ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΕΛΟΠΟΝΝΗΣΟΥ

Σχολή Τεχνολογικών Εφαρμογών

Τμήμα Μηχανικών Πληροφορικής

Διπλωματική Εργασία

Ανάλυση ασφάλειας και απειλών σε Smart Grid και καλές πρακτικές

Συγγραφέας

Αγριμάκης Βασίλειος

Επιβλέπων

Δρ. Ιωάννης Πικραμμένος

Σπάρτη

Ιούλιος 2018

Η παρούσα εργασία πραγματοποιήθηκε στο πλαίσιο του προπτυχιακού προγράμματος, του τμήματος «Μηχανικών Πληροφορικής», του ΤΕΙ Πελοποννήσου. Για την ολοκλήρωσή της νιώθω την υποχρέωση να ευχαριστήσω όσους με βοήθησαν.

Καταρχάς, οφείλω να ευχαριστήσω θερμά, τον Επιβλέποντα καθηγητή, Δρ. Ιωάννη Πικραμμένο, που υπήρξε ιδιαιτέρως υποστηρικτικός όσες φορές χρειάστηκα τη βοήθειά του.

Επιπλέον, ευχαριστώ τους γονείς μου, Πέτρο και Αργυρώ, για τις ευκαιρίες που μου έδωσαν, χάρη στις οποίες έφθασα μέχρι εδώ.

Τέλος, ένα μεγάλο ευχαριστώ οφείλω και στον αδερφό μου και τους φίλους μου, που με στήριξαν διακριτικά αλλά σημαντικά.

ΠΕΡΙΛΗΨΗ

Σε αυτή την εργασία εξετάζεται το θέμα της ασφάλειας και των απειλών που παρουσιάζονται σε σύγχρονα περιβάλλοντα δικτύων ενέργειας Smart Grid και τρόποι και πρακτικές για βελτίωσή τους.
Πιο συγκεκριμένα, αναλύεται η δομή ενός Smart Grid και εντοπίζονται τα ωφέλη και τα προβλήματα που σχετίζονται με αυτό.
Παρουσιάζονται γνωστές απειλές αλλά και απειλές συγκεκριμένες για περιβάλλον Smart Grid, καθώς και το ποιοι υλοποιούν τις επιθέσεις αυτές.
Δείχνονται οι ευπάθειες και οι κίνδυνοι που υπάρχουν σε περιβάλλον Smart Grid.
Εξετάζονται τρόποι προς αποφυγή καταστάσεων όπου σχετιζόμενα αγαθά τίθενται σε κίνδυνο και σχολιάζονται μέθοδοι και καλές πρακτικές. Εντοπίζονται κάποιες αστοχίες στη βελτιστοποίηση λειτουργίας ενός Smart Grid και η ελλιπής αξιοποίηση της κυβερνοασφάλειας σε πλήθος συσκευών που συνδέονται σε ένα Smart Grid.
Τέλος, δίνονται συμπεράσματα που βγαίνουν από τα παραπάνω και προτάσεις για περαιτέρω έρευνα, που θα μπορούσαν ίσως να βοηθήσουν στην καλύτερη οργάνωση των δομών ενός Smart Grid και στη δημιουργία ασφαλέστερης διασύνδεσης.

Λέξεις-Κλειδιά: Ηλεκτρικό δίκτυο, Ευφυές Δίκτυο, κυβερνοεπίθεση, ασφάλεια, απειλές, βέλτιστες πρακτικές, καλές πρακτικές, Συστήματα Ηλεκτρικής Ενέργειας, ΣΗΕ, Έξυπνο δίκτυο, Έξυπνοι μετρητές, μοντελοποίηση δεδομένων, αισθητήρες, βύθιση τάσης, φορτίο αιχμής, ασύρματες επικοινωνίες, ενσύρματες επικοινωνίες, μικροδίκτυο, μακροδίκτυο, απομονωμένο μικροδίκτυο, ηλεκτρικά αυτοκίνητα, ευπάθειες, προστασία προσωπικών δεδομένων, ανανεώσιμες πηγές ενέργειας, ΑΠΕ.

Smart Grid, power system, cyber-attack, security, threats, best practices, good practices, smart meters, risks, attacks, vulnerabilities, security, data modeling, demand profile shaping, wireless communications, peak to average ratio, ad hoc network, blackout, electric grid, sensor, phasor, electric car, virtual power plant, microgrid, macrogrid, islanded microgrid, privacy, renewable sources.

1 ΕΙΣΑΓΩΓΗ

1.1 Διατύπωση του προβλήματος

Η αποτελεσματική μετάδοση και διανομή ηλεκτρικής ενέργειας αποτελεί θεμελιώδη προϋπόθεση για την αειφόρο ανάπτυξη και την ευημερία.

Ο κόσμος αντιμετωπίζει μεγάλες προκλήσεις όσον αφορά την αξιόπιστη ενσωμάτωση των ανανεώσιμων πηγών ενέργειας στο δίκτυο στον 21ο αιώνα.

Τα συστήματα ηλεκτρικής ενέργειας του μέλλοντος απαιτούν θεμελιώδεις καινοτομίες και βελτιώσεις για την αντιμετώπιση αυτών των προκλήσεων.

Το όραμα της Ευρωπαϊκής Ένωσης για το "έξυπνο δίκτυο" παρέχει μια πρώτη επισκόπηση των κατάλληλων μεταβολών στο μετασχηματισμό, τη διανομή και την παροχή ηλεκτρικής ενέργειας.

Αυτό συγκεντρώνει κοινά θέματα που αρχίζουν με τα έξυπνα δίκτυα και τα χαρακτηριστικά των νέων μονάδων παραγωγής ηλεκτρικής ενέργειας που βασίζονται σε ανανεώσιμες πηγές ενέργειας ή και σε πολύ αποδοτικές αρχές παραγωγής.

Καλύπτει, τις προηγμένες τεχνολογίες που εφαρμόζονται σήμερα στα δίκτυα μεταφοράς και διανομής και καινοτόμες λύσεις για τη διατήρηση της σημερινής υψηλής ισχύος ενέργειας υπό τις δύσκολες συνθήκες μεγάλης κλίμακας μεριδίων μεταβλητών ανανεώσιμων πηγών ενέργειας στο ετήσιο ενεργειακό ισοζύγιο.

Εκτός από την εξέταση των νέων πρωτογενών και δευτερογενών λύσεων τεχνολογίας και των εγκαταστάσεων ελέγχου για τα δίκτυα μεταφοράς και διανομής, συζητούνται επίσης οι μελλοντικές συνθήκες της αγοράς που επιτρέπουν στους φορείς εκμετάλλευσης δικτύων και στους χρήστες του δικτύου να επωφεληθούν.

Εξετάζεται ο αυξανόμενος ρόλος των τεχνολογιών της πληροφορίας και της επικοινωνίας.

Η σημασία των νέων προτύπων υπογραμμίζεται και περιγράφονται λεπτομερώς οι τρέχουσες διεθνείς προσπάθειες για την ανάπτυξη συνεκτικού συνόλου προτύπων.

Η παρουσίαση των διεθνών εμπειριών για την εφαρμογή νέων λύσεων Smart Grid στην πρακτική της λειτουργίας του δικτύου καταλήγει στο συμπέρασμα αυτό.

1.2 Σκοπός και Δομή της εργασίας

Σκοπός της παρούσας εργασίας είναι να αναλυθεί το θέμα των Smart Grid ως προς τα θέματα της ασφάλειας και των απειλών και να παρουσιαστούν καλές πρακτικές.

Πιο συγκεκριμένα, η παρούσα εργασία επιδιώκει τα ακόλουθα:

Να εξεταστεί το θέμα της ασφάλειας και των απειλών που παρουσιάζονται σε σύγχρονα περιβάλλοντα δικτύων ενέργειας Smart Grid και τρόποι και πρακτικές για βελτίωσή τους.

Να αναλυθεί η δομή ενός Smart Grid και να εντοπιστούν τα ωφέλη και τα προβλήματα που σχετίζονται με αυτό.

Έτσι, παρουσιάζονται γνωστές απειλές αλλά και απειλές συγκεκριμένες για περιβάλλον Smart Grid, καθώς και το ποιοι υλοποιούν τις επιθέσεις αυτές.

Δείχνονται οι ευπάθειες και οι κίνδυνοι που υπάρχουν σε περιβάλλον Smart Grid.

Εξετάζονται τρόποι προς αποφυγή καταστάσεων όπου σχετιζόμενα αγαθά τίθενται σε κίνδυνο και σχολιάζονται μέθοδοι και καλές πρακτικές.

Εντοπίζονται κάποιες αστοχίες στη βελτιστοποίηση λειτουργίας ενός Smart Grid και η ελλιπής αξιοποίηση της κυβερνοασφάλειας σε πλήθος συσκευών που συνδέονται σε ένα Smart Grid.

Τέλος, δίνονται συμπεράσματα που βγαίνουν από τα παραπάνω και προτάσεις για περαιτέρω έρευνα, που θα μπορούσαν ίσως να βοηθήσουν στην καλύτερη οργάνωση των δομών ενός Smart Grid και στη δημιουργία ασφαλέστερης διασύνδεσης.

1.3 Τι είναι το Smart Grid - δομή - ανάλυση

Σχ. 1 Δίκτυο Μεταφοράς Ενέργειας

Τι είναι το έξυπνο/ευφυές δίκτυο

Η τεχνολογία της ηλεκτρικής υποδομής - ένα κρίσιμο τμήμα κάθε αναπτυγμένης κοινωνίας - παρέμεινε σε μεγάλο βαθμό αμετάβλητη για τα τελευταία 100 περίπου χρόνια. Αν και τα δίκτυα έχουν κλιμακωθεί ανάλογα με την αύξηση της κατανάλωσης ηλεκτρικής ενέργειας, οι αρχές για τον έλεγχο της ροής και της διαχείρισης ενέργειας δεν έχουν δει την ίδια εξέλιξη όπως για παράδειγμα οι βιομηχανίες ηλεκτρονικών υπολογιστών και τηλεπικοινωνιών.

Αυτό αναμένεται να αλλάξει με την εισαγωγή των έξυπνων δικτύων, μιας εξέλιξης των σημερινών ηλεκτρικών δικτύων σε ένα πιο δυναμικό σύστημα, όπου η παρακολούθηση, ο έλεγχος και η επικοινωνία σε πραγματικό χρόνο μεταξύ ευφυών συσκευών σε όλα τα επίπεδα παραγωγής, διανομής και κατανάλωσης ηλεκτρικής

ενέργειας επιτρέπουν τη βέλτιστη χρήση τόσο της υπάρχουσας υποδομής όσο και της ενέργειας από ανανεώσιμες πηγές.

Σε γενικές γραμμές, το ηλεκτρικό δίκτυο χωρίζεται στα επίπεδα μετάδοσης και διανομής. Το επίπεδο μετάδοσης μεταφέρει ηλεκτρισμό υψηλής τάσης σε μεγάλες αποστάσεις και είναι αρκετά καλά εξοπλισμένο και υπόκειται σε αυτοματοποιημένο έλεγχο σε πραγματικό χρόνο.

Το επίπεδο διανομής λαμβάνει ηλεκτρική ενέργεια από το δίκτυο μεταφοράς και το παραδίδει στους τελικούς χρήστες. Σε σύγκριση με το επίπεδο μετάδοσης, αυτό το τμήμα του δικτύου δεν παρακολουθείται στον ίδιο βαθμό και οι ικανότητες ελέγχου των χειριστών του συστήματος είναι περιορισμένες. Αυτός είναι ο λόγος για τον οποίο πρέπει να ενημερωθεί η εταιρεία παροχής ενέργειας όποτε κάτι είναι λάθος (π.χ. διακοπή ρεύματος).
Επιπλέον, οι φορείς διανομής, εκτός της αύξησης της γενικής ζήτησης, θα αντιμετωπίσουν αρκετές προκλήσεις στα επόμενα χρόνια: θα υπάρξει αύξηση της κατανεμημένης παραγωγής (π.χ. ηλιακοί συλλέκτες οροφής, ανεμογεννήτριες, μικρής κλίμακας υδροηλεκτρικοί σταθμοί), αλλαγή στις καταναλωτικές συνήθειες (π.χ. ηλεκτρικών αυτοκινήτων, θερμοσίφωνες χωρίς δεξαμενή, αντλίες θερμότητας). Συν τοις άλλοις, ο σύγχρονος ηλεκτρικός και ηλεκτρονικός εξοπλισμός εξαρτάται περισσότερο από την ποιότητα της ηλεκτρικής ενέργειας σε σχέση με τους λαμπτήρες πυρακτώσεως.

Καθώς η κατασκευή νέων υποδομών είναι πολύ δαπανηρή, είναι επιθυμητό να αντιμετωπιστούν αυτές οι προκλήσεις βελτιστοποιώντας τις υπάρχουσες δυνατότητες του δικτύου. Αυτό προβλέπεται να συμβεί μετατρέποντας τα δίκτυα σε έξυπνα δίκτυα, όπου η ψηφιακή τεχνολογία επιτρέπει την αποτελεσματικότερη χρήση της υπάρχουσας υποδομής.
Στο πλαίσιο της εφαρμογής του έξυπνου δικτύου, εγκαθίστανται έξυπνοι μετρητές στους τελικούς χρήστες. Αυτοί οι μετρητές, καταγράφουν και μεταδίδουν την κατανάλωση ενέργειας σε τακτά χρονικά διαστήματα (συνήθως κάθε ώρα ή κάθε 15 λεπτά), και μπορούν επίσης να λαμβάνουν πληροφορίες (π.χ. κόστος κιλοβατώρας

και σήματα ελέγχου). Η εγκατάσταση των έξυπνων μετρητών θα αποτελέσει σημαντικό τμήμα μιας προηγμένης μετρητικής υποδομής (Advanced Measuring Infrastructure, AMI) και είναι σημαντικό να εκμεταλλευθούν πλήρως οι δυνατότητες και το δυναμικό της νέας αυτής υποδομής.

Πώς καθορίζεται το έξυπνο δίκτυο

Το έξυπνο δίκτυο είναι ένα σύστημα ηλεκτρικής ενέργειας επόμενης γενιάς που χρησιμοποιεί ψηφιακές τεχνολογίες - όπως υπολογιστές, ασφαλή δίκτυα επικοινωνιών, αισθητήρες και χειριστήρια, παράλληλα με τις λειτουργίες του ηλεκτρικού δικτύου - για την ενίσχυση της αξιοπιστίας του δικτύου και των συνολικών δυνατοτήτων του. Το έξυπνο δίκτυο επεκτείνεται στις πηγές καυσίμων για την παραγωγή ηλεκτρικής ενέργειας και στις πολλές συσκευές που χρησιμοποιούν ηλεκτρικό ρεύμα, όπως οικιακά ψυγεία, κατασκευαστικός εξοπλισμός ή φωτιστικά πάρκων.

Ειδικότερα, οι ασφαλείς ψηφιακές τεχνολογίες που προστέθηκαν στο δίκτυο και η αρχιτεκτονική που χρησιμοποιήθηκε για την ενσωμάτωση αυτών των τεχνολογιών στην υποδομή, καθιστούν δυνατή την ηλεκτρονική ρύθμιση και τη δυναμική διαμόρφωση του συστήματος. Αυτό δίνει στο δίκτυο πρωτοφανή ευελιξία και λειτουργικότητα και δυνατότητα αυτοεπιδιόρθωσης. Μπορεί να αντιδράσει και να ελαχιστοποιήσει τις επιπτώσεις απρόβλεπτων συμβάντων, όπως διακοπή ρεύματος, έτσι ώστε οι υπηρεσίες να είναι πιο ισχυρές και πάντα διαθέσιμες.

Το έξυπνο δίκτυο έχει επίσης πολύ σημαντικά χαρακτηριστικά που βοηθούν τον πλανήτη να αντιμετωπίσει τις ενεργειακές και περιβαλλοντικές προκλήσεις και να μειώσει τις εκπομπές διοξειδίου του άνθρακα. Για να δώσουμε μερικά παραδείγματα, ένα ισχυρότερο και πιο έξυπνο δίκτυο, σε συνδυασμό με μαζικές συσκευές αποθήκευσης ηλεκτρικής ενέργειας, μπορεί να αυξήσει σημαντικά την ενσωμάτωση πόρων αιολικής και ηλιακής ενέργειας στο μείγμα παραγωγής ηλεκτρικής ενέργειας. Μπορεί να υποστηρίξει ένα σύστημα ευρείας κλίμακας για τη φόρτιση ηλεκτρικών οχημάτων. Οι επιχειρήσεις κοινής ωφελείας μπορούν να χρησιμοποιούν τις τεχνολογίες τους για να χρεώνουν μεταβλητές τιμές βασισμένες σε διακυμάνσεις της προσφοράς και της ζήτησης σε πραγματικό χρόνο και οι καταναλωτές μπορούν να

διαμορφώσουν απευθείας τις υπηρεσίες τους για να ελαχιστοποιήσουν το κόστος ηλεκτρικής ενέργειας. Ένα 68% των καταναλωτών δεν έχουν ιδέα τι είναι ένα έξυπνο δίκτυο.

1.4 Ορισμός του «έξυπνου δικτύου» (Smart Grid)

Ο πρώτος επίσημος ορισμός του Smart Grid δόθηκε με τον νόμο περί ενεργειακής ανεξαρτησίας και ασφάλειας των ΗΠΑ, το 2007 (EISA-2007), ο οποίος εγκρίθηκε από το αμερικανικό Κογκρέσο τον Ιανουάριο του 2007 και υπογράφηκε στη νομοθεσία από τον Πρόεδρο Τζορτζ Μπους τον Δεκέμβριο του 2007. Το άρθρο 13 αυτού του νομοσχεδίου παρέχει μια περιγραφή, με δέκα χαρακτηριστικά, που μπορεί να θεωρηθεί ένας ορισμός για το Smart Grid. Ο εκσυγχρονισμός ενός συστήματος μεταφοράς και διανομής ηλεκτρικής ενέργειας για τη διατήρηση μιας αξιόπιστης και ασφαλούς υποδομής ηλεκτρικής ενέργειας που να μπορεί να ανταποκριθεί στη μελλοντική ανάπτυξη της ζήτησης, πρέπει να επιτυγχάνει καθένα από τα ακόλουθα, τα οποία όλα μαζί χαρακτηρίζουν ένα έξυπνο δίκτυο:

1. Αύξηση της χρήσης ψηφιακών πληροφοριών και τεχνολογιών ελέγχου για τη βελτίωση της αξιοπιστίας, της ασφάλειας και της αποδοτικότητας του ηλεκτρικού δικτύου
2. Δυναμική βελτιστοποίηση των λειτουργιών του δικτύου και των πόρων, με πλήρη ασφάλεια στον κυβερνοχώρο
3. Ανάπτυξη και ενοποίηση των κατανεμημένων πόρων
4. Ανάπτυξη και ενσωμάτωση της ανταπόκρισης στη ζήτηση, των πόρων της ζήτησης και των πόρων ενεργειακής απόδοσης
5. Ανάπτυξη «έξυπνων» τεχνολογιών (αυτοματοποιημένες και αλληλεπιδραστικές τεχνολογίες σε πραγματικό χρόνο, οι οποίες βελτιστοποιούν τη φυσική τους απόδοση) και την παραγωγή, συμπεριλαμβανομένων των ανανεώσιμων πόρων. λειτουργία συσκευών και συσκευών καταναλωτών) για τη μέτρηση, τις επικοινωνίες σχετικά με τις λειτουργίες και την κατάσταση του δικτύου, και την αυτοματοποίηση της διανομής
6. Ολοκλήρωση "έξυπνων" συσκευών και συσκευών για τους καταναλωτές
7. Ανάπτυξη και ενσωμάτωση προηγμένων τεχνολογιών αποθήκευσης ηλεκτρικής ενέργειας και τεχνολογιών ξυρίσματος αιχμής, συμπεριλαμβανομένων των

ηλεκτρικών και υβριδικών ηλεκτρικών οχημάτων με ηλεκτρική σύνδεση και του κλιματισμού θερμικής αποθήκευσης

8. Παροχή στους καταναλωτές έγκαιρων επιλογών πληροφόρησης και ελέγχου
9. Ανάπτυξη προτύπων επικοινωνίας και διαλειτουργικότητας των συσκευών και του εξοπλισμού που συνδέονται με το ηλεκτρικό δίκτυο, συμπεριλαμβανομένης της υποδομής που εξυπηρετεί το δίκτυο
10. Προσδιορισμός και μείωση των υπερβολικών ή περιττών φραγμών στην υιοθέτηση τεχνολογιών, πρακτικών και υπηρεσιών ευφυούς δικτύου

Ένα κοινό στοιχείο για τους περισσότερους ορισμούς είναι η εφαρμογή της ψηφιακής επεξεργασίας και επικοινωνιών στο ηλεκτρικό δίκτυο, καθιστώντας κεντρική τη ροή δεδομένων και τη διαχείριση πληροφοριών στο έξυπνο δίκτυο. Διάφορες δυνατότητες προκύπτουν από τη βαθιά ολοκληρωμένη χρήση της ψηφιακής τεχνολογίας με τα δίκτυα ηλεκτρικής ενέργειας. Η ενσωμάτωση των νέων πληροφοριών για το δίκτυο είναι ένα από τα βασικά ζητήματα στο σχεδιασμό έξυπνων δικτύων. Οι επιχειρήσεις ηλεκτρικής ενέργειας πρέπει να ολοκληρώσουν αυτή την μετάβαση σε τρία στάδια:

- Βελτίωση των υποδομών (που ονομάζεται ισχυρό δίκτυο στην Κίνα)
- Προσθήκη του ψηφιακού επιπέδου (digital layer), το οποίο αποτελεί την ουσία του έξυπνου δικτύου
- Μετασχηματισμό των επιχειρηματικών διαδικασιών, που είναι αναγκαία για την κεφαλαιοποίηση των επενδύσεων στην έξυπνη τεχνολογία

Μεγάλο μέρος των εργασιών που εκτελούνται στον εκσυγχρονισμό των ηλεκτρικών δικτύων, ιδίως στον αυτοματισμό υποσταθμών και διανομής, περιλαμβάνεται στη γενική έννοια του έξυπνου δικτύου.

1.5 Χαρακτηριστικά του έξυπνου δικτύου

Τα έξυπνο δίκτυα αντιπροσωπεύουν την πλήρη δέσμη τρεχουσών και προτεινόμενων απαντήσεων στις προκλήσεις της παροχής ηλεκτρισμού. Λόγω του ποικίλου φάσματος παραγόντων, υπάρχουν πολυάριθμες ανταγωνιστικές ταξινομίες και δεν υπάρχει συμφωνία σε έναν γενικά αποδεκτό ορισμό. Παρ' όλα αυτά, μπορούμε να προσπαθήσουμε να κάνουμε μια κατηγοριοποίηση των παραγόντων που πρέπει να διέπουν ένα έξυπνο δίκτυο.

Fig. 1. Modified NIST conceptual model of SG architecture.

Σχ. 2 Βελτιστοποιημένο Μοντέλο Αρχιτεκτονικής Smart Grid

1.5.1 Αξιοπιστία (Reliability)

Τα έξυπνα δίκτυα χρησιμοποιούν τεχνολογίες όπως η εκτίμηση της κατάστασης, που βελτιώνουν την ανίχνευση σφαλμάτων και επιτρέπουν την αυτοθεραπεία του δικτύου χωρίς την παρέμβαση των τεχνικών. Αυτό εξασφαλίζει πιο αξιόπιστη παροχή ηλεκτρικής ενέργειας και μειώνει την ευπάθεια σε φυσικές καταστροφές ή πιθανές επιθέσεις.

Παρόλο που οι πολλές διαδρομές αποτελούν χαρακτηριστικό γνώρισμα των έξυπνων δικτύων, τα παλιά δίκτυα διανομής ενέργειας περιείχαν επίσης πολλαπλές διαδρομές. Οι αρχικές γραμμές μεταφοράς ηλεκτρικού ρεύματος στα δίκτυα κατασκευάστηκαν χρησιμοποιώντας ένα ακτινωτό μοντέλο, ενώ η συνδεσιμότητα αργότερα εξασφαλίστηκε μέσω πολλαπλών διαδρομών, που αναφέρονται ως δομή δικτύου. Αυτό, όμως, δημιούργησε ένα νέο πρόβλημα. Αν η τρέχουσα ροή ή συναφή φαινόμενα, σε όλο το δίκτυο, υπερβαίνουν τα κατασκευαστικά όρια ενός συγκεκριμένου υλικού/στοιχείου του δικτύου, αυτό θα μπορούσε να αποτύχει και το ρεύμα να μεταφερθεί σε άλλα στοιχεία του δικτύου, τα οποία ενδεχομένως να αποτύχουν επίσης, προκαλώντας φαινόμενο ντόμινο (με τελικό αποτέλεσμα, μία διακοπή ρεύματος). Μια τεχνική για την αποτροπή αυτού του προβλήματος, είναι η απόρριψη του φορτίου μέσω εκούσιας μηχανικής διακοπής της ηλεκτρικής ενέργειας (blackout), ή η μείωση της τάσης (brownout).

Ο οικονομικός αντίκτυπος της βελτιωμένης αξιοπιστίας του δικτύου και της ανθεκτικότητας, είναι αντικείμενο μελετών και μπορεί να υπολογιστεί χρησιμοποιώντας εξελιγμένα εργαλεία υπολογισμού.

1.5.2 Ευελιξία στην τοπολογία του δικτύου (Topology Flexibility)

Η υποδομή μετάδοσης και διανομής επόμενης γενιάς θα είναι σε θέση να χειρίζεται καλύτερα πιθανές ροές ενέργειας διπλής κατεύθυνσης, επιτρέποντας την κατανεμημένη παραγωγή, όπως από φωτοβολταϊκά πάνελ στις στέγες των κτιρίων, αλλά και τη χρήση κυψελών καυσίμου, στροβίλων, τη φόρτιση από ή προς ηλεκτρικές μπαταρίες, την αντλημένη υδροηλεκτρική ενέργεια και άλλες πηγές.

Τα κλασσικά δίκτυα σχεδιάστηκαν για μονοφασική ροή ηλεκτρικού ρεύματος, αλλά αν ένα τοπικό υποσύστημα παράγει περισσότερη ενέργεια από ότι καταναλώνει, η αντίστροφη ροή μπορεί να προκαλέσει ζητήματα ασφάλειας και αξιοπιστίας. Ένα έξυπνο δίκτυο στοχεύει στη διαχείριση αυτών των καταστάσεων.

1.5.3 Αποδοτικότητα (Efficiency)

Μεγάλη συνεισφορά στη συνολική βελτίωση της αποτελεσματικότητας της ενεργειακής υποδομής, αναμένεται από την ανάπτυξη της τεχνολογίας έξυπνων δικτύων, ιδίως με τη διαχείριση της ζήτησης. Για παράδειγμα, απενεργοποίηση των κλιματιστικών κατά τη διάρκεια μικρής διάρκειας αιχμών στη ζήτηση ηλεκτρικής ισχύος, μειώνοντας την τάση, όταν είναι δυνατό, στις γραμμές διανομής, μέσω της βελτιστοποίησης Τάσης/VAR (VVO). Επίσης, εξαλείφεται η ανάγκη αποστολής υπαλλήλου για ανάγνωση των μετρητών και μειώνεται η ανάγκη αποστολής τεχνικού, μέσω της βελτιωμένης διαχείρισης διακοπών, χρησιμοποιώντας δεδομένα από Υποδομές Προηγμένης Μέτρησης. Το συνολικό αποτέλεσμα είναι η μείωση των πλεονασμάτων στις γραμμές μεταφοράς και διανομής και η αποδοτικότερη χρήση των γεννητριών, πράγμα που οδηγεί σε χαμηλότερες τιμές ενέργειας.

1.5.4 Αειφορία - Βιωσιμότητα (Sustainability)

Η βελτιωμένη ευελιξία των έξυπνων δικτύων, επιτρέπει μεγαλύτερη διείσδυση των μεταβλητής απόδοσης ανανεώσιμων πηγών ενέργειας, όπως η ηλιακή ενέργεια και η αιολική ενέργεια, ακόμη και χωρίς την προσθήκη συστημάτων αποθήκευσης ενέργειας. Η τρέχουσα υποδομή δικτύου, δεν έχει κατασκευαστεί για να επιτρέπει πολλά κατανεμημένα σημεία τροφοδοσίας και, τυπικά, ακόμη και αν επιτρέπεται κάποια τροφοδοσία σε τοπικό επίπεδο (διανομή), η υποδομή σε επίπεδο μεταδόσεως δεν μπορεί να την εξυπηρετήσει. Οι ταχείες διακυμάνσεις της κατανεμημένης παραγωγής, όπως λόγω συννεφιάς ή πολύ δυνατών ανέμων, παρουσιάζουν σημαντικές προκλήσεις για τους μηχανικούς ηλεκτρικής ενέργειας που πρέπει να εξασφαλίσουν σταθερά επίπεδα ισχύος, μέσω της διαφοροποίησης της παραγωγής των «πιο ελεγχόμενων» γεννητριών, όπως αεροστροβίλων και υδροηλεκτρικών

γεννητριών. Για αυτό το λόγο, η τεχνολογία έξυπνων δικτύων είναι απαραίτητη προϋπόθεση για πολύ μεγάλες ποσότητες ανανεώσιμης ηλεκτρικής ενέργειας στο δίκτυο.

Εαν δούμε συγκεντρωτικά τα παραπάνω, φθάνουμε αβίαστα στο συμπέρασμα οτι την επόμενη δεκαετία θα γίνει πλήρης μετατροπή του τρόπου που χρησιμοποιούμε, παράγουμε και σχετιζόμαστε με την ηλεκτρική ενέργεια. Ηλιακοί συλλέκτες οροφής, ηλεκτρικά αυτοκίνητα και έξυπνες συσκευές που προετοιμάζουν (θερμαίνουν ή ψύχουν) το σπίτι μας τις ώρες που η ηλεκτρική ενέργεια είναι φθηνότερη, είναι μόνο μερικά παραδείγματα των αναμενόμενων αλλαγών.

Η υποδομή του ηλεκτρικού δικτύου πρέπει να αλλάξει δραματικά για να υποστηρίξει αυτή την εξέλιξη, με την διάδοση έξυπνων μετρητών με αμφίδρομες δυνατότητες επικοινωνίας ως ένα από τα άμεσα πρώτα βήματα.

Προκειμένου να ενισχυθεί η κατανόηση και να επιτευχθούν οι παραπάνω στόχοι, πολλοί οργανισμοί και ερευνητικά προγράμματα, όπως τα κέντρα ελέγχου επόμενης γενιάς για έξυπνα δίκτυα, αναζητούν ήδη τρόπους αξιοποίησης των δεδομένων προηγμένης υποδομής μετρήσεων πέρα από τις απλές μετρήσεις και χρεώσεις.

Πώς σχεδιάζεται να λειτουργήσει το Smart Grid

Υπάρχουν 2,5 δισεκατομμύρια ηλεκτρικά μέτρα, και μόνο το 8% από αυτά έχουν σήμερα οποιοδήποτε είδος αυτοματισμού. Οι αισθητήρες και τα ασύρματα στοιχεία θα επιτρέψουν στα βοηθητικά προγράμματα να συλλέγουν δεδομένα σχετικά με την κατανάλωση ενέργειας, τα καιρικά δεδομένα και τη χωρητικότητα μετάδοσης. Η αποθήκευση ενέργειας θα διαδραματίσει εξίσου σημαντικό ρόλο. Δεδομένου οτι η ενέργεια πρέπει να καταναλώνεται όταν δημιουργείται, τα σημερινά δίκτυα έχουν σχεδιαστεί ώστε να λειτουργούν πάντα σε μέγιστη χωρητικότητα. Ωστόσο, τα φορτία αιχμής απαιτούνται μόνο γύρω στο 5% του έτους.

Αυτός είναι ο λόγος για τον οποίο οι υπεύθυνοι ανάπτυξης των δικτύων, θέλουν να είναι σε θέση να χρησιμοποιήσουν την επιλογή αποθήκευσης στις μπαταρίες ηλεκτρικών αυτοκινήτων για την αποθήκευση του αχρησιμοποίητου ηλεκτρισμού.

1.5.5 Οι επιπτώσεις της ευρυζωνικότητας στο δίκτυο

Οι επιχειρήσεις κοινής ωφελείας θα χρησιμοποιούν μια ποικιλία από ενσύρματες και ασύρματες, ευρυζωνικές τεχνολογίες και τεχνολογίες στενής ζώνης επικοινωνιών για τα έξυπνα δίκτυά τους. Τα δίκτυα επικοινωνιών θα μεταφέρουν πληροφορίες προς και από τους πολλούς αισθητήρες, τις τεχνολογίες ελέγχου και τις συσκευές μέτρησης που θα χρησιμοποιηθούν σε ένα έξυπνο δίκτυο, συμπεριλαμβανομένων συσκευών που χρησιμοποιούνται σε σπίτια και επιχειρήσεις.

Ένα βοηθητικό πρόγραμμα θα χρησιμοποιήσει ευρυζωνικές συνδέσεις για να συνεργαστεί με τους πελάτες για υπηρεσίες έξυπνων δικτύων. Οι πελάτες θα χρησιμοποιούν εφαρμογές συνδεδεμένες στο δίκτυο για την παρακολούθησης της οικιακής τους ενέργειας, από οικιακούς υπολογιστές, smartphones ή tablets, για να αλληλεπιδρούν με προγράμματα απόκρισης-ζήτησης ή διαχείρισης ενέργειας.
Οι επιχειρήσεις κοινής ωφελείας θα χρησιμοποιήσουν πιθανώς έναν συνδυασμό τεχνολογιών ευρυζωνικών επικοινωνιών, συμπεριλαμβανομένης της δικής τους υποδομής για ευρυζωνικές επικοινωνίες μέσω της γραμμής ισχύος. Θα χρησιμοποιούν επίσης μια ποικιλία οπτικών ινών, καλωδιακών και ασύρματων τεχνολογιών για ευρυζωνικές επικοινωνίες.

2 Smart Grid – Οφέλη / Αγαθά

2.1 Smart Grid - Οφέλη

Χρησιμοποιούμε ηλεκτρική ενέργεια σε διάφορες μορφές, σχεδόν κάθε λεπτό της ημέρας. Η εξάρτησή μας από την τεχνολογία, όπως τα smartphones και οι υπολογιστές, συνεχίζει να αυξάνεται, το ίδιο και η κατανάλωση αυτού του πολύτιμου πόρου. Η αυξημένη ζήτηση και η ώθηση για καθαρότερη ενέργεια απαιτεί, έναν από καιρό καθυστερημένο, εκσυγχρονισμό των ηλεκτρικών δικτύων. Μία μέθοδος αντιμετώπισης αυτής της πρόκλησης είναι η αντικατάσταση των υφιστάμενων δικτύων με "έξυπνα" δίκτυα.
Σε αντίθεση με το παραδοσιακό ηλεκτρικό δίκτυο, το οποίο μεταφέρει ηλεκτρική ενέργεια από μονάδες παραγωγής ενέργειας σε καταναλωτές, ένα έξυπνο δίκτυο περιλαμβάνει ένα "αμφίδρομο" δίκτυο επικοινωνίας που επιτρέπει στους καταναλωτές, τους χειριστές και τις αυτοματοποιημένες συσκευές να παρακολουθούν τα δεδομένα κατανάλωσης ενέργειας σε πραγματικό χρόνο.

Ένας θετικός παράγοντας της τεχνολογίας των έξυπνων δικτύων είναι οτι είναι δυνατή η παρακολούθηση με μεγαλύτερη ακρίβεια και η διαχείριση της χρήσης ενέργειας, ελέγχοντας τους έξυπνους μετρητές. Οι έξυπνοι μετρητές αλληλεπιδρούν με το δίκτυο στέλνοντας δεδομένα κατανάλωσης ενέργειας και παραγωγής εμπρός και πίσω, επιτρέποντας στους καταναλωτές να βλέπουν σε πραγματικό χρόνο τη χρήση ενέργειας.
Επιπλέον, οι έξυπνοι μετρητές επιτρέπουν στις εταιρείες κοινής ωφέλειας να προσφέρουν τιμές σε πραγματικό χρόνο, οι οποίες παρέχουν στους καταναλωτές ένα κίνητρο για αποτελεσματικότερη διαχείριση της κατανάλωσης ενέργειας και εξοικονόμηση χρημάτων.
Ένας άλλος τρόπος με τον οποίο ένα έξυπνο δίκτυο μπορεί να ωφελήσει το περιβάλλον είναι ότι οι παραγωγοί ανανεώσιμων πηγών ενέργειας, όπως οι ηλιακές εγκαταστάσεις και τα αιολικά πάρκα, μπορούν να αποθηκεύουν ή να αποστέλλουν με

ασφάλεια την πλεονάζουσα ενέργεια στο δίκτυο, βελτιώνοντας την παραγωγή και τη διανομή καθαρής ενέργειας.

Η εφαρμογή της τεχνολογίας των έξυπνων δικτύων θα δημιουργήσει επίσης μια νέα αγορά εργασίας για προϊόντα και υπηρεσίες σχετιζόμενα με την ενέργεια. Για παράδειγμα, η ενσωμάτωση της τεχνολογίας έξυπνου δικτύου απαιτεί προηγμένο λογισμικό παρακολούθησης της ενέργειας, οι εταιρείες να εγκαταστήσουν την υποδομή μέτρησης καθώς και τις υπηρεσίες επικοινωνίας, διανομής και αυτοματοποίησης των υποσταθμών.

Σύμφωνα με την Techrepublic.com, η παγκόσμια αγορά τεχνολογιών και υπηρεσιών σχετικών με το έξυπνο δίκτυο θα αυξηθεί από 1,7 δισεκατομμύρια δολάρια το 2014 σε περισσότερα από 11,1 δισεκατομμύρια δολάρια το 2023, ένα ελπιδοφόρο μέλλον για τη δημιουργία προϊόντων και υπηρεσιών σχετικών με την καθαρή ενέργεια.

2.1.1 Οφέλη και ανησυχίες της τεχνολογίας Smart Grid - Πώς επηρεάζει τους καταναλωτές

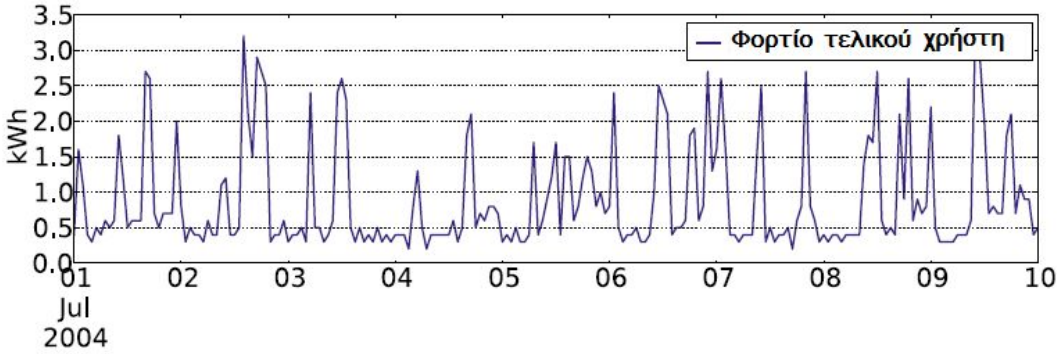
Ένα δίκτυο ηλεκτρικής ενέργειας που χρησιμοποιεί σύγχρονες τεχνολογίες πληροφορικής θα εξαλείψει τις διακοπές και τις υποτάσεις, και θα επιτρέψει καλύτερη συνολική αξιοπιστία μέσω της προηγμένης παρακολούθησης και διαχείρισης. Οι πελάτες θα αποκτήσουν περισσότερες γνώσεις σχετικά με τον τρόπο με τον οποίο χρησιμοποιούν ηλεκτρική ενέργεια, κερδίζοντας πληροφορίες σχετικά με το ενεργειακό τους κόστος σε πραγματικό χρόνο.

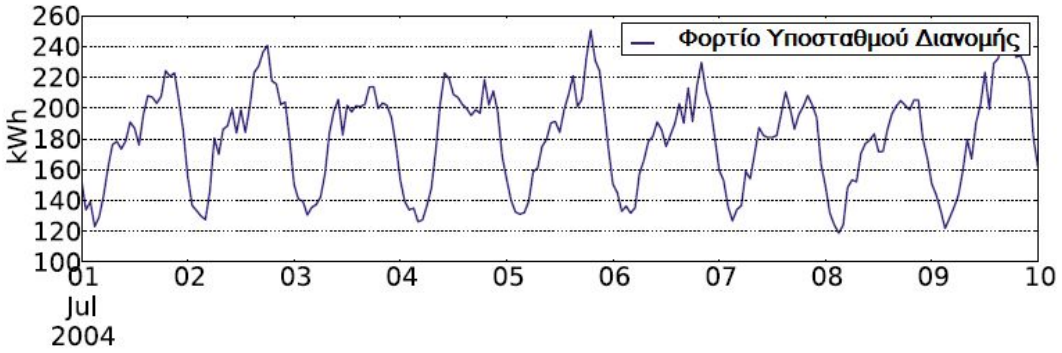
Όπως συνέβη με το Διαδίκτυο, θα γίνει η πλατφόρμα στην οποία θα μπορούν να κατασκευαστούν νέοι τύποι προϊόντων και υπηρεσιών, όπως η χρήση υβριδικών και ηλεκτρικών αυτοκινήτων για την αποθήκευση ενέργειας και στη συνέχεια η πώλησή τους στο δίκτυο. Θα ήταν επίσης ευκολότερο για τις οικιακές γεννήτριες να συνδεθούν στο δίκτυο και να λάβουν πληρωμές από επιχειρήσεις κοινής ωφέλειας για την πλεονάζουσα ηλιακή ενέργεια ή την παραγωγή τους με άλλους τρόπους.

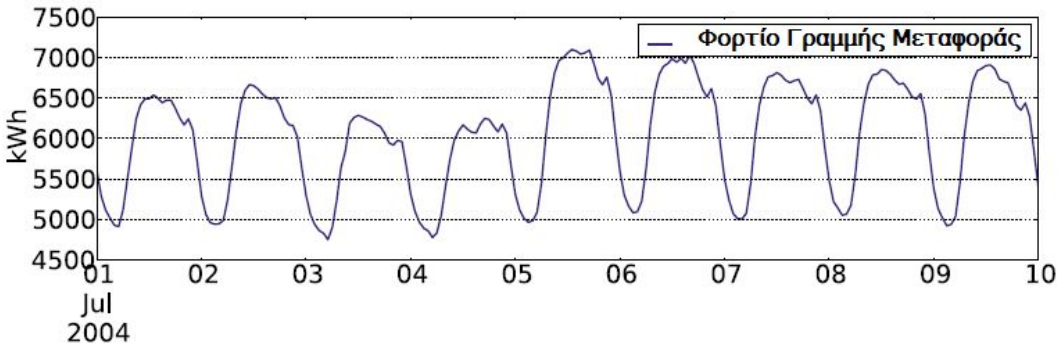
Οι έξυπνοι μετρητές επιτρέπουν στους χρήστες ηλεκτρικής ενέργειας να επιλέξουν να μειώσουν τους λογαριασμούς ηλεκτρικού ρεύματος μεταφέροντας τη χρήση τους σε χαμηλότερες περιόδους κόστους. Αυτή η δραστηριότητα των χρηστών θεωρείται όλο και περισσότερο, από τους υπεύθυνους χάραξης πολιτικής, ως βασικό μέρος ενός

σχεδίου για την αντιμετώπιση των αναγκών ηλεκτρισμού. Η χρησιμότητα ωφελείται επίσης από τη λήψη λεπτομερών πληροφοριών κατά τη διάρκεια διακοπών ρεύματος που θα συντομεύσουν το χρόνο απόκρισης και θα εστιάσουν τις προσπάθειες επισκευής.

Το έξυπνο δίκτυο θα συμβάλει επίσης στην πρόληψη τρομοκρατικών επιθέσεων μέσω, του ενδοκτισμένου στη φιλοσοφία του δικτύου, πλεονασμού και τις ικανότητες αυτοθεραπείας του δικτύου.







Σχ. 3 Δείγμα χρονοσειρών δεδομένων φορτίου ισχύος στον τελικό χρήστη, στον υποσταθμό διανομής και στη γραμμή μεταφοράς.

2.2 Smart Grid - Αγαθά

Με την τεχνολογία έξυπνου δικτύου μπορείτε να εξοικονομήσετε χρήματα, να ελέγχετε αποτελεσματικότερα την καθημερινή κατανάλωση ηλεκτρικής ενέργειας και να προστατεύετε το περιβάλλον. Διαβάστε παρακάτω και θα συμφωνήσετε ότι υπάρχουν πολλοί λόγοι για τους οποίους το ευφυές δίκτυο είναι το ευεργετικό για σας με τους εξής τρόπους:

Εξοικονόμηση χρημάτων: Οι επιχειρήσεις κοινής ωφέλειας μπορούν να παρέχουν προγράμματα απόκρισης ζήτησης, τα οποία έχουν σχεδιαστεί για να βοηθούν τους χρήστες ενέργειας να μειώσουν τη χρήση ενέργειας κατά τη διάρκεια των θερμικών κυμάτων και των κρύων περιόδων, μειώνοντας τις περιόδους μέγιστης ζήτησης στο δίκτυο, εξοικονομώντας χρήματα.

Διαχείριση της κατανάλωσης ενέργειας: Η ψηφιακή μέτρηση επιτρέπει στα άτομα να μετριάσουν τη χρήση της οικιακής τους ενέργειας και να μειώσουν τη ζήτηση. Παρέχει πρόσβαση στα δεδομένα κατανάλωσης ηλεκτρικής ενέργειας, ιδίως κατά τις αιχμές υψηλής κατανάλωσης ενέργειας, οι οποίες βοηθούν τους χρήστες ενέργειας να κάνουν πιο ενημερωμένες ενεργειακές επιλογές.

Αξιοπιστία ενέργειας: Οι ψηφιακοί μετρητές επιτρέπουν στις επιχειρήσεις κοινής ωφέλειας να παρέχουν πιο αξιόπιστη υπηρεσία ενέργειας, η οποία μειώνει την ποσότητα ηλεκτρικών διακοπών. Οι έξυπνοι μετρητές μπορούν να αναφέρουν ηλεκτρονικά τη θέση μιας διακοπής πριν ένα άτομο θα χρειαστεί ποτέ να καλέσει τη χρησιμότητά τους, καθιστώντας την αποκατάσταση ταχύτερη και την κοινοποίηση κατάστασης στα άτομα πολύ ευκολότερη.

Προστασία του περιβάλλοντος: Το έξυπνο δίκτυο μπορεί να μειώσει την ατμοσφαιρική ρύπανση από τον τομέα ηλεκτρικής ενέργειας έως και το 30% μέχρι το 2030, γλιτώνοντας 34.000 θανάτους ετησίως. Επίσης, το έξυπνο δίκτυο διασφαλίζει ότι μπορούν να ενσωματωθούν πηγές ανανεώσιμης ενέργειας όπως αιολικά πάρκα, ηλιακές εγκαταστάσεις και υδροηλεκτρικοί σταθμοί. Η ετήσια εξοικονόμηση ενέργειας από το έξυπνο δίκτυο θα μπορούσε να ισούται με 70 εκατομμύρια οδικές

μετακινήσεις σε όλο τον κόσμο ή την οδήγηση ενός ηλεκτρικού αυτοκινήτου 1,7 τρισεκατομμυρίων μιλίων.

Αναμόρφωση του γηρασμένου εξοπλισμού: Το τρέχον ηλεκτρικό σύστημα είναι ηλικίας δεκαετιών και εξαρτάται από τον εξοπλισμό που πλησιάζει στο τέλος της χρήσιμης ζωής του. Το έξυπνο δίκτυο ενημερώνει αυτήν την υποδομή, εξασφαλίζοντας ότι εξακολουθούν να πληρούνται τα πρότυπα ασφαλείας, ότι η ισχύς παρέχεται με συνέπεια και ότι το σύστημα διαχειρίζεται αποτελεσματικά.

Εξοπλισμός του δικτύου για να καλύψει την αυξανόμενη ζήτηση: Καθώς οι Αμερικανοί σήμερα χρησιμοποιούν περισσότερες ηλεκτρονικές συσκευές από ποτέ, η ζήτηση για ενέργεια συνεχίζει να αυξάνεται με ταχύ ρυθμό. Χωρίς βελτιώσεις στο έξυπνο δίκτυο, το παλαιό σύστημα, το οποίο έχει ήδη στραφεί σε κοντινή δυναμικότητα, δεν θα είναι σε θέση να αντιμετωπίσει τις προκλήσεις του μέλλοντος. Μειώνει τα μειωμένα περιθώρια, τα συσκότισης και τις υπερτάσεις. Δεν γνωρίζουμε πάντα πότε συμβαίνει μία καταιγίδα ή μία υπερβολική αύξηση της ισχύος, αλλά μπορούν να αφήσουν κατεστραμμένες τηλεοράσεις, εξοπλισμό ήχου και υπολογιστές στο πέρασμά τους. Οι έξυπνες εφαρμογές δικτύου εξομαλύνουν τη ροή της ισχύος και όταν συμβαίνουν αποκλίσεις, γίνονται πιο γρήγορα και εύκολα.

Το έξυπνο δίκτυο μειώνει το κόστος ενέργειας: Το έξυπνο δίκτυο δίνει τη δυνατότητα παρακολούθησης και προσαρμογής της κατανάλωσης ενέργειας μέσω έξυπνων μετρητών και συστημάτων διαχείρισης ενέργειας οικιακής χρήσης που προσφέρουν παρακολούθηση της χρήσης 24/7. Αυτό σημαίνει οτι δίνει την δυνατότητα ελέγχου του λογαριασμό και ακόμα καλύτερα, ο καταναλωτής μπορεί να προγραμματίσει τις εργασίες που απαιτούν περισσότερη ενέργεια σε περιόδους χαμηλής ζήτησης όπου το ρεύμα προσφέρεται σε χαμηλότερο κόστος.

Διευκολύνει την αντιμετώπιση προβλημάτων σε πραγματικό χρόνο: Όταν κάτι πάει στραβά στο σημερινό ηλεκτρικό σύστημα, ένας εργαζόμενος στην επιχείρηση κοινής ωφελείας πρέπει να οδηγήσει ως το σημείο του προβλήματος για να συλλέξει δεδομένα πριν να σχεδιαστεί μια λύση. Οι βελτιώσεις του έξυπνου δικτύου μετατρέπουν τα συμβάντα του συστήματος σε ψηφιακές πληροφορίες άμεσης

ανάκτησης, έτσι ώστε η επίλυση προβλημάτων να μπορεί να ξεκινήσει αμέσως. Με τη βελτιωμένη αυτή αποτελεσματικότητα υπάρχει μειωμένο κόστος στην πλευρά της επιχείρηση κοινής ωφελείας, το οποίο αντανακλάται στους καταναλωτές ως μειωμένο κόστος κιλοβατώρας.

Μειώνει τις δαπάνες για τους παραγωγούς ενέργειας: Για να ανταποκριθεί στις αιχμές στην κατανάλωση ενέργειας, το σημερινό σύστημα βασίζεται στην κατασκευή και τη συντήρηση δαπανηρών εγκαταστάσεων εφεδρείας που παραμένουν σε αδράνεια, εκτός από τις σπάνιες κρίσιμες περιόδους ζήτησης. Το έξυπνο δίκτυο επιτρέπει την άμεση επικοινωνία με τον εξοπλισμό του τελικού χρήστη για τη μείωση της κατανάλωσης κατά τη διάρκεια αυτών των περιόδων αιχμής, μειώνοντας την ανάγκη για δαπανηρές εγκαταστάσεις αναμονής.

Κάνει την ανανεώσιμη ενέργεια εφικτή: Απαιτούνται εξελιγμένα συστήματα έξυπνων δικτύων για τη στρατηγική διαχείριση των ποικίλων και γεωγραφικά διασκορπισμένων πηγών ανανεώσιμης ενέργειας όπως αιολικά πάρκα, ηλιακές εγκαταστάσεις και υδροηλεκτρικοί σταθμοί. Το έξυπνο δίκτυο θα διασφαλίσει ότι αυτή η ενέργεια μπορεί να αποθηκευτεί με ασφάλεια και να διανεμηθεί όπου και πότε χρειάζεται.

Διατηρεί την ανταγωνιστικότητα σε παγκόσμιο επίπεδο: Σήμερα, ακόμη και οι αναπτυσσόμενες χώρες χτίζουν την ενεργειακή υποδομή τους με ταχύτερες και πιο σύγχρονες τεχνολογίες. Το ηλεκτρικό δίκτυο δίνει ένα ανταγωνιστικό πλεονέκτημα και εξασφαλίζει την μετάβαση του κόσμου προς ένα μέλλον καθαρής ενέργειας.

Σχ. 4 Smart Grid Τοπολογία (Topology)

3 Γνωστές απειλές

3.1 Το πρόβλημα της κυβερνοασφάλειας στο Smart Grid

3.1.1 Πραγματικά περιστατικά

Πραγματικά περιστατικά ασφάλειας στον κυβερνοχώρο και συναφή συμβάντα, δείχνουν οτι τα υφιστάμενα έξυπνα δίκτυα δεν είναι ασφαλή. Εκτός αυτού, τα έξυπνα δίκτυα γίνονται όλο και πιο έξυπνα χάρη στη μαζική ανάπτυξη των Τεχνολογιών Πληροφορίας και Επικοινωνίας (ΤΠΕ – Information and Communications Technologies, ICT), και ο αριθμός των φορέων θα αυξηθεί σημαντικά (π.χ. πάροχοι υπηρεσιών, έμποροι, προμηθεύτριες εταιρείες κ.λπ.). Αυτό θα εισαγάγει νέους κινδύνους και επομένως θα πρέπει να οριστούν νέες στρατηγικές για την αντιμετώπισή τους.

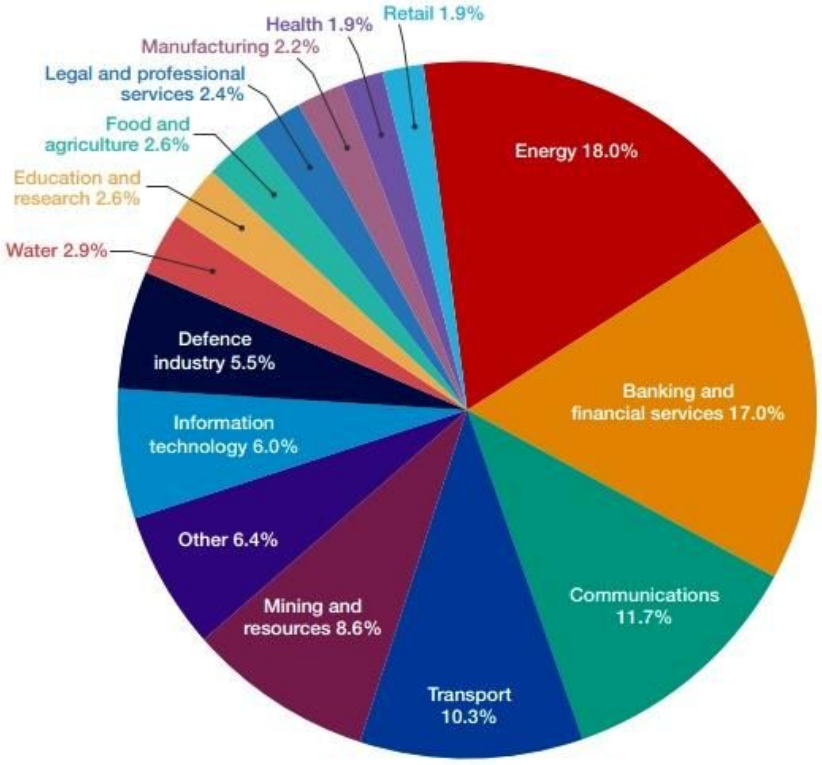
Οι επιθέσεις κατά του ηλεκτρικού δικτύου μπορούν να επηρεάσουν άμεσα τον τρόπο ζωής της κοινωνίας. Οι δημόσιοι φορείς και το διοικητικό προσωπικό των επιχειρήσεων κοινής ωφέλειας που εκμεταλλεύονται τα δίκτυα διανομής και μεταφοράς, καθώς και οι εμπορικές εταιρείες ηλεκτρικής ενέργειας και οι οργανισμοί παραγωγής, πρέπει να γνωρίζουν την κατάσταση αυτή. Χωρίς αυτούς θα ήταν ανέφικτο να δημιουργηθούν οι απαραίτητοι μηχανισμοί για τη βελτίωση της ασφάλειας των σημερινών δικτύων και να συμπεριληφθεί η ασφάλεια στον κυβερνοχώρο ως πρωταρχικός στόχος των έξυπνων δικτύων.

Ορισμένα από τα πραγματικά περιστατικά, μας δείχνουν οτι τα Συστήματα Ελέγχου Διαδικασιών (Process Control Systems, PCS), γενικά, και ειδικά οι υποδομές Συστημάτων Βιομηχανικού Ελέγχου (Industrial Control Systems, ICS) δικτύου (π.χ. συστήματα SCADA, Supervisory Control And Data Acquisition), αρχίζουν να φαίνονται ελκυστικοί στόχοι στον ηλεκτρονικό πόλεμο. Η μελέτη του Ευρωπαϊκού οργανισμού ENISA για την προστασία των ICS καλύπτει ευρέως πολλές σχετικές πτυχές που ισχύουν άμεσα για τα έξυπνα δίκτυα.

Το 2016, το Αυστραλιανό Κέντρο Ασφάλειας κυβερνοχώρου, της Αυστραλιανής Κυβέρνησης (Australian Government's Australian Cyber Security Centre, ACSC) κυκλοφόρησε την Έκθεση για τις απειλές στον κυβερνοχώρο για το 2016. Αναφέρει οτι από τον Ιούλιο του 2015 μέχρι τον Ιούνιο του 2016, η CERT Australia ανταποκρίθηκε σε 14.804 περιστατικά ασφάλειας στον κυβερνοχώρο που επηρέασαν τις επιχειρήσεις της Αυστραλίας, εκ των οποίων τα 418 αφορούσαν Συστήματα Εθνικού Ενδιαφέροντος (Systems of National Interest, SNI), και τις κρίσιμες υποδομές (Critical Infrastructure, CI).

Σύμφωνα με ένα εθελοντικό σύστημα υποβολής εκθέσεων, ο τομέας της ενέργειας προσδιορίστηκε ως ο τομέας με τον μεγαλύτερο αριθμό αναφερόμενων περιστατικών ή πληγμάτων που σχετίζονται με την υποδομή ζωτικής σημασίας.

Το παρακάτω γράφημα παρουσιάζει την Έκθεση, παρουσιάζοντας τα διάφορα περιστατικά που αφορούν τα Συστήματα Εθνικού Ενδιαφέροντος και τις Κρίσιμες Υποδομές.



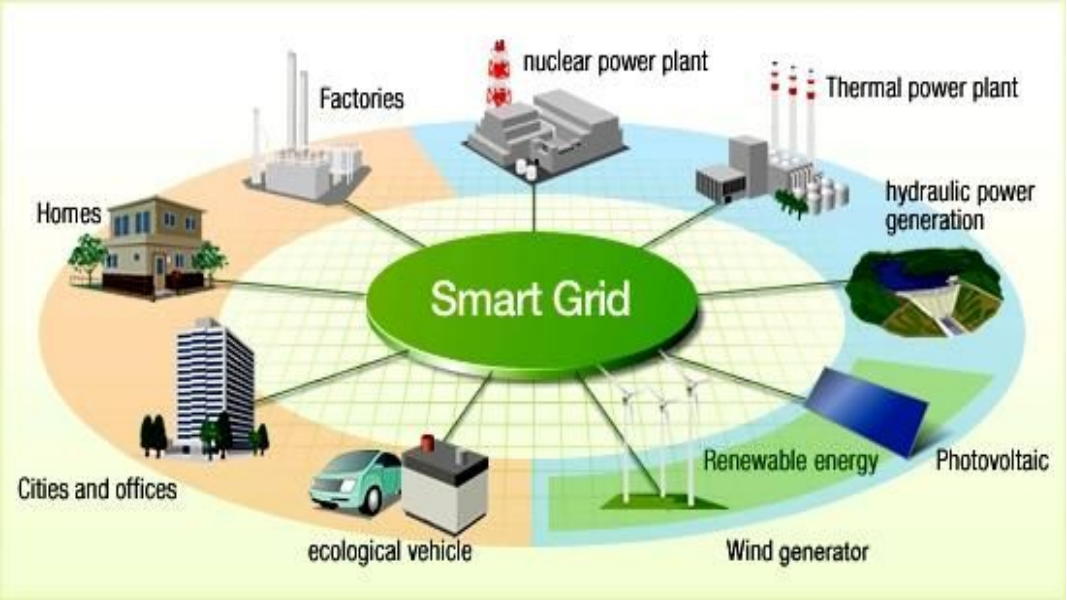
Σχ. 5 Περιστατικά που αφορούν τα Συστήματα Εθνικού Ενδιαφέροντος και τις Κρίσιμες Υποδομές

Το γνωστό τεχνολογικό περιοδικό PCWorld εξέφρασε την ανησυχία του από το 2013 οτι «οι χάκερς θα μπορούσαν να χρησιμοποιήσουν ευάλωτους σταθμούς φόρτισης για να αποτρέψουν τη φόρτιση ηλεκτρικών οχημάτων σε μια συγκεκριμένη περιοχή ή ίσως ακόμη και να χρησιμοποιήσουν τα τρωτά σημεία για να εισβάλουν σε τμήματα του ηλεκτρικού δικτύου».

Ενώ το Αμερικανικό Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology, NIST), αναγνωρίζει επίσης τον κίνδυνο. Οι "Κατευθυντήριες γραμμές για την Ασφάλεια των έξυπνων Δικτύων στον κυβερνοχώρο", αναπτύσσουν το μοντέλο λογικής αναφοράς επτά τομέων, συμπεριλαμβανομένων των "πελατών και των συσκευών των πελατών". Περιλαμβάνονται επίσης τα φορτηγά οχήματα (ηλεκτρικά οχήματα) και τα ηλεκτρικά στοιχεία των οχημάτων.

Η προσθήκη αιολικών πάρκων, ηλιακών συλλεκτών και έξυπνων μετρητών στο σύστημα διανομής ενέργειας ανοίγει πρόσθετες πύλες μέσω των οποίων οι χάκερς μπορούν να επιτεθούν στο δίκτυο.

Αυτά απεικονίζονται καλύτερα στο παρακάτω σχήμα:



Σχ. 6 Πύλες ευπάθειας Smart Grid

3.1.2 Περιστατικά ασφάλειας - Θέματα

Ως περιστατικό στον κυβερνοχώρο για τα δίκτυα ηλεκτρισμού θα μπορούσε να οριστεί κάθε αρνητικό γεγονός που μπορεί να επηρεάσει την εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα των συστημάτων ΤΠΕ που υποστηρίζουν τις διάφορες διαδικασίες των οργανισμών που συμμετέχουν στην καλή λειτουργία του συστήματος ενέργειας, συμπεριλαμβανομένων όλων των τομέων του (π.χ. αγορές, λειτουργία του δικτύου διανομής ή μεταφοράς, πελάτες κ.λπ.). Για παράδειγμα, μια επιτυχής διείσδυση στα συστήματα SCADA σε ένα υποσταθμό διανομής θα μπορούσε να χρησιμοποιηθεί για να επηρεάσει άμεσα τις διαδικασίες αυτοματισμού του υποσταθμού και με τη σειρά της οποιαδήποτε άλλη διαδικασία που θα μπορούσε να είναι κρίσιμη για τη λειτουργία του δικτύου διανομής.

Τα περιστατικά θα μπορούσαν να επηρεάσουν τα ηλεκτρικά δίκτυα με πολλούς διαφορετικούς τρόπους. Οι συνέπειες μπορούν να κυμανθούν από σχετικά καλοήθεις διακοπές σε σκόπιμες πράξεις δολιοφθοράς που έχουν σκοπό να προκαλέσουν βλάβη, απειλώντας τη ζωή των πολιτών και ακόμη και την εθνική ασφάλεια. Εξάλλου, δεν πρέπει να παραβλεφθούν οι οικονομικές ή διοικητικές κυρώσεις στις επιχειρήσεις κοινής ωφελείας. Αυτό θα μπορούσε να είναι το αποτέλεσμα μη συμμόρφωσης με Συμφωνίες Επιπέδου Υπηρεσιών (Service-Level Agreement, SLA) ή με εθνικούς νόμους και άλλους κανονισμούς για την αστική ευθύνη και την εθνική ασφάλεια.

Πρέπει να τονιστεί ότι δεν πρέπει να λαμβάνονται υπόψη μόνο οι σκόπιμες επιθέσεις. Έχει αποδειχθεί ευρέως οτι ένα μεγάλο μέρος των περιστατικών στον κυβερνοχώρο μπορεί να έχει τη ρίζα του σε τυχαία ανθρώπινα λάθη. Τα πιθανά περιστατικά, μπορούν να κατηγοριοποιηθούν ανάλογα με το επίπεδο σκοπιμότητας.

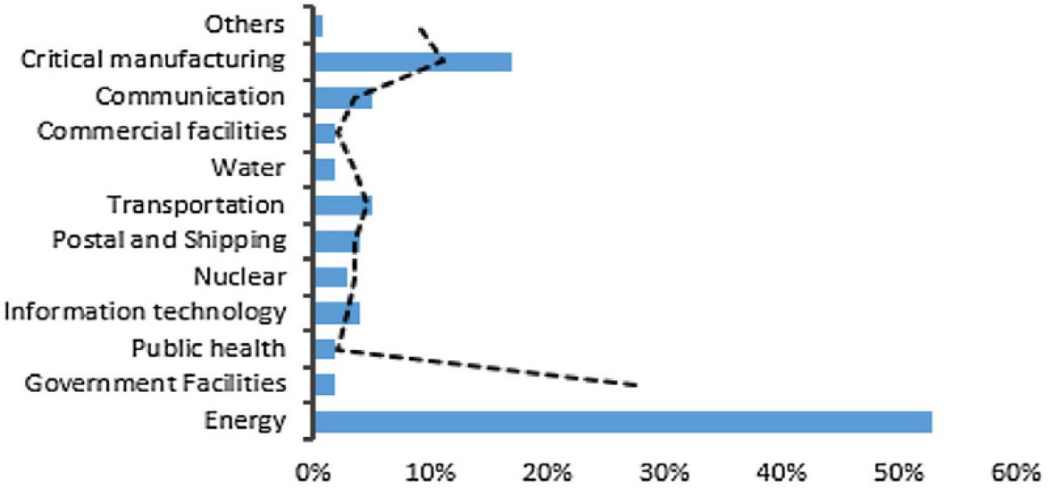


Fig. 6. Percentage cyber-attacks by sectors.

Σχ. 7 Ποσοστό επιθέσεων στον κυβερνοχώρο ανά τομέα

3.1.3 Ευπάθειες στον κυβερνοχώρο

Δίκτυα

Οι εταιρείες παροχής ενέργειας χρησιμοποιούν δίκτυα για τη σύνδεση εξοπλισμού, ελεγκτών, λογισμικού και συστημάτων εντός περιβάλλοντος ΟΤ και πληροφορικής, αντίστοιχα. Επειδή τα ευάλωτα δίκτυα οφείλονται σε λανθασμένη διαμόρφωση, κακή διαχείριση, έλλειψη περιμετρικής ετοιμότητας, μειονεκτήματα στην επικοινωνία, μεταξύ άλλων είναι ήδη γνωστά σε όλους, γι'αυτό τα δίκτυα εξακολουθούν να είναι τα πιο ελκυστικά σημεία εισόδου για τους φορείς απειλής. Σε μια έρευνα του 2014 αποτελούμενη κυρίως από ερωτηθέντες υπηρεσιών ηλεκτρισμού, η χρήση ανασφαλών δικτύων πληροφορικής περιελάμβανε το 41% των συνολικών περιστατικών ασφάλειας – η μεγαλύτερη πηγή συμβάντων από αυτές που αναφέρθηκαν. Παρά την ύπαρξη κοινών μέτρων ασφάλειας δικτύων, ένας καθορισμένος φορέας απειλής συνεχώς αναζητά πιθανά σημεία εισόδου:

Οι επιτιθέμενοι μπορούν να ψάξουν για ηλεκτρονικές τρύπες σε τείχη προστασίας, δρομολογητές και διαμεταγωγείς και να τις χρησιμοποιήσουν για να διαπεράσουν τις

άμυνες. Οι επιτιθέμενοι εκμεταλλεύονται όποιο ελάττωμα βρούν σε αυτές τις συσκευές δικτύου για να αποκτήσουν πρόσβαση στα δίκτυα στόχευσής τους, να ανακατευθύνουν την κυκλοφορία σε ένα άλλο δίκτυο (σε ένα κακόβουλο σύστημα που μεταμφιέζεται ως αξιόπιστο σύστημα) και να παρακολουθήσουν και να αλλάξουν πληροφορίες κατά τη μετάδοση. Μέσα από τέτοιες ενέργειες ο εισβολέας μπορεί να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα, να αλλάξει σημαντικές πληροφορίες ή να χρησιμοποιήσει ένα κατεστραμμένο μηχάνημα για να αποτελέσει ένα άλλο αξιόπιστο σύστημα στο δίκτυο.

Τα πρωτόκολλα επικοινωνίας που χρησιμοποιούνται σε όλα τα δίκτυα ICS προκαλούν πρόσθετη ανησυχία. Κοινά και καθιερωμένα πρωτόκολλα ICS όπως το Modbus και το DNP3 που χρησιμοποιούνται σε όλο το σύστημα ισχύος έχουν ελάχιστα ή καθόλου μέτρα ασφαλείας. Δεν διαθέτουν δυνατότητες ελέγχου ταυτότητας, μηνύματα ενδέχεται να υποκλαπούν, να παραβιάζονται, ή να αλλοιώνονται, ενδεχομένως να προκαλούν επικίνδυνο συμβάν σε περιβάλλον λειτουργίας. Καθώς τα βοηθητικά προγράμματα των ΗΠΑ κινούνται προς ένα «έξυπνο» Smart Grid, οι πωλητές τεχνολογίας εκσυγχρονισμού δικτύου έχουν τυποποιήσει όλο και περισσότερο τα προϊόντα τους για μεγαλύτερη διαλειτουργικότητα. Ένα παράδειγμα αυτού είναι το IECix 61850 με βάση το Ethernet, ένα πρωτόκολλο που χρησιμοποιείται σε μεγάλο βαθμό στην αυτοματοποίηση του υποσταθμού μετάδοσης και διανομής ηλεκτρικής ενέργειας, αλλά ενδέχεται να επεκταθεί στο μέλλον και στο κέντρο ελέγχου. Παραδοσιακά, ένα πρωτόκολλο επικοινωνίας που χρησιμοποιείται σε περιβάλλον γραφείου ή πληροφορικής, το Ethernet χρησιμοποιείται όλο και περισσότερο από επιχειρήσεις κοινής ωφέλειας σε όλη την ICS λόγω της ταχύτητας μεταφοράς δεδομένων και του χαμηλού κόστους. Ωστόσο, το Ethernet δεν σχεδιάστηκε για χρήση σε κρίσιμες λειτουργίες, όπως τα ηλεκτρικά δίκτυα. Τα δίκτυα ICS που επικοινωνούν μέσω Ethernet δεν είναι απομονωμένα, ειδικά κυκλώματα και επομένως είναι δυνητικά πιο ευάλωτα σε κυβερνο-εισβολές .

Επικοινωνία

Οι ICS του ηλεκτρικού τομέα υπάρχουν και βασίζονται σε δίκτυα για την επικοινωνία δεδομένων σχετικά με την κατάσταση λειτουργίας του εξοπλισμού, για την παρακολούθηση των συνθηκών λειτουργίας και για την επικοινωνία των αλλαγών στις λειτουργίες του τρέχοντος εξοπλισμού. Ενώ τα συστήματα ελέγχου ενός βοηθητικού προγράμματος ενδέχεται να μην είναι άμεσα προσβάσιμα εξ αποστάσεως από το Διαδίκτυο, εφαπτομενικά συνδεδεμένες συσκευές και δίκτυα ή κοινά περιφερειακά μπορεί να παρέχουν σημεία εισόδου στο δίκτυο του συστήματος ελέγχου. Για παράδειγμα, η NERC δημιούργησε ένα σύνολο προτύπων αξιοπιστίας για την ασφάλεια του κυβερνοχώρου που δημιουργήθηκαν γύρω από συνδέσεις TCP/IP ("routable"), οι οποίες παρείχαν ένα βαθμό προστασίας στην επικοινωνία με το δίκτυο του συστήματος ελέγχου παραγωγής ενός βοηθητικού προγράμματος. Ωστόσο, οι σειριακές συνδέσεις, οι οποίες συχνά χρησιμοποιούνται για επικοινωνία με υποσταθμό ή και απομακρυσμένες συσκευές όπως προγραμματιζόμενους λογικούς ελεγκτές (PLC) ή απομακρυσμένες τερματικές μονάδες (RTUs), ήταν ένα λιγότερο ασφαλές ρυθμιστικό «τυφλού σημείου» αλλά ακόμα συχνά χρησιμοποιούμενο πρωτόκολλο.

Ομοίως, οι ερευνητές κατέδειξαν πρόσφατα πώς τα τρωτά σημεία που εντοπίστηκαν στην υλοποίηση του πρωτοκόλλου επικοινωνίας DNP3 από έναν τρίτο προμηθευτή θα μπορούσαν να χρησιμοποιηθούν για την πρόσβαση σε ένα σύστημα ελέγχου ενός βοηθητικού προγράμματος: "... ένας εισβολέας θα μπορούσε να στοχεύσει σε μη κρίσιμο, ηλεκτρικό υποσταθμό και να καταστρέψει την ορατότητα σε όλους τους υποσταθμούς μιας υπηρεσίας. Οι ευπάθειες σε ορισμένες υλοποιήσεις DNP3 θα μπορούσαν να επιτρέψουν επιθέσεις εναντίον συστημάτων master ελέγχου από μια συσκευή πεδίου στέλνοντας ένα κακόβουλο πλαίσιο ή ένα μήνυμα στο σύστημα ελέγχου. ".

Συσκευές

Καθώς τα εξαρτήματα αναβαθμίζονται ή προστίθενται στο σύστημα ελέγχου μιας εταιρίας παροχής ενέργειας, η παρακολούθηση της συνδεσιμότητας του δικτύου γίνεται εξίσου σημαντική με τη διατήρηση της τεχνολογίας στην επικαιρότητα. Δεδομένου ότι ο παλαιός εξοπλισμός ενημερώνεται και ενσωματώνεται με τη νέα

τεχνολογία, το ζήτημα της ασφάλειας, για τα παλαιά και τα νέα συστήματα είναι πώς συνδέονται με τα άλλα συστήματα του βοηθητικού προγράμματος και ποια επίπεδα ασφαλείας υπάρχουν για την ανίχνευση και αποτροπή πιθανών εισβολών. Συσκευές που επικοινωνούν ή λειτουργούν ως μέρος του συστήματος ελέγχου ενός βοηθητικού προγράμματος δημιουργούν επίσης νέες απειλές για επιχειρήσεις κοινής ωφελείας και για το ηλεκτρικό δίκτυο. Πολλά εξαρτήματα αυτοματισμού, όπως τα PLCs, λειτουργούν μέσω μικροεπεξεργαστών, περιέχουν προγραμματισμό λογισμικού βάσει λειτουργιών και έχουν επίσης δυνατότητες διαχείρισης και επικοινωνίας μέσω διαδρομών δικτύου.

Απομακρυσμένη πρόσβαση και φορητές συσκευές

Προκειμένου να διαχειριστούν γεωγραφικά διεσπαρμένα στοιχεία, να αυξήσουν την ευκολία και να μειώσουν το κόστος, οι επιχειρήσεις κοινής ωφέλειας εξαρτώνται όλο και περισσότερο από εξ αποστάσεως προσβάσιμο εξοπλισμό και φορητές συσκευές. Ωστόσο, τα τρωτά σημεία που προέρχονται από μη ασφαλή πρόσβαση ή σύνδεση με κρίσιμα συστήματα μέσω απομακρυσμένων εργαλείων και συσκευών αναφέρονται συχνά ως η μεγαλύτερη αναδυόμενη πηγή ευπάθειας στον κυβερνοχώρο. Σε μια έρευνα του 2015 της ΕΥ, περισσότεροι από τους μισούς από διάφορους βιομηχανικούς τομείς, συμπεριλαμβανομένων των εταιρειών ενέργειας και άλλων υπηρεσιών κοινής ωφέλειας αξιολόγησαν την χρήση φορητών υπολογιστών ως ένα μέσο έως και υψηλό παράγοντα που συμβάλλει στην αύξηση της έκθεσης σε κινδύνους. Η ευαισθησία σε μη εξουσιοδοτημένη πρόσβαση εξαρτάται εν μέρει από τους καθιερωμένους ελέγχους και την υγιεινή στον κυβερνοχώρο. Οι ισχυροί κωδικοί πρόσβασης, ο έλεγχος ταυτότητας και η κρυπτογράφηση δεδομένων μπορεί να φαίνονται να είναι προφανή μέτρα για να χρησιμοποιηθούν όταν είναι απαραίτητη η απομακρυσμένη πρόσβαση σε δίκτυα ή συσκευές ICS, αλλά συχνά παραβλέπονται ή αγνοούνται. Σε μια αναφορά δραστηριότητας απόκρισης περιστατικού 2014, η οποία δημοσιεύτηκε από το ICS-CERT, το δίκτυο του συστήματος ελέγχου του δημόσιου βοηθητικού δικτύου περιγράφηκε ως παραβιαζόμενο ως αποτέλεσμα αδύναμων κωδικών πρόσβασης και ελέγχου ταυτότητας σε σημείο απομακρυσμένης πρόσβασης. Η ίδια αναφορά περιγράφει επίσης ένα άλλο μη προστατευμένο σύστημα ελέγχου

συνδεδεμένο στο Internet το οποίο δεν διέθετε ελέγχους ελέγχου ταυτότητας ή ένα τείχος προστασίας. Η μετάβαση σε ένα έξυπνο δίκτυο θα σημαίνει ότι οι επιχειρήσεις κοινής ωφέλειας θα προσθέσουν χιλιάδες συσκευές στις λειτουργίες τους, συμπεριλαμβανομένων νέων αισθητήρων, ελεγκτών, ρελέ, μετρητών κλπ. Οι τεχνολογίες εκσυγχρονισμού του δικτύου θα υπόκεινται ενδεχομένως σε μελλοντική ρύθμιση η περίμετρος είναι αποκλειστικά η ευθύνη της κάθε εταιρίας.

Ο εξοπλισμός που είναι προσβάσιμος από απόσταση είναι ακόμη πιο ευάλωτος στην ανιχνευσιμότητα. Εργαλεία όπως το SHODAN, επιτρέπουν στους χρήστες να αναζητούν συστήματα ελέγχου πρόσβασης, δρομολογητές, συστήματα διαχείρισης κτιρίων και διοικητικές πλατφόρμες σε όλο τον κόσμο. Τα εργαλεία αυτά αφήνουν τους χρήστες να ψάξουν εξ αποστάσεως προσπελάσιμο εξοπλισμό σε ένα εύκολα αναζητήσιμο περιβάλλον, όπου ο εξοπλισμός μπορεί να ταυτοποιηθεί μέσω της διεύθυνσης IP του και σε ορισμένες περιπτώσεις τον αφήνει εύκολα προσπελάσιμο, δημιουργώντας περαιτέρω ευπάθεια σε μια κυβερνο-επίθεση.

Υπηρεσίες τρίτων και αλυσίδες εφοδιασμού

Οι επιχειρήσεις κοινής ωφέλειας βασίζονται σε προμηθευτές, ολοκληρωτές συστημάτων και άλλους παρόχους υπηρεσιών και προϊόντων τρίτων μερών προκειμένου να λειτουργήσουν τις εγκαταστάσεις ισχύος τους. Με εκατοντάδες δευτερεύοντα και τριτεύοντα συμβαλλόμενα μέρη που ανακατεύονται στην κατασκευή και τη συντήρηση της παραγωγής, της μετάδοσης και της διανομής της ενέργειας, οι επιχειρήσεις κοινής ωφέλειας συχνά δυσκολεύονται να εξασφαλίσουν την ακεραιότητα της εφοδιαστικής αλυσίδας. Ορισμένοι προμηθευτές εξοπλισμού ICS προκαλούν ακούσια προβλήματα στον κυβερνοχώρο λόγω πολιτικών συντήρησης προμηθευτών, όπως η δημιουργία σκόπιμων ή ακούσιων «πίσω εισόδων» (backdoors) για πρόσβαση σε συσκευές ή λογισμικό ή απειλώντας να ακυρώσουν τις εγγυήσεις εξοπλισμού, εάν επαναρυθμιστούν από τις εργοστασιακές ρυθμίσεις, π.χ. αλλαγή κωδικών ασφαλείας – ή εγκατάσταση μη εγκεκριμένων πακέτων ασφαλείας.

Το λογισμικό που υποστηρίζει τον εξοπλισμό ICS που χρησιμοποιείται σε όλα τα τμήματα του δικτύου ηλεκτρικού ρεύματος σε περιβάλλοντα πληροφορικής και

τεχνολογίας πληροφοριών πρέπει επίσης να ενημερώνεται τακτικά – αν και ορισμένες φορές απαιτούνται διακοπές λειτουργίας του συστήματος (downtime).

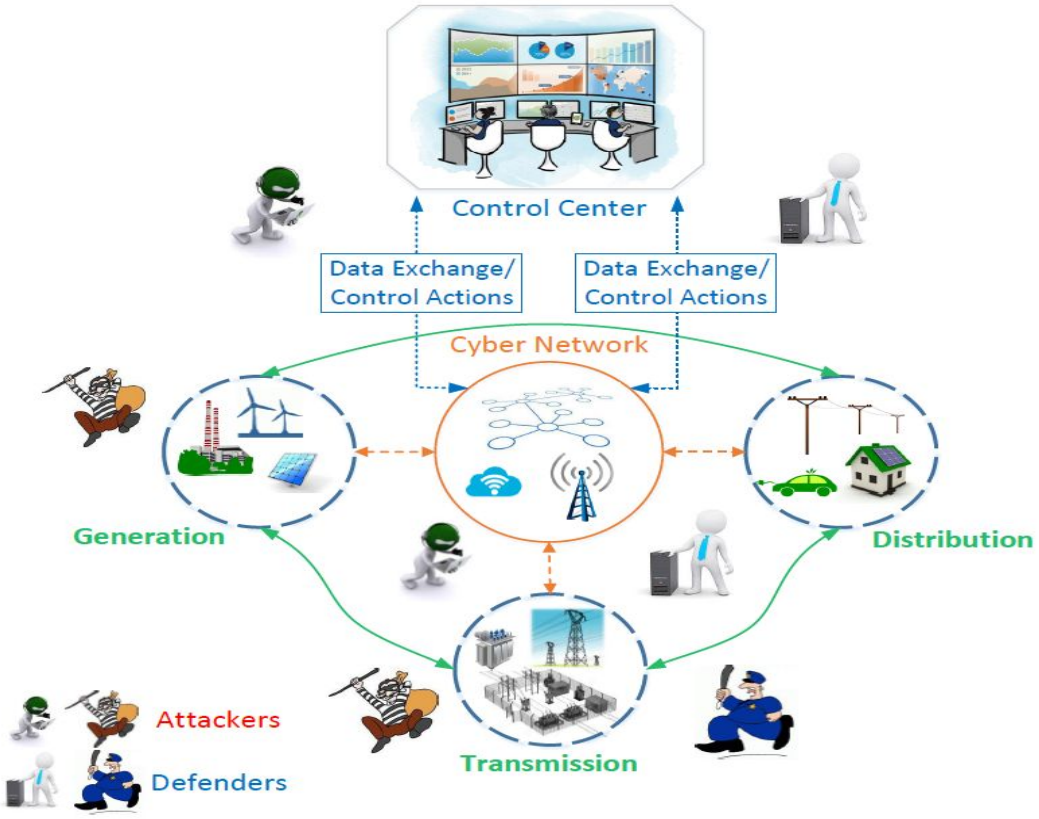


Fig. 1. Illustration of a smart grid architecture highlighting the underlying cyber layer and security threats.

Σχ. 8 Αρχιτεκτονική Smart Grid – οι απειλές του κυβερνο-επίπεδου

4 Συγκεκριμένες απειλές σε Smart Grid περιβάλλον

4.1 Παραδείγματα πραγματικών περιστατικών ασφάλειας που επηρεάζουν τα συστήματα ισχύος

Λαμβάνοντας υπόψη την παραγωγή ενέργειας, τον Μάρτιο του 2008 ο πυρηνικός σταθμός Edwin I στη Γεωργία (ΗΠΑ), αναγκάστηκε να πραγματοποιήσει έκτακτη διακοπή λειτουργίας για 48 ώρες λόγω ενημέρωσης λογισμικού. Αυτή η ενημέρωση λογισμικού εφαρμόστηκε στο σύστημα πληροφορικής που είναι επιφορτισμένο με την παρακολούθηση των χημικών δεδομένων και των δεδομένων διάγνωσης ενός από τα πρωτεύοντα συστήματα ελέγχου της εγκατάστασης.
Μετά την εφαρμογή της ενημέρωσης, ο υπολογιστής επανεκκινήθηκε και αυτό οδήγησε σε έλλειψη πληροφοριών παρακολούθησης. Τα συστήματα ασφαλείας το ερμήνευσαν εσφαλμένα και σηματοδότησαν οτι η στάθμη του νερού στα συστήματα ψύξης για τις ράβδους πυρηνικού καυσίμου είχε πέσει, πράγμα που προκάλεσε αυτόματη απενεργοποίηση. Δεν υπήρχε κίνδυνος για το κοινό, αλλά η εταιρεία ηλεκτρικής ενέργειας έχασε έσοδα εκατομμυρίων δολαρίων και έπρεπε να υποστεί τις σημαντικές δαπάνες για να θέσει το εργοστάσιο πάλι on-line.

Όσον αφορά τον τομέα της διανομής και της μετάδοσης, ένα από τα πιο σημαντικά περιστατικά θα μπορούσε να είναι η επίθεση που υπέστη το αμερικανικό ηλεκτρικό δίκτυο το 2009. Οι υπάλληλοι της αμερικανικής δημόσιας διοίκησης αναγνώρισαν οτι κυβερνοχώροι από την Κίνα και τη Ρωσία είχαν εισβάλει στο αμερικανικό δίκτυο ηλεκτρικής ενέργειας και τοποθέτησαν κρυφό λογισμικό το οποίο θα μπορούσε να χρησιμοποιηθεί για τη διακοπή τροφοδοσίας. Επιβεβαιώθηκε οτι οι επιτιθέμενοι θα μπορούσαν να χρησιμοποιήσουν αυτό το λογισμικό backdoors για να κόψουν την παροχή ηλεκτρικής ενέργειας, κατά βούληση.

Όσον αφορά την AMI, κατά τη διάσκεψη του Black Hat στις ΗΠΑ το 2009, ο Mike Davis, ένας σύμβουλος ασφάλειας IOActive, αποδείκνυε τις αδυναμίες ολόκληρης της αρχιτεκτονικής μέτρησης και ιδιαίτερα των έξυπνων μετρητών που αναπτύχθηκαν

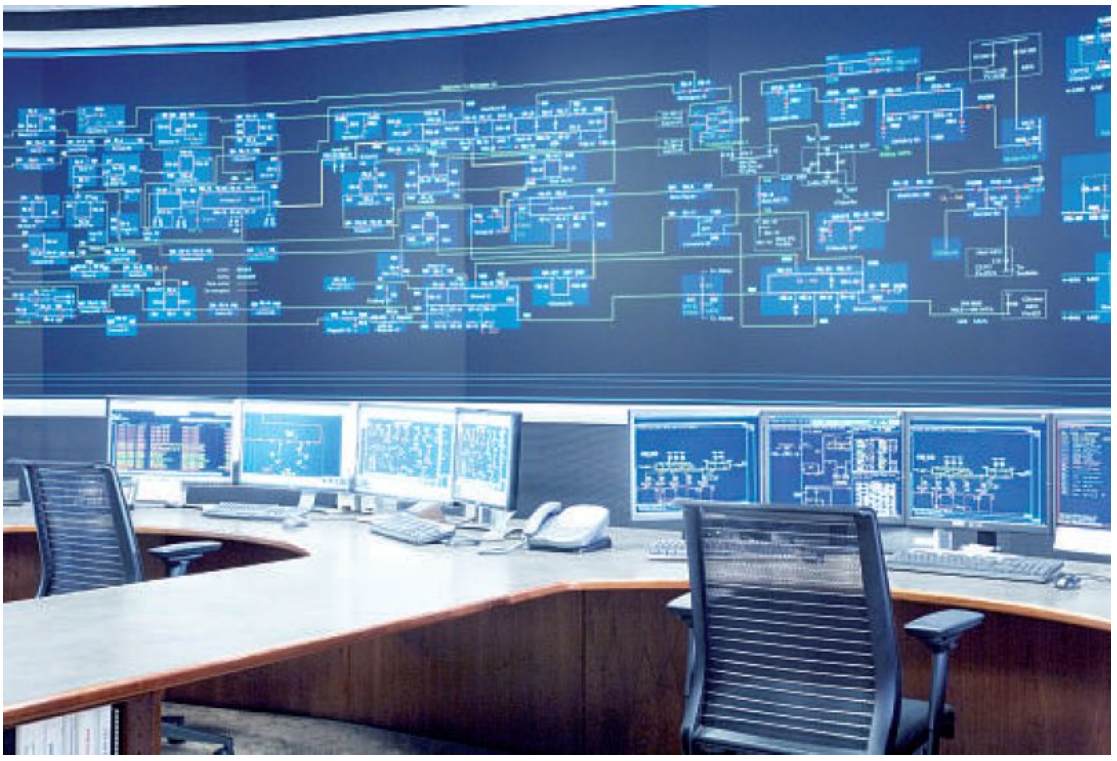
εκείνη την εποχή. Απέδειξε οτι μέσω μιας κυβερνοεπίθεσης θα μπορούσε να αποκτηθεί ο απομακρυσμένος έλεγχος περίπου 15.000 από 22.000 σπίτια μέσα σε 24 ώρες. Για να το δείξει αυτό ο Mike Davis και η ομάδα του δημιούργησαν έναν προσομοιωτή και ένα κακόβουλο λογισμικό (worm), ικανό να αναπαράγεται και να διανέμεται αυτοτελώς σε μια περιοχή όπου όλα τα σπίτια ήταν εξοπλισμένα με την ίδια μάρκα μετρητή.

Δυστυχώς, το FBI ανακάλυψε πρόσφατα οτι οι εγκαταστάσεις έξυπνων μετρητών αντιμετωπίζουν ήδη επιθέσεις στον κυβερνοχώρο. Το 2009, ένα ηλεκτρικό δίκτυο στο Πουέρτο Ρίκο τους ζήτησε να βοηθήσουν στη διερεύνηση εκτεταμένων περιστατικών κλοπών ηλεκτρικής ενέργειας, τα οποία πίστευαν ότι σχετίζονταν με την έξυπνη διασύνδεση του μετρητή.
Το FBI ανακάλυψε οτι οι πρώην υπάλληλοι του κατασκευαστή του μετρητή και οι υπάλληλοι της εταιρείας κατέγραφαν πλαστές καταμετρήσεις έναντι χρημάτων. Πιθανότατα, είχαν «πειράξει» τους μετρητές χρησιμοποιώντας μια οπτική σειριακή θύρα που τους επέτρεψε να συνδέσουν τους υπολογιστές τους τοπικά και να αλλάξουν τις ρυθμίσεις για την καταγραφή της κατανάλωσης ενέργειας. Χρειαζόταν απλώς ένα πρόγραμμα λογισμικού που θα μπορούσε να μεταφορτωθεί απευθείας από το Διαδίκτυο.

4.2 Σχετικά περιστατικά

Τον Ιούνιο του 2010 εντοπίστηκε το κακόβουλο λογισμικό Stuxnet. Αυτό το κομμάτι κακόβουλου λογισμικού έχει τις ιδιότητες ενός worm, δεδομένου ότι εκμεταλλεύεται διάφορες ευπάθειες, προκειμένου να μολύνει άλλα συστήματα και συγχρόνως θεωρείται ένα rootkit ICS, δεδομένου οτι τροποποιεί ακούσια τον τρόπο με τον οποίο συμπεριφέρονται οι Προγραμματιζόμενοι Λογικοί Ελεγκτές (Programmable Logic Controllers, PLCs). Αυτό το κακόβουλο λογισμικό θεωρήθηκε ως κυβερνοόπλο για δολιοφθορά. Επικεντρώνεται στο ειδικό λογισμικό και υλικό της Siemens, τροποποιώντας τις λογικές των μικροελεγκτών Siemens S7 PLC, αποκρύπτοντας την ενέργεια αυτή από την εφαρμογή ή τους χειριστές λογισμικού εποπτείας.

Το Stuxnet είναι ένα πολύ προηγμένο κομμάτι του λογισμικού. Εκμεταλλεύεται αρκετές ευπάθειες μηδενικής-ημέρας, χρησιμοποιεί έγκυρα (κλεμμένα), ψηφιακά πιστοποιητικά και ελέγχει την εφαρμογή Siemens WinCC SCADA. Ο δημόσιος Τύπος ανέφερε οτι οι ειδικοί ασφαλείας θεωρούν οτι μόνο κυβερνητικές υπηρεσίες μπορεί να έχουν την ικανότητα και τους πόρους να παράγουν και να απελευθερώνουν ένα τόσο εξελιγμένο εργαλείο επίθεσης. Δεν υπάρχει επίσημη επιβεβαίωση, αλλά οι ειδικοί ασφαλείας πιστεύουν οτι ο στόχος του Stuxnet ήταν η ιρανική πυρηνική εγκατάσταση του Natanz, η οποία θεωρείται από πολλούς ως βασικό μέρος του προγράμματος πυρηνικών όπλων του Ιράν. Επιπλέον, επιβεβαιώθηκε οτι από την ύπαρξη του Stuxnet και μετά, υπήρξαν πολλά προβλήματα χωρίς καμία λογική εξήγηση.



Σχ. 9 IP-based SCADA Application

Το Night Dragon ήταν το όνομα που δόθηκε σε μια σειρά στοχευμένων επιθέσεων. Ο κύριος στόχος τους ήταν να υπονομεύσουν το βιομηχανικό σύστημα ελέγχου πολλών ενεργειακών εταιρειών στις Ηνωμένες Πολιτείες, συμπεριλαμβανομένων των εταιρειών πετρελαίου, φυσικού αερίου και πετροχημικών. Σύμφωνα με την έκθεση

της εταιρείας McAfee, οι επιθέσεις πιστεύεται οτι έχουν την προέλευσή τους στην Κίνα. Αυτές οι επιθέσεις βασίστηκαν σε ένα συνδυασμό αρκετών τεχνικών, εργαλείων και τρωτών σημείων (π.χ. spear-phishing, κοινωνική μηχανική - social engineering, σφάλματα των Windows και Εργαλεία Απομακρυσμένης Διαχείρισης - Remote Administration Tools – RATs). Αν και οι επιθέσεις δεν ήταν πολύ εξελιγμένες και δεν εκμεταλλεύονταν καμία ευπάθεια μηδενικής-ημέρας, οι πληροφορίες που έλαβαν οι επιτιθέμενοι ήταν πολύτιμες για τους ανταγωνιστές. Αυτές οι πληροφορίες περιλάμβαναν οικονομικά έγγραφα, που αφορούσαν την εξερεύνηση πεδίου πετρελαίου και φυσικού αερίου και τις μεγάλες διαπραγματεύσεις, καθώς και επιχειρησιακές λεπτομέρειες των συστημάτων εποπτείας παραγωγής και συλλογής δεδομένων.

Το Duqu είναι ένα worm υπολογιστή που ανακαλύφθηκε τον Σεπτέμβριο του 2011 και πιστεύεται οτι έχει δημιουργηθεί από τους ίδιους συγγραφείς του Stuxnet ή τουλάχιστον οτι οι συντάκτες του είχαν πρόσβαση στον πηγαίο κώδικα του Stuxnet. Ωστόσο, ο σκοπός του ήταν τελείως διαφορετικός από αυτόν του Stuxnet.
Ο κύριος στόχος του Duqu ήταν να συλλέξει πληροφορίες, όπως πληκτρολογήσεις και πληροφορίες συστήματος για να προετοιμάσει μελλοντικές επιθέσεις εναντίον βιομηχανικών συστημάτων ελέγχου. Τα εκτελέσιμα αρχεία του Duqu έχουν βρεθεί σε περιορισμένο αριθμό οργανισμών, συμπεριλαμβανομένων εκείνων που εμπλέκονται στην κατασκευή βιομηχανικών συστημάτων ελέγχου. Οι ειδικοί εξακολουθούν να αναλύουν τον κώδικα, αλλά θεωρούν οτι το Duqu μπορεί να χρησιμοποιηθεί για να επιτρέψει μια μελλοντική επίθεση που μοιάζει με του Stuxnet ή μπορεί να έχει ήδη χρησιμοποιηθεί ως βάση για την επίθεση Stuxnet.

5 Smart Grid αγαθά που τίθενται σε κίνδυνο σε κυβερνοαπειλές

5.1 Τα Smart Grids γίνονται πιο πράσινα αλλά και ευκολότερο να χακαριστούν

Οι υπεύθυνοι χάραξης πολιτικής πρέπει να προβλέπουν τις εξελιγμένες ομάδες που αναπτύσσουν δυνατότητες hacking παγκόσμιας κλάσης. Οι υπεύθυνοι χάραξης πολιτικής για την ενέργεια επιταχύνουν πράσινες πρωτοβουλίες που θα καταστήσουν τα ηλεκτρικά δίκτυα πιο ευάλωτα στις επιθέσεις στον κυβερνοχώρο.

Το πρόβλημα είναι οτι το "πιο έξυπνο" και "πιο πράσινο" απαιτεί το δίκτυο να είναι πληρέστερα συνδεδεμένο με το Διαδίκτυο. Τα "έξυπνα" δίκτυα εξαρτώνται από την εξυπνάδα και του Διαδικτύου. Και η ηλιακή και η αιολική ενέργεια απαιτούν μηχανισμούς που στοχεύουν στο Internet για να ανταποκριθούν στην πρόκληση της χρήσης επεισοδιακών προμηθειών για να τροφοδοτήσουν πάντα τη ζήτηση ενέργειας της κοινωνίας.

Έτσι, οι πολιτικές από την Καλιφόρνια στη Νέα Υόρκη, καθώς και το Σχέδιο Καθαρής Ισχύος του EPA, προβλέπουν την προσθήκη εκατομμυρίων συσκευών συνδεδεμένων στο Διαδίκτυο σε ηλεκτρικά δίκτυα, νοσοκομεία και πόλεις. Για τους χάκερ, αυτό ονομάζεται εκτεταμένη επέκταση της επιφάνειας επίθεσης. Σε αυτό το «πιο έξυπνο» μέλλον, οι κακοί ηγέτες στον κυβερνοχώρο έχουν επιτύχει να σπάσουν τα ιδιωτικά και τα οικονομικά δεδομένα, μπορούν να στραφούν στην καταστροφή και στον έλεγχο των κρίσιμων υλικών υποδομών.

Οι εμπειρογνώμονες έχουν επιδείξει μεθόδους διείσδυσης σε ολόκληρη την γκάμα των συσκευών που σχετίζονται με έξυπνη και πράσινη ενέργεια, από έξυπνα φώτα και μετρητές ισχύος έως τα ηλεκτρονικά ισχύος σε ηλιακούς συλλέκτες. Η ασφάλεια στον κυβερνοχώρο απλώς δεν ήταν η προτεραιότητα στους τομείς της πράσινης πολιτικής - παρόλο που τα τεχνικά και μηχανικά μηνύματα και οι εκδόσεις γεμίζουν με παραδείγματα ευπάθειας στον κυβερνοχώρο ή με αδύναμα ή ανύπαρκτα χαρακτηριστικά ασφάλειας στον κυβερνοχώρο. Με την πλήρη ανάπτυξη ευφυέστερων υποδομών, τι ακριβώς θα αντιμετωπίσουμε;

Ας φανταστούμε, για παράδειγμα, ότι είναι μια καυτή καλοκαιρινή μέρα στο Λος Άντζελες κάποια στιγμή στο εγγύς μέλλον και η ισχύς σε μια πτέρυγα ενός νοσοκομείου πέφτει, παίρνοντας μαζί της τον κλιματισμό και όλο τον κρίσιμο νοσοκομειακό εξοπλισμό - από τα MRI μέχρι την υποστήριξη ζωής. Ο διευθύνων σύμβουλος παίρνει ένα κείμενο από το διευθυντή των εγκαταστάσεών του λίγα λεπτά πριν μια άλλη πτέρυγα σε ένα διαφορετικό, μεγαλύτερο νοσοκομείο στο δίκτυο περάσει στο μαύρο, καθώς η γεννήτρια εφεδρείας δεν ξεκινά. Αυτό ακολουθείται από ένα μήνυμα ηλεκτρονικού ταχυδρομείου από τον χάκερ που αναφέρει ότι η ισχύς σε όλα τα νοσοκομεία θα διακοπεί μέσα σε μια ώρα. Τα λύτρα είναι, για παράδειγμα, 10 εκατομμύρια δολάρια σε Bitcoins.

Τώρα, ας φανταστούμε ένα διαφορετικό σενάριο, αυτή τη φορά ένα καυτό βράδυ του Μανχάταν, όταν πολλά οικοδομικά τετράγωνα ξαφνικά σκοτεινιάζουν. Δεν είναι λύτρα αυτή τη φορά, αλλά απειλή: έρχονται περισσότερα. Ο δήμαρχος παίρνει μια εικόνα στο smartphone του, που καλύπτει το περιοδικό Time της 25ης Ιουλίου 1977 με τον τίτλο «Νύχτα της Τρομοκρατίας». Η έκρηξη ταραχών της Νέας Υόρκης του 1977 διήρκεσε 25 ώρες, περιλάμβανε χιλιάδες κλεμμένα καταστήματα και πυρκαγιές, 4.000 συλλήψεις και 300 εκατομμύρια δολάρια αποζημίωση. Αυτή τη φορά, ο δήμαρχος ανησυχεί επίσης ότι ο επιτιθέμενος θα μπορούσε να συντονίσει μια σειρά φυσικών επιθέσεων τύπου Orlando για να δημιουργήσει χάος.

Στην πρώτη περίπτωση, τα λύτρα πληρώνονται και η δύναμη επανέρχεται. Στο δεύτερο σενάριο, δεν συμβαίνουν φυσικές επιθέσεις, αλλά χρειάζονται δύο μέρες και ηρωικές προσπάθειες από τα πληρώματα του ConEd για την αποκατάσταση και επαναφορά της ισχύος, με την επιστροφή σε παλαιότερα χειροκίνητα συστήματα που παρακάμπτουν το «έξυπνο» υλικό. Αλλά οι τρομοκράτες πέτυχαν τον στόχο τους. Και στις δύο περιπτώσεις οι ομάδες εγκληματολογίας από το Τμήμα Εσωτερικής Ασφάλειας, το FBI και η Cyber -Command της DOD καταφθάνουν.

Μαθαίνουν ότι μια εξελιγμένη απάτη ηλεκτρονικού «ψαρέματος» εισήγαγε έναν ιό τύπου worm σε συνδυασμό με το κακόβουλο λογισμικό που φορτώθηκε νωρίτερα σε ένα hack-backdoor σε μια συσκευή παρακολούθησης ισχύος, επιτρέποντας την απομακρυσμένη κατάληψη των τοπικών συστημάτων ελέγχου δικτύου. Η NSA ανιχνεύει τις ιστότοπους του κυβερνοχώρου σε ανώνυμους διακομιστές στη Γεωργία (η χώρα και όχι η πολιτεία) ή το Ιράν ή η Κίνα και ... αδιέξοδο.

Ακούγεται υπερβολικό; Εξετάστε πού είμαστε σήμερα: Οι επιθέσεις ransomware είναι ήδη μια μάστιγα. Η Αμερικανική Νοσοκομειακή Ένωση ανέφερε ότι αρκετές εταιρείες υγείας και νοσοκομεία χτυπήθηκαν νωρίτερα αυτό το έτος με ransomware (τα περισσότερα πληρωμένα). Μέχρι στιγμής, όμως, οι hackers μπορούν να κλείσουν μόνο την πρόσβαση μιας στοχευόμενης οργάνωσης στο δικό τους σύστημα ηλεκτρονικών υπολογιστών ή στον ιστότοπο ηλεκτρονικού εμπορίου. Όσον αφορά το μέλλον, θεωρήστε ότι για τους χάκερ, τα σημερινά αυτοκίνητα που συνδέονται με το Διαδίκτυο φαίνονται ακριβώς όπως τα συνδεδεμένα πλέγματα του αύριο. Οι ερευνητές έχουν χακάρει ήδη το Ford Escape, το Toyota Prius, το Nissan Leaf, ακόμη και ένα Jeep Grand Cherokee.

Το προπερασμένο έτος, το «cyber-jacking» ενός τζιπ πήρε τον πλήρη έλεγχο από δέκα μίλια μακριά εκμεταλλευόμενο τις ευπάθειες του συστήματος πληροφοριών ψυχαγωγίας που συνδέονται με το Διαδίκτυο με το backdoor στους μικροϋπολογιστές του αυτοκινήτου που λειτουργούν το τιμόνι και τα φρένα. Μετά από αυτή την επίδειξη, η Chrysler ανακάλεσε πάνω από ένα εκατομμύριο αυτοκίνητα για να διορθώσει αυτές τις συγκεκριμένες ευπάθειες. Ακόμη, το FBI και το NHTSA εξέδωσαν μια γενική ειδοποίηση σχετικά με τα ευάλωτα σημεία στον κυβερνοχώρο των οχημάτων. Όλοι και από τις δύο πλευρές γνωρίζουν ότι είναι μόνο η κορυφή του «ψηφιακού παγόβουνου».

5.2 Μέγεθος του κινδύνου

Στην πραγματικότητα, έχουν ήδη υπάρξει περιπτώσεις hacking δικτύων ενέργειας. Το 2008, ένας Πολωνός έφηβος μπήκε στους ελέγχους ελαφρών σιδηροδρόμων της πόλης και προκάλεσε εκτροχιασμό. Το 2010, ο κόσμος έμαθε για μια παράνομη απόπειρα – κατά τα φαινόμενα αμερικανο-ισραηλινή – που εισήγαγε τον ιό υπολογιστή Stuxnet για να βλάψει την ηλεκτρική υποδομή των πυρηνικών εγκαταστάσεων του Ιράν. Το 2015, οι χάκερ παραβίασαν το λειτουργικό σύστημα ενός γερμανικού εργοστασίου παραγωγής χάλυβα, προκαλώντας τεράστια φυσική καταστροφή. Και τον περασμένο Δεκέμβριο, οι χάκερ έσβησαν το ηλεκτρικό δίκτυο της Ουκρανίας.

Μέχρι στιγμής δεν έχουν υπάρξει τέτοιες διεισδύσεις στα ηλεκτρικά δίκτυα των Η.Π.Α. τις οποίες να γνωρίζουμε, βέβαια. Και οι εμπειρογνώμονες που έδωσαν μαρτυρίες ενώπιον του Κογκρέσου σχετικά με την επίθεση της Ουκρανίας ισχυρίστηκαν αξιόπιστα ότι τα μεγάλα δίκτυα της Αμερικής προστατεύονται καλύτερα - τουλάχιστον προς το παρόν. Αλλά αυτό δεν είναι το θέμα.

Η έκθεση είναι ένα πρόβλημα - όχι τόσο με τα δίκτυα μακρινών αποστάσεων αλλά με τα τοπικά δίκτυα σε πόλεις και κοινότητες, εκεί όπου σχεδιάζεται και προγραμματίζεται όλη η «εξυπνάδα» του Διαδικτύου. Καθώς η πράσινη συνδεσιμότητα επιταχύνεται σε αυτά τα δίκτυα, η επιφάνεια προσβολής επεκτείνεται. Τα σημερινά δίκτυα, σύμφωνα με τα πρότυπα της Silicon Valley, είναι χαζά - έστω και σκόπιμα. Αλλά γνωρίζουμε ήδη τι επιτρέπει να γίνει εφικτό η προσθήκη περισσότερης συνδεσιμότητας στο Διαδίκτυο.

Το Υπουργείο Εσωτερικής Ασφάλειας υποστηρίζει ότι οι τομείς παραγωγής και ενέργειας της Αμερικής είναι οι δύο μεγαλύτεροι στόχοι για επιθέσεις σε κυβερνο-φυσικά συστήματα. Και η Cisco αναφέρει ότι το 70% των επαγγελματιών στον τομέα της πληροφορικής ασφάλειας των δικτύων ενέργειας ανακάλυψαν οτι υπήρξαν διεισδύσεις, σε σύγκριση με το 55% σε άλλους κλάδους και βιομηχανίες.

Εδώ είναι και το σημείο καμπής. Οι πράκτορες πράσινης ενέργειας πιέζουν για πολιτικές που θα δημιουργήσουν περισσότερη έκθεση στο Internet - ακριβώς όταν οι μεμονωμένοι κακοί και τα εχθρικά κράτη κλιμακώνουν γρήγορα τις δεξιότητές τους.

Οι υπεύθυνοι χάραξης πολιτικής αποκαλύπτουν τη σημασία της ασφάλειας και της αξιοπιστίας. Αλλά οι ενέργειες ηχούν πιο δυνατά από τα λόγια. Κατά την τελευταία δεκαετία οι ομοσπονδιακές και κρατικές πράσινες και έξυπνες τεχνολογικές χρηματοδοτήσεις ανήλθαν σε 175 δισεκατομμύρια δολάρια. Χίλιες φορές περισσότερα χρήματα από ό,τι η DOE αναφέρει οτι δαπανά για την έρευνα στον τομέα της κυβερνο-φυσικής ασφάλειας.

Μήπως αυτό σημαίνει ότι θα πρέπει να αποφύγουμε να μεταφέρουμε ελέγχους της κατηγορίας αυτών που έχουμε στο Internet στα δίκτυα ενέργειας και στις υποδομές; Χλωμό! Οι μηχανικοί και οι επιχειρηματίες -και όχι οι γραφειοκράτες- θα αναπτύξουν τελικά έξυπνα και ασφαλή συστήματα. Αλλά η ασφάλεια πρέπει να είναι η προτεραιότητα. Σε κάθε υποδομή της ιστορίας – από την εξουσία και το νερό μέχρι τα νοσοκομεία, τα αυτοκίνητα και τα αεροσκάφη – η πολιτική έχει, και σωστά, θέσει

πρώτη την ασφάλεια εμψύχων και αψύχων. Με την κοινωνία να εξαρτάται από τον ηλεκτρισμό περισσότερο από ποτέ, δεν είναι ο κατάλληλος καιρός να αντιστρέψουμε τις προτεραιότητες.

Η γνωστή έκθεση Cyber-Jihad καταλήγει στο ακόλουθο συμπέρασμα: «Ευτυχώς, ακόμη και επιτυχείς κυβερνο-επιθέσεις στον τομέα της ενέργειας των Ηνωμένων Πολιτειών δεν θα είχαν τον ίδιο αντίκτυπο με εκείνες κατά της Ουκρανίας το 2015, επειδή το δίκτυο είναι πολύ μεγαλύτερο και λεπτότατα κατακερματισμένο». Αυτό είναι αληθές, για τώρα. Αλλά σε έναν κόσμο όπου οι τρομοκρατικές επιθέσεις είναι πολύ συνηθισμένες, προωθώντας πρόωρα την «πράσινη» ή την «έξυπνη» τεχνολογία στο δίκτυο ενέργειας - αφήνοντας τον κυβερνο-ασφάλεια στον μετακαυστήρα - θα θέσει τις συνθήκες για μια τέλεια καταιγίδα στον κυβερνοχώρο.

6 Ποιοι υλοποιούν τις επιθέσεις αυτές

Το Διαδίκτυο δημιούργησε έναν κόσμο όπου μπορούμε να είμαστε σε συνεχή επικοινωνία μέσω των υπολογιστών μας, αλλά προκάλεσε επίσης προβλήματα στον τομέα της ιδιωτικής ζωής και της οικονομικής ασφάλειας.

Το Wall Street Journal ανέφερε οτι κατάσκοποι από την Κίνα, τη Ρωσία και άλλες χώρες είχαν διεισδύσει στο αμερικανικό ηλεκτρικό δίκτυο, αφήνοντας πίσω τους λογισμικό που θα μπορούσε να χρησιμοποιηθεί για τη διακοπή του συστήματος. Οι Κινέζοι προσπάθησαν να χαρτογραφήσουν την υποδομή του ηλεκτρικού δικτύου. Το ίδιο και οι Ρώσοι. Το 2002, το 70% των εταιρειών ηλεκτρικής ενέργειας αντιμετώπισαν κάποιο είδος σοβαρής επιθέσεις στον κυβερνοχώρο, στα συστήματα πληροφορικής ή διαχείρισης ενέργειας. ("A Systems View of the Modern Grid", έκθεση που δημοσιεύθηκε το 2007 από το Εθνικό Εργαστήριο Ενεργειακής Τεχνολογίας για το Υπουργείο Ενέργειας των Η.Π.Α.).

Οι εμπειρογνώμονες κακόβουλου λογισμικού έχουν τρέξει προσομοιώσεις που δείχνουν ότι μια επίθεση σε έναν έξυπνο μετρητή μπορεί να εξαπλωθεί σε 15.000 άλλους έξυπνους μετρητές μέσα σε μία ημέρα, με την προϋπόθεση οτι όλοι οι μετρητές είναι ίδιοι. Το κακόβουλο λογισμικό μπορεί να γραφτεί για να απενεργοποιήσει εξ αποστάσεως τους έξυπνους μετρητές.

Η μεγαλύτερη ανησυχία είναι οτι οι πληροφορίες που συλλέγονται θα μοιραστούν με άλλες εταιρείες και οτι κυβερνήσεις θα μπορούν να παρακολουθούν τις πληροφορίες και να περιορίζουν την χρήση βάσει άγνωστων κριτηρίων επιλογής.

6.1 ICS Cyber Kill Chain

Χρησιμοποιούμενες σε μεμονωμένες επιθέσεις ή σε ευρύτερες εκστρατείες και σε συνδυασμό με έναν ή περισσότερους φορείς επίθεσης, οι μέθοδοι επίθεσης που εφαρμόζονται σε εισβολές στον κυβερνοχώρο προσφέρουν την διείσδυση και την μεταφερτότητα των επιτιθέμενων σε όλη την επιχειρηματική δραστηριότητα μιας εταιρείας-στόχου ή και σε περιβάλλοντα λειτουργίας. Ορισμένες κοινές μέθοδοι

περιλαμβάνουν το phishing, την εισαγωγή μολυσμένων αφαιρούμενων μέσων (όπως USB sticks), την εκμετάλλευση ανθρώπινου σφάλματος, την εισαγωγή κακόβουλου λογισμικού μέσω οδών επικοινωνίας του διαδικτύου και τη χρήση επιθέσεων με «τρύπες ποτίσματος» (μια επίθεση «τρύπας ποτίσματος» είναι μια τεχνική στην οποία ένας εισβολέας μολύνει έναν ιστότοπο με κακόβουλο λογισμικό με την πρόθεση να έχει πρόσβαση σε αυτό μια ομάδα-στόχος χρηστών που συχνάζουν στον ιστότοπο και τουλάχιστον κάποιοι χρήστες θα κατεβάσουν εν αγνοία τους το κακόβουλο λογισμικό).

Ένας επιτιθέμενος που επιδιώκει να δημιουργήσει ένα γεγονός με υψηλού επιπέδου αποτέλεσμα και σημαντικές συνέπειες στον κυβερνοχώρο, πρέπει να αναλάβει τον προγραμματισμό και την έρευνα για την αποτελεσματική επίθεση σε έναν στόχο, η πολυπλοκότητα του οποίου εξαρτάται από την κρισιμότητα του στόχου και, συνεπώς, από την προστασία του κυβερνοχώρου. Τα βήματα που πρέπει να αναλάβει ένας εισβολέας για να υπονομεύσει το ICS μπορούν να περιγραφούν από την ICS Cyber-Kill Chain, τα βήματα της οποίας παρατίθενται παρακάτω. Η ICS Cyber-Kill Chain υπάρχει ως επίθεση δύο σταδίων με πολλαπλά βήματα σε κάθε στάδιο. Το πρώτο στάδιο βασίζεται στο μοντέλο κυβερνο-αλυσίδας φονιάς που αναπτύχθηκε από την Lockheed Martin και το δεύτερο στάδιο επικεντρώνεται στην επίτευξη ενός αποτελέσματος ICS. Κάθε βήμα εκπονείται χρησιμοποιώντας το παράδειγμα ενός επιτιθέμενου που σχεδιάζει να διακόψει τις εγκαταστάσεις παραγωγής ενός ή περισσότερων μεγάλων ενεργειακών παρόχων.

6.1.1 Στάδιο 1

1) Σχεδιασμός: Ο εισβολέας διεξάγει αναγνωρίσεις για να κατανοήσει όσο το δυνατόν περισσότερο έναν στόχο. Αυτό μπορεί να περιλαμβάνει τη συλλογή πληροφοριών σχετικά με το σύστημα ICS, την εταιρεία κοινής ωφέλειας, το προσωπικό του φορέα εκμετάλλευσης κ.λπ. Μερικές φορές μπορεί να βρεθεί εύκολα σε απευθείας σύνδεση ένας μεγάλος αριθμός πληροφοριών, που συχνά περιλαμβάνουν τεχνικές λεπτομέρειες και ακόμη και σχηματικά διαγράμματα. Τον Ιανουάριο του 2016, οι ερευνητές δημοσίευσαν μια λίστα με τους κωδικούς πρόσβασης προεπιλογής του κατασκευαστή για περισσότερα

από 100 προϊόντα ICS, πολλά φτιαγμένα από τα «μεγάλα ονόματα» εταιριών πώλησης που βρέθηκαν στο μεγαλύτερο μέρος της υπηρεσίας ICS και ορισμένες φορές παρέμειναν αμετάβλητοι από τους χειριστές. Όπως αναφέρθηκε προηγουμένως, εργαλεία όπως το SHODAN μπορούν επίσης να επιτρέψουν σε έναν εισβολέα να βρει τη φυσική θέση του εξοπλισμού ICS που είναι άμεσα προσβάσιμο από το Διαδίκτυο και ακόμη και να έχει πρόσβαση σε εφαρμογές που βασίζονται στον ιστό και που σχετίζονται με τον έλεγχό του.

2) Προετοιμασία: Έχοντας προσδιορίσει ένα κατάλληλο σημείο εισόδου, όπως ένα δίκτυο πληροφορικής μιας εταιρίας παραγωγής ή διανομής ενέργειας, που συνδέεται με μια αξιόπιστη σύνδεση σε ένα δίκτυο OT για σκοπούς επιδόσεων μονάδας και ανάλυσης, ένας εισβολέας που εκτελεί χαρτογράφηση δικτύου και ανακάλυψη θα αποφασίσει ποιο εργαλείο είναι πιο κατάλληλο για την επίτευξη του στόχου. Η επίτευξη ενός στόχου σε ένα περιβάλλον-στόχος είναι ένα σημαντικό πρώτο βήμα και πρόσφατα, το ανθρώπινο λάθος αποδείχθηκε ένας ιδιαίτερα αποτελεσματικός τρόπος για κυβερνο-εισβολές. Σύμφωνα με την ICS-CERT, το spear-phishing αντιπροσώπευε τον πιο κοινό γνωστό φορέα πρόσβασης για το 2014 και το 2015 (δεύτερο σε άγνωστους φορείς πρόσβασης) (το spear-phishing είναι μια τεχνική με την οποία ένας εισβολέας χρησιμοποιεί ηλεκτρονικό ταχυδρομείο για να προσπαθήσει να δελεάσει ένα θύμα να ανοίξει αρχεία ή συνδέσμους συνημμένων που θα προκαλέσουν στο θύμα τη λήψη κακόβουλου λογισμικού ή θα παράσχει στον εισβολέα μη εξουσιοδοτημένη πρόσβαση σε υπολογιστή, δίκτυο ή εφαρμογή. Το θύμα μπορεί να επιλεγεί προσεκτικά από τον εισβολέα χρησιμοποιώντας τεχνικές κοινωνικής μηχανικής βασισμένες στην πρόσβαση του θύματος σε συγκεκριμένα πράγματα).

3) Cyber-Intrusion: Ένας εισβολέας επιχειρεί να εκμεταλλευτεί μια επιλεγμένη οδό επίθεσης. Μέθοδοι όπως οι επιθέσεις ηλεκτρονικού ψαρέματος (phishing) ή «watering holes» είναι συχνά επιτυχείς. Η κατάχρηση του ανθρώπινου σφάλματος για να αποκτηθεί πρόσβαση σε δίκτυα είναι γρήγορη και μπορεί να προσφέρει πολλές ευκαιρίες, ιδιαίτερα εάν το προσωπικό κοινής ωφέλειας δεν εκπαιδεύεται για να εντοπίσει κακόβουλη δραστηριότητα. Σύμφωνα με έρευνα της Unisys για τις επιχειρήσεις κρίσιμης σημασίας υποδομής το 2014, η παροχή εκπαίδευσης στον κυβερνοχώρο για όλους τους εργαζόμενους ήταν η χαμηλότερη προτεραιότητα μεταξύ των στόχων για την ασφάλεια

στον κυβερνοχώρο, ενώ μόνο το 6% των επιχειρήσεων έδειξαν να έχουν την εκπαίδευση των εργαζόμενων σαν μια από τις κορυφαίες τρεις προτεραιότητές τους.

4) Διαχείριση και Ενεργοποίηση: Μετά την επιτυχή επέμβαση, ο εισβολέας μπορεί να εξερευνήσει ένα δίκτυο ή ένα σύστημα για συνδέσεις για περαιτέρω εκμετάλλευση. Οι φορείς απειλών συχνά δημιουργούν πολλαπλές πρόσθετες οδούς εισόδου για να εξασφαλίσουν την πρόσβαση σε περίπτωση ανίχνευσης ή κατάργησης μιας από αυτές.

5) Βιωσιμότητα, Ενίσχυση, Ανάπτυξη, Εκτέλεση: Τώρα ένας επιτιθέμενος μπορεί να εκτελέσει τα μέσα επίτευξης ενός στόχου όπως η ανάπτυξη κακόβουλου λογισμικού για να πάρει τον έλεγχο άλλων υπολογιστών δικτύου ή να χειριστεί τις επικοινωνίες μεταξύ των μηχανών. Αυτό το βήμα είναι κρίσιμο για την ικανότητα ενός δράστη να επιτύχει απώλεια, άρνηση ή χειρισμό ενός στόχου. Σηματοδοτεί επίσης ένα χάσμα μεταξύ των δραστηριοτήτων που οδηγούν σε κυβερνο-εισβολή σε σχέση με εκείνες που οδηγούν σε κυβερνο-επιθέσεις. Πολλές εταιρείες δεν διαθέτουν αποτελεσματική ανίχνευση εισβολών και δεν γνωρίζουν αυτό το είδος δραστηριότητας στα συστήματά τους. Μια έρευνα του 2015 από την SANS ανέφερε ότι το 49% των ερωτηθέντων δεν γνώριζαν καμία διείσδυση ή μόλυνση των συστημάτων ελέγχου τους. Το 32 τοις εκατό ανέφερε ότι τα δίκτυα συστημάτων ελέγχου τους είχαν διεισδυθεί. Στο πλαίσιο ειδικών εφαρμογών, λίγο περισσότερο από το ήμισυ των ερωτηθέντων στην έρευνα της PWC για το 2015 έδειξε τη χρήση εργαλείων ανίχνευσης εισβολής, μια μείωση κατά δέκα τοις εκατό από το προηγούμενο έτος.

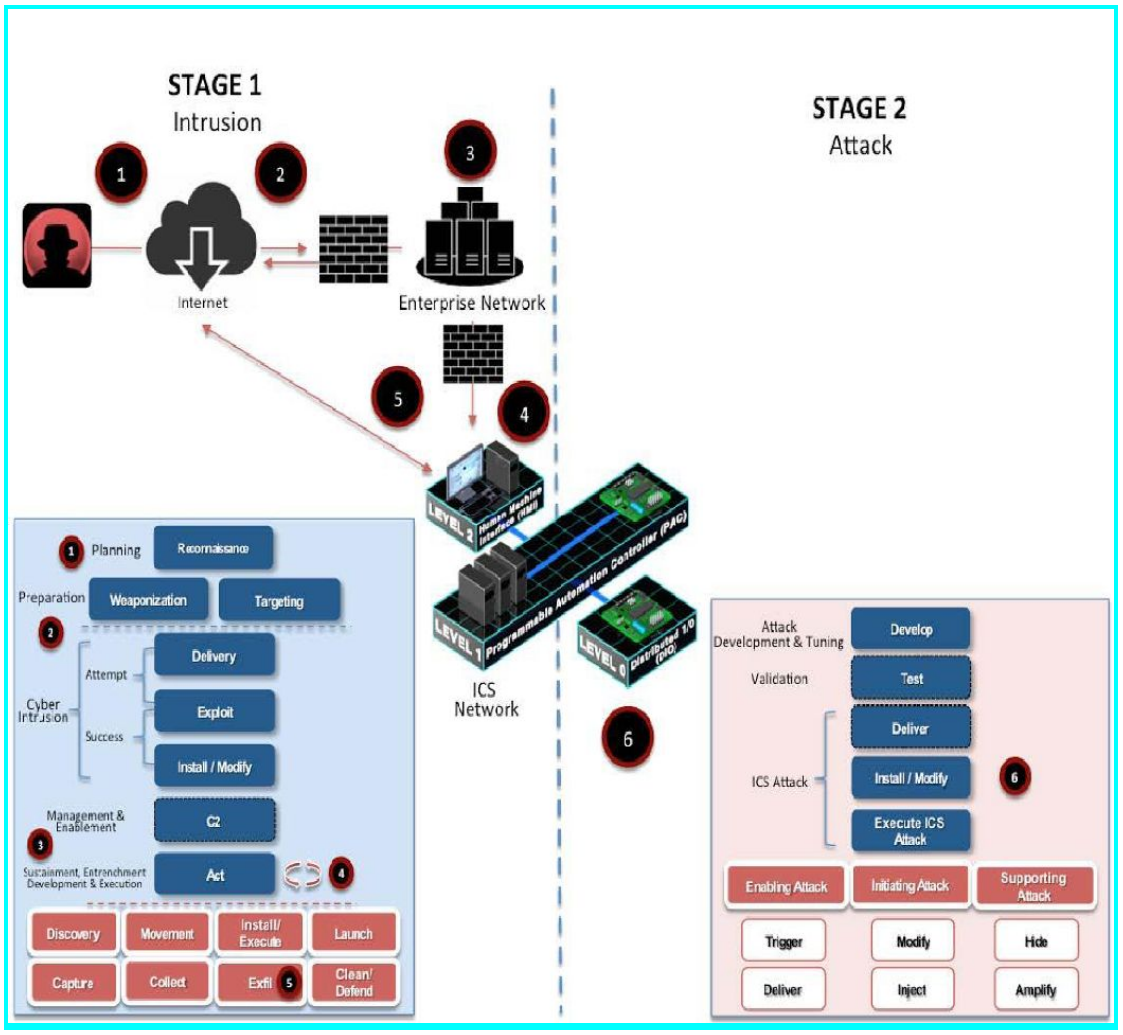
6.1.2 Στάδιο 2

6) Ανάπτυξη και συντονισμός επίθεσης: Με μη-ανιχνεύσιμη ελευθερία κινήσεων μέσα σε ένα δίκτυο-στόχο, ο επιτιθέμενος μπορεί τώρα να χρησιμοποιήσει τα ευρήματα σχετικά με τον ανακαλυφθέντα εξοπλισμό ICS για να «προσαρμόσει» την ικανότητα επίθεσής του, για να επιτύχει το επιθυμητό αποτέλεσμα.

7) Επικύρωση: Ένας εισβολέας ελέγχει την επιλεγμένη ικανότητα επίθεσης. Αυτό μπορεί να πραγματοποιηθεί μέσω προσομοίωσης - ή σε ορισμένες περιπτώσεις, ιδιαίτερα μιας εξελιγμένης επίθεσης που διεξάγεται από έναν εθνικό φορέα - ένας επιτιθέμενος μπορεί πράγματι να αποκτήσει έναν φυσικό εξοπλισμό ICS όμοιο με αυτόν ενός στόχου για διεξαγωγή δοκιμών. Τέτοιος εξοπλισμός μπορεί συχνά να αγοραστεί εύκολα από τους ηλεκτρονικούς εμπόρους λιανικής πώλησης όπως το eBay, όπου οι εικόνες ή οι περιγραφές μπορούν επίσης να παρέχουν χρήσιμες πληροφορίες σχετικά με τον τελευταίο τρόπο ανάπτυξης του εξοπλισμού ICS και τον τόπο λειτουργίας του. Οι ερευνητές της ασφάλειας πραγματοποίησαν πρόσφατα μια δοκιμή αγοράζοντας έναν διακομιστή SCADA από το eBay για λιγότερο από είκοσι δολάρια, ο οποίος περιείχε άσχημα προστατευμένα αρχεία διαμόρφωσης, διαγράμματα, δεδομένα υποσταθμών σε λειτουργία και άλλες ευαίσθητες πληροφορίες από τον προηγούμενο ιδιοκτήτη του. Η εταιρεία είχε πρόσφατα αναβαθμίσει τον εξοπλισμό της και υπέθεσε εσφαλμένα ότι ο διακομιστής SCADA είχε «απολυμανθεί» ως μέρος της πολιτικής για τον εξοπλισμό στο τέλος του κύκλου ζωής του, προτού πωληθεί.

8) Επίθεση ICS: Ο επιτιθέμενος ενεργοποιεί ή αναπτύσσει μια ικανότητα επίθεσης «ωφέλιμου φορτίου» (payload) για να επιτύχει το επιθυμητό αποτέλεσμα. Σε αντίθεση με μια επίθεση σε εξαρτήματα πληροφορικής – που μπορεί να οδηγήσει σε απώλεια δεδομένων, χρόνου ή χρήματος – μια αποτελεσματική επίθεση ενός περιβάλλοντος χρήσης που βασίζεται σε ICS μπορεί να οδηγήσει σε απώλεια παραγωγής ή μετάδοσης ηλεκτρικής ενέργειας για παρατεταμένο χρονικό διάστημα και οι ακραίες συνέπειες μπορεί να είναι η απώλεια της ζωής, άμεσα (αστάθεια ηλεκτρικής γραμμής προκαλεί ηλεκτροπληξία σε τεχνίτη) ή έμμεσα (νοσοκομεία μένουν χωρίς ηλεκτρική ισχύ). Αν και η επιτυχής επίθεση της τελευταίας τάξης θα ήταν δύσκολο να επιτευχθεί και πιθανόν να απαιτεί πόρους σε εθνικό επίπεδο, οι επιχειρήσεις κοινής ωφέλειας αντιμετωπίζουν όλο και περισσότερο προσπάθειες επιθέσεων στον κυβερνοχώρο. Μια έρευνα των επιχειρήσεων κοινής ωφελείας που ανέθεσαν δύο μέλη του αμερικανικού Κογκρέσου το 2013 διαπίστωσε ότι πάνω από δώδεκα επιχειρήσεις κοινής ωφελείας ανέφεραν «καθημερινές», «σταθερές» ή «συχνές» απόπειρες επιθέσεων στον κυβερνοχώρο, με μία από αυτές να αναφέρει ότι υπέστη περίπου 10.000 απόπειρες το μήνα. Η εκτίμηση της πρόθεσης της δημιουργίας μιας επικοινωνίας είναι δύσκολη και ως αποτέλεσμα πολλές επιχειρήσεις κοινής ωφέλειας θα θεωρούσαν αυτές τις χιλιάδες απόπειρες επιθέσεων στον

κυβερνοχώρο ως απλά σαρώσεις δικτύου ή ανιχνευτές που μπορεί να είναι αρχική αναγνώριση Σταδίου 1. Το αν οι χιλιάδες αυτές προσπάθειες αναγνώρισης σκοπεύουν να οδηγήσουν σε επιθέσεις Σταδίου 1 ή να εξελιχθούν σε επιθέσεις ICS Σταδίου 2 είναι άγνωστο και ως εκ τούτου οι αμυνόμενοι πρέπει να αξιοποιήσουν τις κατάλληλες δυνατότητες παρακολούθησης και αντίδρασης.

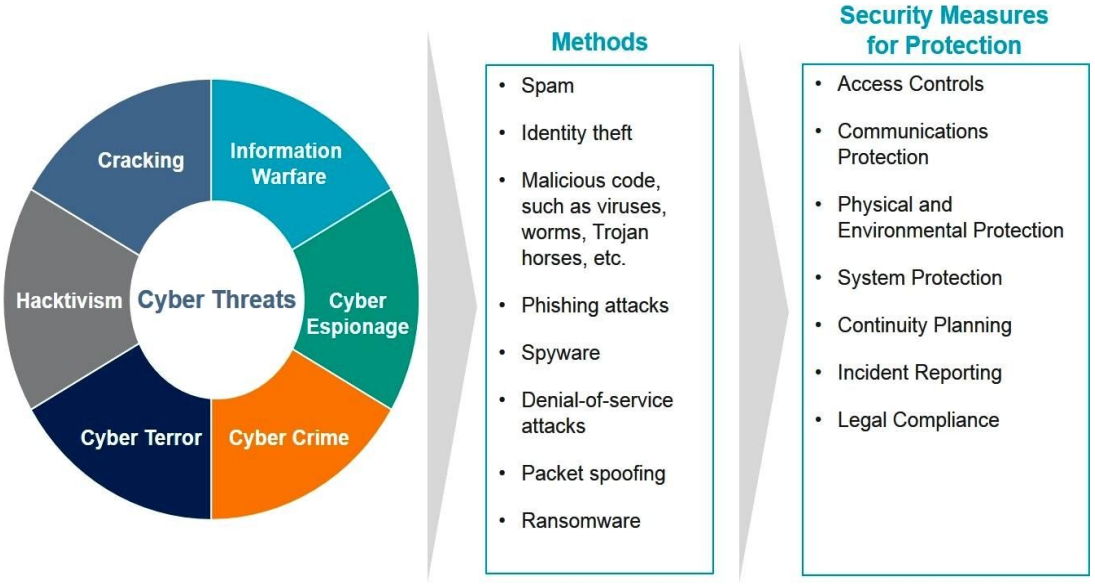


Σχ. 10 ICS Cyber Kill Chain - Εισβολή, Προετοιμασία και Εκτέλεση

Ένα ενδεικτικό παράδειγμα για το πώς ένας επιτιθέμενος στον κυβερνοχώρο στοχεύει, προσεγγίζει και κινείται σε όλα τα δίκτυα.

6.2 Οι επιθέσεις στον κυβερνοχώρο με την χρήση τεχνητής νοημοσύνης (Artificial Intelligence, A.I.)

Οι επιθέσεις στον κυβερνοχώρο με την χρήση τεχνητής νοημοσύνης (Artificial Intelligence, A.I.), αναμένεται να προκαλέσουν έκρηξη των διεισδύσεων στα δίκτυα, των κλοπών προσωπικών δεδομένων και της εξάπλωσης «επιδημιών» ευφυών ιών υπολογιστών. Η μόνη ελπίδα για να καταπολεμηθούν οι επιθέσεις με χρήση τεχνητής νοημοσύνης, είναι να χρησιμοποιηθεί, επίσης, τεχνητή νοημοσύνη. Αυτό, είναι πολύ πιθανό να οδηγήσει σε διαμάχες στον κυβερνοχώρο, με χρήση «όπλων» τεχνητής νοημοσύνης. Οι συνέπειες μπορεί να είναι πολύ ανησυχητικές μακροπρόθεσμα, ειδικά καθώς μεγάλοι κυβερνητικοί φορείς θα συμμετέχουν στις διαμάχες αυτές.



Σχ. 11 Απειλές στον κυβερνοχώρο – Μέθοδοι επίθεσης και μέτρα ασφαλείας για προστασία

Σύμφωνα με έρευνα, τα εγκλήματα στον κυβερνοχώρο έχουν πάνω από 1,5 εκατομμύριο «θύματα» την ημέρα – τα οποία ανέρχονται σε περισσότερα από 500 εκατομμύρια «θύματα» ετησίως. Η παγκόσμια αγορά ασφάλειας υπολογιστικών συστημάτων, υπολογίζεται σε €100 δισ. το 2017 – από €55 εκατ. το 2011.

Υπάρχει μια τεράστια ποικιλία επιθέσεων και απειλών. Οι πιο σοβαρές από αυτές παρατίθενται παρακάτω:

- Viruses
- Trojans
- SQL injection
- Worms
- Malware
- Identity theft

Μια, ιδιαίτερα προτιμητέα, μορφή επιθέσεων, είναι η κλοπή ταυτότητας (identity theft). Σε αυτόν τον τύπο επίθεσης, οι κλέφτες μπαίνουν σε δίκτυο αποκτώντας μη εξουσιοδοτημένη πρόσβαση σε ασφαλείς πληροφορίες. Στηρίζονται σε αυτήν την προσέγγιση για να στοχεύσουν μεμονωμένους χρήστες - που έχουν εξαπατηθεί ώστε να γνωστοποιήσουν τους κωδικούς πρόσβασής τους ή να εγκαταστήσουν κακόβουλο λογισμικό στους υπολογιστές τους – πρακτική που παρέχει πρόσβαση του επιτιθέμενου στη διαχείριση του δικτύου.

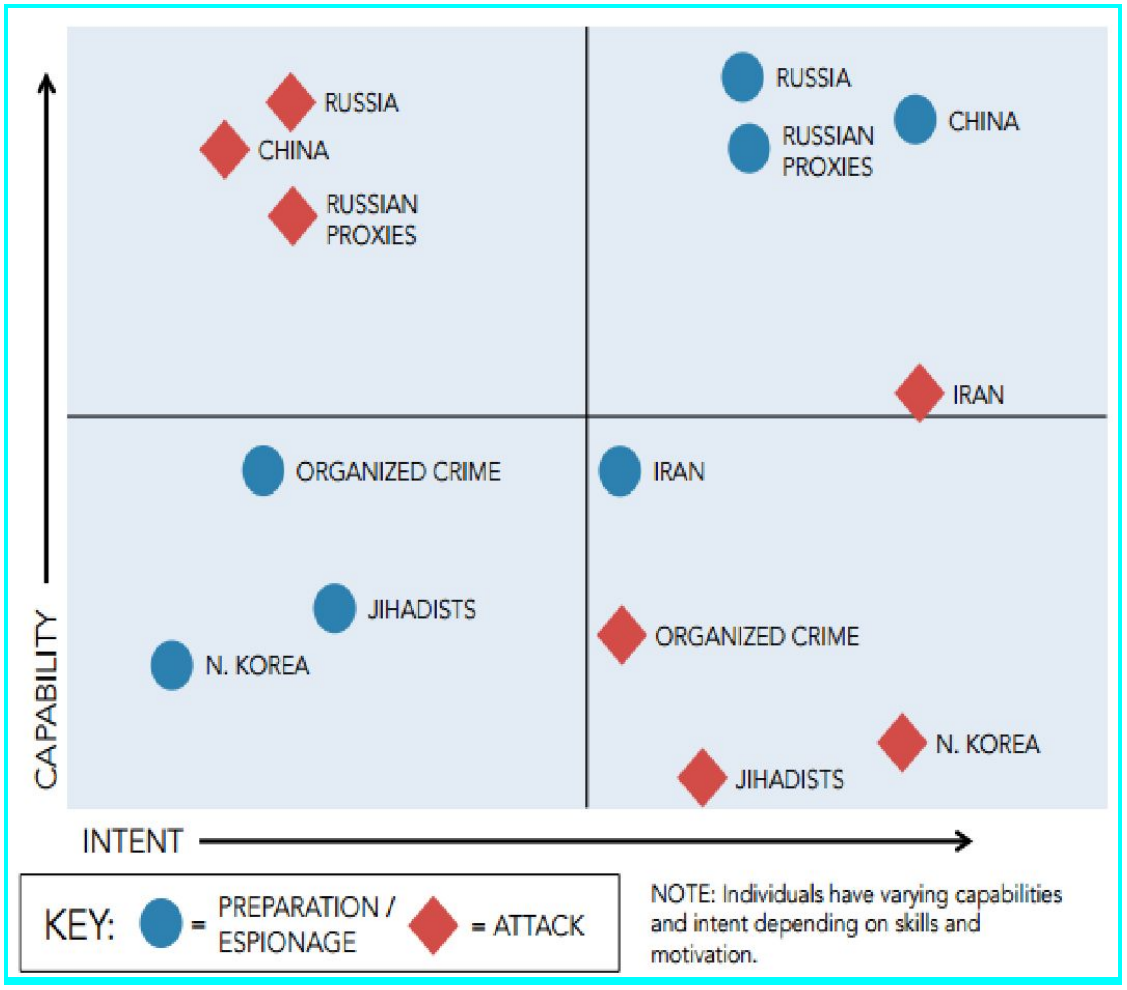
6.3 Παράγοντες απειλής

Οι επιθέσεις στα Συστήματα Βιομηχανικού Ελέγχου (ICS), έχουν γίνει πιο στοχευμένες από ότι στο παρελθόν. Οι επιτιθέμενοι έχουν εντρυφήσει για το πώς να επιτεθούν, χρησιμοποιώντας επιθέσεις προσαρμοσμένες ειδικά για να εκμεταλλευτούν τα ICS. Επιπλέον, οι εισβολείς δίνουν ιδιαίτερη προσοχή όχι μόνο στο «ωφέλιμο φορτίο» (payload), αλλά και στην παράδοσή του, εστιάζοντας στις αξιόπιστες σχέσεις των ICS. Το «ωφέλιμο φορτίο», αναφέρεται σε κακόβουλο λογισμικό ή ιούς υπολογιστών που παράγουν επιβλαβή αποτελέσματα στο σύστημα στόχο στο οποίο παραδίδεται το «ωφέλιμο φορτίο». Η «παράδοση», αναφέρεται στον φορέα ή τη διαδρομή μέσω της οποίας ένας εισβολέας εισάγει το «ωφέλιμο φορτίο» σε έναν στόχο.

Ως αποτέλεσμα, έχουν αυξηθεί οι επιθέσεις τύπου phishing κατά των μηχανικών σχεδιασμού και εκείνων στις εγκαταστάσεις παραγωγής ενέργειας, καθώς και οι

επιθέσεις τύπου watering hole σε σημεία όπου υπάρχουν πληροφορίες για τους μηχανικούς των ICS. Οι επιτιθέμενοι αρχίζουν να τροφοδοτούν τα αρχεία και τα στοιχεία ICS που είναι διαθέσιμα για την ενημέρωση του υλικολογισμικού και την εξεύρεση τρόπων για την αντικατάστασή τους στην αλυσίδα εφοδιασμού, προκειμένου να αποκτήσουν κακόβουλα προγράμματα μέσω του τείχους προστασίας και σε περιβάλλοντα παραγωγής. Πολλοί παράγοντες απειλών σε πολλαπλά μέτωπα εξακολουθούν να επιδιώκουν να εκμεταλλευτούν τις ευπάθειες του κυβερνοχώρου στο ηλεκτρικό δίκτυο. Κράτη και μη κρατικοί φορείς, συμπεριλαμβανομένων ξένων τρομοκρατικών ομάδων και εγκληματικών οργανώσεων, αποτελούν απειλή για το ηλεκτρικό δίκτυο, αν και σε διαφορετικά επίπεδα.
Οι επιθέσεις στον κυβερνοχώρο με πολιτικά κίνητρα είναι πλέον μια αυξανόμενη πραγματικότητα και οι ξένοι φορείς αναβαθμίζουν και αναπτύσσουν, κρυφά, πρόσβαση σε συστήματα υποδομής ζωτικής σημασίας, τα οποία ενδέχεται να εκμεταλλευτούν για να προκαλέσουν άμεσα διακοπές στην παροχή ηλεκτρικής ενέργειας, εφόσον η πρόθεση του αντιπάλου γίνει εχθρική. Επιπλέον, όσοι διενεργούν κατασκοπεία στον κυβερνοχώρο, στρέφονται καθημερινά σε κυβερνητικά, στρατιωτικά και εμπορικά δίκτυα.

Κράτη όπως η Ρωσία και η Κίνα επιδιώκουν να εκμεταλλευτούν τις ευπάθειες των δικτύων των Η.Π.Α., για να εξυπηρετήσουν στρατηγικούς στόχους κατά τη διάρκεια ενός ενδεχόμενου πολέμου, και αυξάνουν τις ικανότητες για να χτυπήσουν σε κρίσιμες υποδομές. Χώρες όπως το Ιράν και η Βόρεια Κορέα έχουν πραγματοποιήσει επιθετικές επιχειρήσεις στον κυβερνοχώρο, στοχεύοντας στις επιθέσεις τους σε διαταραχές ή ασύμμετρες επιπτώσεις από πλευράς εθνικής, οικονομικής και αστικής ασφάλειας. Οι μη κρατικοί φορείς στοχεύουν σε εγκαταστάσεις δικτύου όχι μόνο για τις ασύμμετρες επιπτώσεις, αλλά και για να προβούν σε πολιτικές δηλώσεις και να προκαλέσουν αντιλήψεις για τη διακυβέρνηση και τη σταθερότητα.



Σχ. 12 Οι προθέσεις και η ικανότητα των φορέων απειλής

Η ικανότητα που απαιτείται για το σχεδιασμό έναντι της εκτέλεσης μιας επιθέσεις στον κυβερνοχώρο διαφέρει, ακόμη και εντός της ίδιας ομάδας. Η υψηλή δεξιότητα δεν είναι πάντα ενδεικτική της μεγαλύτερης πρόθεσης επίθεσης. Για παράδειγμα, οι εθνικοί φορείς μπορούν να επωφεληθούν σε μεγάλο βαθμό από τις διεισδύσεις στον κυβερνοχώρο σε αντίπαλο έθνος, αλλά μια επίθεση στον κυβερνοχώρο μπορεί να σημαίνει μια πράξη πολέμου.

6.3.1 Ρωσία

Η Ρωσία διαθέτει μια ουσιαστική και καλά εξοπλισμένη κεντρική διοίκηση στον κυβερνοχώρο. Στο παρελθόν, οι εισβολές κυβερνοχώρου των Αμερικανικών

κυβερνητικών οργανώσεων, συμπεριλαμβανομένου του Υπουργείου Εξωτερικών, του Υπουργείου Άμυνας και του Λευκού Οίκου, αποδόθηκαν σε Ρώσους χάκερς που χρηματοδοτήθηκαν από το κράτος.

Το 2007, η Ρωσία διενήργησε κυβερνοεπιθέσεις στην κρίσιμη τεχνολογική υποδομή της Εσθονίας, προκαλώντας προβλήματα Distributed Denial of Service (DDoS), στον κυβερνητικό, οικονομικό και τηλεπικοινωνιακό τομέα.

Το 2009 αναφέρθηκε οτι η Ρωσία και η Κίνα είχαν κάνει προσπάθειες να διεισδύσουν στο ηλεκτρικό δίκτυο των ΗΠΑ, χρησιμοποιώντας προγράμματα λογισμικού για να χαρτογραφήσουν τις υποδομές των ΗΠΑ και ενδεχομένως να διαταράξουν το δίκτυο ηλεκτρικής ενέργειας.

Στα τέλη Δεκεμβρίου του 2015, με την πληρέστερη επίθεση στον κυβερνοχώρο σε ισχύ μέχρι σήμερα, έμπειροι χάκερς, οι οποίοι, από πολλούς, είναι ύποπτοι οτι εργάζονται για λογαριασμό της ρωσικής κυβέρνησης, στόχευσαν τον Ουκρανικό ενεργειακό τομέα χρησιμοποιώντας πολλαπλά εργαλεία στον κυβερνοχώρο, συμπεριλαμβανομένου του BlackEnergy, για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε δίκτυα εταιρειών παροχής ενέργειας. Το κακόβουλο λογισμικό, εντοπίστηκε ότι υπήρχε στα δίκτυα της Ουκρανίας από τον Μάιο του 2014.

6.3.2 Κίνα

Η Κίνα είναι ένας εξαιρετικά ενεργός, προηγμένος κυβερνοχώρος εδώ και αρκετό καιρό - ειδικά όσον αφορά την οικονομική κατασκοπεία ενάντια στις αμερικανικές επιχειρήσεις - αν και χρησιμοποιούν συχνά εργαλεία (όπως σαρωτές δικτύου, ιούς και botnets) για πρόσβαση σε στόχους. Πολλαπλές εισβολές από την Κίνα στα ICS/SCADA και τα έξυπνα δίκτυα των ΗΠΑ, μπορεί να στοχεύουν περισσότερο στην κλοπή πνευματικής ιδιοκτησίας και τη συλλογή πληροφοριών για την ενίσχυση της δικής τους υποδομής, αλλά είναι πιθανό να χρησιμοποιούν αυτές τις εισβολές για να αναπτύξουν ικανότητες για να επιτεθούν στο BES. Για παράδειγμα, ένα από τα στρατιωτικά στελέχη του Λαϊκού Απελευθερωτικού Στρατού της μονάδας 61398, που κατηγορήθηκε για την κλοπή των οικονομικών μυστικών των ΗΠΑ τον Μάιο του 2014, συνδέθηκε με το UglyGorilla, ένα ψευδώνυμο χάκερ υπεύθυνου για εισβολές

στον κυβερνοχώρο μιας εγκατάστασης των Βορειοανατολικών ΗΠΑ τουλάχιστον από το 2012.

Όπως και η Ρωσία, η Κίνα είναι απίθανο να εκτελέσει επιθέσεις στον κυβερνοχώρο, με στόχο τη γενικευμένη ζημιά στο ηλεκτρικό δίκτυο των ΗΠΑ, λόγω των πολιτικών συνεπειών που θα μπορούσε να επιφέρει μια τέτοια εχθρική πράξη.

6.3.3 Ιράν

Το Ιράν χρησιμοποιεί το κυβερνοχώρο ως εργαλείο κατά των πολιτικών εχθρών και της συλλογής πληροφοριών και έχει αποδειχθεί οτι είναι ένας πολύ εξειδικευμένος, αν και κάπως λιγότερο περίπλοκος, κυβερνοχώρος σε σύγκριση με τη Ρωσία και την Κίνα. Ένα ομοσπονδιακό κατηγορητήριο των ΗΠΑ το 2016 απέδωσε ένα περιστατικό του 2013 που αφορούσε πολλαπλές απομακρυσμένες εισβολές ενός υπολογιστή ελέγχου του φράγματος Bowman στο Rye της Νέας Υόρκης σε ιδιωτικές ομάδες ασφάλειας υπολογιστών που λειτουργούσαν για λογαριασμό της Ισλαμικής Επαναστατικής Φρουράς του Ιράν. Από το 2012 έως το 2013, σε απευθείας σύνδεση τραπεζικές τοποθεσίες, χτυπώντας τους με επιθέσεις DDoS. Συνολικά, το Ιράν και κυβερνητικές οργανώσεις σε ολόκληρη τη χώρα συνεχίζουν να επεκτείνουν την ικανότητά τους να διεξάγουν σημαντικές επιθέσεις στον κυβερνοχώρο.

6.3.4 Βόρεια Κορέα

Αν και λιγότερο εξελιγμένη, η Λαϊκή Δημοκρατία της Κορέας (ΛΔΚ) έχει αποδείξει οτι η πρόθεσή της να διενεργήσει επιθέσεις στον κυβερνοχώρο είναι κάπως απρόβλεπτη, όπως στην παραβίαση της Sony το 2014. Η ΛΔΚ εστιάζει κατά κύριο λόγο τις κυβερνοεπιχειρησιακές της δραστηριότητες στη συλλογή πληροφοριών και όχι στην καταστροφή, κυρίως επί της Νότιας Κορέας. Τουλάχιστον, η ΛΔΚ έχει επιδείξει ενδιαφέρον για την πολεμική της στον κυβερνοχώρο ως τρόπο αντιπαράθεσης των δυνατοτήτων της Νότιας Κορέας και των ΗΠΑ.

6.3.5 Τρομοκράτες

Οι τρομοκρατικές ομάδες όπως το ISIS, έχουν φιλόδοξους στόχους επίθεσης όσον αφορά τον κυβερνοχώρο. Ενώ οι προσπάθειες να «καταρρίψουν» το αμερικανικό δίκτυο ηλεκτρικής ενέργειας δεν θεωρούνταν απειλητικές μέχρι πρότινος, οι παρα-τρομοκρατικές ομάδες αντιπροσωπεύουν μια ιδιαίτερα ορατή απειλή και το ISIS έχει αποδειχθεί οτι είναι ένας από τους σημαντικότερους παράγοντες της δραστηριότητας hacktivist, καθ' όλη τη διάρκεια του 2015. Ωστόσο, οι τρομοκρατικές ομάδες όπως το ISIS ενδέχεται να έχουν υψηλό κίνητρο να διαταράξουν ή να προκαλέσουν βλάβη στο ηλεκτρικό δίκτυο, δεν διαθέτουν επί του παρόντος τα εξελιγμένα εργαλεία ή τις δεξιότητες που είναι απαραίτητες για την εκτέλεση επιθέσεων στον κυβερνοχώρο, οι οποίες θα μπορούσαν να έχουν εκτεταμένο ή σημαντικό αντίκτυπο στο σύστημα ισχύος.

6.3.6 Απλοί Hackers

Απλοί χάκερς χωρίς καν ιδεολογικά κίνητρα. Συνήθως νεαροί προγραμματιστές ή και πρωτάρηδες μεάφθονο ελεύθερο χρόνο και διάθεση να μάθουν. Αυτό που τους προκαλεί είναι η συγκίνηση του να τα καταφέρουν να διεισδύσουν σε κάτι απαγορευμένο. Συνήθως δεν καταφέρνουν και πολλά. Παρ'όλα αυτά πάντα υπάρχει ο κίνδυνος να κάνουν αρκετή ζημιά, έστω και από τύχη.

6.3.7 Hacktivists

Hacktivists – ή χάκερς με ιδεολογικά κίνητρα – θέτουν μια άλλη απειλή στον κυβερνοχώρο δύσκολο να προγραμματιστεί ενάντια. Ομάδες όπως οι Anonymous, συνήθως επιτίθενται σε εταιρείες και κυβερνητικές υπηρεσίες εκθέτοντας διαβαθμισμένα δεδομένα ή «βομβαρδίζοντας» τα συστήματά τους με επιθέσεις DDoS. Ο Οργανισμός Εθνικής Ασφάλειας των Η.Π.Α., δήλωσε οτι οι Anonymous ενδέχεται να είναι σε θέση να προκαλέσουν μια περιορισμένη διακοπή ρεύματος και ορισμένοι ομοσπονδιακοί αξιωματούχοι πιστεύουν οτι οι Anonymous στρέφονται σε

μια πιο καταστροφική κατεύθυνση πέρα από τις επιθέσεις σε εταιρείες και κυβερνητικές ιστοσελίδες.

7 Ευπάθειες και κίνδυνοι που υπάρχουν σε περιβάλλον Smart Grid

7.1 Ευπάθειες σε περιβάλλον Smart Grid

7.1.1 Θέματα ευπάθειας και παράγοντες κινδύνου

Όπως ήδη αναφέρθηκε, οι ΤΠΕ είναι κρίσιμες για την υλοποίηση έξυπνων δικτύων. Οι ΤΠΕ θα διαδραματίσουν ζωτικό ρόλο στην αξιοπιστία και την ασφάλεια των συστημάτων ηλεκτρικής ενέργειας και επομένως η προστασία των σημερινών και των νέων τεχνολογιών ΤΠΕ πρέπει να αντιμετωπιστεί από τον τομέα της ηλεκτρικής ενέργειας. Αυτό δεν είναι μόνο καθήκον των φορέων εκμετάλλευσης δικτύων, αλλά και των δημόσιων φορέων, των οργανισμών τυποποίησης, των ακαδημαϊκών κύκλων, των νέων παρόχων υπηρεσιών και οποιουδήποτε άλλου ενδιαφερόμενου μέρους.

Η ασφάλεια στον κυβερνοχώρο πρέπει να εξεταστεί σε όλους τους τομείς των έξυπνων δικτύων και σε όλες τις φάσεις του κύκλου ζωής του συστήματος, από τη φάση σχεδιασμού έως τον παροπλισμό, μέσω της ανάπτυξης, της εγκατάστασης, της συντήρησης κλπ. Επιπλέον, η ασφάλεια στον κυβερνοχώρο πρέπει να αντιμετωπίσει όχι μόνο εσκεμμένες επιθέσεις από δυσαρεστημένους εργαζόμενους, πράκτορες βιομηχανικής κατασκοπείας ή τρομοκράτες. Θα πρέπει επίσης να ληφθεί υπόψη η ακούσια έκθεση της υποδομής των πληροφοριών λόγω σφαλμάτων χρηστών, αποτυχιών εξοπλισμού και φυσικών καταστροφών.

Η επίτευξη ενός ασφαλούς έξυπνου δικτύου δεν είναι εύκολο έργο. Υπάρχει μια σειρά τρωτών σημείων ή αδυναμιών που πρέπει πρώτα να προσδιοριστούν και να αναλυθούν και στη συνέχεια να επιχειρηθεί να επιλυθούν μέσω διαδικασιών διαχείρισης κινδύνων. Ωστόσο, υπάρχουν ορισμένες προκλήσεις, όπως τεχνολογικά κενά, οργανωτικά προβλήματα ή ζητήματα ευαισθητοποίησης που πρέπει να επιλυθούν για την επίτευξη αυτού του στόχου.

7.1.2 Γενικές σκέψεις / εκτιμήσεις

Τα τρωτά σημεία ή αδυναμίες κυβερνοασφάλειας, είναι συνθήκες που υπάρχουν σε οποιοδήποτε στοιχείο του κυβερνοχώρου ή οργανωτική διαδικασία σε διαφορετικά επίπεδα, συμπεριλαμβανομένου του σχεδιασμού, της υλοποίησης, της διαμόρφωσης, της λειτουργίας ή της διαχείρισης. Τα έξυπνα δίκτυα χρησιμοποιούν πολύ τις ΤΠΕ και συνεπώς οι επιτιθέμενοι θα μπορούσαν να εκμεταλλευτούν αυτές τις ευπάθειες για πολλούς διαφορετικούς σκοπούς:

- να διεισδύσουν στον Διαχειριστή του Συστήματος Διανομής (Distribution System Operator, DSO), του έξυπνου δικτύου
- να αποκτήσουν πρόσβαση στο λογισμικό ελέγχου είτε σε υποσταθμούς είτε σε κεντρικά συστήματα
- να χειραγωγήσουν έξυπνους μετρητές για να διαπράξουν απάτες
- να εισαγάγουν κακόβουλο λογισμικό για να αποκτήσουν απομακρυσμένο έλεγχο, κ.λπ.

Εκτός αυτού, τα έξυπνα δίκτυα προσφέρουν στους κυβερνοεγκληματίες περισσότερα σημεία διείσδυσης από τα υπάρχοντα σημερινά δίκτυα. Μια αμφίδρομη υποδομή επικοινωνίας θα συνδέει κάθε σπίτι και κτίριο με το DSO, πράγμα που διευρύνει σημαντικά την επιφάνεια επίθεσης.

Από την άλλη πλευρά, τα έξυπνα δίκτυα μπορούν να θεωρηθούν ως ένα μεγάλο σύστημα από συστήματα. Εκτείνονται σε ολόκληρη την αλυσίδα της ηλεκτρικής ενέργειας, από την παραγωγή μέχρι την κατανάλωση. Πολλές εφαρμογές και λειτουργίες των έξυπνων δικτύων, εξαρτώνται η μία από την άλλη και πολλές φορές αυτές οι εφαρμογές και οι λειτουργίες δεν ελέγχονται από τον ίδιο διαχειριστή. Μια τέτοια περίπτωση είναι η προηγμένη αυτοματοποίηση διανομής (Advanced Distribution Automation, ADA), η οποία εξαρτάται σε μεγάλο βαθμό από την αυτοματοποίηση του υποσταθμού, αλλά χρειάζεται επίσης δεδομένα AMI και πληροφορίες σχετικά με τα κατανεμημένα ενεργειακά μέσα να εκτελούνται σωστά. Ως εκ τούτου, τα έξυπνα δίκτυα μπορούν να θεωρηθούν ως ένα σύστημα ετερογενών διασυνδεδεμένων συστημάτων (δηλαδή εικονικών σταθμών ηλεκτροπαραγωγής, πλέγματος μεταφοράς, δικτύων διανομής κ.λπ.), το καθένα με δικό του σύνολο

εξοπλισμού και τεχνολογιών επικοινωνίας, έξυπνες συσκευές, αυτοματοποιημένα στοιχεία ελέγχου και αλγόριθμους, οι διαφορετικές οργανωτικές προσεγγίσεις κλπ. Αυτή η ανομοιογένεια, πολυμορφία και πολυπλοκότητα καθιστούν εξαιρετικά δύσκολη την προστασία της και ταυτόχρονα εισάγουν νέες και πολύπλοκες (και πιθανώς ευάλωτες) αλληλεπιδράσεις και εξαρτήσεις που δεν υπήρχαν στην παραδοσιακή εξουσία συστημάτων.

7.1.3 Ευαίσθητα στοιχεία ΤΠΕ στον κυβερνοχώρο

Οι ευπάθειες μπορούν να είναι διαφορετικού είδους (π.χ. διαχειριστικές, οργανωτικές, κ.λπ.). Ένας σύντομος κατάλογος των στοιχείων ΤΠΕ των έξυπνων δικτύων που πρέπει να θεωρηθούν ως πηγή ευπάθειας, είναι ο εξής:

- **Λειτουργικά συστήματα:** γεννήτριες, μετασχηματιστές, συστήματα εποπτείας και αποκτήσεως δεδομένων (SCADA), συστήματα προγραμματισμού λογικών ελεγκτών (PLC), υποσταθμοί, έξυπνοι μετρητές και άλλες ευφυείς ηλεκτρικές συσκευές (Intelligent Electronic Devices, IED).
- **Κλασικά συστήματα πληροφορικής:** υπολογιστές, διακομιστές, κεντρικοί υπολογιστές, εφαρμογές, βάσεις δεδομένων, ιστότοποι, υπηρεσίες ιστού, κλπ., μεταξύ των οποίων περιλαμβάνονται τα στοιχεία εταιρικής υποδομής.
- **Δίκτυα και πρωτόκολλα επικοινωνιών:** Ethernet, Wifi, PRIME, DLMS ή COSEM, Zigbee, 4G, DNP3, κ.λπ.
- **Τερματικά σημεία:** έξυπνοι μετρητές, Η/Υ, έξυπνα τηλέφωνα και άλλες κινητές συσκευές. Λαμβάνοντας υπόψη τόσο τις φυσικές όσο και τις λογικές πτυχές.

Πρόκειται για κατηγοριοποίηση ανώτατου επιπέδου των στοιχείων υποδομής των υπηρεσιών κοινής ωφέλειας που μπορεί να έχουν ευπάθειες στον κυβερνοχώρο.

Για κάθε συγκεκριμένη περίπτωση, πρέπει να διεξαχθεί μια διαδικασία εντοπισμού και αναγνώρισης ευπάθειας, προκειμένου να εντοπιστούν όλες οι αδυναμίες ή οι αδυναμίες που επηρεάζουν την εταιρεία κοινής ωφέλειας.

7.1.4 Τεχνολογικές ευπάθειες

Τα έξυπνα δίκτυα φέρνουν ένα ολόκληρο φάσμα εφαρμογών και βασικών τεχνολογιών και πρωτοκόλλων επικοινωνίας. Ωστόσο, οι τεχνολογίες που είναι βασισμένες σε δομημένες γλώσσες και στο διαδίκτυο (π.χ. εφαρμογές ιστού και υπηρεσίες ιστού, διακομιστές εφαρμογών και http), πρόκειται να αποτελέσουν κύριο παράγοντα υλοποίησης έξυπνων δικτύων. Για παράδειγμα, αυτές οι τεχνολογίες θα επιτρέψουν τον απομακρυσμένο έλεγχο των έξυπνων συσκευών και των συστημάτων διαχείρισης ενέργειας που βρίσκονται στα οικιακά δίκτυα (Home Area Networks, HANs), είτε από τον ιδιοκτήτη του σπιτιού είτε από την εταιρεία που παρέχει υπηρεσίες σχετικές με την ενέργεια στον τελικό καταναλωτή. Ένα άλλο παράδειγμα, όπου οι εφαρμογές που βασίζονται στο διαδίκτυο θα διαδραματίσουν σημαντικό ρόλο, είναι οι εξελιγμένες εφαρμογές μέτρησης. Τέτοιες εφαρμογές θα έχουν πρόσβαση, σε πραγματικό χρόνο, στους ενεργειακούς συντελεστές και τις πληροφορίες κατανάλωσης για τις λειτουργίες ζήτησης-απόκρισης και με στόχο την επίτευξη αποδοτικότερης χρήσης της παραγόμενης ισχύος. Παρόλο που άλλες τεχνολογίες – παλαιές και νέες – θα συνυπάρχουν με τις εφαρμογές μέσω διαδικτύου, οι τελευταίες είναι η αιχμή του δόρατος του «καινούριου», και αποτυπώνουν τέλεια το τι θα μπορούσε να είναι η επόμενη γενιά τρωτών σημείων που βασίζονται στις ΤΠΕ στα ηλεκτρικά δίκτυα. Όπως έχει αποδειχθεί σε άλλες επιχειρήσεις, με την εφαρμογή αυτών των τεχνολογιών, οι επιχειρήσεις κοινής ωφελείας θα πρέπει να καταβάλουν μεγάλη προσπάθεια για να αποφύγουν την αποτυχία έστω κι ενός σημείου. Οι επιθέσεις που στο παρελθόν θα απαιτούσαν την εκμετάλλευση πολλαπλών τρωτών σημείων για την παράκαμψη πολλών επιπέδων ελέγχου ή την έλλειψη διαλειτουργικότητας μεταξύ των συστημάτων, μπορούν τώρα να απλοποιηθούν σε ένα μόνο φορέα επίθεσης στα έξυπνα δίκτυα.

Τα πρωτόκολλα επικοινωνιών που χρησιμοποιούνται στα έξυπνα δίκτυα αποτελούν επίσης σημαντική πηγή ευπάθειας. Συγκεκριμένα, ορισμένα από τα ασύρματα πρωτόκολλα που χρησιμοποιούνται σε έξυπνα δίκτυα (π.χ. Zigbee, Wimax, Wifi, LTE, UMTS, GPRS, κ.λπ.), χρησιμοποιούνται ήδη ευρέως σε άλλες επιχειρήσεις και ως εκ τούτου πολλές από τις ευπάθειές τους είναι γνωστές στους εισβολείς και υπάρχουν διαθέσιμα αυτοματοποιημένα εργαλεία, διευκολύνοντας την εκμετάλλευσή τους. Στις περισσότερες περιπτώσεις, οι επιτιθέμενοι που στοχεύουν έξυπνα δίκτυα, θα επιχειρήσουν να επιτεθούν σε ασύρματα δίκτυα, προκειμένου να προκαλέσουν άρνηση παροχής υπηρεσιών (Denial Of Service, DOS), να αποκτήσουν ευαίσθητες πληροφορίες ή να παρακάμψουν τους περιμετρικούς ελέγχους ασφάλειας, ώστε να αποκτήσουν πρόσβαση σε εσωτερικά δίκτυα. Δυστυχώς, δεν επηρεάζονται μόνο ασύρματα πρωτόκολλα από ευπάθειες. Η χρήση ορισμένων τεχνολογιών εφαρμογών, όπως οι προαναφερόμενες τεχνολογίες μέσω διαδικτύου, συνεπάγεται επίσης τη χρήση ορισμένων πρωτοκόλλων επιπέδου εφαρμογής. Αυτή είναι η περίπτωση της XML μέσω HTTP για εφαρμογές web service ή της αρχιτεκτονικής DLMS (Device Language Message Specification), για εφαρμογές DLMS ή COSEM (Companion Specification for Energy Metering). Πολλά από αυτά τα πρωτόκολλα έχουν σχεδιαστεί με την έλλειψη εγγενών μηχανισμών ασφαλείας. Επιπλέον, ορισμένα από τα νεότερα πρωτόκολλα, τα οποία περιλαμβάνουν ήδη προφίλ ασφαλείας υψηλού επιπέδου, περιλαμβάνουν επίσης προφίλ ασφαλείας «χαμηλό επίπεδο» ή «όχι ασφάλεια». Η διασφάλιση πολλών από αυτά τα πρωτόκολλα απαιτεί σε πολλές περιπτώσεις την εφαρμογή εξαιρετικά πολύπλοκων τεχνολογιών κρυπτογράφησης που απαιτούν αντίστοιχα και αρκετή υπολογιστική ισχύ. Οι πιέσεις από τις επιχειρήσεις κοινής ωφέλειας για μείωση του κόστους, καθώς και η έλλειψη εμπειρογνωμοσύνης στον τομέα της ασφάλειας και η έλλειψη επίγνωσης των κινδύνων από την πλευρά κατασκευαστών και πωλητών έξυπνων δικτύων, έχουν ως αποτέλεσμα την παραγωγή εξοπλισμού χωρίς τις απαιτούμενες δυνατότητες ασφάλειας ώστε να εξασφαλίζεται το απαραίτητο επίπεδο ασφάλειας για τις επικοινωνίες των έξυπνων δικτύων. Τέλος, δεν πρέπει να παραληφθεί η χρήση των παλαιότερων πρωτοκόλλων SCADA, που είχαν αναπτυχθεί χωρίς να ληφθούν υπόψη οι απαιτήσεις ασφαλείας, των οποίων η εξασφάλιση προστασίας δεν είναι απλή.

7.1.5 Ανθρώπινος Παράγοντας

Ο ανθρώπινος παράγοντας περιλαμβάνει όλες εκείνες τις ανθρώπινες πτυχές και τις συνθήκες που ένας επιτιθέμενος θα μπορούσε να εκμεταλλευτεί για να πετύχει επιτυχώς τους κακόβουλους στόχους του. Αυτές οι ανθρώπινες πτυχές και συνθήκες εξαρτώνται άμεσα από την κατάρτιση των εργαζομένων στον τομέα της ασφάλειας και από τις δράσεις ευαισθητοποίησης που αναλαμβάνουν οι οργανισμοί.

Οι επιθέσεις κοινωνικής μηχανικής (Social engineering attacks), θα ελέγξουν την ευαισθητοποίηση σχετικά με την ασφάλεια και την κατάρτιση των υπαλλήλων των φορέων εκμετάλλευσης έξυπνων δικτύων, των κατασκευαστών, των τελικών καταναλωτών, κλπ. Για παράδειγμα, ένας εισβολέας μπορεί να προσπαθήσει να μιμηθεί έναν υπάλληλο από τον ανάδοχο της υπηρεσίας χρηστών για να εξακριβώσει εμπιστευτικές πληροφορίες όπως διαπιστευτήρια πιστοποίησης ή για να λάβει επιπλέον προνόμια σε συγκεκριμένο εξοπλισμό. Τα συνήθη παραδείγματα επιθέσεων κοινωνικής μηχανικής περιλαμβάνουν, επίσης, τα ακόλουθα:

- Μίμηση ενός υπαλλήλου προς στο IT Help Desk, ώστε να αλλάξει τον κωδικό του πραγματικού υπαλλήλου
- Μίμηση συνεργαζόμενου εργολάβου για τη λήψη δυνητικά ευαίσθητων πληροφοριών ή εξοπλισμού για δολιοφθορά
- Αφήνοντας USB συσκευές αποθήκευσης που περιέχουν κακόβουλο λογισμικό, σε στρατηγικές τοποθεσίες, έτσι ώστε με την χρήση τους να εγκατασταθεί ένα πρόγραμμα Δούρειος ίππος (backdoor), στην υποδομή πληροφορικής του στοχοποιημένου έξυπνου δικτύου
- Αποστολή ηλεκτρονικών μηνυμάτων ηλεκτρονικού "ψαρέματος" (phishing), που στοχεύουν σε ευαίσθητες πληροφορίες, όπως πληροφορίες πελατών. Σήμερα, υπάρχουν πολλά κοινωνικά δίκτυα (π.χ. επαγγελματικά δίκτυα), που καθιστούν πολύ πιο εύκολο αυτό το έργο

7.1.6 Φυσική ασφάλεια

Οι επιχειρήσεις κοινής ωφελείας, μπορούν να έχουν χιλιάδες χιλιόμετρα ηλεκτρικών γραμμών που θα μπορούσαν να είναι επιρρεπείς σε φυσικές επιθέσεις. Αυτό ισχύει ιδιαίτερα για τα έξυπνα δίκτυα, όπου η ηλεκτρική ενέργεια παράγεται από ένα συνδυασμό κατανεμημένων ενεργειακών πόρων που βασίζονται σε ανανεώσιμες πηγές ενέργειας και συμβατικές μονάδες παραγωγής ενέργειας. Εκτός αυτού, τα δίκτυα διανομής τείνουν να είναι δίκτυα σε μορφή πλέγματος, ώστε να υποστηρίζουν την έξυπνη αναδρομολόγηση της ηλεκτρικής ισχύος. Ομοίως, έξυπνοι μετρητές θα εγκατασταθούν στα σπίτια και τις επιχειρήσεις των πελατών. Ως εκ τούτου, η ενίσχυση της υποδομής πληροφοριών του έξυπνου δικτύου είναι μερικές φορές μια δύσκολη πρόκληση λόγω του εκτεταμένου δικτύου πελατών και του μεγάλου αριθμού τμημάτων από τα οποία αποτελείται. Για παράδειγμα, μία εφαρμογή μπορεί να κάνει λίγα πράγματα για να αποτρέψει ένα άτομο που έχει σκοπό να κόψει μια γραμμή μεταφοράς ή να παραβιάσει έναν έξυπνο μετρητή. Ως εκ τούτου, η φυσική ασφάλεια και η ασφάλεια στον κυβερνοχώρο, θα πρέπει να αντιμετωπίζονται με έναν ολοκληρωμένο τρόπο.

7.1.7 Κοινή χρήση πληροφοριών

Ο κλάδος της ηλεκτρικής ενέργειας δεν διαθέτει αποτελεσματικούς μηχανισμούς για την ανταλλαγή και τη διαχείριση πληροφοριών σχετικά με τα περιστατικά ασφάλειας στον κυβερνοχώρο. Δεν διαθέτει αποτελεσματικό μηχανισμό για την εξαγωγή πληροφοριών σχετικά με ευπάθειες, περιστατικά, απειλές, διδάγματα και βέλτιστες πρακτικές σχετικά με την ασφάλεια των ευφυών δικτύων στον κυβερνοχώρο. Επιπλέον, σε ορισμένες περιοχές, όπως οι ΗΠΑ, το υφιστάμενο ρυθμιστικό περιβάλλον συμβάλλει κατά κάποιο τρόπο στη δημιουργία μιας νοοτροπίας συμμόρφωσης, αντί μιας κουλτούρας που επικεντρώνεται στην επίτευξη μιας ολοκληρωμένης και αποτελεσματικής ασφάλειας στον κυβερνοχώρο. Από την άποψη αυτή και εξαιτίας του ανωριμότητας της βιομηχανίας όσον αφορά την ασφάλεια στον κυβερνοχώρο, οι πωλητές και οι φορείς εκμετάλλευσης εφαρμόζουν ελέγχους ασφαλείας χρησιμοποιώντας ποικίλα πρότυπα σε συνδυασμό με δικούς του, ο

καθένας, μηχανισμούς. Αυτό οδηγεί σε προβληματική διαλειτουργικότητα, έλλειψη πραγματικής ασφάλειας, ακόμη και σε ανάδυση δυσκολιών στην διαχείριση των θεμάτων ασφάλειας.

7.1.8 Εκπαίδευση και κατάρτιση

Είναι απαραίτητο να τονιστεί ότι οι καταναλωτές και οι επιχειρήσεις κοινής ωφέλειας δεν ενημερώνονται επαρκώς σχετικά με τα οφέλη, το κόστος και τους κινδύνους που συνδέονται με τα συστήματα έξυπνων δικτύων. Αυτή η έλλειψη συνειδητοποίησης μπορεί να οδηγήσει σε έλλειψη των απαραίτητων επενδύσεων, δημιουργίας προτύπων, ρυθμιστικές και πολιτικές πρωτοβουλίες, κλπ. Συνεπώς, πρέπει να ενθαρρυνθεί η εκπαίδευση και η κατάρτιση μαζί με πρωτοβουλίες ευαισθητοποίησης, ώστε να δημιουργηθεί η απαραίτητη δυναμική για την εξέλιξη και την πλήρη ανάπτυξη ασφαλών έξυπνων δικτύων.

7.2 Κίνδυνοι σε περιβάλλον Smart Grid

Οι επιθέσεις στα έξυπνα δίκτυα στον κυβερνοχώρο είναι αναμφισβήτητα οι πιο συζητημένες επιθέσεις, λόγω των τρωτών σημείων της υποδομής στις ψηφιακές επιθέσεις. Οι επιθέσεις αυτές, είναι ικανές να οδηγήσουν το σύστημα σε πλήρη κατάρρευση, αν δεν προστατεύεται σωστά.

Ένας αριθμός σημαντικών τρωτών σημείων του Smart Grid έχουν εντοπιστεί.

Οποιαδήποτε σημαντική επίθεση είναι ικανή να παραπλανήσει τις επιχειρήσεις κοινής ωφέλειας, να τις οδηγήσει να πάρουν λανθασμένες αποφάσεις σχετικά με τη χρήση και την ικανότητα του δικτύου, καθώς και να τις «τυφλώσει» από το να αντιληφθούν τα επικείμενα προβλήματα ή τις επί τόπου επιθέσεις.

Η εμπιστευτικότητα, ο έλεγχος ταυτότητας και η προστασία της ιδιωτικότητας των δεδομένων που είναι κρίσιμα για την αξιοπιστία και την αποτελεσματικότητα του δικτύου πρέπει να διασφαλίζονται ώστε να αποφεύγονται μη εξουσιοδοτημένες τροποποιήσεις μέσω της υποδομής.

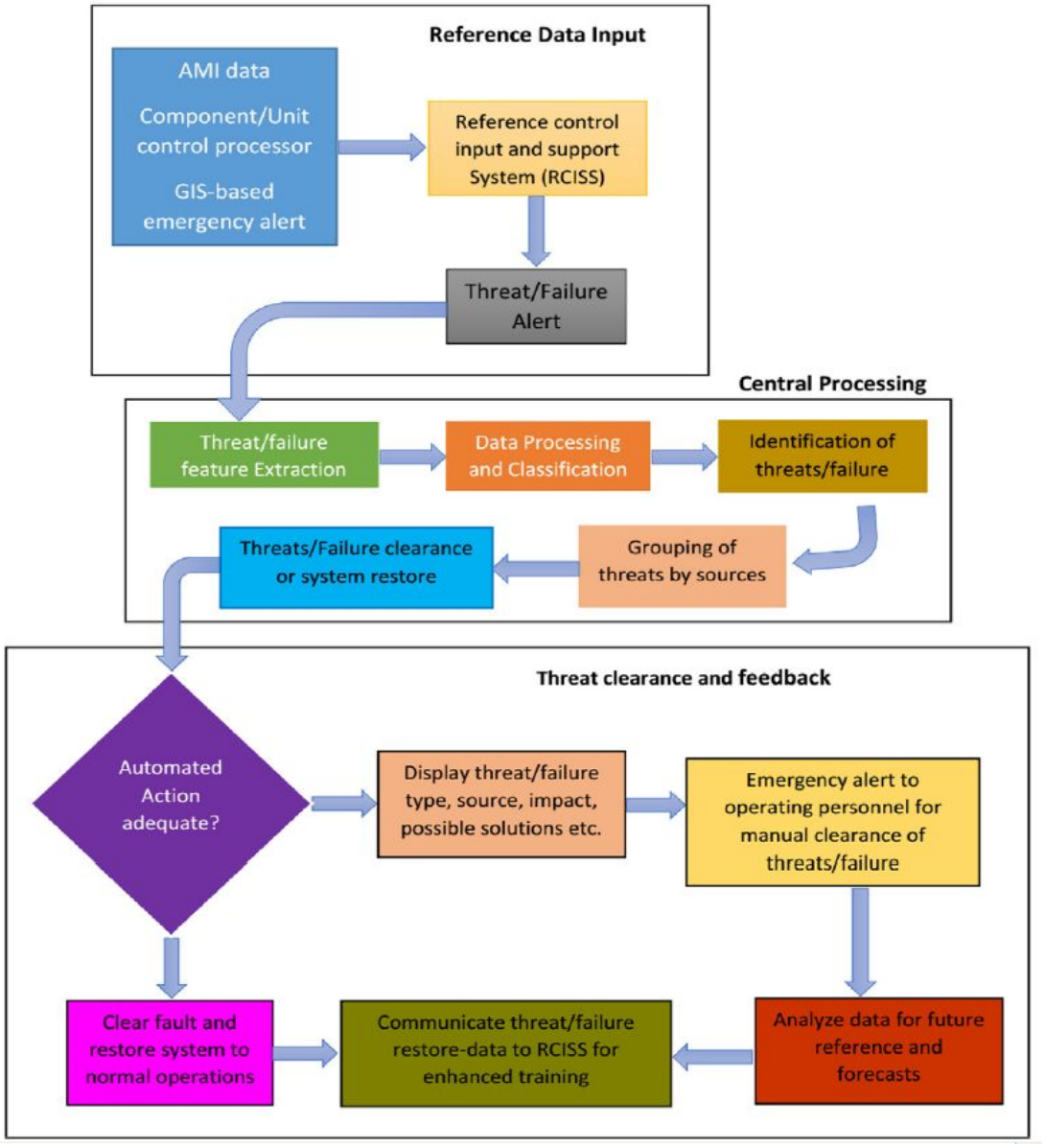
Παραδείγματα αξιοσημείωτων επιθέσεων στον κυβερνοχώρο είναι οι εκθέσεις για τις επιθέσεις στον κυβερνοχώρο στο δίκτυο των αμερικανικών συστημάτων ηλεκτροπαραγωγής, όταν λέγεται οτι έχουν διεισδύσει κατάσκοποι, από την Εσθονία, τη Γεωργία, τη Λιθουανία, την Κιργισία, το Καζακστάν και το Ηνωμένο Βασίλειο έχουν επίσης στοχευθεί. Οι εκθέσεις για επιθέσεις στον κυβερνοχώρο αφθονούν σε διάφορες πτυχές των υποδομών σε όλο τον κόσμο. Τα κατανεμημένα συστήματα ασφαλείας στον κυβερνοχώρο έχουν σχεδιαστεί για να παρακολουθούν την αρχιτεκτονική στη διατήρηση της ακεραιότητας των δεδομένων. Ενώ η φυσική καταστροφή από σκόπιμη ή μη σκόπιμη ενέργεια, η κλοπή υποδομών και η κλοπή ηλεκτρικής ισχύος, αποτελούν κοινές απειλές για τη λειτουργία και την ασφάλεια των SG, οι ανησυχίες των πελατών είναι η πιθανή παραβίαση της ιδιωτικής ζωής και ο κακόβουλος έλεγχος προσωπικών συσκευών. Η ανάπτυξη του Power Meter της Google, ικανή να λαμβάνει στατιστικά στοιχεία κατανάλωσης ενέργειας σε πραγματικό χρόνο, παρέχοντας πρόσβαση μέσω μιας προσαρμογής σε απευθείας σύνδεση με μία διαδικτυακή σελίδα για την ανάλυση και την παρακολούθηση του μοτίβου της καθημερινής τους κατανάλωσης, έχει ωθήσει τους πελάτες να

αναθεωρήσουν περαιτέρω την ασφάλεια των δεδομένων κατανάλωσης ενέργειας, που μπορούν να αποκαλύψουν περαιτέρω τις δραστηριότητές τους στους επικείμενους εγκληματίες στον κυβερνοχώρο. Για παράδειγμα, μπορούν να εκμεταλλευτούν κακώς ρυθμισμένα τείχη προστασίας για να εισάγουν κακόβουλα δεδομένα στις μονάδες ελέγχου. Οι επιθέσεις στον κυβερνοχώρο μπορούν να οδηγήσουν σε καταστροφικές συνέπειες, οι οποίες θα μπορούσαν να οδηγήσουν σε κατάρρευση της υποδομής και σε διαταραχές της οικονομίας, καθώς η βασική υποδομή βασίζεται στην παροχή ηλεκτρικού ρεύματος.

Οι έρευνες επικεντρώνονται στον τρόπο με τον οποίο μπορούν να μετριαστούν αυτές οι επιθέσεις. Βασίζονται τώρα στην παροχή μετρητών-bots, κατανεμημένων επιθέσεων DoS, καταγραφή χρήσης, rootkits SM, anti-virus για βελτιωμένη ασφάλεια. Το US DOE και η βιομηχανία ηλεκτρικής ενέργειας έχουν επενδύσει από κοινού μεταξύ του 2009 και του 2015, 7 δισεκατομμύρια δολάρια σε έργα εκσυγχρονισμού συστημάτων για την εφαρμογή των SG, τη βελτίωση της ασφάλειας στον κυβερνοχώρο και τη βελτίωση της διαλειτουργικότητας. Για την κάλυψη του σχεδίου ανάπτυξης από το 2012 έως το 2017, το κόστος της ασφάλειας του Global Smart Grid στον κυβερνοχώρο αναμένεται να φθάσει τα 1,8 δισεκατομμύρια δολάρια το 2017 και αντίστοιχα τα 3,2 δισεκατομμύρια δολάρια το 2026.

Στο εννοιολογικό πλαίσιο που παρουσιάζεται στο Σχήμα 7 παρουσιάζεται μια ολιστική άποψη, με βάση την προέλευση των απειλών, για την αναγνώριση και την εκκαθάριση της ανιχνευθείσας απειλής. Το πλαίσιο αυτό επικεντρώνεται εξ ολοκλήρου στη χρήση της τεχνικής εντοπισμού απειλών στην πηγή τους, για ένα περιεκτικό, αν και περίπλοκο, αλλά πιο αποτελεσματικό μέσο για την καταπολέμηση των κινδύνων που παρουσιάζονται από τις εντοπισθείσες απειλές. Όπως υποδηλώνεται με έντονα γράμματα στο σχήμα, στην είσοδο αναφοράς (Reference Data Input), οι προειδοποιήσεις από τα δεδομένα AMI, τους αισθητήρες ή το σύστημα που βασίζεται στο GIS, διασταυρώνονται με τη μονάδα συστήματος ελέγχου και υποστήριξης για τον προσδιορισμό κάθε απειλής. Στο κεντρικό στάδιο επεξεργασίας, το οποίο θα μπορούσε να είναι ανάλογο με ένα κέντρο ελέγχου, τα αναγκαία χαρακτηριστικά που απαιτούνται εξάγονται από τα δεδομένα,

ταξινομούνται, αναγνωρίζονται και ομαδοποιούνται για την αποτελεσματική εκκαθάριση και αποκατάσταση του συστήματος. Το στάδιο εκκαθάρισης απειλών ανάδρασης φροντίζει για τα δεδομένα εξόδου και παρέχει δεδομένα για περαιτέρω ανάλυση και εισαγωγή αναφοράς στο Σύστημα Ελέγχου Αναφοράς και Υποστήριξης (RCISS). Αυτό το σύστημα δεν μπορεί να καταγραφεί αποκλειστικά για όλες τις περιπτώσεις πριν από τις επιχειρήσεις ή σε μία μόνο λειτουργία, αλλά περιλαμβάνει την ευφυή συλλογή και ανάλυση δεδομένων με την πάροδο του χρόνου. Ως εκ τούτου, το προτεινόμενο πλαίσιο είναι ανοιχτό σε περαιτέρω τροποποιήσεις και βελτιώσεις καθώς περνά ο καιρός.



Σχ. 13 Εννοιολογικό πλαίσιο για την ταυτοποίηση και την εκκαθάριση των απειλών ασφάλειας σε Smart Grid βασισμένο στις πηγές των απειλών

Σε ένα σύστημα ευέλικτου δικτύου, η έγκαιρη αναγνώριση και διάγνωση των προβληματικών συνθηκών αποτελούν βασικούς παράγοντες για την πρόληψη της διάδοσης των προβλημάτων. Αυτό γίνεται με τη χρήση πρακτικής προσέγγισης, αναλυτικών εργαλείων και τεχνολογιών που βασίζονται στις εξελίξεις στους τομείς του υπολογισμού (computation), του ελέγχου και των επικοινωνιών για την παροχή λύσεων για δίκτυα ηλεκτρικής ενέργειας και άλλες υποδομές οι οποίες αυτορυθμίζονται και αναδιαρθρώνονται αυτόματα, τοπικά, σε περίπτωση αποτυχίας, απειλής ή προβλήματος, ώστε να είναι αδιάλειπτη η λειτουργία τους. Επειδή τα σφάλματα μπορούν επίσης να συμβούν λόγω αστοχίας των προστατευτικών διατάξεων, υπάρχει ανάγκη σχεδιασμού του συστήματος για αυτοθεραπεία με την εξασφάλιση αποδεκτού επιπέδου ανοχής σφάλματος και παροχή απαιτούμενης πλεονασμού για την επίτευξη αξιόπιστης επιχειρησιακής ασφάλειας. Η βασική αρχή πίσω από τον αυτοθεραπεία και τον κατανεμημένο έλεγχο ενός συστήματος ηλεκτρικής ενέργειας περιλαμβάνει τη αντιμετώπιση των επιμέρους συστατικών ως ανεξάρτητων ευφυών παραγόντων με την ενσωμάτωση ενός επεξεργαστή σε κάθε ένα από τα συστατικά στοιχεία του υποσταθμού που αλληλεπιδρούν, παρακολουθούν και συνεργάζονται, για την επίτευξη της βέλτιστης λειτουργίας. Ο σχεδιασμός περιλαμβάνει τη μοντελοποίηση, τον υπολογισμό, την ανίχνευση και τον έλεγχο.

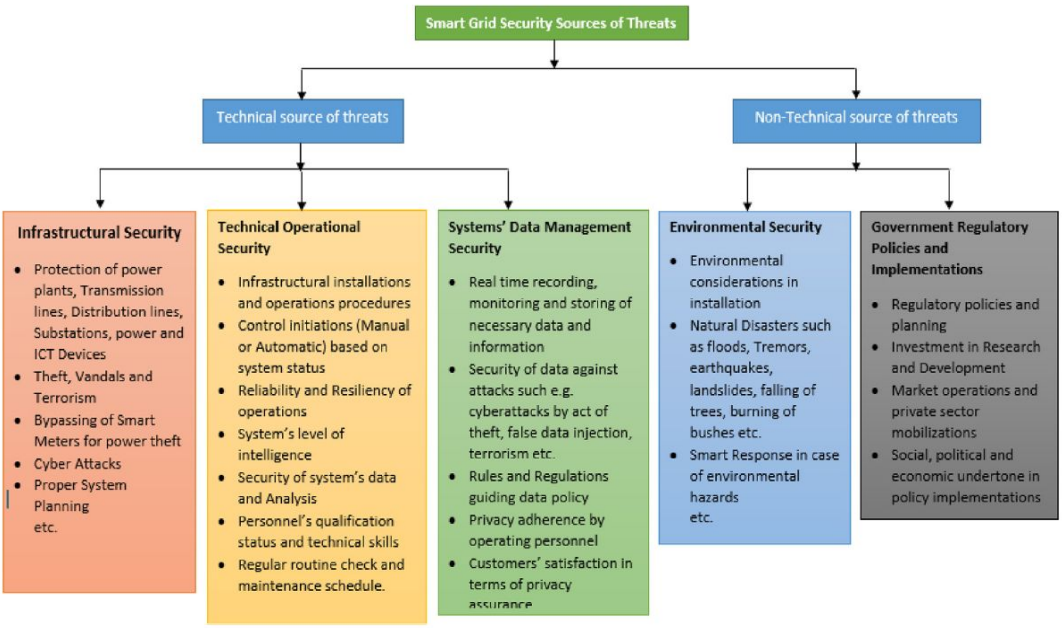


Fig. 4. Classification of SG threats by sources.

Σχ. 14 Κατηγοριοποίηση απειλών σε Smart Grid, ανάλογα με την πηγή

Αυτή η πτυχή καλύπτει την καταγραφή, παρακολούθηση και αποθήκευση σε πραγματικό χρόνο των απαραίτητων δεδομένων και πληροφοριών, την ασφάλεια των δεδομένων από επιθέσεις, τους κανόνες και τους κανονισμούς που καθοδηγούν την πολιτική δεδομένων, την τήρηση της εμπιστευτικότητας από το επιχειρησιακό προσωπικό, την ικανοποίηση των πελατών όσον αφορά τη διασφάλιση της εμπιστευτικότητας, κλπ. Τα κρίσιμα δεδομένα των μεταδόσεων, των δικτύων διανομής, τα χαρακτηριστικά φορτίου των καταναλωτών και οι παράμετροι απόδοσης, καθώς και τα χαρακτηριστικά του εξοπλισμού ελέγχου τους, πρέπει να συλλέγονται, να αναλύονται και να προσομοιώνονται, ώστε να αξιολογείται η αξιοπιστία και το επίπεδο συντήρησης των συστημάτων ώστε να είναι δυνατός ο σχεδιασμός νέων εγκαταστάσεων και αναβαθμίσεων. Οι αυξανόμενες ανησυχίες σχετικά με τις δυνατότητες παραβίασης της εμπιστευτικότητας από τις εταιρείες κοινής ωφέλειας στην ενδεχόμενη αποκάλυψη των δεδομένων των πελατών αποτελεί μείζονα ανησυχία για τους πελάτες. Παρόλο που οι έξυπνοι μετρητές έχουν αλλάξει τη φύση (και πιθανότατα τον όγκο), στις απάτες ή τις επιθέσεις δεδομένων, η παραβίαση του έξυπνου μετρητή με απομακρυσμένη διείσδυση και ο έλεγχος των εγγεγραμμένων και αποθηκευμένων δεδομένων, μπορεί να αποτελέσει πηγή πολύ εξελιγμένων επιθέσεων ικανών να επιτρέψουν ξεχωριστές αλλαγές στις χρήσεις του

πελάτη και παραπλάνηση με στόχο τα θύματα ή ανάλογα με την πρόθεση των επιτιθέμενων, να ξεκινήσουν επιθέσεις μεγάλης κλίμακας στον κύριο όγκο του δικτύου.

Τα πρότυπα τεχνολογίας είναι απαραίτητα ώστε τα προϊόντα να μπορούν να διαλειτουργούν και οι επιχειρήσεις να μπορούν να διανέμουν τα προϊόντα τους σε πολλές χώρες ή περιφέρειες. Οι οικονομίες κλίμακας, που δημιουργεί η τυποποίηση, μπορούν να μειώσουν το κόστος, το οποίο ωφελεί όλους. Και επειδή περισσότεροι πωλητές μπορούν να συμμετέχουν σε μια αγορά, οι πελάτες έχουν περισσότερες επιλογές προϊόντων. Επίσης, όταν μια τεχνολογία είναι τυποποιημένη, οι πελάτες μπορούν να έχουν περισσότερη εμπιστοσύνη οτι τα προϊόντα τους θα λειτουργήσουν όπως αναμενόταν.
Η Ένωση Προτύπων IEEE έχει αναπτύξει ή έχει υπό ανάπτυξη, περισσότερα από 100 πρότυπα έξυπνων δικτύων και αυτά θα υποστηρίξουν ένα ευρύ φάσμα τεχνολογιών και υπηρεσιών που θα χρησιμοποιηθούν σε ένα σύστημα έξυπνου δικτύου. Πολλοί άλλοι περιφερειακοί και διεθνείς οργανισμοί ανάπτυξης προτύπων δημιουργούν επίσης πρότυπα έξυπνων δικτύων. Το IEEE και άλλες κορυφαίες ομάδες συνεργάζονται σε πρότυπα έξυπνων δικτύων επειδή αναγνωρίζουν ότι η συνεργασία είναι απαραίτητη για να εξασφαλιστεί η επιτυχία του έξυπνου δικτύου.
Αυτός ο τύπος συνεργασίας αντιπροσωπεύει ένα παράδειγμα στην ανάπτυξη προτύπων σήμερα. Η συνεργασία θεωρείται πρακτικό μέσο επίλυσης προβλημάτων που είναι κοινά σε όλες τις συμμετέχουσες ομάδες και ενδιαφερόμενα μέρη, ανεξάρτητα από το τυπικό καθεστώς ενός συγκεκριμένου προτύπου σε μια βιομηχανία ή χώρα.

Η ασφάλεια, η οποία περιλαμβάνει την προστασία της ιδιωτικής ζωής και του κυβερνοχώρου, είναι απαραίτητη για την αξιόπιστη λειτουργία των δικτύων και την αποδοχή των έξυπνων δικτύων από τους πελάτες, ενώ πολλοί στην IEEE και στην κοινότητα των έξυπνων δικτύων αναπτύσσουν τεχνολογίες και πρότυπα που αντιμετωπίζουν αυτό το ζήτημα. Αυτό που είναι πολύ σημαντικό, ωστόσο, είναι ότι η ασφάλεια ενσωματώνεται στην αρχιτεκτονική και τα σχέδια από την αρχή, όχι ως μια δεύτερη σκέψη. Στα microgrids, χρησιμοποιούνται τεχνολογίες ασφαλείας για κάθε

συστατικό εξοπλισμού που χρησιμοποιείται και για κάθε εφαρμογή πελάτη που αναπτύσσεται - και αυτό γίνεται με τρόπο που δεν μπορεί να αντιστραφεί. Χρησιμοποιείται μια αρχιτεκτονική που δεν μπορεί να καταρρεύσει. Αν κάποιο τμήμα του συστήματος υποστεί βλάβη, το σύστημα επαναπροσδιορίζεται για να προστατευθεί, να εντοπίσει και να αποτρέψει τις επιθέσεις.

8 Smart Grid και καλές πρακτικές

8.1 Smart Grid και καλές πρακτικές

8.1.1 Στοιχεία των υποδομών AMI - Ελάχιστες απαιτήσεις ασφάλειας

Με βάση τις εργασίες που πραγματοποιήθηκαν στο πλαίσιο της Ομάδας Συντονισμού Έξυπνων Μετρητών (Smart Metering Co-ordination Group, SM-CG), στην οποία συγκεντρώθηκαν οι απαιτήσεις ασφάλειας ορισμένων μεγάλων κρατών μελών της Ε.Ε., αναπτύχθηκε ένα γενικό σύνολο ελάχιστων απαιτήσεων που ισχύουν για τα περισσότερα από τα ευρωπαϊκά κράτη μέλη.

Το πεδίο εφαρμογής αυτών των απαιτήσεων είναι οποιαδήποτε Υποδομή Προηγμένων Μετρήσεων (Advanced Metering Infrastructure, AMI), ακολουθώντας την αρχιτεκτονική που ορίζεται στην έκθεση της SM-CG "Αρχιτεκτονική λειτουργικής αναφοράς για επικοινωνίες σε συστήματα έξυπνης μέτρησης". Οι απαιτήσεις καλύπτουν όλα τα εξαρτήματα από τους Έξυπνους Μετρητές (Smart Meters) μέχρι τα Συστήματα Αιχμής – Head End (ένα σύστημα Head End, είναι το υλικό και το λογισμικό που λαμβάνει τη ροή δεδομένων μετρητών που επιστρέφουν στην υπηρεσία κοινής ωφέλειας, μέσω των AMI. Τα συστήματα Head End, μπορούν να εκτελέσουν περιορισμένο αριθμό επικυρώσεων δεδομένων πριν από τη διάθεση των δεδομένων σε άλλα συστήματα για να ζητήσουν ή να προωθήσουν τα δεδομένα σε άλλα συστήματα.).

Σχ. 15 Έξυπνος Μετρητής (Smart Meter)

Στόχοι

Οι απαιτήσεις που ορίζονται μπορούν να χρησιμεύσουν ως βάση για τις ειδικές απαιτήσεις των κρατών μελών. Οι συγκεκριμένες αυτές απαιτήσεις βασίζονται σε ανάλυση κινδύνου (Risk Analysis), που αξιολογεί την τοπική κατάσταση, οπου λαμβάνονται υπόψη τα συγκεκριμένα στοιχεία και παράγοντες.

Διαδικασία

Η διαδικασία καθορισμού των ελάχιστων απαιτήσεων ξεκίνησε με τη συγκέντρωση της συνολικής δέσμης απαιτήσεων που συγκεντρώθηκαν στο αποθετήριο SM-CG. Οι κατηγορίες ομαδοποίησης προέκυψαν από τα κοινά κριτήρια (Common Criteria). Η συγκέντρωση αυτών των απαιτήσεων δείχνει οτι για πολλές κοινές απαιτήσεις τα κράτη μέλη της Ε.Ε. χρησιμοποιούν διαφορετικά συστήματα ονομασίας. Επιπλέον, η

ιεράρχηση των ειδικών απαιτήσεων εξαρτάται σε μεγάλο βαθμό από το κράτος μέλος. Οι αναγνωρισμένες κατηγορίες ομαδοποίησης, είναι:

- Ειδοποίηση ασφαλείας (Security Notification)
- Ασφαλής επικοινωνία (Secure Communication)
- Κρυπτογραφική Υποστήριξη (Cryptographic Support)
- Έλεγχος πρόσβασης (Access Control)
- Προστασία δεδομένων (Data Protection)
- Αυτοπροστασία (Self-Protection)
- Διαχείριση Ασφαλείας (Security Management)

Αυτές οι κατηγορίες είναι μοναδικά συνδεδεμένες με τις κατηγορίες λειτουργικών απαιτήσεων των κοινών κριτηρίων.

Η αναφορά της SM-CG σχετικά με αυτή τη διαδικασία και τα αποτελέσματά της στο επικαιροποιημένο αποθετήριό της και στην έκθεση του 2015 της ομάδας εργασίας "Privacy and Security".

8.1.2 Σύνοψη των απαιτήσεων

A: Όλα τα στοιχεία AMI ΠΡΕΠΕΙ να παρέχουν ένα ημερολόγιο συμβάντων ασφαλείας

B: Όλες οι ανταλλαγές δεδομένων ΠΡΕΠΕΙ να πραγματοποιούνται με ασφαλή τρόπο (από άκρο σε άκρο)

C: Η διαθεσιμότητα του συστήματος (στοιχεία AMI και δίκτυο επικοινωνίας), ΠΡΕΠΕΙ να είναι επαρκής για την εκτέλεση των περιπτώσεων χρήσης που έχει σχεδιαστεί για το σύστημα

D: Ο μηχανισμός κρυπτογράφησης και η διαχείριση των κλειδιών ΠΡΕΠΕΙ να τεκμηριώνονται και να συμμορφώνονται με αναγνωρισμένα και εγκεκριμένα ανοιχτά πρότυπα

E: Κάθε στοιχείο AMI ΠΡΕΠΕΙ να ελέγξει την εξουσιοδότηση οποιασδήποτε οντότητας που ζητεί πρόσβαση σε αυτήν και να παραχωρήσει ή να αρνηθεί την πρόσβαση βάσει του αποτελέσματος αυτού του ελέγχου
F: Τα δεδομένα σε ηρεμία ΠΡΕΠΕΙ να προστατεύονται σε όλα τα εξαρτήματα του συστήματος
G: Τα στοιχεία AMI ΠΡΕΠΕΙ να είναι αναβαθμίσιμα ώστε να ενσωματώνται νέες λειτουργίες ασφαλείας
H: Οι λειτουργίες στα μέρη των AMI ΘΑ ΠΡΕΠΕΙ να περιορίζονται στις προβλεπόμενες επιχειρησιακές περιπτώσεις και ΔΕΝ ΠΡΕΠΕΙ να είναι σε θέση να θέτουν σε κίνδυνο τις λειτουργίες ασφαλείας
I: Τα στοιχεία AMI και το δίκτυο επικοινωνιών ΠΡΕΠΕΙ να προστατεύονται επαρκώς από εξωτερικές ενοχλήσεις ή/και επιθέσεις και ΠΡΕΠΕΙ να αποδείξουν ανθεκτικότητα έναντι επιθέσεων

ΠΡΕΠΕΙ - Αυτή η λέξη (ή οι όροι "ΑΠΑΙΤΕΙΤΑΙ" ή "ΕΙΝΑΙ ΑΠΑΡΑΙΤΗΤΟ"), δηλώνει τις απαιτήσεις που πρέπει να ακολουθούνται αυστηρά για να είναι σύμφωνες με το έγγραφο και από τις οποίες δεν επιτρέπεται καμιά απόκλιση.
ΘΑ ΠΡΕΠΕΙ - Αυτή η λέξη (ή η λέξη "ΣΥΝΙΣΤΆΤΑΙ"), δηλώνει ότι μεταξύ πολλών δυνατοτήτων, συνιστάται ως ιδιαίτερα κατάλληλη, χωρίς να δηλώνει ή να αποκλείει άλλες, ή ότι προτιμάται κάποια συγκεκριμένη κατεύθυνση δράσης αλλά όχι απαραίτητα, ή οτι (στην αντίθετη περίπτωση), μια συγκεκριμένη πιθανή δράση ή κατεύθυνση δράσης είναι μη επιθυμούμενη αλλά δεν απαγορεύεται.
ΙΣΩΣ - δηλώνει οτι η διαδικασία είναι αποδεκτή εντός των απιτήσεων.

Αναλυτικότερα:

A: Όλα τα στοιχεία AMI ΠΡΕΠΕΙ να παρέχουν ένα ημερολόγιο συμβάντων ασφαλείας

Τα στοιχεία AMI είναι εξοπλισμένα με επαρκείς δυνατότητες για:

- να καταγράφουν συνεδρίες επικοινωνίας και να εντοπίζουν τους χρήστες ·

- καταγράφει προσπάθειες για να θέσει σε κίνδυνο την ασφάλεια της συσκευής.
- παροχή συναγερμού για συγκεκριμένα συμβάντα,
- να καταστήσει το ημερολόγιο προσβάσιμο για αξιολόγηση μέσω μιας τυποποιημένης διεπαφής.

Β: Όλες οι ανταλλαγές δεδομένων ΠΡΕΠΕΙ να πραγματοποιούνται με ασφαλή τρόπο (από άκρο σε άκρο)

Προστασία κατά της αναπαραγωγής, αποκάλυψη, τροποποίηση, πλαστοπροσωπία κατά την ανταλλαγή δεδομένων (π.χ. αναγνώσεις, εντολές, συναγερμοί, διαπιστευτήρια κ.λπ.).

Όλες οι ανταλλαγές δεδομένων πρέπει να προστατεύονται κρυπτογραφικά και προαιρετικά επίσης να προστατεύονται φυσικά.

C: Η διαθεσιμότητα του συστήματος (στοιχεία AMI και δίκτυο επικοινωνίας), ΠΡΕΠΕΙ να είναι επαρκής για την εκτέλεση των περιπτώσεων χρήσης που έχει σχεδιαστεί για το σύστημα

Πρέπει να παρακολουθείται η διαθεσιμότητα του συστήματος.

Παρακολουθείται η διαθεσιμότητα των στοιχείων AMI και του δικτύου επικοινωνίας.

Ο διαχειριστής δικτύου επικοινωνιών παρέχει στατιστικά στοιχεία σχετικά με την αξιοπιστία της ανταλλαγής μηνυμάτων στο δίκτυο.

Το σύστημα και τα εξαρτήματά του πρέπει να ξεκινήσουν και να αποκατασταθούν από αποτυχίες με έναν καθορισμένο και ασφαλή τρόπο.

Το σύστημα πρέπει να σχεδιάζεται κατά τέτοιο τρόπο ώστε, σε περίπτωση αποτυχίας επικοινωνίας, να έχει ελάχιστες επιπτώσεις στη διαθεσιμότητα του συστήματος.

Σε περίπτωση βλάβης, τα εξαρτήματα του συστήματος δεν πρέπει να θέτουν σε κίνδυνο τη δική τους ασφάλεια ή ασφάλεια άλλων εξαρτημάτων του AMI.

Τα μέτρα προστασίας λογισμικού περιλαμβάνονται στη διαδικασία σχεδιασμού (π.χ. εφαρμόζοντας τους κανόνες MISRA).

D: Ο μηχανισμός κρυπτογράφησης και η διαχείριση των κλειδιών ΠΡΕΠΕΙ να τεκμηριώνονται και να συμμορφώνονται με αναγνωρισμένα και εγκεκριμένα ανοιχτά πρότυπα

Η περιγραφή των μηχανισμών κρυπτογράφησης και της διαχείρισης κλειδιού θα είναι διαθέσιμη στο κοινό (βάσει ανοικτών προτύπων).
Οι μηχανισμοί που παρέχουν κρυπτογράφηση και έλεγχο ταυτότητας θεωρούν την συνιστώμενη NIST (ή NSA, ακολουθία Β), κρυπτογραφία κατάλληλη για εφαρμογές AMI:

- Κρυπτογραφικοί αλγόριθμοι
- Μήκος κλειδιού και υπογραφής
- Πιστοποίηση πελάτη "ή" διακομιστή
- Προδιαγραφή της εντροπίας
- Δημιουργία κρυπτογραφικών τυχαίων αριθμών
- Αποθήκευση κλειδιών

F: Τα δεδομένα σε ηρεμία ΠΡΕΠΕΙ να προστατεύονται σε όλα τα εξαρτήματα του συστήματος

Η προστασία αφορά μη εξουσιοδοτημένη αποκάλυψη και τροποποίηση.
Παρέχονται διαφορετικά επίπεδα προστασίας, ανάλογα με την κατηγορία εφαρμογής των δεδομένων. Οι κατηγορίες περιλαμβάνουν:

- Πιστοποιημένα δεδομένα Μέτρησης (π.χ. κατανάλωση, προδιαγραφές)
- Πιστοποιητικά
- Διαμόρφωση
- Firmware

Τα παρωχημένα δεδομένα πρέπει να διαγράφονται οριστικά.

G: Τα στοιχεία AMI ΠΡΕΠΕΙ να είναι αναβαθμίσιμα ώστε να είναι δυνατή η ενσωμάτωση νέων λειτουργιών ασφαλείας

Η λειτουργικότητα ασφαλείας στα στοιχεία AMI πρέπει να ενημερώνεται (διορθώσεις σφαλμάτων), και να αναβαθμίζεται (πρόσθετες λειτουργίες).
Τα στοιχεία AMI πρέπει να επιτρέπουν την εφεδρική χωρητικότητα (μνήμη και επεξεργαστική ισχύς), για ενημερώσεις και αναβαθμίσεις.
Η ακεραιότητα και η αυθεντικότητα των εικόνων ενημέρωσης πρέπει να επαληθεύονται πριν εφαρμοστούν ή ενεργοποιηθούν.

Η: Οι λειτουργίες στα μέρη των AMI ΘΑ ΠΡΕΠΕΙ να περιορίζονται στις προβλεπόμενες επιχειρησιακές περιπτώσεις και ΔΕΝ ΠΡΕΠΕΙ να είναι σε θέση να θέτουν σε κίνδυνο τις λειτουργίες ασφαλείας

Οι διασυνδέσεις που δεν χρησιμοποιούνται πρέπει να απενεργοποιούνται.

Οι απενεργοποιημένες λειτουργίες των μερών των AMI δεν πρέπει να θέτουν σε κίνδυνο τις λειτουργίες ασφαλείας.

Το σύστημα να έχει σχεδιαστεί με τέτοιο τρόπο ώστε τα μπλοκ λειτουργικότητας να μην παρεμποδίζουν τις λειτουργίες ασφαλείας με ακούσιο τρόπο.

Ι: Τα στοιχεία AMI και το δίκτυο επικοινωνιών ΠΡΕΠΕΙ να προστατεύονται επαρκώς από εξωτερικές ενοχλήσεις ή/και επιθέσεις και ΠΡΕΠΕΙ να αποδείξουν ανθεκτικότητα έναντι επιθέσεων

Οι διαταραχές και οι επιθέσεις μπορεί να είναι:

- Παραβίαση
- Ηλεκτρομαγνητική υπερφόρτωση (ElectroMagnetic Charge, EMC)
- Πρόβλημα ρολογιού ή ημερομηνίας ή αλλαγής ώρας
- Άρνηση Παροχής Υπηρεσίας (DoS)

8.1.3 Βέλτιστες πρακτικές υπηρεσιών κοινής ωφέλειας και προκλήσεις

Πολλές υπηρεσίες κοινής ωφέλειας κατανοούν τη σημασία της ασφάλειας στον κυβερνοχώρο και έχουν αναπτύξει ή αναπτύσσουν μια βασική γραμμή για τις τεχνικές πρακτικές. Συγκεκριμένα, η αναβάθμιση στο έξυπνο δίκτυο στις Η.Π.Α. απαιτούσε υπηρεσίες κοινής ωφέλειας για την εφαρμογή νέων τεχνικών πρακτικών για την προστασία ενός ευάλωτου συνδυασμού επικοινωνίας, πληροφορικής και OT καθώς και για την προστασία της ιδιωτικότητας των πελατών. Η αρχιτεκτονική λογισμικού έξυπνου δικτύου που αναπτύχθηκε ή βοήθησε στην ανάπτυξη από επιχειρήσεις κοινής ωφέλειας, όπως το Ασφαλές Κοινό Επιχειρησιακό Περιβάλλον (Secure Common Operating Environment, SCOE), χρησιμοποιήθηκε για να συνδέσει την ασφάλεια στον κυβερνοχώρο με τεχνολογίες έξυπνων δικτύων. Επιπλέον, η

αναβάθμιση του έξυπνου δικτύου δεν απαιτεί μόνο ισχυρή ασφάλεια στον κυβερνοχώρο, αλλά θα πρέπει να ενσωματώσει την φυσική ασφάλεια - αυτή που παρέχει προστασία στο προσωπικό, το υλικό, τα προγράμματα, τα δίκτυα και τα δεδομένα από μη εξουσιοδοτημένη φυσική διαχείριση. Σε αυτόν τον τομέα, ορισμένα προγράμματα κοινής ωφέλειας έχουν αρχίσει να εξασφαλίζουν αλυσίδες εφοδιασμού για τη μείωση της ευπάθειας στον εξοπλισμό που παρέχεται από τον προμηθευτή.
Για να συμπληρωθούν οι βέλτιστες τεχνικές και φυσικές πρακτικές, οι επιχειρήσεις κοινής ωφέλειας συμμετέχουν όλο και περισσότερο σε εταιρικές σχέσεις δημόσιου και ιδιωτικού τομέα, αναπτύσσοντας και εφαρμόζοντας ολοκληρωμένα πλαίσια, αναδιοργανώνοντας τον τρόπο με τον οποίο αντιμετωπίζονται οι απειλές στον κυβερνοχώρο στη δομή του ανθρώπινου δυναμικού των επιχειρήσεων κοινής ωφέλειας, και καθορίζοντας το επίπεδο οργανισμού που είναι υπεύθυνο για την αντιμετώπιση απειλών στον κυβερνοχώρο και την επίβλεψη του τμήματος διαδικτυακής ασφάλειας. Για παράδειγμα, ο Χάρτης Συντονισμού του Υποτομέα Ηλεκτρικής Ενέργειας (Electricity Sub-Sector Coordinating Council Charter, ESCC) - ένας εθελοντικός οργανισμός που δημιουργήθηκε για να διευκολύνει τον διάλογο και την ανταλλαγή πληροφοριών σχετικά με τις απειλές, τις αδυναμίες, τα περιστατικά και τα προστατευτικά μέτρα στον κυβερνοχώρο (εκτός από άλλα θέματα που ενδιαφέρουν τον υποτομέα), μεταξύ των συμμετεχόντων - επιτρέπει στον υποτομέα ηλεκτρικής ενέργειας να συμμετέχει με τους εθελοντές και την ομοσπονδιακή κυβέρνηση για τις απειλές στον κυβερνοχώρο, την ευελιξία και την ετοιμότητα, μεταξύ άλλων θεμάτων. Τέτοιες πρακτικές υποδεικνύουν οτι οι υπηρεσίες κοινής ωφέλειας αποκτούν όλο και μεγαλύτερη ανταπόκριση στις απειλές στον κυβερνοχώρο και καταβάλλουν προσπάθειες για την ενσωμάτωση προσεγγίσεων στην ασφάλεια.

Τεχνικές πρακτικές

Υπάρχουν διάφορες ειδικές τεχνικές και διοικητικές βέλτιστες πρακτικές για την ασφάλεια στον κυβερνοχώρο που εφαρμόζουν οι επιχειρήσεις κοινής ωφέλειας. Αυτές οι τεχνικές πρακτικές περιλαμβάνουν firewalls δικτύου, λογισμικό προστασίας από ιούς, λογισμικό ελέγχου εφαρμογών, κρυπτογράφηση δεδομένων επικοινωνίας, διασφάλιση αναβαθμίσεων τεχνολογίας έξυπνου δικτύου, συστήματα ανίχνευσης εισβολών κ.λπ.. Πολλές από αυτές τις πρακτικές ήταν αρχικά προσαρμοσμένα σχέδια

ασφάλειας IT και εφαρμόστηκαν σε λογισμικό επιχειρήσεων ηλεκτρικής ενέργειας που ελέγχει το φυσικό OT μιας υπηρεσίας. Μεγάλο μέρος του OT που χρησιμοποιείται σήμερα από επιχειρήσεις κοινής ωφέλειας δεν σχεδιάστηκε με την ασφάλεια του κυβερνοχώρου, θέτοντας την ευθύνη στις εταιρείες κοινής ωφελείας και τους εταίρους να βρουν καινοτόμες πρακτικές και λύσεις για την προστασία του ηλεκτρικού δικτύου. Αυτό ενισχύει την ανάγκη οι επιχειρήσεις κοινής ωφέλειας να εφαρμόζουν διοικητικές πρακτικές για την ενίσχυση των πρακτικών τεχνικής και φυσικής ασφάλειας στον κυβερνοχώρο.

Οι πρώτες γραμμές που χρησιμοποιούνται από τις επιχειρήσεις κοινής ωφέλειας για την προστασία των συστημάτων πληροφορικής από την κακόβουλη δραστηριότητα στον κυβερνοχώρο, είναι δικτυακά τείχη προστασίας. Τα τείχη προστασίας δεν πρέπει μόνο να μπορούν να αποκλείουν εξωτερικές απειλές, αλλά πρέπει επίσης να αποκλείουν και να ελέγχουν την κυκλοφορία σε διαφορετικές εσωτερικές ζώνες του δικτύου και να διαχωρίζουν το δίκτυο σε ξεχωριστές ζώνες εμπιστοσύνης. Τα όρια για αυτές τις ζώνες εμπιστοσύνης είναι ιδιαίτερα σημαντικά για τα δίκτυα κοινής ωφέλειας που συνδυάζουν συστήματα πληροφορικής και τεχνολογίας αιχμής. Ανύπαρκτα ή εύκολα στο να διεισδύσει κανείς, εσωτερικά όρια τείχους προστασίας, επιτρέπουν σε έναν δυνητικό χάκερ εύκολη πρόσβαση σε οποιοδήποτε μέρος των στοιχείων μιας επιχείρησης. Ορισμένα τείχη προστασίας χρησιμοποιούν τώρα ένα σύστημα γνωστό ως βαθύ έλεγχο πακέτων (Deep Packet Inspection, DPI), για να επιθεωρήσει την κυκλοφορία δικτύου που μεταβαίνει προς και από τα συστήματα ελέγχου και αυτοματοποιημένων συστημάτων και εμποδίζει την ακατάλληλη κίνηση. Τα τείχη προστασίας DPI εφαρμόζουν λεπτομερέστερη επιθεώρηση στην κυκλοφορία δικτύου, αντί να εφαρμόζουν απλώς μια παραδοσιακή μέθοδο μαύρης/λευκής λίστας. Πιο συγκεκριμένα, τα τείχη προστασίας DPI μπορούν να χρησιμοποιηθούν για να διαχωρίσουν κακόβουλα μηνύματα δεδομένων από καλοήθη. Αυτό είναι ιδιαίτερα χρήσιμο σε συστήματα SCADA, όπου τα κακόβουλα μηνύματα δεδομένων πρέπει να διαφοροποιούνται από τα μηνύματα ελέγχου ρουτίνας.

Όπως και οι περισσότερες επιχειρήσεις συνειδητής ασφάλειας στον κυβερνοχώρο, πολλά προγράμματα κοινής ωφέλειας εφαρμόζουν κάποιο είδος λογισμικού προστασίας από ιούς σε υπολογιστές συνδεδεμένους σε δίκτυο για να αποτρέψουν τις

παραδοσιακές επιθέσεις στον κυβερνοχώρο. Μια εναλλακτική λύση από το παραδοσιακό λογισμικό προστασίας από ιούς που πολλές εφαρμογές αρχίζουν να εφαρμόζουν ή εξετάζουν είναι η χρήση λογισμικού ασφαλούς ελέγχου εφαρμογών, εάν μπορεί να υποστηριχθεί σε περιβάλλον ICS. Το λογισμικό ελέγχου εφαρμογών επιτρέπει την εκτέλεση ποικιλίας αξιόπιστων εφαρμογών σε ένα σύστημα κρίσιμης υποδομής. Όλες οι άλλες επικίνδυνες εφαρμογές ή υψηλότερου κινδύνου είναι απλά αποκλεισμένες και δεν επιτρέπονται να εκτελούνται στο σύστημα. Αυτό έρχεται σε αντίθεση με την απλή μαύρη λίστα όπου δεν εκτελούνται οι γνωστές επικίνδυνες εφαρμογές και επιτρέπονται όλες οι υπόλοιπες - ακόμη και οι άγνωστες εφαρμογές. Εκτός από την αύξηση της ασφάλειας στον κυβερνοχώρο, οι υπηρεσίες κοινής ωφέλειας έχουν διαπιστώσει οτι ορισμένοι τύποι λογισμικού ελέγχου εφαρμογών μπορούν επίσης να μειώσουν τον αριθμό των απαιτούμενων κύκλων επιδιόρθωσης και να διατηρήσουν τα ρυθμιστικά πρότυπα ασφαλείας για τα βοηθητικά συστήματα.
Μια άλλη κοινή πρακτική που έχουν υιοθετήσει πολλές επιχειρήσεις κοινής ωφέλειας είναι η κρυπτογράφηση δεδομένων, ιδιαίτερα η κρυπτογράφηση δεδομένων επικοινωνίας. Η κρυπτογράφηση έχει χρησιμοποιηθεί από καιρό σε συστήματα πληροφορικής για να αποτρέψει ανεπιθύμητα τρίτα μέρη να παρακολουθούν και να διαβάζουν μηνύματα δεδομένων. Ορισμένες υπηρεσίες κοινής ωφέλειας χρησιμοποιούν σήμερα λογισμικό κρυπτογράφησης για την κρυπτογράφηση των επικοινωνιών SCADA για να αποτρέψουν τους χάκερς να συλλέγουν πληροφορίες σχετικά με τις διαδικασίες ελέγχου του ηλεκτρικού δικτύου. Η κρυπτογράφηση είναι ιδιαίτερα σημαντική για τις υπηρεσίες κοινής ωφέλειας για την προστασία της ασφάλειας των δεδομένων επικοινωνίας των έξυπνων μετρητών. Η εμφάνιση της τεχνολογίας μέτρησης των έξυπνων δικτύων στη Βόρεια Αμερική και σε όλο τον κόσμο κατέστησε την κρυπτογράφηση δεδομένων επικοινωνίας ακόμη μεγαλύτερη προτεραιότητα για τις ηλεκτρικές επιχειρήσεις. Για να διασφαλιστεί η σωστή κρυπτογράφηση, έχουν ήδη αναπτυχθεί κρυπτογραφικά πρωτόκολλα, όπως το IEEExv P1711, για την κρυπτογράφηση πληροφοριών που μεταδίδονται από υποσταθμούς ενέργειας. Μια πρόσφατη έρευνα δείχνει ότι πολλές υπηρεσίες κοινής ωφέλειας κινούνται προς την κατεύθυνση της εφαρμογής κρυπτογράφησης για υποσταθμούς. Από τις υπηρεσίες κοινής ωφέλειας που εξετάστηκαν, το 41% ισχυρίζεται οτι χρησιμοποιεί κρυπτογραφημένα πρωτόκολλα ενώ η πλειονότητα έχει

κρυπτογραφημένα πρωτόκολλα που δραστηριοποιούνται στην επικοινωνία από τον υποσταθμό στον σταθμό ελέγχου, σε αντίθεση για την επικοινωνία από υποσταθμό σε υποσταθμό ή εντός του υποσταθμού.

Εκπαίδευση εργαζομένων για υγιεινή στον κυβερνοχώρο

Οι επιτιθέμενοι στον κυβερνοχώρο ενδέχεται να στοχεύουν τους εργαζόμενους σε υπηρεσίες κοινής ωφέλειας με παραπλανητικές τεχνικές, όπως το phishing να αποκτά πρόσβαση ή πληροφορίες. Σύμφωνα με την έκθεση του Ponemon για την Υποδομή Ζωτικής Σημασίας του 2014, η χρήση προσωπικού προσωπικών συσκευών αντιπροσώπευε το 32% των συγκεκριμένων περιστατικών ασφάλειας που αναφέρθηκαν από τις εταιρείες υποδομής ζωτικής σημασίας που συμμετείχαν στην έρευνα, στη δεύτερη μόνο στη χρήση ανασφαλών δικτύων. Ορισμένες υπηρεσίες κοινής ωφέλειας εκτελούν εκπαίδευση για να εκπαιδεύουν και να ελέγχουν την ευαισθητοποίηση των εργαζομένων στον κυβερνοχώρο και τη σωματική ασφάλεια Για παράδειγμα, η Αρχή Ηλεκτρισμού της Νέας Υόρκης (NYPA) ενημερώνει τους υπαλλήλους της για «συγκεκριμένους κινδύνους και απειλές στον κυβερνοχώρο και για στρατηγικές πρόληψης», όπως η αποφυγή χρήσης USB sticks ή παρόμοιων περιφερειακών συσκευών που διανέμονται σε συνέδριο ή άλλους δημόσιους χώρους στον εξοπλισμό της εταιρείας. Ορισμένες υπηρεσίες κοινής ωφέλειας απαιτούν από τους υπαλλήλους να υποβάλλονται σε διαδικτυακή εκπαίδευση, η αποτελεσματικότητα των οποίων αξιολογείται αργότερα με εσωτερική εικονική άσκηση. Ενώ οι τεχνολογικές απολύσεις συνιστώνται γενικά, η κατάρτιση στον τομέα της ασφάλειας στον κυβερνοχώρο, συμπεριλαμβανομένης της φυσικής ασφάλειας, έχει υιοθετηθεί από επιχειρήσεις κοινής ωφέλειας για την άμβλυνση των κινδύνων που παρουσιάζουν οι υπάλληλοί τους.

Ασφάλεια αλυσίδας εφοδιασμού

Κατά την αναβάθμιση και τη μετασκευή εξαρτημάτων του ηλεκτρικού δικτύου, είναι σημαντικό να διασφαλιστεί ότι ο εξοπλισμός αυτός αγοράζεται από έναν αξιόπιστο προμηθευτή με αξιόπιστα προϊόντα. Πολλές εταιρείες κοινής ωφέλειας αφιερώνουν τώρα το χρόνο για να διασφαλίσουν ότι ο αγορασμένος εξοπλισμός προέρχεται από

έναν αξιόπιστο προμηθευτή και ότι το υλικό ή το λογισμικό δεν παρουσιάζουν σημαντικές αδυναμίες ασφαλείας. Ορισμένα βοηθητικά προγράμματα, όπως το SMUD, εξετάζουν το ενδεχόμενο να συνεργαστούν με τους προμηθευτές για να εξασφαλίσουν ότι η ασφάλεια υλικού και λογισμικού είναι υψηλή προτεραιότητα, ακόμη και όσον αφορά τον ορισμό ενός αξιωματικού για να συνεργαστεί με τις επιχειρησιακές γραμμές και για την αξιολόγηση των κινδύνων ασφαλεία;. Καθώς οι επιχειρήσεις κοινής ωφελείας αναβαθμίζονται σε ένα έξυπνο δίκτυο, έχει καταστεί αναγκαίο να εξασφαλιστεί ότι οι πωλητές που πωλούν την τεχνολογία μέτρησης θα εφαρμόσουν τις απαραίτητες προφυλάξεις ασφαλείας, όπως κρυπτογράφηση μετρητών, διαχείριση υλικολογισμικού κλπ.

Μια μέθοδος που σύντομα θα χρησιμοποιηθεί για τη μείωση του κινδύνου για την ασφάλεια στον κυβερνοχώρο τόσο για το υλικό όσο και για το λογισμικό είναι πρότυπα που πιστοποιούν ότι ένα προϊόν που αγοράστηκε από έναν προμηθευτή έχει σχεδιαστεί με ασφάλεια. Βάσει των προτύπων που εφαρμόζονται σήμερα στον κλάδο της πληροφορικής, ορισμένοι οργανισμοί προωθούν την ανάπτυξη προτύπων πιστοποίησης προμηθευτών για την εξασφάλιση προϊόντων ηλεκτρικού δικτύου ελέγχου, όπως η Διεθνής Εταιρεία Αυτοματισμού (ISA), η οποία πρότεινε ένα σύνολο προτύπων γνωστών ως ISA99 . Η χρήση προτύπων όπως αυτά έχουν ήδη εφαρμοστεί για σκοπούς βιομηχανίας πληροφορικής για να πιστοποιήσουν την ασφάλεια των προϊόντων λογισμικού υπολογιστών στο πλαίσιο των κοινών κριτηρίων αξιολόγησης της ασφάλειας τεχνολογίας των πληροφοριών και έχουν συμβάλει σημαντικά στην ενίσχυση της ασφάλειας στον κυβερνοχώρο των δικτύων συστημάτων πληροφορικής. Ως απάντηση σε αυτή την ώθηση, ο FERC, από τον Ιούλιο του 2016, διέταξε τη NERC να αναπτύξει ένα σύνολο προτύπων ασφάλειας της αλυσίδας εφοδιασμού. Αυτή η εντολή FERC αποτελεί ένα ουσιαστικό πρώτο βήμα στην ανάπτυξη προτύπων για τη στήριξη των τρωτών σημείων στην τεχνολογία που αγοράστηκε από τον προμηθευτή και τη βελτίωση της συνολικής ασφάλειας στον κυβερνοχώρο του υλικού και του λογισμικού που επηρεάζονται.

9 Συμπεράσματα και προτάσεις για περαιτέρω έρευνα

Στην ενότητα που ακολουθεί θα γίνει προσπάθεια συνθετικής καταγραφής των στοιχείων που συνελέγησαν και των συμπερασμάτων που βγήκαν, καθώς και μερικών προτάσεων για περαιτέρω έρευνα.

9.1 Συμπεράσματα

Καθώς οι υπηρεσίες έξυπνων δικτύων διευρύνονται, οι συμβατικές υπηρεσίες κοινής ωφέλειας αντιμετωπίζουν ολοένα και περισσότερες προκλήσεις λόγω των νέων τεχνολογιών, των πολιτικών, των αυξανόμενων απαιτήσεων σε ηλεκτρική ενέργεια και των επιχειρηματικών μοντέλων που εμπλέκονται στη μετάβαση στα νέα έξυπνα δίκτυα. Συνεπώς, η εμπλοκή των κυβερνήσεων στην παροχή των απαιτούμενων ρυθμιστικών πολιτικών για την ενίσχυση της ομαλής λειτουργίας της αγοράς και την κινητοποίηση του ιδιωτικού τομέα, είναι καθοριστικής σημασίας για την επίτευξη των καθορισμένων στόχων της ανάπτυξης των έξυπνων δικτύων. Εκτός της απαιτούμενης δέσμευσης των κυβερνήσεων με σωστές πολιτικές υλοποιήσεις, οι τεχνικές, κοινωνικές, πολιτικές, περιβαλλοντικές, νομοθετικές και οικονομικές δεσμεύσεις θα μπορούσαν να αποδειχθούν ένας ικανοποιητικός στρατηγικός παράγοντας για την επίτευξη της επιθυμητής ανάπτυξης,. Τα καθήκοντα των κυβερνήσεων σε αυτό το πλαίσιο πρέπει, επίσης, να περιλαμβάνουν ευαισθητοποίηση του κοινού, δεδομένου οτι οι καταναλωτές είναι βασικοί συντελεστές του ενεργειακού τομέα, καθώς τα καταναλωτικά τους πρότυπα και η συνεργασία τους με τους φορείς εκμετάλλευσης θα προωθήσουν πολύ την επίτευξη ομαλής λειτουργίας. Ως εκ τούτου, οι κυβερνήσεις σε όλα τα επίπεδα πρέπει να παίξουν τον δικό τους ρόλο για να εξασφαλίσουν έγκαιρη πολιτική υποστήριξη και υλοποίηση. Επίσης, έχουν σημαντικό ρόλο στον τομέα των επενδύσεων στην Έρευνα και Ανάπτυξη (Research and Development, RnD). Πρέπει να υπάρξει ένας καλά σχεδιασμένος

οδικός χάρτης, ο οποίος να τηρείται από τις διαδοχικές κυβερνήσεις για να εξασφαλιστεί η συνεκτικότητα στην ανάπτυξη.

9.2 Προτάσεις για περαιτέρω έρευνα

Οι υποδομές ηλεκτρικής ενέργειας είναι δαπανηρές για την προμήθεια και την περιπλοκότητα της εγκατάστασής τους, και ως εκ τούτου απαιτείται μια ολοκληρωμένη πρόβλεψη ασφάλειας για κάθε πιθανή απειλή που θα μπορούσε να οδηγήσει σε αποτυχία οποιασδήποτε μονάδας ή οποιουδήποτε συστήματος, ή ακόμη και να προκαλέσει το φαινόμενο χιονοστιβάδας σε όλη την υποδομή. Συνεπώς, είναι σκόπιμο να αναπτυχθεί ένα ευφυές λειτουργικό σύστημα ασφάλειας όλων των διασυνδεδεμένων στοιχείων για βελτιωμένη ασφάλεια και ανθεκτικότητα.

Κατά τη διάρκεια της παρούσας εργασίας εντοπίστηκαν κάποια στοιχεία, που θα μπορούσαν να αποτελέσουν αντικείμενο περαιτέρω ερευνών.

Αναλυτικότερα, σε αυτή την εργασία, αναφέρθηκαν διάφορες απειλές και προκλήσεις ασφάλειας έξυπνων δικτύων καθώς επίσης και μια ταξινόμηση απειλών που θα μπορούσε να βελτιώνεται και να ενημερώνεται συνεχώς, ώστε να παρέχει ένα καλύτερο μοντέλο για την αντιμετώπιση των θεμάτων ασφάλειας και ευελιξίας ανάλογα με την προέλευση των απειλών.

Εντοπίστηκαν κάποια στοιχεία, που θα μπορούσαν να αποτελέσουν αντικείμενο περαιτέρω ερευνών:

1. Με σωστή επαλήθευση, ανάλυση, προσομοιώσεις και εργαλεία βελτιστοποίησης, το δίκτυο διανομής ενέργειας μπορεί να προσαρμοστεί σε διάφορες συνθήκες. Αυτό θα πρέπει να ληφθεί υπόψη σε μεγάλο βαθμό τόσο στον σχεδιασμό όσο και στο επιχειρησιακό στάδιο για ένα ισχυρό, βελτιστοποιημένο, καλά ασφαλές και ανθεκτικό δίκτυο διανομής ενέργειας (καθώς, η αντίδραση στις απειλές, η προέλευση τέτοιων απειλών, ο αντίκτυπος και ακόμη και η φύση των απειλών, θα

εντοπιστούν εύκολα, κβαντισμένες – όπου είναι δυνατόν – και επεξεργασμένες για αντιμετώπιση επί τόπου, παρακολούθηση και έλεγχο, πολύ πριν από την εμφάνιση των απειλών).

2. Επίσης, απαιτείται εκτεταμένη έρευνα από κυβερνητικούς οργανισμούς, ακαδημαϊκούς, βιομηχανικούς κλάδους, επαγγελματικούς φορείς και συναφείς οργανισμούς για την αξιολόγηση των θεμάτων ασφάλειας των έξυπνων δικτύων με σκοπό την ενίσχυση της εμπιστοσύνης και της ευαισθητοποίησης των πελατών. Ως εκ τούτου, διάφοροι ενδιαφερόμενοι πρέπει να επενδύσουν στην ανάπτυξη των έξυπνων δικτύων, με τα ζητήματα ασφάλειας και ευελιξίας ως προτεραιότητα.
3. Μελλοντικά, μπορεί να εξεταστεί η παροχή κατάλληλων μοντέλων για την αντιμετώπιση των απειλών ασφάλειας των έξυπνων δικτύων με ταξινόμηση των απειλών με βάση την προέλευσή τους, τόσο για την επιθυμητή ευελιξία όσο και για την ανάπτυξη ενός ισχυρού εργαλείου προσομοίωσης απειλών για ανίχνευση και απόκριση, για ένα σταθερό δίκτυο διανομής ενέργειας.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

CEN-CENELEC Sectors, Energy management & energy efficiency, Smart grids, https://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx

CEN-CENELEC Sectors, Energy management & energy efficiency, Smart meters, https://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartMeters/Pages/default.aspx

European Network and Informations Security Agency (ENISA). Critical Information Infrastructures and Services. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems

Ebinger, Charles and Massy, Kevin. Software and hard targets: enhancing Smart Grid cyber security in the age of information warfare. s.l.: http://www.brookings.edu/~/media/Files/rc/papers/2011/02_smart_grid_ebinger/02_smart_grid_ebinger.pdf , 2011.

Gorman, Siobhan. Electricity Grid in U.S. Penetrated By Spies.

Davis, Mike. SmartGrid Device Security. Adventures in a new medium. s.l.: https://www.blackhat.com/presentations/bh-usa-09/MDAVIS/BHUSA09-Davis-AMI-SLIDES.pdf , 2009.

Falliere, Nicolas, Murchu, Liam O and Chien, Eric. W32.Stuxnet Dossier. Symantec. 2011.

McAfee. Global Energy Cyberattacks: “Night Dragon”. [Online] 2011. http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf

National Institute of Standards and Technology (NIST). NISTIR 7628: Guidelines for Smart Grid Cyber Security. Smart Grid Interoperability Panel–Cyber Security Working Group (SGIP–CSWG). 2010.

“Best Practices for Cyber Security in the Electric Power Sector” IBM, 2012, accessed September 24, 2015

“Siemens: Cyber Security,” Siemens AG, 2015, accessed October 26, 2015

"SCADA over IP-based LAN-WAN Connections," ABB, 2011, https://library.e.abb.com/public/09e2909e92d2ce8ac1257863004e7da0/SCADA application flyer_small.pdf

"IEEE Smart Grid Cybersecurity Round Up," IEEE Smart Grid, accessed November 9, 2015, http://smartgrid.ieee.org/resources/interviews/363-ieee-smart-grid-cyber-security-round-up?highlight=WyJjeWJlciIsInNlY3VyaXR5IiwiY3liZXIgc2VjdXJpdHkiXQ==

Mo, Yilin, et al., et al. Cyber–Physical Security of a Smart Grid Infrastructure. s.l.: http://sparrow.ece.cmu.edu/group/pub/Mo-Kim-etal-ProcIEEE-2011.pdf , 2011.

Yin Hong, Chang. Cyber Security of a Smart Grid: Vulnerability Assessment. s.l.: http://www.ece.nus.edu.sg/stfpage/elejp/FYP/CYH09.pdf , 2010.

Flick, Tony and Morehouse, Justin. Securing the Smart Grid. Next Generation Power Grid Security. 2011.

Clemente, Jude. The Security Vulnerabilities of Smart Grid. s.l.: http://www.ensec.org/index.php?option=com_content&view=article&id=198:the-security-vulnerabilities-of-smart-grid&catid=96:content&Itemid=345 , 2009.

Government Accountability Office (GAO). Electricity grid modernization. Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed. s.l.: http://www.gao.gov/new.items/d11117.pdf , 2011.

Berger, Lars T.; Iniewski, Krzysztof, eds. (April 2012). Smart Grid - Applicacions, Communications and Security. John Wiley and Sons. ISBN 978-1-1180-0439-5.

Yih-Fang Huang; Werner, S.; Jing Huang; Kashyap, N.; Gupta, V., "State Estimation in Electric Power Grids: Meeting New Challenges Presented by the Requirements of the Future Grid," Signal Processing Magazine, IEEE, vol.29, no.5, pp.33,43, Sept. 2012

Tomoiagă, B.; Chindriş, M.; Sumper, A.; Sudria-Andreu, A.; Villafafila-Robles, R. Pareto Optimal Reconfiguration of Power Distribution Systems Using a Genetic Algorithm Based on NSGA-II. Energies 2013, 6, 1439-1455.

Dow Jones & Company, Inc. The Wall Street Journal. [Online] http://europe.wsj.com/home-page

Stouffer, Keith, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, Adam Hahn, "NIST 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security,"

National Institute of Standards and Technology, May 2015, accessed May 1, 2016

“Critical Infrastructure: Security Preparedness and Maturity,” Ponemon Institute: Unisys, July 2014, accessed September 30, 2015

“Vulnerability Analysis of Energy Delivery Control Systems,” Idaho National Laboratory, September 2011, accessed February 16, 2016

Robinson, Michael, “The SCADA Threat Landscape,” BCS, September 2013, accessed February 22, 2016

Weiss, Joseph, Protecting Industrial Control Systems from Electronic Threats (New York, N.Y: Momentum Press, 2010), 36-37

"Access to the Control System LAN,” ICS-CERT, accessed November 9, 2015, https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities

Mimoso, Michael, "Electric Utility Cybersecurity Regulations Have a Problem,” Threat Post, January 24, 2014, accessed November 9, 2015, www.threatpost.com

Campbell, Richard J., “Cybersecurity Issues for the Bulk Power System,” Congressional Research Service, June 10, 2015, accessed February 15, 2016

“Creating Trust in the Digital World: EY’s Global Information Security Survey 2015,” EY, October 2015, accessed May 5, 2016

“ICS-CERT Monitor January 2014—April 2014,” ICS-CERT, May 16, 2015, accessed November 9, 2015

“ICS-CERT Monitor January 2014—April 2014,” ICS-CERT, May 16, 2015, accessed November 9, 2015

Contos, Brian, "Five More Reasons ICS Security is Fragile,” Darkmatters, March 22, 2015, accessed February 26, 2016, www.darkmatters.norsecorp.com

“Shodan,” accessed May 4, 2016, https://www.shodan.io/

"Interview with Manimaran Govindarasu," IEEE Smartgrid, July 2012, accessed February 24, 2016, www.smartgrid.ieeee.org

Mateski, Mark, Cassandra M. Trevino, Cynthia K. Veitch, John Michalski, J. Mark Harris, Scott Maruoka, and Jason Frye, “Cyber Threat Metrics,” Sandia National Laboratories, September 2011, accessed February 16, 2016

Assante, Michael J., Robert M. Lee, “The Industrial Control System Cyber Kill Chain,” SANS Institute, October 2015, accessed February 24, 2016

“Cyber Kill Chain,” Lockheed Martin, accessed May 4, 2016, http://cyber.lockheedmartin.com/solutions/cyber-kill-chain

Higgins, Kelly J., "Researchers Out Default Passwords Packaged With ICS/SCADA Wares," DarkReading, January 4, 2016, accessed February 25, 2016, www.darkreading.com

“Industrial Control Systems,” Shodan, accessed May 4, 2016 https://www.shodan.io/explore/category/industrial-control-systems

“ICS-CERT Year in Review 2014” ICS-CERT, May 16, 2015, accessed February 12, 2016

“Critical Infrastructure: Security Preparedness and Maturity,” Ponemon Institute: Unisys, July 2014, accessed September 30, 2015

Harp, Derek, Bengt Gregory-Brown, “The State of Security in Control Systems Today,” SANS Institute, June 2015, accessed February 22, 2016

“Managing Cyber Risks in an Interconnected World: Key Findings from The Global State of Information Security Survey 2015,” PWC, September 30, 2014, accessed September 30, 2015

“ICS-CERT Monitor November—December 2015,” ICS-CERT, May 16, 2015, accessed February 12, 2016

“Industrial Control System (ICS) Security,” Corero Network Security, 2014, accessed February 22, 2016

Staff of Congressmen Edward J. Markey (D-MA) and Henry Waxman (D-CA), “Electric Grid Vulnerability: Industry Responses Reveal Security Gaps,” U.S. House of Representatives, May 21, 2013, accessed October 9, 2015

Lee, Robert M., Michael J. Assante, Tim Conway, “SANS ICS Defense Use Case 3.v1.1” SANS Institute, April 23, 2015, accessed May 6, 2016

Assante, Mike, "The Six Most Dangerous New Attack Techniques and What's Coming Next," RSA Conference, May 7, 2015, RSAConference.com

"Worldwide Cyber Threats," Office of the Director of National Intelligence, House Permanent Select Committee on Intelligence, September 10, 2015

McLarty III, Thomas F., Thomas J. Ridge; Project Chairs, "Securing the U.S. Electrical Grid," Center for the Study of The Presidency & Congress, October 2014, accessed February 16, 2016

"US should be More Worried about Russia's Cyber Capabilities," ValueWalk, October 2, 2015, accessed May 20, 2016, www.valuewalk.com

Davis, Joshua, "Hackers Take Down the Most Wired Country in Europe," Wired, August 21, 2007, accessed May 4, 2016, www.wired.com

Gorman, Siobhan, "Electricity Grid in U.S. Penetrated by Spies," Wall Street Journal, April 8, 2009, accessed 22 February 2015, www.wsj.com

"Hackers Caused Power Cut in Western Ukraine," BBC, January 12, 2016, accessed March 9, 2016, www.bbc.com

"2015 Global Threat Report," Crowdstrike Intelligence Threat Team, June 10, 2015, accessed February 18, 2016, www.crowdstrike.com

Cyber Behavior: Concepts, Methodologies, Tools, and Applications (Hershey, P.A.: IGI Global, 2014), 795, Information Resources Management Association, ed

Riley, Michael, and Jordan Robertson, "UglyGorilla Hack of U.S. Utility Exposes Cyberwar Threat," Bloomberg Business, June 13, 2014, accessed March 8, 2016, www.bloomberg.com

"United States of America v. Fathi et. Al," U.S. District Court Southern District of New York, 2016, accessed March 28, 2016, https://www.justice.gov/opa/file/834996/download

McLarty III, Thomas F., Thomas J. Ridge; Project Chairs, "Securing the U.S. Electrical Grid," Center for the Study of The Presidency & Congress, October 2014, accessed February 16, 2016

"Solutions 2016: Cybersecurity," Heritage Foundation, 2016, accessed March 8, 2016, www.solutions.heritage.org

Beach-Westmoreland, Nathaniel, “If North Korea Did Hack Sony, It’s a Whole New Kind of Cyberterrorism,” Wired, December 23, 2014, accessed March 8, 2016, www.wired.com

Pagliery, Jose, “ISIS is Attacking the U.S. Energy Grid (and Failing),” CNN Money, October 16, 2015, accessed May 20, 2016, www.money.cnn.com

“Mitigating Cyber-Security Risk of Smart-Grid AMI,” Oracle, 2012, accessed September 25, 2015

“Southern California Edison Smart Grid Strategy & Roadmap,” Southern California Edison 2010, accessed September 30, 2015

“Physical Security,” Techtarget, accessed February 15, 2016, http://searchsecurity.techtarget.com/definition/physical-security

“Comments of the Electric Trade Association in Response to NIST’s Request for Information on ‘Developing a Framework to Improve Critical Infrastructure Cyber security,’” Sacramento Municipal Utility District, April 8, 2013

“Electricity Sub-Sector Coordinating Council Charter,” Electricity Sub-Sector Coordinating Council, 2013, accessed July 21, 2016

“Protecting Our Critical Utilities with Integrated Control Systems,” Motorola, 2012, accessed September 29, 2015

Gauci, Adam, Didier Giarratano, and Sandeep Pathania, “A Framework for Developing and Evaluating Utility Substation Cyber Security,” Schneider Electric, 2014, accessed October 26, 2015

Rosenbush, Stephen, Rachael King, "Utilities Race to Protect Electric Grid Before ‘Disaster Strikes’,” Deloitte CIO Journal, February 19, 2013, accessed October 22, 2015, www.wsj.com

“Belden, Schneider Electric Pair on Cybersecurity Firewall,” Electric Light & Power, January 28, 2014

Byres, Eric, “SCADA Security & Deep Packet Inspection,” March 29, 2012, accessed October 26, 2015, www.tofinosecurity.com

Cornell, Scott, “Cyber Security for the Electric Grid,” Faronics Blog, September 26, 2012, accessed October 26, 2015, www.faronics.com

"S&C Enhances Security of Smart Grid Controls with McAfee Solutions," S&C Electric Company News Center, May 9, 2012, accessed October 26, 2015, www.sandc.com

Ozturk, Metin, and Philip Aubin, "SCADA Security: Challenges and Solutions," June 2011, accessed October 26, 2015

"Understanding the Facts: Edison Electric Institute's Positions on Radio Frequency, Cyber Security and Data Privacy," Pepco, accessed October 26, 2015, www.pepcoholdings.com

Hurd, Steven, Rhett Smith, and Garrett Leischner, "Tutorial: Security in Electric Utility Control Systems," IEEE, 2008, accessed October 26, 2015

"Encryption of Substation Communication Protocols on the Rise in North American Electric Utilities," Newton-Evans Research Company, Inc., February 26, 2014

"Critical Infrastructure: Security Preparedness and Maturity," Ponemon Institute: Unisys, July 2014, accessed September 30, 2015

Clamp, Alice, "Cyber and Physical Security: Evolving Threats and Defense Mechanisms," American Public Power Association, August 30, 2014, accessed December 16, 2015, www.publicpower.org

Wieck, Angie, "Cyber-security Professionals Say Employees are Biggest Threat to Network Security," Dickinson Press, September 27, 2015, accessed December 16, 2015, www.thedickinsonpress.com

"Comments of the Electric Trade Association in Response to NIST's Request for Information on 'Developing a Framework to Improve Critical Infrastructure Cyber security,'" Sacramento Municipal Utility District, April 8, 2013

Henderson, Cam, and Behzad Hosseini, "UE 262 Information Technology: Direct Testimony and Exhibits of Cam Henderson, Behzad Hosseini," Portland General Electric Company, February 15, 2013, accessed October 8, 2015

Rivaldo, Alan, "Report on Electric Grid Cybersecruity in Texas," Public Utility Commission of Texas, November 2012, accessed September 29, 2015

"FERC Directs Development of Standards for Supply Chain Cyber Controls," Federal Energy Regulatory Commission (FERC), July 21, 2016