ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΕΝΙΣΧΥΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΥΠΟΔΟΜΩΝ ΖΩΤΙΚΗΣ ΣΗΜΑΣΙΑΣ (ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ) ΜΕ ΤΗ ΒΟΗΘΕΙΑ IOT ΣΥΣΚΕΥΩΝ ΠΟΥ ΠΑΡΑΓΟΥΝ BIGDATA ΔΕΔΟΜΕΝΑ

Διπλωματική Εργασία

του

Σπανίδη Θεόφιλου

Θεσσαλονίκη, Φεβρουάριος 2020

ΕΝΙΣΧΥΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΥΠΟΔΟΜΩΝ ΖΩΤΙΚΗΣ ΣΗΜΑΣΙΑΣ (ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ) ΜΕ ΤΗ ΒΟΗΘΕΙΑ IOT ΣΥΣΚΕΥΩΝ ΠΟΥ ΠΑΡΑΓΟΥΝ BIGDATA ΔΕΔΟΜΕΝΑ

Σπανίδης Θεόφιλος

Πτυχίο πληροφορικής, ΕΑΠ, 2016

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΗΝ ΕΦΑΡΜΟΣΜΕΝΗ ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων καθηγητής:
Ψάννης Κωνσταντίνος

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την

Ψάννης Κωνσταντίνος	Ξυνόγαλος Στυλιανός	Κολωνιάρη Γεωργία
.....	.....	.....

Σπανίδης Θεόφιλος

.....

Περίληψη

Αρκετές εταιρίες , από διάφορους τομείς Κρίσιμων Υποδομών (ΚΥ) έχουν πέσει θύματα περιστατικών ασφαλείας από κυβερνοεπιθέσεις. Οι δομές αυτές εξαρτώνται όλο και περισσότερο από Τεχνολογίες Πληροφορικής και Επικοινωνιών (ΤΠΕ) (ο οποίος αναγνωρίζεται επίσης ως ΚΥ σε πολλές αναφορές). Η αλληλεξάρτησητων διαφόρων ΚΥ με τον τομέα των ΤΠΕ είναι κάτι που χρειάζονται όλοι οι τομείς για να εξελιχθούν και να αναπτυχθούν σε μια αγορά με παγκόσμιο χαρακτήρα. Πρέπει λοιπόν να δοθεί ιδιαίτερη προσοχή στις υπηρεσίες που χρησιμοποιούνται για την επικοινωνία και την ανταλλαγή δεδομένων μέσω δημόσιων / ιδιωτικών και άλλων δικτύων.

Η παρούσα αναφορά παρέχει πληροφορίες σχετικά με διάφορα περιβάλλοντα Κρίσιμων Υποδομών (ΚΥ) ανάλογα με τις ανάγκες τους και τι πιστεύει η κοινότητα τους ότι πρέπει να προστατευθεί από διαδικτυακές επιθέσεις κι όχι μόνο (εσωτερικές, εξωτερικές, φυσικές). Η εργασία αυτή θα προσπαθήσει να παράσχει μια επισκόπηση κάποιων γνωστών ΚΥ και των αναγκών που σχετίζονται με την ασφάλεια.

Οι επόμενες ενότητες της εργασίας θα παρέχουν πληροφορίες σχετικά με τις συσκευές IoT και πώς μπορούν να χρησιμοποιηθούν για την ενίσχυση της ασφάλειας αυτών των υποδομών. Είναι γνωστό ότι η ευρεία χρήση συσκευώνIoT, μπορεί να δημιουργήσει τεράστιο όγκο δεδομένων προς ανάλυση, οπότε στην εργασία θα συμπεριλάβουμε επίσης πληροφορίες που σχετίζονται με BigDataκαι πως μπορεί να γίνει καλύτερη επεξεργασία κι ανάλυση αυτών των δεδομένων για να βελτιωθεί η ακρίβεια των ευρημάτων και να γίνει κατάλληλη χρήση για να μετριαστούν οι επιθέσεις κι οι πιθανές καταστροφές.

Στη τελευταία ενότητα, θα περιγράψουμε μια ενδεικτική εφαρμογή για το πώς μια απλή χρήση συσκευών IoT μπορεί να ενισχύσει την ασφάλεια των Κρίσιμων Υποδομών.

Abstract

Various companies (from various CI domains) have been victims of such Cyber security issues. The CI domains are more and more relying on the ICT domain (which is also identified as a CI domain in many reports). Their interdependence with the ICT domain is something that all sectors need in order to evolve and grow in a market which goes global. So special care should be provided to services used for communication and data exchange via public/private and other networks.

This report provides information about various Critical Infrastructure (CI) environments according to their needs and what their community thinks should be protected against any type of attacks (internal, external, physical). The current report will try to provide an overview of example CIs and their security related needs.

Next sections will provide information about IoT devices and how they can be used to strengthen the security of such infrastructures. It is well-known that IoT devices when spread can provide an enormous amount of data to analyze, thus we will also provide some Big Data related insights and how data can be better processed/analyzed to improve the accuracy of the findings and direct to the appropriate security mitigations and activities.

Last but not least we will provide a proof of concept example on how a simple implementation with IoT devices can strengthen the security of Critical Infrastructures across all CI domains.

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

<u>Κεφάλαιο 1</u>: Δομές ζωτικής σημασίας (Ευρωπαϊκή Ένωση)

Τα τελευταία χρόνια πολλές Ευρωπαϊκές χώρες έχουν δημοσιεύσει αναφορές με στοχο να αναγνωρίσουν τις δομές ζωτικής σημασίας τους (CI) και να ορίσουν πως θα αντιμετωπίσουν πιθανούς κινδύνους Κυβερνοασφάλειας. Πολλά μέλη της Ευρωπαϊκής Ένωσης έχουν δημοσιεύσει αντίστοιχες αναφορές για Κρίσιμες Υποδομές. Στις επόμενους παραγράφους , θα παρουσιάσουμε μια λίστα δομών (ΚΥ) ζωτικής σημασίας ανά Ευρωπαϊκή χώρα, αποτυπώνοντας έτσι τις διαφορετικές δομές ζωτικής σημασίας που υπάρχουν στις χώρες της Ε.Ε.

Σύμφωνα με το σχετικό έγγραφο του ENISA, ορισμένες χώρες όπως η Αυστρία, η Κύπρος, η Τσεχία καθώς και κάποιες άλλες, έχουν συντάξει σχετικές αναφορές κι έχουν αναγνωρίσει τις δομές ζωτικής σημασίας τους. Οι υποενότητες που ακολουθούν περιλαμβάνουν τις δομές ζωτικής σημασίας για κάποιες χώρες της Ε.Ε. (με βάση τις αναφορές τόσο από την αναφορά του ENISA όσο κι από άλλες πηγές.)

Γαλλία – Δομές Ζωτικής Σημασίας

Η παρακάτω λίστα παρουσιάζει τις δομές ζωτικής σημασίας που είναι πιο σημαντικές για τη Γαλλία. Αυτές οι δομές αναφέρονται στην αναφορά του ENISA. Σύμφωνα με την αναφορά, οι κοινές δομές με άλλες χώρες περιλαμβάνουν: Τρόφιμα, Ενέργεια, Τεχνολογίες Πληροφορικής και Επικοινωνιών, Οικονομία, Ύδατα, Υγεία και Μεταφορές.

1. Δημόδιες Υπηρεσίες
2. Δικαστικές Υπηρεσίες
3. Στρατιωτικές Υπηρεσίες
4. Τρόφιμα
5. Ηλεκτρονικές , Οπτικοακουστικές και Πληροφοριακές επικοινωνίες
6. Ενέργεια
7. Διάστημα κι Έρευνα
8. Οινονομία
9. Διαχείρηση Υδάτων
10. Βιομηχανία

11. Υγεία
12. Μεταφορές

Ολλανδία – Δομές Ζωτικής Σημασίας

Η Ολλανδία επίσης παρουσιάζει τις δικές της δομές ζωτικής σημασίας . Οι πιο κοινές περιλαμβάνουν: Ενέργεια, Τεχνολογίες Πληροφορικής και Επικοινωνιών, Τρόφιμα, Υγεία, Οικονομία, Δημόσια Διαχείριση και Στρατιωτικές Δυνάμεις

1. Ενέργεια : ηλεκτρισμός , Φυσικόαέριο , πετρέλαιο.
2. Τηλεπικοινωνίες και Τεχνολογίες Πληροφορικής & Επικοινωνιών: Σταθερή και κινητή τηλεφωνία, Ραδιόφωνο, Εκπομπές και το Διαδίκτυο.
3. Πόσιμο Νερό: Η παροχή νερού
4. Τρόφιμα: Προμήθεια τροφίμων και ασφάλεια τροφίμων.
5. Υγεία: Νοσοκομειακή φροντίδα και επειγόντων περιστατικών, Φάρμακα, Εμβόλια
6. Τομές οικονομίας: Πληρωμές και χρηματικές μεταφορές από Δημόσιους Φορείς
7. Διαχείριση επίγειων Υδάτων: Ποιότητα & Ποσότητα υδάτων (Παρακολούθηση και διαχείριση)
8. Δημόσια Τάξη κι Ασφάλεια
9. Έννομη Τάξη: Δικαστήρια και Φυλακές, επιβολή νομοθεσίας
10. Δημόσια Διαχείρηση: Διπλωματία, Πληροφόρηση κοινού, Στρατιωτικές δυνάμεις, Λήψη αποφάσεων
11. Μεταφορές: Αεροδρόμιο Amsterdam Schiphol, το λιμάνι του Rotterdam, εθνικοί οδοί, πλωτές μεταφορές, σιδηρόδρομοι
12. Πυρηνικές βιομηχανίες: μεταφορές, αποθήκευση, παραγωγή και επεξεργασία υλικών.

Πολωνία – Δομές Ζωτικής Σημασίας

Η Πολωνία έχει αναγνωρίσει έντεκα τομείς ζωτικής σημασίας για τις οποίες ενδιαφέρεται. Οι κοινές με τις άλλες χώρες περιλαμβάνουν: Ενέργεια, Επικοινωνίες, Οικονομία, Τρόφιμα, Ύδατα, Υγεία, Μεταφορές, Δημόσια Διαχείρηση και Χημικός τομέας.

1. Ενέργεια, Καύσιμα και συστήματα παροχής ενέργειας
2. Συστήματα επικοινωνιών
3. Συστήματα τηλεπικοινωνιών & δικτύων
4. Οικονομικά Συστήματα
5. Συστήματα διάθεσης Τροφίμων
6. Συστήματα παροχής Νερού
7. Συστήματα Υγεονομικής Προστασίας
8. Συστήματα μεταφορών
9. Συστήματα Διάσωσης
10. Συστήματα διασφάλισης της συνέχειας της δημόσιας διοίκησης
11. Συστήματα Παραγωγής, αποθήκευσης και χρήσης χημικών ραδιενεργών ουσιών, περιλαμβανομένων αγωγών επικίνδυνων ουσιών.

Ισπανία – Δομές Ζωτικής Σημασίας

Η Ισπανία έχει και αυτή αναγνωρίσει τους δώδεκα τομείς ζωτικής σημασίας για τους οποίους ενδιαφέρεται και οι κοινοί τομείς περιλαμβάνουν: Διοίκηση, Χημεία, Ενέργεια, Οικονομία, Τρόφιμα, Υγεία, Τεχνολογίες Πληροφορικής & Επικοινωνίες, Πυρηνική (Με τη Γαλλία μόνο), Μεταφορές και Ύδατα.

1. Διοίκηση
2. Χημική βιομηχανία
3. Ενέργεια
4. Οικονομία και φορολογικό σύστημα
5. Αλυσίδα εφοδιασμού τροφίμων
6. Υγεία
7. Τεχνολογίες πληροφορικής και Επικοινωνιών
8. Πυρηνική βιομηχανία
9. Εργαστήρια έρευνας

10. Διάστημα
11. Μεταφορές
12. Ύδατα

Γερμανία – ΔομέςΖωτικήςΣημασίας

Σύμφωνα με την ομοσπονδιακή κυβέρνηση της Γερμανίας ο ορισμός των δομών ζωτικής σημασίας είναι η εξής: «Οι δομές ζωτικής σημασίας, είναι οργανωτικές και φυσικές δομές και λειτουργίες τέτοιας ζωτικής σημασίας για την κοινωνία και την οικονομία ενός Έθνους, που η κατάρρευση και υποβάθμισή τους θα προκαλούσε διαρκείς ελλείψεις προμηθειών, διαταραχές της δημόσιας ασφάλειας και προστασίας, ή άλλες δραματικές συνέπειες» Οργανισμοί και εγκαταστάσεις που εμπλέκονται στους παρακάτω τομείς, χαρακτηρίζονται και αναγνωρίζονται ως δομές ζωτικής σημασίας (www.kritis.bund.de, 2020). Αυτοί οι τομείς περιλαμβάνουν :

1. Ενέργεια
2. Υγεία
3. Τεχνολογίες πληροφορικής και επικοινωνιών
4. Μεταφορές και Κυκλοφορία
5. Μέσα ενημέρωσης και κουλτούρα
6. Ύδατα
7. Οικονομίακιασφάλιση
8. Τρόφιμα
9. Κράτος και διοίκηση

Ιταλία – Δομές Ζωτικής Σημασίας

Παρακάτω περιλαμβάνονται οι δομές της Ιταλίας σύμφωνα με την "Ασφάλεια δικτύου σε δομές ζωτικής σημασίας» που έχουν επιδείξει αρκετοί φορείς της Ιταλίας, έχουν αναγνωριστεί οι παρακάτω έντεκα δομές ζωτικής σημασίας (www.isticom.it, 2020):

1. Μεταφορά ενέργειας και δίκτυα διανομής (ενέργεια, αέριο κλπ)
2. Δίκτυα τηλεπικοινωνιών
3. Συστήματαμεταφορών (αγαθών–επιβατών)

4. Υπηρεσίες έκτακτων αναγκών
5. Δομές Άμυνας
6. Τραπεζικό κι οικονομικό κύκλωμα
7. Υπηρεσίες δημόσιας υγείας
8. Μεταφορά , διανομή και διαχείρηση υδάτων
9. Δίκτυα μέσως ενημέρωσης και δημόσιων πληροφοριών
10. Γεωργία και βιομηχανία επεξεργασίας τροφίμων
11. Κυβερνητικά δίκτυα

Ελλάδα – Δομές Ζωτικής Σημασίας

Το επίσημο πλαίσιο NCSS (Εθνικό Πλάίσιο για την Κυβερνοασφάλεια) για την Ελλάδα, δεν είναι ακόμη διαθέσιμο. Υπάρχει μια μελέτη ενός μη κερδοσκοπικού οργανισμού (www.dianeosis.org, 2020) η οποία συνοψίζει τις δομές της Ελλάδας που θα μπορούσαν να αναγνωριστούς ως ζωτικές (ΚΥ). Η μελέτη αναφέρει δεκατρείς πιθανές δομές που θα μπορούσαν δυνητικά να χαρακτηριστούνώς δομές ζωτικής σημασίας:

1. Ενέργεια
2. Τεχνολογίες οληροφορικής κι επικοινωνιών - επικοινωνίες
3. Ύδατα
4. Τρόφιμα
5. Υγεία
6. Οικονομία
7. Δημόσια ασφάλεια και προστασία
8. Μεταφορές
9. Βιομηχανία
10. Δημόσια διοίκηση
11. Πολιτική διοίκηση
12. Περιβάλλον

13. Άμυνα

Ηνωμένες Πολιτείες – Δομές Ζωτικής Σημασίας

Οι Ηνωμένες Πολιτείες, και συγκεκριμένα η Υπηρεσία Εσωτερικής Ασφάλειας, έχει αναγνωρίσει δεκαέξι διακριτούς τομείς ζωτικής σημασίας. Έχουν συντάξει έγγραφα στα οποία περιγράφουν κάθε τομέα ζωτικής σημασίας. Τα αναφερθέντα έγγραφα περιλαμβάνουν πληροφορίες σχετικά με το τι περιλαμβάνεται σε κάθε τομέα, τα χαρακτηριστικά τους, θέματα ασφάλειας (γενικά) τα οποία θα πρέπει να ληφθούν υπόψιν καθώς και κάποιες πληροφορίες που αναφέρουν πτυχές σχετικές με την Κυβερνοασφάλεια. Τέτοιες αναφορές ανά τομέα φαίνεται να λείπουν από τις αναφορές που έχουν συντάξει οι χώρες της ΕΕ και άλλες χώρες. Παρακάτω, απαριθμούνται οι αναγνωρισμένοι τομείς, κάποιοι από τους οποίους δεν έχουν αναφερθεί σε παρόμοιες ευρωπαϊκέςαναφορές, Περιγράφονται ως εξής (www.dhs.gov, 2020):

1. Χημικός τομέας
2. Τομέας εμπορικών υπηρεσιών
3. Τομέας επικοινωνιών
4. Τομέας ζωτικής βιομηχανίας
5. Τομέας φραγμάτων
6. Τομέας άμυνας σε βιομηχανική βάση
7. Τομέας επείγοντων υπηρεσιών
8. Τομέας ενέργειας
9. Τομεάς οικονομικών υπηρεσιών
10. Τομέας τροφίμων και Γεωργίας
11. Τομέας κυβερνητικών υπηρεσιών
12. Τομέας Υγείας & δημόσιας Υγείας
13. Τομέας πληροφοριών Τεχνολογίας
14. Τομέας πυρηνικών αντιδραστήρων , Υλικών & Αποβλήτων
15. Τομέας μεταφορών
16. Τομέας ύδρευσης και επεξεργασίας λυμάτων

Ιαπωνία – Δομές Ζωτικής Σημασίας

Το 2009 το Συμβούλιο σχετικά με την προστασία των πληροφοριών συνέταξε ένα έγγραφο με όνομα σχετικά με τα μέρτα προστασίας σε δομές ζωτικής σημασίας. Η αναφορά δημιουργήθηκε από οργανισμούς που ενδιαφέρονται για δομές ζωτικής σημασίας ή και από οργανισμούς που τις λειτουργούν ήδη , το κράτος και δέκα (10) τομείς ζωτικής σημασίας, όπως έχουν αναγνωριστεί από την Ιαπωνία. Η αναφορά στοχεύει στην «ελαχιστοποίηση των περιστατικών δυσλειτουργίας σε δομές ζωτικής σημασίας» (www.nisc.go.jp, 2020). Οι δέκα (10) δομές που περιγράφονται στις σχετικές αναφορές είναι οι εξής:

1. Πληροφορία - Επικοινωνία
2. Οικονομία
3. Αεροπορία
4. Σιδηρόδρομος
5. Ηλεκτρική ενέργεια
6. Αέριο
7. Κυβερνητικές και διοικητικές υπηρεσίες
8. Ιατρική
9. Ύδρευση
10. Διοικητική μέριμνα

Αυστραλία – Δομές Ζωτικής Σημασίας

Το 2014 πέντε (5) χώρες (ΗΠΑ, Αυστραλία, Νέα Ζηλανδία, Καναδάς και Ηνωμένο Βασίλειο) συνέταξαν ένα έγγραφο το οποίο περιλαμβάνει πληροφορίες για τις δομές ζωτικής σημασίας τους. Η αναφορά στόχευε στην «αναγνώριση κοινών δομών ζωτικής σημασίας, ομοιότητες, προσέγγιση, αντίληψη, και πως εφαρμόζονται με σκοπό να υπάρξει μια κοινή κατανόηση των δομών ζωτικής σημασίας» (www.infrastructure.govt.nz, 2020). Από την συγκεκριμένη αναφορά αντλήθηκαν πληροφορίες αναφορικά με τις δομές ζωτικής σημασίας της Αυστραλίας και του Καναδά (αναφέρονται στην παρακάτω ενότητα)

1. Οικονομία & τραπεζική
2. Επικοινωνίες

    a. Εκπομπή μέσων
    b. Υπηρεσίες ταχυδρομείων
    c. Δίκτυα Τηλεπικοινωνιών
3. Ενέργεια
    a. Συστήματα ηλεκτρισμού
    b. Υπεράκτιο πετρέλαιο κι Αέριο
    c. Παράλιοπετρέλαιο κι Αέριο
    d. Παροχή κάρβουνου
4. Τροφική αλυσίδα
5. Υγεία
6. Μεταφορές
    a. Αεροπορία
    b. Χερσαίες μεταφορές επιβατών
    c. Χερσαίες μεταφορές φορτίων
    d. Ναυτιλιακά: Μεταφορές και λιμάνια
7. Υπηρεσίες ύδρευσης
8. Άλλες δομές ζωτικής σημασίας
    a. Εργαστήριαπουκατέχουνβιολογικά προϊόντα υψηλού κινδύνου
    b. Βιομηχανία κατασκευής χημικών
    c. Βιομηχανίες άμυνας
    d. Υπηρεσίες επειγόντων

Καναδάς – Δομές Ζωτικής Σημασίας

Από την ίδια αναφορά (όπως και στην περίπτωση της Αυστραλίας), απαριθμούνται οι δομές ζωτικής σημασίας για τον Καναδά (www.infrastructure.govt.nz, 2020):

1. Ενέργεια κι υπηρεσίες κοινής ωφέλειας
2. Τεχνολογίες πληροφορικής και επικοινωνιών

3. Οικονομία
4. Κατασκευές
5. Τρόφιμα
6. Ασφάλεια
7. Κυβέρνηση
8. Μεταφορές
9. Υγεία
10. Ύδατα

Κεφάλαιο 2: Επιλογή παραδειγμάτων δομών ζωτικής σημασίας

Στις προηγούμενες ενότητες παρουσιάστηκαν οι αναγνωρισμένες δομές ζωτικής σημασίας σε διάφορες χώρες. Αυτές οι δομές προέρχονται κυρίως από δημοσιευμένα έγγραφα. Οι ενοτητες που ακολουθούν παρέχουν πληροφορίες για συγκεκριμένες δομές ζωτικής σημασίας και προσπαθούν να παρέχουν (α) μια σύντομη περιγραφή από κάθε δομή και τι περιλαμβάνεται σε κάθε μία και (β) τα χαρακτηριστικά ή συγκεκριμένα στοιχεία που έχουν αναφερθεί και πρέπει να προστατευτούν. Σημαντικές πληροφορίες έχουν συλλεχθεί για τα στοιχεία που θα πρέπει να προστατευθούν, από την Υπηρεσία Εσωτερικής Ασφάλειας των ΗΠΑ, η οποία έχει προχωρήσει ένα βήμα περαιτέρω και αναφέρει συγκεκριμένα χαρακτηριστικά για κάθε δομή ζωτικής σημασίας. Σε κάποιες περιπτώσεις, αυτά είναι χαρακτηριστικά που σχετίζονται με την ασφάλεια και είναι άμεσα συνδεδεμένα με την συγκεκριμένη μελέτη. Επομένως σε αυτήν την ενότητα απαριθμούνται και αναλύονται οι δομές ζωτικής σημασίας που χρήζουν ασφάλειας. Αυτή δεν είναι μια πλήρης λίστα με τις δομές, αλλά είναι μια λίστα που περιλαμβάνει εκείνες τις δομές ζωτικής σημασίας για τις οποίες έχουμε πληροφορίες για θέματα ασφάλειας.

2.1 Κλάδος Χημείας

2.1.1 Επισκόπηση και χαρακτηριστικά

Ο Χημικός κλάδος δεν είναι κοινός ανάμεσα στις δομές ζωτικής σημασίας, σύμφωνα με διάφορες πηγές που έχουν μελετηθεί, έχουν όμως προκύψει αξιόλογες πληροφορίες σχετικά με την Κυβερνοασφάλεια στα αντίστοιχα έγγραφα και αυτός είναι ο λόγος που συμπεριλαμβάνεται σε αυτή την ενότητα. Ο κλάδος των Χημικών Υπηρεσιών είναι αρκετά ευρύς και περιλαμβάνει πολλές υποκατηγορίες όπως γεωργικά χημικά, φαρμακευτικά και καταναλωτικά προϊόντα. Όλες οι παραπάνω κατηγορίες χρησιμοποιούνται και χρήζουν προστασίας από απειλές Κυβερνοασφάλειας.

Η αναφορά (www.dhs.gov, 2019) των ΗΠΑ που εκδόθηκε από την Υπηρεσία Εσωτερικής Προστασίας (www.dhs.gov, 2019) των ΗΠΑ αναγνωρίζει απειλές και τομείς που θα πρέπει να τεθούν υπό ιδιαίτερη προσοχή με στόχο να βελτιωθεί η Κυβερνοασφάλεια των Χημικών δομών ζωτικής σημασίας και των υπηρεσιών αυτών. Αυτές οι απειλές περιλαμβάνουν:

- Εσωτερικές απειλές
- Κυβερνοαπειλές
- Φυσικέςκαταστροφέςκι ακραίες καιρικές συνθήκες

- Σκόπιμες επιθέσεις και τρομοκρατία
- Βιολογικές απειλές και πανδημίες

Οι περιπτώσεις που έχουν σκιαγραφηθεί αφορούν περιπτώσεις της Κυβερνοασφάλειας που είναι ενδιαφέρουσες για την παρούσα μελέτη, επομένως περιλαμβάνονται οι αντίστοιχες πληροφορίες στις ενότητες που ακολουθούν:

Εσωτερικές απειλές

Αυτές φαίνεται να είναι ένας κοινός προβληματισμός σε πολλές επιχειρήσεις και οργανισμούς. Δεν θα μπορούσε να λείπει από τις δομές ζωτικής σημασίας. Υπάρχουν αρκετές πρακτικές που μπορούν να καθιερώσουν συστήματα Κυβερνοασφάλειας και φυσικής προστασίας ικανές να προλάβουν πολλές από τις γνωστές εξωτερικές απειλές. Σε περίπτωση βέβαια που κάποιος θέλει να αναφέρει το θέμα των εσωτερικών απειλών τότε η περίπτωση είναι διαφορετική. Μπορεί να υπάρχουν άτομα εκ των έσω με πρόσβαση στις εγκαταστάσεις και συστήματα οι οποίοι θα μπορούσαν να βλάψουν τις υπηρεσίες και τις δομές είτε εσκεμμένα είτε άθελα τους. Τέτοιες δραστηριότητες όπως ο Χημικός τομέας δημιουργεί συνεργασίες με τρίτους για μια πληθώρα λόγων με αποτέλεσμα να τους παρέχει πρόσβαση σε υπηρεσίες και εγκαταστάσεις. Αυτοί οι συνεργάτες μπορεί να μην περνάνε από τον ίδιο έλεγχο όπως το μόνιμο προσωπικό.

Κυβερνοαπειλές

Ο Χημικός Τομέας περιλαμβάνει συστήματα που ανήκουν στην κατηγορία των Εσωτερικών Βιομηχανικών Συστημάτων για μεγάλα εθνικά και παγκόσμια δίκτυα ασφάλειας, επομένως αντιμετωπίζουν μια πληθώρα απειλών συμπεριλαμβανόμενων

- Ανθρώπινεσκόπιμεςεπιθέσεις
- Τεχνολογικές αποτυχίες
- Ανθρώπινα λάθη και
- Ευπάθειεςηαλυσίδαςεφοδιασμού

Οποιαδήποτε διαταραχή αυτών των συστημάτων και υπηρεσιών θα μπορούσε να οδηγήσει σε απώλειες στις λειτουργικές δυνατότητες, χημικές κλοπές ή κλοπή πνευματικών ιδιοκτησιών. Παρόλο που αναφέρεται ότι οι δομές ζωτικής σημασίας που επικαιροποιούνται μέσω διαδικτυακών συστημάτων και εφαρμογές τρίτων δεν είναι πολλές, αυτό δεν απαλείφει τον κίνδυνο για Κυβερνοεπιθέσεις.

Σκόπιμες επιθέσεις και τρομοκρατία

Τα προϊόντα και τα υλικά που χρησιμοποιούνται στον χημικό κλάδο αποτελούν στόχο για επιθέσεις λαμβάνοντας υπόψιν την ζημιά που θα προκαλούσαν (στους ανθρώπους και στο περιβάλλον) αν χρησιμοποιούνταν για τρομοκρατικούς σκοπούς. Χημικές εγκαταστάσεις, υπηρεσίες και υλικά είναι επίσης στόχος κλοπή ώστε είτε να χρησιμοποιηθούν αυτούσια είτε για την δημιουργία όπλων μαζικής καταστροφής και αυτοσχέδιους εκρηκτικούς μηχανισμούς.

2.1.2 Κρίσιμα στοιχεία για προστασία

Σύμφωνα με την έκθεση (www.scadahacker.com, 2019)τα ακόλουθα πολλά στοιχεία έχουν προσδιοριστεί ως σημαντικά και πρέπει να αντιμετωπιστούν / προστατευθούν στη χημική βιομηχανία. Μεταξύ αυτών των στοιχείων απομονώσαμε τα ακόλουθα που σχετίζονται με την παρούσα έκθεσή μας:

- Πληροφοριακά συστήματα (συμπεριλαμβανομένων λειτουργικών συστημάτων, βάσεων δεδομένων, εφαρμογών της εταιρείας, συμπεριλαμβανομένων των κοινοπραξιών και άλλων επιχειρηματικών δραστηριοτήτων τρίτων).
- Συστήματα κατασκευής και ελέγχου (συμπεριλαμβανομένου του Εποπτικού Ελέγχου και Απόκτησης Δεδομένων (SCADA), Προγραμματιζόμενου Λογικού Ελεγκτή (PLC), Κατανεμημένου Συστήματος Ελέγχου (DCS) και Σταθμών εργασίας διαμόρφωσης).
- Δίκτυα, τοπικά δίκτυα (LAN), δίκτυα ευρείας περιοχής (WAN) (συμπεριλαμβανομένου υλικού, εφαρμογών, τείχη προστασίας, συστήματα ανίχνευσης εισβολών).

Ο χημικός τομέας είναι περισσότερο ή λιγότερο αλληλεξαρτώμενος με όλους τους άλλους τομείς που παρέχουν προϊόντα και υπηρεσίες ή ζητούν προϊόντα και υπηρεσίες για να συνεχίσουν τις ομαλές λειτουργίες τους. Οι εκθέσεις αναφέρουν ότι τέσσερις από αυτές είναι πιο σημαντικές για τον τομέα των χημικών. Αυτές οι ΚΥ περιλαμβάνουν το νερό, τις μεταφορές, τις επικοινωνίες και την ενέργεια ως τομείς, υπηρεσίες και πόρους που είναι ουσιώδεις για τον τομέα των χημικών ουσιών.

2.2 Τεχνολογίες πληροφοριών και επικοινωνιών (ΤΠΕ)

2.2.1 Επισκόπησηκαιχαρακτηριστικά

Υπάρχουν χώρες που προσδιορίζουν δύο διαφορετικούς τομείς ΚΥ (τον τομέα των επικοινωνιών και τον τομέα πληροφορικής (Information Technologies), ενώ άλλες χώρες χειρίζονται και τους δύο τομείς ως ένα. Στη παρούσα μελέτη θα τον αντιμετωπίσουμε ως ένα τομέα. Ο τομέας των επικοινωνιών

αποτελεί βασικό στοιχείο για την οικονομία παγκοσμίως και σχεδόν όλες οι επιχειρήσεις και οι επιχειρήσεις στηρίζονται σε μεγάλο βαθμό σε αυτό. Τα τελευταία χρόνια, οι επικοινωνίες εξελίχθηκαν ραγδαία. Ο τομέας των επικοινωνιών ξεκίνησε κυρίως ως πάροχος φωνητικών υπηρεσιών και τώρα (με την υποστήριξη τεχνολογιών πληροφορικής) διασυνδέει πολλούς επιχειρηματικούς τομείς και βιομηχανικά συστήματα. Αυτός ο στόχος έχει επιτευχθεί χρησιμοποιώντας ενσύρματα, δορυφορικά και ασύρματα συστήματα επικοινωνίας.

Μεταξύ των πολλών φυσικών περιστατικών που πρέπει να αντιμετωπίσει ο τομέας, μεγάλοι σεισμοί, τυφώνες και διαστημικές καιρικές συνθήκες, ο τομέας πρέπει επίσης να αντιμετωπίσει πολλές διαταραχές του κυβερνοχώρου. Οι προκλήσεις που παρουσιάζονται σε διάφορεασυστήματαμε τα συστήματα επικοινωνιών και πληροφορικής παρουσιάζουν μοναδικές προκλήσεις λόγω της παγκόσμιας συνδεσιμότητας. Η εκμετάλλευση των τρωτών σημείων μπορεί εύκολα να επηρεάσει ΚΥ σε λίγα λεπτά, επηρεάζοντας έτσι σχεδόν όλες τις διασυνδεμένες δομές.

Από μόνη της η τεχνολογία πληροφορικής αποτελεί σήμερα ουσιαστικό μέρος σχεδόν όλων των υποδομών ζωτικής σημασίας. Είναι επίσης ο συνδετικός κρίκος που διασυνδέει πολλά συστατικά που σχηματίζουν τις ΚΥ και τον συνδετικό κρίκο που ενώνει τις ΚΥ μεταξύ τους.Επιπλέον, η τεχνολογία πληροφορικής αναγνωρίζεται ως ένας από τους τομείς του ΚΥ σχεδόν σε κάθε χώρα, όπως αναφέρεται στις προηγούμενες ενότητες

2.2.2 Κρίσιμα στοιχεία για προστασία

Ο Εθνικός οδηγός στρατηγικής για την ασφάλεια στον κυβερνοχώρο (www.itu.int, 2019)έχει προσδιορίσει ορισμένα τεχνικά μέτρα που θα πρέπει να εξετάσουν το σύνολο των τομέων των τηλεπικοινωνιών και των επικοινωνιών προκειμένου να παρέχουν αδιάλειπτες υπηρεσίες στους πολίτες και τις επιχειρήσεις.

- Ομοιόμορφη διαχείριση πρόσβασης:
  - Κεντρικός έλεγχος ταυτότητας. Ο μηχανισμός καταργεί την ανάγκη αποθήκευσης διαπιστευτηρίων (κωδικών πρόσβασης ή πιστοποιητικών) σε τοπικό ή κεντρικό υπολογιστή,.
  - Κεντρική εξουσιοδότηση. Αυτή η προσέγγιση διασφαλίζει ότι η πρόσβαση στους πόρους του συστήματος διαχειρίζεται με διαφάνεια και έλεγχο.

- Ασφαλής καταγραφή όλων των συμβάντων σε σχέση με τον έλεγχο ταυτότητας και την εξουσιοδότηση.
- Επιβολή κανόνων πολύπλοκων κωδικών πρόσβασης. Χρήση ισχυρών κωδικών πρόσβασης
- Ασφαλής αποθήκευση όλων των κωδικών πρόσβασης.

- Ασφαλείς επικοινωνίες. Οι ισχυροί κρυπτογραφικοί ψηφιακοί επεξεργαστές θα πρέπει να προστατεύουν δεδομένα, φωνή και δίκτυα κινητής τηλεφωνίας.
- Χρήση DMZ. Παρέχετε μεταβλητή ασφάλεια βάθους ή ζώνη για μη αξιόπιστες υπηρεσίες.
- Πολυεπίπεδη ασφάλεια: χρήση πολλαπλών ελέγχων και διαφορετικών προϊόντων ασφαλείας για να μετριαστούν οιαπειλές κατά της ασφάλειας. (π.χ. τείχη προστασίας, συστήματα ανίχνευσης εισβολών (IDS), συστήματα πρόληψης εισβολής (IPS) και λογισμικό προστασίας από ιούς.
- Ανάκαμψη δικτύου μετά από επίθεση. Πρέπει να εκπληρώνει ένα ελάχιστο σύνολο βασικών λειτουργιών προκειμένου να ανακάμψει εγκαίρως σε περίπτωση επιθέσεων.

Άλλα σημαντικά πράγματα που πρέπει να προστατευθούν σε αυτόν τον τομέα έναντι των επιθέσεων στον κυβερνοχώρο και των απειλών είναι τα ακόλουθα:

- Προστασία των κρίσιμων λειτουργιών από τις απειλές. Ειδικά αυτές που θα υποβαθμίσουν την εμπιστευτικότητα, την ακεραιότητα και / ή τη διαθεσιμότητα τους.
- Αποφυγή, αν είναι δυνατόν, από ακούσιες δραστηριότητες (χωρίς δόλο) που θα μπορούσαν π.χ. να διαταράξουν τις υπηρεσίες ISP και τις εκούσιες δραστηριότητες (με δόλο) που θα μπορούσαν να οδηγήσουν σε απώλεια της διαλειτουργικότητας των συστημάτων.
- Μια άλλη ανάγκη που προκύπτει από τη βιομηχανία σχετικά με τον τομέα ΤΠΕ σχετίζεται με επιθέσεις που στοχεύουν σε διαδικτυακή ταυτότητα που μπορεί να οδηγήσει σε οικονομικές απώλειες και κλοπή ταυτότητας. Οι ταυτότητες μπορούν στη συνέχεια να χρησιμοποιηθούν για
  - εγκληματικές δραστηριότητες και
  - μη εξουσιοδοτημένη πρόσβαση σε διαβαθμισμένες πληροφορίες και εγκαταστάσεις.

Σύμφωνα με γνωστή μεθοδολογία, οι τρεις πρώτες μέθοδοι επίθεσης που χρησιμοποιούν οι χάκερ για την ανάκτηση ευαίσθητων πληροφοριών είναι (i) η εφαρμογή απομακρυσμένης πρόσβασης (ii) η συνδεσιμότητα με τρίτους και (iii) SQLInjection.

2.3 Ενέργεια

2.3.1 Επισκόπησηκαιχαρακτηριστικά

Σύμφωνα με ορισμένες αναφορές, ο τομέας της ενέργειας περιλαμβάνει τρεις (3) υποκατηγορίες, συμπεριλαμβανομένης της ηλεκτρικής ενέργειας, του πετρελαίου και του φυσικού αερίου. Οι ίδιες κατηγορίες έχουν επίσης προσδιοριστεί από την ευρωπαϊκή οδηγία υποδομές ζωτικής σημασίας.Υπάρχει αρκετά μεγάλο και ευρύ φάσμα απειλών (www.icitech.org, 2019)που θα μπορούσε να βλάψει τον τομέα της ενέργειας. Αυτές περιλαμβάνουν αθέμιτες απειλές, τρωτά σημεία (zerodayworms), botnetsκαι ακολουθία απλών συμβάντων που εκμεταλλεύονται μια ευπάθεια καθώς και πολλά άλλα όπως αναφέρονται παρακάτω.

2.3.2 Κρίσιμα στοιχεία για προστασία

Σύμφωνα με ορισμένες αναφορές, οι πτυχές ασφαλείας που σχετίζονται με τον τομέα της ενέργειας μπορούν να κατηγοριοποιηθούν σε τρεις (3) κατηγορίες:

- Τοπεδίο που στοχεύουν οι απειλές,
- Οι απειλές και
- Οι φορείς των απειλών.

Θα παρουσιάσουμε παρακάτω από πιο σχετικό για την έκθεσή μας, συμπεριλαμβανομένης σύντομης περιγραφής για καθένα από αυτά. Οι παρακάτω πίνακες περιλαμβάνουν πληροφορίες σχετικά με τις πρώτες κατηγορίες. Μεταξύ άλλων hacktivists, Cyberterrorists, και οι εγκληματίες του κυβερνοχώρου χαρακτηρίζονται ως πιθανοί παράγοντες για επιθέσεις στον τομέα της Ενέργειας CI.

Τοπίο Απειλής	
IT-OT (Information technology – operational technology)	Εφαρμογές ICTαλληλοσυνδέονται όλο και περισσότερο με την SCADA.PLC, ICS και συστήματα αισθητήρων
Διεπαφές με τον άνθρωπο	Είναι συνήθως ένας κεντρικός υπολογιστής MS windows ο οποίος συνδέεται άμεσα με τα PLC (τα οποία είναι επίσης ευάλωτα σε επιθέσεις).
Σταθμοίεργασίας	Οι σταθμοί εργασίας είναι συνήθως διασυνδεδεμένοι και μερικοί από αυτούςσυνδέονται και με το Διαδίκτυο, καθιστώντας τους έτσι ευκολότερους στόχους για τους επιτιθέμενους
Προγραμματιζόμενοι λογικοί ελεγκτές	Οι PLCs μπορεί να είναι προσβάσιμοι με διάφορους τρόπους. Ένας από αυτούςείναι μέσωτουδικτύου.
Τεχνολογίες Smart Grid	Smart Grid Technologies χρησιμοποιούνται ως επί το πλείστονγια την αύξησητης αξιοπιστίας τουδικτύουGrid. Αυτά εξαρτώνται σε μεγάλο βαθμό από αυτοματοποιημένες διαδικασίες, οι οποίες συχνά αποτελούν πιθανό στόχογια τους επιτιθέμενους.
Τεχνολογίες Cloud Computing	Υπηρεσίες νέφους και η αποθήκευση επιτρέπει την ανταλλαγή πληροφοριών σε πραγματικό χρόνο μεταξύ των ενδιαφερομένων. Αυτό φυσικά θα πρέπει να γίνεται με ιδιαίτερη προσοχή επειδή οι ευαίσθητες πληροφορίες είναι πάντα στόχοι για τους επιτιθέμενους.

Πίνακας 1 : Τοπίο Απειλής

Η ενεργειακή τεχνολογία σχετίζεται σε μεγάλο βαθμό με τις ΤΠΕ για τη βελτίωση της αποτελεσματικότητας και της αξιοπιστίας των διαδικασιών παραγωγής, διανομής και τιμολόγησης της ενέργειας. Αυτό όμως έχει αυξήσει την επιφάνεια επίθεσης που θα μπορούσε να εκμεταλλευτεί από διάφορες απειλές. Μερικά από αυτάείναι τα ακόλουθα:

Απειλές	
Εργαλεία και τεχνικές που χρησιμοποιούνται	Παρόλο που οι διαχειριστές χρησιμοποιούν τείχη προστασίας για την προστασία των συστημάτων τους, υπάρχουν περιπτώσεις όπου η λανθασμένη διαμόρφωση τους μπορεί να βοηθήσει τους επιτιθέμενους σε πιο στοχευμένες επιθέσεις.
Τα γνωστά Phishing emails	π.χ. μηνύματα ηλεκτρονικού ταχυδρομείου που ζητούν δράσεις και δραστηριότητες του θύματος που θα αποκαλύψουν ή θα δημιουργήσουν ευπάθειες.
Botnets	Οι σταθμοί εργασίας μηχανικών ενδέχεται να μολυνθούν από τα botnets. Κοινό λογισμικό κακόβουλου λογισμικού botnet που βρέθηκαν περιλαμβάνει τα TDSS, Carufax, ZeroAccess, Sality και Banloa.
Ανακάλυψη αδυναμιών δικτύου	Τα δίκτυα θα πρέπει να προστατεύονται αρκετάώστε να αρνούνται την κακόβουλη εισερχόμενηκίνηση όπως (π.χ. σάρωσηports)
Εσωτερική απειλή	Οι εσωτερικές απειλές είναι πράγματι γεγονός λόγω σκόπιμης ή ακούσιας κατάχρησης των εγκαταστάσεων.
Cross-site Scripting (XSS)	XSS είναι μια μέθοδος για να μολύνει κάποιον υπολογιστή με την τοποθέτηση κακόβουλου λογισμικού στον διακομιστή εφαρμογών του. Οι

	συνηθισμένες επιθέσεις XSS συνήθως καταγράφουν διαπιστευτήρια ή εγκαθιστούν κακόβουλο λογισμικό.
Malicious Downloads	Σε αυτήτην περίπτωση, οι μολυσμένοι ιστότοποι "προσφέρουν" κακόβουλο λογισμικό σε όλους όσους τις επισκέπτονται.
Zero dayworms	Αυτού του είδους οι απειλές συνήθως συνδυάζονται και χρησιμοποιούν τεχνικές επίθεσης όπως Zero dayworms, XSS ή μεταφορτώνουν προς μια συγκεκριμένη υπηρεσία προορισμού.
Wrappers / Packers / Crypter	Αυτοί είναι μηχανισμοί για την ενσωμάτωση του κακόβουλου κώδικα έτσι ώστε οι εφαρμογές που βασίζονται στην υπογραφή και το IDS να μην εντοπίσουν το κακόβουλο λογισμικό
Πολυμορφισμός	Χρήσιμη τεχνική όταν ο κακόβουλος κώδικας δεν πρέπει να ανιχνεύεται από συστήματα ανίχνευσης / πρόληψης εισβολών. Η κακόβουλη εφαρμογή αλλάζει ελαφρώς τον ίδιο της τον εαυτό.
Ransomware	Τα Ransomwares μολύνουν επίσης τις ΚΥ. Το 2015 το Υπουργείο Εσωτερικής Ασφάλειας ανέφερε 295 περιστατικά μολυσμένων συστημάτων βιομηχανικού ελέγχου

Πίνακας 2 : Απειλές

Ιδιαίτερο ενδιαφέρον για τους επιτιθέμενους είναι τα συστήματα βιομηχανικού ελέγχου (www.paconsulting.com, 2019)(όπως συστήματα ελέγχου, αυτοματοποίησης ή SCADA) που λειτουργούν ως υποδομές κρίσιμης σημασίας για την αποστολή και την ασφάλεια, όπως η γεώτρηση πετρελαίου και φυσικού αερίου, παραγωγή, μεταφορά και διανομή ηλεκτρικής ενέργειας.

Οι κίνδυνοι για την ασφάλεια θα αυξηθούν καθώς ο τομέας αναπτύσσει νέες και ισχυρότερες τεχνολογίες μέσω πρωτοβουλιών όπως τα έξυπνα δίκτυα όπως αναφέρονται στους παραπάνω πίνακες.

Άλλα στοιχεία που πρέπει να προστατεύονται από κυβερνοεπιθέσεις περιλαμβάνουν επίσης:

- Υποδομή ηλεκτρικής ενέργειας, η οποία είναι ιδιαίτερα αυτοματοποιημένη και ελέγχεται από σύνθετα και εξελιγμένα συστήματα διαχείρισης της ενέργειας.
- Δίκτυα συστημάτων ελέγχου που είναι συνδεδεμένα στο επιχειρηματικό δίκτυο και επίσης συνδεδεμένα στο Internet.
- Απειλές προς εμπιστευτικές πληροφορίες, οι οποίες κινήθηκαν από (υφιστάμενους, πρώην) εργαζομένους εκ προθέσεως ή ακούσια.

2.4 Οικονομικές Υπηρεσίες

2.4.1 Επισκόπησηκαιχαρακτηριστικά

Ο τομέας CI των χρηματοπιστωτικών υπηρεσιών είναι ένα μείζων και σημαντικό συστατικό στοιχείο της δομής κάθε χώρας. Οι χρηματοοικονομικές υπηρεσίες βασίζονται σε υποδομές που έχουν χαρακτηριστεί κρίσιμες και από τις εκθέσεις των ΗΠΑ και της ΕΕ.

Τα χρηματοπιστωτικά ιδρύματα παρέχουν ένα ευρύ φάσμα προϊόντων και υπηρεσιών σε μεγάλους και μικρούς οργανισμούς και πιστωτικές ενώσεις. Όπως αναφέρεται στην αντίστοιχη έκθεση των ΗΠΑ (www.hsdl.org, 2019)τα προϊόντα αυτά ταξινομούνται σε τέσσερις κατηγορίες: (1) προϊόντα καταθέσεων, καταναλωτικής πίστης και συστήματα πληρωμών · (2) προϊόντα πίστωσης και ρευστότητας · (3) επενδυτικά προϊόντα · και (4) προϊόντα μεταφοράς κινδύνου.

Παραδοσιακά, ο τομέας των χρηματοπιστωτικών υπηρεσιών περιλαμβάνει τις τράπεζες (είτε ως ιδρύματα καταθέσεων είτε ως επενδυτές), ασφαλιστικές εταιρείες, οικονομικές ρυθμιστικές αρχές, εμπορικούς συλλόγους και άλλους πιστωτικούς και χρηματοδοτικούς οργανισμούς.

Εν τω μεταξύ, ο όρος Οικονομική Υπηρεσία περιλαμβάνει αναδιανομή κεφαλαίων πέραν της ασφάλισης, της συνταξιοδότησης ή της υποχρεωτικής κοινωνικής ασφάλισης σύμφωνα με τονENISA, ο οποίος καλύπτει την αλληλεπίδραση μεταξύ χρηματοπιστωτικών επιχειρήσεων και εθνικών κεντρικών τραπεζών, ευρωπαϊκών πλατφορμών και φυσικά ιδιωτικών δικτύων που λειτουργούν από εξειδικευμένους διαχειριστές. Η προκύπτουσα ταξινόμηση κατηγοριοποιεί:

- Τα ενδιαφερόμενα μέρη, σύμφωνα μετέσσερις βασικές κατηγορίες: Τράπεζες, Παροχείς Υπηρεσιών, Επαγγελματικές ενώσεις και Αρχές (Εθνικές ΕποπτικέςΑρχές και Ευρωπαϊκές ΕποπτικέςΑρχές).

- Δραστηριότητες: Νομισματική διαμεσολάβηση (Transactions)Εταιρείες χαρτοφυλακίου · Εμπιστοσύνη, κεφάλαια και παρόμοιεςχρηματοπιστωτικές οντότητες και άλλεςδραστηριότητες χρηματοπιστωτικών υπηρεσιών, εκτός από την ασφάλιση και τησυνταξιοδοτική χρηματοδότηση.

Απειλές στον κυβερνοχώρο

Οι χρηματοπιστωτικές υπηρεσίες είναι διασυνδεδεμένες με ιδιωτικά και δημόσια δίκτυα και αποτελούν πιθανό στόχο για τρομοκράτες, διακρατικούς εγκληματίες και άλλους εγκληματίες του κυβερνοχώρου που γνωρίζουν και μπορούν να χρησιμοποιήσουν ιούς υπολογιστών, Trojanhorses, worms, malware, sniffers, και άλλα εργαλεία που μπορούν να καταστρέψουν, την παρακολούθηση και την άρνηση πρόσβασης σε δεδομένα και υπηρεσίες. Συγκεκριμένες απειλές στον κυβερνοχώρο, όπως οι παράνομες προσβάσεις λογαριασμών, οι συνεχιζόμενες απειλές, η παράνομη εξαργύρωση αξιών σεATM, οι επιθέσεις σε υποδομές cloud, η κρυπτογράφηση, η κυβερνοτρομοκρατία και οι κρατικές επιθέσεις.

Εσωτερικές Απειλές

Όπως και στην πιο συνηθισμένη περίπτωση, όπως και σε όλους τους άλλους κλάδους Υποδομής Ζωτικής Σημασίας, οι χρηματοπιστωτικές υπηρεσίες ενδέχεται επίσης να υποφέρουν από απειλές εκ των εσω. Αυτές οι απειλές μπορεί να προέρχονται από πρώην ή τρέχοντες υπαλλήλους και μέλη οργανωμένου εγκλήματος. Οι απειλές των εσωτερικών παραγόντων ενδέχεται να έχουν σημαντικό αντίκτυπο στη φήμη του εμπορικού σήματος των χρηματοπιστωτικών ιδρυμάτων και να δημιουργούν ανησυχίες, δεδομένου ότι οι εν λόγω υπάλληλοι έχουν συνήθως καλή γνώση των συστημάτων και έχουν άμεση πρόσβαση στην υποδομή και τις υπηρεσίες. Επιπλέον, οποιοσδήποτε ενδιαφερόμενος (υπάλληλος, ανάδοχος, προμηθευτής ή συνεργάτης) θα μπορούσε να θέσει σε κίνδυνο την ασφάλεια της εταιρείας, ενεργώντας τόσο εκ προθέσεως ή ακούσια, ακόμη και με τη χρήση προσωπικών συσκευών αποθήκευσης USB.

2.4.2 Κρίσιμα στοιχεία για προστασία

Τα καταθετικά ιδρύματα, μέσω των παρόχων υπηρεσιών τεχνολογίας, αποτελούν την κύρια είσοδο στον τομέα για πολλούς μεμονωμένους πελάτεςόταν πραγματοποιούν συναλλαγές σε όλη την υποδομή πληρωμών, συμπεριλαμβανομένων ηλεκτρονικών συστημάτων μεταφοράς μεγάλης αξίας, πλατφόρμες διακανονισμού

Στο χρηματοπιστωτικό τομέα χρησιμοποιούνται τέσσερις βασικές κατηγορίες δικτύων:

- Δημόσιο, το οποίο χρησιμοποιείται κυρίως για την αλληλεπίδραση των πελατών;
- Μισθωμένα δίκτυα, τα οποία χρησιμοποιούνται για πρόσβαση
- «Επαγγελματικά» δίκτυα
- Οι μισθωμένες / ιδιωτικές (ιδιωτικές) γραμμές συνήθως συνδέουν τα κεντρικά γραφεία με τοπικά καταστήματα ή με κέντρα δεδομένων. παρέχει γραμμές που σχετίζονται με μια υπηρεσία ή μια πλατφόρμα.

Οι χρηματοπιστωτικές υπηρεσίες υπήρξαν παραδοσιακά επιρρεπείς στη χρήση τρίτων για την άσκηση δραστηριοτήτων της επιχειρησιακής τους αλυσίδας αξίας, γεγονός που συνεπάγεται λειτουργικό κίνδυνο εξαιτίας της αποτυχίας της τεχνολογίας, ανεπαρκούς υποδομής ή τυχόν καθυστέρηση στην παροχή υπηρεσιών πληροφορικής από τον πάροχο υπηρεσιών.

Μια άλλη σημαντική πτυχή που μπορεί να δημιουργήσει κίνδυνο για την κατάχρηση των χρηματοοικονομικών πληροφοριών είναι η τραπεζική υπηρεσία κινητής τηλεφωνίας, η οποία συνεπάγεται την πρόσβαση των δικαιούχων στους λογαριασμούς τους για τον έλεγχο των υπολοίπων και τη μεταφορά χρημάτων από τους λογαριασμούς τους χρησιμοποιώντας μια κινητή συσκευή. Οιχαμένες / κλεμμένεςσυσκευές, οι ιοί και οι κακόβουλες εφαρμογές αποτελούν πραγματικές απειλές για τον τελικό χρήστη, ενώ τα χρηματοπιστωτικά ιδρύματα συνεργάζονται με τεχνικές και άλλες μεθόδους για την προστασία των δεδομένων λογαριασμών.

Το κρίσιμο πλαίσιο των χρηματοπιστωτικών υπηρεσιών δεν αποτελείται μόνο από υποδομές, αλλά κι από διαδικασίες. Ο εντοπισμός παραγόντων (βασικών υποδομών, διαδικασιών και θεσμών) που είναι υπεύθυνοι για την εκτέλεση κρίσιμων ενεργειών για τον τομέα είναι απαραίτητος για να εξασφαλιστούν ταχείες και κατάλληλες αντιδράσεις και αντίμετρα αντιμετώπισης διαταραχών. Αυτό είναι το σκεπτικό που προέκυψε από την ανάγκη του ENISA να συμπεριληφθεί ολόκληρη η αλυσίδα εφοδιασμού ως μέρος των βασικών μέτρων ασφαλείας.

Ο ENISAεπισημαίνει επίσης την έλλειψη ειδικευμένου και ικανού προσωπικού στελέχωσης στον τομέα της ασφάλειας ΤΠ στον τομέα των χρηματοπιστωτικών υπηρεσιών, η οποία οδηγεί πολλούς οικονομικούς φορείς να συνάπτουν συμβάσεις με εξωτερικούς «ειδικούς» για την εξασφάλιση των υποδομών και των επικοινωνιών τους σε μια κρίσιμη εξέλιξη των καθηκόντων τους βάσει συμφωνιών μη δημοσιοποίησης.

Σύμφωνα με την έκθεση του ENISA "Ασφαλής Χρήση του CloudComputing στον Τομέα Οικονομικών" (www.enisa.europa.eu, 2020), η ευρωπαϊκή βιομηχανία χρηματοπιστωτικών υπηρεσιών βρίσκεται ακόμη στα αρχικά στάδια της υιοθέτησης του νέφους (cloud). Επιπλέον, οι υπηρεσίες που

απαιτούνται συχνότερα από χρηματοπιστωτικούς οργανισμούς από δημόσιους παρόχους υπηρεσιών νέφους είναι η διαχείριση ηλεκτρονικού ταχυδρομείου.Η μελέτη τουENISAS δείχνει τη συνεχιζόμενη ανησυχία για θέματα ασφάλειας που σχετίζονται με το σύννεφο, κυρίως απώλεια ελέγχου των δεδομένων, έλεγχος λογαριασμού χρήστη, κλείδωμα παρόχου, αποτυχία απομόνωσης, συμμόρφωση και νομικά ζητήματα, εμπιστευτικότητα δεδομένων, ακεραιότητα, διαθεσιμότητα, ασφαλής διαγραφή, , έλλειψη στοιχείων ελέγχου, έλλειψη διαφάνειας, απώλεια δεδομένων, παραβίαση δεδομένων, παρακολούθηση / καταγραφή δραστηριοτήτων των χρηστών και έλλειψη δυνατοτήτων εγκληματολογίας.

2.5 Βιομηχανία τροφίμων

2.5.1Επισκόπησηκαιχαρακτηριστικά

Στις επιχειρήσεις τροφίμων και ποτών, καθώς και στα συστήματα παραγωγής τροφίμων και γεωργίας, οι τεχνολογικές εξελίξεις είναι ζωτικής σημασίας για την επιτυχή λειτουργία τους, ενώ συγχρόνως ο κίνδυνος των απειλών στον κυβερνοχώρο και της απάτης αυξάνεται τα τελευταία χρόνια.

Όπως και στους περισσότερους από τους τομείς που περιγράφονται στην έκθεσή μας, η τυποποίηση των συστημάτων πληροφορικής είναι ζωτικής σημασίας και για τον τομέα των τροφίμων. Εάν ένα συγκεκριμένο σύστημα υποφέρει από μια γνωστή αδυναμία, τότε μπορεί εύκολα να εξαπλωθεί μέσω ολόκληρου του δικτύου επιχειρήσεων βιομηχανιών τροφίμων δημιουργώντας πολλαπλές επιθέσεις. Για παράδειγμα, η διασύνδεση μεταξύ franchises θα μπορούσε να οδηγήσει σε ένα ελάττωμα ασφαλείας για τη δημιουργία μιας αλυσίδας επιθέσεων στον κυβερνοχώρο σε όλους τους κλάδους πολλαπλασιάζοντας έτσι τον αντίκτυπο της επίθεσης. Ένα υψηλό ποσοστό επιχειρήσεων που έχουν δεχτεί επιθέσεις σε αυτόν τον τομέα, προέρχονται μέσα από την επιχείρηση κι έχει ως αποτέλεσμα μεγάλες οικονομικές απώλειες.

Εκτός από την οικονομική ζημία, η εκ προθέσεως μόλυνση του εφοδιασμού σε τρόφιμα θα μπορούσε να προκαλέσει βλάβη ή ακόμη κι απώλεια ανθρώπινης ζωής. Περίπου δύο εκατομμύρια άνθρωποι ετησίως, τα περισσότερα παιδιά, πεθαίνουν από τροφικές ή υδατογενείς ασθένειες και πάνω από το ένα τρίτο ή περίπου 1,3 δισεκατομμύρια τόνοι των τροφίμων που παράγονται για κατανάλωση από τον άνθρωπο κάθε χρόνο χάνονται ή αλλοιώνονται. Στον τομέα των τροφίμων, η χρήση συστημάτων ICS, όπως το SCADA, αυξάνει τον κίνδυνο επιθέσεων στον κυβερνοχώρο. Για παράδειγμα, εάν οι hackers αποκτήσουν πρόσβαση στο δίκτυο ενός προμηθευτή τροφίμων, θα μπορούσαν να εισάγουν επικίνδυνες

ποσότητες χημικών ουσιών στο τρόφιμο. Ακόμη και η δυνατότητα απομακρυσμένης απενεργοποίησης των συστημάτων ψύξης που είναι ζωτικής σημασίας για τη διατήρηση της καλής κατάστασης των τροφίμων μπορεί να είναι καταστροφική για τον τομέα ζωτικής σημασίας Τροφίμων.

2.5.1Κρίσιμα στοιχεία για προστασία

Τα πιο συνηθισμένα συστήματα στις ΚΥ τροφίμων είναι ICSκαιSCADA συστήματα, Κατανεμημένα Συστήματα Ελέγχου (DCS) και προγραμματιζόμενοι λογικοί ελέκτές (PLC). Αυτά τα συστήματα ελέγχου συμβάλλουν στη ρύθμιση και διαχείριση των διαφόρων κατανεμημένων περιουσιακών στοιχείων στη διαδικασία παραγωγής. Τα τελευταία χρόνια τα ICS ήταν ως επί το πλείστον απομονωμένα, λειτουργούσαν με υλικό ειδικού σκοπού και αναπτύχθηκαν με ειδικό λογισμικό επίσης. Σήμερα η τάση κάθε επιχείρησης είναι να χρησιμοποιεί λογισμικό ευρείας χρήσης και να αντικαταστήσει αυτά τα παραδοσιακά ICS με άμεσα διαθέσιμες και οικονομικά αποδοτικότερες λύσεις.

Αυτά τα νέα συστήματα ενθαρρύνουν την εταιρική συνδεσιμότητα και περιλαμβάνουν δυνατότητες απομακρυσμένης πρόσβασης, οι οποίες συνάδουν με τις βέλτιστες πρακτικές για αποδοτικότητα, καινοτομία και ανάπτυξη της βιομηχανίας. Ωστόσο, η διασύνδεση όλων αυτών των ICS αποτελεί ευκαιρία για κακόβουλες δραστηριότητες με επιβλαβείς συνέπειες. Ορισμένες πιθανές απειλέγγια τοντομέα ενδέχεται να περιλαμβάνουν:

- Αποκλεισμός ή καθυστέρηση ροής πληροφοριών μέσω δικτύων ICS (π.χ. σε περίπτωση επίθεσης DDoS)
- Μπορούν να πραγματοποιηθούν μη εξουσιοδοτημένες αλλαγές σε οδηγίες, εντολές ή όρια συναγερμού που θα μπορούσαν ενδεχομένως να καταστρέψουν, να εξαφανίσουν ή να απενεργοποιήσουν τον εξοπλισμό
- Οι υπεύθυνοι συστημάτων μπορούν να μεταδίδουν ανακριβείς πληροφορίες, οδηγώντας έτσι σε ψευδείς συναγερμούς και ακατάλληλες διορθωτικές ενέργειες
- Τροποποίηση λογισμικού ή ρυθμίσεων ICS ή μόλυνσης λογισμικού ICS με κακόβουλο λογισμικό

2.6 Υγεία

2.6.1 Επισκόπησηκαιχαρακτηριστικά

Η προστασία του τομέα της υγειονομικής περίθαλψης είναι πολύ σημαντική για τη διεθνή οικονομία και την ανθρώπινη ζωή. Η προστασία περιλαμβάνει δράσεις για την προστασία όλων των περιουσιακών στοιχείων της υγειονομικής περίθαλψης, των ψηφιακών συστημάτων και των προσωπικών δεδομένων από την έκθεση.

Σύμφωνα με έρευνα της Sophos (www.blogs.sophos.com, 2016), ο τομέας της υγειονομικής περίθαλψης είχε ένα από τα χαμηλότερα ποσοστά κρυπτογράφησης δεδομένων, ενώ μόνο το 31% των οργανισμών υγειονομικής περίθαλψης ανέφερε εκτεταμένη χρήση κρυπτογράφησης, ενώ το 20% δήλωσε ότι δεν χρησιμοποιούν κρυπτογράφηση καθόλου. Πέντε από τις οκτώ μεγαλύτερες παραβιάσεις της υγειονομικής περίθαλψης από τις αρχές του 2010 - εκείνες με περισσότερα από ένα εκατομμύριο αρχεία έρχονται σε κίνδυνο—πραγματοποιήθηκε κατά τη διάρκεια των πρώτων έξι μηνών του 2015. Στην πραγματικότητα, περισσότερα από 100 εκατομμύρια αρχεία υγειονομικής περίθαλψης αναφέρθηκαν σε κίνδυνο το 2015 (www.nakedsecurity.sophos.com, 2019).

Τα αρχεία υγείας περιέχουν αριθμούς κοινωνικής ασφάλισης, αριθμούς φαρμάκων, αριθμούς πιστωτικών καρτών, ηλεκτρονικό ταχυδρομείο και φυσικές διευθύνσεις και γενικά πολλά προσωπικά δεδομένα του ασθενούς. Οι επιτιθέμενοι επιδιώκουν την πρόσβαση σε αυτές τις πληροφορίες που μπορούν να χρησιμοποιηθούν για την κλοπή της ταυτότητας και την απάτη.

2.6.2 Κρίσιμα στοιχεία για προστασία

Τα νοσοκομεία και οι κλινικές στον κόσμο γίνονται όλο και πιο προηγμένες από την άποψη της τεχνολογίας. Ο τομέας της υγείας χρησιμοποιεί μια ποικιλία ψηφιακών συστημάτων, για παράδειγμα, για να ικανοποιήσει τις απαιτήσεις του προσωπικού και των ασθενών για πρόσβαση σε ιατρικά αρχεία σε πραγματικό χρόνο (αποτελέσματα των εξετάσεων, επερχόμενες εξετάσεις κ.λπ.), την παρακολούθηση της κατάστασης του ασθενούς και τη χρήση φαρμάκων, τη διασφάλιση της ασφάλειας στις νοσοκομειακές υποδομές, τη διασφάλιση της ιδιωτικής ζωής στα προσωπικά δεδομένα των ασθενών, την άμεση αντίδραση σε καταστάσεις έκτακτης ανάγκης.

Έχουν εντοπιστεί πολυάριθμα κρίσιμα στοιχεία που πρέπει να προστατεύονται και να αναφέρονται. Μερικά από αυτά περιλαμβάνουν:

- Κάμερες επιτήρησης που εξασφαλίζουν ασφάλεια στις υποδομές του νοσοκομείου.

- Συστήματα ελέγχου πρόσβασης όπως βιομετρικοί έλεγχοι που επαληθεύουν ταυτότητα για ασφαλή πρόσβαση σε ηλεκτρονικά συστήματα και εξασφαλίζουν εξουσιοδοτημένη πρόσβαση στα νοσοκομειακά κτίρια.
- Ενεργοί αισθητήρες RFID για τη θερμοκρασία και το αέριο
- Εξοπλισμός ψυχρής παραγωγής, λέβητες και κλιματιστικά
- Σύστημα κλήσεων νοσηλευτών που βασίζεται σε smartphones
- Βάσεις δεδομένων που αποθηκεύουν ιατρικά αρχεία ασθενών και βίντεο από κάμερες παρακολούθησης.
- Κάθε δίκτυο μετάδοσης δεδομένων (Wifi, κεραίες RF, IPTV, VOIP)

2.7 Μεταφορές

2.7.1 Επισκόπιση και χαρακτηριστικά

Στις μεταφορές, η νέα τεχνολογία δημιουργεί απίστευτες ευκαιρίες για τη βελτίωση της ασφάλειας και της αποδοτικότητας των αεροπλάνων, των αεροδρομίων, των τρένων, των σιδηροδρόμων, των οχημάτων, των αυτοκινητοδρόμων και του θαλάσσιου τομέα. Ωστόσο, οι νέες τεχνολογίες και η αυξανόμενη συνδεσιμότητα αντιπροσωπεύουν επίσης νέες προκλήσεις στον τομέα της ασφάλειας και της ασφάλειας στον κυβερνοχώρο. Τα συστήματα μεταφορών έχουν γίνει όλο και πιο ψηφιακά, με ένα ευρύ φάσμα δεδομένων που διακινούνται μεταξύ των συστημάτων, παρακολουθώντας και παρακολουθώντας τόσο τα ψηφιακά όσο και τα φυσικά δίκτυα. Καθώς συνδέονται περισσότερες συσκευές και συστήματα ελέγχουσε απευθείας σύνδεση, θα εμφανιστούν περισσότερες αδυναμίες και απειλές στον κυβερνοχώρο, αυξάνοντας τις δυνατότητες διακοπής των κανονικών λειτουργιών**Error! Bookmark not defined.**.

Αερομεταφορά

Στην αεροπορική βιομηχανία, η τεχνική πρόοδος στα συστήματα πλοήγησης και στη σχεδίαση των αεροσκαφών έχει μειώσει τις πιθανότητες ενός ατυχήματος.Ωστόσο, η αυξανόμενη εξάρτηση από τους υπολογιστές δημιουργεί μια διαφορετική απειλή. Καθώς τα αεροσκάφη τείνουν να γίνουν πλήρως αυτόνομα και η αυτοματοποίηση αυξάνεται, οι πιλοτικές πρακτικές και η εκπαίδευση θα πρέπει να προσαρμοστούν σε περίπτωση βλάβης του συστήματος ή παραβίασης της ασφάλειας (www.oliverwyman.com, 2015).

Σιδηροδρομική μεταφορά

Ο κλάδος των σιδηροδρόμων εξαρτάται επίσης σε μεγάλο βαθμό από την πληροφορική και τον αυτοματισμό. Τα συστήματα που ελέγχουν την κίνηση των αμαξοστοιχιών, παρέχουν ισχύ στο δίκτυο, ελέγχουν την υποδομή σηματοδότησης, αναφέρουν την κατάσταση του τροχαίου υλικού και της συναφούς υποδομής και υποστηρίζουν τον επιχειρησιακό προγραμματισμό και το χρονοδιάγραμμα, ενδέχεται να υπόκεινται σε επιθέσεις στον κυβερνοχώρο.

Οδικές μεταφορές

Στον τομέα αυτό, σημαντικά συστήματα είναι τα ηλεκτρονικά προειδοποιητικά σήματα σε εργοτάξια οδοποιίας και φανάρια. Η αλλαγή του συστήματος χρονισμού των φωτεινών σηματοδοτών μπορεί να σημαίνει πολλούς τραυματισμούς και ενδεχομένως απώλεια ανθρώπινης ζωής. Σήμερα υπάρχει μια τάση από πολλές αυτοκινητοβιομηχανίες προς αυτοκίνητα χωρίς οδηγό που θα αυξήσουν την πιθανή επιφάνεια επίθεσης του τομέα (www.driverless-future.com, 2019).

Ναυτιλιακές μεταφορές

Όπως και οι άλλοι υποτομείς, ο τομέας της ναυτιλίας υποστηρίζει επίσης την οικονομία μέσω της μεταφοράς αγαθών (όπως η ενέργεια, το πετρέλαιο, το φυσικό αέριο, τα τρόφιμα κ.λπ.) και η κυκλοφορία των ανθρώπων. Ο ναυτιλιακός τομέας βασίζεται επίσης στις νέες τεχνολογίες Πληροφορικής και Επικοινωνιών και θα πρέπει επίσης να αντιμετωπίσει τις πτυχές της ασφάλειας στον κυβερνοχώρο όπως και οι υπόλοιποι υποτομείς των μεταφορών.

2.7.2 Κρίσιμα στοιχεία για προστασία

Σε όλους τους τομείς των μεταφορών, οι ψηφιακές τεχνολογίες διαδραματίζουν καθοριστικό ρόλο στη βελτίωση της εξυπηρέτησης πελατών ενώ είναι συνεχώς εκτεθημένες σε επιθέσεις. Τα συστήματα πλοήγησης, εντοπισμού σηματοδότησης, εντοπισμούθέσης, επικοινωνίας και δεδομένων καθώς και στοιχεία διοίκησης επιχειρήσεων συνδέονται μέσω δικτύων και τερματικών απομακρισμένης πρόσβασης τα οποία τα εκθέτουν σε πιθανές επιθέσεις στον κυβερνοχώρο (internet).

Στον τομέα των σιδηροδρόμων είναι σημαντικό να γόνει διάκριση μεταξύ ασφάλειας και προστασίας.Ένα σύστημα είναι ασφαλές όταν είναι απαλλαγμένο από μη αποδεκτούς κινδύνους που καλύπτουν σφάλματα και αποτυχίες.Κάθε σιδηροδρομικό σύστημα που είναι κρίσιμο για την ασφάλεια πρέπει να γίνετε δεκτό από μία εθνική αρχή ασφαλείας. Προστασία είναι η ικανότητα του συστήματος

να υπερασπίζεται και ν ανιχνεύει σκόπιμες επιθέσεις εναντίον του. Είναι απαραίτητο να διατηθεί η ασφάλεια του σιδηροδρομικού συστήματος.

Ενώ η κίνηση των αμαξοστοιχιών πρέπει να πραγματοποιείται με ασφάλεια , απαιτείται επίσης να είναι διαθέσιμο ολόκληρο το σύστημα , προκειμένου να διατηρηθεί ένα ικανοποιητικό επίπεδο λειτουργίας.Από την άλλη πλευρά , η διαθεσιμότητα υποστηρίζει επίσης την ασφάλεια καθώς η έλλειψη ενός κρίσιμου συστήματος (π.χ. φωτεινοί σηματοδότες) μπορεί να αποτελεί απειλή για την ασφάλεια.

Ο τομέας των σιδηροδρόμων χρησιμοποιεί ολοένα και περισσότερα ανοιχτά δίκτυα απικοινωνιών .Αυτό περιλαμβάνει επίσης το επίπεδο ελέγχου της αμαξοστοιχίας που είναι κρίσιμο για την ασφαλή λειτουργία .Επιπλέον σε αυτόν τον τομέα χρησιμοποιούνται όλο και περισσότερα εμπορικά προϊόντα τυποποιημένα – προκατασκευασμένα, τα οποία εκτός από valueformoney , υποστηρίζουν και την ταχύτερη υλοποίηση έργων.

Σε αντίθεση με τα υφιστάμενα δίκτυα , τα οποία βασίζονται σε κλειστή ή ιδιόκτητη υποδομή δικτύωσης ή ακόμη και σε ηλεκτρικά κυκλώματα μεταφοράς πληροφοριών , τα ανοικτά δίκτυα και τα προϊόντα COTS πρέπει να προστατεύονται από τους επιτιθέμενους που επιθυμούν να βλάψουν σκόπιμα την υποδομή. Η ασφάλεια είναι μία συνεχής διαδικάσία , στην οποία οι φορείς επίθεσης και τα αντίμετρα πρέπει να επανεκτιμηθούν σε τακτική βάση , καθώς ανακαλύπτονται νέες ευπάθειες με τη πάροδο του χρόνου. Ο τομέας των θάλλάσιων μεταφορών κι οι συναφείς πτυχές της ασφάλειας στοinternet εντοπίστηκαν στην αντίστοιχη έκθεση του ENISA (ec.europa.eu, 2009). Η έκθεση επισημαίνει ότι η τεχνολογία των Η έκθεση επισημαίνει ότι η τεχνολογία των ICTχρησιμοιποιείται μεταξύ άλλων , για τη στήριξη των θαλάσιων δραστηριοτήτων , όπως η διαχείρηση των λιμένων κι οι εποκοινωνίεςπλοίων.Ο τομέας χρησιμοποιεί συσκευές SCADA, οι οποίες σε ορισμένες περιπτώσεις συνδέονται στο internet κι είναι επιρρεπείς κι ευάλωτες στις επιθέσεις . Οι επιθέσεις σε αυτά τα συστήματα είναι πιθανό να επηρεάσουν τις συσκευές και τις κοινόχρηστες υποδομές (π.χ. βάσεις δεδομένων , συστήματα που φιλοξενούν ευαίσθητες πληροφορίες κ.α.). Επιπλέον η έκθεση παρουσιάζει την έλλειψη ορθής ορακτικής χρήσης κι άλλων προτύπων που θα βοηθούσαν στη θέσπιση διαδικασιών ασφαλείας καθώς και μέτρων που απαιτούνται.

Επιπλέον, μια έκθεση της Επιπλέον, μια έκθεση της EC[1], η οποία διεξήχθη κατόπιν αιτήματος των ευρωπαϊκών αρχών, προσδιορίζει ως κρίσιμα τα εξής:

- ΥψηλήεξάρτησηαπότασυστήματαSCADA, τασυστήματαLAN (ταοποίααπαιτούνται για αερομεταφορές , σιδηροδρομικές μεταφορές καθώς και οδικές μεταφορές
- Υπηρεσίες ασφαλών μηνυμάτων για τη μεταφορά δεδομένων μεταξύ συστημάτων ελέγχου , ραδιοφωνικών συνδέσεων , δορυφορικών συνδέσεων και κινητών τηλεπικοινωνιών (όλα απαιτούνται από την αεροπορική μεταφορά)
- Ραδιοεπικοινωνία με τρένα (απαιτούνται από τη σιδηροδρομική μεραφορά)

2.8 Συστήματα νερού και εγκαταστάσεις

2.8.1 Επισκόπιση και χαρακτηριστικά

Το ασφαλές πόσιμο νερό αποτελεί προϋπόθεση για τη προστασία της δημόσιας υγείας και της ανθρώπινης δραστηριότητας. Τα σώστα επεξεργασμένα λύματα είναι ζωτικής σημασίας για τη πρόληψη ασθενειών και τη προστασία του περιβάλλοντος.Οι κρίσιμες υποδομές , όπως είναι η ενέργεια, οι μεταφορές , τα τρόφιμα , εξαρτώνται από την υποδομή ύδατος για τη διατήρηση της ροής συμαντικών αγαθών κι υπηρεσιών. Η διασφάλιση τηα ασφάλειας αυτής της κρίσιμης υποδομής είναι πολύ σημαντική για τη σύγχρονη ζωή.

Σύμφωνα με το υπουργείο εσωτερικής ασφάλειας (www.dhs.gov, n.d.) της Αμερικής υπάρχουν περίπου 153.000 δημόσια συστήματα πόσιμου νερού και περισσότερα από 16.000 δημόσια συστήματα επεξεργασίας λυμάτων. Περισσότεροι από 80% των Αμερικάνων έχουν πρόσβαση σε πόσιμο νερό από αυτά τα συστήματα και περίπου 75% των Αμερικανών έχουν αποχετευτικό δίκτυο υγειονομικής ταφής επεξεργασμένο από αυτά τα συστήματα αποχέτευσης. Η Ευρωπαϊκή ένωση από την άλλη, έχει εδώ και 30 έτη μία πολιτική για το πόσιμο νερό η οποία διασφαλίζει ότι το νερό που προορίζεται για κατανάλωση από τους πολίτες, είναι ασφαλές σε διαρκή βάση κι αυτό είναι δείγμα υψηλού επιπέδου προστασίας της υγείας. Αυτή η πολιτική, μεταξύ άλλων αποσκοπεί:

- Στη βεβαιότητα ότι η ποιότητα του πόσιμου νερού ελέγχεται συνεχώς βάση των διαδικασιών
- Διασφάλιση αποτελεσματικής παρακοπούθησης, αξιολόγησης και επιβολής της ποιότητας του πόσιμου νερού.

2.8.2 Κρίσιμα στοιχεία για προστασία

Τα βιομηχανικά συστήματα ελέγχου όπως SCADA, PLCs και DCS χρησιμοποιούνται ευρέως σε εγκαταστάσεις ύδρευσης και αποχέτευσης για τη μεγιστοποίηση των πόρων και την παρακολούθηση των λειτουργιών. Τα συστήματα ICS εκτελούν επίσης καταγραφή δεδομένων, συναγερμούς και διαγνωστικές λειτουργίες, έτσι ώστε να μπορούν να λειτουργούν μεγάλα και πολύπλοκα συστήματα διεργασιών με ασφαλή τρόπο που διατηρούνται κεντρικά από το υπεύθυνο προσωπικό.

Παρακάτω συνοψίζουμε μερικά βασικά στοιχεία ενός τυπικού ICS σε μια εγκατάσταση επεξεργασίας και διανομής νερού. Τα κύρια στοιχεία ελέγχου που χρησιμοποιούνται στον τομέα των υδάτων είναι τα ακόλουθα:

- Κεντρικός σταθμός ελέγχου: Αυτή είναι η κύρια μονάδα του ICS που λειτουργεί παράλληλα με τους τοπικούς επεξεργαστές που βρίσκονται σε απομακρυσμένες περιοχές πεδίου. Οι διακομιστές εισόδου / εξόδου χρησιμοποιούνται για τη συλλογή, την προσωρινή αποθήκευση και την παροχή πρόσβασης σε πληροφορίες επεξεργασίας από τους τοπικούς επεξεργαστές. Οι κεντρικοί σταθμοί ελέγχου χρησιμοποιούν έναν ή περισσότερους κεντρικούς υπολογιστές για να παρέχουν τις γραφικές οθόνες καθώς και την απαραίτητη υπολογιστική και δικτυακή ιπποδύναμη.
- Διεπαφές ανθρώπου μηχανής: όπως στην περίπτωση του τομέα της ενέργειας, επιτρέπει στο προσωπικό να παρακολουθεί την κατάσταση μίας διαδικασίας υπό έλεγχο, να τροποποιεί τις ρυθμίσεις ελέγχου και να παρακάμπτει χειροκίνητα τις διαδικασίες αυτόματου ελέγχου σε περίπτωση έκτακτης ανάγκης. Εμφανίζει επίσης πληροφορίες σχετικά με την κατάσταση της διαδικασίας, πληροφορίες ιστορικού, αναφορές και άλλες πληροφορίες σε φορείς εκμετάλλευσης, χειριστές, διαχειριστές, επιχειρηματικούς συνεργάτες και άλλους εξουσιοδοτημένους χρήστες.
- Τοπικοί επεξεργαστές: Οι απομακρυσμένοι τερματικοί σταθμοί (RTUs) και οι ευφυείς ηλεκτρονικές συσκευές (IED), επιτρέπουν τον αυτόματο έλεγχο των οργάνων επεξεργασίας και του εξοπλισμού λειτουργίας. Αυτές οι συσκευές αποκτούν δεδομένα, επικοινωνούν με άλλες συσκευές και εκτελούν τοπική παρακολούθηση, επεξεργασία και έλεγχο
- Όργανα και Λειτουργικός Εξοπλισμός: παρέχουν μετρήσεις σε απευθείας σύνδεση και εκτός σύνδεσης χλωρίου, διαλυμένου οξυγόνου, χρώματος / θολερότητας, αγωγιμότητας, pH, πίεσης, στάθμης υγρού, ρυθμού ροής και άλλων κρίσιμων στοιχείων. Σε ορισμένα συστήματα

νερού, οι αισθητήρες επικοινωνούν με τους τοπικούς επεξεργαστές για να ελέγχουν τις λειτουργίες βαλβίδων, αντλιών και αναμικτήρων

2.9 Πυρηνικά

2.9.1 Επισκόπιση και χαρακτηριστικά

Οποιαδήποτε υποδομή που παρέχει παρακολούθηση ή λειτουργικές δυνατότητες για την αποτελεσματική λειτουργία του Πυρηνικού τομέα μπορεί να υποστεί επιθέσεις. Τα σημερινά συστήματα στον πυρηνικό τομέα χρησιμοποιούν κοινά πρότυπα για πρωτόκολλα επικοινωνίας και βασίζονται σε μεγάλο βαθμό στο διαδύτκυο, σε σύγκριση με τα συστήματα των προγόνων τους που λειτουργούσαν σε απομονωμένα περιβάλλοντα και συνήθως βασίζονταν σε ιδιωτικό λογισμικό, υλικό και τεχνολογίες επικοινωνιών. Πολλά κυβερνητικά συστήματα που χρησιμοποιούνται σήμερα στον πυρηνικό τομέα συνδέονται στο Διαδίκτυο προκειμένου να αυξηθεί η συνδεσιμότητα και το επίπεδο διαλειτουργικότητας των πληροφοριών που απαιτείται μεταξύ των σύγχρονων υποδομών. Τα συστήματα που χρησιμοποιούνται για τη λειτουργία του πυρηνικού σταθμού ηλεκτροπαραγωγής συχνά απομονώνονται από εξωτερικά δίκτυα και άλλα συστήματα. Ωστόσο, τα τυποποιημένα λειτουργικά συστήματα όπως τα Windows ή το UNIX χρησιμοποιούνται όλο και περισσότερο σε άλλους τομείς των εγκαταστάσεων. Αυτά μπορεί να συνδέονται με απομακρυσμένα συστήματα μέσω ιδιωτικών δικτύων που παρέχονται από εταιρείες τηλεπικοινωνιών.

2.9.2 Κρίσιμα στοιχεία για προστασία

Τα Βιομηχανικά Συστήματα Ελέγχου (ICS) στα πυρηνικά εργοστάσια είναι τα ζωτικά συστατικά που επηρεάζουν κάθε πτυχή της λειτουργίας των εγκαταστάσεων. Τα στοιχεία και οιλειτουργίεστους περιλαμβάνουν τα ακόλουθα:

- Αισθητήρες που αλληλεπιδρούν με τις φυσικές διεργασίες μέσα σε μια μονάδα και λαμβάνουν συνεχώς μετρήσεις φυσικών μεταβλητών όπως θερμοκρασία, πίεση και ροή.

- Συστήματα ελέγχου, ρύθμισης και ασφάλειας που επεξεργάζονται δεδομένα μέτρησης για τη διαχείριση των λειτουργιών των εγκαταστάσεων, βελτιστοποιούν την απόδοση των εγκαταστάσεων.

- Συστήματα επικοινωνίας για μεταφορά δεδομένων και πληροφοριών μέσω καλωδίων, οπτικών ινών και ασύρματων δικτύων.

- Διεπαφές ανθρώπινου συστήματος για την παροχή πληροφοριών και την παροχή δυνατότητας αλληλεπίδρασης με το προσωπικό χειρισμού των εγκαταστάσεων.

- Συστήματα παρακολούθησης και διάγνωσης που παρακολουθούν σήματα αισθητήρων για ανωμαλίες.

- Ενεργοποιητές (π.χ. βαλβίδες και κινητήρες) που λειτουργούν από τα συστήματα ελέγχου και ασφάλειας για την προσαρμογή των φυσικών διεργασιών της εγκατάστασης.

- Ενδείξεις κατάστασης των ενεργοποιητών (π.χ. εάν οι βαλβίδες είναι ανοιχτές ή κλειστές και εάν οι κινητήρες είναι ενεργοποιημένοι ή απενεργοποιημένοι) παρέχοντας σήματα για αυτόματη και χειροκίνητη ρύθμιση.

Τα αναφερόμενα στοιχεία θα πρέπει να προστατεύονται επαρκώς από κάθε είδους επιθέσεις που αποσκοπούν στην τροποποίηση, καταστροφή ή συμβιβασμό στην ακεραιότητα ή την εμπιστευτικότητα δεδομένων ή λογισμικού. Θα πρέπει να υπάρχουν κατάλληλοι μηχανισμοί για την άρνηση πρόσβασης σε συστήματα, υπηρεσίες και δεδομένα και ως εκ τούτου μπορεί να έχουν καταστροφικές επιπτώσεις στη λειτουργία συστημάτων, δικτύων και εξοπλισμού.

2.10 Υπηρεσίες έκτακτης ανάγκης

2.10.1 Επισκόπηση και χαρακτηριστικά

Ο τομέας των υπηρεσιών έκτακτης ανάγκης αποσκοπεί στην προστασία της περιουσίας και του περιβάλλοντος, στη διάσωση ανθρώπινων ζωών, στην παροχή βοήθειας στις κοινότητες που πλήττονται από καταστροφές και στην ενίσχυση της ανάκαμψης σε καταστάσεις έκτακτης ανάγκης. Συνήθως ο τομέας αυτός αποτελείται από πέντε διαφορετικούς κλάδους οι οποίοι είναι:

- Επιβολή του Νόμου,
- Υπηρεσίες πυρασφάλειας και έκτακτης ανάγκης,
- Ιατρικές υπηρεσίεςέκτακτης ανάγκης,
- Διαχείριση έκτακτης ανάγκης και
- Δημόσια Έργα.

Οι υπηρεσίες έκτακτης ανάγκης συνδέονται στενά με τις επικοινωνίες έκτακτης ανάγκης, οι οποίες, σύμφωνα με την έκθεση του ENISA με τίτλο "Απολογισμός επειγόντων επικοινωνιών" (www.enisa.europa.eu, n.d.)αποτελούν ένα σύνολο συστημάτων και διαδικασιών που επιτρέπουν στις υπηρεσίες έκτακτης ανάγκης να διαχειρίζονται την αντιμετώπιση περιστατικών, καταστροφών και κρίσεων. Η έκθεση προσδιορίζει επίσης τα καίρια στοιχεία που είναι κρίσιμα κάθε φορά που συμβαίνει ένα περιστατικό και θα αναφερθούν στην παρακάτω ενότητα.

2.10.2 Κρίσιμα στοιχεία για προστασία

Σύμφωνα με την προηγούμενη κατάτμηση του τομέα που παρέχεται στις 5 κατηγορίες, υπάρχει ένας κατάλογος στοιχείων για προστασία και μεγάλης σημασίας για καθένα από αυτά. Επομένως, σε έναν υποτομέα έχουν εντοπιστεί τα ακόλουθα κρίσιμα στοιχεία (www.dhs.gov, n.d.):

- Επιβολήτουνόμου:
  - Η απώλεια των γραμμών επικοινωνίας μπορεί να οδηγήσει σε υποβάθμιση της απόκρισης της υπηρεσίας έκτακτης ανάγκης.
  - Επιπλέον, ανακριβείς πληροφορίες από δημόσια συστήματα ειδοποίησης και προειδοποίησης μπορεί να οδηγήσουν σε σπατάλη πόρων και δημιουργία δημόσιας σύγχυσης και πανικού.
- Υπηρεσίες πυρασφάλειας και έκτακτης ανάγκης:

- Η πιθανή επίθεση στις γραμμές επικοινωνίας έκτακτης ανάγκης μπορεί να προκαλέσει την αδυναμία του ευρύτερου κοινού να έχει πρόσβαση στην υπηρεσία και την ανικανότητα του τμήματος να αντιδράσει αποτελεσματικά.

- Ιατρικές υπηρεσίεςέκτακτης ανάγκης:
  - Η έλλειψη διαθεσιμότητας στη βάση δεδομένων προκαλεί διακοπή της ικανότητας αποστολής, η οποία μπορεί να οδηγήσει σε αδυναμία πρόσβασης στο θέμα που επηρεάζει τις διαδικασίες αντιμετώπισης καταστάσεων έκτακτης ανάγκης.
  - Η αλλοίωση κρίσιμων πληροφοριών μπορεί να οδηγήσουν σε βραδύτερο συνολικό χρόνο απόκρισης και αδυναμία του εσωτερικού προσωπικού να εμπιστευτεί την ακεραιότητα των δεδομένων
- Διαχείριση έκτακτης ανάγκης:
  - Λανθασμένη λειτουργία συστήματος δημόσιας ειδοποίησης και προειδοποίησης,
  - απώλεια γραμμών επικοινωνίας και
  - η υπερφόρτωση στο δίκτυο επικοινωνιών μπορεί να προκαλέσει ψευδείς συναγερμούς, σπατάλη πόρων, απώλεια υπηρεσιών και αναποτελεσματικότητα λειτουργίας
- Δημόσιες Υπηρεσίες: η απώλεια γραμμών επικοινωνίας και τα αποκλεισμένα συστήματα παρακολούθησης ενδέχεται να προκαλέσουν πανικό και να βλάψουν τους πολίτες.

Ανά υποκατηγορία χρησιμοποιείται η ακόλουθη υποδομή για κυβερνοχώρο και πρέπει να προστατεύεται από απειλές και επιθέσεις στον κυβερνοχώρο:

Επιβολή του νόμου:

Συστήματα Ασφαλείας και Επιτήρησης, Προειδοποιητικά Συστήματα, Συστήματα Πληροφορικής, Ψηφιακά Εργαλεία και Συστήματα,Δίκτυα και συστήματα ποινικής δικαιοσύνης, διαδίκτυο, τηλεπικοινωνιακά συστήματα και ραδιοφωνική υποδομή.

Υπηρεσίες πυρασφάλειας και έκτακτης ανάγκης:

Συστήματα Τηλεπικοινωνιών, Διαδίκτυο, Τηλεπικοινωνιακά Συστήματα, Υποδομή Ραδιοφώνου, Συστήματα Πυρανίχνευσης και Ιατρικών Συναγερμών, Συστήματα Ασφαλείας Προειδοποίησης Προσωπικού, Εργαλεία Μοντελοποίησης και Προσομοίωσης

Ιατρικές υπηρεσίες έκτακτης ανάγκης:

Διαδίκτυο, Τηλεπικοινωνιακά Συστήματα, Υποδομή Ραδιοφώνου, Συστήματα Συναγερμού Πυρκαγιάς και Ιατρικής, Εργαλεία Μοντελοποίησης και Προσομοίωσης

Διαχείριση έκτακτης ανάγκης:

Συστήματα Προειδοποίησης, Γεωπεριφερειακά Εργαλεία και Συστήματα, Διαδίκτυο, Τηλεπικοινωνιακά Συστήματα, Υποδομή Ραδιοεπικοινωνιών, Εργαλεία Μοντελοποίησης και Προσομοίωσης

Δημόσια Έργα:

Συστήματα Προειδοποίησης, Γεωπεριφερειακά Εργαλεία και Συστήματα, Διαδίκτυο, Τηλεπικοινωνιακά Συστήματα, Υποδομή Ραδιοφώνου

Τα προηγούμενα στοιχεία στις 5 κατηγορίες που αναφέρθηκαν είναι τα κυριότερα από αυτά που προσδιορίζονται στο έγγραφο ENISA, τα οποία περιλαμβάνουν:

- Εκπομπή: συμπεριλαμβανομένων των ραδιοφωνικών και τηλεοπτικών σημάτων για την ορθή και την λήψη σημαντικών πληροφοριών στο κοινό
- Τηλεφωνία: συμπεριλαμβανομένων συστημάτων φωνής για κατάλληλους διαύλους επικοινωνίας μεταξύ πολιτών και υπηρεσιών έκτακτης ανάγκης
- Διαδίκτυο: συμπεριλαμβανομένων των ηλεκτρονικών επικοινωνιών μέσω ηλεκτρονικού ταχυδρομείου ή φωνητικής τηλεφωνίας μέσω IP (VOIP)
- Δικτύωση δεδομένων: συνήθως ιδιωτικά δίκτυα IP που χρησιμοποιούνται για ηλεκτρονική ανταλλαγή πληροφοριών.
- Ραδιοεπικοινωνία έκτακτης ανάγκης: συμπεριλαμβανομένων ιδιωτικών ραδιοφωνικών εγκαταστάσεων υψηλής ραδιενέργειας και υποδομών που χρησιμοποιούνται από τις υπηρεσίες έκτακτης ανάγκης, οι οποίες χρησιμοποιούνται κυρίως για σκοπούς διαχείρισης σε περίπτωση κρίσης και διάφορα επεισόδια έκτακτης ανάγκης.

Κεφάλαιο 3: Το Διαδίκτυο των πραγμάτων (IoT)

Το διαδίκτυο των πραγμάτων (IoT) είναι μία από τις πιο γρήγορα αναπτυσσόμενες πλατφόρμες για την ψηφιακή οικονομία. Πρόκειται για ένα web δίκτυο, το οποίο συνδέει έξυπνες συσκευές επικοινωνίας, μεταφοράς δεδομένων, νομισματικής ανταλλαγής και λήψης αποφάσεων. Σύμφωνα με διάφορες εκθέσεις (Forbes 2014), τόσο ο αριθμός των καναλιών επικοινωνίας όσο και ο όγκος των δεδομένων που μεταδίδονται αυξάνουν εκθετικά μαζί με τον αριθμό των συσκευών που είναι συνδεδεμένες με αυτό το δίκτυο.

Πολλές ανεπτυγμένες χώρες εφαρμόζουν ή σχεδιάζουν να εφαρμόσουν IoT σε έξυπνες κατοικίες και πόλεις. Για παράδειγμα, η Ιαπωνία παρέχει εξειδικευμένη ευρυζωνική πρόσβαση για την επικοινωνία "συσκευών προς συσκευές", ενώ η Νότια Κορέα κατασκευάζει έξυπνα συστήματα ελέγχου στο σπίτι, τα οποία είναι προσβάσιμα εξ αποστάσεως. Η Ευρώπη από την άλλη πλευρά πρότεινε μια σειρά έργων διαδικτύου και δημιούργησε ένα διεθνές φόρουμ για τα IoT για την ανάπτυξη κοινού στρατηγικού και τεχνικού οράματος για τη χρήση του Ίντερνετ. Η εξάληψη στο διαδίκτυο είναι επίσης εμφανής από τον αριθμό των δημοσιεύσεων που σχετίζονται με τον τομέα. Τοαναπτυσσόμενοδίκτυο IoTπαράγει ένα τεράστιο όγκο δεδομένων που θα πρέπει να υποβληθούν σε επεξεργασία και ανάλυση. Για την επεξεργασία και την ανάλυση πολύ μεγάλων συνόλων δεδομένων-Big Data-ένα νέο πεδίο έρευνας και η σχετική συλλογή μεθόδων και τεχνικών έχει προκύψει τα τελευταία χρόνια. Παρόλο που δεν υπάρχει σαφής ορισμός για τα μεγάλα δεδομένα, ένας χαρακτηριστικός χαρακτήρας που αναφέρεται συνήθως είναι ο "V's": όγκος, ποικιλία, ταχύτητα, μεταβλητότητα και αξία.

Όγκος

Υπάρχουν περισσότερα δεδομένα από ποτέ.Ο όγκος του συνεχίζει να αναπτύσσεται ταχύτερα από ό, τι μπορούμε να αναπτύξουμε κατάλληλα εργαλεία για να το επεξεργαστούμε.

Ποικιλία

Υπάρχουν πολλοί διαφορετικοί και συχνά ασυμβίβαστοι τύποι δεδομένων, όπως δεδομένα κειμένου, δεδομένα αισθητήρων, ηχητικές και βιντεοσκοπημένες εγγραφές, γραφήματα, οικονομικά δεδομένα και στοιχεία για την υγεία.

Ταχύτητα

Τα δεδομένα μπορούν να μεταδίδονται συνεχώς, δηλαδή φθάνουν συνεχώς σε πραγματικό χρόνο και μας ενδιαφέρει να λάβουμε άμεσα χρήσιμες πληροφορίες.

Μεταβλητότητα

Τα δεδομένα έχουν διαφορές στη δομή και την ερμηνεία ανάλογα με τις εφαρμογές.

Αξία

Τα δεδομένα έχουν μια πραγματική επιχειρηματική αξία που δίνει στους οργανισμούς ένα ανταγωνιστικό πλεονέκτημα. Αυτό οφείλεται στην ικανότητα λήψης αποφάσεων βάσει εκτεταμένης ανάλυσης δεδομένων που προηγουμένως είχε θεωρηθεί ότι δεν είναι εφικτή.

Τα δεδομένα του IoT ικανοποιούν τα κριτήρια της κατηγορίας μεγάλων δεδομένων που ορίζεται ως "V". Από πολλούς συγγραφείς προέβλεπε ότι ο μεγάλος αριθμός των συνδεδεμένων αντικειμένων στο IoT θα δημιουργήσει ένα τεράστιο όγκο δεδομένων.Τα δεδομένα που παράγονται από τη διαδικτυακή πύλη είναι μεταβλητά από άποψη δομής, συχνά φθάνουν σε πραγματικό χρόνο και ενδέχεται να είναι αβέβαιης προέλευσης. Αυτές οι μεγάλες ποσότητες δεδομένων απαιτούν μηχανές ταξινόμησης, επεξεργασίας, ανάλυσης και λήψης αποφάσεων για εμπορικά βιώσιμη χρήση. Θα χρειαστεί να αναπτυχθούν τεχνικές που θα μετατρέπουν αυτά τα πρωτογενή δεδομένα σε χρήσιμες γνώσεις.Για παράδειγμα, στον ιατρικό τομέα, οι ακατέργαστες ροές πληροφορίας πρέπει να μετατραπούν σε σημασιολογικά σημαντικές δραστηριότητες όπως η κατανάλωση τροφής, η κακή αναπνοή ή η εμφάνιση σημείων κατάθλιψης που εκτελούνται από ένα άτομο (Stankovic, 2014)

<u>Κεφάλαιο 4:</u> Big Data στους τομείς εφαρμογών του IoT

Big Data στο περιβάλλον IoT είναι μια μεγάλη και ταχύτατα αναπτυσσόμενη περιοχή όπου πολλές διαφορετικές μέθοδοι και τεχνικές μπορούν να παίξουν σημαντικό ρόλο λόγω της ταχείας ανάπτυξης του «Machine Learning», μπορεί να παρατηρηθεί μια δυναμική ανάκαμψη μεθόδων και τεχνολογιών για επεξεργασία πληροφοριών. Στις επόμενες υποενότητες παρουσιάζεται μόνο λίγες από τις δομές ζωτικής σημασίας που αναλύσαμε νωρίτερα και πως οι τομείς «Big Data» & «IoT» συνυπάρχουν αρμονικά στο περιβάλλον των σύγχρονων τεχνολογιών πληροφορικής οι οποίες επιτρέπουν την πρόσβαση στις δομές ζωτικής σημασίας.

4.1 Υγεία – Δομές ζωτικής Σημασίας

Το IoT παρέχει νέες ευκαιρίες για τη βελτίωση των συστημάτων υγεονομικής περίθαλψης συνδέοντας τον ιατρικό εξοπλισμό, τα αντικείμενα και τους ανθρώπους. Οι τεχνολογικές εξελίξεις που συνδέονται με τους ασύρματους αισθητήρες καθιστούν τις υπηρεσίες υγειονομικής περίθαλψης που βασίζονται στο IoT προσβάσιμες ακόμη και σε μεγάλες αποστάσεις. Οι υπηρεσίες υγειονομικής περίθαλψης μέσω διαδικτύου ή οι υπηρεσίες ηλεκτρονικής υγείας (eHealth) είναι μερικές φορές φθηνότερες και πιο άνετες από τη συνηθισμένη επίσκεψηστο γιατρό. Επιπρόσθετα, οι πανταχού παρούσες δυνατότητες αναγνώρισης, ανίχνευσης και επικοινωνίας του IoT σημαίνουν ότι όλες οι οντότητες του συστήματος υγείας (άνθρωποι, εξοπλισμός, φάρμακα κλπ.) μπορούν να παρακολουθούνται συνεχώς. Το Cloud computing, τα μεγάλα δεδομένα και το IoT και η ανάπτυξη αντικειμένων του τομέα πληροφορικής κι επικοινωνιών , μπορούν να συνδυαστούν στη διαμόρφωση της επόμενης γενιάς συστημάτων ηλεκτρονικής υγείας (Suciuetal, 2015). Η επεξεργασία μεγάλων ποσοτήτων ετερογενών ιατρικών δεδομένων, τα οποία συλλέγονται από δίκτυα WSN ή M2M, υποστηρίζει μια μετακίνηση μακριά από την έρευνα που βασίζεται σε υποθέσεις, με στόχο την έρευνα που βασίζεται περισσότερο σε δεδομένα. Οι μεγάλες μέθοδοι αναζήτησης δεδομένων μπορούν να βρουν μοτίβα στα δεδομένα που προέρχονται από την παρακολούθηση και τη θεραπεία συγκεκριμένων συνθηκών υγείας. Έχει περιγραφεί και αξιολογηθεί πρόσφατα ένα λεπτομερές πλαίσιο για τα συστήματα υγειονομικής περίθαλψης που βασίζονται στην ενσωμάτωση του IoT και του cloud computing (Hassan, 2017). Σύμφωνα με αυτή την προσέγγιση, οι ασύρματοι αισθητήρες εγκαθίστανται σε αντικείμενα καθημερινής χρήσης, όπως ρούχα και παπούτσια, για να παρακολουθούνται οι φυσιολογικές παράμετροι κάθε ασθενούς, όπως τα επίπεδα σακχάρου στο αίμα, γλυκόζη αίματος, παλμός και ηλεκτροκαρδιογράφημα. Τα δεδομένα που συλλέγονται στη συνέχεια αποθηκεύονται σε εξατομικευμένους λογαριασμούς σε κεντρικό

διακομιστή. Αυτός ο διακομιστής παρέχει μια σύνδεση μεταξύ του υποσυστήματος IoT και της υποδομής του cloud. Στο νέφος έχουν εγκατασταθεί διάφορα προγράμματα ανάλυσης δεδομένων για να επεξεργαστούν τις πληροφορίες για κλινική παρατήρηση και να ειδοποιήσουν τις επαφές έκτακτης ανάγκης εάν και πότε ενεργοποιείται ένας συναγερμός. Άλλα προγράμματα, όπως οι μηχανές ανάλυσης, εξαγάγουν τα χαρακτηριστικά και ταξινομούν τα δεδομένα για να βοηθήσουν τους επαγγελματίες υγείας να παρέχουν την κατάλληλη ιατρική περίθαλψη (Abawajy&Hassan, 2017)Στον τομέα της κλινικής διαχείρισης, τα κύρια πλεονεκτήματα που παρέχονται από αυτά τα αλληλεπιδρώντα συστήματα περιλαμβάνουν (i) τη βελτίωση της λήψης αποφάσεων σχετικά με την αποτελεσματική θεραπεία, (ii) την έγκαιρη ανίχνευση των σφαλμάτων στη θεραπεία, (iii) τη βελτίωση της εκτίμησης των επιδόσεων των επαγγελματιών του τομέα της ιατρικής , (iv) ανάπτυξη νέων μοντέλων κατακερματισμού και πρόβλεψης που αφορούν στα δεδομένα καταγραφής εταιρικών μονάδων για τα προφίλ των ασθενών, (v) αυτοματοποίηση του συστήματος πληρωμών και έλεγχος του κόστους, και (vi) διαβίβαση πληροφοριών στους κατάλληλους ανθρώπους την κατάλληλη στιγμή . Η διάγνωση θα βελτιωθεί επίσης επειδή κάθε κέντρο υγείας μπορεί να έχει πρόσβαση στις απαιτούμενες πληροφορίες για τον ασθενή ανεξάρτητα από το πού διεξάγονται οι εξετάσεις.Επιπλέον, τα δεδομένα δοκιμών μπορούν να αποθηκευτούν σε πραγματικό χρόνο, επιτρέποντας τη λήψη αποφάσεων από τη στιγμή που ολοκληρώθηκε η δοκιμή. Με τη δραστική μείωση του χρόνου αποθήκευσης και επεξεργασίας, οι εφικτές τεχνικές Big Data μπορούν επίσης να υποστηρίξουν την ερευνητική δραστηριότητα. Οι τεχνολογίες NOSQL που επικεντρώνονται στον ασθενή θα επιτρέπουν επίσης την παρακολούθηση και αποθήκευση δεδομένων που συλλέγονται τόσο από το εσωτερικό όσο και έξω από το σπίτι, με έγκαιρες προειδοποιήσεις σχετικά με τις αλλαγές στην κατάσταση υγείας και τα συστήματα συναγερμού, προσδιορίζοντας την ανάγκη προληπτικής δράσης που οδηγεί σε εξοικονόμηση κόστους μειώνοντας τον αριθμό των επισκέψεων έκτακτης ανάγκης και της διάρκειας των επακόλουθων διαμονών στο νοσοκομείο.

4.2 Τρόφιμα – Δομές ζωτικής Σημασίας

Οι υπάρχουσες αλυσίδες εφοδιασμού τροφίμων είναι πολύ σύνθετες κι ευρέως διεσπαρμένες διαδικασίες που επηρρεάζουν την ανθρώπινη κοινότητα. Αυτή η πολυπλοκότη τα δημιούργησε προβλήματα για τη διαχείρηση της λειτουργικής αποτελεσματικότητας , της ποιότητας και της δημόσιας ασφάλειας των τροφίμων. Οι τεχνολογίες IoT προσφέρουν ελπιδοφόρες δυνατότητες αντιμετώπισης της ανιχνευσιμότητας, της ορατότητας και της δυνατότητας ελέγχου αυτών των προκλήσεων στις αλυσίδες εφοδιασμού τροφίμων ειδικά μέσω της χρήσης τεχνολογιών barcode και συστημάτων ασύρματης παρακολούθησης όπως GPS και RFID σε κάθε στάδιο της διαδικασίας γεωργικής παραγωγής, επεξεργασίας , αποθήκευσης , διανομής και κατανάλωσης. Μια τυπική λύση IoT για αυτές τις αλυσίδες περιλαμβάνει τρία μέρη: συσκευές πεδίου όπως κόμβοι WSNs, αναγνώστες , ετικέτες RFID, τερματικά διεπαφής χρήστη κλπ , συστήματα κορμού όπως βάσεις δεδομένων , διακομιστές και πολλά είδη τερματικών συσκευών που συνδέονται με κατανενημένα δίκτυα υπολογιστών κτλ και επικοινωνιακή υποδομή όπως WLAN, κινητής (κυψέλες) , δορυφορικής , ρεύμαροδότηση , Ethernet,κλπ (Xuetal, 2014)

4.3Ενέργεια– Δομές ζωτικής Σημασίας

Έξυπνο σύστημα τροφοδοσίας

Με την πρόοδο της τεχνολογίας IoT,των έξυπνων συστημάτων και των αναλύσεων Big Data ,οι πόλεις εξελίσσονται και μετατρέπονται σε «έξυπνεςπόλεις» (Stankovic, 2014). Για παράδειγμα τα νοικοκυριά που καταναλώνουν ενέργεια μπορούν να παρακολουθούνται και να αναλύονται σε διαφορετικές χρονικές περιόδους για τη διαχείρηση του κόστους ρεύματος (Rathoreetal, 2017). Πρόσφατες έρευνες έδειξαν ότι η τεχνολογία έξυπνων δικτύων αποτελεί εφικτή λύση που συμβάλλει στον περιορισμό της υπέρβασης των παραδοσιακών συστημάτων ηλεκτρικού δικτύου.

Έξυπνο σπίτι

Οι Stojkoska & Trivodaliev περιέγραψαν και πρότειναν ένα γενικευμένο πλαίσιο για ένα έξυπνο σπίτι που βασίζεται στο IoT (Stojkoska&Trivodaliev, 2017). Το πρόγαμμά τους συνδέει το σπίτι, τις επιχειρήσεις κοινής ωφέλειας και τους παρόχους εφαρμογών σε ένα δίκτυο cloud, με αισθητήρες συνδεδεμένους στο σύστημα έξυπνου δικτύου που συγκεντρώνουν τα δεδομένα από τις έξυπνες οικιακές συσκευές. Καθώς οι περισσότερες επιχειρήσεις κοινής ωφέλειας εφαρμόζουν χρεώσεις χρόνου χρησης, οι πάροχοι εφαρμογών μπορούν να μειώσουν το κόστος χρήσης συνδυάζοντας

συσκευές όπως φορτιστές μταταριών με ψυγεία και φούρνους που μπορεί να ελέγχονται μέσω του internet (Buckletal, 2009). Αυτό ισχύει και για τις ανανεώσιμες πηγές ενέργειας με μετρητές που βασίζονται στο internet κι υπολογίζουν πόση ενέργεια θα χρειαστεί το σπίτι από το ηλεκτρικό δίκτυο.

Έξυπνο περιβάλλον ελέγχου

Πολλές βιομηχανικές επιχειρήσεις έχουν αυστηρές απαιτήσεις όσον αφορά τις συνθήκες εργασίας του εξοπλισμού και τις συνθήκες περιβάλλοντος για προϊόντα υψηλής ποιότητας, ειδικά σε εργοστάσια κατασκευής chip, φαρμακευτικά εργοστάσια και εργοστάσια τροφίμων (Ding, 2010).Στη διαδικασία παραγωγής προϊόντων, πρέπει να συλλέγονται, να αποθηκεύονται και να αναλύονται δεδομένα σε πραγματικές περιόδους λειτουργίας και περιβαλλοντικές συνθήκες, ώστε να εντοπίζονται οι κίνδυνοι και οι ανωμαλίες. Προγνωστικά και τηλεχειριζόμενα συστήματα παραγωγής

4.4 Μεταφορές – Δομές ζωτικής Σημασίας

Η βιομηχανία μεταφορών και εφοδιαστικής αλυσίδας υφίσταται τεράστιες τεχνολογικές αλλαγές που προκλήθηκαν από την εισαγωγή τεχνολογιών παρακολούθησης και ανίχνευσης. Οι τεχνολογίες RFID και NFC μπορούν να χρησιμοποιηθούν για την παρακολούθηση σε πραγματικό χρόνο σχεδόν κάθε συνδέσμου στην αλυσίδα εφοδιασμού, από το σχεδιασμό των βασικών προϊόντων, την αγορά πρώτων υλών, την παραγωγή, τη μεταφορά και αποθήκευση έως τη διανομή, την πώληση ημιπροϊόντων και προϊόντων,επεξεργασίας και εξυπηρέτησης μετά την πώληση (Atzori, 2010). Ειδικότερα, η άμεση παρακολούθηση της παράδοσης πακέτων μειώνει το χρόνο μεταφοράς σε διαφορετικά επίπεδα του συστήματος μεταφοράς, με υπηρεσίες ταχυμεταφορών που παρέχουν άμεση παρακολούθηση μέσω εφαρμογών κινητής τηλεφωνίας. Τα WSNs χρησιμοποιούνται στην εφοδιαστική αλυσίδας που χρησιμοποιεί θερμικές και ψυκτικές μεθόδους γήρανσης για τη μεταφορά ευαίσθητων στην θερμοκρασία προϊόντων (Hsueh&Chang, 2010). Έχει σχεδιαστεί ένα έξυπνο σύστημα ανίχνευσης για την παρακολούθηση της θερμοκρασίας και της υγρασίας μέσα στα φορτηγά ψυγεία χρησιμοποιώντας ετικέτες RFID, αισθητήρες και τεχνολογία ασύρματης επικοινωνίας. Τα WSNs χρησιμοποιούνται επίσης για συστήματα συντήρησης και παρακολούθησης.Για παράδειγμα, η General Electric εφαρμόζει αισθητήρες για την προληπτική συντήρηση των αεριωθούμενων κινητήρων, των στροβίλων και των αιολικών πάρκων. Ομοίως, η American Airlines χρησιμοποιεί αισθητήρες ικανούς να καταγράφουν 30 terabyte δεδομένων ανά πτήση για το σκοπό αυτό. Οι κατασκευαστές αυτοκινήτων τοποθετούν υπέρυθρες, θερμικές πιέσεις και άλλους αισθητήρες για την παρακολούθηση της υγείας ενός αυτοκινήτου, ενώ οι συσκευές GPS παρέχουν πληροφορίες θέσης για τον προσδιορισμό της αυξημένης

κίνησης στους δρόμους κυκλοφορίας και της βοήθειας πλοήγησης (Qinetal, 2013). Η ιδέα των μηχανοκίνητων οχημάτων είναι κεντρική στο σχεδιασμό του μέλλοντος των μεταφορών μας. Τα αυτοκίνητα χωρίς οδηγό συνδέονται με το δίκτυο χρησιμοποιώντας τεχνολογίες WSN για την παροχή δεδομένων από τους αισθητήρες τους και για την λήψη ανατροφοδότησης μετά από ανάλυση δεδομένων. Τα αυτοκίνητα μπορούν να έχουν πρόσβαση σε πληροφορίες από μια βάση δεδομένων με χάρτες και δορυφορικές πληροφορίες για τον εντοπισμό του GPS και τη βελτιστοποίηση της παγκόσμιας κυκλοφορίας και της ζήτησης. Κρίσιμη για την ασφάλεια είναι η επικοινωνία μεταξύ των αυτοκινήτων που κινούνται σε κοντινή απόσταση, με σημαντικά δεδομένα από τους αισθητήρες οράσεως που είναι επεξεργασμένοι επί του σκάφους και σε πραγματικό χρόνο, χρησιμοποιώντας συμπαγείς συσκευές υψηλής απόδοσης όπως οι κάρτες GPU.

Στην υποενότητα αυτή θα κάνουμε μια συσχέτιση διαφόρων εργασιών του τομέα του IoT σε σχέση με τις κρίσιμες υποδομές. Δηλαδή σε ποιές κρίσιμες υποδομές που περιγράφονται στις προηγούμενες ενότητες μπορούν να εφαρμοστούν οι λύσεις/ιδέες των σχετικών αναφορών. Αναμένουμε κάποιες εργασίες να συσχετίζονται με περισσότερες εκ των μία Κρίσιμων Υποδομών. Καλύτερη εικόνα προς τον αναγνώστη της μελέτης μας παραθέτουμε στη συνέχεια μια λίστα με τις ΚΥ που περιγράφηκαν στις προηγούμενες ενότητες.

1. Κλάδος Χημείας
2. Τεχνολογίες πληροφοριών και επικοινωνιών (ΤΠΕ)
3. Ενέργεια
4. Οικονομικές Υπηρεσίες
5. Βιομηχανία τροφίμων
6. Υγεία
7. Μεταφορές
8. Συστήματα νερού κι εγκαταστάσεις
9. Πυρηνικά

Υπηρεσίες έκτακτης ανάγκης

Πολλές αναφορές κάνουν συχνή χρήση των συσκευών IoT με τα Big Data και είναι λογικό μιας και αυτές οι συσκευές σε μεγάλο αριθμό και μεγάλη διάρκεια λειτουργίας (π.χ για πολλούς μήνες ή ακόμα και χρόνια) μπορούν να δημιουργήσουν όγκο δεδομένων που να απαιτούνται ειδικές τεχνικές ώστε να προβεί κάποιος σε αναζήτηση με ουσιαστικά αποτελέσματα. Για παράδειγμα υπάρχουν αναφορές κατά τις οποίες συλλέγονται και αποθηκεύονται Big Data από αισθητήρες σε μεγάλες κατασκευές (π.χ κτίρια, έξυπνα σπίτια) (Psannis E. Kostas, 2017)

Αυτό μπορεί να κλιμάκωθεί σε πόλεις και μεγάλες εγκαταστάσεις άρα υπάρχει μεγάλη συσχέτιση με σχεδόν όλες τις ΚΥ αλλά θεωρούμε μεγαλύτερη συσχέτιση με τις ΚΥ (3, 4, 5, 6, 8, 9). Σε άλλες αναφορές περιγράφονται τρόποι ασφαλούς μεταφοράς των δεδομένων από τους αισθητήρες προς τα σημεία στα οποία πρέπει να αποθηκευτούν και στη συνέχεια να επεξεργαστούν τα δεδομένα αυτά (Psannis E. Kostas and Christos Stergiou, 2017) . Παρόμοιες εργασίες με ευαίσθητα δεδομένα θα μπορούν να έχουν χρήση στις ΚΥ (2, 4, 6, 9, 10) χωρίς να αποκλείουμε και τμήματα των άλλων ΚΥ που όντως πραγματεύονται προσωπικά δεδομένα ή εμπορικές πληροφορίες που δεν πρέπει να πέσουν σε λάθος χέρια. Παρόμοιες εργασίες είναι περισσότερο προσανατολισμένες για ασύρματα δίκτυα (Kostas E. Psannis, 2018) . ΚΥ που χρησιμοποιούν ασύρματα δίκτυα είναι οι 2, 4, 7, και φυσικά οι δομές που περιλαμβάνουν τις υπηρεσίες έκτακτης ανάγκης 10. Παρόμοια με τις εργασίας που αναφέρονταν σε αισθητήρες και Big Data σε κτιριακές εγκαταστάσεις [1]. υπάρχουν και στοχευμένες εργασίες που φαίνεται να εφαρμόζονται άμεσα σε κάποιες συγκεκριμένες ΚΥ, όπως τον τομέα της υγείας (Psannis E. Konstantinos, 2017) (6). Προσανατολισμένες προς την ασφάλεια είναι κάποιες εργασίας που μελετάνε ασφαλείς τρόπους με τους οποίους μπορούν να συνεργαστούν και να συνυπάρξουν οι συσκευές IoT και η τεχνολογία Cloud Computing (K. E. Psannis C. S.-G., 2018). Αρκετές ΚΥ χρησιμοποιούνε IoT και Cloud Computing τεχνολογίες αλλά πιό άμεσες με αυτή την εργασία θα θεωρούσαμε τις (1, 2, 4). Είναι επίσης γνωστό πως με την χρήση συσκευών αλλά και τα αποτελέσματα που παίρνουμε από της ανάλυση μεγάλου όγκου δεδομένων προσπαθούν οι διάφοροι τομείς να βελτιώσουν την απόδοσή τους καθώς και υπηρεσίες που δίνουν προς τους πολίτες. Τέτοιο παράδειγμά υπηρεσιών είναι τα κοινωνικά δίκτυα που εκτός από μια μέθοδο επικοινωνίας των πολιτών είναι πλέον πλατφόρμες που μπορούν να δεχτούν και να υποστηρίξουν πληθώρα υπηρεσίων αλλά και

και συσκευές με εξειδικευμένες υπηρεσίες που προορίζονται να διευκολύνουν την καθημερινή ζωή των πολιτών (K. E. Psannis P. P., 2018). ΚΥ που κάνουν τέτοια χρήση συσκευών για να δίνουν παρόμοιες υπηρεσίες είναι οι (2, 4, 7, 10).

Για να αποδώσουμε γραφικά και με πιο ευανάγνωστο τρόπο στον αναγνώστη την κατηγοριοποίηση των προαναφερθέντων εργασιών θα μπορούσαμε να δημιουργήσουμε έναν πίνακα στον οποίο στη πρώτη στήλη να εμφανίζονται οι σχετικές εργασίες και στις υπόλοιπες στήλες οι ΚΥ που έχουν περιγραφεί στις προηγούμενες ενότητες. Ένας τέτοιος πίνακας εμφανίζεται παρακάτω:

Εργασία/ΚΥ	Κλάδος Χημείας	Τεχνολογίες πληροφοριών & επικοινωνιών (ΤΠΕ)	Ενέργεια	Οικονομικές Υπηρεσίες	Βιομηχανία τροφίμων	Υγεία	Μεταφορές	Συστήματα νερού κι εγκαταστάσεις	Πυρηνικά	Υπηρεσίες έκτακτης ανάγκης
Efficient IoT-based Sensor BIG Data Collection-Processing and Analysis in Smart Buildings			x	x	x	x		x	x	
Efficient and secure BIG data delivery in Cloud Computing		x		x		x			x	x
Secure Integration of Internet-of-Things and Cloud Computing		x		x			x			x
Solutions for Inter-connectivity and Security in a Smart Hospital Building						x				
Secure integration of IoT and Cloud Computing	x	x		X						
Efficient IoT-based Sensor BIG Data Collection-Processing and Analysis in Smart Buildings		x		x			x			x

Πίνακας 3: Συσχέτιση διαφόρων εργασιών του τομέα του IoT σε σχέση με τις κρίσιμες υποδομές

Κεφάλαιο 5: Απόδειξη της προσέγγισης

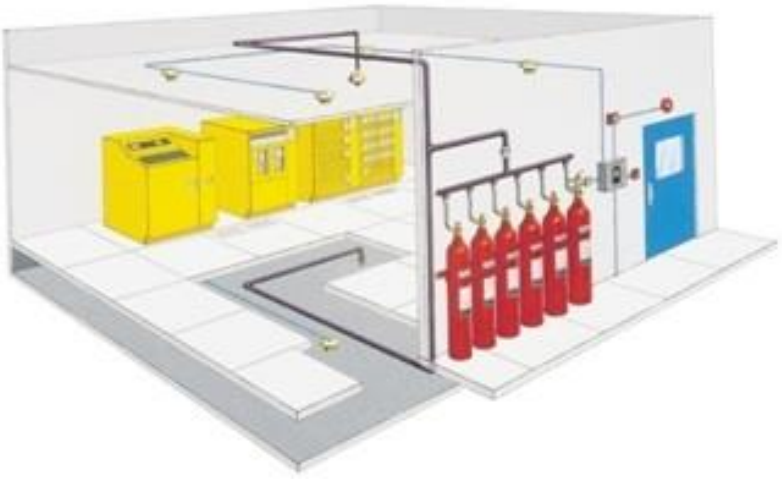
Με βάση την ανάλυση που έγινε στις προηγούμενες ενότητες, παρουσιάζεται πόσο σημαντική θα ήταν η χρήση συσκευών IoT στις δίαφορες δομές ζωτικής σημασίας, όταν ελέγχονται απλά χαρακτηριστικά (όπως π.χ. η θερμοκρασία) τα οποία είναι πολύ σημαντικά στοιχεία για τις υποδομές αυτές. Για παράδειγμα , οι πυροσβεστήρες οποιουδήποτε χώρου ελέγχου των υποδομών που παρουσιάστηκαν προηγουμένως. Σε περίπτωση αποτυχίας ελέγχου του χώρου, ολόκληρη η δομή ζωτικής σημασίας είναι εκτός λειτουργίας και στην περίπτωση αυτή η ζημιά που θα προκληθεί μπορεί να είναι από εκατομμύρια Ευρώ έως και ανθρώπινες ζωές. Η ιδέα αυτή δεν ισχύει μόνο για τους χώρους ελέγχου αλλά σε όλους τους τομείς μιας δομής ζωτικής σημασίας με μικρές παραλλαγές / τροποποιήσεις στην υλοποίηση.

Έτσι, έχοντας υπόψιν ότι κάθε χώρος ελέγχου (ο οποίος είναι πλήρης από ηλεκτρολογικό εξοπλισμό και κυκλώματα), διαθέτει σύστημα πυρόσβεσης που θέλουμε να λειτουργεί ΜΟΝΟ σε περίπτωση πυρκαγιάς, επιβάλεται να βεβαιωθούμε ότι τα σήματα είναι ακριβή. Σε περίπτωση ψευδούς συναγερμού, η διαδικασία πυρόσβεσης με βάσητο Co2 μπορεί να είναι δαπανηρή και επιβλαβής για το προσωπικό που ενδεχομένως εργάζεται στο χώρο ελέγχου εκείνη τη στιγμή.

Στα παραδοσιακά συστήματα πυρόσβεσης, κάθε φορά που ένας αισθητήρας εντοπίζει πυρκαγιά ή μια υπέρβαση της θερμοκρασίας του χώρου, στέλνει ένα σήμα στην κεντρική μονάδα επεξεργασίας με σκοπό να ενεργοποιηθεί η διαδιακασία πυρόσβεσης. Με την οικονομική λύση που παρουσιάζεται στην εργασία αυτή, η οποία βασίζεται σε αισθητήρες IoT, θέλουμε να είμαστε βέβαιοι ότι η διαδικασία κατάσβεσης της φωτιάς ΔΕ θα ξεκινήσει τυχαία από έναν ελλατωματικό αισθητήρα που προκαλεί ψευδή συναγερμό. Η ιδέα προσπαθεί να εξαλείψει την πιθανότητα ψευδούς ενεργοποίησης ολόκληρης της διαδικασίας πυρόσβεσης.

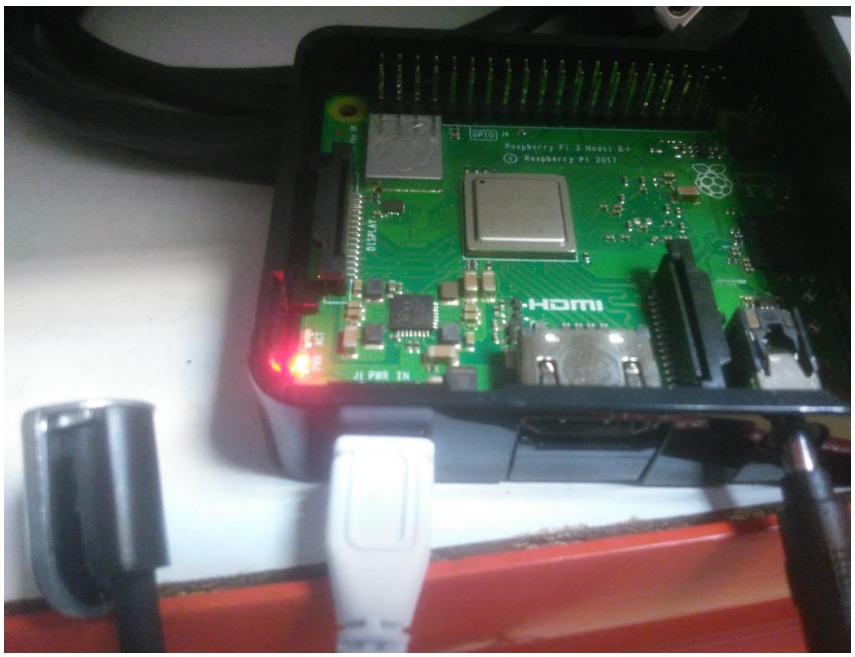
Ένα παραδοσιακό σύστημα πυρόσβεσης περιλαμβάνει πολλούς αισθητήρες σε μία αίθουσα ελέγχου, μία κεντρική μονάδα επεξεργασίας των σημάτων και το σύστημα πυρόσβεσης. Ένα τέτοιο σύστημα παρουσιάζεται στις παρακάτω εικόνες.

Εικόνα 1: Το σύστημα πυρόσβεσης



Εικόνα 2: Ένα σύστημα πυρόσβεσης καθώς και ένα τυπικό παράδειγμα τοποθέτησης αισθητήρων σε ένα control room

Στη περίπτωση που παρουσιάζουμε στην εργασία, τοποθετούμε στο δωμάτιο οικονομικούς ασύρματους αισθητήρες που είναι σε θέση να παρακολουθούν συνεχώς τη θερμοκρασίατης αίθουσας ελέγχου. Τέτοιοι αισθητήρες μπορεί να είναι τα γνωστά raspberryPIs συνδεδεμένα με έναν θερμικό αισθητήρα όπως παρουσιάζεται στην παρακάτω είκόνα.



Εικόνα 3: Το Raspberry PI και ο αισθητήρας θερμοκρασίας που συνεχόμενα καταγράφει την θερμοκρασία του control room

Ο αισθητήρας τρέχει ένα συνηθησμένο λειτουργικό σύστημα Linux που είναι σε θέση να παρακολουθεί τα σήματα από τον αισθητήρα θερμοκρασίας. Τα αποτελέσματα συλλέγονται στην κεντρική μονάδα επεξεργασίας η οποία μπορεί να είναι μία άλλη συσκευή RaspberryPI ή ακόμη κι η κεντρική μονάδα επεξεργασίας του συστήματος πυρόσβεσης εάν υποστηρίζει τέτοια επικοινωνία με εξωτερικές συσκευές.

Όπως αναφέραμε προηγουμένως, η ιδέα είναι να εξαλείψουμε τελείως την πιθανότητα ψευδούς ενεργοποίησης του συστήματος. Για το λόγο αυτό τοποθετήσαμε τρία (3) RaspberryPIs στην αίθουσα ελέγχου που είναι σε θέση να παρακολουθούν τη θερμοκρασία του ίδιου χώρου ελέγχου. Έτσι παρουσιάζουμε μία υποδομή παρακολούθησης όπως αυτή παρουσιάζεται στην εικόνα 4.

SENSOR 1

SENSOR2

SENSOR 3

Εικόνα4: Η υποδομή με τους αισθητήρες που καταγράφουν θερμοκρασίες

Κάθε ένα από τα RaspberryPI προωθεί τα αποτελέσματά του στην κεντρική μονάδα επεξεργασίας. Το μόνο που πρέπει να κάνει η κεντρική μονάδα, είναι να αποθηκεύει και να συγκρίνει τις τιμές που λαμβάνει από τους απομακρυσμένους αισθητήρες. Η κεντρική μονάδα επεξεργασίας δε θα ξεκινήσει ποτέ τη διαδικασία πυρόσβεσης εκτός εάν δύο από τους τρεις αισθητήρες στείλουν μετρήσεις θερμοκρασίας που υπερβαίνουν το όριο που ο χειριστής έχει δείξει ώς κρίσιμο. Με αυτόν τον τρόπο είμαστε σχεδόν βέβαιοι ότι ακόμη κι ένας αισθητήρας να είναι ελλατωματικός και να στέλνει λάθος μετρήσεις, η κεντρική μονάδα θα μπορέσει να επεξεργαστεί σωστά τις τα αποτελέσματα του συνόλου των αισθητήρων και να μην ενεργοποιήσει λανθασμένα το σύστημα πυρόσβεσης. Παρακάτω υπάρχει ένας πίνακας που θα μας βοηθήσει να κατανοήσουμε καλύτερα το σύματα που στέλνουν οι αισθητήρες και τις «τιμές» που πρέπει να επεξεργαστεί η κεντρική μονάδα επεξεργασίας. Υποθέτουμε ότι «κρίσιμος» αριθμός που ενεργοποιεί και στέλνει σήμα κατάσβεσης είναι 30^{o}C. Σε περίπτωση που δύο

από τους τρεις αισθητήρες στείλουν σήμα για θερμοκρασία μεγαλύτερη των 30^{o}C, τότε ενεργοποιείται το σύστημα. Σε αντίθετη περίπτωση δε γίνετε καμία ενέργεια.

Κεντρική μονάδα επεξεργασίας	Αισθητήρας 1	Αισθητήρας 2	Αισθητήρας 3	Ενέργειες
	23oC	23oC	23oC	Καμία ενέργεια
	23oC	25oC	43oC	Καμία ενέργεια
	32oC	23oC	23oC	Καμία ενέργεια
	32oC	31oC	23oC	ΕΝΕΡΓΟΠΟΙΗΣΗ ΣΥΣΤΗΜΑΤΟΣ

Πίνακας 4: Ενδεικτικές πειραματικές μετρήσεις από την υποδομή με τους αισθητήρες καταγραφής θερμοκρασίας του control room

Όσο πιο κρίσιμη είναι η υποδομή που θέλουμε να προστατέψουμε, τόσο περισσότερους αισθητήρες θα πρέπει να τοποθετήσουμε και να συνδέσουμε στην κεντρική μονάδα επεξεργασίας. Για παράδειγμα μπορούμε να χρησιμοποιήσουμε 10 αισθητήρες και να δώσουμε εντολή στην κεντρική μονάδα επεξεργασίας, να λαμβάνει υπόψιν και τους 10 αισθητήρες και να δράσει μόνο σε περίπτωση που 8 απ αυτούς εντοπίσουν επικύνδυνες τιμές στη θερμοκρασία.Με αυτό τον τρόπο περιορίζουμε ακόμη περισσότερο τη πιθανότητα λανθασμένης ενεργοποίησης του συστήματος πυρόσβεσης εξαιτίας λανθασμένης ένδειξης θερμοκρασίας από τους αισθητήρεςοι οποίοι κοστίζουν ελάχιστα μπροστά στην υποδομή που είναι σε θέση να προστατέψουν.

Κεφάλαιο 6: Συμπεράσματα

Η συγκεκριμένη αναφορά περιγράφει διάφορες ΚΥ σύμφωνα με τις ανάγκες τους και πως πρέπει να θωρακιστούν για πιθανές ενδεχόμενες επιθέσεις (εσωτερικές ή/ κι εξωτερικές)

Είναι σαφές ότι πολλές Κρίσιμες Υποδομές είναι εκτεθιμένες σε εξωτερικές και εσωτερικές απειλές. Επιπλέον σχεδόν όλες οι υποδομές αυτές βασίζονται επί του παρόντος σε νέες τεχνολογίες (Κυρίως ΤΠΕ) για τη βελτίωση της αποτελεσματικότητας και την αύξηση της παραγωγικότητας. Αυτό έχει ως φαινόμενο την αύξησητων πιθανών απειλών που μπορεί να δεχθούν καθώς και το κόστος σε περίπτωση βλάβης.

Η παρούσα εργασία παρέχει πληροφορίες σχετικά με διάφορες Κρίσιμες Υποδομές ανάλογα με τις ανάγκες τους καθώς και τις ανάγκες για την προστασία τους. Η τρέχουσα αναφορά επίσης, παρέχει μια επισκόπηση δομών ζωτικής σημασίας και των αναγκών που σχετίζονται με την ασφάλειά τους.

Η αναφορά επίσης παρέχει πληροφορίες σχετικά με συσκευές IOT και τον τρόπο με τον οποίο μπορούν να χρησιμοποιηθούν για την ενίσχυση της ασφάλειας των εν λόγω δομών. Είναι επίσης γνωστό ότι οι συσκευές IOT μπορούν να προσφέρουν έναν τεράστιο όγκο δεδομένων για ανάλυση (Big Data) οι οποίες με κατάλληλες μεθόδους μπορούν να επεξεργαστούν – αναλυθούν καλύτερα για να βελτιωθεί η ακρίβεια των ευρημάτων με σκοπό την καλύτερη προστασία από τις ενδεχόμενες επιθέσεις , από όπου κι αν αυτές προέρχονται (εσωτερικές – εξωτερικές – φυσικές).

Τέλος, στη παρούσα αναφορά, παρέχουμε μια ενδεικτική πρόταση για το πώς μια απλή εφαρμογή με οικονομικές συσκευές IoT μπορεί να ενισχυθεί η ασφάλειατων υποδομών ζωτικής σημασίας.

Βιβλιογραφία

(n.d.). Retrieved from www.dhs.gov: https://www.dhs.gov/water-and-wastewater-systems-sector

(n.d.). Retrieved from www.enisa.europa.eu: https://www.enisa.europa.eu/publications/emergency-communications-stocktaking

(n.d.). Retrieved from www.dhs.gov: https://www.dhs.gov/sites/default/files/publications/Emergency-Services-Sector-Cyber-Risk-Assessment-508.pdf

(2009). Retrieved from ec.europa.eu: http://ec.europa.eu/dgs/home-affairs/e-library/docs/pdf/2009_dependencies_en.pdf

(2015). Retrieved from www.oliverwyman.com: http://www.oliverwyman.com/content/dam/marsh/Documents/PDF/UK-en/Cyber%20Risk%20in%20the%20Transportation%20Industry-03-2015.pdf

(2016). Retrieved from www.blogs.sophos.com: https://blogs.sophos.com/2016/01/28/this-infographic-shows-the-state-of-encryption-today/

(2019). Retrieved from www.dhs.gov: https://www.dhs.gov/sites/default/files/publications/nipp-ssp-chemical-2015-508.pdf

(2019). Retrieved from www.dhs.gov: https://www.dhs.gov

(2019). Retrieved from www.scadahacker.com: https://scadahacker.com/library/Documents/Best_Practices/CIDX%20-%20Guidance%20for%20Addressing%20Cybersecurity%20in%20the%20Chemical%20Sector.pdf

(2019). Retrieved from www.itu.int: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

(2019). Retrieved from www.icitech.org: http://icitech.org/icit-brief-the-energy-sector-hacker-report-profiling-the-hacker-groups-that-threaten-our-nations-energy-sector/

(2019). Retrieved from www.paconsulting.com: http://www.paconsulting.com/industries/energy-and-utilities/cyber-security/securing-industrial-control-systems/

(2019). Retrieved from www.hsdl.org: https://www.hsdl.org/?view&did=754033

(2019). Retrieved from www.nakedsecurity.sophos.com: https://nakedsecurity.sophos.com/2016/04/26/why-cybercriminals-attack-healthcare-more-than-any-other-industry/

(2019). Retrieved from www.driverless-future.com: http://www.driverless-future.com/?page_id=384

(2020). Retrieved from www.dhs.gov: https://www.dhs.gov/critical-infrastructure-sectors

(2020). Retrieved from www.dianeosis.org: http://www.dianeosis.org/wp-content/uploads/2016/06/infrastucture_paradoteo2_Version_020616_3.pdf

(2020). Retrieved from www.isticom.it: http://www.isticom.it/documenti/news/pub_003_eng.pdf

(2020). Retrieved from www.nisc.go.jp: http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v2.pdf

(2020). Retrieved from www.infrastructure.govt.nz: http://www.infrastructure.govt.nz/publications/critical5/crit5-narrative-v2.pdf

(2020). Retrieved from www.infrastructure.govt.nz: http://www.infrastructure.govt.nz/publications/critical5/crit5-narrative-v2.pdf

(2020). Retrieved from www.enisa.europa.eu: https://www.enisa.europa.eu/publications/cloud-in-finance

Atzori, L. (2010). https://www.cs.mun.ca/courses/cs6910/IoT-Survey-Atzori-2010.pdf.

Buckletal. (2009). https://ieeexplore.ieee.org/document/5136693.

Ding. (2010). https://ieeexplore.ieee.org/document/7111303.

Hassan, A. &. (2017). https://ieeexplore.ieee.org/document/7823337.

Hsueh&Chang. (2010). https://link.springer.com/article/10.1007/s13177-009-0004-y.

C. Stergiou, K. E. Psannis, B.-G. Kim, B. Gupta, “Secure integration of IoT and Cloud Computing”, Elsevier, Future Generation Computer Systems, vol. 78, part 3, pp. 964-975, January 2018

A. P. Plageras, K. E. Psannis, C. Stergiou, H. Wang, B. B. Gupta, “Efficient IoT-based sensor BIG Data collection-processing and analysis in Smart Buildings”, Future Generation Computer Systems, vol. 82, pp. 349-357, May 2018.

C. Stergiou, K. E. Psannis, B.-G. Kim, B. Gupta, “Secure integration of IoT and Cloud Computing”, Elsevier, Future Generation Computer Systems, vol. 78, part 3, pp. 964-975, January 2018.

A. P. Plageras, C. Stergiou, K. E. Psannis, Byung-Gyu Kim, Brij Gupta, Y. Ishibashi, “Solutions for Inter-connectivity and Security in a Smart Hospital Building”, in Proceedings of 15th IEEE International Conference on Industrial Informatics (INDIN 2017), 24-26 July 2017, Emden, Germany

C. Stergiou, A. P. Plageras, K. E. Psannis, B. B. Gupta, “Secure Machine Learning scenario from Big Data in Cloud Computing via Internet of Things network”, Springer, Handbook of Computer Networks and Cyber Security: Principles and Paradigms, Multimedia Systems and Applications, in Press, 2019.

A. P. Plageras, K. E. Psannis, C. Stergiou, H. Wang, B. B. Gupta, “Efficient IoT-based sensor BIG Data collection-processing and analysis in Smart Buildings”, Future Generation Computer Systems, vol. 82, pp. 349-357, May 2018

Qin E., Long Y., Zhang C., Huang L. (2013) Cloud Computing and the Internet of Things: Technology Innovation in Automobile Service. In: Yamamoto S. (eds) Human Interface and the Management of Information. Information and Interaction for Health, Safety, Mobility and Complex Environments. HIMI 2013. Lecture Notes in Computer Science, vol 8017. Springer, Berlin, Heidelberg

Rathore, Muhammad Mazhar & Paul, Anand & Ahmad, Awais & Jeon, Gwanggil. (2017). IoT-Based Big Data: From Smart City towards Next Generation Super City Planning. International Journal on Semantic Web and Information Systems (IJSWIS). 13. 28-47. 10.4018/IJSWIS.2017010103.

J. A. Stankovic, "Research Directions for the Internet of Things," in *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3-9, Feb. 2014..

Suciu, George & Suciu, Victor & Martian, Alexandru & Craciunescu, Razvan & Vulpe, Alexandru & Marcu, Ioana & Halunga, Simona & Fratu, Octavian. (2015). Big Data, Internet of Things and Cloud Convergence - An Architecture for Secure E-Health Applications. Journal of medical systems. 39. 327. 10.1007/s10916-015-0327-y.

www.kritis.bund.de. (2020,1). Retrieved from http://www.kritis.bund.de/SubSites/Kritis/EN/introduction/introduction_node.html

L. D. Xu, W. He and S. Li, "Internet of Things in Industries: A Survey," in *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233-2243, Nov. 2014.