ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2021-2022

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της Ελένης Ψυχιά (Α.Μ.: ΜΔΙ2053)

SMART HOME RISK ANALYSIS FROM THE PERSPECTIVE OF PRIVACY AND SECURITY

Επιβλέπουσα:

Λίλιαν Μήτρου

Πειραιάς, Φεβρουάριος 2022

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Μια από τις μεγαλύτερες εφευρέσεις της ανθρωπότητας, αποτελεί το Διαδίκτυο, το οποίο χρηματοδοτήθηκε από το κράτος των Ηνωμένων Πολιτειών το 1962, ως έργο ενίσχυσης των εθνικών μέτρων άμυνας και εξελίχθηκε στο ARPANET, το οποίο άνοιξε τον δρόμο στην τεχνολογική καινοτομία.

Το Διαδίκτυο, λόγω των εφευρέσεων που ακολούθησαν τις επόμενες δεκαετίες,γνώρισε μεγάλη επιτυχία και οδήγησε στην δημιουργία νέων τεχνολογιών. Είναι γεγονός πως εξελίσσεται σε ένα τεράστιο δίκτυο που διαθέτει πολλές υπηρεσίες, όπως είναι οι ιστότοποι ηλεκτρονικού εμπορίου, τα μέσα κοινωνικής δικτύωσης, οι ειδησεογραφικοί ιστότοποι καθώς και άλλα αντίστοιχα.

Μια από τις σπουδαιότερες τεχνολογικές εξελίξεις η οποία κατέχει πολύ σημαντικό βήμα στο χώρο της τεχνολογίας, είναι οι τεχνολογίες Υπολογιστικού Νέφους και του Ίντερνετ των πραγμάτων, όπου συνηθίζεται να χρησιμοποιείται ο αγγλικός όρος, Internet of Things (IoT). Ο όρος περιγράφει τη σύνδεση φυσικών συσκευών ή αντικειμένων που ενσωματώνουν ηλεκτρονικό υλικό και αποκτούν συνδεσιμότητα στο διαδίκτυο, ώστε να επιτευχθεί η ανταλλαγή δεδομένων.

Άρρηκτα συνδεδεμένο με το IoT είναι τα έξυπνα σπίτια, τα οποία υπόσχονται να βελτιώσουν την ποιότητα ζωής των ανθρώπων. Βασίζονται στη συλλογή τεράστιων ποσοτήτων προσωπικών και ευαίσθητων δεδομένων, καθιστώντας την προστασία της ιδιωτικής ζωής εξαιρετικά σημαντική. Αυτόματα, προκύπτουν ερωτήματα και ανησυχίες σχετικά με την ανάλυση των κινδύνων προστασίας της ιδιωτικής ζωής των έξυπνων κατοικιών.

Παρά τις δυνατότητες που παρέχονται, σημειώνεται μεγάλη ανάπτυξη, η οποία ακολουθείται από σημαντικές

προκλήσεις. Μερικές από τις βασικές προκλήσεις είναι η προστασία των δεδομένων για την εξασφάλιση της ιδιωτικότητας και της ασφάλειας. Μια επίσημη διαδικασία αξιολόγησης κινδύνου μπορεί να βοηθήσει να αναγνωριστούν κίνδυνοιοι οποίοι δεν έχουν γίνει αντιληπτοί, και να συνεισφέρει στην εξάλειψή τους.

Ο Γενικός Κανονισμός για την Προστασία Προσωπικών Δεδομένων (ΓΚΠΔ) εισήγαγενέες κατευθυντήριες σχετικά με την αξιολόγηση κινδύνου, την Εκτίμηση Αντικτύπου Προστασίας Δεδομένων (ΕΑΠΔ), που οι οργανισμοί οφείλουν να ακολουθήσουν. Υπάρχουν πολλές μεθοδολογίες αξιολόγησης κινδύνου σήμερα, καθώς και πλήθος οδηγιών σχετικά μετον τρόπο διενέργειας της εκτίμησης. Στόχος αυτής της διπλωματικής εργασίας είναι να αναλύσει πως η Μεθοδολογία Αξιολόγησης Κινδύνου NIST, σε συνδυασμό με τις κατευθυντήριες που έχουνδοθεί από τον ΓΚΠΔ, μπορεί να συνεισφέρει ουσιαστικά στην αποτελεσματική εκτέλεση της ΕΑΠΔ.

Λέξεις κλειδιά: Internet of Things, Ασφάλεια δεδομένων, Ανάλυση κινδύνων , ΓΚΠΔ, ΕΑΠΔ,Έξυπνο σπίτι (Smart Home)

1. ΕΙΣΑΓΩΓΗ

Στην σύγχρονη κοινωνία η χρήση του διαδικτύου και των υπηρεσιών είναι ιδιαίτερα διαδεδομένη. Οι ευκολίες που προσφέρει στους χρήστες, οδηγούν στο να το χρησιμοποιούν όλο και περισσότερο και να εμπιστεύονται σε αυτό διάφορα προσωπικά τους δεδομένα ώστενα επωφεληθούν των υπηρεσιών του. Με αυτό τον τρόπο δημιουργείται μια βάση δεδομένωνγια τον κάθε χρήστη, που αποτελείται από απλά ή/και ευαίσθητα προσωπικά δεδομένα, όπως είναι το ονοματεπώνυμο, ο αριθμός τηλεφώνου, στοιχεία λογαριασμών ή πιστωτικών καρτών, βιομετρικά και βιολογικά στοιχεία, ακόμα και καταγραφή προσώπων μέσω των φωτογραφιών.

Επιπλέον, από την πλοήγηση των χρηστών στο διαδίκτυο συλλέγονται ψηφιακά αποτυπώματα καθώς και οι καταναλωτικές συνήθειες τους. Αυτή η συλλογή πληροφοριώνέχει ως αντάλλαγμα την παροχή υπηρεσιών και ευκολιών, οι οποίες πριν μερικά χρόνια έμοιαζαν μακρινό όνειρο. Η ακατάπαυστη συλλογή δεδομένων, κρύβει κινδύνους για την ιδιωτικότητα των ατόμων και έτσι δημιουργήθηκε μια νέα ανάγκη, αυτή της προστασίας των προσωπικών δεδομένων.

Εκτιμάται ότι κάθε μήνα, 330 νέες συσκευές συνδέονται στο διαδίκτυο. Όπως υποδηλώνεται από την αύξηση του αριθμού συσκευών και των πολλαπλών περιπτώσεων χρήσης, το IoT είναι σίγουρα μία από τις τεχνολογίες που προκαλούν ζήτηση σήμερα. Η λέξη «Smart» είναι μια πολυδιάστατη λέξη, η οποία αναφέρεται σε ένα έξυπνο, πλήρες περιβάλλον και αλληλοεπιδρά δυναμικά στις εντολές του χρήστη. Το έξυπνο σπίτι, είναι προγραμματισμένο να πραγματοποιεί τις εντολές του χρήστη αλλά και να προσαρμόζει τις συνθήκες με βάση τις παραμέτρους που έχει δηλώσει ο χρήστης. Για να επιτευχθεί η αλληλεπίδραση του χρήστη με το σύστημα απαιτείται η συγχώνευση τεχνολογιών από διάφορους τομείς.

Εκτός ότι η επίτευξη της αλληλεπίδρασης αποτελεί πρόκληση λόγω των πολυάριθμων εφαρμογών που δύναται να συνδεθούν στο οικοσύστημα του σπιτιού, η πολυπλοκότητα αυξάνεται, καθώς κύριο πλέον μέλημα είναι το σύστημα εκτός από λειτουργικό να είναι αξιόπιστο και ασφαλές, λόγω των δεδομένων που αποθηκεύονται κατάτη χρήση του.

Στην παρούσα διπλωματική εργασία θα μελετήσουμε την εφαρμογή των έξυπνων σπιτιών (Smart Homes), τους πιθανούς κινδύνους που υπάρχουν καθώς και τον τρόπο που μπορούμε να προστατέψουμε τα δεδομένα μας. Για τον εντοπισμό των κινδύνων ως προς την ασφάλεια, την προστασία των δεδομένων αλλά και την συμμόρφωση των Εταιριών που δραστηριοποιούνται στο τομέα των τεχνολογικών καινοτομιών, θα αναπτυχθούν ερωτηματολόγια για την συλλογή των κινδύνων αλλά και μεθοδολογίες αξιολόγησης του. Θα γίνει επίσης προσπάθεια ένταξης των μεθοδολογιών αξιολόγησης κινδύνων ασφάλειας στην μεθοδολογία εκτίμησης επιπτώσεων σχετικά με την προστασία των προσωπικών δεδομένων που συλλέγονται κατά τη χρήση καινοτόμων τεχνολογιών όπως το Smart Home. Στόχος είναι να αναπτυχθεί μια τελική μεθοδολογία βασιζόμενη στη μεθοδολογία DPIA που περιγράφεται στα άρθρα του Κανονισμού GDPR, που θα είναι κατάλληλη να παρουσιάσει τόσο τις απειλές ως προς την ασφάλεια αλλά και τις διάφορες αποκλίσεις της Εταιρίας Χ, η οποία εισάγει εφαρμογές διαχείρισης Smart Home στην αγορά, με τον Κανονισμό. Η μεθοδολογία αυτή, θα αναπτυχθεί με την παραδοχή ότι δεν μπορούμε να θεωρήσουμε ότι η προστασία των δεδομένων αλλά και η εξασφάλιση των ελευθεριών και των δικαιωμάτων των υποκειμένων των δεδομένων, μπορεί να επιτευχθεί χωρίς να ληφθεί υπόψη η ασφάλεια των συστημάτων που φιλοξενούν τα δεδομένα αυτά.

2. ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

2.1 Ιστορική Αναδρομή

Από τα τέλη του 1970, παρατηρείται η επίτευξη της απομακρυσμένης σύνδεσης σε συσκευές. Το πρώτο παράδειγμα, αποτέλεσε η χρήση των τηλεφωνικών γραμμών για την παρακολούθηση των ενδείξεων των μετρητών στο ηλεκτρικό δίκτυο. Η ιδέα της προσθήκης νοημοσύνης σε καθημερινά αντικείμενα συζητήθηκε σε όλη τη διάρκεια της δεκαετίας του 1980 και του 1990.

Στις αρχές της δεκαετίας του '80, εμφανίστηκε η πρώτη συσκευή IoT, μια μηχανή παροχής αναψυκτικών στο Πανεπιστήμιο Carnegie Melon στο Πίτσμπουργκ της Πενσυλβανίας. [1]Η λύση δημιουργήθηκε από έναν φοιτητή, ο οποίος επιθυμούσε να είχε την ικανότητα να εντοπίσει απομακρυσμένα αν η μηχανή είχε διαθέσιμα αναψυκτικά και αν ήταν κρύα, αντί να χάνει χρόνο του για να το διαπιστώσει με φυσική παρουσία του. Για το σκοπό αυτό, ακολούθησε η σύνδεση του μηχανήματος στον κεντρικό υπολογιστή του Πανεπιστημίου (στον οποίο εισήχθη σχετικός κώδικας) ο οποίος ήταν συνδεδεμένος στο ARPANET. Η σύνδεση αυτή βέβαια, οδήγησε στο να έχει πρόσβαση στην κατάσταση του μηχανήματος όποιος υπολογιστής ήταν συνδεδεμένος στο ARPANET, ώστε να ελέγχουν την διαθεσιμότητα και την κατάσταση θερμοκρασίας των αναψυκτικών. Σύμφωνα να με πολλές πηγές, αυτό θεωρείται ως το πρώτο παράδειγμα ενός νέου είδους συσκευών, τις οποίες ονομάζουμε σήμερα Internet of Things ή αλλιώς IoT.

---

1 "The "Only" Coke Machine on the Internet". Carnegie Mellon University. Retrieved 10 November 2021

Το 1991, η πρώτη κάρτα Sim, επέτρεψε στις συσκευές να επικοινωνούν μεταξύ τους με δεδομένα κινητής τηλεφωνίας. Επίσης, οδήγησε στο να γίνουν ευρέως γνωστές λύσεις M2M ('machine to machine'), που όμως ήταν εφικτές σε κλειστά δίκτυα ή σε διαφορετικά πρωτόκολλά από το IP- το οποίο χρησιμοποιείται ευρέως στο διαδίκτυο. [2]Η πρώτη επίσημη συσκευή IoT, δημιουργήθηκε και παρουσιάστηκε στο συνέδριο INTEROP το 1990 από τον John Romke. Η συσκευή αυτή, αποτελούσε την πρώτη έξυπνη τοστιέρα που θα μπορούσε ναελεγχθεί από το Διαδίκτυο με τη χρήση του πρωτοκόλλου IP .

Ο όρος IoT επινοήθηκε το 1999, κατά τη παρουσίαση ετικετών RFID, που πραγματοποιήθηκε σε μια εταιρεία καλλυντικών από τον επιχειρηματία Kevin Ashton. [3]Μπορούμε θεωρήσουμε την ετικέτα RFID, ως συσκευή IOT, καθώς εκτός μνήμη που περιέχει,μπορεί να διαθέτει και αισθητήρες. θα πρέπει να είναι συνδεδεμένη στο διαδίκτυο. Όλα όσα αναφέραμε παραπάνω, αποτέλεσαν τα θεμέλια για την ανάπτυξη του Δικτύου των πραγμάτων όπως το γνωρίζουμε σήμερα.

2.2 Χαρακτηριστικά

Σύμφωνα με τον ορισμό του Yang, (2007), «Το Διαδίκτυο των Πραγμάτων ("Internet of Things" – IoT)» είναι μια συλλογή από "πράγματα", αντικείμενα καθημερινά, που έχουν ενσωματωμένα μικροκυκλώματα, αισθητήρες και ισχύ επεξεργασίας, τα οποία επιτρέπουν την σύνδεση των συσκευών στο διαδίκτυο για τη συλλογή και ανταλλαγή πάσης φύσεως δεδομένων μεταξύ τους, με

---

[2] Asif, Saad Z. (2011). *Next Generation Mobile Communications Ecosystem*. John Wiley & Sons. p. 306

[3] Magrassi, P. (2 May 2002). "Why a Universal RFID Infrastructure Would Be a Good Thing". Gartner research report G00106518.

το cloud computing που αναφέραμε παραπάνω ως ενοποιητικό πλαίσιο.

Σήμερα, το IoT βρίσκει εφαρμογή σε διαφορετικούς τομείς (γεωργία μεταφορά,ιατρική περίθαλψη, κατοικίες, σχολεία κ.λπ.) και παράγει και ανταλλάσσει πολλά ήδη δεδομένων, όπως η θερμοκρασία τόπου και σώματος, καρδιακοί παλμοί, βίντεο, ταχύτητα, κατανάλωση τροφίμων ή καυσίμων κ.ο.κ. Όλο και περισσότερα καθημερινά αντικείμενα να συνδέονται ανά πάσα στιγμή και από οποιοδήποτε μέρος στο διαδίκτυο, χάρη στο Διαδίκτυο των πραγμάτων. Τα τελευταίαχρόνια, το Διαδίκτυο των πραγμάτων έχει λάβει μεγάλη προσοχή από ακαδημαϊκούς και βιομηχανικούς οργανισμούς και αποτελεί πλέον αναπόσπαστο κομμάτι της Τέταρτης Βιομηχανικής Επανάστασης (Industry 4.0). Με τον αυξανόμενο αριθμό των συνδεδεμένων συσκευών, το Διαδίκτυο των πραγμάτων μπορεί να θεωρηθεί ως μια τεχνολογική επανάσταση για την πανταχού παρούσα συνδεσιμότητα, τον υπολογιστή και τις επικοινωνίες.

Ο όρος "πραγμάτων" αναφέρεται σε συσκευές που μπορεί να είναι πολύ διαφορετικές η μια από την άλλη, όπως για παράδειγμα μια καφετέρια, ένα ξυπνητήρι, περίπλοκους αισθητήρες αποφυγής σύγκρουσης των οχημάτων. Χάρη στους φθηνούς επεξεργαστές και τα ασύρματα δίκτυα, οτιδήποτε, από λάμπα μέχρι ελικόπτερο, μπορεί ναμετατραπεί σε κομμάτι του IoT, προσθέτοντας ένα επίπεδο ψηφιακής νοημοσύνης συσκευές. επιτρέποντάς τους να επικοινωνούν χωρίς ανθρώπινη παρέμβαση και να ενώσουν στην ουσία τον ψηφιακό και τον φυσικό κόσμο. Στην καθημερινή μας ζωή, χρησιμοποιούμε ήδη μερικές από αυτές τις συσκευές, όπως για παράδειγμα το smart watch,που καταγράφει τις ενέργειες μας (ακόμα και όταν κοιμόμαστε) ,το οποίο στη συνέχεια αναλύει τα δεδομένα και δημιουργεί διαγράμματα για την ποιότητα της ζωής μας. Παράλληλα παρέχει και συμβουλευτικές υπηρεσίες με σκοπό να γίνει καλύτερη.

2.3 Μοντέλα Επικοινωνίας

Όπως αναφέραμε μια συσκευή IoT είναι ικανή να επικοινωνεί με άλλες συσκευές και πληροφοριακά συστήματα. Οι συσκευές επικοινωνούν μέσω διαφορετικών μέσων, συμπεριλαμβανομένων τεχνολογιών κινητής τηλεφωνίας (3G ή LTE), WLAN, ασύρματων Δικτύων ή άλλων τεχνολογιών.[4] Ο τρόπος επικοινωνίας εξαρτάται από το μέγεθος της συσκευής, την κινητικότητα της, δηλαδή αν πρόκειται για συσκευή η οποία παραμένει σταθερή ή κινείται, από το αν περιέχει εσωτερική πηγή ενέργειας, αν απαιτείται ανταλλαγή δεδομένων ή κατά διαστήματα και τέλος, αν η συσκευές αποτελούν αντικείμενα με δυνατότητα απόκτησης διεύθυνσης IP.

Οι υπηρεσίες IoT διευκολύνουν την ενσωμάτωση των συσκευών IoT στον κόσμο της αρχιτεκτονικής προσανατολισμένης σε υπηρεσίες (SOA).[5] Μια υπηρεσία IoT αποτελεί συνήθως μια ανταλλαγή δεδομένων μεταξύ δύο μερών: του παρόχου υπηρεσιών και του καταναλωτή υπηρεσιών. Μια υπηρεσία παρέχει μια καλά καθορισμένη και τυποποιημένη διεπαφή, που προσφέρει όλες τις απαραίτητες λειτουργίες για την επίτευξη της αλληλεπίδραση με τις συσκευές.

Η ικανότητα της συσκευής να αλληλοεπιδρά και να επικοινωνεί με άλλους εξοπλισμούς, αντικείμενα και

---

[4] M. Welsh and G. Mainland, "Programming Sensor Networks Using Abstract Regions," in NSDI, 2004, pp. 3-3.

[5] Q. Zhu, R. Wang, Q. Chen, Y. Liu, and W. Qin, "Iot gateway: Bridging wireless sensor networks into internet of things," in 2010 IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC), 2010, pp. 347-352.

περιβάλλοντα επιτυγχάνεται από τεχνικής άποψης με τα παρακάτω είδη μοντέλων επικοινωνίας.

- Device-to-Device

Το device to device μοντέλο επικοινωνίας, επιτρέπει σε δύο η περισσότερες συσκευές να επικοινωνούν και να ανταλλάσσουν δεδομένα μεταξύ τους, μέσω του Internet, ή με χρήσησυγκεκριμένων πρωτοκόλλων όπως Bluetooth ή ZigBee42.Η αυτονομία, η επικοινωνία και η συνεργασία μεταξύ συσκευών παίζουν πολύ σημαντικό ρόλο στη μεταμόρφωση τον ψηφιακού κόσμου. Η αναδυόμενη τεχνολογία που επιτρέπει την επικοινωνία από συσκευή σε συσκευή (D2D) διευκολύνει την λειτουργία των peer-to-peer δικτύων.[6]

- Device-to-Cloud

Σε ένα μοντέλο επικοινωνίας Device to Cloud, η συσκευή IoT συνδέεται απευθείας σεμια εφαρμογή/ υπηρεσία που φιλοξενείται στο cloud, προκειμένου να επιτευχθεί η ανταλλαγή δεδομένων. Σε αυτή τη προσέγγιση για να επιτευχθεί η σύνδεση της συσκευής IoT με το cloud, χρησιμοποιούνται οι υπάρχοντες μηχανισμοί επικοινωνίας όπως παραδοσιακές ενσύρματες συνδέσεις Ethernet ή Wi-Fi.[7]

- Device-to-Gateway

---

[6] M. Chui, M. Löffler, and R. Roberts, "The internet of things," McKinsey Quarterly, vol. 2, pp. 1-9, 2010.

[7] Jun Wei Chuah —The Internet of Things: An Overview and New Perspectives in Systems Design‖ 2014 International Symposium on Integrated Circuits 978-1-4799-4833-8/14.

Στο μοντέλο αυτό, για να επιτευχθεί η σύνδεση, η συσκευή IoT συνδέεται μέσω μιασυπηρεσίας ALG ως ενδιάμεσος.[8] Ο ρόλος του ενδιάμεσου (gateway) είναι η μετάφραση πρωτοκόλλων, ανάλυση δεδομένων και ενίσχυση της ασφάλειας.

- Back-End Data-Sharing Model

Στο μοντέλο ανταλλαγής δεδομένων back-end, οι χρήστες εξάγουν και αναλύουν δεδομένα από την IoT συσκευή, τόσο από μια υπηρεσία cloud όσο και με δεδομένα από άλλες πηγές. Αυτή η προσέγγιση είναι μια επέκταση της Device-to-Cloud επικοινωνίας, το οποίο επιτρέπει την ανάλυση δεδομένων που συλλέγονται από συσκευές IoT.[9]

2.4 Αρχιτεκτονική Μοντέλων Επικοινωνίας

Η αρχιτεκτονική του διαδικτύου των πραγμάτων έχει σχεδιαστεί με τρόπο, κατά τον οποίο η διαχείριση μεγάλου όγκου δεδομένων, είναι εφικτή. Είναι αρκετά αξιόπιστη δομή, που μπορεί να ενσωματώσει και να επεξεργαστεί κάθε στοιχείο/δεδομένο μιας έξυπνης συσκευής. Αυτή η αρχιτεκτονική έχει σχεδιαστεί με αναφορά στην αρχιτεκτονική των σημερινών συστημάτων και τα επίπεδα παρατίθενται παρακάτω[10]:

---

[8] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari and Moussa Ayyash ―Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications‖ ieee communication surveys & tutorials, vol. 17, no. 4, fourth quarter 2015.

[9] K. Bing, L. Fu, Y. Zhuo, and L. Yanlei, "Design of an Internet of Things-based Smart Home System," 2nd International Conference on Intelligent Control and Information Processing, 2011, pp. 921-924

[10] Andrea Zanella, Nicola Bui, Angelo Castellani, Lorenzo Vangelista and Michele Zorzi , "IoT for Smart Cities" , IEEE IoT Journal, Vol. 1, No. 1, February 2014.

- Επίπεδο έξυπνων συσκευών / αισθητήρων: Επιτρέπουν τη διασύνδεση του φυσικού και ψηφιακού κόσμου, με σκοπό τη συλλογή και την επεξεργασία πληροφοριών σε πραγματικό χρόνο.
- Επίπεδο πυλών και δικτύων: Η υποδομή ενσύρματου ή ασύρματου δικτύου λειτουργεί ως μέσο μεταφοράς των παραγόμενων από τους αισθητήρες δεδομένων.
- Επίπεδο διαχείρισης υπηρεσιών: Στο επίπεδο αυτό είναι δυνατή η επεξεργασία πληροφοριών, μέσω μεθόδων ανάλυσης, ελέγχων ασφαλείας, μοντελοποίησης διαδικασιών και διαχείρισης συσκευών.
- Επίπεδο εφαρμογής: Ορίζει τις εφαρμογές και τους τομείς της οικονομίας, στους οποίους μπορεί να αναπτυχθεί το IoT, όπως για παράδειγμα πόλεις, μεταφορές, κτήρια, λιανική πώληση, εφοδιαστική αλυσίδα, γεωργία, βιομηχανία, υγεία, αλληλεπίδραση χρηστών, πολιτισμό και τουρισμό, περιβάλλον και ενέργεια.

2.5 Συσκευές IoT

2.5.1 Αισθητήρες στην υγεία

Στον χώρο της υγείας, υπάρχουν πολλές συσκευές οι οποίες είναι συνήθως φορητές και απλοποιούν την επικοινωνία με πληροφοριακά συστήματα. Οι φορητές συσκευές μπορούν να συνδεθούν ασύρματα με συσκευές όπως μετρητές αρτηριακής πίεσης και γλυκόζης αίματος, έξυπνες κάρτες που αποθηκεύουν ιατρικές πληροφορίες ασθενών και άλλα. Για παράδειγμα, για να πραγματοποιηθεί λεπτομερής ανάλυση ύπνου, οι ιχνηλάτες ύπνου πρέπει να συνδέονται στα άτομα κάθε βράδυ. Επομένως, για να υπολογιστεί με ακρίβεια η κατανάλωση θερμίδων, ο χρήστης πρέπει να τοποθετεί συνεχώς το βηματόμετρο. Υπάρχουν επίσης και άλλες συσκευές που φοράει ο χρήστης, όπως ρολόγια ή γυαλιά.

Ενώ οι χρήστες των συσκευών είναι πιθανό να γνωρίζουν τις δυνατότητες άλλων ατόμων να έχουν πρόσβαση στα εν λόγω δεδομένα τους που συλλέγονται για αυτούς (π.χ. βίντεο ή μικρόφωνο) δεν είναι σε θέση να γνωρίζουν εάν οι ηλεκτρονικές αυτές συσκευές είναι ενεργοποιημένες ή όχι.

Παραδείγματα φορετών συσκευών, αποτελούν:

α. Φίλτρο ανθρώπινου νερού: Για την υποστήριξη των ασθενών που πάσχουν από νεφρική ανεπάρκεια και επομένως είναι απαραίτητη η αιμοκάθαρση ή μεταμόσχευση νεφρού, χρησιμοποιείτε φίλτρο νερού που έχει δημιουργηθεί με χρήση νανοτεχνολογίας.

β. Οθόνη κίνησης ασθενών με Πάρκινσον: Αυτή η οθόνη που φοριέται από τον ασθενή, καταγράφει τις κινήσεις του, με σκοπό να αντισταθμιστεί όποια διακύμανση στην κίνηση

γ. Συσκευή χορήγησης ινσουλίνης: Οι διαβητικοί ασθενείς, μπορούν να πάρουν την δόση στην ώρα που πρέπει, χάρη στην συσκευή αυτή.

δ. Συσκευή ενημέρωσης των τυφλών: Τα άτομα με απώλεια όρασης, μπορούν με αυτή τη συσκευή να ενημερώνονται για το αντικείμενα που βρίσκονται γύρω τους.

ε. Ακουστικά βαρηκοΐας: Τα άτομα με μειωμένη ακουστική ικανότητα, χάρη στη συγκεκριμένη συσκευή, που επεξεργάζεται το ψηφιακό σήμα και εξάγει αναλογικό, μπορούν να βελτιώσουν την αίσθηση της ακοής.

στ. Συσκευές με τεχνολογία παροχής πληροφοριών για το περιβάλλον: Αυτές οι συσκευές βοηθούν τα άτομα με απώλεια γεωγραφικού προσανατολισμού, που παρουσιάζουν δηλαδή δυσκολία στην κίνηση και προσανατολισμό σε εσωτερικούς χώρους

ζ. Συσκευές μέτρησης αρτηριακής πίεσης και καρδιακών παλμών

η. Συσκευές που δίνουν τη δυνατότητα στους ίδιους τους ασθενείς και ταυτόχρονα στους επιβλέποντες ιατρούς να παρακολουθούν την κατάσταση της υγείας και την πορεία της ακολουθουμένης φροντίδας με τη χρήση κινητών συσκευών

θ. Βηματοδότες: Συμβάλλουν στην επίλυση καρδιακών προβλημάτων. Στη σημερινή εποχή, οι βηματοδότες είναι εμφυτεύσιμοι. Όταν εφευρέθηκαν ήταν φορετές συσκευές

ι. Συσκευή θεραπείας πόνου: Μέσω της θέρμανσης των ιστών, συμβάλει στην τοπική θεραπεία του πόνου, κάνοντας χρήση χαμηλής συχνότητας και έντασης υπερήχων

κ. Σύστημα που παρακολουθεί και επιταχύνει την πώρωση καταγμάτων μακρών οστών

2.5.2 Συσκευές οικιακού αυτοματισμού

Οι συσκευές δεν περιορίζονται στην παρακολούθηση ατόμων αλλά μπορούν επίσης να εγκατασταθούν σε σπίτια και γραφεία για την παρακολούθηση διαφόρων περιβαλλοντικών αλλαγών παρέχοντας μηχανισμούς ελέγχου. Οι κατασκευαστές έχουν βρει δημιουργήσει ψυγεία, πλυντήρια ρούχων, φούρνους και θερμοστάτες που μπορούν να ελέγχονται ή να παρακολουθούνται απομακρυσμένα. Οι περισσότερες συσκευές οικιακού

αυτοματισμού συνδέονται συνεχώς στο διαδίκτυο και ανταλλάσσουν δεδομένα στον κατασκευαστή ή και σε τρίτες Εταιρείες. Δεδομένα που μπορεί να μην θεωρούνται πάντα ευαίσθητα, αλλά σε κάθε περίπτωση μπορούν να χρησιμοποιηθούν για την παροχή πληροφοριών σχετικά με το εάν οι χρήστες του έξυπνου σπιτιού βρίσκονται στο σπίτι. Η συνδεδεμένη συσκευή χρησιμοποιείται επίσης για τον εντοπισμό ενεργειών, όπως το άναμμα των φώτων, η αλλαγή της θερμοκρασίας του δωματίου κ.λπ. Οι κατηγορίες αυτές δεν είναι αποκλειστικές. Χαρακτηριστικό παράδειγμα αποτελεί ένα έξυπνο ρολόι που μπορεί παράλληλα να καταγράφει και τους καρδιακούς παλμούς.

2.6 Πλεονεκτήματα και Μειονεκτήματα Συσκευών IoT

Οποιαδήποτε διαθέσιμη τεχνολογία δεν έχει φτάσει στο μέγιστο των δυνατότητων της. Μπορούμε λοιπόν να πούμε ότι το IoT αποτελεί μια σημαντική τεχνολογία που σίγουρα θα συνεισφέρει στο να φτάσουν στο μέγιστο των δυνατοτήτων τους, άλλες τεχνολογίες.

Το Διαδίκτυο των πραγμάτων διευκολύνει την καθημερινή ζωή και μερικά από τα οφέλη του είναι τα εξής:

• Αποτελεσματική χρήση πόρων: Εάν οι λειτουργίες κάθε συσκευής είναι γνωστές, η αποτελεσματική χρήση της θα αυξηθεί σίγουρα, ενώ θα είναι δυνατός ο αποκρουσμένος έλεγχος των φυσικών πόρων της.

• Μείωση της ανθρώπινης παρέμβασης: Καθώς οι συσκευές IoT δύναται να λάβουν αυτοματοποιημένες αποφάσεις, ελαχιστοποιείται η ανθρώπινη παρέμβαση και προσπάθεια.

• Εξοικονόμηση χρόνου: Με την αυτοματοποίηση, μειώνεται το ανθρώπινο δυναμικό και εξοικονομείται σίγουρα χρόνος.

• Βελτίωση της συλλογής δεδομένων.

Το Διαδίκτυο των πραγμάτων όμως έχει και κάποια σημαντικά μειονεκτήματα όπως:

- Ζητήματα ασφάλειας και ιδιωτικότητας.
- Τεχνική πολυπλοκότητα: Αν και φαίνεται ότι οι συσκευές IoT εκτελούν απλές εργασίες, η τεχνολογία που εμπλέκεται στη δημιουργία τους είναι εξαιρετικά πολύπλοκη.
- Εξάρτηση από συνδεσιμότητα στο Διαδίκτυο και από παροχή ενέργειας: Πολλές συσκευές εξαρτώνται από συνεχή τροφοδοσία ή σύνδεση στο Διαδίκτυο για να λειτουργούν σωστά. Όταν κάποιο από τα δύο δεν είναι διαθέσιμο, το ίδιο συμβαίνει και με τη συσκευή IoT και οτιδήποτε συνδέεται με αυτήν.
- Χρονοβόρο και δαπανηρό: Η ανάπτυξη συσκευών IoT συνήθως συνδέεται με υψηλές απαιτήσεις επένδυσης χρόνου και χρήματος, καθώς πρέπει να αγοραστούν και να διαμορφωθούν οι συσκευές IoT, να εγκατασταθούν από προσωπικό και να ενσωματωθούν στο δίκτυο με πολύ συγκεκριμένες παραμετροποιήσεις.

3. ΕΞΥΠΝΟ ΣΠΙΤΙ (SMART HOME)

Γενικός ορισμός ή κοινή αποδοχή για το τι πραγματικά είναι ένα «έξυπνο σπίτι » δενυφίσταται. Ο ορισμός ποικίλλει ανάλογα με την τεχνολογία ή τη λειτουργικότητα που εφαρμόζει το σπίτι. Τα τελευταία χρόνια, έχουν χρησιμοποιηθεί διάφορες εναλλακτικές ονομασίες για το έξυπνο σπίτι, όπως «έξυπνη διαβίωση», «ψηφιακό σπίτι», «έξυπνα περιβάλλοντα» και άλλα [11].

---

[11] Marie Chan, Eric Campo, Daniel Estève, and Jean-Yves Fourniols. Smart Homes – Current Features and Future Perspectives. Maturitas,64(2):90–97, 2009.

Ο κοινός, απλός και καθιερωμένος ορισμός προήλθε από το Υπουργείο Εμπορίου και Βιομηχανίας του Ηνωμένου Βασιλείου (DTI), όπου ένα έξυπνο σπίτι χαρακτηρίστηκε ως «μιακατοικία που ενσωματώνει ένα δίκτυο επικοινωνίας, συνδέει τις βασικές ηλεκτρικές συσκευές και υπηρεσίες και επιτρέπει τον εξ αποστάσεως έλεγχο, παρακολούθηση ή πρόσβαση σε αυτές».[12]Ωστόσο, σήμερα τα σπίτια αυτά εξελίσσονται σε έξυπνους χώρους διαβίωσης όπου τα περιβάλλοντα και ο τύπος των υπηρεσιών που προσφέρονταιυπερβαίνουν τα έξυπνα σπίτια και περιλαμβάνουν και άλλες πτυχές της ανθρώπινης καθημερινότητας, όπως η εκπαίδευση, η εργασία και η κοινωνική ζωή. Επιπλέον, εκτός από τις δυνατότητες αυτοματισμού και ελέγχου, τα έξυπνα σπίτια παρέχουν πλέον υπηρεσίες προληπτικού ελέγχου, όπως η παροχή έγκαιρης υποστήριξης στους κατοίκους μέσω τεχνολογιών αισθητήρων και αλγορίθμων που βασίζονται στην Τεχνητή Νοημοσύνη (AI) και τη μηχανική μάθησης.

Τα έξυπνα σπίτια ανήκουν στο ευρύ φάσμα του Διαδικτύου των Πραγμάτων. Ουσιαστικά, ο ορισμός αποδίδεται σε ένα σπίτι όπως το γνωρίζουμε, που αποτελείται από ένα πλήθος συσκευών που περιλαμβάνουν « αισθητήρες, λογισμικό και συνδεσιμότητα δικτύου»[13]. Η υλοποίηση αυτή, δίνει στους κατοίκους τη δυνατότητα να λαμβάνουν πληροφορίες, να ελέγχουν και να αυτοματοποιούν διαφορετικά τμήματα του σπιτιού και ναβελτιώνουν την ποιότητα

---

[12] Nicola King. Smart Home – a Definition. Intertek Research and Testing Center, page 1–6, 2003.

[13] Mussab Alaa, Aws Alaa Zaidan, Bilal Bahaa Zaidan, Mohammed Talal, and Miss Laiha Mat Kiah. A Review of Smart Home Applications based on Internet of Things. Journal of Network and Computer Applications, 97:48–65, 2017.

των καθημερινών εργασιών σε μια κατοικία, ενδεχομένως από οπουδήποτε και οποιαδήποτε στιγμή, συνήθως μέσω Διαδικτύου μέσω μιας εφαρμογής για κινητές συσκευές[14]. Ουσιαστικά, τα έξυπνα σπίτια επικεντρώνονται στην εφαρμογή τεχνολογιών με σκοπό την αύξηση της αποδοτικότητας, της οικονομικής προσιτότητας και της βιωσιμότητας των πόρων [15].

3.1 Εξέλιξη

Η τεχνολογία των έξυπνων κατοικιών δεν αποτελεί εύρημα των τελευταίων χρόνων. Στην πραγματικότητα, ο πρώτος χαρακτηρισμός του «έξυπνου σπιτιού» προήλθε αρχικά από την Αμερικανική Ένωση Οικοδόμων το έτος 1984 16. Έτσι, αν και η έννοια του έξυπνου σπιτιού υπάρχει εδώ και καιρό, το έξυπνο σπίτι έχει πάρει την δυναμική που γνωρίζουμε μόνο τα τελευταία χρόνια. Το ορόσημο για την άνθηση και την ανάπτυξη της τεχνολογίας των έξυπνων σπιτιών ήταν η είσοδος της ηλεκτρικής ενέργειας στις κατοικίες στις αρχές του 20ου αιώνα.[17]Η ηλεκτρική ενέργεια πυροδότησε την εισαγωγή νέου εξοπλισμού στο σπίτι, όπως τις οικιακές συσκευές.

---

[14] Vincent Ricquebourg, David Menga, David Durand, Bruno Marhic, Laurent Delahoche, and Christophe Loge. The Smart Home Concept: our Immediate Future. In 1st IEEE International Conference on E-learning in Industrial Electronics, page 23–28. IEEE, 2006.

[15] Mu-Yen Chen, Edwin Lughofer, and Ken Sakamura. Information Fusion in Smart Living Technology Innovations. Information Fusion, (21):1–2, 2015.

[16] Sam Solaimani, Wally Keijzer-Broers, and Harry Bouwman. What we do – and don't – know about the Smart Home: an analysis of the Smart Home Literature. Indoor and Built Environment, 24(3):370–383, 2015.

[17] Richard Harper. Inside the Smart Home: Ideas, Possibilities andMethods. In Harper R. (eds) Inside the Smart Home, page 1–13. Springer, 2003.

Ένα άλλο σημαντικό σημείο αναφοράς του 20ου αιώνα ήταν η εισαγωγή της τεχνολογίας της πληροφορίας και της επικοινωνίας στα σπίτια. Το γεγονός αυτό δημιούργησε νέες δυνατότητες για την ανταλλαγή πληροφοριών που συνείσφεραν ουσιαστικά την εξέλιξη της τεχνολογίας έξυπνου σπιτιού[18].Ο πιο πρόσφατος και καθοριστικός παράγοντας της εξέλιξης του έξυπνου σπιτιού είναι οι συσκευές IoT και το σύνολο των τεχνολογιών που περιλαμβάνουν, όπως οι αισθητήρες.

Μπορούμε λοιπόν να ομαδοποιήσουμε την εξέλιξη του έξυπνου σπιτιού σε δύο στάδια:έξυπνα συνδεδεμένα σπίτια πριν από το IoT και έξυπνα συνδεδεμένα σπίτια με χρήση συσκευών IoT.

- Το 1966 – 1967 η πρώτη έξυπνη συσκευή η οποία όμως δεν έφτασε ποτέ στην αγορά, ήταν η ECHO IV. Αυτή η έξυπνη συσκευή μπορούσε να υπολογίσει τις λίστες αγορών, να ελέγχει τη θερμοκρασία του σπιτιού και να ενεργοποιεί και να απενεργοποιεί συσκευές όπως το κλιματιστικό και την τηλεόραση. Ένα χρόνο αργότερα, αναπτύχθηκε ο υπολογιστής κουζίνας από την εταιρεία Honeywell, ο οποίος είχε τηνδυνατότητα να αποθηκεύει συνταγές[19]
- Το 1991, η γεροντολογία ή αλλιώς γεροτεχνολογία εστίασε στην προαγωγή της ανθρώπινης υγείας και ευημερίας με σκοπό να κάνει τη ζωή των ηλικιωμένων πιο εύκολη. Στη δεκαετία του 1990, αναπτύχθηκε έρευνα και τεχνολογίες

---

[18] Drew Hendricks. The History of Smart Homes. https://www.iotevolutionworld.com/m2m/articles/376816-history-smart-homes.htm, 2014. Accessed: December 31, 2021

[19] Spicer, Dag (August 12, 2000). "If You Can't Stand the Coding, Stay Out of the Kitchen: Three Chaptersin the History of Home Automation". Dr. Dobb's Journal.

παρεμβάσεις όπως για παράδειγμα της πρόληψης και αποζημίωσης.[20]

- Το 1998 και στις αρχές της δεκαετίας του 2000, ο οικιακός αυτοματισμός, άρχισε να αυξάνεται σε δημοτικότητα. Ως εκ τούτου, άρχισε να αναδύεται καινούρια 20ου αιώνα.[7] Η ηλεκτρική ενέργεια πυροδότησε την εισαγωγή νέου εξοπλισμού στο σπίτι, όπως τις οικιακές συσκευές.
- Ένα άλλο σημαντικό σημείο αναφοράς του 20ου αιώνα ήταν η εισαγωγή της τεχνολογίας της πληροφορίας και της επικοινωνίας στα σπίτια. Το γεγονός αυτόδημιούργησε νέες δυνατότητες για την ανταλλαγή πληροφοριών που συνείσφεραν ουσιαστικά την εξέλιξη της τεχνολογίας έξυπνου σπιτιού[21].Ο πιο πρόσφατος και καθοριστικός παράγοντας της εξέλιξης του έξυπνου σπιτιού είναι οι συσκευές IoT και το σύνολο των τεχνολογιών που περιλαμβάνουν, όπως οι αισθητήρες.

- Το Νοέμβριο του 2014, η Amazon κυκλοφόρησε το πρώτο της ηχείο χρησιμοποιώντας τη φωνή ως κανάλι εισόδου παρέχοντας ένα πλήρες οικοσύστημα προγραμματιζόμενων δυνατοτήτων, με σκοπό τον έλεγχο του έξυπνου σπιτιού. Την ίδια χρονιά, η SmartThings παρήγαγε μια σουίτα προσαρμοσμένων υπηρεσιών, συμπεριλαμβανόμενων ενός κόμβου που λειτουργούσε ως

[20] http://www.gerontechjournal.net/

[21] Pogue, David (November 30, 2011). "A Thermostat That's Clever, Not Clunky". New York Times.Retrieved 2021-08-22

πύλη (gateway ή hub) που επέτρεπε την σύνδεση και την επικοινωνία διαφορετικών συσκευών.[22]

- Το 2015, η Apple κυκλοφόρησε το HomeKit3, το οποίο είχε ενσωματώσει ένα πλαίσιολογισμικού και ένα πρωτόκολλο δια λειτουργικότητας που επέτρεπε την επικοινωνίαμεταξύ διαφορετικών συσκευών.
- Σήμερα, στα έξυπνα σπίτια συναντάμε διάφορα είδη συσκευών, από εξελιγμένους αισθητήρες που χρησιμοποιούν τεχνολογίες AI, μέχρι μπάτλερ-ρομπότ που ακολουθούν τους χρήστες μέσα στο σπίτι, βοηθώντας τους στις δουλειές τους.[23]

3.2 Τομείς Εφαρμογής

Η ψυχαγωγία, η ασφάλεια και η υγειονομική περίθαλψη αποτελούν τους κυριότερους τομείς που βρίσκουν εφαρμογή οι πολλαπλές υπηρεσίες (εφαρμογές) που απαρτίζεται το έξυπνο σπίτι. [24] Τα έξυπνα σπίτια αυξάνονται ραγδαία σε αριθμό και σε δημοτικότητα στην εποχή του Διαδικτύου των πράγματων (IoT). Σύμφωνα με τα στατιστικά στοιχεία, ο αριθμός των έξυπνων οικιακών συσκευών υπολογίζεται σε 258.54 εκατομμύρια και αναμένεται να αυξηθεί σε 478.2 εκατομμύρια μέχρι το 2025.[25] Οι

---

[22] Ke Xu, Xiaoliang Wang, Wei Wei, Houbing Song, and Bo Mao.Toward Software Defined Smart Home. IEEE Communications Magazine, 54(5):116–122, 2016.

[23] https://news.samsung.com/us/samsung-ballie-ces-2020/

[24] https://www.statista.com/forecasts/887613/number-of-smart-homes-in-the-smart-home-market-in-the- world

[25] Tiago DP Mendes, Radu Godina, Eduardo MG Rodrigues, João CO Matias, and João PS Catalão. Smart Home Communication Technologies and Applications: Wireless

συσκευές, ιδίως μέσω της χρήσης αισθητήρων, συλλέγουν δεδομένα για τα οποία λαμβάνονται αποφάσεις. Η συλλογή περιλαμβάνει διαφορετικούς τύπους δεδομένων, μερικά από τα οποία είναι προσωπικά και ευαίσθητα. Τα παραδείγματα του πεδίου εφαρμογής των έξυπνων συσκευών καθώς και το είδος των δεδομένων που επεξεργάζονται, συνοψίζονται στο Πίνακα 1.

Πίνακας 1: Κατηγορίες πεδίου εφαρμογής των συσκευών IoT και αντίστοιχοι τύποι δεδομένων.

Κατηγορία	**Τύπος Συσκευής**	**Συλλεγόμενα δεδομένα**
Συστήματα ελέγχουκαι επιτήρησης ενέργειας	Έξυπνοι αισθητήρες ανίχνευσης κίνησης και συνθηκών περιβάλλοντος (νύχτα/ημέρα), Έξυπνες λάμπες, Έξυπνος διακόπτης για διαχείριση του θερμοσίφωνα, Έξυπνος θερμοστάτης	Δεδομένα κίνησης και θέσης, δεδομένα κατανάλωσης
Συστήματα οικιακήςψυχαγωγίας	Ηχεία με φωνητικές εντολές, αισθητήρες ανίχνευσης κίνησης, αισθητήρες εικόνας σε κινούμενα σχέδια, παιχνίδια, βίντεο, αντάπτορες μουσικής	Δεδομένα ήχου φωνής, Ερωτήματα αναζήτησης
Υγεία	Έξυπνες συσκευές μέτρησης αρτηριακής πίεσης και καρδιακών παλμών, Έξυπνες συσκευές μέτρησης σακχάρου	Δεδομένα υγείας, φυσικής κατάστασης, μετρήσεων του σώματος

Protocol Assessment for Home Area Network Resources. Energies, 8(7):7279–7311, 2015.

Παρακολούθηση καιασφάλεια	Κάμερες παρακολούθησης, αισθητήρας παραβίασης πόρτας, σειρήνα Smart	Δεδομένα κίνησης και θέσης, Δεδομένα εικόνας και ήχου, Προτιμήσεις επικοινωνίας
Δίκτυα και βοηθητικά προγράμματα	Πύλη/διανομέας, επέκταση ασυρμάτου δικτύου	Δεδομένα σχετικά με την συνδεσιμότητα, Προσωπικές προτιμήσεις
Αισθητήρες	Αισθητήρες ανίχνευσης καπνού, ανιχνευτής διαρροής νερού, μονάδα ποιότητας αέρα	Κατάσταση συσκευής, Δεδομένα θερμοκρασίας, τοποθεσίας ή αέρα
Οικιακές συσκευές	Έξυπνη σκούπα, έξυπνο πιρούνι, έξυπνος φούρνος, έξυπνη ζυγαριά	Μετρήσεις κατανάλωσης φαγητού, κατάστασησυσκευής

3.3 Αρχιτεκτονική Έξυπνου Σπιτιού

Το έξυπνο σπίτι αποτελείται από διάφορα δομικά στοιχεία που αλληλοεπιδρούν μεταξύ τους (βλ. Πίνακα 2), ανταλλάσσοντας δεδομένα σχετικά με την κατάσταση των αισθητήρων, καθώς και τις δραστηριότητες και τη συμπεριφορά των κατοίκων του.

Τα στοιχεία αυτά τείνουν να λειτουργούν ή να διαχειρίζονται από διαφορετικούς φορείς, εξυπηρετώντας τους εξής εμπλεκόμενους: τους τελικούς χρήστες δηλαδή τα υποκείμενα των δεδομένων, τους ελεγκτές δηλαδή τους υπεύθυνους επεξεργασίας των δεδομένων και τους διαχειριστές δεδομένων. Τα υποκείμενα των δεδομένων αντιπροσωπεύουν συνήθως τους κατοίκους έξυπνων σπιτιών, των οποίων τα δεδομένα υποβάλλονται σε επεξεργασία. Οι υπεύθυνοι επεξεργασίας δεδομένων, οι οποίοι μερικές φορές αναφέρονται και ως «κάτοχοι δεδομένων» ή «ελεγκτές δεδομένων» είναι οι οντότητες, συνήθως πάροχοι υπηρεσιών ή κατασκευαστές συσκευών, που συλλέγουν, αποθηκεύουν και επεξεργάζονται δεδομένα που δημιουργούνται από την εγγραφή στην εφαρμογή ελέγχου και την χρήση των συνδεδεμένων οικιακών συσκευών. Οι διαχειριστές των δεδομένων

αντιπροσωπεύουν τις οντότητες που έχουν πρόσβαση στα δεδομένα αυτά με σκοπό την αντιμετώπιση προβλημάτων για την ομαλή λειτουργία του συστήματος και της εφαρμογής.

Όσον αφορά την αρχιτεκτονική των δομικών στοιχείων του έξυπνου σπιτιού, αυτή αποτελείται από τα ακόλουθα:

- Σπίτι: Αντιπροσωπεύει το σύνολο των φυσικών τοποθεσιών που απαρτίζουν την κατοικία, π.χ. διαμέρισμα, συμπεριλαμβανομένων όλων των περιοχών που βρίσκονται εντός του.
- Συσκευή IoT: Ο όρος αναφέρεται στις οικιακές συσκευές, όπως φώτα ή αισθητήρες, που μπορούν να ανιχνεύσουν, να ενεργοποιήσουν, να επεξεργαστούν δεδομένα και να επικοινωνήσουν με τον τελικό χρήστη μέσω της εφαρμογής από την κινητή συσκευή του. Οι τρεις βασικές συσκευές είναι οι αισθητήρες, οι ενεργοποιητές και οι κινητές συσκευές του τελικού χρήστη. Οι αισθητήρες ανιχνεύουν, παρακολουθούν και μετρούν ιδιότητεςαντικειμένων όπως η θερμοκρασία δωματίου. Οι ενεργοποιητές εκτελούν ενέργειες στο φυσικό περιβάλλον, όπως ενεργοποίηση ή απενεργοποίηση φώτων. Οι συσκευές του τελικού χρήστη, όπως τα smartphones, χρησιμοποιούνται συνήθως από τα υποκείμενα των δεδομένων για την αλληλεπίδραση και τη διαχείριση του έξυπνου σπιτιού.

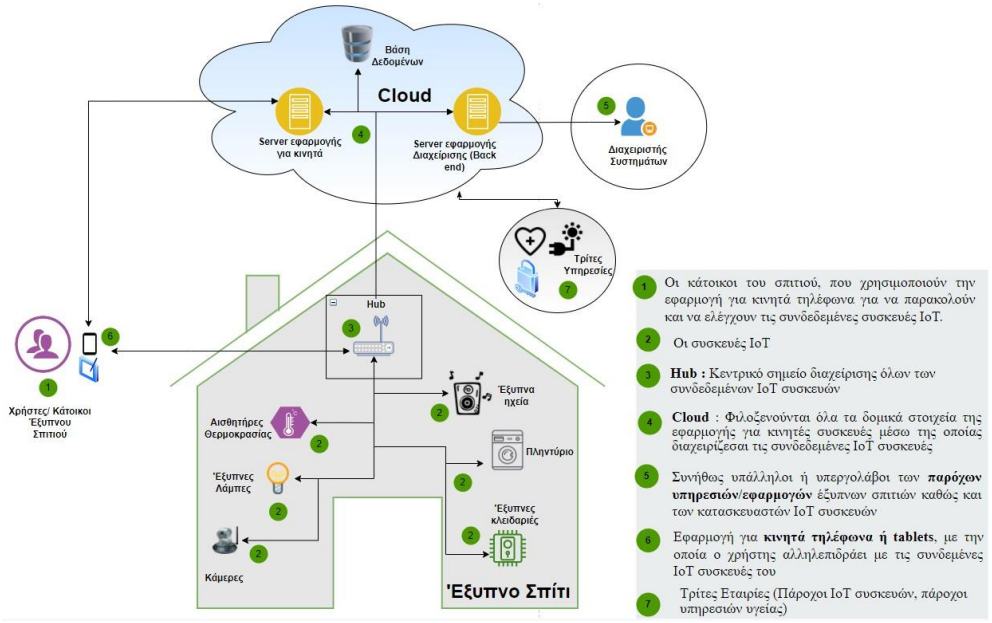
- Πύλη. Η πύλη (hub) είναι μια εξειδικευμένη συσκευή που συλλέγει δεδομένα από όλες τιςεγκατεστημένες IoT συσκευές, είναι σε θέση να μεταφράζει πολλά διαφορετικά πρωτόκολλα και λειτουργεί συνήθως ως το κεντρικό σημείο για τη διαχείριση των συνδεδεμένων συσκευών, από τους τελικούς χρήστες. Ορισμένες IoT συσκευές, όπως τα έξυπνα ηχεία, παρέχουν ενσωματωμένη λειτουργία πύλης.

- Σύννεφο. Το cloud χρησιμοποιείται από ορισμένες IoT συσκευές ως back-end για την αποθήκευση και την επεξεργασία

δεδομένων, και μερικές φορές ως μηχανισμός για την ενσωμάτωση διαφορετικών αυτόνομων συνδεδεμένων συσκευών. Στο cloud αποθηκεύονται οι βάσεις δεδομένων, το λειτουργικό της εφαρμογής για κινητές συσκευές, οι εφαρμογές λογισμικού που παρέχουν τη δυνατότητα ελέγχου, διαχείρισης και λειτουργίας του συστήματος έξυπνου σπιτιού και άλλα τεχνικά δομικά στοιχεία.

• Χρήστη: Το ενδιαφερόμενο μέρος που χρησιμοποιεί και επωφελείται από τις υπηρεσίες που προσφέρει το έξυπνο σπίτι. Συνήθως, ο όρος αντιπροσωπεύει τα υποκείμενα των δεδομένων.

Σχήμα 1: Επικρατέστερη αρχιτεκτονική έξυπνου σπιτιού.



Συνήθως, οι χρήστες/ υποκείμενα των δεδομένων (ένας τύπος χρήστη) έχουν πρόσβαση σε συνδεδεμένες IoT συσκευές τους, μέσω smartphone. Συνήθως, η αλληλεπίδραση μεταξύ του smartphone και μιας συνδεδεμένης IoT συσκευής, πραγματοποιείται μέσω μιας πύλης (hub). Ανάλογα με τομοντέλο επικοινωνίας, ορισμένες IoT συσκευές μπορούν να στείλουν δεδομένα απευθείας στο cloud. Ωστόσο, αυτό συχνά διευκολύνεται μέσω της πύλης.

3.4 Ζητήματα Ιδιωτικότητας

Όπως αναφέραμε παραπάνω, εκτός όμως από τα θετικά και τα οφέλη του IoT, προκύπτουν τόσο ζητήματα προστασίας των δεδομένων που συλλέγονται από το IoT, όσο και ζητήματα ασφάλειας για τις ίδιες τις συσκευές. Για τον λόγο αυτό, δεν πρέπει να αγνοούνται οι επιπτώσεις τους στην ιδιωτική ζωή του χρηστών του. Ορισμένες συσκευές καταμετρούν τους καρδιακούς παλμούς και τα κύματα του εγκεφάλου. Με την παρατήρηση των δεδομένων αυτών, συνάγονται πληροφορίες σχετιζόμενες με την υγεία του χρήστη. Δεν είναι λίγες οι περιπτώσεις που οι συσκευές στέλνουν ειδοποιήσεις, όταν ο χρήστης παραμελεί τη φυσική του κατάσταση αναγνωρίζοντας κάποια συμπτώματα ασθένειας.

Η ανάπτυξη και η παρουσία IoT συσκευών εντός του σπιτιού μπορεί μεν να αυξήσει την αποτελεσματικότητα και την ποιότητα ζωής των κατοίκων αλλά ταυτόχρονα, οι συσκευές συλλέγουν, επεξεργάζονται και μεταδίδουν δεδομένα σχετικά με τους κατοίκους και τις καθημερινές δραστηριότητες τους, σε άγνωστα μέρη χωρίς την προηγούμενη ενημέρωση τους. Τα δεδομένα μπορεί να είναι προσωπικά και μερικές φορές ευαίσθητα, οδηγώντας παράλληλα σε όλο και περισσότερη γνώση σχετικά με την ιδιωτική ζωή των κατοίκων που χρησιμοποιούν την υπηρεσία Smart Home.

Ένα πλήρως εξοπλισμένο έξυπνο σπίτι, με συσκευές IoT στην κουζίνα, στο μπάνιο, στο αυτοκίνητο, στον κήπο ή οπουδήποτε αλλού, συλλέγει δεδομένα όπως την ώρα που επιστρέφει ο κάτοικος στο σπίτι από τη δουλειά, μέσω των αισθητήρων της γκαραζόπορτας. Το έξυπνο κρεβάτι αλλά και το έξυπνο ρολόι συλλέγουν πληροφορίες για τις ώρες που κοιμάται ο κάτοικος, ενώ το έξυπνο ψυγείο γνωρίζει το αγαπημένο του σνακ, μια έξυπνη κλειδαριά πόρτας γνωρίζει τις καθημερινές εισόδους και εξόδους κάποιου κατοίκου, η έξυπνη τηλεόραση είναι σε θέση

να παρακολουθεί τις συνήθειες θέασης αλλά και να καταγράφει συνομιλίες των θεατών. Το υποκείμενο των δεδομένων μπορεί βέβαια να αγνοεί τελείως την ίδια την ύπαρξη των αισθητήρων καθώς ενσωματώνονται σε μη εμφανή χώρο, στο εσωτερικό της συσκευής. Έτσι λοιπόν, ένας χρήστης μπορεί να μην γνωρίζει ότι η γενικότερη συμπεριφορά του αποθηκεύεται σε κεντρική βάση με αποτέλεσμα να δημιουργείται ένα προφίλ για τον χρήστη. Για παράδειγμα, συνδυάζοντας και συνδέοντας δεδομένα που σχετίζονται με κινήσεις, καρδιακούς παλμούςκαι ρυθμό αναπνοής, είναι δυνατόν να συναχθούν πιθανές ψυχολογικές διαταραχές λόγω αϋπνίας και εν τέλει να δημιουργηθεί ψυχογράφημα του ατόμου. Τα ζητήματα ιδιωτικότητας γίνονται ακόμη πιο περίπλοκα όταν εξετάζουμε το αποκεντρωμένο σενάριο IoT όπου οι συσκευές έχουν την δυνατότητα να επεξεργάζονται και να μοιράζονται δεδομένα αναμεταξύ τους. Σε αυτό το σενάριο, ευαίσθητες πληροφορίες των κατόχων δεδομένων μπορούν να εξαχθούν μέσω της ανάλυσης. Μέθοδοι δημιουργίας προφίλ χρησιμοποιούνται ως επί το πλείστων για την προσωποποιημένη διαφήμιση στο ηλεκτρονικό εμπόριο (π.χ. σε συστήματα προτάσεων για ενημερωτικά δελτία και διαφημίσεις) αλλά και για την βελτιστοποίηση των εσωτερικών διαδικασιών των Εταιριών με βάση τα ενδιαφέροντα του χρήστη και τα δημογραφικά του στοιχεία. Η αναγνώριση ομιλίας επίσης χρησιμοποιείται ευρέως σε διάφορες εφαρμογές διαθέσιμες σε κινητά τηλέφωνα και ήδη κατασκευάζονται τεράστιες βάσεις δεδομένων με δείγματα ομιλίας. Με την αναγνώριση ομιλίας να εξελίσσεται ως ο επικρατέστερος τρόπος αλληλεπίδρασης των ανθρώπων με τις συσκευές IoT στο Smart Home, πληθαίνουν ακόμα περισσότερο οι στόχοι επιθέσεων και τα ρίσκα σχετικά με την ιδιωτικότητα. Τα παραπάνω δείχνουν, ότι ο κίνδυνος στην δημιουργία προφίλ, βρίσκεται στη ταξινόμηση του ίδιου του υποκειμένου σε διάφορες κατηγορίες, όπως, σε σπάταλους, επικίνδυνους, διάγοντες

ανθυγιεινό τρόπο ζωής και στην μεταφορά των δεδομένων από τρίτους. Παραδείγματα όπου η δημιουργία προφίλ οδηγεί σε παραβίαση της ιδιωτικότητας είναι οι διακρίσεις στις προνομιακές τιμές,[2627] οι ανεπιθύμητες διαφημίσεις,[28] η κοινωνική μηχανική[29] και η εσφαλμένη αυτοματοποιημένη λήψη αποφάσεων.

Στο Smart Home, συχνά συναντάται η μη ύπαρξη προηγούμενης ενημέρωσης σχετικά με τον τρόπο κοινοποίησης και επεξεργασίας των δεδομένων. Τα δεδομένα αυτά συλλέγονται κατά κύριο λόγο από τους κατασκευαστές των έξυπνων συσκευών ή/και τις Εταιρίες που πωλούν την εφαρμογή για την διαχείριση έξυπνων οικιακών συσκευών, με σκοπό την ομαλή λειτουργία της υπηρεσίας και την αυτοματοποίηση ενισχύοντας τα πλεονεκτήματα που προσφέρονται από τεχνολογίες έξυπνων κατοικιών. Πράγματι, σχεδόν όλες οι συσκευές χρειάζεται να συλλέξουν και να αναλύσουν τα δεδομένα και τις συνήθειες των

---

[26] Odlyzko A. Privacy, economics, and price discrimination on the internet. Proceedings of the 5thinternational conference on Electronic commerce, ICEC '03, ACM, 2003; 355–366, doi:10.1145/948005.948051.

[27] Kwasniewski N. Apple-nutzer zahlen mehr fur¨ hotelzimmer. http://bit.ly/MRBTwT

[28] Orgill GL, Romney GW, Bailey MG, Orgill PM. The urgency for effective user privacy education tocounter social engineering attacks on secure computer systems. Proceedings of the 5th conference on Information technology education, CITC5 '04, ACM, 2004; 177–181, doi:10.1145/ 1029533.1029577

[29] Spiekermann S, Cranor L. Engineering Privacy. Software Engineering, IEEE Transactions on 2009; 35(1):67 –82, doi:10.1109/TSE.2008.88.

χρηστών προκειμένου να λειτουργούν στο μέγιστο των δυνατοτήτων τους. Για παράδειγμα, πόσο χρήσιμο θα ήταν εν τέλει ένα έξυπνο ψυγείο αν δεν μπορεί να επεξεργαστεί τις συνήθειες των κατοίκων με σκοπό να συνεισφέρει σε πιο ουσιαστικές αγορές. Παράλληλα, είναι ζωτικής σημασίας να καθορίσουμε όλα τα μέρη και πληροφοριακά συστήματα που αποθηκεύουν τα προσωπικά μας δεδομένα καθώς ο αυξανόμενη αριθμός κυβερνοεπιθέσεων σε υπηρεσίες και συσκευές Smart Home, θέτει σε κίνδυνο το απόρρητο και την ασφάλεια των ίδιων των κατοίκων. Η ενσωμάτωση οργανωτικών και τεχνικών μέτρων για την ενίσχυση του απορρήτου και της ασφάλειας είναι ένα κρίσιμο ζήτημα στο Smart Home. Έρευνες, όπως θα δούμε και παρακάτω, παρουσιάζουν ότι πολλοί από τους ανθρώπους που χρησιμοποιούν αυτές τις υπηρεσίες αυτές, ανησυχούν για τη μη εξουσιοδοτημένη πρόσβαση στα σπίτια τους και για το απόρρητο των δεδομένων τους.

Η προστασία της ταυτότητας και, κατ' επέκταση , η προστασία από την ταυτοποίηση ενός ατόμου είναι κυρίαρχο ζήτημα στην προστασία της ιδιωτικής ζωής στις RFID τεχνολογίες, αλλά αποτελεί και το πρώτο μέλημα για τις τεχνολογίες ανωνυμοποίησης δεδομένων[30] [31] [32], που σκοπό έχουν την ενίσχυση

---

[30] Sweeney L. k-anonymity: a model for protecting privacy. Int. J. Uncertain. Fuzziness Knowl.Based Syst. 2002; 10(5):557–570, doi:10.1142/S0218488502001648.

[31] Uzuner ¨O, Luo Y, Szolovits P. Evaluating the Stateof-the-Art in Automatic De-identification. Journal

of the American Medical Informatics Association 2007; 14(5):550–563, doi:10.1197/jamia.M2444.

[32] Fung BCM, Wang K, Chen R, Yu PS. Privacy preserving data publishing: A survey of recentdevelopments. ACM Comput. Surv. 2010; 42(4):14:1– 14:53, doi:10.1145/1749603.1749605.

της προστασίας της ιδιωτικότητας [33] [34]. Ωστόσο, αυτές οι λύσεις είναι δύσκολα εφαρμόσιμες στο Smart Home, καθώς οι περισσότερες τεχνικές ανωνυμοποίησης δεδομένων μπορούν να παρακαμφθούν με την χρήση συμπληρωματικών δεδομένων [35] [36], που είναι πολύ πιθανό να είναι διαθέσιμα κατά τη διάρκεια χρήσης των συσκευών στο Smart Home. Επίσης, οι λύσεις κρυπτογράφησης, είναι κυρίως σχεδιασμένες για πολύ πιο απλά δικτυακά περιβάλλοντα, όπως δίκτυα επιχειρήσεων ή οικιακά δίκτυα και έτσι είναι δύσκολο να εφαρμοστούν στο κατανεμημένο και ετερογενές περιβάλλον του IoT. Οι λύσεις RFID τεχνολογίας, θα μπορούσαν να εφαρμοστούν για την ενίσχυση της ιδιωτικότητας, λόγω της ομοιότητας τους στους περιορισμένους πόρους. Ωστόσο, αυτές οι προσεγγίσεις δεν λαμβάνουν υπόψη τις διαφορετικές πηγές δεδομένων που διατίθενται στο IoT όπως π.χ. εικόνες κάμερας και δείγματα ομιλίας.

Ο εντοπισμός και η παρακολούθηση των δεδομένων κίνησης και θέσης ενός ατόμουαποτελούν επίσης απειλή για την

---

[33] Camenisch J, Van Herreweghen E. Design and implementation of the idemix anonymous credential system. Proceedings of the 9th ACM conference on Computer and communications security, CCS '02, ACM, 2002; 21–30, doi:10.1145/586110.586114.

[34] Camenisch J, shelat a, Sommer D, Fischer-H¨ubner S, Hansen M, Krasemann H, Lacoste G, Leenes R, Tseng J. Privacy and identity management for everyone. Proceedings of the 2005 workshop on Digital identity management, DIM '05, ACM, 2005; 20–27, doi:10.1145/1102486.1102491.

[35] Barbaro M, Zeller T. A Face Is Exposed for AOL Searcher No. 4417749. New York Times.http://nyti.ms/H6vd2 [Online]

[36] Narayanan A, Shmatikov V. Myths and fallacies of "Personally Identifiable Information".
Communications of the ACM 2010; 53:24–26, doi:10.1145/ 1743546.1743558

ιδιωτικότητα. Ήδη στις μέρες μας, η παρακολούθηση είναι δυνατή με διάφορα μέσα, π.χ. GPS, μέσω της διαδικτυακής μασκίνησης ή μέσω της τοποθεσίας του κινητού μας τηλεφώνου. Μέσω των παραπάνω μέσων έχουν υπάρξει πολλές παραβιάσεις στην ιδιωτικότητα, όπως για παράδειγμα η επίμονη παρακολούθηση των μετακινήσεων ενός ατόμου,[37] η αποκάλυψη σχετικά με την κατάσταση υγείας ενός ατόμου,[38] ή το δυσάρεστο αίσθημα ότι παρακολουθείσαι[39]. Παρά ταύτα, ο εντοπισμός και η παρακολούθηση είναι από τις σημαντικές λειτουργίες πολλών IoT συστημάτων, οι χρήστες του όμως δεν αντιλαμβάνονται ως παραβίαση το ότι δεν έχουν έλεγχο των δεδομένων κίνησης και θέσης τους ή το ότι δεν έχουν γνώση αν η πληροφορία αυτή διαμοιράζεται. Παραδοσιακά, ο εντοπισμός και η παρακολούθηση αποτελούν απειλή κυρίως στη φάση της επεξεργασίας πληροφοριών, όταν τα δεδομένα κίνησης και θέσης αποθηκεύονται στο backend οπού εκεί χάνεται ο έλεγχος του υποκειμένου.

Η εξέλιξη της τεχνολογίας του IoT αλλάζει και επιδεινώνει τον κίνδυνο με τρεις διαφορετικούς τρόπους: αρχικά παρατηρείται αύξηση των υπηρεσιών που βασίζονται στην τοποθεσία για την λειτουργία τους. Δεύτερον, οι τεχνολογίες IoT όχι μόνο

---

[37] Voelcker J. Stalked by satellite - an alarming rise in GPS-enabled harassment. Spectrum, IEEE 2006;(7):15–16, doi:10.1109/MSPEC.2006.1652998.

[38] Chow CY, Mokbel MF. Privacy in location based services: a system architecture perspective. SIGSPATIAL Special 2009; 1(2):23–27, doi:10.1145/1567253.1567258

[39] Toch E, Wang Y, Cranor LF. Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems. User Modeling and User-Adapted Interaction 2012; 22(1):203–220, doi: 10.1007/s11257-011-9110-z.

ενθαρρύνουν την ανάπτυξη υπηρεσιών που βασίζονται σε δεδομένα κίνησης και θέσης αλλά βελτιώνουν και την ακρίβεια των δεδομένων αυτών. Το σημαντικότερο βέβαια είναι πως καθώς η συλλογή δεδομένων γίνεται πιο παθητική, πιο διαδεδομένη και λιγότερο εμφανώς παρεμβατική, οι χρήστες δεν είναι ενήμεροι για το πότε παρακολουθούνται και για τους σχετικούς κινδύνους. Τρίτον, η αυξανόμενη αλληλεπίδραση με έξυπνα πράγματα και συστήματα αφήνει ίχνη δεδομένων που όχι μόνο θέτουν τον χρήστη στον κίνδυνο ταυτοποίησης, αλλά κάνει δυνατή την παρακολούθηση της τοποθεσίας και της δραστηριότητά του, π.χ. με NFC enabled smartphones για την αγορά εισιτηρίου στο λεωφορείο. Με αυτές τις εξελίξεις, ο κίνδυνος τουεντοπισμού και της παρακολούθησης θα εμφανίζεται επίσης στην φάση αλληλεπίδρασης, καθιστώντας το θέμα ανιχνεύσιμο σε καταστάσεις όπου αυτός μπορεί να αντιληφθεί ψευδώς τον φυσικό διαχωρισμό από άλλους, π.χ. από τοίχους ή ράφια, ως απόρρητο.

Καταλαβαίνουμε λοιπόν, ότι τα δεδομένα που παράγονται από τις IoT είναι συνυφασμένα με πολλές πτυχές της καθημερινής μας ζωής αν λάβουμε υπόψη πόσες διαφορετικές συσκευές επεξεργάζονται τα προσωπικά μας δεδομένα. Με τόσο μεγάλο αριθμό συσκευών που συλλέγουν και επεξεργάζονται προσωπικά δεδομένα, το άτομο είναι υπό μη ελεγχόμενη, αλλά και άγνωστη επιτήρηση[40], με αποτέλεσμα η προστασία της ιδιωτικής ζωής των ατόμων αποτελεί σημαντική πρόκληση.

---

[40] Neil M. Richards, Symposium: Privacy and Technology: The Dangers of Surveillance, 126 Harvard Law Review 2013, σ. 1934 επ. (1935).

3.4.1 Ένδικες Διαφορές - Ιδιωτικότητα

Ένα παράδειγμα στο οποίο γίνονται κατανοητά τα ζητήματα που απορρέουν απότης χρήση συσκευών IoT γενικότερα, είναι υπόθεση Zak vs Bose Corp, U.S. District Court, Northern District of Illinois, No. 17-0292831.Το 2017 ο Kyle Zak κατέθεσε μήνυση κατά της Bose ισχυριζόμενος ότι η εταιρεία κατασκοπεύει τους πελάτες της, παρακολουθώντας τη μουσική που ακούνε, τα podcast τους μέσω της εφαρμογής Bose Connect που συνδέεται με τα ασύρματα ακουστικά τους και στη συνέχεια πουλά αυτές τις πληροφορίες χωρίς την άδεια τους. ο Zak ζήτησε αποζημίωση εκατομμυρίων δολαρίων εκ μέρους αγοραστών ακουστικών και ηχείων Bose καθώς και τη διακοπή της συλλογής δεδομένων, η οποία, παραβιάζει τον ομοσπονδιακό νόμο περί υποκλοπών (Wiretap Act) και τους νόμους του Ιλινόι κατά της υποκλοπής και τηςαπάτης των καταναλωτών. [41]Η υπόθεση πήρε μεγάλη διάσταση διότι έφερε στο φως πολλές από τις ανησυχίες του κοινού σχετικά με τις συσκευές IoT, οι οποίες τις περισσότερες φορέςέχουν ως γνώμονα μόνο την λειτουργικότητα παραμερίζοντας την ασφάλεια των δεδομένων των καταναλωτών.

Η Bose κατασκευάζει και πουλάει προϊόντα ήχου, μεταξύ άλλων και ασύρματα ακουστικά, τα οποία και χρησιμοποιούν οι καταναλωτές για να ακούν μουσική από streaming πλατφόρμες, όπως το Spotify και το Apple Music. Μαζί με τα ακουστικά η BOSE, κατά την αγορά, ενθαρρύνει τους πελάτες της να κατεβάσουν και το Bose Connect app, για να μεγιστοποιήσουν τις δυνατότητες των ακουστικών τους. Η εφαρμογή αυτή δίνει τη δυνατότητα στον χρήστη να ρυθμίζει βασικές λειτουργίες των ακουστικών, να κάνει παύση,να αλλάζει τραγούδια κλπ. Επίσης η εφαρμογή εμφανίζει

---

[41] https://law.justia.com/cases/federal/district-courts/illinois/ilndce/1:2017cv02928/338970/70/

τον τίτλο του κομματιού που αναπαράγεται, τον καλλιτέχνη και το άλμπουμ. Οι ισχυρισμοί επισήμαναν ότι η εφαρμογήμπαίνει σαν ενδιάμεσος μεταξύ της streaming πλατφόρμας και του χρήστη, παίρνοντας σαν πληροφορία τα στοιχεία του τραγουδιού που ακούει ο χρήστης και στη συνέχεια τα εμφανίζει στην οθόνη του. Με αυτό τον τρόπο η Bose συγκεντρώνει δεδομένα για τις ακουστικές συνήθειες του κάθε πελάτη της και στη συνέχεια, κατά τον Kyle Zak, πουλάει αυτά τα δεδομένα σε άλλες εταιρείες, χωρίς αυτό να αναφέρεται στην πολιτική απορρήτου και στους όρους και προϋποθέσεις της εφαρμογής.[42] Σύμφωνα με τον Zak, η Bose πούλησε αυτά τα δεδομένα σε μια εταιρεία που κάνει data mining την Segment.i.o, της οποίας η Bose είναι πελάτης. Αυτές οι πληροφορίες, σε συνδυασμό με τα προσωπικά στοιχεία που έδωσαν οι χρήστες κατά την εγγραφή στην εφαρμογή, δίνουν μια δυνητικά αρκετά εμπορεύσιμη βάση δεδομένων. Ο Zak ισχυρίστηκε ότι δεν έδωσε στη Bose άδεια να συγκεντρώσει αυτά τα δεδομένα, πόσο μάλλον πουλήσει αυτές τις πληροφορίες σε τρίτους.

Ανεξάρτητα από το αν οι ισχυρισμοί του Ζακ είναι πραγματικοί, το περιεχόμενο πολυμέσων, όπως τα podcasts, μπορεί να αποκαλύψει σημαντικά στοιχεία για το άτομο, όπως τις πεποιθήσεις του, τις πολιτικές του τοποθετήσεις, τις σεξουαλικές του προτιμήσεις, τη θρησκεία του, μέχρι και την κατάσταση της υγείας του. Αυτό επιτρέπει σε κάθε συλλέκτη τέτοιων δεδομένων να δημιουργήσει ένα ακριβές, προσωπικό προφίλ, θέτοντας τον σε κίνδυνο και παραβιάζοντας τα θεμελιώδη δικαιώματα του.

---

[42] https://www.cpomagazine.com/data-privacy/bose-hit-privacy-infringement-claim/

3.4.2 Κανονιστικό πλαίσιο

Οι παραπάνω επικρατούσες καταστάσεις και συνθήκες, έκριναν από απαραίτητη την ανάπτυξη και εφαρμογή ενός ισχυρού και συνεκτικού πλαισίου προστασίας των προσωπικών δεδομένων των πολιτών της ΕΕ. Προκειμένου λοιπόν να διασφαλιστεί η προστασία των προσωπικών δεδομένων των πολιτών της Ευρωπαϊκής Ένωσης, δημιουργήθηκε ο Γενικός Κανονισμός Προστασίας Δεδομένων της Ευρωπαϊκής Ένωσης (GDPR)[43], ο οποίος εισάγαγε αρχές προστασίας δεδομένων και αυξημένα δικαιώματα των υποκειμένων των δεδομένων[44].

Κύρια και βασική αρχή αποτέλεσε η παραδοχή ότι τα φυσικά πρόσωπα έχουν δικαίωμα προστασίας της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Και το δικαίωμα αυτό είναι θεμελιώδες, το οποίο και θα ρυθμίζεται με συνέπεια σε όλα τα κράτη – μέλη της Ευρωπαϊκής Ένωσης, μέσω της εφαρμογής του νέου Κανονισμού. Αυτό ορίζεται στο Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (άρθρο 8, παράγραφος 1), καθώς και στη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης (άρθρο 16, παράγραφος 1).

Συνεπώς, ο βαθμός και το βάθος της επεξεργασίας στην οποία υπόκεινται και υποβάλλονται τα δεδομένα προσωπικού

---

[43] Toch E, Wang Y, Cranor LF. Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems. User Modeling and User-Adapted Interaction 2012; 22(1):203–220, doi: 10.1007/s11257-011-9110-z.

[44] Yod-Samuel Martin and Antonio Kung. Methods and tools for gdpr compliance through privacy and data protection engineering. In 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pages 108–111. IEEE, 2018.

χαρακτήρα, θα πρέπει να γίνεται με γνώμονα την εξυπηρέτηση του ανθρώπου. Στην εποχή του big data, του cloud computing και του IoT ο Κανονισμός στοχεύει στην μεγίστη προστασία των δεδομένων προσωπικού χαρακτήρα από την όποια επεξεργασία στην οποία υποβάλλονται.

Παρέχει ο Κανονισμός τη δυνατότητα στα φυσικά πρόσωπα να ασκούν μεγαλύτερο έλεγχο επί των προσωπικών τους δεδομένων. Αυτό διασφαλίζεται μέσω της απαραίτητης συγκατάθεσης του ατόμου για την δυνατότητα επεξεργασίας των προσωπικών του δεδομένων, της απλοποίησης των διαδικασιών πρόσβασης στα αρχεία που τηρούνται τα προσωπικά του δεδομένα, του δικαιώματος διόρθωσης, διαγράφης και λήθης, καθώς και εναντίωσης στη χρήση των προσωπικών δεδομένων προκειμένου να καταρτιστεί προφίλ. Παράλληλα, τίθενται περιορισμοί και υποχρεώσεις στις επιχειρήσεις ως προς την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, τη δυνατότητα μεταβίβασης και διακίνησης σε αλλά κράτη, την προστασία των δικαιωμάτων των ανθρώπων, την εμπιστευτικότητα, διαθεσιμότητα, ακεραιότητα και γενικά την ασφάλεια των προσωπικών δεδομένων, καθώς και τις ενέργειες γνωστοποιήσεως στις οποίες οφείλει να προβεί η επιχείρηση σε περιπτώσεις παραβίασης της ασφάλειας.

3.4.3 Συσκευές IoT και ΓΚΠΔ

Μία διεθνής μελέτη που διεξήχθη από 25 ρυθμιστικές αρχές προστασίας δεδομένων και συντονίστηκε από το Παγκόσμιο Δίκτυο Προστασίας Προσωπικών Δεδομένων εξέτασε περισσότερες από 300 συσκευές, όπως έξυπνους μετρητές, θερμοστάτες και ρολόγια που παρακολουθούν την υγεία, και διαπίστωσε ότι έξι στις δέκα συσκευές Internet of Things (IoT)δεν ενημερώνουν επαρκώς τα δεδομένα σχετικά με τον τρόπο συλλογής και χρήσης των προσωπικών τους στοιχείων.

Η μελέτη διαπίστωσε επίσης ότι:

- Το 59% των συσκευών δεν κατάφεραν να ενημερώσουν επαρκώς τους χρήστες πώς συλλέχθηκαν, χρησιμοποιήθηκαν και κοινοποιήθηκαν τα προσωπικά τους δεδομένα.
- Το 68% απέτυχε να εξηγήσει ορθά και αναλυτικά το τρόπο που αποθηκεύονται οι πληροφορίες.
- Το 72% απέτυχε να εξηγήσει πώς οι χρήστες μπορούν να διαγράψουν τα δεδομένα τους από τη συσκευή.
- Το 38% απέτυχε να συμπεριλάβει στοιχεία επικοινωνίας σε περίπτωση που κάποιος χρήστης θελήσει περαιτέρω ενημέρωση σχετικά με τον τρόπο επεξεργασίας των δεδομένων τους.

Τα δεδομένα από τις συσκευές IoT, μεταφέρονται στον κατασκευαστή της συσκευής κάτι που τον καταστεί υπεύθυνο επεξεργασίας των δεδομένων[45]. Όπως δηλώνεται από τον ΓΚΠΔ, τα υποκείμενα των δεδομένων πρέπει να έχουν μεγαλύτερη διαφάνεια σχετικά με τον τρόπο επεξεργασίας των δεδομένων τους[46]. Κατά τον ΓΚΠΔ, ο υπεύθυνος της επεξεργασίας είναι υπεύθυνος για την ενημέρωση των υποκειμένων των δεδομένων σχετικά με το ποια δεδομένα υπόκεινται σε επεξεργασία, ποιος έχει πρόσβαση σε αυτά, τον τόπο αποθήκευσης και τον χρόνο διατήρησης τους και τα μέτρα ασφαλείας που έχουν εφαρμοστεί.

---

[45] Βλ. Ομάδα Εργασίας του Άρθρου 29, Γνώμη 1/2010, σκ. III.1.α, σχετικά με τις έννοιες του «υπευθύνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία», διαθέσιμη σε: https://ec.europa.eu/%20justice/policies/privacy/docs/wpdocs/2010/wp169_el.pdf#h2-5

[46] euΓΚΠΔ.org/the-regulation/ΓΚΠΔ-faqs

Επομένως, τα παραπάνω στατικά καθώς και το ότι δεν υπάρχει ευρεία γνώση για τις δυνατότητες του IoT, υφίσταται ο κίνδυνος η επεξεργασία των δεδομένων προσωπικού χαρακτήρα να λαμβάνει χώρα χωρίς έγκυρη νομική βάση. Δεδομένου ότι ο χρήστης δεν είναισε θέση να γνωρίζει την εν λόγω επεξεργασία δεδομένων και τους αποδέκτες των δεδομένων του[47], δεν μπορεί να δώσει και την συγκατάθεση του.

4. ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ

Στο πέρασμα των χρόνων, έχουν προταθεί πολλοί διαφορετικοί ορισμοί σχετικά με τον κίνδυνο. Ο διεθνής τυποποιημένος ορισμός είναι ότι ο κίνδυνος αποτελεί την ανεπιθύμητη επίδραση της αβεβαιότητας στην επίτευξη των στόχων. [48] Με απλά λόγια, ο κίνδυνος είναι άμεσα συνδεδεμένος με τη πιθανότητα να συμβεί κάτι ανεπιθύμητο ή κακό [49].Ο κίνδυνος περιλαμβάνει την αβεβαιότητα εστιάζοντας σε αρνητικές, ανεπιθύμητες συνέπειες σχετικά με τα αποτελέσματα μιας δραστηριότητας σε σχέση με τις αρχικές προσδοκίες (όπως η κατάσταση υγείας, η ευημερία, ο πλούτος, η περιουσία, το περιβάλλον, το αποτέλεσμα ενός έργου). Η κατανόηση και η περιγραφή του κινδύνου, οι μέθοδοι αξιολόγησης και διαχείρισης του, ακόμη και οι ορισμοί του διαφέρουν σε ανάλογα με τον

---

[47] Βλ. With tracking devices, employers may track workers' health, 4.1.2013, διαθέσιμο σε: "http://www.

advisory.com/Daily-Briefing/2013/01/04/With-tracking-devicesemployers-may-track-workers-health,

[48] "Guide 73:2009 Risk Management - Vocabulary". ISO.

[49] "Risk". Cambridge Dictionary.

τομέα εφαρμογής του (επιχειρήσεις, οικονομία, περιβάλλον, χρηματοοικονομικά, τεχνολογία, υγεία, ασφάλιση, ασφάλεια συστημάτων, προστασία δεδομένων κλπ.).

Ο κίνδυνος στο τομέα της πληροφορικής (ή ο κίνδυνος στον κυβερνοχώρο) προκύπτει από την πιθανότητα μια απειλή να εκμεταλλευτεί μια ευπάθεια του πληροφοριακού συστήματος ή του οργανισμού που ανήκει το πληροφοριακό σύστημα με σκοπό να παραβιάσει την ασφάλεια του και να προκαλέσει ζημιά. Ο κίνδυνος όμως δεν περιορίζεται μόνο στην πρόκληση ζημιάς στο πληροφοριακό σύστημα διαταράσσοντας τις επιχειρηματικές λειτουργίες ενός οργανισμού, αλλά μπορεί να περιλαμβάνει και κίνδυνο για την ανθρώπινη ζωή (π.χ. στα βιομηχανικά σύστημα), κίνδυνο μη συμμόρφωσης με νόμους και κανονισμούς, κίνδυνο για την φήμη της εταιρείας κλπ. Ο κίνδυνος στο τομέα της πληροφορικής εστιάζεται στην ασφάλεια των ηλεκτρονικών υπολογιστών, οι κίνδυνοι όμως επεκτείνονται όπως, έντυπες μορφές των πληροφοριών (π.χ. χαρτί, μικροφίλμ).

Παραδείγματα απειλών για τα πληροφοριακά συστήματα αποτελούν το ηλεκτρονικό έγκλημα, η πλαστοπροσωπία, η υποκλοπή, η εξαπάτηση, η εισβολή στο σύστημα, η πρόκληση αδυναμίας παροχής υπηρεσιών, διείσδυση συστήματος, η αλλοίωση συστήματος, οικονομική εκμετάλλευση, η κλοπή πληροφοριών, το Social engineering (phishing, trojans), η μη εξουσιοδοτημένη πρόσβαση στο σύστημα, η έλλειψη διαθεσιμότητας/ ακεραιότητας.

Παραδείγματα ευπαθειών (τρωτών σημείων) αποτελούν οι ασθενείς μηχανισμοί αυθεντικοποίησης, η έλλειψη σχεδίου επιθεώρησης των μηχανισμών ασφάλειας, η ανεπαρκής εκπαίδευση στην ασφάλεια πληροφοριών, η έλλειψη μηχανισμών προστασίας των εγγραφών του συστήματος, η έλλειψη

μηχανισμών προστασίας των προσωπικών δεδομένων, η έλλειψη οργανωτικής δομής σε θέματα ασφάλειας των πληροφοριών κτλ.

Η αναγνώριση και ο προσδιορισμός του κινδύνου αποτελείται από τον εντοπισμό και την αξιολόγηση όλων των απειλών για την προσδοκώμενη λειτουργία ενός συστήματος ή ενός οργανισμού. Ο προσδιορισμός του κινδύνου για ένα πληροφοριακό σύστημα περιλαμβάνει την αξιολόγηση απειλών για την ασφάλεια του συστήματος, για παράδειγμα την εγκατάσταση κακόβουλου λογισμικού, τις φυσικές καταστροφές και άλλα δυνητικά επιβλαβή γεγονότα που θα μπορούσαν να διαταράξουν τις επιχειρηματικές δραστηριότητες. Ο προσδιορισμός κινδύνου δεν είναι μια διαδικασία που γίνεται εφάπαξ. Αντίθετα, η διαδικασία θα πρέπει να είναι αυστηρή, στοχαστική και συνεχής.

Υπάρχουν δύο τύποι απειλών, οι αναγνωρισμένες και οι μη αναγνωρισμένες. Οι αναγνωρισμένες απειλές, είναι εκείνες που έχουν εντοπισθεί ήδη και αναλυθεί. Οι αναγνωρισμένες απειλές πρέπει να διαχειρίζονται προληπτικά από τους υπεύθυνους διαχείρισης ενός έργου ή ενός πληροφοριακού συστήματος, καθ' όλη την διάρκεια ζωής τους,περιγράφοντας τον κίνδυνο που μπορεί να οδηγήσει η εμφάνιση τους και τις συνέπειές πουθα επιφέρει ο ίδιος ο κίνδυνος, προκειμένου είτε να αποφευχθεί η εμφάνιση του, είτε να μειωθεί το αντίκτυπο από τις επιπτώσεις.

Οι μη αναγνωρισμένες απειλές είναι εκείνες που δεν έχουν εντοπιστεί. Παραδείγματα μη αναγνωρισμένων απειλών είναι αλλαγές της νομοθεσίας, φυσικές καταστροφές, αναπάντεχη απώλεια πόρων. Οι μη αναγνωρισμένες απειλές δεν μπορούν να διαχειριστούν πάντα προληπτικά για να μην οδηγήσουν στην εμφάνιση κινδύνου, και συχνάδιευθετούνται μέσω της αποδοχής του κινδύνου.

Μερικές από τις τεχνικές αναγνώρισης απειλών, περιλαμβάνουν μερικά από τα παρακάτω παραδείγματα:

- Προσαρμοσμένα ερωτηματολόγια
- Ανάλυση SWOT
- Επιχειρησιακές Μελέτες, οι οποίες εξετάζουν κάθε επιχειρησιακή διεργασία
- Τεχνικές Delphi
- Root Cause Analysis (RCA) - Ανάλυση Αιτιών
- Η σύσκεψη για ανταλλαγή ιδεών (brainstorming)
- Η συγκριτική αξιολόγηση (benchmarking)
- Η ανάλυση σεναρίων κινδύνου

Μετά τον εντοπισμό των απειλών, ακολουθεί η ανάλυση του κινδύνου. Η έννοια της εκτίμησης και αξιολόγησης του κινδύνου έχει μακρά ιστορία. Από τον 5ο αιώνα π.χ. , στην Αθήνα αξιολογούσαν τον κίνδυνο πριν λάβουν αποφάσεις σχετικά με την έναρξη πολέμων και συγκεκριμένα με τους Πέρσες[50]. Από τον 13ο αιώνα αναπτύχθηκαν θεωρίες, πιθανότητες και αριθμητικές έννοιες που σχετίζονται με την εκτίμηση κινδύνων όπως για παράδειγμα η «Ακολουθία Φιμπονάτσι» από τον Fibonacci. Τον 18ο αιώνα, αρχίζουν επίσης να εμφανίζονται και οι πρώτες μελέτες στην «Θεωρία Παιγνίων» του Blaise Pascal. Ωστόσο,η ανάλυση και η διαχείριση κινδύνων αναγνωρίζεται ως επιστημονικό πεδίο τα

[50] Basil Bernstein (1996). Pedagogy, symbolic control and identity. London: Taylor & Francis. In BritishJournal of Sociology of Education, 18(1), pp.119-124

τελευταία 30 με 40 χρόνια. Από αυτήν την περίοδο και μετά, ολοένα και εμφανίζεται η έννοια στα πρώτα επιστημονικά περιοδικά, εργασίες και συνέδρια κάνοντας λόγο στις θεμελιώδεις αρχές σχετικά με τον κατάλληλο τρόπο αξιολόγησης και διαχείρισης του κινδύνου. Στα τέλη του 19ου αιώνα, ξεκίνησε η κατασκευή πολυώροφων κτιρίων, πολύπλοκων σιδηροδρομικών υποδομών, μεγάλων φραγμάτων και καναλιών, με αποτέλεσμα οι τεχνικές διαχείρισης κινδύνου να διαδοθούν με σκοπό να συνεισφέρουν στον προσδιορισμό του αποτελέσματος ενός έργου. Ωστόσο, την εποχή εκείνη, οι τεχνικές διαχείρισης κινδύνου ήταν όλες σε μεγάλο βαθμό ποιοτικές, δηλαδή επικεντρωνόταν μόνο στον εντοπισμό απειλών (ή ευκαιριών), στον υποκειμενικό προσδιορισμό της πιθανότητας εμφάνισης του κινδύνου και στον εντοπισμό των πιθανών επιπτώσεων.

Αυτή η διαδικασία των τριών βημάτων παραμένει το θεμέλιο τηςποιοτικής ανάλυσης κινδύνου που θα δούμε παρακάτω, αν και σήμερα έχουμε επίσημες μεθόδους και κατευθυντήριες γραμμές για να καθορίσουμε τη σοβαρότητα αυτών των κινδύνων, η οποία συνήθως πραγματοποιείται χρησιμοποιώντας έναν πίνακα κατάταξης Πιθανοτήτων/Επίπτωσης.

Η ανάλυση κινδύνου ασχολείται πρωτίστως με την ιεράρχηση και την ταξινόμηση των κινδύνων και, στη συνέχεια, με την προτεραιοποίηση τους με σκοπό την ανάπτυξη στρατηγικών μετριασμού και/ή σχεδίων έκτακτης ανάγκης. Καθορίζει λοιπόν, ποιοι κίνδυνοι θα είχαν δυνητικά το μεγαλύτερο αντίκτυπο και, ως εκ τούτου, πρέπει να διαχειρίζονται αφενός πρώτοι και αφετέρου με ιδιαίτερη φροντίδα. Συνεπώς, αντανακλά την αντοχή ενός έργου ή ενός οργανισμού στον κίνδυνο και καθορίζει τα όρια του σε τομείςόπως το κόστος, το χρονοδιάγραμμα, το προσωπικό, οι πόροι, η ποιότητα κ.λπ. Η ανάλυση κινδύνου αποτελεί μια επαναληπτική διαδικασία που εκτελείται συνεχώς σε όλη τη διάρκεια του έργου καθώς εντοπίζονται συνεχώς νέες απειλές ή ευάλωτα σημεία.

Υπάρχουν πολλές μεθοδολογίες αλλά και προσεγγίσεις για την ανάλυση κινδύνου. Υπάρχουν τρία είδη μεθόδων που χρησιμοποιούνται για τον προσδιορισμό του επιπέδουκινδύνου:

- Ποιοτική
- Ημι-ποσοτική
- Ποσοτικές Μέθοδοι

Η ποιοτική ανάλυση κινδύνου χρησιμοποιείται για την ιεράρχηση των εντοπισμένων κινδύνων για περαιτέρω ανάλυση είτε με τη χρήση ποσοτικής ανάλυσης κινδύνου είτε με σχεδιασμό σχεδίων απόκρισης κινδύνου. Με απλά λόγια, η ποιοτική ανάλυση αξιολογεί την προτεραιότητα των εντοπισμένων κινδύνων χρησιμοποιώντας την πιθανότητα εμφάνισης τους, τον αντίστοιχο αντίκτυπο στους στόχους του έργου ή του πληροφοριακού συστήματος.Η μέθοδος αυτή, χρησιμοποιείται συχνότερα για τη λήψη αποφάσεων σχετικά με τον μετριασμό των ήδη εντοπισμένων κινδύνων, κυρίως σε επιχειρηματικά έργα. Αποτελεί μια ευρέως διαδεδομένη και απλή, και συνήθως χρησιμοποιείται όταν το επίπεδο κινδύνου θεωρείται γενικά χαμηλό καθώς δεν απαιτείται ιδιαίτερος χρόνος και πόροι όπως σε μια ολοκληρωμένη ανάλυση.

Ωστόσο, για να ολοκληρωθεί σωστά η ανάλυση, θα πρέπει να ακολουθείται σωστή καταγραφή των πηγών της κάθε απειλής, των προσώπων που κινδυνεύουν και του τρόπου που κινδυνεύουν. Επιπρόσθετα, πρέπει να περιλαμβάνει την αξιολόγηση των υφιστάμενων μέτρων και την επιλογή επιπλέον τεχνικών και οργανωτικών μέτρων για την προστασία και την πρόληψη των κινδύνων. Μπορούν επίσης να χρησιμοποιηθούν όταν τα διαθέσιμα αριθμητικά δεδομένα δεν είναι επαρκή για μια ποσοτική ανάλυση.

Σημαντικό μέρος της ποιοτικής εκτίμησης κινδύνου, αποτελεί η καταγραφή του υπεύθυνου προσώπου για τη λήψη των μέτρων, του χρονικού ορίζοντα για τη λήψη των μέτρων και ο μετέπειτα έλεγχος (επιβεβαίωση) της λήψης των μέτρων. Η ημι-ποσοτική μέθοδος αποτελεί το συνδυασμό της ποιοτικής και της ποσοτικής μεθόδου. Στην μέθοδο αυτή χρησιμοποιούνται μοντέλα για τον ακριβή προσδιορισμό του αντικτύπου και της πιθανότητας να επισυμβεί κάποιος κίνδυνος, με σκοπό την ταξινόμησητους. Η μέθοδος αυτή χρησιμοποιεί τις ποιοτικές κατηγορίες (τιμές όπως υψηλή, μεσαία ή χαμηλή) αποδίδοντας τους αριθμητικές τιμές που επιτρέπουν την αριθμητική εκτίμηση των κινδύνων και την αξιολόγηση τους έναντι καθορισμένων δεικτών, ως προς το επίπεδο του κινδύνου. Η τελική αριθμητική αξιολόγηση για κάθε κίνδυνο καθορίζει τις προτεραιότητες στη λήψη των πιο κατάλληλων μέτρων προστασίας και πρόληψης. Τυπικό παράδειγμα ημι- ποσοτικής μεθοδολογίας είναι ο παρακάτω Πίνακας Κινδύνου (Risk Rating Matrix).

Η πιθανότητα εμφάνισης ενός κινδύνου στην ημι-ποσοτική μεθοδολογία υπολογίζεται με βάση τον ακόλουθο πίνακα:

Πίνακας 2: Εκτίμηση Πιθανότητας

Αποτελεσματικότητα του μηχανισμού ελέγχου	**Πιθανότητα εμφάνισης της απειλής ή κίνητρο/ικανότητα της απειλής**		
	Χαμηλή	Μεσαία	Υψηλή
Χαμηλή	Μεσαία	Υψηλή	Υψηλή
Μεσαία	Χαμηλή	Μεσαία	Υψηλή
Υψηλή	Χαμηλή	Χαμηλή	Μεσαία

Πιθανότητας εμφάνισης του κινδύνου	**Προσδιορισμός Πιθανότητας**
Χαμηλή (0.1)	Η πηγή απειλών δεν έχει κίνητρα ή ικανότητα, και οι έλεγχοι είναι σε θέση να προστατέψουν, ή τουλάχιστον να εμποδίσουν σημαντικά την εκμετάλλευση της ευπάθειας.
Υψηλή (1.0)	Η πηγή απειλών έχει υψηλά κίνητρα και είναι επαρκώς ικανή, και οι έλεγχοι για να προστατέψουν την ευπάθεια είναι μη αποτελεσματικοί.
Μεσαία (0.5)	Η πηγή απειλών έχει μέτρια κίνητρα και είναι ικανή, αλλά οι έλεγχοι είναι σε θέση να μπορούν να εμποδίσουν την εκμετάλλευση της ευπάθειας.

Η επίπτωση εμφάνισης ενός κινδύνου στην ημι-ποσοτική μεθοδολογία υπολογίζονται μεβάση τον ακόλουθο πίνακα:

Πίνακας 3: Εκτίμηση Επιπτώσεων

Επίπτωση (βαθμός)	**Προσδιορισμός Επιπτώσεων**
Υψηλή **(100)**	> Σημαντική οικονομική απώλεια στις επιχειρηματικές δραστηριότητες της Εταιρείας (π.χ. απώλεια μεγάλου οικονομικά ποσού (>1.000.000 €), κ.λπ.) > Σημαντική ζημιά στα πληροφοριακά αγαθά > Τραυματισμός ο οποίος οδηγεί στον θάνατο, πολύ σημαντικός τραυματισμός ή θάνατος υπαλλήλου
Μεσαία **(50)**	> Σοβαρή οικονομική απώλεια στις επιχειρηματικές δραστηριότητες της Εταιρείας (π.χ. απώλεια μεσαίου οικονομικάποσού [>500.000 €, <1.000.000 €], κ.λπ.) > Σημαντική ζημιά στα πληροφοριακά αγαθά > Τραυματισμός ο οποίος δεν οδηγεί στον θάνατο υπαλλήλου
Χαμηλή **(10)**	> Μικρή οικονομική απώλεια στις επιχειρηματικές δραστηριότητες της Εταιρείας (π.χ. απώλεια μικρού οικονομικά ποσού [<500.000 €], κ.λπ.) > Μικρή ζημιά στα πληροφοριακά αγαθά > Ελαφρύς τραυματισμός υπαλλήλου

Το επίπεδο του κινδύνου υπολογίζεται λαμβάνοντας υπόψιν την πιθανότητα εμφάνισης του κινδύνου και το μέγεθος του αντικτύπου, σύμφωνα με τον ακόλουθο τύπο:

Κίνδυνος = επίπεδο αντικτύπου * πιθανότητα κινδύνου

Οι δυνατές τιμές του κινδύνου παρουσιάζονται στον επόμενο πίνακα:

Πίνακας 4: Προσδιορισμός επικινδυνότητας

Επικινδυνότητα		Επίπτωση		
		Χαμηλή-10	**Μεσαία-50**	**Υψηλή-100**
Πιθανότητας εμφάνισης του κινδύνου	**Υψηλή-1**	Χαμηλή επικινδυνότητα (10 x 1.0=10)	Μεσαία επικινδυνότητα (50x1.0=50)	Υψηλή επικινδυνότητα (100x1.0=100)
	Μεσαία-0.5	Χαμηλή επικινδυνότητα (10 x 0.5=5)	Μεσαία επικινδυνότητα (50 x 0.5=25)	Μεσαία επικινδυνότητα (100x0.5=50)
	Χαμηλή-0.1	Χαμηλή επικινδυνότητα (10 x 0.1=1)	Χαμηλή Επικινδυνότητα (50x0.1=5)	Χαμηλή επικινδυνότητα (100x0.1=10)

Η πρώτη γνωστή μέθοδος ποσοτικής ανάλυσης κινδύνου αναπτύχθηκε από τον Henry Gantt το 1917 με τη μορφή του Διαγράμματος Gantt το οποίο, εκείνη την εποχή, χρησιμοποιήθηκε αποκλειστικά για την ανάλυση κινδύνου ως προς το χρονοδιάγραμμα ενός έργου. Τα διαγράμματα Gantt εξακολουθούν να αποτελούν τη βάση των περισσότερων χρονοδιαγραμμάτων που χρησιμοποιούνται σήμερα, αλλά οι διαθέσιμες μέθοδοι της ποσοτικής ανάλυσης κινδύνου, έχουν εξελιχθεί και διαφοροποιηθεί

σημαντικά, παρέχοντάς μια σειρά επιλογών για διαφορετικούς τύπους κινδύνου και επιπτώσεων. Η ποσοτική ανάλυση κινδύνου εκτελείται σε κινδύνους που έχουν δοθεί προτεραιότητα ύστερα από τη διαδικασία ποιοτικής ανάλυσης κινδύνου. Αναλύει την επίδραση αυτών και αποδίδει μια αριθμητική βαθμολογία. Όταν ολοκληρωθεί, παρουσιάζει επίσης μια ποσοτική προσέγγιση στη λήψη αποφάσεων όταν προκύπτει αβεβαιότητα. Αποτελεί μια πιο περίπλοκη μεθοδολογία, που χρησιμοποιείται σε μεγάλες βιομηχανίες με πιο πολύπλοκες διεργασίες. Μέθοδοι ποσοτικής ανάλυσης κινδύνου περιλαμβάνουν, μεταξύ άλλων, την Ανάλυση Monte-Carlo, την Ανάλυση LOPA, την Ανάλυση Επιπτώσεων (FMEA), την Ανάλυση Markovκαι την Ανάλυση Bayesian.

Στις περισσότερες εγκαταστάσεις όπου υπάρχουν εγγενείς κίνδυνοι που απειλούν τη ζωή, όπως εγκαταστάσεις διύλισης ή αποθήκευσης πετρελαίου και φυσικού αερίου, μονάδες επεξεργασίας χημικών, ορυχεία κ.λπ., έχει καταστεί υποχρεωτική πρακτική η διεξαγωγή μιας ανάλυσης ποσοτικού κινδύνου για την αξιολόγηση των κινδύνων για το προσωπικό που εργάζεται στην εγκατάσταση αυτή.

4.1 Ανάλυση Κινδύνων Ασφάλειας Συστημάτων

Η πιο συνηθισμένη μέθοδος μέτρησης του κινδύνου ως προς την ασφάλεια των συστημάτων είναι η ποιοτική μέθοδος, κάνοντας χρήση των τιμών της κλίμακας που είδαμεπαραπάνω. Ακόμη και το πρότυπο NIST 800-30, που αποτελεί το πιο γνωστό οδηγό σχετικά με την αξιολόγηση του κινδύνου, ορίζει μια ποιοτική προσέγγιση για τη μέτρηση του κινδύνου.

Στην μεθοδολογία αυτή, η ιδέα πίσω από την ανάλυση κινδύνου είναι ο υπολογισμόςκαι η αποτίμηση αντικτύπου ως προς τα στοιχεία του ενεργητικού της Εταιρείας. Η εξέτασηλοιπόν, των τρωτών σημείων και των απειλών αξιολογείται ως προς τα

στοιχεία αυτά. Για να καταλήξουμε στην πραγματική εκτίμηση του κινδύνου, συνυπολογίζονται όλα τα μέτρα προστασίας και τα αντίμετρα που εφαρμόζονται και ξανά υπολογίζεται η πιθανότητα και το αντίκτυπο εμφάνισης του κινδύνου. Τέλος, απομείνει η παρουσίαση των τελικών κινδύνων προκειμένου να αποφασίσει η Διοίκηση, αν το υπολειπόμενο ρίσκο είναι αποδεκτόή θα πρέπει να ληφθούν επιπλέον μέτρα.

Για τον εντοπισμό όλων των ευπαθειών ενός οργανισμού είναι απαραίτητη, μια ολοκληρωμένη προσέγγιση. Για τον λόγο αυτό, μια διεξοδική αξιολόγηση κινδύνων θα πρέπει να πραγματοποιείται όχι μόνο μόνο από μέλη της ομάδας πληροφορικής ή της ασφάλειας συστημάτων, αλλά θα πρέπει να περιλαμβάνει εκπροσώπους από άλλες οργανωτικές μονάδες, οι οποίοι γνωρίζουν πώς διαχειρίζονται τα δεδομένα εντός της εταιρείας, προκειμένου να συνεισφέρουν στον εντοπισμό και τον περιορισμό των τρωτών σημείων.

Προκειμένου να ξεκινήσει η αξιολόγηση κινδύνου ασφάλειας πληροφορικής, πρέπεινα απαντηθούν τρεις σημαντικές ερωτήσεις:

1. Ποια είναι τα κρίσιμα πληροφοριακά σύστημα του οργανισμού; Για παράδειγμα, τα δεδομένα των οποίων η απώλεια ή η έκθεση θα επιφέρει σημαντικό αντίκτυπο στις επιχειρηματικές λειτουργίες.
2. Ποιες είναι οι κρίσιμες επιχειρηματικές διαδικασίες που χρησιμοποιούν ή απαιτούν αυτές τις πληροφορίες για την εύρυθμη λειτουργία τους;
3. Ποιες απειλές θα μπορούσαν να επηρεάσουν την εύρυθμη λειτουργία των πληροφοριακών συστημάτων που εξυπηρετούν οι κρίσιμες επιχειρηματικές διαδικασίες;

Από τα παραπάνω συμπεραίνουμε ότι για την αξιολόγηση κινδύνου είναι κρίσιμο να εντοπιστούν ποια είναι και που βρίσκονται τα στοιχεία του ενεργητικού της Εταιρείας, όχι μόνο τα υλικά (π.χ. τα πληροφοριακά συστήματα αυτά καθαυτά) αλλά και τα άυλα (π.χ. οι πληροφορίες, η πνευματική ιδιοκτησία, η φήμη της εταιρείας). Μόλις αποκτηθεί η γνώση των περιουσιακών στοιχείων που πρέπει να προστατευτούν, εκτιμάται η οικονομική αξία τους και ο αντίκτυπος για την Εταιρεία, σε περίπτωση που τεθούν σε κίνδυνο. Για να υπολογιστεί καλύτερα ο κίνδυνος και εφόσον η ακρίβεια δεν είναι τόσο κρίσιμη στην ποιοτική μεθοδολογία που ακολουθείται, θα πρέπει να εκτιμάται η επίπτωση που ενδεχομένως επιφέρει η πλήρη απώλεια του περιουσιακού στοιχείου. Στην συνέχεια, ακολουθεί η ανάπτυξη στρατηγικών για κάθε ένα κίνδυνο, ο οποίος υπολογίζεται με βάση την παρακάτω συνάρτηση:

Κίνδυνος = Απειλή x Ευπάθεια x Περιουσιακό στοιχείο

Αν και ο κίνδυνος αναπαρίσταται παραπάνω ως μαθηματικός τύπος, η τελική εκτίμηση δεν πρόκειται για αριθμούς, καθώς εφαρμόζεται η ποιοτική μεθοδολογία. Για παράδειγμα, αν θέλουμε να αξιολογήσουμε τον κίνδυνο που σχετίζεται με την απειλή κάποιος κακόβουλος να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε ένα συγκεκριμένο σύστημα, το αποτέλεσμα θα επιφέρει ότι κίνδυνος είναι υψηλός, μέτριος ή χαμηλός . Εάν το δίκτυό που φιλοξενείται το σύστημα που εξετάζεται είναι ευάλωτο, (για παράδειγμα, επειδή δεν εφαρμόζεται τείχος προστασίας ή λύση προστασίας από ιούς) και ο πληροφοριακός πόρος είναι κρίσιμος, ο κίνδυνος είναι υψηλός. Ωστόσο, εάν εφαρμόζονται μέτρα προστασίας, όπως πολιτική εφαρμογής ισχυρών κωδικών, η πιθανότητα να πραγματοποιηθεί ο κίνδυνος είναι μικρότερη, και παρόλο που το περιουσιακό στοιχείο είναι ακόμα κρίσιμο, ο κίνδυνος από υψηλός θα χαρακτηριστεί μέτριος.

Η διεξαγωγή μιας ενδελεχούς αξιολόγησης κινδύνων σε τακτική βάση βοηθάει τους οργανισμούς να διασφαλίσουν την επιχειρηματική τους επιτυχία και συνέχεια. Ειδικότερα, τους δίνει τη δυνατότητα:

- Να προσδιορίσουν και να αποκαταστήσουν τα κενά ασφάλειας των συστημάτων
- Να αποτρέψουν τις παραβιάσεις δεδομένων
- Να επιλέξουν κατάλληλα πρωτόκολλα και ελέγχους για τον μετριασμό τωνκινδύνων
- Να δώσουν προτεραιότητα στην προστασία του περιουσιακού στοιχείου με τηνυψηλότερη αξία και τον υψηλότερο κίνδυνο
- Να εξαλείψουν τα περιττά ή τα απαρχαιωμένα μέτρα ελέγχου
- Να αξιολογήσουν πιθανούς συνεργάτες ως προς την ασφάλεια
- Να καθιερώσουν, να διατηρήσουν και να αποδείξουν συμμόρφωση με τουςκανονισμούς
- Να προβλέψουν με ακρίβεια μελλοντικές ανάγκες

4.2 Μεθοδολογία Αξιολόγησης Κινδύνων Ασφάλειας Συστημάτων

4.2.1 Προσδιορισμός Πόρων

Το πρώτο βήμα για μια επιτυχημένη αξιολόγηση κινδύνων είναι ο προσδιορισμός και η ιεράρχηση των περιουσιακών στοιχείων της Εταιρείας. Τα στοιχεία του ενεργητικού περιλαμβάνουν διακομιστές (server), δεδομένα πελατών (π.χ. στοιχεία επικοινωνίας) , ευαίσθητα έγγραφα συνεργατών, εμπορικά

μυστικά και ούτω καθεξής. Για τον προσδιορισμό και την ιεράρχηση, θα πρέπει να υπάρχει συνεργασία μεταξύ προσωπικού που ασχολείται με την πληροφορική και την ασφάλεια, με την επίτευξη επιχειρησιακών στόχων και τη Διοίκηση, με σκοπό να δημιουργηθεί μια λίστα με όλα τα πολύτιμα στοιχεία του ενεργητικού.

Για κάθε περιουσιακό στοιχείο, θα πρέπει να συγκεντρώνονται οι ακόλουθες πληροφορίες, ανάλογα με την περίπτωση:

Πίνακας 5: Ερωτηματολόγιο αξιολόγησης κρισιμότητας περιουσιακών στοιχείων.

Γενικά
Ποιος είναι ο Ιδιοκτήτης (Επιχειρησιακή μονάδα) του συστήματος/υπηρεσίας/δεδομένων
Περιγραφή του συστήματος/υπηρεσίας/δεδομένων
Επιχειρηματικός σκοπός που εξυπηρετεί το σύστημα/υπηρεσία/δεδομένα;
Προμηθευτής
Στοιχεία επικοινωνίας για τεχνική υποστήριξη
Κρισιμότητα του συστήματος/υπηρεσίας/ δεδομένων
Τα δεδομένα του συστήματος/ υπηρεσίας περιλαμβάνουν εμπιστευτικές εταιρικές πληροφορίες (επιχειρηματικά σχέδια, δεδομένα ανθρώπινου δυναμικού, οικονομικά κ.λπ.);
Τα δεδομένα του συστήματος/ υπηρεσίας αφορούν προσωπικά δεδομένα
Τα δεδομένα του συστήματος/ υπηρεσίας αφορούν ευαίσθητα προσωπικά δεδομένα
Πόσοι υπάλληλοι/εργαζόμενοι χρησιμοποιούν το σύστημα
Ποιος είναι δηλαδή ο αριθμός των προσώπων που θα επηρεαστούν από ένα περιστατικό ασφάλειας

Προβλεπόμενη απώλεια εσόδων
Κίνδυνος για νομικά / κανονιστικά πρόστιμα
Κίνδυνος για τη φήμη της Εταιρείας
Έκθεση συστήματος/υπηρεσίας/ δεδομένων (Πιθανότητα εμφάνισης)
Αριθμός χρηστών που συνδέονται κεντρικά στο σύστημα
Αριθμός χρηστών με αυξημένα δικαιώματα που συνδέονται κεντρικά στο σύστημα
Αριθμός εξωτερικών συνεργατών που συνδέονται κεντρικά στο σύστημα
Απομακρυσμένη Πρόσβαση στο σύστημα από εσωτερικούς χρήστες
Απομακρυσμένη Πρόσβαση στο σύστημα από εξωτερικούς χρήστες
Διασύνδεση με άλλα συστήματα/ υπηρεσίες/ δεδομένα
Τύποι και όγκος συνδέσεων
Μέθοδος αυθεντικοποίησης στο σύστημα/ υπηρεσία/ δεδομένα
Υποδομή που φιλοξενείται το σύστημα / υπηρεσία
Φιλοξενείται το σύστημα σε δικτυακές υποδομές του οργανισμού
Οι υποδομές βρίσκονται στο cloud (public, private ή hybrid) ή στις εγκαταστάσεις του οργανισμού
Αν φιλοξενούνται στο cloud, ποιο είναι το μοντέλο υπηρεσίας;(Λογισμικό ως Υπηρεσία - SaaS, Πλατφόρμα ως Υπηρεσία - PaaS και Υποδομή ως Υπηρεσία (IaaS).
Η διαχείριση του συστήματος/ υπηρεσίας/ δεδομένων πραγματοποιείται εσωτερικά ή από εξωτερικούς συνεργάτες
Υποσυστήματα που απαρτίζεται η υπηρεσία/ φιλοξενούνται τα δεδομένα (Λειτουργικό σύστημα, Βάση Δεδομένων, Εφαρμογή)

Καθώς οι περισσότεροι οργανισμοί αφιερώνουν περιορισμένους χρηματικούς αλλά και ανθρώπινους πόρους για την αξιολόγηση κινδύνου, οι παραπάνω ερωτήσεις θα πρέπει να περιοριστούν στα κρίσιμα συστήματα/υπηρεσίες/ δεδομένα της Εταιρείας. Κατά συνέπεια, θα πρέπει να οριστεί ένα πρότυπο για τον προσδιορισμό της σημασίας κάθε περιουσιακού στοιχείου. Τα κοινά κριτήρια περιλαμβάνουν τη χρηματική αξία του περιουσιακού στοιχείου, τη νομική υπόσταση και τη σημασία του για την λειτουργία του οργανισμού. Το πρότυπο προσδιορισμού της σημασίας κάθε περιουσιακού στοιχείου, θα πρέπει να είναι εγκεκριμένο από τη Διοίκηση και να ενσωματώνεται επίσημα στην πολιτική σχετικά με την αξιολόγηση του κινδύνου ως προς την ασφάλεια, που εφαρμόζει ένας οργανισμός. Με τον τρόπο αυτό, κάθε περιουσιακό στοιχείο ταξινομείται ως κρίσιμο, κύριο ή δευτερεύον.

4.2.2 Προσδιορισμός Απειλών

Το δεύτερο βήμα είναι ο προσδιορισμός απειλών, δηλαδή ο εντοπισμός γεγονότων που ενδέχεται να προκαλέσουν βλάβη σε ένα οργανισμό. Ο προσδιορισμός των απειλών είναι ένα πολύ σημαντικό βήμα σε όλη τη διάρκεια ζωής ενός συστήματος. Για παράδειγμα απειλές που σχετίζονται με φυσικές καταστροφές, πρέπει να συνεκτιμώνται, όταν λαμβάνεται η απόφαση για το πού θα στεγαστούν οι servers (διακομιστές). Υπάρχουν πολλοί τύποι απειλών, οι οποίοι κατηγοριοποιούνται παρακάτω:

Πίνακας 6: Κατηγορίες απειλών

Πηγή Απειλής	**Ενέργειες απειλής**
Ανθρώπινες απειλές	
Hackers, Crackers	Hacking
	Social engineering (phishing, trojans, etc.)
	Διείσδυση του συστήματος, διάρρηξη
	Μη εξουσιοδοτημένη πρόσβαση στο Σύστημα
Spammers	Spam e-mails
	Spoof e-mails
	Βομβαρδισμός με e-mails
Εγκληματίες Κυβερνοχώρου	Ηλεκτρονικό έγκλημα
	Παράνομη πράξη (π.χ. επανάληψη, πλαστοπροσωπία, υποκλοπή)
	Εξαπάτηση
	Εισβολή στο Σύστημα
Τρομοκράτες	Επίθεση στο Σύστημα
	Πρόκληση αδυναμίας παροχής υπηρεσιών
	Διείσδυση Συστήματος
	Αλλοίωση Συστήματος
Ανταγωνιστές	Οικονομική εκμετάλλευση
	Κλοπή πληροφοριών
	Social engineering (phishing, trojans, etc.)

	Διείσδυση Συστήματος
	Μη εξουσιοδοτημένη πρόσβαση στο σύστημα (πρόσβαση σε διαβάθμιση)
Εσωτερική απειλή (υπάλληλος με κακή εκπαίδευση, θυμό, κακεντρεχής, αμελής, ανειλικρινής, απολυόμενος)	Επίθεση σε υπάλληλο
	Εκβιασμός
	Πρόσβαση εμπιστευτικής πληροφορίας
	Κατάχρηση υπολογιστή
	Απάτη και κλοπή
	Κακόβουλος κώδικας (πχ. ιός, logic bomb, Trojan)
	Πώληση προσωπικών πληροφοριών
	Εισαγωγή σφαλμάτων στο Σύστημα
	Εισβολή στο Σύστημα
	Μη εξουσιοδοτημένη πρόσβαση στο Σύστημα
	Μη εξουσιοδοτημένη πρόσβαση στο Σύστημα
Φυσικές Απειλές	
Σεισμοί	Έλλειψη διαθεσιμότητας/ ακεραιότητας
Πλημμύρες/Αυξημένη υγρασία	Έλλειψη διαθεσιμότητας/ ακεραιότητας
Καθίζηση εδάφους	Έλλειψη διαθεσιμότητας/ ακεραιότητας
Κεραυνοί	Έλλειψη διαθεσιμότητας/ ακεραιότητας
Φωτιά	

4.2.3 Προσδιορισμός Ευπαθειών

Το τρίτο βήμα, αποτελεί τον προσδιορισμό των τρωτών σημείων/ευπαθειών ενός συστήματος. Η ευπάθεια είναι μια αδυναμία που θα μπορούσε να επιτρέψει σε μια απειλή να βλάψει τον οργανισμό ή το σύστημα. Τα τρωτά σημεία ενός οργανισμού μπορούν να εντοπιστούν μέσω συλλογής πληροφοριών με χρήση ερωτηματολογίων, εκθέσεων εσωτερικού ελέγχου, από την βάση δεδομένων ευπαθειών του NIST, από δεδομένα που συλλέγονται από τον ίδιο τον προμηθευτή του συστήματος, από αυτοματοποιημένα εργαλεία ανίχνευσης ευπαθειών τα οποία σαρώνουν τα συστήματα και το δίκτυο, με δοκιμές διείσδυσης (penetration testing) κτλ.

Οι ευπάθειες δεν περιορίζονται μόνο σε τρωτά σημεία του συστήματος ή του δικτύου, καθώς υπάρχουν ευπάθειες που απορρέουν από ανθρώπινα λάθη. Για παράδειγμα, ένας διακομιστής (server) ο οποίος είναι εγκατεστημένος στο υπόγειο, αυξάνει την ευπάθειά τουσυστήματος στην απειλή της πλημμύρας καθώς και η αποτυχία εκπαίδευσης των υπαλλήλων αυξάνει την ευπάθεια του οργανισμού στην απειλή της εγκατάστασης κακόβουλου λογισμικού. Παραδείγματα ευπαθειών για τα πληροφοριακά συστήματα, αποτελούν: Ασθενής μηχανισμοί αυθεντικοποίησης, έλλειψη κρυπτογράφησης, μη ενημερωμένο λογισμικού, ‘έλλειψη κριτηρίων ασφάλειας για την αποδοχή του νέου ή ανανέωση του υπάρχοντος συστήματος, έλλειψη πολιτικών ασφάλειας πληροφοριακών συστημάτων, έλλειψη συμμόρφωσης με νομικά πρότυπα, έλλειψη σχεδίου επιθεώρησης των μηχανισμών ασφάλειας.

Απειλές και ευπάθειες στο Smart Home

Το σημαντικότερο ζήτημα που σχετίζεται με το απόρρητο δεδομένων στο IoT είναι ηαποκάλυψη προσωπικών πληροφοριών

σε μη εξουσιοδοτημένα άτομα. Με τον αριθμό των συσκευών IoT να αυξάνεται , οι πελάτες που κάνουν χρήση αυτής της τεχνολογίας αυξάνονται επίσης, με αποτέλεσμα τη μείωση των τιμών και την αύξηση του αριθμού των υποστηριζόμενων λειτουργιών. Επιπλέον, οι συσκευές IoT αποτελούν πλέον ένα κρίσιμο κομμάτι των φυσικών συστημάτων, που αποτελούν τον πυρήνα πολλών κρίσιμων υποδομών.

Αξίζει να σημειωθεί ότι υπάρχουν σημαντικές διαφορές μεταξύ του παραδοσιακού τομέα πληροφορικής και του τρέχοντος περιβάλλοντος του IoT. Οι διαφορές αυτές επηρεάζουν πραγματικά τον τύπο των επιθέσεων που απειλούν αυτές τις συσκευές καθώς και τον τρόπο διαχείρισης τους. Οι κύριες διαφορές προέρχονται από τον δυναμικό και μεταβαλλόμενο χαρακτήρα των συσκευών IoT, όπως και στον μεγάλο αριθμό συσκευών που συνδέονται και αποσυνδέονται, εγκαθίστανται και απεγκαθίστανται σε σύντομο χρονικό διάστημα. Το γεγονός αυτό, καθιστά δύσκολες και δαπανηρές δραστηριότητες όπως η ενημέρωση του κώδικα της συσκευής το οποίο αποτελεί βασικό μέτρο προστασίας, σε τέτοια μεταβαλλόμενα περιβάλλοντα.

Σχετικά με τη δυναμικότητα των πλατφορμών IoT, αξίζει να σημειωθεί η ποσότητα παλαιών συσκευών, από διαφορετικούς προμηθευτές που χρησιμοποιούν διαφορετικά πρωτόκολλα και έχουν διαφορετικές δυνατότητες. Μερικές φορές υποστηρίζουν μόνο αναλογικά σήματα που πρέπει να μετατραπούν σε ψηφιακά για να χρησιμοποιηθεί σωστά η συσκευή. Αυτό συνιστά ένα ζήτημα που έχει μεγάλο αντίκτυπο στην ασφάλεια των IoT, καθώς πολλά παλαιά συστήματα απαιτούν προσαρμοσμένες λύσεις και μηχανισμούς ασφαλείας. Για άλλες συσκευές, λόγω περιορισμένων πόρων, αυτοί οι μηχανισμοί ασφαλείας δεν είναι καν δυνατοί. Μια άλλη πτυχή εγγενής στο IoT, είναι οι δυνατότητες του να λειτουργούν και να ανταλλάσσουν δεδομένα σε πραγματικό χρόνο που, πολύ συχνά, επηρεάζει τον τρόπο διαχείρισης των

συμβάντων ασφαλείας και των πιθανών απειλών, καθώς η διαθεσιμότητα μπορεί να γίνει μια από τις βασικές πτυχές που πρέπει να ληφθούνυπόψη, ειδικά για πολύ κρίσιμους τομείς όπως η υγεία και η ενέργεια.

Οι περισσότερες συσκευές IoT δεν είναι προσβάσιμες, καθώς τις περισσότερες φορές οι συσκευές παραμένουν αποσυνδεδεμένες ή χάνουν τη σύνδεση τους με το διαδίκτυο. Επίσης, οι συσκευές είναι ευάλωτες στο να κλαπούν, καθιστώντας έτσι την ασφάλεια τους ένα δύσκολο εγχείρημα. Η προσδοκία της ισχυρής ασφάλειας των συσκευών είναι δύσκολη χωρίς επεξεργασία ισχύος. Ύστερα οι περισσότερες συσκευές είναι αισθητήρες, η διάρκεια ζωής τους είναι άρρηκτα συνδεδεμένη με τη διάρκεια ζωής της μπαταρίας τους, και δυστυχώς οι συσκευές διατηρούν μια πεπερασμένη διάρκεια ζωής. Οι απαιτήσεις ασφαλείας στις IoT συσκευές πρέπει να περιλαμβάνουν διασφάλιση της ανάλυσης και αξιολόγησης
των κινδύνων, έλεγχο της δικτυακής αρχιτεκτονικής, κρυπτογράφηση τόσο της διαδικτυακής κίνησης όσο και των δεδομένων που αποθηκεύονται σε αυτές καθώς και μέτραγια την προστασία ιδιωτικότητας, της ταυτότητας των υποκειμένων καθώς και πιθανή αξιολόγηση κινδύνων σχετικά με την προστασία των δεδομένων [51].

Η πρώτη προτεραιότητα για την επίτευξη της ασφάλειας στο IoT εξαρτάται κυρίως από την ικανότητα των χρηστών να έχουν πίστη στο περιβάλλον που αποθηκεύει ταδεδομένα τους. Οι συσκευές IoT που δεν έχουν σχεδιαστεί ή δεν εφαρμόζουν κάποιο μέτρο ασφάλειας, είναι αρκετά ευάλωτες σε κακόβουλες επιθέσεις

---

[51] J. Liu, and L. Yang, "Application of Internet of Things in the Community Security Management," Computational Intelligence, Communication Systems and Networks,Third International Conference onIEEE, 2011, pp. 314-318.

με στόχο τον επαναπρογραμματισμό των συσκευών, την πρόκληση κάποιας δυσλειτουργίας και τηνκλοπή των πολυτίμων δεδομένων που παράγουν. Η τεράστια αύξηση του αριθμού και της φύσης των συσκευών IoT σε συνδυασμό με την σύνδεση των συσκευών στο διαδίκτυο[52].

Το αυξανόμενο επίπεδο εξάρτησης στις συσκευές IoT και στις διαδικτυακές υπηρεσίες στις οποίες βασίζονται, ενισχύουν τους τρόπους με τους οποίος κάποιος κακόβουλος χρήστης μπορεί να αποκτήσει πρόσβαση και κατ' επέκταση τον έλεγχο των συσκευών. Η μη διασύνδεση των συσκευών στο διαδίκτυο δεν αποτελεί λύση , επομένως, η ασφάλεια των συσκευών και υπηρεσιών IoT είναι ένα κρίσιμο ζήτημα. Ωστόσο, η ασφάλειαόλων των συστημάτων αλλά ιδιαίτερα των IoT συσκευών, δεν μπορεί να είναι απόλυτη για τους παρακάτω λόγους [53]:

- Η ασφάλεια δεν πληρείται εκ σχεδιασμού των συστημάτων. Εκ σχεδιασμού, στις συσκευές δίνεται προτεραιότητα στην διαθεσιμότητα και την προστασία τους από φυσικές απειλές. Οι προμηθευτές συσκευών δεν θεωρούν την ασφάλεια ως πρωταρχικόστόχο στην παραγωγή συσκευών IoT[54], προκειμένου

---

[52] D. Jiang and C. ShiWei, "A study of information security for m2m of Internet of Things," in AdvancedComputer Theory and Engineering (ICACTE), 2010 3rd International Conference on, vol. 3. IEEE, 2010, pp. V3–576.

[53] Isam Ishaq , David Carels, Girum K. Teklemariam, Jeroen Hoebeke, Floris Van den Abeele, Eli De Poorter, Ingrid Moerman and Piet Demeester , "IETF Standardization in the Field of the IoT:A Survey", Journal of Sensor and Actuator Networks, ISSN 2224-2708,

[54] O. Arias, J. Wurm, K. Hoang, and Y. Jin. Privacy and security in internet of things and wearable devices. Multi-Scale Computing Systems, IEEE Transactions on, 1(2):99–109,

να παράγουν συσκευές IoT γρήγοραγια να καλύψουν τις τάσεις της αγοράς και να αυξήσουν τα επιχειρηματικά τους κέρδη.

- Περιορισμένη ορατότητα της ασφάλειας των συσκευών: Οι περισσότερες λύσεις και μηχανισμοί ασφάλειας δεν έχουν σχεδιαστεί για να παρακολουθούν ή να προστατεύουν τις συγκεκριμένες συσκευές.
- Έλλειψη συνεργασίας των κατασκευαστών των συσκευών και των επαγγελματιών ασφάλειας συστημάτων.
- Αυξημένη διασυνδεσιμότητα με το διαδίκτυο. Η διασύνδεση των συσκευών με το διαδίκτυο όλο και μεγαλώνει καθώς και γίνεται περισσότερη πολύπλοκη.
- Τα υπάρχοντα εργαλεία, μέθοδοι και στρατηγικές που σχετίζονται με την ασφάλεια των συσκευών IoT χρειάζονται επανεξέταση σε σύγκριση με τα συμβατικά συστήματα και τις κλασσικές στρατηγικές.
- Ζητήματα ασφάλειας ενδέχεται να προκύψουν κατά την αναβάθμιση των συσκευών από το διαδίκτυο. Για να μπορέσουν πολλές φορές να αναβαθμιστούν οι συσκευές πρέπει να ανοίξει η πρόσβαση τους από το διαδίκτυο, κάτι που μπορεί να εκμεταλλευτεί.
- Μη επαρκή γνώση σχετικά με τις λειτουργίες και την χρήση της συσκευής από τουςτελικούς χρήστες.
- Οι κακόβουλοι χρήστες ενδέχεται να αποκτήσουν άμεση φυσική πρόσβαση στις συσκευές IoT. Θα πρέπει να λαμβάνονται μέτρα κατά των αθέμιτων επεμβάσεων στις συσκευές.
- Παραβιάσεις ασφάλειας τις περισσότερες φορές δεν εντοπίζονται για μεγάλα χρονικά διαστήματα.

‘Όλα τα παραπάνω, μετέτρεψαν το IoT σε στόχο κυβερνοεπιθέσεων, καθώς κάποιοςκακόβουλος θα μπορούσε να

αποκτήσει εύκολα τον έλεγχο των συσκευών IoT[55]. Οι επιπτώσεις που προκαλούνται από την παραβίαση των συσκευών IoT είναι σοβαρές για τηνασφάλεια των διαδικτυακών υπηρεσιών, καθώς: οι εισβολείς ενδέχεται στα πλαίσια μιας επίθεσης να δημιουργήσουν κακόβουλα botnets ή να αποκτήσουν πρόσβαση σε εμπιστευτικές πληροφορίες. Ένα κακόβουλο botnet αποτελείται από μια συλλογή παραβιασμένων υπολογιστών που ελέγχεται εξ αποστάσεως μέσω του Internet, τις περισσότερες φορές με σκοπό την επίτευξη επιθέσεων με κατανεμημένη άρνηση υπηρεσίας (DDOS)[56]. Συνήθως, οι επιτιθέμενοι προσπαθούν μολύνουν όσο το δυνατόν περισσότερες συσκευές για να αυξήσουν την ισχύ και το αποτέλεσμα των επιθέσεων τους. Πράγματι, το 2016 το κακόβουλο λογισμικό Mirai[57] μόλυνε μεγάλο αριθμό συσκευών IoT, για να εκτελέσουν επιθέσεις DDOS, δημιουργώντας εκτεταμένη κίνηση στο Διαδίκτυο (πάνω από 1 tbps).

Ωστόσο, οι αποτελεσματικές και κατάλληλες λύσεις ασφαλείας μπορούν να επιτευχθούν μόνο εάν οι χρήστες που χρησιμοποιούν ή δημιουργούν τις συσκευές στο IoT, εμφανίσουν ευαισθητοποίηση σε θέματα ασφάλειας. Το συνεργατικό αυτό μοντέλο αναδύεται ως μια αποτελεσματική προσέγγιση στη βιομηχανία, τις κυβερνήσεις και τις δημόσιες αρχές για τη

---

[55] O. Arias, J. Wurm, K. Hoang, and Y. Jin. Privacy and security in internet of things and wearable devices. Multi-Scale Computing Systems, IEEE Transactions on, 1(2):99–109,

[56] Gernot Vormayr, Tanja Zseby, and Joachim Fabini. Botnet communication patterns. IEEECommunications Surveys & Tutorials, 19(4):2768–2796, 201

[57] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J Alex Halderman, Luca Invernizzi, Michalis Kallitsis, et al. Understanding the mirai botnet.In USENIX Security Symposium

διασφάλιση της ασφάλειας στο Διαδικτύου. Αυτό το μοντέλο περιλαμβάνει μια σειρά πρακτικών και εργαλείων, όπως αμφίδρομη ανταλλαγή πληροφοριών, ασκήσεις αντιμετώπισης περιστατικών ασφάλειας, ευαισθητοποίηση και εκπαίδευση των χρηστών, και συμμόρφωση με τα διεθνή πρότυπα ασφάλειας και πρακτικών.

Ωστόσο, οι συνεργατικές και κοινές προσεγγίσεις που βασίζονται στη διαχείριση κινδύνων ασφάλειας των συσκευών, πρέπει να συνεχίσουν να εξελίσσονται με γνώμονα τηνκλίμακα και την πολυπλοκότητα των προκλήσεων ασφάλειας συσκευών IoT. Εκτός από την ασφαλή εκκίνηση των συσκευών, τον έλεγχο πρόσβασης σε αυτές, τα τείχη προστασίας, τηδιεύθυνση IP, τον έλεγχο ταυτότητας και τις ενημερώσεις στον κώδικα των συσκευών θα πρέπει να δίνεται βάση στην ασφάλεια των συσκευών σε όλα τα επίπεδα τόσο συσκευής, εφαρμογής όσο και δικτύου[58].

Είναι πραγματικότητα ότι οι υποδομές Smart Home , απειλούνται από πληθώρα κυβερνοεπιθέσεων. Σχεδόν κάθε εβδομάδα εμφανίζεται κάποιο νέο περιστατικό που αφορά κυβερνοεπιθέσεις στο IoT. Μια από τις πρώτες αποδεδειγμένες μαζικές επιθέσεις που επηρέασαν συσκευές IoT συνέβη το 2014, όταν στάλθηκαν 750.000 κακόβουλα email από 100.000 συσκευές όπως τηλεοράσεις ή ψυγεία. Τον Οκτώβριο του 2015 μια μαζική επίθεση DDoS, που προκλήθηκε από έξυπνους λαμπτήρες, κάμερες ή θερμοστάτες, επηρέασε σημαντικούς διακομιστές DNS στις ΗΠΑ. Μια άλλη μαζική επίθεση DDoS που προκλήθηκεαπό πολλές διαφορετικές συσκευές, προκάλεσε την κατάρρευση του

[58] D. Jiang, and C. ShiWei, "A Study of Information Security for M2M of IoT," 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010, pp. 576-579

κεντρικού συστήματοςθέρμανσης μιας φινλανδικής πόλης, για μια ολόκληρη εβδομάδα τον Νοέμβριο του 2016.[59]

4.2.4 Εντοπισμός Υφιστάμενων Μέτρων Προστασίας

Στο τέταρτο βήμα, πραγματοποιείται η ανάλυση των επιμέρους μέτρων προστασίαςπου εφαρμόζονται στον οργανισμό και στα πληροφοριακά συστήματα, προκειμένου να ελαχιστοποιηθεί η πιθανότητα μια απειλή να εκμεταλλευτεί μια ευπάθεια. Τα μέτρα προστασίας είναι είτε τεχνικά είτε μη τεχνικά, δηλαδή οργανωτικά. Μπορούν επίσης να ταξινομηθούν περαιτέρω σε προληπτικά, περιοριστικά, μέτρα ανίχνευσης και ανάκαμψης. Όπως υποδηλώνει το όνομα, τα προληπτικά μέτρα προσπαθούν να προβλέψουν και να μειώσουν τις πιθανότητες πραγμάτωσης κάποιας απειλής. Τα περιοριστικά μέτρα έχουν στόχο την μείωση των επιπτώσεων από την πραγμάτωση κάποιας απειλής. Τα μέτρα ανίχνευσης χρησιμοποιούνται για την ανακάλυψη περιστατικών. Τέλος, τα μέτρα ανάκαμψης περιλαμβάνουν ίχνη ελέγχου και συστήματα ανίχνευσης εισβολών.

Ενδεικτικά τεχνικά μέτρα προστασίας αποτελούν: η διαχείριση ενημερώσεων κώδικα, ο μηχανισμός ελέγχου των πορτών σύνδεσης φορητών μέσων αποθήκευσης (π.χ. USB), ενεργοποίηση προστασίας από ιούς, η κρυπτογράφηση, επιβολή πολυπλοκότητας κωδικού πρόσβασης, προστασία από DDOs επιθέσεις, παράγοντας αυθεντικοποίησης δύο παραγόντων.

---

[59] Y. Gao, Y. Peng, F. Xie, W. Zhao, D. Wang, X. Han et al. Analysis of security threats and vulnerability for cyber-physical systems. In Computer Science and Network Technology (ICCSNT), 2013 3rd International Conference (IEEE, 2013), pp. 50–5

Ενδεικτικά οργανωτικά μέτρα προστασίας αποτελούν: σετ από πολιτικές ασφάλειας, απαιτήσεις ασφάλειας στις συμβάσεις, πολιτικές και διαδικασίες ελέγχου πρόσβασης, αφαίρεση αυξημένων δικαιωμάτων στα τερματικά των χρηστών.

Η μέθοδος συλλογής όλων των μέτρων προστασίας αλλά και πιθανών ευπαθειών που δεν έχουν βρεθεί με χρήση εργαλείων, μπορεί να πραγματοποιηθεί με τον διαμοιρασμό ερωτηματολογίων στους υπεύθυνους του κάθε συστήματος. Από τις παρακάτω ερωτήσεις, μπορεί να συλλεχθεί μεγάλος όγκος δεδομένων σχετικά με τα μέτρα και τις ευπάθειες.

Πίνακας 7: Ερωτηματολόγιο συλλογής ευπαθειών και μέτρων προστασίας.

Μέτρα προστασίας & ευπάθειες
Οι υπολογιστές των χρηστών διαθέτουν λογισμικό προστασίας από κακόβουλο λογισμικό (antivirus);
Οι servers του συστήματος διαθέτουν λογισμικό προστασίας από κακόβουλο λογισμικό (antivirus);
Χρησιμοποιούνται προσωποποιημένοι κωδικοί πρόσβασης για την πρόσβαση στους servers;
Εφαρμόζεται πολιτική περιοδικής αλλαγής και ελέγχου της πολυπλοκότητας των κωδικών πρόσβασης στους servers;
Τηρούνται αρχεία καταγραφής των ενεργειών των διαχειριστών των servers;
Υπάρχουν απομακρυσμένες προσβάσεις τρίτων μερών στους servers για τις οποίες δεν εφαρμόζεται διαδικασία ελέγχου;
Οι απομακρυσμένες προσβάσεις απενεργοποιούνται μετά από εύλογο χρονικό διάστημα;
Οι απομακρυσμένες προσβάσεις ανασκοπούνται περιοδικά (κατ' ελάχιστο σε ετήσια βάση);
Καταγράφονται όλες οι κρίσιμες αλλαγές στα συστήματα των servers;

Γίνεται σχεδιασμός για την επαναφορά της αλλαγής στην προηγούμενη κατάσταση σε περίπτωση αποτυχίας (servers);
Γίνεται έλεγχος αποδοχής της αλλαγής μετά την ένταξη στην παραγωγή (servers);
Καταγράφονται όλες οι κρίσιμες αλλαγές στα δικτυακά συστήματα που χρησιμοποιούνται για την επικοινωνία των servers;
Καταγράφονται σενάρια ελέγχου για κάθε αλλαγή στα δικτυακά συστήματα που χρησιμοποιούνται για την επικοινωνία των servers;
Έχουν γίνει τεχνικοί έλεγχοι ασφαλείας στην εφαρμογή (Vulnerability Assessment/ Penetration Test);
Έχουν αντιμετωπιστεί τα κρίσιμα ευρήματα ή ευρήματα υψηλής διαβάθμισης που έχουν προκύψει από τεχνικούς ελέγχους;
Έχουν αντιμετωπιστεί τα ευρήματα μεσαίας διαβάθμισης που έχουν προκύψει από τεχνικούς ελέγχους;
Οι servers είναι εγκατεστημένοι σε δικτυακή ζώνη στην οποία δεν συνδέονται υπολογιστές χρηστών;
Οι servers είναι εγκατεστημένοι σε δικτυακή ζώνη στην οποία υπάρχουν συνδεδεμένα αποκλειστικά συστήματα τα οποία υποστηρίζονται από τον κατασκευαστή τους;
Σε περίπτωση που οι servers δεν είναι προσβάσιμοι από το διαδίκτυο, είναι εγκατεστημένοι σε ζώνη όπου δεν υπάρχουν servers που είναι προσβάσιμοι από το διαδίκτυο;
Η πρόσβαση στη ζώνη των servers ελέγχεται μέσω firewall ή access lists;
Στη δικτυακή ζώνη των servers, έχουν απομακρυνθεί τα συστήματα που συνδέονται σε άλλες ζώνες μέσω διπλών Ethernet καρτών;
Η επικοινωνία των servers γίνεται μέσω δικτυακού εξοπλισμού που υποστηρίζεται από τον κατασκευαστή του;
Η επικοινωνία των servers γίνεται μέσω δικτυακού εξοπλισμού στον οποίο οι διαχειριστές συνδέονται με προσωποποιημένους λογαριασμούς;

Είναι ενεργοποιημένη η παραγωγή καταγραφών στο δικτυακό εξοπλισμό που χρησιμοποιείται για την επικοινωνία των servers;
Οι διαχειριστές χρησιμοποιούν ασφαλή κανάλια επικοινωνίας κατά τη σύνδεσή τους στον δικτυακό εξοπλισμό;

Μέτρα Προστασίας στο Smart Home

Καθώς οι απειλές είναι αναπόφευκτες, κάθε σύστημα πρέπει να σχεδιάζεται με το σκεπτικό ότι οι πιθανότητες να αποτελέσει στόχο επιθέσεων είναι μεγάλες. Η αυξανόμενη ανησυχία για την προστασία IoT, σχετίζεται με τις βασικές αρχές της έγκαιρης πρόληψης,
ανίχνευσης, αποκατάστασης, ανθεκτικότητας και αποτροπής κακόβουλων επιθέσεων[60]. Η πρόληψη αποτελεί την πρώτη γραμμή άμυνας εναντίον των επιθέσεων κατά της ασφάλειας των συστημάτων, και το γεγονός ότι οι συσκευές IoT εξυπηρετούν πολλούς διαφορετικούς τομείς με διαφορετικές τεχνολογίες αποτελεί πρόκληση ως προς την επίτευξη της [61] Για το λόγο αυτό, έχουν δημιουργηθεί πολλά πρότυπα ασφάλειας συστημάτων ανάλογα με τον εκάστοτε τομέα. Για παράδειγμα, στον ηλεκτρικό τομέα δημιουργήθηκε πρότυπο ασφάλειας από τη North American Electric Reliability Corporation (NERC). Το NIST έχει επίσης δημοσιεύσει ένα σύνολο βέλτιστων πρακτικών όπως το NIST SP 800-53, με ένα σύνολο συστάσεων που παρέχουν καθοδήγηση για την επίτευξη της ασφάλειας συστημάτων των περισσότερων εταιρειών. Το ISA (International Society of Automation) αναπτύσσει

[60] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, S. Sastry, Challenges for securing cyber physicalsystems. Proceedings of the Workshop on future directions in cyber-physical systems security (2009), p. 5

[61] Ziegler, Sébastien, Internet of Things Security and Data Protection.2019, p.51

το ISA99, το οποίο περιλαμβάνει ένα σύνολο προτύπων, προτεινόμενων πρακτικών, τεχνικών αναφορών και σχετικών πληροφοριών που θέτουν τα θεμέλια για την δημιουργία διαδικασιών, με στόχο την βελτίωση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των συστημάτων ελέγχου.

Η έγκαιρη ανίχνευση και η ανάκαμψη από οποιαδήποτε επιτυχημένη επίθεση κατά της ασφάλειας των συστημάτων, αποτελεί το κυριότερο αντίμετρο καταπολέμησης. Η χρήση εργαλείων συνεχούς παρακολούθησης της κίνησης των συστημάτων, αποτελεί πλέον το πρώτο μηχανισμό για την ανίχνευση επιθέσεων. Για το σκοπό αυτό, μια βασική πτυχή για την ανίχνευση επιθέσεων είναι η πλήρης και βαθιά γνώση των συστημάτων. Πολύ συχνά αυτό πραγματοποιείται μέσω ανθρώπινης παρέμβασης, αν και η ανάγκη αυτοματοποιημένης ανάκαμψης και αντιμετώπισης περιστατικών γίνεται μία από τις πρωταρχικές προκλήσεις που αντιμετωπίζει σήμερα η βιομηχανία. Η ανθεκτικότητα των συστημάτων, μαζί με τις βασικές αρχές ασφάλειας κατά τον σχεδιασμό, αποτελούν μια άλλη σημαντική πτυχή που χρησιμοποιείται για την αντιμετώπιση ή την πρόληψη επιθέσεων. Ορισμένες ενέργειες που σχετίζονται με τα παραπάνω είναι τα εφεδρικά συστήματα (για την αποφυγή ενός σημείου αποτυχίας), η διαφορετικότητα (με την ίδια υπηρεσία να εκτελείται σε διαφορετικά συστήματα) ή ο περιορισμός των προνομίων/δικαιωμάτων των χρηστών (διαχωρισμός προνομίων μεταξύ διαφορετικών χρηστών για τον περιορισμό της πρόσβασης).

4.2.5 Εκτίμηση Πιθανότητας και Αντικτύπου

Μετά την συλλογή των παραπάνω πληροφοριών, ακολουθεί το πέμπτο βήμα, η εκτίμηση της πιθανότητας μια απειλή να εκμεταλλευτεί κάποια ευπάθεια, λαμβάνοντας υπόψη τον τύπο της ευπάθειας, την ικανότητα και το κίνητρο της πηγής απειλής, καθώς καιτην ύπαρξη και την αποτελεσματικότητα των

μέτρων προστασίας. Στην συνέχεια ακολουθεί η αξιολόγηση του αντικτύπου που θα μπορούσε να επιφέρει η απειλή. Για να αξιολογηθεί το αντίκτυπο, πρέπει να συνυπολογιστούν ποιο σκοπό εξυπηρετεί το περιουσιακό στοιχείο και τυχόν επιχειρηματικές δραστηριότητες που εξαρτώνται από αυτό,η αξία του περιουσιακού στοιχείου για τον οργανισμό και η ευαισθησία του περιουσιακού στοιχείου. Οι παραπάνω πληροφορίες μπορούν να συλλεχθούν από την ανάλυση επιχειρηματικού αντίκτυπου (BIA), η οποία προσδιορίζει τον αντίκτυπο ως προς την απώλεια εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας. Η πιθανότητα και το αντίκτυπο στο σύστημα μπορούν να αξιολογηθούν ποιοτικά με χρήση της διαβάθμισης 'υψηλός, μεσαίος ή χαμηλός κίνδυνος.

4.2.6 Προσδιορισμός του Επίπεδου Κινδύνου

Στο έκτο βήμα, για κάθε ζεύγος απειλής/ευπάθειας, προσδιορίζεται το επίπεδο κινδύνου, με βάση την συνάρτηση που είδαμε παραπάνω : Κίνδυνος = Απειλή x Ευπάθεια x Περιουσιακό στοιχείο. Στην συνέχεια, εκτιμάται το κατά προσέγγιση κόστος που θα προκύψει σε περίπτωση που συμβεί κάποιο περιστατικό, καθώς και η επάρκεια των υφιστάμενων ή προγραμματισμένων ελέγχων ασφάλειας του πληροφοριακού συστήματος για την εξάλειψη ή τη μείωση του κινδύνου και επανεξετάζεται η πιθανότητα και το αντίκτυπο εμφάνισης του κινδύνου.

Ένα χρήσιμο εργαλείο για την εκτίμηση του κινδύνου είναι ο πίνακας επιπέδου κινδύνου που είδαμε παραπάνω. Για παράδειγμα, για μια μεγάλη πιθανότητα να συμβεί η απειλή δίνεται η τιμή 1,0. Σε μια μεσαία πιθανότητα αποδίδεται μια τιμή 0,5 και σε μια χαμηλή πιθανότητα εμφάνισης δίδεται βαθμολογία 0,1. Ομοίως, σε ένα υψηλό επίπεδο επιπτώσεων εκχωρείται η τιμή 100, σε ένα μεσαίο επίπεδο επίπτωσης το 50 και σε ένα χαμηλό επίπεδο επίπτωσης το 10. Ο κίνδυνος υπολογίζεται

πολλαπλασιάζοντας την τιμή πιθανότητας απειλής με την τιμή του αντίκτυπου και οι κίνδυνοι κατηγοριοποιούνται σευψηλούς, μεσαίους ή χαμηλά με βάση το αποτέλεσμα.

Πίνακας 8: Εφαρμογή μεθοδολογίας αξιολόγησης κινδύνων Smart Home.

Ευπάθεια	Πληροφοριακό Σύστημα	Πηγή Απειλής	Ενέργεια Απειλής	Κίνδυνος έκθεσης	Περίληψη Κινδύνου	ΕΚΤΙΜΗΣΗ ΚΙΝΔΥΝΟΥ			Υπάρχοντα Μέτρα	ΥΠΑΡΧΟΥΣΑ ΚΑΤΑΣΤΑΣΗ		
						Πιθανότητα Εμφάνισης Κινδύνου	Επίπτωση	Συνολική αξιολόγηση Κινδύνου		Πιθανότητα Εμφάνισης Κινδύνου	Επίπτωση	Συνολική αξιολόγηση Κινδύνου
Δεν εφαρμόζεται κρυπτογράφηση	Βάση Δεδομένων	Hackers, spammers, Εγκληματίες Κυβερνοχώρου, Ανταγωνιστές	Υποκλοπή, τροποποίηση δεδομένων	Εμπιστευτικότητα, Ακεραιότητα	Κλοπή/Αποκάλυψη/Τροποποίηση δεδομένων που περιέχουν εμπιστευτικές πληροφορίες	Μεσαία-0.5	Υψηλή-100	Μεσαία επικινδυνότητα (100x0.5=50)	Υπάρχει password policy για την είσοδο στην βάση δεδομένων. Επίσης, κατά την ενεργοποίηση χρήστη και σε περίπτωση reset του password, ο χρήστης υποχρεούται από το σύστημα να αλλάξει το password κατά την αρχική σύνδεση. Υπάρχει επίσης firewall	Χαμηλή-0.1	Υψηλή-100	Χαμηλή επικινδυνότητα (100x0.1=10)
Έλλειψη σχεδίου διαχείρισης των περιστατικών ασφάλειας	Όλοι οι πόροι του smart home	Κάθε απειλή	Ενέργεια κάθε απειλής	Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα	Αυξημένο επίπεδο επικινδυνότητας για όλους τους κινδύνους	Μεσαία-0.5	Υψηλή-100	Μεσαία επικινδυνότητα (100x0.5=50)	Υπάρχει πολιτική και διαδικασία διαχείρισης περιστατικών ασφάλειας	Χαμηλή-0.1	Υψηλή-100	Χαμηλή επικινδυνότητα (100x0.1=10)
Έλλειψη τεκμηριωμένης πολιτικής backup και restore	Όλοι οι πόροι του smart home	Αστοχία Υλικού	Απώλεια δεδομένων σε περίπτωση αστοχίας μέρους εξοπλισμού	Διαθεσιμότητα	Άρση της διαθεσιμότητας	Υψηλή-1	Υψηλή-100	Υψηλή επικινδυνότητα (100x1.0=100)	Λαμβάνονται καθημερινά αντίγραφα ασφάλειας (backup) από τους παραγωγικούς servers, υπάρχει το backup plan	Μεσαία-0.5	Υψηλή-100	Μεσαία επικινδυνότητα (100x0.5=50)

4.2.7 Αντιμετώπιση Κινδύνων

Στο τελευταίο βήμα, χρησιμοποιώντας το επίπεδο κινδύνου ως βάση, καθορίζονται οι μέθοδοι αντιμετώπισης του κινδύνου, δηλαδή τυχών ενέργειες που απαιτούνται για τον μετριασμό του κινδύνου. Ο σχεδιασμός για την αντιμετώπιση κινδύνων περιλαμβάνει την ανάληψη ευθύνης από ένα ή περισσότερα άτομα προκειμένου να αποφασιστεί αν θα πρέπει να προχωρήσει ο οργανισμός σε μετριασμό ή σε αποδοχή κάθε εντοπισμένου κίνδυνου. Ο υπεύθυνος σε συνεργασία με τα αρμόδια τμήματα ενός οργανισμού (π.χ. ασφάλεια πληροφοριακών συστημάτων, πληροφορική), καθορίζει τις ενέργειες που πρέπει να ληφθούν έναντι αυτού του κινδύνου μέσω της ανάπτυξης μέτρων και σχεδίων δράσης. Ο σχεδιασμός αντιμετώπισης κινδύνου αποτελεί τη διαδικασία ανάπτυξης επιλογών και ενεργειών για την μείωση των απειλών με αποτέλεσμα την επίτευξη των επιχειρησιακών στόχων. Ακολουθούν ορισμένες γενικές οδηγίες για κάθε επίπεδο κινδύνου:

Υψηλό — Θα πρέπει να αναπτυχθεί ένα σχέδιο για διορθωτικά μέτρα το συντομότεροδυνατό.

Μεσαίο — Ένα σχέδιο για διορθωτικά μέτρα θα πρέπει να αναπτυχθεί μέσα σε εύλογοχρονικό διάστημα.

Χαμηλό — Η ομάδα πρέπει να αποφασίσει αν θα αποδεχτεί τον κίνδυνο ή θα εφαρμόσειδιορθωτικές ενέργειες.

Οι ενέργειες αντιμετώπισης κινδύνου περιλαμβάνουν:

Αποφυγή: Λήψη μέτρων για την εξάλειψη της απειλής ή της ευπάθειας που μπορεί ναοδηγήσει στην εκδήλωση του κινδύνου.

Μεταβίβαση: Ανάθεση της ευθύνης των κινδύνων σε τρίτα μέρη (ασφαλιστικές εταιρείες,υπηρεσίες ασφαλείας και συντήρησης).

Μείωση: Λήψη μέτρων που δεν οδηγούν στην εξάλειψη του κινδύνου αλλά στη μείωση τηςσοβαρότητάς του.

Αποδοχή: Συνειδητή απόφαση αποδοχής της ύπαρξης του κινδύνου και των συνεπειών σεπερίπτωση εκδήλωσης του.

Ως επί το πλείστων, ο σχεδιασμός του τρόπου ανταπόκρισης στον κίνδυνο αποτελείται από τον καθορισμό ορίων αποδοχής του κινδύνου, τον εντοπισμό των παραγόντων εμφάνισης του και, στη συνέχεια, τον σχεδιασμό μιας στρατηγικής μετριασμούτου αλλά και την ανάπτυξη σχεδίων έκτακτης ανάγκης. Οι στρατηγικές μετριασμού του κινδύνου εντοπίζουν τυχόντα τεχνικά ή οργανωτικά μέτρα που πρέπει να ληφθούν για να ελαχιστοποιούν ή να εξαλείφουν τους κινδύνους πριν καν εμφανιστούν. Οι δραστηριότητες μετριασμού του κινδύνου έχουν στόχο να εξισορροπήσουν την πιθανότητα και τη σοβαρότητα της εμφάνισης του σε συνάρτηση πάντα με το κόστος και την αποτελεσματικότητα της στρατηγικής. Για να είναι αποτελεσματικές οι στρατηγικές μετριασμού ενός κίνδυνου πρέπει να ανιχνεύονται οι παράγοντες ενεργοποίησης που υποδεικνύουν πότε η στρατηγική δεν είναι πλέον αποτελεσματική και πρέπει να εκτελούνται σχέδια έκτακτης ανάγκης.

Η ανίχνευση και ο έλεγχος κινδύνου παρακολουθούν την πρόοδο της πιθανότητας εμφάνισης του και, εάν είναι απαραίτητο, εντοπίζουν πότε οι συνέπειες εμφάνισης του κινδύνου κλιμακώνονται σε σημείο που απαιτείται η εφαρμογή σχεδίων έκτακτης ανάγκης.Με την συνεχή παρακολούθηση του επιπέδου του κινδύνου, τα σχέδια ανάκαμψης μπορούννα προσαρμοστούν με βάση τις αλλαγές που μπορεί να επηρεάσουν τα επίπεδα κινδύνου. Έτσι, σε περίπτωση που ο κίνδυνος συμβεί, τα καθορισμένα σχέδια έκτακτης ανάγκης ελαχιστοποιούν την επίδραση του κινδύνου στα παραδοτέα του έργου ή στη συνολική λειτουργία ενός οργανισμού.

5. ΜΕΛΕΤΗ ΕΚΤΙΜΗΣΗΣ ΑΝΤΙΚΤΥΠΟΥ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Καθώς οι σύγχρονες τεχνολογίες εξελίσσονται ραγδαία, εισάγονται νέοι νόμοι για την αντιμετώπιση των μεταβαλλόμενων συνθηκών στο χώρο του διαδικτύου. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ), όπως είδαμε και παραπάνω, αποτελεί μια πρόσφατη προσθήκη στους νόμους και έχει εφαρμογή σε όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης (ΕΕ), αλλά και σε οργανισμούς οι οποίοι ενώ δεν εδρεύουν στην Ευρωπαϊκή Ένωση, επεξεργάζονται δεδομένα Ευρωπαίων πολιτών.

Μεταξύ των πολλών αλλαγών που έχει επιφέρει ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) εισάγονται νέες κατευθυντήριες σχετικά με την αξιολόγηση του κινδύνου ως προς την προστασία της ιδιωτικότητας. Η Εκτίμηση Επιπτώσεων ως προς την Ιδιωτικότητα (PIA) και η Εκτίμηση Επιπτώσεων ως προς την Προστασία Δεδομένων (ΕΑΠΔ) αποτελούν μεθοδολογίες ανάλυσης του αντίκτυπου που θα μπορούσε να επιφέρει η πραγμάτωση του κινδύνου στα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Στην περίπτωση του ΓΚΠΔ, τα δεδομένα που αποτελούν κίνδυνο για τους οργανισμούς είναι τα προσωπικά δεδομένα που διαχειρίζονται και επεξεργάζονται - και η αποτυχία διασφάλισής τους μπορεί να καταλήξει σε πολύ μεγάλα πρόστιμα. Η αποτυχία διασφάλισης των δεδομένων, έχει ως αποτέλεσμα και άλλες απώλειες πέρα τις οικονομικέςσε έναν οργανισμό, επομένως όσο πιο ακριβής είναι η εκτίμηση κινδύνου

τόσο καλύτερη είναι η διαχείριση των δεδομένων αυτών[62]. Ωστόσο, μια αποτελεσματική ΕΑΠΔ μπορεί επίσης να αποφέρει ευρύτερη απόδειξη ως προς τη συμμόρφωση, οικονομικά κέρδη και οφέλη για τη φήμη, βοηθώντας έναν οργανισμό να επιδείξει υπευθυνότητα και να δημιουργήσει εμπιστοσύνη και δέσμευση στα άτομα. Η ΕΑΠΔ είναι σημαντικό να ενσωματώνεται στις τακτικές διαδικασίες και να διασφαλίζεται ότι το αποτέλεσμα μπορεί να επηρεάσει τα επιχειρηματικά σχέδιά σας. Η ΕΑΠΔ δεν αποτελεί εφάπαξ άσκηση, θα πρέπει να αποτελεί μια συνεχή διαδικασία που υπόκειται σε τακτική επανεξέταση.

Η εκτίμηση κινδύνου όπως είδαμε παραπάνω είναι η διαδικασία εντοπισμού των απειλών, ο προσδιορισμός της πιθανότητας εκμετάλλευσης τους, ο προσδιορισμός τουαντίκτυπου που θα επέλθει από την πραγματοποίηση των κινδύνων, η ποσοτικοποίηση των κινδύνων, καθώς και η ανάπτυξη των απαραίτητων στρατηγικών μετριασμού. Υπάρχουν διαφορετικές μεθοδολογίες για την αξιολόγηση των κινδύνων ως προς την ασφάλεια των συστημάτων, εκ των οποίων τα πιο δημοφιλή από αυτά είναι το OCTAVE, NIST και ISO.[63]Ταπρότυπα αυτά παρέχουν κατευθυντήριες γραμμές για την αξιολόγηση του κινδύνου σε έναν οργανισμό εκτελώντας τρία σημαντικά βήματα: ανάλυση κινδύνου, αξιολόγηση κινδύνου και αξιολόγηση επιχειρηματικού αντίκτυπου. Ωστόσο, οι παραπάνω μεθοδολογίες αξιολόγησης κινδύνου, εμφανίζουν περιορισμούς όταν χρησιμοποιούνται για την ανάλυση της συμμόρφωσης ως προς την προστασία των

---

[62] Haes S., Debreceny R., Van Grembergen W. (2013). Understanding the Core Concepts in COBIT 5, Information Systems Audit and Control Association Journal, Vol 5, pp. 1-8

[63] "Risk Assessment & Data Protection Impact Assessment Guide" - Bitkom e. V. Federal Association forInformation Technology

προσωπικών δεδομένων. Οι περιορισμοί εμφανίζονται διότι οι μεθοδολογίες αυτές δεν είναι σε θέση να προσδιορίσουν ορισμένες πτυχές ή κινδύνους στους οποίους υπόκεινται τα δεδομένα προσωπικού χαρακτήρα, και φυσικά, τα πλαίσια αξιολόγησης κινδύνου είναι περιορισμένα , επειδή δεν είναι σε θέση να αναλύσουν τον τρόπο που θίγονται τα δικαιώματα και οι ελευθερίες των ατόμων[64].

Ωστόσο, έχουν αναπτυχθεί κατάλληλες μεθοδολογίες για την αξιολόγηση των κινδύνων ως προς την ιδιωτικότητα, οι οποίες εφαρμόζονται σε όλους τους τομείς. Η πιο γνωστή είναι η μεθοδολογία της Γαλλικής Αρχής Προστασίας Δεδομένων (CNIL), η οποία στοχεύει να συμπληρώσει και να διευκρινίσει, από επιχειρησιακή άποψη, τις συστάσεις 01/2020 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων («EDPB»), για τη διασφάλιση της συμμόρφωσης με τον ΓΚΠΔ.

Παρακάτω θα αναλύσουμε, ένα συνδυασμό της μεθοδολογίας της Γαλλικής Αρχής Προστασίας Δεδομένων (CNIL)[65], του προτύπου ISO29134:2017 και της αξιολόγησης κινδύνων σύμφωνα με το NIST, που είδαμε παραπάνω. Το ISO/IEC 29134:2017 παρέχει κατευθυντήριες γραμμές για τη διαδικασία σχετικά με την διεκπεραίωση της εκτίμησης επιπτώσεων, καθώς και τη δομή και το περιεχόμενο της. Το πρότυπο αυτό βρίσκει εφαρμογή σε όλους τους τύπους και τα μεγέθη οργανισμών, συμπεριλαμβανομένων των δημόσιων εταιρειών, ιδιωτικών εταιρειών, κρατικών φορέων και μη κερδοσκοπικών οργανισμών.

---

[64] ISO/IEC 27005, International Standard, 15.06.2008

[65] "PRIVACY IMPACT ASSESSMENT (PIA) Methodology (how to carry out a PIA)" – CNIL June2015 Edition

Για την ορθή διενέργεια της ΕΑΠΔ, πρέπει να παρέχεται συστηματική περιγραφή των πράξεων επεξεργασίας δηλαδή να λαμβάνονται υπόψη η φύση, η έκταση, το πλαίσιο και οι σκοποί της επεξεργασίας, να καταγράφονται τα δεδομένα προσωπικού χαρακτήρα, οι αποδέκτες και η περίοδος αποθήκευσης τους, να προσδιορίζονται τα στοιχεία του ενεργητικού στα οποία εναποτίθενται τα δεδομένα (υλικό, λογισμικό, δίκτυα, πρόσωπα, έντυπα ή δίαυλοι διαβίβασης εντύπων) και να λαμβάνεται υπόψη η συμμόρφωση με εγκεκριμένους κώδικες δεοντολογίας. Επίσης, εκτιμώνται η αναγκαιότητα και η αναλογικότητα, δηλαδή καθορίζονται τα προβλεπόμενα μέτρα συμμόρφωσης με τον κανονισμό λαμβάνοντας υπόψη τα μέτρα που κατατείνουν στην αναλογικότητα και την αναγκαιότητα της επεξεργασίας, να τελούν υπό διαχείριση οι κίνδυνοι για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και να συμμετέχουν τα ενδιαφερόμενα μέρη.

Τα βήματα που θα ακολουθηθούν για την διεκπεραίωση της εκτίμησης αντικτύπου είναι τα παρακάτω:

1. Προσδιορισμός της ανάγκη για ΕΑΠΔ

2. Περιγραφή της επεξεργασίας

3. Απεικόνιση της ροής της επεξεργασίας

4. Αξιολόγηση της αναγκαιότητας και της αναλογικότητας

5. Προσδιορισμός των υφιστάμενων μέτρων προστασίας

6. Αξιολόγηση κινδύνων

7. Σχέδιο Δράσης

8. Αποδοχή και καταγραφή των αποτελεσμάτων

5.1 Προσδιορισμός Ανάγκης Διεκπεραίωσης ΕΑΠΔ

Η εκτίμηση αντικτύπου προσωπικών δεδομένων είναι πρακτική αυτοαξιολόγησης, ηοποία βοηθάει στη λήψη αποφάσεων σχετικά με τα οργανωτικά και τεχνικά μέτρα που πρέπει να λάβει ένας οργανισμός, στην συμμόρφωση του καθώς και στο σχεδιασμό μιας νέας υπηρεσίας ή έργου. Η ΕΑΠΔ θα πρέπει να διενεργείται από τον Υπεύθυνο Επεξεργασίας, «πριν από την επεξεργασία» προκειμένου να συνάδει με τις αρχές της εξ ορισμού και της εκ σχεδιασμού προστασίας των δεδομένων.

Σύμφωνα με το άρθρο 35 του ΓΚΠΔ, η ανάλυση αντικτύπου είναι υποχρεωτική και πρέπει να πραγματοποιείται σε έναν οργανισμό σε περιπτώσεις όπου η επεξεργασία δεδομένων προσωπικού χαρακτήρα συνιστά υψηλό κίνδυνο για τα δικαιώματα και τιςελευθερίες ενός φυσικού προσώπου ιδίως με τη χρήση νέων τεχνολογιών και συνεκτιμώνταςτη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας. Ο κανονισμός όμως δεν ορίζει τον «υψηλό κίνδυνο».[54] Ωστόσο, ορίζει κριτήρια για τον χαρακτηρισμό του «υψηλού κινδύνου» μέσα από νομοθετικές διατάξεις και κατευθυντήριες γραμμές. Ενδεικτικά είδη πράξεων επεξεργασίας οι οποίες ενέχουν υψηλό κίνδυνο παρατίθενται στο άρθρο 35 παρ. 3 του ΓΚΠΔ (βλ. αιτ. 91 του ΓΚΠΔ) και έχουν υιοθετηθεί εννέα κριτήρια, προκειμένου να καθοριστεί η ανάγκη διενέργειας της μελέτης και έχει προδιαγραφεί η κατάρτιση ειδικών καταλόγων από τα κράτη μέλη σε εθνικό επίπεδο [66]. Σύμφωνα με την απόφαση 65/2018,της Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, τα κριτήρια για την

[66] Article 29 Working Party. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk, for the purposes of Regulation 2016/679," WP 250.

διενέργεια ΕΑΠΔ ομαδοποιούνται σε τρεις κατηγορίες.[67] Η διενέργεια ΕΑΠΔ κρίνεται υποχρεωτική όταν πληρούνται τουλάχιστον ένα από τα κριτήρια της 1ης ή της 2ης κατηγορίας. Η πρώτη κατηγορία αφοράει τα είδη και τους σκοπούς της επεξεργασίας και συμπεριλαμβάνει τη συστηματική αξιολόγηση, βαθμολόγηση, πρόβλεψη, πρόγνωση και κατάρτιση προφίλ ιδίως σε ότι αφορά κατάσταση υγείας, προσωπικές προτιμήσεις, αξιοπιστία ή συμπεριφορά, τη θέση και τις κινήσεις και την πιστοληπτική ικανότητα καθώς και συστηματική επεξεργασία δεδομένων με σκοπό την κατάρτιση προφίλ για το σκοπό της προώθησης προϊόντων και υπηρεσιών. Στη πρώτη κατηγορία εμπίπτει και η συστηματική επεξεργασία δεδομένων που αποσκοπεί στη λήψη αυτοματοποιημένων αποφάσεων όπως για παράδειγμα το screening των βιογραφικών χωρίς ανθρώπινη παρέμβαση καθώς και η συστηματική επεξεργασία δεδομένων που ενδέχεται να εμποδίζει το υποκείμενο να ασκήσει τα δικαιώματά του ή να χρησιμοποιήσει μια υπηρεσία ή σύμβαση. Τέλος, στη πρώτη κατηγορία εμπίπτει η συστηματική και σε μεγάλη κλίμακα επεξεργασία για την παρακολούθηση, την παρατήρηση ή τον έλεγχο των φυσικών προσώπων με χρήση δεδομένων που συλλέγονται μέσω συστημάτων βιντεοεπιτήρισης, για δεδομένα που αφορούν την υγεία και τη δημόσια υγεία για σκοπούς δημοσίου συμφέροντος και μεγάλη κλίμακας επεξεργασία δεδομένων με σκοπό την χρήση των υπηρεσιών ηλεκτρονικής διακυβέρνησης.

Η δεύτερη κατηγορία αφοράει το είδος δεδομένων ή/και κατηγορίες υποκειμένων. Πιο συγκεκριμένα, σε αυτή τη κατηγορία περιλαμβάνονται μεγάλης κλίμακας επεξεργασία των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παρ. 1 και

---

[67] Απόφαση 65/2018, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Αθήνα, 16-10-2018, Αθήνα, 16-10-2018

των δεδομένων που αναφέρονται στο άρθρο 10 του ΓΚΠΔ. Στη κατηγορία αυτή, εμπίπτει και η συστηματική και σε μεγάλη κλίμακα επεξεργασία δεδομένων ιδιαίτερης σημασίας ή εξαιρετικού χαρακτήρα όπως: δεδομένα κοινωνικής πρόνοιας, δεδομένα ηλεκτρονικών επικοινωνιών, περιλαμβανομένων των δεδομένων περιεχομένου όπως του ηλεκτρονικού ταχυδρομείου, μεταδεδομένων και των δεδομένων γεωγραφικής θέσης/τοποθεσίας, δεδομένα που αφορούν εθνικό αριθμό ταυτότητας ή άλλο αναγνωριστικό στοιχείο ταυτότητας γενικής εφαρμογής ή αλλαγή των προϋποθέσεων και όρων επεξεργασίας και χρήσης αυτών και των συναφών με αυτά δεδομένων προσωπικού χαρακτήρα, δεδομένα που περιλαμβάνονται σε προσωπικά έγγραφα, ημερολόγια, σημειώσεις από ηλεκτρονικό αναγνώστη και σε εφαρμογές καταγραφής βίου ,που προσφέρουν δυνατότητες τήρησης σημειώσεων και πολύ προσωπικών πληροφοριών, δεδομένα που συλλέγονται ή παράγονται από συσκευές (όπως αυτές με αισθητήρες) ιδίως μέσω των εφαρμογών του 'διαδικτύου των πραγμάτων -IoT' (όπως έξυπνες τηλεοράσεις, έξυπνες οικιακές συσκευές, συνδεδεμένα παιχνίδια, έξυπνες πόλεις, έξυπνοι μετρητές ενέργειας κλπ.) και/ή με τη χρήση άλλων μέσων.

Τέλος, η δεύτερη κατηγορία αφοράει τη συστηματική παρακολούθηση –εφόσον είναι επιτρεπτή –της θέσης/τοποθεσίας καθώς και του περιεχομένου και των μεταδεδομένων των επικοινωνιών των εργαζομένων με εξαίρεση τα αρχεία καταγραφής για λόγους ασφάλειας εφόσον η επεξεργασία περιορίζεται στα απολύτως απαραίτητα δεδομένα και είναι ειδικά τεκμηριωμένη καθώς και η η συστηματική επεξεργασία βιομετρικών δεδομένων των εργαζομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου καθώς και γενετικών δεδομένων των εργαζομένων.

Η Εκτίμηση Αντικτύπου Προσωπικών Δεδομένων (DPIA), είναι υποχρεωτική όταν συντρέχει ένα τουλάχιστον κριτήριο ως προς την τρίτη κατηγορία που σχετίζεται με τα πρόσθετα χαρακτηριστικά ή/και χρησιμοποιούμενα μέσα της επεξεργασίας και η επεξεργασία αφορά είδη και σκοπούς επεξεργασίας της πρώτης κατηγορίας, ή/και είδη δεδομένων ή/και κατηγορίες υποκειμένων της δεύτερης κατηγορίας. Χαρακτηριστικά παραδείγματα της τρίτης κατηγορίας είναι η καινοτόμος χρήση εφαρμογή νέων τεχνολογιών ή οργανωτικών λύσεων (όπως η συνδυασμένη χρήση των δακτυλικών αποτυπωμάτων και η αναγνώριση προσώπου για βελτιωμένο φυσικό έλεγχο πρόσβασης, ή εφαρμογές τεχνητής νοημοσύνης), ο συνδυασμός και/ή συσχέτιση προσωπικών δεδομένων από πολλαπλές πηγές ή τρίτους, από δύο ή περισσότερες πράξεις επεξεργασίας και τέλος σε περίπτωση που η επεξεργασία αφορά δεδομένα, τα οποία δεν έχουν συλλεγεί από το υποκείμενο και η ενημέρωση των υποκειμένων σύμφωνα με το άρθρο 14 ΓΚΠΔ αποδεικνύεται αδύνατη.

Στην περίπτωση που κάποια διεργασία δεν περιλαμβάνεται στις παραπάνω κατηγορίες επεξεργασίας, πρέπει να ελεγχθούν άλλοι παράγοντες που μπορεί να υποδεικνύουν ότι ηεπεξεργασία πιθανώς οδηγήσει σε υψηλό κίνδυνο. Εάν αποφασιστεί ότι δεν απαιτείται ΕΑΠΔ για την συγκεκριμένη επεξεργασία, είναι απαραίτητη η τεκμηρίωση και ο λόγος της απόφασης αυτής, συμπεριλαμβανομένων των κατευθυντήριων του Υπεύθυνο Προστασίας Προσωπικών Δεδομένων. Ωστόσο, αν υπάρχει οποιαδήποτε αμφιβολία για την διενέργεια της ΕΑΠΔ, θα πρέπει να υλοποιείται.

Σε αυτό το σημείο, είναι αναγκαίο να εντοπίσουμε την υποχρέωση του Υπευθύνου Επεξεργασίας δεδομένων να διενεργεί Μελέτη Εκτίμησης Αντικτύπου (DPIA), πριν από την επεξεργασία των δεδομένων κατά τα πλαίσια λειτουργίας του έξυπνου σπιτιού.

Η DPIA αποτελεί μια προσέγγιση διαχείρισης κινδύνων, η οποία αξιολογεί τον κίνδυνο κάθε επεξεργασίας σε ένα συγκεκριμένο πλαίσιο όπως είδαμε παραπάνω. Με βάση τα παραπάνω κριτήρια είναι φανερό ότι η DPIA στο Smart Home είναι υποχρεωτική, λόγω του είδους των δεδομένων και συγκεκριμένα της συστηματικής και σε μεγάλης κλίμακας επεξεργασία δεδομένων με χρήση καινοτόμων τεχνολογιών[68], όπως οι αισθητήρες. Οι IoT συσκευές των έξυπνων κατοικιών επεξεργάζονται συνεχώς μεγάλης κλίμακας δεδομένα όπως πχ. βιντεογραφικό υλικό από τις κάμερες για την επίτευξη της ασφάλειας του σπιτιού, τις καταναλώσεις ενέργειας, φωνητικές εντολές και πολλά άλλα δεδομένα. Ένα άλλο σημαντικό ζήτημα που προκύπτει και απαιτεί τη διενέργεια μελέτης αντικτύπου είναι η συστηματική και εκτενής αξιολόγηση προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ[69]. Πιο συγκεκριμένα, οι έξυπνες οικιακές συσκευές 'γνωρίζουν' διαφορετικές πτυχές της προσωπικότητας των μελών του σπιτιού, αυξάνοντας τη δυνατότητα στοχευμένης διαφήμισης. [70]

Άλλο ένα σημαντικό ζήτημα, είναι ότι στα πλαίσια λειτουργίας του Smart Home, ενδέχεται να επεξεργαστούν δεδομένα παιδιών που κατοικούν στο έξυπνο σπίτι (φωνητικές εντολές, βιντεογραφικό υλικό από τις κάμερες κλπ.). Σύμφωνα με

---

[68] 'Άρθρο 35 παράγραφος 1, ΕΕ Γενικός Κανονισμός για την Προστασία Δεδομένων

[69] Άρθρο 35 παράγραφος 3, ΕΕ Γενικός Κανονισμός για την Προστασία Δεδομένων

[70] J. Bugeja and A. Jacobsson, "On the design of a privacy centered data lifecycle for smart living spaces," IFIP International Summer School on Privacy and Identity Management, Springer, Cham, August 2019, pp. 126-141.

τον Κανονισμό τα παιδιά θεωρούνται ευάλωτα υποκείμενα, τα οποία μπορεί να θεωρηθεί ότι δεν είναι σε θέση να εναντιωθούν ή να συναινέσουν μετά λόγου γνώσης ή συνειδητά στην επεξεργασία των δεδομένων τους [71]. Δεδομένου αυτού, η επεξεργασία ενδέχεται να οδηγήσει σε υψηλό κίνδυνο για τις ελευθερίες και τα δικαιώματα των φυσικών προσώπων. [72] Ως προς την επεξεργασία προσωπικών δεδομένων παιδιών, μέσω αυτοματοποιημένης λήψης αποφάσεων, η επεξεργασία επιτρέπεται μόνο με τις εξαιρέσεις του άρθρου 22 παράγραφος 2 στοιχεία α), β) ή γ). Δεδομένου ότι τα παιδιά δεν μπορούν να συναινέσουν συνειδητά, η κατάρτιση προφίλ θα αποτελούσε μη σύννομη επεξεργασία.

5.2 Προσδιορισμός Υπεύθυνου Επεξεργασίας

Στο πλαίσιο της ανάπτυξης υπηρεσιών Smart Home, είναι πολύ σημαντικό να αποσαφηνιστούν οι ρόλοι και να καθοριστεί ποιος είναι ο υπεύθυνος επεξεργασίας των δεδομένων, ο οποίος θα εκτελέσει και την DPIA. Το άρθρο 4 παράγραφος 7 του ΓΚΠΔ ορίζει ότι «υπεύθυνος επεξεργασίας» είναι ένα φυσικό ή νομικό πρόσωπο, μια δημόσια αρχή, ένας οργανισμός ή άλλος φορέας που καθορίζει τους σκοπούς και τα μέσα επεξεργασίας των προσωπικών δεδομένων. Σύμφωνα με αυτόν τον ορισμό και λαμβάνοντας υπόψη τον τρόπο υλοποίησης του Smart Home, οι επιχειρηματικοί οργανισμοί που αναλαμβάνουν την πώληση των εφαρμογών που θα διαχειρίζονται τις έξυπνες συσκευές, καθορίζουν τους σκοπούς και τα μέσα επεξεργασίας των προσωπικών δεδομένων, είναι οι

---

[71] ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ ΤΟΥ ΑΡΘΡΟΥ 29 ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ, Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679.

[72]

υπεύθυνοι επεξεργασίας. Ο υπεύθυνος επεξεργασίαςυποχρεούται να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για τη διασφάλιση της συμμόρφωσης των υπηρεσιών με τον ΓΚΠΔ σύμφωνα με το άρθρο 24. Με τον τρόπο αυτόκαι σε συνδυασμό με άλλους παράγοντες, οι υπεύθυνοι επεξεργασίας οφείλουν να εξετάσουν «την πιθανότητα εμφάνισης του κινδύνου και την σοβαρότητα του για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων». Η διάταξη αυτή μεταφέρει στον υπεύθυνο επεξεργασίας την υποχρέωση, να διαχειρίζεται κατάλληλα τους κινδύνους.

Το άρθρο 26 παράγραφος ορίζει ότι: «Όταν δύο ή περισσότεροι υπεύθυνοιεπεξεργασίας καθορίζουν από κοινού τους σκοπούς και τα μέσα επεξεργασίας, είναι από κοινού υπεύθυνοι. Πρέπει με διαφανή τρόπο να καθορίσουν τις αντίστοιχες ευθύνες τους για τη συμμόρφωση με τις υποχρεώσεις που απορρέουν από τον Κανονισμό». Σύμφωνα με την απαίτηση του άρθρου 26, οι από κοινού υπεύθυνοι πρέπει να καθορίζουν αντίστοιχες υπευθυνότητες τους ως προς την προστασία των δεδομένων, όπως για παράδειγμα να παρέχουν επαρκείς πληροφορίες για την επεξεργασία στα υποκείμενα των δεδομένων, έτσι ώστε να έχουν την δυνατότητα να ασκήσουν τα δικαιώματά τους. Είναι σημαντικό λοιπόν να καθοριστούν οι ρόλοι των προαναφερθέντων οντοτήτων, αφού πολλοί από αυτούς μπορούν να ενεργούν ως από κοινού υπεύθυνοι.

Στην περίπτωση εφαρμογής λύσεων Smart Home είναι πολύ πιθανόν να αναπτυχθεί και να διατηρείται ένα οικοσύστημα δεδομένων στο οποίο συμμετέχουν διαφορετικά μέλη, όπως Εταιρείες που τους ανήκει η εφαρμογή διαχείρισης του Smart Home, πάροχοι Υπηρεσιών Διαδικτύου, τελικοί χρήστες, προγραμματιστές των εφαρμογών, κέντρο υποστήριξης προβλημάτων που μπορούν να προκύψουν στην λειτουργία του και πολλοί άλλοι.

Ιδιαίτερη σημασία έχει μια πρόσφατη απόφαση ορόσημο του Δικαστηρίου της Ευρωπαϊκής Ένωσης (ΔΕΕ), στην οποία ο προγραμματιστής της ιστοσελίδας Fahion ID, ο οποίος ενσωμάτωσε το χαρακτηριστικό κουμπί «Μου αρέσει» στον ιστότοπο της Εταιρίας και προκάλεσε τη μετάδοση των προσωπικών δεδομένων των χρηστών του ιστότοπου, μπορεί να θεωρηθεί από κοινού υπεύθυνος, μαζί με το Facebook, σύμφωνα με τον ΓΚΠΔ. Το ΔΕΕ υιοθέτησε μια ευρεία άποψη για την ερμηνεία της έννοιας της κοινής ευθύνης ως προς τη προστασία των προσωπικών δεδομένων μέσω αυτής της απόφασης.[74]

Για τους προγραμματιστές έξυπνων οικιακών (π.χ. ο αρχιτεκτονικός σχεδιαστής του συστήματος είτε οι συνεργαζόμενοι ή ανεξάρτητοι προγραμματιστές), το διευρυμένο πεδίο εφαρμογής του από κοινού υπεύθυνου επεξεργασίας, σημαίνει ότι μπορεί κάλλιστα να εμπίπτουν στον ορισμό του κοινού υπεύθυνου, καθώς ορίζουν με τεχνικούς όρους πώς συλλέγονται τα δεδομένα από το έξυπνο σπίτι και για ποιους πιθανούς σκοπούς. Στη περίπτωση αυτή, μπορεί να υποστηριχθεί ότι σε ορισμένα τεχνικά μοντέλα όπου οι προγραμματιστές δεν έχουν πρόσβαση στα προσωπικά δεδομένα, δεν μπορεί να θεωρηθούν υπεύθυνοι επεξεργασίας. Ωστόσο, το ΔΕΕ έχει αποφανθεί σε πολλές περιπτώσεις ότι δεν έχει σημασία εάν ένα ενδιαφερόμενο μέρος έχει πραγματική πρόσβαση ή όχι στα δεδομένα όταν πρόκειται να εξακριβωθεί ο υπεύθυνος επεξεργασίας [73] .Το γεγονός αυτό εγείρει μια σειρά ερωτημάτων σχετικά με τον τρόπο άσκησης των δικαιωμάτων των υποκειμένων των δεδομένων έναντι πολλαπλών υπευθύνων επεξεργασίας όταν πολλά από αυτά τα αιτήματα —όπως πρόσβαση, διόρθωση, διαγραφή— μπορούν να εκπληρωθούν μόνο όταν ο υπεύθυνος

---

[73] Wirtschaftsakademie (n 42) para 38; Jehovan todistajat (n 46) para 69; Fashion ID (n 49) para 82.

επεξεργασίας έχει άμεσο ή έμμεσο έλεγχο των προσωπικών δεδομένων. Εξίσου σημαντικές είναι οι επιπτώσεις για τους χρήστες αυτών των τεχνολογιών, οι οποίοι όταν κάνουν χρήση των εφαρμογών διαχείρισης των έξυπνων σπιτιών προσδοκούν αυξημένο επίπεδο ως προς το απόρρητο και την ασφάλεια των δεδομένων των ίδιων, των οικογενειών τους ή ακόμα και των επισκεπτών τους, αλλά καταλήγουν να θεωρούνται από κοινού υπεύθυνοι, καθώς κατά κάποιο τρόπο εφόσον επιλέγουν τις συσκευές που θα τεθούν σε εφαρμογή αποφασίζουν οι ίδιοι για τα προσωπικά δεδομένα τους που θα υποστούν επεξεργασία. Από τεχνική άποψη όμως, υπάρχει ουσιαστική διαφορά μεταξύ της λειτουργίας μιας έξυπνης οικιακής συσκευής που επιτρέπει τη συλλογή δεδομένων και την ενσωμάτωση του κουμπιού «Μου αρέσει» σε έναν ιστότοπο που ενεργοποιεί τη μετάδοση δεδομένων.

Ακόμη και αν διαπιστωθεί ότι ένας κάτοικος έξυπνου σπιτιού ενεργεί ως υπεύθυνος επεξεργασίας των δεδομένων, αποκλειστικά ή από κοινού, δεν συνεπάγεται πάντα ότι τον βαραίνει το φάσμα των υποχρεώσεων του υπευθύνου επεξεργασίας δεδομένων. Στην πραγματικότητα, σύμφωνα με το άρθρο 2 παρ. 2 του ΓΚΠΔ το οποίο περιγράφει το πεδίο εφαρμογής, αναγράφεται ότι ο κανονισμός δεν εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα, από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής δραστηριότητας. Η αιτιολογική σκέψη 18 διευκρινίζει περαιτέρω την έννοια της «αποκλειστικής προσωπικής ή οικιακής δραστηριότητας» με τον χαρακτηρισμό «χωρίς σύνδεση με κάποια επαγγελματική ή εμπορική δραστηριότητα». Στην ίδια αιτιολογική σκέψη δίνονται επίσης ορισμένα παραδείγματα, τα οποία «θα μπορούσαν να περιλαμβάνουν την αλληλογραφία και την κατοχή διευθύνσεων ή την κοινωνική δικτύωση και τη επιγραμμική δραστηριότητα που ασκείται στο πλαίσιο τέτοιων δραστηριοτήτων» . Ωστόσο, στην ίδια αιτιολογική σκέψη περιγράφεται ρητά ότι κανονισμός εφαρμόζεται

σε υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία οι οποίοι παρέχουν τα μέσα επεξεργασίας δεδομένων προσωπικού χαρακτήρα για τέτοιες προσωπικές ή οικιακές δραστηριότητες. Στο πλαίσιο του έξυπνου σπιτιού, είναι απίθανο οι κατασκευαστές των συσκευών ή οι προγραμματιστές του λογισμικού να επωφεληθούν από αυτήν την εξαίρεση. Πρώτον, υπάρχει μια σαφής επαγγελματική ή και εμπορική ανάμειξη (ανεξάρτητα από το καθεστώς μη/κερδοσκοπικού χαρακτήρα τους) που θα απέκλειε τον ισχυρισμό της καθαρά προσωπικής δραστηριότητας. Εξάλλου, πολλοί από τους κατασκευαστές ή προγραμματιστές δεν είναι απλώς φυσικά πρόσωπα, αλλά μάλλον εταιρίες, κάτι που επίσης αποκλείεται σαφώς από την εξαίρεση. Εδώ τίθεται το ερώτημα αν είναι από κοινού υπεύθυνοι ή ποιες είναι οι υπευθυνότητες που έχουν σε αυτή την περίπτωση. Το σίγουρο πάντως είναι ότι δύσκολα μπορούν να αποφύγουν την εφαρμογή του GDPR επικαλούμενοι την απαλλαγή της οικιακής δραστηριότητας.

Σε μια ακόμα απόφαση του ΔΕΕ, που έχει ιδιαίτερη σημασία καθώς αφορά τη χρήση CCTV σε ιδιωτική κατοικία—μιας συσκευής οικιακής ασφάλειας, αν και όχι έξυπνη στη συγκεκριμένη περίπτωση, [74] το Δικαστήριο κλήθηκε να αποφασίσει εάν η λειτουργία ενός κλειστού κυκλώματος τηλεόρασης που είναι εγκατεστημένο στο σπίτι αλλά εν μέρει παρακολουθεί δημόσιο χώρο εμπίπτει στην εξαίρεση του οικιακής δραστηριότητας. Στην απόφαση αυτή, το ΔΕΕ ακολουθεί μια εξαιρετικά αυστηρή προσέγγιση όσον αφορά το πεδίο εφαρμογής της εξαίρεσης, βασιζόμενη σε δύο εκτιμήσεις που καθορίστηκαν σε προηγούμενες υποθέσεις που αποκλείουν τη δυνατότητα εφαρμογής της εξαίρεση της οικιακής χρήσης: την πρόσβαση από απεριόριστο αριθμό ατόμων και την επέκταση σε δημόσιο χώρο πέρα από το ιδιωτικό

[74] Case C-212/13 Rynes [2014] OJ C 46/688

περιβάλλον του ατόμου.[75] Στην υπόθεση Ryneš , παρόλο που το Δικαστήριο έχει επίγνωση ότι η χρήση κλειστού κυκλώματος τηλεόρασης εξυπηρετεί τον σκοπό της προστασίας της οικογένειάς, απορρίπτει τη δυνατότητα εφαρμογής της εξαίρεσης.

Από αυτή την άποψη, το κεντρικό ερώτημα για τη χρήση έξυπνων συσκευών αφορά τον βαθμό στον οποίο η χρήση δεδομένων περιορίζεται στην ιδιωτική σφαίρα του χρήστη και της οικογένειάς του. Σε αντίθεση με την περίπτωση των καμερών, ωστόσο, δεν υπάρχουν σαφή φυσικά όρια, ανάλογα με το ακριβές τεχνικό μοντέλο, το οποίο μπορεί να επιτρέπει την σύνδεση στις συσκευές από άτομα εκτός οικογένειας, είτε σε φυσική εγγύτητα (π.χ γείτονες, επισκέπτες) ή σε απόσταση (π.χ. άλλοι χρήστες που είναι συνδεδεμένοι στην ίδια υπηρεσία). Το γεγονός και μόνο ότι αυτές οι τεχνολογίες περιλαμβάνουν συλλογή προσωπικών δεδομένων εκτός της οικογένειας ή διάδοση προσωπικών δεδομένων εκτός της οικιακής σφαίρας αποκλείει την εφαρμογή της εξαίρεσης της οικιακής δραστηριότητας. Τα παραπάνω δημιουργούν νομική αβεβαιότητα ως προς το ποιος θα πρέπει να αναλάβει την κύρια ευθύνη μεταξύ μιας ομάδας ενδιαφερόμενων μερών στο Smart Home και κατ' επέκταση ποιος θα εξυπηρετήσει τα δικαιώματα των υποκειμένων ή θα εκτελέσει ΕΑΠΔ.

5.3 Μελέτη Περίπτωσης

Σε αυτό το κεφάλαιο θα προσπαθήσουμε να περιγράψουμε τα βήματα που ακολουθούνται στη ΕΑΠΔ. Δεδομένου ότι απαιτείται περαιτέρω έρευνα καθώς και περαιτέρω κατευθυντήριες για την εξακρίβωση των ακριβών ευθυνών των διαφορετικών εμπλεκόμενων μερών ως προς τη προστασία προσωπικών δεδομένων, θα παρουσιάσουμε την πρακτική

---

[75] Jehovan todistajat (n 46) para 42.

εφαρμογή της ΕΑΠΔ με ένα εξαιρετικά απλό παράδειγμα. Δεδομένου ότι οι Εταιρίες οι οποίες υλοποιούν και εμπορεύονται εφαρμογές για την διαχείριση και τον έλεγχο των IoT συσκευών στο Smart Home αποθηκεύουν μεγάλο όγκο προσωπικών δεδομένων τόσο για την εγγραφή όσο και για την χρήση της εφαρμογής, ως Υπεύθυνοι Επεξεργασίας οφείλουν να διενεργούν ΕΑΠΔ. Στο παράδειγμα μας, θα αναφερθούμε στην νεοσύστατη εταιρεία Asmart Α.Ε., η οποία αναπτύσσει εφαρμογές για να προσφέρει στους πελάτες της τον έλεγχο των IoT συσκευών στο Smart Home. Συνεργάζεται με Εταιρία που κατασκευάζει έξυπνες συσκευές και τους προμηθεύει λάμπες, πρίζες, λεντοταινίες, αισθητήρες, ανίχνευσης διαρροής νερού, αισθητήρες ανοίγματος πόρτας και παραθύρου. Η Εταιρία που προμηθεύει τις συσκευές στην Asmart, πρόκειται να λαμβάνει και να αποθηκεύει μια ένδειξη σχετικά με το αν είναι σε λειτουργία η συσκευή της χωρίς δεδομένα που μπορούν άμεσα η έμμεσα να ταυτοποιήσουν το υποκείμενο των δεδομένων. Όλα τα δεδομένα αποθηκεύονται στις υποδομές cloud της Εταιρίας Asmart. Η Εταιρία δεν προβαίνει σε κατάρτιση προφίλ των πελάτων της αλλά ούτε και στέλνει newsletters. Η Asmart συνεργάζεται επίσης με εξωτερική εταιρία για την εξυπηρέτηση των πελατών της, η οποία έχει πρόσβαση στην εφαρμογή διαχείρισης που αποθηκεύονται όλα τα δεδομένα των πελατών της Asmart . Στην κεντρική εφαρμογή που προσφέρει, οι χρήστες κάτω των 18 ετών δεν μπορούν να δημιουργήσουν λογαριασμό για τον έλεγχο των συσκευών. Οι επιμέρους λεπτομέρειες της λύσης που προσφέρει περιγράφονται στο πίνακα που θα δούμε παρακάτω, καθώς μετά τον προσδιορισμό της ανάγκης για διενέργεια ΕΑΠΔ, το δεύτερο βήμα που ακολουθεί είναι η περιγραφή του τρόπου που πρόκειται να χρησιμοποιηθούν τα προσωπικά δεδομένα. Η περιγραφή πρέπει να περιλαμβάνει την υπό εξέταση επεξεργασία, το πεδίο

εφαρμογής της, καθώς και τη καταγραφή των ρόλων που επιτελούν τα εμπλεκόμενα μέρη.

Για την διεκπεραίωση του βήματος αυτού, θα πρέπει να απαντηθούν οι παρακάτω ερωτήσεις σχετικά με την επεξεργασία των προσωπικών δεδομένων μέσα από τη λύση Smart Home:

Πίνακας 9: Γενική Περιγραφή Επεξεργασίας Προσωπικών Δεδομένων

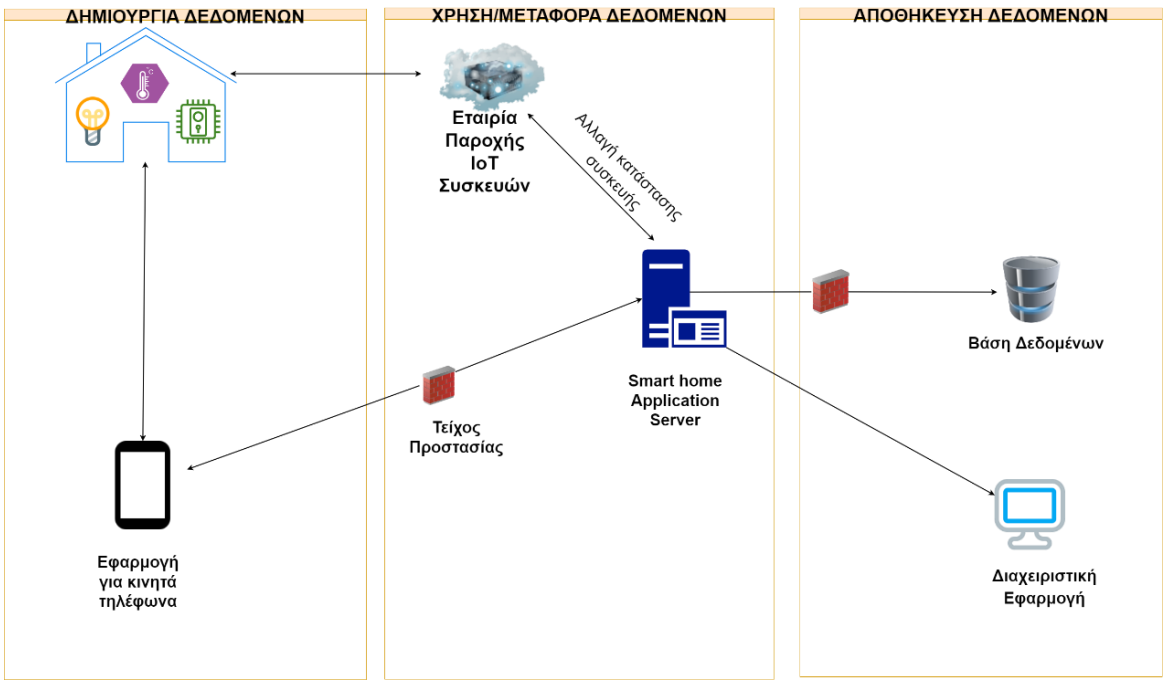
Επισκόπηση	**Επεξήγηση ερώτησης**	**Παράδειγμα Smart Home**
Ποια είναι η υπόεξέταση επεξεργασία;	Περιγραφή της υπό εξέτασης επεξεργασία και ενδεικτικά το σκοπό για τον οποίο διενεργείται, τις ενέργειες που λαμβάνουν χώρα από τις εμπλεκόμενες Διευθύνσεις στοπλαίσιο της εν λόγω επεξεργασίας κλπ.	Επεξεργασία δεδομένων προσωπικού χαρακτήρα που συλλέγονται από την χρήση της mobile εφαρμογής για να πραγματοποιηθεί ο έλεγχος και η χρήση όλων των IoT συσκευών (π.χ. λάμπες, πρίζες, λεντοταινίες, αισθητήρες ανίχνευσης διαρροής νερού, αισθητήρες ανοίγματος πόρτας και παραθύρου) κατά τα πλαίσια συμβατικής σχέσης με το Υποκείμενο των δεδομένων.
Ποιους ρόλους επιτελούν τα εμπλεκόμενα μέρη;	Καταγραφή ποιος είναι ο υπεύθυνος επεξεργασίας, ο εκτελών την επεξεργασία και οαπό κοινού υπεύθυνος επεξεργασίας.	Υπεύθυνος Επεξεργασίας είναι η Asmart A.E.. Εκτελών την Επεξεργασία είναι η Εταιρεία που παρέχει υποστήριξη στους χρήστες της εφαρμογής και έχει πρόσβαση στα δεδομένα του.
Υπάρχουν κώδικες δεοντολογίας ή/και πιστοποιήσεις αναφορικά με τηνπροστασία προσωπικώνδεδομένων;	Καταγραφή των εγκεκριμένων κωδικών δεοντολογίας, καθώς και τις πιστοποιήσεις σχετικά με την προστασία προσωπικών δεδομένων.	Δεν υπάρχουν

Ποια είναι τα προσωπικά δεδομέναπου υποβάλλονται ;	Καταγραφή των δεδομένων που αποτελούν αντικείμενο επεξεργασίας και προσδιορισμός για κάθε ένα από αυτά της προβλεπόμενης περιόδου αποθήκευσής τους.	Μέσω της διαδικασίας εγγραφής στην εφαρμογή, μέσω των ρυθμίσεων του λογαριασμού, συλλέγονται προσωπικά δεδομένα, όπως το ονοματεπώνυμο (username), η διεύθυνση ηλεκτρονικού ταχυδρομείου, το όνομα της τοποθεσίας, τα ονόματα των IoT συσκευών. Κατά την σύνδεση μιας έξυπνης συσκευής (π.χ. αισθητήρα θερμοκρασίας στην εφαρμογή, οι πληροφορίες θερμοκρασίας από αυτόν τον αισθητήρα μαζί με τυχόν πληροφορίες ταυτοποίησης που έχουν επιλεγεί να συσχετιστούν)με αυτόν τον αισθητήρα (π.χ. το όνομα της συσκευής ή/και το όνομα δωματίου/τοποθεσίας που έχει αντιστοιχιστεί στοναισθητήρα). Ο τύπος των πληροφοριών που συλλέγονται από κάθε συσκευή ποικίλλει ανάλογα με τον τύπο της συσκευής.
Ποιοι είναι οι πληροφοριακοίπόροι που εμπλέκονται στηνυπό εξέταση επεξεργασία ;	Καταγραφή των πληροφοριακών πόρων στους οποίους εμπεριέχονται τα παραπάνω προσωπικά δεδομένα στους οποίους έχουν άμεση πρόσβαση οι υπάλληλοι της Εταιρείας που διενεργεί την υπό εξέταση επεξεργασία.	Εφαρμογή Διαχείρισης τωνχρηστών του Smart Home. Εφαρμογή για κινητά τηλέφωνα, Βάση Δεδομένων, IoT συσκευές

5.4 Απεικόνιση Ροής Πληροφορίας

Σκοπός του τρίτου βήματος είναι η απεικόνιση της ροής της πληροφορίας εντός και εκτός της Εταιρίας Asmart. Το διάγραμμα πρέπει να απεικονίζει κατ' ελάχιστον και με συνοπτικό τρόπο τα βασικά στοιχεία των εμπλεκόμενων πόρων (π.χ. τις εμπλεκόμενες εφαρμογές, τα πληροφοριακά συστήματα, τον τρόπο μετάδοσης της πληροφορίας κλπ.), καθώς και τις επιμέρους ενέργειες που λαμβάνουν χώρα από τις εμπλεκόμενες. Στο παρακάτω σχήμα, εμφανίζεται το στάδιο δημιουργίας των δεδομένων, το οποίο περιλαμβάνει τις έξυπνες συσκευές που είναι τοποθετημένες στο σπίτι και την εφαρμογή διαχείρισης των συσκευών στην οποία η σύνδεση πραγματοποιείται με ονομαστικό λογαριασμό. Στο στάδιο μεταφοράς των δεδομένων, ο server ο οποίος φιλοξενεί την εφαρμογή για κινητά τηλέφωνα, λαμβάνει τα δεδομένα και στην συνέχεια μεταφέρει την ένδειξη σχετικά με κατάσταση της συσκευής στην Εταιρία παροχής των έξυπνων συσκευών. Ο server που φιλοξενεί την εφαρμογή αποστέλλει όλα τα δεδομένα στην βάση δεδομένων που φιλοξενείται σε δικτυακές υποδομές της Asmart και στην διαχειριστική εφαρμογή, όπου συνδέεται η Εταιρία που παρέχει υποστήριξη στους πελάτες της Asmart.

Σχήμα 2: Ροή Δεδομένων



5.5 Αξιολόγηση Αναγκαιότητας και Αναλογικότητας

Στο τέταρτο βήμα, πραγματοποιείται ο νομικός έλεγχος της επεξεργασίας. Σκοπός της εξέτασης είναι η αξιολόγηση της συμμόρφωσης της επεξεργασίας με τις βασικές αρχές και τα δικαιώματα των υποκειμένων, που διέπουν τον ΓΚΠΔ, καθ' όλη τη διάρκεια εκτέλεσης της υπό εξέταση επεξεργασίας. Ο βαθμός συμμόρφωσης είναι μη διαπραγματεύσιμος και ως εκ τούτου πρέπει τόσο οι αρχές, όσο και τα δικαιώματα των υποκειμένων να γίνονται απολύτως σεβαστά και να μην υπόκεινται σε καμία μεταβολή, ανεξαρτήτως των όποιων κινδύνων. Περαιτέρω, σε αυτό το βήμα αξιολογείται το επίπεδο συμμόρφωσης της Asmart σε ειδικά ζητήματα, όπως η λήψη της συναίνεσης του υποκειμένου των δεδομένων, η εκτέλεση της υπό εξέταση επεξεργασίας από τρίτο μέρος, καθώς και η διαβίβαση των προσωπικών δεδομένων σε τρίτες χώρες ή διεθνείς οργανισμούς. Για να αξιολογηθεί το επίπεδο συμμόρφωσης της επεξεργασίας με τον Κανονισμό, ο Υπεύθυνος επεξεργασίας πρέπει να τεκμηριώσει τα μέτρα που έχει λάβει για τη διασφάλιση της συμμόρφωσης με τις βασικές αρχές του του ΓΚΠΔ ,σύμφωνα με το άρθρο 5.

Το πρώτο βήμα είναι η καταγραφή της νομικής βάσης που νομιμοποιεί την υπόψη επεξεργασία (π.χ. συναίνεση, εκτέλεση σύμβασης, εκδήλωση ενδιαφέροντος για εκτέλεση σύμβασης, έννομη υποχρέωση, ζωτικό συμφέρον των ατόμων, δημόσιο συμφέρον ή έννομο συμφέρον). Στο smart home η νομική βάση είναι η εκτέλεση σύμβασής της Asmart για τη χρήση της εφαρμογής για τον έλεγχο των συσκευών IoT που η ίδια προμηθεύει, με τον πελάτη για παροχή υπηρεσιών Smart Home. Στην συνέχεια, πραγματοποιείται η καταγραφή του σκοπού και ο έλεγχος ότι είναι καθορισμένος, ειδικός και νόμιμος και αν υποβάλλονται σε περαιτέρω επεξεργασία τα δεδομένα κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς.

Ο σκοπός συλλογής των προσωπικών δεδομένων στο smart home είναι νόμιμος καθώς αποτελεί την εκτέλεση της σύμβασης με τα υποκείμενα

που κάνουν χρήση της υπηρεσίας. Χωρίς την επεξεργασία των προσωπικών δεδομένων δεν θα ήταν δυνατή η χρήση των υπηρεσιών, όπως για παράδειγμα το email, το οποίο επιτρέπει την εγγραφή στην υπηρεσία και την ταυτοποίηση του για λόγους ασφάλειας. Επίσης, δεν υφίσταται περαιτέρω επεξεργασία (π.χ. για αποστολή διαφημιστικών μηνυμάτων ή διαβίβαση τους σε τρίτους) εκτός από τον αρχικό σκοπό που συλλέχθηκαν στα δεδομένα. Σε συνέχεια του άρθρου 5 του ΓΚΠΔ και συγκεκριμένα της αρχής της αναλογικότητας («ελαχιστοποίηση των δεδομένων»), ο Υπεύθυνος επεξεργασίας πρέπει να προβεί σε καταγραφή εάν τα προσωπικά δεδομένα, που συλλέγονται και επεξεργάζονται, είναι τα κατάλληλα κατ' είδος και αριθμό για την επίτευξη του σκοπού της επεξεργασίας. Στην εφαρμογή που παρέχει η Asmart, τα δεδομένα που συλλέγονται είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία. Πιο συγκεκριμένα, η διεύθυνση ηλεκτρονικού ταχυδρομείου που συλλέγεται χρησιμοποιείται για την ταυτοποίηση δύο παραγόντων κατά την αρχική είσοδο στην εφαρμογή. Το ονοματεπώνυμο χρησιμοποιείται ως username για την είσοδο στην εφαρμογή. Τα ονόματα των δωματίων είναι απαραίτητα για την ομαλή διαχείριση της εφαρμογής από το χρήστη καθώς και την υποστήριξη σε περίπτωση βλάβης.

Σύμφωνα με την αρχή της ακρίβειας των δεδομένων, ο Υπεύθυνος Επεξεργασίας πρέπει να προβεί σε καταγραφή των μέτρων που έχουν ληφθεί για τη διασφάλιση της ποιότητας των δεδομένων, την επικαιροποίηση τους, όποτε αυτό απαιτείται, καθώς και την ασφαλή διόρθωση ή διαγραφή τους σε περίπτωση που διαπιστωθεί ότι αυτά είναι ανακριβή. Στο παράδειγμα του smart home, τα δεδομένα που συλλέγονται είναι ακριβή. Αν ο αριθμός τηλεφώνου και το email δεν πιστοποιηθούν ότι είναι σωστά, ο χρήστης δεν μπορεί να ολοκληρώσει την εγγραφή του στην εφαρμογή για κινητά λόγω ότι δεν θα μπορεί να λάβει τον 6ψήφιο κωδικό (ταυτοποίηση δύο παραγόντων). Τα δεδομένα που συλλέγονται από τους αισθητήρες είναι επίσης ακριβή λόγω τις τεχνολογίας που χρησιμοποιήθηκε κατά την κατασκευή τους. Σύμφωνα με την αρχή του

καθορισμού της χρονικής διάρκειας της επεξεργασίας («περιορισμός της περιόδου αποθήκευσης»), πρέπει να οριστεί και να καταγραφεί το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα, καθώς και τα κριτήρια που καθορίζουν το εν λόγω διάστημα. Τα δεδομένα που συλλέγονται για τον πελάτη κατά την εγγραφή και χρήση της εφαρμογής όπως το username,το email και το τηλέφωνο, διατηρούνται για ολόκληρη τη διάρκεια της σύμβασης, δηλαδή μέχρι την στιγμή που ο χρήστης θα διαγράψει τον λογαριασμό του και θα σταματήσει τη χρήση της εφαρμογής καθώς τα δεδομένα αυτά είναι απαραίτητα για την ταυτοποίηση του. Τα δεδομένα από τους αισθητήρες συλλέγονται και διατηρούνται από την Εταιρία για 6 μήνες ώστε οι αλγόριθμοι να μπορέσουν να εκπαιδευτούν για το μοτίβο λειτουργίας των συσκευών και να παραχθούν χρήσιμες αναφορές στο κάτοικο του σπιτιού.

Στην συνέχεια, ο Υπεύθυνος Επεξεργασίας καταγράφει όλα τα μέτρα προστασίας που έχει λάβει για τη διασφάλιση της ικανοποίησης των αιτημάτων των υποκειμένων των δεδομένων, συμπεριλαμβανομένων των πληροφοριών που παρέχονται στο υποκείμενο των δεδομένων αναφορικά με την επεξεργασία των προσωπικών του δεδομένων και το μέσο γνωστοποίησής τους. Η καταγραφή πρέπει να περιλαμβάνει εάν η σχετική ενημέρωση γίνεται σε συνοπτική, κατανοητή και εύκολα προσβάσιμη μορφή. Στο παράδειγμα της Asmart, τα υποκείμενα των δεδομένων, έχουν ενημερωθεί μέσω της αποδοχής της πολιτικής απορρήτου κατά την εγγραφή τους στην εφαρμογή Smart Home. Η πολιτική είναι γραμμένη σε σαφή και απλή γλώσσα, περιλαμβάνει όλες τις απαιτήσεις του Κανονισμού, ενημερώνεται σε κάθε αλλαγή, ζητείται εκ νέου η αποδοχή της και είναι πάντα διαθέσιμη στον χρήση. Κατόπιν, εξετάζεται εάν παρέχεται στο υποκείμενο των δεδομένων η δυνατότητα εξάσκησης των δικαιωμάτων, σύμφωνα με τα άρθρα 15-22 του ΓΚΠΔ, καθώς και για το δικαίωμα ανάκλησης της συγκατάθεσης σύμφωνα με το άρθρο 7. Στο βήμα αυτό, ο Υπεύθυνος Επεξεργασίας καλείται να συμπληρώσει την καταγραφή της διαδικασίας, συμπεριλαμβανομένων

των μέσων, που επιτρέπει τόσο την άσκηση από το υποκείμενο των δεδομένων των εν λόγω δικαιωμάτων του, όσο και την ικανοποίησή τους.

Στο παράδειγμα της υπηρεσίας smart home της Εταιρίας που αναφέραμε, τα υποκείμενα έχουν ενημερωθεί για την εξάσκηση των δικαιωμάτων, σύμφωνα με τα άρθρα 15-22 του ΓΚΠΔ, καθώς και για το δικαίωμα ανάκλησης της συγκατάθεσης, σύμφωνα με το άρθρο 7, μέσα από την Πολιτική Απορρήτου που είναι αναρτημένη στην εφαρμογή για κινητά τηλέφωνα. Μέσα από την Πολιτική ενημερώνονται, ότι μπορούν να επικοινωνήσουν γραπτώς με ταχυδρομική επιστολή στην έδρα της Εταιρείας ή στην ηλεκτρονική διεύθυνση dpo@asmarthome.gr. Μέσα από την Πολιτική οι χρήστες ενημερώνονται, ότι μόλις αποσταλεί κάποιο αίτημα ο DPO θα ελέγξει την εγκυρότητα του αιτήματος και θα ενημερώσει σχετικά το υποκείμενο των δεδομένων σε 14 μέρες με τον τρόπο που έχει επιλέξει από την φόρμα. Εάν εντοπίσει ότι η Εταιρεία μπορεί να ικανοποιήσει το αίτημα και αποφανθεί την εκπλήρωση του, όλα τα αιτήματα μπορούν να ικανοποιηθούν εντός 25 ημερών από την υποβολή τους, με τις βέλτιστες προδιαγραφές ασφάλειας. Αν υφίσταται επεξεργασία που βασίζεται στη Νομική βάση επεξεργασίας της συναίνεσης, εξετάζονται τα μέτρα που διασφαλίζουν ότι η συγκατάθεση του υποκειμένου των δεδομένων, παρέχεται με σαφή θετική ενέργεια, η οποία συνιστά ελεύθερη, συγκεκριμένη, ρητή, εν πλήρη επίγνωσή ένδειξη της συμφωνίας του υπέρ της επεξεργασίας των προσωπικών του δεδομένων και εάν η παροχή της συγκατάθεσης του συνοδεύεται πάντα από το δικαίωμά του να την ανακαλέσει οποτεδήποτε. Στο παράδειγμα μας δεν υπάρχει επεξεργασία που να βασίζεται στην νομική βάση επεξεργασίας της συναίνεσης. Θα υπήρχε αν η εταιρεία επεξεργαζόταν τα δεδομένα που της παρείχε ο χρήστης για διαφημιστικούς λόγους. Τέλος εξετάζονται τα μετρά για τη διασφάλιση της συμμόρφωσης με τον ΓΚΠΔ σε περιπτώσεις ανάθεσης της υπό εξέταση επεξεργασίας σε τρίτο μέρος και διαβίβασης των προσωπικών δεδομένων.

Οι ερωτήσεις που πρέπει να απαντηθούν από τον Υπεύθυνο Επεξεργασίας είναι εάν έχει ανατεθεί η εκτέλεση της υπόψη

επεξεργασίας σε τρίτο μέρος, ενεργό ως εκτελούντα την επεξεργασία και αν υπάρχει σύμβαση με αυτόν που να εμπεριέχονται σε αυτή οι υποχρεώσεις του σύμφωνα με τον ΓΚΠΔ. Στο παράδειγμα μας, η Asmart έχει σύμβαση που αναγράφεται ότι καθ' όλη τη διάρκεια της, ο εκτελών τηρεί τις υποχρεώσεις του ως εκτελούντος την επεξεργασία, όπως απορρέουν από την ισχύουσα νομοθεσία, όπως ενδεικτικά διορίζει πρόσωπα αρμόδια για την προστασία των προσωπικών δεδομένων, τηρεί αρχεία των δραστηριοτήτων επεξεργασίας που τελούν υπό την ευθύνη του, συνεργάζεται με την Αρχή, εγγυάται ότι παρέχει επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων, κατά τρόπο ώστε η επεξεργασία να είναι σύννομη και να διασφαλίζεται η προστασία των δικαιωμάτων των υποκειμένων των δεδομένων και το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων. Σε περίπτωση που υπάρχει διαβίβαση των δεδομένων σε χώρα εκτός Ε.Ε., εξετάζεται εάν διασφαλίζεται το επίπεδο προστασίας των υποκειμένων, των οποίων τα προσωπικά δεδομένα επεξεργάζονται ή προορίζονται να υποβληθούν σε επεξεργασία αφού διαβιβαστούν σε τρίτη χώρα κι αν ναι, με ποιόν τρόπο. Στη μελέτη περίπτωσης που παρουσιάζεται, δεν υπάρχει διαβίβαση ΓΚΠΔ σε τρίτη χώρα. Αν υπήρχε θα πρέπει να πληρούνται τα κριτήρια σύμφωνα με το άρθρο 44 του ΓΚΠΔ.

5.6 Προσδιορισμός Υφιστάμενων Μέτρων Προστασίας

Στο πέμπτο βήμα επεξεργασίας γίνεται η καταγραφή των τεχνικών και οργανωτικών μέτρων προστασίας δεδομένων. Σκοπός είναι η καταγραφή όλων των μέτρων, που η Asmart έχει υιοθετήσει ή επρόκειτο να υιοθετήσει για την προστασία και την ασφάλεια των προσωπικών δεδομένων. Στο παρακάτω πίνακα παρουσιάζονται τα μέτρα προστασίας:

Πίνακας 11: Μέτρα Προστασίας Smart Home

Μέτρο Προστασίας Δεδομένων	**Είδος**	**Περιγραφή**
Προστασία βάσης δεδομένων	**Λογικό μέτρο ασφάλειας**	• Αυθεντικοποίηση με χρήση κωδικού πρόσβασης στη βάση δεδομένων • Ενεργοποιημένο τείχος προστασίας, • Υποχρεωτική επιβολή πολύπλοκου κωδικού (μέγεθος, σύμβολο) • Υπάρχουν διακριτοί ρόλοι για κάθεχρήστη, Αυξημένα δικαιώματα εκτέλεσης ερωτημάτων στη βάση έχουν μόνο δύο χρήστες.
Ελαχιστοποίησητων δεδομένων	**Οργανωτικό μέτρο**	Έχει πραγματοποιηθεί η διαγραφή περιττών δεδομένων πριν από την εγκατάσταση και εφαρμογή των συστημάτων IoT.
Προστασία δεδομένων ήδη απότο σχεδιασμό και εξ' ορισμού	**Οργανωτικό μέτρο**	Η ομάδα ασφάλειας πληροφοριακών συστημάτων έχει συμμετάσχει από την αρχήτου έργου και έχουν ενσωματωθεί όλες οι απαιτήσεις ασφάλειας.
Προστασία της εφαρμογής διαχείρισης των πελατών/χρηστών	**Λογικό μέτρο ασφάλειας**	• Ενεργοποίηση των αρχείων καταγραφής ελέγχου (audit logs) • Ελάχιστοι διαχειριστές στην εφαρμογή • Ζητείται εξαψήφιος κωδικός από το τελικό χρήστη πριν ο διαχειριστής αποκτήσει πρόσβαση στα δεδομένα του • Χρόνος λήξης συνεδρίας (1 ώρα) • Πολυπλοκότητα κωδικού πρόσβασης • Πραγματοποίηση δοκιμής παρείσφρησης (penetration test) πριν ξεκινήσει η παραγωγική

		λειτουργία της εφαρμογής και διόρθωση των ευρημάτων.
Ενέργειες συμμόρφωσης	**Οργανωτικό μέτρο**	• Υπάρχει καταγεγραμμένη και διαθέσιμη πολιτική προστασίας των δεδομένων στην εφαρμογή • Έχουν εντοπιστεί όλοι οι εκτελούντες την επεξεργασία και έχουν υπογράψει σύμφωνο προστασίας ως προς τα προσωπικά δεδομένα
Μέτρα προστασίαςως προς την διαθεσιμότητα	**Λογικό μέτρο**	Λαμβάνονται καθημερινά αντίγραφα ασφαλείας (back up) σε όλη την υποδομή
Προστασία εφαρμογής για κινητά τηλέφωνα	**Λογικό μέτρο**	• Χρόνος λήξης συνεδρίας (1 ώρα) • Πολύπλοκος κωδικός πρόσβασης • Δοκιμή παρείσφρησής πριν την παραγωγική λειτουργία της εφαρμογής, • Υλοποίηση/Προγραμματισμός της εφαρμογής με βάση πρότυπα ασφάλειας (OWASP - Open Web Application Security Project)

5.7 Αξιολόγηση Κινδύνων

Στο έκτο βήμα πραγματοποιείται η αξιολόγηση των κινδύνων που πιθανώς προκύψουν για τα υποκείμενα των δεδομένων από την υπό εξέταση επεξεργασία, λαμβάνοντας υπόψη τα μέτρα που εφαρμόζονται για την προστασία των προσωπικών τους δεδομένων. Πρόκειται επί της ουσίας για υποθετικά σενάρια, σύμφωνα με τα οποία, μια πηγή απειλής θα μπορούσε να εκμεταλλευτεί τις ευπάθειες των πληροφοριακών πόρων και να οδηγήσει σε κίνδυνο των υποκειμένων των δεδομένων. Για την ανάλυση των κινδύνων, ακολουθείται η ποιοτική τους ανάλυση, η οποία αναφέρεται στο παραπάνω κεφάλαιο.

Μερικοί από τους κινδύνους που εξετάζονται στην ΕΑΠΔ, είναι:

1. Έλλειψη συμμόρφωσης με τις βασικές αρχές του ΓΚΠΔ: όταν τα προσωπικά δεδομένατυγχάνουν επεξεργασίας με τρόπο που αντιβαίνει τις βασικές αρχές που διέπουν τονΓΚΠΔ.
2. Διαβιβάσεις εκτός Ευρωπαϊκής Ένωσης, άνευ επάρκειας και κατάλληλων εγγυήσεων: όταν ο οργανισμός διαβιβάζει προσωπικά δεδομένα προς τρίτη χώρα ή διεθνή οργανισμό χωρίς να υπάρχει απόφαση επάρκειας της Ευρωπαϊκής Επιτροπής ή χωρίς να παρέχονται από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία κατάλληλες εγγυήσεις.
3. Επεξεργασία από αναξιόπιστα τρίτα μέρη: όταν ο εκτελών την επεξεργασία, ή οι υπεργολάβοι, επεξεργάζονται προσωπικά δεδομένα με τρόπο που αντιβαίνει τις οικείες διατάξεις του ΓΚΠΔ.
4. Διακύβευση των δικαιωμάτων και των ελευθεριών των υποκειμένων: όταν η επεξεργασία ενδέχεται να θέσει σε κίνδυνο τα θεμελιώδη δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων.

5. Παράνομη πρόσβαση ή αποκάλυψη προσωπικών δεδομένων: όταν τα προσωπικά δεδομένα αποκαλύπτονται ή ενδέχεται να αποκαλυφθούν σε μη εξουσιοδοτημένα άτομα.

6. Ανεπιθύμητη τροποποίηση προσωπικών δεδομένων: Όταν τα προσωπικά δεδομένα τροποποιούνται, αφαιρούνται ή προστίθενται από μη εξουσιοδοτημένα άτομα.
7. Μη διαθεσιμότητα των προσωπικών δεδομένων: όταν τα προσωπικά δεδομένα δεν είναι στη διάθεση των χρηστών.

Στην συνέχεια συνεκτιμώνται οι απειλές, δηλαδή ενέργειες οι οποίες ενδέχεται να θέσουν σε κίνδυνο μία ή περισσότερες λειτουργίες των πληροφοριακών συστημάτων που περιέχουν προσωπικά δεδομένα, για τον προσδιορισμό του επιπέδου του ρίσκου. Παραδείγματα απειλών είναι:

1) Έλλειψη συμμόρφωσης με τις βασικές αρχές του ΓΚΠΔ υφίστανται όταν ενδεικτικά:

    - Η συναίνεση του υποκειμένου δεν λαμβάνεται με τον προβλεπόμενο από τονΓΚΠΔ τρόπο.
    - Ο επιπλέον σκοπός επεξεργασίας των προσωπικών δεδομένων δεν είναισυμβατός με τον αρχικό σκοπό συλλογής τους.
    - Τα προσωπικά δεδομένα αποθηκεύονται για μεγαλύτερο χρονικό διάστημααπό το προβλεπόμενο.
    - Η επεξεργασία των προσωπικών δεδομένων δεν είναι σύννομη.

2) Διαβιβάσεις εκτός Ευρωπαϊκής Ένωσης άνευ επάρκειας και κατάλληλων εγγυήσεων’υφίσταται όταν ενδεικτικά:
    - Ο Υπεύθυνος Προστασίας Δεδομένων, δεν έχει λάβει υπόψη του τις αποφάσεις της Επιτροπής σχετικά με

την επάρκεια προστασίας της χώρας όπου πρόκειται να διαβιβάσει προσωπικά δεδομένα.

3) Επεξεργασία από αναξιόπιστα τρίτα μέρη υφίσταται όταν ενδεικτικά:

- Ο εκτελών την επεξεργασία δεν εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την ασφάλεια των προσωπικών δεδομένων.
- Η σύμβαση με τον εκτελούντα την επεξεργασία δεν είναι έγγραφη και δεν εμπεριέχει τις κατ' ελάχιστον υποχρεώσεις που αναλαμβάνει βάσει του ΓΚΠΔ.
- Πρόσληψη υπεργολάβου για την επεξεργασία των προσωπικών δεδομένων, χωρίς προηγούμενη ειδική ή γενική γραπτή άδεια του υπεύθυνου επεξεργασίας.
- Έλλειψη μηχανισμών και διαδικασιών αξιολόγησης κινδύνων των τρίτων μερών που δρουν ως εκτελούντες την επεξεργασία.

4) Διακύβευση των δικαιωμάτων και των ελευθεριών του υποκειμένου υφίσταται όταν ενδεικτικά:

- Απουσιάζουν οι διαδικασίες για την άσκηση και ικανοποίηση των δικαιωμάτων του υποκειμένου των δεδομένων, που απορρέουν από τον ΓΚΠΔ
- Απουσιάζουν οι διαδικασίες για την άσκηση και ικανοποίηση των θεμελιωδών δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων, όπως ελευθερία του λόγου, ελευθερία της κίνησης, δικαίωμα στην ελευθερία και στην ασφάλεια, δικαίωμα στην ελευθερία της σκέψης, συνείδησης και θρησκείας, δικαίωμα ίσης μεταχείρισης.

5) Παράνομη πρόσβαση ή αποκάλυψη προσωπικών δεδομένων υφίσταται όταν ενδεικτικά:

- Γίνεται χρήση φορητών μέσων αποθήκευσης με τρόπο ο οποίος ενδέχεται να είναι επιβλαβής για τα προσωπικά δεδομένα.
- Υπάρχουν ευπάθειες στα πληροφοριακά σύστημα, όπως ασθενής μηχανισμοί αυθεντικοποίησης, έλλειψη συστήματος διαβάθμισης και διανομής δεδομένων, έλλειψη συστήματος διαχείρισης των συνθηματικών, έλλειψη συστήματος καταγραφής γεγονότων, έλλειψη τεκμηριωμένων ρόλων και διακριτών καθηκόντων, έλλειψη τεκμηρίωσης των μηχανισμών προστασίας των δικτυακών μέσων.

6) Ανεπιθύμητη τροποποίηση των δεδομένων υφίσταται όταν ενδεικτικά:

- Δεν γίνεται ανάκληση, όποτε απαιτείται, των δικαιωμάτων πρόσβασης των χρηστών στις εφαρμογές και στα συστήματα.
- Πραγματοποιείται τροποποίηση των προσωπικών δεδομένων που περιέχονται σε ένα έγγραφο.

7) Μη διαθεσιμότητα των προσωπικών δεδομένων υφίσταται όταν ενδεικτικά:

- Υπάρχει έλλειψη συστήματος υψηλής διαθεσιμότητας, έλλειψη σχεδίου ανάκαμψης από καταστροφή.
- Αποσπάται λόγω κλοπής το επαγγελματικό κινητό τηλέφωνο ή φορητός υπολογιστής από κάποιον επιτήδειο.

Οι πηγές απειλών, αποτελούνται από οτιδήποτε μπορεί να οδηγήσει, εκούσια ή ακούσια, σε κίνδυνο για το υποκείμενο των δεδομένων, όπως για παράδειγμα:

- Άνθρωποι εντός οργανισμού : εργαζόμενοι, δανειζόμενο προσωπικό κ.λπ.
- Άνθρωποι εκτός οργανισμού: αποδέκτες προσωπικών δεδομένων, πάροχοι υπηρεσιών, hackers, επισκέπτες, πρώην εργαζόμενοι, ακτιβιστές, ανταγωνιστές, πελάτες, προσωπικό συντήρησης, συνδικαλιστικές οργανώσεις, δημοσιογράφοι, μη κυβερνητικές οργανώσεις, εγκληματικές/ τρομοκρατικές οργανώσεις κ.λπ.
- Μη – ανθρώπινες πηγές: Κακόβουλος κώδικας, εύφλεκτα υλικά, φυσικές καταστροφές κ.λπ.

Στην συνέχεια, εκτιμάται η πιθανότητα πραγμάτωσης της απειλής, η οποία θα οδηγήσει σε κίνδυνο, συνυπολογίζοντας τα μέτρα προστασίας που πιθανόν έχουν ληφθεί. Σε περίπτωση που συντρέχουν περισσότερες από μία απειλές, καταγράφεται μόνο εκείνη που ενέχει τη μεγαλύτερη πιθανότητα πραγμάτωσης. Η πιθανότητα αποτελεί το ενδεχόμενο εκδήλωσης του κινδύνου, το οποίο εξαρτάται από τις ευπάθειες των πληροφοριακών πόρων, καθώς και από την ικανότητα της πηγής της απειλής να τις εκμεταλλευτεί.

Τα επίπεδα πιθανότητα που χρησιμοποιούνται είναι:

- Αμελητέα: Η πραγμάτωση του κινδύνου από την πηγή της απειλής εκτιμάται απίθανη (π.χ. κλοπή φυσικών εγγράφων αποθηκευμένα σε δωμάτιο προστατευμένο από αναγνωριστικό εισόδου και κωδικό πρόσβασης).
- Περιορισμένη: Η πραγμάτωση του κινδύνου από την πηγή της απειλής εκτιμάται δύσκολη, αλλά όχι απίθανη (π.χ. κλοπή έγχαρτων εγγράφων αποθηκευμένα σε δωμάτιο προστατευμένο μόνο από αναγνωριστικό εισόδου).
- Σημαντική: Η πραγμάτωση του κινδύνου από την πηγή της απειλής εκτιμάται αρκετά πιθανή (π.χ. κλοπή έγχαρτων εγγράφων αποθηκευμένα σε γραφεία που δεν είναι

προσβάσιμα χωρίς να έχει προηγηθεί φυσικός έλεγχος στην υποδοχή τουκτιρίου).

- Μέγιστη: Η πραγμάτωση του κινδύνου από την πηγή της απειλής εκτιμάται εξαιρετικά πιθανή (π.χ. κλοπή έγχαρτων εγγράφων που είναι αποθηκευμένα σε δημόσιο χώρο, χωρίς καμία δικλείδα ασφαλείας).

Ακολουθεί η εκτίμηση της σοβαρότητας που ενδεχομένως έχει η επίπτωση του κινδύνου,συνυπολογίζοντας τα μέτρα προστασίας που πιθανόν να έχουν ληφθεί. Σε περίπτωση που συντρέχουν περισσότερες από μία επιπτώσεις, καταγράφεται μόνο η σοβαρότερη εξ αυτών. Η σοβαρότητα επίπτωσης κινδύνου εξαρτάται από τη βλάβη (π.χ. σωματική, ψυχική, κοινωνική, οικονομική κ.λπ.), που μπορεί να προκληθεί στο υποκείμενο των δεδομένων. Το επίπεδο σοβαρότητας του κινδύνου κατηγοριοποιείται σε :

- Αμελητέα: Όταν το υποκείμενο των δεδομένων δεν επηρεάζεται από τις επιπτώσεις του κινδύνου ή οι δυσκολίες που ενδέχεται να αντιμετωπίσει μπορούν εύκολα να ξεπεραστούν. Ενδεικτικά: παροδική αναστάτωση, χάσιμο χρόνου λόγω έλλειψης διαδικασίας, λήψη αυθαίρετης ηλεκτρονικής αλληλογραφίας, μικροενόχληση του υποκειμένου των δεδομένων λόγω επαναλαμβανόμενης παροχής πληροφοριών, φόβος ότι θα χαθούν τα προσωπικά δεδομένα.
- Περιορισμένη: Όταν το υποκείμενο των δεδομένων δύναται να αντιμετωπίσει προβλήματα που εύκολα όμως ξεπερνιούνται. Ενδεικτικά: άγχος λόγω εκτεταμένης αναμονής ικανοποίησης αιτήματος, απόγνωση λόγω έλλειψης κατανόησης, λήψη εσφαλμένων προστίμων, άρνηση παροχής υπηρεσιών, λήψη στοχευμένης ηλεκτρονικής αλληλογραφίας, μπλοκάρισμα λογαριασμού διαδικτυακώνυπηρεσιών.

- Σημαντική: Όταν το υποκείμενο των δεδομένων μπορεί να αντιμετωπίσει μεγάλα προβλήματα που δύσκολα ξεπερνιούνται. Ενδεικτικά: σοβαρές σωματικές βλάβες, κατάθλιψη, φοβίες, υπεξαίρεση χρημάτων, άρνηση χορήγησης δανείου, απώλεια εργασίας, απώλεια σημαντικών χρηματικών ποσών, δυσφήμιση του υποκειμένου, εκφοβισμός (bullying).
- Μέγιστη: Όταν το υποκείμενο των δεδομένων ενδέχεται να αντιμετωπίσει ανεπανόρθωτη βλάβη. Ενδεικτικά: μακροχρόνιες ή μόνιμες σωματικές βλάβες, ψυχιατρικής φύσεως ασθένειες, θάνατος, πτώχευση, αδυναμία εργασίας λόγω δυσφήμισης, απώλεια αποδεικτικών στοιχείων στο πλαίσιο δικαστικών υποθέσεων, αδυναμία πρόσβασης σε παροχές κοινής ωφέλειας, καταδίκη σε φυλάκιση.

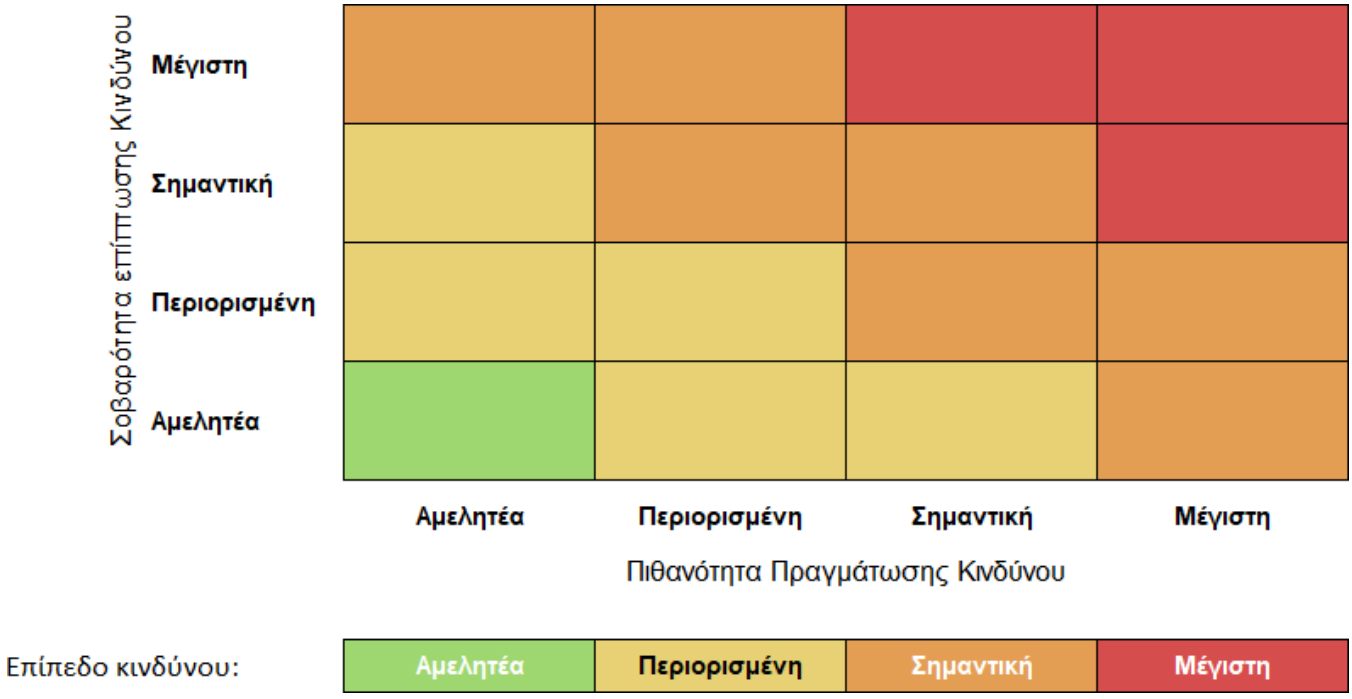
Στο τελευταίο βήμα υπολογίζεται το επίπεδο του κινδύνου για το υποκείμενο τωνδεδομένων, το οποίο εξαρτάται από το βαθμό απειλής των δικαιωμάτων και των ελευθεριώντου, αποτελώντας συνάρτηση του επιπέδου της σοβαρότητας της επίπτωσης του εκτιμώμενου κινδύνου με το επίπεδο της πιθανότητας πραγμάτωσης του. Ο ακόλουθος πίνακας απεικονίζει τη διαβάθμιση του κινδύνου για το υποκείμενο των δεδομένων, η οποία αποτελεί συνάρτηση του επιπέδου της σοβαρότητας της επίπτωσης του εκτιμώμενου κινδύνου με το επίπεδο της πιθανότητας πραγμάτωσής του. Αναλυτικότερα, το επίπεδο του κινδύνου υπολογίζεται επί τη βάση:

- της σοβαρότητάς του, η οποία αντικατοπτρίζει το μέγεθος της επίπτωσης του κινδύνου για το υποκείμενο των δεδομένων και εξαρτάται από τις πιθανές βλάβες που μπορεί να προκληθούν στο υποκείμενο, ήτοι σωματικές, υλικές ή άυλες. Σε περίπτωση δε που ένας κίνδυνος ενδέχεται να επιφέρει περισσότερες από μία επιπτώσεις για το υποκείμενο, τότε το συνολικό επίπεδο της

σοβαρότητάς του θα ισούται με το επίπεδο της επίπτωσης που επιφέρει τις σοβαρότερες βλάβες στο υποκείμενο.

- της πιθανότητάς του, η οποία αντικατοπτρίζει τη δυνατότητα πραγμάτωσης του εκτιμώμενου κινδύνου και εξαρτάται από τη πιθανότητα πραγματοποίησης της απειλής που μπορεί να οδηγήσει στον εν λόγω κίνδυνο.

Σχήμα 3: Υπολογισμός κινδύνου



Πίνακας 12: Αξιολόγηση Κινδύνων Προστασίας Δεδομένων Smart Home

Κίνδυνος για τα υποκείμενα των δεδομένων	**Περιγραφή απειλών/ ευπαθειών**	**Πληροφοριακό Σύστημα**	**Μέτρα προστασίας**	**Πιθανότητα**	**Σοβαρότητα επίπτωσης κινδύνου**	**Επίπεδο κινδύνου**
Παράνομη πρόσβαση ή αποκάλυψη προσωπικών δεδομένων	Έλλειψη κρυπτογράφησης και ανωνυμοποίησης	Βάση Δεδομένων	1.Ενεργοποιημένο τείχος προστασίας, 2.Υποχρεωτική επιβολή πολύπλοκου κωδικού (μέγεθος, σύμβολο) 3.Υπάρχουν διακριτοί ρόλοι για κάθε χρήστη. 4.Δικαιώματα εκτέλεσης ερωτημάτων στη βάση έχουν μόνο δύο χρήστες.	**Περιορισμένη**	**Σημαντική**	**Σημαντικό**
Παράνομη πρόσβαση ή αποκάλυψη προσωπικών δεδομένων	Η εφαρμογή διαχείρισης είναι ελεύθερα προσβάσιμη από το διαδίκτυο	Εφαρμογή διαχείρισης των πελατών/χρηστών	Κεφάλαιο 7.5.1	**Περιορισμένη**	**Περιορισμένη**	**Περιορισμένο**
Έλλειψη συμμόρφωσης με τις βασικές αρχές του ΓΚΠΔ	Δεν μπορεί να επιβεβαιωθεί ότι η επεξεργασία που πραγματοποιείται στα προσωπικά δεδομένα, μόνο στον βαθμό που είναι κατάλληλα και συναφή με τους παραπάνω σκοπούς, περιορίζοντας την ταυτόχρονα στο αναγκαίο για τους σκοπούς αυτούς μέτρο.	N/A	Κεφάλαιο 7.5.1	**Αμελητέα**	**Αμελητέα**	**Αμελητέο**

Επεξεργασία από αναξιόπιστα τρίτα μέρη	Απουσία επαρκών εγγυήσεων για την προστασία των προσωπικών δεδομένων από τους εκτελών την επεξεργασία.	N/A	Κεφάλαιο 7.5.1	**Αμελητέα**	**Αμελητέα**	**Αμελητέο**
Έλλειψη συμμόρφωσης με τις βασικές αρχές του ΓΚΠΔ	Τα προσωπικά δεδομένα αποθηκεύονται για μεγαλύτερο χρονικό διάστημα από τον προβλεπόμενο σε περίπτωση που έχει διαφύγει η υπογραφή κάποιου σύμφωνου προστασίας προσωπικών δεδομένων από εξωτερικό συνεργάτη.	N/A	Κεφάλαιο 7.5.1	**Αμελητέα**	**Αμελητέα**	**Αμελητέο**
Έλλειψη συμμόρφωσης με τις βασικές αρχές του ΓΚΠΔ	Αποτυχία εξυπηρέτησης των δικαιωμάτων των υποκειμένων.	N/A	Κεφάλαιο 7.5.1	**Αμελητέα**	**Αμελητέα**	**Αμελητέο**

5.8 Σχέδιο Δράσης

Στο έβδομο βήμα, για να αντιμετωπιστούν οι κίνδυνοι που διαπιστώθηκαν προηγουμένως, πρέπει τα μέτρα αντιμετώπισης να είναι προγραμματισμένα με λεπτομέρεια και ακρίβεια. Επιπλέον, στις προτάσεις παρέχεται η δυνατότητα καταγραφής τυχόν προτάσεων του Υπεύθυνου Προστασίας Δεδομένων επί του εν λόγω σχεδίου δράσης, καθώς και τυχόν απόψεων των υποκείμενων των δεδομένων ή των εκπροσώπων τους.

Πίνακας 13: Προτεινόμενα μέτρα προστασίας στο Smart Home

Κίνδυνος	**Επίπεδο κινδύνου**	**Τρόπος αντιμετώπισης κινδύνου**	**Μέτρα αντιμετώπισης**	**Επίπεδο κινδύνου μετά τη λήψη μέτρων**	**Υπεύθυνος διασφάλισης αντιμετώπισης κινδύνου**	**Γνώμη των εμπλεκόμενων μερών (όπου υφίστανται)**	**Πρόταση DPO**
Ασφάλεια Βάσεων Δεδομένων	**Περιορισμένη**	Μετριασμός κινδύνου	Κρυπτογράφηση της Βάσης	**Αμελητέα**			
Ασφάλεια Δεδομένων - Εφαρμογή διαχείρισης	**Περιορισμένη**	Μετριασμός κινδύνου	Ενεργοποίηση της επαλήθευσης σε 2 βήματα (2FA) για τους διαχειριστές	**Αμελητέα**			
Έλλειψη συμμόρφωσης με τις βασικές αρχές του ΓΚΠΔ	**Αμελητέα**	Διατήρηση κινδύνου	Δεν χρειάζεται να ληφθούν επιπλέον μέτρα	**Αμελητέα**			
Επεξεργασία από αναξιόπιστα τρίτα μέρη	**Αμελητέα**	Διατήρηση κινδύνου	Δεν χρειάζεται να ληφθούν επιπλέον μέτρα	**Αμελητέα**			
Διατήρηση δεδομένων επιπλέον χρονικό διάστημα	**Αμελητέα**	Διατήρηση κινδύνου	Δεν χρειάζεται να ληφθούν επιπλέον μέτρα	**Αμελητέα**			

6. ΕΠΙΛΟΓΟΣ

Στις μέρες μας, η αποδοχή, εισαγωγή, υιοθέτηση και εφαρμογή πληροφοριακών συστημάτων αποτελεί πρώτιστο μέλημα της πολιτείας. Κανείς δεν μπορεί να αρνηθεί ότι η τεχνολογία αναπτύσσεται με ρυθμούς που είναι δύσκολο να γίνουν αντιληπτοί από τον μέσο άνθρωπο. Οι ηλεκτρονικές συσκευές, αλλά και οι εφαρμογές του IoT, διαδραματίζουν πλέον ουσιαστικό ρόλο καθώς διευκολύνουν με πολλαπλούς τρόπους την καθημερινότητα μας. Μια σημαντική καινοτομία είναι το έξυπνο σπίτι, το οποίο παρέχει ευκολία, χάρη στους αισθητήρες που σου επιτρέπουν να ελέγχεις την κατοικία σου, οπουδήποτε στο κόσμο και αν βρίσκεσαι. Επίσης, επιτυγχάνεται ασφάλεια και ηρεμία, καθώς με την χρήση καμερών μπορείς να γνωρίζεις ανά πάσα στιγμή ποιος μπαίνεις και ποιος βγαίνει αλλά και να κλειδώσεις απομακρυσμένα την πόρτα του σπιτιού σου σε περίπτωση που μείνει ανοικτή. Για την ορθή λειτουργία αλλά και την αυτοματοποίηση του Smart Home, υφίσταται επεξεργασία μεγάλου όγκου δεδομένων, όπου η διαρροή του μπορεί να επιφέρει σοβαρά ζητήματα ιδιωτικότητας.

Η ασφάλεια των δεδομένων που αποθηκεύονται, τα οποία τις περισσότερες φορές είναι αυστηρά προσωπικά (π.χ. το υλικό από τις κάμερες παρακολούθησης), είναι άμεσα συνδεδεμένη και απαραίτητη προϋπόθεση για την επίτευξη της ιδιωτικότητας. Η εξασφάλιση της όμως αποτελεί δύσκολο έργο, καθώς τις περισσότερες φορές υπάρχουν ευπάθειες τόσο στις συσκευές IoT (Internet of Things), όσο και στο λογισμικό και στις βάσειςπου τα δεδομένα αυτά φιλοξενούνται.

Σε περίπτωση πιθανής διαρροής των δεδομένων, οι άνθρωποι και το κοινωνικό σύνολο γενικότερα, αισθάνεται φόβο και σταματά να εμπιστεύεται τα υπολογιστικά συστήματα καθώς και τους διαχειριστές του. Αρκετές φορές έχουν δημοσιευθεί άρθρα που αναφέρουν ότι οι έξυπνες συσκευές που κυκλοφορούν στο εμπόριο καταγράφουν συνομιλίες ή ακόμα και ότι μας φωτογραφίζουν και μας βιντεοσκοπούν, με αποδέκτη όλωναυτών των δεδομένων την κυβέρνηση.

Για την υιοθέτηση μέτρων που θα εξαλείψουν το κίνδυνο διαρροής, είναι απαραίτητηη εις βάθος κατανόηση του εννοιολογικού πλαισίου του κινδύνου αλλά και ο προσδιορισμόςόλων των κινδύνων. Ο κίνδυνος αναγνωρίζεται μέσω των συνεπειών που έχει, δηλαδή των απωλειών που προκαλεί. Στο πέρασμα των χρόνων, έχουν αναπτυχθεί πολλές μεθοδολογίες και πρότυπα τα οποία υποστηρίζουν την ορθή αξιολόγηση των

κινδύνων ασφάλειας. Αν και η αναγνώριση και διαχείριση των κινδύνων, αποτελεί αναπόσπαστο μέρος του σχεδίου διαχείρισης και επίτευξης της ασφάλειας, η ουσιαστική εφαρμογή των μεθοδολογιών είναι περιορισμένη.

Η ανάγκη για εκτίμηση των κινδύνων έχει κατοχυρωθεί πλέον και ως νομική υποχρέωση μέσω της ΕΑΠΔ του ΓΚΠΔ, για τις διεργασίες που ενδέχεται να επιφέρουν στα υποκείμενα των δεδομένων μεγάλο κίνδυνο. Η ΕΑΠΔ περιλαμβάνει μια όσο το δυνατόν πιοαναλυτική και συστηματική περιγραφή των πράξεων επεξεργασίας και σκοπών που προβλέπονται και που επιδιώκει ο Υπεύθυνος Επεξεργασίας, την εκτίμηση της αναγκαιότητας και της αναλογικότητας της σκοπούμενης πράξης επεξεργασίας, τον προσδιορισμό των κινδύνων και το πλάνο αντιμετώπισης τους. Για τον προσδιορισμό των κινδύνων, τα πρότυπα και οι μεθοδολογίες διαχείρισης κινδύνων στην ασφάλεια μπορούν να φανούν πολύ χρήσιμα. Τα βήματα που προτείνονται, για παράδειγμα από το Πλαίσιο Διαχείρισης Κινδύνων για Πληροφοριακά Συστήματα NIST, είναι: η προετοιμασία, η κατηγοριοποίηση κινδύνων, η επιλογή τρωτών σημείων και υφιστάμενων μέτρων προστασίας, η εκτίμηση πιθανότητας και αντικτύπου, η παρακολούθηση και η συνεχής διαχείριση όλων των ευρημάτων, στοιχείαπου πρέπει να εξετάζονται και στη ΕΑΠΔ.

Η ΕΑΠΔ όπως και οι μεθοδολογίες αξιολόγησης κινδύνων στα πληροφοριακά συστήματα δεν πρέπει να αποτελούν μια εφάπαξ δραστηριότητα, αλλά μια διαρκής διαδικασία όπου ακόμη και τα παραδοτέα δεν είναι εντελώς τελικά, καθώς όσο διαρκεί το έργο θα πρέπει να υπάρχει συνεχής παρακολούθηση και ενημέρωσή τους. Τα κριτήρια για μια αποδεκτή ΕΑΠΔ, που προβλέπονται στο τέλος των κατευθυντήριων γραμμών του άρθρου 29, οφείλουν να εξετάζονται σε όλα τα βήματα της διαδικασίας διαχείρισης κινδύνου, καθώς το επίπεδο μεταβάλλεται ως αποτέλεσμα αλλαγών σε ένα έργο. Αξίζει να σημειωθεί ότι το πιο πρόσφατο Πλαίσιο Διαχείρισης Κινδύνων για Πληροφοριακά Συστήματα NIST, μπορεί να χρησιμοποιηθεί με ευκολία από ειδικούς ασφάλειας συστημάτων που γνωρίζουν τον ΓΚΠΔ, προκειμένου να διενεργήσουν τη ΕΑΠΔ και να προτείνουν μέτρα ως προς την ιδιωτικότητα και ασφάλεια, που θα συνάδουν με τις αρχές και τις απαιτήσεις του ΓΚΠΔ. Ως συμπέρασμα, η υιοθέτηση κατάλληλων μέτρων και διαδικασιών, ήδη από τον σχεδιασμό των έξυπνων σπιτιών, είναι πλέον επιτακτική ανάγκη για την εξασφάλιση δικαιοσύνης, εμπιστευτικότητας, εγκυρότητας, διαθεσιμότητας και αξιοπιστίας στα δεδομένα που συλλέγονται.

Ωστόσο είναι πολύ δύσκολο, αν όχι αδύνατο, να δηλώσουμε με βεβαιότητα ότι μία μεθοδολογία ή ένα πλαίσιο είναι ιδανικό για τη διεξαγωγή ΕΑΠΔ. Καταρχάς, δεν παρέχεται απευθείας από τις αρχές της ΕΕ καμία μέθοδος, ούτε έχει αναγνωριστεί επίσημα από σχετικές πιστοποιήσεις. Δεύτερον, οι αρχές της ΕΕ τείνουν να είναι ουδέτερες όχι μόνο ως προς τα τεχνολογικά μέτρα, αλλά και ως προς τις λειτουργικές λύσεις που μπορούν να χρησιμοποιηθούν για τη συμμόρφωση με το ΓΚΠΔ. Ακόμα όμως και να υπήρχε ένας ένα ιδανικό πλαίσιο για τη διεξαγωγή της ΕΑΠΔ για το Smart Home, τα διαφορετικά εμπλεκόμενα μέρη έχουν δημιουργήσει νομική αβεβαιότητα ως προς το ποιος θα πρέπει να αναλάβει την κύρια ευθύνη της προστασίας των δεδομένων και θα εκτελέσει την εκτίμηση, καθώς και πώς μπορεί να επιτευχθεί η λογοδοσία με συντονισμένο και κοινό τρόπο.

Το ζήτημα της υπευθυνότητας ως προς τα δεδομένα που επεξεργάζονται κατά τη λειτουργία του Smart Home, υπερβαίνει την απλή ερμηνεία του κανονισμού. Απαιτείται περαιτέρω έρευνα για τον εντοπισμό των ενεργειών και των διαφόρων μέτρων προστασίας που πρέπει να υιοθετηθούν από διαφορετικούς φορείς. Ιδανικά, θα πρέπει να αναπτυχθεί ένα αναλυτικό πλαίσιο για τον εντοπισμό των ενδιαφερομένων μερών σύμφωνα με την ρόλο που έχουν στη διασφάλιση της συλλογικής λογοδοσίας. Για να πραγματοποιηθεί αυτό, απαιτούνται περαιτέρω μελέτες για την καλύτερη κατανόηση της σχέσης μεταξύ των φορέων που συνδράμουν στην υλοποίηση και την ομαλή λειτουργία συσκευών και εφαρμογών Smart Home , καθώς και για τις αντιλήψεις του κοινού για το τι ισοδυναμεί με δίκαιη ανάθεση ευθύνης και λογοδοσίας στο Smart Home.

Όλοι οι παραπάνω προβληματισμοί, εάν διερευνηθούν και μεταφραστούν σωστά με την βοήθεια επαγγελματιών από διάφορους κλάδους όπως μηχανικούς υπολογιστών, επαγγελματίας ασφάλειας δεδομένων, νομικών θα συνεισφέρουν ουσιαστικά τόσο τον σχεδιασμό μελλοντικών συστημάτων Smart Home όσο και τη δημιουργία του ευρύτερου ρυθμιστικού πλαισίου για την υποστήριξη νέων τεχνολογιών. Εν κατακλείδι, οι αρχές δεν πρέπει να εφησυχάζουν και να σταματούν στις διατυπώσεις διατάξεων που απαιτούν την εκτίμηση των κινδύνων, αλλά συνεχώς να ελέγχουν σχολαστικά την εφαρμογή των διατάξεων και όπου χρειαστεί να δημοσιεύουν κατευθυντήριες. Τέλος, στην περίπτωση που βρεθούν αποκλίσεις, οι κυρώσεις που θα επιβληθούν θα πρέπει να είναι αυστηρές και άμεσες.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman,A., Invernizzi, L. and Kallitsis, M. (2017). Understanding the Mirai Botnet. [online] 26th USENIX Security Symposium. Available athttps://www.usenix.org/system/files/conference/usenixsecurity17/sec17- antonakakis.pdf.

Du, J. and Chao, S. (2010). A study of information security for M2M of IOT. 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE). [online] Available at: https://www.infona.pl/resource/bwmeta1.element.ieee-art-000005579563

Gao, Y., Peng, Y., Xie, F., Zhao, W., Wang, D., Han, X., Lu, T. and Li, Z. (2013). Analysis of security threats and vulnerability for cyber-physical systems. Proceedings of 2013 3rd International Conference on Computer Science and Network Technology.

Cárdenas, A.A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., & Sastry, S. (2009). Challenges for Securing Cyber Physical Systems.

Sébastien Ziegler (2019). Internet of Things security and data protection. Cham Springer.

Sicari, S., Rizzardi, A., Grieco, L.A. and Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, [online] 76, pp.146–164. Available at: http://tarjomefa.com/wp-content/uploads/2016/07/5009-English.pdf.

Vormayr, G., Zseby, T. and Fabini, J. (2017). Botnet Communication Patterns. IEEE Communications Surveys & Tutorials, [online] 19(4), pp.2768–2796. Available at:https://publik.tuwien.ac.at/files/publik_262720.pdf.

Liu, J. and Yang, L. (2011). Application of Internet of Things in the Community Security Management. 2011 Third International Conference on Computational Intelligence, Communication Systems and Networks.

Du, J. and Chao, S. (2010). A study of information security for M2M of IOT. 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE). [online] Available at: https://www.infona.pl/resource/bwmeta1.element.ieee-art-000005579563.

Ishaq, I., Carels, D., Teklemariam, G., Hoebeke, J., Abeele, F., Poorter, E., Moerman, I. and Demeester, P. (2013). IETF Standardization in the Field of the Internet of Things (IoT): A Survey. Journal of Sensor and Actuator Networks, [online] 2(2), pp.235–287. Available at: https://cyberleninka.org/article/n/907388.pdf

Arias, O., Wurm, J., Hoang, K. and Jin, Y. (2015). Privacy and Security in Internet of Things and WearableDevices. IEEE Transactions on Multi-Scale Computing Systems, 1(2), pp.99–109.

Odlyzko, A. (2003). Privacy, economics, and price discrimination on the Internet. Proceedings of the 5thinternational conference on Electronic commerce - ICEC '03.

Datenauswertung bei Orbitz: Apple-User zahlen mehr für Hotelzimmer. (2012). Der Spiegel. [online] 26Jun. Available at: http://bit.ly/MRBTwT

Orgill, G.L., Romney, G.W., Bailey, M.G. and Orgill, P.M. (2004). The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. Proceedings of the 5th conference on Information technology education - CITC5 '04.

Spiekermann, S. and Cranor, L.F. (2009). Engineering Privacy. IEEE Transactions on Software Engineering,[online] 35(1), pp.67–82. Available at: https://ieeexplore.ieee.org/document/4657365

Social networks scan for sexual predators, with uneven results. (2012). Reuters. [online] 12 Jul. Available at: https://www.reuters.com/article/oukin-uk-usa-internet-predators-idUKBRE86B05M20120712

Voelcker, J. (2006). Stalked by satellite - an alarming rise in GPS-enabled harassment. IEEE Spectrum, 43(7),pp.15–16.

Chow, C.-Y. and Mokbel, M.F. (2009). Privacy in location-based services. SIGSPATIAL Special, 1(2), pp.23–27.

Senior, A.W., Brown, L., Hampapur, A., Shu, C.-F. ., Zhai, Y., Feris, R.S., Tian, Y.-L. ., Borger, S. and Carlson, C. (2007). Video analytics for retail. [online] IEEEXplore. Available at: https://ieeexplore.ieee.org/abstract/document/4425348?casa_token=VZTX-HMA4hoAAAAA:QSpg0f09iBXdTODHJMMfSBxSOK9cZie78zbI--6lM5V87IA9IttthtXZrjkfCuedULiFWlbfH

Xiaoming Liu, Krahnstoever, N., Ting Yu and Tu, P. (2007). What are customers looking at? 2007 IEEEConference on Advanced Video and Signal Based Surveillance.

Fischer-Hübner, S., Duquenoy, P., Hansen, M., Leenes, R. and Zhang, G. eds., (2011). Privacy and IdentityManagement for Life. IFIP Advances in Information and Communication Technology. Berlin, Heidelberg:Springer Berlin Heidelberg.

Toch, E., Wang, Y. and Cranor, L.F. (2012). Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems. User Modeling and User-Adapted Interaction, 22(1-2), pp.203–220.

Ovidiu Vermesan and Friess, P. (2013). Internet of Things : converging technologies for smart environments and integrated ecosystems. Aalborg Denmark: River Publishers. Copyright.

Ιγγλεζάκης, Ι. (2004). Ευαίσθητα Προσωπικά Δεδομένα. Αθήνα: Σάκκουλα.

Καλαφατούδης, Σ., Δροσίτης, Ι. & Λοίλιας, Χ. (2012). Εισαγωγή στις Τεχνολογίες Πληροφορίας και Επικοινωνίας. Αθήνα: Νέες Τεχνολογίες.

Κανελλοπούλου – Μπότη, Μ. (2004). Νομική Προστασία Βάσεων Δεδομένων. Αθήνα: Νομική Βιβλιοθήκη.

Λαμπρινουδάκης, Κ., Μήτρου, Λ., Γκρίτσαλης, Σ. & Κάτσικας, Σ. (2009). Προστασία της Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών: Τεχνικά και Νομικά Θέματα. Αθήνα: Παπασωτηρίου.

Λαζακίδου, Α. (2009). Προηγμένα Συστήματα και Υπηρεσίες Πληροφορικής στο Χώρο της Υγείας.Αθήνα: Λαζακίδου.

Φερενίκη Παναγοπούλου- Κουτνατζή, "Διαδίκτυο των πραγμάτων (Internet of Things-IoT):Αποικισμός της καθημερινής ζωής1 ή νέα τεχνολογική πρόκληση;", ΔΙΜΕ 3/2014 – Έτος 11ο