Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Κατανεμημένα Συστήματα, Ασφάλεια και Αναδυόμενες Τεχνολογίες Πληροφορίας»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Κυβερνοαπειλές και Τεχνικές Κυβερνοεπιθέσεων σε Βιομηχανικά Συστήματα Ελέγχου (Cyberthreats and Cyber Attack Techniques for Industrial Control Systems)**
Ονοματεπώνυμο Φοιτητή	**Τσάδαρης Κωνσταντίνος**
Πατρώνυμο	**Τσάδαρης Αντώνιος**
Αριθμός Μητρώου	**ΜΠΚΣΑ 18023**
Επιβλέπων	**Κοτζανικολάου Παναγιώτης** **Αναπληρωτής Καθηγητής**

Οκτώβριος 2021

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Κοτζανικολάου Παναγιώτης	Δουληγέρης Χρήστος	Ψαράκης Μιχαήλ
Αναπληρωτής Καθηγητής	Καθηγητής	Αναπληρωτής Καθηγητής

Περιεχόμενα

Περίληψη 6

Λέξεις Κλειδιά: Βιομηχανικά Συστήματα Ελέγχου, Κατανεμημένα Συστήματα, Ασφάλεια 6

Abstract 7

Πίνακας Συντομογραφιών 8

Κεφάλαιο 1°: Εισαγωγή 9

Κεφάλαιο 2°: Επισκόπηση Βιομηχανικών Συστημάτων Ελέγχου (ΒΣΕ) 10

2.1. Κρίσιμες Υποδομές 10

2.2. Βιομηχανικό Σύστημα Ελέγχου (Industrial Control System-ICS) 10

2.3. Εποπτικός έλεγχος και απόκτηση δεδομένων 12

2.4. Κατανεμημένο Σύστημα Ελέγχου (Distributed Control System-DCS) 15

2.5. Διάφοροι τύποι ICS 16

2.6. Προγραμματιζόμενοι Λογικοί Ελεγκτές (Programmable Logic Controllers -PLC) 16

2.7. Προβλήματα Συστημάτων SCADA 17

2.8. Δηλώσεις Προβλημάτων: SCADA System 19

Κεφάλαιο 3ο : Απόδοση και Τεχνικές Απόδοσης Κυβερνοεπιθέσεων στα ΒΣΕ 23

3.1. Νομικές απαιτήσεις για την ανάθεση 24

3.2. Απόδοση Κυβερνοεπιθέσεων 26

3.3. Ταξινόμηση Τεχνικών Ανάθεσης των Κυβερνοεπιθέσεων 29

3.4. Ανασκόπηση Τεχνικών Απόδοσης 32

3.4.1. Traceback 32

3.4.2. Honeypots 34

3.4.3. Ψηφιακή Εγκληματολογική Τεχνική 36

3.4.5. Εγκληματολογία Δικτύου 37

3.4.6. Ανάλυση κακόβουλου λογισμικού 38

3.4.7. Απόδοση βάσει πληροφοριών 39

Κεφάλαιο 4ο : Ανασκόπηση Κυβερνοαπειλών στα ΒΣΕ 41

4.1. Σημεία σε ΒΣΕ που Εκτίθενται σε Κυβερνοαπειλές 41

4.2. Οργανωτικές Απειλές στα ΒΣΕ 43

4.2.1. Αρχιτεκτονικές και Τεχνολογικές Απειλές 43

4.2.2. Παλαιά Τεχνολογία 43

4.2.3. Έλλειψη Ασφάλειας Λόγω Σχεδιασμού 44

4.2.4. Νέα Λειτουργικότητα Παλαιών Συστημάτων 45

4.2.5. Πρωτόκολλα 45

4.3. Παραδείγματα Επιθέσεων 47

Κεφάλαιο 5ο : Μηχανισμοί Προστασίας ΒΣΕ από Κυβερνοεπιθέσεις 57

5.1. Ανάγκη για Προστασία ΒΣΕ από Κυβερνοεπιθέσεις 57

5.2. Βιομηχανικά Standards και Βέλτιστες Πρακτικές 59

5.3. Ασφάλεια Πρωτοκόλλων ΒΣΕ 61

Κεφάλαιο 6° 65

6.1. Κύρια Συμπεράσματα 65

6.2. Ανοικτά προβλήματα και μελλοντικές επεκτάσεις 67

Βιβλιογραφία 69

Περίληψη

Τα βιομηχανικά συστήματα ελέγχου αποτελούν μέρος της βασικής υποδομής κάθε χώρας. Η τυπική μονάδα παραγωγής ενέργειας ή η εγκατάσταση είναι γεμάτη με συνδεδεμένα στο Διαδίκτυο συστήματα και ελεγκτές ελεγχόμενους από υπολογιστή. Αυτές οι συσκευές συνδέονται επίσης, με άλλα ηλεκτρονικά συστήματα που αποτελούν μέρος της διαδικασίας ελέγχου. Αυτό δημιουργεί ένα πολύπλοκο συνδεδεμένο οικοσύστημα, που λόγω της ύπαρξης ευάλωτων συσκευών, το εκθέτει σε εισβολείς στον κυβερνοχώρο. Οι επιτιθέμενοι μπορεί να είναι αυτόνομοι χειριστές, μέρος μεγαλύτερων συνδικάτων οργανωμένου εγκλήματος, εθνικών κρατών ή ακόμη και τρομοκρατικών οργανώσεων. Ορισμένοι επιτιθέμενοι ενδιαφέρονται να καταλάβουν τον έλεγχο της διαδικασίας παραγωγής, ώστε να μπορούν να εκβιάσουν για οικονομικό κέρδος. Άλλοι επιτιθέμενοι επικεντρώνονται στην κλοπή πνευματικής ιδιοκτησίας. Τέλος, υπάρχουν εκείνοι οι επιτιθέμενοι που θέλουν να κάνουν επιθέσεις σε μια προσπάθεια να καταστρέψουν την κρίσιμη υποδομή και να προκαλέσουν σωματική βλάβη στο προσωπικό κοντά σε αυτές τις επιθέσεις. Σκοπός της παρούσας εργασίας είναι να μελετηθεί το ζήτημα των κυβερνοεπιθέσεων και των κυβερνοαπειλών των βιομηχανικών συστημάτων ελέγχου και να αναλυθούν οι μηχανισμοί για την προστασία τους, όπως παρουσιάζονται από τη σύγχρονη βιβλιογραφία. Η εργασία δομείται σε έξι κεφάλαια, μέσα από τα οποία, αρχικά παρουσιάζεται η επισκόπηση των βιομηχανικών συστημάτων ελέγχου, στη συνέχεια πραγματοποιείται η ανασκόπηση των κυβερνοεπιθέσεων στα βιομηχανικά συστήματα ελέγχου, καθώς και οι κυβερνοαπειλές από τις οποίες κινδυνεύουν. Τέλος, παρουσιάζονται οι μηχανισμοί προστασίας των βιομηχανικών συστημάτων ελέγχου, ενώ στο τέλος εκτίθενται τα συμπεράσματα ολόκληρης της εργασίας.

Λέξεις Κλειδιά: Βιομηχανικά Συστήματα Ελέγχου, Κατανεμημένα Συστήματα, Ασφάλεια

Abstract

Industrial control systems are part of every country's basic infrastructure. The standard power plant or installation is packed with Internet-connected systems and computer-controlled controllers. These devices are also connected with other electronic systems that are part of the control process. This creates a complex connected ecosystem that due to the existence of vulnerable devices is exposed to cyber intruders. The attackers can be autonomous operators, part of larger organized crime teams, nation states or even terrorist organizations. Some attackers are interested in taking control of the production process so that they can extort money for financial gain. Other attackers focus on intellectual property theft. Finally, there are attackers who want to make an attack in an attempt to destroy critical infrastructure and inflict bodily harm on the staff that is close to these attacks. The purpose of this thesis is to study the issue of cyber attacks and threats of industrial control systems and to analyze the mechanisms for their protection, as presented by the modern literature. The work is structured in six chapters, through which, first the overview of the industrial control systems is presented, then the cyber attacks on the industrial control systems are carried out, as well as the cyber threats from which they are endangered. Finally, the mechanisms for the protection of industrial control systems are presented, while at the end the conclusions of the whole work are described, too.

Keywords: Industrial Control Systems, Distributed Systems, Security

Πίνακας Συντομογραφιών

Βιομηχανικά Συστήματα Ελέγχου (ΒΣΕ)	Industrial Control System (ICS)
Κατανεμημένα Συστήματα Ελέγχου (ΚΣΕ)	Distributed Control Systems (DCS)
Συστήματα Εποπτικού Ελέγχου και Απόκτησης Δεδομένων (ΣΕΕΑΔ)	Supervisory Control and Data Acquisition (SCADA)
Προγραμματιζόμενοι Λογικοί Ελεγκτές (ΠΛΕ)	Programmable Logic Controllers (PLC)
Διεπαφή Ανθρώπου Μηχανής (ΔΑΜ)	Human Machine Interface (HMI)
Κύρια Τερματική Μονάδα (ΚΤΜ)	Master Terminal Unit (MTU)
Δημόσιο Τηλεφωνικό Δίκτυο Μεταγωγής (ΔΤΔΜ)	Public Switched Telephone Network (PSTN)
Τοπικό Δίκτυο (ΤΔ)	Local Area Network (LAN)
Απομακτυσμένη Τερματική Μονάδα (ΑΤΜ)	Remote Terminal Unit (RTU)
Δίκτυο Ευρείας Περιοχής (ΔΕΠ)	Wide Area Network (WAN)
Πρωτόκολλο Ελέγχου Μεταφορών (ΠΕΜ)	Transport Control Protocol (TCP)
Προηγμένα Πρότυπα Κρυπτογράφησης (ΠΠΚ)	Advanced Encryption Standard (AES)
Έξυπνη Ηλεκτρονική Συσκευή (ΕΗΣ)	Intelligent Electonic Device (IED)
Πιθανή Σήμανση Πακέτων	Probabilistic Packet Marketing (PPM)
Προσδιοριστική Σήμανση Πακέτων	Deterministic Packet Marking (DPM)
Μηχανισμός Απομόνωσης Πηγαίου-Διαύλου (ΜΑΠΔ)	Source-Path Isolation Engine (SPIE)
Μοντέλιο Ευπάθειας-Ζημίας	Attack Vulnerability Damage (AVD) Model
Προηγμένα και Αυθεντικά Σχέδια Σήμανσης (ΠΑΣΣ)	Advanced and Authenticated Marking Schemes (AMS)
Πρωτόκολλο Υπερκειμενικής Μεταφοράς	Hypertext Transfer Protocol (HTTP)
Πρωτόκολλο Μεταφοράς Αρχείων	File Transfer Protocol (FTP)
Σύστημα Δαχείρισης Βάσης Δεδομένων	Database Management System (DBMS)
Σύστημα Πληροφορικής	Information Technology (IT)
Οργανισμός Ηλεκτρικής Αξιοπιστίας Βόρειας Αμερικής, Δομή Κριτικής Προστασίας	North American Electric Reliability Corporation, Critical Infrastructure Protection (NERC CIP)
Επιχειρησιακή Τεχνολογία	Operational Technology (OT)
Σύστημα Αυτοματισμού Κτηρίων (ΣΑΚ)	Building Automation Systems (BAS)

Κεφάλαιο 1°: Εισαγωγή

Τα βιομηχανικά συστήματα ελέγχου αποτελούν μέρος της βασικής υποδομής κάθε χώρας, βρίσκονται στο επίκεντρο όλων των συστημάτων παραγωγής και ελέγχου διεργασιών σε όλο τον κόσμο. Είναι ενσωματωμένα παντού στις μονάδες παραγωγής ενέργειας, στις χημικές μονάδες, στις εγκαταστάσεις επεξεργασίας τροφίμων και ποτών, στην αυτοκινητοβιομηχανία, στην αεροδιαστημική, στα φαρμακευτικά συστήματα, στα συστήματα διαχείρισης νερού και λυμάτων και σε πολλούς άλλους τύπους κρίσιμων βιομηχανικών διεργασιών. Η τυπική μονάδα παραγωγής ενέργειας ή η εγκατάσταση είναι γεμάτη με συνδεδεμένα στο Διαδίκτυο συστήματα και ελεγκτές ελεγχόμενους από υπολογιστή. Αυτές οι συσκευές συνδέονται επίσης, με άλλα ηλεκτρονικά συστήματα που αποτελούν μέρος της διαδικασίας ελέγχου. Αυτό δημιουργεί ένα πολύπλοκο συνδεδεμένο οικοσύστημα που λόγω της ύπαρξης ευάλωτων συσκευών το εκθέτει σε εισβολείς στον κυβερνοχώρο. Οι επιτιθέμενοι μπορεί να είναι αυτόνομοι χειριστές, μέρος μεγαλύτερων συνδικάτων οργανωμένου εγκλήματος, εθνικών κρατών ή ακόμη και τρομοκρατικών οργανώσεων. Ορισμένοι επιτιθέμενοι ενδιαφέρονται να καταλάβουν τον έλεγχο της διαδικασίας παραγωγής, ώστε να μπορούν να εκβιάσουν για οικονομικό κέρδος. Άλλοι επιτιθέμενοι επικεντρώνονται στην κλοπή πνευματικής ιδιοκτησίας. Τέλος, υπάρχουν εκείνοι οι επιτιθέμενοι που θέλουν να κάνουν επιθέσεις σε μια προσπάθεια, να καταστρέψουν την κρίσιμη υποδομή και να προκαλέσουν σωματική βλάβη στο προσωπικό κοντά σε αυτές τις επιθέσεις.

Σκοπός της παρούσας εργασίας είναι να μελετηθεί το ζήτημα των κυβερνοεπιθέσεων και των κυβερνοαπειλών των βιομηχανικών συστημάτων ελέγχου και να αναλυθούν οι μηχανισμοί για την προστασία τους, όπως παρουσιάζονται από τη σύγχρονη βιβλιογραφία. Η εργασία δομείται σε έξι κεφάλαια, μέσα από τα οποία, αρχικά παρουσιάζεται η επισκόπηση των βιομηχανικών συστημάτων ελέγχου, στη συνέχεια πραγματοποιείται η ανασκόπηση των κυβερνοεπιθέσεων στα βιομηχανικά συστήματα ελέγχου, καθώς και οι κυβερνοαπειλές από τις οποίες κινδυνεύουν. Τέλος, παρουσιάζονται οι μηχανισμοί προστασίας των βιομηχανικών συστημάτων ελέγχου, ενώ στο τέλος εκθέτονται τα συμπεράσματα ολόκληρης της εργασίας.

Κεφάλαιο 2ο: Επισκόπηση Βιομηχανικών Συστημάτων Ελέγχου (ΒΣΕ)

2.1. Κρίσιμες Υποδομές

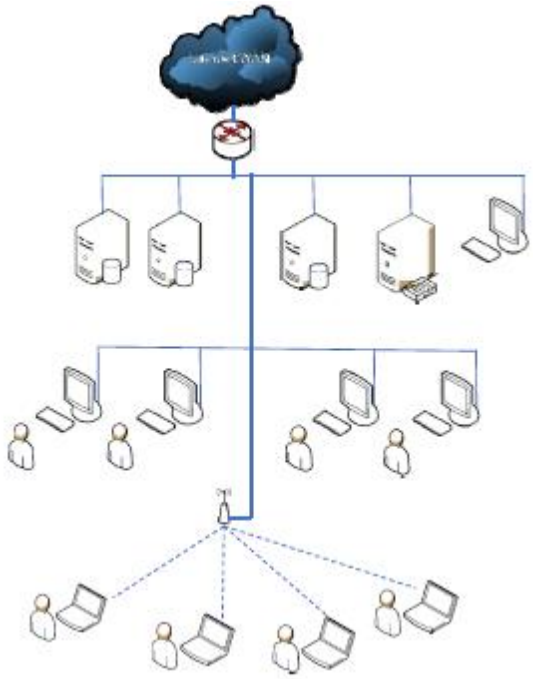
Οι κρίσιμες υποδομές αποτελούν τα αγαθά, τα φυσικά και εικονικά (cyber) συστήματα και υποσυστήματα και γενικά τα περιουσιακά στοιχεία, που είναι τόσο υψίστης ζωτικής σημασίας για μια χώρα, που η υποβάθμιση τους ή η καταστροφή τους θα έχει σοβαρό αντίκτυπο στην δημόσια υγεία, στην φυσική προστασία, στην ασφάλεια, καθώς και στην οικονομική και κοινωνική ευημερία των πολιτών.

Οι κρίσιμες υποδομές ενός έθνους παρέχουν τις βασικές υπηρεσίες που υποστηρίζουν την κοινωνία και χωρίζονται στους παρακάτω τομείς:

- Ενέργεια
- Μεταφορές
- Τράπεζες
- Χρηματοπιστωτικές υποδομές
- Τομέας υγείας
- Προμήθεια και διανομή πόσιμου ύδατος
- Ψηφιακή υποδομή

2.2. Βιομηχανικό Σύστημα Ελέγχου (Industrial Control System-ICS)

Ένα Πληροφοριακό Σύστημα (IS) είναι ένα οργανωμένο σύνολο πόρων (υλικό, λογισμικό, προσωπικό, δεδομένα, διαδικασίες κ.λπ.) για την απόκτηση, επεξεργασία και αποθήκευση πληροφοριών (με τη μορφή δεδομένων, κειμένου, εικόνων, ήχων κ.λπ.) εντός και μεταξύ οργανισμών. Πολλά IS επεξεργάζονται μόνο πληροφορίες ενώ άλλα επηρεάζουν τον φυσικό κόσμο.



Σχήμα 1. Πληροφοριακό σύστημα. Η έγχρωμη έκδοση αυτού του σχήματος υπάρχει στο www.iste.co.uk/flaus/cybersecurity.zip

Ο όρος Βιομηχανικό Σύστημα Ελέγχου (ICS) χρησιμοποιείται σε διάφορους τύπους υποδομών σε πραγματικό χρόνο (συστήματα), όπως σε Κατανεμημένα Συστήματα Ελέγχου (Distributed Control Systems-DCS), σε Συστήματα Εποπτικού Ελέγχου και Απόκτησης Δεδομένων (Supervisory Control And Data Acquisition-SCADA) και σε Προγραμματιζόμενους Λογικούς Ελεγκτές (Programmable Logic Controllers-PLC). Ο γενικός όρος Βιομηχανικό Σύστημα Ελέγχου (ICS) είχε χρησιμοποιηθεί για βιομηχανίες ή/και υποδομές πραγματικού χρόνου (Stouffer et al., 2006). Οι υποδομές βιομηχανικού συστήματος ελέγχου (ICS) βασίζονται σε διάφορους τύπους συσκευών πεδίου, οι οποίες επικοινωνούν εντός του δικτύου ICS για τους σκοπούς της παράδοσης μηνυμάτων/δεδομένων και εντολών και ανατροφοδότησης από τον απομακρυσμένο σταθμό στον κύριο σταθμό.

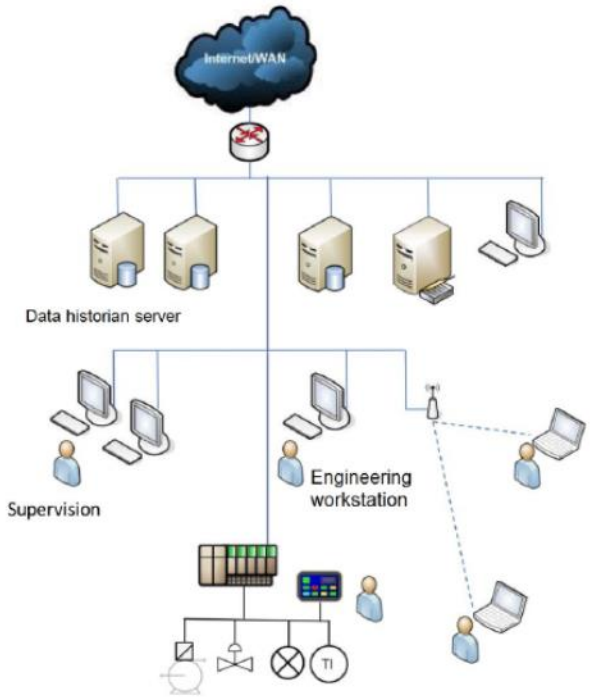
Η επικοινωνία μεταξύ συσκευών πεδίου βασίζεται σε εποπτικές/αυτοματοποιημένες εντολές, όπως η οδηγία για τη συλλογή δεδομένων από αισθητήρα συνδεδεμένο με απομακρυσμένο σταθμό, έλεγχο της κατάστασης συναγερμού, πληροφορίες κατάστασης ανοίγματος και κλεισίματος διακοπτών και συγχρονισμό χρόνου, που μεταδίδονται από το σταθμό ελέγχου ή τον κύριο σταθμό σε συσκευές πεδίου που χρησιμοποιούν Διεπαφή Ανθρώπου Μηχανής (Human Machine Interface-HMI). Το Βιομηχανικό Σύστημα Ελέγχου (ICS) είχε σχεδιαστεί για κρίσιμους τομείς υποδομής και το 90% αυτών των συστημάτων ανήκουν σε ιδιωτικούς οργανισμούς και λειτουργούν από αυτούς. Το Βιομηχανικό Σύστημα Ελέγχου (ICS) χρησιμοποιείται επίσης, από ομοσπονδιακές υπηρεσίες, συνήθως για σκοπούς ελέγχου του συστήματος

εναέριας κυκλοφορίας, λειτουργίας και ελέγχου πυρηνικών εργοστασίων και χρήσεων στη βιομηχανία πετρελαίου, τη βιομηχανία φυσικού αερίου, τη χημική βιομηχανία, το σύστημα μεταφορών και τη φαρμακευτική παραγωγή (Stouffer et al., 2006). Στις παρακάτω υποενότητες θα δούμε κάποια μέρη και τύπους των Βιομηχανικών Συστημάτων Ελέγχου (Industrial Control System-ICS).

2.3. Εποπτικός έλεγχος και απόκτηση δεδομένων

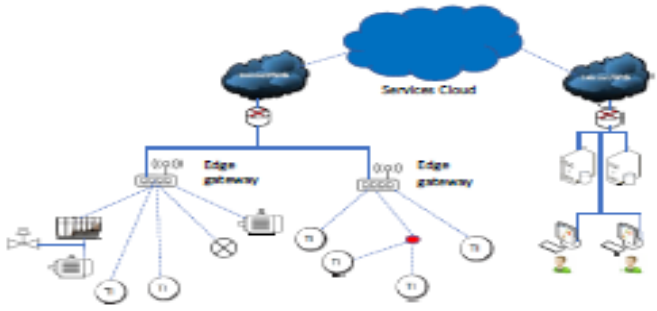
Το σύστημα Εποπτικού Ελέγχου και Απόκτησης Δεδομένων (Supervisory Control And Data Acquisition-SCADA) είναι Σύστημα Βιομηχανικού Ελέγχου (ICS) σε πραγματικό χρόνο. Συνήθως χρησιμοποιείται για την παρακολούθηση και τον έλεγχο βιομηχανικών διεργασιών μεταξύ συσκευών πεδίου συνδεδεμένων εντός του δικτύου SCADA. Τα συστήματα SCADA ή οι συσκευές πεδίων διανέμονται γεωγραφικά σε διαφορετικές τοποθεσίες και παρακολουθούνται/ελέγχονται από το κέντρο ελέγχου χρησιμοποιώντας HMI και αξιοποιούνται σε κρίσιμες διεργασίες, συμπεριλαμβανομένων των μονάδων διανομής και επεξεργασίας νερού, σταθμών παραγωγής ενέργειας, σταθμών συλλογής και επεξεργασίας ύδατος, εγκαταστάσεων κατασκευής και διύλισης, σταθμών αιολικών πάρκων, συστημάτων τηλεπικοινωνιών, σταθμών διύλισης πετρελαίου, σταθμών συλλογής και άντλησης φυσικού αερίου, μονάδων ηλεκτρικής ενέργειας, συστημάτων παρακολούθησης και ελέγχου αεροδρομίων, συστημάτων παρακολούθησης και ελέγχου πλοίων, σταθμών παρακολούθησης και ελέγχου χώρου και εγκαταστάσεως/ συστημάτων εξαερισμού κλιματισμού και θέρμανσης.

Ένα Βιομηχανικό Πληροφοριακό σύστημα (IS), ή ένα βιομηχανικό σύστημα ελέγχου (industrial control system-ICS), είναι ένα σύστημα που αποτελείται από ένα IS και ειδικό εξοπλισμό για έλεγχο και μέτρηση. Η αρχιτεκτονική ενός παραδοσιακού βιομηχανικού IS φαίνεται στο ακόλουθο σχήμα , το οποίο ονομάζεται Εποπτικός Έλεγχος και Απόκτηση Δεδομένων (Supervisory Control And Data Acquisition-SCADA) ή Κατανεμημένο Σύστημα Ελέγχου (Distributed Control System-DC).



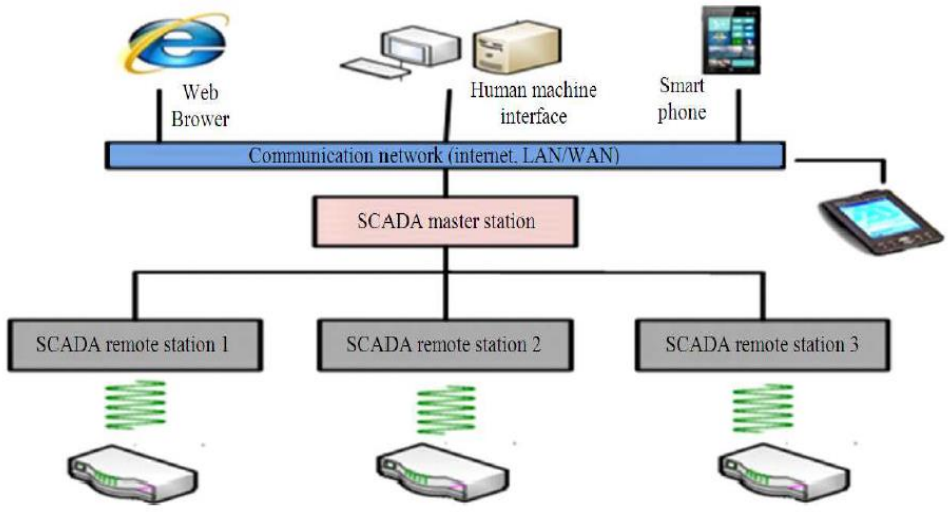
Σχήμα 2. Βιομηχανικό Πληροφοριακό Σύστημα. Η έγχρωμη έκδοση του σχήματος φαίνεται στο www.iste.co.uk/flaus/cybersecurity.zip

Η αρχιτεκτονική ενός βιομηχανικού IS που βασίζεται στο Διαδίκτυο των πραγμάτων (IoT) φαίνεται στο παρακάτω σχήμα. Βασίζεται στο Cloud και εισάγει νέες συνιστώσες και πρωτόκολλα. Σε γενικές γραμμές, ένα ICS αποτελείται από τα ίδια στοιχεία με ένα IS διαχείρισης με, επιπλέον, ειδικό εξοπλισμό και λογισμικό όπως προγράμματα εντολών ελέγχου. Αυτά διασφαλίζουν τον έλεγχο σε πραγματικό χρόνο και διαχειρίζονται την αρχειοθέτηση δεδομένων, τα οποία χαρακτηρίζουν την εξέλιξη της εγκατάστασης (ιστορικό και αρχεία καταγραφής συναγερμών).



Σχήμα 3. IoT πληροφοριακό σύστημα. Η έγχρωμα έκδοση φαίνεται στο: www.iste.co.uk/flaus/cybersecurity.zip

Στο σύστημα SCADA, τα δεδομένα/πληροφορίες συλλέγονται από συσκευές ή ενεργοποιητές/αισθητήρες συνδεδεμένους εντός δικτύου και αυτές οι πληροφορίες θα προχωρήσουν στο κύριο κέντρο ελέγχου για σκοπούς παρακολούθησης και ελέγχου. Κατά τη διάρκεια της επικοινωνίας SCADA, οι πληροφορίες έχουν οπτικοποιηθεί με τη μορφή κειμένου ή γραφικής παράστασης, οπότε διευκολύνονται οι οπτικοποιήσεις και ο διαχειριστής στο κέντρο ελέγχου ελέγχει και παρακολουθεί το περιβάλλον σε πραγματικό συνήθως χρόνο, αυτόματα ή με τη λειτουργία εντολών. Στο παρακάτω σχήμα, το σύστημα SCADA παρέχει επικοινωνία μεταξύ των συσκευών πεδίου όπως Κύρια Τερματική Μονάδα (Master Terminal Unit-MTU), Απομακρυσμένη Τερματική Μονάδα (Remote Terminal Units-RTUs) και Προγραμματιζόμενοι λογικοί ελεγκτές (Programmable Logic Controllers -PLCs) και ολόκληρη η επικοινωνία παρακολουθείται και διαχειρίζεται από τον κεντρικό έλεγχο χρησιμοποιώντας διάφορους τύπους δικτύων επικοινωνίας, συμπεριλαμβάνομένου του δημοσίου τηλεφωνικού δικτύου μεταγωγής (Public Switched Telephone Network-PSTN), του τοπικού δικτύου (Local Area Network-LAN), του δικτύου ευρείας περιοχής (Wide Area Network-WAN) και του συστήματος SCADA. Έχουν επίσης, αναπτυχθεί ασύρματες τεχνολογίες, όπως για την επικοινωνία μεταξύ της κύριας μονάδας τερματικού (MTU) και των απομακρυσμένων τερματικών μονάδων (RTU) ή/και συσκευές πεδίου (Shahzad et al., 2014a; Musa and Aborujilah, 2013a). Η παρακάτω εικόνα απεικονίζει τις πληροφορίες υπηρεσιών που συνήθως εκτελούνται από το σύστημα SCADA.



Σχήμα 4. Επικοινωνία συστήματος SCADA (Πηγή: (Shahzad et al., 2014))

Το σύστημα SCADA παρέχει έλεγχο επίβλεψης επί των επιτόπιων συσκευών και παρακολουθεί ολόκληρη την επικοινωνία από την κεντρική τοποθεσία, συνήθως από το λογισμικό (HMI). Έχει χρησιμοποιήσει διάφορους τύπους μέσων περιλαμβανομένων των ραδιοσημάτων, των τηλεφωνικών γραμμών, των καλωδιακών συνδέσεων, των δορυφορικών και μικροκυματικών μέσων για επικοινωνία

μεταξύ των συσκευών πεδίου που βρίκονται σε απόσταση. Το κέντρο ελέγχου, όπως ο κεντρικός τερματικός σταθμός, χρησιμοποιείται ως κεντρικός ελεγκτής για τον έλεγχο και την παρακολούθηση των συσκευών πεδίου στο δίκτυο SCADA, όπως η επικοινωνία μεταξύ της Κεντρικής Τερματικής Μονάδας (MTU) και των Απομακρυσμένων Τερματικών Μονάδων (RTUs). Οι Απομακρυσμένες Τερματικές Μονάδες (RTU) χρησιμοποιούνται για τη συλλογή πληροφοριών/δεδομένων από αισθητήρες/ενεργοποιητές, οι οποίοι συνδέονται με φυσικό περιβάλλον και μεταδίδουν τις πληροφορίες στο κέντρο ελέγχου ή στην Κεντρική Τερματική Μονάδα (MTU) για σκοπούς παρακολούθησης. Η τοπολογία του δικτύου αναπτύσσεται ως στατική στο σύστημα SCADA και οι κόμβοι των δικτύων είναι γνωστοί εκ των προτέρων, για επικοινωνία μεταξύ της Κεντρικής Τερματικής Μονάδας και των Απομακρυσμένων Τερματικών Μονάδων.

2.4. Κατανεμημένο Σύστημα Ελέγχου (Distributed Control System-DCS)

Το Κατανεμημένο Σύστημα Ελέγχου (DCS) είναι ένα άλλο μέρος του Βιομηχανικού Συστήματος Ελέγχου (Industrial Control System-ICS) και χρησιμοποιείται για τον έλεγχο και την παρακολούθηση της βιομηχανικής παραγωγής που περιλαμβάνει τομείς επεξεργασίας όπως εγκαταστάσεις διανομής και επεξεργασίας νερού, σταθμούς παραγωγής ηλεκτρικής ενέργειας, εγκαταστάσεις συλλογής και επεξεργασίας λυμάτων, εγκαταστάσεις κατασκευής και διύλισης, σταθμοί αιολικών πάρκων, σταθμοί διύλισης πετρελαίου, σταθμοί συλλογής και άντλησης φυσικού αερίου, μονάδες ηλεκτρικής ενέργειας και εγκαταστάσεις/ συστήματα εξαερισμού κλιματισμού και θέρμανσης.

Το Κατανεμημένο Σύστημα Ελέγχου (DCS) χρησιμοποιεί συνήθως, έλεγχο βρόχου εποπτικού σταθμού και περιέχει επίσης, βρόχους ελέγχου και ενδιάμεσο έλεγχο για τους σκοπούς της διανομής εργασιών, για τη διαχείριση των διεργασιών / εργασιών, οι οποίες κατανέμονται τοπικά μεταξύ των ελεγκτών εντός του δικτύου DCS. Το σύστημα αυτό συλλέγει όλες τις πληροφορίες από αυτούς τους εντοπισμένους ελεγκτές και, στη συνέχεια, παράγει αποτελέσματα ολόκληρης της παραγωγής ή των επιμέρους διαδικασιών. Οι εφαρμογές DCS κατανέμονται μεταξύ πολλών ελεγκτών (ή υπολογιστών) για την ελαχιστοποίηση του φορτίου σε κάθε ελεγκτή ή / και στον κύριο ελεγκτή (ή στον κύριο διακομιστή).

Η βασική εφαρμογή του Κατανεμημένου Συστήματος Ελέγχου (DCS) είναι συγκριτικά ίδια με το σύστημα SCADA αλλά σε φάση παραγωγής, η εφαρμογή ή οι εργασίες κατανέμονται μεταξύ πολλών τοπικών ελεγκτών, έτσι ώστε σε κάθε ελεγκτή να έχει εκχωρηθεί λειτουργία από τον εποπτικό ελεγκτή. Ο εποπτικός ή κύριος ελεγκτής αρχικοποιεί το αίτημα και το στέλνει σε συσκευές πεδίου. Κατά την απόκριση, οι τοπικοί ελεγκτές δημιουργούν τα αποτελέσματα σύμφωνα με το αίτημα ελέγχου εποπτείας, συλλέγουν δεδομένα/πληροφορίες από συσκευές πεδίου και, στη συνέχεια, στέλνουν την απόκριση πίσω στον κύριο διακομιστή ή τον εποπτικό ελεγκτή (Stouffer et al., 2006).

2.5. Διάφοροι τύποι ICS

Τα ICS χρησιμοποιούνται σε πολλούς βιομηχανικούς τομείς και υποδομές ζωτικής σημασίας. Γίνεται διάκριση μεταξύ του μεταποιητικού τομέα (π.χ. της χημικής βιομηχανίας ή των συστημάτων διαχείρισης κτιρίων) και του τομέα διανομής (π.χ. νερό ή ενέργεια). Στην πρώτη περίπτωση, η εγκατάσταση εντοπίζεται γεωγραφικά. Οι διαδικασίες κατασκευής μπορούν να είναι:

- **Συνεχής:** αυτές οι διαδικασίες λειτουργούν συνεχώς, συχνά με μεταβάσεις για την παραγωγή διαφορετικών ιδιοτήτων ενός προϊόντος. Οι ποσότητες τις οποίες διαχειρίζονται, είναι πραγματικές ποσότητες. Χρησιμοποιούνται στις χημικές βιομηχανίες ή στις βιομηχανίες πετρελαίου.
- **Σύνολο παραγωγής (παρτίδα):** αυτές οι διαδικασίες έχουν διακριτά στάδια επεξεργασίας, που εκτελούνται σε μια δεδομένη ποσότητα υλικού. Υπάρχει ένα ξεχωριστό βήμα έναρξης και λήξης για την επεξεργασία της παρτίδας, με τη δυνατότητα σύντομων λειτουργιών σταθερής κατάστασης κατά τη διάρκεια των ενδιάμεσων βημάτων. Οι τυπικές διαδικασίες παραγωγής παρτίδων περιλαμβάνουν την παρασκευή φαρμάκων ή τροφίμων.
- **Διακριτά:** αυτά τα συστήματα εκτελούν γενικά, μια σειρά βημάτων σε μία μόνο συσκευή ή μια διαδοχή μηχανών για τη δημιουργία του τελικού προϊόντος. Η συναρμολόγηση ηλεκτρονικών και μηχανικών εξαρτημάτων και η κατεργασία εξαρτημάτων είναι τυπικά παραδείγματα αυτού του τύπου βιομηχανίας.

Στον τομέα της διανομής, τα ICS χρησιμοποιούνται για τον έλεγχο γεωγραφικά διασκορπισμένων περιουσιακών στοιχείων, συχνά πάνω από χιλιάδες τετραγωνικά χιλιόμετρα, συμπεριλαμβανομένων συστημάτων διανομής νερού, συλλογής λυμάτων και διαχείρισης ενέργειας. Ένα βιομηχανικό IS αποτελείται από στοιχεία παρόμοια με ένα παραδοσιακό IS (σταθμούς εργασίας, διακομιστές, εξοπλισμός δικτύου, εκτυπωτές, συστήματα αποθήκευσης και δημιουργίας αντιγράφων ασφαλείας), αλλά και από συγκεκριμένα στοιχεία που έχουν σχεδιαστεί για τη διαχείριση της αλληλεπίδρασης με το φυσικό σύστημα και την παροχή κατάλληλου HMI: Αυτά περιλαμβάνουν το PLC, τις απομακρυσμένες τερματικές μονάδες (Remote Terminal Units-RTUs) και το σύστημα απόκτησης.

2.6. Προγραμματιζόμενοι Λογικοί Ελεγκτές (Programmable Logic Controllers -PLC)

Τόσο το σύστημα SCADA όσο και τα συστήματα κατανεμημένου ελέγχου (DCS), χρησιμοποιούν PLC, για τον έλεγχο της συνολικής αρχιτεκτονικής του δικτύου. Τα PLC χρησιμοποιούνται, κυρίως, για τη συλλογή δεδομένων/πληροφοριών από φυσικό περιβάλλον και κατά τη συλλογή, κατευθύνουν τις πληροφορίες πίσω στον κύριο σταθμό με βάση το αίτημα αυτού. Οι απομακρυσμένες τερματικές μονάδες (RTUs) στο σύστημα

SCADA χρησιμοποιούνται ως PLC για τη συλλογή δεδομένων/πληροφοριών από αισθητήρες/ενεργοποιητές και μετάδοση αυτών πίσω στον κύριο σταθμό με σκοπό τον έλεγχο και την παρακολούθηση. Από την άλλη πλευρά, οι ελεγκτές πεδίου ή οι τοπικοί ελεγκτές, εκτελούν λειτουργίες ή χρησιμοποιούνται ως PLC εντός του Κατανεμημένου Συστήματος Ελέγχου (DCS). Οι τοπικοί ελεγκτές συλλέγουν δεδομέν /πληροφορίες από συσκευές πεδίου και στέλνουν την απόκριση πίσω στον κύριο ελεγκτή ή στον εποπτικό ελεγκτή. Συνήθως, όλοι οι τύποι PLC έχουν τη δική τους μνήμη ή χώρο αποθήκευσης πληροφοριών που σχετίζονται με οδηγίες που εκτελούνται ή βασίζονται στο αίτημα του κύριου ελεγκτή / του κεντρικού σταθμού ή στην εφαρμογή λειτουργιών όπως λειτουργίες ελέγχου εισόδου/εξόδου, διαχείρισης συνεδρίας, αριθμητικές και λογικές συναρτήσεις, λειτουργία ελέγχου συναγερμού και επεξεργασίας δεδομένων/πληροφοριών, (Shahzad et al., 2013; 2014b). Στη συνέχεια, θα δούμε τις συνθήκες κατά τις οποίες προκύπτουν τα προβλήματα και τις περιπτώσεις των δηλώσεων προβλημάτων των Συστημάτων SCADA.

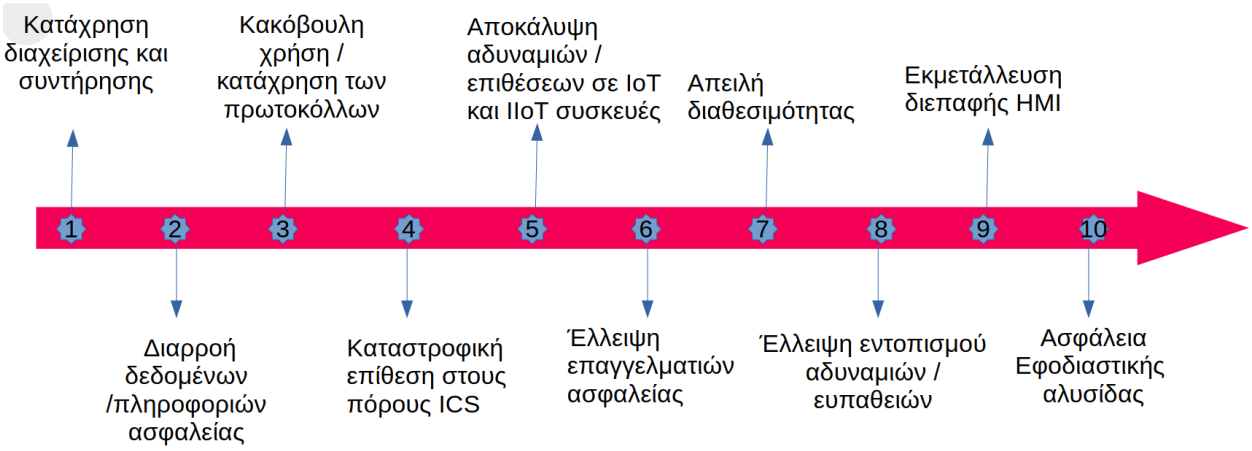
2.7. Προβλήματα Συστημάτων SCADA

Τα συστήματα SCADA έχουν διανεμηθεί γεωγραφικά σε διαφορετικές τοποθεσίες σε όλο τον κόσμο χρησιμοποιώντας την τεχνολογία Δικτύου ευρείας περιοχής (Wide Area Network-WAN). Συνδέονται με πλήθος απομακρυσμένων τερματικών συσκευών ή PLC μέσω διαφόρων τύπων δικτύων όπως LAN / WAN, πρωτοκόλλων και μέσων μετάδοσης, όπως ενσύρματα/ασύρματα. Η μεγάλη βελτίωση στο SCADA, η συνδεσιμότητα με πολλά δίκτυα προηγμένης τεχνολογίας και η χρήση προηγμένων υποδομών I.T, έκαναν την επικοινωνία SCADA πιο απαιτητική για τους τελικούς χρήστες. Το SCADA χρησιμοποιεί κεντρικό σταθμό με προηγμένη υποδομή I.T, που μπορεί να ελέγχει χιλιάδες απομακρυσμένους τερματικούς σταθμούς ή συσκευές πεδίου ταυτόχρονα χωρίς περιορισμό δικτύων και πρωτοκόλλων ή ανοιχτών προτύπων. Από την άλλη, η μεγάλη διασύνδεση ανοικτών προτύπων δικτύων, πρωτοκόλλων και χρήσεων ανοιχτής υποδομής I.T στο σύστημα SCADA, έκανε την πλατφόρμα SCADA πιο ευάλωτη σε διάφορους τύπους απειλών και επιθέσεων (Stouffer et al., 2006; Musa and Aborujilah, 2013b). Περισσότερες λεπτομέρειες σχετικά με τις ευπάθειες και τις απειλές του SCADA παρουσιάζονται παρακάτω.

Τα συστήματα SCADA σχεδιάστηκαν για να πληρούν τις βασικές απαιτήσεις, όπως είναι η απόδοση του συστήματος και η αξιοπιστία του και άλλες βασικές ανάγκες που σχετίζονται με τις λειτουργίες του συστήματος SCADA σε βιομηχανική υποδομή σε πραγματικό χρόνο, χωρίς διασύνδεση με δημόσια/ιδιωτικά δίκτυα καθώς και συνδεσιμότητα στο Διαδίκτυο. Παραδοσιακά, τα συστήματα SCADA συνδέθηκαν με ιδιόκτητο υλικό / λογισμικό και πρωτόκολλα. Με την επανάσταση της προηγμένης υποδομής πληροφορικής, τα συστήματα SCADA αλλάζουν από παραδοσιακά σε προηγμένα δίκτυα ή ανοιχτά πρότυπα πρωτοκόλλων δικτύου, αντί για ιδιόκτητα όπως LAN/WAN μέσω της σύνδεσης στο Διαδίκτυο και αυξάνουν σημαντικά την απόδοση, την αξιοπιστία και την επεκτασιμότητα του συστήματος (Musa και Aborujilah, 2013a; Raghini et

al., 2013). Με προηγμένη διασύνδεση, η πλατφόρμα SCADA ήταν ευάλωτη από διάφορα είδη επικοινωνιών και επιθέσεων στον κυβερνοχώρο. Αρκετές λύσεις αναπτύχθηκαν για την ασφάλεια της επικοινωνίας SCADA, αλλά βασίστηκαν κυρίως στη φυσική ασφάλεια και την ασφάλεια περιορισμένης επικοινωνίας χρησιμοποιώντας στρώμα ασφαλούς υποδοχής ή πρωτόκολλο SSL / internet ή ασφάλεια IP. Ωστόσο, αυτές οι λύσεις παρουσιάζουν πλήθος περιορισμών, ενώ αναπτύσσονται εντός της επικοινωνίας SCADA, επειδή εξαρτώνται από αλγόριθμους κρυπτογράφησης. Έτσι, η τρέχουσα έρευνα προτείνει τη λύση που έχει αναπτυχθεί επιτυχώς στο σύστημα SCADA και διασφαλίζει με επιτυχία την επικοινωνία SCADA μεταξύ της Κύριας Τερματικής μονάδας MTU και των Απομακρισμένων Τερματικών Μονάδων RTU ή/και αντίστροφα. Παραδοσιακά, τα συστήματα SCADA έχουν πολλά χαρακτηριστικά, κινδύνους και προτεραιότητες που διαφέρουν αρκετά από τα συστήματα επικοινωνίας, τα οποία βασίζονται στο Διαδίκτυο, καθώς και διαφορετικές προδιαγραφές επικοινωνίας, όπως απαιτήσεις δικτύου και πρωτοκόλλων

Υπάρχουν λίγες εκτιμήσεις που πρέπει να ληφθούν υπόψη, όταν η παραδοσιακή υποδομή SCADA αντικαθίσταται από την τρέχουσα υποδομή επικοινωνίας με τη χρήση ανοιχτών προτύπων πρωτοκόλλων και δικτύων όπως επιδόσεις διαχείρισης συνεδρίας / χρόνου, διαχείριση αναμενόμενων / απροσδόκητων αποτελεσμάτων, διαχείριση κινδύνου και καταστροφής, θέματα ασφάλειας υποδομής, συνέπειες διεργασιών, διαχείριση απόκρισης επικοινωνίας, διαχείριση λειτουργίας, διαχείριση πόρων, πρωτόκολλα και διαχείριση μέσων και αντικατάσταση συσκευών πεδίου, ζωή συσκευών, άδειας πρόσβασης και υποστήριξης οργανισμού. Υπάρχει πλήθος απειλών που συσχετίζονται με την τεχνολογία λειτουργίας όπως φαίνεται παρακάτω:



Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

Σχήμα 5. Απειλές στην τεχνολογία λειτουργίας (Πηγή: Απειλές-και-προστασία-κρισίμων-υποδομών ,MITRE ATT&CK για ICS)

Υπάρχουν και άλλες που διαταράσσουν ή παρεμποδίζουν την επικοινωνία SCADA, όπως οι εισβολείς επικοινωνίας εντός/εκτός του οργανισμού, εισβολείς ή δίκτυο bot, εισβολείς που χρησιμοποιούν spam, ηλεκτρονικό ψάρεμα, spyware ή κακόβουλο λογισμικό.

Οι ευπάθειες, όπως εγκατάσταση και διαμόρφωση δικτύων ή ακατάλληλη, αρχιτεκτονική επικοινωνίας, πολιτική κωδικού πρόσβασης, έλεγχος ταυτότητας και εξουσιοδότηση συστήματος, ανυπαρξία συστήματος εντοπισμού και πρόληψης εισβολών, ανυπαρξία τείχους προστασίας λογισμικού / υλικού και προστασία κρυπτογράφησης βρίσκονται συνήθως στο σύστημα SCADA και καθιστούν την επικοινωνία μέσω αυτού περισσότερο ανασφαλή. Μετά τη διεξαγωγή της λεπτομερούς ανάλυσης, η οποία βασίστηκε σε θέματα ασφάλειας επικοινωνίας SCADA, όπως απειλές, ευάλωτες πλατφόρμες και μη κατάλληλες πολιτικές ασφάλειας και ανάλυση λύσεων στην επικοινωνία SCADA, η λύση ασφάλειας έχει αναπτυχθεί επιτυχώς στο σύστημα αυτό και διασφαλίζει με επιτυχία την επικοινωνία μέσω αυτού, ενώ δίνει ερευνητικές οδηγίες για να ξεπεραστούν τα ζητήματα ασφαλείας (Musa και Aborujilah, 2013a).

2.8. Δηλώσεις Προβλημάτων: SCADA System

Η δήλωση προβλήματος έχει πραγματοποιηθεί από λεπτομερή μελέτη, με βάση τα υπάρχοντα ζητήματα ασφαλείας του SCADA, όπως απειλές/επιθέσεις και ευπάθειες. Περισσότερες λεπτομέρειες που σχετίζονται

με τα συστήματα SCADA και τα πρωτόκολλα ζητημάτων ασφάλειας και προκλήσεις απεικονίζονται παρακάτω. Αρκετά ζητήματα ασφάλειας και προκλήσεις έχουν αναθεωρηθεί από τις υπάρχουσες εφαρμογές SCADA. Σύμφωνα με την ανάλυση επισκόπησης, δεν υπάρχουν κατάλληλες λύσεις ώστε η επικοινωνία SCADA να διασφαλίζει απόλυτα τα ζητήματα ασφαλείας, όπως υποκλοπές, τροποποίηση δεδομένων, επανάληψη δεδομένων, κατανομή κλειδιών και άλλες γενικές επιθέσεις (Anandkumar and Jayakumar, 2012; Manikandan και Manimegalai, 2012).

Με βάση την επισκόπηση, όλες οι υπάρχουσες λύσεις (γενικές λύσεις ασφαλείας) βασίστηκαν σε τεχνικές κρυπτογράφησης, όπως αλγόριθμοι κρυπτογράφησης, ψηφιακής υπογραφής και κατακερματισμού, με σκοπό την ασφαλή επικοινωνία δεδομένων/μηνυμάτων μεταξύ κόμβων SCADA (Hong and Lee, 2008; Bhaya και AlAsady , 2012). Η επικοινωνία SCADA ήταν ευάλωτη από διάφορους τύπους επιθέσεων στον κυβερνοχώρο εξαιτίας της γρήγορης αύξησης της συνδεσιμότητας του συστήματος SCADA με πρωτόκολλα που βασίζονται σε IP ή ανοιχτά τυπικά πρωτόκολλα. Με βάση την ασφάλεια του SCADA, έχουν αναπτυχθεί λύσεις κρυπτογράφησης όπως το Symmetric και το Asymmetric για την επίτευξη των στόχων των υπηρεσιών ασφαλείας όπως η εμπιστευτικότητα δεδομένων, ο έλεγχος ταυτότητας δεδομένων, η ακεραιότητα των δεδομένων, η λειτουργία μη αποποίησης και η ασφαλής επικοινωνία SCADA μακροπρόθεσμα (Drahansky and Balitanas, 2011; Majdalawieh et al., 2006).

Τα συστήματα SCADA είναι ευάλωτα σε επιθέσεις στον κυβερνοχώρο. Αρκετές υπάρχουσες λύσεις αντιμετωπίζουν την ασφάλεια που σχετίζεται με την επικοινωνία SCADA με περιορισμούς. Τέσσερα βασικά στοιχεία έχουν επισημανθεί για ζητήματα ασφαλείας SCADA όπως η αυθεντικότητα, η διαθεσιμότητα, η ακεραιότητα, η εμπιστευτικότητα. Το σύστημα SCADA έχει μειώσει τους κινδύνους, κερδίζει έλεγχο και παρέχει ασφαλή επικοινωνία εναντίον των επιθέσεων/απειλών χρησιμοποιώντας κρυπτογραφική λύση ή μονάδα (AGA, 2003; Aris et al., 2011). Οι ασύμμετρες και συμμετρικές λύσεις αναπτύσσονται σε διάφορα δίκτυα και παρουσίασαν επιτυχία στις υπηρεσίες ασφαλείας που περιλαμβάνουν έλεγχο ταυτότητας, ακεραιότητα, μη αποποίηση και εμπιστευτικότητα ως κύριο μέρος της προστασίας ασφάλειας SCADA. Οι λύσεις ασφαλείας SSL / TLS και IP έχουν εφαρμοστεί σε διάφορες παραδοσιακές εφαρμογές δικτύων ή/και δίκτυο επικοινωνίας ή πρωτόκολλα SCADA. Οι λύσεις SSL / TLS και IP έχουν πλήθος θεμάτων που σχετίζονται με την επικοινωνία και την ασφάλειά τους, συμπεριλαμβανομένης της λειτουργίας του Πρωτοκόλλου Ελέγχου Μεταφορών (Transport Control Protocol-TCP), το οποίο βασίζεται σε αλγόριθμους κρυπτογράφησης για λόγους ασφαλείας και ο μηχανισμός ασφαλείας είναι περιορισμένος για τη λειτουργία μη αποποίησης και άλλες μη διαθέσιμες δυνατότητες ασφαλείας (Patel και Graham, 2009; Preneel, 1993).

Θέματα ασφαλείας SCADA, όπως ο μη κατάλληλος μηχανισμός ελέγχου ταυτότητας για το σύστημα SCADA όσον αφορά τη σχεδίαση και την επεξεργασία ή τη λειτουργία, τις χρήσεις ιδιόκτητου ή προμηθευτή πρωτοκόλλων με ανοιχτά πρότυπα Πρωτόκολλα (TCP / IP), δείχνουν εμπιστοσύνη στις έννοιες φυσικής ασφάλειας και μειωμένης απόδοσης μέσω Διαδικτύου με πολλά τρωτά σημεία. Από αυτά τα

ζητήματα ασφαλείας, κρυπτογραφική λύση όπως π.χ. ασύμμετρη χρήση αλγορίθμου ECC και συμμετρική χρήση αλγόριθμου AES έχει αναπτυχθεί εντός της επικοινωνίας SCADA από άκρο σε άκρο και έχει επιτύχει υπηρεσίες ασφαλείας όπως εμπιστευτικότητα, έλεγχο ταυτότητας, και ακεραιότητα δεδομένων καθώς και λειτουργία μη αποποίησης. Η «Schweitzer Engineering Laboratories, Inc» πρότεινε ότι οι λύσεις κρυπτογράφησης είναι οι καλύτερες προσεγγίσεις για να ξεπεραστούν τα ζητήματα ασφαλείας του SCADA κατά τη διάρκεια της επικοινωνίας (Risley and Ladow, 2003).

Με βάση τις ευπάθειες του SCADA. η ασφάλεια της πατρίδας (τμήμα) έχει χρησιμοποιήσει μηχανισμό κρυπτογράφησης (λύση) για να εξασφαλίσει την κρίσιμη υποδομή του «Έθνους» από επιθέσεις στον κυβερνοχώρο. Συμπερασματικά, οι κρυπτογραφικές λύσεις είναι οι καλύτερες προσεγγίσεις για την ασφάλεια ή την προστασία της επικοινωνίας SCADA μέσω Διαδικτύου και για τη επιτυχή μείωση των κινδύνων (Shahzad et al., 2014a; Asenjo, 2005; Babu and Singh, 2013). Προηγμένα πρότυπα κρυπτογράφησης (AES) 256, HMAC και MD5 ως μέρος των λύσεων κρυπτογραφησης έχουν αναπτυχθεί, για την προστασία της επικοινωνίας SCADA, ενώ οι εισβολές (ανωμαλία) εντοπίζονται από την Έξυπνη Ηλεκτρονική Συσκευή (IED) ως μέρος του ελεγκτή υποσταθμού (Musa και Aborujilah, 2013a · Hong, 2010; AL-Saidi et al., 2011).

Η «Αμερικανική Υπηρεσία Εθνικής Ασφάλειας» υποφέρει από πιθανές επιθέσεις και χάκερς που αποτελούν σοβαρά προβλήματα για κρίσιμους τομείς υποδομών. Χρειάζεται, λοιπόν, μια λύση που διασφαλίζει σημαντικά την επικοινωνία υποδομής ζωτικής σημασίας, ενώ συνδέεται με ανοιχτά τυπικά δίκτυα ή πρωτόκολλα (Pollet, 2002). Οι προμηθευτές και οι προγραμματιστές του συστήματος SCADA εστιάζουν μόνο σε λειτουργικά μέρη του συστήματος, όπως επεκτασιμότητα, αξιοπιστία, απόδοση και έλεγχο πρόσβασης χωρίς να ληφθεί υπόψη η ασφάλεια. Δεν υπάρχει διαθέσιμη γενική λύση που να πληροί τις απαιτήσεις ασφάλειας συστήματος SCADA. Όλες οι λειτουργικές επιδόσεις SCADA εξαρτώνται από ζητήματα ασφαλείας. Εάν το σύστημα SCADA είναι απόλυτα ασφαλές, τότε θα επιτυγχάνονταν απολύτως όλες οι επιδόσεις του συστήματος (Rautmare, 2011).

Εφαρμογές συστήματος SCADA που χρησιμοποιούν πρωτόκολλα ελέγχου, όπως πρωτόκολλο κατανεμημένου δικτύου (DNP3), fieldbus, modbus και άλλα πρωτόκολλα που βασίζονται σε IP είναι επιβλαβή και κρίσιμα για την επικοινωνία SCADA μεταξύ συσκευών πεδίου. Αυτά τα πρωτόκολλα έχουν σχεδιαστεί χωρίς καμία ασφάλεια που να παρέχει πλήρη ή εν μέρει προστασία από επιθέσεις στον κυβερνοχώρο. Διάφορα τείχη προστασίας έχουν χρησιμοποιηθεί μεταξύ του συστήματος SCADA και των εταιρικών δικτύων ή του Διαδικτύου, αλλά δεν μπορούν να ενσωματωθούν πλήρως με δίκτυα SCADA, όπως όσον αφορά τα πρωτόκολλα SCADA για την ανάπτυξη και διαμόρφωση του DNP3 ή του Modbus. Επομένως, η έλλειψη ενημέρωσης σχετικά με την ασφάλεια και τη διαμόρφωση των πρωτοκόλλων, αυξάνει με γρήγορο ρυθμό το πλήθος των ευπαθειών για την πλατφόρμα SCADA και προκαλεί σημαντικά ζητήματα ασφαλείας για κρίσιμες υποδομές (Cai et al., 2008; Shahzad et al., 2013).

Το DNP3 είναι η πιο σημαντική χρήση πρωτοκόλλου στο σύστημα SCADA. Το DNP3 χρησιμοποιείται σχεδόν σε όλο τον κόσμο, περίπου το 70% στην Αμερική για υπηρεσίες ηλεκτρικού ρεύματος και νερού και το υπόλοιπο 30% σε άλλα μέρη του κόσμου όπως η Ευρώπη, η Ασία και η Αυστραλία (TD, 2011). Η εξασφάλιση πρωτοκόλλου DNP3 ή η ανάπτυξη ασφάλειας εντός του πρωτοκόλλου DNP3, βελτιώνει σημαντικά την ασφάλεια του συστήματος SCADA και μειώνει τις πιθανές επιθέσεις και ευπάθειες στην επικοινωνία.

Στο επόμενο κεφάλαιο θα γίνει μια ανακεφαλαίωση των κυβερνοεπιθέσεων στα Βιομηχανικά Συστήματα Ελέγχου (ΒΣΕ).

Κεφάλαιο 3ο : Απόδοση και Τεχνικές Απόδοσης Κυβερνοεπιθέσεων στα ΒΣΕ

Τα Βιομηχανικά Συστήματα Ελέγχου (Industrial Control Systems - ICS) γίνονται όλο και περισσότερο αντικείμενο επιθέσεων σε δίκτυα υπολογιστών. Τα συστήματα αυτά παρέχουν βασικές υπηρεσίες για υποδομές ζωτικής σημασίας για τα κυρίαρχα έθνη και ως εκ τούτου, οι επιθέσεις αυτές αποτελούν σημαντική απειλή για τη συνεχή ασφάλεια αυτών των χωρών. Το ICS έχει απαιτήσεις απόδοσης και αξιοπιστίας που μπορεί να θεωρηθούν μη συμβατικές από τους σύγχρονους επαγγελματίες της τεχνολογίας πληροφορικής. Οι απαιτήσεις αυτές περιλαμβάνουν τη διαχείριση των διαδικασιών που, εάν δεν εκτελεστούν σωστά, συνιστούν σημαντικό κίνδυνο για την υγεία και την ασφάλεια των ανθρώπινων ζωών, προκαλούν σοβαρές ζημιές στο περιβάλλον, καθώς και σοβαρά οικονομικά ζητήματα, όπως οι απώλειες στην παραγωγή, οι οποίες ενδέχεται να έχουν αρνητικό αντίκτυπο στην οικονομία ενός έθνους (Stouffer et al., 2011).

Στην έρευνα των Cook et al. (2016) συζητούνται οι θεμελιώδεις πτυχές της απόδοσης των επιθέσεων στον κυβερνοχώρο όταν εξετάζονται τα συστήματα βιομηχανικού ελέγχου. Εξ όσων είναι γνωστά, οι πληροφορίες είναι ανόμοιες και δεν είναι αυτοτελείς, παρέχοντας έτσι κίνητρα για την εργασία μας. Εξετάζονται τεχνικά και μη τεχνικά ζητήματα, όπως το τρέχον νομικό προηγούμενο και τα πρότυπα που θα διαμορφώσουν τη μελλοντική κατεύθυνση αυτού του τομέα. Το θέμα της ανάθεσης των επιθέσεων στον κυβερνοχώρο που στοχεύουν στα συστήματα βιομηχανικού ελέγχου είναι ένα αναδυόμενο ζήτημα.

Οι Zhu et al (2011) περιγράφουν τον τρόπο με τον οποίο αυτά τα συστήματα "είναι βαθιά ριζωμένα στη δομή των υποδομών ζωτικής σημασίας", αλλά υπόκεινται σε διαταραχή ή βλάβη λόγω επιπτώσεων στον κυβερνοχώρο. Περιγράφουν, συγκεκριμένα, τις δυνατότητες για επιθέσεις στον κυβερνοχώρο, όπου ο αντίκτυπος των επιθέσεων στον κυβερνοχώρο μπορεί να οδηγήσει σε αποτελέσματα στον φυσικό κόσμο. Οι Miller & Rowe (2012) περιέγραψαν παραδείγματα αυτών των φυσικών αποτελεσμάτων σε μια σειρά συμβάντων μεταξύ 1982 και 2012. Προκειμένου να ασκηθεί δίωξη, ως απάντηση στις επιθέσεις στον κυβερνοχώρο κατά των συστημάτων βιομηχανικού ελέγχου, θα πρέπει να αποδοθεί στον επιτιθέμενο και να καθοριστεί το είδος της επίθεσης, έτσι ώστε οι διεθνείς υπηρεσίες επιβολής του νόμου ή οι εθνικές κυβερνήσεις να μπορούν να αποφασίσουν για την κατάλληλη προσφυγή. Η απόδοση χρησιμεύει ως αποτρεπτικό μέσο για μελλοντικές επιθέσεις, μπορεί να αποτελέσει τη βάση για τη διακοπή των εν εξελίξει επιθέσεων και μπορεί να υποστηρίξει τις συνολικές βελτιώσεις των αμυντικών τεχνικών [32].

Η απόδοση των επιθέσεων στον κυβερνοχώρο στερείται ενός καθολικά αποδεκτού ορισμού. Οι προτεινόμενοι ορισμοί έχουν συχνά περιοριστεί στην προσέγγισή τους, περιορίζοντας τον καθένα σε υποσύνολα κατανομής. Για παράδειγμα, οι ορισμοί που προσφέρονται από τους Hunker et al (2008) περιορίζουν την απόδοση σε "οποιαδήποτε τεχνική απόδοσης που αρχίζει με τον υπερασπιζόμενο υπολογιστή και προχωρά αναδρομικά στην πορεία επίθεσης προς τον επιτιθέμενο". Οι Wheeler et al. (2003) όρισε την

απόδοση ως "προσδιορισμό της ταυτότητας ή της θέσης ενός επιτιθέμενου ή του ενδιάμεσου του επιτιθέμενου". Πριν, όμως, εξεταστούν οι διαθέσιμες τεχνικές για την απόδοση επιθέσεων, είναι απαραίτητο να κατανοηθούν οι νομικές απαιτήσεις για τη δίωξη μιας επίθεσης στον κυβερνοχώρο και ο ρόλος που διαδραματίζει η απόδοση.

3.1. Νομικές απαιτήσεις για την ανάθεση

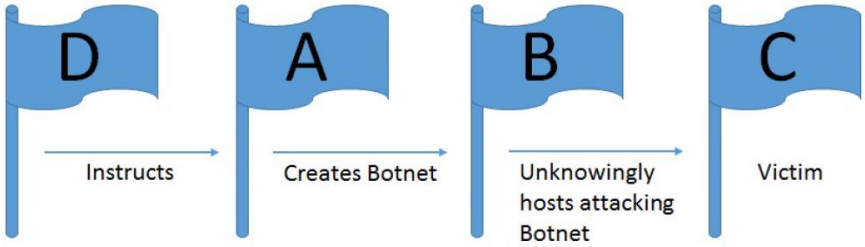
Οι νομικές απαιτήσεις για την ανάθεση περιγράφονται από την Brenner (2006) ως απάντηση σε δύο θεμελιώδη ερωτήματα: πρώτον, ποιος πραγματοποίησε την επίθεση και δεύτερον, τι είδους επίθεση ήταν. Η πρώτη αναθέτει την ευθύνη για τη διάπραξη μιας πράξης, ενώ η δεύτερη αναθέτει την ευθύνη για την αντίδραση σε μια επίθεση.

Όσον αφορά την ευθύνη για τη διάπραξη μιας ενέργειας, ο Keyser (2002) υπογράμμισε την έγκριση της σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο ως "de facto" πρότυπο για το διακρατικό πλαίσιο δίωξης εγκλημάτων στον κυβερνοχώρο για τις χώρες της Δυτικής Ευρώπης και τη Βόρεια Αμερική εναρμονίζοντας τους τοπικούς νόμους. Επίσης, συζήτησε το Άρθρο 5 της συνθήκης, σχετικά με την "παρεμβολή του συστήματος" και το στόχο της να αποτρέψει την σκόπιμη "παρεμπόδιση" της λειτουργίας ενός συστήματος υπολογιστών παρεμβαίνοντας ή χειριζόμενη τα δεδομένα των υπολογιστών χωρίς δικαίωμα. Συνέχισε με συζήτηση για τις παραβιάσεις του άρθρου και την απαίτηση για επίδειξη του ανθρώπινου παράγοντα, αν και αναφέρει ότι ο ορισμός της σκόπιμης δράσης παραμένει άλυτο ζήτημα και έχει τύχει διαφορετικής μεταχείρισης στις υπογράφουσες χώρες.

Συνεπώς, η απλή ανίχνευση επίθεσης κατά του ICS στην πηγή του δεν θα οδηγήσει απαραίτητα σε επαρκείς αποδείξεις για δίωξη. Κάθε τεχνικό γεγονός πρέπει να στηρίζεται από κίνητρο ή πρόθεση. Όσον αφορά την ευθύνη για την αντιμετώπιση μιας επίθεσης, η Brenner (2006) έθιξε τις εθνικές δικαιοδοσίες και τον διεθνικό χαρακτήρα του εγκλήματος στον κυβερνοχώρο. Ο Keyser (2002) περιέγραψε με ποιον τρόπο οι κυβερνοεγκληματίες και οι κακόβουλοι φορείς είτε στηρίζουν τις δραστηριότητές τους σε κομητείες εκτός των νομικών πλαισίων, όπως η σύμβαση για το έγκλημα στον κυβερνοχώρο, είτε δρομολογούν την κυκλοφορία τους μέσω των χωρών αυτών. Ο Kohl (2002) μίλησε για το πώς μια απάντηση σε μια επίθεση στον κυβερνοχώρο γίνεται τότε ερώτημα για το ποια χώρα ή υπηρεσία επιβολής του νόμου έχει την ευθύνη και την αρμοδιότητα να διερευνήσει, σύμφωνα με το οποίο το νομικό πλαίσιο μπορεί να διωχθεί από τους δράστες και ποιοι νόμοι ισχύουν.

Αυτό το διακρατικό ζήτημα διερευνήθηκε πιο πρόσφατα στο εγχειρίδιο του Ταλίν για το διεθνές δίκαιο που εφαρμόζεται στον κυβερνοπόλεμο (Schmitt, 2013) κατά τη συζήτηση των πράξεων ενός εθνικού κράτους. Ο κανόνας 6 περιέγραφε πώς ένα εθνικό κράτος "φέρει διεθνή νομική ευθύνη για μια κυβερνοεπιχείρηση που αποδίδεται σε αυτό", αλλά αναγνώρισε ότι η τοποθεσία από την οποία έλαβε χώρα η

επίθεση δεν καθορίζει απαραιτήτως εάν το εν λόγω εθνικό κράτος είναι υπεύθυνο. Περιέγραψε ένα σενάριο σύμφωνα με το οποίο το Εθνικό Κράτος Α, σύμφωνα με τις οδηγίες του Εθνικού Κράτους Δ, δημιούργησε ένα δίκτυο τερματικών στο Εθνικό Κράτος Β για να επιτεθεί σε στόχους στο Εθνικό Κράτος Γ (Εικόνα 1). Υπό αυτές τις συνθήκες, το Εγχειρίδιο του Ταλίν όριζε ότι το Εθνικό Κράτος Β δεν μπορούσε να θεωρηθεί υπεύθυνο για την επίθεση, και ότι το Εθνικό Κράτος Δ, από το οποίο προέρχεται η πρόθεση, μπορούσε να αποδοθεί στις ενέργειες. Η συμμετοχή του Εθνικού Κράτους Α συζητήθηκε ως λιγότερο προσδιορισμένη περιοχή, καθώς δεν μπορούσε να θεωρηθεί υπεύθυνη λόγω του γεγονότος ότι η κίνηση επίθεσης προήλθε από εκεί. Για άλλη μια φορά, απαίτησε τη λήψη μέτρων για τον καθορισμό της νομικής ευθύνης.



Σχήμα 6. Παράδειγμα της πολυπλοκότητας της ευθύνης του κράτους-έθνους στην απόδοση (Πηγή: An illustration of the complexity of nation-state responsibility in attribution)

Επομένως, είναι προφανές ότι, υπό το πρίσμα των ασάφειας των διεθνών νόμων, οι μέθοδοι που αποδίδουν την εκτέλεση μιας επίθεσης πρέπει να περιλαμβάνουν όχι μόνο την τεχνική ανοικοδόμηση της πορείας της επίθεσης στην πηγή, αλλά και ένα μέσο με το οποίο επιτυγχάνεται η πρόθεση του δράστη. Ομοίως, προκειμένου να υποστηριχθεί η απόφαση του ποιος πρέπει να απαντήσει σε ένα συμβάν, απαιτείται μια ταξινόμηση των τύπων επίθεσης, προκειμένου να καταστεί δυνατή η διεθνής κατανόηση της φύσης και του αντικτύπου των επιδράσεων στον κυβερνοχώρο. Η σημασία αυτής της εκτίμησης αυξάνεται κατά προτεραιότητα, εάν το βιομηχανικό σύστημα ελέγχου δεχθεί επίθεση, έχει ως αποτέλεσμα απώλεια ζωών ή σημαντικό αντίκτυπο σε ένα εθνικό κράτος. Υπό το πρίσμα αυτού του κινδύνου, είναι ίσως πιο πρακτικό να επικεντρωθούμε στην αποτροπή παρά στη δίωξη.

Ο Libicki (2009), αναφορικά με τις κυβερνοεπιθέσεις στο πλαίσιο του κυβερνοπολέμου, υποστήριξε ότι "οι κυβερνοεπιθέσεις μπορούν να εκτοξευτούν κυριολεκτικά από οπουδήποτε, συμπεριλαμβανομένων των ίντερνετ-καφέ, των ανοιχτών κόμβων WiFi και των υποδεέστερων υπολογιστών τρίτων, δεν απαιτούν σπάνια ή ακριβά μηχανήματα και δεν αφήνουν κανένα ίχνος. Έτσι, η απόδοση είναι συχνά εικασία. Αξίζει να σημειωθεί πως η ασυγκράτητη απόδοση δεν είναι απαραίτητη για την αποτροπή όσο οι δράστες μπορούν να πειστούν ότι οι ενέργειές τους μπορεί να προκαλέσουν αντίποινα. Ωστόσο, μπορεί να είναι απαραίτητες κάποιες αποδείξεις υπό το πρίσμα (1) ότι ο δράστης μπορεί να πιστεύει ότι μπορεί να ταρακουνήσει την πεποίθηση του αντιποίνων ότι έχει δίκιο κάνοντας τίποτα διαφορετικό σε απάντηση αντιποίνων, (2) ότι η

εσφαλμένη απόδοση προκαλεί νέους εχθρούς και (3) ότι ουδέτεροι παρατηρητές μπορεί να χρειαστεί να πειστούν ότι τα αντίποινα δεν είναι επιθετικότητα" (Libicki, 2009).

Αν και η αναφορά παραβιάσεων της ασφάλειας αυξάνεται, υπάρχουν ελάχιστα διαθέσιμα στοιχεία για τον εντοπισμό των πηγών τέτοιων επιθέσεων. Το πρόβλημα της απόδοσης των επιπτώσεων στον κυβερνοχώρο είναι, γενικά, ένα καλά τεκμηριωμένο ζήτημα, ωστόσο, ελάχιστα έχουν προκύψει από την ακαδημαϊκή ή βιομηχανική έρευνα για να ικανοποιηθούν οι νομικές απαιτήσεις για την ακρίβεια, ώστε να υποστηριχθεί η δίωξη των εμπνευστών των επιθέσεων. Οι τεχνικές που διαθέτουν οι δράστες για να συγκαλύψουν την τοποθεσία και την πορεία τους για να στοχεύσουν, δημιουργούν υπερβολική αβεβαιότητα σε ένα δικαστήριο (Geers, 2010).

3.2. Απόδοση Κυβερνοεπιθέσεων

Η απόδοση των κυβερνοεπιθέσεων σε περιβάλλοντα ICS αποτελεί σημαντική πρόκληση σε σύγκριση με την απόδοση των κυβερνοεπιθέσεων σε εταιρικά περιβάλλοντα. Παρακάτω εντοπίζονται αυτές οι διαφορές, όπως και το τι σημαίνει αυτό για την απόδοση.

Το ICS διαφέρει από τις παραδοσιακές αρχιτεκτονικές τεχνολογίας πληροφορικής, καθώς γενικά δεν διαθέτει όλες τις δυνατότητες IP και ενσωματώνει ορισμένα πρωτόκολλα αποκλειστικής εκμετάλλευσης ή ειδικά για τον κλάδο πρωτόκολλα που βασίζονται σε σειριακές επικοινωνίες ή επικοινωνίες με λεωφορεία. Ακόμη και όταν χρησιμοποιείται IP, οι απαιτήσεις απόδοσης απαιτούσαν τη χρήση τροποποιημένων IP ή βελτιστοποιημένων δρομολογητών που περιορίζουν το διαθέσιμο επίπεδο ελέγχου και επιθεώρησης. Τα πρωτόκολλα αυτά αναπτύσσονται σε διαφορετικά επίπεδα της αρχιτεκτονικής και συχνά απαιτούν πύλες για διαλειτουργικότητα (Galloway & Hancke, 2012).

Αυτό το ετερογενές περιβάλλον επικοινωνιών παρέχει διάφορες συσκευές μέτρησης και ελέγχου και συχνά λειτουργούν για 10-20 χρόνια με τα ίδια λειτουργικά συστήματα και λειτουργούν με περιορισμένη υπολογιστική ικανότητα, σχεδιασμένες για απόδοση και αξιοπιστία αντί για ασφάλεια (Carr, 2014).

Το ICS είναι ένας γενικός όρος που περιλαμβάνει μια οικογένεια τεχνολογιών αυτοματοποίησης διεργασιών, συμπεριλαμβανομένων των συστημάτων εποπτικού ελέγχου και απόκτησης δεδομένων (Supervisory Control and Data Acquisition - SCADA) και των κατανεμημένων συστημάτων ελέγχου (Distributed Control Systems - DCS). Αυτά τα συστήματα ελέγχου χρησιμοποιούν προγραμματιζόμενους λογικούς ελεγκτές (Programmable Logic Controllers - PLC) ή παρόμοιες μονάδες απομακρυσμένου τερματικού (Remote Terminal Units - RTU) και έξυπνες ηλεκτρονικές συσκευές (Intelligent Electronic Devices - IED) για τη διαχείριση ηλεκτρομηχανικού εξοπλισμού σε τοπικά ή κατανεμημένα περιβάλλοντα. Η εφαρμογή τους καλύπτει μια σειρά βιομηχανικών τομέων και κρίσιμων υποδομών, όπως παραγωγή και

διανομή ηλεκτρικής ενέργειας, επεξεργασία και παροχή νερού, διύλιση πετρελαίου, παραγωγή τροφίμων και διοικητική μέριμνα (Nickolson et al., 2013).

Τα εν λόγω συστήματα ελέγχου παρέχουν αυτοματοποίηση και έλεγχο των διαδικασιών των συστημάτων που παρέχουν την αξιόπιστη ροή προϊόντων και υπηρεσιών που απαιτούνται για την ασφάλεια και τις λειτουργίες των βιομηχανικών κρατών-εθνών. Ως παράδειγμα των διαφορών μεταξύ ICS και συμβατικής IT επιχειρήσεων, ο Πίνακας 1 συγκρίνει ένα PLC με έναν γενικευμένο υπολογιστή IT. Κατά την εξέταση της ποικιλομορφίας των συστημάτων βιομηχανικού ελέγχου, είναι χρήσιμο να υπάρχει ένα κοινό πλαίσιο στο οποίο να καθορίζονται οι κοινές πτυχές αυτών των συστημάτων και τα επίπεδα ιεραρχίας των διαδικασιών που υπάρχουν (Moteff, & Parfomak, 2004).

Ο Williams (1994) περιέγραψε το μοντέλο Purdue, μια αρχιτεκτονική αναφοράς για την ιεραρχία ελέγχου που έχει καταστεί το πρότυπο στο πλαίσιο του ICS (Zhu et al., 2011). Περιέγραψε έξι επίπεδα στο πλαίσιο ενός οργανισμού που διαχειρίζεται ένα σύστημα βιομηχανικού ελέγχου, όπως φαίνεται στην Εικόνα 3.

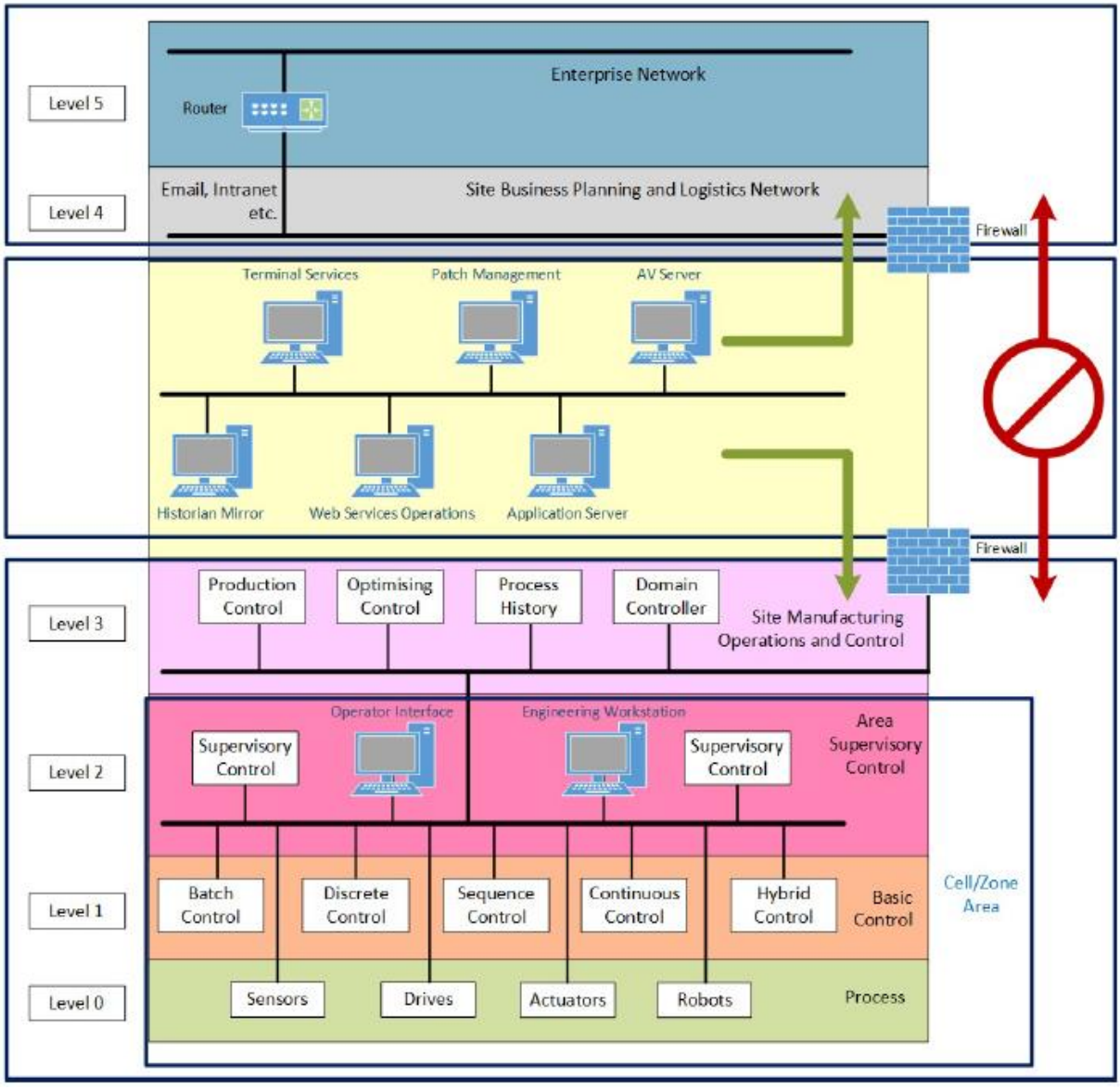
Πίνακας 1. PLC έναντι υπολογιστή γενικής χρήσης

PLC	Υπολογιστής
Ανθεκτική σχεδίαση για βιομηχανικά περιβάλλοντα	Σχεδιασμένη κυρίως για επεξεργασία και υπολογισμό δεδομένων
Ικανότητα λειτουργίας σε υψηλές θερμοκρασίες και υγρασία	Περιορισμένο εύρος περιβάλλοντος
Υψηλή ατρωσία στο θόρυβο σήματος	Βελτιστοποιημένη για ταχύτητα
Ενσωματωμένος διερμηνέας εντολών αποκλειστικής ιδιοκτησίας	Υποστήριξη για περιβάλλοντα πολλαπλής ανάπτυξης
Περιορισμένη μνήμη	Σημαντική και επεκτάσιμη μνήμη
Βελτιστοποιημένος για επεξεργασία μονού νήματος	Δυνατότητα εκτέλεσης πολλαπλών εργασιών

Το επίπεδο 5 περιγράφει το εταιρικό δίκτυο ενός οργανισμού που εκτελεί τις εφαρμογές και τις υπηρεσίες διαχείρισης επιχειρήσεων. Σε αυτό το επίπεδο υπάρχει πρόσβαση στο Internet. Το επίπεδο 4 παρουσιάζει τις υπηρεσίες διαχείρισης του σχεδιασμού, του προγραμματισμού και της εφοδιαστικής των επιχειρήσεων. Το επίπεδο 3 περιλαμβάνει τη διαχείριση των καθημερινών βιομηχανικών δραστηριοτήτων της μονάδας, συμπεριλαμβανομένου του προγραμματισμού της παραγωγής, της εξασφάλισης της ποιότητας, της βελτιστοποίησης των διεργασιών κ.λ.π. Το επίπεδο 2 παρέχει εποπτικό έλεγχο του εξοπλισμού που συμμετέχει στη συνολική βιομηχανική διαδικασία. Το επίπεδο 1 περικλείει τον έλεγχο μεμονωμένων συσκευών και εξοπλισμού που εμπλέκονται σε διακριτά στοιχεία της συνολικής διαδικασίας (PLC, RTU, BE

κ.λπ.) Το επίπεδο 0 περιλαμβάνει τις συσκευές, τους αισθητήρες και τον σχετικό εξοπλισμό που εκτελεί τη βιομηχανική διαδικασία.

Αν και το μοντέλο αναφοράς Purdue δεν χρησιμοποιείται για τη διαχείριση των υλοποιήσεων ICS, αντικατοπτρίζει τις γενικές αρχιτεκτονικές αρχές που έχουν υιοθετηθεί, σύμφωνα με τις οποίες η διαχείριση του ελέγχου του βιομηχανικού εξοπλισμού γίνεται σε ιεραρχία με επίπεδα, η οποία λογικά, αν όχι φυσικά, είναι διαχωρισμένη από τη διαχείριση της βιομηχανικής εγκατάστασης και τις επιχειρηματικές διαδικασίες της. Σημαντικό είναι ότι καθορίζει τις περιοχές μιας αρχιτεκτονικής βιομηχανικού ελέγχου όπου τα πρωτόκολλα βάσει IP μεταβαίνουν σε παλαιότερες σειριακές επικοινωνίες.



Σχήμα 7. Purdue Model για την ιεραρχία στοιχείων ελέγχου (Πηγή: Purdue Model for Control Hierarchy)

Στην περίπτωση επίθεσης στον κυβερνοχώρο κατά του ICS είναι πιθανό να υπάρξει κάποια πραγματική φυσική εκδήλωση της κατάχρησης. Στις χειρότερες περιπτώσεις αυτό θα μπορούσε να έχει ως αποτέλεσμα ζημίες, τραυματισμούς, περιβαλλοντικές επιπτώσεις ή απώλεια ζωών. Στις περιπτώσεις αυτές, όπου είναι πιθανό να απαιτηθεί κάποια νομική ή κανονιστική έρευνα, η σημασία της ανάθεσης των τεχνουργημάτων αυξάνεται. Θα ήταν απαραίτητο να προσδιοριστεί αν η συμπεριφορά του ICS προκλήθηκε από σφάλμα στις λειτουργίες της εγκατάστασης, βλάβη συσκευής ασφαλείας ή αν οι διαδικασίες και οι συσκευές χειραγωγήθηκαν κακόβουλα για την επίτευξη του τελικού αποτελέσματος. Αυτά τα τεχνουργήματα, ιδανικά, θα πρέπει να είναι σε μορφή που να εγγυάται την αυθεντικότητά τους και να εντοπίζει την κυκλοφορία και τις εντολές ICS καθ' όλη τη διάρκεια της επιχειρησιακής διαδικασίας, διασφαλίζοντας ολοκληρωμένη ακεραιότητα. Η διασφάλιση αυτή πρέπει να περιλαμβάνει τα αρχεία καταγραφής των συσκευών και των κατασκευαστικών στοιχείων που έλεγχαν τον σχετικό βιομηχανικό εξοπλισμό.

3.3. Ταξινόμηση Τεχνικών Ανάθεσης των Κυβερνοεπιθέσεων

Επί του παρόντος, οι μελέτες σχετικά με το φάσμα των τεχνικών ανάθεσης για επιθέσεις κατά του ICS είναι περιορισμένες. Η ταξινόμηση των τεχνικών ανάθεσης των επιθέσεων στον κυβερνοχώρο από τους Nicholson et al. (2012) παρέχει μια επισκόπηση των διαθέσιμων τεχνικών επιλογών και ταξινομεί τις αποδιδόμενες και πρακτικές τους πτυχές. Μια πρώτη έρευνα για την απόδοση στα συστήματα SCADA, επίσης από τους Nicholson et al (2012), διερευνά πέντε γνωστές τεχνικές ανάθεσης και συζητά τη βιωσιμότητά τους σε ένα περιβάλλον ICS. Οι ερευνητές έχουν ερευνήσει μεμονωμένες τεχνικές προσεγγίσεις στην απόδοση, μεταξύ άλλων: ανίχνευση - όπου η κυκλοφορία από μια συσκευή-στόχο πραγματοποιείται διαδοχικά μέσω της διαδρομής δρομολόγησής της προς την πηγή προέλευσης και τις κυψέλες - όπου φιλοξενούνται ευάλωτα λογισμικά και υπηρεσίες προκειμένου να είναι δυνατή η παρακολούθηση των δραστηριοτήτων.

Οι Kuznetsov et al. (2002) αξιολόγησαν τέσσερις προσεγγίσεις ανίχνευσης. Τα κριτήριά τους αξιολόγησαν τον αριθμό των απαιτούμενων πακέτων, την πολυπλοκότητα, την ευρωστία και την ευκολία υλοποίησης. Διαπίστωσαν ότι οι τρέχουσες προσεγγίσεις βρίσκονται σε μειονεκτική θέση, καθώς χρειάζονται μεγάλο αριθμό επιθετικών πακέτων και χρειάζονται αλλαγές στην υποδομή του Διαδικτύου. Οι Kuznetsov et al. (2002) κατέληξαν στο συμπέρασμα ότι μια καλύτερη λύση θα ήταν η ενσωμάτωση της λειτουργικότητας παρακολούθησης εντός των βασικών διαδικτυακών συσκευών.

Οι Belenky & Ansari (2003) πρότειναν ένα πλαίσιο για την αξιολόγηση των συστημάτων ιχνηλάτησης IP. Τα κριτήριά τους για τις ιδιότητες ιχνηλάτησης περιλαμβάνουν επιπτώσεις της μερικής υλοποίησης, της επεξεργασίας και της υπέρβασης του εύρους ζώνης, απαιτήσεις μνήμης και δυνατότητα

κλιμάκωσης. Οι ίδιοι θεωρούν ότι κανένα σύστημα ιχνηλασιμότητας δεν μπορεί να ικανοποιήσει κάθε κριτήριο.

Οι Strayer et al. (2003) παρήγαγαν μια ταξινόμηση τεχνικών ανίχνευσης σκαλοπατιών και αξιολόγησαν τις εξής πέντε τεχνικές ανίχνευσης: Πιθανή σήμανση πακέτων (Probabilistic Packet Marking - PPM), ICMP Traceback (iTrace), Προσδιοριστική σήμανση πακέτων (Deterministic Packet Marking - DPM), Μηχανισμός απομόνωσης πηγαίου-διαύλου (Source-Path Isolation Engine - SPIE) και υβριδική προσέγγιση CenterTrack, που ταξινομείται βάσει παραγόντων όπως υπολογιστική επιβάρυνση και αξιοπιστία.

Οι Hamadeh & Kesidis (2006) συνέταξαν μια ταξινόμηση των τεχνικών Internet Traceback, διαχωρίζοντας το πρόβλημα σε ανίχνευση IP, ανίχνευση κατά μήκος σκαλοπατιών και ανίχνευση σκωλήκων. Οι Vincent & Raja (2010) δημοσίευσαν έρευνα σχετικά με τους μηχανισμούς παρακολούθησης IP, εξετάζοντας συγκεκριμένα την υπέρβαση των επιθέσεων DoS με τη χρήση των εξής δύο τύπων τεχνικών ανίχνευσης IP: σήμανση πακέτων και καταγραφή πακέτων, με μια εξερεύνηση ενός υβριδικού από αυτά και τα δύο. Αυτές οι ταξινομήσεις και έρευνες εστιάζουν σε συγκεκριμένες κατηγορίες τεχνικών, οι οποίες αποτελούν κάθε μία κατηγορία στον τομέα της τεχνικής ανάθεσης και ως εκ τούτου, είναι περιορισμένες στην προσέγγισή τους όταν εξετάζουν ολιστικά την απόδοση, αυτές οι έρευνες δεν διαθέτουν σημαντικές τεχνικές όταν δεν τις καλύπτουν όλες.

Οι Wheeler & Larsen (2003) ήταν οι πρώτοι που ταξινόμησαν το τοπίο των τεχνικών τεχνικής απόδοσης και ως εκ τούτου, επικρίνουν τα συνδυασμένα πλεονεκτήματά τους. Μια σειρά ταξινομήσεων ακολούθησαν αυτή την προσέγγιση. Για παράδειγμα, οι Thing et al. (2009) εξέτασαν μια σειρά τεχνικών ανάθεσης στο πλαίσιο προσαρμοστικών απαντήσεων σε επιθέσεις DoS. Ο Blakely (2012) θεώρησε επίσης την ανίχνευση ως μηχανισμό για τον εντοπισμό των επιτιθέμενων στον κυβερνοχώρο με ανάλυση χαρακτηριστικών. Η πρόθεση επίθεσης διερευνήθηκε από τον Duggan (2005) και περιελάμβανε αξιολόγηση της ικανότητας επίθεσης. Η έρευνα πρότεινε ένα σύνολο έξι προφίλ παραγόντων γενικής απειλής και το επίπεδο επάρκειάς τους σε επτά χαρακτηριστικά, μεταξύ των οποίων: διαθέσιμη χρηματοδότηση, αποφασιστικότητα, στεγανότητα, φυσική πρόσβαση στο στόχο, δεξιότητες ανάπτυξης λογισμικού, ο χρόνος που θα ήταν αντιληπτός για την ανάπτυξη ενός αποτελέσματος και τελικά το μέγεθος του οργανισμού που απαιτείται για την ανάπτυξη του αποτελέσματος.

Ο Barnum (2008) περιέγραψε ένα πιο λεπτομερές μοντέλο δυνατοτήτων. Στην ταξινόμηση αυτή τα επτά χαρακτηριστικά ουσιαστικά αποσυντίθενται σε χαμηλότερο επίπεδο κοκκιογραφίας. Ο Barnum στην έρευνά του περιελάμβανε επίσης τη σοβαρότητα των επιπτώσεων. Οι Miller & Rowe (2012), σε μια έρευνα για την SCADA και τα συμβάντα κρίσιμης υποδομής, περιελάμβαναν τον αντίκτυπο της επίθεσης, αναφέροντας τα αποτελέσματα των επιδράσεων στον κυβερνοχώρο στο ICS όπως διακοπή, στρέβλωση, καταστροφή, αποκάλυψη ή θάνατος.

Οι Fleury et al. (2008) δεν καλύπτουν τα κίνητρα ή τις προθέσεις, αλλά πρότειναν ένα πλαίσιο βασισμένο σε ένα μοντέλο "ευπάθειας-ζημίας" (attack vulnerability damage AVD). Οι Zhu et al. (2011) περιέγραψαν μια ταξινόμηση των επιθέσεων στον κυβερνοχώρο στα συστήματα SCADA και εισήγαγαν τον εσωτερικό χαρακτήρα του ICS στις διάφορες μεθόδους επίθεσης που αντιμετωπίζουν αυτά τα συστήματα. Η έρευνα εξήγησε την εστίαση στην ακεραιότητα και τη διαθεσιμότητα των δεδομένων εντός των συστημάτων αυτών, με μια αισθητή μειωμένη ανάγκη (τουλάχιστον στο παρελθόν) για εμπιστευτικότητα. Συνέχισαν αναφέροντας παραδείγματα διαφόρων επιφανειών και διανυσμάτων επίθεσης, αλλά δεν προσέφεραν ένα επαναλαμβανόμενο μοντέλο για κατηγοριοποίηση και ανάλυση των επιθέσεων. Αυτές οι ταξινομήσεις και έρευνες εστιάζουν σε συγκεκριμένες κατηγορίες τεχνικών, οι οποίες αποτελούν κάθε μία κατηγορία στον τομέα της τεχνικής ανάθεσης, και ως εκ τούτου, είναι περιορισμένες στην προσέγγισή τους όταν εξετάζουν ολιστικά την απόδοση, αυτές οι έρευνες δεν διαθέτουν σημαντικές τεχνικές και όταν δεν τις καλύπτουν όλες.

Οι Wheeler & Larsen (2003) ήταν οι πρώτοι που ταξινόμησαν το τοπίο των τεχνικών τεχνικής απόδοσης και ως εκ τούτου, επικρίνουν τα συνδυασμένα πλεονεκτήματα τους. Μια σειρά ταξινομήσεων ακολούθησαν αυτή την προσέγγιση. Για παράδειγμα, οι Thing et al. (2009) εξέτασαν μια σειρά τεχνικών ανάθεσης, όπως και ο Blakely (2012). Καμία από τις επιμέρους ταξινομήσεις που εξετάστηκαν δεν προσφέρει το επίπεδο λεπτομέρειας που απαιτείται για τον επαρκή καθορισμό της πρόθεσης, της ικανότητας, του επιπέδου εκμετάλλευσης και του αντίκτυπου μιας επίθεσης σε ένα ICS, αλλά αξίζει να εξεταστεί το ενδεχόμενο μιας συγχώνευσης διαφόρων στοιχείων τους, προκειμένου να δημιουργηθεί ένα μοντέλο επαρκούς αξιοπιστίας για την υποστήριξη ενός διεθνούς ορισμού του αποτελέσματος μιας επίθεσης, ώστε να καταστεί δυνατή η συμφωνία σχετικά με τους τρόπους και τα μέσα για την κατανομή ευθυνών και πόρων για τη διερεύνηση.

Δεδομένου ότι καμία από τις ταξινομήσεις που εξετάστηκαν δεν παρέχει το απαιτούμενο επίπεδο λεπτομέρειας, είναι επομένως αναγκαίο να επανεξεταστούν οι επιμέρους τεχνικές. Προκειμένου να αξιολογηθεί η χρησιμότητα μιας τεχνικής ανάθεσης στο ICS, απαιτείται ένα σύνολο κριτηρίων βάσει των οποίων, μπορεί να κριθεί η αποτελεσματικότητα της τεχνικής. Τα παρακάτω χαρακτηριστικά έχουν χρησιμοποιηθεί για τη μέτρηση της αποτελεσματικότητας κάθε μεθόδου κατανομής στο πλαίσιο ενός βιομηχανικού συστήματος.

- **Απόδοση:** Η δυνατότητα παροχής λειτουργιών απόδοσης χωρίς υποβάθμιση της απόδοσης του ICS.
- **Αξιοπιστία:** Ικανότητα παροχής λειτουργιών ανάθεσης χωρίς να επηρεάζονται αρνητικά οι διαδικασίες λειτουργίας και ασφάλειας της εγκατάστασης ICS.
- **Έκταση:** Δυνατότητα παρακολούθησης της κυκλοφορίας από την πηγή προέλευσης στην τελική συσκευή ICS, συμπεριλαμβανομένων όλων των μετασχηματισμών πρωτοκόλλου κατά τη διαδρομή, για την παροχή πλήρους εικόνας της συμπεριφοράς του δικτύου.

- **Συνοχή:** Η δυνατότητα παραπομπής της κυκλοφορίας με συμπεριφορές συσκευών ICS μέσω του συγχρονισμού των αρχείων καταγραφής συσκευών για να επιτραπεί ο έλεγχος της εκτέλεσης της εντολής.
- **Ταυτοποίηση:** Η ικανότητα αναγνώρισης του επιτιθέμενου από συμπεριφορές ή τεχνικές υπογραφές.
- **Πρόθεση:** Η ικανότητα προσδιορισμού του σκοπού της επίθεσης, είτε είναι επιτυχής είτε όχι, για την παροχή κατάλληλων αποδεικτικών στοιχείων και μέσων προκειμένου να υποστηριχθεί η δίωξη.

3.4. Ανασκόπηση Τεχνικών Απόδοσης

3.4.1. Traceback

Το Traceback είναι μια κατηγορία μεθόδων που περιλαμβάνει τεχνικές με τις οποίες η επισκεψιμότητα από μια συσκευή προορισμού αναδρομικά υποχωρεί μέσω της διαδρομής δρομολόγησης προς τη συσκευή προέλευσης (Stefan Savage et al., 2000).

Οι (Kuznetsov et al., 2002) συγκέντρωσαν τη σημαντική έρευνα σε αυτόν τον τομέα σε τρεις διαφορετικές προσεγγίσεις και αξιολόγησαν την πρακτικότητά τους. Η πρώτη κατηγορία περιελάμβανε μη αυτόματες μεθόδους **traffic tracing** και απαιτούσε τη συσκευή δρομολόγησης για τον εντοπισμό σφαλμάτων εισόδου, καθώς και τον περιορισμό της περιόδου ανάλυσης στη διάρκεια της ίδιας της επίθεσης. Η δεύτερη κατηγορία διέθετε τεχνικές καταγραφής, σύμφωνα με τις οποίες οι δρομολογητές διατηρούν πληροφορίες σχετικά με την κίνηση που αντιμετώπισαν.

Αυτά περιγράφηκαν ως μη πρακτικά εξαιτίας των απαιτήσεων αποθήκευσης ενός τέτοιου μηχανισμού. Μια παραλλαγή, ωστόσο, οι τεχνικές μηχανής απομόνωσης διαδρομής πηγής (Source Path Isolation Engine- SPIE) των (Snoeren et al., 2001) ικανές να εντοπίσουν τη διαδρομή ενός μόνο πακέτου μέσω δρομολογητών συμβατών με SPIE, θα μπορούσαν να εντοπίσουν τα ζητήματα αποθήκευσης που αντιμετωπίστηκαν συλλέγοντας μόνο κατακερματισμούς των πακέτων. Ενώ αυτό μείωσε τα γενικά έξοδα αποθήκευσης, οι (Gao & Ansari, 2005) υπογράμμισαν ότι οι υπολογιστικές απαιτήσεις αυξήθηκαν. Η τρίτη κατηγορία περιελάμβανε τις διάφορες μεθόδους πιθανότητας σήμανσης πακέτων (PPM) και ICMP traceback (iTrace).

Το PPM, που προτάθηκε αρχικά από τους (Savage et al., 2000), και επεκτάθηκε από τους (Song & Perrig, 2001) και (Belinky & Ansari, 2003), χρησιμοποίησε σήμανση πακέτων για δειγματοληψία ενός αριθμού πακέτων με δεδομένα διαδρομής, ώστε σε περίπτωση που μια συσκευή-στόχος λάβει επαρκή όγκο τέτοιων πακέτων θα μπορούσε να ανακατασκευάσει ολόκληρη τη διαδρομή πίσω προς την πηγή. Οι πληροφορίες σήμανσης αποθηκεύονται σε αχρησιμοποίητα ή σπάνια χρησιμοποιούμενα πεδία κεφαλίδας

πακέτων, όπως το πεδίο αναγνώρισης (Identification field)16-bit. Οι (Savage et al., 2000) πρότειναν ότι 75 πακέτα θα ήταν επαρκή όταν το μήκος της διαδρομής είναι 10 και ο αριθμός των επιτιθέμενων είναι μικρός. Όταν ο αριθμός των επιτιθέμενων είναι μεγάλος, αυτή η τεχνική καθίσταται αναποτελεσματική. Χιλιάδες πακέτα απαιτούνται και ο χρόνος σύγκλισης αυξάνεται.

Οι (Song & Perrig, 2001) πρότειναν Προηγμένα και Αυθεντικά Σχέδια Σήμανσης (Advanced and Authenticated Marking Schemes- AMS και AMS II). Η AMS προχωρά στην εργασία των (Savage et al.,) συμπιέζοντας ολόκληρα δεδομένα παρακολούθησης στο πεδίο Αναγνώρισης. Το AMS II παρουσίασε έλεγχο ταυτότητας ώστε κάθε δρομολογητής να χρησιμοποιεί ένα μοναδικό μυστικό κλειδί για την επισήμανση πακέτων. Παρά τις τροποποιήσεις αυτές, η τεχνική παρέμεινε αδύναμη ενάντια στις κατανεμημένες επιθέσεις άρνησης υπηρεσίας (Distributed Denial of Service-DDoS) και την πλαστογράφηση. Ο (Goodrich, 2002) στην εργασία του πρότεινε το μοντέλο Τυχαιοποίησης και Σύνδεσης (Randomize-and-Link) που αποσκοπούσε στην αντιμετώπιση αυτών των αδυναμιών. Αυτή η τεχνική χρησιμοποίησε μεγάλα αθροίσματα ελέγχου για να συνδέσει πακέτα σε ένα ευρύ φάσμα που σημαίνει ότι ελαχιστοποιήθηκε η πιθανότητα παραβίασης ενός εισβολέα. Τέλος, οι (Belenky & Ansari, 2003) πρότειναν το ντετερμινιστικό πακέτο σήμανσης (Deterministic Packet Marking-DPM), το οποίο είχε ως στόχο να σταματήσει την πλαστογράφηση και να επιτρέψει την χαμηλή ποσότητα πακέτου.

Το iTrace, που προσφέρθηκε για πρώτη φορά από τους (Bellovin et al, 2003), δημιούργησε μηνύματα ICMP εκτός ζώνης που περιέχουν την ίδια διεύθυνση προορισμού IP, όπως και την κεφαλίδα IP του πακέτου που εντοπίστηκε. Περιέλαμβανε επίσης, τη διεύθυνση IP των εισερχόμενων και εξερχόμενων διεπαφών. Εφ' όσον η συσκευή θύματος-στόχου είχε λάβει αρκετά από αυτά τα μηνύματα θα μπορούσε να ανακατασκευάσει τη διαδρομή επίθεσης, αν και αυτό εξαρτιόταν από τον σωστό χειρισμό της κυκλοφορίας ICMP σε όλα τα στάδια της διαδρομής. Οι (Kim et al., 2005) υπογράμμισαν την εξάρτηση από αυτήν τη μέθοδο στις σωστές διαδρομές δρομολόγησης BGP, τις ανεπάρκειες του ελέγχου ταυτότητας BGP και της παρακολούθησης των αλλαγών. Πρότειναν μια επαυξημένη μέθοδο iTrace σύμφωνα με την οποία AS-PATH και δεδομένα σύνδεσης συνδέθηκαν επίσης, στο μήνυμα προκειμένου να διευκολυνθεί η σωστή επικύρωση της δρομολόγησης μέσω αυτόνομων συστημάτων.

Οι μέθοδοι Traceback απαιτούν συνήθως μια τροποποίηση στην δομή δικτύου στην οποία θα λειτουργούν και είναι αμφισβητήσιμο πόσο αποδοτικό θα ήταν αυτό δεδομένης της κλίμακας του σύγχρονου Διαδικτύου. Το πιο σημαντικό, ωστόσο, είναι ότι όλες οι τεχνικές ανίχνευσης, συμπεριλαμβανομένου ενός υβριδικού μοντέλου που προτάθηκε από τους (Korkmaz et al., 2007), απέτυχαν στο να αντιμετωπίσουν τη φύση των σύγχρονων επιθέσεων πολλαπλών σταδίων που περιεγράφηκαν στην εργασία των (Clark & Landau, 2010), όπου οι ενδιάμεσες συσκευές εξαναγκάζονται από κακόβουλο λογισμικό να διεισδύσουν σε έναν υπολογιστή τον οποίο χρησιμοποιούν ως πλατφόρμα για επίθεση σε ένα δεύτερο κλπ., σε μια

συνεχιζόμενη διαδικασία συρρίκνωσης του πρωτουργού. Στην καλύτερη περίπτωση, θα αποδώσουν την επίθεση μόνο σε μια εξαναγκασμένη συσκευή.

Οι τεχνικές ανίχνευσης υποφέρουν από διάφορα προβλήματα που σημαίνει ότι η ανάπτυξη στο περιβάλλον του Διαδικτύου είναι απίθανη. Οι τεχνικές αυτές παρέχουν άμεσα τεχνουργήματα, όπως η διεύθυνση προέλευσης IP, ωστόσο, δεδομένου ότι οι διευθύνσεις IP ενδέχεται να σχετίζονται με παραβιασμένα μηχανήματα, αυτό το στοιχείο είναι ελάχιστα χρήσιμο. Είναι χρήσιμο, μόνο εάν ο κάτοχος του τελικού σημείου διεύθυνσης IP είναι πρόθυμος να συνεργαστεί πλήρως και να επιτρέψει την εγκληματολογική έρευνα των μηχανημάτων τους. Το Traceback είναι ενοχλητικό και απαιτεί αλλαγές στη δομή για ανάπτυξη και τροποποιήσεις πακέτων/δρομολογητών, πρόσθετη κίνηση ή πρόσθετες απαιτήσεις αποθήκευσης και επεξεργασίας. Επιπλέον, το βάρος του ποιος πρέπει να διαχειριστεί αυτές τις πτυχές είναι ασαφές. Τέλος, οι τεχνικές ανίχνευσης μπορούν να εισαγάγουν νέους φορείς επίθεσης. Για παράδειγμα, η καταγραφή πακέτων παράγει επιπλέον κίνηση και θα μπορούσε να προκαλέσει από μόνη της επίθεση DDoS.

3.4.2. Honeypots

Τα Honeypots προσεγγίζουν το ζήτημα της απόδοσης των επιθέσεων με διαφορετικές μεθόδους από αυτές των Traceback, παρατηρώντας μια επίθεση επί τόπου. Το honeypot είναι ένα σύστημα ή ένα σύνολο συστημάτων, όπου φιλοξενούνται ευάλωτα προγράμματα και υπηρεσίες προκειμένου να επιτρέπεται η παρακολούθηση και καταγραφή των δραστηριοτήτων.

Οι (Franz & Pothamsetty, 2008), δημιούργησαν το πρώτο δημοσίως αναγνωρισμένο SCADA honeypot. Ο στόχος τους ήταν να προσδιορίσουν τη δυνατότητα δημιουργίας ενός πλαισίου λογισμικού για την προσομοίωση μιας ποικιλίας βιομηχανικών δικτύων και συσκευών. Διαπίστωσαν ότι υπήρχε γενική έλλειψη πληροφοριών σχετικά με τις ευπάθειες και τις επιθέσεις της SCADA. Παρασκευάστηκε ένα τεχνικό παραδοτέο, ένα SCADA honeypot βασισμένο σε ένα χαμηλό επίπεδο αλληλεπίδρασης, το Honeyd, το οποίο προσομοίωσε πολλά πρωτόκολλα δικτύου όπως HTTP, SMTP και FTP.

Το Honeyd θα μπορούσε να επεκταθεί για να προσομοιώσει περισσότερα πρωτόκολλα δικτύου χρησιμοποιώντας απλά σενάρια. Οι Franz και Pothamsetty δημιούργησαν σενάρια για την προσομοίωση της λειτουργικότητας SCADA μιας συσκευής Modicon Quantum με υπηρεσίες HTTP, FTP, Telnet και Modbus. Δημιούργησαν επίσης, μια μικροεφαρμογή Java, την "StatusApplet.java", η οποία θα μπορούσε να έχει πρόσβαση μέσω ενός διακομιστή ιστού και να προσομοιώσει την κατάσταση μιας συσκευής πεδίου SCADA. Η τεχνική υλοποίηση αυτού του honeynet ήταν πρωτόγονη. Στη συνέχεια, καταβλήθηκε μικρή προσπάθεια για την απόκρυψη της κατάστασης του honeypot. Για παράδειγμα, το συμβάν δράσης στις φόρμες HTML διαβάζει 'action = "honeyd-feedback.py" ", μια ένδειξη ότι το σύστημα SCADA είναι στην πραγματικότητα ένα honeypot.

Οι ερευνητές στο Digital Bond επεκτάθηκαν στην εργασία των Franz και Pothamsetty όταν κυκλοφόρησαν δύο εικονικές εικόνες VMWare (Wade, 2011). Μία εικόνα περιείχε ένα SCADA honeypot βασισμένο στην εργασία των Franz και του Pothamsetty και μια άλλη περιείχε το Honeywall για την παρακολούθηση της δραστηριότητας, τη συλλογή δεδομένων και την αποτροπή εξερχόμενων συνδέσεων από παραβιασμένα honeypots. Το Digital Bond περιελάμβανε επίσης τους κανόνες Quickdraw τους, μια συλλογή προεπεξεργαστών και προσθηκών συστήματος (Snort Intrusion Detection-IDS) ειδικά για πρωτόκολλα SCADA. Αυτό που έκανε αυτό το έργο μοναδικό ήταν, ότι η εικόνα Honeywall θα μπορούσε να τοποθετηθεί μπροστά, είτε από το SCADA honeypot, είτε από ένα πραγματικό PLC χωρίς παραγωγή. Η τελευταία διαμόρφωση ήταν σημαντική επειδή επέτρεψε τη χρήση μιας φυσικής συσκευής SCADA ως honeypot.

Τον επόμενο χρόνο οι (Rrushi & Campbell, 2008), συνέχισαν την τάση της χρήσης πραγματικών συσκευών όταν πρότειναν τη «θεωρία αντικατοπτρισμού αντιδραστήρων». Η πρότασή τους αποσκοπούσε στη χρήση εξαπάτησης για τον εντοπισμό εισβολών στον τομέα της πυρηνικής ενέργειας. Το πρωτότυπο τους έπαιρνε ενεργές αποφάσεις για να προσελκύσει τους αντιπάλους προς ένα honeypot που χρησιμοποιούσε πραγματικές βιομηχανικές συσκευές ως honeypots. Γεμίζοντας το περιβάλλον με παραπλανητικά συστήματα αύξησαν την πιθανότητα ενός αντιπάλου να στοχεύει ένα μη παραγωγικό σύστημα. Ομοίως, χρησιμοποιώντας πραγματικές συσκευές ως συστήματα εξαπάτησης και δημιουργώντας προσομοιωμένη δραστηριότητα, την κίνηση πρωτόκολλου Modbus, αύξησαν τον ρεαλισμό και μείωσαν την πιθανότητα ενός αντιπάλου να ανακαλύψει ότι αλληλεπιδρά με ένα honeypot. Παρά αυτά τα οφέλη, το κόστος που σχετίζεται με την ανάπτυξη πολλών πραγματικών συσκευών για λόγους εξαπάτησης είναι υψηλό και κάθε αύξηση της κυκλοφορίας του δικτύου άμεσα ή έμμεσα σε ένα δίκτυο παραγωγής SCADA θα πρέπει να προσεγγιστεί με προσεκτικό έλεγχο.

Σε μια άλλη ακαδημαϊκή πρόταση το 2009, ο (Valli, 2009) περιέγραψε ένα πλαίσιο εγκληματολογίας SCADA το οποίο συνδύαζε το Snort IDS με δύο honeypots χαμηλής αλληλεπίδρασης, τα Honeyd και Nepenthes. Η ιδέα ήταν να ξαναπαιχθούν γνωστές SCADA εκμεταλλεύσεις σε ένα ελεγχόμενο εργαστήριο για να δημιουργήσουμε κανόνες IDS δικτύου που θα επηρέαζαν τις διαμορφώσεις για τα δύο honeypots. Ωστόσο, δεν είναι σαφές εάν αυτή η αρχική πρόταση έλαβε περαιτέρω προσοχή.

Οι (Dacier et al., 2009) θεώρησαν ότι η απόδοση στη μελέτη τους σχετικά με τα χαμηλής αλληλεπίδρασης honeypots διαφέρει από εκείνη του traceback, δηλαδή «προσδιορισμός της ταυτότητας ή της θέσης ενός εισβολέα ή ενός ενδιάμεσου επιτιθέμενου». Αντ 'αυτού, πλησίασαν το ζήτημα όσον αφορά τον καθορισμό μιας σειράς "γεγονότων επίθεσης" που παρατηρήθηκαν για να μοντελοποιήσουν την έξοδο των εισβολέων. Τα συμβάντα επίθεσης περιελάμβαναν μια σειρά συμβάντων μικροεπίθεσης που εμφανίστηκαν κατά τη διάρκεια παρατηρούμενων χρονικών περιόδων, τα οποία στη συνέχεια αναλύθηκαν για να προσπαθήσουν να δημιουργήσουν συνδέσεις μεταξύ τους προκειμένου να σχηματίσουν ένα σύνολο δραστηριοτήτων σε ένα "Κακής συμπεριφοράς σύννεφο" (Misbehaving Cloud-MC).

Το έγγραφο απεικόνισε διάφορα μέσα για να συσχετίσει τις παρατηρούμενες δραστηριότητες σε τέτοια MC σε επίπεδο επίθεσης, καταδεικνύοντας έτσι τις τεχνικές επίθεσης, αλλά δεν εφαρμόζεται σε μια ευρύτερη ανάλυση των δεδομένων που διαφημίζονται στα honeypots και τη συσχέτιση μεταξύ της μεθόδου επίθεσης και του τελικού στόχου του εισβολέα. Οι (Pouget et al., 2004), προσπάθησαν να το αντιμετωπίσουν σε μια μεταγενέστερη εργασία που χρησιμοποίησε αλγόριθμους συμπλέγματος για να αναλύσει τα δεδομένα που συλλέχθηκαν από ένα honeypot και παρουσίασε μεθόδους για τον εντοπισμό των βασικών αιτίων των επιθέσεων, δηλώνοντας ότι «ο εντοπισμός των βασικών αιτίων είναι απαραίτητη προϋπόθεση για την καλύτερη κατανόηση κακόβουλης δραστηριότητας ». Ωστόσο, τα αποτελέσματα δεν πρότειναν ένα πλαίσιο στο οποίο να προσπαθήσει κανείς να αξιολογήσει την πρόθεση του επιτιθέμενου.

Ο (Spitzner, 2003) επισήμανε τους περιορισμούς των honeypots λόγω του στενού οπτικού πεδίου που διαθέτουν, και ότι επιτρέπουν μόνο την εστίαση σε επιθέσεις εναντίον συγκεκριμένων στόχων (δηλαδή το honeypot). Τόνισε ότι, ενώ η λήψη δεδομένων μπορεί να είναι πολύ πλούσια, δεν περιλαμβάνει όλη τη γύρω συμπεριφορά που μπορεί να συμβεί έξω από το honeypot και η οποία, πιθανόν, να υποδηλώνει τα ευρύτερα συμβάντα που σχετίζονται με μια επίθεση.

3.4.3. Ψηφιακή Εγκληματολογική Τεχνική

Η Ψηφιακή Εγκληματολογία είναι ένα ευρύ θέμα που περιλαμβάνει την ανάκτηση, απόκτηση και διερεύνηση ψηφιακών στοιχείων. Σε παραδοσιακούς τομείς πληροφορικής, τα εμπορικά εργαλεία όπως το EnCase (Guidance Software, 2016) και το FTK (FTK, 2016) και τα εργαλεία ανοιχτού κώδικα όπως το Sleuthkit και το Autopsy (sleuthkit.org, 2016) χρησιμοποιούνται για την απόκτηση, ανάλυση και αναφορά ψηφιακών αποδεικτικών στοιχείων. Αυτά τα εργαλεία τείνουν να είναι ειδικά για αρχιτεκτονικές επεξεργαστών x86 και x64 και στοχεύουν σε συστήματα αρχείων, όπως FAT, NTFS και δημοφιλή λειτουργικά συστήματα, όπως τα Windows και το Linux.

Η εγκληματολογία σε ένα περιβάλλον SCADA θα μπορούσε να εντοπίσει δεδομένα απόδοσης για τον εντοπισμό των δραστών. Στο τμήμα δικτύου SCADA και σε τμήματα συσκευών πεδίου υπάρχει ένα ευρύ φάσμα συσκευών που μπορούν να αποθηκεύσουν πληθώρα ψηφιακών στοιχείων. Ωστόσο, τα συστήματα SCADA έρχονται με ένα μοναδικό σύνολο προκλήσεων για εγκληματολογική ανάλυση. Για παράδειγμα, η τυπική εγκληματολογική διαδικασία για την απόκτηση δίσκου bit-for-bit περιλαμβάνει την απενεργοποίηση ενός συστήματος, τη σύνδεση του σκληρού δίσκου με ένα σύστημα αποκλεισμού εγγραφής και απόκτησης και στη συνέχεια την αναμονή για την ολοκλήρωση της απόκτησης. Η απενεργοποίηση ενός συστήματος SCADA που παρακολουθεί και ελέγχει κρίσιμη υποδομή είναι απίθανο να είναι μια επιλογή. Ένας τρόπος για να μετριαστεί αυτό το ζήτημα είναι η αποτυχία σε συστήματα. Ωστόσο, το παραπάνω είναι δαπανηρό και εάν

το σύστημα αποτυχίας είναι αντίγραφο του αρχικού συστήματος, μπορεί να μολυνθεί με τον ίδιο ακριβώς τρόπο.

Η ποικιλία των συσκευών που μπορεί να αντιμετωπίσει ένας εγκληματολογικός ερευνητής στο περιβάλλον SCADA είναι ευρύτερη από αυτήν του παραδοσιακού τομέα πληροφορικής. Τα παραδοσιακά συστήματα πληροφορικής έχουν διάρκεια ζωής μερικών ετών, ίσως το πολύ 10, ενώ το ICS θα παραμείνει σε λειτουργία για 20 χρόνια (Naedele, 2007), (Barbosa, 2014). Ωστόσο, καθώς τα PLC και άλλες συσκευές SCADA συνεχίζουν να κινούνται προς εμπορικό υλικό και λογισμικό, η εγκληματολογική ανάλυση των συστημάτων SCADA γίνεται τυποποιημένη και επομένως απλούστερη.

Μεταξύ των διαφορετικών συσκευών που βρέθηκαν σε περιβάλλοντα SCADA είναι ο Ιστορικός (Historian), ο οποίος ουσιαστικά είναι ένα σύστημα διαχείρισης βάσεων δεδομένων (DBMS). Συλλέγει πληθώρα δεδομένων που επιτρέπουν τον έλεγχο, την ανάλυση τάσεων και τον εντοπισμό ανωμαλιών. Ως DBMS, οι παραδοσιακές τεχνικές εγκληματολογικής βάσης δεδομένων θα πρέπει να είναι κατάλληλες για αυτές τις συσκευές. Ωστόσο, σε αντίθεση με τον Ιστορικό, πολλές από αυτές τις συσκευές που παρουσιάζονται είναι απίθανο να έχουν μόνιμη μνήμη. Είναι αλήθεια ότι «τα περισσότερα συστήματα ελέγχου διεργασιών δεν δημιουργήθηκαν για να παρακολουθούν τις διαδικασίες τους, αλλά απλώς για τον έλεγχο αυτών» (Nance et al., 2009). Για παράδειγμα, το Siemens S7-300 PLC χρησιμοποιεί μια micro κάρτα μνήμης (micro memory card-MMC) για αποθήκευση (Siemens, 2013) που κυμαίνεται από 64KB έως 8MB, ενώ η ενσωματωμένη μνήμη CPU για αυτήν τη συσκευή κυμαίνεται από 32KB έως 2MB.

3.4.5. Εγκληματολογία Δικτύου

Ένας άλλος τομέας της εγκληματολογίας που χρησιμοποιείται στα παραδοσιακά συστήματα πληροφορικής είναι η εγκληματολογία δικτύου. Αυτό το πεδίο περιλαμβάνει κυρίως δύο στάδια: συλλογή μηνυμάτων δικτύου και ανάλυση μηνυμάτων δικτύου. Η υπάρχουσα υποδομή, όπως διακόπτες και δρομολογητές, μπορεί να ρυθμιστεί για τη συλλογή μηνυμάτων ή μπορεί ακόμη να αναπτυχθεί επιπλέον εξοπλισμός, όπως μια συσκευή βρύσης δικτύου. Με την καταγραφή μηνυμάτων σε αρχεία, η ανάλυση μπορεί να πραγματοποιηθεί κατά τη διάρκεια μιας επίθεσης ή μετά την επίθεση. Κατά την ανάλυση της κίνησης δικτύου, μπορούν να βρεθούν δεδομένα απόδοσης, όπως πηγή σύνδεσης, χρόνος σύνδεσης, εντολές που εστάλησαν και δεδομένα ωφέλιμου φορτίου.

Η συλλογή δεδομένων είναι σχετικά απλή. Ένας οργανισμός πρέπει να προσδιορίσει σημεία στο δίκτυο από όπου επιθυμεί να συλλέξει δεδομένα δικτύου. Οι (Mahmood et al., 2010) περιέγραψαν παραδοσιακά προβλήματα ανάλυσης δικτύου και ανάπτυξη δικτύου sniffer σε περιβάλλον SCADA. Ένας τομέας που θα απαιτήσει περαιτέρω προσοχή είναι όταν χρησιμοποιούνται παραδοσιακά κανάλια επικοινωνίας εκτός του Ethernet, όπως RS232 και η ραδιοσύνδεση. Σε αυτήν την περίπτωση θα απαιτηθούν

ειδικοί sniffers. Η επισκεψιμότητα πρέπει να αποθηκεύεται σε γνωστές μορφές λήψης δικτύου, όπως το PCAP. Το Wireshark, ένα δημοφιλές εργαλείο sniffer δικτύου και αναλυτών πακέτων, έχει ήδη διαχωριστικά για ορισμένα πρωτόκολλα SCADA, όπως Modbus (National Instruments Inc, 2014), DNP3 (Curtis, 2005) και FINS (Omron, 2012), ένα ιδιόκτητο πρωτόκολλο, ωστόσο υπάρχουν πολλά πρωτόκολλα SCADA που δεν υποστηρίζονται.

Η πλήρης λήψη πακέτων σε ένα παραδοσιακό σύστημα πληροφορικής μπορεί να προκαλέσει προβλήματα λόγω του μεγάλου όγκου και του μεγάλου μεγέθους πακέτων. Σε ένα περιβάλλον SCADA ο όγκος της κυκλοφορίας είναι γενικά πολύ χαμηλότερος και τα μεγέθη των μηνυμάτων είναι πολύ μικρότερα. Το περιεχόμενο των μηνυμάτων είναι πιθανό να είναι ελαφρώς διαφορετικό, καθώς το περιεχόμενο δημιουργείται από μηχανή και όχι από χρήστη. Αυτό έχει ως αποτέλεσμα συσκευές συλλογής δικτύου που απαιτούν λιγότερη ισχύ αποθήκευσης και επεξεργασίας, πράγμα που σημαίνει ότι οι οργανισμοί μπορούν να εξοικονομήσουν χρήματα ή να αναπτύξουν περισσότερες συσκευές.

3.4.6. Ανάλυση κακόβουλου λογισμικού

Το κακόβουλο λογισμικό, στις διάφορες μορφές του: ο ιός, το worm, το trojan, το adware, το spyware, οι πίσω πόρτες (back doors) και τα rootkit, μπορούν να αναλυθούν για να προσδιοριστούν χαρακτηριστικά που θα μπορούσαν να χρησιμοποιηθούν ως πηγή δεδομένων απόδοσης. Η ανάλυση κακόβουλου λογισμικού στον παραδοσιακό τομέα IT μπορεί να χωριστεί σε δύο τομείς: ανάλυση συμπεριφοράς και ανάλυση κώδικα.

Η ανάλυση συμπεριφοράς εξετάζει τον τρόπο με τον οποίο το κακόβουλο λογισμικό αλληλεπιδρά με το περιβάλλον. Το κακόβουλο λογισμικό ενδέχεται να κάνει αλλαγές στο μητρώο, να δημιουργήσει νέες διεργασίες, να αποκρύψει αρχεία, να εκτελέσει άλλα δυαδικά αρχεία, να επικοινωνήσει με διακομιστές εντολών και ελέγχου, να καλύψει κομμάτια διαγράφοντας αποδεικτικά στοιχεία για τις τροποποιήσεις του (όπως έκανε το Stuxnet), να απενεργοποιήσει προστασία ασφαλείας, να καταγράψει αλληλεπίδραση χρήστη (π.χ. keylogging) , να συγκεντρώσει ευαίσθητα δεδομένα, να εξάγει δεδομένα, να αποπειραθεί ενημέρωση, να περιστρέφεται γύρω από άλλα συστήματα, να δημιουργεί πίσω πόρτες και πολλά άλλα. Συνήθως δημιουργείται ένα ελεγχόμενο περιβάλλον δοκιμών για την εξέταση αυτής της συμπεριφοράς. Οι εικονικές μηχανές χρησιμοποιούνται συνήθως για αυτήν την εργασία, καθώς μπορούν να επαναφερθούν γρήγορα με λειτουργίες snapshot/roll-back. Διατίθεται ένα ευρύ φάσμα εργαλείων για την ανάλυση συμπεριφοράς κακόβουλου λογισμικού στον παραδοσιακό τομέα πληροφορικής, όπως η ακολουθία Microsoft Windows SysInternals (Microsoft, 2016).

Η απόκριση ή η έλλειψη απόκρισης βοηθά στον εντοπισμό του τί κάνει το κακόβουλο λογισμικό. Η διαδικασία ανάλυσης συμπεριφοράς μπορεί να αυτοματοποιηθεί με εργαλεία όπως το CWSandbox (sandbox.org, 2016) που παρακολουθεί τις κλήσεις συστήματος των Windows που πραγματοποιούνται από

κακόβουλο λογισμικό. Τα εργαλεία και τα περιβάλλοντα ανάλυσης συμπεριφοράς περιορίζονται αρκετά σε λειτουργικά συστήματα που χρησιμοποιούνται σε παραδοσιακά περιβάλλοντα πληροφορικής π.χ. Windows και Linux. Δεν υποστηρίζουν όμως το υλικολογισμικό που βρίσκεται σε SCADA PLC και RTUs. Οι (Ahmed et al., 2012) εντόπισαν ότι θα πρέπει να δημιουργηθούν περιβάλλοντα προσομοίωσης SCADA, πιθανώς από πανεπιστήμια και βιομηχανίες, και αυτό σίγουρα θα βοηθούσε στην διόρθωση του ζητήματος.

Η ανάλυση κώδικα αφορά την εξέταση του κώδικα που αποτελεί το κακόβουλο λογισμικό. Ο πηγαίος κώδικας για κακόβουλο λογισμικό μπορεί να είναι διαθέσιμος, αν και είναι απίθανο. Εάν ωστόσο συμβαίνει αυτό, τότε μπορεί να πραγματοποιηθεί ανάλυση του κώδικα αυτού. Διαφορετικά, πραγματοποιείται αντίστροφη μηχανική και εντοπισμός σφαλμάτων. Η αντίστροφη μηχανική περιλαμβάνει την επαναφορά του δυαδικού κώδικα μηχανικού κακόβουλου λογισμικού σε αναγνώσιμο από τον άνθρωπο κώδικα συναρμολόγησης, χρησιμοποιώντας εργαλεία όπως το IDA Pro (Hunker et al., 2008) και το OllyDbg (OllyDbg.de, 2016). Αυτά τα εργαλεία είναι ιδιαίτερα αποτελεσματικά στην αναστροφή δυαδικών αρχείων που έχουν συνταχθεί για αρχιτεκτονικές επεξεργαστών x86, x64 και ARM. Ο κώδικας μπορεί στη συνέχεια να εκτελεστεί σε ένα πρόγραμμα εντοπισμού σφαλμάτων για να ακολουθήσει τις οδηγίες, να επιθεωρήσει το περιεχόμενο εγγραφής, να εντοπίσει ενσωματωμένες συμβολοσειρές και να ορίσει σημεία διακοπής για να προσδιορίσει τη λειτουργικότητα του κακόβουλου λογισμικού.

3.4.7. Απόδοση βάσει πληροφοριών

Ορισμένες -μη τεχνικές- ερευνητικές τεχνικές μπορεί να προσφέρουν εναλλακτικές ή συμπληρωματικές προσεγγίσεις για την ανάθεση της απόδοσης σε μια επίθεση στον κυβερνοχώρο. Για τους σκοπούς αυτής της έρευνας, αυτές έχουν κατηγοριοποιηθεί ως «τεχνικές που οδηγούνται από την ευφυΐα» (âAŸintelligence-ledâAZ techniques)

Καθώς οι τεχνικές τεχνικής απόδοσης προσφέρουν περιορισμένους και ποικίλους βαθμούς δεδομένων με δυνατότητα δράσης. Ο (Carr, 2011) πρότεινε ότι «ένα πράγμα που είναι σίγουρο, είναι ότι κάποιος πρέπει να πληρώσει για τις ανάγκες της εικονικής μάχης. Επομένως, μια ορθή στρατηγική σε οποιαδήποτε έρευνα στον κυβερνοχώρο είναι να ακολουθηθεί το ίχνος χρημάτων που δημιουργήθηκε από την απαραίτητη εφοδιαστική για την οργάνωση μιας κυβερνο-επίθεσης - εγγραφή τομέα, υπηρεσίες φιλοξενίας, απόκτηση λογισμικού, εύρος ζώνης και ούτω καθεξής. "Τόνισε ότι παρόλο που οι ψευδείς ταυτότητες χρησιμοποιούνται συχνά κατά την εγγραφή και την απόκτηση υπηρεσιών, η αυξημένη χρήση των μέσων κοινωνικής δικτύωσης και το αυξανόμενο μέγεθος των ατομικών και εταιρικών ψηφιακών αποτυπωμάτων επιτρέπει μια εγκληματολογική εξέταση της διαδικτυακής παρουσίας και ταυτότητας και μπορεί να αποκαλύψει τέτοιες εξαπατήσεις. Οι (Gantz & Chute, 2008) υπολόγισαν ότι υπήρχαν περίπου 45 GB δεδομένων για κάθε άτομο στον πλανήτη. Συζήτησαν επίσης, την ανάλυση του «Digital Shadows» AZ,

για τα δεδομένα περιεχομένου περιβάλλοντος που δημιουργήθηκαν από κάμερες κυκλοφορίας, χρήση ATM, διαδικτυακές συναλλαγές κ.λπ.

Μια ανάλυση της υποτιθέμενης συμπεριφοράς της κινεζικής επίθεσης σε υπολογιστή (Mandiant Intelligence Center, 2013) που προέκυψε από μια επταετή μυστική παρατήρηση και προσέφερε μια εικόνα για την κλίμακα και την πολυπλοκότητα των επιθέσεων κατά του ICS. Οι στόχοι περιελάμβαναν μεταφορά, πλοήγηση, μηχανική, τρόφιμα και γεωργία, χημικά, ενέργεια, αεροδιαστημική και εξόρυξη - οπουδήποτε ήταν πιθανό να χρησιμοποιηθούν βιομηχανικά συστήματα ελέγχου. Η απόδοση της παρατηρούμενης συμπεριφοράς επίθεσης στην Κίνα, βασίστηκε σε ένα συνδυασμό τεχνικών μέτρων και έξυπνης συλλογής και ανάλυσης δεδομένων πληροφοριών. Συγκεκριμένα, η έκθεση επικεντρώθηκε σε ομοιότητες μεταξύ μεθόδων επίθεσης, συνέπειας στις συμβάσεις ονομασίας και συγκριτικής ανάλυσης κακόβουλου λογισμικού.

Τόσο η (Fireeye, 2013) όσο και ο (Shivraj, 2011) περιέγραψαν τη συνέπεια στη συμπεριφορά επίθεσης που παρατηρήθηκε από κοινές πηγές. Η Fireye αξιοποίησε τη θέση της ως προμηθευτή εμπορικών προϊόντων ασφαλείας για να συγκεντρώσει και να αναλύσει την επιστροφή επισκεψιμότητας και εκδηλώσεων APT προκειμένου να καθιερώσει πρότυπα συμπεριφοράς και διοίκησης και ελέγχου της κυκλοφορίας. Ο (Shivraj, 2011) καθόρισε τα στάδια της σύγχρονης συμπεριφοράς APT με έμφαση στις επιθέσεις SCADA και επεσήμανε πώς μπορούν να εφαρμοστούν κοινές προσεγγίσεις κακόβουλου λογισμικού σε στόχους ICS με περιορισμένη τροποποίηση, τουλάχιστον στα αρχικά στάδια μιας επίθεσης. Τα συνδυασμένα ευρήματα και των δύο εργασιών θα μπορούσαν ενδεχομένως να συνδυαστούν για να παρέχουν μια ένδειξη της απόδοσης επίθεσης και μια απτή αξιολόγηση του πού βρίσκεται ο στόχος στον κύκλο επίθεσης, και συνεπώς, ποια προληπτικά μέτρα μπορεί να είναι κατάλληλα.

Κεφάλαιο 4ο : Ανασκόπηση Κυβερνοαπειλών στα ΒΣΕ

4.1. Σημεία σε ΒΣΕ που Εκτίθενται σε Κυβερνοαπειλές

Τα σημεία που εκθέτουν το βιομηχανικό σύστημα ελέγχου σε κυβερνο-επιθέσεις, διαιρούνται κυρίως, σε τρεις ευρύτερες κατηγορίες. Πρώτον, η φυσική ασφάλεια του τρόπου με τον οποίο ο εισβολέας φθάνει φυσικά στο σύστημα-στόχο, συμπεριλαμβανομένων και των δύο ΟΤ ή ΙΤ συστημάτων, που εκτίθενται κυρίως σε στοιχεία επιπέδου δικτύου και συστήματος. Παρόλο που αυτή η μελέτη των (Mounesh Marali et al., 2020) δεν εστίασε σε βάθος τη φυσική ασφάλεια, είναι εξίσου σημαντική με τη λογική ασφάλεια. Μερικές από τις βασικές απειλές φυσικής ασφάλειας εκτέθηκαν από στοιχεία που λείπουν, όπως, στοιχεία παρακολούθησης ασφάλειας, βασικά στοιχεία ελέγχου πρόσβασης, πυρασφάλεια, αδιάλειπτα τροφοδοτικά και φυσική κλοπή υπολογιστικών συσκευών (Vávra & Hromada, 2015).

Δεύτερον, οι θεμελιώδεις απειλές στις οποίες υπόκεινται τα συστήματα ΟΤ και ΙΤ από εσκεμμένες ή τυχαίες επιθέσεις κατηγοριοποιούνται σε σημεία ως ακολούθως (Luiijf, 2016):

- **Ακεραιότητα:** Η ακεραιότητα αναφέρεται σε λειτουργίες συστήματος και δεδομένα που δεν προστατεύονται από την τροποποίηση από μη εξουσιοδοτημένα άτομα ή συστήματα. Για βιομηχανικά συστήματα ελέγχου, αυτό ειδικά σχετίζεται με λειτουργίες και δεδομένα που επηρεάζουν άμεσα ή έμμεσα τη διαδικασία, όπως προγράμματα ελέγχου, συνταγές προϊόντων, τιμές αισθητήρα ή εντολές ελέγχου. Η απώλεια ακεραιότητας αυτών μπορεί να προκαλέσει απώλεια παραγωγής και στη χειρότερη περίπτωση σωματική βλάβη.
- **Εμπιστευτικότητα:** Η Εμπιστευτικότητα αναφέρεται σε ορισμένες πληροφορίες που δεν προστατεύονται από την αποκάλυψή τους σε μη εξουσιοδοτημένα άτομα ή συστήματα. Για τα συστήματα βιομηχανικού ελέγχου αυτό αφορά κυρίως πληροφορίες όπως συνταγές προϊόντων και δεδομένων απόδοσης του εργοστασίου και παραγωγής, τα οποία μπορεί να αντιπροσωπεύουν πολύτιμη πνευματική ιδιοκτησία και επιχειρηματικά περιουσιακά στοιχεία. Η απώλεια εμπιστευτικότητας για αυτούς τους τύπους πληροφοριών μπορεί να προκαλέσει σημαντικές οικονομικές απώλειες. Επίσης, πρέπει να προστατεύονται τα μυστικά των ίδιων των μηχανισμών ασφαλείας, όπως κωδικοί πρόσβασης και κλειδιά κρυπτογράφησης - εάν αποκαλυφθούν, το σύστημα καθίσταται απροστάτευτο από επιθέσεις.
- **Διαθεσιμότητα:** Οι στόχοι διαθεσιμότητας αναφέρονται σε μη εξουσιοδοτημένους χρήστες που δεν εμποδίζονται από την άρνηση νόμιμης πρόσβασης ή χρήσης των λειτουργιών του συστήματος, π.χ. υπερφορτώνοντάς το ή προκαλώντας κατάρρευση αυτού. Για βιομηχανικά συστήματα ελέγχου, το παραπάνω ιδιαίτερα σχετίζεται με λειτουργίες που εμπλέκονται άμεσα ή έμμεσα στον έλεγχο της διαδικασίας, όπως οι ελεγκτές και το πεδίο Ι / Ο, αλλά και η ικανότητα των χειριστών να

παρακολουθούν και να ελέγχουν τη διαδικασία. Η απώλεια διαθεσιμότητας αυτών των λειτουργιών μπορεί να προκαλέσει απώλεια παραγωγής και πιθανώς και σωματική βλάβη.

- **Έλεγχος ταυτότητας:** Αναφέρεται στην έλλειψη δυνατότητας ταυτοποίησης και χαρτογράφησης προφίλ χρηστών με τα έγκυρα δικαιώματα τους λογαριασμού και πρόσβασης και προστασία από μη εξουσιοδοτημένες αλλαγές στο σύστημα ελέγχου. Μερικά καλύτερα παραδείγματα θα μπορούσαν να είναι ο ελλιπής έλεγχος πρόσβασης βάσει ρόλου σε συστήματα OT ή μη εξουσιοδοτημένες επικοινωνίες σε δίκτυα OT / IPSec.
- **Εξουσιοδότηση:** Αναφορά σε ελλιπή στοιχεία ελέγχου πρόσβασης από μη εξουσιοδοτημένους χρήστες που έχουν πρόσβαση στα βιομηχανικά συστήματα ελέγχου και εφαρμόζουν αλλαγές που επηρεάζουν τα συστήματα OT και IT με συνέπεια να προκύπτουν θέματα ασφάλειας του εργοστασίου.
- **Μη προστατευμένα δίκτυα:** Αναφέρεται σε ελλιπή στοιχεία στην ασφάλεια πρωτοκόλλου διαδικτύου (internet protocol security-IPSec) για την προστασία της εσωτερικής επικοινωνίας του τομέα και των δικτύων διακομιστή πελατών. Κόμβοι συστήματος OT χωρίς τείχη προστασίας που βασίζονται σε κεντρικούς υπολογιστές: Στα δίκτυα OT λείπουν ενσωματωμένα ειδικά τείχη προστασίας μεταξύ ελεγκτών και των μονάδων επικοινωνίας τους που προστατεύουν από ανεπιθύμητη επικοινωνία και υπερφόρτωση που προκαλείται από καταιγίδες δικτύου.
- **Ανασφαλής αρχιτεκτονική:** Η αρχιτεκτονική συστήματος που δεν διαθέτει καθιερωμένες αρχές ασφαλείας, όπως η άμυνα σε βάθος και οι ζώνες ασφαλείας. Η αρχή των Ζωνών Ασφαλείας σημαίνει τμηματοποίηση ενός συστήματος σε διαφορετικές ζώνες για διαφορετικά επίπεδα ασφάλειας. Οι πόροι του συστήματος πληροφορικής (IT) ποικίλουν στο βαθμό κατά τον οποίο μπορούν να θεωρηθούν αξιόπιστοι για να μην παραβιαστούν. Μια κοινή αρχιτεκτονική ασφάλειας βασίζεται επομένως σε μια πολυεπίπεδη προσέγγιση που χρησιμοποιεί ζώνες εμπιστοσύνης για την παροχή αυξανόμενων επιπέδων ασφάλειας ανάλογα με τις αυξανόμενες ανάγκες ασφάλειας. Κάθε ζώνη βρίσκεται μέσα στην επόμενη, οδηγώντας από το λιγότερο ασφαλές στο πιο αξιόπιστο.

Τρίτον, η έλλειψη ασφάλειας από το σχεδιασμό εκθέτει τα βιομηχανικά συστήματα ελέγχου με ανοιχτές απειλές στον κύκλο ζωής των προϊόντων τους. Για να επιτευχθούν όλοι οι στόχοι ασφάλειας, η ασφάλεια στον κυβερνοχώρο πρέπει να ενσωματωθεί σε κύκλο ζωής βιομηχανικών συστημάτων ελέγχου από τη φάση σχεδιασμού, ανάπτυξης, δοκιμών και θέσης σε λειτουργία. Επιπλέον, η ασφαλής λειτουργία του εργοστασίου πρέπει να διασφαλίσει τη λειτουργία του βιομηχανικού συστήματος ελέγχου και η ασφάλειά και των δύο είναι ενσωματωμένη στο σύστημα διαχείρισης ποιότητας. Οι επίσημες επικυρώσεις της συμμόρφωσης ασφαλείας με τα πρότυπα ασφαλείας και η ανάλυση & μοντελοποίηση απειλών παρέχουν τη βάση για τις απαιτήσεις ασφαλείας και τις αρχές σχεδιασμού του συστήματος. Τα σημεία ελέγχου ασφαλείας στις πύλες

του έργου ανάπτυξης πρέπει να διασφαλίζουν την επίτευξη των στόχων ασφαλείας (Vávra & Hromada, 2015).

4.2. Οργανωτικές Απειλές στα ΒΣΕ

Σε αυτήν την ενότητα παρουσιάζονται διάφορες πτυχές της απειλής για τους επιχειρηματικούς στόχους λόγω των οργανωτικών πτυχών που σχετίζονται με ICS.

4.2.1. Αρχιτεκτονικές και Τεχνολογικές Απειλές

Όπως φαίνεται σε μεγαλύτερα περιβάλλοντα ελεγχόμενα από το ICS, για παράδειγμα ένα διυλιστήριο, ένα σύνολο απειλών πηγάζει από την ανάγκη να γίνουν οι παλαιές τεχνολογίες ICS συμβατές με τις νέες τεχνολογίες, τις πτυχές της γήρανσης και της παλαιότητας, και την άγνωστη χρήση μιας νέας λειτουργικότητας χωρίς διαμόρφωση. Μικρότερα περιβάλλοντα ICS ενδέχεται να αντιμετωπίσουν μερικές από αυτές τις προκλήσεις. Ο μετριασμός των περισσότερων απειλών που σχετίζονται με την τεχνολογία, ωστόσο, δεν απαιτεί τεχνολογικές αλλαγές, αλλά αλλαγές στην οργανωτική ηγεσία (εσωτερικό ζήτημα) και αλλαγή νοοτροπίας κατασκευαστών και ολοκληρωτών συστημάτων (έλεγχος εξωτερικών αποκτημένων υπηρεσιών) (BSI 2014) και αποτελεί ένα πρώτο βήμα προς αυτήν την κατεύθυνση.

4.2.2. Παλαιά Τεχνολογία

Καθώς τα στοιχεία ICS έχουν μεγάλη διάρκεια ζωής, η χωρητικότητα επεξεργασίας και μνήμης μπορεί να είναι πολύ περιορισμένη για την εκτέλεση νεότερων εφαρμογών ICS. Η αντιμετώπιση τέτοιων στοιχείων εμποδίζει την εφαρμογή ή/και την ενεργοποίηση κρυπτογραφικών μονάδων ασφαλείας που απαιτούν ισχύ και μνήμη επεξεργαστή, απαραίτητες και οι δύο για τον έλεγχο των διεργασιών. Επιπλέον, πολλά στοιχεία και λογισμικά εφαρμογών ICS αναπτύχθηκαν κατά την περίοδο ανάπτυξης σε ένα καλοηθές περιβάλλον, όπου μόνο ένα περιορισμένο σύνολο χρηστών κατανοούσε το εσωτερικό των ICS. Οι εργοστασιακοί προεπιλεγμένοι κωδικοί πρόσβασης ενσωματώθηκαν βαθιά στο υλισμικό και το λογισμικό. Δεν ήταν συνηθισμένη πρακτική η αντικατάσταση αυτών των εργοστασιακών προεπιλεγμένων κωδικών πρόσβασης παρόλο που υπήρχε και αυτό ως επιλογή. Η Stuxnet (βλ. Ενότητα 6.3) κατάφερε να παραβιάσει έναν ενσύρματο κωδικό πρόσβασης στο προϊόν Siemens WinCC SCADA που ελέγχει τις φυγόκεντρες εμπλουτισμού ουρανίου στο Nąţanz του Ιράν (Falliere, 2011). Χρειάστηκε πολύς χρόνος έως ότου η Siemens να επιτρέψει σε άλλους χρήστες των προϊόντων να αλλάξουν τον εργοστασιακό κωδικό πρόσβασης, καθώς δεν μπορούσε να εκτιμήσει την επίδραση στα λειτουργικά συστήματα που θα είχε η αλλαγή του κωδικού πρόσβασης (Espiner 2010).

Η γήρανση των εξαρτημάτων ICS επιφέρει νέα απειλή: οι κατασκευαστές παύουν να υπάρχουν ή για άλλους λόγους δεν είναι σε θέση να προμηθεύουν ανταλλακτικά. Στην εργασία του ο (Luiijf 2016) συνάντησε οργανισμούς με μηχανικούς συντήρησης που είναι ειδικοί στην συγκόλληση και αντικατάσταση ελαττωματικών τρανζίστορ, πυκνωτών και διακριτών λογικών τσιπ σε PLC και συναφών εξαρτημάτων. Όταν η επισκευή γίνει ανέφικτη, μπορεί να χρειαστεί πολύς χρόνος έως ότου οι διαδικασίες που ελέγχονται από το ICS να λειτουργήσουν ξανά κανονικά. Η διαχείριση τέτοιων οργανισμών δηλώνει ότι ο χειροκίνητος έλεγχος των ελεγχόμενων διαδικασιών είναι μια εναλλακτική λύση όταν συμβαίνει breakdown. Παραβλέπεται το γεγονός ότι, το εργατικό δυναμικό μειώθηκε πριν από χρόνια λόγω της αυτοματοποίησης των διαδικασιών, με συνέπεια εκείνοι που βρίσκονται τώρα στις αντίστοιχες θέσεις να έχουν χάσει όλη την πρακτική εμπειρία, όσον αφορά τις χειροκίνητες λειτουργίες.

4.2.3. Έλλειψη Ασφάλειας Λόγω Σχεδιασμού

Μια άλλη απειλή ICS είναι ότι τα στοιχεία είναι συσκευασμένα με προεπιλεγμένους εργοστασιακούς κωδικούς πρόσβασης. Οι επιλογές ασφαλείας είναι απενεργοποιημένες από προεπιλογή. Η εγκατάσταση στοιχείων στον τομέα ICS είναι επομένως, εύκολη αλλά εγγενώς ανασφαλής. Ένας βασικός κανόνας είναι ότι, το 30% των βοηθητικών προγραμμάτων δεν καταβάλουν προσπάθειες και είτε τεχνικά δεν μπορούν είτε δεν επιτρέπεται συμβατικά να αλλάξουν τους εργοστασιακούς κωδικούς πρόσβασης.

Οι κατασκευαστές ICS είναι δύσκολο να πειστούν να μετακινηθούν σε εξαρτήματα που είναι ασφαλή έξω από το κουτί. Μόλις πρόσφατα, ορισμένοι κατασκευαστές ICS άρχισαν να αλλάζουν τα προϊόντα τους ώστε να έχουν μια προεπιλεγμένη ασφαλή κατάσταση, η οποία απαιτεί αλλαγές κωδικού πρόσβασης κατά την εγκατάσταση.

Μια σημαντική απειλή είναι ότι, οι πληροφορίες ελέγχου ταυτότητας συμπεριλαμβανομένων των κωδικών πρόσβασης, συχνά δεν είναι κρυπτογραφημένες και μπορούν να βρεθούν από επιτιθέμενους στον κυβερνοχώρο σε καθαρό κείμενο στη μνήμη ή σε υποκλοπή επικοινωνίας.

Ένα παράδειγμα αυτού του συνόλου απειλών είναι ένα PLC ενός γνωστού κατασκευαστή που είναι τυλιγμένο σε ένα φυλλάδιο. Το φυλλάδιο δείχνει ένα πρότυπο τρυπάνι και καθορίζει το πού πρέπει να συνδεθεί το φις τροφοδοσίας και ένα καλώδιο UTP. Το CD και ένας δισέλιδος οδηγός εγκατάστασης δείχνει ότι η εκκίνηση του CD πρέπει να γίνει σε έναν υπολογιστή στο δίκτυο όπου είναι συνδεδεμένο το PLC. Το εκτελέσιμο αρχείο στο δίκτυο προσπαθεί στη συνέχεια να ανακαλύψει το PLC. Μια διαδικτυακή διεπαφή βοηθά στη διαμόρφωση του PLC. Μόνο στη σελίδα 52 του εγχειριδίου, το οποίο είναι ένα pdf (στο CD), μπορεί κανείς να διαβάσει πώς να ρυθμίσει ή να αφαιρέσει (τέσσερα κενά) έναν κωδικό πρόσβασης. Καθώς οι περισσότεροι δεν διαβάζουν εγχειρίδια, αυτός ο τύπος PLC εγκαθίσταται χωρίς προστασία με κωδικό πρόσβασης και συνδέεται απευθείας στο Διαδίκτυο. Χρησιμοποιώντας το εργαλείο Shodan (Shodan 2015), οι

χάκερς βρήκαν τέτοια PLC χωρίς καμία προστασία ελέγχου ταυτότητας ή απλά id = owner, password = owner στο Βέλγιο και τις Κάτω Χώρες. Τα εν λόγω PLC έλεγχαν τις αντλίες ενός τροπικού παραδείσου κολύμβησης, το σύστημα θέρμανσης της έδρας του Salvation Army στο Άμστερνταμ, μια γεννήτρια αιολικής ενέργειας, αντλίες λυμάτων και άλλες λειτουργίες (Luiijf 2013).

4.2.4. Νέα Λειτουργικότητα Παλαιών Συστημάτων

Πολλά ICS αναπτύχθηκαν τη δεκαετία του εξήντα ως ιδιόκτητο υλικό βασισμένο σε τεχνολογία τρανζίστορ (Russel 2015). Τα εξαρτήματα αντικατάστασης για εγκαταστάσεις δέκα ετών και άνω θα βασίζονται εσωτερικά σε πιο σύγχρονη τεχνολογία, αλλά θα εξακολουθούν να διαθέτουν συμβατές διεπαφές πεδίου. Οι κατασκευαστές ενδέχεται να έχουν προσθέσει νέα λειτουργικότητα στο στοιχείο που τεκμηριώνεται μόνο στο εγχειρίδιο. Για παράδειγμα, τα PLC ενδέχεται σήμερα να περιέχουν έναν διακομιστή ιστού «σε ένα τσιπ» που προσφέρει φιλική προς τον χρήστη πρόσβαση στη λειτουργικότητα του PLC, ενός ενσωματωμένου πελάτη email και ενός πράκτορα SNMP. Οι μηχανικοί ενδέχεται να μην αναγνωρίσουν την αλλαγή. Αντικαθιστούν ένα ελαττωματικό εξάρτημα το συντομότερο δυνατό από ένα νέο στα μέσα της νύχτας. Η νέα λειτουργικότητα θα περιμένει σε κατάσταση «μη διαμορφωμένη» εκτός συσκευασίας για το πρώτο μη εξουσιοδοτημένο άτομο που θα συνδεθεί.

4.2.5. Πρωτόκολλα

Πολλά ICS και τα πρωτόκολλά τους σχεδιάστηκαν κατά την περίοδο ιδιοκτησιακών προϊόντων και καλοήθων κλειστών περιβαλλόντων. Όταν συζητάμε για την απειλή των πρωτοκόλλων ICS, πρέπει να κάνουμε διάκριση μεταξύ δυσκολίας για διόρθωση σφαλμάτων στην προδιαγραφή του πρωτοκόλλου ICS και αδυναμίας στην εφαρμογή του πρωτοκόλλου (Igure et al. 2006).

Όσον αφορά την προδιαγραφή του πρωτοκόλλου, οι αρχιτεκτονικές και τα σχέδια του ICS ανέλαβαν μια στάση ασφάλειας από την αφάνεια, την έλλειψη γνώσεων σχετικά με την τεχνολογία ICS και χωρίς να υπάρχουν φορείς που να ενδιαφέρονται και να θέλουν να επιτεθούν και να διαταράξουν τα ICS. Επομένως, η ποικιλία των πρωτοκόλλων ICS δεν προστατεύει το περιεχόμενο των μηνυμάτων πρωτοκόλλου, δεν προστατεύει από επιθέσεις man-in-the-middle και δεν ορίζει τι να κάνει όταν εντοπίζεται ένα παράλογο στοιχείο πρωτοκόλλου. Πρόσφατες μελέτες έχουν αναλύσει την ασφάλεια πρωτοκόλλων όπως Modbus και Modbus over TCP (Fovino 2014; Huitsing et al. 2008), KNX / IP και KNX / EIB (Judmayer et al. 2014) και άλλα πρωτόκολλα ICS. Από αυτές τις μελέτες είναι σαφές ότι τα πρωτόκολλα ICS δεν είναι ασφαλή και ανθεκτικά στις επιθέσεις στον κυβερνοχώρο. Αυτά τα ανασφαλή πρωτόκολλα ICS σχηματίζουν ένα φορέα απειλής ICS που εκμεταλλεύονται οι hackers (SCADAhacker.com 2015) και το λογισμικό Trojan.

Εκτός από τα βασικά σφάλματα και αδυναμίες του πρωτοκόλλου, οι εφαρμογές του πρωτοκόλλου ICS δεν γίνονται ισχυρές. Σύμφωνα με τους κατασκευαστές και τους ολοκληρωτές συστημάτων, οι τελικοί χρήστες ICS ενδιαφέρονται συχνά, μόνο για νέες λειτουργίες ICS και όχι για την ασφάλεια και την ευρωστία των εφαρμογών πρωτοκόλλου. Ο κόσμος του Διαδικτύου έχει μάθει τα μαθήματά του με έναν σκληρό τρόπο με την πάροδο του χρόνου, π.χ. με την επίθεση ping-of-death και τις αδυναμίες DNS BIND. Μαθήματα που δεν έχουν βρει ακόμη το δρόμο τους σε υλοποιήσεις πρωτοκόλλου ICS. Τα sniffers δικτύου χρησιμοποιούνται συχνά από διαχειριστές δικτύου στον κόσμο των ICT για σάρωση ενεργών συστημάτων και θυρών στο δίκτυό τους. Ωστόσο, όταν τα ICS λαμβάνουν ένα απροσδόκητο πακέτο που αποστέλλεται από ένα τέτοιο εργαλείο ή ένα πακέτο που δεν συμμορφώνεται με το πρωτόκολλο ICS, τα ICS είτε μπορεί να αγνοήσουν το πακέτο, είτε να σταματήσουν την επικοινωνία ακόμη και τη λειτουργία τους (crash).

Οι δοκιμές του CERN 2 που πραγματοποιήθηκαν σε 25 συσκευές ICS από επτά διαφορετικούς κατασκευαστές στο περίπτερο δοκιμών TOCSSiC έδειξαν ότι το 32% των συσκευών ICS καταστράφηκαν όταν αντιμετώπισαν μια επίθεση άρνησης υπηρεσίας: «Στο 21% των δοκιμών Nessus, η συσκευή καταστράφηκε κατά τη διάρκεια της σάρωσης. Μετά την ενεργοποίηση της συσκευής, η σάρωση επαναλήφθηκε χωρίς την αντίστοιχη προσθήκη. Στο υπόλοιπο 18%, ο Nessus ανέφερε σημαντικά κενά ασφαλείας {..} "(Lüders 2005). Για παράδειγμα, ένας διακομιστής Modbus καταστράφηκε όταν έγινε σάρωση της θύρας Modbus 502 και η είσοδος σε διάφορα άλλα πρωτόκολλα σε εξοπλισμό ICS για μεγαλύτερο χρονικό διάστημα από το αναμενόμενο, προκάλεσε τη διακοπή λειτουργίας του ICS ως ping-of-death.

Ομοίως, οι δοκιμές διείσδυσης ανάγκασαν ένα βιομηχανικό ρομπότ να κάνει μια απροσδόκητη περιστροφή (Duggan 2005), προκάλεσαν στο σβήσιμο του φωτισμού μιας πόλης και πολλά άλλα.

Παρά τις πτυχές που σχετίζονται με την ασφάλεια των διαδικασιών που ελέγχονται από το ICS, αυτή η απειλή έλλειψης επικύρωσης εισόδου, (Luiijf 2014) και η έλλειψη ευρωστίας των εφαρμογών πρωτοκόλλου ICS εξακολουθεί να υπάρχει στα περισσότερα τρέχοντα στοιχεία και εφαρμογές ICS, όπως αποδεικνύεται από ορισμένες ειδοποιήσεις και συμβουλές (ICS-CERT 2015).

Τα ICS σχεδιάστηκαν παραδοσιακά γύρω από την αξιοπιστία και την ασφάλεια. Η ασφάλεια στον κυβερνοχώρο δεν ήταν σχεδιαστικό και λειτουργικό ζήτημα. Η έλλειψη κατανόησης της απειλής για την ασφάλεια στον κυβερνοχώρο μπορεί να βρεθεί σε όλα τα επίπεδα οργάνωσης. Τα περισσότερα τμήματα ICS μεταφέρουν τις ανάγκες τους σε επίπεδο εκτελεστικού, στο οποίο υπάρχει γενική έλλειψη κατανόησης. Οι «αντιλήψεις» των τμημάτων IT / ICT και ICS συχνά διαφέρουν σε μεγάλο βαθμό. Ο τομέας ICS εστιάζει καταρχάς στη διαθεσιμότητα, την ορατότητα και τη λειτουργικότητα των 24/7 ελεγχόμενων ICS διαδικασιών, την αποτελεσματικότητα της διαδικασίας και την ασφάλεια. Τα τμήματα ICT, από την άλλη πλευρά, επικεντρώνονται κυρίως σε ελέγχους ICT, που σχετίζονται με την εμπιστευτικότητα και την ακεραιότητα. Στη συνέχεια, επιβάλλουν αυστηρή εφαρμογή των στοιχείων ελέγχου ICT στον τομέα ICS όταν αυτά τα

στοιχεία ελέγχου δεν είναι βέλτιστα ή σχετικά. Οι χειριστές και οι μηχανικοί της ICS, οι πωλητές, οι ολοκληρωτές συστημάτων και το προσωπικό συντήρησης δεν είναι γενικά εκπαιδευμένοι στην ασφάλεια των ICS στον κυβερνοχώρο. Ορισμένα παγκόσμια περιστατικά hacks ICS προέρχονται από αυτήν την απειλή ICS.

Η γήρανση της τεχνολογίας του υλισμικού ICS αποτελεί σημαντική απειλή, καθώς η παλιά τεχνολογία με περιορισμένη χωρητικότητα επεξεργασίας και μνήμης δεν είναι σε θέση να εκτελεί ασφαλείς εφαρμογές ICS της τρέχουσας ή της μελλοντικής εποχής. Οι απειλές πηγάζουν από την ανάγκη να καταστούν οι παλαιές τεχνολογίες ICS συμβατές με τη νέα. Τα στοιχεία ICS είναι συσκευασμένα με εργοστασιακούς προεπιλεγμένους κωδικούς πρόσβασης. Τα ICS και τα πρωτόκολλά τους σχεδιάστηκαν κατά την περίοδο ιδιοκτησιακών προϊόντων και καλοήθους κλειστού περιβάλλοντος.

Οι πολιτικές ασφαλείας (π.χ. για USB stick) δεν ακολουθούνται σωστά, αφαιρώντας αποτελεσματικά τη φυσική προστασία ενός κλειστού περιβάλλοντος. Οι τρέχουσες επιθυμίες και απαιτήσεις για απομακρυσμένη πρόσβαση, πρόσβαση από τρίτα μέρη και ελεύθερη πρόσβαση μεταξύ του τομέα ICT και του τομέα ICS δημιουργούν νέες απειλές για τα ICS. Γενικά, τα μέτρα ασφαλείας πρέπει να είναι λογικά και να έχουν όσο το δυνατόν λιγότερες επιπτώσεις στις καθημερινές επιχειρησιακές εργασίες. Διαφορετικά, οι άνθρωποι θα αναζητήσουν μια λύση που σίγουρα θα μειώσει τη συνολική στάση ασφάλειας του οργανισμού.

Η αποφυγή ορισμένων από αυτές τις απειλές μπορεί να επιτευχθεί χρησιμοποιώντας μερικά από τα ακόλουθα μέτρα:

- Χαρτογράφηση του δικτύου ICS και κατανόηση όλων των ζητημάτων συνδεσιμότητας και απόδοσης. Στη συνέχεια, πρέπει να μειωθεί το σύνολο των εξωτερικών συνδέσεων σε μία λογική, καλά προστατευμένη και ελεγμένη σύνδεση, ενώ για μεγαλύτερες εγκαταστάσεις πρέπει να τοποθετηθεί η παλαιά σε ξεχωριστό τείχος προστασίας.
- Πρέπει να οικοδομηθεί σχέση εμπιστοσύνης και αμοιβαίας κατανόησης ανάμεσα σε όλο το προσωπικό στο τμήμα ICS με το προσωπικό του τμήματος ICT.
- Υποστήριξη ηγεσίας από πάνω προς τα κάτω, διαφορετικά οποιαδήποτε προσπάθεια βελτίωσης της ασφάλειας του ICS δεν θα έχει κανένα νόημα. Μπορεί να χρειαστεί οργανωτική αλλαγή.
- Εκτέλεση αξιολόγησης κινδύνου-απειλής και διαχείριση απειλών όπως η ευαισθητοποίηση των χρηστών, η κληρονομιά, η πρόσβαση τρίτων και η προμήθεια με ισορροπημένο τρόπο.

4.3. Παραδείγματα Επιθέσεων

Σε αυτήν την παράγραφο θα δούμε παραδείγματα επιθέσεων, σε ποιο συστατικό της κρίσιμης υποδομής αναφέρεται και συνοπτικά, όλες τις επιθέσεις στην παρακάτω εικόνα. Τέτοια παραδείγματα είναι:

- Saudi Aramco: Ο Shamoon επίσης γνωστός ως W32.DistTrack, είναι ένας modular ιος, που στόχευε τις πρόσφατες εκδόσεις πυρήνα NT των Microsoft Windows των 32 bit . Ο ιός ήταν αξιοσημείωτος λόγω της καταστροφικής φύσης της επίθεσης και του κόστους ανάκαμψης. Το Shamoon μπορεί να εξαπλωθεί από ένα μολυσμένο μηχάνημα σε άλλους υπολογιστές στο δίκτυο . Μόλις μολυνθεί ένα σύστημα, ο ιός συνεχίζει να συγκεντρώνει μια λίστα αρχείων από συγκεκριμένες τοποθεσίες στο σύστημα, να τα ανεβάζει στον εισβολέα και να τα διαγράφει. Τέλος, ο ιός αντικαθιστά την κύρια εγγραφή εκκίνησηςτου μολυσμένου υπολογιστή, καθιστώντας τον άχρηστο. Ο ιός χρησιμοποιήθηκε για τον κυβερνοχώρο εναντίον εθνικών πετρελαϊκών εταιρειών, συμπεριλαμβανομένης της Saudi Aramco της Σαουδικής Αραβίας και του RasGas του Κατάρ (Shamoon 2012). Η συγκεκριμένη επίθεση στόχευε στο IT εταιρικό δίκτυο να προκαλέσει την διαγραφή των δεδομένων.

- Steel Mill Germany: Η επίθεση, η οποία φάνηκε να στοχεύει συγκεκριμένα χειριστές βιομηχανικών εργοστασίων, προκάλεσε την αποτυχία εξαρτημάτων των ελέγχων της μονάδας, με αποτέλεσμα έναν μη ρυθμιζόμενο φούρνο, ο οποίος στη συνέχεια προκάλεσε φυσική ζημιά στο χαλυβουργείο. Το άτομο ή η ομάδα που ήταν υπεύθυνη για την επίθεση ήταν σε θέση να διεισδύσει στο σύστημα χρησιμοποιώντας τεχνικές ψαρέματος, ψαρέματος και κοινωνικής μηχανικής. Αυτές οι δύο μέθοδοι είναι αποδεδειγμένοι τρόποι με τους οποίους οι ηθοποιοί απειλής δελεάζουν τα θύματά τους χρησιμοποιώντας μηνύματα ηλεκτρονικού ταχυδρομείου ή συνδέσμους κοινωνικών μέσων που φαίνεται να προέρχονται από νόμιμη πηγή, αλλά στην πραγματικότητα μπορούν να εισαγάγουν απειλές για εισβολείς να εισέλθουν στο δίκτυο. Ορισμένες ειδήσεις ανέφεραν αυτή τη δεύτερη επίθεση στον κυβερνοχώρο που προκάλεσε ποτέ σωματική ζημιά, καθώς το εξαιρετικά εξελιγμένο κακόβουλο λογισμικό Stuxnet προκάλεσε καταστροφή στο εργοστάσιο εμπλουτισμού ουρανίου Natanz στο Ιράν. Ωστόσο, οι επιθέσεις που επηρεάζουν τις πραγματικές λειτουργίες των εγκαταστάσεων έχουν συνεχιστεί, αλλά ενδέχεται να παραμείνουν αναφερόμενες από τους πληγέντες οργανισμούς. Ως εκ τούτου, η επίθεση των γερμανικών εργοστασίων χάλυβα είναι ακριβέστερα η δεύτερη από τη Stuxnet που είχε φυσική επίπτωση και επιβεβαιώθηκε από μια νόμιμη κυβερνητική πηγή. Μια ανασκόπηση Stuxnet το 2010 περιελάμβανε επίσης σημειώσεις για το σκουλήκι Slammer που έπληξε μια πυρηνική εγκατάσταση στο Οχάιο και το σκουλήκι DOWNAD / Conficker που προκάλεσε δυσλειτουργίες σε ορισμένα ιδρύματα υψηλού προφίλ. Η συγκεκριμένη επίθεση στόχευε στο OT/ICS δίκτυο να προκαλέσει την καταστοφή του συστήματος (Steel Mill Germany 2015).

- Advantech: Το Conti είναι ransomware που έχει παρατηρηθεί από το 2020. Είναι γνωστό ότι επηρεάζονται όλες οι εκδόσεις των Microsoft Windows. Το λογισμικό χρησιμοποιεί τη δική του εφαρμογή του AES-256 που χρησιμοποιεί έως και 32 μεμονωμένα λογικά νήματα, καθιστώντας το πολύ πιο γρήγορο από τα περισσότερα ransomware. Η μέθοδος παράδοσης δεν είναι σαφής. Μόλις βρεθεί σε ένα σύστημα, θα προσπαθήσει να διαγράψει τα Volume Shadow Copies . Θα προσπαθήσει να τερματίσει έναν αριθμό υπηρεσιών, χρησιμοποιώντας το Restart Manager για να διασφαλίσει ότι μπορεί να κρυπτογραφήσει αρχεία που χρησιμοποιούν. Η προεπιλεγμένη συμπεριφορά είναι η κρυπτογράφηση όλων των αρχείων σε τοπικές και δικτυωμένες μονάδες μπλοκ μηνυμάτων διακομιστή , αγνοώντας αρχεία με επεκτάσεις DLL , .exe , .sys και .lnk . Είναι επίσης, σε θέση να στοχεύει συγκεκριμένες μονάδες δίσκου καθώς και μεμονωμένες διευθύνσεις IP (Advantech 2020). Η συγκεκριμένη επίθεση στόχευε στο IT δίκτυο.

- Nork Hydro: LockerGoga, μια μορφή ransomware. Κρυπτογράφησε τα αρχεία σε επιτραπέζιους υπολογιστές, φορητούς υπολογιστές και διακομιστές σε όλη την εταιρεία. Δημοσίευσε επίσης μια σημείωση λύτρων στις οθόνες των κατεστραμμένων υπολογιστών. Όλες αυτές οι ζημιές τέθηκαν σε κίνηση τρεις μήνες νωρίτερα όταν ένας υπάλληλος άνοιξε, κατά λάθος, ένα μολυσμένο email από έναν έμπιστο πελάτη. Αυτό επέτρεψε στους χάκερς να εισβάλουν στην υποδομή πληροφορικής και να φυτέψουν κρυφά τον ιό τους (Nork Hydro 2019). Η συγκεκριμένη επίθεση στόχευε στο IT/OT δίκτυο.

- Stuxnet: Το Stuxnet είναι ένα κακόβουλο worm υπολογιστή που ανακαλύφθηκε για πρώτη φορά το 2010 και πιστεύεται ότι έχει αναπτυχθεί τουλάχιστον από το 2005. Το Stuxnet στοχεύει συστήματα ελέγχου και απόκτησης δεδομένων (SCADA) και πιστεύεται ότι είναι υπεύθυνο για την πρόκληση σημαντικών ζημιών στο πυρηνικό πρόγραμμα του Ιράν . Το Stuxnet στοχεύει συγκεκριμένα προγραμματιζόμενους λογικούς ελεγκτές (PLC), οι οποίοι επιτρέπουν την αυτοματοποίηση ηλεκτρομηχανικών διεργασιών, όπως αυτές που χρησιμοποιούνται για τον έλεγχο μηχανημάτων και βιομηχανικών διεργασιών, συμπεριλαμβανομένων των φυγοκεντρικών αερίων για το διαχωρισμό πυρηνικού υλικού. Αξιοποιώντας τέσσερα zero-day ελαττώματα. Το Stuxnet λειτουργεί στοχεύοντας μηχανές που χρησιμοποιούν το λειτουργικό σύστημα και τα δίκτυα των Microsoft Windows και, στη συνέχεια, αναζητούν το λογισμικό Siemens Step7. Σύμφωνα με πληροφορίες, η Stuxnet έθεσε σε κίνδυνο τα ιρανικά PLC, συλλέγοντας πληροφορίες σχετικά με βιομηχανικά συστήματα και προκαλώντας την ταχεία περιστροφή των φυγοκεντρητών. Ο σχεδιασμός και η αρχιτεκτονική του Stuxnet δεν είναι συγκεκριμένοι για τον

τομέα και θα μπορούσε να προσαρμοστεί ως πλατφόρμα επίθεσης σύγχρονων συστημάτων SCADA και PLC (π.χ. σε εργοστασιακές γραμμές συναρμολόγησης ή σταθμούς παραγωγής ενέργειας), τα περισσότερα από τα οποία βρίσκονται στην Ευρώπη, την Ιαπωνία και τις ΗΠΑ. Σύμφωνα με πληροφορίες, η Stuxnet κατέστρεψε σχεδόν το ένα πέμπτο των πυρηνικών φυγοκεντρητών του Ιράν. Στοχεύοντας στα βιομηχανικά συστήματα ελέγχου, το worm μόλυνε περισσότερους από 200.000 υπολογιστές και προκάλεσε την υποβάθμιση 1.000 μηχανημάτων. Το Stuxnet έχει τρεις ενότητες: ένα worm που εκτελεί όλες τις ρουτίνες που σχετίζονται με το κύριο ωφέλιμο φορτίο της επίθεσης. ένα αρχείο συνδέσμου που εκτελεί αυτόματα τα πολλαπλασιασμένα αντίγραφα του worm · και ένα στοιχείο rootkit που είναι υπεύθυνο για την απόκρυψη όλων των κακόβουλων αρχείων και διαδικασιών, για την αποτροπή της ανίχνευσης του Stuxnet. Εισάγεται, συνήθως, στο περιβάλλον προορισμού μέσω μολυσμένης μονάδας USB. Το worm διαδίδεται στη συνέχεια σε όλο το δίκτυο, σαρώνοντας για λογισμικό Siemens Step7 σε υπολογιστές που ελέγχουν PLC. Ελλείψει οποιουδήποτε κριτηρίου, το Stuxnet αδρανοποιείται μέσα στον υπολογιστή. Εάν πληρούνται και οι δύο προϋποθέσεις, το Stuxnet εισάγει το μολυσμένο rootkit στο λογισμικό PLC και Step7, τροποποιώντας τον κώδικα και δίνοντας απροσδόκητες εντολές στο PLC ενώ επιστρέφει στους χρήστες ένα βρόχο κανονικών λειτουργικών συστημάτων (Stuxnet 2010). Η συγκεκριμένη επίθεση στόχευε στο ICS δίκτυο.

- Triton SIS: Triton είναι malware που ανακαλύφθηκε για πρώτη φορά σε εργοστάσιο πετροχημικών της Σαουδικής Αραβίας το 2017. Μπορεί να απενεργοποιήσετε την ασφάλεια των συστημάτων και στη συνέχεια να συμβάλει στην καταστροφή των φυτών. Ονομάστηκε «το πιο δολοφονικό κακόβουλο λογισμικό στον κόσμο». Τον Δεκέμβριο του 2017, αναφέρθηκε ότι τα συστήματα ασφαλείας ενός μη αναγνωρισμένου σταθμού παραγωγής ενέργειας, που πιστεύεται ότι ήταν στη Σαουδική Αραβία , παραβιάστηκαν όταν η τεχνολογία βιομηχανικής ασφάλειας Triconex που κατασκευάστηκε από την Schneider Electric SE στοχεύτηκε σε μια επίθεση που θεωρείται κρατική. Η εταιρεία ασφάλειας υπολογιστών Symantec ισχυρίστηκε ότι το κακόβουλο λογισμικό , γνωστό ως "Triton", εκμεταλλεύτηκε μια ευπάθεια σε υπολογιστές που εκτελούν το λειτουργικό σύστημα Microsoft Windows (Triton SIS 2017). Η συγκεκριμένη επίθεση στόχευε στο ICS δίκτυο πιο συγκεκριμένα τα PLC .

- Ukraine power grid cyberattack: Στις 23 Δεκεμβρίου 2015, οι χάκερ έθεσαν σε κίνδυνο τα πληροφοριακά συστήματα τριών εταιρειών διανομής ενέργειας στην Ουκρανία και διέκοψαν προσωρινά την παροχή ηλεκτρικής ενέργειας στους καταναλωτές. Είναι η πρώτη γνωστή

επιτυχημένη επίθεση στον κυβερνοχώρο σε ένα ηλεκτρικό δίκτυο. 30 υποσταθμοί (επτά υποσταθμοί 110kv και 23 υποσταθμοί 35kv) απενεργοποιήθηκαν και περίπου 230000 άτομα δεν είχαν ηλεκτρικό ρεύμα για μια περίοδο από 1 έως 6 ώρες . Η επίθεση στον κυβερνοχώρο ήταν περίπλοκη και αποτελείται από τα ακόλουθα βήματα:

- Παραβίαση εταιρικών δικτύων που χρησιμοποιούν ηλεκτρονικά μηνύματα ηλεκτρονικού ψαρέματος (phear -phishing) με κακόβουλο λογισμικό BlackEnergy

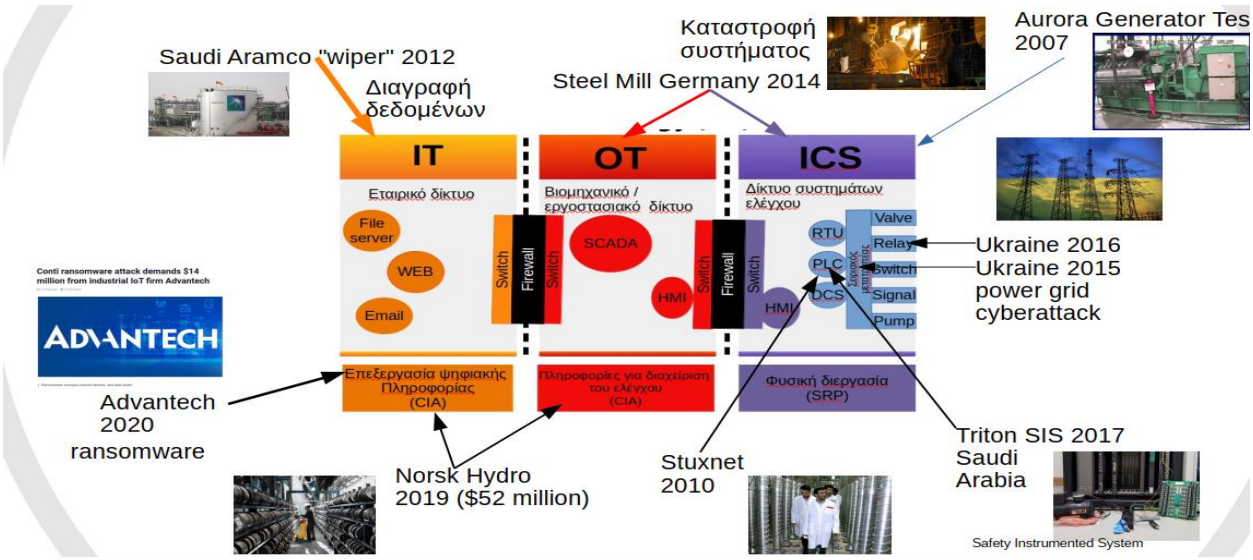
- κατάσχεση του SCADA υπό έλεγχο, απενεργοποίηση των υποσταθμών από απόσταση

- απενεργοποίηση / καταστροφή εξαρτημάτων υποδομής πληροφορικής (αδιάλειπτα τροφοδοτικά , μόντεμ , RTUs , commutators)

- καταστροφή αρχείων που είναι αποθηκευμένα σε διακομιστές και σταθμούς εργασίας με το κακόβουλο λογισμικό KillDisk

- επίθεση άρνησης υπηρεσίας στο τηλεφωνικό κέντρο για την άρνηση ενημέρωσης των καταναλωτών σχετικά με τη διακοπή λειτουργίας

Η συγκεκριμένη επίθεση στόχευε στο ICS δίκτυο (Ukraine power grid cyberattack 2015-2016).



Σχήμα 8. Παραδείγματα Επιθέσεων (Πηγή: IT vs OT)

- Trend Micro: Το 2013 μια εταιρεία ασφαλείας Trend Micro ανέπτυξε ένα δίκτυο Honeypots που μοιάζει με ICS, δηλαδή εικονικά συστήματα που μιμούνται πραγματικά συστήματα ICS, σε οκτώ διαφορετικές χώρες, προκειμένου να συλλέξει δεδομένα πραγματικών επιθέσεων. Από τον Μάρτιο έως τον Ιούνιο του 2013 παρατήρησαν 74 επιθέσεις που προέρχονταν από 16 χώρες (περίπου το 58% από αυτές προέρχονταν από τη Ρωσία) με 11 επιθέσεις να θεωρούνται κρίσιμες. Οι περισσότερες κρίσιμες επιθέσεις εντοπίστηκαν από ειδοποιήσεις που προκλήθηκαν όταν, ένας μη εξουσιοδοτημένος πελάτης Modbus επιχείρησε να διαβάσει ή να γράψει σε συσκευές PLC. Οι περισσότερες από αυτές τις επιθέσεις απέκτησαν πρόσβαση στο Modbus, διακυβεύοντας πρώτα στοιχεία του κέντρου C&C. Οι HMI αποδείχτηκε ότι ήταν η πύλη προς τα συστήματα SCADA σε πολλές περιπτώσεις. Οι επιτιθέμενοι προσπάθησαν να εκμεταλλευτούν HMI μέσω τυπικών επιθέσεων στο Διαδίκτυο όπως SQL injection, CSRF (cross-site request πλαστογράφηση) και λεξικών επιθέσεων. Επειδή το πρωτόκολλο Modbus δεν απαιτεί έλεγχο ταυτότητας, μπορεί να χρησιμοποιηθεί ένα συμβιβασμένο HMI για την αποστολή έγκυρων εντολών στα PLC. Σημειώστε ότι, στις περισσότερες περιπτώσεις η αναγνώριση του honeypot επιτεύχθηκε μέσω μιας διαδικτυακής αναζήτησης μέσω της μηχανής αναζήτησης Shodan IoT.
- LogicLocker: Μια άλλη ερευνητική ομάδα δημιούργησε ένα αυτοαποδομημένο worm ransomware, με το όνομα LogicLocker, το οποίο θα μπορούσε να μολύνει τρία δημοφιλή PLC που συνδέονται στο Διαδίκτυο (Modicon M221, ένα Allen Bradley MicroLogix 1400 και ένα Schneider Modicon) M241). Περισσότερες από 1500 συσκευές των μοντέλων PLC, που αποδείχθηκαν επιρρεπείς σε αυτή τη συγκεκριμένη επίθεση ransomware, ανακαλύφθηκαν μέσω της μηχανής αναζήτησης Shodan. Το μολυσμένο PLC χρησιμοποιήθηκε ως backdoor στο εσωτερικό δίκτυο SCADA και

μπόρεσε να μολύνει με ransomware άλλα PLC του ίδιου προμηθευτή. Εκτός από την αρχική μόλυνση, χρησιμοποιήθηκαν διάφορες τεχνικές για την αποφυγή γρήγορης αποκατάστασης, όπως κλείδωμα πρόσβασης PLC και κρυπτογράφηση προγράμματος PLC. Στη συνέχεια, επιδείχθηκε μια επίθεση ransomware μικρής κλίμακας: Σε ένα προσομοιωμένο περιβάλλον ενός εργοστασίου επεξεργασίας νερού της πόλης ένας κακόβουλος δράστης θέτει σε κίνδυνο τα PLC ελέγχου και απειλεί να απελευθερώσει μεγάλες ποσότητες χλωρίου στο νερό, εκτός εάν πληρώσουν τα λύτρα. (Stellios et al., 2018).

- Rapid7: Οι αυτοματοποιημένοι μετρητές δεξαμενών (ATG) είναι συστήματα SCADA μικρής κλίμακας που χρησιμοποιούνται για την παρακολούθηση των επιπέδων αποθέματος ρεζερβουάρ καυσίμου και την αύξηση συναγερμών (π.χ. διαρροή καυσίμου). Τα περισσότερα ATG μπορούν να ελέγχονται και να παρακολουθούνται μέσω μιας ενσωματωμένης σειριακής διεπαφής. Πολλοί χειριστές επιλέγουν να αντιστοιχίσουν τη σειριακή θύρα σε μια θύρα TCP που είναι προσβάσιμη μέσω του Διαδικτύου, προκειμένου να ενεργοποιηθούν οι υπηρεσίες τηλεχειρισμού. Σύμφωνα με μια τεχνική έκθεση που δημοσίευσε η εταιρεία ασφαλείας Rapid7 περίπου 5800 ATG ανακαλύφθηκαν ότι εκτίθενται στο Διαδίκτυο μέσω της θύρας 10001 / TCP, στην οποία θα μπορούσαν να προσπελαστούν χωρίς καν να απαιτείται κωδικός πρόσβασης ή να χρησιμοποιηθούν άλλοι έλεγχοι ταυτότητας μηχανισμός. Μέσω της θύρας TCP που βλέπει στο Διαδίκτυο, ένας αντίπαλος μπορεί να αποτρέψει από απόσταση τη χρήση του ρεζερβουάρ καυσίμου αλλάζοντας τις ρυθμίσεις πρόσβασης, προσομοιώνοντας ψευδείς συνθήκες ή ενεργοποιώντας χειροκίνητο τερματισμό. Σε ένα παρόμοιο πείραμα μεγάλης κλίμακας, η Trend Micro παρουσίασε το 2015 ένα honeypot: δημιουργήθηκαν πλήρως λειτουργικά εικονικά συστήματα παρακολούθησης δεξαμενών έτσι ώστε να μιμούνται πραγματικά συστήματα. Τα εικονικά ATG διανεμήθηκαν σε οκτώ χώρες και ήταν ορατά από μηχανές αναζήτησης όπως το Shodan. Κατά τη διάρκεια της πειραματικής περιόδου οι περισσότερες από τις επιθέσεις (44%) εμφανίστηκαν στους ATGs, όπου αναπτύχθηκαν στις ΗΠΑ, συμπεριλαμβανομένης μιας επίθεσης DDoS 2 ημερών, 2Gbps, που χρησιμοποίησε το εργαλείο Low-Orbit Ion Cannon (LOIC), κατά εικονικό ATG που βρίσκεται στην Ουάσιγκτον, DC. (Stellios et al., 2018).
- Επιθέσεις σε βιομηχανικά ρομπότ: Τα βιομηχανικά ρομπότ είναι μηχανογραφημένα μηχανικά «όπλα» πολλαπλών αξόνων που χρησιμοποιούνται σε σύγχρονα έξυπνα εργοστάσια για την αυτοματοποίηση διαφόρων λειτουργιών, όπως συγκόλληση, συσκευασία, επεξεργασία τροφίμων κ.λπ. Για παράδειγμα, τα ρομπότ της ABB είναι εξοπλισμένα με τη λεγόμενη Υπηρεσία Ιστού Ρομπότ που δέχεται αιτήματα HTTP ή υποστηρίζουν εύχρηστα APIs που επιτρέπουν το τηλεχειριστήριο μέσω smarthphones. Ωστόσο, η ολοένα αυξανόμενη πολυπλοκότητα και διασύνδεση των βιομηχανικών συστημάτων ελέγχου και της ρομποτικής φέρνουν μια ευρύτερη

επιφάνεια επίθεσης, όπου μπορούν να συνδυαστούν διαφορετικοί τύποι επίθεσης. Πρόσφατες μελέτες έδειξαν σενάρια επίθεσης σε πραγματικά βιομηχανικά ρομπότ IoT-enabled σε ελεγχόμενο περιβάλλον. Χρησιμοποιώντας μηχανές αναζήτησης, όπως οι Shodan, ZoomEye και Censys, οι ερευνητές ασφαλείας κατάφεραν να ανακαλύψουν βιομηχανικά ρομπότ που εκτίθενται απευθείας στο Διαδίκτυο μέσω υπηρεσιών FTP ή μέσω βιομηχανικών δρομολογητών. Από συνολικό αριθμό 83673 ρομπότ που ανακαλύφθηκαν, 5105 δεν απαιτούσαν έλεγχο ταυτότητας, 59 είχαν ενσωματωμένες γνωστές ευπάθειες, ενώ νέες ευπάθειες εντοπίστηκαν σε 6 ρομπότ. Τα ευρήματά τους περιελάμβαναν ξεπερασμένα στοιχεία λογισμικού (π.χ. βιβλιοθήκες επιπέδου εφαρμογής, μεταγλωττιστή, πυρήνα), κακά σχήματα ελέγχου ταυτότητας, ανασφαλείς διασυνδέσεις Ιστού, ξεπερασμένο κώδικα ανοιχτού κώδικα, κακή προστασία λογισμικού (π.χ., μη αποσπασμένα δυαδικά αρχεία), εικόνες υλικολογισμικού προσβάσιμες στο κοινό, τεκμηρίωση και σχετικές λογισμικό, πρόσβαση WAN σε θύρες LAN χωρίς τείχος, ασύρματη πρόσβαση (GSM ή WAN) σε απομακρυσμένες εγκαταστάσεις υπηρεσιών. (Stellios et al., 2018).

Δεδομένου ότι τα έξυπνα ηλεκτρικά δίκτυα ελέγχονται, κυρίως, από συστήματα SCADA, είναι επιρρεπή σε παρόμοια προβλήματα ασφάλειας. Όπως και το SCADA, οι έμμεσες διαδρομές συνδεσιμότητας, που υπάρχουν μεταξύ των έξυπνων δικτύων και των εταιρικών δικτύων IT, όπως οι διαχειριστές δικτύου και οι πάροχοι υπηρεσιών, επεκτείνουν την επιφάνεια επίθεσης των έξυπνων δικτύων SCADA.

- Aurora: Ένα από τα πρώτα πειράματα δοκιμών ασφαλείας σε ηλεκτροπαραγωγούς είναι η επίθεση Aurora, που επιδείχθηκε το 2007 στα Idaho U.S. National Labs. Μια επίθεση Aurora αναγκάζει έναν ή περισσότερους διακόπτες κυκλώματος να ανοίγουν και να κλείνουν με πολύ γρήγορο ρυθμό (π.χ. κάθε 0.25 δευτερόλεπτα), με αποτέλεσμα τον αποσυγχρονισμό της γεννήτριας ισχύος και τελικά τη φυσική της ζημιά. Ο αντίκτυπος μιας τέτοιας επίθεσης μπορεί να κυμαίνεται από βραχυπρόθεσμη διακοπή ρεύματος έως έλλειψη μακροπρόθεσμης παραγωγής. Η επίθεση aurora μπορεί να εκτελεστεί με συμβιβασμό των σχετικών PLC μέσω της ένεσης εντολών. Παρόμοια αναφέρθηκαν αρκετές πραγματικές παραβιάσεις ασφάλειας κατά σταθμών παραγωγής ενέργειας στις Ηνωμένες Πολιτείες, συμπεριλαμβανομένου ενός πυρηνικού σταθμού στο Κάνσας. Παρά τις υποψίες ότι αυτό το περιστατικό συνδέεται με τις επιθέσεις στα ουκρανικά έξυπνα δίκτυα, δεν εντοπίστηκαν ψηφιακά δακτυλικά αποτυπώματα. Παρόλο που οι χάκερ κατάφεραν να διεισδύσουν στα εταιρικά δίκτυα των χειριστών, δεν αναφέρθηκαν λειτουργικές επιπτώσεις στους σταθμούς παραγωγής ενέργειας, λόγω του γεγονότος ότι τα βιομηχανικά συστήματα υπολογιστών ήταν εντελώς ξεχωριστά από το εταιρικό δίκτυο. Οι ειδικοί προειδοποιούν ότι παρά το γεγονός ότι οι επιθέσεις δεν έφτασαν σε κανένα από τα κρίσιμα συστήματα παραγωγής, θα μπορούσαν να χρησιμοποιηθούν ως προκαταρκτικά βήματα αναγνώρισης για τη συλλογή πολύτιμων πληροφοριών. (Stellios et al., 2018).

- CrashOverride: Τον επόμενο χρόνο, μια παρόμοια, αλλά πολύ πιο κρυφή, επίθεση στον κυβερνοχώρο συνέβη με στόχο το σταθμό μετάδοσης του Κιέβου. Αυτή τη φορά, ο κεντρικός σταθμός που δέχτηκε επίθεση ήταν μεγέθους 200 μεγαβάτ, αντικαθιστώντας έτσι τη συνολική ισχύ όλων των σταθμών που χάθηκαν στην επίθεση του προηγούμενου έτους. Οι αντίπαλοι χρησιμοποίησαν την ίδια προσέγγιση και φύτεψαν το κακόβουλο λογισμικό CrashOverride / Win32 / Industroyer μέσω καμπανιών ηλεκτρονικού ψαρέματος. Το κακόβουλο λογισμικό παρέμεινε μυστικό μέχρι να ενεργοποιηθεί από τους αντιπάλους. Περιλάμβανε ένα πλαίσιο που ενσωματώνει λειτουργικές μονάδες για πολλές στοίβες πρωτοκόλλου ICS, όπως IEC 101, IEC 104, IEC 61850 και OPC, έναν εκκαθαριστή για τη διαγραφή αρχείων και διαδικασιών, καθώς και λειτουργικές μονάδες για το άνοιγμα διακοπτών κυκλώματος σε RTUs και να τα αναγκάζει σε ατέρμονα βρόχο. Μια ανάλυση κακόβουλου λογισμικού από την εταιρεία ασφαλείας ESSET αποκάλυψε ότι το σκουλήκι θα μπορούσε να προγραμματιστεί για τη σάρωση του δικτύου του θύματος, την ανακάλυψη πιθανών στόχων και διακοπτών ανοικτού κυκλώματος αυτόνομα, χωρίς παρέμβαση των αντιπάλων. (Stellios et al., 2018).
- Ανανεώσιμες πηγές ενέργειας & συστήματα διανομής: Οι πραγματικές επιθέσεις καθώς και οι επιθέσεις PoC απεικονίζουν το τοπίο απειλών στο Advanced Metering Infrastructure (AMI) (στους έξυπνους μετρητές). Οι ερευνητές ασφαλείας παρουσίασαν πιθανά σενάρια επιπτώσεων που προέρχονται από τη σύνδεση ευάλωτων έξυπνων μετρητών σε οικιακό δίκτυο και ανέλυσαν τα χαρακτηριστικά ανασφάλειας του υλικού, του ενσωματωμένου λογισμικού και των δικτύων του AMI. Το 2010, μια έκθεση του FBI ανέλυσε την υπόθεση του Πουέρτο Ρίκο, όπου αποκαλύφθηκε απάτη εναντίον εταιρείας ηλεκτρικής ενέργειας. Οι αντίπαλοι (πρώην υπάλληλοι της εταιρείας) παραβίασαν έξυπνους μετρητές και τροποποιούσαν δεδομένα μέτρησης και χρέωσης, χρησιμοποιώντας μια θύρα επικοινωνίας υπερύθρων. Όπως αναφέρθηκε, η εκτιμώμενη οικονομική απώλεια θα μπορούσε να φτάσει τα 400 εκατομμύρια δολάρια. Το 2016, ένας ερευνητής ασφαλείας παρουσίασε μια ευπάθεια έγχυσης εντολών (ICSA-16-231-01) που επιτρέπει στους χάκερ να ελέγχουν εξ αποστάσεως ευάλωτους έξυπνους ηλιακούς μετρητές (Locus Energy) και αναφορές επιπέδου ισχύος ή να εκτελούν DDoS. Με σχεδόν 100K συσκευές τριγύρω, η εταιρεία κυκλοφόρησε μια ενημερωμένη έκδοση υλικολογισμικού για την αντιμετώπιση του προβλήματος. (Stellios et al., 2018).

Τα συστήματα ανανεώσιμης ενέργειας, όπως οι ανεμογεννήτριες και οι ηλιακοί συλλέκτες αλληλεπιδρούν άμεσα με το δίκτυο ισχύος διανομής και, στις περισσότερες περιπτώσεις, συνδέονται απευθείας με το Διαδίκτυο. Το 2016, ένας ερευνητής ασφαλείας έσπασε τη δική του μονάδα διαχείρισης ηλιακών συλλεκτών (Tigo Energy MMU) για να ανακαλύψει ένα ανοιχτό σημείο πρόσβασης για τηλεχειριστήριο, καθώς και μια μόνιμη σύνδεση μέσω σήραγγας VPN από τη συσκευή του στις

εγκαταστάσεις του πωλητή. Χρησιμοποιώντας τον κινητήρα Wigle.net, μπόρεσε να εντοπίσει σχεδόν 10.000 παρόμοια συστήματα εκτεθειμένα στο Διαδίκτυο, εκ των οποίων 160 ήταν συνεχώς συνδεδεμένα. Οι διασυνδέσεις Ιστού τους ήταν ευάλωτες σε απομακρυσμένη εκτέλεση κώδικα, χρησιμοποίησαν μη κρυπτογραφημένες διασυνδέσεις HTTP και χρησιμοποίησαν εύκολες εκτιμήσεις / προεπιλεγμένα διαπιστευτήρια (π.χ. διαχειριστής / υποστήριξη). Το 2015, ένας άλλος ερευνητής ασφαλείας εντόπισε πολλά ελαττώματα στα συστήματα καθαρής ενέργειας, όπως το XZERES 442SR Wind Turbine, το Sinapsi eSolar Light και το RLE Nova-Wind Turbine. Αυτές οι ευπάθειες έχουν αναφερθεί στο ICS-CERT και περιλαμβάνουν, μεταξύ άλλων, κωδικούς πρόσβασης που είναι αποθηκευμένοι σε αρχεία απλού κειμένου και / ή τη χρήση της ευπάθειας CrossSite Request Forgery (CSRF) για αλλαγή του κωδικού πρόσβασης διαχειριστή διεπαφής Web. Και για τις τρεις συσκευές που εξετάστηκαν, οι ερευνητές θα μπορούσαν να χρησιμοποιήσουν κάποιο μηχανισμό ασφαλείας και να εκτελέσουν διάφορες ενέργειες ελέγχου, όπως αλλαγή διόρθωσης ανεμοδείκτη ή αλλαγή των ρυθμίσεων δικτύου για να κάνουν μια διεπαφή Ιστού απρόσιτη. (Stellios et al., 2018).

Κεφάλαιο 5ο : Μηχανισμοί Προστασίας ΒΣΕ από Κυβερνοεπιθέσεις

5.1. Ανάγκη για Προστασία ΒΣΕ από Κυβερνοεπιθέσεις

Λόγω της αυξημένης διασύνδεσης των δικτύων "Επιχειρησιακής Τεχνολογίας (Operational Technology – OT)" με δίκτυα "Τεχνολογία Πληροφοριών (Information Technology – IT)", τα βιομηχανικά συστήματα ελέγχου εκτίθενται όλο και περισσότερο σε κυβερνο-απειλές. Αυτές οι απειλές επηρεάζουν επίσης, τα συστήματα καθώς αυξάνουν τις συνδέσεις με την ικανότητα υπολογιστικού νέφους και αποτελούν πρόκληση για εξειδικευμένους χάκερς (Asghar et al., 2019). Η κοινότητα των χάκερς γίνεται όλο και πιο ικανή και δημιουργική όσον αφορά τις δεξιότητες και τις ικανότητές τους. Αυτές οι κοινότητες είναι καλά οργανωμένες και δομημένες, ώστε να προκαλούν ζημιές στο βιομηχανικό σύστημα ελέγχου και στις εγκαταστάσεις υποδομής με κόστος εκατομμυρίων και δισεκατομμυρίων δολαρίων. Μπορεί κανείς να θυμηθεί το περιστατικό που συνέβη κατά τη διάρκεια του 2010 στη μονάδα επεξεργασίας πυρηνικών καυσίμων της Natanz στο Ιράν, όπου το κακόβουλο λογισμικό που εισήγαγε ο χάκερ «μόλυνε» και κατέστρεψε ολόκληρο το εργοστάσιο. Παρομοίως, μπορεί κανείς να δει και τις ανησυχίες που εγείρονται από τον ιό Flame, τον εξαιρετικά εξελιγμένο κακόβουλο κώδικα που έχει υπάρξει ποτέ (Marali et al., 2019).

Οι επικίνδυνες κυβερνο-επιθέσεις στο βιομηχανικό σύστημα ελέγχου έχουν τεθεί υπό το βλέμμα των κυβερνητικών φορέων που εμπλέκονται στη ρύθμιση της κυβερνο-ασφάλειας είτε σε περίπτωση που οι επιχειρήσεις το κάνουν είτε όχι. Το Κογκρέσο των Ηνωμένων Πολιτειών και άλλες κυβερνήσεις σχεδιάζουν να ρυθμίσουν την ασφάλεια στον κυβερνοχώρο. Εάν επιχειρήσεις, όπως τα εργοστάσια, δεν αντιμετωπίζουν το ζήτημα, οι κυβερνήσεις θα θεσπίσουν κανόνες και κανονισμούς που όλοι πρέπει να ακολουθούν. Αν και αυτό δεν είναι κακή ιδέα, τι γίνεται αν οι κανονισμοί που επιβάλλονται από την κυβέρνηση χάσουν το στόχο, ή είναι επαχθείς ή προσθέτουν περιττό κόστος; Ο τρόπος για να αποφευχθεί το λάθος φάρμακο που συνταγογραφείται από κυβερνήσεις με καλές προθέσεις είναι να δείξει η βιομηχανία ότι αντιμετωπίζει η ίδια σωστά και προληπτικά την κυβερνο-ασφάλεια. Από την άλλη πλευρά, ο κυβερνητικός κανονισμός για την ασφάλεια στον κυβερνοχώρο ενδέχεται να προσθέσει περιττό επιπλέον κόστος, ενώ επίσης ενδέχεται να μην αντιμετωπίσει κινδύνους ασφαλείας (Drias et al., 2015). Ως εκ τούτου, οι ιδιοκτήτες εργοστασίων πρέπει να εφαρμόσουν προληπτικές στρατηγικές για την αντιμετώπιση των κυβερνο-απειλών, ειδικά όσον αφορά τα δίκτυα OT που εκτίθενται εκτός ασφαλείας. Το κόστος των μέτρων ασφαλείας πρέπει να είναι ισορροπημένο έναντι της επιτευχθείσας μείωσης του κινδύνου. Ο κίνδυνος πρέπει να μετρηθεί με πιθανότητα επιτυχούς επίθεσης και πιθανές συνέπειες σε συστήματα IT και OT (Knowles et al., 2015).

Οι απαντήσεις των επιχειρήσεων σε επιθέσεις στον κυβερνοχώρο εξαρτώνται εξ ολοκλήρου από τις ανατεθείσες ευθύνες τους για την παραγωγή OT και εταιρικών IT δικτύων. Το εταιρικό υπεύθυνο IT τμήμα παρέχει μεγάλη προσοχή στην προστασία των συστημάτων τεχνολογίας πληροφοριών, όπως ο

Επιχειρησιακός Προγραμματισμός Πόρων (Enterprise Resource Planning), διατηρεί την εμπιστευτικότητα (Confidentiality), την ακεραιότητα (Integrity) και τη διαθεσιμότητα (Availability), γνωστή ως «CIA Τριάδα» ως βασικές αρχές της ασφάλειας των πληροφοριών. Αν και οι τρείς παραπάνω ιδιότητες είναι σημαντικές, η εμπιστευτικότητα υπερτερεί των άλλων δύο ως προς τη σημασία της (Asghar et al., 2019).

Το τμήμα OT για συστήματα βιομηχανικού ελέγχου τονίζει ότι η διαθεσιμότητα είναι πιο σημαντική από την εμπιστευτικότητα. Αυτό οφείλεται στο γεγονός ότι, ο κύριος σκοπός των συστημάτων ελέγχου είναι η ασφαλής και αδιάκοπη εκτέλεση της διαδικασίας παραγωγής και όχι η αποθήκευση ευαίσθητων εγγράφων, αλλά η ενεργοποίηση του χρόνου λειτουργίας της παραγωγής. Ωστόσο, λόγω του απομονωμένου χαρακτήρα τους, παρουσιάζουν έλλειψη στην έκθεση και την εξειδίκευση όσον αφορά την κυβερνο-ασφάλεια. Εξαιτίας αυτού, τα δίκτυα παραγωγής OT είναι επιρρεπή σε κυβερνοεπιθέσεις εναντίων της ασφάλειας ενώ το εταιρικό IT τμήμα γενικά δεν κατανοεί τις απαιτήσεις και τις πολυπλοκότητές τους (Drias et al., 2015).

Επομένως, απαιτείται κοινό τμήμα, το οποίο παραβλέπει τις προκλήσεις, τις προσεγγίσεις λύσεων, συμπεριλαμβανομένων ειδικών δικτύων IT που μιλούν την ίδια γλώσσα με το δίκτυο OT. Η βιομηχανία σημείωσε σημαντική αύξηση στο μέγεθος της αποκάλυψης τρωτών σημείων από έτος από το 1996, ενώ φαίνεται επίσης ότι νέα τρωτά σημεία αναφέρονται κάθε ώρα κάθε μέρα (Marali et al., 2019).

Κατά τη δημιουργία και την εφαρμογή της στρατηγικής προστασίας της ασφάλειας, πρέπει να παρέχεται αρκετή προσοχή στον εντοπισμό των κινδύνων και των σχεδίων μετριασμού σε περίπτωση κυβερνοεπιθέσεων σε ολόκληρη την εταιρεία. Επιπλέον πρέπει να γίνει περαιτέρω ισότιμη κατάταξη κινδύνων δίνοντας έμφαση στην εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα συστημάτων βιομηχανικού ελέγχου (Kriaa et al., 2015).

Τα βιομηχανικά συστήματα ελέγχου πρέπει να προστατεύονται με τις πιο πρόσφατες ενημερώσεις, συμπεριλαμβανομένων στοιχεία τρίτων, χρησιμοποιώντας βέλτιστες πρακτικές και τεχνογνωσία στον κυβερνοχώρο. Το περαιτέρω σχέδιο συμμόρφωσης του βιομηχανικού συστήματος ελέγχου πρέπει να περιλαμβάνει μέτρα για την αύξηση της προστασίας των δικτύων OT & IT, τη μείωση του κινδύνου διαδικτυακών επιθέσεων, τη μείωση των βλαβών του συστήματος, τη μείωση του κόστους της αναγνώρισης και της προστασίας της ασφάλειας στον κυβερνοχώρο, εισαγωγή αξιόπιστης στρατηγικής κυβερνο-ασφάλειας για χρήστες και διαχειριστές εργοστασίων προς τη διαθεσιμότητα, την ακεραιότητα και την εμπιστευτικότητα των συστημάτων τους (Asghar et al., 2019).

Μέχρι στιγμής, οι δαπάνες που προκαλούνται από επιθέσεις στον κυβερνοχώρο και οι επιπτώσεις τους είναι τουλάχιστον τρεις φορές υψηλότερες από το κόστος που επιφέρουν μέτρα προστασίας από κυβερνοεπιθέσεις. Καθώς η διαδικασία παραγωγής και τα μέτρα ασφάλειας των εγκαταστάσεων προχωρούν, η ασφάλεια στον κυβερνοχώρο για τη βελτίωση δικτύων OT και IT πρέπει να εφαρμόζεται συνεχώς για καλύτερη προστασία (Marali et al., 2019).

5.2. Βιομηχανικά Standards και Βέλτιστες Πρακτικές

Σε αντίθεση με παλαιότερες εποχές, τα βιομηχανικά συστήματα ελέγχου δεν είναι πλέον απομονωμένα από τα συστήματα πληροφοριών των εγκαταστάσεων. Λαμβάνοντας υπόψη τις οικονομικές καταστάσεις και την αυξανόμενη ζήτηση των επιχειρήσεων, τα βιομηχανικά συστήματα ελέγχου επιβάλλεται να είναι πολύ πιο αλληλένδετα με τα εταιρικά δίκτυα. Οι βιομηχανίες διεργασιών, συμπεριλαμβανομένης της ενέργειας και των επιχειρήσεων κοινής ωφέλειας, απαιτούν άνευ προηγουμένου ανταλλαγή πληροφοριών για να αποκτήσουν επιχειρηματική σαφήνεια και καλύτερη λήψη αποφάσεων κατά τη διαδικασία εκτέλεσης κατασκευής τους (Drias et al., 2015). Αυτό το ζητούμενο, επιβάλλει στα βιομηχανικά συστήματα ελέγχου να δικτυωθούν με συστήματα πληροφοριών εγκαταστάσεων και έτσι με την τυποποίηση πρωτοκόλλων επικοινωνίας, οι συνιστώσες υλικού και λογισμικού να διασφαλίσουν την αποδοτικότητα και την παραγωγικότητα της λειτουργίας των εγκαταστάσεων. Ωστόσο, εκθέτει τα βιομηχανικά συστήματα ελέγχου στο έλεος του εισβολέα. Δεδομένου ότι, οι συνέπειες τέτοιων κυβερνο-επιθέσεων συνεπάγονται τεράστιες επιπτώσεις, οι κυβερνητικοί φορείς αντιδρούν συνεχώς εισάγοντας κανονιστικές συμμορφώσεις για την υποδομή συστημάτων βιομηχανικών εγκαταστάσεων (Kriaa et al., 2015).

Μερικές από τις κανονιστικές συμμορφώσεις είναι οι απαιτήσεις NERC CIP (North American Electric Reliability Corporation, Critical Infrastructure Protection), η νομοθεσία περί ασφάλειας IT της Γερμανίας, η ANSSI (Agence nationale de la sécurité des Systems d'information) ένας νέος κανονισμός στη Γαλλία κ.λπ. Επιπλέον, υπάρχουν άλλα διεθνή πρότυπα που καλύπτουν τεχνικές πτυχές της ασφάλειας στον κυβερνοχώρο, για παράδειγμα, οι σειρές NIST 800 - 53, CPNI, ISA99, ISO 27K, IEC 623513, IEC 62351, IEEE P1686 και ISO / IEC 27000 είτε καλύπτουν άμεσα τομείς OT και IT που εστιάζουν γενικά σε μηχανισμούς ασφάλειας στον κυβερνοχώρο. Η ISA αποφάσισε να μετονομάσει το πρότυπο ISA99 σε ISA 62443 για να τονίσει την ευθυγράμμιση με τη σειρά IEC 62443 (Marali et al., 2019).

Είναι σημαντικό να γίνει κατανοητό το εύρος των απαιτήσεων σχεδιασμού και η πληρότητα των προτύπων με βάση ευρέως χρησιμοποιούμενα βιομηχανικά πρότυπα και βέλτιστες πρακτικές.

Στο πρόσφατο παρελθόν έχουν σημειωθεί σημαντικές αλλαγές στον αυτοματισμό βιομηχανικών διεργασιών που αφορούν τόσο την παραγωγή όσο και την υποδομή του δικτύου πληροφοριών της εγκατάστασης με τη συμμετοχή πολλών διακριτών παραγόντων στη διαθεσιμότητα αποτελεσματικής λειτουργίας μονάδας ολοκληρωμένης διεργασίας τόσο στην επιχειρησιακή τεχνολογία (operational technology-OT) όσο και στην τεχνολογία πληροφοριών (Information technology-IT). Η εταιρική επιχείρηση και η λειτουργία της μονάδας διεργασιών αλληλεπιδρούν μεταξύ των παραγόντων του ενεργητικού των OT και IT (Knowles et al., 2015). Η αυξανόμενη κοινωνικοοικονομική πίεση, οδηγεί στη χρήση τυπικών τμημάτων πληροφορικής, τυποποιημένων πρωτοκόλλων βασισμένων σε IP και υποδομών δημόσιας επικοινωνίας. Επομένως, η βιομηχανική υποδομή συστήματος ελέγχου είναι αξιοσημείωτα πιο ευάλωτη σε

κυβερνοαπειλές, από ότι τα απομονωμένα συστήματα που συνδέονται μέσω μιας ειδικής υποδομής. Παραδείγματα τέτοιων απειλών που προκαλούνται από τη δυνατότητα σύνδεσης απομακρυσμένης πρόσβασης για δραστηριότητες συντήρησης και ενημέρωσης εγκαταστάσεων που είναι ενεργοποιημένες μέσω του Διαδικτύου είναι η απομακρυσμένη πρόσβαση για τη συντήρηση που διοχετεύεται μέσω του Διαδικτύου ή οι ευπάθειες που προκαλούνται από στοιχεία λογισμικού που οδηγούν σε πλαστοπροσωπία του συστήματος παραγωγής ή των στοιχείων του υποσυστήματος των διαδικασιών του εργοστασίου (Asghar et al., 2019).

Επιπλέον, μια επίθεση σε ένα σύστημα ελέγχου μπορεί να έχει πολύ διαφορετικές συνέπειες από μια επίθεση σε ένα επιχειρηματικό σύστημα. Αντί για πληροφοριακές και οικονομικές απώλειες, ο αντίκτυπος θα μπορούσε να παραβιάζει τις κανονιστικές απαιτήσεις, να καταστρέψει τον εξοπλισμό, να οδηγήσει σε απώλεια παραγωγής, να βλάψει το περιβάλλον ή να απειλήσει την ασφάλεια του κοινού και των εργαζομένων. Ωστόσο τα βασικά μέτρα ασφαλείας θα μπορούσαν εύκολα να αποτρέψουν ή να μειώσουν τις επιπτώσεις των περισσότερων εισβολών. Επομένως, με τη χρήση βιομηχανικών πρακτικών, πρότυπα όπως οι σειρές ISO / IEC 270001, NERC-CIP2 και ISA-62443 (ISA-99), πρέπει να ληφθούν μέτρα πολιτικής και διαδικασιών για την προστασία της υποδομής, χρησιμοποιώντας προσεγγίσεις τριών βημάτων, προσδιορίζοντας πρώτα τις ευπάθειες, δεύτερον, μετριάζοντας τους πιθανούς κινδύνους με την εφαρμογή διορθωτικών μέτρων για τα κενά που εντοπίστηκαν και τρίτον, με την παρακολούθηση του συστήματος σε ταχέως εξελισσόμενο περιβάλλον (Marali et al., 2019).

Ανεξάρτητα από τις προσεγγίσεις τριών βημάτων που παρουσιάστηκαν παραπάνω αναμένεται ότι, ο χειρισμός όλων των τρωτών σημείων και της ενημέρωσης συστήματος που περιλαμβάνει στοιχεία λογισμικού και λειτουργικών συστημάτων τρίτων πρέπει να γίνεται σε συνεργασία με τη λειτουργία εγκατάστασης, τη συντήρηση (συμπεριλαμβανομένων των OT & IT) τρίτων προμηθευτών κατά τη διάρκεια ζωής του κύκλου συστήματος για την αντιμετώπιση των απειλών για την ασφάλεια στον κυβερνοχώρο (Kriaa et al., 2015).

5.3. Ασφάλεια Πρωτοκόλλων ΒΣΕ

Οι λύσεις ασφάλειας στον κυβερνοχώρο δεν είναι μοναδικές που ταιριάζουν συνήθως σε όλες τις εφαρμογές του οργανισμού. Όπως οι βελτιώσεις στη διαδικασία και την ασφάλεια, η ασφάλεια στον κυβερνοχώρο απαιτεί συνεχή παρακολούθηση και προσδιορισμό των ευκαιριών βελτίωσης που αφορούν την τεχνολογία, τους οργανισμούς και τους ανθρώπους (Knowles et al., 2015).

Ενώ γίνεται κατανοητό ότι, στην πραγματικότητα καμία λύση ασφάλειας στον κυβερνοχώρο δεν μπορεί να είναι 100% αποτελεσματική, ο προσεκτικός σχεδιασμός και η εφαρμογή μέτρων ασφάλειας στον κυβερνοχώρο, βάσει μιας συστηματικής αξιολόγησης κυβερνο-κινδύνων, μπορεί να φέρει την ασφάλεια σε επίπεδο κατάλληλο για οποιαδήποτε εφαρμογή και εγκατάσταση. Προστατεύοντας το σύστημα από παραβίαση από σκόπιμες ή τυχαίες επιθέσεις, οι διαδικασίες πρέπει να αναπτύσσονται και να ακολουθούνται χωρίς διαταραχές και με τρόπο που δεν θέτει σε κίνδυνο ανθρώπους ή εξοπλισμό (Marali et al., 2019).

Για την προστασία των δικτύων συστήματος OT & IT, πρέπει να διασφαλιστεί η τήρηση τριών βημάτων προκειμένου να επιτευχθεί η κυβερνο-ασφάλεια (Asghar et al., 2019).

- **Ακεραιότητα:** Οι λειτουργίες και τα δεδομένα του συστήματος πρέπει να προστατεύονται από την τροποποίηση από μη εξουσιοδοτημένα άτομα ή συστήματα.
- **Διαθεσιμότητα:** Οι μη εξουσιοδοτημένοι χρήστες πρέπει να εμποδίζονται από την άρνηση νόμιμης πρόσβασης ή χρήσης των λειτουργιών του συστήματος
- **Εμπιστευτικότητα:** Ορισμένες πληροφορίες πρέπει να προστατεύονται από την αποκάλυψη σε μη εξουσιοδοτημένα άτομα ή συστήματα.

Βέλτιστη συμμόρφωση για να αναγνωριστεί η σημασία των προτύπων ασφάλειας στον κυβερνοχώρο και να συμπεριληφθούν διάφορες πρωτοβουλίες του κλάδου, συμπεριλαμβανομένης της ενεργού συμμετοχής στα ISA και IEC.

Η ασφάλεια στον κυβερνοχώρο πρέπει να ενσωματωθεί στον κύκλο ζωής προϊόντων των συστημάτων ελέγχου. Η αρχιτεκτονική του συστήματος πρέπει να βασίζεται σε καθιερωμένες αρχές ασφαλείας, όπως η άμυνα σε βάθος και οι ζώνες ασφαλείας.

Το σύστημα OT πρέπει να προστατεύεται με τακτική αξιολόγηση κινδύνου συμμόρφωσης στον κυβερνοχώρο και δημιουργίας έκθεσης συμμόρφωσης σύμφωνα με τα πρότυπα ασφαλείας όπως η εφαρμογή εταιρικού προτύπου ασφάλειας OT ή εθνικού κανονισμού από στενά λειτουργικές μονάδες και προμηθευτές. Περαιτέρω διαχείριση ευπάθειας απόκρισης σε περιστατικά πρέπει να εφαρμοστεί σε δίκτυα OT & IT, συμπεριλαμβανομένου του στόλου του συστήματος, για να εκτιμηθούν προβλέψεις (Drias et al., 2015).

Ανασκόπηση Προτεινόμενων Λύσεων Ασφάλειας ICS (Asghar et al., 2019).

Κατηγορία	Μέτρα Κυβερνοασφάλειας	Περιγραφή
Ανίχνευση εισβολής και πρόληψη	Παρακολούθηση Ασφάλειας	Καλύπτουν το τεχνικό κενό στην ασφάλεια τόσο από φυσικές όσο και από κυβερνοεπιθέσεις. Οι λύσεις προσομοιώνουν τη συμπεριφορά του συστήματος σε ένα περιβάλλον δοκιμών, καθώς και τις ευπάθειες ασφάλειας των ICS. Επιτρέπουν την παρακολούθηση του συστήματος, την ταξινόμηση οποιαδήποτε μη φυσιολογικής και κακόβουλης δραστηριότητας και την ενημέρωση του υπεύθυνου ατόμου όταν εντοπίζεται οποιαδήποτε κακόβουλη συμπεριφορά.
	Ανίχνευση Εισβολής	
	Ανίχνευση Ευπάθειας	
	Αυθεντικοποίηση	
	Λύσεις Επιπέδου Δικτύου	
	Αρχιτεκτονική Ασφάλειας	
	Πολιτικές Ασφαλείας	
Διαδικασία ασφαλείας	Εκτίμηση Κινδύνου	Υψηλό υπολογιστικό κόστος καθώς και υψηλό κόστος για λύσεις κρυπτογράφησης. Δεν υπάρχουν ομοιόμορφα πρότυπα και ορισμένες οδηγίες δεν είναι εύκολο να κατανοηθούν από όλους.
	Μετρικές Ασφαλείας	
	Συμβάντα και μηχανική μάθηση	
Προσομοιωτές ICS	Εξοπλισμός ICS	Χαμηλό κόστος ανάπτυξης αλλά χαμηλή απόδοση ανίχνευσης σε καινούρια είδη επιθέσεων.
	Συσκευές δικτύου ICS	
	Επιθέσεις ICS	
Ολιστικές	Άμυνα-εις-βάθος	Υψηλό κόστος ανάπτυξης και πολυπλοκότητα.

Τα συστήματα πληροφορικής (IT) σε επίπεδο εγκατάστασης πρέπει να τονίζονται με αποκλειστικό υπεύθυνο ασφαλείας που έχει την ευθύνη εφαρμογής ασφάλειας για ολόκληρο τον ιστότοπο, ο οποίος είναι συνδεδεμένος με τα συστήματα OT. Πρέπει να διασφαλιστεί η επιδιόρθωση ασφαλείας, η δημιουργία αντιγράφων ασφαλείας συστήματος, η απαραίτητη ρύθμιση παραμέτρων τείχους προστασίας και η επιτρεπόμενη λίστα και η ανάπτυξη SIEM για αποτελεσματική προστασία (Marali et al., 2019).

Τα σημερινά βιομηχανικά συστήματα ελέγχου είναι πιο ευάλωτα σε απειλές στον κυβερνοχώρο από ποτέ, λόγω της αυξημένης διασυνδεσιμότητας, του υπολογιστικού νέφους και των όλο και πιο επιδέξιων χάκερς. Τα βιομηχανικά συστήματα ελέγχου πρέπει να αναπτύξουν προληπτικά την ευαισθητοποίηση για την ασφάλεια στον κυβερνοχώρο για συστήματα OT & IT και να απαιτούν λύσεις ασφαλείας. Οι λειτουργίες των βιομηχανικών διεργασιών πρέπει να μάθουν συνεχώς διαφορετικές προσεγγίσεις για την ασφάλεια στον κυβερνοχώρο για έναν προσεκτικό σχεδιασμό και εφαρμογή μέτρων ασφαλείας σύμφωνα με τα πρότυπα ασφαλείας και οι περαιτέρω εφαρμοζόμενες λύσεις πρέπει να αξιολογούνται περιοδικά για νέους κινδύνους και να ενημερώνονται αναλόγως. Η εργασία του προσωπικού σε συστήματα OT & IT πρέπει να κατανοήσει σε βάθος τους μηχανισμούς ασφάλειας στον κυβερνοχώρο και τις λύσεις για βιομηχανικά συστήματα ελέγχου και να διερευνήσει πιθανούς κινδύνους, συμπεριλαμβανομένων των σωστών στρατηγικών μετριασμού (Asghar et al., 2019).

Η διαρκής εξερεύνηση, η επανεξέταση νέων πρότυπων ασφαλείας όπως το IEC / ISO 27000 και το ISA 99, η δημιουργία ευαισθητοποίησης και η εφαρμογή διαχείρισης αλλαγών που καλύπτει ολόκληρο τον κύκλο ζωής των βιομηχανικών συστημάτων ελέγχου, η περιγραφή των μηχανισμών επίθεσης στον κυβερνοχώρο, των επιπτώσεως κινδύνου, του κύκλου εκμετάλλευσης της ευπάθειας, συμπεριλαμβανομένης της διαχείρισης του εντοπισμού εισβολής, η δημιουργία και εκτέλεση κριτικών συμμόρφωσης ασφαλείας, συμπεριλαμβανομένης της ευρωστίας του συστήματος δοκιμών, με τη χρήση ενημερωμένων εργαλείων, τεχνικών για τον εντοπισμό πιθανών τρωτών σημείων και επανεξέταση των σχεδίων μετριασμού είναι βήματα που πρέπει να γίνουν προκειμένου να επιτευχθούν τα αναμενόμενα αποτελέσματα. Επιπλέον, απαιτούνται η δημιουργία διαδικασίας δημιουργίας αντιγράφων, η εφαρμογή προηγμένων αρχιτεκτονικών δικτύου (όπως π.χ. ζωνών ασφαλείας, τεχνικών VLAN και ασφαλούς επικοινωνίας), η δημιουργία ασφαλούς διασύνδεσης μεταξύ δικτύων με τη χρήση τειχών προστασίας (είτε μέσω γραμμής εντολών είτε μέσω του γραφικού περιβάλλοντος χρήστη), η εφαρμογή των ενημερώσεων ασφαλείας σε βιομηχανικά συστήματα ελέγχου, η εφαρμογή μοντέλου ασφαλείας συστήματος και η εφαρμογή των μηχανισμών ασφαλείας του (ρόλοι χρήστη, δικαιώματα, κωδικούς πρόσβασης, έλεγχος ταυτότητας) (Marali et al., 2019).

Βέλτιστες πρακτικές σχετικά με το είδος των επιθέσεων (CISA, Recommended Cybersecurity Practices for Industrial Control Systems). https://us-cert.cisa.gov/ics/Recommended-Practices.

Διαχείριση Κινδύνου και Διακυβέρνηση Ασφάλειας	**Φυσική Ασφάλεια**	**Αρχιτεκτονική Δικτύου ICS**	**Ασφάλεια Περιμέτρου Δικτύου ICS**	**Ασφάλεια Ξενιστή**	**Άνθρωπος**
• Προσδιορίστε απειλές για τον οργανισμό. • Διατηρήστε το απόθεμα περιουσιακών στοιχείων ICS όλων των υλικών, λογισμικού και υποστηρικτικών τεχνολογιών υποδομής. • Ανάπτυξη πολιτικών, διαδικασιών, εκπαίδευσης και εκπαιδευτικού υλικού ασφάλειας στον κυβερνοχώρο που ισχύουν για το ICS του οργανισμού. • Ανάπτυξη και εξάσκηση διαδικασιών απόκρισης συμβάντων που ενώνουν τις διαδικασίες απόκρισης πληροφορικής και OT	• Κλείδωμα ηλεκτρονικών πεδίου και ρύθμιση μηχανισμών ειδοποίησης για χειρισμό συσκευών, όπως διακοπή παροχής, επαναφορά συσκευών και αλλαγές καλωδίωσης. • Βεβαιωθείτε ότι μόνο εξουσιοδοτημένο προσωπικό έχει πρόσβαση σε ελεγχόμενους χώρους που στεγάζουν εξοπλισμό ICS. • Κάντε χρήση ελέγχου ταυτότητας πολλαπλών παραγόντων, φύλακες και εμπόδια για τον έλεγχο της λογικής και φυσικής πρόσβασης σε εξοπλισμό και εγκαταστάσεις ICS.	• Χρήση της κατάτμησης των δικτύων όπου είναι δυνατόν. • Εφαρμογή τοπολογίας δικτύου για ICS που έχει πολλαπλά επίπεδα, με τις πιο κρίσιμες επικοινωνίες να συμβαίνουν στο πιο ασφαλές και αξιόπιστο επίπεδο. • Κάντε χρήση των μονόδρομων διόδων επικοινωνίας για να αποτρέψετε την εξωτερική πρόσβαση, όποτε είναι δυνατόν. • Ρυθμίστε αποστρατικο-ποιημένες ζώνες (DMZ) για να δημιουργήσετε ένα φυσικό και λογικό υποδίκτυο.	• Διαμορφώστε τείχη προστασίας για τον έλεγχο της κίνησης μεταξύ του δικτύου ICS και του εταιρικού δικτύου πληροφορικής. • Χρήση γεωγραφικού αποκλεισμού IP ανάλογα με την περίπτωση. • Προστατέψτε τη διαδικασία απομακρυσμένης πρόσβασης • Χρήση διακομιστών ως κεντρική τοποθεσία εξουσιοδότησης μεταξύ των ζωνών ασφαλείας δικτύου ICS • Μην επιτρέπετε απομακρυσμένη μόνιμη σύνδεση προμηθευτή ή υπαλλήλου στο δίκτυο ελέγχου.	• Προώθηση μιας κουλτούρας επιδιόρθωσης και διαχείρισης ευπάθειας. • Δοκιμάστε όλες τις ενημερώσεις κώδικα σε περιβάλλον δοκιμών • Εφαρμόστε τη λίστα επιτρεπόμενων εφαρμογών σε διεπαφές ανθρώπινου μηχανήματος • Θωρακίστε συσκευές πεδίου, τηλεφώνων κ.τ.λ. • Αντικαταστήστε παλιές συσκευές λογισμικού και υλικού. • Απενεργοποιήστε τις αχρησιμοποίητες θύρες και υπηρεσίες σε συσκευές • Εφαρμόστε και δοκιμάστε τα αντίγραφα ασφαλείας του συστήματος και τις διαδικασίες αποκατάστασης • Διαμόρφωση κρυπτογράφησης και ασφάλειας για πρωτόκολλα ICS	• Έκδοση διαδικασιών που δηλώνουν πώς το προσωπικό πρέπει να διαχειρίζεται το ICS με ασφαλή τρόπο. • Προώθηση μιας κουλτούρας διαλόγου και ανταλλαγής πληροφοριών μεταξύ προσωπικού ασφαλείας, πληροφορικής και OT.

Κεφάλαιο 6°

6.1. Κύρια Συμπεράσματα

Το τοπίο απειλών ICS περιλαμβάνει ένα ευρύ φάσμα. Αν και οι περισσότερες απειλές ICS υπήρχαν πάντα σε λανθάνουσα κατάσταση, μόλις στις αρχές της δεκαετίας του 2000 εμφανίστηκαν στο προσκήνιο ως απειλές. Από τις αρχές της δεκαετίας του 2000, ορισμένοι μηχανικοί ICS, όπως ο Joe Weiss και ο Eric Byers, καθώς και ειδικοί στον τομέα της ασφάλειας στον κυβερνοχώρο προειδοποίησαν για την έλλειψη ασφάλειας των ICS και τον σχετικό κίνδυνο για κρίσιμες υποδομές (Averill & Luiijf 2010; Dubowski 2004; Luiijf & Lassche 2006; Weiss 2009). Τα ICS σχεδιάστηκαν παραδοσιακά, γύρω από την αξιοπιστία και την ασφάλεια (Russel, 2015). Για μεγάλο χρονικό διάστημα, η ασφάλεια στον κυβερνοχώρο και ο αμοιβαίος έλεγχος ταυτότητας των στοιχείων δεν αποτελούσε προβληματισμό ούτε σε λειτουργικό ούτε σε σχεδιαστικό επίπεδο για τα ICS επειδή:

- Τα ICS βασίστηκαν σε εξειδικευμένα πρότυπα υλικού, ιδιόκτητου κώδικα και πρωτοκόλλου. Μόνο ειδικοί γνώριζαν πως να τα χρησιμοποιήσουν, και ούτως ή άλλως, κανένας άλλος, συμπεριλαμβανομένων των χακερς, δεν θα μπορούσε να ενδιαφέρεται για τον τομέα ICS, τα πρωτόκολλα και τις επικοινωνίες.
- Τα ICS λειτουργούν σε κλειστό περιβάλλον χωρίς σύνδεση με άλλους τομείς. Πρόκειται, δηλαδή, απλά για κάποια φυσική ασφάλεια.
- Τα ICS λειτουργούν μόνο σε καλοήθες περιβάλλον. Επομένως, δεν υπήρχε κανένας λόγος για τη δημιουργία ασφαλών και ισχυρών πρωτοκόλλων ICS, ώστε να εφαρμοστεί οποιαδήποτε κρυπτογραφική προστασία εκτός από έναν κυκλικό έλεγχο πλεονασμού σε πακέτα και τη δοκιμή αντοχής των εφαρμογών του πρωτοκόλλου ICS.

Η υιοθέτηση των γρήγορων κύκλων καινοτομίας σε υλικό πληροφορικής, λογισμικό πληροφορικής και δικτύωση από τον τομέα ICS, έχουν φέρει στο προσκήνιο μια σειρά κυβερνοαπειλών για αυτά τα συστήματα. Όλες αυτές οι βασικές παραδοχές σχετικά με το πλαίσιο ασφάλειας στον κυβερνοχώρο των ICS έχουν ελαττωθεί από αυτές τις εξελίξεις (Luiijf & Te Paske 2015, pp. 23–24):

- Εφαρμογές ICS, MES, HMI και κρίσιμες υπηρεσίες ICS λειτουργούν όλο και περισσότερο και χρησιμοποιούν εμπορικό υλικό εύκολα διαθέσιμο, κοινά λειτουργικά συστήματα (π.χ. Windows και Unix), τη συνέχεια πρωτοκόλλου TCP / IP και περιβάλλοντα ανοιχτού κώδικα. Η νέα τάση είναι οι εφαρμογές SCADA σε έξυπνα τηλέφωνα οι οποίες σύντομα θα εμφανιστούν και σε έξυπνα ρολόγια.
- Η γνώση και η τεκμηρίωση του ICS για τις υπηρεσίες ICS, τα πρωτόκολλα ICS και τις αδυναμίες τους είναι στοιχεία ευρέως διαθέσιμα στο Διαδίκτυο.

- Τα δίκτυα ICS συνδέονται άμεσα ή έμμεσα με δημόσια δίκτυα όπως το Διαδίκτυο. Ορισμένες φορές, τα ICS ελέγχονται ακόμη και από μια διεπαφή HMI που λειτουργεί σε ένα tablet από τοποθεσίες σπιτιού και τα Trojans και τα «σκουλήκια» βρίσκουν τρύπες στις συνδέσεις δικτύου για να μολύνουν διακομιστές ICS, υπηρεσίες και HMI. Οι χάκερς μπορούν να εντοπίσουν το ICS που είναι προσβάσιμο στο Διαδίκτυο και ευάλωτο από την υπηρεσία και τον κατασκευαστή με πολύ αποτελεσματικό τρόπο, χρησιμοποιώντας μηχανή αναζήτησης Shodan (Shodan 2015).
- Τα ICS έχουν πέσει θύματα δυσμενών εμπιστευτικών πληροφοριών και οι χάκερς έχουν ενδιαφερθεί πολύ για τα ICS, όπως φαίνεται από τον αριθμό των συνομιλιών που σχετίζονται με το ICS σε συνόδους χάκερς όπως το Black Hat και το DEF CON® στις ΗΠΑ και τα ισοδύναμά τους στην Ευρώπη και στην Ασία. Τα πλαίσια δοκιμών ασφάλειας ICS για το σύνολο εργαλείων MetaSploit διατίθενται στο κοινό, όχι μόνο για μηχανικούς συστημάτων και διεργασιών, αλλά και για τις κακόβουλες κοινότητες πειρατείας. Τέτοιο παράδειγμα φαίνεται στο (SCADAhacker.com 2015).

Επιπλέον, τα ICS δεν βρίσκονται μόνο στις κύριες διαδικασίες ενός οργανισμού αλλά ενσωματώνουν και κρύβονται σε αναβαθμίσεις γνωστής «λειτουργικότητας», την οποία βιώνει κανείς καθημερινά χωρίς να συνειδητοποιεί ότι περιέχει και λειτουργεί από ένα ή περισσότερα ICS, τέτοια παραδείγματα είναι: ένα σύστημα αυτοματισμού κτιρίων (BAS), ένα σύστημα ελέγχου πυρκαγιάς, κλιματισμού ή ελέγχου πρόσβασης. Συχνά, ούτε το τμήμα πληροφορικής, ούτε το τμήμα ICS είναι υπεύθυνο για την ασφάλεια στον κυβερνοχώρο. Αυτή είναι η απειλή ICS που σέρνεται σε οργανισμούς μέσω του backdoor όπως έχει εξηγηθεί στις εργασίες (Luiijf, 2013) και (GAO, 2015). Η παραβίαση τέτοιων ICS μπορεί να επηρεάσει τις κύριες λειτουργίες όπως αποδείχθηκε όταν οι χάκερς άλλαξαν το σύστημα κλιματισμού ενός κέντρου υπολογιστών μιας μεγάλης τράπεζας. Ταυτόχρονα, αυτά τα μη ασφαλή ICS μπορούν να αποτελέσουν σημείο εισόδου των χάκερς σε συστήματα ICT, όπως αποδείχθηκε από την παραβίαση των σημείων πώλησης της Target χρησιμοποιώντας συστήματα HVAC ως είσοδο (Krebs 2014).

Αν και είναι σημαντικές, αυτές οι απειλές ICS αντιπροσωπεύουν μόνο μία και κυρίως τεχνολογική πτυχή του τοπίου απειλών ICS. Άλλες συγκεκριμένες απειλές τομέα ICS πρέπει να κατανοηθούν καλά από τον οργανισμό προτού οι διάφοροι παράγοντες κινδύνου για την επιχείρηση, συμπεριλαμβανομένων εκείνων που προέρχονται από τα συστήματα και τα δίκτυα ICT και ICS μπορούν να αντιμετωπιστούν με ισορροπημένο τρόπο, λαμβάνοντας υπόψη το σύνολο των παραγόντων απειλών. Οι παράγοντες απειλών, ακούσια ή εκούσια, εξερευνούν τις απειλές. Εάν υπάρχουν ευπάθειες στην οργανωτική δομή, στα συστήματα και στα δίκτυα ICS, καθώς και στις διαδικασίες τους και ούτω καθεξής, παράγοντες απειλών όπως ανίκανη διαχείριση, χειριστές, χρήστες ICS, μηχανικοί ελέγχου διεργασιών, μηχανικοί τρίτων, μηχανικοί συντήρησης, (πρώην) εμπιστευτικοί υπάλληλοι (π.χ., δυσαρεστημένοι υπάλληλοι), χάκερς, hacktivists, οργανωμένο έγκλημα, ξένες πληροφορίες, και ξένοι κρατικοί φορείς και κρατικοί φορείς ενδέχεται να προκαλέσουν ένα

ανεπιθύμητο γεγονός. Το συμβάν μπορεί να επηρεάσει τις επιχειρήσεις, τις κρίσιμες λειτουργίες υποδομής και την ασφάλεια.

Η ασφάλεια των επικοινωνιών SCADA γίνεται πιο περίπλοκη επειδή έχει ληφθεί η απόφαση για σύνδεση των δικτύων SCADA με δίκτυα πληροφορικής, ώστε να επιτρέπονται καλύτερες και ταχύτερες επικοινωνίες. Αυτά τα νέα χαρακτηριστικά ωστόσο, έχουν αυξήσει τις απειλές και τους κινδύνους στις επικοινωνίες SCADA. Προς το παρόν δεν υπάρχουν πειστικές λύσεις για την ενίσχυση της ασφάλειας των επικοινωνιών SCADA με αυτήν την προοπτική. Η ιδέα της προσθήκης ευφυίας στο πεδίο δεν είναι νέα. Ηλεκτροβαλβίδες για αγωγούς αερίου είναι διαθέσιμες στην αγορά που, σε περίπτωση που λαμβάνουν μια γρήγορη ακολουθία εντολών ανοιχτού κλεισίματος, δεν τις εκτελούν για να αποφευχθεί η συνέπεια του μηχανικού σοκ. Ορισμένα έργα της ΕΕ (Ευρωπαϊκή Ένωση) όπως το FP6 SAFEGUARD και το FP7 CRUTIAL (Critical Utility Infrastructural Resilience) έχουν διερευνήσει την τεχνική σκοπιμότητα για τη βελτίωση της ασφάλειας στον κυβερνοχώρο του συστήματος SCADA βελτιώνοντας την ευφυΐα των συσκευών πεδίου.

Περαιτέρω επιπλοκές εμφανίζονται επειδή είναι γνωστό ότι, μεγάλο ποσοστό επιθέσεων προκαλείται από εσωτερικούς εισβολείς. Έτσι, η περιμετρική άμυνα από μόνη της δεν μπορεί να υπερασπιστεί το σύστημα. Σε τέτοιες περιπτώσεις, το ερώτημα που αντιμετωπίζει κανείς είναι αν υπάρχει επαρκής ένδειξη για μια συνεχιζόμενη επίθεση στη δυναμική του ίδιου του συστήματος (Shukla, 2016). Παρά το εύρος δραστηριοτήτων, έχει αποδειχθεί ότι οι μισές από αυτές έχουν ανθρώπινο σφάλμα στον πυρήνα τους (Evans et al., 2016). Ως εκ τούτου, θα πρέπει να αυξηθεί η εμπειρική και θεωρητική έρευνα σε ανθρώπινες πτυχές της ασφάλειας στον κυβερνοχώρο με βάση τον όγκο των περιστατικών που σχετίζονται με ανθρώπινα λάθη, προκειμένου να καθοριστούν τρόποι με τους οποίους μπορεί να ωφεληθεί η γενική πρακτική ασφάλειας στον κυβερνοχώρο.

6.2. Ανοικτά προβλήματα και μελλοντικές επεκτάσεις

Τα μέτρα ασφαλείας τείνουν να αγνοούν ότι, οι επίμονοι επιτιθέμενοι θα αποκτήσουν τελικά πρόσβαση σε όποια και αν είναι η περιμετρική προστασία. Ένας κύριος στόχος από τις σύγχρονες λύσεις ασφάλειας θα ήταν η ανάπτυξη νέων μεθόδων που θα μπορούσαν να ανιχνεύσουν και να διαταράξουν τις δραστηριότητες των εισβολέων μόλις αποκτήσουν πρόσβαση μέσα στο σύστημα. Ιδιαίτερη προσοχή πρέπει να δοθεί στην εφαρμογή νέων στρατηγικών που μπορούν να ανιχνεύσουν, να αποτρέψουν και να μετριάσουν τις επιθέσεις εξάλειψης δεδομένων, καθώς οι στρατηγικές ανίχνευσης/πρόληψης εισβολών θεωρούνται πλέον ακατάλληλες για την προστασία των δεδομένων (Rashid et al., 2014).

Προκειμένου να ενισχυθεί η ασφάλεια των συστημάτων SCADA, μία λύση είναι να παρασχεθεί η άμυνα σε βάθος (Wood et al., 2016) με την τοποθέτηση ελέγχων ασφαλείας έτσι ώστε να μειωθεί ο κίνδυνος

για τα μονάδες που προστατεύονται. Εφαρμόζοντας πολλαπλούς ελέγχους πάνω από τη μονάδα (σε αυτήν την περίπτωση τα δεδομένα διαμόρφωσης και διαχείρισης SCADA και ICS) ο αρχιτέκτονας εισάγει περαιτέρω εμπόδια, τα οποία πρέπει να ξεπεράσει ένας παράγοντας απειλής. Για τους πιο ικανούς παράγοντες απειλής αυτό θα δράσει επιβραδυντικά. Εντός του χρονικού διαστήματος που απαιτείται για να περάσει από ορισμένα από τα στοιχεία ελέγχου, η προστατευτική υπηρεσία παρακολούθησης θα πρέπει να έχει ειδοποιήσει κάποιον για την επίθεση, κάτι που θα επιτρέψει τη λήψη περαιτέρω μέτρων (όπως διακοπή της σύνδεσης των φορέων απειλής). Η άμυνα σε βάθος διασφαλίζει ότι δεν υπάρχει κανένα σημείο αποτυχίας από απειλές μονάδων, παρέχοντας διαφορετικά εμπόδια (έλεγχοι) σε μια πολυεπίπεδη προσέγγιση.

Η συνέργεια μεταξύ του ICS και του IoT έχει προκύψει σε μεγάλο βαθμό φέρνοντας νέες προκλήσεις ασφάλειας. Έχουν εντοπιστεί βασικά ζητήματα ασφαλείας για το ICS και τις τρέχουσες λύσεις. Η μελλοντική εργασία θα πρέπει πρωτίστως, να επικεντρώνεται στην ισορροπία μεταξύ ολιστικών προσεγγίσεων που μπορούν να αντιμετωπίσουν μια μεγάλη ποικιλία επιθέσεων, αναγνώριση σε πραγματικό χρόνο των εισβολέων με υψηλή ακρίβεια και λύσεις που επιβάλλουν χαμηλή επιβάρυνση στην επικοινωνία και την απόδοση των συστημάτων SCADA / ICS.

Βιβλιογραφία

Ahmed, I., Obermeier, S., Naedele, M., & Richard III, G. G. (2012). Scada systems: Challenges for forensic investigators. *Computer*, *45*(12), 44-51.

Al-saidi, N. M., Said, M. R. M., & Ahmed, A. M. (2011). Efficiency analysis for public key systems based on fractal functions.

Anandkumar, K. M., & Jayakumar, C. (2012). Pro-active prevention of clone node attacks in wireless sensor networks. *Journal of computer Science*, 1691.

Aris, S., Messai, A., Benslama, M., Nadjim, M., & M-Elharti, M. (2011). Integration of quantum cryptography through satellite networks transmission. *American Journal of Applied Sciences*, *8*(1), 71.

Asghar, M. R., Hu, Q., & Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. *Computer Networks*, *165*, 106946.

Averill, B., & Luiijf, H. A. M. (2010). Canvassing the cyber security landscape: Why Energy companies need to pay attention. *Journal of Energy Security, May*, *1-7*.

Babu, A. M., & Singh, K. J. (2013). Performance evaluation of chaotic encryption technique. *American Journal of Applied Sciences*, *10*(1), 35.

Barbosa, R. R. R. (2014). Anomaly detection in SCADA systems: a network based approach.

Barnum, S. (2008). Common attack pattern enumeration and classification (capec) schema description. *Cigital Inc, http://capec. mitre. org/documents/documentation/CAPEC_Schema_Descr iption_v1*, *3*.

Belenky, A., & Ansari, N. (2003). IP traceback with deterministic packet marking. *IEEE communications letters*, *7*(4), 162-164.

Belenky, A., & Ansari, N. (2003). IP traceback with deterministic packet marking. *IEEE communications letters*, *7*(4), 162-164.

Bellovin, S. M., Leech, M., & Taylor, T. (2003). ICMP traceback messages.

Bhaya, W. S., & AlAsady, S. A. (2012). Prevention of Spoofing Attacks in the Infrastructure wireless networks. *Journal of Computer Science*, *8*(10), 1769-1779.

Blakely, B. A. (2012). Cyberprints: identifying cyber attackers by feature analysis.

Brenner, S. W. (2006). At light speed: Attribution and response to cybercrime/terrorism/warfare. *J. Crim. L. & Criminology*, *97*, 379.

Cai, N., Wang, J., & Yu, X. (2008, July). SCADA system security: Complexity, history and new developments. In *2008 6th IEEE International Conference on Industrial Informatics* (pp. 569-574). IEEE.

Carr, J. (2012). *Inside cyber warfare: Mapping the cyber underworld*. " O'Reilly Media, Inc.".

Carr, N. B. (2014). *Development of a tailored methodology and forensic toolkit for industrial control systems incident response*. NAVAL POSTGRADUATE SCHOOL MONTEREY CA.

Clark, D. D., & Landau, S. (2010, November). The problem isn't attribution: it's multi-stage attacks. In *Proceedings of the Re-architecting the Internet Workshop* (pp. 1-6).

Cook, A., Nicholson, A., Janicke, H., Maglaras, L. A., & Smith, R. (2016). Attribution of cyber attacks on industrial control systems. *EAI Endorsed Trans. Indust. Netw. & Intellig. Syst.*, *3*(7), e3.

Curtis, K. (2005). A DNP3 protocol primer. *DNP User Group*, *2005*.

Dacier, M., Pham, V. H., & Thonnard, O. (2009, December). The WOMBAT Attack Attribution method: some results. In *International Conference on Information Systems Security* (pp. 19-37). Springer, Berlin, Heidelberg.

Drahansky, M., & Balitanas, M. (2011). Cipher for internet-based supervisory control and data acquisition architecture. *보안공학연구논문지 제권제호 년월 (Journal of Security Engineering)*, *8*(3), 6.

Drias, Z., Serhrouchni, A., & Vogel, O. (2015, August). Analysis of cyber security for industrial control systems. In *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)* (pp. 1-8). IEEE.

Dubowski, J., Tao, Y., & Py, C. (2004). *U.S. Patent Application No. 10/763,212*.

Duggan, D. P. (2005). *Generic threat profiles* (No. SAND2005-5411). Sandia National Laboratories.

Duggan, D. P. (2005). *Generic threat profiles* (No. SAND2005-5411). Sandia National Laboratories.

Espiner, T. (2010). Siemens warns Stuxnet targets of password risk. *CNet. Retrieved November*, *8*, 2015.

Fleury, T., Khurana, H., & Welch, V. (2008, March). Towards a taxonomy of attacks against energy control systems. In *International Conference on Critical Infrastructure Protection* (pp. 71-85). Springer, Boston, MA.

Fovino, I. N. (2014). SCADA system cyber security. In *Secure smart embedded devices, platforms and applications* (pp. 451-471). Springer, New York, NY.

Galloway, B., & Hancke, G. P. (2012). Introduction to industrial control networks. *IEEE Communications surveys & tutorials*, *15*(2), 860-880.

Gantz, J. F. (2008). The diverse and exploding digital universe-An updated forecast of worldwide information growth through 2011. *An IDC White Paper sponsored by EMC*.

Gao, W. (2015). The chemistry of graphene oxide. In *Graphene oxide* (pp. 61-95). Springer, Cham.

Gao, Z., & Ansari, N. (2005). Tracing cyber attacks from the practical perspective. *IEEE Communications Magazine*, *43*(5), 123-131.

Geers, K. (2010). The challenge of cyber attack deterrence. *Computer Law & Security Review*, *26*(3), 298-303.

Goodrich, M. T. (2002, November). Efficient packet marking for large-scale IP traceback. In *Proceedings of the 9th ACM Conference on Computer and Communications Security* (pp. 117-126).

Hamadeh, I., & Kesidis, G. (2006). A taxonomy of internet traceback. *International Journal of Security and Networks*, *1*(1-2), 54-61.

Hong, S., & Lee, S. (2008). Challenges and pespectives in security measures for the SCADA system. In *Proc. 5th Myongji-Tsinghua University Joint Seminar on Prototection & Automation*.

Hong, S., Lee, M., & Shin, D. Y. (2010, March). Experiments for embedded protection device for secure SCADA communication. In *2010 Asia-Pacific Power and Energy Engineering Conference* (pp. 1-4). IEEE.

Huitsing, P., Chandia, R., Papa, M., & Shenoi, S. (2008). Attack taxonomies for the Modbus protocols. *International Journal of Critical Infrastructure Protection*, *1*, 37-44.

Hunker, J., Hutchinson, B., & Margulies, J. (2008). Role and challenges for sufficient cyber-attack attribution. *Institute for Information Infrastructure Protection*, 5-10.

Igure, V. M., & Sean, A. (2009). Laughter, and Ronald D. Williams." Security issues in SCADA networks.". *Computers & Security*, *25*.

Judmayer, A., Krammer, L., & Kastner, W. (2014, May). On the security of security extensions for IP-based KNX networks. In *2014 10th IEEE Workshop on Factory Communication Systems (WFCS 2014)* (pp. 1-10). IEEE.

Keyser, M. (2002). The Council of Europe Convention on Cybercrime. *J. Transnat'l L. & Pol'y*, *12*, 287.

Kim, E., Massey, D., & Ray, I. (2005, February). Global Internet routing forensics. In *IFIP International Conference on Digital Forensics* (pp. 165-176). Springer, Boston, MA.

Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International journal of critical infrastructure protection*, *9*, 52-80.

Kohl, U. (2002). Eggs, jurisdiction, and the internet. *The International and Comparative Law Quarterly*, *51*(3), 555-582.

Korkmaz, T., Gong, C., Sarac, K., & Dykes, S. G. (2007). Single packet IP traceback in AS-level partial deployment scenario. *International Journal of Security and Networks*, *2*(1-2), 95-108.

Krebs, B. (2014). Target hackers broke in via HVAC company. *Krebs on Security*, *5*.

Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., & Halgand, Y. (2015). A survey of approaches combining safety and security for industrial control systems. *Reliability engineering & system safety*, *139*, 156-178.

Kuznetsov, V., Sandström, H., & Simkin, A. (2002, December). An evaluation of different IP traceback approaches. In *International Conference on Information and Communications Security* (pp. 37-48). Springer, Berlin, Heidelberg.

Kuznetsov, V., Sandström, H., & Simkin, A. (2002, December). An evaluation of different IP traceback approaches. In *International Conference on Information and Communications Security* (pp. 37-48). Springer, Berlin, Heidelberg.

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. RAND corporation.

Lüders, S. (2005). *Control systems under attack?* (No. CERN-OPEN-2005-025).

Luiijf, E. (2013). Why are we so unconsciously insecure?. *International journal of critical infrastructure protection (Print)*, *6*(3-4), 179-181.

Luiijf, E. (2016). Threats in industrial control systems. In *Cyber-security of SCADA and Other Industrial Control Systems* (pp. 69-93). Springer, Cham.

Luiijf, E. A. (2014). Are we in love with cyber insecurity?. *Int. J. Crit. Infrastructure Prot.*, *7*(3), 165-166.

Luiijf, E., & Te Paske, B. J. (2015). *Cyber security of industrial control systems* . Den Haag: TNO. Retrieved November 8, 2015, from http://www.tno.nl/ICS-security .

Luiijf, H. A. M., & Lassche, R. (2006). SCADA (on) veiligheid: een rol voor de overheid?(SCADA (in) security: a role for the government). *TNO/KEMA report,[Unclassified](June 2006)*.

Mahmood, A. N., Leckie, C., Hu, J., Tari, Z., & Atiquzzaman, M. (2010). Network traffic analysis and SCADA security. In *Handbook of Information and Communication Security* (pp. 383-405). Springer, Berlin, Heidelberg.

Majdalawieh, M., Parisi-Presicce, F., & Wijesekera, D. (2007). DNPSec: Distributed network protocol version 3 (DNP3) security framework. In *Advances in Computer, Information, and Systems Sciences, and Engineering* (pp. 227-234). Springer, Dordrecht.

Manikandan, S. P., & Manimegalai, R. (2012). Survey on mobile Ad Hoc network attacks and mitigation using routing protocols. *American Journal of Applied Sciences*, *9*(11), 1796.

Marali, M., Sudarsan, S. D., & Gogioneni, A. (2019, April). Cyber security threats in industrial control systems and protection. In *2019 International Conference on Advances in Computing and Communication Engineering (ICACCE)* (pp. 1-7). IEEE.

Miller, B., & Rowe, D. (2012, October). A survey SCADA of and critical infrastructure incidents. In *Proceedings of the 1st Annual conference on Research in information technology* (pp. 51-56).

Miller, B., & Rowe, D. (2012, October). A survey SCADA of and critical infrastructure incidents. In *Proceedings of the 1st Annual conference on Research in information technology* (pp. 51-56).

Moteff, J., & Parfomak, P. (2004, October). Critical infrastructure and key assets: definition and identification. LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE.

Musa, S., Shahzad, A., & Aborujilah, A. (2013, January). Secure security model implementation for security services and related attacks base on end-to-end, application layer and data link layer security. In *Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication* (pp. 1-8).

Naedele, M. (2007, January). Addressing IT security for critical control systems. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)* (pp. 115-115). IEEE.

Nance, K., Hay, B., & Bishop, M. (2009, January). Digital forensics: defining a research agenda. In *2009 42nd Hawaii International Conference on System Sciences* (pp. 1-6). IEEE.

Nicholson, A., Janicke, H., & Watson, T. (2013, September). An initial investigation into attribution in SCADA systems. In *1st International Symposium for ICS & SCADA Cyber Security Research 2013 (ICS-CSR 2013) 1* (pp. 56-65).

Nicholson, A., Watson, T., Norris, P., Duffy, A., & Isbell, R. (2012, July). A taxonomy of technical attribution techniques for cyber attacks. In *European conference on information warfare and security* (p. 188). Academic Conferences International Limited.

November 8, 2015, from https://scadahacker.com/resources/msf-scada.html .

Patel, S. C., Bhatt, G. D., & Graham, J. H. (2009). Improving the cyber security of SCADA communication networks. *Communications of the ACM*, *52*(7), 139-142.

Pollet, J. (2002, November). Developing a solid SCADA security strategy. In *2nd ISA/IEEE Sensors for Industry Conference* (pp. 148-156). IEEE.

Pothamsetty, V., & Franz, M. (2005). Scada honeynet project: Building honeypots for industrial networks. *SCADA Honeynet Project*, *15*.

Pouget, F., & Dacier, M. (2004, May). Honeypot-based forensics. In *AusCERT Asia Pacific Information Technology Security Conference*.

Raghini, M., Maheswari, N. U., & Venkatesh, R. (2013). Overview on key distribution primitives in wireless sensor network. *Journal of Computer Science*, *9*(5), 543.

Rautmare, S. (2011, December). SCADA system security: Challenges and recommendations. In *2011 Annual IEEE India Conference* (pp. 1-4). IEEE.

Risley, A., Roberts, J., & LaDow, P. (2003). Electronic security of real-time protection and SCADA communications. *Schweitzer Engineering Laboratories, SEL*.

Rrushi, J., & Campbell, R. (2008, March). Detecting cyber attacks on nuclear power plants. In *International Conference on Critical Infrastructure Protection* (pp. 41-54). Springer, Boston, MA.

Russel, J. (2015). *A brief history of SCADA/EMS* . Scadahistory.com. Retrieved November 8, 2015, from http://scadahistory.com/ .

Savage, S., Wetherall, D., Karlin, A., & Anderson, T. (2001). Network support for IP traceback. *IEEE/ACM transactions on networking*, *9*(3), 226-237.

SCADAhacker.com. (2015). *Metasploit modules for SCADA-related ulnerabilities* . Retrieved

Schmitt, M. N. (Ed.). (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press.

Shahzad, A., Musa, S., Aborujilah, A., & Irfan, M. (2014). A review: industrial control system (ICS) and their secuity issues. *American Journal of Applied Sciences*, *11*(8), 1398-1404.

Shahzad, A., Musa, S., Aborujilah, A., & Irfan, M. (2014, January). Industrial control systems (icss) vulnerabilities analysis and scada security enhancement using testbed encryption. In *Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication* (pp. 1-6).

Shahzad, S., Musa, S., Aborujilah, A., Ismail, M. N., & Irfan, M. (2013). Conceptual model of real time infrastructure within cloud computing environment. *Int. J. Comput. Networks*, *5*, 18-24.

Shodan. (2015). *Shodan* . Retrieved November 8, 2015, from http://www.shodanhq.com/ .

Snoeren, A. C., Partridge, C., Sanchez, L. A., Jones, C. E., Tchakountio, F., Kent, S. T., & Strayer, W. T. (2001). Hash-based IP traceback. *ACM SIGCOMM Computer Communication Review*, *31*(4), 3-14.

Song, D. X., & Perrig, A. (2001, April). Advanced and authenticated marking schemes for IP traceback. In *Proceedings IEEE INFOCOM 2001. Conference on Computer Communications. Twentieth Annual Joint Conference of the IEEE Computer and Communications Society (Cat. No. 01CH37213)* (Vol. 2, pp. 878-886). IEEE.

Spitzner, L. (2003). *Honeypots: tracking hackers* (Vol. 1). Reading: Addison-Wesley.

Stouffer, K., Falco, J., & Kent, K. (2006). Guide to Supervisory Control and Data Acquisition (SCADA) and industrial control systems security–initial public draft. *National Institute of Standards and Technology, Gaithersburg, Maryland*.

Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. *NIST special publication*, *800*(82), 16-16.

Strayer, W. T., Jones, C. E., Castineyra, I., Levin, J. B., & Hain, R. R. (2003). An integrated architecture for attack attribution. *BBN Technologies*, *10*.

Thing, V. L., Sloman, M., & Dulay, N. (2009, June). Adaptive response system for distributed denial-of-service attacks. In *2009 IFIP/IEEE International Symposium on Integrated Network Management* (pp. 809-814). IEEE.

Valli, C. (2009). SCADA forensics with Snort IDS.

Vávra, J., & Hromada, M. (2015, May). An evaluation of cyber threats to industrial control systems. In *International Conference on Military Technologies (ICMT) 2015* (pp. 1-5). IEEE.

Vincent, S., & Raja, J. I. J. (2010, February). A survey of IP traceback mechanisms to overcome denial-of-service attacks. In *Proceedings of the 12th international conference on Networking, VLSI and signal processing* (pp. 93-98). World Scientific and Engineering Academy and Society (WSEAS).

Wade, S. M. (2011). SCADA Honeynets: The attractiveness of honeypots as critical infrastructure security tools for the detection and analysis of advanced threats.

Weiss, J. (2009, July 21). *Securing the modern electric grid from physical and cyber attacks* . Statement for the Record, July 21, 2009 Hearing before the Subcommittee on Emerging. Washington, DC, USA. Retrieved November 8, 2015, from http://chsdemocrats.house.gov/SiteDocuments/20090722115326-92965.pdf .

Wheeler, D. A., & Larsen, G. N. (2003). *Techniques for cyber attack attribution*. INSTITUTE FOR DEFENSE ANALYSES ALEXANDRIA VA.

Wheeler, D. A., & Larsen, G. N. (2003). *Techniques for cyber attack attribution*. INSTITUTE FOR DEFENSE ANALYSES ALEXANDRIA VA.

Williams, T. J. (1994). The Purdue enterprise reference architecture. *Computers in industry*, *24*(2-3), 141-158.

Zhu, Q., Rieger, C., & Başar, T. (2011, August). A hierarchical security architecture for cyber-physical systems. In *2011 4th international symposium on resilient control systems* (pp. 15-20). IEEE.

Shamoon 2012**. https://en.wikipedia.org/wiki/Shamoon**

Steel Mill Germany 2015. https://www.trendmicro.com/vinfo/fr/security/news/cyber-attacks/german-steel-plant-suffers-significant-damage-from-targeted-attack

Advantech 2020. https://en.wikipedia.org/wiki/Conti_(ransomware)

Nork Hydro 2019. https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/

Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., & Lopez, J. (2018). A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. IEEE Communications Surveys & Tutorials, 20(4), 3453-3495.

Stuxnet 2010. https://en.wikipedia.org/wiki/Stuxnet

Triton SIS 2017. https://en.wikipedia.org/wiki/Triton_(malware)

Ukraine power grid cyberattack 2015-2016. https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyberattack

An illustration of the complexity of nation-state responsibility in attribution. https://www.researchgate.net/figure/An-illustration-of-the-complexity-of-nation-state-responsibility-in-attribution_fig1_293811556

Purdue Model for Control Hierarchy. https://www.researchgate.net/figure/Purdue-Model-for-Control-Hierarchy18_fig2_293811556

MITRE ATT&CK για ICS Matrix. https://collaborate.mitre.org/attackics/index.php/Main_Page

IT vs OT. http://icsmodel.infracritical.com/

Απειλές-και-προστασία-κρισίμων-υποδομών. Παπαγεωργίου Σπυρίδων: Απειλές-και-προστασία-κρισίμων-υποδομών-08-12-20.pdf