Τι είναι το IoT; Όλα όσα πρέπει να γνωρίζετε για το Διαδίκτυο των πραγμάτων

Συνέχεια απ το 1ο μέρος:

Τι είναι το Industrial Internet of Things;

Το Industrial Internet of Things (IIoT) ή η τέταρτη βιομηχανική επανάσταση ή το Industry 4.0 είναι όλα, ονόματα που δίνονται στη χρήση της τεχνολογίας IoT σε ένα επιχειρηματικό περιβάλλον. Η ιδέα είναι η ίδια όπως για τις καταναλωτικές συσκευές IoT στο σπίτι, αλλά σε αυτήν την περίπτωση ο στόχος είναι να χρησιμοποιηθεί ένας συνδυασμός αισθητήρων, ασύρματων δικτύων, μεγάλων δεδομένων, τεχνητής νοημοσύνης και αναλυτικών στοιχείων για τη μέτρηση και τη βελτιστοποίηση των βιομηχανικών διαδικασιών.

Εάν εισαχθεί σε μια ολόκληρη αλυσίδα εφοδιασμού και όχι μόνο σε μεμονωμένες εταιρείες, ο αντίκτυπος θα μπορούσε να είναι ακόμη μεγαλύτερος με την έγκαιρη παράδοση των υλικών και τη διαχείριση της παραγωγής από την αρχή μέχρι το τέλος. Η αύξηση της παραγωγικότητας του εργατικού δυναμικού ή η εξοικονόμηση κόστους είναι δύο πιθανοί στόχοι, αλλά το IIoT μπορεί επίσης να δημιουργήσει νέες ροές εσόδων για τις επιχειρήσεις. Οι κατασκευαστές μπορούν επίσης να πουλήσουν μια προγνωστική συντήρηση του κινητήρα, αντί να πουλήσουν απλώς ένα αυτόνομο προϊόν – για παράδειγμα, όπως έναν κινητήρα.

Ποια είναι τα οφέλη του Διαδικτύου των Πραγμάτων για τους καταναλωτές;

Το IoT υπόσχεται να κάνει το περιβάλλον μας -- τα σπίτια, τα γραφεία και τα οχήματά μας -- πιο έξυπνο, πιο μετρήσιμο και... πιο φλύαρο. Τα έξυπνα ηχεία όπως το Echo της Amazon και το Google Home διευκολύνουν την αναπαραγωγή μουσικής, τη ρύθμιση χρονοδιακόπτη ή τη λήψη πληροφοριών. Τα συστήματα οικιακής ασφάλειας διευκολύνουν την παρακολούθηση του τι συμβαίνει μέσα και έξω ή την προβολή και τη συζήτηση με τους επισκέπτες. Εν τω μεταξύ, οι έξυπνοι θερμοστάτες μπορούν να μας βοηθήσουν να θερμάνουμε τα σπίτια μας πριν φτάσουμε πίσω, και οι έξυπνοι λαμπτήρες μπορούν να κάνουν να φαίνεται σαν να είμαστε σπίτι ακόμα και όταν είμαστε έξω.

Κοιτάζοντας πέρα από το σπίτι, οι αισθητήρες μπορούν να μας βοηθήσουν να καταλάβουμε πόσο θορυβώδες ή μολυσμένο μπορεί να είναι το περιβάλλον μας. Τα αυτόνομα αυτοκίνητα και οι έξυπνες πόλεις θα μπορούσαν να αλλάξουν τον τρόπο με τον οποίο κατασκευάζουμε και διαχειριζόμαστε τους δημόσιους χώρους μας.

Ωστόσο, πολλές από αυτές τις καινοτομίες θα μπορούσαν να έχουν σημαντικές επιπτώσεις στο προσωπικό μας απόρρητο .

Το Διαδίκτυο των Πραγμάτων και τα έξυπνα σπίτια

Για τους καταναλωτές, το έξυπνο σπίτι είναι πιθανώς το σημείο όπου είναι πιθανό να έρθουν σε επαφή με πράγματα που υποστηρίζουν το Διαδίκτυο και είναι ένας τομέας όπου οι μεγάλες εταιρείες τεχνολογίας (ιδίως η Amazon, η Google και η Apple) ανταγωνίζονται σκληρά.

Τα πιο προφανή από αυτά είναι τα έξυπνα ηχεία όπως το Echo της Amazon, αλλά υπάρχουν επίσης έξυπνα βύσματα, λαμπτήρες, κάμερες, θερμοστάτες και το πολυσυζητημένο έξυπνο ψυγείο . Αλλά εκτός από το να επιδεικνύετε τον ενθουσιασμό σας για λαμπερά νέα gadget, υπάρχει και μια πιο σοβαρή πλευρά στις εφαρμογές έξυπνου σπιτιού. Μπορούν να βοηθήσουν τους ηλικιωμένους να διατηρηθούν ανεξάρτητοι, διευκολύνοντας την οικογένεια και τους φροντιστές να επικοινωνούν μαζί τους και να παρακολουθούν πώς τα πάνε. Η καλύτερη κατανόηση του τρόπου λειτουργίας των σπιτιών μας και η δυνατότητα προσαρμογής αυτών των ρυθμίσεων θα μπορούσε να βοηθήσει στην εξοικονόμηση ενέργειας -- μειώνοντας , για παράδειγμα, το κόστος θέρμανσης .

Τι γίνεται με την ασφάλεια στο Internet of Things;

Η ασφάλεια είναι ένα από τα μεγαλύτερα προβλήματα με το IoT. Αυτοί οι αισθητήρες συλλέγουν σε πολλές περιπτώσεις εξαιρετικά ευαίσθητα δεδομένα -- τι λέτε και τι κάνετε στο σπίτι σας , για παράδειγμα. Η διατήρηση αυτής της ασφάλειας είναι ζωτικής σημασίας για την εμπιστοσύνη των καταναλωτών, αλλά μέχρι στιγμής το ιστορικό ασφάλειας του IoT ήταν εξαιρετικά φτωχό. Πάρα πολλές συσκευές IoT δίνουν ελάχιστη σκέψη στα βασικά στοιχεία της ασφάλειας, όπως η κρυπτογράφηση δεδομένων κατά τη μεταφορά και την ηρεμία.

Τα ελαττώματα στο λογισμικό -- ακόμη και παλιός και καλά χρησιμοποιημένος κώδικας -- ανακαλύπτονται σε τακτική βάση, αλλά πολλές συσκευές IoT δεν έχουν τη δυνατότητα να διορθωθούν, πράγμα που σημαίνει ότι βρίσκονται σε μόνιμο κίνδυνο. Οι χάκερ στοχεύουν πλέον ενεργά συσκευές IoT, όπως δρομολογητές και κάμερες ιστού, επειδή η εγγενής έλλειψη ασφάλειας τους καθιστά εύκολο να παραβιαστούν και να συγκεντρωθούν σε γιγάντια botnet .

Τα ελαττώματα έχουν αφήσει ανοιχτές στους χάκερ έξυπνες οικιακές συσκευές, όπως ψυγεία, φούρνους και πλυντήρια πιάτων. Οι ερευνητές βρήκαν 100.000 κάμερες ιστού που θα μπορούσαν να παραβιαστούν

εύκολα , ενώ ορισμένα έξυπνα ρολόγια για παιδιά συνδεδεμένα στο Διαδίκτυο έχουν βρεθεί ότι περιέχουν ευπάθειες ασφαλείας που επιτρέπουν στους χάκερ να παρακολουθούν την τοποθεσία του χρήστη, να κρυφακούουν συνομιλίες ή ακόμα και να επικοινωνούν με τον χρήστη.

Οι κυβερνήσεις ανησυχούν όλο και περισσότερο για τους κινδύνους εδώ. Η κυβέρνηση του Ηνωμένου Βασιλείου δημοσίευσε τις δικές της οδηγίες σχετικά με την ασφάλεια των καταναλωτικών συσκευών IoT . Αναμένει ότι οι συσκευές θα έχουν μοναδικούς κωδικούς πρόσβασης, ότι οι εταιρείες θα παρέχουν ένα δημόσιο σημείο επαφής, ώστε ο καθένας να μπορεί να αναφέρει μια ευπάθεια (και ότι θα ληφθούν μέτρα) και ότι οι κατασκευαστές θα αναφέρουν ρητά πόσο καιρό οι συσκευές θα λαμβάνουν ενημερώσεις ασφαλείας. Είναι μια μικρή λίστα, αλλά μια αρχή.

Όταν το κόστος κατασκευής έξυπνων αντικειμένων γίνει αμελητέο, αυτά τα προβλήματα θα γίνουν πιο διαδεδομένα και δυσεπίλυτα.

Όλα αυτά ισχύουν και για τις επιχειρήσεις, αλλά το διακύβευμα είναι ακόμη μεγαλύτερο. Η σύνδεση βιομηχανικών μηχανημάτων σε δίκτυα IoT αυξάνει τον πιθανό κίνδυνο να ανακαλύψουν και να επιτεθούν οι χάκερ σε αυτές τις συσκευές. Η βιομηχανική κατασκοπεία ή μια καταστροφική επίθεση σε υποδομές ζωτικής σημασίας είναι και οι δύο πιθανοί κίνδυνοι. Αυτό σημαίνει ότι οι επιχειρήσεις θα πρέπει να βεβαιωθούν ότι αυτά τα δίκτυα είναι απομονωμένα και προστατευμένα, ενώ η κρυπτογράφηση δεδομένων με ασφάλεια αισθητήρων, πυλών και άλλων στοιχείων είναι απαραίτητη. Η τρέχουσα κατάσταση της τεχνολογίας IoT καθιστά δυσκολότερη τη διασφάλιση, ωστόσο, όπως και η έλλειψη συνεπούς σχεδιασμού ασφάλειας IoT μεταξύ των οργανισμών. Αυτό είναι πολύ ανησυχητικό αν λάβουμε υπόψη την τεκμηριωμένη προθυμία των χάκερ να παραβιάσουν βιομηχανικά συστήματα που έχουν συνδεθεί στο διαδίκτυο αλλά έχουν μείνει απροστάτευτα .

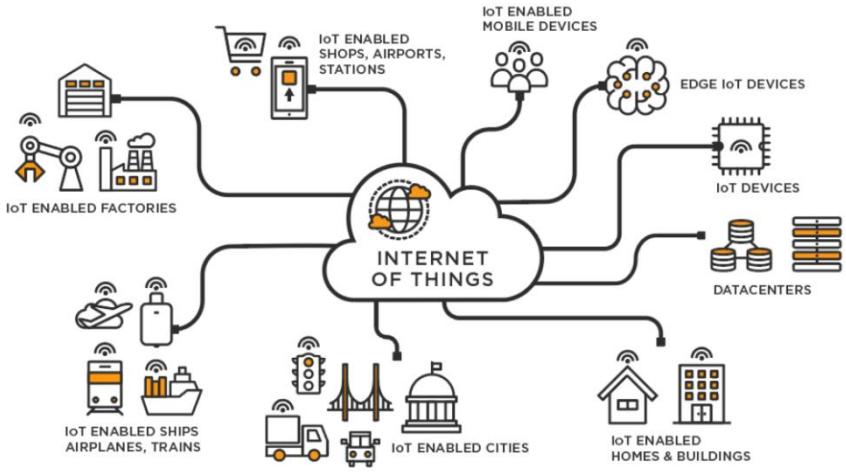
Το IoT γεφυρώνει το χάσμα μεταξύ του ψηφιακού κόσμου και του φυσικού κόσμου, πράγμα που σημαίνει ότι η εισβολή σε συσκευές μπορεί να έχει επικίνδυνες συνέπειες στον πραγματικό κόσμο. Η παραβίαση των αισθητήρων που ελέγχουν τη θερμοκρασία σε ένα σταθμό παραγωγής ενέργειας θα μπορούσε να ξεγελάσει τους χειριστές ώστε να λάβουν μια καταστροφική απόφαση. Ο έλεγχος ενός αυτοκινήτου χωρίς οδηγό θα μπορούσε επίσης να καταλήξει σε καταστροφή.

Τι γίνεται με το απόρρητο και το Διαδίκτυο των πραγμάτων;

Με όλους αυτούς τους αισθητήρες που συλλέγουν δεδομένα για οτιδήποτε κάνετε, το IoT είναι ένας δυνητικά τεράστιος πονοκέφαλος απορρήτου και ασφάλειας. Πάρτε το έξυπνο σπίτι: μπορεί να πει πότε ξυπνάτε (πότε ενεργοποιείται η έξυπνη καφετιέρα) και πόσο καλά βουρτσίζετε τα δόντια σας (χάρη στην έξυπνη οδοντόβουρτσά σας), ποιον ραδιοφωνικό σταθμό ακούτε (χάρη στο έξυπνο ηχείο σας) τι είδους φαγητό τρώτε (χάρη στον έξυπνο φούρνο ή το ψυγείο σας), τι σκέφτονται τα παιδιά σας (χάρη στα έξυπνα παιχνίδια τους) και ποιος σας επισκέπτεται και

περνά από το σπίτι σας (χάρη στο έξυπνο κουδούνι της πόρτας σας). Ενώ οι εταιρείες θα κερδίσουν χρήματα από την πώληση του έξυπνου αντικειμένου εξαρχής, το επιχειρηματικό τους μοντέλο IoT πιθανότατα περιλαμβάνει την πώληση τουλάχιστον μερικών από αυτά τα δεδομένα.

Το τι συμβαίνει με αυτά τα δεδομένα είναι ένα ζωτικής σημασίας ζήτημα απορρήτου. Δεν χτίζουν όλες οι εταιρείες έξυπνων κατοικιών το επιχειρηματικό τους μοντέλο γύρω από τη συγκομιδή και την πώληση των δεδομένων σας, αλλά ορισμένες το κάνουν.



Και αξίζει να θυμάστε ότι τα δεδομένα IoT μπορούν να συνδυαστούν με άλλα κομμάτια δεδομένων για να δημιουργήσουν μια εκπληκτικά λεπτομερή εικόνα σας. Είναι εκπληκτικά εύκολο να μάθετε πολλά για ένα άτομο από μερικές διαφορετικές μετρήσεις αισθητήρων. Σε ένα έργο, ένας ερευνητής διαπίστωσε ότι αναλύοντας δεδομένα που απεικονίζουν μόνο την κατανάλωση ενέργειας του σπιτιού, τα επίπεδα μονοξειδίου του άνθρακα και διοξειδίου του άνθρακα, τη θερμοκρασία και την υγρασία κατά τη διάρκεια της ημέρας, μπορούσαν να καταλάβουν τι έτρωγε κάποιος για δείπνο.

IoT, ιδιωτικότητα και επιχειρήσεις

Οι καταναλωτές πρέπει να κατανοήσουν την ανταλλαγή που πραγματοποιούν και αν είναι ευχαριστημένοι με αυτό. Μερικά από τα ίδια ζητήματα ισχύουν και για τις επιχειρήσεις: η διευθυντική ομάδα σας θα ήταν πρόθυμη να συζητήσει μια συγχώνευση σε μια αίθουσα συσκέψεων εξοπλισμένη με έξυπνα ηχεία και κάμερες, για παράδειγμα; Μια πρόσφατη έρευνα διαπίστωσε ότι τέσσερις στις πέντε εταιρείες δεν θα μπορούσαν να αναγνωρίσουν όλες τις συσκευές IoT στο δίκτυό τους.

Τα προϊόντα IoT με κακή εγκατάσταση θα μπορούσαν εύκολα να ανοίξουν τα εταιρικά δίκτυα σε επιθέσεις από χάκερ ή απλώς να διαρρεύσουν δεδομένα. Μπορεί να φαίνεται σαν μια ασήμαντη απειλή, αλλά φανταστείτε εάν οι έξυπνες κλειδαριές στο γραφείο σας αρνούνταν να ανοίξουν ένα πρωί ή ο έξυπνος μετεωρολογικός σταθμός στο γραφείο του Διευθύνοντος Συμβούλου χρησιμοποιήθηκε από χάκερ για να δημιουργήσουν μια κερκόπορτα στο δίκτυό σας.

Σωτήρης Σιαμανδούρας , Τομεάρχης τομέα Ηλεκτρολόγων και Ηλεκτρονικών ΕΚ Λιβαδειάς. Νοέμβρης 2021.

Πηγές – Πληροφορίες :

1. zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/
2. collettsystems.com/
3. inductiveautomation.com/resources/article/what-is-iiot
4. athenarc.gr/el/news/viomihaniko-diadiktyo-ton-pragmaton-iiot-kai-eyfyi-perivallonta-stin-ekdilosi-toy-invis
5. softwaretestinghelp.com/iot-devices/

Συνέχεια στο επόμενο (3ο μέρος) :