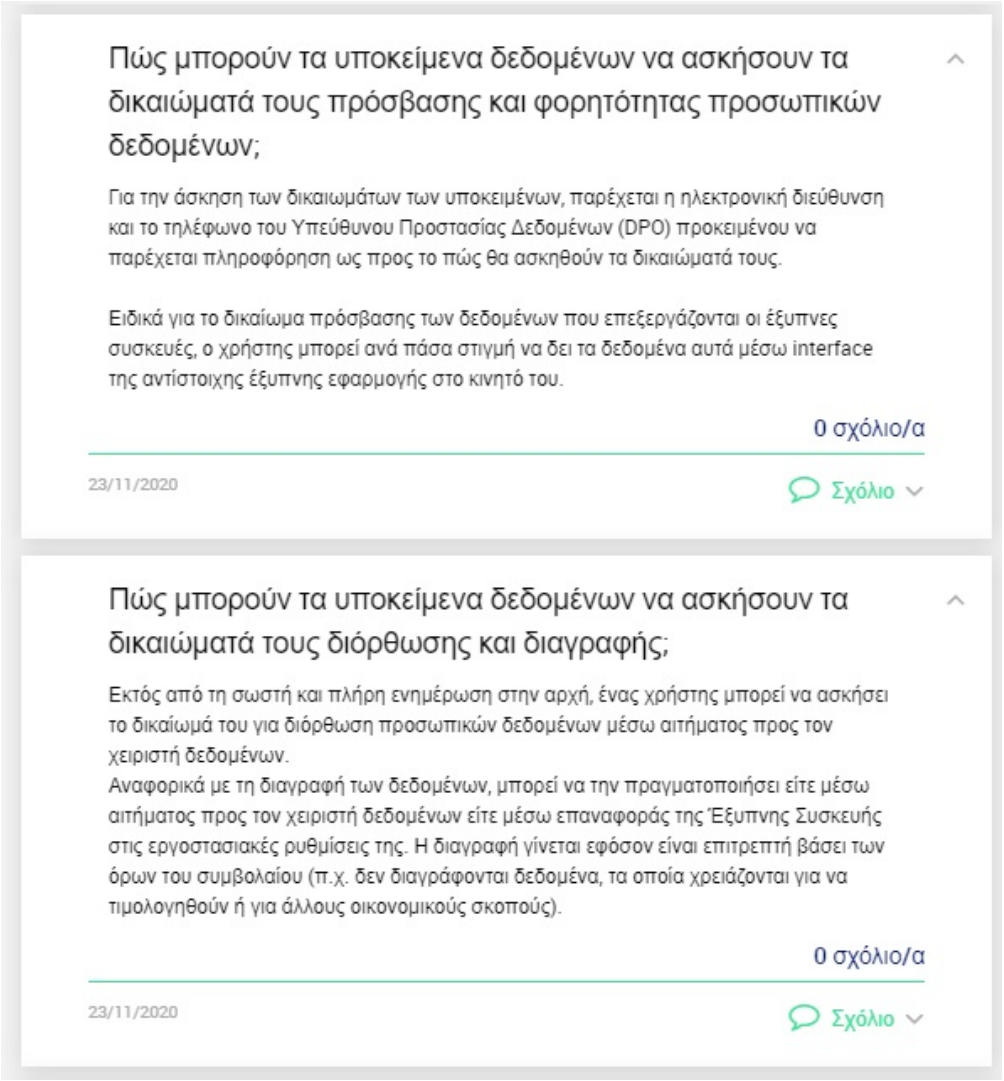
Για την άσκηση των δικαιωμάτων των υποκειμένων, παρέχεται η ηλεκτρονική διεύθυνση και το τηλέφωνο του Υπεύθυνου Προστασίας Δεδομένων (DPO) προκειμένου να παρέχεται πληροφόρηση ως προς το πώς θα ασκηθούν τα δικαιώματά τους.

Ειδικά για το δικαίωμα πρόσβασης των δεδομένων που επεξεργάζονται οι έξυπνες συσκευές, ο χρήστης μπορεί ανά πάσα στιγμή να δει τα δεδομένα αυτά μέσω interface της αντίστοιχης έξυπνης εφαρμογής στο κινητό του.

Πώς μπορούν τα υποκείμενα δεδομένων να ασκήσουν τα δικαιώματά τους διόρθωσης και διαγραφής;

Εκτός από τη σωστή και πλήρη ενημέρωση στην αρχή, ένας χρήστης μπορεί να ασκήσει το δικαίωμά του για διόρθωση προσωπικών δεδομένων μέσω αιτήματος προς τον χειριστή δεδομένων.

Αναφορικά με τη διαγραφή των δεδομένων, μπορεί να την πραγματοποιήσει είτε μέσω αιτήματος προς τον χειριστή δεδομένων είτε μέσω επαναφοράς της Έξυπνης Συσκευής στις εργοστασιακές ρυθμίσεις της. Η διαγραφή γίνεται εφόσον είναι επιτρεπτή βάσει των όρων του συμβολαίου (π.χ. δεν διαγράφονται δεδομένα τα οποία χρειάζονται για να τιμολογηθούν ή για άλλους οικονομικούς σκοπούς).



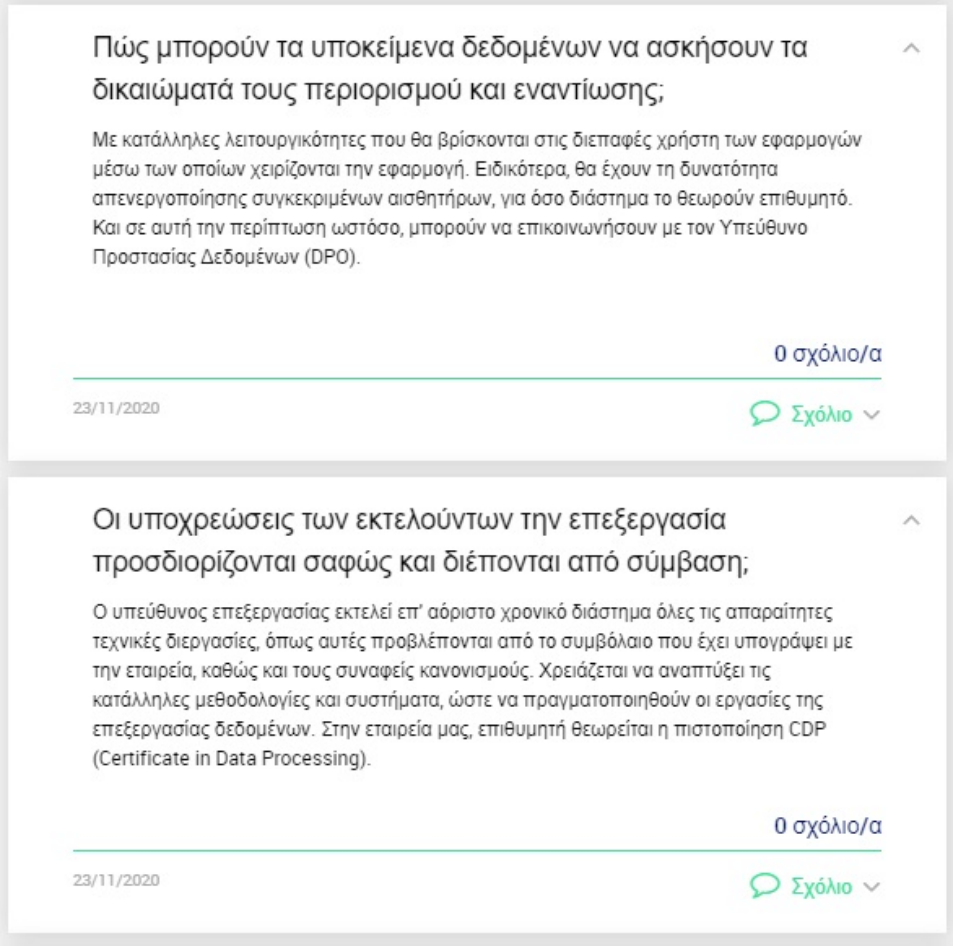
Εικόνα 51. Άσκηση δικαιωμάτων πρόσβασης και φορητότητας, διόρθωσης και διαγραφής δεδομένων

Πώς μπορούν τα υποκείμενα δεδομένων να ασκήσουν τα δικαιώματά τους περιορισμού και εναντίωσης;

Με κατάλληλες λειτουργικότητες που θα βρίσκονται στις διεπαφές χρήστη των εφαρμογών μέσω των οποίων χειρίζονται την εφαρμογή. Ειδικότερα, θα έχουν τη δυνατότητα απενεργοποίησης συγκεκριμένων αισθητήρων, για όσο διάστημα το θεωρούν επιθυμητό. Και σε αυτή την περίπτωση ωστόσο, μπορούν να επικοινωνήσουν με τον Υπεύθυνο Προστασίας Δεδομένων (DPO).

Οι υποχρεώσεις των εκτελούντων την επεξεργασία προσδιορίζονται σαφώς και διέπονται από σύμβαση;

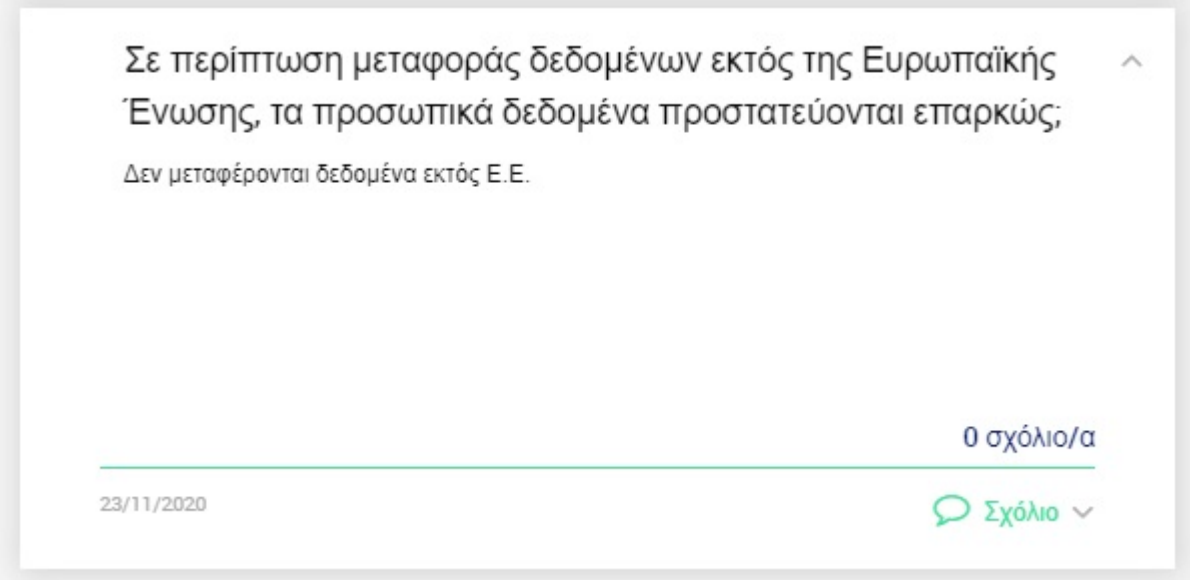
Ο υπεύθυνος επεξεργασίας εκτελεί επί αόριστο χρονικό διάστημα όλες τις απαραίτητες τεχνικές διεργασίες, όπως αυτές προβλέπονται από το συμβόλαιο που έχει υπογράψει με την εταιρεία, καθώς και τους συναφείς κανονισμούς. Χρειάζεται να αναπτύξει τις κατάλληλες μεθοδολογίες και συστήματα, ώστε να πραγματοποιηθούν οι εργασίες της επεξεργασίας δεδομένων. Στην εταιρεία μας, επιθυμητή θεωρείται η πιστοποίηση CDP (Certificate in Data Processing).



Εικόνα 52. Άσκηση δικαιωμάτων περιορισμού επεξεργασίας και εναντίωσης, καθορισμός υποχρεώσεων επεξεργαστή δεδομένων

Σε περίπτωση μεταφοράς δεδομένων εκτός της Ευρωπαϊκής Ένωσης, τα προσωπικά δεδομένα προστατεύονται επαρκώς;

Δεν μεταφέρονται δεδομένα εκτός Ε.Ε.



Εικόνα 53. Διασφάλιση προστασίας δεδομένων εκτός χωρών Ε.Ε.

Στο σημείο αυτό ολοκληρώνεται το συγκεκριμένο στάδιο της PIA μέσω του ομώνυμου εργαλείου και για το δεύτερο στάδιο και περνάμε στο τρίτο τμήμα, που αφορά τη χαρτογράφηση και καταγραφή των κινδύνων.

Στη συνέχεια, περνάει η υλοποίηση της μεθοδολογίας DPIA στην καταγραφή των Κινδύνων και των παραμέτρων τους. Εκ προοιμίου αναφέρεται ότι σε ό,τι αφορά την καταγραφή ασφάλειας που έχει πραγματοποιηθεί από την ENISA (Ταξινόμηση Απειλών), συναντάμε τα ακόλουθα στοιχεία (Baseline Security Recommendations for IoT, 2017):

- Διαρροή ευαίσθητων δεδομένων[2]
- Αποτυχίες τρίτων μερών (Υπηρεσίες ύδρευσης, ρεύματος, φ. Αερίου)
- Εγκατάσταση κακόβουλου λογισμικού
- Τροποποίηση πληροφορίας

[2] Η διαρροή των ευαίσθητων δεδομένων θα μπορούσε να πραγματοποιηθεί με πολλούς τρόπους. Ένας τρόπος θα ήταν η παραβίαση της εμπιστευτικότητας από δημόσιες εταιρείες παροχής ύδρευσης και άλλες παρόμοιες. Δεύτερος τρόπος είναι η παραβίαση της εξουσιοδότησης μέσα στην εταιρεία. Εάν ιδιαίτερα υποτεθεί ότι ο Αντίπαλος που επιχειρεί την παραβίαση της ιδιωτικότητας βρίσκεται εντός της εταιρείας, τότε μπορεί να με διάφορες επιθέσεις (Man In The Middle κ.ά.) να προβαίνει σε Υποκλοπή των Δεδομένων, με συνέπεια την παραβίαση της εμπιστευτικότητας και της ιδιωτικότητας και σε αυτή την περίπτωση.

- Υποκλοπή πληροφοριών

Επιλέξαμε, λοιπόν, να λάβουμε υπόψιν τους κινδύνους που περιγράφει ο οργανισμός ENISA, το αρμόδιο όργανο της Ευρωπαϊκής Ένωσης για την κυβερνοασφάλεια, προκειμένου να γίνει εκτίμηση αντικτύπου ως προς την ασφάλεια της επεξεργασίας μας. Παρακάτω αποτυπώνονται τα μέτρα ασφαλείας που λαμβάνονται για την αντιμετώπιση των κινδύνων:

Κρυπτογράφηση:

Οι συσκευές IoT θα μεταδίδουν κρυπτογραφημένα δεδομένα και το άκρο του δικτύου θα αποκρυπτογραφεί μηνύματα χρησιμοποιώντας ένα κοινόχρηστο μυστικό κλειδί.

Ψευδωνυμοποίηση:

Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα για σκοπούς στατιστικής ανάλυσης, θα γίνεται με τέτοιο τρόπο, ώστε τα δεδομένα να μην μπορούν πλέον ν' αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο.

Διαχωρισμός προσωπικών δεδομένων:

Μέθοδος οργάνωσης δεδομένων που μειώνει την πιθανότητα συσχέτισης των προσωπικών δεδομένων και παραβίασης όλων των προσωπικών δεδομένων. Για παράδειγμα, με το να προσδιοριστούν τα προσωπικά δεδομένα που είναι χρήσιμα μόνο για την κάθε επιχειρηματική διαδικασία και με το να διαχωριστούν αυτά λογικά.

Εφαρμογή πολιτικής για χρήση ισχυρού κωδικού ταυτοποίησης χρήστη:

Οι κωδικοί πρόσβασης πρέπει ν' αποτελούνται από τουλάχιστον οκτώ χαρακτήρες, να ανανεώνονται εάν υπάρχει η ελάχιστη ανησυχία ότι ενδέχεται να έχουν τεθεί σε κίνδυνο και, ενδεχομένως, περιοδικά (κάθε έξι μήνες ή μία φορά το χρόνο) και να περιλαμβάνουν τουλάχιστον τρία από τα τέσσερα είδη χαρακτήρων (κεφαλαία γράμματα, μικρά γράμματα, αριθμούς και ειδικούς χαρακτήρες). Όταν αλλάξει ένας κωδικός πρόσβασης, οι

τελευταίοι πέντε κωδικοί πρόσβασης δεν επιτρέπεται να επαναχρησιμοποιηθούν. Ο ίδιος κωδικός πρόσβασης δεν πρέπει να χρησιμοποιείται για διαφορετικές προσβάσεις. Οι κωδικοί πρόσβασης δεν πρέπει να σχετίζονται με προσωπικά στοιχεία (συμπεριλαμβανομένου του ονόματος ή της ημερομηνίας γέννησης.).

Τακτική ενημέρωση των συσκευών του οικοσυστήματος του smart home:

Οι συσκευές θα πρέπει να ενημερώνονται τακτικά με την τελευταία έκδοση του λογισμικού τους, ώστε να καλύπτονται τυχόν κενά ασφαλείας τους.

Ασφάλεια δικτύου:

Καθορισμός τείχους προστασίας στη συσκευή, σύστημα ανίχνευσης εισβολών (IDS system) ή άλλων ενεργών/παθητικών βοηθημάτων που να ευθύνονται για την εξασφάλιση της ασφάλειας του δικτύου.

Καταστολή κακόβουλου λογισμικού:

Εφαρμόζεται σε σταθμούς εργασίας και διακομιστές για την προστασία τους από κακόβουλο λογισμικό κατά την πρόσβαση σε λιγότερο ασφαλή δίκτυα.

Σουίτα πρωτοκόλλων ZigBee:

Η Σουίτα Πρωτοκόλλων Zigbee θεωρείται ως μία από τις σειρές πρωτοκόλλων εκείνες που διασφαλίζουν το σύνολο των συνιστωσών που συναποτελούν την ασφάλεια δεδομένων:

α) εμπιστευτικότητα δεδομένων,

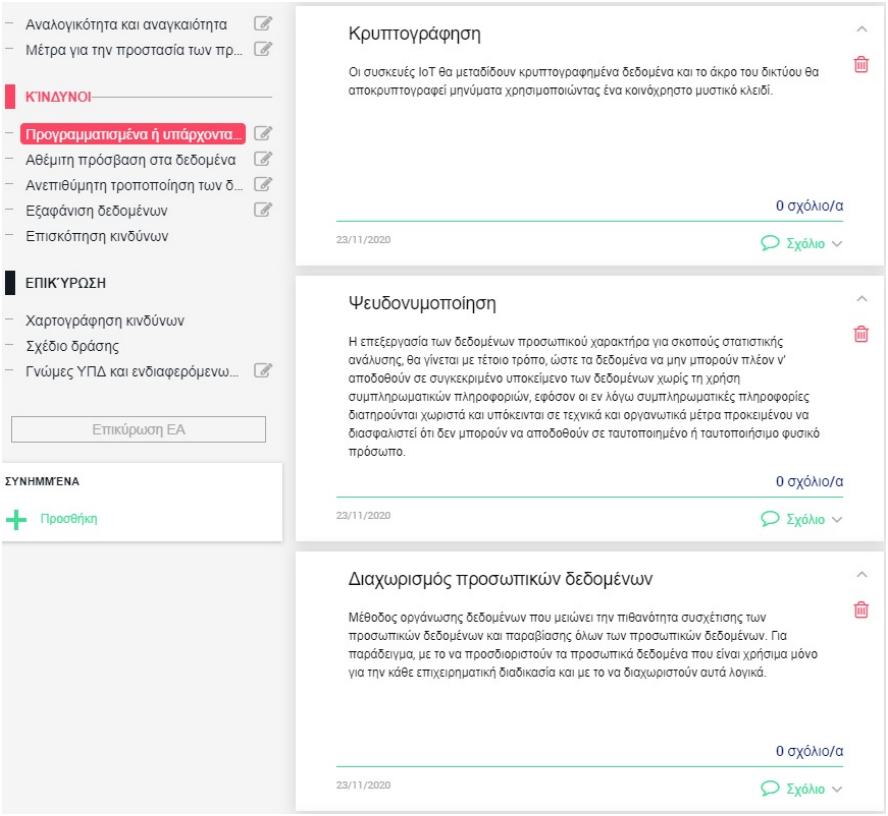
β) ακεραιότητα δεδομένων

γ) διαθεσιμότητα δεδομένων

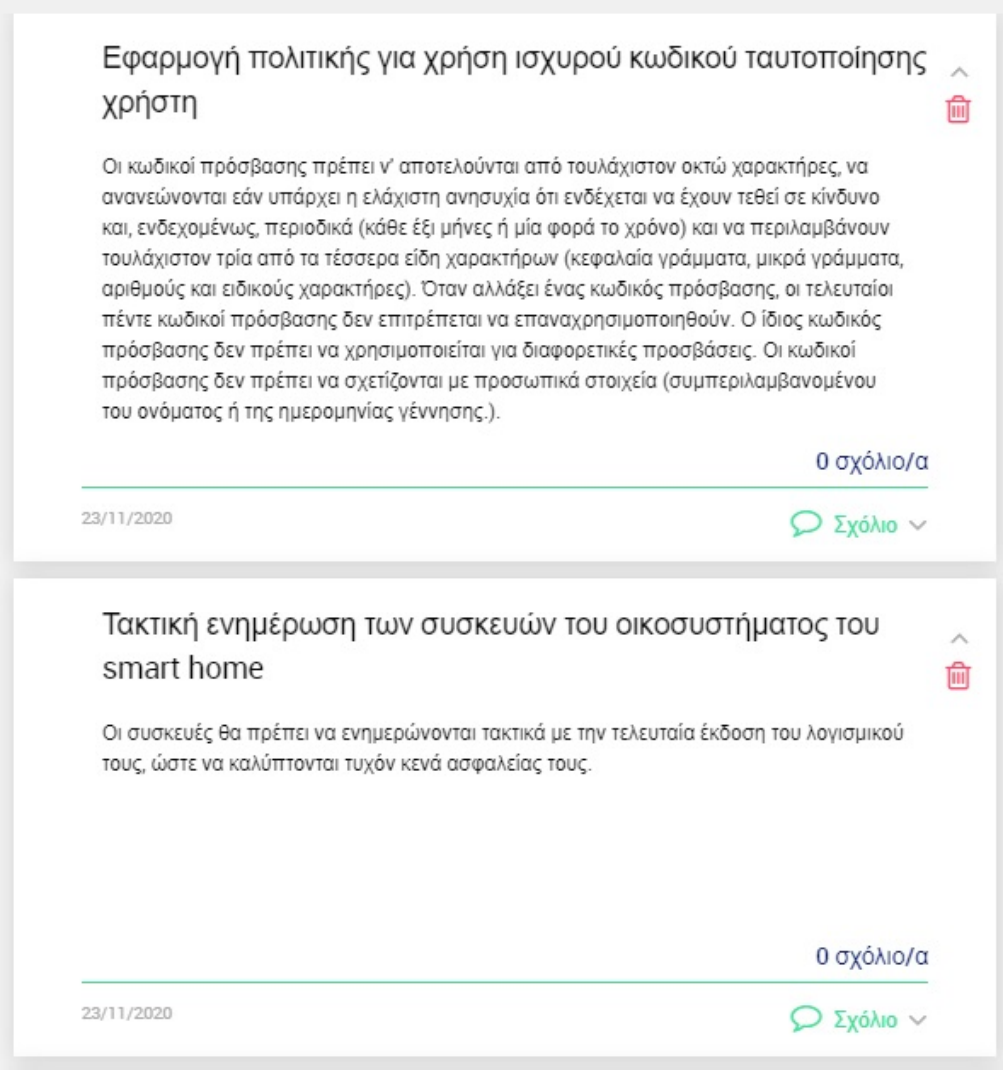
Ειδικότερα, με τη βοήθεια του AES-CCS, πραγματοποιείται η κρυπτογράφηση των δεδομένων και η αυθεντικοποίηση του χρήστη. Επιπλέον, με τη βοήθεια του Μετρητή των Πλαισίων (Frame Counter) και ειδικού κώδικα ακεραιότητας μηνύματος διασφαλίζεται μεταξύ άλλων και η ακεραιότητα του μηνύματος, δηλαδή των εκάστοτε δεδομένων.

Επιπλέον, με το Zigbee διασφαλίζεται και η ανωνυμία του χρήστη.

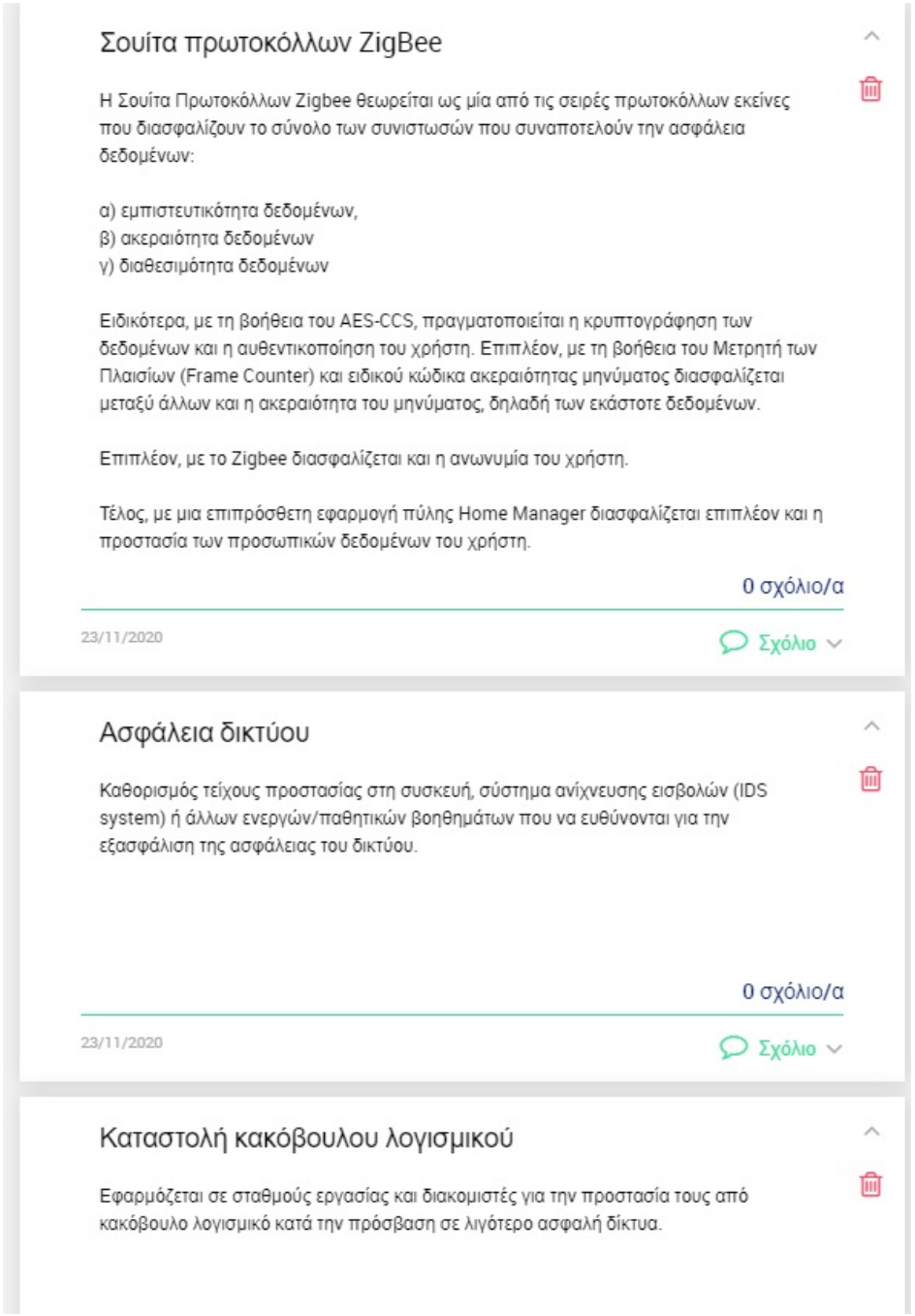
Τέλος, με μια επιπρόσθετη εφαρμογή πύλης Home Manager διασφαλίζεται επιπλέον και η προστασία των προσωπικών δεδομένων του χρήστη.



Εικόνα 54. Καταγραφή προγραμματισμένων ή υπαρχόντων μέτρων



Εικόνα 55. Καταγραφή προγραμματισμένων ή υπαρχόντων μέτρων-2

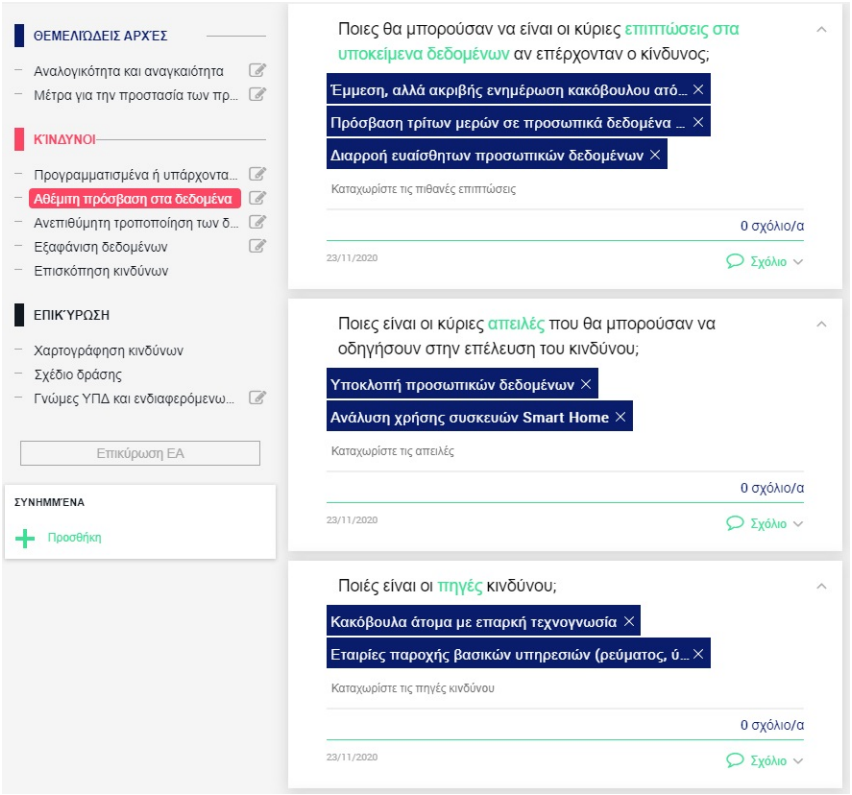


Εικόνα 56. Καταγραφή προγραμματισμένων ή υπαρχόντων μέτρων-3

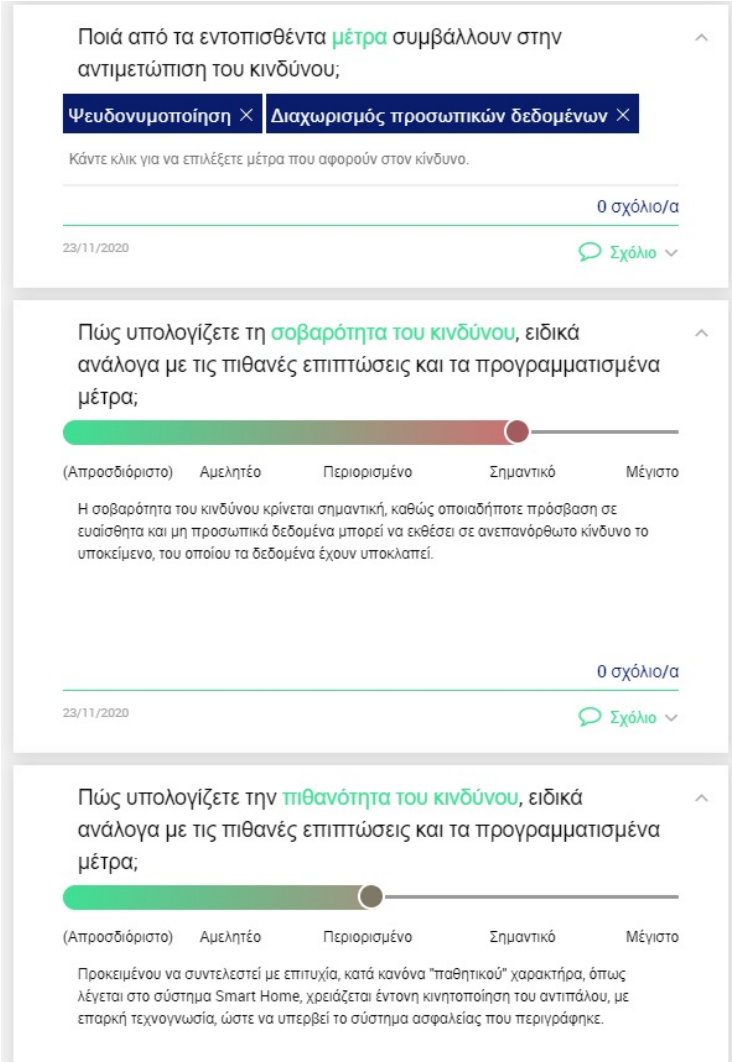
Στη συνέχεια, καταγράφονται οι αιτίες και οι συνέπειες που αφορούν τους κινδύνους της αθέμιτης πρόσβασης στα δεδομένα.

Η σοβαρότητα του κινδύνου κρίνεται σημαντική, καθώς οποιαδήποτε πρόσβαση σε ευαίσθητα και μη προσωπικά δεδομένα μπορεί να εκθέσει σε ανεπανόρθωτο κίνδυνο το υποκείμενο, του οποίου τα δεδομένα έχουν υποκλαπεί.

Προκειμένου να συντελεστεί με επιτυχία, κατά κανόνα "παθητικού" χαρακτήρα, όπως λέγεται στο σύστημα Smart Home, χρειάζεται έντονη κινητοποίηση του αντιπάλου, με επαρκή τεχνογνωσία, ώστε να υπερβεί το σύστημα ασφαλείας που περιγράφηκε.



Εικόνα 57. Καταγραφή αιτίων και συνεπειών αθέμιτης πρόσβασης στα δεδομένα

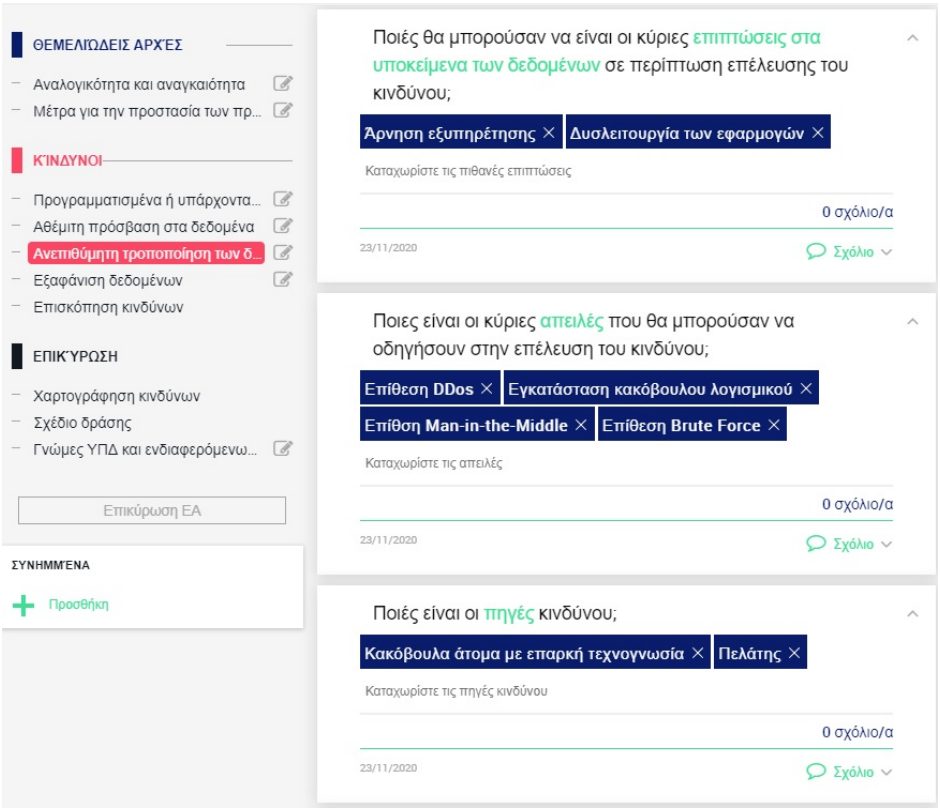


Εικόνα 58. Καταγραφή αιτίων και συνεπειών αθέμιτης πρόσβασης στα δεδομένα-2

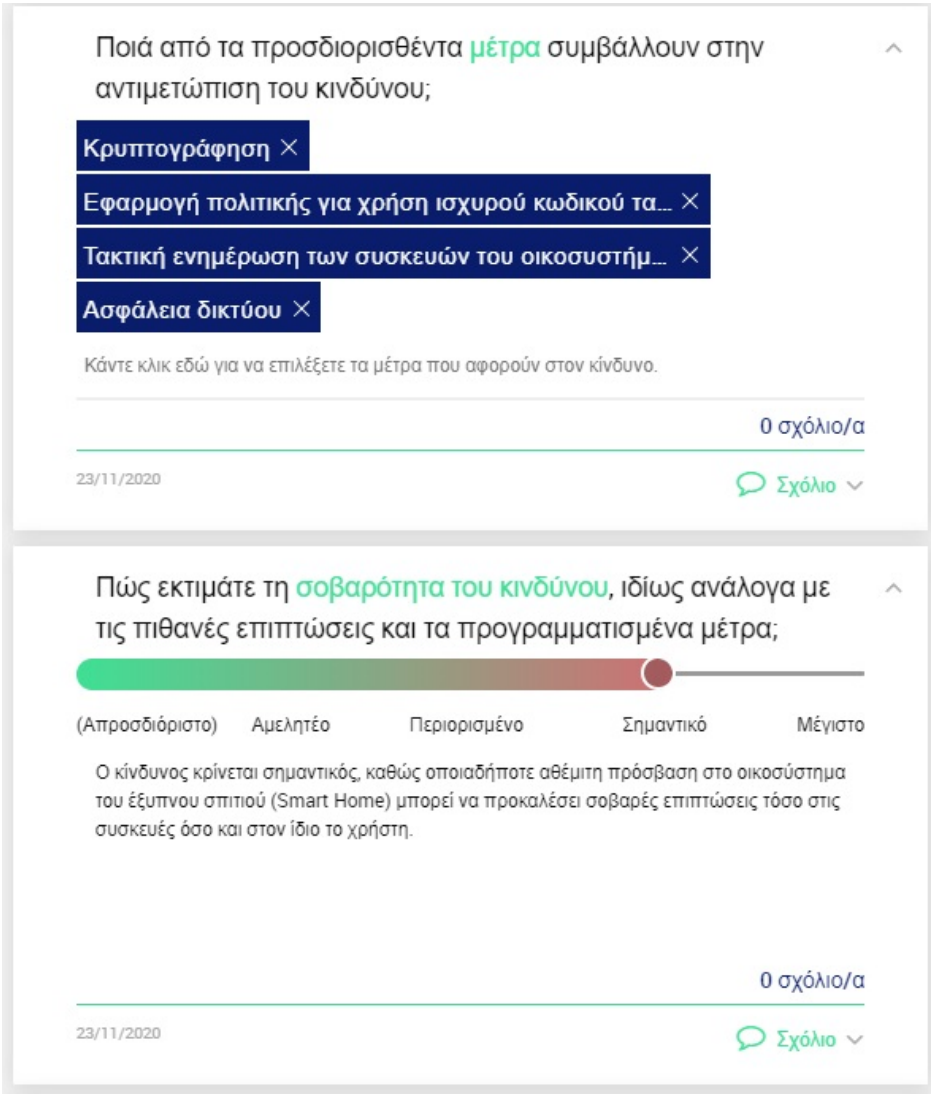
Τα δύο τελευταία βήματα αυτού του σταδίου αφορούν την καταγραφή των αιτίων και συνεπειών μιας ανεπιθύμητης τροποποίησης των δεδομένων. Παρακάτω δίνονται οι σχετικές καταχωρήσεις στο εργαλείο.

Ο κίνδυνος κρίνεται σημαντικός, καθώς οποιαδήποτε αθέμιτη πρόσβαση στο οικοσύστημα του έξυπνου σπιτιού (Smart Home) μπορεί να προκαλέσει σοβαρές επιπτώσεις τόσο στις συσκευές όσο και στον ίδιο το χρήστη.

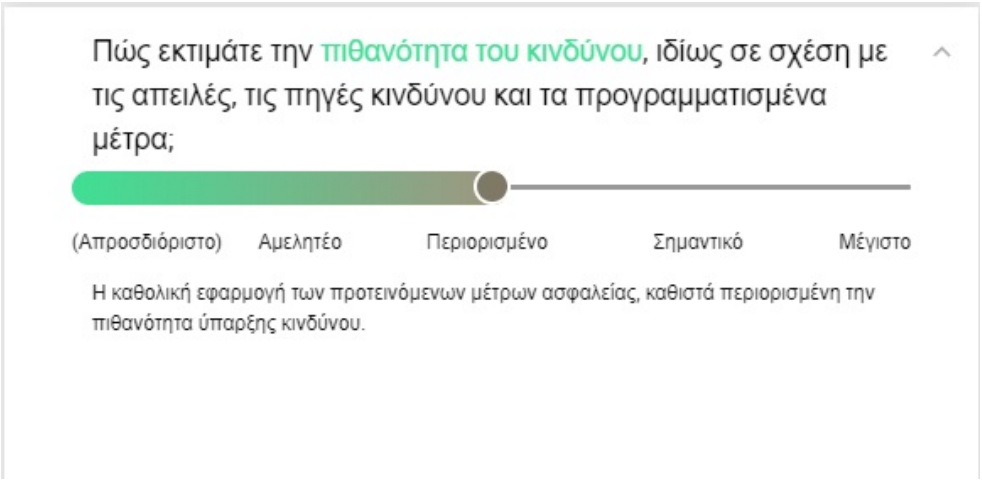
Η καθολική εφαρμογή των προτεινόμενων μέτρων ασφαλείας, καθιστά περιορισμένη την πιθανότητα ύπαρξης κινδύνου.



Εικόνα 59. Καταγραφή αιτίων και συνεπειών ανεπιθύμητης τροποποίησης των δεδομένων

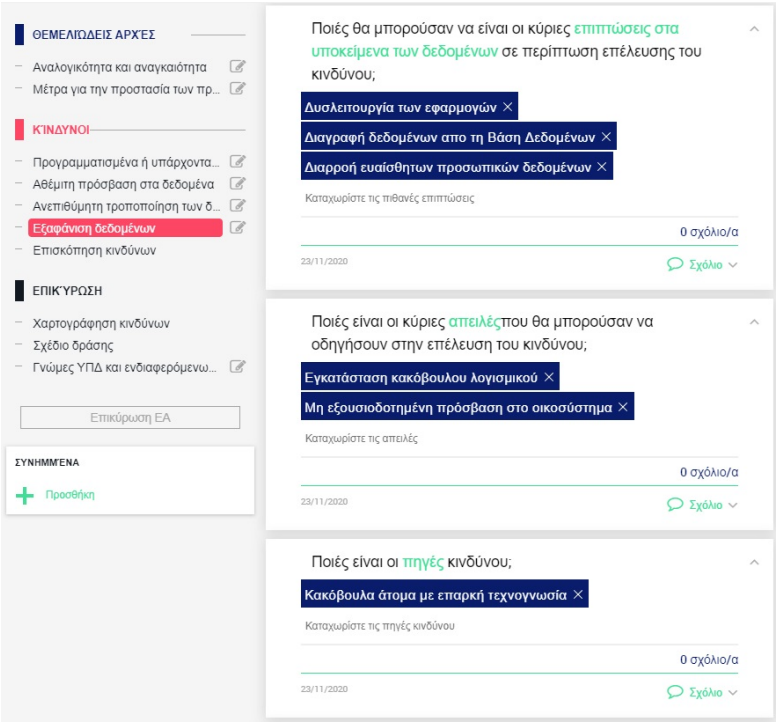


Εικόνα 60. Καταγραφή αιτίων και συνεπειών ανεπιθύμητης τροποποίησης των δεδομένων-2

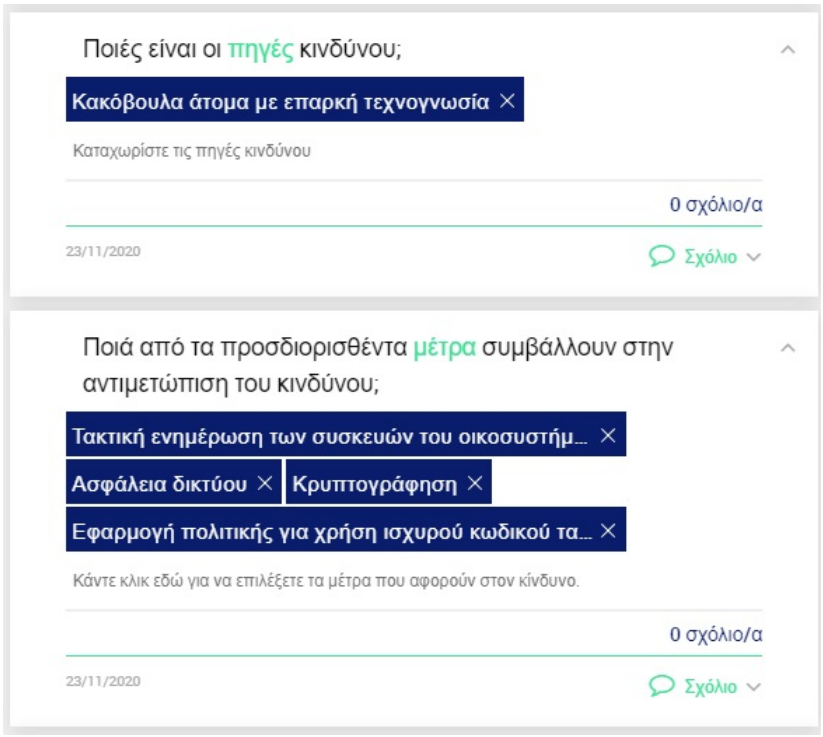


Εικόνα 61. Καταγραφή αιτίων και συνεπειών ανεπιθύμητης τροποποίησης των δεδομένων-3

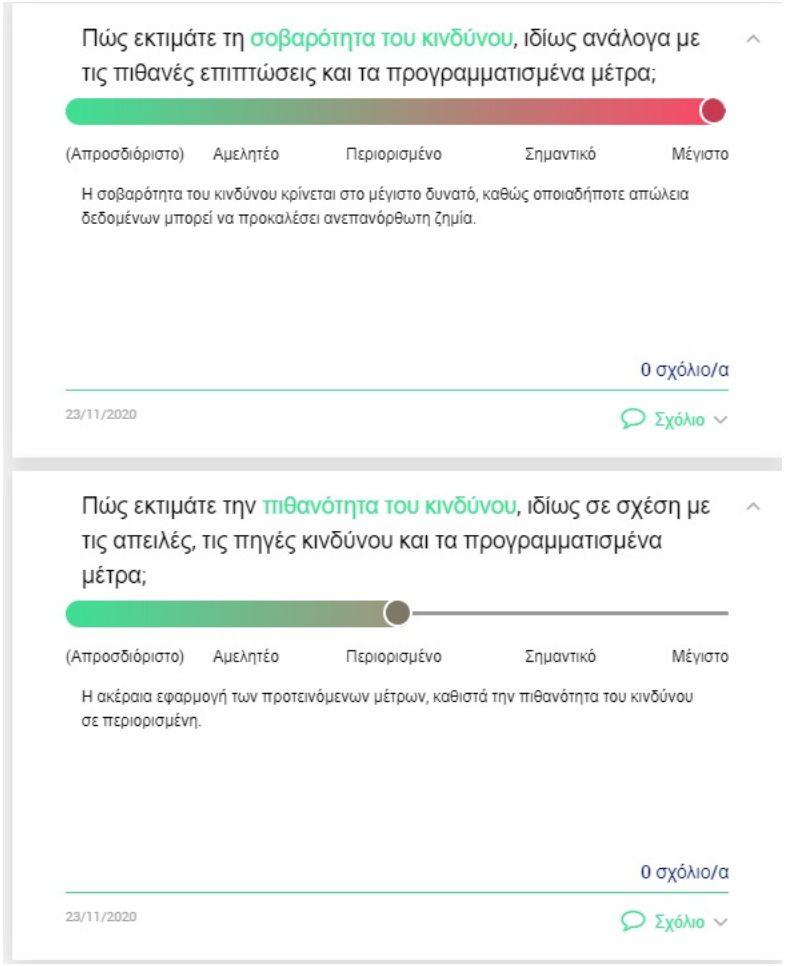
Εν συνεχεία γίνεται καταγραφή των αιτίων και συνεπειών εξαφάνισης των δεδομένων.



Εικόνα 62. Καταγραφή αιτίων και συνεπειών εξαφάνισης των δεδομένων



Εικόνα 63. Καταγραφή αιτίων και συνεπειών εξαφάνισης δεδομένων-2



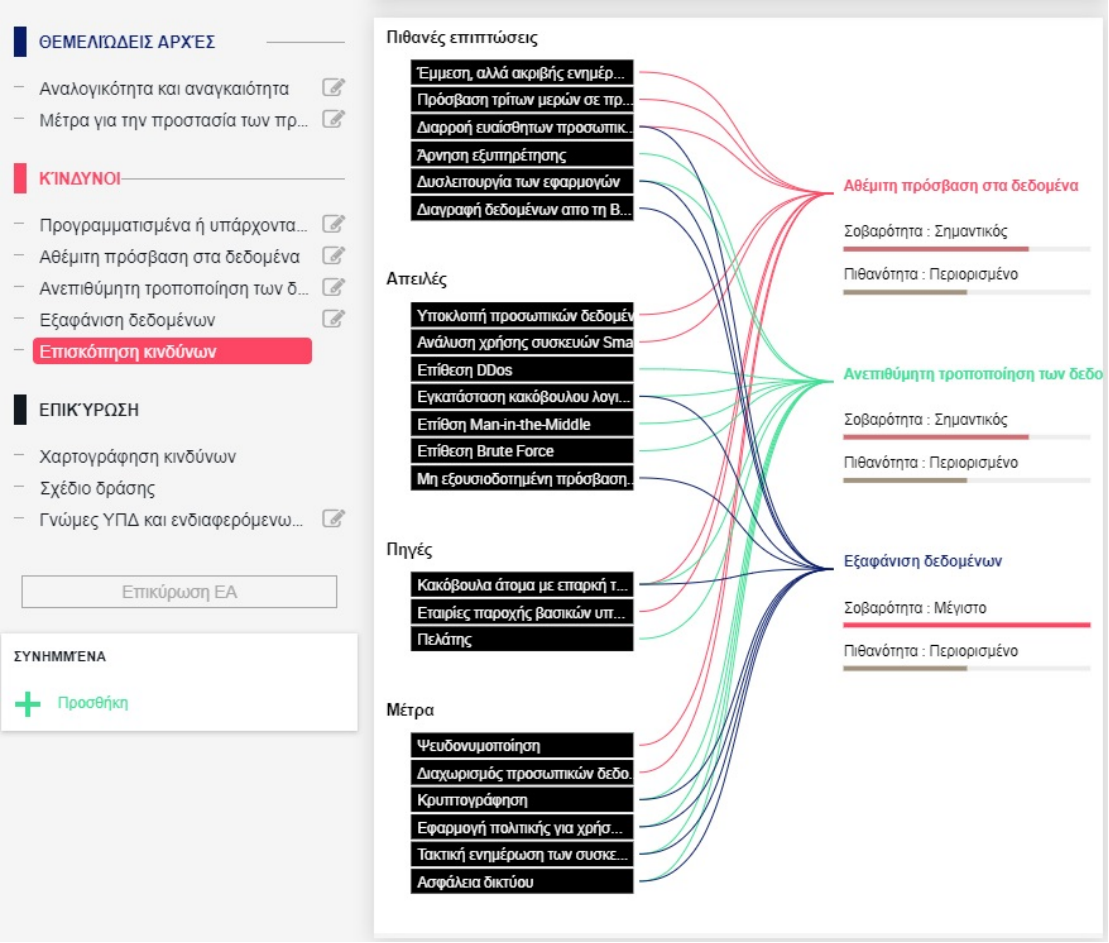
Εικόνα 64. Καταγραφή αιτίων και συνεπειών εξαφάνισης δεδομένων-3

Η σοβαρότητα του κινδύνου κρίνεται στο μέγιστο δυνατό, καθώς οποιαδήποτε απώλεια δεδομένων μπορεί να προκαλέσει ανεπανόρθωτη ζημία.

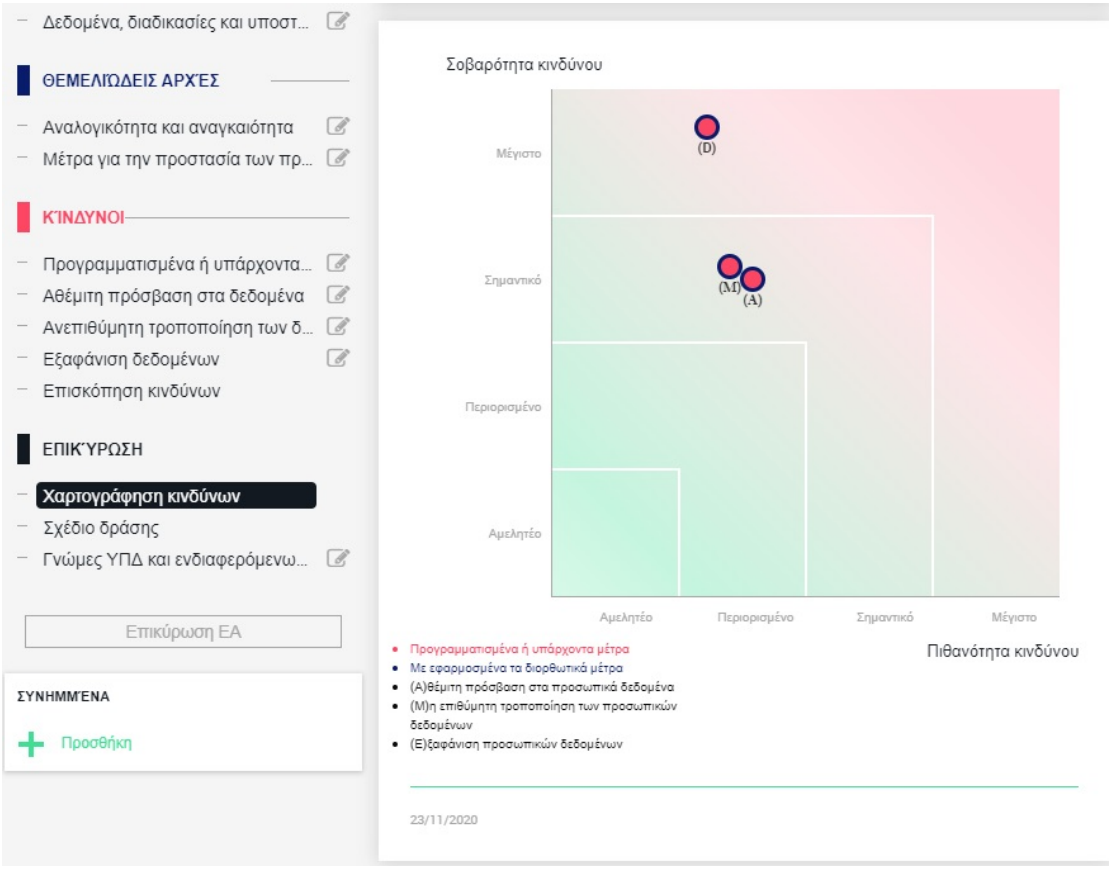
Η ακέραια εφαρμογή των προτεινόμενων μέτρων, καθιστά την πιθανότητα του κινδύνου σε περιορισμένη.

Μετά και αυτό το βήμα, η υλοποίηση της μεθοδολογίας DPIA μέσω του εργαλείου PIA έχει ολοκληρωθεί.

Στο σημείο αυτό, το εργαλείο PIA παρέχει κάποιους χρήσιμους συγκεντρωτικούς πίνακες ως επιστέγασμα του συνόλου της καταγραφής που πραγματοποιήθηκε.



Εικόνα 65. Πίνακας Επισκόπησης Κινδύνων PIA



Εικόνα 66. Πίνακας Χαρτογράφησης Κινδύνων PIA

5.6 Αξιολόγηση της Εκτίμησης Αντίκτυπου Προστασίας Δεδομένων

Μετά την ολοκλήρωση της ως άνω διαδικασίας, γίνεται αξιολόγηση των κινδύνων που απομένουν μετά την υιοθέτηση όλων των ανωτέρω μέτρων, προκειμένου να ληφθούν διορθωτικά μέτρα εάν χρειάζονται (ενώ, σύμφωνα με τον GDPR, εάν οι κίνδυνοι που απομένουν είναι σημαντικοί, τότε απαιτείται διαβούλευση με την αρμόδια εποπτική αρχή). Για την αξιολόγηση, ζητείται και η γνώμη/ συνεισφορά του Data Protection Officer.

Στο παράδειγμα ανωτέρω, μπορούμε να αναγνωρίσουμε τα εξής ζητήματα που χρήζουν αντιμετώπισης:

1) Δεν υπάρχει σαφήνεια στο χρόνο τήρησης των δεδομένων, ανά σκοπό επεξεργασίας. Η διατύπωση «τα δεδομένα τηρούνται για απολύτως απαραίτητο χρονικό διάστημα» δεν ικανοποιεί την απαίτηση της διαφάνειας της

επεξεργασίας, ενώ επίσης δεν διαφοροποιεί το χρόνο τήρησης ανά σκοπό επεξεργασίας (π.χ. δεδομένα που σχετίζονται με τη χρέωση υπηρεσιών μπορούν να τηρούνται για συγκεκριμένο χρονικό διάστημα βάσει της εθνικής νομοθεσίας, αλλά τα δεδομένα για στατιστική ανάλυση υπόκεινται σε άλλες απαιτήσεις ως προς το χρόνο τήρησης. Αντίστοιχα άλλες απαιτήσεις υπάρχουν για την τήρηση των δεδομένων για σκοπούς αντιμετώπισης προβλημάτων τεχνικών κτλ. Όλα τα ανωτέρω πρέπει να συγκεκριμενοποιηθούν).

2) Για την άσκηση των δικαιωμάτων των χρηστών, γίνεται αναφορά σε ψηφιακές φόρμες συναίνεσης. Εδώ πρέπει να ληφθούν πρόσθετα μέτρα για την ασφαλή ταυτοποίηση των χρηστών, προκειμένου να διασφαλίζεται ότι πράγματι ο σωστός χρήστης δίνει τη συναίνεσή του (π.χ. μέσω two-factor authentication μεθόδου). Αντίστοιχη ανάγκη ισχυρής ταυτοποίησης του χρήστη υπάρχει και σε κάθε διαδικασία άσκησης των δικαιωμάτων του.

3) Γίνεται αναφορά σε ψευδωνυμοποίηση των δεδομένων για στατιστική τους ανάλυση, αλλά η τεχνική ψευδωνυμοποίησης πρέπει να περιγραφεί με ακρίβεια, καταδεικνύοντας την αποτελεσματικότητά της στο να μην είναι επιτρεπτό, για το τμήμα του οργανισμού που κάνει στατιστική ανάλυση, να ταυτοποιεί/αναγνωρίζει του χρήστες.

4) Πρέπει να καθοριστεί πλάνο ελέγχου και επανα-αξιολόγησης των τεχνικών μέτρων ασφάλειας (προτείνεται τουλάχιστον μία αναφορά ανά έξι μήνες).

Κεφάλαιο 6

Συμπεράσματα – Επίλογος

Στο πλαίσιο της μεταπτυχιακής αυτής διατριβής, πραγματοποιήθηκε μια γενική ανασκόπηση της τεχνολογίας και της αρχιτεκτονικής του Internet of Things (IoT), αναλύθηκαν οι επιθέσεις, απειλές αλλά και οι τεχνικές αντιμετώπισης των κινδύνων αυτών, μελετήθηκε η φύση των προσωπικών δεδομένων και από ποιους νόμους διέπεται η προστασία τους, μελετήθηκε η τεχνολογία του «Έξυπνου» σπιτιού, μιας καινοτόμου εφαρμογής του Διαδικτύου των Πραγμάτων, καθώς επίσης μελετήθηκε το εργαλείο PIA (Privacy Impact Assessment) και με τη χρήση ενός υποθετικού σεναρίου πραγματοποιήθηκε ανάλυση DPIA (Data Privacy Impact Assessment).

Η μεταπτυχιακή αυτή διατριβή εστίασε σε μία έννοια η οποία εισήχθη ως νομική υποχρέωση, μέσω του GDPR (General Data Protection Regulation), το Μάιο του 2018. Πρόκειται δηλαδή για μία έννοια όπου ακόμη δεν έχουν αναπτυχθεί εκτενείς μεθοδολογίες. Επίσης, για την εκπόνηση εκτίμησης αντικτύπου, διαχειριστήκαμε ένα υποθετικό σενάριο, το οποίο με τη σειρά του εισάγει περιορισμούς στην έρευνα. Ωστόσο, μέσα από αυτό το σενάριο το οποίο είναι, κατά το δυνατόν, ρεαλιστικό, κατέστη εφικτό το να αναδειχτούν βασικοί κίνδυνοι ασφάλειας αλλά και συμμόρφωσης με τη νομοθεσία προσωπικών δεδομένων που αναδεικνύονται, καθώς και η αξία της εκπόνησης εκτίμησης αντικτύπου ως προς το αναγνωριστούν οι κίνδυνοι αυτοί έγκαιρα και να αντιμετωπιστούν συστηματικά.

Το αποτέλεσμα που λαμβάνεται είναι ότι υπάρχουν διακριτοί κίνδυνοι, που ενώ η επίπτωση τους είναι αρκετά σοβαρή, παρ’ όλα αυτά υπάρχουν μέθοδοι προστασίας, που αν εφαρμοστούν στο ακέραιο, μπορούν να μετριάσουν τις πιθανότητες εμφάνισής των κινδύνων αυτών. Ένα, επίσης, συμπέρασμα που απορρέει από την έρευνα αυτή είναι ότι για να μπορέσει ένας πάροχος IoT υπηρεσιών να καταφέρει να αντιμετωπίσει πιθανούς κινδύνους, πρέπει να επεξεργαστεί όλο και περισσότερα προσωπικά

δεδομένα, πράγμα το οποίο αυξάνει τις προκλήσεις της ταυτόχρονης συμμόρφωσης με τις απαιτήσεις για ιδιωτικότητα και για προστασία των δεδομένων.

Είναι σαφές ότι οι μελλοντικές έρευνες θα έχουν ένα ευρύτατο πεδίο να συνεχίσουν στις κατευθύνσεις που έχτισε η συγκεκριμένη μεταπτυχιακή διατριβή, για τους λόγους που αναφέρθηκαν. Πολύ περισσότερο ίσως, επειδή η μεθοδολογία όπως και η νομοθεσία GDPR αναμένεται να έχει μακροχρόνια ισχύ. Ειδικότερα, μια μελλοντική έρευνα μπορεί να διερευνήσει άλλες εφαρμογές IoT ή να εστιάσει την προσοχή της στο πώς θ' αντιμετωπιστεί αυτή η οξύμωρη κατάσταση που επικρατεί στην επεξεργασία των δεδομένων για την ανάπτυξη κατάλληλων μέτρων ασφάλειας της ιδιωτικότητας. Παράλληλα, νέες τεχνολογίες αντιμετώπισης κινδύνων ασφάλειας σε IoT πρέπει να αξιοποιούνται κατάλληλα, καθώς επίσης και να εξετάζονται - στο πλαίσιο μίας εκτίμησης αντικτύπου – ως προς την αποτελεσματικότητά τους.

Βιβλιογραφία

1. Atzori, L., Iera, A. and Morabito, G. (2010). The Internet of things: A survey. Computer Networks 54 (15): 2787– 2805.
2. Ευρωπαϊκό Ινστιτούτο Έρευνας (IERC). Internet of Things. Διαθέσιμο στο διαδικτυακό ιστότοπο: http://www.internet-of-things-research.eu/about_iot.htm [Πρόσβαση: 22.09.2020]
3. Minoli, D. (2013). Building the Internet of things with IPv6 and MIPv6: The Evolving World of M2M Communications . Hoboken, NJ: Wiley.
4. Παπαζώης, Π. (2019). Ασφάλεια στο Διαδίκτυο των Πραγμάτων. Διπλωματική Εργασία. Πανεπιστήμιο Αιγαίου, Σάμος.
5. ISO/IEC, JTC1 (2016). Information technology - Internet of Things Reference Architecture (IoT RA). Διαθέσιμο στο διαδικτυακό ιστότοπο: https://www.iso.org/standard/65695.html [Πρόσβαση: 23.09.2020]
6. Bassi, A., Bauer M., Fiedler, M., Kramp, T., Van Kranenburg, R., Lange, S. and Meissner, S. (2013). Enabling Things to Talk: Designing IoT Solutions with the IoT Architectural Reference Model, Berlin: Springer, p.p. 163– 211.
7. Adolphs, P., Bedenbender, H., Ehlich, M., Epple, U., Hankel, M., Heidel, R., Hoffmeister, M. (2015). Reference Architecture Model for Industries 4.0 (RAMI 4.0). Διαθέσιμο στο διαδικτυακό ιστότοπο: https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2016/januar/GMA_Status_Report__Reference_Archtitecture_Model_Industrie_4.0__RAMI_4.0_/GMA-Status-Report-RAMI-40-July-2015.pdf [Πρόσβαση: 24.09.2020]
8. Cisco. 2014. The Internet of things reference model. Διαθέσιμο στο διαδικτυακό ιστότοπο: http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf [Πρόσβαση: 24.09.2020]
9. Shanhong Liu (2018). Distribution of enterprise Internet of Things (IoT) projects worldwide as of January 2018, by segment. Διαθέσιμο στο διαδικτυακό ιστότοπο: https://www.statista.com/statistics/869335/world-internet-of-things-projects-by-segment-enterprise [Πρόσβαση: 25.09.2020]
10. Statista Research Department, 2019. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). Διαθέσιμο στο

διαδικτυακό ιστότοπο: https://www.statista.com/statistics/471264/iot-number-of-connected-devices–worldwide [Πρόσβαση: 25.09.2020]

11. NIST – National Institute of Standards and Technology (2013). Foundations for Innovation in Cyber-Physical Systems, Workshop Report, Διαθέσιμο στο διαδικτυακό ιστότοπο: http://www.nist.gov/el/upload/CPS-WorkshopReport-1-30-13-Final.pdf [Πρόσβαση: 26.09.2020]
12. Vermesan, O., Friess, P. (2013) Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystem. Aalborg, Denmark: River Publishers.
13. Kale, V. (2018). Creating Smart Enterprises. Leveraging Cloud, Big Data, Web, Social Media, Mobile and IoT Technologies. N.Y.: CRC Press.
14. Tschofenig, H., et. al., (2015) "Architectural Considerations in Smart Object Networking. Tech", Internet Architecture Board.
15. Duffy Marsan, C. (2015) "IAB Releases Guidelines for Internet-of-Things Developers." IETF Journal 11.1, Internet Engineering Task Force.
16. Kulkarni, S. & Kulkarni, S. (2017). Communication Models in Internet of Things: A Survey. IJSTE - International Journal of Science Technology & Engineering. Vol.3(11), p.p. 87-91.
17. Jayaraman, P., Perera, C., Georgakopoulos, D., Dustdar, S., Thakker, D. and Ranjan, R. (2017). Analyticsas- a-service in a multi-cloud environment through semanticallyenabled hierarchical data processing. Software: Practice and Experience. Vol.47(8), p.p. 1139– 1156.
18. Daghighi, B., Kiah, M., Shamshirband, S. and Rehman. H. (2015). Toward secure group communication in wireless mobile environments: Issues, solutions, and challenges. Journal of Network and Computer Applications. Vol.50, p.p. 1– 14.
19. Hsing Yen, L., Ting Tsai, W. (2010). The room shortage problem of tree-based ZigBee/IEEE 802.15.4 wireless networks. Elsevier Publisher.
20. Gutierrez, Jose A., et al., (2001). IEEE 802.15. 4: a developing standard for low-power low-cost wireless personal area networks. IEEE network. Vol.15(5), p.p. 12-19.
21. Baronti, P., Pillai, P., et al. (2006). Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards - Paolo Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards. Elsevier Publisher.

22. Jianpo, L., Xuning, Z., Ning, T., Jisheng, S. (2010). Study on ZigBee network architecture and routing algorithm - Signal Processing Systems (ICSPS), 2nd International Conference.
23. Ανδριτσάκης, Δ. (2018). Ασφάλεια σε τεχνολογίες του Διαδικτύου των Πραγμάτων (IoT): Μελέτη περίπτωσης και δοκιμαστική υλοποίηση με τη χρήση Raspberry Pi και Arduino Security in Internet of Things (IoT) technologies: A full stack paradigm with Raspberry Pi and Arduino. Μεταπτυχιακή Διατριβή. Πανεπιστήμιο Πειραιάς, Πειραιάς.
24. Li, S., Xu, L. (2017). Securing the Internet of Things. U.S.A.: Syngress
25. Τζιούφα, Π. (2019). Internet of Things-RFID και Προσωπικά Δεδομένα: Θέματα Ασφάλειας και Απορρήτου στο Διαδίκτυο των Πραγμάτων (IoT). Διπλωματική Εργασία. Πανεπιστήμιο Μακεδονίας, Θεσσαλονίκη.
26. Macaulay, T. (2017). RIoT Control. Understanding and Managing Risks and the Internet of Things. U.K.: Morgan Kaufmann.
27. Chakravorty, Antorweep, Tomasz Wlodarczyk, and Chunming Rong. "Privacy preserving data analytics for smart homes." 2013 IEEE Security and Privacy Workshops. IEEE, 2013.
28. Cnil.fr. 2018. The Open Source PIA Software Helps To Carry Out Data Protection Impact Assesment | CNIL. [online] Available at: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment [Πρόσβαση: 28.09.2020]
29. Enisa.europa.eu. 2017. Baseline Security Recommendations For Iot. [online] Available at: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot [Πρόσβαση: 07.11.2020]
30. Harding, J., n.d. Smart Washing Machines Explained - Which?. [online] Which?. Available at: https://www.which.co.uk/reviews/washing-machines/article/smart-washing-machines-explained> [Πρόσβαση: 28.09.2020]
31. Ico.org.uk. n.d. Data Protection Impact Assessments. [online] Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/ [Πρόσβαση: 28.09.2020]
32. IoT Now - How to run an IoT enabled business. 2020. Iot And Home Automation: What Does The Future Hold? - Iot Now - How To Run An Iot Enabled Business.

[online] Available at: https://www.iot-now.com/2020/06/10/98753-iot-home-automation-future-holds/ [Πρόσβαση: 28.09.2020]

33. Pau, G., Colotta, M., Ruano, A. and Qin, J., 2017. Smart Home Energy Management. [ebook] Available at: https://www.mdpi.com/1996-1073/10/3/382/pdf#:~:text=In%20general%2C%20a%20Smart%20Home,concept%20of%20the%20smart%20grid. [Πρόσβαση: 28.09.2020]
34. Tarekegn, B., 2016. Associating The Impact Of Smart Home Technologies On Privacy. Master. Ca' Foscari University of Venice.
35. Todde, M., Beltrame, M., Marceglia, S., & Spagno, C. (2020). Methodology and workflow to perform the Data Protection Impact Assessment in healthcare information systems. Informatics in Medicine Unlocked, 100361.
36. Αντωνάτος, Ι., 2018. Internet Of Things Based Smart Home Environment. M. Sc. University of Macedonia.
37. Gdprgreece.com. n.d. GDPR Greece - Τι Είναι Το GDPR Και Πως Επηρεάζει Τις Επιχειρήσεις;. [online] Available at: https://www.gdprgreece.com/article/5/gdpr [Πρόσβαση: 07.11.2020]
38. Safari, B. A. (2016). Intangible privacy rights: How europe's gdpr will set a new global standard for personal data protection. Seton Hall L. Rev., 47, 809.
39. Nicholas Kolokotronis, Konstantinos Limniotis, Stavros Shiaeles, and Romain Griffiths (2019). Secured by Blockchain: Safeguarding Internet of Things device
40. NIST, Lightweight Cryptography. [online] Available at: https://csrc.nist.gov/projects/lightweight-cryptography [Πρόσβαση: 07.11.2020]