ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ & ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Πρόγραμμα Προπτυχιακών Σπουδών

Προπτυχιακή Διατριβή

ΑΣΦΑΛΙΣΗ ΟΙΚΙΑΚΩΝ ΣΥΣΚΕΥΩΝ IoT ΜΕ ΧΡΗΣΗ MUD

ΟΝΟΜΑ ΦΟΙΤΗΤΗ : ΝΙΚΟΛΑΟΣ ΧΑΡΑΛΑΜΠΟΣ ΚΑΡΚΑΛΗΣ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ : ΠΑΡΑΣΚΕΥΑΣ ΚΙΤΣΟΣ, ΑΝΑΠΛΗΡΩΤΗΣ ΚΑΘΗΓΗΤΗΣ

Διατριβή υποβληθείσα στο Τμήμα Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών του Πανεπιστημίου Πελοποννήσου. Η παρούσα διατριβή αποτελεί μέρος των απαιτήσεων για την απόκτηση του Προπτυχιακού Πτυχίου.

Πάτρα, Ιανουάριος 2024

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ & ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Πρόγραμμα Προπτυχιακών Σπουδών

Τριμελής Εξεταστική Επιτροπή

Παρασκευάς Κίτσος
Καθηγητής, Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών, Έρευνας & Καινοτομίας

Σωτήρης Χριστοδούλου
Επίκουρος Καθηγητής, Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών, Έρευνας & Καινοτομίας

Ιωάννης Τζήμας
Καθηγητής, Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών, Έρευνας & Καινοτομίας

UNIVERSITY OF PELOPONNESE
DEPARTMENT OF ELECTRICAL & COMPUTER ENGINEERING

Undergraduate Program

Undergraduate Thesis

INSURING IoT HOME APPLIANCES USING MUD

Student Name : NIKOLAOS CHARALAMPOS KARKALIS

Supervising Professor: PARASKEVAS KITSOS

Thesis submitted to the Department of Electrical & Computer Engineering of the University of Peloponnese. This dissertation is part of the requirements for obtaining the Master's Degree in "Smart – ICT"

Patras, January 2024

UNIVERSITY OF PELOPONNESE
DEPARTMENT OF ELECTRICAL & COMPUTER ENGINEERING

Undergraduate Program

Thesis Committee

Paraskevas Kitsos

Professor, Electrical & Computer Engineering, Research & Innovation

Sotiris Christodoulou

Assistant Professor, Electrical & Computer Engineering, Research & Innovation

Ioannis Tzimas

Professor, Electrical & Computer Engineering, Research & Innovation

Ο Νικόλαος Χαράλαμπος Καρκαλής

δηλώνω υπεύθυνα ότι:

1) Είμαι ο κάτοχος των πνευματικών δικαιωμάτων της πρωτότυπης αυτής εργασίας και απ' όσο γνωρίζω η εργασία μου δε συκοφαντεί πρόσωπα, ούτε προσβάλλει τα πνευματικά δικαιώματα τρίτων.

2) Αποδέχομαι ότι το Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών μπορεί, χωρίς να αλλάξει το περιεχόμενο της εργασίας μου, να τη διαθέσει σε ηλεκτρονική μορφή μέσα από την ψηφιακή Βιβλιοθήκη του Ιδρύματος, να την αντιγράψει σε οποιοδήποτε μέσο ή/και σε οποιοδήποτε μορφότυπο καθώς και να κρατά περισσότερα από ένα αντίγραφα για λόγους συντήρησης και ασφάλειας.

ΕΥΧΑΡΙΣΤΙΕΣ

Για τη διεκπεραίωση της παρούσας πτυχιακής εργασίας, θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου Παρασκευά Κίτσο για τη συνεργασία μας και που με την πολύτιμη βοήθειά του συνέβαλε στην αρτιότερη εκπόνησή της.

ΠΕΡΙΕΧΟΜΕΝΑ

Περίληψη ……..…..8

Abstract ……..8

Εισαγωγή ……..8

Κεφάλαιο 1 : ΜΙΑ ΠΡΩΤΗ ΠΡΟΣΕΓΓΙΣΗ ……10

1.1 Η Δημιουργία του MUD (NCCoE) ……...10

1.2 Ο Σκοπός του MUD ……10

1.3 Το Πρότυπο Λογισμικού MUD ……11

1.4 Η Αναγκαία Χρήση του MUD ……11

1.5 Σενάρια MUD ……..12

1.6 Εκτίμηση Κινδύνου ……13

1.7 Απειλές ……13

1.8 Ανάλυση Χαρακτηριστικών Ασφάλειας ……14

Κεφάλαιο 2 : ΑΡΧΙΤΕΚΤΟΝΙΚΗ MUD, ΥΠΟΣΤΗΡΙΞΗ & ΣΥΣΚΕΥΕΣ ……14

2.1 Μορφές Προστασίας ……..14

2.2 Αρχιτεκτονική Αναφοράς Σχήμα 1 ……15

2.3 Αρχιτεκτονική Αναφοράς Σχήμα 2 ……17

2.4 Υποστήριξη MUD & Μηχανισμοί ……...19

2.5 Υποστήριξη για Ενημερώσεις ……20

2.6 Υποστήριξη για Σηματοδότηση Απειλών ……20

2.7 Ειδικά Χαρακτηριστικά Κατασκευής ……..20

2.8 Η Φυσική Αρχιτεκτονική ……22

Κεφάλαιο 3 : ΑΝΑΛΥΣΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ ……24

3.1 Χάρτης Ελέγχου Ασφαλείας ……25

3.2 Προστασία Πληροφοριών και Συστημάτων με Έλεγχο Ασφάλειας και Απορρήτου ……..25

3.3 Πλαίσιο Διαχείρισης Κινδύνων (RMF) ……25

3.4 Χαρακτηριστικά Υλοποίησης & Προσεγγίσεις ……...…26

3.5 Στόχοι του Έργου στο Cybersecurity Framework & Αναφορά στον Πληροφοριακό Έλεγχο Ασφάλειας ……33

Κεφάλαιο 4 : ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ……..…..83

4.1 Ευρήματα ……83

4.2 Θέματα Ασφάλειας ……..89

4.3 Συστάσεις Ασφάλειας ……..91

4.4 Θεωρήσεις Μελλοντικής Δόμησης ……..94

Ιστότοποι……....96

ΠΕΡΙΛΗΨΗ

Στόχος της πτυχιακής εργασίας είναι η παροχή μίας ολοκληρωμένης ανάλυσης για την ασφαλή ενσωμάτωση και διαχείριση των συσκευών IoT σε περιβάλλοντα επιχειρήσεων και οικιακών δικτύων. Αναγνωρίζει τις προκλήσεις που συνδέονται με την ασφάλεια των συσκευών IoT, όπως η αναγνώριση, η πιστοποίηση και η προστασία των συσκευών από επιθέσεις. Προσφέρονται λεπτομερείς οδηγίες για την εφαρμογή ασφάλειας σε συσκευές IoT, συμπεριλαμβανομένων μεθόδων προσαρμογής, διαμόρφωσης και παρακολούθησης. Επίσης, αναλύεται ο τρόπος αντιμετώπισης πιθανών απειλών και επιθέσεων, παρέχοντας προτάσεις για την ενίσχυση της ασφάλειας των συσκευών. Αποτελείται από αναλύσεις, προτάσεις και πρακτικά παραδείγματα για τη βελτίωση της κυβερνοασφάλειας των συσκευών IoT σε επιχειρησιακά και οικιακά περιβάλλοντα. Μέσω της εφαρμογής των συστάσεων που παρέχονται οι οργανισμοί και τα οικιακά περιβάλλοντα μπορούν να ενισχύσουν την ασφάλεια των συσκευών IoT που χρησιμοποιούν στο περιβάλλον τους.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ : IoT , Ασφάλεια , Συσκευές

ABSTRACT

The bachelor's thesis aims to comprehensively analyze the secure integration and management of IoT devices in both business and home network environments. It acknowledges the challenges associated with the security of IoT devices, such as identification, certification, and safeguarding against attacks. Detailed guidelines are presented for implementing security measures on IoT devices, including adaptation, configuration, and monitoring methods. Additionally, it delves into the approach to address potential threats and attacks, offering suggestions to enhance device security. The work encompasses analyses, proposals, and practical examples aimed at improving the cybersecurity of IoT devices in operational and domestic settings. Through the application of the recommendations provided, organizations and home environments can strengthen the security of the IoT devices they utilize within their respective contexts.

KEYWORDS : IoT , Security , Devices

ΕΙΣΑΓΩΓΗ

Η τεχνολογία Internet of Things (IoT) έχει επανασχεδιάσει τον τρόπο με τον οποίο αλληλεπιδρούμε με τον κόσμο μας. Τονίζοντας τη σημαντική παρουσία των συνδεδεμένων

συσκευών IoT στην καθημερινή μας ζωή, από έξυπνα ψυγεία που διαχειρίζονται τα τρόφιμα μας μέχρι έξυπνες λάμπες που προσαρμόζουν τον φωτισμό στις προτιμήσεις μας. Αυτή η τεχνολογία έχει την άνεση και την ευφυΐα του σπιτιού μας, προσφέροντας λύσεις που πριν από λίγα χρόνια θα φαινόνταν αδιανόητες. Ωστόσο, παρά τα πλεονεκτήματα, η εξάπλωση των συσκευών IoT έχει αυξήσει τις ανησυχίες για την ασφάλεια. Η συνδεσιμότητα αυτών των συσκευών στο διαδίκτυο δημιουργεί νέες προκλήσεις και απειλές. Κακόβουλοι χρήστες μπορούν να προσπελάσουν και να εκμεταλλευτούν αυτές τις συσκευές, απειλώντας την ιδιωτικότητά μας, καθώς και την κυβερνοασφάλειά μας. Στην παρούσα πτυχιακή εργασία, θα εξετάσουμε τη σημασία της ασφάλειας στο πεδίο των οικιακών συσκευών IoT και πώς η τεχνολογία Manifest-Based Usage Description (MUD) αναδεικνύεται ως ένας σημαντικός παράγοντας για την εξάλειψη των κινδύνων που συνδέονται με αυτήν την τεχνολογία.

Η τεχνολογία Manifest-Based Usage Description (MUD) αντιπροσωπεύει μια σημαντική εξέλιξη στον τομέα της ασφάλειας των συσκευών Internet of Things (IoT). Η ουσία της MUD είναι η δυνατότητα των συσκευών να περιγράφουν λεπτομερώς τις λειτουργίες τους και τις απαιτήσεις πρόσβασης στο δίκτυο. Ένα από τα σημαντικότερα πλεονεκτήματα της τεχνολογίας MUD είναι ότι επιτρέπει στις συσκευές IoT να προσδιορίζουν την πρόσβαση. Δηλαδή, μπορούν να περιορίσουν τον αριθμό των συσκευών ή των εφαρμογών που έχουν πρόσβαση σε αυτές. Αυτό εξαλείφει τον κίνδυνο της μη εξουσιοδοτημένης πρόσβασης και της κακόβουλης χρήσης των συσκευών. Προκειμένου να επιτύχει την ασφάλεια των συσκευών IoT, η τεχνολογία MUD βασίζεται σε ένα σύνολο προδιαγραφών που καθορίζουν το πώς θα πρέπει να διαχειρίζονται οι συσκευές. Περιλαμβάνει τον καθορισμό των προτύπων επικοινωνίας, των προνομιακών δικαιωμάτων και των περιορισμών πρόσβασης. Επιπλέον, η τεχνολογία MUD επιτρέπει την ενημέρωση αυτών των προδιαγραφών με τον χρόνο, προσαρμόζοντας τις συσκευές στις αλλαγές στο περιβάλλον και στις ανάγκες ασφάλειας. Συνολικά, η τεχνολογία MUD είναι ένα ισχυρό εργαλείο για την ασφάλιση των συσκευών IoT και την εξάλειψη των αδυναμιών ασφαλείας που σχετίζονται με αυτές. Προάγει την ευαισθητοποίηση και την αυτοπροστασία των συσκευών, βοηθώντας στη δημιουργία ενός περισσότερο ασφαλούς περιβάλλοντος για το Internet of Things.

Η υλοποίηση της τεχνολογίας MUD για την ασφάλιση των οικιακών συσκευών IoT αποτελεί μια πρόκληση που απαιτεί συνεργασία ανάμεσα στους κατασκευαστές των συσκευών και τους παρόχους υπηρεσιών. Οι κατασκευαστές πρέπει να ενσωματώσουν την τεχνολογία MUD στις συσκευές τους, περιγράφοντας σωστά τις λειτουργίες και τις απαιτήσεις πρόσβασης. Οι πάροχοι υπηρεσιών, από την άλλη πλευρά, πρέπει να υποστηρίξουν την ανάγνωση και τον έλεγχο των περιγραφών MUD για να διασφαλίσουν τη σωστή λειτουργία τους. Αυτή η συνεργασία είναι ουσιώδης για την επιτυχή εφαρμογή της τεχνολογίας MUD. Η προσεκτική υλοποίηση και δοκιμή είναι βασικοί παράγοντες. Η τεχνολογία MUD πρέπει να εφαρμοστεί με ακρίβεια και να δοκιμαστεί προσεκτικά προτού ενσωματωθεί στις συσκευές και τα δίκτυα. Αυτό περιλαμβάνει τον έλεγχο της συμβατότητας με τις προδιαγραφές MUD και την παρακολούθηση της συμπεριφοράς των συσκευών κατά την λειτουργία τους στο δίκτυο. Οι μελλοντικές επεκτάσεις της έρευνας προορίζονται για την ενίσχυση της ασφάλειας του IoT. Περιλαμβάνεται την ανάπτυξη προηγμένων μηχανισμών ασφάλειας που θα αντιμετωπίζουν τις αναδυόμενες απειλές του IoT, όπως οι επιθέσεις με βάση την τεχνητή νοημοσύνη και η ανάγκη για αυτόνομη ανίχνευση κινδύνων. Επίσης, η προσαρμογή της τεχνολογίας MUD σε νέες συσκευές και περιβάλλοντα συνεισφέρει στην επέκταση της ασφάλειας σε περισσότερους τομείς του IoT. Συνολικά, η πτυχιακή εργασία αυτή αναδεικνύει τη σημασία της τεχνολογίας MUD στην ασφάλεια του Internet of Things και επισημαίνει τη συνεχή ανάγκη για εξέλιξη και προσαρμογή προκειμένου να ανταποκριθούμε στις αυξανόμενες απαιτήσεις της κυβερνοασφάλειας και της προστασίας του ιδιωτικού χώρου μας.

ΚΕΦΑΛΑΙΟ 1
ΜΙΑ ΠΡΩΤΗ ΠΡΟΣΕΓΓΙΣΗ

1.1 Η Δημιουργία του MUD (NCCoE)

Το National Cybersecurity Center of Excellence (NCCoE) απηύθυνε ανοιχτή πρόκληση σε παρόχους τεχνολογίας να συμμετάσχουν στην επίδειξη μιας προσέγγισης για την ανάπτυξη συσκευών IoT σε οικιακά δίκτυα μικρών επιχειρήσεων με τρόπο που να παρέχει υψηλότερη ασφάλεια από ότι επιτυγχάνεται συνήθως στα σημερινά περιβάλλοντα. Σε αυτό το έργο, η προδιαγραφή εφαρμόζεται σε δίκτυα οικιακών και μικρών επιχειρήσεων που αποτελούνται τόσο από IoT όσο και από πλήρως εξοπλισμένες συσκευές (π.χ. προσωπικούς υπολογιστές και κινητές συσκευές). Το MUD έχει ως σκοπό να περιορίσει την δυνατότητα μη εξουσιοδοτημένης επικοινωνίας μεταξύ των συσκευών. Τα στοιχεία της πύλης του δικτύου και οι συσκευές IoT αξιοποιούν το MUD για να διασφαλίσουν ότι οι συσκευές IoT στέλνουν και λαμβάνουν μόνο την κίνηση που χρειάζονται για να εκτελέσουν την προβλεπόμενη λειτουργία τους.

1.2 Ο Σκοπός του MUD

Το συγκεκριμένο έργο έχει ως σκοπό να ελέγξει μέσω του MUD τις επιθέσεις που βασίζονται στο δίκτυο. Οι συσκευές που διαθέτουν ή που δεν διαθέτουν την δυνατότητα MUD προστατεύονται με την χρήση σήματος απειλής. Το έργο επίσης μας δείχνει πώς το πρωτόκολλο Wi-Fi Easy Connect μπορεί να ενσωματωθεί στις συσκευές παρέχοντας έτσι με ασφάλεια μοναδικά διαπιστευτήρια για σύνδεση στο δίκτυο. Το πρωτόκολλο MUD περιλαμβάνει υποστήριξη για αυτόματες και ασφαλείς ενημερώσεις λογισμικού όπου κάθε μια ενημέρωση περιλαμβάνει έναν διακομιστή ενημέρωσης στον οποίο το MUD θα επιτρέπει τη σύνδεση συσκευών.

Η κάθε συσκευή IoT δεν αποτελεί μια συσκευή γενικής χρήσης καθώς έχει μια προβλεπόμενη λειτουργία η οποία είναι αρκετά συγκεκριμένη ώστε οι απαιτήσεις επικοινωνίας της κάθε συσκευής να μπορούν να καθοριστούν με ακρίβεια και πληρότητα. Η επικοινωνία μιας συσκευής IoT θα πρέπει να περιορίζεται μόνο σε ό,τι απαιτείται για την εκτέλεση της λειτουργίας

της συσκευής .Οι δρομολογητές δικτύου μπορούν να ρυθμιστούν αυτόματα για να επιβάλλουν αυτές τις επικοινωνίες έτσι ώστε να επιτρέπονται οι προβλεπόμενες επικοινωνίες απαγορεύονται οι ακούσιες επικοινωνίες. Σε περίπτωση που όλα τα στοιχεία του δικτύου με δυνατότητα MUD έχουν αναπτυχθεί και λειτουργούν όπως προβλέπεται, η επίθεση βάσει του δικτύου σε μια συσκευή IoT απαιτεί να παραβιαστεί ένα από τα συστήματα με τα οποία επιτρέπεται να επικοινωνεί η συσκευή IoT. Εάν μια συσκευή επρόκειτο να παραβιαστεί, θα μπορούσε να χρησιμοποιηθεί σε μια επίθεση που βασίζεται σε δίκτυο μόνο εναντίον συστημάτων με τα οποία επιτρέπεται να επικοινωνεί.

1.3 Το Πρότυπο Λογισμικού MUD

Μια λύση για το πρόβλημα της ευπάθειας που δημιουργείτε με την ανταλλαγή μηνυμάτων μέσω ενός δικτύου επικοινωνίας ήρθε να δώσει το πρότυπο λογισμικού MUD το οποίο είναι σε θέση να αντιμετωπίζει τις απειλές για κάθε συσκευή. Η κάθε συσκευή θα είναι σε θέση να λειτουργεί υπό τον περιορισμό ορισμένων παραμέτρων κόβοντας κάθε επικοινωνία εκτός αυτών θέτοντας την ως μη ασφαλής. Όταν μια συσκευή είναι συνδεδεμένη στο δίκτυο τότε εκπέμπει μια διεύθυνση URL η οποία περνά από επεξεργασία έτσι ώστε να διαπιστωθεί η εγκυρότητα του ασφαλούς μηνύματος και στην συνέχεια το αίτημα οδηγείτε προς τον Server. Από την άλλη πλευρά ο Server στέλνει προς το αντικείμενο IoT αφού διαπιστωθεί ότι το μήνυμα της απάντησης είναι οριοθετημένο σύμφωνα με την πολιτική πρόσβασης.

Οι συσκευές IoT έχουν σχεδιαστεί κατάλληλα ώστε να υλοποιούν μια συγκεκριμένη συμπεριφορά. Η υποχρέωση του MUD είναι να διασφαλίσει ότι αυτή η συμπεριφορά δεν θα παραμορφωθεί από κανέναν κακόβουλο και μη εξουσιοδοτημένο παράγοντα. Ακόμα και αν μια συσκευή IoT παραβιαστεί, το MUD θα αποτρέψει τη χρήση της σε οποιαδήποτε επίθεση που θα απαιτούσε από τη συσκευή να στείλει κίνηση σε μη εξουσιοδοτημένο προορισμό.

Το πρότυπο MUD περιβάλλεται από τεχνικά στοιχεία που είναι κατάλληλα διαμορφωμένα με σκοπό την υποστήριξη και την υλοποίησή του. Τα τεχνικά στοιχεία που χρησιμοποιούνται περιλαμβάνουν πύλες δικτύου (gateways), δρομολογητές (routers) και διακόπτες (switches) που υποστηρίζουν την ενσύρματη και ασύρματη πρόσβαση στο δίκτυο. Για την αντιμετώπιση των απειλών χρησιμοποιεί έναν διακομιστές σηματοδότησης απειλών καθώς και διακομιστές αρχείων MUD με σκοπό την διατήρηση των αρχείων. Οι διακομιστές MUD είναι απαραίτητο να αναβαθμίζονται συνεχώς με νέες ενημερώσεις έτσι ώστε στην συνέχεια να ενημερώνονται και οι συσκευές IoT με σκοπό την ασφάλεια σε οικιακά δίκτυα και δίκτυα μικρών επιχειρήσεων.

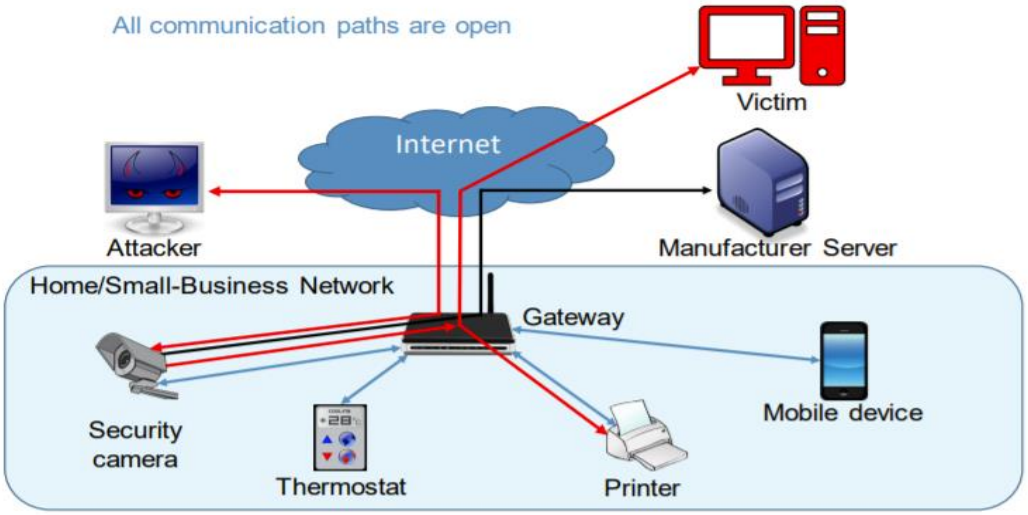
1.4 Η Αναγκαία Χρήση του MUD

Σημαντική αύξηση τον τελευταίο καιρό έχει εμφανιστεί σε μη διαχειριζόμενες συσκευές IoT οι οποίες είναι συνδεδεμένες στο δίκτυο. Οι συγκεκριμένες συσκευές αποτελούν ισχυρή ευπάθεια και χρήζουν μέτρα ασφαλείας. Όταν χρησιμοποιούμε το MUD το δίκτυο επιτρέπει αποκλειστικά την κίνηση στο δίκτυο που χρειάζεται αποκλείοντας οποιαδήποτε άλλη επικοινωνία με την συσκευή.

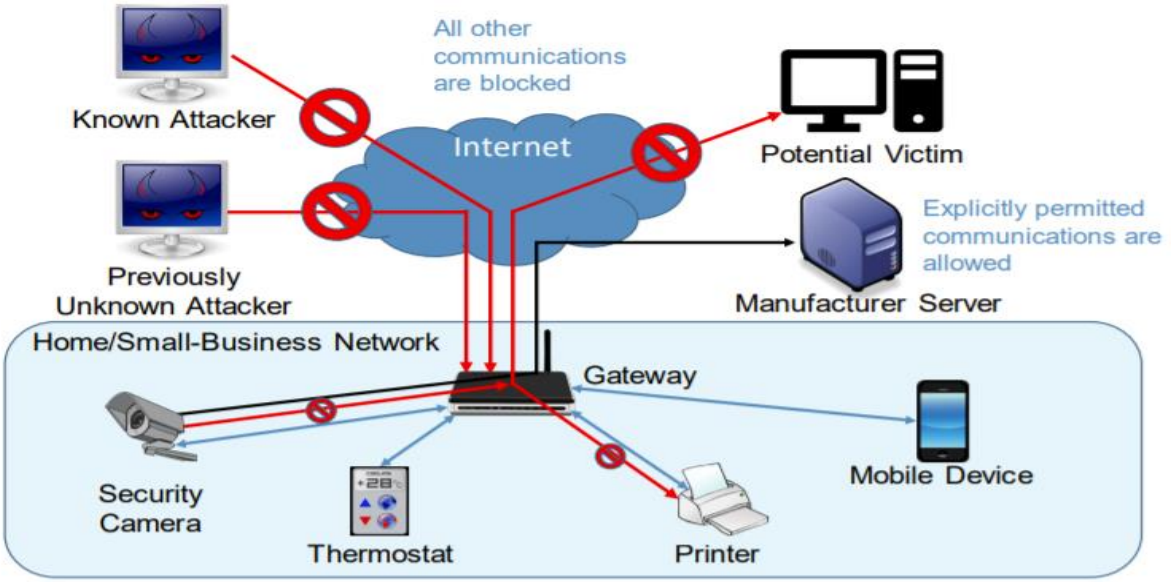
Για συσκευές όπως τα laptop, τα smartphones και τα tablet η τεχνολογία ασφάλειας είναι αρκετά ανεπτυγμένη ωστόσο αυτό δεν ισχύει για συσκευές IoT όπως : οι κάμερες ασφαλείας, οι αισθητήρες περιβάλλοντος ή οι ιατρικές συσκευές. Σε μια εποχή όπου ακόμα και τα δαχτυλικά αποτυπώματα μπορούν να πλαστογραφηθούν είναι αναγκαία η διασφάλιση των οικιακών συσκευών καθώς και η ασφαλείς επικοινωνία τους μέσω του δικτύου. Χωρίς τον καθορισμό μέτρων ασφαλείας το σύστημα μας μπορεί ανά πάσα στιγμή να δεχτεί επίθεση μεγάλης κλίμακας. Μία

τέτοιου είδους επίθεση θα μπορούσε να δώσει στον εισβολέα τον απόλυτο έλεγχο ώστε να κυβερνά ένα σετ παραβιασμένων συσκευών που ονομάζουμε botnets.
Μία τέτοια εισβολή θα μπορούσε να είχε ως αποτέλεσμα μία επίθεση κατανεμημένης άρνησης υπηρεσίας (DdoS) καθώς και άλλες επιθέσεις που βασίζονται στο δίκτυο.

1.5 Σενάρια MUD



Στο πρώτο σενάριο το MUD δεν αναπτύσσεται στο δίκτυο επομένως οι συσκευές IoT είναι ευάλωτες και οι θύρες είναι επιρρεπής στο να σαρωθούν από κακόβουλους χρήστες. Όπως φαίνεται και στην παρακάτω εικόνα το σπίτι ή η μικρή επιχείρηση (που απεικονίζεται από το μπλε ορθογώνιο πλαίσιο) δεν έχει καμία απολύτως ασφάλεια. Όλες οι συσκευές στο περιβάλλον όπως η κάμερα ασφαλείας, ο θερμοστάτης, ο εκτυπωτής, το κινητό καθώς και ο σταθερός υπολογιστής είναι εκτεθειμένοι σε κάθε είδους επίθεση καθώς και σε κλοπή δεδομένων. Μέσω της συσκευής router ο επιτιθέμενος μπορεί να επιτεθεί στον server που φιλοξενείται το σύστημα μας έχοντας την δυνατότητα να υποκλέψει, να αλλοιώσει, ή να τροποποιήσει σημαντικές πληροφορίες.



Στο δεύτερο σενάριο όπου το MUD αναπτύσσεται στο δίκτυο έχει ως αποτέλεσμα να κόβει κάθε μια εξουσιοδοτημένη κίνηση ώστε να εξαλειφθεί η οποιαδήποτε πιθανότητα εισβολής, συνεπώς οι συσκευές δεν μπορούν να λαμβάνουν επισκεψιμότητα από εξωτερικούς ιστότοπους που δεν περιλαμβάνονται στην λίστα αρχείων MUD αυτών των συσκευών. Ένας από τους εξωτερικούς ιστότοπους με τους οποίους επιτρέπεται να επικοινωνεί μία συσκευή IoT με δυνατότητα MUD είναι με τον διακομιστή ενημέρωσης κατασκευαστή από τον οποίο η συσκευή IoT λαμβάνει τακτικές ενημερώσεις λογισμικού με σκοπό να διασφαλίσει ότι εγκαθιστά τις πιο πρόσφατες ενημερώσεις κώδικα ασφαλείας.

1.6 Εκτίμηση Κινδύνου

Ο κίνδυνος χαρακτηρίζει μια πιθανή απειλή ή κάποιο γεγονός το οποίο αν συμβεί θα μπορούσε να βλάψει το έργο μας και να καταστήσει ευάλωτες τις συσκευές που βρίσκονται στον χώρο καθώς και τα δεδομένα τους. Η αξιολόγηση του κινδύνου ορίζεται ως ο εντοπισμός, η εκτίμηση και η ιεράρχηση των κινδύνων για τις λειτουργίες των συσκευών, την οργάνωση των περιουσιακών στοιχείων που προκύπτουν από τη λειτουργία ενός συστήματος. Ένα σημαντικό μέρος της διαχείρισης κινδύνου αποτελείται από τις αναλύσεις απειλών και τρωτών σημείων και λαμβάνει υπόψη τους μετριασμούς που παρέχονται από προγραμματισμένους ή υφιστάμενους ελέγχους ασφαλείας.

1.7 Απειλές

Ιστορικά, οι συσκευές Διαδικτύου είχαν πλήρη συνδεσιμότητα στα επίπεδα δικτύου και μεταφοράς. Οποιαδήποτε συσκευή με έγκυρες διευθύνσεις πρωτοκόλλου IP συχνά επικοινωνεί μέσω του Πρωτοκόλλου Ελέγχου Μετάδοσης TCP όταν οι επικοινωνίες είναι προσανατολισμένες στην σύνδεση αλλιώς χρησιμοποιείται το Πρωτόκολλο Δεδομένων Χρήστη UDP για πρωτόκολλα χωρίς σύνδεση. Με σκοπό να μετριάσουν οι απειλές μέσω του δικτύου επιτρέπουμε στην κάθε συσκευή να έχει περιορισμένες δυνατότητες οι οποίες θα καλύπτουν τις ανάγκες μας καθώς και ο αποκλεισμός συσκευών ή τομέων που θεωρούνται ύποπτοι. Σε τυπικά περιβάλλοντα δικτύωσης,

ένας κακόβουλος παράγοντας μπορεί να εντοπίσει μια συσκευή IoT επειδή εκθέτει τις υπηρεσίες της απευθείας στο Διαδίκτυο. Με αυτόν τον τρόπο μπορεί να εξαπολύσει επίθεση σε αυτήν τη συσκευή από οποιοδήποτε σύστημα στο Διαδίκτυο. Μόλις παραβιαστεί, αυτή η συσκευή μπορεί να χρησιμοποιηθεί για επίθεση σε οποιοδήποτε άλλο σύστημα στο Διαδίκτυο. Επειδή οι συσκευές που αναπτύσσονται συχνά έχουν γνωστά ελαττώματα ασφαλείας, το ποσοστό επιτυχίας για την παραβίαση των ανιχνευμένων συστημάτων είναι πολύ υψηλό. Συνήθως, το κακόβουλο λογισμικό έχει σχεδιαστεί για να υπονομεύει μια λίστα συγκεκριμένων συσκευών, καθιστώντας τέτοιες επιθέσεις πολύ επεκτάσιμες. Μόλις παραβιαστεί, μια συσκευή IoT μπορεί να χρησιμοποιηθεί για να παραβιάσει άλλες συσκευές που είναι συνδεδεμένες στο διαδίκτυο, να εξαπολύσει επιθέσεις σε οποιαδήποτε συσκευή στο Διαδίκτυο ή να εξαπολύσει επιθέσεις σε συσκευές εντός του τοπικού δικτύου που φιλοξενεί τη συσκευή.

1.8 Ανάλυση χαρακτηριστικών ασφαλείας

Ο σκοπός της ανάλυσης των χαρακτηριστικών ασφαλείας είναι να κατανοήσει τον βαθμό στον οποίο το έργο ανταποκρίνεται στον στόχο του να επιδείξει την ικανότητα αναγνώρισης στοιχείων IoT στους διαχειριστές MUD καθώς και στην διαχείριση της πρόσβασης σε αυτά τα στοιχεία περιορίζοντας ταυτόχρονα τη μη εξουσιοδοτημένη πρόσβαση. Επιπλέον, επιδιώκει να κατανοήσει τα πλεονεκτήματα ασφάλειας της συγκεκριμένης προσέγγισης. Η ανάλυση χαρακτηριστικών ασφαλείας μπορεί επίσης να ενημερώσει την ανάπτυξη ενός σχεδίου ασφάλειας. Η ανάλυση χαρακτηριστικών ασφαλείας δεν αποτελεί μια ολοκληρωμένη δοκιμή όλων των στοιχείων ασφαλείας και δεν είναι ικανή να εντοπίσει όλες τις αδυναμίες. Η δοκιμή των συσκευών IoT θα μας ενημέρωνε σχετικά με τις αδυναμίες στην υλοποίηση της κάθε συσκευής.

ΚΕΦΑΛΑΙΟ 2
ΑΡΧΙΤΕΚΤΟΝΙΚΗ MUD, ΥΠΟΣΤΗΡΙΞΗ & ΣΥΣΚΕΥΕΣ

2.1 Μορφές Προστασίας

Το πρωτόκολλο MUD καθώς και η αρχιτεκτονική ολόκληρου του έργου προορίζεται για οικιακά δίκτυα και δίκτυα μικρών επιχειρήσεων και χρησιμοποιείται από συσκευές όπως για παράδειγμα ο ηλεκτρονικός υπολογιστής ή το smartphone αλλά μπορεί να χρησιμοποιηθεί επίσης και από άλλες πλήρως εξοπλισμένες συσκευές όπως το ψυγείο ή ο θερμοστάτης. Η αρχιτεκτονική είναι κατάλληλα σχεδιασμένη ώστε να παρέχει τριών ειδών μορφές προστασίας.

Πρώτη Μορφή Προστασίας

Η πρώτη προστασία που παρέχει η αρχιτεκτονική είναι η χρήση της προδιαγραφής MUD με σκοπό να επιτρέπει σε μια συσκευή IoT να στέλνει και να λαμβάνει μόνο τα μηνύματα που

αποτελούνται από εξουσιοδοτημένες κινήσεις στο δίκτυο έχοντας ως αποτέλεσμα η συσκευή να μην πέσει θύμα εκμετάλλευσης κακόβουλου λογισμικού, σε επιθέσεις DDoS ή άλλες επιθέσεις μέσω του δικτύου.

Δεύτερη Μορφή Προστασίας

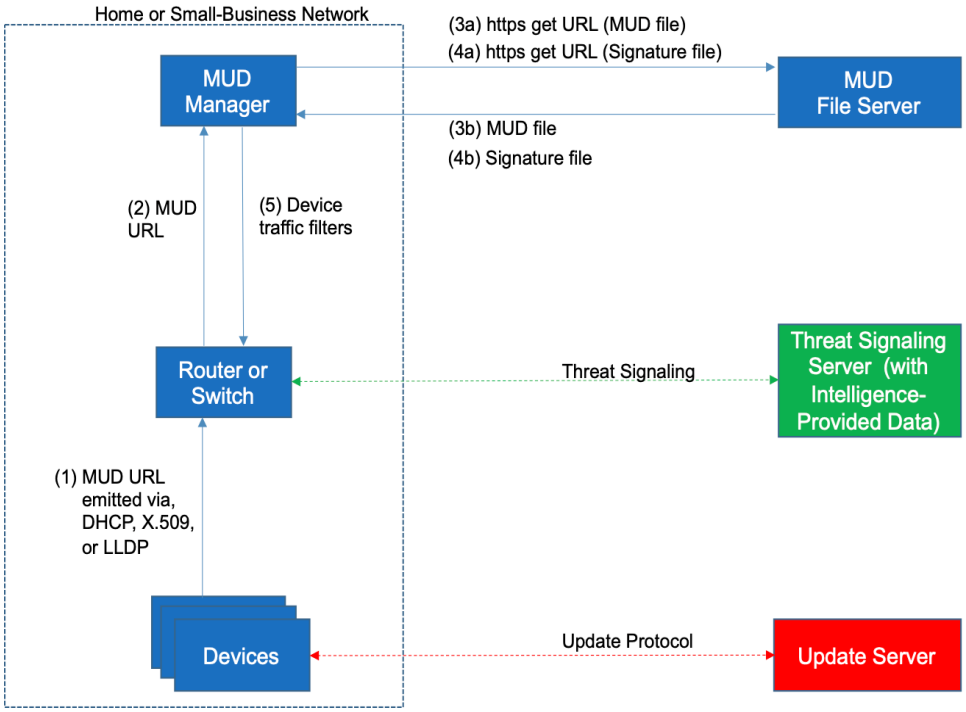
Το πρωτόκολλο MUD έχει την δυνατότητα να ελέγχει την πρόσβαση σε όλο το δίκτυο με σηματοδότηση απειλών έτσι ώστε να προστατευτεί όλες οι συσκευές IoT, με ή χωρίς υποστήριξη MUD.

Τρίτη Μορφή Προστασίας

Η αρχιτεκτονική του πρωτοκόλλου είναι κατάλληλη ώστε να υπάρχουν ασφαλείς αυτοματοποιημένες ενημερώσεις λογισμικού σε όλες τις συσκευές έχοντας ως σκοπό την διασφάλιση σχετικά με τις ενημερώσεις κώδικα του λειτουργικού συστήματος.

2.2 Αρχιτεκτονική Αναφοράς

Σχήμα 1



Η παραπάνω εικόνα μας δείχνει τη λογική αρχιτεκτονική του σχεδίου αναφοράς η οποία αποτελείται από τρία κύρια στοιχεία, την υποστήριξη για το πρωτόκολλο MUD, την υποστήριξη για την σηματοδότηση απειλών καθώς και την υποστήριξη ενημερώσεων. Μέσα στο οικιακό δίκτυο ή στο δίκτυο της μικρής επιχείρησης υπάρχει ο Διαχειριστής MUD , η πύλη ή ο μεταγωγέας και οι συσκευές. Με τον έξω κόσμο το σύστημα αλληλεπιδρά με τον Update Server όπου ανανεώνει το σύστημα με τυχόν καινούργιες ενημερώσεις που θα συνεισφέρουν στα επίπεδα της ασφάλειας, με τον σηματοδότη και τον διαχειριστή αρχείων MUD. Όπως φαίνεται και στο σχήμα οι συσκευές αλληλεπιδρούν με το router / switch μέσω διάφορων πρωτοκόλλων. Στη συνέχεια οι συσκευές

δικτύου στέλνουν το URL MUD στον διαχειριστή MUD ο οποίος με την σειρά του το προάγει μαζί με την υπογραφή του αρχείου στον διακομιστή αρχείων MUD. Ο διαχειριστής αρχείων MUD με τη σειρά του αφού ταυτοποιήσει την εγκυρότητα του αρχείου το επιστρέφει στον MUD Manager. Ο MUD Manager αφού λάβει το αρχείο μέσω του φίλτρου κυκλοφορίας συσκευών το επιστρέφει στη πύλη / μεταγωγέα όπου αλληλεπιδρά με τον σηματοδότη απειλών. Επίσης οι συσκευές αλληλεπιδρούν με τον Update Server.

Πιο αναλυτικά…

Η συσκευή IoT εκπέμπει μια διεύθυνση URL MUD χρησιμοποιώντας έναν μηχανισμό όπως το πιστοποιητικό DHCP, LLDP ή X.509. Οι συσκευές είναι σε άμεση επικοινωνία με τον Update Server η οποία γίνεται μέσω του Update Protocol με σκοπό την συνεχή αναβάθμιση του λογισμικού των συσκευών που βρίσκονται εντός του δικτύου. (Βήμα 1)

Ο δρομολογητής εξάγει την διεύθυνση URL MUD από το πλαίσιο πρωτοκόλλου οποιουδήποτε μηχανισμού ο οποίος χρησιμοποιήθηκε για τη μεταφορά της κάθε διεύθυνσης και προωθεί αυτή την διεύθυνση URL MUD στον διαχειριστή MUD. (βήμα 2)

Μόλις ληφθεί η διεύθυνση URL MUD, ο διαχειριστής MUD χρησιμοποιεί το Hypertext Transfer Protocol Secure (https) για να ζητήσει το αρχείο MUD από τον διακομιστή αρχείων MUD χρησιμοποιώντας τη διεύθυνση URL MUD που παρέχεται στο προηγούμενο βήμα (βήμα 3a). Εάν είναι επιτυχής, ο διακομιστής αρχείων MUD στην καθορισμένη θέση θα εξυπηρετήσει το αρχείο MUD (βήμα 3b).

Στη συνέχεια, ο διαχειριστής MUD χρησιμοποιεί το https για να ζητήσει το αρχείο υπογραφής που σχετίζεται με το αρχείο MUD (βήμα 4a) και κατά την παραλαβή (βήμα 4b) επαληθεύει το αρχείο MUD χρησιμοποιώντας το αρχείο υπογραφής του.

Το αρχείο MUD περιγράφει τις απαιτήσεις επικοινωνίας για τη συσκευή IoT. Μόλις ο διαχειριστής MUD καθορίσει ότι το αρχείο MUD είναι έγκυρο, ο διαχειριστής MUD μετατρέπει τους κανόνες ελέγχου πρόσβασης στο αρχείο MUD σε εγγραφές ελέγχου πρόσβασης (π.χ. λίστες ελέγχου πρόσβασης—ACL, κανόνες τείχους προστασίας ή κανόνες ροής) και τους εγκαθιστά στο δρομολογητή ή διακόπτη (βήμα 5).

Σε περίπτωση που χρησιμοποιηθεί μια εναλλακτική μέθοδος για την μεταφορά της διεύθυνσης του αρχείου MUD από την συσκευή προς το αρχείο MUD, τα βήματα 1 και 2 της παραπάνω εικόνας θα αντικατασταθούν σύμφωνα με τον εναλλακτικό μηχανισμό. Μόλις εφαρμοστούν οι κανόνες ελέγχου πρόσβασης της συσκευής στο δρομολογητή ή τον διακόπτη, η συσκευή IoT με δυνατότητα MUD θα μπορεί να επικοινωνεί με εγκεκριμένους τοπικούς κεντρικούς υπολογιστές και κεντρικούς υπολογιστές διαδικτύου όπως ορίζονται στο αρχείο MUD. Σε περίπτωση που εντοπισθούν προσπάθειες επικοινωνίας οι οποίες είναι μη εγκεκριμένες θα έχουν ως αποτέλεσμα τον αποκλεισμό.

Όπως περιγράφεται στην προδιαγραφή MUD, οι κανόνες του αρχείου MUD μπορούν να περιορίσουν τόσο την κυκλοφορία μεταξύ της συσκευής και των εξωτερικών τομέων διαδικτύου, όσο και την κυκλοφορία μεταξύ της συσκευής και άλλων συσκευών στο τοπικό δίκτυο, οι συγκεκριμένοι περιορισμοί μπορούν να υλοποιηθούν χρησιμοποιώντας τις ακόλουθες κατασκευές:

Controller: Ένας ελεγκτής δικτύου είναι ένα λογισμικό που ενορχηστρώνει τις λειτουργίες

του δικτύου. Χρησιμεύει ως ενδιάμεσος μεταξύ της επιχείρησης / οικίας και της υποδομής δικτύου. Αφού εισαχθούν οι στόχοι στον ελεγκτή τότε με την σειρά του δημιουργεί το δίκτυο κατάλληλα ώστε να επιτευχθούν οι στόχοι που αναφέρθηκαν. Οι ελεγκτές δικτύου υλοποιούν την εργασία τους με την αυτοματοποίηση και ανάλυση των λειτουργιών των συσκευών. Θα μπορούσαμε να περιγράψουμε γνωστές υπηρεσίες όπως το DNS ή το Πρωτόκολλο ώρας δικτύου (NTP). Ένας ελεγκτής δικτύου μπορεί να διασφαλίσει ότι τα μέτρα ασφαλείας είναι ενσωματωμένα στο δίκτυο.

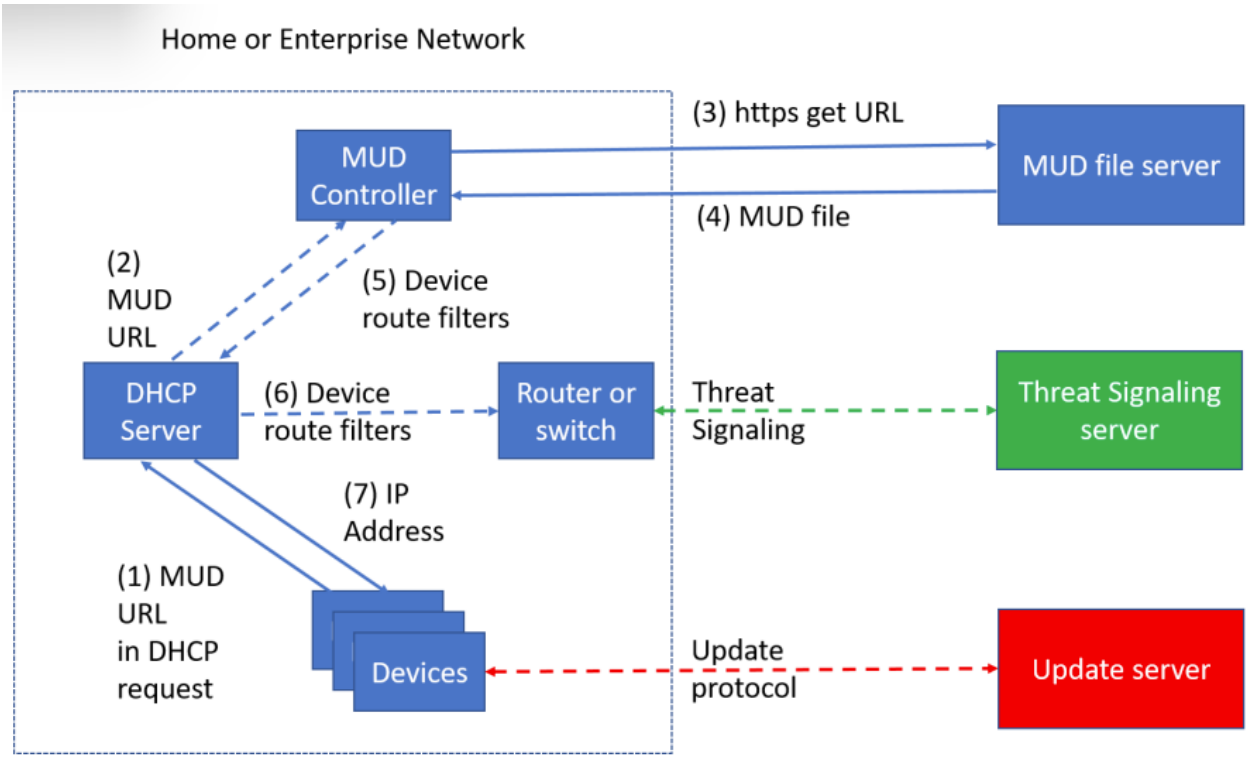
Τοπικά δίκτυα : Το τοπικό δίκτυο (LAN) είναι μια συλλογή συσκευών που συνδέονται μεταξύ τους σε μια φυσική τοποθεσία, στην περίπτωση μας είτε σε ένα οικιακό δίκτυο είτε σε μια μικρή επιχείρηση. Ένα LAN περιλαμβάνει καλώδια, σημεία πρόσβασης, διακόπτες, δρομολογητές και άλλα στοιχεία που επιτρέπουν στις συσκευές να συνδέονται με εσωτερικούς διακομιστές και διακομιστές Ιστού.

Same Manufacturer: Σε αυτή την περίπτωση βρίσκεται η κατηγορία των συσκευών οι οποίες ανήκουν στον ίδιο κατασκευαστή με την εν λόγω συσκευή IoT. Οι συγκεκριμένες συσκευές κατασκευάζονται από έναν συγκεκριμένο κατασκευαστή όπως προσδιορίζεται από το εξουσιοδοτημένο στοιχείο της διεύθυνσης URL MUD.

Αξίζει να σημειωθεί ότι ενώ το MUD απαιτεί τη χρήση ενός δρομολογητή με δυνατότητα MUD στο τοπικό δίκτυο, είτε αυτός ο δρομολογητής είναι αυτόνομος εξοπλισμός που παρέχεται από τρίτο προμηθευτή εξοπλισμού δικτύου είτε ενσωματωμένο με τον εξοπλισμό πύλης κατοικίας του παρόχου υπηρεσιών δεν σχετίζεται με την ικανότητα του MUD να προστατεύει το δίκτυο. Ενώ ένας πάροχος υπηρεσιών θα είναι ελεύθερος να υποστηρίξει το MUD στον εξοπλισμό και την υποδομή της πύλης Διαδικτύου, αυτή η υποστήριξη από τον πάροχοι υπηρεσιών Διαδικτύου (ISP) δεν είναι απαραίτητη. Ένα οικιακό δίκτυο ή ένα δίκτυο μικρών επιχειρήσεων μπορεί να επωφεληθεί από τις προστασίες που έχει να προσφέρει το MUD χωρίς οι πάροχοι υπηρεσιών Internet να χρειάζεται να κάνουν αλλαγές ή να παρέχουν οποιαδήποτε υποστήριξη εκτός από τη βασική σύνδεση στο Διαδίκτυο.

Το πρωτόκολλο MUD διαθέτει υποστήριξη για σηματοδότηση απειλών όπου παρέχεται για συσκευές με δυνατότητα MUD όσο και για συσκευές που δεν διαθέτουν την δυνατότητα MUD. Ο δρομολογητής (router) ή ο μεταγωγέας (swtich) μπορεί να λαμβάνει ροές απειλών από έναν πλασματικό διακομιστή σηματοδότησης απειλών για χρήση ως βάση για τον περιορισμό ορισμένων τύπων κυκλοφορίας δικτύου. Το αποτέλεσμα είναι ότι οποιαδήποτε συσκευή μπορεί να μην έχει την δυνατότητα συνδέσεις με τομείς Διαδικτύου που έχουν αναγνωριστεί ως κακόβουλοι.

2.3 Αρχιτεκτονική Αναφοράς
Σχήμα 2



Στο συγκεκριμένο σενάριο η συσκευές αποστέλλουν το MUD URL μέσω ενός αιτήματος DHCP. “Το Dynamic Host Configuration Protocol (DHCP) είναι ένα πρωτόκολλο πελάτη/διακομιστή που παρέχει αυτόματα σε έναν κεντρικό υπολογιστή πρωτοκόλλου Internet (IP) τη διεύθυνση IP του καθώς και άλλες σχετικές πληροφορίες όπως την μάσκα του υποδικτύου και την προεπιλεγμένη πύλη» ”. Ο DHCP Server εκχωρεί δυναμικές διευθύνσεις και επικοινωνεί με τον MUD Controller ο οποίος υπάρχει σε ένα οικιακό περιβάλλον ή σε μια μικρή επιχείρηση στο δίκτυο με σκοπό να ενισχύσει την δικτύωση του δρομολογητή ή του μεταγωγέα. Στο βήμα (3) ο MUD file Server παίρνει το αίτημα που περιέχει την URL μέσω του πρωτοκόλλου https το οποίο θεωρείται ασφαλέστερη και εξελιγμένη μορφή του http. “Ο MUD Controller ανακτά ένα αρχείο MUD από έναν ιστότοπο που δηλώνεται ως MUD Server” έχοντας τη δυνατότητα της λήψης, επαλήθευσης καθώς και επεξεργασίας αρχείων. Το αρχείο MUD περιγράφει τις απαιτήσεις και τους κανόνες επικοινωνίας για την κάθε συσκευή. Ο DNS ή το cloud φιλτράρουν ορισμένους τύπους κακόβουλης κίνησης οι οποίοι έρχονται ως ειδοποίηση στο router/switch μέσω του Threat Signaling Server. Ο δρομολογητής ή ο διακόπτης φιλτράρει τα πακέτα πληροφοριών στην κίνηση του δικτύου μέσω του BCP38 που επιτρέπει πακέτα εισόδου στο δίκτυο μόνο από εκχωρημένες IP ώστε να θωρακιστεί η ασφαλέστερη επικοινωνία. Το BCP38 αποτρέπει τις επιθέσεις DDoS μιας και απορρίπτει κάθε εισερχόμενο κακόβουλο πακέτο πληροφορίας. Οι συσκευές IoT ζητά μια IP διεύθυνση με την χρήση DHCP κατά την επέκταση MUD και έχουν την δυνατότητα επαλήθευσης και εφαρμογής ενημερώσεων λογισμικού.

2.4 Υποστήριξη MUD & Μηχανισμοί

Ο διαχειριστής MUD (MUD Manager) είναι ένα στοιχείο το οποίο εισάγεται έχοντας ως στόχο να αυξήσει την υπάρχουσα λειτουργικότητα δικτύωσης που προσφέρεται από τον δρομολογητή ή τον διακόπτη δικτύου της οικίας / της μικρής επιχείρησης. Ο διαχειριστής MUD είναι ένα λογικό στοιχείο και λαμβάνει το URL από τον router ή τον switch όπου αντίστοιχα έχει ληφθεί από τις συσκευές του περιβάλλοντα χώρου. Από την άλλη μεριά στέλνει μία μέθοδο που φιλτράρει την κίνηση των συσκευών η οποία χρησιμοποιείται για την παροχή ασφάλειας του δικτύου φιλτράροντας την κίνηση του δικτύου με βάση πολλούς τύπους κριτηρίων προτού φτάσει στις συσκευές δικτύου. Τα εν λόγω φίλτρα κυκλοφορίας χρησιμοποιούνται ως συσκευές προστασίας DDoS με κατάλληλο φίλτρο εισόδου, περιορισμού ρυθμού ώστε να μην λαμβάνουμε υπέρογκους αριθμούς πακέτων, αντίστροφη αναζήτηση διευθύνσεων και παρακολούθηση κυκλοφορίας δικτύου. Η λειτουργικότητα που παρέχει ο διαχειριστής MUD μπορεί και συνδυάζεται συχνά με αυτή του δρομολογητή δικτύου σε μία μόνο συσκευή.

Όλες οι συσκευές IoT έχουν άμεση σχέση με ένα αρχείο MUD. Η προδιαγραφή MUD περιγράφει τρεις πιθανούς μηχανισμούς μέσω των οποίων η συσκευή IoT μπορεί να παρέχει τη διεύθυνση URL του αρχείου MUD στο δίκτυο :

Μηχανισμός 1

Με την εισαγωγή της διεύθυνσης URL MUD σε αιτήματα διεύθυνσης DHCP τα οποία δημιουργούνται από την στιγμή που οι συσκευές συνδεθούνε στο δίκτυο. Χρησιμοποιώντας το DHCP μπορούμε να έχουμε μοναδικές διευθύνσεις IP και να ρυθμίζεται αυτόματα κάποιες πληροφορίες του δικτύου και προάγει την σωστή επικοινωνία των συσκευών εντός του δικτύου.

Μηχανισμός 2

Ένας πιθανός μηχανισμός είναι η παροχή μιας διεύθυνσης URL MUD στο Πρωτόκολλο Ανακάλυψης Επιπέδου Σύνδεσης (LLDP). Χρησιμοποιώντας το εν λόγω πρωτόκολλο οι πληροφορίες μίας συσκευής όπως για παράδειγμα το αναγνωριστικό πλαισίου, το id θύρας, η περιγραφή θύρας, οι διευθύνσεις IP/MAC καθώς και άλλες πληροφορίες μεταδίδονται στις γειτονικές συσκευές. Αυτές οι πληροφορίες αποθηκεύονται επίσης σε τοπικές Βάσεις Δεδομένων και μπορούν να αναζητηθούν με το Simple Network Managment Protocol (SNMP) το οποίο χρησιμοποιείται για την παρακολούθηση της δραστηριότητας του δικτύου και κατ' επέκταση για την παρακολούθηση των δικτυακών συσκευών.

Μηχανισμός 3

Παρέχοντας τη διεύθυνση URL MUD ως πεδίο σε ένα πιστοποιητικό X.509 που η συσκευή παρέχει στο δίκτυο μέσω ενός πρωτοκόλλου όπως το πρωτόκολλο EAP (Extensible Authentication Protocol). Το εν λόγω πρωτόκολλο χρησιμοποιείται για ασύρματα δίκτυα και οι μέθοδοί του έχουν σαν αποτέλεσμα μόνο οι χρήστες με κλειδί ελέγχου ταυτότητας ή κωδικό πρόσβασης να έχουν πρόσβαση στο δίκτυο.

Επιπλέον, η προδιαγραφή MUD παρέχει ευελιξία για την ενεργοποίηση άλλων μηχανισμών

μέσω των οποίων οι διευθύνσεις URL αρχείων MUD μπορούν να συσχετιστούν με συσκευές IoT. Ένας εναλλακτικός μηχανισμός είναι να συσχετιστεί η συσκευή με το αρχείο MUD χρησιμοποιώντας τις πληροφορίες που μεταφέρει η συσκευή ως μέρος της διαδικασίας ενσωμάτωσης του Wi-Fi Easy Connect όπου προσφέρει μία απλή και ασφαλή σύνδεση.
Το παραπάνω σχήμα απεικονίζει τα βήματα που απαιτούνται για την υποστήριξη MUD όταν μια συσκευή IoT εκπέμπει τη διεύθυνση URL του αρχείου MUD χρησιμοποιώντας έναν από τους μηχανισμούς που καθορίζονται στην προδιαγραφή MUD.

2.5 Υποστήριξη για Ενημερώσεις

Το πρωτόκολλο MUD προσφέρει υποστήριξη για τις ενημερώσεις των IoT συσκευών με σκοπό να παρέχεται πρόσθετη ασφάλεια. Οι εκδόσεις των ενημερώσεων ενσωματώνουν έναν διακομιστή ο οποίος αντιπροσωπεύει έναν διακομιστή ενημέρωσης στον οποίο το πρωτόκολλο MUD επιτρέπει την σύνδεση συσκευών. Για κάθε συσκευή που ανήκει σε ένα απολύτως λειτουργικό δίκτυο είναι απαραίτητο να γίνουν οι κατάλληλες ρυθμίσεις ώστε επικοινωνεί με τον διακομιστή ενημέρωσης για την λήψη και εφαρμογή ενημερώσεων κώδικα ασφαλείας, διασφαλίζοντας ότι εκτελεί τον πιο ενημερωμένο και ασφαλή διαθέσιμο κώδικα. Κάθε συσκευή IoT είναι αναγκαίο να επιτρέπει την επικοινωνία της με τον διακομιστή ενημερώσεων με σκοπό να μπορεί ανά πάσα στιγμή να λάβει την κάθε νέα ενημέρωση που είναι διαθέσιμη.

2.6 Υποστήριξη για Σηματοδότηση Απειλών

Προκειμένου να παρέχεται πρόσθετη ασφάλεια για τις συσκευές που διαθέτουν ή δεν διαθέτουν την δυνατότητα MUD η αρχιτεκτονική αναφοράς προσφέρει υποστήριξη ώστε να σηματοδοτούνται οι απειλές. Για την συγκεκριμένη ενέργεια ο δρομολογητής ή ο μεταγωγέας έχει την δυνατότητα να λαμβάνει ροές απειλών από τον διακομιστή σηματοδότησης απειλών ώστε να υπάρχει περιορισμός ορισμένων τύπων κυκλοφορίας δικτύου οι οποίες μπορούν να βλάψουν τις συσκευές στο περιβάλλοντα χώρο των συσκευών. Επομένως όλες οι συσκευές μπορούν να αποτρέψουν τη σύνδεσή τους σε ορισμένους τομείς του Διαδικτύου που έχουν αναγνωριστεί ως δυνητικά κακόβουλοι. Οι επικοινωνίες μεταξύ του διακομιστή σηματοδότησης απειλών και του δρομολογητή/διακόπτη δεν είναι τυποποιημένες

2.7 Ειδικά Χαρακτηριστικά Κατασκευής

Η αρχιτεκτονική αναφοράς εξηγεί πως κάθε κατασκευή την ενσωματώνει ανάλογα με τον εξοπλισμό που χρησιμοποιείται καθώς και τις δυνατότητες που υποστηρίζονται. Κατά κύριο λόγο οι τέσσερις εκδόσεις που υποστηρίζουν το MUD με δυνατότητα λήψης ψευδών ενημερώσεων μόνο το Build 2 υποστηρίζει σηματοδότηση απειλών ώστε να μην γίνει καμία κακόβουλη λήψη ή ενημέρωση στις συσκευές IoT. Δύο εκδόσεις όπου ενσωματώνουν μια άτυπη τεχνολογία εντοπισμού συσκευών με σκοπό την ανακάλυψη, την απογραφή καθώς και την ταξινόμηση των συνδεδεμένων συσκευών είναι οι εκδόσεις Build 1 και Build 2. Αυτή η ταξινόμηση μπορεί να χρησιμοποιηθεί για να επιβεβαιωθεί ότι η πρόσβαση που παρέχεται σε κάθε συσκευή είναι σύμφωνη με τον κατασκευαστή και το μοντέλο αυτής της συσκευής.

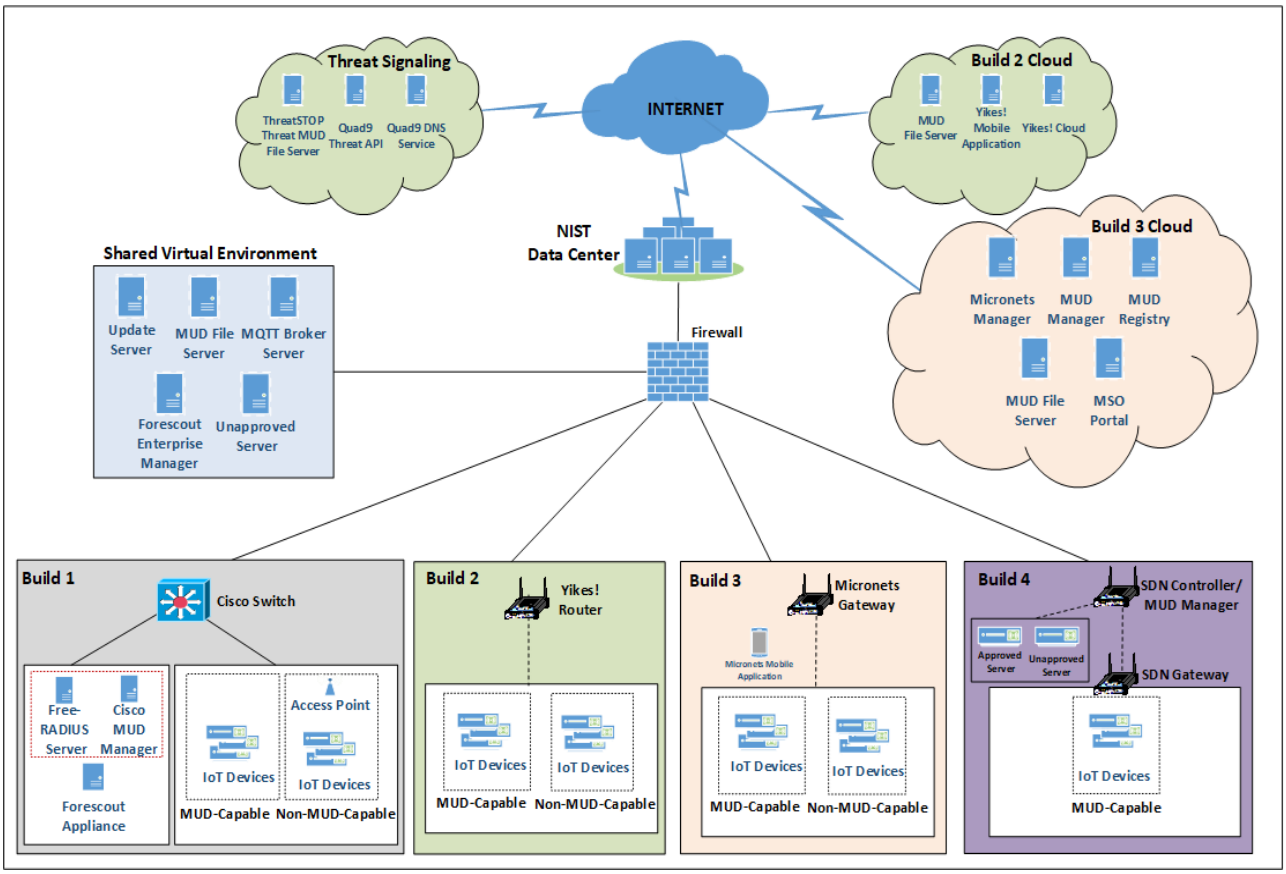
Το *Build 1* χρησιμοποιεί προϊόντα των Cisco Systems η οποία σχεδιάζει και εμπορεύεται ηλεκτρονικά προϊόντα, συσκευές δικτύωσης υπολογιστών, προϊόντα καθώς και υπηρεσίες τηλεπικοινωνιών.Επίσης χρησιμοποιεί προϊόντα Forescout και Molex. Ο διαχειριστής MUD της Cisco υποστηρίζει MUD και οι εικονικές συσκευές Forescout και ο διαχειριστής επιχειρήσεων εκτελούν εντοπισμό συσκευών που δεν σχετίζονται με το MUD στο δίκτυο. Το Molex Power over Ethernet (PoE) Gateway και το Light Engine χρησιμοποιούνται ως συσκευές IoT με δυνατότητα MUD. Χρησιμοποιούνται επίσης πιστοποιητικά από το DigiCert.

Στο *Build 2* όπως φαίνεται και στο παρακάτω σχήμα χρησιμοποιούνται προϊόντα από διάφορες εταιρείες στον χώρο της τεχνολογίας όπως από την MasterPeace Solutions που ασχολείται στον κυβερνοχώρο και στην ασφάλεια , την Ltd. GCA όπου παρέχει ηλεκτρονικά είδη και εξαρτήματα με σκοπό την δικτύωση του περιβάλλοντα χώρου, την ThreatSTOP που προσφέρει προστατευτικό DNS και αποτρέπει την καταστροφή από καθημερινές απειλές. Το ThreadSTOP αντιμετωπίζει τα κενά προστασίας τόσο για την εισερχόμενη όσο και για την εξερχόμενη κυκλοφορία δικτύου με αυτοματοποιημένη ευφυΐα απειλών που βασίζεται σε cloud μετατρέποντας τα πιο πρόσφατα δεδομένα απειλών σε πολιτικές επιβολής, ενημερώνοντας τις συσκευές για να σταματήσουν τις επιθέσεις προτού γίνουν παραβιάσεις. Τέλος παρέχεται ασφαλισμένος ιστότοπος ώστε να φιλοξενεί τους διακομιστές του συστήματός μας από την DigiCert. Στο Build 2 ο κατασκευαστής καθώς και το μοντέλο της κάθε συσκευής μπορούν να χρησιμοποιηθούν ως βάση για την εντοπισμό και την επιβολή του προφίλ επισκεψιμότητας της εν λόγω συσκευής.

Το *Build 3* εφαρμόζει το πρωτόκολλο Wi-Fi Easy Connect σε συσκευές με δυνατότητα MUD και μη, παρέχοντας έτσι με ασφάλεια σε κάθε συσκευή μοναδικά διαπιστευτήρια για σύνδεση στο δίκτυο. Με την χρήση του Wi-Fi Easy Connect παρέχεται μια απλή και ασφαλή μέθοδο για ενσωματωμένες συσκευές Wi-Fi σε ένα δίκτυο χωρίς την εισαγωγή κωδικού πρόσβασης δίνοντας την δυνατότητα οι συσκευές να αλληλεπιδρούν μεταξύ τους στον περιβάλλοντα χώρο.Το Build 3 χρησιμοποιεί προϊόντα από την CableLabs και την DigiCert. Η CableLabs είναι ένα σύστημα διαχείρισης δικτύου επόμενης γενιάς που παρέχει εξαιρετική ασφάλεια σε οικιακά δίκτυα και μικρές επιχειρήσεις. Χρησιμοποιεί τεχνολογίες όπως Software Defined Networking (SDN) που έχει ως πρωτεύοντα σκοπό να καθορίσει το δίκτυο.

Το *Build 4* χρησιμοποιεί λογισμικό που αναπτύχθηκε στο NIST Advanced Networking Technologies Laboratory. Αυτό το λογισμικό υποστηρίζει MUD και προορίζεται να χρησιμεύσει ως λειτουργικό πρωτότυπο της προδιαγραφής MUD για να αποδείξει τη σκοπιμότητα και την επεκτασιμότητα. Χρησιμοποιούνται επίσης πιστοποιητικά από το DigiCert.

2.8 Η Φυσική Αρχιτεκτονική



Το παραπάνω σχήμα δείχνει την φυσική αρχιτεκτονική υψηλού επιπέδου του εργαστηριακού περιβάλλοντος NCCoE. Όπως απεικονίζεται και στην εικόνα το δίκτυο εργαστηρίου NCCoE είναι συνδεδεμένο στο διαδίκτυο μέσω του κέντρου δεδομένων NIST. Λόγω της απόλυτης ασφάλειας που πρέπει να κατέχει το περιβάλλον μας η κίνηση από και προς το σύστημα προστατεύεται από ένα τείχος προστασίας ώστε να εμποδίσει τυχόν κακόβουλες κυκλοφορίες. Το δίκτυο περιβάλλεται από έναν κοινόχρηστο εικονικό περιβάλλον ο οποίος περιέχει τον Update Server όπου είναι υπεύθυνος για τυχόν νέες ενημερώσεις στο σύστημα μας , τον MUD File Server που διαχειρίζεται τα αρχεία του συστήματος, τον MQTT Broke Server που λαμβάνει όλα τα μηνύματα από όλο το περιβάλλον και τα δρομολογεί στον προορισμό , το ForeScout Enterprise Manager που είναι μία πλατφόρμα διαχείρισης ασφάλειας για συσκευές σε ένα δίκτυο και τον unapproved Server όπου καθορίζει την εγκυρότητα του διακομιστή.

Το Build 1 αποτελείται από έναν switch Cisco Catalyst 3850-S ώστε να είναι συνδεδεμένες όλες η συσκευές στο δίκτυο μεταξύ τους χάρις το μεγάλο εύρος των θυρών που διαθέτει, έναν διαχειριστή MUD Cisco, έναν διακομιστή FreeRADIUS και μια εικονική συσκευή Forescout στο τοπικό δίκτυο. Χρησιμοποιεί προϊόντα των Cisco Systems η οποία είναι μια επωνυμία πληροφορικής και δικτύωσης που ειδικεύεται στους διακόπτες (switches), στους δρομολογητές (routers), στην ασφάλεια στον κυβερνοχώρο και στο Internet of Things. Παράλληλα το συγκεκριμένο build χρησιμοποιεί προϊόντα της DigiCert καθώς το πιο σημαντικό μέρος ενός πιστοποιητικού SSL είναι ότι είναι ψηφιακά υπογεγραμμένο από μία αξιόπιστη αρχή όπως το

DigiCert. Στο build που αναλύουμε χρησιμοποιούνται επίσης προϊόντα της Forescout καθώς και Molex. Το Build 1 απαιτεί επίσης υποστήριξη από όλα τα στοιχεία που βρίσκονται στο κοινόχρηστο εικονικό περιβάλλον, συμπεριλαμβανομένου του διαχειριστή επιχειρήσεων Forescout.

Το Build 2 αποτελείται από έναν δρομολογητή Yikes! της MasterPeace Solutions Ltd στο τοπικό δίκτυο παρέχοντας μια ολοκληρωμένη λύση ασφάλειας δικτύου για μικρές και μεγάλες επιχειρήσεις καθώς και για οικιακά δίκτυα. Ο δρομολογητής Yikes! Έχει την δυνατότητα να αναγνωρίζει αυτόματα κάθε συνδεδεμένη συσκευή στο δίκτυο, να ασφαλίζει και ταξινομεί την επικοινωνία των συσκευών στο δίκτυο μας με τον συνδυασμό στρατηγικών από την μηχανική ασφάλειας δικτύου και την άμυνα των λειτουργιών δικτύου. Ο Yikes! Αυτοματοποιεί διαδικασίες ώστε να μειώνει τις επιθέσεις επιτρέποντας πιο ενεργές ειδοποιήσεις και διασφαλίζοντας τη σωστή επικοινωνία μεταξύ όλων των συσκευών. Αντιμετωπίζει απειλές τόσο από το Διαδίκτυο όσο και απειλές από άλλες συσκευές εντός του δικτύου όπως οι συσκευές επισκεπτών οι οποίες μπορεί να έχουν μολυνθεί και κατ' επέκταση να μολύνουν και το δίκτυο. Με την εφαρμογή της πιο πρόσφατης δικτύωσης και μικροτμηματοποίηση η οποία ορίζεται από λογισμικό παρέχει ασφάλεια επόμενης γενιάς για οικιακά δίκτυα και μικρές επιχειρήσεις. Το Build 2 χρειάζεται την υποστήριξη από υπηρεσίες cloud σηματοδότησης απειλών που αποτελούνται από τον διακομιστή αρχείων απειλής ThreadSTOP MUD, τη διεπαφή προγραμματισμού εφαρμογής απειλών Quad9 (API) καθώς και την υπηρεσία Quad9 DNS. Το Quad9 είναι μια δωρεάν υπηρεσία που αντικαθιστά τον προεπιλεγμένο ISP ή την διαμόρφωση του DNS.

Το Build 3 χρησιμοποιεί εξοπλισμό που παρέχεται από την CableLabs σε ενσωματωμένες συσκευές για την υποστήριξη MUD. Το εν λόγω build αξιοποιεί όλες τις προδιαγραφές Wi-Fi Easy Connect με σκοπό την ασφάλεια των συσκευών στο δίκτυο, με αυτόν τον τρόπο παρέχει μοναδικά διαπιστευτήρια δικτύου σε κάθε συσκευή. Με σκοπό την χρήση κάθε συσκευής αναλόγως την λειτουργία τους σε ξεχωριστές ζώνες όπως είναι τα τμήματα του δικτύου το build 3 χρησιμοποιεί το SDN. Η τεχνολογία δικτύωσης που ορίζεται από λογισμικό (SDN) είναι μια προσέγγιση στη διαχείριση δικτύου που επιτρέπει τη δυναμική διαμόρφωση δικτύου προκειμένου να βελτιωθεί η απόδοση και η παρακολούθηση του δικτύου. Η πλατφόρμα που χρησιμοποιεί το build 3 ονομάζεται micronets. Τα μικροδίκτυα αποτελούνται από μια εσωτερική πύλη με δυνατότητα Micronets που βρίσκεται στο δίκτυο της οικίας ή της μικρής επιχείρησης. Ένα μικροδίκτυο είναι μια ζώνη αξιοπιστίας που υλοποιείται ως τμήμα δικτύου και χρησιμοποιείται για την ομαδοποίηση συσκευών σε τομείς αξιοπιστίας που απομονώνουν συσκευές με βάση τη λειτουργία και την πολιτική πρόσβασής τους. Το Micronets Gateway διαχειρίζεται και επιβάλλει μικροδίκτυα για συγκεκριμένες υπηρεσίες και μικροδίκτυα που ορίζονται από τον πελάτη.

Το Build 2 Cloud , το Build 3 Cloud καθώς και η σηματοδότηση απειλών είναι συνδεδεμένες στο Διαδίκτυο . Το Build 2 Cloud περιέχει τον διακομιστή αρχείων MUD , την εφαρμογή κινητού Yikes η οποία μπορεί να δώσει στον χρήστη την δυνατότητα αλληλεπίδρασης με το περιβάλλον καθώς και το Cloud της εφαρμογής Yikes. Επίσης το Build 3 Cloud αποτελείται από τον διαχειριστή μικροδικτύων (micronets) , τον MUD Manager , το MUD Registry , τον διαχειριστή αρχείων MUD και το MSO Portal όπου παρέχει παρακολούθηση σε πραγματικό χρόνο.

Το Build 4 αποτελείται από μία πύλη με δυνατότητα δικτύωσης SDN που ορίζεται από λογισμικό στο τοπικό δίκτυο, από έναν ελεγκτή SDN / διαχειριστή MUD και εγκεκριμένους και μη εγκεκριμένους διακομιστές που βρίσκονται απομακρυσμένα από το τοπικό δίκτυο. Το build 4 χρησιμοποιεί επίσης τον διακομιστή αρχείων MUD που βρίσκεται στο κοινόχρηστο εικονικό περιβάλλον. Η υλοποίηση του Build 4 χρησιμοποιεί λογισμικό που ονομάζεται NIST-MUD που αναπτύχθηκε στο Εργαστήριο NIST Advanced Networking Technologies Laboratory. Ο σκοπός αυτής της υλοποίησης είναι να χρησιμεύσει ως ένα λειτουργικό πρωτότυπο του MUD RFC για να

αποδείξει τη σκοπιμότητα και την επεκτασιμότητα.Ο διαχειριστής NIST MUD υλοποιείται ως δυνατότητα που εκτελείται σε έναν ελεγκτή OpenDaylight SDN. Το Build 4 χρησιμοποιεί επίσης πιστοποιητικά από το DigiCert.

ΚΕΦΑΛΑΙΟ 3
ΑΝΑΛΥΣΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

Η ανάλυση χαρακτηριστικών ασφαλείας δείχνει τον βαθμό κατανόησης του έργου να ανταποκρίνεται στον στόχο του με σκοπό να φανεί η ικανότητα αναγνώρισης στοιχείων IoT στους διαχειριστές MUD καθώς και η διαχείριση της πρόσβασης στα στοιχεία περιορίζοντας ταυτόχρονα τη μη εξουσιοδοτημένη πρόσβαση από και προς τα στοιχεία που βρίσκονται στο περιβάλλον. Με αυτόν τον τρόπο είναι εμφανή και αναλύονται τα οφέλη ασφάλειας της συγκεκριμένης προσέγγισης. Μέσω της ανάλυσης χαρακτηριστικών ασφάλειας μπορεί να ενημερωθεί η ανάπτυξη ενός σχεδίου ασφάλειας.

Η ανάλυση χαρακτηριστικών ασφάλειας απαρτίζεται από περιορισμούς και υποθέσεις με σκοπό την επίτευξη του έργου. Η ανάλυση δεν αποτελεί μια ολοκληρωμένη δοκιμή όλων των στοιχείων ασφάλειας ούτε μια άσκηση της κόκκινης ομάδας. Η κόκκινη ομάδα (Red Team) είναι ηθικοί hacker που βοηθούν στη δοκιμή άμυνας εντοπίζοντας τρωτά σημεία και εξαπολύοντας επιθέσεις σε ένα ελεγχόμενο περιβάλλον. Μέσω της ανάλυσης δεν μπορεί να εντοπιστούν όλες οι αδυναμίες του συστήματος. Η ανάλυση των χαρακτηριστικών ασφάλειας δεν μπορεί να περιλαμβάνει την εργαστηριακή υποδομή του έργου. Η δοκιμή αυτών των συσκευών θα αποκάλυπτε μόνο τις αδυναμίες που έχουν στην υλοποίηση. Για την ανάλυση των χαρακτηριστικών ασφάλειας είναι απαραίτητος ο σχεδιασμός ασφάλειας του συστήματος με σκοπό την βελτίωση της προστασίας των πόρων του συστήματος πληροφοριών. Η προστασία ενός συστήματος πρέπει να τεκμηριώνεται σε ένα σχέδιο ασφάλειας συστήματος. Σκοπός του σχεδίου ασφάλειας συστήματος είναι να παρέχει μια επισκόπηση των απαιτήσεων ασφαλείας του συστήματος και να περιγράψει τους ελέγχους που υπάρχουν ή σχεδιάζονται για την εκπλήρωση αυτών των απαιτήσεων. Ένα ένα περιβάλλον όπου απαρτίζεται από συσκευές IoT είναι πιθανό να έρχεται σε αλληλεπίδραση με περισσότερα από ένα άτομο. Για τον συγκεκριμένο λόγο το σχέδιο ασφάλειας συστήματος οριοθετεί τις ευθύνες καθώς και την αναμενόμενη συμπεριφορά όλων των ατόμων που έχουν πρόσβαση στο σύστημα.

3.1 Χάρτης Ελέγχου Ασφαλείας

Η ανάλυση των χαρακτηριστικών ασφάλειας διαθέτει πολλές πτυχές και φάσεις ώστε να ολοκληρωθεί. Μία πτυχή της είναι η αξιολόγηση του κατά πόσο καλός είναι ο σχεδιασμός αναφοράς και πώς αντιμετωπίζει τα χαρακτηριστικά ασφάλειας που πρόκειται να υποστηρίξει. Κάθε πλαίσιο ασφάλειας αναφέρεται κατηγορίες καθώς και υποκατηγορίες. Για την παροχή δομής στην αξιολόγηση ασφάλειας χρησιμοποιούνται οι υποκατηγορίες Πλαισίου Κυβερνοασφάλειας. Με την χρήση των υποκατηγοριών Πλαισίου Κυβερνοασφάλειας για την οργάνωση της ανάλυσης επιτρέπεται η συστηματική εξέταση για το πόσο καλή είναι η σχεδίαση αναφοράς και αν υποστηρίζει τα χαρακτηριστικά ασφαλείας. Η ανάλυση πραγματοποιείται σε σενάρια χρήσης οικιακών δικτύων και μικρών επιχειρήσεων.

3.2 Προστασία Πληροφοριών και Συστημάτων με Έλεγχο Ασφάλειας και Απορρήτου

Με την άνοδο του τεχνολογικού τομέα και την εφαρμογή και δημιουργία όλο και μεγαλύτερων τεχνολογικών επιτευγμάτων διογκώνεται η ανάγκη για προστασία πληροφοριών καθώς και συστημάτων. Τα σύγχρονα πληροφοριακά συστήματα μπορούν να περιλαμβάνουν ποικίλες πλατφόρμες υπολογιστών όπως υπολογιστικά συστήματα γενικής χρήσης ώστε να καλύψουν τις ανάγκες των ατόμων που διαμένουν σε μια οικία ή των μικροεπιχειρήσεων. Σε ένα τέτοιο σύστημα υπάρχει επίσης κατάλληλο σύστημα επικοινωνιών για την σωστή επικοινωνία μεταξύ των συσκευών καθώς και ενσωματωμένες συσκευές με κατάλληλο λογισμικό και υλικό που θα εξυπηρετεί όλες τις ανάγκες. Οι περισσότεροι χρήστες διαθέτουν σταθερούς ή φορητούς υπολογιστές , κινητές συσκευές ακόμα και tablet. Όλες αυτές οι πλατφόρμες μοιράζονται μια κοινή υπολογιστική βάση με πολύπλοκο υλικό και λογισμικό με μοναδικό στόχο την υποστήριξη των λειτουργιών για τους χρήστες. Οι έλεγχοι ασφάλειας που χρησιμοποιούνται στο σύστημα είναι υπεύθυνοι για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας του συστήματος. Μέσω την διαχείρισης κινδύνου ασφάλειας πληροφοριών το σύστημα είναι σε θέση να μετριάσει κάθε κίνδυνο και διαρροή ευαίσθητων πληροφοριών και δεδομένων έτσι ώστε να είναι ακέραια η ιδιωτικότητα. Η παροχή ικανοποιητικών ελέγχων ασφαλείας σε ένα σύστημα υπολογιστή αποτελεί πρόβλημα σχεδιασμού συστήματος. Γι’ αυτό τον λόγο απαιτείται συνδυασμός υλικού, λογισμικού, επικοινωνιών και προσωπικών και διαδικαστικών διασφαλίσεων για ολοκληρωμένη ασφάλειας.Οι διασφαλίσεις μόνο του λογισμικού είναι ανεπαρκής. (Defense Science Board Task Force on Computer Security, 1970).

3.3 Πλαίσιο Διαχείρισης Κινδύνων (RMF)

Το Πλαίσιο Διαχείρισης Κινδύνων παρέχει μια διαδικασία που ενσωματώνει την ασφάλεια, το απόρρητο και τις δραστηριότητες διαχείρισης κινδύνου της αλυσίδας εφοδιασμού στον κυβερνοχώρο και στον κύκλο ζωής ανάπτυξης του συστήματος. Η προσέγγιση βάσει κινδύνου για την επιλογή και την προδιαγραφή ελέγχου λαμβάνει υπόψη την αποτελεσματικότητα, την αποδοτικότητα και τους περιορισμούς που οφείλονται σε ισχύοντες νόμους, οδηγίες, εκτελεστικές εντολές, πολιτικές, πρότυπα ή κανονισμούς. Η διαχείριση του οργανωτικού κινδύνου είναι πρωταρχικής σημασίας για αποτελεσματικά προγράμματα ασφάλειας πληροφοριών και απορρήτου. Η προσέγγιση RMF μπορεί να εφαρμοστεί σε νέα και παλαιού τύπου συστήματα, οποιουδήποτε τύπου συστήματος ή τεχνολογίας (π.χ. IoT, συστήματα ελέγχου) και σε οποιονδήποτε τύπο

οργανισμού ανεξαρτήτως μεγέθους ή τομέα. Το RMF παρέχει μια πειθαρχημένη , δομημένη και ευέλικτη διαδικασία για τη διαχείριση κινδύνου. Επίσης περιλαμβάνει κατηγοριοποίηση ασφάλειας πληροφοριών, ελέγχου επιλογής , υλοποίησης και αξιολόγησης σε ένα φάσμα συνεχής παρακολούθησης. Το RMF προωθεί τη διαχείριση κινδύνων σε πραγματικό χρόνο.

Ένα πλαίσιο διαχείρισης κινδύνου είναι μία δομημένη διαδικασία που χρησιμοποιείται για τον εντοπισμό πιθανών απειλών για την εξάλειψη ή την ελαχιστοποίηση των επιπτώσεων των εν λόγω κινδύνων. Ο σκοπός του RMF είναι η ενημέρωση των διαδικασιών διαχείρισης κινδύνου του οικιακού περιβάλλοντος ή της μικρής επιχείρησης. Η διαχείριση κινδύνου επιτρέπει την επίτευξη ισορροπίας μεταξύ της ανάληψης κινδύνων και της μείωσής τους. Ορίζουμε ως κίνδυνο την πιθανότητα για ανεξέλεγκτη απώλεια κάτι που έχει αξία. Κίνδυνο επίσης εμπεριέχει η αβεβαιότητα. Το πλαίσιο διαχείρισης κινδύνου διαθέτει τρία στάδια. Αρχικά είναι απαραίτητη η ταυτοποίηση του κινδύνου ώστε να υπάρχει η σιγουριά ότι η συγκεκριμένη ενέργεια οδηγεί σε αβέβαιο καθώς και κακόβουλο αποτέλεσμα. Ο κόσμος του κινδύνου είναι μία λίστα με όλους τους πιθανούς κινδύνους που καλεί το RMF να αντιμετωπίσει. Στη συνέχεια ακολουθεί η εκτίμηση του κινδύνου με αποτέλεσμα να υπάρχει μια γενική εικόνα του μεγέθους του άρα και της σοβαρότητας της κατάστασης. Η μέτρηση του κινδύνου παρέχει πληροφορίες για την ποσότητά του καθώς και μία συνολική εικόνα για τυχόν απώλεια. Υπάρχουν διάφορα μέσα και τεχνάσματα ώστε να εκτιμηθεί και να μετρηθεί κατάλληλα ένας κίνδυνος. Τέλος ο μετριασμός του κινδύνου είναι καταλυτικό στάδιο, το οποίο θα δώσει λύση και εξάλειψη χωρίς να υπάρξουν καταστροφές , απώλεια ή και διάρρευση προσωπικών δεδομένων. Αφού έχουν αναγνωριστεί και κατηγοριοποιηθεί οι κίνδυνοι στη συνέχεια μπορεί να παρθεί η απόφαση για την αντιμετώπιση τους.

3.4 Χαρακτηριστικά Υλοποίησης & Προσεγγίσεις

Το πλαίσιο NIST (NIST CSF) είναι μία δημιουργία της Βιομηχανίας της Πληροφορικής και της κυβέρνησης των Ηνωμένων Πολιτειών Αμερικής με σκοπό τον μετριασμό κινδύνων στον Κυβερνοχώρο. Το NIST Cyber Security Framework προετοιμάζει τους υπεύθυνους ασφάλειας για τον εντοπισμό επιθέσεων και παρέχει μέτρα πρόληψης και τρόπους αντίδρασης. Το πλαίσιο μέσω των λειτουργιών ***Αναγνώρισης (Identify)***, ***Προστασίας (Protect)*** , ***Ανίχνευσης (Detect)*** , ***Απόκρισης (Respond)*** και ***Ανάρρωσης (Recover)*** κατηγοριοποιεί όλες τις δυνατότητες Κυβερνοασφάλειας**.**

Μέσω της **Αναγνώρισης** δίνεται η δυνατότητα καλύτερης κατανόησης καθώς και διαχείρισης του κάθε κινδύνου που προσπαθεί να βλάψει το σύστημα, κάποιο περιουσιακό στοιχείο ακόμα και δεδομένα. Διαθέτει το Asset Management(ID.AM), το επιχειρηματικό περιβάλλον (ID.BE), την Διακυβέρνηση (ID,GV), την εκτίμηση κινδύνου (ID.RA) και τη στρατηγική διαχείρισης κινδύνων (ID.RM).

Με την συνάρτηση της **Προστασίας** διασφαλίζεται η παροχή υπηρεσιών ζωτικής σημασίας. Περιλαμβάνει την κατηγορία του ελέγχου πρόσβασης (PR.AC), την ευαισθητοποίηση και εκπαίδευση των χρηστών για ασφάλεια στον Κυβερνοχώρο (PR.AT), την ασφάλεια δεδομένων σύμφωνα με τις στρατηγικές κινδύνου (PR.DS), τις διαδικασίες προστασίας πληροφοριών (PR.IP), την συντήρηση των συστημάτων πληροφοριών (PR.MA) και την προστατευτική τεχνολογία με σκοπό τις λύσεις τεχνικής ασφάλειας (PR.PT).

Μέσω της **Ανίχνευσης** και του εντοπισμού κακόβουλων κινήσεων και συμβάντων θέτεται πιο ασφαλές το σύστημα. Στην συγκεκριμένη συνάρτηση περιλαμβάνονται οι Ανωμαλίες και τα Συμβάντα (DE.AE), η Συνεχής Παρακολούθηση Ασφάλειας (DE.CM) και οι Διαδικασίες Ανίχνευσης (DE.DP).

Το πλαίσιο Κυβερνοασφάλειας NIST διαθέτει την συνάρτηση της **Απόκρισης** η οποία με την σειρά της περιέχει τον Σχεδιασμό Απόκρισης (RS.RP) με σκοπό την έγκαιρη απόκριση σε τυχόν εντοπισμένα συμβάντα στον Κυβερνοχώρο, τις Επικοινωνίες (RS.CO), την Ανάλυση (RS.AN), τον Μετριασμό (RS.MI) και τις Βελτιώσεις (RS.IM).

Η συνάρτηση της **Ανάρρωσης** συμβάλει στην εφαρμογή δραστηριοτήτων για την ανθεκτικότητα και την αποκατάσταση περιλαμβάνοντας την Σχεδίαση Ανάκτησης για έγκυρη αποκατάσταση (RC.RP), τις βελτιώσεις στον σχεδιασμό (RC.IM) και τις επικοινωνίες (RC.CO).

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Το NIST SP 800-53 διαθέτει μεγάλο εύρος στοιχείων ελέγχου όπου είναι περισσότερα από 1000. Αυτοί οι έλεγχοι ασφάλειας και απορρήτου βοηθούν στον μετριασμό από επιθέσεις στον κυβερνοχώρο και σε άλλα ζητήματα ασφάλειας. Στον παρακάτω πίνακα θα αναφερθούν μερικά από τα σημαντικότερα στοιχεία ελέγχου όπου ένα εύρος τους θα χρησιμοποιηθεί στις προσεγγίσεις.

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

Προσέγγιση 1

Το σύστημα περιλαμβάνει μηχανισμούς για κάθε συσκευή που κατέχει διεύθυνση URL την οποία μπορεί να χρησιμοποιήσει κατάλληλα με σκοπό τον εντοπισμό καθώς και τον εντοπισμό του αρχείου MUD της. Η εν λόγω εκπομπή μπορεί να πραγματοποιηθεί με ποικίλους τρόπους. Όταν η κάθε συσκευή είναι συνδεδεμένη στο οικιακό δίκτυο ή στην μικρή επιχείρηση τότε έχει την δυνατότητα να εκπέμπει τη διεύθυνση URL του αρχείου MUD της μέσω αιτημάτων διεύθυνσης DHCP όπου είναι ένας μηχανισμός διαχείρισης πρωτοκόλλων TCP/IP. Μέσω του Πρωτοκόλλου Ανακάλυψης Επιπέδου Σύνδεσης (Link Layer Discovery Protocol) είναι δυνατή είναι δυνατόν ο εντοπισμός του URL MUD εναλλακτικά μπορεί να βρεθεί στο πιστοποιητικό X.509. Μία διεύθυνση URL MUD έχει την δυνατότητα να αποκομίσει πλήθος πληροφοριών μέσω του δικτύου με την βοήθεια άλλων μέσων. Η κάθε συσκευή διαθέτει ενσωματωμένο το αναγνωριστικό της. Στο περιβάλλον χρησιμοποιείται το απόθεμα στοιχείων συστήματος CM-8 το οποίο απεικονίζει το σύστημα περιλαμβάνοντας όλα τα στοιχεία του συστήματος και όχι άλλα στοιχεία που έχουν εκχωρηθεί σε οποιοδήποτε άλλο σύστημα. Το CM-8 είναι απαραίτητο για την παρακολούθηση και την αναφορά ενώ για την απογραφή του συστήματος χρησιμοποιείται το PM-5. Μέσω του NIST Cybersecurity Framework ID.AM-1 υπάρχει η γνώση για όλες τις συσκευές και τα συστήματα όπου περιλαμβάνονται στο οικιακό δίκτυο ή στο δίκτυο της μικρής επιχείρησης.

Προσέγγιση 2

Συσκευές οι οποίες υποστηρίζουν το πρωτόκολλο Wifi – Easy Connect οι οποίες είναι ρυθμισμένες με το δικό τους ζεύγος δημόσιου και ιδιωτικού κλειδιού bootstrapping. Το μενού κλειδιών Bootstrap περιέχει τα κλειδιά εξουσιοδότησης που είναι απαραίτητα για την εκκίνηση απομακρυσμένων συσκευών. Το μενού δίνει την δυνατότητα της αυτόματης αποδοχής συσκευών χωρίς να είναι απαραίτητη η χειροκίνητη αλληλεπίδραση. Ένα κλειδί μπορεί να χειρίζεται ένα συγκεκριμένο πλήθος συσκευών οι οποίες αντιστοιχούν σε μία συγκεκριμένη ομάδα. Επιπρόσθετα είναι εφικτή η προσθήκη πολλαπλών κλειδιών και ο ορισμός πολλαπλών πλήκτρων εκκίνησης. Για την ασφάλεια του περιβάλλοντα χώρου καθώς και των συσκευών είναι δυνατή η ανάκληση των κλειδιών bootstrap. Η κάθε συσκευή όπως και στη Προσέγγιση 1 έχει ενσωματωμένο μοναδικό αναγνωριστικό και διαθέτει CM-8, PM-5 και ID.AM-1.

Προσέγγιση 3

Μία διεύθυνση URL του MUD File δίνει της πληροφορία του τύπου της κάθε συσκευής και προωθείται στον MUD Manager. Ο MUD Manager με την σειρά του ανακτά ένα αρχείο MUD χρησιμοποιώντας το https πρωτόκολλο το οποίο θεωρείται πιο ασφαλές από το http λόγω της κρυπτογράφησης του. Κάθε συσκευή έχει ορισμένες απαιτήσεις επικοινωνίας για την ομαλή της λειτουργία στο οικιακό δίκτυο ή στο δίκτυο μικρής επιχείρησης , οι οποίες καλύπτονται από το αρχείο MUD. Με την σειρά του ο MUD Manager μετατρέπει αυτές τις απαιτήσεις σε πληροφορίες ελέγχου πρόσβασης για επιβολή από το δρομολογητή ή το διακόπτη. Η κάθε συσκευή μπορεί να διασυνδέεται με συστήματα διαχείρισης περιουσιακών στοιχείων της επιχείρησης ή της οικίας. Η διαχείριση περιουσιακών στοιχείων είναι ένας συνδυασμός λογισμικού, συστημάτων και υπηρεσιών που χρησιμοποιούνται για τη συντήρηση και τον έλεγχο περιουσιακών στοιχείων και εξοπλισμού.

Στην εποχή του Διαδικτύου των Πραγμάτων και την ραγδαία εξέλιξη της τεχνολογίας όπου πλήθος συσκευών είναι συνδεδεμένες με αισθητήρες και συστήματα, ενσωματώνονται προηγμένα αναλυτικά στοιχεία και Τεχνητή Νοημοσύνη στη Διαχείριση Περιουσιακών Στοιχείων. Παρέχει το AC-3 Access Enforcement για λογική πρόσβαση σε πληροφορίες και πόρους του συστήματος καθώς και το AC-18 για ασύρματη πρόσβαση στο σύστημα. Η εν λόγω προσέγγιση παρέχει το Cm-7 με σκοπό την ρύθμιση του συστήματος ώστε να παρέχει μόνο βασικές δυνατότητες και να απαγορεύει ή να περιορίζει την χρήση ορισμένων λειτουργιών όπως ορισμένες θύρες , χρήση λογισμικού, πρωτόκολλα ή/και υπηρεσίες.

Για την προστασία άρνησης υπηρεσίας όπου θα συμβάλει στην αντιμετώπιση των επιθέσεων DDoS χρησιμοποιείται το στοιχείο ελέγχου SC-5 έτσι ώστε οι προστατευόμενες συσκευές να μπορούν να φιλτράρουν ορισμένους τύπους πακέτων πληροφοριών με αποτέλεσμα να κρατούν ασφαλή το δίκτυο. Στην ίδια οικογένεια στοιχείων ελέγχου βρίσκεται και το SC-7 που ελέγχει τις επικοινωνίες εντός και εκτός των ορίων του συστήματος. Μέσω της τεχνικής της πλαστογράφησης ο κυβερνοεγκληματίας μπορεί να δώσει την εντύπωση στο σύστημα ότι τα πακέτα πληροφοριών, μια διεύθυνση IP, ένα DNS , καθώς και άλλες πηγές προέρχονται από μια αξιόπιστη πηγή.

Η πλαστογράφηση καθώς και η αποκάλυψη πληροφοριών του συστήματος ή των χρηστών μπορούν να εξαλειφθούν με το AC-4. Παράλληλα εφαρμόζοντας το AC-6 παρέχεται ο απαραίτητος έλεγχος ώστε να επιτρέπεται αποκλειστικά η χρήση από εξουσιοδοτημένες συσκευές οι οποίες είναι απαραίτητες. Μέσω του στοιχείου ελέγχου AC-24 υπάρχει η δυνατότητα αποφάσεων για τον έλεγχο πρόσβασης στο σύστημα οι οποίες προκύπτουν όταν οι πληροφορίες εξουσιοδότησης εφαρμόζονται σε συγκεκριμένες προσβάσεις.

Με το CM-8 απεικονίζεται το σύστημα καθώς και τα στοιχεία που υπάρχουν σε αυτό ενώ με την χρήση του PM-5 δίνεται η δυνατότητα δημιουργίας, διατήρησης καθώς και ενημέρωσης του αποθέματος του συστήματος και των εφαρμογών που επεξεργάζονται πληροφορίες. Είναι κρίσιμης ανάγκης ο έλεγχος της πρόσβασης στο σύστημα με σκοπό την ενσωμάτωση της ελάχιστης λειτουργικότητας χρησιμοποιώντας το PR.PT-3. Για την καταγραφή των συσκευών υποστηρίζει το ID.AM-1, παράλληλα το ID.AM-2 για την καταγραφή της κάθε πλατφόρμας λογισμικού και εφαρμογής εντός του οικιακού δικτύου ή της μικρής επιχείρησης.

Η χαρτογράφηση επικοινωνιών και των ροών δεδομένων υλοποιούνται με το ID.AM-3. Όλες οι συσκευές του συστήματος διαθέτουν άδεια πρόσβασης η οποία διαχειρίζεται με το PR.AC-4 και έχει την δυνατότητα να παραχωρήσει σε έναν χρήστη ή μια διεργασία πρόσθετη πρόσβαση στο σύστημα χωρίς εξουσιοδότηση. Το κάθε δίκτυο έχει δυνατότητες διαχωρισμού αλλά και

τμηματοποίησης η οποία είναι μία διαδικασία διαίρεσης του δικτύου με σκοπό την βελτίωση απόδοσης και ασφάλειας. Η ακεραιότητα του δικτύου αναλαμβάνεται από το PR.AC-5. Σε ένα σύστημα IoT είναι απαραίτητο να μην υπάρχει διαρροή δεδομένων και ασφάλεια πληροφοριών η οποία αποφεύγεται μέσω του PR.DS-5 όπου διαχειρίζεται πληροφορίες και αρχεία δεδομένων θέτοντας ένα πλάνο προστασίας της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών. Με το στοιχείο DE.AE-1 του NIST Cybersecurity Framework δημιουργούνται και διαχειρίζονται οι λειτουργίες του δικτύου καθώς και οι ροές δεδομένων των χρηστών και των συστημάτων.

Προσέγγιση 4

Η κάθε συσκευή στο οικιακό δίκτυο ή στο δίκτυο της μικρής επιχείρησης επικοινωνεί τακτικά με τον server ενημερώσεων με σκοπό την λήψη νέων ενημερώσεων κώδικα ασφάλειας. Ο κατασκευαστής θα παρέχει ενημερώσεις κώδικα ή αναβαθμίσεις για όλο το λογισμικό και το υλικολογισμικό καθ' όλη τη διάρκεια ζωής κάθε συσκευής. Για τον εντοπισμό , την αναφορά και την διόρθωση ελαττωμάτων του συστήματος πληροφοριών χρησιμοποιείται το SI-02. Με το PR.IP-1 δημιουργείται και διατηρείται η διαμόρφωση συστήματος τεχνολογίας πληροφοριών ενσωματώνοντας τις αρχές ασφάλειας. Σύμφωνα με το PR.IP-3 τίθενται σε εφαρμογή ορισμένες διαδικασίες ελέγχου αλλαγής διαμόρφωσης.

Προσέγγιση 5

Σε αυτή την προσέγγιση ο Server σηματοδότησης απειλών ενημερώνει τον router ή τον switch για τον εντοπισμό κακόβουλων κινήσεων με σκοπό τον περιορισμό των συγκεκριμένων τύπων κυκλοφορίας δικτύου. Μέσω της τροποποίησης του συστήματος ή των δεδομένων με διάφορους τρόπους θέτεται πιο ασφαλές το δίκτυο και κατ’ επέκταση ολόκληρο το έργο IoT. Η κάθε συσκευή είτε υποστηρίζει τη χρήση σαρωτών ευπάθειας είτε παρέχει ενσωματωμένες δυνατότητες αναγνώρισης ευπάθειας και αναφοράς.

Υποστηρίζει το AC-24 για τις αποφάσεις ελέγχου πρόσβασης. Για την καλύτερη εκτίμηση κινδύνου υποστηρίζεται το RA-5 όπου με τις τεχνικές σάρωσης ενημερώνει για τυχόν τρωτά σημεία που είναι απαραίτητο να σαρωθούν και μπορεί να αναλάβει μεγάλο πλάτος και βάθος κάλυψης. Οι ειδοποιήσεις για την ασφάλεια , οι συμβουλές καθώς και οι οδηγίες είναι πολύ σημαντικές για την ακεραιότητα του συστήματος και καλύπτονται από το SI-5.

Με την υποστήριξη του ID.RA-2 και ID.RA-3 πληροφορίες για εσωτερικές ή εξωτερικές απειλές λαμβάνονται από διάφορες πηγές ανταλλαγής πληροφοριών, εντοπίζονται και τεκμηριώνονται ενώ με το DE.CM-8 πραγματοποιούνται σαρώσεις ευπάθειας.

Προσέγγιση 6

Με την χρήση του Wi-Fi Easy Connect σε ενσωματωμένες συσκευές εξασφαλίζει ότι δεν είναι απαραίτητη η γνώση των διαπιστευτηρίων δικτύου της κάθε συσκευής. Το πρωτόκολλο ενσωμάτωσης παρέχει τα διαπιστευτήρια δικτύου στη συσκευή αυτόματα, χρησιμοποιώντας ένα

ασφαλές κανάλι, και στη συνέχεια η συσκευή μπορεί να παρουσιάσει τα διαπιστευτήριά της στο δίκτυο ως μέρος της τυπικής χειραψίας σύνδεσης δικτύου Wi-Fi. Δεν χρειάζεται να εισαχθεί ο κωδικός πρόσβασης δικτύου της συσκευής από άνθρωπο και τα διαπιστευτήρια δεν εμφανίζονται ποτέ, επομένως η παρουσίαση των διαπιστευτηρίων δικτύου της συσκευής στο δίκτυο δεν ενέχει κανέναν κίνδυνο να προβληθούν τα διαπιστευτήρια και να αποκαλυφθούν σε τρίτους.
Η συσκευή μπορεί να αποκρύψει χαρακτήρες κωδικού πρόσβασης από την οθόνη όταν ένα άτομο εισάγει έναν κωδικό πρόσβασης από συσκευές εισόδου όπως το πληκτρολόγιο ή μια οθόνη αφής.

Υποστηρίζει IA-6 με σκοπό τα σχόλια ελέγχου ταυτότητας και παρέχει PR.AC-7 ώστε οι χρήστες , οι συσκευές και άλλα στοιχεία να ελέγχονται κατάλληλα ανάλογα με τον κίνδυνο της συναλλαγής τους. Με την υποστήριξη του IA-6 το σύστημα πληροφοριών αποκρύπτει την ανατροφοδότηση πληροφοριών ελέγχου ταυτότητας κατά την διαδικασία ελέγχου ταυτότητας με σκοπό να προστατεύσει τις πληροφορίες από πιθανή εκμετάλλευση και χρήση από μη εξουσιοδοτημένα άτομα. Τα σχόλια από το σύστημα πληροφοριών δεν παρέχουν πληροφορίες που θα επέτρεπαν σε μη εξουσιοδοτημένο χρήστη να υπονομεύσει τον μηχανισμό ελέγχου ταυτότητας. Η εμφάνιση αστερίσκων όταν ένας χρήστης πληκτρολογεί έναν κωδικό πρόσβασης είναι ένα παράδειγμα απόκρυψης ανατροφοδότησης πληροφοριών ελέγχου ταυτότητας.

Προσέγγιση 7

Ο διακομιστής MUD λαμβάνει την διεύθυνση URL του MUD file από έναν ορισμένο ιστότοπο ο οποίος είναι ο διακομιστής των αρχείων που χρησιμοποιεί το ασφαλή πρωτόκολλο https. Ο MUD File Server πρέπει να διαθέτει ένα έγκυρο TLS καθώς και το ίδιο αρχείο MUD πρέπει να περιέχει έγκυρη υπογραφή. Το Transport Layer Security (TLS) και το Secure Sockets Layer (SSL) είναι πρωτόκολλα κρυπτογράφησης που παρέχουν ασφάλεια επικοινωνίας σε ένα δίκτυο υπολογιστών. Οι απαιτήσεις κάθε συσκευής περιγράφονται από το αρχείο MUD ενώ παράλληλα ο διαχειριστής MUD μετατρέπει αυτές τις απαιτήσεις σε πληροφορίες ελέγχου πρόσβασης για επιβολή από το δρομολογητή. Η κάθε συσκευή έχει την δυνατότητα να χρησιμοποιεί ελέγχους ταυτότητας και μηχανισμούς ελέγχου ταυτότητας.

Το πληροφοριακό σύστημα του οικιακού περιβάλλοντος ή της μικρής επιχείρησης επαληθεύει μοναδικά όλους τους οργανωμένους χρήστες που αλληλοεπιδρούν με το σύστημα με την βοήθεια του υποστηριζόμενου IA-2. Με τον διαχειριστή επαληθευτή IA-5 υπάρχει διαχείριση των ελέγχων ταυτότητας των συστημάτων πληροφοριών. Με το IA-8 ταυτοποιούνται και ελέγχονται οι ταυτότητες για τους μη οργανωμένους χρήστες.

Μέσω του παρεχόμενου PR.AC-1 οι ταυτότητες και τα διαπιστευτήρια εκδίδονται, διαχειρίζονται, επαληθεύονται, ανακαλούνται και ελέγχονται για εξουσιοδοτημένες συσκευές. Για την πραγματοποίηση της απομακρυσμένης πρόσβασης παρέχεται PR.AC-3. Με την παροχή του PR.AC-7 ελέγχονται για τυχόν κίνδυνο οι χρήστες καθώς και οι συσκευές.

Προσέγγιση 8

Κάθε συσκευή που είναι ενσωματωμένη χρησιμοποιώντας το πρωτόκολλο Wi-Fi Easy Connect διαθέτει μοναδικά διαπιστευτήρια δικτύου που επιτρέπουν στη συσκευή τον έλεγχο ταυτότητας στο δίκτυο ως μέρος της τυπικής χειραψίας σύνδεσης δικτύου Wi-Fi. Η κάθε συσκευή

χρησιμοποιεί ελέγχους ταυτότητας και όπως στην Προσέγγιση 7 υποστηρίζεται το IA-2, το IA-5, το IA-8 ενώ παρέχεται το PR.AC-1, το PR.AC-3 και το PR.AC-7.

Προσέγγιση 9

Στη συγκεκριμένη προσέγγιση υπάρχει ένας μηχανισμός όπου μπορεί να συσχετίσει μια διεύθυνση URL με μία συσκευή έτσι ώστε να μπορεί να βρεθεί το αρχείο MUD της. Η διεύθυνση URL του αρχείου MUD μεταβιβάζεται στον διαχειριστή MUD, ο οποίος ανακτά ένα αρχείο MUD από τον καθορισμένο ιστότοπο χρησιμοποιώντας το https. Το αρχείο MUD έχει την ιδιότητα να περιγράφει τις απαιτήσεις της κάθε συσκευής. Ο διαχειριστής MUD μετατρέπει τις απαιτήσεις σε πληροφορίες ελέγχου πρόσβασης για επιβολή από τον router. Η κάθε συσκευή έχει την δυνατότητα να αποτρέψει μια μη εξουσιοδοτημένη πρόσβαση σε δεδομένα τα οποία μεταδίδονται από αυτήν μέσω του δικτύου.

Το σύστημα διαθέτει ισχυρούς μηχανισμούς με σκοπό την αυθεντικότητα των συνεδριών επικοινωνίας με το SC-23. Αυτό το στοιχείο ελέγχου στοχεύει στην προστασία των επικοινωνιών. Για την ασύρματη πρόσβαση υποστηρίζεται το στοιχείο ελέγχου AC-18. Μέσω της εγκατάστασης του Privotal Cloud Foundry (PCF) που είναι μια πλατφόρμα πολλαπλών νεφών (Clouds) με στόχο την ανάπτυξη αξιοποιούνται κατάλληλα οι πόροι του δικτύου που παρέχονται από το επίπεδο IaaS. Η υποδομή ως υπηρεσία (IaaS) είναι ένας τύπος υπολογιστικού νέφους προσφέροντας υπολογιστικούς και αποθηκευτικούς πόρους. Για την εμπιστευτικότητα και ακεραιότητα μετάδοσης παρέχεται το SC-8.

Για να αποφευχθεί η μη εξουσιοδοτημένη πρόσβαση μιας διαδικασίας ή ενός χρήστη καθώς και την επέκταση του ελέγχου του δικτύου πέρα από το αρχικό σημείο συμβιβασμού παρέχεται το PR.PT-3. Υποστηρίζοντας το PR.DS-5 εφαρμόζονται ασφάλειες ώστε να περιοριστούν ή και να εξαλειφθούν οι διαρροές δεδομένων. Για την επαλήθευση της ακεραιότητας του λογισμικού, του υλικολογισμικού και των πληροφοριών χρησιμοποιούνται έλεγχοι ακεραιότητες παρεχόμενοι από το PR.DS-6.

Προσέγγιση 10

Για τον εντοπισμό ενός αρχείο MUD είναι απαραίτητη η συσχέτιση της συσκευής με μία διεύθυνση URL η οποία στη συνέχεια μεταβιβάζει το εν λόγω URL στον διαχειριστή MUD ο οποίος με την σειρά του ανακτά ένα αρχείο MUD από τον προκαθορισμένο ιστότοπο με χρήση του https. Το αρχείο MUD έχει την δυνατότητα περιγραφής των απαιτήσεων επικοινωνίας για την συγκεκριμένη συσκευή. Ο διαχειριστής MUD μετατρέπει τις απαιτήσεις σε πληροφορίες ελέγχου πρόσβασης για επιβολή από τον δρομολογητή ο οποίος λαμβάνει ανά διαστήματα σήματα για απειλές από τον αντίστοιχο σηματοδότη. Σε περίπτωση εντοπισμού απειλής ο δρομολογητής περιορίζει ορισμένες κυκλοφορίες δικτύου που κρίνονται απειλούμενες. Υπάρχει επαρκής κεντρικός έλεγχος για την εφαρμογή πολιτικών ή κανονιστικών απαιτήσεων σε προσωπικά αναγνωρίσιμες πληροφορίες. Για να πραγματοποιείται κοινή χρήση πληροφοριών με εξωτερικά μέρη πέρα του συστήματος υποστηρίζεται το PA-4.

3.5 Στόχοι του Έργου στο Cybersecurity Framework & Αναφορά στον Πληροφοριακό Έλεγχο Ασφάλειας

Παράδειγμα Υλοποίησης 1
Διαχείρισης Περιουσιακών Στοιχείων (Asset Management (ID.AM))

Η χρήση της **Διαχείρισης Περιουσιακών Στοιχείων (Asset Management (ID.AM))** είναι μία κατηγορία πλαισίου Κυβερνοασφάλειας και ο σκοπός της είναι τα δεδομένα, το προσωπικό, οι συσκευές, τα συστήματα και οι εγκαταστάσεις που επιτρέπουν στους χρήστες να επιτύχουν σκοπούς να προσδιορίζονται και να διαχειρίζονται σύμφωνα με τη σχετική σημασία τους για τους στόχους και τη στρατηγική κινδύνου της οικίας ή της μικρής επιχείρησης. Διαθέτει τρεις υποκατηγορίες οι οποίες είναι η ID.AM-1 που είναι υπεύθυνη για την καταγραφή των φυσικών συσκευών και συστημάτων εντός του δικτύου ,η ID.AM-2 που καταγράφει τις πλατφόρμες λογισμικού καθώς και τις εφαρμογές και η ID.AM-3 που έχει σαν στόχο την χαρτογράφηση των επικοινωνιών και των ροών δεδομένων.

Υποκατηγορία Πλαισίου Κυβερνοασφάλειας ID.AM-1

Στις ενημερωτικές αναφορές τις υλοποίησης με χρήση ID.AM-1 περιλαμβάνεται το CIS CSC 1 της οικογένειας των CIS Controls όπου παρέχουν μία λίστα αποτελεσματικών εργασιών υψηλής προτεραιότητας για άμυνα από επιθέσεις στον Κυβερνοχώρο. Το CIS Critical Security Control 1 είναι υπεύθυνο για την απογραφή και τον έλεγχο περιουσιακών στοιχείων της οικίας ή της μικρής επιχείρησης. Το CIS CSC 1 διαχειρίζεται ενεργά συσκευές χρήστη όπως οι φορητοί υπολογιστές και τα κινητά, δικτυακές συσκευές καθώς και συσκευές Internet of Things. Είναι επίσης υπεύθυνο για τον εντοπισμό μη εξουσιοδοτημένων και μη διαχειριζόμενων περιουσιακών στοιχείων προς κατάργηση ή αποκατάσταση.

Με την ενημερωτική αναφορά BAI09.01 προσδιορίζονται και καταγράφονται τα περιουσιακά στοιχεία διατηρώντας ένα ολοκληρωμένο αρχείο αυτών τα οποία απαιτούνται για την παροχή υπηρεσιών. Παράλληλα με την χρήση του BAI09.02 διαχειρίζονται τα κρίσιμα περιουσιακά στοιχεία για την παροχή δυνατοτήτων υπηρεσίας.

Στην υποκατηγορία ID.AM-1 για την ασφάλεια στα συστήματα βιομηχανικού ελέγχου αναφέρεται το πρότυπο **ISA 62443-2-1:2009** 4.2.3.4 όπου περιγράφει τα στοιχεία που περιέχονται σε ένα σύστημα διαχείρισης ασφάλειας στον κυβερνοχώρο σε περιβάλλον βιομηχανικού αυτοματισμού και συστημάτων ελέγχου.

Οι λεπτομερείς απαιτήσεις του συστήματος για τον τεχνικό έλεγχο παρέχονται από το πρότυπο **ISA 62443-3-3:2013** SR 7.8 όπου η σχεδίασή του βασίζεται σε επτά απαιτήσεις συμπεριλαμβάνοντας τον έλεγχο επιπέδων ασφαλείας του συστήματος. Ο ρόλος του είναι η παροχή ενός πλαισίου που κάνει πιο εύκολη την αντιμετώπιση τρωτών σημείων καθώς και εφαρμογή μέτρων ασφάλειας.

«Η αναφορά "**ISO 27001 A.8.1.1**: Απογραφή Περιουσιακών Στοιχείων" σχετίζεται με τα περιουσιακά στοιχεία που σχετίζονται με πληροφορίες και εγκαταστάσεις επεξεργασίας πληροφοριών που θα εντοπιστούν και θα καταρτιστεί και θα τηρηθεί απογραφή αυτών των περιουσιακών στοιχείων.Αυτή η αναφορά εμφανίζει τη λίστα περιουσιακών στοιχείων χρησιμοποιώντας την προβολή "ISO 27001 A.8.1.1: Inventory of Assets"».

Με την αναφορά στο **NIST SP 800-53 Rev. 4** CM-8, PM-5 περιγράφονται οι αλλαγές σε κάθε βελτίωση στο επίπεδο ελέγχου, δίνοντας μια σύντομη περίληψη των αλλαγών και συμπεριλαμβάνοντας μια αξιολόγηση της σημασίας των αλλαγών. Αυτή η σύγκριση συντάχθηκε από την The MITER Corporation για τον Διευθυντή Εθνικής Πληροφοριών (DNI) και κοινοποιείται με άδεια από την DNI.

<u>Υποκατηγορία Πλαισίου Κυβερνοασφάλειας ID.AM-2</u>

Για την ασφάλεια του περιβάλλοντα χώρου είναι απαραίτητο να ελέγχεται η εγκατάσταση οποιουδήποτε λογισμικού και να ταυτοποιείται η εγκυρότητα της εξουσιοδότησης του καθώς και να υπάρχει η ανάλογη καταγραφή σου στο σύστημα. Αυτές τις λειτουργίες τις παρέχει η χρήση και η ακολουθία των κανόνων του ID.AM-2 όπου θεωρείται επιτυχείς ένας έλεγχος μόνο στην περίπτωση της ανίχνευσης και αποκλεισμού κάθε κακόβουλου λογισμικού. Το ID.AM-1 διαθέτει ελέγχους και κατανόηση του λογισμικού που βρίσκεται στο περιβάλλον ενώ είναι πανομοιότυπο με το πλαίσιο ασφάλειας ID.AM-1.

Το **CIS CSC 2** εφαρμόζεται στην υποκατηγορία ID.AM-2 με σκοπό την διαχείριση του λογισμικού στο δίκτυο ώστε να είναι εγκατεστημένο και πλήρως ενημερωμένο για να εκτελεί αποκλειστικά εξουσιοδοτημένο λογισμικό καθώς και να εμποδίζει την εγκατάσταση ή την εκτέλεση με εξουσιοδοτημένου λογισμικού.

Η διαχείριση των κινδύνων της οικίας ή της μικρής επιχείρησης διαχειρίζεται από το **COBIT** (Control Objectives for Information and Related Technology). Η έκδοση πλαισίου COBIT 5 που χρησιμοποιείται στην συγκεκριμένη περίπτωση κυκλοφόρησε το 2012. Το COBIT 5 περικλείεται από 5 απαραίτητες αρχές : την ικανοποίηση αναγκών & συμφερόντων, την κάλυψη της επιχείρησης (end to end), την εφαρμογή ενός ενιαίου ολοκληρωμένου πλαισίου, την ενεργοποίηση μιας ολιστικής προσέγγισης και τον διαχωρισμό της διακυβέρνησης από την διαχείριση. Το COBIT 5 βοηθάει στο έργο με την βελτίωση και την διατήρηση πληροφοριών υψηλής ποιότητας και με την διασφάλιση κινδύνων.

Στην υποκατηγορία πλαισίου κυβερνοασφάλειας ID.AM-1 επεξηγήθηκαν οι αναφορές και οι χρήσεις σε ISA 62443-2-1:2009 , ISA 62443-3-3:2013 , ISO/IEC 27001:2013 καθώς και NIST SP 800-53 Rev. 4. Οι ίδιες αναφορές συναντιούνται και στην υποκατηγορία ID.AM-2 με μία πρόσθετη αναφορά , την **ISO/IEC 27001:2013** A.12.5.1. Η συγκεκριμένη αναφορά εξηγεί την εγκατάσταση λογισμικού σε λειτουργικά συστήματα και τις διαδικασίες για τον έλεγχο της

εγκατάστασής τους. Ένας απ τους κυριότερους λόγους επιθέσεων είναι η εγκατάσταση κακόβουλο ή και μολυσμένου λογισμικού όπου εγκαθιστά κάποιος χρήστης του δικτύου. Είναι σημαντικό να υπάρχει κατάλληλος έλεγχος για την εγκυρότητα και νομιμότητα κάθε λογισμικού καθώς επίσης η συστηματική ενημέρωση για τυχόν νέες εκδόσεις.

<u>Υποκατηγορία Πλαισίου Κυβερνοασφάλειας ID.AM-3</u>

Το **ID.AM – 3** όπου χαρτογραφεί ροές δεδομένων αναφέρεται στο **CIS Critical Security Control 12** που είναι υπεύθυνο για την διαχείριση της υποδομής του οικιακού δικτύου ή του δικτύου της μικρής επιχείρησης. Ο εν λόγω έλεγχος ασφάλειας δημιουργεί , εφαρμόζει και διαχειρίζεται ενεργά μέσω παρακολούθησης και αναφοράς όλες τις συσκευές δικτύου ώστε να αποτρέψει τους εισβολείς από την εκμετάλλευση ευάλωτων υπηρεσιών δικτύου και σημείων πρόσβασης.

Η **COBIT 5** έχει 7 πρακτικές η δεύτερη εκ των οποίων είναι η διαχείριση ασφάλειας δικτύου και συνδεσιμότητας χρησιμοποιώντας μέτρα ασφάλειας και σχετικές διαδικασίες διαχείρισης για την προστασία πληροφοριών σε όλες τις μεθόδους σύνδεσης. Εφαρμόζοντας την πρακτική **COBIT 5 DSS05.02** προστατεύονται οι πληροφορίες της μικρής επιχείρησης και της οικίας διατηρώντας ακέραιο το επίπεδο ασφάλειας του δικτύου σύμφωνα με την πολιτική ασφάλειας. Ο σκοπός είναι η μείωση καθώς και εξάλειψη των τρωτών σημείων και των κακόβουλων συμβάντων.

Το σύστημα είναι απαραίτητο να ανταπεξέλθει σε υψηλά επίπεδα άμυνας ενώ παράλληλα να είναι έτοιμο να αντιμετωπίσει πλήθος επιθέσεων διαφορετικού τύπου και τεχνικής. Ένας εισβολέας θέλει να αποκτήσει πληροφορίες για το υπολογιστικό σύστημα αντλώντας από διαφορετικές τεχνικές όσα περισσότερα στοιχεία μπορεί όπως για παράδειγμα τις ανοιχτές θύρες στο δίκτυο ή ακόμα και το λειτουργικό σύστημα της συσκευής. Η τεχνική spoofing (πλαστογράφηση) είναι μία τεχνική όπου ο χάκερ μεταμφιέζεται σε μια αξιόπιστη πηγή γνωστή στο σύστημα. Αυτή η τεχνική έχει πολλούς διαφορετικούς τύπους, από πλαστογράφηση μίας διεύθυνσης IP, πλαστογράφηση DNS, ιστότοπου μέχρι και πλαστογράφηση κλήσεων. Έτσι ο επιτιθέμενος είναι δυνατόν να αποκτήσει πρόσβαση σε συστήματα και συσκευές έχοντας την δυνατότητα κλοπής πληροφοριών ακόμα και εγκατάσταση κακόβουλου λογισμικού. Για την καταπολέμηση αυτών των κακόβουλων κινήσεων εφαρμόζεται η ενημερωτική αναφορά NIST SP 800-53 Rev. 4 **AC-4** προερχόμενο από την οικογένεια ελέγχου πρόσβασης (Access Control). Το AC-4 υποχρεώνει την εξουσιοδότηση για τον έλεγχο ροής πληροφοριών εντός του συστήματος και μεταξύ συνδεδεμένων συστημάτων.

Σε κάθε πληροφοριακό σύστημα έρχεται η ανάγκη της διασύνδεσης συστήματος και αυτή την ανάγκη ήρθε να καλύψει το NIST SP 800-53 Rev 4 **CA-3**. Με το CA-3 μπορούν να εξουσιοδοτηθούν συνδέσεις του συστήματος σε άλλα συστήματα μέσω χρήσης συμφωνιών ασφάλειας διασύνδεσης κοινοποιώντας έγγραφα για κάθε διασύνδεση, χαρακτηριστικά και απαιτήσεις ασφάλειας. «Αυτός ο έλεγχος ισχύει για αποκλειστικές συνδέσεις μεταξύ συστημάτων πληροφοριών (δηλαδή, διασυνδέσεις συστήματος) και δεν ισχύει για μεταβατικές, ελεγχόμενες από τον χρήστη συνδέσεις, όπως η περιήγηση ηλεκτρονικού ταχυδρομείου και η περιήγηση σε ιστότοπους». Για την άρτια ασφάλεια ελέγχονται όλοι οι πιθανοί κίνδυνοι που μπορούν να εισέρθουν στο σύστημα όταν συνδέεται με διαφορετικά συστήματα ως προς τις απαιτήσεις και τους ελέγχους ασφάλειας τους.

Το σύστημα εκτός από εξωτερικές διασυνδέσεις έχει και εσωτερικές συνδέσεις όπως αναφέρει η **CA-9** όπου επιτρέπει την εξουσιοδότηση εσωτερικών συνδέσεων που καθορίζονται στο

σύστημα. Με την ενημερωτική αναφορά CA-9 τεκμηριώνονται τα χαρακτηριστικά της διεπαφής, οι απαιτήσεις ασφάλειας που κοινοποιούνται εσωτερικά του συστήματος. Όταν κρίνεται αναγκαίος ο τερματισμός των εσωτερικών συνδέσεων πρέπει να εφαρμόζεται εφόσον είναι καθορισμένος από εξουσιοδοτημένους χρήστες.

Στις σύγχρονες αρχιτεκτονικές των υπολογιστών γίνεται όλο και λιγότερος ο έλεγχος όλων των πόρων από τους χρήστες. Η δημιουργία, η ανάπτυξη, η τεκμηρίωση και η διατήρηση υπό έλεγχο διαμόρφωσης μιας βασικής διαμόρφωσης για οργανωτικά συστήματα είναι κρίσιμης σημασίας για την εφαρμογή και τη διατήρηση αποτελεσματικών αρχιτεκτονικών. Η τεκμηρίωση, ωστόσο, μπορεί απλώς να αντικατοπτρίζει τις συνδυασμένες αρχιτεκτονικές. Η σχεδίαση **PL-8** εφαρμόζει την αρχιτεκτονική ασφάλειας και απορρήτου περιγράφοντας τις αναφορές και την προσέγγιση που είναι αναγκαία να ακολουθηθεί για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της ασφάλειας των πληροφοριών. Σε αυτό το στοιχείο περιγράφεται η προσέγγιση για την επεξεργασία στοιχείων προσωπικής ταυτοποίησης καθώς και η ελαχιστοποίησης του κινδύνου απορρήτου.

Παράδειγμα Υλοποίησης 2
Εκτίμηση Κινδύνου (ID.RA)

Η μικρή επιχείρηση ή η οικία είναι σε θέση να κατανοήσει τον κίνδυνο κυβερνοασφάλειας για διάφορες λειτουργίες όπως η εικόνα της , η φήμη της καθώς και τα περιουσιακά στοιχεία των ατόμων του περιβάλλοντος. Με τον όρο περιουσιακά στοιχεία εννοούμε τα φυσικά , τα άυλα , τα λειτουργικά ή τα μη λειτουργικά μέρη του συστήματος. Ο σωστός προσδιορισμός και η ταξινόμηση των τύπων περιουσιακών στοιχείων είναι ζωτικής σημασίας για τη φερεγγυότητα και τον αποτροπή κινδύνων.

Υποκατηγορία Πλαισίου Κυβερνοασφάλειας ID.RA-2

Οι πληροφορίες για την απειλή στον κυβερνοχώρο λαμβάνονται από φόρουμ και πηγές ανταλλαγής πληροφοριών. Οι πηγές λήψης είναι πολυποίκιλες και το σύστημα έχει ως μοναδικό σκοπό την ακεραιότητα της ασφάλειας του οικιακού δικτύου ή του δικτύου της μικρής επιχείρησης. Μια ισχυρή πηγή για απειλές είναι το Υπουργείο Εσωτερικής Ασφάλειας κάθε χώρας. «Το Υπουργείο Εσωτερικής Ασφάλειας και οι συνιστώσες του διαδραματίζουν πρωταγωνιστικό ρόλο στην ενίσχυση της ανθεκτικότητας στον κυβερνοχώρο σε ολόκληρη τη χώρα και τους τομείς, στη διερεύνηση της κακόβουλης δραστηριότητας στον κυβερνοχώρο και στην προώθηση της ασφάλειας στον κυβερνοχώρο». Η άντληση πληροφοριών σχετικά με τις απειλές είναι εφικτό να γίνει μέσω των social media όπως για παράδειγμα το Facebook και το Twitter με την χρήση OSINT (Open Source Intelligence). «Το πρώτο βήμα σε μία στοχευμένη επίθεση ή ένα τεστ διείσδυσης ή μια δραστηριότητα είναι η συλλογή πληροφοριών στον στόχο. Αν και υπάρχουν τρόποι και μέσα για να γίνει αυτό κρυφά, η συλλογή πληροφοριών ξεκινά συνήθως με τη συλλογή πληροφοριών από δημόσιες πηγές, γνωστές συλλογικά ως ευφυΐα ανοιχτού κώδικα ή OSINT»

Ένα ψηφιακό αποτύπωμα είναι εύκολο να ανιχνευθεί με τα κατάλληλα εργαλεία. Η υποκατηγορία πλαισίου κυβερνοασφάλειας **ID.RA-2** αναφέρεται στις εν λόγω λαμβανόμενες πληροφορίες από διάφορες πηγές ανταλλαγής πληροφοριών. Κάθε σύστημα όπου περιλαμβάνει σύγχρονες τεχνολογίες και συσκευές IoT διαθέτουν μηχανισμούς ειδοποίησης σχετικά με την

ακεραιότητα της ασφάλειας , συμβουλές και οδηγίες. Στην υποκατηγορία ID.RA-2 γίνεται αναφορά στο **SI-5** όπου δημιουργεί ειδοποιήσεις εσωτερικής ασφάλειας , συμβουλές και οδηγίες όπως κρίνεται απαραίτητο. Είναι σε θέση να διαδώσει αυτές της πληροφορίες και να εφαρμόσει οδηγίες ασφάλειας σύμφωνα με τα καθορισμένα χρονικά πλαίσια.

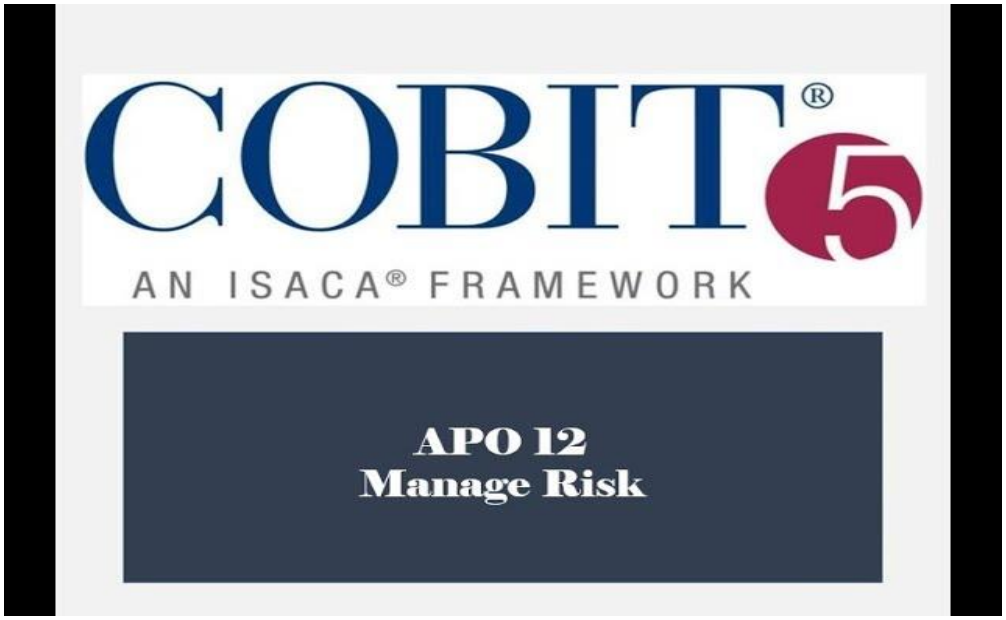
Το NIST 800-53 παρέχει τον έλεγχο ασφάλειας **PM-15** όπου αναφέρεται στο Παράδειγμα Υλοποίησης 2 και ανήκει στην οικογένεια του Control Statement. Ο στόχος του PM-15 είναι η συνεχή εκπαίδευση του προσωπικού της επιχείρησης ή των χρηστών του οικιακού δικτύου και κατάρτιση για την ασφάλεια και το απόρρητο. Αυτό είναι εφικτό μέσω πρακτικών, τεχνικών και τεχνολογιών ασφάλειας και απόρρητου ώστε να μπορούν εντέλει να μοιραστούν πληροφορίες σχετικά με την ασφάλεια όπου συμπεριλαμβάνει απειλές, τρωτά σημεία και συμβάντα στο σύστημα.

Όσο περνάνε τα χρόνια τόσο η τεχνολογική εξέλιξη γίνεται όλο και πιο περίπλοκη με πολλές δυνατότητες που μπορούν να επηρεάσουν την καθημερινότητα μας. Έτσι και η τεχνογνωσία των αντιπάλων που θέλουν να βλάψουν ένα σύστημα είναι όλο και πιο ισχυρή μέσω εξελιγμένων τεχνικών διείσδυσης. Ειδικά με την προηγμένη επίμονη απειλή (Advanced Persistent Threat) γίνεται πιο πιθανό οι αντίπαλοι να παραβιάσουν ένα σύστημα πληροφοριών. Τα APT αρχικά συνδέονταν κυρίως με φορείς εθνικών κρατών που ήθελαν να κλέψουν κυβερνητικά ή βιομηχανικά μυστικά. Πλέον βρίσκονται πιο κοντά και στους hackers όπου προσπαθούν να υποκλέψουν δεδομένα ή πνευματική ιδιοκτησία. Οι hackers και το κακόβουλο λογισμικό APT είναι πιο διαδεδομένα και εξελιγμένα από ποτέ. Ένα αποτελεσματικό μέτρο για όλους αυτούς τους κινδύνους είναι το μοίρασμα των πληροφοριών σχετικά με απειλές περιλαμβάνοντας για παράδειγμα τακτικές, τεχνικές και διαδικασίες που έχουν φανεί αποτελεσματικές στο παρελθόν σε τέτοιες επιθέσεις. Αυτός είναι ο λόγος της αναφοράς και χρήσης του **PM-16** όπου είναι πρόγραμμα για την ευαισθητοποίηση σχετικά με απειλές.

<u>Υποκατηγορία Πλαισίου Κυβερνοασφάλειας ID.RA-3</u>

Μέσω του ελέγχου και αξιολόγησης κινδύνου **ID.RA-3** εντοπίζονται και τεκμηριώνονται οι εσωτερικές και οι εξωτερικές απειλές για τα περιουσιακά στοιχεία. Χρησιμοποιώντας ένα μητρώο κινδύνου είναι ένας τρόπος να μπορέσουμε να τεκμηριώσουμε τις απειλές. Στις εσωτερικές απειλές είναι απαραίτητο να συμπεριληφθούν και οι εσφαλμένες χρήσεις στο περιβάλλον από τους υπαλλήλους της κάθε επιχείρησης ώστε να μειωθούν μελλοντικές απειλές. Στην υποκατηγορία ID.RA-3 χρησιμοποιείται η αναφορά στο **CIS CSC 4** μιας και είναι αναγκαία για την διατήρηση της ασφάλειας και την διαμόρφωση των περιουσιακών στοιχείων της μικρής επιχείρησης ή της οικίας. ΤΟ CIS CSC 4 αξιολογεί και αποκαθιστά και αναλαμβάνει δράση σε νέες πληροφορίες του συστήματος προκειμένου να εντοπισθούν τρωτά σημεία.

Το COBIT 5 παρέχει βέλτιστες πρακτικές σχετικά με την ασφάλεια των επιχειρήσεων που περιέχει το **APO12.01** με σκοπό την διαχείριση κινδύνου. Κάθε πλαίσιο ή πρότυπο αναφέρει το APO12 ως κρίσιμο για την ασφάλεια πληροφοριών. Μια επιχείρηση για τον εντοπισμό κινδύνου και την εστίαση των πόρων στις πιο κρίσιμες, ευαίσθητες και απειλούμενες περιοχές πρέπει να χρησιμοποιεί κατάλληλες διαδικασίες αξιολόγησης κινδύνου όπου προσφέρονται από το APO12.



"Τα δεδομένα πρέπει να συλλέγονται από όλες τις σχετικές πηγές (π.χ. συστήματα, εφαρμογές, δίκτυα, βάσεις δεδομένων) σε πολλαπλές κατηγορίες (π.χ. πρόσβαση, διαμορφώσεις) για την υποστήριξη της κατανόησης του κινδύνου **(APO12.01**). Αυτά τα δεδομένα θα πρέπει να λαμβάνονται υπόψη στην ανάλυση κινδύνου, ειδικά για την ανάλυση επιχειρηματικών επιπτώσεων (τι είναι σημαντικό για την επιχείρηση), εκτιμώντας την πιθανότητα διαφορετικών απειλών και προσδιορίζοντας τους ισχύοντες περιοριστικούς ελέγχους **(APO12.02)**". Όλες οι πληροφορίες που διαθέτει μία επιχείρηση για έναν κίνδυνο είναι απαραίτητο να απογραφεί στο υπολογιστικό της σύστημα, τα δεδομένα και τις εγκαταστάσεις της **(APO12.03).** Τα περιουσιακά στοιχεία είναι κρίσιμα απλώς ορισμένα από αυτά κρίνονται άκρως αναγκαία και χρήζουν μεγαλύτερη προσοχή λόγω του μεγαλύτερου στόχου που έχουν σε ενδεχόμενες επιθέσεις. Τα μέρη του συστήματος πρέπει να ενημερώνονται σχετικά με την κατάσταση του κινδύνου καθώς και για τα χειρότερα πιθανά σενάρια που ενδέχεται να προκύψουν **(APO12.04).**

Στην υποκατηγορία ID.RA-3 γίνεται ενημερωτική αναφορά σε **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 όπως ακριβώς και στην υποκατηγορία ID.RA-2. Απαιτούμενη δραστηριότητα για την ασφάλεια πληροφοριών κρίνεται η ρήτρα **(clause) 6.1.2** του **ISO 27001** που αξιολογεί και αναλύει τον κάθε κίνδυνο. "Ο προσδιορισμός κινδύνου είναι η διαδικασία εύρεσης, αναγνώρισης και περιγραφής των κινδύνων. Αυτό περιλαμβάνει τον προσδιορισμό των πηγών κινδύνου, των γεγονότων, των αιτιών τους και των πιθανών συνεπειών τους. Ο στόχος της αναγνώρισης κινδύνου είναι να αποκτήσει μια ολοκληρωμένη λίστα κινδύνων που υποστηρίζονται εκείνα τα γεγονότα που μπορεί να δημιουργήσουν, να ενισχύσουν, να αποτρέψουν, να υποβαθμίσουν, να επιταχύνουν ή να καθυστερήσουν την επίτευξη των στόχων ασφάλειας δεδομένων". Για τον προσδιορισμό ενός κινδύνου για την ασφάλειας δεδομένων χρησιμοποιούνται διάφορες προσεγγίσεις, όπως η προσέγγιση βάσει συμβάντων που εξετάζει τις πηγές κινδύνου και τον εντοπισμό απειλών και τρωτών σημείων.

Στην υποκατηγορία ID.RA-3 χρησιμοποιείται ο έλεγχος για την εκτίμηση κινδύνου **RA-3** όπου διενεργεί σε αξιολόγηση του κινδύνου συμπεριλαμβανόμενης της πιθανότητας και του μεγέθους ζημιάς από μη εξουσιοδοτημένη πρόσβαση. Μία κακόβουλη κίνηση εκτός από πρόσβαση είναι σε θέση να φέρει και άλλες ζημιές στο σύστημα όπως η χρήση του, η διακοπή του, η

τροποποίηση του ακόμα και η καταστροφή του δημιουργώντας φθορά σε επεξεργασμένες, αποθηκευμένες και μεταδιδόμενες πληροφορίες. Το RA-3 είναι σε θέση να ενημερώνει διαρκώς το σύστημα για την εκτίμηση του κάθε κινδύνου ή σε οποιαδήποτε αλλαγή στο σύστημα πληροφοριών συμπεριλαμβανομένων και των εντοπισμών νέων απειλών και τρωτών σημείων.

Για την εφαρμογή προγράμματος εσωτερικών απειλών που περιλαμβάνει μια διεπιστημονική ομάδα διαχείρισης περιστατικών απειλών από εμπιστευτικές πληροφορίες χρησιμοποιείται το εργαλείο ελέγχου **PM-12.** Στις ενημερωτικές αναφορές στην υποκατηγορία ID.RA-3 αναφέρονται οι έλεγχοι SI-5 και PM-16 όπου έχουν αναληθή στην υποκατηγορία ID.RA-2.

Παράδειγμα Υλοποίησης 3
Διαχείριση Ταυτότητας & Έλεγχος Πρόσβασης (PR.AC)

Η πρόσβαση σε φυσικά στοιχεία του συστήματος όπως για παράδειγμα η πρόσβαση σε ηλεκτρονικούς υπολογιστές θερμοστάτες, fax και αισθητήρες είναι αποκλειστικά με περιορισμένη σε εξουσιοδοτημένους χρήστες του συστήματος. Κατάλληλη εξουσιοδότηση μπορεί να έχουν και διαδικασίες καθώς και συσκευές ώστε να μπορούν να επικοινωνούν αρμονικά μεταξύ τους στο περιβάλλον με σκοπό την εξυπηρέτηση και την κάλυψη των αναγκών των χρηστών. Η διαχείριση της ταυτότητας γίνεται σύμφωνα με τον εκτιμώμενο κίνδυνο της μη εξουσιοδοτημένης πρόσβασης σε εξουσιοδοτημένες δραστηριότητες και συναλλαγές.

Υποκατηγορία Πλαισίου Κυβερνοασφάλειας PR.AC-1

Σε ένα περιβάλλον IoT υπάρχουν χρήστες , συσκευές και διαδικασίες ώστε να υπάρχουν οι ανάλογες εξειδικευμένες ενέργειες. Για την ακεραιότητα της ασφάλειας όλα τα εξουσιοδοτημένα στοιχεία του περιβάλλοντος καθώς και οι ταυτότητες και τα διαπιστευτήρια τους εκδίδονται, διαχειρίζονται, επαληθεύονται, ανακαλούνται και ελέγχονται.

Με την εφαρμογή του κρίσιμου ελέγχου ασφάλειας **CIS 1** γίνεται απογραφή και έλεγχος περιουσιακών στοιχείων της μικρής επιχείρησης και της οικίας. Ο εν λόγω έλεγχος διαχειρίζεται ενεργά όλα τα περιουσιακά στοιχεία συμπεριλαμβανομένων και των φορητών και κινητών συσκευών καθώς και διακομιστές που συνδέονται με την υποδομή IoT φυσικά, εικονικά ή εξ' αποστάσεως. Μέσω αυτών των ενεργειών είναι εφικτός και ο εντοπισμός μη εξουσιοδοτημένων και μη διαχειριζόμενων περιουσιακών στοιχείων όπου θα οδηγηθούν σε κατάργηση ή αποκατάσταση.

Στην υποκατηγορία PR.AC-1 μέσω του ελέγχου ασφάλειας **CIS 5** χρησιμοποιούνται διαδικασίες και εργαλεία για την εκχώρηση και διαχείριση εξουσιοδότησης σε διαπιστευτήρια για λογαριασμούς χρηστών, συμπεριλαμβανομένων και λογαριασμών διαχειριστών καθώς και λογαριασμούς υπηρεσιών.

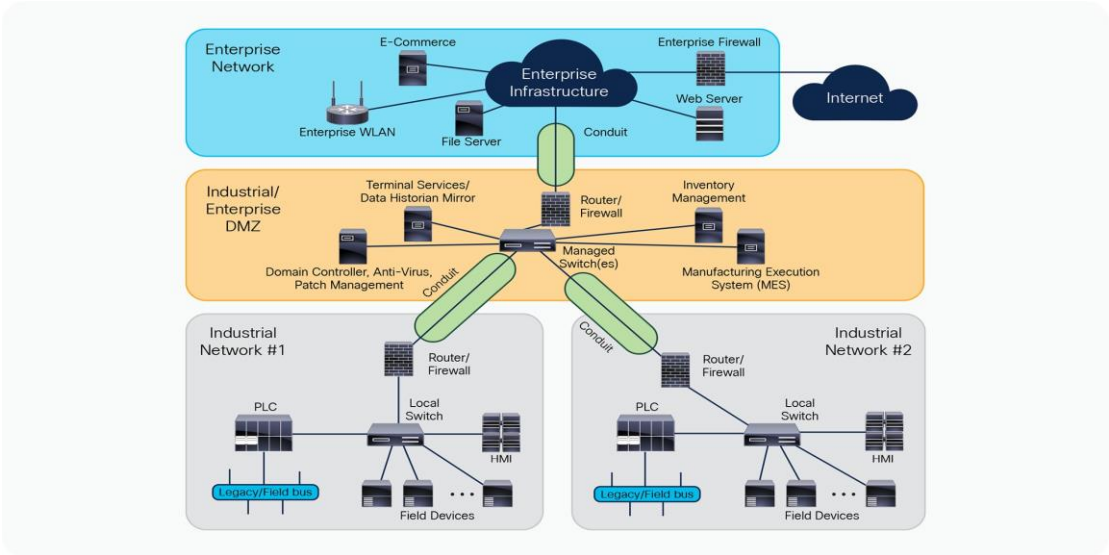
Κάθε έργο έχει την ανάγκη της ασφάλισης των δεδομένων του τα οποία υπάρχουν σε παρόχους υπηρεσιών που κατέχουν αυτά τα δεδομένα ή είναι υπεύθυνοι για κρίσιμες πλατφόρμες. Μέσω μιας διαδικασίας που αναπτύσσεται σύμφωνα με το **CIS 15** διασφαλίζεται ότι οι πάροχοι προστατεύουν κατάλληλα πλατφόρμες και δεδομένα.

Με το **CIS 16** δίνεται η δυνατότητα της διαχείρισης του κύκλου ζωής ασφάλειας του εσωτερικά αναπτυγμένου, φιλοξενούμενου ή αποκτημένου λογισμικού για την πρόληψη, τον εντοπισμό και την αποκατάσταση αδυναμιών ασφάλειας προτού επηρεάσουν την επιχείρηση ή το οικιακό δίκτυο.

Το **COBIT 5 DSS05.04** αναφέρεται σε ένα από τα πολλά στοιχεία του πλαισίου διαχείρισης τεχνολογίας πληροφοριών (IT) COBIT 5. Συγκεκριμένα, αναφέρεται στον κατάλογο ελέγχου (control objectives) DSS05 που αναπτύχθηκε για τη διαχείριση της ασφάλειας των πληροφοριακών συστημάτων σε μια επιχείρηση. Αναφέρεται στην ανίχνευση, την αντιμετώπιση και την αναφορά των περιστατικών ασφαλείας στα πληροφοριακά συστήματα της επιχείρησης. Αυτό περιλαμβάνει την αξιολόγηση του αντίκτυπου των περιστατικών ασφαλείας, τη διενέργεια έρευνας και τη λήψη μέτρων για την πρόληψη της επανάληψης τέτοιων περιστατικών στο μέλλον.

Στην εν λόγω υποκατηγορία πλαισίου κυβερνοασφάλειας αναφέρεται το στοιχείο καταλόγου ελέγχου **DSS06.03** το οποίο αναφέρεται στη διαχείριση των δικαιωμάτων πρόσβασης στις εφαρμογές. Το στοιχείο αυτό περιλαμβάνει την ανάπτυξη και την εφαρμογή ενός συστήματος διαχείρισης δικαιωμάτων πρόσβασης που θα διασφαλίζει ότι οι χρήστες έχουν πρόσβαση μόνο στις εφαρμογές και τις πληροφορίες που απαιτούνται για την εκτέλεση των καθηκόντων τους στην μικρή επιχείρηση ή στο οικιακό δίκτυο. Αυτό περιλαμβάνει την καταγραφή και τη διαχείριση των δικαιωμάτων πρόσβασης στις εφαρμογές, τη διαχείριση της διαδικασίας ανάθεσης και ανάκλησης δικαιωμάτων πρόσβασης και την ανάπτυξη και εφαρμογή πολιτικών ασφαλείας για τη διαχείριση των δικαιωμάτων πρόσβασης.

Για την ασφάλεια βιομηχανικών συστημάτων ελέγχου αναφέρεται το πρότυπο ασφάλειας **ISA 62443-2-1:2009**. Το **4.3.3.5.1** είναι ένα συγκεκριμένο τμήμα αυτού του προτύπου που αναφέρεται στην απομόνωση του δικτύου. Το πρότυπο ISA 62443-2-1:2009 χρησιμοποιείται στην ασφάλεια των συστημάτων IoT για την προστασία τους από επιθέσεις και κακόβουλες ενέργειες. Το MUD (Manufacturer Usage Description) στην γενική του έννοια είναι ένας τρόπος για να εντοπίσουμε τη χρήση της συσκευής IoT και να την περιορίσουμε σε αυτό που αναμένουμε, κατά την επικοινωνία της με άλλες συσκευές στο δίκτυο. Συνδυάζοντας το πρότυπο ISA 62443-2-1:2009 με το MUD, είναι δυνατή η επιτυχία υψηλότερου επιπέδου ασφαλείας στις συσκευές IoT.



Η **ISA 62443-3-3:2013** είναι μια τεχνική προδιαγραφή του διεθνούς οργανισμού προτύπων ISA (International Society of Automation) που περιγράφει τις απαιτήσεις ασφάλειας για τα βιομηχανικά ελεγκτικά συστήματα. Οι συγκεκριμένες παραπομπές (SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9) αναφέρονται στην προετοιμασία και στην εφαρμογή της ασφάλειας.

Τόσο για την ανάλυση κινδύνων όσο και για την αναγνώριση και τον έλεγχο ταυτότητας του ανθρώπινου χρήστη αναφέρεται η παραπομπή **SR1.1** ενώ η **SR1.2** αναφέρεται στην ανάλυση απαιτήσεων ασφάλειας. Για τον σχεδιασμό, την διαχείριση λογαριασμών και την ανάπτυξη ασφαλών λειτουργιών και διαδικασιών είναι απαραίτητη η αναφορά της **SR1.3**. Όλη η ανταλλαγή της πληροφορίας παρέχεται από αναπτυσσόμενα ασφαλή κανάλια επικοινωνιών σύμφωνα με την αναφορά **SR1.4**.

Με την αναφορά **SR1.5** για την σωστή διαχείριση ελέγχου ταυτότητας το CISCO ISE έχει την δυνατότητα να αναγκάσει τους χρήστες να αλλάξουν των κωδικό πρόσβασης τους μετά την πρώτη σύνδεση και στη συνέχεια να αλλάξουν των κωδικό πρόσβασής τους μετά από έναν καθορισμένο χρονικό κύκλο.

Η ασφάλεια του λογισμικού είναι σημαντική για την προστασία των δικτύων και των συστημάτων από επιθέσεις και απειλές. Η αξιολόγηση της ασφάλειας του λογισμικού αποτελεί σημαντικό βήμα για την εξασφάλιση ότι το λογισμικό που χρησιμοποιείται είναι ασφαλές και δεν θα προκαλέσει προβλήματα ασφαλείας στο δίκτυο ή το σύστημα στο οποίο χρησιμοποιείται.

Η **SR1.7** αναφέρεται στην ασφάλεια του λογισμικού. Πιο συγκεκριμένα, απαιτείται η αξιολόγηση της ασφάλειας του λογισμικού κατά τη διάρκεια όλου του κύκλου ζωής του, από τη σχεδίαση έως τη συντήρηση και απόσυρση.

Η **SR1.8** αναφέρεται στον έλεγχο των προνομιακών δικαιωμάτων στα συστήματα και τις εφαρμογές. Ο έλεγχος των προνομιακών δικαιωμάτων είναι σημαντικός για την προστασία των συστημάτων και των δεδομένων από εξωτερικές απειλές και εσωτερικούς κινδύνους. Η SR1.8 προτείνει να χρησιμοποιούνται μηχανισμοί ελέγχου πρόσβασης που διαχειρίζονται την πρόσβαση σε προνομιακά δικαιώματα και περιορίζουν τις επιλογές που διατίθενται σε κάθε χρήστη.
Ο έλεγχος των προνομιακών δικαιωμάτων είναι σημαντικός για την ασφάλεια των συστημάτων, καθώς η κακόβουλη χρήση προνομιακών δικαιωμάτων μπορεί να οδηγήσει σε σοβαρές επιπτώσεις, όπως η κλοπή δεδομένων ή η διάβρωση της εμπιστοσύνης των χρηστών. Η SR1.8 προτείνει να διαχειρίζονται οι διαχειριστές τον έλεγχο πρόσβασης στα προνομιακά δικαιώματα, ενώ πρέπει να χρησιμοποιούνται και άλλα μέτρα ασφαλείας, όπως η κρυπτογράφηση.

Η **SR1.9** αναφέρεται στη διαχείριση των προνομιακών δικαιωμάτων (privileged access) στο πλαίσιο της ασφάλειας της ταυτότητας, της πιστοποίησης και του ελέγχου πρόσβασης (identity management, authentication, and access control). Η αποτελεσματική διαχείριση των προνομιακών δικαιωμάτων είναι κρίσιμης σημασίας για την προστασία του συστήματος από επιθέσεις και αποτελεί μια από τις βασικές πρακτικές ασφαλείας.
Συγκεκριμένα, η SR1.9 απαιτεί την ταυτοποίηση των χρηστών που έχουν προνομιακά δικαιώματα, τη διαχείριση και την παρακολούθηση των προνομιακών δικαιωμάτων, την ελαχιστοποίηση του αριθμού των χρηστών που έχουν προνομιακή πρόσβαση, καθώς και τη διασφάλιση ότι οι προνομιακοί λογαριασμοί δεν χρησιμοποιούνται για προσωπικούς σκοπούς ή από άλλους χρήστες που δεν έχουν την κατάλληλη εξουσιοδότηση.

Στην υποκατηγορία πλαισίου κυβερνοασφάλειας PR.AC-1 ανήκουν τα στοιχεία ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 όπου το καθένα επιτελεί ένα μοναδικό έργο με σκοπό την ασφάλεια.

Πιο συγκεκριμένα το στοιχείο **A.9.2.1** αποτελεί μια πολιτική πρόσβαση όπου Πρόκειται για τη διαμόρφωση και την επικαιροποίηση μιας πολιτικής που να καθορίζει τους κανόνες και τις διαδικασίες πρόσβασης στις πληροφορίες. Το A.9.2.1 αναφέρεται στον έλεγχο των προνομίων πρόσβασης των χρηστών σε ευαίσθητα δεδομένα. Αυτό περιλαμβάνει τη διασφάλιση ότι η πρόσβαση σε ευαίσθητα δεδομένα επιτρέπεται μόνο σε χρήστες που έχουν το απαραίτητο επίπεδο προνομίων και ότι οι χρήστες αυτοί είναι αξιόπιστοι. Αυτός ο έλεγχος βοηθά στη διατήρηση της εμπιστοσύνης και στη μείωση του κινδύνου παραβίασης της ασφάλειας δεδομένων.

Με σκοπό την πρόσβαση στο δίκτυο και στις λειτουργίες αναφέρεται το **A.9.2.2** το οποίο αφορά τον έλεγχο του συστήματος πληροφορικής. Το A.9.2.2 αναφέρεται στον έλεγχο των δικαιωμάτων πρόσβασης στα δίκτυα και τα λογισμικά. Πιο συγκεκριμένα, αυτός ο έλεγχος αφορά τη διαχείριση των χρηστών και των δικαιωμάτων πρόσβασής τους σε δίκτυα και λογισμικά, με σκοπό την προστασία από την μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες πληροφορίες. Αυτό περιλαμβάνει τη διαχείριση των δικαιωμάτων πρόσβασης για τους χρήστες σε όλα τα στάδια τους, από την πρόσβαση στα δίκτυα και τα συστήματα μέχρι την ανάκληση των δικαιωμάτων πρόσβασης όταν δεν απαιτούνται πλέον. Επίσης, αυτός ο έλεγχος αφορά τη διαχείριση των δικαιωμάτων πρόσβασης για τα προσωπικά δεδομένα των χρηστών για τα οποία πρέπει να υπάρχουν κανόνες προστασίας και προστασία από ανεπιθύμητη πρόσβαση και κακόβουλη χρήση.

Το **A.9.2.3** αναφέρεται στον έλεγχο των δικαιωμάτων πρόσβασης σε εφαρμογές και συστήματα λογισμικού. Πιο συγκεκριμένα, αυτός ο έλεγχος απαιτεί την παροχή ελέγχου και περιορισμού των δικαιωμάτων πρόσβασης των χρηστών σε εφαρμογές και συστήματα λογισμικού, ώστε να αποτραπεί η μη εξουσιοδοτημένη πρόσβαση και η κακόβουλη χρήση των δεδομένων. Επιπλέον, αυτός ο έλεγχος προβλέπει την ανάθεση διαφορετικών δικαιωμάτων πρόσβασης σε διαφορετικές ομάδες χρηστών, ανάλογα με την εργασιακή τους θέση και τις ανάγκες της επιχείρησης. Τέλος, ο έλεγχος αυτός απαιτεί την παροχή μηχανισμών ανίχνευσης και παρακολούθησης των προσπαθειών μη εξουσιοδοτημένης πρόσβασης και κακόβουλης χρήσης των δεδομένων, ώστε να διασφαλίζεται η ασφάλεια των εφαρμογών και των συστημάτων λογισμικού.

Το **A.9.2.4** αναφέρεται στον έλεγχο των λογαριασμών χρηστών και τη διαχείριση των προνομιακών δικαιωμάτων. Αυτός ο έλεγχος απαιτεί τη θέσπιση διαδικασιών για τη διαχείριση των λογαριασμών χρηστών, την ανάθεση δικαιωμάτων πρόσβασης και τον έλεγχο της χρήσης αυτών των λογαριασμών. Ο έλεγχος περιλαμβάνει την ανάπτυξη και την εφαρμογή μηχανισμών για την ανίχνευση και την αντιμετώπιση παραβιάσεων ασφαλείας σχετικά με τους λογαριασμούς χρηστών και προβλέπει την ανάπτυξη πολιτικών για την αποδοχή, την αλλαγή και τη διαγραφή των λογαριασμών χρηστών, καθώς και για τη διαχείριση των κωδικών πρόσβασης.

Το **A.9.2.6** είναι ένα στοιχείο του προτύπου ISO/IEC 27001:2013 και αναφέρεται στη διαχείριση της ευθύνης των παροχών υπηρεσιών. Πρόκειται για την αναγνώριση των απαιτήσεων ασφαλείας που πρέπει να πληρούν οι πάροχοι υπηρεσιών και την επιβολή αυτών των απαιτήσεων στους παρόχους, προκειμένου να διασφαλιστεί ότι οι υπηρεσίες που παρέχονται από αυτούς είναι ασφαλείς και προστατεύουν τα δεδομένα της επιχείρησης.

Για τον έλεγχο της ασφάλειας των πληροφοριακών συστημάτων και των δεδομένων γίνεται αναφορά στο **A.9.3.1** το οποίο είναι υπεύθυνο για τον έλεγχο της αποτελεσματικότητας των μέτρων ασφαλείας που εφαρμόζονται στα πληροφοριακά συστήματα, καθώς και στην παρακολούθηση των πιθανών απειλών ασφαλείας και στη λήψη κατάλληλων μέτρων για την αντιμετώπισή τους.

Στον κατάλογο ελέγχου ISO 27001 για την διαχείριση των αδειών λογισμικού αναφέρεται το στοιχείο ελέγχου **A.9.4.2** . Συγκεκριμένα, απαιτείται να υπάρχουν διαδικασίες για τον έλεγχο της χρήσης του λογισμικού και τη διασφάλιση ότι οι άδειες χρήσης είναι έγκυρες και ενημερωμένες. Επιπλέον, πρέπει να υπάρχουν διαδικασίες για την αναγνώριση και επίλυση προβλημάτων σχετικά με τη χρήση των άδειων λογισμικού. Η συμμόρφωση με αυτήν την απαίτηση βοηθά στη διασφάλιση της νομιμότητας της χρήσης του λογισμικού και στη μείωση των κινδύνων ασφαλείας που σχετίζονται με την παράνομη χρήση ή τη χρήση μη ενημερωμένου λογισμικού.

Τέλος, Το **A.9.4.3** αναφέρεται στον κατάλογο ελέγχου ISO 27001 και αφορά τη διαχείριση των αδειών χρήσης του εξοπλισμού. Η απαίτηση αυτή απαιτεί την ύπαρξη διαδικασιών για τον έλεγχο της χρήσης του εξοπλισμού και τη διασφάλιση ότι οι άδειες χρήσης είναι έγκυρες και ενημερωμένες. Πιο ειδικά, η απαίτηση αυτή απαιτεί την καταγραφή και τον έλεγχο των αδειών χρήσης του εξοπλισμού που χρησιμοποιείται στο πλαίσιο της οργάνωσης, καθώς και την αναγνώριση και επίλυση προβλημάτων σχετικά με τη χρήση των αδειών χρήσης.

Η συμμόρφωση με αυτήν την απαίτηση βοηθά στη διασφάλιση της νομιμότητας της χρήσης του εξοπλισμού και στη μείωση των κινδύνων ασφαλείας που σχετίζονται με την παράνομη χρήση ή τη χρήση μη ενημερωμένου εξοπλισμού. Επιπλέον, η διαχείριση των αδειών χρήσης του εξοπλισμού συντελεί στη βελτίωση της διαθεσιμότητας του εξοπλισμού και της απόδοσης του.

Τα πρότυπα ασφαλείας **NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10 και IA-11** της υποκατηγορίας κυβερνοασφάλειας PR.AC-1 παραθέτονται στην ασφάλεια της πληροφορίας και των συστημάτων πληροφορικής. Οι AC-1 και AC-2 πρότυπα αναφέρονται στον έλεγχο της πρόσβασης στα συστήματα και τα δεδομένα και στη διαχείριση ταυτοποίησης και ελέγχου πρόσβασης. Τα πρότυπα IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10 και IA-11 αναφέρονται στην αντιμετώπιση των προβλημάτων ασφαλείας της πληροφορίας, όπως οι κίνδυνοι και οι απειλές από εξωτερικούς εχθρούς, οι εσωτερικοί κίνδυνοι και οι απειλές, και η προστασία της ακεραιότητας, εμπιστευτικότητας καθώς και διαθεσιμότητας της πληροφορίας. Αυτά τα πρότυπα απαιτούν την εφαρμογή αυστηρών πολιτικών ασφαλείας και τη χρήση τεχνολογικών λύσεων για την προστασία της πληροφορίας, και πρέπει να τηρούνται από οργανισμούς και επιχειρήσεις για τη διασφάλιση της ασφάλειας των πληροφοριακών συστημάτων τους. Η συμμόρφωση με αυτά τα πρότυπα απαιτεί συνεχή παρακολούθηση και αξιολόγηση των μέτρων ασφαλείας, καθώς και συστηματική κατάρτιση του προσωπικού για την αντιμετώπιση προβλημάτων. Τα πρότυπα αυτά έχουν σχεδιαστεί για να διασφαλίζουν την προστασία της πληροφορίας και την αποτελεσματική διαχείριση των κινδύνων ασφαλείας των συστημάτων πληροφορικής, προκειμένου να διατηρηθεί η αξιοπιστία, η εμπιστοσύνη και η αποτελεσματικότητα των οργανισμών και επιχειρήσεων. Οι προδιαγραφές αυτές καλύπτουν πολλούς τομείς της ασφάλειας των πληροφοριακών συστημάτων, όπως η αναγνώριση και αξιολόγηση των κινδύνων ασφαλείας, η εφαρμογή αυστηρών πολιτικών ασφαλείας, η παρακολούθηση και έλεγχος της πρόσβασης στις πληροφορίες, η προστασία της απορρήτου και η αντιμετώπιση των παραβιάσεων ασφαλείας. Η εφαρμογή αυτών των προδιαγραφών είναι αναγκαία για τη διασφάλιση της ακεραιότητας, της εμπιστοσύνης και της διαθεσιμότητας των πληροφοριακών συστημάτων.

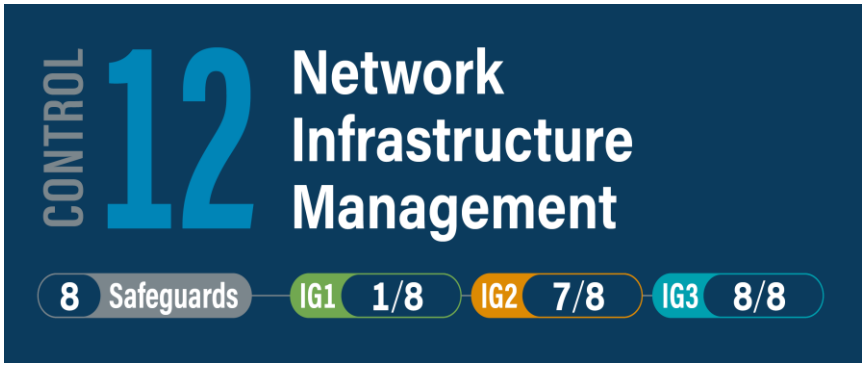
<u>Υποκατηγορία Πλαισίου Κυβερνοασφάλειας PR.AC-3</u>

Ο κίνδυνος στον κυβερνοχώρο ενός οικιακού δικτύου ή ενός δικτύου μίας μικρής επιχείρησης αυξάνεται όταν υπάρχει οποιοδήποτε είδος απομακρυσμένης πρόσβασης. Σε ένα σενάριο χειρότερης περίπτωσης (που είναι σχετικά συνηθισμένο σε κυβερνοεπιθέσεις που σχετίζονται με ransomware και παραβίαση δεδομένων), ο κίνδυνος αποδεικνύεται σίγουρος, καθώς

οι φορείς απειλών αξιοποιούν την μη ασφαλή απομακρυσμένη πρόσβαση ως αρχικό φορέα για μια επίθεση. Το πλαίσιο PR.AC-3 βασίζεται στην αναγνώριση των απειλών και των ευπαθειών των κρίσιμων πληροφοριακών συστημάτων και προτείνει μια σειρά από μέτρα για την προστασία αυτών των συστημάτων. Τα μέτρα αυτά περιλαμβάνουν τη διαχείριση της ασφάλειας των πληροφοριακών συστημάτων, την ανίχνευση και αντιμετώπιση παραβιάσεων ασφαλείας.

Το **PR.AC-3** αναφέρεται σε ένα σύστημα που διαχειρίζεται την απομακρυσμένη πρόσβαση. Αυτό σημαίνει ότι το σύστημα επιτρέπει σε χρήστες να συνδέονται από μακριά σε υπολογιστές ή δίκτυα και να αποκτούν πρόσβαση σε πόρους όπως αρχεία, εφαρμογές και συστήματα. Η διαχείριση της απομακρυσμένης πρόσβασης είναι σημαντική για την επιχειρησιακή ασφάλεια και τη διαχείριση των προνομίων πρόσβασης των χρηστών. Το PR.AC-3 είναι ένα σύστημα που βοηθά στην αποτροπή των απειλών ασφαλείας που προκύπτουν από την απομακρυσμένη πρόσβαση και διασφαλίζει ότι οι χρήστες έχουν την απαραίτητη πρόσβαση στους απαραίτητους πόρους με τον ασφαλέστερο δυνατό τρόπο.

Το CIS CSC 12 περιγράφει την ανάγκη για τον έλεγχο των συνόρων του δικτύου και την προστασία τους από ανεπιθύμητη πρόσβαση. Στην υποκατηγορία PR.AC-3, το CIS CSC 12 αναφέρεται στην ανάγκη να ελέγχονται οι απομακρυσμένες συνδέσεις στο δίκτυο και να διαχειρίζεται η πρόσβαση σε αυτές. Πιο συγκεκριμένα, πρέπει να εφαρμόζονται κατάλληλα μέτρα ασφαλείας, όπως ο έλεγχος της ταυτότητας και τα διαπιστευτήρια πρόσβασης, η επαλήθευση της ταυτότητας του χρήστη και η παρακολούθηση της πρόσβασης στο δίκτυο για την ανίχνευση απειλών και παραβιάσεων. Το CIS CSC 12 σε συνδυασμό με το PR.AC-3 είναι σημαντικό για τη διατήρηση της ασφάλειας του δικτύου και των πόρων του, ειδικά όταν οι απομακρυσμένες συνδέσεις είναι αναπόφευκτες για τη λειτουργία της επιχείρησης.



Τα **COBIT 5 APO13.01, DSS01.04** και **DSS05.03** είναι ενημερωτικές αναφορές στο πλαίσιο κυβερνοασφάλειας PR.AC-3 που αναφέρονται σε διαφορετικές πτυχές της ασφάλειας των πληροφοριών.

Το **COBIT 5 APO13.01** αφορά τον έλεγχο των προνομίων πρόσβασης. Αυτό σημαίνει ότι παρέχει κατευθυντήριες γραμμές για το πώς πρέπει να ελέγχεται η πρόσβαση στα συστήματα και τις εφαρμογές πληροφορικής, ώστε να μην δίνεται ανεξέλεγκτη πρόσβαση σε ευαίσθητα δεδομένα. Από την άλλη το **DSS01.04** αναφέρεται στη διαχείριση της ασφάλειας των πληροφοριών. Προτείνει μια σειρά από ελέγχους και διαδικασίες για τη διαχείριση των κινδύνων ασφαλείας των πληροφοριών και τη διασφάλιση της συμμόρφωσης με τις νομοθεσίες και τους κανονισμούς που αφορούν την ασφάλεια των πληροφοριών. Τέλος το **DSS05.03** αναφέρεται στον

έλεγχο των εφαρμογών πληροφορικής. Παρέχει κατευθυντήριες γραμμές για το πώς πρέπει να ελέγχονται οι εφαρμογές πληροφορικής ώστε να διασφαλίζεται η προστασία των ευαίσθητων δεδομένων που επεξεργάζονται οι εφαρμογές.

Η παράγραφος **4.3.3.6.6 του προτύπου ISA 62443-2-1:2009** περιγράφει τις απαιτήσεις για τον έλεγχο της κατανόησης και της συμμόρφωσης με τις αρχές της κυβερνοασφάλειας από το προσωπικό που ασχολείται με τα συστήματα ελέγχου και αυτοματισμού σε μια εγκατάσταση είτε πρόκειται για ένα οικιακό δίκτυο είτε για ένα δίκτυο μικρών επιχειρήσεων. Η εν λόγω ενημερωτική αναφορά που υπάρχει στην υποκατηγορία κυβερνοασφάλειας PR.AC-3 προσδιορίζει ότι το προσωπικό που ασχολείται με τα συστήματα ελέγχου και αυτοματισμού πρέπει να είναι εξοικειωμένο με τις απαιτήσεις ασφάλειας της εγκατάστασης και του χώρου εργασίας της. Επιπλέον, πρέπει να είναι ενημερωμένοι σχετικά με τις τεχνικές και τις διαδικασίες που χρησιμοποιούνται για την προστασία των συστημάτων αυτών από κυβερνοεπιθέσεις και ανεπιθύμητες εισβολές.

Στην υποκατηγορία πλαισίου κυβερνοασφάλειας PR.AC-3 διακρίνονται οι αναφορές **SR 1.13** και **SR 2.6** του προτύπου ISA 62443-3-3:2013 αφορούν στον έλεγχο και τη διαχείριση των κινδύνων ασφαλείας στο πλαίσιο της κυβερνοασφάλειας.

Η αναφορά **SR 1.13** απαιτεί από τους χρήστες του προτύπου να αξιολογούν τους κινδύνους ασφαλείας που σχετίζονται με τα συστήματα ελέγχου και αυτοματισμού και να λαμβάνουν μέτρα για τη μείωσή τους. Αυτό βοηθά στη διατήρηση ενός υψηλού επιπέδου ασφάλειας των συστημάτων αυτών και στην προστασία από επιθέσεις και καταστροφές.

Η αναφορά **SR 2.6** απαιτεί την υιοθέτηση ενός συστήματος διαχείρισης κινδύνων ασφαλείας που θα περιλαμβάνει την ανάλυση και την αξιολόγηση των κινδύνων ασφαλείας. Μέσω αυτής της αναφοράς, διασφαλίζεται ότι όλοι οι κίνδυνοι ασφαλείας συλλέγονται, αναλύονται και αξιολογούνται κατάλληλα, ώστε να ληφθούν τα απαραίτητα μέτρα για την πρόληψη των κινδύνων αυτών και την ελαχιστοποίηση των επιπτώσεών τους.

Η υποκατηγορία πλαισίου κυβερνοασφάλειας PR.AC-3 αναφέρεται στη διαχείριση των ενημερωτικών αναφορών και περιλαμβάνει ορισμένες απαιτήσεις.

Για την διαχείριση των τεκμηριωμένων πληροφοριών ασφάλειας διακρίνεται η ενημερωτική αναφορά **A.6.2.1** που σχετίζεται με τη διαχείριση των πληροφοριών ασφαλείας που έχουν τεκμηριωθεί και πρέπει να είναι προσβάσιμες από εξουσιοδοτημένα άτομα. Πρέπει να υπάρχει μια διαδικασία για τη συλλογή, τη διατήρηση και τη διανομή των πληροφοριών αυτών.

Παράλληλα γίνεται η αναφορά στο **A.6.2.2** το οποίο είναι υπεύθυνο για την επαλήθευση της εγκυρότητας των ενημερωτικών αναφορών που λαμβάνονται από διάφορες πηγές, όπως προειδοποιήσεις ασφαλείας, συμβουλές και ενημερώσεις ασφαλείας. Η επαλήθευση πρέπει να γίνεται πριν από τη διανομή των αναφορών αυτών στους ενδιαφερόμενους.

Το **A.11.2.6** αναφέρεται για την διαχείριση της ασφαλείας των πληροφοριακών συστημάτων των παρόχων. Οι πάροχοι πρέπει να διασφαλίζουν ότι τα πληροφοριακά τους συστήματα είναι ασφαλή και δεν υπάρχει κίνδυνος διαρροής ή κλοπής των ενημερωτικών αναφορών που φιλοξενούνται σε αυτά.

Στη διαχείριση των ευπαθειών ασφάλειας των πληροφοριακών συστημάτων συμβάλει η απαίτηση **A.13.1.1**. Αυτή η απαίτηση αφορά στη διαχείριση των ευπαθειών ασφαλείας των πληροφοριακών συστημάτων που χρησιμοποιούνται για την ανταλλαγή και την αποθήκευση ενημερωτικών αναφορών. Πρέπει να υπάρχει μια διαδικασία για την ανίχνευση και την επίλυση ευπαθειών ασφαλείας, καθώς και μια στρατηγική για την πρόληψη ευπαθειών στο μέλλον.

Τέλος το **A.13.2.1** αφορά στη διαχείριση των ιχνηλατών ασφαλείας και αναλύσεων. Αυτή η απαίτηση αφορά στη διαχείριση των στοιχείων που αφορούν στην ασφάλεια των ενημερωτικών αναφορών. Πρέπει να υπάρχει μια διαδικασία για τη συλλογή και τη διατήρηση στοιχείων που σχετίζονται με την ασφάλεια των ενημερωτικών αναφορών. Επίσης, πρέπει να υπάρχει μια διαδικασία για την ανάλυση αυτών των στοιχείων ώστε να αξιολογηθούν τυχόν προβλήματα και να ληφθούν μέτρα πρόληψης για το μέλλον.

Συνολικά, οι ενημερωτικές αναφορές πρέπει να διασφαλίσουν ότι φιλοξενούνται στα πληροφοριακά τους συστήματα και προστατεύονται από κινδύνους καθώς και διασφαλίζουν την εμπιστευτικότητα, τη διαθεσιμότητα και την ακεραιότητά τους. Η συμμόρφωση με τις απαιτήσεις της υποκατηγορίας πλαισίου κυβερνοασφάλειας PR.AC-3 εξασφαλίζει την προστασία των ενημερωτικών αναφορών και τη διασφάλιση της εμπιστευτικότητάς τους, ενισχύοντας έτσι την εμπιστοσύνη των πελατών και των επιχειρήσεων στην ποιότητα και ασφάλεια των υπηρεσιών που παρέχονται από τον πάροχο ενημερωτικών αναφορών.

Στην υποκατηγορία πλαισίου κυβερνοασφάλειας που αναλύεται αναφέρονται οι κανονισμοί **AC-1, AC-17, AC-19, AC-20, SC-15** όπου αποτελούν μέρος του NIST SP 800-53 Rev.4 ο οποίος είναι ένας οδηγός για την ανάπτυξη και την εφαρμογή ασφαλούς πληροφοριακής αρχιτεκτονικής για την προστασία των ευαίσθητων πληροφοριών και των συστημάτων. Οι κανονισμοί AC-1, AC-17, AC-19, AC-20 και SC-15 αναφέρονται σε μέτρα πρόληψης και ανίχνευσης παραβιάσεων στοιχείων ελέγχου πρόσβασης και αποτροπής μη εξουσιοδοτημένης πρόσβασης σε ευαίσθητες πληροφορίες και συστήματα.

Συγκεκριμένα, ο κανονισμός **AC-1** αναφέρεται στην ανίχνευση, την παρακολούθηση και την αντίδραση σε παραβιάσεις στοιχείων ελέγχου πρόσβασης. Ο κανονισμός **AC-17** περιγράφει τη διαχείριση των ηλεκτρονικών κλειδιών, των πιστοποιητικών και των ψηφιακών υπογραφών για την αυθεντικοποίηση και την επικύρωση των πληροφοριών.

Οι απαιτήσεις του **AC-19** προσδιορίζουν τις διαδικασίες και τα μέτρα που πρέπει να ληφθούν για τη διαχείριση των δικαιωμάτων πρόσβασης σε ευαίσθητες πληροφορίες. Οι οργανισμοί πρέπει να διασφαλίζουν ότι οι χρήστες έχουν την κατάλληλη πρόσβαση στις

πληροφορίες που χρειάζονται για την εκτέλεση των καθηκόντων τους, ενώ ταυτόχρονα πρέπει να περιορίζεται η πρόσβαση σε πληροφορίες που δεν είναι απαραίτητες ή δεν έχουν άδεια πρόσβασης.

Ο κανονισμός **AC-20** απαιτεί τη λήψη μέτρων για την ασφάλεια των δεδομένων, την επιλογή μιας αξιόπιστης CSP και τη διασφάλιση ότι οι χρήστες του CSP είναι εξουσιοδοτημένοι να αποκτούν πρόσβαση σε αυτά. Ο CSP (Cloud Service Provider) αναφέρεται σε μια εταιρεία ή πάροχο υπηρεσιών που προσφέρει υπηρεσίες στον τομέα του cloud computing. Οι υπηρεσίες αυτές μπορούν να περιλαμβάνουν αποθήκευση δεδομένων, επεξεργασία δεδομένων, διαχείριση βάσεων δεδομένων, εφαρμογές λογισμικού και άλλες υπηρεσίες που παρέχονται μέσω του διαδικτύου. Η πολιτική αυτή απαιτεί επίσης τη διασφάλιση ότι ο CSP διαθέτει μέτρα αντιμετώπισης περιστατικών και ανάκαμψης σε περίπτωση που παρουσιαστεί πρόβλημα στο πάροχο υπηρεσιών.

Ο κανονισμός **SC-15** αναφέρεται στην παρακολούθηση των συστημάτων πληροφορικής για ενδεχόμενες ασφαλείας παραβιάσεις ή παρατυπίες στη λειτουργία τους. Απαιτεί επίσης την ανάπτυξη επαρκών μηχανισμών παρακολούθησης και την καταγραφή των συμβάντων αυτών, καθώς και τη διασφάλιση ότι οι αναφορές αυτές θα αναλυθούν και θα διαχειριστούν με επαγγελματισμό και εγκυρότητα.

Υποκατηγορία Πλαισίου Κυβερνοασφάλειας PR.AC-4

Ο κανόνας **PR.AC-4** αναφέρεται στη διαχείριση των δικαιωμάτων πρόσβασης στις πληροφορίες και στα συστήματα. Η διαχείριση αυτών των δικαιωμάτων πρέπει να γίνεται με βάση τις αρχές του λιγότερου δυνατού προνομίου (least privilege) και του διαχωρισμού των καθηκόντων (separation of duties). Η αρχή του λιγότερου δυνατού προνομίου αναφέρεται στην αρχή ότι ο κάθε χρήστης ή διαχειριστής θα πρέπει να έχει μόνο τα απαραίτητα δικαιώματα που απαιτούνται για να εκτελέσει τις εργασίες του. Αυτό μειώνει τον κίνδυνο ανεπιθύμητης πρόσβασης σε ευαίσθητες πληροφορίες ή συστήματα. Ο διαχωρισμός των καθηκόντων αναφέρεται στον διαχωρισμό των καθηκόντων μεταξύ διαφορετικών χρηστών ή διαχειριστών. Αυτό αποτρέπει τη δυνατότητα ενός χρήστη ή διαχειριστή να εκτελέσει κακόβουλες ενέργειες ή να κάνει λάθος λόγω των καθηκόντων του στο σύστημα.

Οι ελέγχοι ασφαλείας **CIS Critical Security Control 3** που εφαρμόζονται στην υποκατηγορία πλαισίου κυβερνοασφάλειας **PR.AC-4** περιλαμβάνουν μια σειρά από πρακτικές που στοχεύουν στην προστασία των δεδομένων από απώλεια, κλοπή ή αποκάλυψη σε μη εξουσιοδοτημένα πρόσωπα. Οι πρακτικές αυτές περιλαμβάνουν την κρυπτογράφηση δεδομένων, την απομάκρυνση περιττών δεδομένων και την υλοποίηση αυστηρών πολιτικών για τη διαχείριση των δικαιωμάτων πρόσβασης σε δεδομένα. Με την εφαρμογή αυτών των ελέγχων ασφαλείας, οι

οργανισμοί μπορούν να διασφαλίσουν ότι οι ευαίσθητες πληροφορίες και άλλα ευαίσθητα δεδομένα παραμένουν ασφαλή και προστατευμένα.

Για την διαχείριση των λογαριασμών των χρηστών στο σύστημα ενός οικιακού δικτύου ή ενός δικτύου μιας μικρής επιχείρησης είναι υπεύθυνος ο έλεγχος ασφάλειας **CIS Critical Security Control 5**. Αυτός ο έλεγχος περιλαμβάνει επίσης τη διαχείριση των δικαιωμάτων πρόσβασης στους λογαριασμούς και των περιορισμών των δικαιωμάτων που επιτρέπουν σε κάθε χρήστη να προσπελαύνει συγκεκριμένα στοιχεία του συστήματος. Η εφαρμογή του CIS Critical Security Control 5 βοηθά στην αποτροπή της χρήσης μη εξουσιοδοτημένων λογαριασμών για πρόσβαση σε ευαίσθητα δεδομένα και συστήματα, ενώ επίσης μπορεί να βοηθήσει στην πρόληψη εσωτερικών απειλών από κακόβουλους χρήστες. Με την εφαρμογή αυτού του ελέγχου μπορεί να διασφαλιστεί ότι οι λογαριασμοί χρηστών διαχειρίζονται αποτελεσματικά και ασφαλώς, μειώνοντας τον κίνδυνο απώλειας δεδομένων ή παραβίασης της ασφάλειας του συστήματος.

Ο έλεγχος ασφαλείας **CIS Critical Security Control 12** αφορά τη διαχείριση των δικτυακών υποδομών ενός οργανισμού, συμπεριλαμβανομένων των δικτύων, των συσκευών δικτύου και των εφαρμογών δικτύου και κρίνεται άκρως απαραίτητη η εφαρμογή του. Η διαχείριση αυτή πρέπει να εστιάζει στην εξασφάλιση της διαθεσιμότητας, της ακεραιότητας και της εμπιστευτικότητας των δικτυακών συστημάτων. Ο έλεγχος CIS Critical Security Control 12 περιλαμβάνει τη διαχείριση των δικτυακών πρωτοκόλλων και των ασφαλών συνδέσεων, καθώς και την παρακολούθηση της δικτυακής κυκλοφορίας για την ανίχνευση επιθέσεων.

Οι CIS Critical Security Controls αποτελούν ένα σύνολο από προτεινόμενες πρακτικές ασφαλείας πληροφορικής, τις οποίες μπορεί να χρησιμοποιήσει μια εταιρεία για να βελτιώσει το επίπεδο ασφάλειας των συστημάτων και των δεδομένων της. Ο έλεγχος **CIS CSC 14** αναφέρεται στην ανάγκη για ευαισθητοποίηση και εκπαίδευση του προσωπικού σε θέματα ασφάλειας. Πρόκειται για ένα κρίσιμο βήμα για την πρόληψη των επιθέσεων στο δίκτυο και των παραβιάσεων της ασφάλειας δεδομένων. Η εκπαίδευση του προσωπικού πρέπει να περιλαμβάνει την αναγνώριση των απειλών ασφαλείας και τη χρήση ασφαλών πρακτικών.

Στην εν λόγω υποκατηγορία πλαισίου κυβερνοασφάλειας εμφανίζεται ο έλεγχος **CIS Critical Security Control 15** όπου αναφέρεται στη διαχείριση των παρόχων υπηρεσιών ασφάλειας. Πρόκειται για μια σειρά από συστάσεις και βέλτιστες πρακτικές που αποσκοπούν στην προστασία των πληροφοριακών συστημάτων ενός οργανισμού από επιθέσεις που μπορούν να προέλθουν από τους παρόχους των υπηρεσιών του. Οι παρόχοι υπηρεσιών ασφάλειας περιλαμβάνουν όλους τους φορείς που παρέχουν υπηρεσίες σχετικές με την ασφάλεια των πληροφοριακών συστημάτων.

Ένας απ τους πιο αναγκαίους τομείς στην ασφάλεια IoT συσκευών είναι η ασφάλεια του λογισμικού. Το **CIS Critical Security Control 16** αναφέρεται στην ασφάλεια του λογισμικού εφαρμογών και αποτελεί μια σειρά από πρακτικές που στοχεύουν στην πρόληψη και αντιμετώπιση επιθέσεων που στοχεύουν σε ευπάθειες του λογισμικού εφαρμογών. Με την αύξηση της χρήσης λογισμικού και την εξάπλωση του διαδικτύου, η ασφάλεια του λογισμικού εφαρμογών έχει γίνει ουσιώδη και απαραίτητη. Το CIS Control 16 τονίζει τη σημασία της διαχείρισης του κύκλου ζωής ασφαλείας του λογισμικού για την πρόληψη, τον εντοπισμό και την αποκατάσταση αδυναμιών ασφάλειας. Οι εφαρμογές είναι ζωτικής σημασίας για την παροχή στους χρήστες ενός εύκολου τρόπου πρόσβασης και διαχείρισης ευαίσθητων δεδομένων. Οι εισβολείς μπορούν να εκμεταλλευτούν ευπάθειες σε εφαρμογές για να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα ή να πάρουν τον έλεγχο των ευάλωτων περιουσιακών στοιχείων. Οι σύγχρονες εφαρμογές αναπτύσσονται, λειτουργούν και διατηρούνται σε ένα εξαιρετικά περίπλοκο, ποικιλόμορφο και δυναμικό περιβάλλον. Οι παραδοσιακές προσεγγίσεις ασφάλειας είναι προκλητικές λόγω των μικρότερων κύκλων ανάπτυξης, του συνδυασμού πλαισίων ανάπτυξης και των εξελισσόμενων κανονισμών προστασίας δεδομένων. Η απόκτηση πλατφορμών λογισμικού ως υπηρεσίας (SaaS) φέρνει πρόσθετες προκλήσεις, καθώς οι επιχειρήσεις ενδέχεται να μην έχουν ορατότητα στις πρακτικές ασφαλείας αυτών των πλατφορμών.

Τέλος , τα **18 CIS Critical Security Controls** (Κρίσιμοι Έλεγχοι Ασφαλείας CIS) είναι μια σειρά από βασικές ασφαλείας πληροφορικής πρακτικές που έχουν σχεδιαστεί για να βοηθήσουν τους οργανισμούς και τις οικίες να προστατεύσουν τα συστήματά τους από επιθέσεις και απειλές ασφαλείας. Οι κρίσιμοι έλεγχοι ασφαλείας CIS είναι σχεδιασμένοι ώστε να παρέχουν μια συγκεκριμένη λίστα από βασικές ασφαλείς πρακτικές και προτείνουν μια μεθοδολογία για την εφαρμογή τους στον οργανισμό σας. Η λίστα περιλαμβάνει τις κοινές πρακτικές που χρησιμοποιούνται σήμερα από τους ειδικούς σε ασφάλεια πληροφορικής και βοηθά τους οργανισμούς να εφαρμόζουν αποτελεσματικές πολιτικές ασφαλείας πληροφορικής.

Όπως και στην υποκατηγορία πλαισίου κυβερνοασφάλειας PR.AC-1 ομοίως και στην υποκατηγορία PR.AC-4 αναφέρεται το **COBIT 5 DSS05.04** όπου αφορά την ανάπτυξη και την εφαρμογή ενός συστήματος ελέγχου πρόσβασης στα δεδομένα, με σκοπό την προστασία της εχεμύθειας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων. Το συγκεκριμένο μοντέλο αποτελεί μέρος του COBIT 5, ενός πλαισίου διαχείρισης και ελέγχου της πληροφοριακής τεχνολογίας που αναπτύχθηκε από το ISACA (Information Systems Audit and Control Association). Ο στόχος του COBIT 5 DSS05.04 είναι η διασφάλιση ότι οι πρόσβαση στα δεδομένα επιτρέπεται μόνο σε αυτούς που έχουν την εξουσιοδότηση να τα χρησιμοποιούν και ότι τα δεδομένα διατηρούνται ασφαλή κατά τη διάρκεια της χρήσης τους. Περιλαμβάνει οδηγίες για το σχεδιασμό, την υλοποίηση και τη διαχείριση ενός συστήματος ελέγχου πρόσβασης στα δεδομένα.

Για την διαχείριση των αποτελεσμάτων ασφάλειας που προκύπτουν από τις διαδικασίες αξιολόγησης των απαιτήσεων ασφαλείας του συστήματος ελέγχου αναφέρεται το σημείο **4.3.3.7.3** του προτύπου **ISA 62443-2-1:2009**. Συγκεκριμένα, αναφέρεται στην ανάγκη για διαχείριση των αποτελεσμάτων των διαδικασιών αξιολόγησης που έχουν πραγματοποιηθεί στο σύστημα ελέγχου.

Το πρότυπο **ISA 62443-3-3:2013 SR 2.1** που αναφέρεται στην συγκεκριμένη υποκατηγορία αφορά την ασφάλεια των συστημάτων ελέγχου και της επεξεργασίας δεδομένων στα βιομηχανικά συστήματα ελέγχου. Πιο συγκεκριμένα, το πρότυπο απαιτεί την ανάπτυξη και εφαρμογή μέτρων ασφαλείας για να προστατεύσει τα βιομηχανικά συστήματα ελέγχου από επιθέσεις, κακόβουλο λογισμικό και άλλους κινδύνους ασφαλείας. Μερικά από τα στοιχεία ασφάλειας που αναφέρονται στο πρότυπο περιλαμβάνουν την προστασία των συστημάτων ελέγχου από ανεπιθύμητη πρόσβαση, την ασφαλή αποθήκευση και επεξεργασία δεδομένων, τη διαχείριση αποτυχιών και την ασφαλή επαναφορά του συστήματος σε περίπτωση προβλήματος.

Στην PR.AC-4 για να καλυφθούν ορισμένα από τα μέτρα ασφαλείας αναφέρονται οι τα σημεία A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 και A.9.4.5 στο πλαίσιο του προτύπου **ISO/IEC 27001:2013** με σκοπό τη διαχείριση της ασφάλειας των πληροφοριών. Συγκεκριμένα, το σημείο **A.6.1.2** αναφέρεται στον περιορισμό των δικαιωμάτων πρόσβασης σε συστήματα και εφαρμογές ενώ το σημείο **A.9.1.2** αναφέρεται στη διαχείριση των προνομίων πρόσβασης. Για την φυσική ασφάλεια των συστημάτων πληροφορικής αναφέρεται το σημείο **A.9.2.3** το οποίο εξασφαλίζει την ανάγκη προστασίας των φυσικών εγκαταστάσεων της επιχείρησης ή της οικίας από κλοπές, ζημιές ή καταστροφή συστημάτων πληροφορικής ενώ για την πρόσβαση των δικαιωμάτων του χρήστη εφαρμόζεται το **A.9.4.1** όπου αναφέρεται στον έλεγχο της πρόσβασης των χρηστών στα συστήματα πληροφορικής και τις πληροφορίες της επιχείρησης ή της οικίας. Προκειμένου να επιτευχθεί η ασφάλεια των συστημάτων πληροφορικής και επικοινωνιών διακρίνονται δύο επιπλέον ενότητες του προτύπου , η ενότητα **A.9.4.4** και η **A.9.4.5**. Πιο συγκεκριμένα, η ενότητα **A.9.4.4** δίνει λύσεις στη διαχείριση των κλειδιών κρυπτογράφησης, δηλαδή στη διαχείριση των μέσων που χρησιμοποιούνται για την προστασία των πληροφοριών από μη εξουσιοδοτημένη πρόσβαση. Σε αυτήν την ενότητα, πρέπει να καθοριστούν και να εφαρμοστούν κατάλληλοι μηχανισμοί για την ασφαλή αποθήκευση, χρήση και διαχείριση των κλειδιών κρυπτογράφησης. Η ενότητα **A.9.4.5** του προτύπου αυτού δίνει εφαρμογές στην ασφάλεια των δικτύων επικοινωνίας στα συστήματα ελέγχου. Πιο αναλυτικά, η ενότητα αυτή ασχολείται με τις τεχνικές που αφορούν στην προστασία των δικτύων επικοινωνίας, τη διαχείριση των κλειδιών ασφαλείας, καθώς και την ασφαλή αποθήκευση και μεταφορά των πληροφοριών. Είναι σημαντική για την εξασφάλιση της αποτελεσματικότητας και αξιοπιστίας των συστημάτων ελέγχου καθώς και τη διατήρηση της ασφάλειας των επικοινωνιών τους.

Στην εν λόγω υποκατηγορία γίνεται αναφορά στο **NIST SP 800-53 Rev. 4** και πιο συγκεκριμένα οι αναφορές σε **AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24**. Σύμφωνα με τον κωδικό ελέγχου **AC-4** είναι απαραίτητο ότι όλοι οι χρήστες που θέλουν να έχουν πρόσβαση στο σύστημα ή στις εφαρμογές πρέπει να προσδιορίζονται, να επαληθεύονται και να εξουσιοδοτούνται πριν τους επιτραπεί η πρόσβαση σε ευαίσθητα δεδομένα. Το **AC-5** είναι ένας κωδικός ελέγχου ασφάλειας που αναφέρεται στη διαχείριση της δικτυακής πρόσβασης. Συγκεκριμένα, απαιτείται η εφαρμογή τεχνικών ελέγχου πρόσβασης στα δικτυακά συστήματα και η παρακολούθηση των δραστηριοτήτων στο δίκτυο. Αυτό σημαίνει ότι πρέπει να εγκατασταθούν και να χρησιμοποιηθούν μέτρα ασφαλείας όπως έλεγχος πρόσβασης με βάση τον ρόλο και περιορισμοί πρόσβασης σε ευαίσθητα δεδομένα. Το **AC-6** είναι ένας από τους κανόνες ασφαλείας που περιλαμβάνονται σε αυτό το πρότυπο και αναφέρεται στη διαχείριση και τον έλεγχο των δικαιωμάτων πρόσβασης στα πληροφοριακά συστήματα. Το AC-6 απαιτεί τη διαχείριση των δικαιωμάτων πρόσβασης στα πληροφοριακά συστήματα με βάση τον ρόλο του χρήστη, τον τύπο των δεδομένων στα οποία έχει πρόσβαση ο χρήστης. Ο έλεγχος **AC-14** αφορά τον περιορισμό της πρόσβασης σε πόρους του συστήματος πληροφορικής μόνο στους χρήστες που έχουν την ανάγκη να τους χρησιμοποιήσουν στο πλαίσιο των επαγγελματικών τους καθηκόντων. Αυτό συμβάλλει στη διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών που επεξεργάζεται το σύστημα πληροφορικής. Ο έλεγχος **AC-16** αφορά τη διαχείριση των λογαριασμών χρηστών του συστήματος πληροφορικής, συμπεριλαμβανομένων των δικαιωμάτων πρόσβασης και των διαδικασιών διαχείρισής τους. Αυτός ο έλεγχος εξασφαλίζει ότι οι χρήστες έχουν μόνο τα απαραίτητα δικαιώματα πρόσβασης σε πόρους και λειτουργίες του συστήματος πληροφορικής. Το **AC-24** είναι ένας από τους κανονισμούς του προτύπου που αφορά την ανίχνευση και την πρόληψη της εισβολής σε ευαίσθητα δίκτυα. Συγκεκριμένα, ο κανονισμός απαιτεί από τις επιχειρήσεις ή τα οικιακά δίκτυα να εγκαταστήσουν και να διατηρήσουν μηχανισμούς ανίχνευσης εισβολών σε κατάλληλα σημεία εντός των δικτύων τους, ώστε να μπορούν να εντοπίζουν και να αντιμετωπίζουν αποτελεσματικά οποιεσδήποτε απόπειρες εισβολής.

<u>Υποκατηγορία Πλαισίου Κυβερνοασφάλειας PR.AC-5</u>

Το NCCoE (National Cybersecurity Center of Excellence) του NIST (National Institute of Standards and Technology) δημοσίευσε μια ανάλυση των χαρακτηριστικών ασφάλειας που απαιτούνται για να προστατευθούν τα δίκτυα IoT. Η πρακτική **PR.AC-5** αφορά την προστασία της ακεραιότητας του δικτύου, και συμπεριλαμβάνει την ενσωμάτωση απομόνωσης του δικτύου όταν αυτό είναι αναγκαίο. Η απομόνωση του δικτύου είναι μια τεχνική ασφάλειας που χρησιμοποιείται για να διαχωρίσει τμήματα του δικτύου και να περιορίσει την πρόσβαση σε αυτά. Με αυτόν τον τρόπο, η απομόνωση του δικτύου μπορεί να βοηθήσει στην πρόληψη ή τη μείωση των απειλών ασφαλείας, καθώς περιορίζει την επίδραση πιθανών επιθέσεων σε ένα τμήμα του δικτύου, αντί να επεκτείνονται σε ολόκληρο το δίκτυο.

Τα CIS CSC (Center for Internet Security Critical Security Controls) είναι ένα σύνολο από χαρακτηριστικά ασφάλειας που απαιτούνται για την προστασία των πληροφοριακών συστημάτων.

Για την προστασία των εφαρμογών και των δεδομένων από κακόβουλο λογισμικό (malware defense) εφαρμόζεται το στοιχείο ελέγχου **CSC 9**. Το CSC 9 προτείνει μέτρα προστασίας όπως η χρήση ενημερωμένου antivirus και firewall, η παρακολούθηση της κίνησης δεδομένων στο δίκτυο και η εφαρμογή περιορισμών στις δικτυακές συνδέσεις. Το CSC 9 δίνει μία προστασία σε email καθώς και στο πρόγραμμα περιήγησης στο Web.

Η εκπαίδευση του εργατικού δυναμικού και των χρηστών του συστήματος σε ένα οικιακό δίκτυο με συσκευές IoT κρίνεται αναγκαία. Με τη κατάλληλη ενημέρωση και επίγνωση για θέματα ασφάλειας μέσω ενός προγράμματος ευαισθητοποίησης μπορεί να επηρεαστεί η συμπεριφορά των χρηστών για την ασφάλεια σύμφωνα με το **CIS CSC 14**.

Η διαχείριση παρόχου υπηρεσιών (Service Provider Management) με το **CIS CSC 15** αποσκοπεί στην ενίσχυση της ασφάλειας των συστημάτων πληροφορικής και της προστασίας των δεδομένων σε επιχειρήσεις και οικιακά δίκτυα. Το Service Provider Management περιγράφει τα κατάλληλα μέτρα ασφάλειας που πρέπει να ληφθούν από τους πάροχους υπηρεσιών πληροφορικής (service providers) για τη διασφάλιση της ασφάλειας των δεδομένων του πελάτη, καθώς και την προστασία των συστημάτων και του δικτύου τους από επιθέσεις. Οι πάροχοι υπηρεσιών πρέπει να λάβουν υπόψη τους πτυχές όπως η διαχείριση πρόσβασης στα συστήματα, η κρυπτογράφηση των δεδομένων και η επιθεώρηση της ασφάλειας του συστήματος. Επίσης, πρέπει να εφαρμόσουν μέτρα ασφάλειας όπως τη χρήση αυθεντικοποίησης δύο παραγόντων, την ανίχνευση και αποτροπή των επιθέσεων DDoS και την επιβολή αυστηρών κανόνων ασφάλειας στα εσωτερικά τους συστήματα.

Στην υποκατηγορία πλαισίου κυβερνοασφάλειας PR.AC-5 αναφέρεται ο έλεγχος **CIS CSC 18** που είναι υπεύθυνος για την καταγραφή συμβάντων ασφάλειας σε πραγματικό χρόνο για διάφορα συστήματα και εφαρμογές καθώς και για όλες τις παραμέτρους που σχετίζονται με την καταγραφή ασφάλειας όπως για παράδειγμα η ημερομηνία και η ώρα που ο χρήστης πραγματοποίησε κάποια ενέργεια. Με τον συγκεκριμένο έλεγχο τακτικά συλλέγονται, αναλύονται και αποθηκεύονται οι καταγραφές ασφάλειας.

Από το πλαίσιο διαχείρισης τεχνολογίας πληροφοριών COBIT 5 εμφανίζονται δύο κωδικοί **DSS01.05** και **DSS05.02** που συμβάλουν στο έργο της ασφάλειας. Πιο αναλυτικά ο κωδικός **DSS01.05** αφορά ζητήματα της ασφάλειας δεδομένων και γενικώς συστημάτων πληροφορικής. Συμβάλει στην προστασία δεδομένων από κακόβουλες χρήσεις και είναι σημαντική η διατήρησή του για θέματα όπως η εμπιστοσύνη των χρηστών που χειρίζονται μια επιχείρηση ή ένα οικιακό δίκτυο.

Παράλληλα ο κωδικός **DSS05.02** ανάγεται στην ασφάλεια του δικτύου και τη διασύνδεση με το διαδίκτυο. Ανήκει στην προστασία του δικτύου από επιθέσεις κακόβουλου λογισμικού καθώς και σε άλλου τύπου απειλές. Είναι σημαντική η χρήση του για την διατήρηση της ασφάλειας και της ακεραιότητας των συστημάτων πληροφορικής.

Η αναφερόμενη ενότητα **4.3.3.4** της προδιαγραφής ασφάλειας **ISA 62443-2-1:2009** είναι αρμόδια για την αποθήκευση κωδικών πρόσβασης και συνθηματικών φράσεων σε αυτά τα συστήματα. Αυτή η υποενότητα ορίζει τις απαιτήσεις για τη διαχείριση των κωδικών πρόσβασης, συμπεριλαμβανομένων των προδιαγραφών για την αποθήκευση τους, των περιόδων αλλαγής, των απαιτήσεων για την πολυπλοκότητα και των προτεινόμενων μεθόδων κρυπτογράφησης για την προστασία τους από ανεξουσίαστη πρόσβαση και καταστροφή.

Η **ISA 62443-3-3:2013** αναφέρεται στην εν λόγω υποκατηγορία πλαισίου κυβερνοασφάλειας. Η συγκεκριμένη προδιαγραφή ασφάλειας είναι υπεύθυνη για τα συστήματα ελέγχου και την αυτοματισμού που χρησιμοποιούνται σε βιομηχανικές και κρίσιμες εφαρμογές. Στην **SR 3.1** αναφέρεται στην αναγκαιότητα της δημιουργίας ενός σχεδίου ασφάλειας που θα περιλαμβάνει μια ανάλυση των απειλών και των ευπαθειών του συστήματος, καθώς και τις αντίστοιχες πολιτικές, διαδικασίες και μέτρα που απαιτούνται για την προστασία του. Στην **SR 3.8**, η προδιαγραφή αναφέρεται στον έλεγχο των πρόσβασης και των δικαιωμάτων των χρηστών στο σύστημα. Πιο συγκεκριμένα, αυτή η υποενότητα απαιτεί την καθιέρωση ελέγχων αυθεντικοποίησης και εξουσιοδότησης, περιορισμού των προνομιακών δικαιωμάτων πρόσβασης, παρακολούθησης των δραστηριοτήτων των χρηστών και αντίδρασης σε παραβιάσεις ασφάλειας. Οι δύο αυτές αναφορές κρίνονται άκρως απαραίτητες και η χρήση τους αναγκαία.

Η ψηφιακή ασφάλεια αποτελεί ένα από τα πιο σημαντικά θέματα για κάθε οικιακό δίκτυο ή επιχείρηση όπου διαχειρίζεται προσωπικά δεδομένα και ευαίσθητες πληροφορίες. Το πρότυπο **ISO/IEC 27001:2013** αποτελεί ένα από τα πιο αναγνωρισμένα πλαίσια για τον έλεγχο και τη διαχείριση της ασφάλειας. Συγκεκριμένα απ'το πρότυπο ISO/IEC 27001:2013 αναφέρονται τα στοιχεία **A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3**. Το A.13.1.1, A.13.1.3 και A.13.2.1 αναφέρονται στην ανίχνευση, την αποτροπή και τη διαχείριση των κακόβουλων λογισμικών, των ιών και των κακόβουλων προγραμμάτων στα συστήματα πληροφορικής. Παράλληλα το A.14.1.2 και A.14.1.3 ανήκουν στη διαχείριση της πρόσβασης στα συστήματα πληροφορικής και την επαλήθευση της ταυτότητας των χρηστών που έχουν πρόσβαση σε αυτά τα συστήματα.

Ένα σύστημα με γνώμονα την ασφάλεια έχει πολλές απαιτήσεις οι οποίες μπορούν να καλυφθούν με την περιγραφή των **NIST SP 800-53 Rev. 4 AC-4, AC-10 και SC-7** που συμβάλουν

στη διασφάλιση της εχεμύθειας, της διαθεσιμότητας και της ακεραιότητας των πληροφοριών που επεξεργάζονται και αποθηκεύονται σε πληροφοριακά συστήματα και εξασφαλίζουν την προστασία από ανεπιθύμητη πρόσβαση, διαρροή και καταστροφή των δεδομένων. Πιο συγκεκριμένα η **AC-4** (Αναγνώριση/Πιστοποίηση Χρηστών) αναφέρεται στην αναγνώριση και πιστοποίηση της ταυτότητας των χρηστών πριν από την παροχή πρόσβασης στο πληροφοριακό σύστημα. Αυτό συνήθως επιτυγχάνεται μέσω της χρήσης μοναδικών συνδυασμών χρηστών/κωδικών πρόσβασης, πιστοποιητικών και άλλων ταυτοποιητικών μεθόδων. Η **AC-10** (Παρακολούθηση και Συγκέντρωση Πρόσβασης) δηλώνει τον έλεγχο και την καταγραφή της πρόσβασης στο πληροφοριακό σύστημα. Αυτό περιλαμβάνει την παρακολούθηση των προσπαθειών πρόσβασης, των περιεχομένων που προβάλλονται και των ενεργειών που πραγματοποιούνται στο πληροφοριακό σύστημα.
Η προστασία των πληροφοριών κατά τη μεταφορά είναι ένας σημαντικός παράγοντας για την ασφάλεια των πληροφοριακών συστημάτων. Το NIST SP 800-53 Rev. 4 περιλαμβάνει πολλά επιμέρους μέτρα ασφαλείας που σχετίζονται με την προστασία των πληροφοριών κατά τη μεταφορά τους. Μία από αυτές τις απαιτήσεις είναι η **SC-7** (Προστασία των Πληροφοριών σε Μεταφορά), η οποία περιγράφει τα μέτρα ασφαλείας που πρέπει να ληφθούν για να διασφαλιστεί η προστασία των πληροφοριών που μεταφέρονται μεταξύ πληροφοριακών συστημάτων ή συστημάτων επικοινωνιών. Η αποτελεσματική εφαρμογή των μέτρων αυτών συμβάλλει στην εξασφάλιση της ακεραιότητας, της εχεμύθειας και της διαθεσιμότητας των πληροφοριών κατά τη μεταφορά τους, προστατεύοντάς τες από τις απειλές των κακόβουλων επιθέσεων και εξασφαλίζοντας την αξιοπιστία και την αποτελεσματικότητα των πληροφοριακών συστημάτων.

Υποκατηγορία Πλαισίου Κυβερνοασφάλειας PR.AC-7

Μια υποκατηγορία της κατηγορίας PR.AC είναι η **PR.AC-7** η οποία είναι υπεύθυνη για την πιστοποίηση της ταυτότητας των χρηστών, συσκευών και άλλων πόρων που επιθυμούν να αποκτήσουν πρόσβαση σε ασφαλή συστήματα και δεδομένα, και αυτή η πιστοποίηση πρέπει να είναι ανάλογη με τον κίνδυνο της συναλλαγής και τον κίνδυνο απώλειας ασφάλειας ή παραβίασης της ιδιωτικότητας των δεδομένων. Αυτό σημαίνει ότι η πιστοποίηση της ταυτότητας των χρηστών και των συσκευών πρέπει να πραγματοποιείται με διάφορα επίπεδα επαλήθευσης (όπως μονοπαραμετρική ή πολυπαραμετρική επαλήθευση), ανάλογα με τον κίνδυνο της συναλλαγής. Για παράδειγμα, για ευαίσθητες πληροφορίες, όπως η πρόσβαση σε ευαίσθητα δεδομένα του συστήματος, ενδέχεται να απαιτείται πολυπαραμετρική επαλήθευση (όπως κωδικοί πρόσβασης και ταυτόχρονη χρήση δύο παραγόντων, όπως κωδικός πρόσβασης και αναγνώριση προσώπου ή δακτυλικών αποτυπωμάτων).

Για λιγότερο ευαίσθητες συναλλαγές, όπως η πρόσβαση σε ένα ηλεκτρονικό κατάστημα για αγορές μη ευαίσθητων προϊόντων, μπορεί να απαιτείται μονοπαραμετρική επαλήθευση, όπως ένας απλός κωδικός πρόσβασης. Η απαίτηση αυτή συνάδει με την αρχή της αναλογικότητας, δηλαδή την αρχή ότι οι μέθοδοι ασφαλείας πρέπει να είναι ανάλογες με τον κίνδυνο που αντιμετωπίζεται. Στην πράξη, αυτό σημαίνει ότι πρέπει να υπάρχει μια ανάλυση κινδύνου για κάθε συναλλαγή, ώστε να καθοριστεί το κατάλληλο επίπεδο επαλήθευσης της ταυτότητας που απαιτείται για τη διασφάλιση της ασφάλειας και της ιδιωτικότητας των χρηστών και των συσκευών.

Στην συγκεκριμένη υποκατηγορία χρησιμοποιούνται οι έλεγχοι **CIS CSC 1,12,15,16** όπου σαν σύνολο καλύπτουν ένα επαρκή εύρος ως στόχο την κυβερνοασφάλεια. Εκτός από το **CIS CSC 12** οι υπόλοιποι έλεγχοι συναντώνται στην υποκατηγορία κυβερνοασφάλειας **PR.AC-1**. Με την αναφορά αυτών των ελέγχων υπάρχει επιτήρηση των συστημάτων και εφαρμογών σε πραγματικό χρόνο, παρακολούθηση και ανίχνευση των δικαιωμάτων πρόσβασης καθώς και προστασία των δικτύων και συσκευών. Η έκδοση **CIS CSC 12** επικεντρώνεται σε θέματα όπως η προστασία της πληροφοριακής υποδομής από τις επιθέσεις με ransomware, η ενίσχυση των πολιτικών ασφαλείας των συστημάτων και η βελτίωση της διαχείρισης των προνομιακών δικαιωμάτων στα πληροφοριακά συστήματα. Η τήρηση των CIS CSC 12 είναι ζωτικής σημασίας για την επίτευξη ενός υψηλού επιπέδου ασφάλειας στα πληροφοριακά συστήματα προσφέροντας παρακολούθηση αναφορά και διόρθωση μέσω της διαχείρισης των συσκευών δικτύου.

Τα COBIT 5 **DSS05.04, DSS05.10** και **DSS06.10** είναι κωδικοί αναφοράς του πλαισίου διακυβέρνησης τεχνολογίας πληροφορικής (IT) COBIT 5, και αναφέρονται σε συγκεκριμένες επιχειρησιακές διαδικασίες της διαχείρισης της ασφάλειας των πληροφοριακών συστημάτων. Το **DSS05.04** που χαρακτηρίζεται από τη διαχείριση των κινδύνων της ασφάλειας της πληροφορίας και την ανάπτυξη πολιτικών και διαδικασιών για την αντιμετώπισή τους εφαρμόζεται επίσης και στο PC.AC-4. Η αναφορά του **DSS05.10** έχει ως σκοπό την καλύτερη διαχείριση των διακυμάνσεων και του κινδύνου του συστήματος πληροφορικής σε σχέση με την αποφυγή απωλειών και τη διασφάλιση του επιχειρηματικού περιβάλλοντος ή του οικιακού δικτύου. Το COBIT 5 δεν έχει άμεση συνεισφορά στο IoT μεταφορτώνοντας άμεσα δεδομένα στον κόσμο του IoT. Ωστόσο, μπορεί να χρησιμοποιηθεί για τη διαχείριση των πληροφοριακών συστημάτων που χρησιμοποιούνται στο περιβάλλον του IoT.

Το **DSS06.10** αναφέρεται στη διαχείριση των αδυναμιών ασφαλείας στα πληροφοριακά συστήματα. Πιο συγκεκριμένα, παρέχει οδηγίες για την αξιολόγηση και τη διαχείριση των αδυναμιών ασφαλείας που ανακαλύπτονται στο πλαίσιο της διαχείρισης κινδύνων ασφαλείας των πληροφοριακών συστημάτων.Μια αδυναμία ασφαλείας αποτελεί μια ευπάθεια στο πληροφοριακό σύστημα που μπορεί να εκμεταλλευτεί ένας επιτιθέμενος για να προκαλέσει ζημιά ή να κλέψει πληροφορίες. Η αξιολόγηση και η διαχείριση αυτών των αδυναμιών ασφαλείας είναι σημαντική για τη διασφάλιση της ασφάλειας και της προστασίας του πληροφοριακού συστήματος.

Η συμμόρφωση με το DSS06.10 μπορεί να βοηθήσει τις επιχειρήσεις να αναγνωρίζουν και να αξιολογούν τις αδυναμίες ασφαλείας τους, να προβλέπουν πιθανούς κινδύνους και να αναπτύσσουν σχέδια διαχείρισης κινδύνων για τη μείωση των κινδύνων ασφαλείας στο πληροφοριακό σύστημα.

Οι κωδικοί **ISA 62443-2-1:2009 4.3.3.6.1 έως 4.3.3.6.9** αναφέρονται σε απαιτήσεις ασφάλειας για τα συστήματα ελέγχου βιομηχανικής αυτοματισμού. Συγκεκριμένα, αναφέρονται

στη διαχείριση των αδειών πρόσβασης και των ταυτοτήτων των χρηστών, στην επαλήθευση ταυτοποίησης και εξουσιοδότησης χρηστών, στην προστασία της επικοινωνίας και των δεδομένων κατά τη μεταφορά, στην ανίχνευση και αντιμετώπιση απειλών ασφαλείας και στην παρακολούθηση των δραστηριοτήτων των χρηστών για τον εντοπισμό τυχόν παραβάσεων. Οι κωδικοί αυτοί αποτελούν μέρος του προτύπου ISA 62443, το οποίο αποσκοπεί στην ασφάλεια των συστημάτων ελέγχου βιομηχανικής αυτοματισμού.

Οι κωδικοί **SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9 και SR 1.10** που αναφέρονται στην εν λόγω υποκατηγορία ανήκουν στην υποκατηγορία "System and Communications Protection" του προτύπου ISA 62443-3-3:2013. Η υποκατηγορία αυτή αφορά την προστασία των συστημάτων και των επικοινωνιών από απειλές ασφαλείας. Συγκεκριμένα, ο SR 1.1 αναφέρεται στην προστασία των συστημάτων από ανεπιθύμητη πρόσβαση, ενώ ο SR 1.2 χρειάζεται στην αποτροπή μη εξουσιοδοτημένης πρόσβασης σε απομακρυσμένα συστήματα. Ο SR 1.5 αφορά την παρακολούθηση των επικοινωνιών στο δίκτυο, ενώ ο SR 1.7 απαιτεί την προστασία της εμπιστευτικότητας των δεδομένων κατά τη μεταφορά τους. Οι κωδικοί SR 1.8 και SR 1.9 αφορούν την προστασία των συστημάτων από κακόβουλο λογισμικό και ιούς, ενώ ο SR 1.10 απαιτεί τη διαχείριση των προνομιακών δικαιωμάτων στα συστήματα και των δικαιωμάτων πρόσβασης σε αυτά. Οι κωδικοί αυτοί είναι σημαντικοί για την ασφάλεια των συστημάτων και των δεδομένων τους και αποτελούν κρίσιμο κομμάτι της ασφάλειας.

Στην PR.AC-7 εμφανίζονται οι κωδικοί **A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 και A.18.1.4** που ανήκουν στο πρότυπο ISO/IEC 27001:2013, το οποίο αφορά τη διαχείριση της ασφάλειας των πληροφοριών. Οι κωδικοί A.9.2.1 και A.9.2.4 εφαρμόζονται για τη διαχείριση των προνομιακών δικαιωμάτων στα συστήματα πληροφορικής και των δικαιωμάτων πρόσβασης σε αυτά. Ο κωδικός A.9.3.1 απαιτεί την εφαρμογή πολυπλοκότητας κωδικών πρόσβασης, ενώ ο A.9.4.2 είναι υπεύθυνος για τη διαχείριση των πιστοποιητικών ασφαλείας και των κλειδιών πρόσβασης. Για την προστασία των κλειδιών κρυπτογράφησης χρησιμοποιείται ο κωδικός A.9.4.3 όσο για την διαχείριση της παρακολούθησης των συστημάτων πληροφορικής και εφαρμογών με σκοπό την ανίχνευση απειλών χρησιμοποιείται ο A.18.1.4.

Η αυθεντικοποίηση και η διαχείριση των ταυτοτήτων είναι υψίστης σημασίας διότι μπορεί να εξασφαλίσει ότι μόνο εξουσιοδοτημένα άτομα έχουν πρόσβαση σε ευαίσθητες πληροφορίες μέσω της χρήσης του **AC-7**. Για την περαιτέρω ασφάλεια γίνεται η αναφορά σε **AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11.** Μέσω του AC-8 είναι δυνατή η παρακολούθηση της χρήσης του συστήματος όπως για παράδειγμα οι ενέργειες των χρηστών ενώ η αναφορά σε AC-9 είναι υπεύθυνη για την πρόσβαση σε περιορισμένους πόρους απαιτώντας την εφαρμογή μέτρων πρόληψης πρόσβασης αποκλειστικά σε εξουσιοδοτημένα άτομα. Κρίσιμης απαίτησης είναι η συνεισφορά του AC-11 όπου προστατεύει το σύστημα έναντι κακόβουλου περιεχομένου κατά τη διαχείριση πληροφοριών ενώ παράλληλα το AC-12 είναι υπεύθυνο για την διαχείριση συστημάτων αποθήκευσης δεδομένων. Το AC-14 ανιχνεύει και προστατεύει το σύστημα από ανεπιθύμητη λειτουργία σε προγράμματα εφαρμογής.

Οι έλεγχοι ασφαλείας **IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10 και IA-11** είναι όλοι σημαντικοί έλεγχοι που αφορούν την πολιτική ασφαλείας των πληροφοριών και την προστασία των πληροφοριακών συστημάτων. Ο έλεγχος IA-1 αναφέρεται στην αυθεντικοποίηση της πρόσβασης χρήστη και τη διαχείριση των δικαιωμάτων πρόσβασης σε συστήματα πληροφοριών. Ο έλεγχος IA-2 αφορά τη διαχείριση των αποδείξεων ταυτότητας των χρηστών που ζητούν πρόσβαση σε πληροφορίες ή συστήματα. Ο έλεγχος IA-3 επικεντρώνεται στην προστασία των πληροφοριών που

διακινούνται, ενώ ο έλεγχος ΙΑ-4 αναφέρεται στη διαχείριση των πρόσβασης και της ασφάλειας σε συστήματα πληροφοριών. Οι έλεγχοι ΙΑ-5, ΙΑ-8 και ΙΑ-9 αφορούν την ασφάλεια των δεδομένων και την προστασία τους από απώλεια, καταστροφή, αλλοίωση ή μη εξουσιοδοτημένη πρόσβαση. Ο έλεγχος ΙΑ-10 διαχειρίζεται τα κλειδιών κρυπτογράφησης και την αποθήκευσή τους με ασφάλεια. Η διαχείριση των κλειδιών είναι ζωτικής σημασίας για την προστασία των πληροφοριών και τη διατήρηση της ακεραιότητας των δεδομένων. Ο έλεγχος ΙΑ-11 από την άλλη διαχειρίζεται τη προσβάση στους πόρους του συστήματος πληροφοριών. Αυτό περιλαμβάνει τη διαχείριση των δικαιωμάτων πρόσβασης σε αρχεία, φακέλους και άλλους πόρους του συστήματος, καθώς και την εφαρμογή των κατάλληλων πολιτικών ασφαλείας για τη διασφάλιση της ακεραιότητας και της εμπιστευτικότητας των δεδομένων.

Η υποκατηγορία κυβερνοασφαλείας **PR.AC-7** αναφέρεται στη διαχείριση πρόσβασης σε πληροφοριακά συστήματα και εφαρμόζεται για την προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση. Η εφαρμογή των κωδικών ασφαλείας που αναφέρονται στις παραπάνω προδιαγραφές **(ISA 62443-2-1:2009, ISA 62443-3-3:2013, ISO/IEC 27001:2013, NIST SP 800-53 Rev. 4)** είναι απαραίτητη για τη διασφάλιση της πρόσβασης μόνο από εξουσιοδοτημένα άτομα και την αποτροπή επιθέσεων που στοχεύουν στην παραβίαση της ασφάλειας του συστήματος. Επίσης, η εφαρμογή αυτών των κωδικών ασφαλείας βοηθάει στη διασφάλιση της συμμόρφωσης με τους κανονισμούς και τις προδιαγραφές των αρχών που είναι υπεύθυνες για την κυβερνοασφάλεια, όπως η NIST και η ISO.

<u>Παράδειγμα Υλοποίησης 4</u>
<u>Ασφάλεια Δεδομένων (PR.DS)</u>

Η ασφάλεια δεδομένων είναι ένας σημαντικός τομέας στην προστασία των πληροφοριών από απειλές όπως η κλοπή, η απώλεια ή η καταστροφή. Στη σύγχρονη ψηφιακή εποχή, η ασφάλεια των δεδομένων είναι ιδιαίτερα σημαντική καθώς όλο και περισσότερες πληροφορίες αποθηκεύονται και επεξεργάζονται σε ψηφιακή μορφή. Οι απειλές ασφαλείας δεδομένων περιλαμβάνουν την κλοπή προσωπικών δεδομένων, τη διασπορά κακόβουλου λογισμικού (malware), την κατάχρηση προνομίων από μέλη του προσωπικού και τη φυσική καταστροφή των δεδομένων λόγω πυρκαγιάς ή πλημμύρας, μεταξύ άλλων. Για την αποτελεσματική προστασία των δεδομένων, οι οργανισμοί πρέπει να θεσπίζουν πολιτικές ασφαλείας και να λαμβάνουν μέτρα πρόληψης και προστασίας. Αυτά μπορούν να περιλαμβάνουν την κρυπτογράφηση δεδομένων, την επιβολή περιορισμών πρόσβασης, τη δημιουργία αντιγράφων ασφαλείας, την ενημέρωση και την εκπαίδευση των χρηστών του συστήματος.

Η ασφάλεια δεδομένων σύμφωνα με το **PR.DS** περιγράφει την ανάγκη διαχείρισης των πληροφοριών και των αρχείων σε έναν οργανισμό σύμφωνα με τη στρατηγική κινδύνου του οργανισμού ή του οικιακού δικτύου, προκειμένου να προστατευθεί η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των πληροφοριών. Αυτό σημαίνει ότι ο οργανισμός πρέπει να έχει έναν σχεδιασμό κινδύνου που θα τον βοηθήσει να αναγνωρίσει τους κινδύνους ασφαλείας που αντιμετωπίζει και να αναπτύξει μια στρατηγική ασφαλείας που θα προστατεύει τις πληροφορίες και τα αρχεία του. Στο πλαίσιο της ασφάλειας δεδομένων, οι τρεις βασικές αρχές είναι η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των πληροφοριών. Η εμπιστευτικότητα

αφορά τη διατήρηση της απόρρητης φύσης των πληροφοριών, η ακεραιότητα αφορά τη διατήρηση της ακεραιότητας των δεδομένων και η διαθεσιμότητα αφορά τη διατήρηση της διαθεσιμότητας των πληροφοριών για τους χρήστες.

<u>Υποκατηγορία Πλαισίου Κυβερνοασφάλειας PR.DS-5</u>

Η προστασία κατά των διαρροών δεδομένων είναι ένας σημαντικός τομέας της ασφάλειας δεδομένων. Οι διαρροές δεδομένων μπορούν να οφείλονται σε διάφορους παράγοντες, όπως ανθρώπινο λάθος, κακόβουλη ενέργεια, εσωτερική απειλή. Η διαρροή δεδομένων μπορεί να έχει σοβαρές συνέπειες για την επιχείρηση, όπως απώλεια εμπιστευτικότητας, οικονομικές απώλειες ή ζημιές στη φήμη. Για την αντιμετώπιση αυτής της απειλής, οι οργανισμοί πρέπει να λαμβάνουν μέτρα προστασίας κατά των διαρροών δεδομένων. Αυτά μπορούν να περιλαμβάνουν την κρυπτογράφηση των δεδομένων, την επιβολή περιορισμών πρόσβασης, τη δημιουργία κανόνων ασφαλείας, τη διαχείριση ταυτοποίησης και πρόσβασης, την εκπαίδευση του προσωπικού και την ανάπτυξη σχεδίων αντιμετώπισης κρίσεων σε περίπτωση που σημειωθεί μια διαρροή δεδομένων.

Στο σύντομο μέλλον τα οικιακά δίκτυα και οι επιχειρήσεις που θα είναι εξοπλισμένες με συσκευές IoT θα είναι απαραίτητο να χρησιμοποιούν όλο και περισσότερα εργαλεία ασφάλειας με σκοπό την θωράκιση των δικτύων ακόμα και στις πιο πολύπλοκες μορφές επιθέσεων. Το Κέντρο Ασφάλειας Διαδικτύου (Center for Internet Security – CIS) παρέχει το **CIS 13** για την παρακολούθηση και την άμυνα του δικτύου. Είναι απαραίτητη η γνώση των συνδεδεμένων συσκευών στο δίκτυο καθώς και η παρακολούθηση τους ώστε να μην υπάρχει μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα. Ο ρόλος του **CIS 13** είναι ο εντοπισμός ύποπτων σχηματισμών και η έγκαιρη ανίχνευση προτού την οποιαδήποτε παραβίαση. Το CIS 13 για την βέλτιστη ασφάλεια συνιστά για τα οικιακά δίκτυα ή τις μικρές επιχειρήσεις διασφαλίσεις όπως η συγκέντρωση ειδοποιήσεων για συμβάντα ασφάλειας, η ανάπτυξη λύσης για την ανίχνευση εισβολής στο δίκτυο και η συλλογή αρχείων καταγραφής της ροής κυκλοφορίας του δικτύου.

Στην υποκατηγορία κυβερνοασφάλειας PR.DS-5 αναφέρονται τα **COBIT 5 APO01.06, DSS05.04, DSS05.07** και **DSS06.02** τα δραστηριοποιούνται σε συγκεκριμένες διαδικασίες και πρακτικές που σχετίζονται με τη διαχείριση και την ασφάλεια της πληροφορίας σε μια επιχείρηση ή σε ένα οικιακό δίκτυο. Πιο συγκεκριμένα, με το **APO01.06** γίνεται λόγος για τον καθορισμό των επιχειρησιακών στόχων και στρατηγικών στηριζόμενων στην τεχνολογία της πληροφορίας. Το **DSS05.04** περιγράφει τη διαχείριση των κινδύνων ασφαλείας της πληροφορίας, ενώ το **DSS05.07** εφαρμόζεται στη διαχείριση των κινδύνων από ανεπαρκείς επιλογές και παραμέτρους ασφάλειας.

Εν κατακλείδι το **DSS06.02** αφορά την αξιολόγηση και την παρακολούθηση των καταγεγραμμένων αποτελεσμάτων ασφαλείας. Αυτές οι διαδικασίες συνδέονται με τα χαρακτηριστικά ασφάλειας του πλαισίου εργασίας NIST Cybersecurity Framework, τα οποία είναι: Αντίληψη, Προστασία, Ανάκαμψη, Ανίχνευση και Αντίδραση.

Ως στόχο την ασφάλεια των συστημάτων ελέγχου και αυτοματισμού αναφέρεται η προδιαγραφή **ISA 62443-3-3:2013 SR 5.2**. Η συγκεκριμένη προδιαγραφή αναλύει τις απαιτήσεις ασφάλειας για το σχεδιασμό και την ανάπτυξη των συστημάτων ελέγχου και αυτοματισμού. Στο SR 5.2, περιγράφονται οι απαιτήσεις για τη διαχείριση των αντικειμενικών κινδύνων, δηλαδή των κινδύνων που προκύπτουν από έτη χρήση των συστημάτων ελέγχου και αυτοματισμού. Αυτό συμπεριλαμβάνει την αναγνώριση και την ανάλυση των κινδύνων, την εκτίμηση των επιπτώσεων και της πιθανότητας εμφάνισής τους, καθώς και τον καθορισμό των αναγκαίων μέτρων ασφαλείας για την αντιμετώπισή τους. Η προδιαγραφή ISA 62443-3-3:2013 SR 5.2 είναι σημαντική για τη βιομηχανία και την κριτική υποδομή, καθώς βοηθά στη διασφάλιση της ασφάλειας των συστημάτων ελέγχου και αυτοματισμού και στην πρόληψη ανεπιθύμητων συμβάντων που μπορεί να έχουν σημαντικές επιπτώσεις στην παραγωγική διαδικασία ή στην ανθρώπινη ζωή και

ασφάλεια.

Οι οργανισμοί πρέπει να εφαρμόζουν μια συνεκτική και καθολική διαδικασία εξουσιοδότησης που θα περιλαμβάνει την αξιολόγηση των απαιτήσεων πρόσβασης για κάθε οντότητα ή ρόλο στο σύστημα πληροφορικής και την ανάθεση των απαραίτητων εξουσιοδοτήσεων σε αυτούς που έχουν ανάγκη πρόσβασης σε πληροφορίες και πόρους. Η διαδικασία αυτή πρέπει να περιλαμβάνει την επαλήθευση των ταυτοτήτων και των δικαιωμάτων των χρηστών που αιτούνται πρόσβαση, καθώς και την αξιολόγηση της αποτελεσματικότητας των μέτρων ασφαλείας που υπάρχουν. Για την επιτυχία της διεργασίας χρησιμοποιείται η προδιαγραφή **ISO/IEC 27001:2013 A.6.1.2** η οποία ζητά από τους οργανισμούς να διασφαλίζουν ότι οι εξουσιοδοτήσεις για την πρόσβαση σε πληροφορίες και πόρους του συστήματος πληροφορικής είναι κατάλληλες για τους σκοπούς τους.

Δύο χρησιμοποιούμενες προδιαγραφές είναι η **ISO/IEC 27001:2013 A.7.1.1** (Πολιτική ασφαλείας της πληροφορίας) και η **ISO/IEC 27001:2013 A.7.1.2** (Αξιολόγηση των κινδύνων ασφαλείας της πληροφορίας).

Η προδιαγραφή **ISO/IEC 27001:2013 A.7.1.1** αναφέρεται στην ανάγκη για μια συγκεκριμένη και κατανοητή πολιτική ασφαλείας της πληροφορίας σε έναν οργανισμό. Αυτή η

πολιτική πρέπει να καλύπτει τις διάφορες πτυχές της ασφάλειας των πληροφοριών, όπως οι απαιτήσεις για τον καθορισμό των κανόνων πρόσβασης σε ευαίσθητες πληροφορίες, οι περιορισμοί στην χρήση φορητών συσκευών και οι κατευθυντήριες αρχές για τη διαχείριση των κινδύνων πληροφορικής ασφάλειας.

Η προδιαγραφή **ISO/IEC 27001:2013 A.7.1.2** αφορά τη διαδικασία αξιολόγησης των κινδύνων ασφαλείας της πληροφορίας σε έναν οργανισμό. Εμπεριέχει την αναγνώριση των απειλών και των ευπαθειών του συστήματος πληροφορικής και την ανάπτυξη μέτρων για τη μείωση του κινδύνου.

Για τον ορισμό, την υλοποίηση, την επανεξέταση και τη βελτίωση των διαδικασιών που αφορούν στη διαχείριση των κινδύνων ασφαλείας της πληροφορίας είναι αναγκαία η εφαρμογή της προδιαγραφής **ISO/IEC 27001:2013 A.7.3.1** με σκοπό την αναγνώριση των κινδύνων, την αξιολόγησή τους και τη λήψη μέτρων για τη μείωση του κινδύνου. Η προδιαγραφή αυτή απαιτεί από τον οργανισμό να αναπτύξει και να εφαρμόσει μια διαδικασία διαχείρισης των κινδύνων ασφαλείας της πληροφορίας, που θα επιτρέπει την αναγνώριση και την αντιμετώπιση των αδυναμιών στα συστήματα ασφαλείας της πληροφορίας του οργανισμού. Η διαδικασία αυτή πρέπει να είναι συνεχής και να πραγματοποιείται τακτικά, προκειμένου να εξασφαλίζεται ότι οι κίνδυνοι ασφαλείας της πληροφορίας είναι αποτελεσματικά διαχειρισμένοι και μειωμένοι στο ελάχιστο δυνατό επίπεδο.

Οι προδιαγραφές **ISO/IEC 27001:2013 A.8.2.2** και **A.8.2.3** που αναφέρονται στην υποκατηγορία κυβερνοασφάλειας είναι υπεύθυνες για τη διαχείριση των προνομιακών δικαιωμάτων στα συστήματα πληροφορικής και προσδιορίζουν τις απαιτήσεις για την ασφαλή λειτουργία και διαχείριση αυτών των δικαιωμάτων.

Η προδιαγραφή **A.8.2.2** απαιτεί την επαλήθευση της ταυτότητας του χρήστη που ζητά πρόσβαση σε προνομιακά δικαιώματα. Αυτό συμβάλλει στην πρόληψη της παράνομης πρόσβασης σε ευαίσθητες πληροφορίες από μη εξουσιοδοτημένα πρόσωπα. Επιπλέον, η προδιαγραφή αυτή απαιτεί την επαλήθευση ότι οι χρήστες με προνομιακά δικαιώματα έχουν ανάγκη για αυτά τα δικαιώματα για να εκτελέσουν τις εργασίες τους και ότι τα προνομιακά δικαιώματα έχουν αποδοθεί σε συμμόρφωση με τις αρχές του λιγότερου δικαιώματος (principle of least privilege). Από την άλλη πλευρά η προδιαγραφή **A.8.2.3** απαιτεί τη διαχείριση της χρήσης των προνομιακών δικαιωμάτων και την καταγραφή των ενεργειών που πραγματοποιούνται από χρήστες με προνομιακά δικαιώματα.

Οι αναφορές στο **ISO/IEC 27001:2013 A.9** από τον κατάλογο των ελέγχων ασφάλειας πληροφοριών πρέπει να υλοποιηθούν στην υποκατηγορία που αναλύεται σύμφωνα με το πρότυπο. Οι έλεγχοι αυτοί σχετίζονται με την ασφάλεια των πληροφοριών και απαιτούνται για τη συμμόρφωση με το πρότυπο. Συγκεκριμένα η αναφορά στον A.9.1.1 **αφορά** στην αξιολόγηση των απειλών ασφαλείας για τα συστήματα πληροφοριών. Αυτό περιλαμβάνει την αναγνώριση των απειλών και την ανάλυση των επιπτώσεών τους στην ασφάλεια των πληροφοριών. Για την αξιολόγηση των απειλών από εσωτερικούς παράγοντες, όπως οι εργαζόμενοι εφαρμόζεται ο **A.9.1.2** όπου περιλαμβάνει την αναγνώριση των πιθανών απειλών από τους εσωτερικούς παράγοντες και την ανάλυση των επιπτώσεών τους στην ασφάλεια των πληροφοριών. Την διαχείριση των κλειδιών κρυπτογράφησης αναλαμβάνει ο **A.9.2.3** όπου περιλαμβάνει την αναγνώριση των κλειδιών και την εφαρμογή πολιτικών που αφορούν στην προστασία των κλειδιών κρυπτογράφησης και στη διαχείριση τους, που πρέπει να είναι αποτελεσματική και ασφαλής.

Πρέπει να υπάρχει μια πολιτική για τη διαχείριση των κλειδιών κρυπτογράφησης και ένας μηχανισμός για τη διασφάλιση της ακεραιότητας και της εμπιστευτικότητας των κλειδιών.

Στην υποκατηγορία πλαισίου κυβερνοασφάλειας PR.DS-5 γίνεται αναφορά στο **ISO/IEC 27001:2013 A.9.4.1, A.9.4.4** και **A.9.4.5** όπου ευθύνονται για την ασφάλεια, την αντιμετώπιση καθώς και την προστασία από κακόβουλο λογισμικό. Πιο αναλυτικά η αναφορά σε **A.9.4.1** γίνεται ώστε να υπάρχει απαίτηση της λήψης κατάλληλων μέτρων για την προστασία της ασφάλειας των συνεδριάσεων των χρηστών στο σύστημα πληροφορικής. Αυτό περιλαμβάνει τη χρήση κρυπτογράφησης, τη διαχείριση των προσβάσεων, την επαλήθευση της ταυτότητας των χρηστών και την περιορισμένη πρόσβαση σε ευαίσθητες πληροφορίες. Με την κατηγορία **A.9.4.4** απαιτείται η ανάληψη μέτρων για την πρόληψη και αντιμετώπιση των απειλών από κακόβουλο λογισμικό. Αυτό επιτυγχάνεται με την εγκατάσταση ενημερώσεων λογισμικού, τη χρήση κρυπτογράφησης, την εφαρμογή πολιτικών ασφαλείας για τους χρήστες και την περιορισμένη πρόσβαση σε ευαίσθητες πληροφορίες. Τέλος το **A.9.4.5** αντιμετωπίζει τις απειλές από κακόβουλο λογισμικό μέσω της εφαρμογής μέτρων όπως η χρήση αντιικών λογισμικών (antivirus) και των ενημερώσεων λογισμικού, η διαχείριση των προνομίων των χρηστών, η εφαρμογή πολιτικών ασφαλείας για την αντιμετώπιση των απειλών και η παρακολούθηση των δραστηριοτήτων στο δίκτυο για την ανίχνευση επιθέσεων και κακόβουλου λογισμικού. Επιπλέον, αυτή η κατηγορία περιλαμβάνει την πρόληψη και την αντιμετώπιση των κινδύνων που προκύπτουν από τη χρήση φορητών συσκευών και τη δικτύωση τους με το κεντρικό δίκτυο της επιχείρησης.

Η **A.10.1.1** είναι μια κατηγορία του προτύπου ISO/IEC 27001:2013 που αναφέρεται στην πολιτική ασφαλείας των πληροφοριών καθώς και στην εν λόγω υποκατηγορία. Αναφέρεται στην ανάγκη για μια τυποποιημένη πολιτική ασφαλείας που θα ορίζει τις γενικές αρχές και τους στόχους για την ασφάλεια των πληροφοριών στην επιχείρηση. Καλύπτει αρκετά θέματα της ασφάλειας πληροφοριών μερικά εκ των οποίων είναι η διαχείριση των κινδύνων ασφαλείας των πληροφοριών, η πρόληψη και η αντιμετώπιση των απειλών ασφαλείας των πληροφοριών, η διαχείριση των προνομίων πρόσβασης στις πληροφορίες, η διαχείριση των περιβαλλοντικών απειλών στις εγκαταστάσεις της επιχείρησης και η συμμόρφωση με τους νομικούς και κανονιστικούς απαιτήσεις σχετικά με την ασφάλεια των πληροφοριών.

Στο πλαίσιο του προτύπου ISO/IEC 27001:2013 εμπεριέχονται και οι κατηγορίες **A.11.1.4, A.11.1.5** και **A.11.2.1** που περιγράφουν τις απαιτήσεις της ασφάλειας των πληροφοριών. Πιο αναλυτικά η κατηγορία **A.11.4** αξιολογεί τους κινδύνους στα συστήματα πληροφορικής , η **A.11.1.5** διαχειρίζεται τους κινδύνους ενώ η **A.11.2.1** είναι υπεύθυνη για την επείγουσα κατάσταση δηλαδή απαιτεί από τους οργανισμούς να αναπτύσσουν και να υλοποιούν ένα σχέδιο αντιμετώπισης επειγουσών καταστάσεων στα συστήματα πληροφορικής τους, προκειμένου να αντιμετωπίζουν απρόβλεπτα γεγονότα ή απειλές που θα μπορούσαν να επηρεάσουν την ασφάλεια των συστημάτων.

Οι παράγραφοι **A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3** και **A.13.2.4** του προτύπου ISO/IEC 27001:2013 αφορούν την προστασία των πληροφοριών από απώλεια, καταστροφή, οικειοθελή ή μη εξουσιοδοτημένη αλλαγή ή αποκάλυψη. Είναι απαραίτητη η χρήση τους για την περαιτέρω ασφάλεια. Αυτά τα μέτρα ασφαλείας περιλαμβάνουν την τακτική δημιουργία αντιγράφων ασφαλείας των πληροφοριών, την εφαρμογή πολύπλοκων κωδικών πρόσβασης, την περιορισμένη πρόσβαση στα δεδομένα από μη εξουσιοδοτημένα άτομα και την τακτική αναθεώρηση των μέτρων ασφαλείας για να εξασφαλίζεται ότι είναι επαρκή. Επιπλέον, αυτές οι παράγραφοι αναφέρονται στην προστασία από κακόβουλο λογισμικό και στην πρόληψη της φθοράς των φυσικών μέσων αποθήκευσης

Με σκοπό τον έλεγχο της πρόσβασης στα συστήματα πληροφορικής και στις εφαρμογές γίνονται επίσης αναφορές στις κατηγορίες **A.14.1.2** και **A.14.1.3** του πρότυπου ISO/IEC 27001:2013. Η παράγραφος **A.14.1.2** αφορά τον έλεγχο της πρόσβασης στο λειτουργικό σύστημα, ενώ η παράγραφος **A.14.1.3** αφορά τον έλεγχο της πρόσβασης σε εφαρμογές. Με την αναφορά **A.14.1.2** προτείνεται να υπάρχουν μέτρα ασφαλείας για τον έλεγχο της πρόσβασης στα λειτουργικά συστήματα, ώστε να εξασφαλίζεται ότι μόνο εξουσιοδοτημένα άτομα έχουν πρόσβαση σε αυτά. Τα μέτρα ασφαλείας μπορεί να περιλαμβάνουν τη χρήση πολύπλοκων κωδικών πρόσβασης, τον περιορισμό της πρόσβασης σε εξουσιοδοτημένα άτομα, τη χρήση του δικτύου Virtual Private Network (VPN) για ασφαλή πρόσβαση από απομακρυσμένες τοποθεσίες και άλλα παρόμοια μέτρα. Παράλληλα μέσω της παραγράφου **A.14.1.3** θα υπάρχουν μέτρα ασφαλείας για τον έλεγχο της πρόσβασης στις εφαρμογές, ώστε να εξασφαλίζεται ότι μόνο εξουσιοδοτημένα άτομα έχουν πρόσβαση σε αυτές. Τα μέτρα ασφαλείας μπορεί να περιλαμβάνουν την αυθεντικοποίηση των χρηστών πριν την είσοδο στην εφαρμογή, την παρακολούθηση της δραστηριότητας των χρηστών, τον περιορισμό των εξουσιών πρόσβασης στο ελάχιστο απαραίτητο επίπεδο και τη χρήση κρυπτογραφημένων συνδέσεων. Επιπλέον, μπορεί να απαιτείται η επαλήθευση της ταυτότητας των χρηστών μέσω διαφόρων μεθόδων όπως οι κωδικοί πρόσβασης ή οι βιομετρικοί αισθητήρες. Όλα αυτά τα μέτρα έχουν στόχο να διασφαλίσουν ότι η πρόσβαση στις εφαρμογές είναι περιορισμένη σε εξουσιοδοτημένα άτομα και να προστατεύουν τις ευαίσθητες πληροφορίες που περιέχονται σε αυτές.

Το **NIST SP 800-53 Rev. 4 AC-4** είναι μια από τις προδιαγραφές ασφαλείας που προτείνονται από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ (NIST) για τον δημόσιο τομέα. Αυτή η προδιαγραφή αφορά στον έλεγχο των αναγκών πρόσβασης σε πόρους των πληροφοριακών συστημάτων και τον περιορισμό της πρόσβασης σε εξουσιοδοτημένους χρήστες και ρόλους. Η αναφορά του γίνεται διότι απαιτεί την εφαρμογή μέτρων για τον έλεγχο της πρόσβασης σε πόρους, συμπεριλαμβανομένης της αυθεντικοποίησης των χρηστών, της εξουσιοδότησης τους για πρόσβαση σε συγκεκριμένους πόρους καθιστώντας πιο ακέραιο το σύστημα που διέπει το οικιακό δίκτυο ή το δίκτυο της μικρής επιχείρησης δίνοντας περαιτέρω ασφάλεια δεδομένων.

Κάθε χρήστης στο σύστημα έχει διαφορετικές λειτουργικές ανάγκες και αναγκαίο είναι η ύπαρξη ενός ελέγχου πρόσβασης στους πόρους του συστήματος. Αυτό τον έλεγχο καλείται να καλύψει η πρακτική ασφάλειας **AC-5** του **NIST SP 800-53 Rev. 4**. Συγκεκριμένα, προτείνεται οι πόροι του συστήματος να διαχωρίζονται σε λογικά σύνολα και να εφαρμόζονται ανάλογα μέτρα ασφαλείας για την πρόσβαση σε κάθε σύνολο, λαμβάνοντας υπόψη τις ανάγκες των διαφορετικών χρηστών. Επιπλέον, προτείνεται να γίνεται συνεχής παρακολούθηση της πρόσβασης στους πόρους του συστήματος, έτσι ώστε να διασφαλίζεται ότι οι χρήστες έχουν πρόσβαση μόνο στα απαραίτητα στοιχεία για την εκτέλεση των καθηκόντων τους και όχι σε πληροφορίες που δεν είναι αναγκαίες για τη δουλειά τους.

Για τον περιορισμό των δικαιωμάτων πρόσβασης σε λογαριασμούς χρηστών εφαρμόζεται ο κανόνας **AC-6**. Ο κανόνας αυτός ορίζει ότι οι διαχειριστές θα πρέπει να περιορίζουν τα δικαιώματα πρόσβασης σε λογαριασμούς χρηστών στο ελάχιστο απαραίτητο για να εκτελέσουν τα καθήκοντά τους, καθώς αυτό μειώνει τον κίνδυνο ανεπιθύμητης χρήσης ή κακόβουλης δραστηριότητας από μη εξουσιοδοτημένα άτομα.

Με την χρήση του **PE-19** επαληθεύεται η απαίτηση αρχειοθέτησης δεδομένων σε αποθετήριο μόνιμης αποθήκευσης. Ο κανόνας αυτός προσδιορίζει τα απαραίτητα βήματα για τη διασφάλιση ότι τα αποθηκευμένα δεδομένα είναι ακέραια και προστατευμένα από απώλεια ή καταστροφή. Αυτό περιλαμβάνει την επαλήθευση των αρχείων και των δεδομένων για την αποτελεσματική λειτουργία τους και την εφαρμογή μέτρων ασφαλείας όπως η κρυπτογράφηση και ο έλεγχος πρόσβασης. Η επαλήθευση αυτή είναι σημαντική για τη διατήρηση της ακεραιότητας των δεδομένων και την αποφυγή διαρροών πληροφοριών.

Όταν το σύστημα εμπεριέχει μεθόδους κρυπτογράφησης είναι αναγκαία η ασφαλέστερη διαχείριση των κλειδιών που χρησιμοποιούνται στην κρυπτογραφία. Με το **PS-3** διαχειρίζονται, ανακτώνται και αποθηκεύονται τα κλειδιά καθιερώνοντας μια πολιτική διαχείριση. Τα κλειδιά διαχειρίζονται σε όλη την διάρκεια του κύκλου ζωής τους, από τη δημιουργία έως την καταστροφή τους.

Το **NIST SP 800-53 Rev. 4 PS-6** είναι ένας κανόνας ασφαλείας που αναφέρεται στη διαχείριση των πιστοποιητικών και των αρμοδιοτήτων ελέγχου σε ένα πλαίσιο ασφάλειας των πληροφοριών. Ο κανόνας αυτός απαιτεί τη δημιουργία μιας πολιτικής διαχείρισης πιστοποιητικών και αρμοδιοτήτων ελέγχου που να περιλαμβάνει τα πρότυπα για την έκδοση, την απόσυρση και τη διαχείριση πιστοποιητικών, καθώς και την ανάθεση, την ανάκληση και τη διαχείριση των αρμοδιοτήτων ελέγχου. Η εφαρμογή του είναι άκρως απαραίτητη διότι διασφαλίζει την εμπιστοσύνη στα πιστοποιητικά και στις αρμοδιότητες ελέγχου, εξασφαλίζοντας την πρόληψη μη εξουσιοδοτημένης πρόσβασης ή της χρήσης τους από μη εξουσιοδοτημένους χρήστες.

Τα **SC-7, SC-8, SC-13** και **SC-31** είναι κανόνες ασφαλείας που περιλαμβάνονται στο NIST SP 800-53 Rev. 4 και αφορούν τον έλεγχο πρόσβασης στα συστήματα πληροφοριών. Η αναφορά τους στην υποκατηγορία πλαισίου κυβερνοασφάλειας PR.DS-5 είναι άκρως αναγκαία για την διαχείριση και τον έλεγχο ορισμένων πεδίων. Πιο αναλυτικά ο κανόνας **SC-7** αναφέρεται στη

διαχείριση των ιδιωτικών κλειδιών και των πιστοποιητικών που χρησιμοποιούνται για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων. Απαιτείται η ασφαλής διαχείριση των κλειδιών και των πιστοποιητικών για να διασφαλιστεί η προστασία των δεδομένων κατά τη μετάδοση και την αποθήκευσή τους. Επιπρόσθετα ο κανόνας **SC-8** εφαρμόζει τον έλεγχο των δικαιωμάτων πρόσβασης των χρηστών στα συστήματα πληροφοριών. Αυτό εξηγείται με τη δημιουργία και τη διαχείριση των λογαριασμών χρηστών, την ανάθεση δικαιωμάτων πρόσβασης σε συγκεκριμένους χρήστες και τη διαχείριση των δικαιωμάτων πρόσβασης κατά την εκτέλεση εργασιών σε ένα σύστημα πληροφοριών. Ο κανόνας **SC-13** ελέγχει τις απομακρυσμένες συνεδρίες χρηστών.

Περιλαμβάνει τη διασφάλιση ότι οι χρήστες που συνδέονται στο σύστημα από απομακρυσμένες τοποθεσίες έχουν ελεγχόμενη πρόσβαση στο σύστημα και ότι η πρόσβασή τους είναι ασφαλής.Αυτό συμβαίνει με τη χρήση ασφαλών πρωτοκόλλων για την απομακρυσμένη σύνδεση, όπως το SSH (Secure Shell) και το SSL/TLS (Secure Sockets Layer/Transport Layer Security), καθώς και τη χρήση ελέγχων πρόσβασης, όπως η διαχείριση δικαιωμάτων πρόσβασης και ο έλεγχος ταυτότητας των χρηστών μέσω του δικτύου.

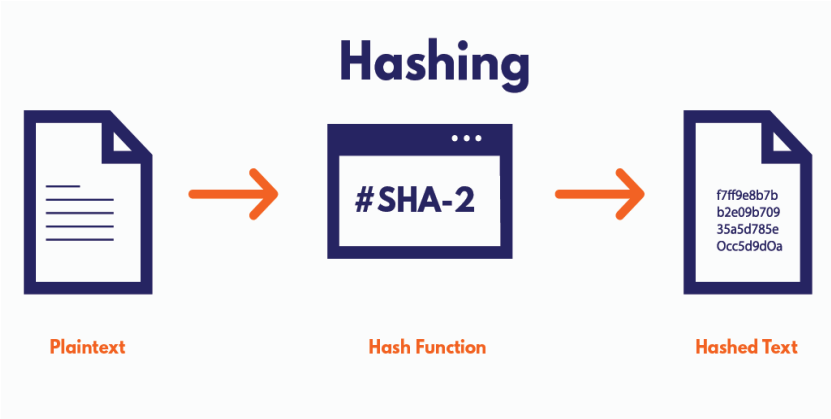
Τέλος, σύμφωνα με τον **SC-31** θα πρέπει να περιλαμβάνεται μια διαδικασία για την ανάλυση των κινδύνων ασφαλείας και την ανάπτυξη σχεδίων αντιμετώπισής τους. Οι οργανισμοί πρέπει να αναλύουν τους κινδύνους που σχετίζονται με τα συστήματά τους, λαμβάνοντας υπόψη τις απειλές που αντιμετωπίζουν, τις ευπαθείς περιοχές και τα είδη των δεδομένων που αποθηκεύουν και επεξεργάζονται. Αυτό πρέπει να γίνεται τακτικά και κατά την ανάπτυξη νέων συστημάτων. Στη συνέχεια, οι οργανισμοί πρέπει να αναπτύξουν σχέδια αντιμετώπισης των κινδύνων αυτών, τα οποία θα περιλαμβάνουν τις δράσεις που πρέπει να αναληφθούν για τη μείωση των κινδύνων, τους υπευθύνους για την εφαρμογή τους και τα χρονοδιαγράμματα για την υλοποίησή τους.

Ως στόχο τον έλεγχο της πρόσβασης στα ευαίσθητα πληροφοριακά συστήματα και στα δεδομένα που αποθηκεύονται εφαρμόζεται ο κανόνας ασφαλείας **SI-4** ο οποίος διασφαλίζει ότι οι χρήστες που έχουν πρόσβαση στα συστήματα και τα δεδομένα αυτά είναι εξουσιοδοτημένοι και έχουν ανάγκη από αυτά για την εκτέλεση των εργασιών τους. Για την εφαρμογή του κανόνα SI-4, οι οργανισμοί πρέπει να ελέγχουν τη ταυτότητα του χρήστη που προσπαθεί να αποκτήσει πρόσβαση στα συστήματα και τα δεδομένα, να ελέγχουν αν ο χρήστης έχει την εξουσιοδότηση για να αποκτήσει πρόσβαση στα ευαίσθητα συστήματα και δεδομένα και να υπάρχει υποχρεωτική πρόσβαση για τους χρήστες στα ευαίσθητα συστήματα και δεδομένα με περιορισμό της πρόσβασης στα δεδομένα που απαιτούνται για την εργασία τους.

<u>Υποκατηγορία Πλαισίου Κυβερνοασφάλειας PR.DS-6</u>

Η διατήρηση της ακεραιότητας του λογισμικού, του firmware και των πληροφοριών αποτελεί ένα σημαντικό ζήτημα για την ασφάλεια των συστημάτων πληροφορικής. Οι μηχανισμοί επαλήθευσης ακεραιότητας (integrity-checking mechanisms) χρησιμοποιούνται για την εξασφάλιση ότι το λογισμικό, το firmware ή οι πληροφορίες παραμένουν ασφαλή και δεν έχουν υποστεί καμία αλλαγή ή διαφοροποίηση από την αρχική τους κατάσταση.

Οι μηχανισμοί επαλήθευσης ακεραιότητας μπορούν να λειτουργήσουν με διάφορους τρόπους. Για παράδειγμα, μπορεί να χρησιμοποιηθεί μια συνάρτηση κατακερματισμού (hash function) για τον υπολογισμό ενός μοναδικού αναπαραστατικού κώδικα (hash) για το λογισμικό ή τις πληροφορίες. Αυτός ο κώδικας μπορεί στη συνέχεια να χρησιμοποιηθεί για να επιβεβαιωθεί αν οι πληροφορίες ή το λογισμικό έχουν αλλάξει ή όχι. Άλλοι μηχανισμοί μπορεί να χρησιμοποιούν κρυπτογραφία ή ψηφιακές υπογραφές για τον έλεγχο ακεραιότητας.



Η ψηφιακή υπογραφή είναι ένας αποτελεσματικός τρόπος για τον έλεγχο της ακεραιότητας ενός αρχείου ή ενός κώδικα λογισμικού. Μια ψηφιακή υπογραφή παρέχει έναν τρόπο για τη διασφάλιση του ότι ο κώδικας λογισμικού ή το αρχείο δεν έχει αλλοιωθεί από τη στιγμή που υπογράφτηκε από τον αρχικό του δημιουργό. Η ψηφιακή υπογραφή δημιουργείται με τη χρήση ενός ισχυρού αλγορίθμου κρυπτογράφησης, ο οποίος υπολογίζει έναν μοναδικό αριθμό που

αντιστοιχεί στο αρχείο ή στον κώδικα λογισμικού. Η διαδικασία επαλήθευσης μπορεί να επιβεβαιώσει την ακεραιότητα του αρχείου ή του κώδικα λογισμικού επικυρώνοντας την ψηφιακή υπογραφή με το δημόσιο κλειδί του αρχικού δημιουργού. Εάν η ψηφιακή υπογραφή είναι έγκυρη, τότε ο διαδικτυακός χρήστης μπορεί να είναι σίγουρος ότι το αρχείο ή ο κώδικας λογισμικού που λαμβάνει είναι αυθεντικός και δεν έχει υποστεί αλλαγές.

Οι μηχανισμοί αυτοί είναι σημαντικοί για τη διατήρηση της ακεραιότητας του λογισμικού, του firmware και των πληροφοριών, καθώς παρέχουν έναν τρόπο για την επαλήθευση της αυθεντικότητας και της ακεραιότητάς τους. Μπορούν να χρησιμοποιηθούν για τον έλεγχο των αρχείων λογισμικού και του firmware που χρησιμοποιούνται σε συστήματα ελέγχου, σε ευαίσθητες βιομηχανικές διεργασίες ή σε άλλες εφαρμογές που απαιτούν ασφάλεια και αξιοπιστία. Η χρήση αυτών των μηχανισμών επιτρέπει επίσης στους χρήστες να βεβαιωθούν ότι ο κώδικας λογισμικού που εκτελούν είναι αυθεντικός και δεν έχει τροποποιηθεί από κακόβουλο λογισμικό ή hackers.

Η προδιαγραφή **ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4** και **SR 3.8** περιλαμβάνει τέσσερα σημαντικά απαιτήσεις ασφάλειας για τα συστήματα ελέγχου βιομηχανικών διαδικασιών (ICS) που αναφέρονται στην υποκατηγορία πλαισίου κυβερνοασφάλειας PR.DS-6. Πιο συγκεκριμένα η απαίτηση ασφάλειας **SR 3.1** ανιχνεύει και προλαμβάνει τη μη εξουσιοδοτημένη πρόσβαση. Η **SR 3.3** προστατεύει τα ευαίσθητα δεδομένα. Αυτή η απαίτηση περιλαμβάνει την προστασία των ευαίσθητων δεδομένων που αποθηκεύονται στο σύστημα ελέγχου βιομηχανικών διαδικασιών (ICS) από μη εξουσιοδοτημένη πρόσβαση ή αλλοίωση.

Για την προστασία του συστήματος ελέγχου από κακόβουλο λογισμικό αναφέρεται η απαίτηση **SR 3.4** η οποία περιλαμβάνει προστασία από ιούς, κατασκόπους και άλλους κακόβουλους κώδικες. Τέλος η SR 3.8 διαχειρίζεται τα αποτελέσματα ασφάλειας. Αυτή η απαίτηση εμπεριέχει την ανάλυση και την αξιολόγηση των αποτελεσμάτων ασφάλειας για τη διασφάλιση ότι όλα τα αδύνατα σημεία του συστήματος ελέγχου έχουν ανιχνευθεί και αντιμετωπιστεί επαρκώς.

Επιπροσθέτως αναφέρεται το **ISO/IEC 27001:2013** όπου είναι ένα πρότυπο για το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS) που παρέχει ένα πλαίσιο για την καθιέρωση, την εφαρμογή, τη διατήρηση και τη συνεχή βελτίωση της διαχείρισης της ασφάλειας πληροφοριών σε έναν οργανισμό. Οι απαιτήσεις που εφαρμόζονται είναι οι **A.12.2.1**, **A.12.5.1, A.14.1.2, A.14.1.3**. Πιο αναλυτικά η **A.12.2.1** είναι υπεύθυνη για την ορθή επεξεργασία σε εφαρμογές. Αυτή η απαίτηση επικεντρώνεται στη διασφάλιση ότι οι πληροφορίες που υποβάλλονται σε επεξεργασία από μια εφαρμογή είναι σωστές, πλήρεις και έγκαιρες. Αυτό περιλαμβάνει την εφαρμογή ελέγχων για τον εντοπισμό και τη διόρθωση σφαλμάτων και την πρόληψη μη εξουσιοδοτημένης τροποποίησης δεδομένων. Η **A.12.5.1** εφαρμόζεται με σκοπό την ασφάλεια πληροφοριών στη διαχείριση έργου. Αυτή η απαίτηση υπογραμμίζει την ανάγκη ενσωμάτωσης της ασφάλειας πληροφοριών στις διαδικασίες διαχείρισης έργου για να διασφαλιστεί ότι οι απαιτήσεις ασφάλειας εντοπίζονται, αξιολογούνται και αντιμετωπίζονται καθ' όλη τη διάρκεια του κύκλου ζωής του έργου. Με σκοπό την πολιτική ασφαλούς ανάπτυξης αναφέρεται η απαίτηση **A.14.1.2** όπου επιβάλλει τη δημιουργία και την εφαρμογή μιας πολιτικής που περιγράφει την προσέγγιση του οργανισμού για την ασφαλή ανάπτυξη λογισμικού. Διαθέτει οδηγίες για ασφαλείς πρακτικές κωδικοποίησης, δοκιμές και επαλήθευση λογισμικού και διαχείριση κινδύνων καθ' όλη τη διάρκεια του κύκλου ζωής ανάπτυξης λογισμικού. Εν κατακλείδι η **A.14.1.3** περιλαμβάνει την εφαρμογή ελέγχων για τη διασφάλιση της ασφάλειας των συστημάτων κατά τη διαδικασία ανάπτυξης. Εφαρμόζει επίσης την ασφάλεια διεπαφών συστήματος, μηχανισμούς μεταφοράς δεδομένων και ασφαλείς πρακτικές κωδικοποίησης.

Ένα σύστημα πρέπει να καθορίζει τις απαιτήσεις για κρυπτογραφικές μονάδες κάτι που επιτυγχάνεται με το το **FIPS 140-2** (Federal Information Processing Standard Publication 140-2), ένα πρότυπο που εκδόθηκε από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) στις Ηνωμένες Πολιτείες. Η ενότητα 4 του FIPS 140-2 περιγράφει τις απαιτήσεις για το σχεδιασμό και την υλοποίηση της κρυπτογραφικής μονάδας. Περιλαμβάνει τις προδιαγραφές κρυπτογραφικής μονάδας, τις υπηρεσίες και έλεγχος ταυτότητας, το μοντέλο πεπερασμένης κατάστασης, τη φυσική ασφάλεια, το λειτουργικό περιβάλλον και τη διασφάλιση σχεδίασης.

Για την περαιτέρω ασφάλεια των υπολογιστών αναφέρεται ένα έγγραφο καθοδήγησης, το **NIST SP 800-45 Ver. 2**. Στη συγκεκριμένη περίπτωση εφαρμόζονται μερικές από τις ενότητες του εν λόγο εγγράφου όπως η ενότητα **2.4.2** η οποία εξετάζει τη σημασία της τεκμηρίωσης των αρχικών δραστηριοτήτων αντιμετώπισης περιστατικών. Αυτή η τεκμηρίωση μπορεί να είναι χρήσιμη για τον προσδιορισμό της έκτασης του συμβάντος, τον εντοπισμό των επηρεαζόμενων συστημάτων και δεδομένων και την κατανόηση των πιθανών επιπτώσεων του συμβάντος. Στη συνέχεια η ενότητα **3** περιγράφει τα βήματα που πρέπει να ληφθούν κατά τη διάρκεια της αρχικής φάσης αντιμετώπισης του περιστατικού, συμπεριλαμβανομένου του εντοπισμού και του περιορισμού του συμβάντος, της αξιολόγησης της κατάστασης και της ειδοποίησης των κατάλληλων μερών. Από την άλλη μεριά η εφαρμογή της ενότητας **4.2.3** εξετάζει τη σημασία της διατήρησης της αλυσίδας φύλαξης για αποδεικτικά στοιχεία που συλλέγονται κατά τη διάρκεια μιας αντίδρασης σε περιστατικό. Αυτό περιλαμβάνει τεκμηρίωση ποιος είχε πρόσβαση στα αποδεικτικά στοιχεία και πού είχαν αποθηκευτεί. Η ενότητα **4.3** συζητά τη σημασία της διατήρησης αποδεικτικών στοιχείων κατά τη διάρκεια μιας αντίδρασης σε περιστατικό. Περιγράφει τα βήματα που πρέπει να ληφθούν για να διασφαλιστεί ότι τα αποδεικτικά στοιχεία δεν αλλοιώνονται, καταστρέφονται ή μολύνονται κατά τη διάρκεια της έρευνας. Με την ενότητα **5.1** περιγράφονται τα βήματα που πρέπει να ληφθούν κατά τη φάση ανάλυσης μιας απόκρισης περιστατικού. Αυτό περιλαμβάνει την ανάλυση των αρχείων καταγραφής του συστήματος, τον έλεγχο της κυκλοφορίας του δικτύου και την εξέταση τυχόν συλλεγόμενων στοιχείων. Για την ενημέρωση των ενδιαφερομένων για την κατάσταση του συμβάντος, την παροχή τακτικών ενημερώσεων και τη λήψη της συμβολής εφαρμόζεται η ενότητα **6.1**. Με την **7.2.2** εξετάζεται η σημασία της τεκμηρίωσης των αποτελεσμάτων της έρευνας του συμβάντος. Αυτή η τεκμηρίωση

μπορεί να χρησιμοποιηθεί για τον εντοπισμό περιοχών όπου μπορούν να γίνουν βελτιώσεις για την αποφυγή μελλοντικών συμβάντων. Η σημασία της ανάπτυξης ενός σχεδίου αντιμετώπισης περιστατικών αντιμετωπίζεται με την ενότητα **8.2** η οποία περιλαμβάνει διαδικασίες για τον εντοπισμό και την αναφορά συμβάντων, την αξιολόγηση της κατάστασης, τον περιορισμό και την εξάλειψη του συμβάντος και την ανάκαμψη από το συμβάν. Τέλος με την ενότητα **9.2** τίθεται η σημασία της τακτικής εκπαίδευσης και ασκήσεων για να διασφαλιστεί ότι το προσωπικό αντιμετώπισης περιστατικών είναι έτοιμο να ανταποκριθεί σε περιστατικά. Η εκπαίδευση θα πρέπει να καλύπτει διαδικασίες, εργαλεία και τεχνικές αντιμετώπισης περιστατικών, ενώ οι ασκήσεις θα πρέπει να παρέχουν την ευκαιρία να εξασκηθούν αυτές οι δεξιότητες σε ένα ρεαλιστικό σενάριο.

Το **NIST SP 800-49** που αναφέρεται στην εν λόγω υποκατηγορία είναι μια ειδική έκδοση που παρέχει οδηγίες για την ασφάλεια συστημάτων ηλεκτρονικού ταχυδρομείου (email). Γίνονται αναφορές στις ενότητες 2.2.1, 2.3.2 και στην 3.4. Με αυτόν τον τρόπο παρέχεται καθοδήγηση σχετικά με την εφαρμογή μιας πολιτικής ασφαλείας για συστήματα ηλεκτρονικού ταχυδρομείου τονίζοντας την ανάγκη για ανάπτυξη και εφαρμογή πολιτικών και διαδικασιών για την προστασία συστημάτων και δεδομένων email με την χρήση κρυπτογράφησης ελέγχων πρόσβασης καθώς και παρακολούθησης. Επίσης με την χρήση αυτών των ενοτήτων ασφαλίζονται οι ψηφιακές υπογραφές με τον έλεγχο ταυτότητας του αποστολέα και παρέχονται οδηγίες με τη χρήση κρυπτογράφησης email για τη προστασία απορρήτου των μηνυμάτων email.

Απαραίτητος είναι ο ασφαλής χειρισμός των ασύρματων δικτύων όπου αυτό επιτυγχάνεται με την χρήση του **NIST SP 800-52 Rev. 1**. Γίνονται αναφορές στις ενότητες **3**, **4** καθώς και στην ενότητα **D1.4**. Πιο συγκεκριμένα η ενότητα **3** παρέχει μία επισκόπηση των ελέγχων ασφαλείας που πρέπει να εφαρμοστούν για την προστασία των ασύρματων δικτύων, συμπεριλαμβανομένης της χρήσης ισχυρής κρυπτογράφησης, ελέγχων πρόσβασης και συστημάτων ανίχνευσης εισβολών. Η ενότητα **4** παρέχει οδηγίες για τη διαμόρφωση των σημείων ασύρματης πρόσβασης, συμπεριλαμβανομένης της χρήσης ασφαλών μεθόδων ελέγχου ταυτότητας, όπως το 802.1X και το WPA2, και τη χρήση ισχυρών πρωτοκόλλων κρυπτογράφησης, όπως το AES. Τέλος η ενότητα **D1.4** παρέχει καθοδήγηση σχετικά με τη χρήση συστημάτων εντοπισμού και πρόληψης ασύρματης εισβολής (WIDS/WIPS) για τον εντοπισμό και την αποτροπή μη εξουσιοδοτημένης πρόσβασης σε ασύρματα δίκτυα. Αναλύει τους διάφορους τύπους διαθέσιμων συστημάτων WIDS/WIPS, συμπεριλαμβανομένων συστημάτων που βασίζονται σε δίκτυο και συστημάτων που βασίζονται σε αισθητήρες, και παρέχει συστάσεις για τη χρήση αυτών των συστημάτων για την προστασία των ασύρματων δικτύων.

Το **NIST SP 800-53 Rev. 4** είναι μια ειδική δημοσίευση που παρέχει κατευθυντήριες γραμμές για τη διαχείριση των πληροφοριακών συστημάτων και αναφέρεται στην υποκατηγορία πλαισίου κυβερνοασφάλειας PR.DS-6. Το **SI-7** αναφέρεται στη διαχείριση των προνομίων των χρηστών στα συστήματα πληροφορικής. Η ενότητα SI-7 του NIST SP 800-53 Rev. 4 περιέχει κατευθυντήριες γραμμές για τη διαχείριση των προνομίων των χρηστών στα συστήματα πληροφορικής. Συγκεκριμένα, αναφέρεται στη διαχείριση της πρόσβασης των χρηστών σε ευαίσθητες πληροφορίες και σε λειτουργίες συστημάτων. Ο στόχος είναι να διασφαλιστεί ότι οι χρήστες έχουν μόνο τα απαραίτητα προνόμια για να εκτελέσουν τις εργασίες τους και όχι περισσότερα προνόμια που θα μπορούσαν να χρησιμοποιηθούν για κακόβουλους σκοπούς.

Το **NIST SP 800-57 Part 1 Rev. 4** είναι μια δημοσίευση από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) που παρέχει οδηγίες για τη δημιουργία και την εφαρμογή ενός συστήματος διαχείρισης κρυπτογραφικών κλειδιών (CKMS). Σύμφωνα με την ενότητα **5.5** παρέχεται διευκρίνηση σχετικά με τις βασικές πρακτικές αποθήκευσης. Προτείνει ότι τα κρυπτογραφικά κλειδιά θα πρέπει να αποθηκεύονται σε ασφαλή τοποθεσία που να προστατεύεται από φυσικές και λογικές απειλές. Τα κλειδιά πρέπει να αποθηκεύονται με τρόπο που να διασφαλίζει

την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητά τους. Από την άλλη η ενότητα **6.1** παρέχει οδηγίες σχετικά με τις βασικές πρακτικές εγκατάστασης. Τα κρυπτογραφικά κλειδιά πρέπει να δημιουργηθούν χρησιμοποιώντας μια εγκεκριμένη μέθοδο δημιουργίας κλειδιού που να παρέχει επαρκή αντοχή για την προβλεπόμενη εφαρμογή. Το έγγραφο συνιστά επίσης ότι η εγκατάσταση του κλειδιού θα πρέπει να πραγματοποιείται χρησιμοποιώντας μια μέθοδο ελέγχου ταυτότητας για να διασφαλιστεί η γνησιότητα των κλειδιών. Εκτός από την αποθήκευση και την εγκατάσταση κλειδιού είναι αναγκαία η καθοδήγηση σχετικά με την καταστροφή κλειδιού. Αυτό είναι εφικτό με την εφαρμογή της ενότητας **8.1.5.1** η οποία παρέχει την ιδέα ότι τα κρυπτογραφικά κλειδιά πρέπει να καταστραφούν με τρόπο που να διασφαλίζει την πλήρη και μη αναστρέψιμη καταστροφή τους. Μια επίσης ενότητα που αναφέρεται είναι η **B.3.2** η οποία περιγράφει οδηγίες για τη χρήση ενός κλειδιού. Τα κρυπτογραφικά κλειδιά θα πρέπει να χρησιμοποιούνται μόνο για τον προορισμό τους και ότι η χρήση κλειδιών θα πρέπει να περιορίζεται μόνο σε εξουσιοδοτημένο προσωπικό. Τέλος η ενότητα **B.5** του εγγράφου παρέχει καθοδήγηση σχετικά με τις βασικές πρακτικές συμβιβασμού. Προτείνει ότι εάν υπάρχει υποψία ότι ένα κλειδί έχει παραβιαστεί, θα πρέπει να ληφθούν άμεσα μέτρα για τον μετριασμό του κινδύνου. Το έγγραφο συνιστά να υπάρχει ένα σχέδιο απόκρισης συμβιβασμού σε κλειδί και ότι το σχέδιο πρέπει να περιλαμβάνει διαδικασίες για την ανάκληση και την αντικατάσταση παραβιασμένων κλειδιών.

Το **NIST SP 800-57 Part 2** είναι μια άλλη δημοσίευση από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) που παρέχει οδηγίες για τη διαχείριση κρυπτογραφικών κλειδιών σε συγκεκριμένα περιβάλλοντα, όπως κινητές συσκευές και έξυπνες κάρτες. Στην ενότητα **1** που αναφέρεται έχουμε την εισαγωγή η οποία παρέχει μια επισκόπηση της δημοσίευσης και του σκοπού της. Εξηγεί ότι το έγγραφο παρέχει καθοδήγηση σχετικά με τη διαχείριση κρυπτογραφικών κλειδιών σε διάφορα περιβάλλοντα, συμπεριλαμβανομένων κινητών συσκευών, έξυπνων καρτών και άλλων ενσωματωμένων συστημάτων. Όσον αφορά την δημιουργία κλειδιών εφαρμόζεται η ενότητα **3.1.2.1.2**. Η εν λόγω ενότητα προτείνει ότι τα κρυπτογραφικά κλειδιά θα πρέπει να δημιουργούνται χρησιμοποιώντας μια κρυπτογραφικά ισχυρή γεννήτρια τυχαίων αριθμών. Το έγγραφο συνιστά επίσης ότι η διαδικασία δημιουργίας κλειδιών πρέπει να εκτελείται σε ασφαλές περιβάλλον και ότι τα κλειδιά πρέπει να προστατεύονται κατά τη μετάδοση και την αποθήκευση. Στη συνέχεια με την ενότητα **4.1** παρέχεται η καθοδήγηση σχετικά με τις βασικές πρακτικές εγκατάστασης. Τα κρυπτογραφικά κλειδιά πρέπει να δημιουργηθούν χρησιμοποιώντας μια εγκεκριμένη μέθοδο δημιουργίας κλειδιού που παρέχει επαρκή αντοχή για την προβλεπόμενη εφαρμογή. Η διανομή των κλειδιών σύμφωνα με την ενότητα **4.2** θα πρέπει να διανέμεται χρησιμοποιώντας μια ασφαλή μέθοδο που διασφαλίζει την εμπιστευτικότητα και την ακεραιότητα των κλειδιών. Συνεχίζοντας η ενότητα **4.3** προτείνει τα κρυπτογραφικά κλειδιά να ενεργοποιούνται σε ασφαλές περιβάλλον και η διαδικασία ενεργοποίησης πρέπει να εκτελείται χρησιμοποιώντας μια μέθοδο ελέγχου ταυτότητας για να διασφαλιστεί η γνησιότητα των κλειδιών. Με την εξέλιξη της τεχνολογίας οι έξυπνες κάρτες έχουν μια ισχυρή θέση και είναι αναγκαίο να προστεθούν οδηγίες σχετικά με τις πρακτικές διανομής κλειδιών για έξυπνες κάρτες σύμφωνα με την ενότητα **A.3.2**. Υποδηλώνει ότι οι έξυπνες κάρτες παρουσιάζουν μοναδικές προκλήσεις ασφαλείας λόγω του μικρού τους μεγέθους και της περιορισμένης επεξεργαστικής τους ισχύος. Τέλος η ενότητα **C.2.2** παρέχει καθοδήγηση σχετικά με βασικές πρακτικές αντιμετώπισης συμβιβασμού για ενσωματωμένα συστήματα. Προτείνει ότι εάν υπάρχει υποψία ότι ένα κλειδί έχει παραβιαστεί, θα πρέπει να ληφθούν άμεσα μέτρα για τον μετριασμό του κινδύνου.

Το **NIST SP 800-81-2** είναι ένα πρότυπο ασφαλείας της Εθνικής Υπηρεσίας Προτύπων και Τεχνολογίας (NIST) των Ηνωμένων Πολιτειών το οποίο αναφέρεται στην συγκεκριμένη υποκατηγορία. Αφορά τη χρήση ηλεκτρονικού ταχυδρομείου και άλλων συστημάτων στη διοίκηση

και τον δημόσιο τομέα. Το πρότυπο παρέχει κατευθυντήριες γραμμές για την ανάπτυξη και την υλοποίηση των μέτρων ασφάλειας που απαιτούνται για να διασφαλιστεί η ακεραιότητα, η εμπιστευτικότητα και η διαθεσιμότητα των μηνυμάτων. Η εφαρμογή του προτύπου μπορεί να βοηθήσει στην πρόληψη επιθέσεων και την προστασία των πληροφοριών των χρηστών.

Το **NIST SP 800-130** είναι ένα πρότυπο που δημοσιεύεται από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) στις Ηνωμένες Πολιτείες και αφορά την ασφάλεια πληροφοριών σε κρυπτογραφικά συστήματα. Οι αναφερόμενες ενότητες είναι οι εξής :

2.2: Έλεγχος ταυτότητας: Η διαδικασία επαλήθευσης της ταυτότητας ενός χρήστη ή συστήματος μέσω μέσων όπως κωδικοί πρόσβασης ή πιστοποιητικά.

4.3: Επιλογή κρυπτογραφικού αλγορίθμου: Περιγράφει παράγοντες που πρέπει να λαμβάνονται υπόψη κατά την επιλογή κρυπτογραφικών αλγορίθμων, όπως η ασφάλεια, η απόδοση και η δυνατότητα αναβάθμισης.

6.2.1: Διαχείριση κρυπτογραφικού κλειδιού: Περιγράφει παράγοντες που πρέπει να λαμβάνονται υπόψη κατά τη διαχείριση κρυπτογραφικών κλειδιών, όπως η δημιουργία, η αποθήκευση, η διανομή και η ανάκληση κλειδιών.

6.3: Προστασία κρυπτογραφικού κλειδιού: Περιγράφει τα μέτρα που πρέπει να ληφθούν για την προστασία των κρυπτογραφικών κλειδιών, όπως η φυσική ασφάλεια, οι έλεγχοι πρόσβασης και οι διαδικασίες δημιουργίας αντιγράφων ασφαλείας και ανάκτησης.

6.4: Δημιουργία κρυπτογραφικού κλειδιού: Περιγράφει μεθόδους για τη δημιουργία κρυπτογραφικών κλειδιών, όπως πρωτόκολλα ανταλλαγής κλειδιών και σχήματα συμφωνιών κλειδιών.

6.5: Χρήση κρυπτογραφικού κλειδιού: Περιγράφει τις βέλτιστες πρακτικές για τη χρήση κρυπτογραφικών κλειδιών, όπως ο περιορισμός της χρήσης κλειδιών σε συγκεκριμένους σκοπούς και η περιοδική αλλαγή κλειδιών.

6.6.1: Χρόνος ζωής κρυπτογραφικού κλειδιού: Περιγράφει τις εκτιμήσεις για τον προσδιορισμό της κατάλληλης διάρκειας ζωής των κρυπτογραφικών κλειδιών, όπως η ευαισθησία των πληροφοριών που προστατεύονται και ο ρυθμός τεχνολογικής προόδου.

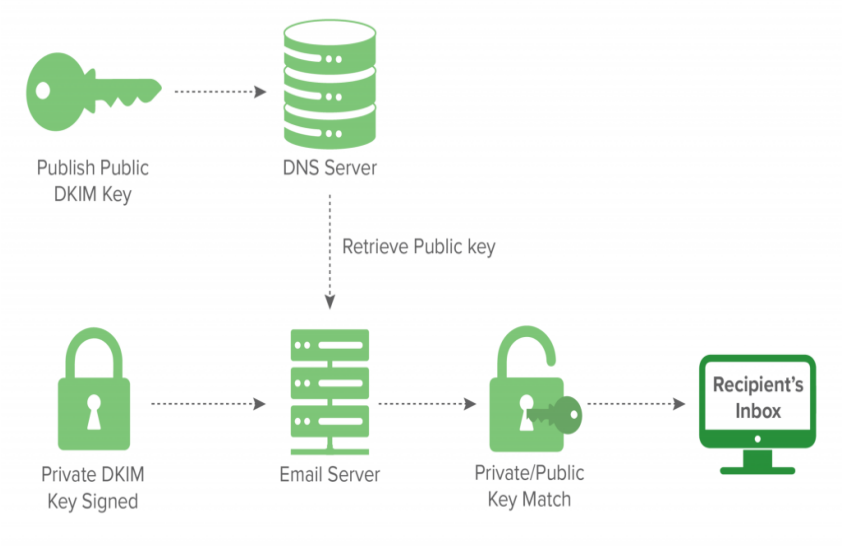
Το **NIST SP 800-152** είναι ένα αναφερόμενο πρότυπο όπου εφαρμόζονται οι ενότητες **6.1.3, 6.2.1, 8.2.1, 8.2.4, 9.4**. Πιο συγκεκριμένα η ενότητα **6.1.3** περιγράφει την πρακτική της διαίρεσης ενός δικτύου σε μικρότερα υποδίκτυα για τη βελτίωση της ασφάλειας και τον μετριασμό των επιπτώσεων μιας παραβίασης ασφάλειας. Η ενότητα **6.2.1** αναλύει τη διαδικασία ελέγχου της πρόσβασης σε πόρους και συστήματα μέσα σε ένα ICS, συμπεριλαμβανομένου του ελέγχου ταυτότητας χρήστη και της εξουσιοδότησης. Παράλληλα η ενότητα **8.2.1** εφαρμόζει τη διαδικασία προετοιμασίας και αντιμετώπισης συμβάντων ασφαλείας εντός ενός ICS, συμπεριλαμβανομένης της σύστασης ομάδων και διαδικασιών αντιμετώπισης περιστατικών. Για την ανάλυση των περιστατικών αναφέρεται η ενότητα **8.2.4** η οποία αναλύει τα συμβάντα ασφαλείας σε ένα ICS για τον εντοπισμό της αιτίας και της έκτασης του συμβάντος, καθώς και τυχόν απαραίτητα βήματα αποκατάστασης. Τέλος η ενότητα **9.4** δείχνει τη σημασία της παροχής προγραμμάτων εκπαίδευσης και ευαισθητοποίησης για το προσωπικό ενός ICS, συμπεριλαμβανομένης της εκπαίδευσης ευαισθητοποίησης για την ασφάλεια και της εκπαίδευσης για την αντιμετώπιση περιστατικών.

Η τελευταία αναφορά στην υποκατηγορία πλαισίου κυβερνοασφάλειας PR.DS-6 είναι η **NIST SP 800-177** όπου αφορά το αξιόπιστο ηλεκτρονικό ταχυδρομείο. Οι ενότητες που αναφέρονται είναι οι ακόλουθες :

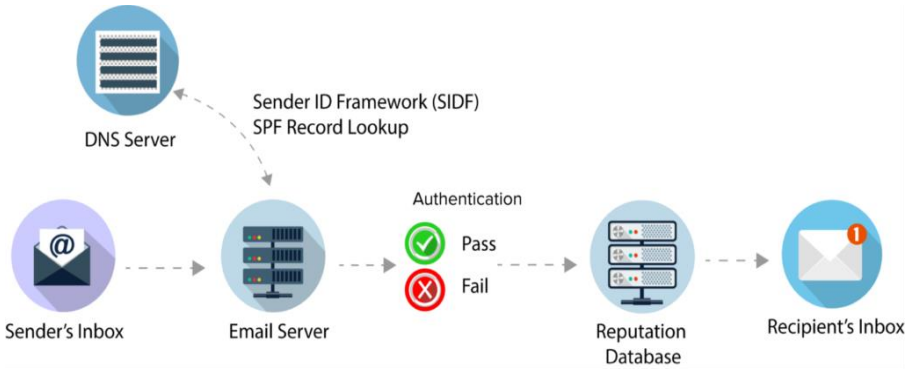
2.2: Αρχιτεκτονική ασφάλειας email: Περιγράφει τα διάφορα στοιχεία μιας αρχιτεκτονικής ασφάλειας email, συμπεριλαμβανομένων των προγραμμάτων-πελατών email, των διακομιστών και των πυλών.

4.1: Έλεγχος ταυτότητας email: Αναλύει την επεξεργασία επαλήθευσης της γνησιότητας των μηνυμάτων email, συμπεριλαμβανομένων μεθόδων όπως DKIM, SPF και DMARC. Οι μέθοδοι DKIM, SPF και DMARC είναι μηχανισμοί επαλήθευσης αυθεντικότητας των email, που χρησιμοποιούνται για την προστασία από την αποστολή ανεπιθύμητων ηλεκτρονικών μηνυμάτων (spam), καθώς και για την αντιμετώπιση του phishing και άλλων επιθέσεων. Η μέθοδος DKIM (DomainKeys Identified Mail) επιτρέπει στον αποστολέα να υπογράφει τα μηνύματά του με μια κρυπτογραφημένη ψηφιακή υπογραφή, η οποία

επαληθεύεται από το διακομιστή - παραλήπτη που λαμβάνει το μήνυμα. Αυτό επιτρέπει στον παραλήπτη να ελέγξει ότι το μήνυμα δεν έχει παραποιηθεί κατά τη διαμετακόμιση.



Η μέθοδος SPF (Sender Policy Framework) είναι μια τεχνολογία που επιτρέπει στον κάτοχο ενός domain να καθορίσει ποιοι διακομιστές email έχουν το δικαίωμα να αποστέλλουν email εξ ονόματος αυτού του domain.



Με το DMARC, ο κάτοχος ενός domain μπορεί να καθορίσει τις ενέργειες που πρέπει να ακολουθούνται όταν ένα email από το domain αυτό δεν περνάει την επαλήθευση DKIM ή SPF. Αυτές οι ενέργειες μπορούν να περιλαμβάνουν την απόρριψη του μηνύματος ή την προώθησή του σε έναν άλλο διακομιστή για περαιτέρω ανάλυση.

4.4: Κρυπτογράφηση email: Περιγράφει μια σειρά ενεργειών κρυπτογράφησης μηνυμάτων email για την προστασία του απορρήτου του περιεχομένου τους.

4.5: Υπογραφή email: Εξηγεί τη διαδικασία ψηφιακής υπογραφής μηνυμάτων email για την επαλήθευση της γνησιότητας και της ακεραιότητάς τους.

4.7: Φιλτράρισμα email: Χαρακτηρίζει το φιλτράρισμα εισερχόμενων μηνυμάτων email για προστασία από ανεπιθύμητα μηνύματα, ηλεκτρονικό ψάρεμα και άλλους τύπους κακόβουλων email.

5.2: Πολιτική ασφαλείας email: Παριστάνει τη σημασία της ανάπτυξης μιας πολιτικής ασφάλειας email, συμπεριλαμβανομένων στοιχείων όπως αποδεκτή χρήση, απόκριση σε περιστατικά και εκπαίδευση και ευαισθητοποίηση.

5.3: Έλεγχοι ασφάλειας email: Εξηγεί τους διάφορους ελέγχους ασφαλείας που πρέπει να εφαρμόζονται για την προστασία των συστημάτων και των μηνυμάτων email, συμπεριλαμβανομένων των ελέγχων πρόσβασης, της παρακολούθησης και καταγραφής και των διαδικασιών δημιουργίας αντιγράφων ασφαλείας και ανάκτησης.

Παράδειγμα Υλοποίησης 5
Διαδικασίες Προστασίας Πληροφοριών (PR.IP)

Η διαδικασία της προστασίας των συστημάτων και των περιουσιακών στοιχείων επιτυγχάνεται μέσω της διατήρησης και χρήσης ασφαλείας πολιτικών, διαδικασιών και διαδικασιών που καλύπτουν τον σκοπό, το πεδίο εφαρμογής, τους ρόλους, τις ευθύνες, τη δέσμευση της διοίκησης και τον συντονισμό μεταξύ των οργανωτικών μονάδων του οργανισμού. Αυτές οι ασφαλείας πολιτικές και διαδικασίες πρέπει να διατηρούνται και να χρησιμοποιούνται σε καθημερινή βάση προκειμένου να διαχειρίζονται την προστασία των συστημάτων και των περιουσιακών στοιχείων του οικιακού δικτύου ή της μικρής επιχείρησης.

Υποκατηγορία Πλαισίου Κυβερνοασφάλειας PR.IP-1

Η πολιτική **PR.IP-1** αναφέρεται στη δημιουργία και διατήρηση μιας βασικής διαμόρφωσης της τεχνολογίας πληροφορικής ή βιομηχανικού ελέγχου, η οποία θα περιλαμβάνει αρχές ασφαλείας όπως η έννοια της ελάχιστης λειτουργικότητας. Αυτό σημαίνει ότι η διαμόρφωση αυτή θα πρέπει να περιορίζει τη λειτουργικότητα του συστήματος στο ελάχιστο απαραίτητο επίπεδο, ώστε να μειώνεται η πιθανότητα επιθέσεων και να διασφαλίζεται η ασφάλεια του συστήματος. Η διαμόρφωση αυτή θα πρέπει να περιλαμβάνει την εφαρμογή προληπτικών μέτρων ασφαλείας, όπως η εγκατάσταση λογισμικού ασφαλείας, η ενεργοποίηση λειτουργιών ασφαλείας στο λειτουργικό σύστημα και η παρακολούθηση της απόδοσης του συστήματος. Η διαμόρφωση αυτή θα πρέπει επίσης να περιλαμβάνει τη δημιουργία και τη διατήρηση ενός ακριβούς εγχειριδίου ασφαλείας που

θα περιγράφει τη σωστή χρήση και τη διαχείριση του συστήματος. Όπως και στην υποκατηγορία πλαισίου κυβερνοασφάλειας ID.AM-1, PR.AC-1 και στην PR.AC-7 έτσι και στη PR.IP-1 γίνεται αναφορά στο CIS CSC 1 με σκοπό την προστασία των πληροφοριακών συστημάτων και των δεδομένων.

Οι αναφορές **COBIT 5 BAI10.01**, **BAI10.02**, **BAI10.03** και **BAI10.05** εφαρμόζουν πρακτικές ασφαλείας που περιλαμβάνονται στο πλαίσιο ελέγχου COBIT 5. Αυτές οι πρακτικές ασφαλείας σχετίζονται με τη διαχείριση ασφαλείας των πληροφοριακών συστημάτων σε μια οργάνωση και προτείνουν τρόπους για την εφαρμογή καλών πρακτικών. Με την **BAI10.01** γίνεται λόγος για τη διαχείριση των αδειών χρήσης λογισμικού, ενώ με την αναφορά **BAI10.02** για τη διαχείριση της ασφάλειας του δικτύου και των εφαρμογών. Η **BAI10.03** αφορά την αντιμετώπιση κινδύνων και προβλημάτων ασφαλείας και η **BAI10.05** αναφέρεται στην παρακολούθηση και τον έλεγχο της ασφάλειας των πληροφοριακών συστημάτων. Εφαρμόζονται στην υποκατηγορία PR.IP-1 ώστε να βελτιωθεί η ασφάλεια των πληροφοριακών συστημάτων με στόχο την προστασία των ευαίσθητων δεδομένων.

Το πλαίσιο αναφοράς **ISA/IEC 62443** επικεντρώνεται στην προστασία των συστημάτων ελέγχου και των δεδομένων από απειλές όπως η κατασκοπεία και η απώλεια δεδομένων. Στην υποκατηγορία PR.IP-1 αναφέρονται οι ενότητες **4.3.4.3.2** και **4.3.4.3.3**. Συγκεκριμένα η ενότητα **4.3.4.3.2** είναι υπεύθυνη για τον έλεγχο της αυθεντικότητας των δεδομένων στο επίπεδο πρωτοκόλλου επικοινωνίας. Απαιτείται η εφαρμογή μέτρων ασφαλείας που εξασφαλίζουν ότι οι αποστολείς και οι παραλήπτες δεδομένων είναι αυθεντικοί και δεν έχουν παραποιηθεί. Από την άλλη στην ενότητα **4.3.4.3.3** γίνεται έλεγχος της ακεραιότητας των δεδομένων στο επίπεδο πρωτοκόλλου επικοινωνίας. Με αυτόν τον τρόπο εξασφαλίζεται ότι τα δεδομένα δεν έχουν τροποποιηθεί κατά την μεταφορά των συσκευών.

Για την εφαρμογή μηχανισμών κρυπτογράφησης όπως το SSL/TLS για την προστασία των δεδομένων που ανταλλάσσονται μεταξύ των συσκευών στο δίκτυο γίνεται αναφορά στο πρότυπο **ISA 62443-3-3:2013 SR 7.6**. Με αυτή την αναφορά προτείνεται η χρήση μηχανισμών αυθεντικοποίησης και εξουσιοδότησης για τη διασφάλιση ότι μόνο εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στο δίκτυο.

Με στόχο την επιθεώρηση της ασφάλειας των πληροφοριακών συστημάτων εμφανίζονται οι αναφορές **ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3** και **A.14.2.4**. Η αναφορά **A.12.1.2** αφορά τη διαδικασία αξιολόγησης των κινδύνων για την ασφάλεια των πληροφοριακών συστημάτων. Η διαδικασία αξιολόγησης των κινδύνων είναι σημαντική για την αναγνώριση και αντιμετώπιση των απειλών που αντιμετωπίζει ένα πληροφοριακό σύστημα. Η **A.12.5.1** είναι υπεύθυνη για την πρόληψη της κακόβουλης χρήσης των πληροφοριακών συστημάτων. Αναφέρεται σε μέτρα ασφάλειας που μπορούν να ληφθούν για να προληφθεί η κακόβουλη χρήση των πληροφοριακών συστημάτων από εσωτερικούς χρήστες, όπως η περιορισμένη πρόσβαση σε ευαίσθητα δεδομένα και η παρακολούθηση των δραστηριοτήτων των χρηστών. Η αναφορά **A.12.6.2** γίνεται για την πρόληψη της διαρροής πληροφοριών προτείνοντας την εφαρμογή τεχνικών μέτρων ασφαλείας όπως η κρυπτογράφηση των πληροφοριών, η ανίχνευση απόπειρας μη εξουσιοδοτημένης πρόσβασης στις πληροφορίες και η επαλήθευση της ταυτότητας των χρηστών που έχουν πρόσβαση σε ευαίσθητες πληροφορίες.

Η αναφορά **A.14.2.2** αφορά τον περιορισμό της πρόσβασης στα συστήματα και τις εφαρμογές προτείνοντας την εφαρμογή αυστηρών μέτρων πρόσβασης στα συστήματα και τις

εφαρμογές που περιέχουν ευαίσθητες πληροφορίες. Για τη πρόληψη της μη εξουσιοδοτημένης πρόσβασης στα δίκτυα αναφέρεται η **A.14.2.3**. Με αυτόν τον τρόπο προτείνεται η χρήση τεχνικών μέτρων ασφαλείας όπως η παρακολούθηση της πρόσβασης στα δίκτυα. Τέλος, η αναφορά **A.14.2.4** αφορά την ανίχνευση και την αντίδραση σε παραβάσεις ασφαλείας των πληροφοριακών συστημάτων και περιγράφει την ανάγκη να υπάρχουν μηχανισμοί ανίχνευσης παραβάσεων ασφαλείας, όπως το monitoring και η λογοκρισία δικτυακών εγγράφων.

Στην υποκατηγορία πλαισίου κυβερνοασφάλειας PR.IP-1 αναφέρονται ορισμένοι έλεγχοι ασφάλειας που είναι οι εξής :

CM-2: Διαχείριση των αδειών χρήσης λογισμικού και άλλων πνευματικών δικαιωμάτων.

CM-3: Διαχείριση εγγράφων και ρυθμίσεων ασφαλείας για τα συστήματα πληροφορικής και επικοινωνιών του οργανισμού.

CM-4: Αξιολόγηση των ασφαλείας του λογισμικού πριν από τη χρήση ή τη διάθεσή του στο κοινό.

CM-5: Παρακολούθηση και ανάλυση των ασφαλείας των συστημάτων πληροφορικής και επικοινωνιών του οργανισμού.

CM-6: Αντιμετώπιση των ασφαλείας των συστημάτων πληροφορικής και επικοινωνιών κατά τη διαχείριση τους.

CM-7: Διαχείριση της παρέμβασης στα συστήματα πληροφορικής και επικοινωνιών κατά τη διάρκεια της εκτέλεσης τους.

CM-9: Διαχείριση των παρατηρήσεων ασφαλείας και των αντίστοιχων ενημερώσεων σχετικά με τα συστήματα.

SA-10: Το SA-10 αναφέρεται στον έλεγχο των προνομίων διαχειριστή (Administrator) σε συστήματα πληροφορικής και επικοινωνιών.

<u>Υποκατηγορία Πλαισίου Κυβερνοασφάλειας PR.IP-3</u>

Η πρακτική **PR.IP-3** αναφέρεται στην ύπαρξη διαδικασιών ελέγχου των αλλαγών ρυθμίσεων στο σύστημα. Αυτό σημαίνει ότι όταν γίνονται αλλαγές στη ρύθμιση του συστήματος, πρέπει να υπάρχει μια διαδικασία ελέγχου και έγκρισης των αλλαγών πριν εφαρμοστούν. Αυτή η πρακτική είναι σημαντική για να αποτραπούν δυνητικά προβλήματα ασφάλειας και απώλεια δεδομένων λόγω λανθασμένων αλλαγών στη ρύθμιση του συστήματος. Η ύπαρξη ελέγχων αλλαγών διασφαλίζει ότι οι αλλαγές είναι προσεκτικά εξετασμένες και έχουν εγκριθεί από τον κατάλληλο φορέα ή πρόσωπο πριν εφαρμοστούν.

Κάθε τεχνολογία IoT είναι απαραίτητο να αναπτύσσει διαδικασίες και τεχνικούς ελέγχους για την αναγνώριση, την ταξινόμηση, τον ασφαλή χειρισμό, την διατήρηση καθώς και την απόρριψη δεδομένων ανάλογα με την ευαισθησία και τη σημασία τους, καθώς και τη διαχείριση τους σύμφωνα με τις αντίστοιχες απαιτήσεις ασφαλείας. Αυτή η επίτευξη είναι επιτυχής με την αναφορά της **CIS CSC 3** η οποία χρησιμοποιεί τεχνικούς ελέγχους που περιλαμβάνουν κρυπτογράφηση δεδομένων, αυστηρό έλεγχο της πρόσβασης, επαλήθευση ταυτότητας καθώς και άλλα μέτρα που θα βοηθήσουν στη διατήρηση της ασφάλειας των δεδομένων. Παράλληλα σύμφωνα με την αναφορά **CIS CSC 11** πρέπει να υπάρχει δημιουργία και συντήρηση πρακτικών ανάκτησης δεδομένων όπου θα είναι αρκετές να αποκαταστήσουν τους ενδιαφερόμενους ενεργητικούς πόρους της επιχείρησης σε μια κατάσταση που ήταν πριν από το περιστατικό και σε μια κατάσταση που θα έχει επαληθευθεί ως αξιόπιστη. Στην περίπτωση που υπάρξει κάποιο περιστατικό ασφαλείας, όπως μια κυβερνοεπίθεση, μια φυσική καταστροφή ή μια αποτυχία του συστήματος, η επιχείρηση πρέπει να έχει τα απαραίτητα μέσα για την αποκατάσταση των επιρρεπών στην επίθεση πόρων και την επαναφορά τους σε μια αξιόπιστη κατάσταση.

Για να υπάρχει άρτια λειτουργικότητα και ασφάλεια σε ένα περιβάλλον IoT σε οικιακά δίκτυα και μικρές επιχειρήσεις με την ανάπτυξη και εφαρμογή πολιτικών ασφάλειας των πληροφοριών αναφέρεται η **BAI01.06** του πλαισίου διαχείρισης τεχνολογίας πληροφοριών COBIT 5. Από την άλλη αναφέρεται η **BAI06.01** για την ανάπτυξη και εφαρμογή τεχνικών ασφάλειας όπως η κρυπτογράφηση δεδομένων και ο έλεγχος πρόσβασης σε συστήματα και δεδομένα.

Το **ISA 62443-2-1:2009** είναι ένα πρότυπο ασφάλειας για τα συστήματα ελέγχου της βιομηχανίας. Οι παράγραφοι **4.3.4.3.2** και **4.3.4.3.3** αναφέρονται στον έλεγχο της πρόσβασης σε δίκτυα και συσκευές συστημάτων ελέγχου και εμφανίζονται και στην συγκεκριμένη υποκατηγορία. Στην παράγραφο **4.3.4.3.2** αναφέρεται ότι πρέπει να υπάρχουν μέτρα για τη διαχείριση των δικαιωμάτων πρόσβασης σε δίκτυα και συσκευές συστημάτων ελέγχου. Αυτό συμβαίνει με τη διαχείριση των δικαιωμάτων πρόσβασης σε επίπεδο χρήστη και τη διαχείριση των δικαιωμάτων πρόσβασης στο λογισμικό. Παράλληλα η παράγραφος **4.3.4.3.3** εξηγεί ότι πρέπει να υπάρχουν μέτρα για τη διαχείριση των απομακρυσμένων προσβάσεων στα συστήματα ελέγχου περιλαμβάνοντας τη διαχείριση των δικαιωμάτων πρόσβασης σε απομακρυσμένα συστήματα ελέγχου και την εφαρμογή μέτρων ασφαλείας για να αποτραπεί η μη εξουσιοδοτημένη πρόσβαση σε απομακρυσμένα συστήματα ελέγχου.

Το **ISA 62443-3-3:2013** είναι ένα πρότυπο που παρέχει οδηγίες για την ασφάλεια των συστημάτων και ελέγχου και αναφέρεται στην υποκατηγορία που αναλύεται. Η ενότητα **SR 7.6** του προτύπου καθορίζει τις απαιτήσεις για την παρακολούθηση της ασφάλειας του δικτύου. Περιλαμβάνει παρακολούθηση για προσπάθειες μη εξουσιοδοτημένης πρόσβασης, κακόβουλη κυκλοφορία και άλλες ανωμαλίες που θα μπορούσαν να υποδηλώνουν παραβίαση ασφάλειας.

Το **ISO/IEC 27001:2013** είναι ένα διεθνές πρότυπο για συστήματα διαχείρισης ασφάλειας πληροφοριών (ISMS). Παρέχει ένα πλαίσιο για τη διαχείριση και την προστασία ευαίσθητων πληροφοριών χρησιμοποιώντας μια προσέγγιση βασισμένη στον κίνδυνο. Οι ενότητες **A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4** αναφέρονται σε συγκεκριμένα στοιχεία ελέγχου εντός του προτύπου που σχετίζονται με τον έλεγχο πρόσβασης, τις πολιτικές ασφάλειας πληροφοριών και τη διαχείριση συμβάντων ασφαλείας.

Η ενότητα **A.12.1.2** προσδιορίζει την ανάγκη τα οικιακά δίκτυα και οι μικρές επιχειρήσεις να διαθέτουν πολιτικές και διαδικασίες για τη διαχείριση των προνομιακών δικαιωμάτων πρόσβασης, τα οποία παραχωρούνται σε χρήστες που έχουν αυξημένα προνόμια ή άδειες σε ένα σύστημα πληροφοριών.

Η **A.12.5.1** περιγράφει την απαραίτητη χρήση πολιτικών και διαδικασιών για τον ασφαλή χειρισμό των πληροφοριών καθ' όλη τη διάρκεια του κύκλου ζωής τους, συμπεριλαμβανομένης της δημιουργίας, αποθήκευσης, μετάδοσης και καταστροφής τους.

Με την αναφορά στην **A.12.6.2** αναπτύσσεται και δοκιμάζεται ένα σχέδιο που επιτρέπει την αντίδραση σε μια κατάσταση έκτακτης ανάγκης όπως για παράδειγμα η διακοπεί των υπηρεσιών. Η δοκιμή αφορά την διενέργεια σεναρίων επαναφοράς των συστημάτων και των δεδομένων καθώς και τη δοκιμή της αποτελεσματικότητας των σχεδίων και των διαδικασιών.

Η πολιτική ασφάλειας της πληροφορίας σύμφωνα με την **A.14.2.2** αφορά την ανάπτυξη μιας πολιτικής ασφάλειας των πληροφοριών που καθορίζει τις αρχές, τους στόχους και τις διαδικασίες για τη διατήρηση της ασφάλειας των πληροφοριών.

Χάρις την **A.14.2.3** είναι δυνατή η αξιολόγηση των κινδύνων ασφάλειας των πληροφοριών όπως η αναγνώριση, η ανάλυση και η αξιολόγηση των κινδύνων ασφάλειας πληροφοριών για την λήψη των κατάλληλων μέτρων προστασίας.

Τέλος, η **A.14.2.4** προτείνει την σχεδίαση και υλοποίηση ελέγχων ασφάλειας των πληροφοριών όπου αφορά τη σχεδίαση και υλοποίηση των ελέγχων ασφάλειας των πληροφοριών για την διασφάλιση της προστασίας.

Τα NIST SP 800-53 Rev. 4 **CM-3, CM-4 και SA-10** είναι τρεις διαφορετικές κατηγορίες ελέγχων ασφάλειας που περιλαμβάνονται στο πρότυπο ασφάλειας NIST SP 800-53 Rev. 4 και αναφέρονται στην υποκατηγορία πλαισίου κυβερνοασφάλειας PR.IP-3. Ο **CM-3** αναφέρεται στον έλεγχο των αλλαγών στα συστήματα και το λογισμικό, περιλαμβανομένων των διαδικασιών εγκρίσεων, των δοκιμών και των αξιολογήσεων ασφάλειας πριν από την εφαρμογή των αλλαγών αυτών.

Από την άλλη ο έλεγχος **CM-4** προτείνει την διαχείριση των επισκευών ασφάλειας συμπεριλαμβανομένης της αναγνώρισης και αντιμετώπισης των προβλημάτων ασφαλείας και της εφαρμογής των κατάλληλων μέτρων για την αντιμετώπισή τους.

Τέλος, ο έλεγχος **SA-10** αναφέρεται στον έλεγχο της χρήσης των προνομιακών δικαιωμάτων στα συστήματα και το λογισμικό, περιλαμβανομένων των διαδικασιών εξουσιοδότησης και ελέγχου της πρόσβασης.

<u>Παράδειγμα Υλοποίησης 6</u>
<u>Προστατευτική Τεχνολογία (PR.PT)</u>

Η τεχνολογία προστασίας (PR.PT) αναφέρεται στη διαχείριση των τεχνικών λύσεων ασφαλείας για τη διασφάλιση της ασφάλειας και ανθεκτικότητας συστημάτων και περιουσιακών στοιχείων, συνεπώς με τα σχετικά πολιτικά, διαδικαστικά και συμβατικά πλαίσια που διέπουν αυτά τα συστήματα και περιουσιακά στοιχεία. Η τεχνολογία προστασίας (PR.PT) αποτελεί μια σημαντική πτυχή της κυβερνοασφάλειας και περιλαμβάνει τη χρήση τεχνικών λύσεων για την προστασία των συστημάτων και των δεδομένων από διάφορες απειλές ασφαλείας, όπως ιοί, κακόβουλο λογισμικό, διαρροές δεδομένων και επιθέσεις από χάκερ. Η διαχείριση της τεχνολογίας προστασίας περιλαμβάνει την επιλογή, την εγκατάσταση και τη συντήρηση των απαραίτητων τεχνικών λύσεων ασφαλείας, όπως προγράμματα αντιικού λογισμικού, firewall και άλλες

τεχνολογίες ασφαλείας, που θα διασφαλίσουν την ανθεκτικότητα των συστημάτων και των δεδομένων σε περίπτωση επιθέσεων ή άλλων απειλών.

Υποκατηγορία Πλαισίου Κυβερνοασφάλειας PR.PT-3

Η αρχή της ελάχιστης λειτουργικότητας (principle of least functionality) αναφέρεται στη διαμόρφωση των συστημάτων ώστε να παρέχουν μόνο τις απαραίτητες λειτουργίες και δυνατότητες, αποφεύγοντας έτσι την παροχή περιττών ή λειτουργιών που ενδέχεται να δημιουργήσουν επιπλέον ευπάθειες στο σύστημα και να δυσχεράνουν τη διαχείριση της ασφάλειας.

Με την εφαρμογή αυτής της αρχής, τα συστήματα διαμορφώνονται μόνο με τις απαραίτητες λειτουργίες για την εκτέλεση των εργασιών τους και τίποτα παραπάνω. Αυτό σημαίνει ότι παρέχονται μόνο οι δυνατότητες που είναι απαραίτητες για τη λειτουργία του συστήματος και την εκτέλεση των εργασιών του χρήστη, χωρίς να επιτρέπονται πρόσβαση ή λειτουργίες που δεν είναι απαραίτητες ή που μπορεί να προκαλέσουν επιπλέον ευπάθειες.

Όπως στην υποκατηγορία πλαισίου κυβερνοασφάλειας PR.IP-3 ομοίως στην **PR.PT-3** αναφέρονται οι έλεγχοι **CIS CSC 3** και **11** με στόχο την εφαρμογή τεχνικών ελέγχων και πρακτικών για την ανάκτηση δεδομένων αντίστοιχα. Επιπλέον η χρήση της πρακτικής ασφάλειας **CIS CSC 14** συνεισφέρει στην σχεδίαση της εξάλειψης των επιθέσεων των δικτύων μέσω της εφαρμογής συστημάτων ελέγχου ασφάλειας.

Η CIS **CSC 14** επικεντρώνεται στην ανίχνευση και την πρόληψη των επιθέσεων μέσω της παρακολούθησης και της ανίχνευσης ασυνήθιστων δραστηριοτήτων στα δίκτυα. Η πρακτική σύσταση περιλαμβάνει την εφαρμογή τεχνολογιών όπως οι ανιχνευτές ασυνήθιστης συμπεριφοράς και οι ανιχνευτές απειλών, καθώς και την εκπαίδευση του προσωπικού για την αναγνώριση και αντιμετώπιση ασυνήθιστων δραστηριοτήτων στο δίκτυο. Η εφαρμογή της CIS CSC 14 μπορεί να βοηθήσει στην αντιμετώπιση πολλών ειδών επιθέσεων, συμπεριλαμβανομένων των επιθέσεων DDoS, των επιθέσεων μελών εσωτερικού προσωπικού και των επιθέσεων χρήστη-κακόβουλου λογισμικού.

Στην υποκατηγορία εφαρμόζονται οι διαδικασίες **COBIT 5 DSS05.02, DSS05.05, DSS06.06** για την περαιτέρω ασφάλεια μέσω της διαχείρισης. Οι διαδικασίες **COBIT 5 DSS05.02, DSS05.05** και **DSS06.06** αναφέρονται στη διαχείριση της ασφάλειας των πληροφοριακών συστημάτων. Πιο συγκεκριμένα η διαδικασία **COBIT 5 DSS05.02** αφορά στη διαχείριση της πολιτικής ασφαλείας της πληροφορίας στην οργάνωση. Αυτό περιλαμβάνει τη διαμόρφωση των απαιτήσεων ασφαλείας, τη δημιουργία πολιτικών ασφαλείας και την επικύρωση αυτών των πολιτικών από την ανώτερη διοίκηση της οργάνωσης. Από την άλλη η διαδικασία **COBIT 5 DSS05.05** διαχειρίζεται την ασφάλεια των δικτύων μέσω της εφαρμογής μέτρων ασφάλειας για την προστασία της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των δεδομένων που

διακινούνται μέσω των δικτύων. Η διαδικασία αυτή αναγνωρίζει των κινδύνων ασφαλείας των δικτύων, αναπτύσσει και εφαρμόζει πολιτικές και διαδικασίες ασφάλειας και διασφαλίζει τη συμμόρφωση με τα πρότυπα ασφάλειας και τους νόμους που διέπουν την ασφάλεια των δικτύων. Εν κατακλείδι η διαδικασία **COBIT 5 DSS06.06** αφορά στη διαχείριση της ασφάλειας των εφαρμογών στην οργάνωση. Αυτό περιλαμβάνει τη διαμόρφωση των απαιτήσεων ασφαλείας για τις εφαρμογές, την ανάπτυξη και τη διαχείριση των πολιτικών και διαδικασιών ασφαλείας για τις εφαρμογές, καθώς και την επιλογή, εγκατάσταση και ρύθμιση των κατάλληλων τεχνολογικών μέσων ασφαλείας για τις εφαρμογές. Περιλαμβάνει επίσης την αξιολόγηση των εφαρμογών ως προς την ασφάλεια, τη διαχείριση των ευαίσθητων δεδομένων και την παρακολούθηση των αποτελεσμάτων των δράσεων ασφαλείας στις εφαρμογές. Η διαδικασία αυτή επιτρέπει στην οργάνωση να διασφαλίζει ότι οι εφαρμογές τηρούν τα πρότυπα ασφαλείας και ότι τα δεδομένα των χρηστών είναι ασφαλή. Επιπλέον, βοηθά στην αναγνώριση των αδυναμιών ασφαλείας και στη λήψη μέτρων για τη βελτίωση της ασφάλειας των εφαρμογών. Η διαδικασία αυτή συμβάλλει στη διασφάλιση ότι οι εφαρμογές είναι ασφαλείς και προστατεύουν τα δεδομένα των χρηστών από απειλές και επιθέσεις.

Η σειρά προτύπων **ISA 62443** που αφορά την ασφάλεια των συστημάτων ελέγχου αναφέρεται στην υποκατηγορία PR.PT-3 και πιο συγκεκριμένα οι εξής κωδικοί :

4.3.3.5.1: Ανίχνευση και αντιμετώπιση κινδύνων από κακόβουλο λογισμικό στα συστήματα ελέγχου και αυτοματισμού.

4.3.3.5.2: Αποφυγή ανεπιθύμητων επιπτώσεων από απρόσεκτη χρήση συστημάτων ελέγχου και αυτοματισμού.

4.3.3.5.3: Αποφυγή ανεπιθύμητων επιπτώσεων από μη αποδεκτές ενέργειες στα συστήματα ελέγχου και αυτοματισμού.

4.3.3.5.4: Περιορισμός της πρόσβασης σε ευαίσθητες λειτουργίες των συστημάτων ελέγχου και αυτοματισμού.

4.3.3.5.5: Ασφάλεια των διασυνδέσεων μεταξύ των συστημάτων ελέγχου και αυτοματισμού και τους υπόλοιπους υπολογιστικούς πόρους.

4.3.3.5.6: Αποτροπή απόρριψης των υπηρεσιών των συστημάτων ελέγχου και αυτοματισμού από κακόβουλη ενέργεια ή κακόβουλο λογισμικό.

4.3.3.5.7: Παρακολούθηση της απόδοσης των συστημάτων ελέγχου και αυτοματισμού και επίλυση προβλημάτων που αφορούν την απόδοση αυτή.

4.3.3.5.8: Εφαρμογή αυθεντικοποίησης και εξουσιοδότησης για την αποτροπή μη εξουσιοδοτημένης πρόσβασης στα συστήματα ελέγχου.

4.3.3.6.1: Καθορισμός των απαιτήσεων ασφαλείας για τα συστήματα ελέγχου και αυτοματισμού.

4.3.3.6.2: Ανάλυση των κινδύνων και των απειλών που μπορεί να αντιμετωπίσουν τα συστήματα ελέγχου και αυτοματισμού και καθορισμός των αντίστοιχων μέτρων ασφαλείας για την αντιμετώπισή τους.

4.3.3.6.3: Καθορισμός των απαιτήσεων αποκατάστασης για τα συστήματα ελέγχου και αυτοματισμού σε περίπτωση αποτυχίας ή παραβίασης της ασφάλειας.

4.3.3.6.4: Ορισμός των απαιτήσεων αποκατάστασης για τα συστήματα επεξεργασίας δεδομένων σε περίπτωση αποτυχίας ή παραβίασης της ασφάλειας.

4.3.3.6.5: Καθορισμός των απαιτήσεων αποκατάστασης για τα συστήματα αποθήκευσης δεδομένων σε περίπτωση αποτυχίας ή παραβίασης της ασφάλειας.

4.3.3.6.6: Καθορισμός των απαιτήσεων αποκατάστασης για τα συστήματα επικοινωνίας σε περίπτωση αποτυχίας ή παραβίασης της ασφάλειας.

4.3.3.6.7: Ορισμός των απαιτήσεων αποκατάστασης για τα φυσικά συστήματα (π.χ. κτίρια, εξοπλισμός, εγκαταστάσεις) σε περίπτωση αποτυχίας ή παραβίασης της ασφάλειας.

4.3.3.6.8: Καθορισμός των απαιτήσεων αποκατάστασης για τα συστήματα ενέργειας σε περίπτωση αποτυχίας ή παραβίασης της ασφάλειας.

4.3.3.6.9: Ορισμός των απαιτήσεων αποκατάστασης για τα συστήματα κίνησης (π.χ. μεταφοράς υλικών, μετακινήσεων προσωπικού) σε περίπτωση αποτυχίας.

4.3.3.7.1: διαχείριση των αδυναμιών και των ευπαθειών του συστήματος κίνησης.

4.3.3.7.2: παρακολούθηση της κατάστασης του συστήματος κίνησης και στη διαχείριση των δεδομένων που συλλέγονται.

4.3.3.7.3: αναφέρεται στην εφαρμογή διαδικασιών ασφαλείας για την αντιμετώπιση παραβιάσεων.

4.3.3.7.4: περιγράφεται η ανάγκη να διατηρείται κατάλληλη τεκμηρίωση των διαδικασιών ασφαλείας που εφαρμόζονται.

Η **ISA 62443-3-3:2013** είναι μια προδιαγραφή που αφορά την ασφάλεια συστημάτων ελέγχου διαδικτύου και αναφέρονται ορισμένοι κωδικοί στην υποκατηγορία PR.PT-3:

SR 1.1: Ορισμός απαιτήσεων ασφαλείας για το σύστημα ελέγχου.
SR 1.2: Περιγραφή της διαδικασίας αξιολόγησης ασφαλείας.
SR 1.3: Ορισμός του επιπέδου αξιολόγησης ασφαλείας.
SR 1.4: Περιγραφή της αναφοράς αξιολόγησης ασφαλείας.
SR 1.5: Ορισμός των απαιτήσεων ασφαλείας για την αποθήκευση και τη μεταφορά των δεδομένων.
SR 1.6: Καθορισμός των απαιτήσεων ασφαλείας για την αυθεντικοποίηση και την εξουσιοδότηση των χρηστών.
SR 1.7: Ορισμός των απαιτήσεων ασφαλείας για τον έλεγχο πρόσβασης.
SR 1.8: Ορισμός των απαιτήσεων ασφαλείας για τη διαχείριση κλειδιών κρυπτογράφησης.
SR 1.9: Ορισμός των απαιτήσεων ασφαλείας για την ανίχνευση και την απόκριση σε απειλές ασφάλειας
SR 1.10: Περιγραφή της διαδικασίας αξιολόγησης αξιοπιστίας του συστήματος ελέγχου.
SR 1.11: Καθορισμός του επιπέδου αξιολόγησης αξιοπιστίας.
SR 1.12: Περιγραφή της αναφοράς αξιολόγησης αξιοπιστίας.

SR 1.13: Ορισμός των απαιτήσεων αξιοπιστίας για το σύστημα ελέγχου.
SR 2.1: Ορισμός της ανάγκης για ανάλυση κινδύνων και αξιολόγησης ασφαλείας. **SR 2.2**: Περιγραφή της διαδικασίας ανάλυσης κινδύνων.
SR 2.3: Περιγραφή της διαδικασίας αξιολόγησης ασφαλείας.
SR 2.4: Ορισμός των απαιτήσεων ασφαλείας για την προστασία της διαδικτυακής επικοινωνίας.
SR 2.5: Ορισμός των απαιτήσεων ασφαλείας για την προστασία των ευαίσθητων δεδομένων.
SR 2.6: Ορισμός των απαιτήσεων ασφαλείας για τη διαχείριση των κλειδιών κρυπτογράφησης.
SR 2.7: Καθορισμός των απαιτήσεων ασφαλείας για τη διαχείριση των αναθέσεων στο σύστημα ελέγχου.

Η **A.9.1.2** που αναφέρεται στην υποκατηγορία είναι μια παράγραφος του κεφαλαίου Α.9 του προτύπου ISO/IEC 27001:2013, με τίτλο "Αξιολόγηση και Αντιμετώπιση των Κινδύνων Ασφαλείας των Πληροφοριακών Συστημάτων". Στο συγκεκριμένο κείμενο αναφέρεται ότι η οργάνωση πρέπει να αναπτύξει, να υλοποιήσει και να διατηρήσει διαδικασίες για την αναγνώριση και αξιολόγηση των κινδύνων ασφαλείας για τα πληροφοριακά συστήματα της οργάνωσης. Η αναγνώριση αυτών των κινδύνων πρέπει να βασίζεται σε αντικειμενικά κριτήρια και να λαμβάνει υπόψη τις ανάγκες και τους στόχους της οργάνωσης.

Τα **NIST SP 800-53 Rev. 4**, **AC-3** και **CM-7** που εφαρμόζονται είναι δύο διαφορετικές αναφορές από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology - NIST) των ΗΠΑ σχετικά με την ασφάλεια των πληροφοριακών συστημάτων. Η **AC-3** διαχειρίζεται τα κλειδιά πιστοποίησης και αποκωδικοποίησης σε ένα σύστημα πληροφορικής. Περιγράφει τις απαιτήσεις για την ασφαλή διαχείριση των κλειδιών και των πιστοποιητικών που χρησιμοποιούνται για να πιστοποιήσουν την ταυτότητα και την ασφάλεια των χρηστών στο σύστημα. Η **CM-7** αναφέρεται στη διαχείριση των δικαιωμάτων χρήσης στο σύστημα και αναλύει τις απαιτήσεις για την ασφαλή διαχείριση των δικαιωμάτων χρήσης, ώστε μόνο οι εξουσιοδοτημένοι χρήστες να έχουν πρόσβαση σε ευαίσθητες πληροφορίες και λειτουργίες του συστήματος.

Παράδειγμα Υλοποίησης 6
Συνεχής Παρακολούθηση Ασφάλειας (DE.CM)

Η **Συνεχής Παρακολούθηση Ασφάλειας** (Security Continuous Monitoring - SCM) είναι μια πρακτική κυβερνοασφάλειας που περιλαμβάνει την τακτική παρακολούθηση των συστημάτων πληροφοριών και των περιουσιακών στοιχείων ενός οργανισμού για τον εντοπισμό συμβάντων ασφαλείας και την επαλήθευση της αποτελεσματικότητας των προστατευτικών μέτρων. Αυτό περιλαμβάνει τη συλλογή και ανάλυση δεδομένων που σχετίζονται με την ασφάλεια από διάφορες πηγές, όπως αρχεία καταγραφής συστήματος, κίνηση δικτύου και σαρώσεις ευπάθειας για τον εντοπισμό ανωμαλιών, ύποπτης δραστηριότητας ή πιθανών απειλών. Το SCM δίνει τη δυνατότητα στους οργανισμούς να εντοπίζουν και να ανταποκρίνονται σε συμβάντα κυβερνοασφάλειας

εγκαίρως, μειώνοντας τον κίνδυνο ζημιάς στα συστήματα, τα δεδομένα και τη φήμη τους. Παρέχει επίσης έναν τρόπο μέτρησης της αποτελεσματικότητας των ελέγχων και των πολιτικών ασφαλείας, επιτρέποντας στους οργανισμούς να εντοπίζουν τομείς προς βελτίωση και να εφαρμόζουν διορθωτικές ενέργειες. Το SCM συνήθως περιλαμβάνει έναν συνδυασμό αυτοματοποιημένων εργαλείων, μη αυτόματων αναθεωρήσεων και αναλύσεων από εκπαιδευμένους επαγγελματίες ασφαλείας για να διασφαλιστεί ότι τα συμβάντα στον κυβερνοχώρο εντοπίζονται και διερευνώνται σωστά. Αποτελεί κρίσιμο στοιχείο ενός ολοκληρωμένου προγράμματος κυβερνοασφάλειας και βοηθά τους οργανισμούς να διατηρήσουν μια ισχυρή στάση ασφαλείας με την πάροδο του χρόνου.

<u>Υποκατηγορία Πλαισίου Κυβερνοασφάλειας PR.PT-3</u>

Το **DE.CM-8** είναι ένα στοιχείο ελέγχου στην κατηγορία "Εντοπισμός" του πλαισίου κυβερνοασφάλειας NIST (CSF) που απαιτεί από τους οργανισμούς να εκτελούν σαρώσεις ευπάθειας για τον εντοπισμό αδυναμιών στα συστήματα, τις εφαρμογές και την υποδομή δικτύου τους. Η σάρωση ευπάθειας είναι ένα προληπτικό μέτρο που βοηθά τους οργανισμούς να εντοπίσουν πιθανές ευπάθειες ασφαλείας προτού μπορέσουν να τις εκμεταλλευτούν οι εισβολείς. Η σάρωση ευπάθειας είναι μια συστηματική ανασκόπηση της υποδομής, των εφαρμογών και των συσκευών πληροφορικής ενός οργανισμού για τον εντοπισμό πιθανών αδυναμιών ασφάλειας. Οι σαρωτές ευπάθειας είναι αυτοματοποιημένα εργαλεία που χρησιμοποιούν ένα σύνολο προκαθορισμένων δοκιμών για τον εντοπισμό γνωστών τρωτών σημείων και σφαλμάτων διαμόρφωσης σε συστήματα, εφαρμογές και συσκευές δικτύου. Αυτά τα εργαλεία μπορούν επίσης να αξιολογήσουν τη σοβαρότητα των εντοπισμένων τρωτών σημείων και να παρέχουν συστάσεις για τον τρόπο αποκατάστασής τους. Εκτελώντας τακτικές σαρώσεις ευπάθειας, οι οργανισμοί μπορούν να εντοπίσουν και να ιεραρχήσουν πιθανές αδυναμίες ασφάλειας, να αξιολογήσουν το επίπεδο κινδύνου και να λάβουν τα κατάλληλα μέτρα για την αποκατάστασή τους. Αυτό μπορεί να περιλαμβάνει την εφαρμογή ενημερώσεων κώδικα λογισμικού, την ενημέρωση των διαμορφώσεων ή την εφαρμογή πρόσθετων ελέγχων ασφαλείας για τον μετριασμό των εντοπισμένων κινδύνων. Η σάρωση ευπάθειας θα πρέπει να διεξάγεται τακτικά, ιδανικά σε προγραμματισμένη βάση, ώστε να διασφαλίζεται ότι τα νέα τρωτά σημεία εντοπίζονται το συντομότερο δυνατό. Είναι σημαντικό να σημειωθεί ότι η σάρωση ευπάθειας είναι μόνο ένα στοιχείο ενός ολοκληρωμένου προγράμματος ασφάλειας και θα πρέπει να χρησιμοποιείται σε συνδυασμό με άλλα μέτρα ασφαλείας, όπως η δοκιμή διείσδυσης και η εκπαίδευση ευαισθητοποίησης σχετικά με την ασφάλεια, για να διασφαλιστεί η συνολική αποτελεσματικότητα του προγράμματος.

CIS CSC σημαίνει Κέντρο για κρίσιμους ελέγχους ασφάλειας στο Διαδίκτυο και αναφέρεται στην PR.PT-3. Εφαρμόζονται δύο αναφορές η **CIS CSC 4** και την **CIS CSC 20**. Το **CIS CSC 4** εστιάζει στη συνεχή διαχείριση τρωτών σημείων, η οποία περιλαμβάνει τον εντοπισμό, την ιεράρχηση και την αντιμετώπιση των τρωτών σημείων στα συστήματα και τις εφαρμογές ενός οργανισμού. Αυτός ο έλεγχος περιλαμβάνει διαδικασίες για τακτική σάρωση και επιδιόρθωση ευπάθειας, καθώς και αποκατάσταση ευπάθειας και εκτίμηση κινδύνου. Ο στόχος αυτού του ελέγχου είναι να μειώσει την επιφάνεια επίθεσης ενός οργανισμού και να μετριάσει τον κίνδυνο εκμετάλλευσης από τους επιτιθέμενους. Το **CIS CSC 20**, από την άλλη πλευρά, επικεντρώνεται στη δημιουργία ενός προγράμματος ευαισθητοποίησης και εκπαίδευσης για την ασφάλεια των εργαζομένων. Αυτός ο έλεγχος αναγνωρίζει ότι το ανθρώπινο λάθος είναι ένας σημαντικός παράγοντας που συμβάλλει σε συμβάντα ασφάλειας και στοχεύει στον μετριασμό αυτού του κινδύνου παρέχοντας στους υπαλλήλους εκπαίδευση ευαισθητοποίησης σχετικά με την ασφάλεια. Ο έλεγχος περιλαμβάνει στοιχεία όπως πολιτικές και διαδικασίες ασφαλείας, εκπαίδευση ευαισθητοποίησης σχετικά με την ασφάλεια και περιοδικές δοκιμές για τη μέτρηση της αποτελεσματικότητας του προγράμματος.

Επίσης αναφέρεται το **BAI03.10** που είναι ένας στόχος ελέγχου εντός του τομέα "Δημιουργία, Απόκτηση και Εφαρμογή" (BAI) του COBIT 5. Σχετίζεται με την εφαρμογή μιας διαδικασίας διαχείρισης αλλαγών για να διασφαλιστεί ότι οι αλλαγές στα συστήματα και την υποδομή πληροφορικής έχουν σχεδιαστεί, εγκριθεί σωστά και σωστά. δοκιμασμένο. Συγκεκριμένα, αυτός ο στόχος ελέγχου απαιτεί όλες οι αλλαγές στα συστήματα και την υποδομή πληροφορικής να τεκμηριώνονται, να ελέγχονται, να εγκρίνονται και να εφαρμόζονται με ελεγχόμενο τρόπο. Απαιτεί επίσης να κοινοποιούνται δεόντως οι αλλαγές σε όλους τους σχετικούς ενδιαφερόμενους φορείς και να εντοπίζονται και να διαχειρίζονται τυχόν σχετικοί κίνδυνοι. Παράλληλα εμφανίζεται η εφαρμογή του **DSS05.01** που είναι ένας στόχος ελέγχου εντός του τομέα "Παράδοση, εξυπηρέτηση και υποστήριξη" (DSS) του COBIT 5. Σχετίζεται με τη δημιουργία ενός πλαισίου διαχείρισης ασφάλειας για τη διασφάλιση ότι τα περιουσιακά στοιχεία πληροφοριών προστατεύονται από μη εξουσιοδοτημένη πρόσβαση, χρήση, αποκάλυψη, διακοπή, τροποποίηση ή καταστροφή. Συγκεκριμένα, αυτός ο στόχος ελέγχου απαιτεί να δημιουργηθεί, να τεκμηριωθεί, να κοινοποιείται και να επανεξετάζεται τακτικά ένα πλαίσιο διαχείρισης ασφάλειας, ώστε να διασφαλίζεται ότι είναι αποτελεσματικό στον μετριασμό των κινδύνων για τα περιουσιακά στοιχεία πληροφοριών. Απαιτεί επίσης την εφαρμογή ελέγχων ασφαλείας για την προστασία των στοιχείων του ενεργητικού και ότι τα περιστατικά και τα τρωτά σημεία εντοπίζονται κατάλληλα, αξιολογούνται και αντιμετωπίζονται έγκαιρα.

Από το πρότυπο ISA 62443-2-1:2009 για την περαιτέρω ασφάλεια εμφανίζονται τα τμήματα **4.2.3.1** και **4.2.3.7**. Το **4.2.3.1** είναι ένα τμήμα του προτύπου που εστιάζει στον έλεγχο πρόσβασης για το IACS. Συγκεκριμένα, απαιτεί η πρόσβαση στο IACS να ελέγχεται και να περιορίζεται σε εξουσιοδοτημένα άτομα, συσκευές και εφαρμογές. Αυτό περιλαμβάνει τη χρήση μηχανισμών ελέγχου ταυτότητας και εξουσιοδότησης για την επαλήθευση της ταυτότητας και των προνομίων των χρηστών και συσκευών που έχουν πρόσβαση στο IACS. Απαιτεί επίσης τη χρήση στοιχείων ελέγχου φυσικής πρόσβασης για την αποτροπή μη εξουσιοδοτημένης φυσικής πρόσβασης σε εξαρτήματα και συσκευές IACS. Το **4.2.3.7** είναι ένα άλλο τμήμα του προτύπου που σχετίζεται με τη διαχείριση συμβάντων και ευπάθειας για το IACS. Αυτή η ενότητα απαιτεί από το IACS να διαθέτει μια διαδικασία για τον εντοπισμό, την αξιολόγηση και τον μετριασμό των συμβάντων και των τρωτών σημείων ασφαλείας. Αυτό περιλαμβάνει την εφαρμογή ελέγχων ασφαλείας και τη χρήση εργαλείων παρακολούθησης ασφαλείας για τον εντοπισμό και την απόκριση σε συμβάντα ασφαλείας. Απαιτεί επίσης το IACS να διαθέτει μια διαδικασία για την αναφορά περιστατικών και τρωτών σημείων ασφάλειας σε σχετικά ενδιαφερόμενα μέρη, όπως ιδιοκτήτες συστημάτων, χειριστές και ρυθμιστικές αρχές.

Το ISO/IEC 27001:2013 είναι ένα πρότυπο για συστήματα διαχείρισης ασφάλειας πληροφοριών (ISMS). Παρέχει ένα πλαίσιο για τη δημιουργία, εφαρμογή, συντήρηση και συνεχή βελτίωση του ISMS ενός οργανισμού. Το **A.12.6.1** είναι ένας έλεγχος εντός του Παραρτήματος Α του προτύπου που σχετίζεται με τη διαχείριση τεχνικών τρωτών σημείων. Συγκεκριμένα, αυτός ο έλεγχος απαιτεί από τους οργανισμούς να καθιερώσουν, να εφαρμόσουν και να διατηρήσουν μια διαδικασία για τον εντοπισμό και την αντιμετώπιση τεχνικών τρωτών σημείων στα πληροφοριακά τους συστήματα. Αυτή η διαδικασία θα πρέπει να περιλαμβάνει τον τακτικό εντοπισμό και την αξιολόγηση τεχνικών τρωτών σημείων στα πληροφοριακά συστήματα του οργανισμού, χρησιμοποιώντας συνδυασμό αυτοματοποιημένων εργαλείων και μη αυτόματων δοκιμών. Περιλαμβάνει την προτεραιότητα των τεχνικών τρωτών σημείων με βάση τη σοβαρότητά τους και τον πιθανό αντίκτυπό τους στην ασφάλεια πληροφοριών του οργανισμού και την εφαρμογή κατάλληλων ελέγχων για την αντιμετώπιση των εντοπισμένων τεχνικών τρωτών σημείων, όπως ενημερώσεις κώδικα, ενημερώσεις ή άλλες ενέργειες αποκατάστασης. Ο στόχος αυτού του ελέγχου

είναι να διασφαλίσει ότι τα συστήματα πληροφοριών του οργανισμού προστατεύονται από γνωστά τρωτά σημεία που θα μπορούσαν να εκμεταλλευτούν οι εισβολείς για να θέσουν σε κίνδυνο την εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα των πληροφοριών του οργανισμού. Εφαρμόζοντας αυτόν τον έλεγχο, οι οργανισμοί μπορούν να μειώσουν τον κίνδυνο συμβάντων ασφαλείας και να προστατεύσουν τα στοιχεία των πληροφοριών τους από μη εξουσιοδοτημένη πρόσβαση, τροποποίηση ή αποκάλυψη.

Τέλος αναφέρεται το **RA-5** του πλαισίου NIST SP 800-53 Rev. 4. Το **RA-5** είναι ένα στοιχείο ελέγχου εντός του πλαισίου που σχετίζεται με τη σάρωση ευπάθειας. Συγκεκριμένα, απαιτεί από τους οργανισμούς να εκτελούν σαρώσεις ευπάθειας στα πληροφοριακά τους συστήματα για να εντοπίσουν και να αποκαταστήσουν αδυναμίες ή ελαττώματα ασφαλείας στα συστήματα. Ο έλεγχος περιγράφει τη συχνότητα των σαρώσεων ευπάθειας που πρέπει να καθορίζεται από τη στρατηγική διαχείρισης κινδύνου του οργανισμού και να βασίζεται στην κρισιμότητα του συστήματος και την πιθανότητα και τον πιθανό αντίκτυπο των απειλών. Με την εφαρμογή του RA-5, οι οργανισμοί μπορούν να μειώσουν τον κίνδυνο συμβάντων ασφαλείας και να προστατεύσουν τα συστήματα πληροφοριών και τα δεδομένα τους από μη εξουσιοδοτημένη πρόσβαση, τροποποίηση ή αποκάλυψη. Η σάρωση ευπάθειας είναι ένα ουσιαστικό συστατικό οποιουδήποτε αποτελεσματικού προγράμματος ασφάλειας πληροφοριών, καθώς επιτρέπει στους οργανισμούς να εντοπίζουν και να αποκαθιστούν προληπτικά τις αδυναμίες ασφαλείας προτού τις εκμεταλλευτούν οι εισβολείς.

ΚΕΦΑΛΑΙΟ 4
ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ

4.1 Ευρήματα

Με τη χρήση του MUD σε οικιακά και μικρά δίκτυα επιχειρήσεων, μπορεί να επιτευχθεί ένα πολύ υψηλό επίπεδο ασφάλειας για τις συσκευές IoT που χρησιμοποιούνται σε αυτά τα δίκτυα. Αυτό επιτυγχάνεται με την περιορισμό των επικοινωνιών των συσκευών IoT, οι οποίες είναι οι πιο ευάλωτες σε κυβερνοεπιθέσεις. Έτσι, μπορεί να εξασφαλιστεί ότι μόνο επικοινωνίες που έχουν επιτραπεί είναι αποδεκτές, μειώνοντας τον κίνδυνο από κακόβουλα λογισμικά και επιθέσεις.

Το MUD είναι σχεδιασμένο για να προστατεύει συσκευές IoT που έχουν συγκεκριμένες ανάγκες επικοινωνίας, όπως οι θύρες και τα πρωτόκολλα που μπορούν να χρησιμοποιήσουν και οι προορισμοί που μπορούν να επικοινωνήσουν. Εάν μια συσκευή δεν είναι συσκευή IoT με συγκεκριμένες ανάγκες επικοινωνίας, τότε δεν μπορεί να προστατευτεί από το MUD. Παραδείγματα τέτοιων συσκευών είναι φορητοί υπολογιστές και τηλέφωνα.

Η απόδειξη του MUD είναι ότι μπορεί να χρησιμοποιηθεί σε δίκτυα που υποστηρίζουν MUD, για να διαχειριστεί την πρόσβαση σε συσκευές IoT με δυνατότητα MUD, διατηρώντας παράλληλα την λειτουργικότητα των συσκευών. Η προσέγγιση αναφέρεται στον τρόπο διαχείρισης της πρόσβασης σε συσκευές IoT με δυνατότητα MUD σε δίκτυα με υποστήριξη για MUD. Η χρήση τέτοιων συσκευών επιτρέπει την αποτροπή πρόσβασης σε αυτές από μη εξουσιοδοτημένες συσκευές εντός του ίδιου δικτύου και τη χρήση των συσκευών IoT με δυνατότητα MUD για πρόσβαση σε μη εξουσιοδοτημένους εξωτερικούς τομείς. Παράλληλα αποτρέπεται η πρόσβασή τους σε άλλες μη εξουσιοδοτημένες συσκευές εντός του ίδιου δικτύου. Συνολικά, ο στόχος είναι η διατήρηση της λειτουργικότητας των συσκευών IoT με δυνατότητα MUD ενώ παράλληλα διασφαλίζεται η ασφαλής τους χρήση.

Η τεχνολογία MUD μπορεί να βοηθήσει στην αποτροπή της χρήσης συσκευών IoT για επιθέσεις DDoS και άλλες επιθέσεις στο δίκτυο. Για να επιτευχθεί αυτό, οι συσκευές IoT πρέπει να διαθέτουν τη δυνατότητα MUD και τα αρχεία MUD πρέπει να είναι διαθέσιμα για αυτές τις συσκευές. Τα αρχεία MUD καθορίζουν ποιες επικοινωνίες μπορούν να πραγματοποιήσουν οι συσκευές IoT, με στόχο να διατηρηθεί η λειτουργικότητα τους και να αποτραπεί η χρήση τους για επιθέσεις. Τέλος, η σωστή χρήση του MUD μπορεί να βοηθήσει στην ασφάλεια των δικτύων μικρών επιχειρήσεων και στα σημερινά οικιακά δίκτυα.

Υπάρχουν τεχνολογίες παρακολούθησης δικτύου που μπορούν να εντοπίζουν τις συσκευές που είναι συνδεδεμένες σε ένα δίκτυο και να παρέχουν πληροφορίες για τα χαρακτηριστικά τους. Αυτές οι τεχνολογίες μπορούν να εντοπίζουν πότε οι συσκευές αποσυνδέονται ή απενεργοποιούνται και να καταγράφουν αλλαγές στην κατάστασή τους. Η συνεχής παρακολούθηση της ασφάλειας των συσκευών στο δίκτυο είναι σημαντική για να διατηρείται η ασφάλεια των πληροφοριών και να αναγνωρίζονται εγκαίρως πιθανές απειλές για την ασφάλεια του οργανισμού.

Για να επιτραπεί στους τυπικούς χρήστες να αναπτύξουν εύκολα ένα MUD στο δίκτυό τους, η εγκατάσταση και η διαμόρφωση των απαραίτητων στοιχείων πρέπει να είναι απλές και φιλικές προς το χρήστη. Υπάρχουν κάποιες εκδόσεις του MUD που είναι plug-and-play και μπορούν να αναπτυχθούν εύκολα, αλλά άλλες εκδόσεις απαιτούν περισσότερη τεχνική γνώση. Είναι σημαντικό να εστιαστεί στην ευκολία χρήσης, ώστε να επιτραπεί η ευρεία χρήση του MUD σε οικιακά και μικρά επιχειρηματικά δίκτυα.

Το MUD μπορεί να βοηθήσει με την ασφάλεια των συσκευών IoT που έχουν διακοπεί και δεν λαμβάνουν πλέον τακτικές ενημερώσεις. Τελικά, οι περισσότερες συσκευές IoT θα φτάσουν σε ένα σημείο όπου δεν θα ενημερώνονται πλέον από τους κατασκευαστές τους. Αυτό είναι ένα επικίνδυνο σημείο στον κύκλο ζωής οποιασδήποτε συσκευής, διότι σημαίνει ότι τυχόν ευπάθειες ασφαλείας που γίνονται γνωστές μετά από αυτό το σημείο δεν θα προστατεύονται, αφήνοντας τη συσκευή ανοιχτή σε επιθέσεις. Στο μέλλον, αναμένεται να υπάρχουν πολλές συσκευές IoT που δεν θα ενημερώνονται πλέον από τους κατασκευαστές τους, αλλά θα συνεχίσουν να χρησιμοποιούνται. Η δυνατότητα αξιοποίησης του MUD για τον περιορισμό του προφίλ επικοινωνίας τέτοιων μη υποστηριζόμενων συσκευών θα είναι σημαντική για την προστασία των δικτύων και την πρόληψη επιθέσεων.

Οι διασυνδέσεις μεταξύ των συστημάτων MUD και των άλλων συστημάτων, όπως οι δρομολογητές/διακόπτες και οι διακομιστές σηματοδότησης απειλών, δεν έχουν καθορισμένο πρότυπο. Αυτό μπορεί να δυσχεράνει τη διασύνδεση των συστημάτων που προέρχονται από διαφορετικούς κατασκευαστές, καθιστώντας δύσκολη την ενσωμάτωση αρχιτεκτονικών στοιχείων από διαφορετικούς προμηθευτές στις αναπτύξεις MUD των καταναλωτών.

Το **RFC 8520** που χρησιμοποιείται περιγράφει τον τρόπο με τον οποίο οι διαχειριστές συσκευών δικτύου μπορούν να χρησιμοποιήσουν ένα Προφίλ Χαρακτηριστικών Χρήσης (MUD) για να περιορίσουν τις δυνατότητες των συνδεδεμένων συσκευών στο δίκτυο. Ο MUD είναι ένα αρχείο που περιγράφει τις επιτρεπόμενες λειτουργίες για μια συγκεκριμένη συσκευή, όπως ένα router ή ένα IoT συσκευή. Η κρυφή μνήμη αποτελεί ένα κρίσιμο στοιχείο για τη λειτουργία του MUD στο πραγματικό δίκτυο. Συγκεκριμένα, όταν μια συσκευή προσπαθεί να συνδεθεί στο δίκτυο, ο διαχειριστής του δικτύου ελέγχει το MUD αρχείο για να εξασφαλίσει ότι η συσκευή που προσπαθεί να συνδεθεί έχει τις επιτρεπόμενες λειτουργίες. Εάν ο διαχειριστής έχει ήδη ελέγξει τη συγκεκριμένη συσκευή πριν, μπορεί να αποθηκεύσει μια κρυφή μνήμη με τις επιτρεπόμενες λειτουργίες της συσκευής, για να μην επαναλαμβάνει τον έλεγχο του MUD αρχείου σε κάθε σύνδεση.

Οι κανόνες MUD χρησιμοποιούν ονόματα τομέα για να περιγράψουν ποια συσκευή επιτρέπεται να επικοινωνήσει με ποιους παρόχους υπηρεσιών. Αλλά όταν αυτοί οι κανόνες εφαρμόζονται στους δρομολογητές, χρησιμοποιούνται διευθύνσεις IP αντί για ονόματα τομέα. Αυτό μπορεί να δημιουργήσει προβλήματα, διότι η διεύθυνση IP στην οποία επιλύεται ένας τομέας μπορεί να αλλάξει. Έτσι, μπορεί να συμβεί ότι μια συσκευή δεν μπορεί να επικοινωνήσει με έναν επιθυμητό τομέα, ακόμα και αν ο κανόνας από το αρχείο MUD της συσκευής επιτρέπει αυτήν την επικοινωνία. Αυτό συμβαίνει επειδή τα φίλτρα κυκλοφορίας στο δρομολογητή είναι προγραμματισμένα να επιτρέπουν την πρόσβαση σε μια συγκεκριμένη διεύθυνση IP για αυτήν τη συσκευή, και όχι σε μια νέα διεύθυνση IP που επιστρέφεται τώρα για τον τομέα. Όταν μια συσκευή συνδέεται στο δίκτυο, μπορεί να έχει πρόσβαση σε συγκεκριμένες διευθύνσεις IP που επιτρέπονται από το δρομολογητή ή το διακόπτη. Ωστόσο, αν οι διευθύνσεις IP για αυτούς τους τομείς αλλάξουν, η συσκευή δεν θα μπορεί πλέον να συνδεθεί σε αυτούς τους τομείς. Για να αντιμετωπιστεί αυτό το πρόβλημα, η υλοποίηση MUD θα πρέπει να κάνει αιτήματα ανάλυσης DNS περιοδικά για τους τομείς που αναφέρονται στο αρχείο MUD. Αν οι διευθύνσεις IP έχουν αλλάξει, τότε τα φίλτρα κυκλοφορίας στη συσκευή θα πρέπει να ενημερωθούν με τις νέες διευθύνσεις IP, ώστε η συσκευή να μπορεί να συνδεθεί και να χρησιμοποιήσει αυτούς τους τομείς κανονικά. Για να αποτραπεί η υπερφόρτωση του συστήματος, η επανεξέταση της ανάλυσης ονομάτων τομέα μπορεί να γίνεται σε συγκεκριμένα χρονικά διαστήματα, που καθορίζονται από τις ρυθμίσεις του DNS.

Προτείνεται να χρησιμοποιείτε ένα χρονικό διάστημα TTL+V για τον έλεγχο των τιμών ανάλυσης ονομάτων τομέα. Το TTL είναι η ώρα που ισχύει η τρέχουσα τιμή της καταχώρησης DNS για τον τομέα, ενώ το V είναι το επιπλέον χρονικό διάστημα που προστίθεται στο TTL. Όταν αλλάξει η διεύθυνση IP ενός τομέα, η συσκευή IoT δεν θα μπορεί να επικοινωνεί με αυτόν τον τομέα για το χρονικό διάστημα του V, μετά τη λήξη του TTL για την καταχώρηση DNS του τομέα.

Όταν μια συσκευή IoT που υποστηρίζει τεχνολογία MUD κάνει αναζήτηση για ένα όνομα τομέα, είναι σημαντικό οι διευθύνσεις IP που χρησιμοποιούνται για να επιλύσουν αυτό το όνομα τομέα να είναι οι ίδιες με αυτές που χρησιμοποιήθηκαν κατά την εγκατάσταση του κανόνα MUD που αναφέρεται σε αυτόν τον τομέα στον δρομολογητή ή διακόπτη. Αν δεν ταιριάζουν, η συσκευή ενδέχεται να αποκλειστεί από την πρόσβαση στον επιθυμητό τομέα, ακόμη και αν υπάρχει ένας κανόνας MUD που επιτρέπει στη συσκευή να τον χρησιμοποιήσει. Στην περίπτωση που ο δρομολογητής ή ο διακόπτης αναζητά ένα όνομα τομέα όταν είναι εγκατεστημένος ο κανόνας MUD και εάν η συσκευή και ο δρομολογητής ή ο διακόπτης βρίσκονται μαζί, τότε η συσκευή και ο δρομολογητής ή ο διακόπτης θα βρίσκονται στην ίδια περιοχή και θα αναμένεται να επιλυθούν οι αναζητήσεις ονομάτων τομέα τους στις ίδιες διευθύνσεις IP.

Όταν ένας διαχειριστής ή ελεγκτής στο cloud αναζητά ένα όνομα τομέα και στέλνει τα φίλτρα κυκλοφορίας σε ένα δρομολογητή ή διακόπτη για εγκατάσταση, είναι πιθανό να βρίσκονται σε διαφορετικές περιοχές, που σημαίνει ότι οι αναζητήσεις ονομάτων τομέων τους για έναν δεδομένο τομέα δεν επιλύονται στις ίδιες διευθύνσεις IP. Για να επιβληθούν οι κανόνες MUD, πρέπει να διασφαλιστεί ότι οι διευθύνσεις IP που χρησιμοποιούνται στα φίλτρα κυκλοφορίας ταιριάζουν με τις διευθύνσεις IP που θα χρησιμοποιούσε η συσκευή IoT στην πραγματικότητα. Κάποιοι τρόποι για να διασφαλιστεί η ευθυγράμμιση των διευθύνσεων είναι να δημιουργηθούν κατάλληλα φίλτρα κυκλοφορίας ή να χρησιμοποιηθούν εργαλεία διαχείρισης δικτύου για να επιτευχθεί η σωστή διαμόρφωση των συσκευών στο δίκτυο.

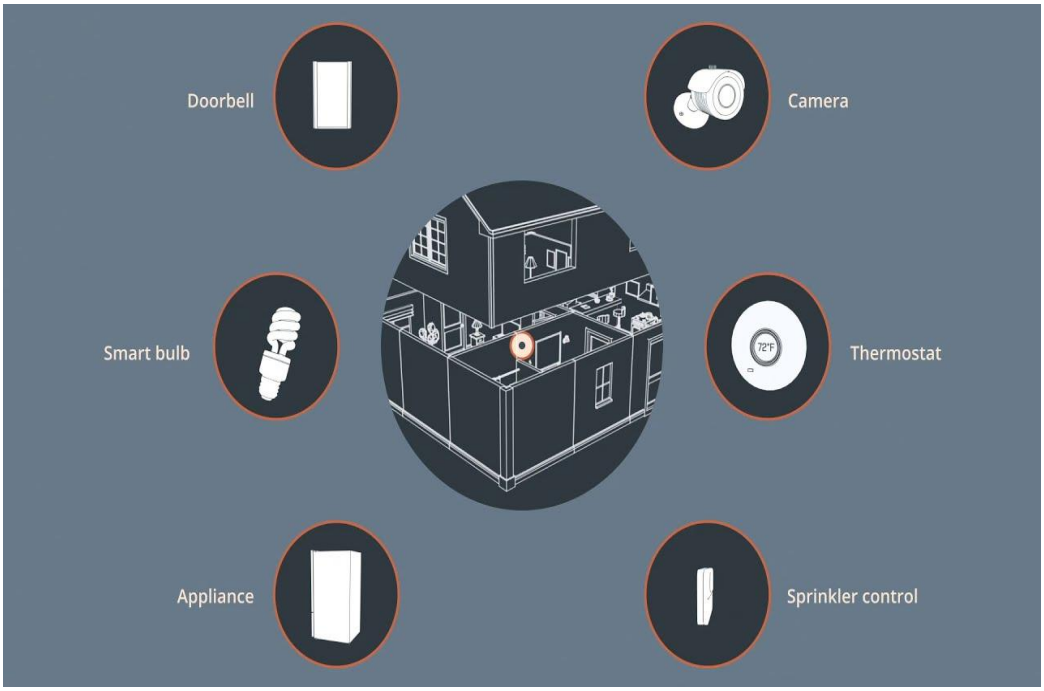
Για να διασφαλιστεί η ευθυγράμμιση των διευθύνσεων στις συσκευές IoT, μπορούν να εφαρμοστούν διάφοροι τρόποι. Κάποιοι από αυτούς είναι:

- Να απαιτείται η χρήση ενός κοινού διακομιστή DNS από τη συσκευή IoT και την οντότητα που δημιουργεί τους κανόνες MUD ως φίλτρα κυκλοφορίας, ώστε να εξασφαλιστεί ότι όλες οι συσκευές χρησιμοποιούν τις ίδιες διευθύνσεις IP.

- Να κρυφακούσουν τα ερωτήματα DNS που γίνονται από τη συσκευή IoT και να αναλύουν τις απαντήσεις DNS για να μάθουν ποιες διευθύνσεις IP λαμβάνει η συσκευή IoT, καθώς αυτό μπορεί να βοηθήσει στην αποφυγή προβλημάτων ευθυγράμμισης.

- Να στέλνουν περιοδικά ερωτήματα DNS για τη λίστα των τομέων που χρησιμοποιούνται σε αρχεία MUD και να ενημερώνουν τα φίλτρα κυκλοφορίας των συσκευών με βάση αυτά τα ερωτήματα, ώστε να διασφαλίζεται ότι οι συσκευές χρησιμοποιούν μόνο επιτρεπόμενες διευθύνσεις IP.

Το National Cybersecurity Center of Excellence (NCCoE) διαπίστωσε ότι για την ασφάλεια του Internet of Things (IoT) είναι σημαντικό να ακολουθούν οι κατασκευαστές των συσκευών IoT τις βέλτιστες πρακτικές ασφάλειας κατά το σχεδιασμό, την κατασκευή και την υποστήριξη των συσκευών τους. Πρέπει να γνωρίζουν και να διαχειρίζονται τους κινδύνους ασφαλείας και απορρήτου που ενέχουν οι συσκευές τους, όπως περιγράφονται σε ένα έγγραφο του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας (NIST) και να ακολουθούν τις κατευθυντήριες γραμμές για τον προσδιορισμό, την αξιολόγηση και τη διαχείριση κινδύνων ασφαλείας που συζητούνται στο πλαίσιο για τη βελτίωση της κυβερνοασφάλειας υποδομής ζωτικής σημασίας. Επιπλέον, οι κατασκευαστές πρέπει να υποστηρίζουν τις συσκευές τους καθ' όλη τη διάρκεια του κύκλου ζωής τους, με τακτικές ενημερώσεις κώδικα και ενημερώσεις.



Το πρωτόκολλο **Wi-Fi Easy Connect R1** ενισχύει την ασφάλεια του δικτύου IoT καθώς παρέχει σε κάθε συσκευή μοναδικά διαπιστευτήρια δικτύου. Αυτά τα διαπιστευτήρια δεν μπορούν να παρουσιαστούν από άλλες συσκευές για να αποκτήσουν πρόσβαση στο δίκτυο, ακόμα και αν είναι γνωστά. Επιπλέον, τα διαπιστευτήρια ορισμένων συσκευών μπορούν να ανακληθούν ή να αλλάξουν χωρίς να παρεμποδίζεται η δυνατότητα σύνδεσης άλλων συσκευών στο δίκτυο. Επιπλέον, τα διαπιστευτήρια δικτύου παρέχονται σε κάθε συσκευή μέσω ενός αυτοματοποιημένου και ασφαλούς πρωτοκόλλου, μειώνοντας την πιθανότητα αποκάλυψής τους. Τέλος, κανένας άνθρωπος δεν έχει τη δυνατότητα να γνωρίζει τα διαπιστευτήρια οποιασδήποτε συσκευής. Το πρωτόκολλο Wi-Fi Easy Connect είναι ένα σύστημα που βοηθά στη σύνδεση μιας συσκευής IoT στο Wi-Fi δίκτυο. Αυτό απαιτεί από ένα άτομο να ενεργοποιήσει τη συσκευή σε λειτουργία onboarding και να σκανάρει τον κωδικό QR της συσκευής. Ο σκοπός είναι να διασφαλίσει ότι η συσκευή συνδέεται με το σωστό Wi-Fi δίκτυο. Ωστόσο, αν ο χρήστης επιλέξει ένα διαφορετικό δίκτυο, μπορεί να προκληθεί επίθεση στη συσκευή IoT, και αυτό μπορεί να οδηγήσει σε ασφαλτικά προβλήματα στο δίκτυο.

Από την άλλη μεριά ένας σημαντικός κίνδυνος είναι η **επίθεση εξαγοράς** ή αλλιώς **takeover attack**. Η επίθεση εξαγοράς μπορεί να γίνει από έναν αδίστακτο επιτιθέμενο, ο οποίος θα εκμεταλλευτεί τις αδυναμίες της ασύρ Το MUD μπορεί να βοηθήσει με την ασφάλεια των

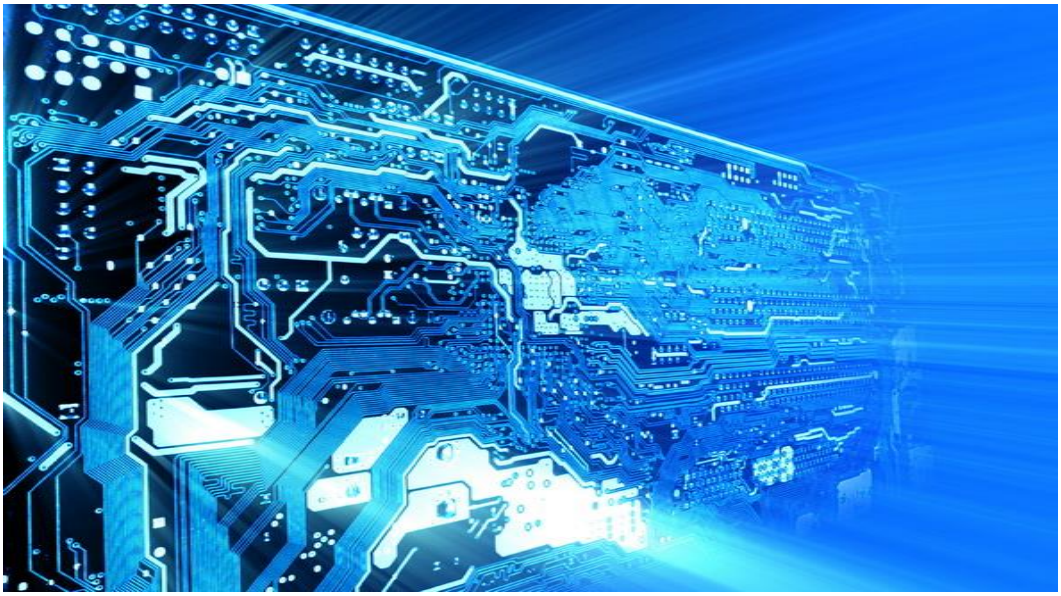
συσκευών IoT που έχουν διακοπεί και δεν λαμβάνουν πλέον τακτικές ενημερώσεις. Τελικά, οι περισσότερες συσκευές IoT θα φτάσουν σε ένα σημείο όπου δεν θα ενημερώνονται πλέον από τους κατασκευαστές τους. Αυτό είναι ένα επικίνδυνο σημείο στον κύκλο ζωής οποιασδήποτε συσκευής, διότι σημαίνει ότι τυχόν ευπάθειες ασφαλείας που γίνονται γνωστές μετά από αυτό το σημείο δεν θα προστατεύονται, αφήνοντας τη συσκευή ανοιχτή σε επιθέσεις. ματης σύνδεσης της συσκευής στο Wi-Fi, για να την ένταξει σε ένα δικτυακό περιβάλλον που ελέγχει αυτός. Ο επιτιθέμενος μπορεί να κερδίσει πρόσβαση στον κωδικό QR της συσκευής ή να αναμείνει μέχρι να τεθεί σε λειτουργία ενσωμάτωσης, για να εντάξει τη συσκευή στο δίκτυο που ελέγχει ο ίδιος, αντί στο δίκτυο που προοριζόταν αρχικά. Με αυτόν τον τρόπο, ο επιτιθέμενος μπορεί να παραβιάσει τη συσκευή και να αποκτήσει πρόσβαση σε προσωπικά δεδομένα ή να αποκλείσει τον κάτοχο της συσκευής από τη χρήση της στο προβλεπόμενο δίκτυο. Επιπλέον, ο επιτιθέμενος μπορεί να επιτρέψει την ενσωμάτωση μιας παραβιασμένης συσκευής στο προβλεπόμενο δίκτυο, με αποτέλεσμα να επιτεθεί στο δίκτυο με τη χρήση μιας παραβιασμένης συσκευής.

4.2 Θέματα Ασφάλειας

Το MUD (Manufacturer Usage Description) είναι ένα πρωτόκολλο που επιτρέπει στους κατασκευαστές συσκευών IoT να περιορίσουν τις επικοινωνίες προς και από αυτές τις συσκευές, προσδιορίζοντας ποιες πηγές και προορισμούς είναι αποδεκτοί. Αυτό μειώνει την επιθετική επιφάνεια των ευάλωτων συσκευών IoT, καθώς περιορίζει τους δυνητικούς τρόπους πρόσβασης και επιθέσεων. Ωστόσο, το MUD από μόνο του δεν παρέχει πλήρη ασφάλεια για τις συσκευές IoT. Αν ένα αρχείο MUD επιτρέπει σε μια συσκευή να επικοινωνεί με κακόβουλους πόρους, αυτό μπορεί να οδηγήσει σε επιθέσεις κατά της συσκευής. Επίσης, αν ένα αρχείο MUD επιτρέπει σε μια παραβιασμένη συσκευή να επικοινωνεί με άλλους πόρους, μπορεί να χρησιμοποιηθεί για επιθέσεις κατά αυτών των πόρων. Για αυτό, οι χρήστες που αναπτύσσουν αρχεία MUD πρέπει να λαμβάνουν υπόψη τους αυτά τα θέματα ασφαλείας.

Αν ένας κακόβουλος παράγοντας δημιουργήσει ένα παραπλανητικό και κακόβουλο αρχείο MUD που φαίνεται να είναι έγκυρο και υπογεγραμμένο, τότε οι επικοινωνίες που θα επιτρέπονται από αυτό το αρχείο MUD θα είναι εμφανείς κατά την ανάγνωσή του. Για να προστατευθούν περαιτέρω, οι χρήστες πρέπει να ελέγχουν τα αρχεία MUD που χρησιμοποιούν για τις συσκευές IoT τους, προκειμένου να βεβαιωθούν ότι περιορίζουν τις επικοινωνίες μόνο σε αυτές που είναι ασφαλείς και κατάλληλες για κάθε συσκευή. Δυστυχώς, σε οικιακά δίκτυα και δίκτυα μικρών επιχειρήσεων, όπου οι χρήστες συνήθως δεν διαθέτουν τεχνικές γνώσεις για να επιθεωρήσουν τα αρχεία MUD, απαιτείται εμπιστοσύνη ότι τα αρχεία MUD που χρησιμοποιούν είναι ασφαλή και προστατεύουν τις συσκευές τους. Διαφορετικά, θα πρέπει να βασίζονται σε εξωτερικά πρόσωπα ή υπηρεσίες για να αξιολογήσουν την ασφάλεια και την καταλληλόλητα των αρχείων MUD που χρησιμοποιούν.

Για την υλοποίηση του MUD, απαιτείται η ύπαρξη ενός ασφαλούς διακομιστή αρχείων MUD από τον οποίο οι συσκευές μπορούν να λάβουν τα αντίστοιχα αρχεία MUD. Ωστόσο, εάν ο κατασκευαστής του διακομιστή σταματήσει τη λειτουργία του ή δεν ακολουθήσει τις βέλτιστες πρακτικές ενημέρωσης του λογισμικού, τότε ο διακομιστής αρχείων MUD γίνεται ευάλωτος σε κακόβουλες επιθέσεις και μπορεί να χρησιμοποιηθεί ως μέσο επίθεσης. Για να αποτραπεί αυτό το σενάριο, απαιτείται η ύπαρξη ενός μηχανισμού που θα επιτρέπει την αποσύνδεση από τον διακομιστή του κατασκευαστή, έτσι ώστε ο διαχειριστής του MUD να προστατεύεται από τη σύνδεση με έναν παραβιασμένο διακομιστή αρχείων MUD, ακόμη κι αν οι συσκευές IoT συνεχίζουν να αποστέλλουν τη διεύθυνση URL του παραβιασμένου διακομιστή. Ένα παράδειγμα τέτοιου μηχανισμού είναι η χρήση πληροφοριών σηματοδότησης απειλής.



Για να προστατεύσουμε τις συσκευές IoT σε ένα δίκτυο, μπορούμε να χρησιμοποιήσουμε την τεχνολογία MUD (Manufacturer Usage Description) ή να αναζητήσουμε εναλλακτικούς μηχανισμούς για συσκευές που δεν υποστηρίζουν MUD. Το MUD επιτρέπει σε μια συσκευή να αποκαλύψει πληροφορίες για τον εαυτό της μέσω μιας διεύθυνσης URL MUD. Ωστόσο, αυτή η διαδικασία μπορεί να αποκαλύψει πληροφορίες σχετικά με τυχόν ευπάθειες της συσκευής και να παράσχει κατευθύνσεις για επιθέσεις. Ένας κακόβουλος εισβολέας μπορεί να παρακολουθήσει τον διαχειριστή MUD για να ανιχνεύσει ποιες συσκευές είναι συνδεδεμένες στο δίκτυο και να χρησιμοποιήσει αυτές τις πληροφορίες για να επιτεθεί. Εάν ο εισβολέας έχει πρόσβαση στο τοπικό δίκτυο, μπορεί ακόμα να χρησιμοποιήσει τον διαχειριστή MUD για να διεξάγει μια επίθεση άρνησης υπηρεσίας, εκπέμποντας πολλαπλές διευθύνσεις URL MUD (με πλαστογραφημένες διευθύνσεις MAC). Όταν ένα σύστημα έχει παραβιαστεί αλλά εξακολουθεί να εκπέμπει τη σωστή διεύθυνση URL MUD, ο διαχειριστής MUD μπορεί να ανιχνεύσει και να αποκλείσει μη εξουσιοδοτημένες επικοινωνίες που προσπαθούν να προέλθουν από την παραβιασμένη συσκευή. Αυτό μπορεί να υποδηλώνει πιθανές προσπάθειες συμβιβασμού. Από την άλλη πλευρά, ένα παραβιασμένο σύστημα μπορεί να τροποποιηθεί έτσι ώστε να εκπέμπει μια νέα διεύθυνση URL που αναφέρεται σε ένα κακόβουλο αρχείο MUD, προκειμένου να επιτρέψει μη εξουσιοδοτημένες επικοινωνίες. Σε αυτήν την περίπτωση, εξαρτάται από τις ρυθμίσεις του διαχειριστή MUD να εντοπίσει αυτήν την αλλαγή στη διεύθυνση URL MUD. Αν ο διαχειριστής MUD απαιτεί από έναν διαχειριστή να αποδεχτεί μια νέα διεύθυνση URL, αλλά ο διαχειριστής αρνείται να την αποδεχτεί,

το MUD θα βοηθήσει στον εντοπισμό του παραβιασμένου συστήματος και στον περιορισμό της δυνατότητας χρήσης του για επιθέσεις. Αντίθετα, αν ο διαχειριστής MUD δεν απαιτεί από έναν διαχειριστή να αποδεχτεί τη νέα διεύθυνση URL ή αν την απαιτεί και ο διαχειριστής την αποδέχεται, το MUD δεν θα βοηθήσει στον εντοπισμό του παραβιασμένου συστήματος και δεν θα περιορίσει την ικανότητά του να χρησιμοποιηθεί για επιθέσεις. Τέλος, υπάρχει η περίπτωση ενός πιο εξελιγμένου παραβιασμένου συστήματος που μπορεί να αλλάξει δυναμικά την ταυτότητά του (π.χ. διεύθυνση MAC) και να εκπέμψει μια νέα διεύθυνση URL. Σε αυτήν την περίπτωση, το παραβιασμένο σύστημα δεν θα εντοπιστεί εκτός αν ο διαχειριστής MUD έχει ρυθμιστεί να απαιτεί από τον διαχειριστή να επιβεβαιώνει κάθε νέα ταυτότητα.

Όταν μια συσκευή IoT χρησιμοποιεί τη διεύθυνση URL MUD της για να ανακοινώσει την ταυτότητά της σε ένα δίκτυο, αλλά χρησιμοποιεί μη ασφαλείς μηχανισμούς όπως το DHCP ή το LLDP αντί για αξιόπιστα πιστοποιητικά X.509 για την επαλήθευση της ταυτότητάς της, μπορεί να υπάρξει το ενδεχόμενο να παραπλανηθεί η αληθινή ταυτότητα της συσκευής και να αποκτήσει πρόσβαση στο δίκτυο που δεν θα έπρεπε να έχει. Σε περιβάλλοντα όπου υπάρχουν τέτοιου είδους μη ασφαλείς μηχανισμοί και υλοποιήσεις MUD που δεν παρέχουν αξιόπιστη συσχέτιση μεταξύ της διεύθυνσης URL MUD και της συσκευής, οι διαχειριστές δικτύου πρέπει να λάβουν επιπλέον προφυλάξεις για να βελτιώσουν την ασφάλεια. Για παράδειγμα, η υλοποίηση του MUD θα πρέπει να ρυθμιστεί έτσι ώστε να αποτρέπει τη παρουσία μη επαληθευμένων συσκευών στο ίδιο επίπεδο με αυστηρά επαληθευμένες συσκευές και να αποτρέπει τις συσκευές που δεν έχουν πιστοποιηθεί από το να μπορούν να χρησιμοποιούν την ίδια διεύθυνση URL MUD με συσκευές που έχουν πιστοποιηθεί αυστηρά. Είναι απαραίτητο επίσης να υπάρχει σύνδεση της επικοινωνίας με τον έλεγχο ταυτότητας που έχει χρησιμοποιηθεί, π.χ. IEEE 802.1X, 802.1AE (MACsec), 802.11i (WPA2), WFA Easy Connect ή μελλοντικούς τύπους ελέγχου ταυτότητας καθώς και κατάργηση κατάστασης εάν χρησιμοποιείται μια μη επικυρωμένη μέθοδος εκπομπής URL MUD και ανιχνευθεί οποιαδήποτε μορφή διακοπής σε αυτήν την περίοδο σύνδεσης. Τέλος δεν πρέπει να περιλαμβάνονται συσκευές χωρίς έλεγχο ταυτότητας και είναι αναγκαία η προειδοποίηση και η ζήτηση της έγκρισης του διαχειριστή MUD σε περιπτώσεις αλλαγής των υπογραφών ενός αρχείου MUD και σε περιπτώσεις αλλαγής μιας συσκευής στο δίκτυο.

Για να προστατευτούμε από κακόβουλους παράγοντες που μπορεί να αλλάξουν την ιδιοκτησία ενός τομέα (domain), πρέπει να λάβουμε τα εξής μέτρα:

1. Οι διαχειριστές MUD θα πρέπει να αποθηκεύουν προσωρινά πιστοποιητικά που χρησιμοποιούνται από τον διακομιστή αρχείων MUD.
2. Όταν ανακτάται ένα νέο πιστοποιητικό, ο διαχειριστής MUD πρέπει να ελέγχει εάν έχει αλλάξει η ιδιοκτησία του τομέα.
3. Αν ανιχνευθεί αλλαγή ιδιοκτησίας του τομέα, ο διαχειριστής πρέπει να ειδοποιήσει και να απαιτήσει έγκριση από τον νέο διαχειριστή.

Με αυτόν τον τρόπο, επιδιώκουμε να αποτρέψουμε την παροχή κακόβουλων αρχείων MUD από κακόβουλους παράγοντες που έχουν αλλάξει την ιδιοκτησία του τομέα.

4.3 Συστάσεις Ασφάλειας

Το MUD (Manufacturer Usage Description) είναι ένα σύστημα που χρησιμοποιείται για την ασφαλή διαχείριση και προστασία των συσκευών IoT (Internet of Things) σε οικιακά και μικρά επιχειρηματικά δίκτυα. Η ανάπτυξη μιας υποδομής με δυνατότητα MUD προσφέρει ασφάλεια και προστασία από πιθανές απειλές και επιτρέπει τον έλεγχο της πρόσβασης των συσκευών στο δίκτυο. Οι ιδιοκτήτες των δικτύων οικιακών και μικρών επιχειρήσεων πρέπει να διασφαλίσουν ότι οι προμηθευτές τους κατανοούν τη σημασία του MUD και απαιτούν τόσο τις συσκευές IoT όσο και τα δικτυακά στοιχεία να υποστηρίζουν τη δυνατότητα MUD. Πρέπει να χρησιμοποιούν συσκευές IoT με δυνατότητα MUD στο δίκτυό τους και να ενεργοποιούν τη λειτουργία MUD στο δίκτυό τους, εγκαθιστώντας όλα τα απαραίτητα στοιχεία δικτύου με δυνατότητα MUD. Οι πάροχοι υπηρεσιών πρέπει να εξετάσουν τη δυνατότητα παροχής και υποστήριξης δρομολογητών με δυνατότητα MUD στα οικιακά και επιχειρηματικά δίκτυα ή να ενθαρρύνουν τους πελάτες τους να χρησιμοποιούν δρομολογητές με δυνατότητα MUD. Αυτό σημαίνει ότι οι πάροχοι υπηρεσιών μπορούν είτε να παρέχουν αυτόνομους δρομολογητές με δυνατότητα MUD από τρίτους προμηθευτές εξοπλισμού δικτύου, είτε να ενσωματώσουν τη λειτουργία MUD στον οικιακό εξοπλισμό πύλης που παρέχουν. Αν και δεν είναι υποχρεωμένοι να το κάνουν, ορισμένοι πάροχοι υπηρεσιών μπορεί να επιλέξουν να καταστήσουν τον οικιακό εξοπλισμό πύλης ικανό για τη λειτουργία MUD. Οι κατασκευαστές συσκευών IoT πρέπει να προγραμματίζουν τις συσκευές τους έτσι ώστε να μεταφέρουν μια διεύθυνση URL MUD ή να την εκπέμπουν με κάποιον άλλο τρόπο. Αυτή η διεύθυνση URL MUD αναφέρεται σε ένα αρχείο MUD που περιέχει πληροφορίες για τον τρόπο πρόσβασης και τις απαιτήσεις ασφαλείας της συσκευής. Οι πάροχοι υπηρεσιών πρέπει να εξετάσουν τη δυνατότητα να παρέχουν και υποστηρίξουν δρομολογητές με δυνατότητα MUD στα οικιακά και επιχειρηματικά δίκτυα. Αυτό σημαίνει ότι οι πάροχοι υπηρεσιών μπορούν να παρέχουν ειδικούς δρομολογητές από εξωτερικούς προμηθευτές που υποστηρίζουν τη λειτουργία MUD ή να ενσωματώσουν τη λειτουργία MUD στον οικιακό εξοπλισμό πύλης που παρέχουν. Αυτό θα επιτρέψει την αυτόματη προστασία και έλεγχο των συνδεδεμένων συσκευών IoT στο δίκτυο. Οι κατασκευαστές συσκευών IoT πρέπει να προγραμματίζουν τις συσκευές τους έτσι ώστε να μεταφέρουν μια διεύθυνση URL MUD ή να την εκπέμπουν με κάποιον άλλο τρόπο. Αυτή η διεύθυνση URL MUD αναφέρεται σε ένα αρχείο MUD που περιέχει πληροφορίες για τον τρόπο πρόσβασης και τις απαιτήσεις ασφαλείας της συσκευής. Με αυτόν τον τρόπο, οι διαχειριστές δικτύου μπορούν να γνωρίζουν ποιες προνόμια πρόσβασης χρειάζεται η συσκευή και ποιες επικοινωνίες επιτρέπονται για την συγκεκριμένη συσκευή. Οι κατασκευαστές πρέπει επίσης να ενημερώνουν τα αρχεία MUD κατά τη διάρκεια του κύκλου ζωής των συσκευών τους, ώστε να ανταποκρίνονται σε εξελίξεις και αλλαγές στα προφίλ επικοινωνίας των συσκευών. Ακόμη και όταν μια συσκευή IoT δεν υποστηρίζεται πλέον και καταργείται, ο κατασκευαστής πρέπει να διατηρεί το αρχείο MUD της συσκευής προσβάσιμο, ώστε οι πολιτικές επικοινωνίας της συσκευής να εξακολουθούν να ισχύουν. Αυτό είναι ιδιαίτερα σημαντικό για συσκευές IoT που έχουν γνωστά αδύναμα σημεία ασφαλείας και έχουν σταματήσει να λαμβάνουν αναβαθμίσεις.

Για να βελτιώσουν την ασφάλεια των δικτύων τους, οι ιδιοκτήτες οικιακών και μικρών επιχειρήσεων πρέπει να χρησιμοποιούν εξοπλισμό και υπηρεσίες που λαμβάνουν υπόψη τους τις απειλές που υφίστανται. Αυτό σημαίνει ότι θα πρέπει να χρησιμοποιούν εργαλεία και υπηρεσίες που είναι σχεδιασμένα να ανιχνεύουν και να αντιμετωπίζουν γνωστές απειλές στην ασφάλεια του δικτύου τους. Αυτό τους επιτρέπει να είναι ενημερωμένοι για τις τελευταίες απειλές και να λαμβάνουν τα αναγκαία μέτρα για την προστασία τους. Για να διασφαλίσουν την ασφάλεια των δικτύων τους, οι ιδιοκτήτες οικιακών και μικρών επιχειρήσεων θα πρέπει να εκτελούν τακτικές ενημερώσεις σε όλες τις συσκευές IoT που χρησιμοποιούν. Οι κατασκευαστές συσκευών IoT θα πρέπει να διασφαλίζουν ότι παρέχουν συνεχή υποστήριξη για τις συσκευές που διαθέτουν, με την παροχή τακτικών ενημερώσεων λογισμικού και κώδικα. Οι ιδιοκτήτες οικιακών και μικρών επιχειρήσεων πρέπει να έχουν πλήρη εποπτεία και γνώση για κάθε συσκευή που συνδέεται στο δίκτυό τους. Κάθε συσκευή μπορεί να αντιπροσωπεύει μια δυνητική απειλή ή ένα πιθανό σημείο εισβολής, και για αυτόν τον λόγο πρέπει να ανακαλυφθεί και να προστατευθεί. Οι συσκευές IoT με

γνωστούς κινδύνους ασφαλείας, όπως αυτές που δεν υποστηρίζουν την τεχνολογία MUD, θα πρέπει να τοποθετούνται σε ξεχωριστό τμήμα του δικτύου, διαφορετικό από τις καθημερινές υπολογιστικές συσκευές που έχουν υψηλότερο επίπεδο προστασίας κυβερνοασφάλειας με τις τακτικές ενημερώσεις λογισμικού και ασφαλείας. Αυτό το μέτρο είναι σημαντικό για την αντιμετώπιση πιθανών απειλών που μπορεί να προκύψουν από τις συσκευές IoT. Είναι αναγκαία η δημιουργία της υποδομής δικτύου με σκοπό την ασφαλή και αυτοματοποιημένη χρήση του πρωτόκολλου ενσωμάτωσης. Επιπλέον, θα πρέπει να χρησιμοποιούν συσκευές IoT που μπορούν να ενσωματωθούν στο δίκτυο μέσω αυτού του πρωτοκόλλου. Οι κατασκευαστές εξοπλισμού δικτύου που προορίζεται για οικιακά δίκτυα και μικρές επιχειρήσεις θα πρέπει να παρέχουν λειτουργίες που επιτρέπουν την ασφαλή, αυτόματη και εύχρηστη ενσωμάτωση συσκευών IoT, την ανίχνευση πιθανών απειλών και την αναγνώριση των συνδεδεμένων συσκευών.

Σε ορισμένες περιπτώσεις ενδέχεται η αναθεώρηση της προδιαγραφής MUD ώστε να υπάρχει η γνώση της συμπεριφοράς του διακομιστή σε περίπτωση που το αρχείο υπογραφής MUD δεν υπάρχει σε ένα αρχείο. Ένας διαχειριστής MUD μπορεί να επεξεργαστεί ένα αρχείο MUD χωρίς να επικυρώσει την υπογραφή του. Αυτό ανοίγει τη δυνατότητα σε κακόβουλους χρήστες (hackers) να τροποποιήσουν το αρχείο MUD και να διαγράψουν την υπογραφή MUD του, προκειμένου να αποφύγουν τον εντοπισμό της τροποποίησης. Σε αυτήν την περίπτωση, ένας διαχειριστής MUD δεν θα μπορεί να διακρίνει ένα αρχείο MUD που δεν έχει υπογραφεί από ένα αρχείο MUD που αρχικά είχε υπογραφεί αλλά έχει τροποποιηθεί μετά από μια επίθεση, καθώς η υπογραφή λάσπης έχει διαγραφεί. Ουσιαστικά γίνεται αναφορά στο γεγονός ότι η απουσία επαλήθευσης της υπογραφής στα αρχεία MUD μπορεί να αποτελέσει ευπάθεια απέναντι σε επιθέσεις, όπου κακόβουλοι χρήστες μπορούν να τροποποιήσουν τα αρχεία χωρίς ανίχνευση. Αν ο διαχειριστής ενός MUD αρχείου διαπιστώσει ότι η υπογραφή του αρχείου έχει διαγραφεί, τότε θα πρέπει να σταματήσει την επεξεργασία του αρχείου και να περιμένει την εισαγωγή του διαχειριστή. Στη συνέχεια, ο διαχειριστής πρέπει να προσπαθήσει να εντοπίσει και να επαληθεύσει την υπογραφή του αρχείου MUD, χρησιμοποιώντας εναλλακτικούς μηχανισμούς. Ωστόσο, το αρχικό RFC δεν παρέχει πληροφορίες σχετικά με τέτοιους εναλλακτικούς μηχανισμούς. Συνεπώς, οι συντάκτες του RFC μπορεί να εξετάσουν την προσθήκη προτάσεων για πιθανούς εναλλακτικούς τρόπους εντοπισμού και επαλήθευσης των υπογραφών των αρχείων MUD, εάν το στοιχείο της υπογραφής MUD δεν παρέχεται αρχικά ή έχει διαγραφεί. Για την περαιτέρω ασφάλεια συνιστάται να εξετασθεί η αναθεώρηση της προδιαγραφής MUD (RFC 8520) προκειμένου να ενημερωθούν οι αναγνώστες σχετικά με μια ευπάθεια ασφαλείας που προκύπτει από τη χρήση ενός διαχειριστή MUD που επεξεργάζεται αυτόματα ένα αρχείο MUD που δεν διαθέτει στοιχείο υπογραφής. Προτείνεται επίσης η αναθεώρηση της προδιαγραφής MUD (RFC 8520) για να διευκρινιστεί ότι δεν διέπει απευθείας τι ενέργειες πρέπει να ακολουθηθούν όταν ο διαχειριστής MUD δεν μπορεί να επικυρώσει το πιστοποιητικό TLS του διακομιστή αρχείων MUD ή την υπογραφή του αρχείου MUD της συσκευής. Το RFC αναφέρει ότι ο διαχειριστής MUD θα πρέπει να σταματήσει την επεξεργασία του αρχείου MUD και να περιμένει την έγκριση του διαχειριστή, αλλά θα ήταν χρήσιμο να προσδιοριστεί ρητά ότι η προδιαγραφή δεν λαμβάνει θέση και αφήνει στην τοπική πολιτική το αν η συσκευή πρέπει να αποκλειστεί από την κυκλοφορία της κίνησης, να της επιτραπεί να επικοινωνεί ελεύθερα ή να ακολουθηθεί μια άλλη πολιτική.

Για την δραστηριότητα με ομάδα συνεργασίας πρωταρχικός στόχος είναι η βελτίωση των δυνατοτήτων MUD. Αυτό σημαίνει ότι υπάρχει συνεργασία για την ανάπτυξη και την εφαρμογή των απαιτήσεων ασφαλείας. Πιο συγκεκριμένα πρέπει να προσαρμόζονται οι συσκευές IoT ώστε να μπορούν να εκπέμπουν με ασφάλεια τις διευθύνσεις URL MUD τους. Αυτό γίνεται παρέχοντας στις συσκευές IoT διαπιστευτήρια και συσχετίζοντας τις διευθύνσεις URL MUD με την ταυτότητά τους. Επιπλέον είναι απαραίτητος ο περιορισμός των αδειών πρόσβασης για τις συσκευές IoT που δεν εκπέμπουν τις διευθύνσεις URL MUD τους με ασφαλή τρόπο, ώστε να μην έχουν περισσότερες

εξουσίες από εκείνες που δεν υπακούν στην πολιτική MUD. Ώστε να ζητά έγκριση από τον διαχειριστή εάν αλλάξει ο υπογράφοντας ενός αρχείου MUD ή το ίδιο το αρχείο MUD θα πρέπει να ρυθμιστεί ο διαχειριστής MUD. Από την άλλη για τις συσκευές IoT που δεν εκπέμπουν τις διευθύνσεις URL MUD τους με ασφαλή τρόπο, είναι απαραίτητη η εκτέλεση πρόσθετων μέτρων επαλήθευσης πριν από την εισαγωγή των συσκευών στη συγκεκριμένη κατηγορία κατασκευαστή. Για παράδειγμα, γίνεται έλεγχος της διεύθυνση MAC κάθε συσκευής και επαλήθευση ότι ο κατασκευαστής που σχετίζεται με αυτήν τη διεύθυνση MAC είναι ο ίδιος με τον κατασκευαστή που καθορίζεται στο πεδίο "κατασκευαστής" στο αρχείο MUD αυτής της συσκευής. Ουσιαστικά, υπάρχει συνεργασία με τους συνεργάτες μας για να εφαρμοστούν πρόσθετα μέτρα ασφαλείας, όπως η ασφαλής εκπομπή των διευθύνσεων URL MUD, η περιορισμένη πρόσβαση σε συσκευές που δεν συμμορφώνονται με τις πολιτικές MUD, η έγκριση αλλαγών στα αρχεία MUD και η επαλήθευση κατασκευαστή για συσκευές που δεν εκπέμπουν τις διευθύνσεις URL MUD τους με ασφαλή τρόπο. Όλα αυτά συμβάλλουν στη βελτίωση της ασφάλειας των εμπορικών προϊόντων που χρησιμοποιούν την τεχνολογία MUD.

Μια προσέγγιση που μπορούμε να εξερευνήσουμε είναι η χρήση crowdsourcing και αναλυτικών για την ανάλυση της ροής κυκλοφορίας των συσκευών IoT με δυνατότητα MUD κατά τη χρήση τους. Αντί να απορρίπτουμε απλά την κίνηση που δεν εμπίπτει στο προφίλ της συσκευής IoT, μπορούμε να την τοποθετούμε σε καραντίνα, να την καταγράφουμε και να την αναλύουμε για περαιτέρω μελέτη. Μια εφαρμογή αναλυτικών δεδομένων μπορεί να συλλέγει αυτήν την κίνηση από πολλές πηγές και να αναλύει τη ροή κυκλοφορίας, προσδιορίζοντας εάν υπάρχουν βάσιμοι λόγοι για την επέκταση του προφίλ επικοινωνίας της συσκευής. Με αυτόν τον τρόπο, μπορούμε να προσαρμόσουμε και να εξελίξουμε τα προφίλ κυκλοφορίας των συσκευών IoT κατά τη διάρκεια της χρήσης τους, αντί να απορρίπτουμε αυθαίρετα την κίνησή τους.

Σε συνεργασία με συνεργάτες, αναπτύσσουμε ένα σχέδιο που θα καθοδηγεί τους κατασκευαστές συσκευών IoT καθ' όλη τη διάρκεια της ενσωμάτωσης της υποστήριξης MUD στις συσκευές τους, από την αρχική διαθεσιμότητα της συσκευής έως τον τελικό παροπλισμό της. Παρέχουμε καθοδήγηση στους κατασκευαστές σχετικά με τις απαιτούμενες και συνιστάμενες δραστηριότητες και εκτιμήσεις που πρέπει να πραγματοποιήσουν.

Πραγματοποιούμε μελέτες απόδοσης για να ενημερώσουμε τους κατασκευαστές δρομολογητών καταναλωτών σχετικά με τον τρόπο με τον οποίο το MUD επηρεάζει την απόδοση τους. Αυτές οι μελέτες έχουν ως στόχο να αντιμετωπίσουν τυχόν ανησυχίες που μπορεί να έχουν ορισμένοι κατασκευαστές σχετικά με τις πιθανές επιπτώσεις του MUD στην απόδοση των συσκευών τους.

4.4 Θεωρήσεις Μελλοντικής Δόμησης

Το πλήθος των συσκευών που υποστηρίζουν MUD διακρίνεται από αυξητική τάση όπου οδηγεί το εξελισσόμενο πρωτόκολλο διαδικτύου IPv6 στην διαδικασία πρόσθεσης μιας νέας

διάστασης στην χρήση MUD με σκοπό την αποτροπή από επιθέσεις DDoS που βασίζονται στο IoT και άλλων επιθέσεων που βασίζονται σε δίκτυο.

Επιπλέον, υπάρχουν αρκετά ενθαρρυντικά πεδία για περαιτέρω έρευνα και ανάπτυξη σχετικά με τη λειτουργικότητα, την ένταξη των συσκευών IoT και τα ζητήματα που αφορούν τον κύκλο ζωής των συσκευών IoT. Όσον αφορά την ένταξη, μπορούμε να εξετάσουμε και να αναπτύξουμε μηχανισμούς που θα εξασφαλίζουν με ασφάλεια τη διεύθυνση URL MUD για τις συσκευές IoT, συμπληρώνοντας έτσι τη χρήση του πρωτοκόλλου Wi-Fi Easy Connect. Αυτή η ιδέα μπορεί να εξεταστεί περαιτέρω μέσω υλοποιήσεων που θα λειτουργούν ως απόδειξη της αποτελεσματικότητας.

Σύμφωνα με το IETF δύο υποψήφιες μελλοντικές εκδόσεις του MUD είναι η καραντίνα συσκευών και η αναφορά MUD για τους κατασκευαστές. Με την καραντίνα συσκευών ο διαχειριστής MUD μπορεί να εφαρμόσει καραντίνα σε μια συσκευή όταν ένα πακέτο που προέρχεται από αυτήν παραβιάζει τους κανόνες MUD. Κατά την καραντίνα, η πρόσβαση της συσκευής περιορίζεται μόνο στους κανόνες που επιτρέπονται για την καραντίνα. Από την άλλη με την αναφορά MUD για τους διαχειριστές ο διαχειριστής MUD μπορεί να εφαρμόσει μια δυνατότητα αναφοράς MUD για τους κατασκευαστές συσκευών, ώστε να λαμβάνουν σχόλια σχετικά με την απόδοση των συσκευών τους που υποστηρίζουν το MUD. Αυτή η αναφορά δεν περιλαμβάνει προσωπικές πληροφορίες που αφορούν τη συσκευή ή το δίκτυο για λόγους απορρήτου.

Οι εταιρίες Arm, CableLabs, Cisco, CTIA, DigiCert, Forescout, Global Cyber Alliance, MasterPeace Solutions, Molex, Patton Electronics και Symantec έχουν συνεργαστεί και υπογράψει συμφωνία συνεργασίας (CRADA) για να αντιμετωπίσουν την αυξανόμενη ποικιλία διαθέσιμων εξαρτημάτων. Πρόκειται για μια συνεργατική προσπάθεια μεταξύ τους για την ανάπτυξη και βελτίωση του πρωτοκόλλου MUD. Υπάρχει επίσης ενδιαφέρον από άλλες εταιρίες να συμμετάσχουν στο έργο, ιδιαίτερα αν επεκτείνουμε το εύρος της συνεργασίας για την ενσωμάτωση του MUD. Ορισμένες εταιρίες έχουν εκφράσει ενδιαφέρον και για την προβολή της εφαρμογής του MUD στην επιχειρηματική και βιομηχανική χρήση του Internet of Things (IoT). Οι νέοι δυνητικοί συνεργάτες μπορούν να υποβάλουν επιστολές ενδιαφέροντος για να συμμετάσχουν σε συμφωνίες συνεργασίας (CRADA) και να συνεισφέρουν στην αντιμετώπιση των προκλήσεων που σχετίζονται με την ενσωμάτωση του MUD και άλλων χαρακτηριστικών ασφαλείας στην επιχειρηματική ή βιομηχανική χρήση του IoT.

Στην αρχική φάση του έργου, λόγω περιορισμών, υποστηρίχθηκε μόνο το IPv4 και δεν εξετάστηκαν ζητήματα που σχετίζονται με το IPv6. Ωστόσο, λόγω της απουσίας του NAT στο IPv6, όλες οι συσκευές που χρησιμοποιούν IPv6 έχουν άμεσες διευθύνσεις. Αυτό σημαίνει ότι οι πιθανότητες για επιθέσεις DDoS και άλλες είδους επιθέσεων σε δίκτυα IPv6 μπορεί να είναι χειρότερες από ό,τι σε δίκτυα IPv4. Για τον λόγο αυτό, συνιστούμε την εκτέλεση της δοκιμής του MUD σε ένα περιβάλλον IPv6, ως μέρος των μελλοντικών εργασιών.

Ιστότοποι

• https://www.nccoe.nist.gov/publication/1800-15/

• https://developer.cisco.com/docs/mud/#!why-mud/why-mud

• https://www.nccoe.nist.gov/

• https://www.mplaunchpad.com/

• https://www.quad9.net/

• https://csrc.nist.gov/

• https://nvlpubs.nist.gov/

• https://www.ibm.com/topics/enterprise-asset-management

• https://csf.tools/reference/

• https://www.opensecurityarchitecture.org/cms/library/08_02_control-catalogue/

• https://www.stigviewer.com/controls/800-53/IA-2

• https://docs.pivotal.io/nist/

• https://www.cisecurity.org/controls/inventory-and-control-of-enterprise-assets

• https://wiki.process-symphony.com.au/framework/lifecycle/process/assets-management-bai09-cobit2019/

• https://www.isa.org/products/isa-62443-2-1-2009-security-for-industrial-automat

• https://cybersecurity.att.com/documentation/usm-anywhere/user-guide/iso-27001/a.8.1.1.htm

• https://www.itgovernance.co.uk/cobit

• https://www.dhs.gov/topics/cybersecurity

• https://www.sentinelone.com/cybersecurity-101/open-source-intelligence-osint/

• https://www.isaca.org/resources/isaca-journal/issues/2015/volume-2/selected-cobit-5-processes-for-essential-enterprise-security

• https://controls-assessment-specification.readthedocs.io/en/stable/control-16/index.html

• https://www.cisecurity.org/controls

• https://blog.netwrix.com/2023/01/19/cis-control-13-network-monitoring-and-defense/