ΑΕΙ ΠΕΙΡΑΙΑΤ.Τ.
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ Τ.Ε.

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Firewall επιχειρησιακής τεχνολογίας εντός βιομηχανικής εγκατάστασης

Ιωάννης Π. Καρελάς

Εισηγητής: Δρ Κωνσταντίνος Κουκουλέτσος, Καθηγητής

ΑΘΗΝΑ
ΔΕΚΕΜΒΡΗΣ 2017

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Firewall επιχειρησιακής τεχνολογίας εντός βιομηχανικής εγκατάστασης

Ιωάννης Π. Καρελάς
Α.Μ. 35866

Εισηγητής:

Δρ Κωνσταντίνος Κουκουλέτσος, Καθηγητής

Εξεταστική Επιτροπή:

Ημερομηνία εξέτασης

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Καρελάς Ιωάννης, του Παναγιώτη, με αριθμό μητρώου 35866, φοιτητής του Τμήματος Μηχανικών Η/Υ Συστημάτων Τ.Ε. του Α.Ε.Ι. Πειραιά Τ.Τ. πριν αναλάβω την εκπόνηση της Πτυχιακής Εργασίας μου, δηλώνω ότι ενημερώθηκα για τα παρακάτω:

«Η Πτυχιακή Εργασία (Π.Ε.) αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο του συγγραφέα, όσο και του Ιδρύματος και θα πρέπει να έχει μοναδικό χαρακτήρα και πρωτότυπο περιεχόμενο.

Απαγορεύεται αυστηρά οποιοδήποτε κομμάτι κειμένου της να εμφανίζεται αυτούσιο ή μεταφρασμένο από κάποια άλλη δημοσιευμένη πηγή. Κάθε τέτοια πράξη αποτελεί προϊόν λογοκλοπής και εγείρει θέμα Ηθικής Τάξης για τα πνευματικά δικαιώματα του άλλου συγγραφέα. Αποκλειστικός υπεύθυνος είναι ο συγγραφέας της Π.Ε., ο οποίος φέρει και την ευθύνη των συνεπειών, ποινικών και άλλων, αυτής της πράξης.

Πέραν των όποιων ποινικών ευθυνών του συγγραφέα σε περίπτωση που το Ίδρυμα του έχει απονείμει Πτυχίο, αυτό ανακαλείται με απόφαση της Συνέλευσης του Τμήματος. Η Συνέλευση του Τμήματος με νέα απόφασης της, μετά από αίτηση του ενδιαφερόμενου, του αναθέτει εκ νέου την εκπόνηση της Π.Ε. με άλλο θέμα και διαφορετικό επιβλέποντα καθηγητή. Η εκπόνηση της εν λόγω Π.Ε. πρέπει να ολοκληρωθεί εντός τουλάχιστον ενός ημερολογιακού 6μήνου από την ημερομηνία ανάθεσης της. Κατά τα λοιπά εφαρμόζονται τα προβλεπόμενα στο άρθρο 18, παρ. 5 του ισχύοντος Εσωτερικού Κανονισμού.»

ΠΕΡΙΛΗΨΗ

Οι επιχειρήσεις προσπαθούν να αποφύγουν και να αντιμετωπίσουν σε καθημερινή βάση, διάφορες απειλές για την επίτευξη των επιχειρηματικών στόχων τους. Οι απειλές αυτές μπορεί να περιλαμβάνουν τον οικονομικό κίνδυνο, τον κίνδυνο αποτυχίας του εξοπλισμού και τον κίνδυνο της ασφάλειας του προσωπικού. Οι οργανισμοί πρέπει να αναπτύξουν διαδικασίες για την αξιολόγηση των κινδύνων που σχετίζονται με την επιχείρησή τους και να αποφασίσουν πώς να αντιμετωπίσουν αυτούς τους κινδύνους με βάση τις οργανωτικές προτεραιότητες και τους εσωτερικούς και εξωτερικούς περιορισμούς.

Αυτή η διαχείριση του κινδύνου διεξάγεται ως μια διαδραστική, συνεχής διαδικασία ως μέρος των κανονικών λειτουργιών. Οι οργανισμοί που χρησιμοποιούν τα συστήματα βιομηχανικού ελέγχου (Industrial Control Systems, ICS) διαχειρίζονται τις διάφορες απειλές μέσω καλών πρακτικών στον τομέα της ασφάλειας. Οι εκτιμήσεις ασφαλείας έχουν καθιερωθεί στους περισσότερους τομείς και συχνά ενσωματώνονται στις κανονιστικές απαιτήσεις. Η διαχείριση κινδύνων ασφάλειας πληροφοριών είναι μια πρόσθετη διάσταση που μπορεί να είναι συμπληρωματική. Η διαδικασία διαχείρισης του κινδύνου και το πλαίσιο που περιγράφεται σε αυτό το τμήμα μπορούν να εφαρμοστούν σε οποιαδήποτε αξιολόγηση κινδύνου, συμπεριλαμβανομένης και της ασφάλειας των πληροφοριών. Μια διαδικασία διαχείρισης κινδύνου πρέπει να εφαρμόζεται σε ολόκληρο τον οργανισμό, χρησιμοποιώντας μια προσέγγιση τριών επιπέδων για την αντιμετώπιση του κινδύνου σε (i) οργανωτικό επίπεδο (ii) σε επίπεδο αποστολής /

επιχειρηματικής διαδικασίας και (iii) σε επίπεδο πληροφοριακού συστήματος (IT και ICS).

Η διαδικασία διαχείρισης κινδύνου διεξάγεται απρόσκοπτα στα τρία επίπεδα, με γενικό στόχο τη συνεχή βελτίωση των δραστηριοτήτων που σχετίζονται με τον κίνδυνο του οργανισμού και την αποτελεσματική επικοινωνία μεταξύ των επιπέδων και των επιπέδων μεταξύ όλων των ενδιαφερομένων που έχουν κοινό συμφέρον στην επιχείρηση. Στην παρούσα εργασία, εξετάζονται οι μηχανισμοί προστασίας με την χρήση firewalls.

ABSTRACT

The enterprises are trying to avoid and face on a daily basis, various threats in order to accomplish their businesslike goals. These threats may include the financial risk, the risk of equipment failure and the risk of safety of their personnel. The organizations must and should develop procedures for the assessment of risks which are relevant to their enterprises and make the decisions of how to confront these risks on the basis of organizational priorities and on the internal and external constraints.

This management of risk is conducted as an interactive and continuous procedure as part of the normal functions. The organizations that use the Industrial Control Systems-ICS, handle the various threats through good practices on the field of security. The evaluations of safety have been a common practice on most fields and often are incorporated in the regulative demands. The handling of risks for secure information is an additional dimension which can be complementary.

The procedure of handling the risk and the frame which is described in this part may apply to any assessment of risk, including safety and security of information. A procedure of handling risk must be applied to the entire organization, using an approach of three standards to deal with the risk in , (i) organizational standard, (ii) the standard of delivery/ business procedure and (iii) the standard of informational system (IT and ICS) .The procedure of risk handling is conducted smoothly with the three standards, having as a general goal the constant improvement of activities which are relevant to the risk of the organization and the effective communication among the standards and the standards among all the concerned, who have common interest in the business. In this present assignment the mechanisms of protection are inquired with the use of firewalls.

Περιεχόμενα

Πίνακας Εικόνων

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

Η αντιμετώπιση των επιθέσεων του δικτύου απαιτεί μια ολοκληρωμένη, end-to-end προσέγγιση που περιλαμβάνει τη δημιουργία και τη διατήρηση πολιτικών ασφάλειας με βάση τις ανάγκες ασφάλειας ενός οργανισμού. Το πρώτο βήμα για τον καθορισμό των αναγκών ασφάλειας ενός οργανισμού είναι να εντοπίσει πιθανές απειλές και να εκτελέσει μια ανάλυση κινδύνου. Τα αποτελέσματα της ανάλυσης κινδύνου χρησιμοποιήθηκαν για τη δημιουργία του υλικού ασφάλειας και εφαρμογών λογισμικού, πολιτικών μετριασμού και το σχεδιασμό του δικτύου. Για να απλοποιηθεί ο σχεδιασμός του δικτύου, συνίσταται ότι όλοι οι μηχανισμοί ασφαλείας πρέπει να προέρχονται από ένα και μόνο προμηθευτή.

Αφού το δίκτυο έχει σχεδιαστεί, οι επιχειρήσεις ασφαλείας περιλαμβάνουν τις πρακτικές που απαιτούνται για την πρώτη ανάπτυξη ημέρα με την ημέρα και στη συνέχεια διατηρούν το ασφαλές σύστημα. Μέρος της διατήρησης ενός ασφαλούς συστήματος είναι ο έλεγχος της ασφάλειας του δικτύου. Ο έλεγχος ασφαλείας γίνεται από την ομάδα λειτουργίας, για να εξασφαλιστεί ότι όλες οι εφαρμογές ασφαλείας λειτουργούν όπως αναμενόταν. Οι δοκιμές επίσης χρησιμοποιούνται για την παροχή της συνεχούς λειτουργίας, η οποία μπορεί να παρεμποδιστεί σε περίπτωση καταστροφής, αναστάτωσης, ή παρατεταμένης διακοπής της υπηρεσίας. Αφού ένα ασφαλές δίκτυο υλοποιείται και τα σχέδια συνέχειας συσταθούν, τα εν λόγω σχέδια και τα έγγραφα πρέπει να ενημερώνονται συνεχώς με βάση τις μεταβαλλόμενες ανάγκες του οργανισμού. Για το λόγο αυτό, είναι απαραίτητο να κατανοήσουμε τον κύκλο ανάπτυξης του συστήματος ζωής (Systems Development Life Cycle, SDLC), για τους σκοπούς της αξιολόγησης αλλαγών του συστήματος και τη ρύθμιση των υλοποιήσεων της ασφάλειας. Το SDLC περιλαμβάνει πέντε στάδια: την

έναρξη, την απόκτηση και ανάπτυξη, την υλοποίηση, τη λειτουργία και συντήρηση και τέλος τη διάθεση (Michael, 2009).

Είναι σημαντικό να συμπεριληφθούν οι παράγοντες ασφαλείας σε όλες τις φάσεις του SDLC. Ένα σύστημα ασφαλείας του δικτύου δεν μπορεί να αποτρέψει εντελώς τα υπολογιστικά συστήματα από το να είναι ευάλωτα σε απειλές. Νέες επιθέσεις αναπτύσσονται και τα τρωτά σημεία προσδιορίζονται, ώστε να μπορούν να χρησιμοποιηθούν για την παράκαμψη των λύσεων ασφάλειας. Επιπλέον, τεχνικά, διοικητικά και φυσικά συστήματα ασφαλείας μπορεί να ηττηθούν, αν η κοινότητα τελικού χρήστη δεν συμμορφώνεται με τις πρακτικές και τις διαδικασίες ασφάλειας. Μια ολοκληρωμένη πολιτική ασφαλείας πρέπει να διατηρηθεί και να προσδιορίζει τα υπολογιστικά συστήματα ενός οργανισμού, να προσδιορίζει το υλικό και τις απαιτήσεις ασφαλείας του λογισμικού για την προστασία του εξοπλισμού και του υλικού, να αποσαφηνίζει τους ρόλους και τις ευθύνες του προσωπικού και να καθιερώνει το σωστό πρωτόκολλο για την αντιμετώπιση των παραβιάσεων της ασφάλειας. Αν οι πολιτικές ασφάλειας έχουν καθιερωθεί και ακολουθούνται, οι οργανισμοί μπορούν να ελαχιστοποιήσουν την απώλεια και τις ζημίες που προκύπτουν από τις επιθέσεις .

1.2. Δομή της εργασίας

Η παρούσα εργασία χωρίζεται σε πέντε κεφάλαια. Στο πρώτο κεφάλαιο, παρουσιάζονται οι κύριες απειλές των δικτύων των υπολογιστών, καθώς και των εικονικών τοπικών δικτύων.

Στο δεύτερο κεφάλαιο, εξετάζονται οι τεχνολογίες ασφάλειας περιφερειακής Άμυνας των Firewalls, οι κατηγορίες τους, καθώς και οι μηχανισμοί ασφάλειας εικονικών δικτύων. Επίσης, μελετάται και παρουσιάζεται ο τρόπος λειτουργίας των συστημάτων ανίχνευσης επιθέσεων (Intrusion Detection Systems, IDS) και των συστημάτων

ανίχνευσης βασισμένα στο υπολογιστικό σύστημα (Host και Network-based detection systems).

Στο τρίτο κεφάλαιο γίνεται μελέτη της χρήση των firewalls στην ασφάλεια των συστημάτων βιομηχανικού ελέγχου. Εξετάζονται οι διάφορες υποδομές των δικτύων, όπως ο κατακερματισμός τους σε μικρότερα δίκτυα και οι διάφορες πιθανές αρχιτεκτονικές καθώς και τα πλεονεκτήματα και τα μειονεκτήματα του καθενός.

Στο τέταρτο κεφάλαιο, παρουσιάζεται ο τρόπος της ασφάλειας των δικτύων των επιχειρήσεων της βιομηχανίας, με την χρήση των συστημάτων βιομηχανικού αυτομάτου ελέγχου και τηλεμετρίας (Supervisory Control and Data Acquisition, SCADA). Επίσης, παρουσιάζεται η αρχιτεκτονική των συστημάτων SCADA, για την καλύτερη κατανόηση του τρόπου λειτουργίας του.

Στο πέμπτο κεφάλαιο εξετάζεται η Ασφάλεια ασυρμάτων δικτύων στις επιχειρήσεις και στις βιομηχανίες, τα δίκτυα αποθήκευσης δεδομένων (Storage area networks, SANs) και η ασφάλεια της τηλεφωνίας μέσω διαδικτύου (Voice over IP , VoIP).

ΚΕΦΑΛΑΙΟ 2- ΑΣΦΑΛΕΙΑ ΣΤΑ ΔΙΚΤΥΑ

2.1. Εισαγωγή

“Η ανάγκη είναι η μητέρα της εφεύρεσης". Αυτό το ρητό ισχύει απόλυτα για την ασφάλεια δικτύων. Κατά τις πρώτες ημέρες του Διαδικτύου, τα εμπορικά συμφέροντα ήταν αμελητέα. Η συντριπτική πλειοψηφία των χρηστών ήταν εμπειρογνώμονες της έρευνας και της ανάπτυξης. Οι πρώτοι χρήστες σπάνια ασχολούνταν με δραστηριότητες που θα μπορούσαν να βλάψουν άλλους χρήστες. Το διαδίκτυο δεν ήταν ένα ασφαλές περιβάλλον, επειδή δεν χρειαζόταν να είναι.

Από νωρίς, η δικτύωση ένωνε ανθρώπους και μηχανές, μέσω των μέσων επικοινωνίας. Η δουλειά ενός networker ήταν να έχει τις συσκευές συνδεδεμένες ώστε να βελτιωθεί η ικανότητα των ανθρώπων να επικοινωνούν με πληροφορίες και ιδέες. Οι πρώτοι χρήστες του διαδικτύου δεν ξόδευαν πολύ χρόνο σκεπτόμενοι για το αν οι online δραστηριότητές τους παρουσίαζαν κάποια απειλή για το δίκτυο και τα δικά τους δεδομένα. Όταν εξαπολύθηκαν οι πρώτοι ιοί και η πρώτη επίθεση «άρνηση υπηρεσίας» (Denial Of Service), ο κόσμος άλλαξε για τους επαγγελματίες δικτύων. Προκειμένου να ανταποκριθούν στις ανάγκες των χρηστών, οι επαγγελματίες έμαθαν τεχνικές για τη διασφάλιση των δικτύων. Ο πρωταρχικός στόχος πολλών επαγγελματιών εξελίχθηκε από το σχεδιασμό, την κατασκευή και την ανάπτυξη των δικτύων για τη διασφάλιση των υφιστάμενων δικτύων.

Σήμερα, το Διαδίκτυο είναι ένα πολύ διαφορετικό δίκτυο σε σχέση με το ξεκίνημά του στη δεκαετία του 1960. Η δουλειά του επαγγελματία της ασφάλειας δικτύων περιλαμβάνει τη διασφάλιση ότι το ενδεδειγμένο προσωπικό είναι έμπειρο σε εργαλεία για την ασφάλεια δικτύων, τις διαδικασίες, τις τεχνικές, τα πρωτόκολλα και τις τεχνολογίες. Συνεπώς, είναι

απαραίτητο οι εταιρίες να διαχειρίζονται τις συνεχώς εξελισσόμενες απειλές για τα δίκτυα.

Δεδομένου ότι η ασφάλεια δικτύων έγινε αναπόσπαστο μέρος της καθημερινής λειτουργίας, προέκυψαν ζητήματα ασφάλειας των δικτύων στα οποία πραγματοποιούνταν η επικοινωνία των χρηστών και η ανταλλαγή των δεδομένων.

Ένα από τα πρώτα εργαλεία για την ασφάλεια δικτύων ήταν το σύστημα ανίχνευσης εισβολής (Intrusion Detection System), που αναπτύχθηκε για πρώτη φορά από την SRI International το 1984. Ένα σύστημα ανίχνευσης εισβολής, παρέχει σε πραγματικό χρόνο ανίχνευση ορισμένων τύπων επιθέσεων, ενώ βρίσκονται σε εξέλιξη. Αυτή η ανίχνευση επιτρέπει στους επαγγελματίες της ασφάλειας δικτύων, την γρήγορη καταπολέμηση των αρνητικών επιπτώσεων από αυτές τις επιθέσεις σε συσκευές δικτύου και στους χρήστες. Στα τέλη της δεκαετίας του 1990, το σύστημα πρόληψης των επιθέσεων (Intrusion prevention System), άρχισε να αντικαθιστά τη λύση του IDS. Οι συσκευές IPS επιτρέπουν την ανίχνευση της κακόβουλης δραστηριότητας και έχουν την ικανότητα να μπλοκάρουν αυτόματα την επίθεση σε πραγματικό χρόνο (Axelsson, 2009).

Εκτός από τις λύσεις των συστημάτων ανίχνευσης και πρόληψης εισβολών, η τεχνολογία του «τείχους προστασίας» (firewall) αναπτύχθηκε για να αποτρέψει την ανεπιθύμητη κυκλοφορία από την είσοδο που προβλέπονται στις περιοχές εντός ενός δικτύου, παρέχοντας έτσι περιμετρική ασφάλεια. Το 1988, η εταιρία «Digital Equipment Corporation» (DEC) δημιούργησε το πρώτο τείχος προστασίας δικτύων, με τη μορφή ενός φίλτρου πακέτων. Τα πρώτα αυτά firewalls έλεγχαν τα πακέτα για να δουν αν ταιριάζουν τα σύνολα των προκαθορισμένων κανόνων, με την επιλογή της αποστολής ή κατάργησης των πακέτων αναλόγως. Τα firewalls φιλτραρίσματος πακέτων, ελέγχουν κάθε πακέτο σε απομόνωση χωρίς να εξετάσουν αν ένα πακέτο είναι μέρος μιας υπάρχουσας σύνδεσης. Το 1989, η

AT & T Bell Laboratories ανέπτυξε το πρώτο «τείχος προστασίας ελέγχου κατάστασης» (stateful firewall). Όπως τα firewalls φιλτραρίσματος πακέτων, τα stateful firewalls χρησιμοποιούν προκαθορισμένους κανόνες για τη χορήγηση ή την απόρριψη της κυκλοφορίας. Σε αντίθεση με τα firewalls φιλτραρίσματος πακέτων, τα stateful firewalls παρακολουθούν εγκατεστημένες συνδέσεις και καθορίζουν αν ένα πακέτο ανήκει σε μια υπάρχουσα ροή δεδομένων, παρέχοντας μεγαλύτερη ασφάλεια και ταχεία επεξεργασία (Axelsson, 2009).

Τα πρωτότυπα firewalls ήταν χαρακτηριστικά λογισμικού που προστέθηκαν σε μια υπάρχουσα δικτύωση συσκευών, όπως οι δρομολογητές (routers). Με τον καιρό, πολλές εταιρίες ανάπτυξαν αυτόνομα, ή "προσηλωμένα" (dedicated) firewalls που ενεργοποιούσαν δρομολογητές (routers) και διακόπτες (switches) για να απαλλαγούν από τη μνήμη και τον επεξεργαστή υψηλής έντασης των πακέτων φιλτραρίσματος (Qing, 2005).

2.2. Απειλές

Η παραδοσιακή ασφάλεια βασίστηκε στη διαστρωμάτωση των προϊόντων και στη χρήση πολλαπλών φίλτρων. Ωστόσο, καθώς οι απειλές έγιναν πιο εξελιγμένες, αυτά τα φίλτρα απαιτήθηκαν για να εξεταστούν βαθύτερα τα επίπεδα ροής Δικτύων και Εφαρμογών. Οι απαιτήσεις ασφάλειας περιελάμβαναν πιο δυναμικές ενημερώσεις των πληροφοριών και μικρότερους χρόνους αντίδρασης σε απειλές. Για το λόγο αυτό, η εταιρία Cisco σχεδίασε την «υπηρεσία ασφάλειας λειτουργιών» (Security Intelligence Operations, SIO). Αυτή η υπηρεσία, βασίζεται στην τεχνολογία υπολογιστικού νέφους (cloud-based), και συνδέει παγκόσμια πληροφορίες απειλών, υπηρεσίες με βάση τη φήμη και εμπεριστατωμένη ανάλυση για τις συσκευές ασφαλείας δικτύων της Cisco για την παροχή ισχυρότερης προστασίας με ταχύτερους χρόνους απόκρισης (Qing, 2005).

Εκτός από την αντιμετώπιση των απειλών εκτός του δικτύου, οι επαγγελματίες της ασφάλειας δικτύων πρέπει επίσης να είναι προετοιμασμένοι για τις απειλές στο εσωτερικό του δικτύου. Οι εσωτερικές απειλές, είτε σκόπιμες είτε τυχαίες, μπορούν να προκαλέσουν ακόμη μεγαλύτερη ζημιά από ό,τι οι εξωτερικές απειλές λόγω της άμεσης πρόσβασης σε αυτά και τη γνώση του εταιρικού δικτύου και των δεδομένων. Παρά το γεγονός αυτό, έχει πάρει περισσότερα από 20 χρόνια μετά την εισαγωγή των εργαλείων και τεχνικών για την καταπολέμηση των εξωτερικών απειλών να αναπτυχθούν εργαλεία και τεχνικές για τον περιορισμό των εσωτερικών απειλών.

Ένα κοινό σενάριο για μια απειλή που προέρχεται από το εσωτερικό του δικτύου είναι ένας δυσαρεστημένος υπάλληλος με κάποιες τεχνικές δεξιότητες και την προθυμία να κάνει τη ζημιά. Οι περισσότερες απειλές από το εσωτερικό του δικτύου αναμοχλεύουν πρωτόκολλα και τεχνολογίες που χρησιμοποιούνται για το τοπικό δίκτυο (local area network, LAN) ή την υποδομή μεταγωγής. Αυτές οι εσωτερικές απειλές εμπίπτουν σε δύο κατηγορίες : α) Στην απάτη (spoofing) και β) στην άρνηση των υπηρεσιών (DoS) (Galbally & Marcel, 2014).

Οι επιθέσεις απάτης (spoofing) είναι επιθέσεις κατά την οποία μία συσκευή επιχειρεί να εμφανιστεί σαν κάποια άλλη με το να παραποιεί τα στοιχεία. Για παράδειγμα, το spoofing της φυσικής διεύθυνσης MAC (Media Access Control) συμβαίνει όταν ένας υπολογιστής δέχεται πακέτα δεδομένων με βάση τη διεύθυνση MAC άλλου υπολογιστή.

Οι επιθέσεις άρνησης υπηρεσίας, καθιστούν τους πόρους του υπολογιστή μη διαθέσιμους στους προβλεπόμενους χρήστες. Οι επιτιθέμενοι χρησιμοποιούν διάφορες μεθόδους για να εξαπολύσουν τις επιθέσεις άρνησης υπηρεσίας.

Ένας επαγγελματίας της ασφάλειας δικτύων, είναι σημαντικό να κατανοήσει τις μεθόδους που έχουν σχεδιαστεί ειδικά για τη στόχευση αυτών των τύπων απειλών και την εξασφάλιση της ασφάλειας των τοπικών δικτύων LAN. Εκτός από την πρόληψη και άρνηση των κακόβουλων κινήσεων, η ασφάλεια δικτύων προϋποθέτει επίσης ότι τα δεδομένα παραμένουν προστατευμένα. Η κρυπτογραφία, η μελέτη και η πρακτική της απόκρυψης πληροφοριών, χρησιμοποιείται διάχυτα στη σύγχρονη ασφάλεια δικτύων. Σήμερα, κάθε είδος της επικοινωνίας δικτύου έχει ένα αντίστοιχο πρωτόκολλο ή τεχνολογία που έχει σχεδιαστεί για να κρύψει αυτήν την επικοινωνία από οποιονδήποτε άλλο εκτός από τον προβλεπόμενο χρήστη (Galbally & Marcel , 2014).

Τα ασύρματα δεδομένα μπορεί να είναι κρυπτογραφημένα χρησιμοποιώντας διάφορες εφαρμογές κρυπτογραφίας. Η συνομιλία μεταξύ δύο χρηστών μέσω τηλεφώνου IP μπορεί να είναι κρυπτογραφημένη. Τα αρχεία σε έναν υπολογιστή μπορεί επίσης να κρυφτούν με κρυπτογράφηση. Αυτά είναι μόνο μερικά παραδείγματα. Η κρυπτογράφηση μπορεί να χρησιμοποιηθεί σχεδόν οπουδήποτε υπάρχει επικοινωνία δεδομένων. Στην πραγματικότητα, η τάση προς όλη την επικοινωνία κρυπτογραφείται (Galbally & Marcel , 2014).

Η κρυπτογραφία διασφαλίζει την εμπιστευτικότητα των δεδομένων, η οποία είναι ένα από τα τρία μέρη της ασφάλειας των πληροφοριών: Εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα.

Η ασφάλεια πληροφοριών ασχολείται με την προστασία των πληροφοριών και των πληροφοριακών συστημάτων από μη εξουσιοδοτημένη πρόσβαση, χρήση, αποκάλυψη, διατάραξη, τροποποίηση ή καταστροφή. Η κρυπτογράφηση παρέχει εμπιστευτικότητα, αποκρύπτοντας τα δεδομένα. Η ακεραιότητα των δεδομένων, (πράγμα που σημαίνει ότι τα δεδομένα διατηρούνται αναλλοίωτα κατά τη διάρκεια οποιασδήποτε λειτουργίας), επιτυγχάνεται με τη χρήση των μηχανισμών κατακερματισμού. Η

διαθεσιμότητα, η οποία είναι η προσβασιμότητα των δεδομένων, είναι εγγυημένη από τους μηχανισμούς σκλήρυνσης του δικτύου και τα εφεδρικά συστήματα (Gao et al., 2010).

2.3. Είδη επιθέσεων

Υπάρχουν πολλοί τρόποι για να διεισδύσει ένας κακόβουλος χρήστης σε ένα υπολογιστικό σύστημα μέσω δικτύου. Άλλοι στοχεύουν σε κακώς ρυθμισμένες δικτυακές υπηρεσίες, άλλοι βασίζονται σε γνωστές αδυναμίες δικτυακών πρωτοκόλλων, μερικοί ποντάρουν σε απροσεξίες των χρηστών μιας υπηρεσίας, ενώ υπάρχουν κι εκείνοι που συνδυάζουν όλες τις προηγούμενες μεθόδους. Η επιλογή της πλέον κατάλληλης μεθόδου διείσδυσης σε ένα δίκτυο φυσικά, εξαρτάται από τη συγκεκριμένη περίπτωση και τις επικρατούσες συνθήκες, κάτι που είναι δύσκολο να το γνωρίζει ακριβώς ο επιτιθέμενος. Για το λόγο αυτό οι περισσότερες επιθέσεις έχουν σαν πρώτο στάδιο την «αναγνώριση του εδάφους». Η μέθοδος αποκαλείται «ανίχνευση θύρας» (port scanning) και στοχεύει στην αναγνώριση των διαθέσιμων υπηρεσιών δικτύου, από τις οποίες θα μπορούσε να δοκιμάσει να εισχωρήσει ο επιτιθέμενος. Η διαδικασία περιλαμβάνει την απόπειρα πραγματοποίησης σύνδεσης σε γνωστές θύρες του διαδικτυακού πρωτοκόλλου IP (Internet Protocol). Η σύνδεση πολλές φορές δεν είναι απαραίτητο να ολοκληρωθεί για να πιστοποιηθεί η ύπαρξη ενός εξυπηρετητή (server) για τη συγκεκριμένη υπηρεσία, λόγω ιδιαιτεροτήτων των πρωτοκόλλων σύνδεσης. Στην περίπτωση αυτή, επειδή η απόπειρα δεν είναι ορατή στο υπολογιστικό σύστημα, μιλάμε για κρυφή ανίχνευση (stealth scanning). Η συγκέντρωση των στοιχείων διαθεσιμότητας δικτυακών υπηρεσιών επιτρέπει στον επιτιθέμενο, να προχωρήσει στο επόμενο στάδιο που είναι η εκμετάλλευση ενδεχόμενων αδυναμιών στη λειτουργία των υπηρεσιών αυτών.

Πολλές δικτυακές υπηρεσίες είχαν προβλήματα ασφαλείας κατά το παρελθόν. Ιδιαίτερα οι υπηρεσίες εκείνες που δημιουργήθηκαν την εποχή που το διαδίκτυο δεν είχε τη σημερινή του μορφή και η έμφαση στην ασφάλεια ήταν ανύπαρκτη, διαθέτουν μηχανισμούς με αμφίβολη χρησιμότητα υπό τις παρούσες συνθήκες. Μια τέτοια περίπτωση εκμεταλλεύεται μια επίθεση που αποκαλείται απόκτηση του πρωτοκόλλου μεταφοράς (File Transfer Protocol bounce). Στο πρωτόκολλο FTP χρησιμοποιείται η εντολή «PORT» για τη δήλωση της θύρας και της διεύθυνσης σύνδεσης για τη δημιουργία του ξεχωριστού καναλιού μετάδοσης των δεδομένων. Οι εξυπηρετητές (servers) που δεν πραγματοποιούν έλεγχο της καθοριζόμενης από το χρήστη διεύθυνσης IP, είναι δυνατόν να χρησιμοποιηθούν σαν ενδιάμεσοι για την πραγματοποίηση μεταφοράς δεδομένων σε μη εξουσιοδοτημένο υπολογιστή, παρακάμπτοντας τον έλεγχο πρόσβασης του εξυπηρετητή.

Παρόμοια περίπτωση είναι οι επιθέσεις στο πρωτόκολλο μεταφοράς υπερκειμένου (Hypertext Transfer Protocol) . Όπως και οι εξυπηρετητές FTP, έτσι και αυτοί εφαρμόζουν ένα σχήμα ελέγχου πρόσβασης πάνω στα περιεχόμενα του συστήματος αρχείων που διαθέτουν. Επειδή κατά κανόνα ο έλεγχος πρόσβασης μπορεί να γίνεται χωριστά σε κάθε υποκατάλογο, η χρήση των Ενιαίων Εντοπιστών Πόρων (Universal Resource Locators, URLs) που περιέχουν συμβολοσειρές του τόπου μπορεί να επιτρέψει την πρόσβαση σε υποκαταλόγους που δεν υπάγονται στο σύστημα ελέγχου πρόσβασης του εξυπηρετητή. Από τη στιγμή που ο επιτιθέμενος κατορθώσει να εισέλθει στο σύστημα και να αποκτήσει κάποια δικαιώματα πρόσβασης, ακολούθως θα προσπαθήσει να αυξήσει τα δικαιώματά του αυτά, προβιβαζόμενος σε υπερχρήστη (superuser), ή στην αντίστοιχη ιδιότητα που διαθέτει το δεδομένο λειτουργικό σύστημα (Vijayakuma et al., 2012).

Αρκεί να ανακαλύψει ένα πρόγραμμα με σφάλματα στο χειρισμό συμβολοσειρών εισόδου από τους χρήστες και να μεταχειριστεί κατάλληλα τη στοίβα εκτέλεσης του προγράμματος.

Μια άλλη τακτική για την απόκτηση ελέγχου, κυρίως σε υπολογιστές χρηστών, είναι η χρήση των ιών (viruses), των κακόβουλων δηλαδή προγραμμάτων. Τα προγράμματα αυτά έχουν τη δυνατότητα να μολύνουν άλλα προγράμματα, έτσι ώστε η εκτέλεση των τελευταίων να προκαλεί και την εκτέλεση των πρώτων. Με τον τρόπο αυτό μπορούν να εξασφαλίσουν και τη μετάδοσή τους από υπολογιστή σε υπολογιστή και να εξαπλωθούν σε ένα ολόκληρο δίκτυο. Η δράση τους εξαρτάται από το φορτίο τους (payload) και κατά κανόνα να περιλαμβάνει μια πρώτη σειρά μέτρων σίγησης των εφαρμογών ανίχνευσης διεισδύσεων και στη συνέχεια την εγκατάσταση κρυφών προγραμμάτων που ανοίγουν μια «πίσω πόρτα» στο σύστημα (back-door programs). Κάτι τέτοιο μπορεί να επιτευχτεί και με τη χρήση Δούρειων Ίππων (Trojan Horses). Οι Δούρειοι Ίπποι είναι κακόβουλα προγράμματα που φαινομενικά κάνουν κάποια χρήσιμη εργασία, αλλά στην πραγματικότητα χρησιμοποιούν αυτή τη λειτουργία σαν προκάλυμμα για την εκτέλεση προγραμμάτων που αναλαμβάνουν τον έλεγχο του συστήματος. Η αποτελεσματικότητά τους εξαρτάται άμεσα από τη δυνατότητά τους να ξεγελάσουν το χρήστη για την πραγματική τους ιδιότητα και από την πρακτική χρήσης του υπολογιστή του τελευταίου. Εάν κάποιος δεν εκτελεί ποτέ ξένες εφαρμογές στο σύστημα του, προφανώς είναι εξ ορισμού ασφαλής από Δούρειους Ίππους. Στην ίδια κατηγορία ανήκει και η περίπτωση των σκουληκιών (worms) που αναφέρθηκε και προηγουμένως. Τα σκουλήκια εξαπλώνονται σαν τους ιούς από μηχάνημα σε μηχάνημα, χρησιμοποιώντας οποιαδήποτε τεχνική τους δίνει τη δυνατότητα να μεταφερθούν και να εκτελεστούν σε ένα άλλο υποσύστημα (Vijayakuma et al, 2012).

2.3.1. Επιθέσεις εικονικών τοπικών δικτύων (Vlan επιθέσεις)

Ένα εικονικό τοπικό δίκτυο VLAN (Virtual Local Area Network), είναι ένας λογικός τομέας μετάδοσης που μπορεί να συνδέει πολλαπλά φυσικά τμήματα LAN. Τα VLANs παρέχουν κατάτμηση και οργανωτική ευελιξία. Μια δομή VLAN μπορεί να σχεδιαστεί για να επιτρέπει ομαδοποίηση των σταθμών λογικά από τη λειτουργία, ομάδα έργου, ή την εφαρμογή, χωρίς να λαμβάνεται υπόψη η γεωγραφική θέση των χρηστών. Κάθε θύρα διακόπτη μπορεί να ανατεθεί σε μία μόνο VLAN, προσθέτοντας έτσι ένα επίπεδο ασφαλείας. Θύρες σε ένα VLAN μοιράζουν μεταδόσεις. Οι θύρες σε διαφορετικά VLANs δεν μοιράζουν μεταδόσεις. Οι περιλαμβανόμενες μεταδόσεις μέσα σ'ένα VLAN βελτιώνουν τις συνολικές επιδόσεις του δικτύου (Kearns & Marmorstein, 2005).

Χρησιμοποιώντας την VLAN τεχνολογία, οι θύρες του δρομολογητή και οι συνδεδεμένοι χρήστες τους μπορούν να ομαδοποιηθούν σε λογικά ορισμένες κοινότητες, όπως οι συνεργάτες στο ίδιο τμήμα, μια σταυρό-λειτουργική ομάδα προϊόντος, ή διαφορετικές ομάδες χρηστών που μοιράζονται την ίδια εφαρμογή του δικτύου. Ένα VLAN μπορεί να υπάρχει σε ένα μόνο διακόπτη ή να συνδέει πολλούς διακόπτες.

Υπάρχει μια σειρά από διαφορετικούς τύπους VLAN επιθέσεων που επικρατούν στα σύγχρονα δίκτυα μεταγωγής. Αντί του καταρτισμού καταλόγου όλων των τύπων επιθέσεων, είναι σημαντικό να κατανοηθεί η γενική μεθοδολογία πίσω από αυτές τις επιθέσεις και τις κύριες προσεγγίσεις για τη καταπολέμησή τους (Kearns & Marmorstein, 2005).

Η αρχιτεκτονική VLAN απλοποιεί τη συντήρηση του δικτύου και βελτιώνει την απόδοση, αλλά ανοίγει το δρόμο για τη κατάχρηση. Υπό ορισμένες συνθήκες, οι επιτιθέμενοι μπορούν να εντοπίσουν τα δεδομένα και να εξάγουν τους κωδικούς πρόσβασης και άλλες ευαίσθητες πληροφορίες. Η επίθεση λειτουργεί εκμεταλλευόμενη τη λανθασμένα ρυθμισμένη ανοιχτή

θύρα. Από προεπιλογή, οι ανοιχτές θύρες έχουν πρόσβαση σε όλα τα VLANs και περνούν τη κίνηση για πολλαπλά VLANs σε όλη την ίδια φυσική σύνδεση, γενικά μεταξύ των δρομολογητών. Τα δεδομένα που διακινούνται μέσω αυτών των συνδέσεων μπορεί να εγκλείονται με το πρότυπο IEEE 802.1Q (Lee et al., 2008).

Σε μια βασική επίθεση VLAN, ο επιτιθέμενος εκμεταλλεύεται την προεπιλεγμένη αυτόματη ρύθμιση παραμέτρων των ανοιχτών θυρών στους δρομολογητές. Ο επιτιθέμενος του δικτύου διαμορφώνει ένα σύστημα ώστε να μοιάζει με ένα δρομολογητή. Αυτή την πλαστογράφηση απαιτεί ο εισβολέας του δικτύου για να είναι σε θέση να μιμηθεί ένα δρομολογητή (Lee et al., 2008).

ΚΕΦΑΛΑΙΟ 3 - FIREWALLS

3.1. Τεχνολογίες ασφάλειας περιφερειακής Άμυνας - Firewall

Ένας από τους αποτελεσματικότερους τρόπους για την προστασία του δικτύου από πιθανούς παραβάτες είναι η χρήση ενός συστήματος Firewall μεταξύ του τοπικού δικτύου και του διαδικτύου. Το Firewall, είναι ένα σύστημα ή μια ομάδα από συστήματα που επιβάλλει μια πολιτική ελέγχου πρόσβασης μεταξύ δύο δικτύων και αποτελεί μια στρατηγική για την προστασία των πόρων ενός οργανισμού, ορατού στο διαδίκτυο. Το Firewall εξασφαλίζει ότι όλη η επικοινωνία μεταξύ του δικτύου μιας επιχείρησης με το διαδίκτυο είναι σύμφωνη με την πολιτική ασφάλειας της επιχείρησης.

Για να το πετύχει αυτό, το σύστημα του Firewall πρέπει να εντοπίζει και να ελέγχει όλη τη ροή επικοινωνίας. Για να ελέγξει τις υπηρεσίες που βασίζονται στο πρωτόκολλο ελέγχου μεταφοράς (Transmission Control Protocol) (να επιτρέψει, απορρίψει, κρυπτογραφήσει ή καταγράψει την επικοινωνία), το Firewall πρέπει να λαμβάνει, να αποθηκεύει και να διαχειρίζεται πληροφορίες που προέρχονται από όλα τα επίπεδα επικοινωνίας και από άλλες εφαρμογές. Οι συσκευές Firewall ενώ συχνά είναι απαραίτητες για την προστασία ενός διαδικτυακού τόπου, αποτελούν και πηγή κινδύνου, γιατί οι χρήστες πιστεύουν ότι από την στιγμή που αγοράσθηκε το προϊόν, η ασφάλεια έχει εξασφαλισθεί, πράγμα που απέχει πολύ από την πραγματικότητα, και επιπλέον ο ίδιος ο κώδικας είναι πιθανόν να μην συμπεριφέρεται όπως θα έπρεπε, με αποτέλεσμα να αφήνει τις πίσω θύρες (backports) ανοικτές.

Ένα firewall αποτελείται από τα εξής (Zhou et al., 2007):

• Φίλτρα για μπλοκάρισμα ή παρακολούθηση μετάδοσης συγκεκριμένου είδους μηνυμάτων (καθορισμένα από τον τύπο, τον προορισμό τους ή συνδυασμό και των δύο).

• Δρομολογητές για προώθηση των αποδεκτών μηνυμάτων από τη μια μεριά του firewall σε κάποια άλλη.

Μερικά από τα σημαντικότερα πλεονεκτήματα της χρήσης των firewalls συνοψίζονται παρακάτω (Zhou et al., 2007):

Προστασία από ευπαθείς υπηρεσίες. Βελτιώνει την ασφάλεια δικτύων και μειώνει τους κινδύνους που προέρχονται από ευαίσθητες υπηρεσίες του πρωτοκόλλου. Έτσι το δίκτυο εκτίθεται σε λιγότερους κινδύνους, δεδομένου ότι μόνο τα επιλεγμένα πρωτόκολλα θα είναι σε θέση να περάσουν μέσω της ζώνης περιφερειακής άμυνας που υλοποιεί το firewall.

• *Ελεγχόμενη πρόσβαση.* Το firewall παρέχει τη δυνατότητα ελέγχου της πρόσβασης στα συστήματα του προστατευόμενου δικτύου. Η λεπτομέρεια του ελέγχου μπορεί να φτάσει έως και στο επίπεδο μιας υπηρεσίας ενός πρωτοκόλλου.

• *Συγκεντρωμένη ασφάλεια.* Ένα firewall μπορεί πραγματικά να είναι λιγότερο ακριβό για ένα οργανισμό όταν διαχειρίζεται λογισμικό το οποίο εναλλακτικά έπρεπε να είναι κατανεμημένο σε διάφορους υπολογιστές του δικτύου. Ιδιαίτερα τα συστήματα ταυτοποίησης, όπως τα συνθηματικά μιας χρήσης ή τα συστήματα αυθεντικοποίησης θα είναι πιο ασφαλή αν είναι εγκατεστημένα κεντρικά στο σύστημα του firewall παρά σε άλλα συστήματα που πρέπει να προσεγγιστούν από το διαδίκτυο.

Μια πολιτική ασφάλειας για διαδικτυακά πληροφοριακά συστήματα που αναπτύσσεται με την χρήση των τεχνολογιών firewall, θα πρέπει να αξιοποιεί τα παρακάτω χαρακτηριστικά (Collin, 2009):

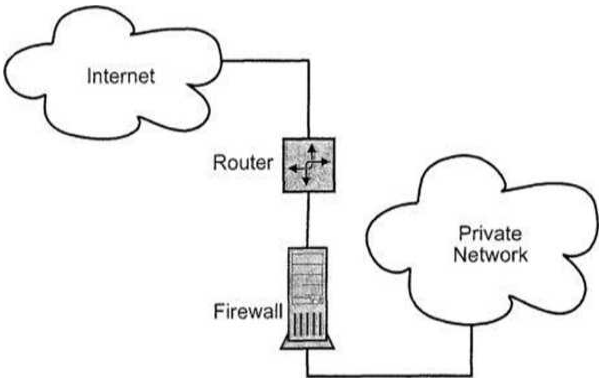
• Ορατότητα. Το firewall πρέπει να είναι το μόνο ορατό σημείο προς το διαδίκτυο, έτσι ώστε να προστατεύεται το πληροφοριακό σύστημα.

• Πιστοποίηση. Η πιστοποίηση χρηστών θα πρέπει να υλοποιείται εξ ολοκλήρου επάνω στο firewall.

• Διαχείριση. Η Διοίκηση και η διαχείριση ενός firewall, θα πρέπει να θεωρείται σημαντικό ζήτημα ασφάλειας, και δεν θα πρέπει να διενεργείται από απόσταση.

3.2. Firewalls

Τα firewalls, είναι μια τεχνολογία που πρωτοεμφανίστηκε στις αρχές της δεκαετίας του '90. Ο σκοπός τους είναι να προστατεύσουν τα συστήματα στο εσωτερικό του δικτύου ευθύνης τους από ανεπιθύμητες απόπειρες πρόσβασης από εξωτερικούς χρήστες. Για το λόγο αυτό αποκαλούνται και μηχανισμοί περιμετρικής άμυνας, καθώς ορίζουν ένα ιδεατό τείχος που προστατεύει το περικλειόμενο δίκτυο από επιθέσεις. Η εικόνα 3.1 απεικονίζει μια ευρύτατα διαδεδομένη διάταξη δικτύου προστατευόμενου από firewall (Collin, 2009).



Εικόνα 3.1- Τυπική διάταξη firewall

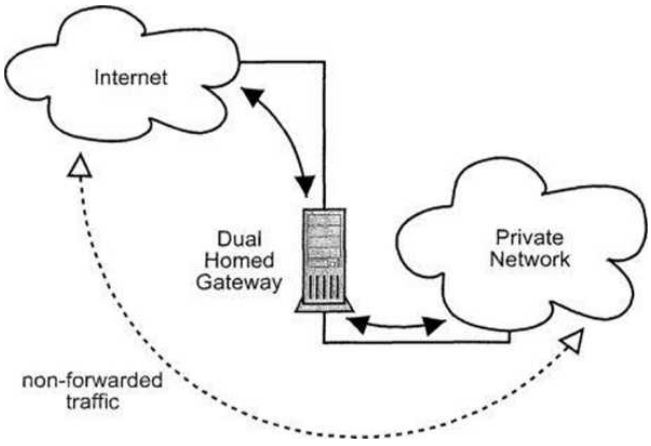
Ο τρόπος λειτουργίας των firewalls χωρίζεται σε διάφορες κατηγορίες. Η πιο κοινή από αυτές είναι οι δρομολογητές ελέγχου (screening routers). Αυτοί δεν είναι παρά απλοί δρομολογητές με την επιπλέον δυνατότητα να εμποδίζουν τη διακίνηση δεδομένων μεταξύ υποδικτύων ή υπολογιστών, βασιζόμενοι στο είδος της δικτυακής υπηρεσίας που αυτά αφορούν. Η διάταξή τους είναι αυτή που φαίνεται στην εικόνα 3.1, εάν θεωρηθούν ο δρομολογητής και το firewall σαν μία οντότητα. Τα πλεονεκτήματά τους είναι η ευκολία εγκατάστασης και λειτουργίας και η μηδαμινή επίδρασή τους στη λειτουργία του δικτύου. Το βασικό τους μειονέκτημα είναι το ότι καθιστούν δυνατή την επικοινωνία μεταξύ των υπολογιστών του εσωτερικού δικτύου και του έξω κόσμου. Εάν δεν έχουν οριστεί κανόνες που να αποτρέπουν κάποιες υπηρεσίες ή πρωτόκολλα δικτύου από το να διασχίζουν το firewall, τότε αυτά είναι δυνατό να χρησιμοποιηθούν για να ξεπεράσουν το εμπόδιο αυτό. Κατά συνέπεια το μοντέλο λειτουργίας τους συνοψίζεται στο: «ότι δεν απαγορεύεται ρητά, επιτρέπεται»(Collin, 2009).

Την αντίθετη προσέγγιση ακολουθεί η κατηγορία των «δρομολογητών διπλής κατεύθυνσης» (dual homed gateways). Αυτά αποτελούνται από ένα υπολογιστικό σύστημα που συνδέεται τόσο στο εσωτερικό, όσο και στο εξωτερικό δίκτυο, όπως φαίνεται και στην εικόνα 3.2.

Η διαφορά όμως έγκειται στο ότι δεν πραγματοποιούν προώθηση των IP πακέτων από το ένα σημείο σύνδεσής τους στο άλλο. Αν και το ίδιο το firewall μπορεί να επικοινωνήσει και με το εσωτερικό και με το εξωτερικό δίκτυο, ούτε ο έξω κόσμος μπορεί να μιλήσει απευθείας με τους υπολογιστές του εσωτερικού δικτύου, ούτε οι τελευταίοι μπορούν να έχουν απευθείας πρόσβαση προς τα έξω. Κατά συνέπεια για να δοθεί η δυνατότητα επικοινωνίας, θα πρέπει αυτό να διαθέτει τις εφαρμογές δρομολογητών μεσολάβησης (application proxies), που δεν είναι παρά εφαρμογές με το

μοναδικό καθήκον να μεσολαβούν για την πραγματοποίηση των συνδέσεων διαμέσου του firewall (Misherghi et al., 2008).

Το καταφανές πλεονέκτημα αυτής της προσέγγισης είναι ότι ακολουθεί το συντηρητικό μοντέλο: «ότι δεν επιτρέπεται ρητά, απαγορεύεται». Το βασικό της μειονέκτημα είναι η υποχρέωση ύπαρξης κατάλληλων δρομολογητών μεσολάβησης, για όλες τις δικτυακές υπηρεσίες που είναι επιθυμητό να διασχίζουν το firewall. Ένα επιπλέον μειονέκτημα εμφανίζεται στις περιπτώσεις εκείνες που το firewall χρησιμοποιείται για να πραγματοποιήσει συνδέσεις απομακρυσμένου τερματικού οι χρήστες του εσωτερικού δικτύου, με πρωτόκολλα όπως το πρωτόκολλο επικοινωνίας διασυνδεδεμένων (σε δίκτυο) υπολογιστών TELNET (TELe communication NETwork). Η μέθοδος αυτή μπορεί να εξαλείψει την αναγκαιότητα των δρομολογητών μεσολάβησης καθώς οι χρήστες συνδέονται πρώτα στο firewall και κατόπιν στο υπόλοιπο δίκτυο, αλλά δίνει τη δυνατότητα σε έναν επιτιθέμενο να παρακάμψει το firewall «σπάζοντας» τον κωδικό ενός μόνο χρήστη του εσωτερικού δικτύου. Για το λόγο αυτό τέτοιες υλοποιήσεις είναι αρκετά περιορισμένες (Misherghi et al., 2008) .

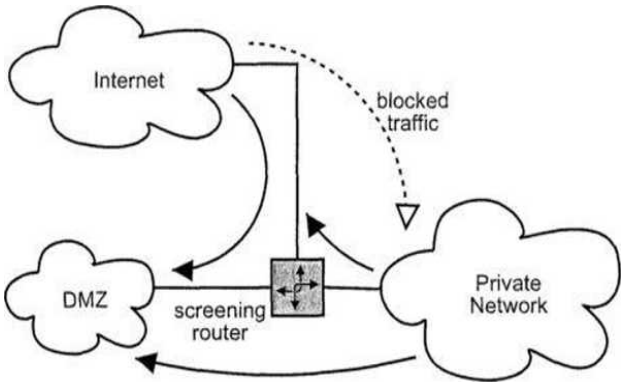


Εικόνα 3.2- dual homed gateways

Πηγή: (Misherghi et al., 2008)

Μια ενδιάμεση προσέγγιση προτείνουν τα υποδίκτυα ελέγχου πρόσβασης (screened subnets), υποκατηγορία των οποίων είναι και οι δρομολογητές ελέγχου (screened host gateways) όπως παρουσιάζονται στην εικόνα 3.3. Σε αυτή την περίπτωση, το εσωτερικό δίκτυο είναι απομονωμένο από τον έξω κόσμο μέσω ενός screening router ή ενός dual homed gateway, το οποίο δεν επιτρέπει την πρόσβαση από έξω στα μηχανήματα του εσωτερικού δικτύου, με την εξαίρεση ενός συγκεκριμένου υποδικτύου, το οποίο διαθέτει όλες τις δικτυακές υπηρεσίες που είναι πιθανόν να ζητηθούν από τους εξωτερικούς χρήστες. Το υποδίκτυο αυτό αποκαλείται συχνά «αποστρατικοποιημένη ζώνη» (demilitarized zone, DMZ).

Επίσης, η πρόσβαση στα μηχανήματα του εσωτερικού δικτύου δεν είναι επιτρεπτή πολλές φορές ούτε από τα μηχανήματα που βρίσκονται στο DMZ. Αντίθετα οι εσωτερικοί χρήστες μπορούν να συνδεθούν απρόσκοπτα σε όλα τα εξωτερικά δίκτυα, για κάθε επιτρεπόμενη υπηρεσία. Με τον τρόπο αυτό μπορεί κανείς να περιορίσει την εντατική παρακολούθηση των συστημάτων του για παραβιάσεις, μονάχα στα συστήματα που βρίσκονται στο DMZ. Κάτι τέτοιο μειώνει αρκετα το διαχειριστικό φόρτο του υπεύθυνου ασφαλείας, χωρίς να θυσιάζονται το μεγαλύτερο μέρος από τα πλεονεκτήματα των screened subnets ή των screened host gateways.



Εικόνα 3.3- screened host gateways

3.3. Μηχανισμοί ασφάλειας Εικονικού Ιδιωτικού Δικτύου

Το Εικονικό Ιδιωτικό Δίκτυο (Virtual Private Network, VPN) εγκαθιστά μια ασφαλή σύνδεση από άκρο σε άκρο (end-to-end secure link) μεταξύ πολλαπλών τοποθεσιών σε ένα δημόσιο δίκτυο δεδομένων (Salah et al., 2012).

Οι δομικές μονάδες και υπηρεσίες ενός Εικονικού Ιδιωτικού Δικτύου είναι (Stallings, 2011)

• Ασφάλεια (Security)

• Ποιότητα παρεχόμενης υπηρεσίας (Quality Of Services, QoS)

• Δυνατότητες Διαχείρισης (Manageability)

• Αξιοπιστία (Reliability)

Τα VPNs χωρίζονται βασικά σε τρεις κατηγορίες:

• Πρόσβασης (Access VPNs), τα οποία χρησιμοποιούνται για τη σύνδεση τηλεργατών (telecommuters) και μη-σταθερών χρηστών (mobile users) σε εσωτερικά δίκτυα (Intranets) και εξωτερικά δίκτυα (Extranets) οργανισμών.

• Εικονικά εσωτερικά δίκτυα (Intranet VPNs), τα οποία συνδέουν κεντρικά και περιφερειακά τμήματα ενός οργανισμού (π.χ. Νοσοκομεία και Κέντρα Υγείας) σε ένα «ιδιωτικό» δίκτυο.

• Εικονικά εξωτερικά δίκτυα (Extranet VPNs), τα οποία επεκτείνουν αυτές τις υπηρεσίες εκτός οργανισμού για να συνδέσουν πελάτες και συνεργάτες. Τρία κύρια πρωτόκολλα έχουν προταθεί για την υλοποίηση VPN

τα οποία εφαρμόζονται επάνω στο επίπεδο Διαδικτύου και πάνω στο επίπεδο μεταφοράς του IP πρωτοκόλλου:

1) Το Point -To-Point Tunneling Protocol (PPTP)
2) το Layer-2 tunneling Protocol (L2TP) και
3) το IP security protocol

Ο πιο διαδεδομένη αρχιτεκτονική υλοποίησης των VPN είναι αυτή που βασίζεται σε firewalls. Αυτό δεν σημαίνει βέβαια ότι αυτού του τύπου τα VPN υπερτερούν σε σχέση με τα υπόλοιπα, απλά οι περισσότεροι οργανισμοί που αυτή τη στιγμή είναι συνδεδεμένοι στο Internet διαθέτουν firewalls, με αποτέλεσμα το μόνο που χρειάζεται να είναι η προσθήκη κατάλληλου λογισμικού που υλοποιεί την κρυπτογράφηση (Stallings, 2011).

3.4. Συστήματα ανίχνευσης επιθέσεων

Τα συστήματα ανίχνευσης διεισδύσεων (Intrusion Detection Systems, IDS) αποτελούν μια τεχνολογία που έχει γνωρίσει σημαντική διάδοση τα τελευταία χρόνια. Όπως φαίνεται και από την ονομασία τους, ο σκοπός τους είναι η ανίχνευση επιθέσεων που έχουν διαπεράσει την πρώτη γραμμή άμυνας ενός δικτύου, η οποία κατά κανόνα απαρτίζεται από firewalls και η ανίχνευση επιθέσεων που προέρχονται από το εσωτερικό του προστατευόμενου δικτύου. Τα συστήματα αυτά σε περιπτώσεις απειλών εφαρμόζουν μια τακτική αντίδρασης, κατά προτίμηση σε πραγματικό χρόνο, αντίθετα με την προληπτική πρακτική που ακολουθούν τα firewalls και διάφοροι μηχανισμοί ελέγχου πρόσβασης. Βασίζονται στην υπόθεση ότι είναι πρακτικά ανέφικτο να αποφευχθούν όλες οι παραβιάσεις ασφαλείας σε μεγάλο χρονικό διάστημα και αντίθετα δίνουν έμφαση στην ανάγκη επισήμανσης, ει δυνατόν σε πραγματικό χρόνο, τέτοιων γεγονότων και στην εκτίμηση των ζημιών που επέφεραν (Salah et al., 2012).

Το μοντέλο λειτουργίας τους προσπαθεί να εντοπίσει επιθετική δραστηριότητα χρησιμοποιώντας αλγορίθμους αναγνώρισης προτύπων και στατιστικά μοντέλα αναπαράστασης της φυσιολογικής συμπεριφοράς ενός συστήματος. Αν και οι πρώτες εργασίες στο χώρο εμφανίστηκαν τη δεκαετία του '80, η προσέγγιση της ανίχνευσης επιθέσεων αντί της αποτροπής τους μελετήθηκε εκτενέστερα τη δεκαετία του '90. Συγκεκριμένα, το 1980, ο James Anderson ήταν ο πρώτος που πρότεινε τη χρησιμοποίηση των αρχείων καταγραφής (audit logs) για την παρακολούθηση απειλών σε υπολογιστικά συστήματα . Η σημασία τέτοιων πληροφοριών δεν είχε γίνει κατανοητή εκείνη την εποχή και όλες οι διαθέσιμες διαδικασίες ασφάλειας συστημάτων στόχευαν στην απαγόρευση πρόσβασης σε ευαίσθητα δεδομένα από μη εξουσιοδοτημένα πρόσωπα. Το 1987, η Dorothy Denning παρουσίασε το αφηρημένο μοντέλο ενός συστήματος ανίχνευσης διεισδύσεων (Salah et al., 2012).

Αυτή η δημοσίευση ήταν η πρώτη που πρότεινε την έννοια της ανίχνευσης διεισδύσεων σαν μια λύση στο πρόβλημα της ασφάλειας υπολογιστικών συστημάτων.

Το 1988, την ίδια χρονιά με το Internet worm, η Teresa Lunt και οι συνεργάτες της επέκτειναν το μοντέλο που είχε προτείνει η Denning και δημιούργησαν το IDES (Intrusion Detection Expert System). Αυτό το σύστημα ήταν σχεδιασμένο με τέτοιο τρόπο, ώστε να μπορεί να ανιχνεύει επιθέσεις ενάντια σε ένα μόνο υπολογιστή. Μια βελτιωμένη έκδοσή του κατασκευάστηκε το 1995, το NIDES (Next-generation Intrusion Detection Expert System). Επίσης το 1988 κατασκευάστηκε το λογισμικο Haystack για να βοηθήσει στον έλεγχο παραβιάσεων ασφαλείας στους κεντρικούς υπολογιστές (mainframes) των αεροπορικών βάσεων στις Η.Π.Α., και το MIDAS (Multics Intrusion Detection and Alerting System) για το MULTICS (Multiplexed Information and Computing Service) mainframe του αμερικανικού κέντρου ασφαλείας υπολογιστών (National Computer Security Center).

Το 1989 εμφανίστηκε το Wisdom and Sense (1990) από το Los Alamos National Laboratory και το Information Security Officer's Assistant (ISOA), από την εταιρία «Planning Research Corporation». Μια καινούργια τεχνική εισήγαγε το 1990 το NSM (Network Security Monitor) (Hebe, 1990), το οποίο στη συνέχεια μετονομάστηκε σε Network Intrusion Detector (NID): αντί να εξετάζει τα αρχεία καταγραφής ενός υπολογιστικού συστήματος, εντόπιζε την ύποπτη συμπεριφορά παρακολουθώντας παθητικά τη δικτυακή κυκλοφορία σε ένα τοπικό δίκτυο. Το 1991 μια διαφορετική ιδέα παρουσιάστηκε από το NADIR (Network Anomaly Detection and Intrusion Reporter) και το DIDS (Distributed Intrusion Detection System) (Snap, 1991): τα δεδομένα ανίχνευσης από πολλαπλούς υπολογιστές συγκεντρώνονταν και συνδυάζονταν για να ανιχνεύσουν συντονισμένες επιθέσεις εναντίον ενός συνόλου υπολογιστικών συστημάτων (Salah et al., 2012).

Το 1994 ο Mark Crosbie και ο Gene Spafford πρότειναν τη χρήση των αυτόνομων πρακτόρων (autonomous agents) στοχεύοντας στην καλύτερη κλιμάκωση (scalability), συντήρηση (maintainability), αποτελεσματικότητα (efficiency) και ανοχή σε σφάλματα (fault tolerance) ενός συστήματος ανίχνευσης διεισδύσεων. Μια άλλη προσέγγιση για την αντιμετώπιση του προβλήματος της καλής κλιμάκωσης των συστημάτων αυτών έγινε το 1996, με το σχεδίασμα και την υλοποίηση των συστημάτων ανίχνευσης επιθέσεων βασισμένων σε γραφήματα (Graph-Based Intrusion Detection System, GrIDS). Το τελευταίο διευκολύνει τον εντοπισμό συντονισμένων επιθέσεων μεγάλης κλίμακας, οι οποίες μπορεί να καλύπτουν χωριστά αυτοδιαχειριζόμενα δίκτυα (Dorothy, 1986).

Και καθώς η έρευνα στο χώρο συνεχίζεται, το μοντέλο της ανίχνευσης διεισδύσεων αρχίζει να χρησιμοποιείται και για την επίλυση των προβλημάτων ασφαλείας συναφών τεχνολογικών περιοχών, όπως τα κινητά δίκτυα επικοινωνιών (mobile networks). Για την ταξινόμηση όλων αυτών των

συστημάτων όμως, καθώς και άλλων που δεν έχουν αναφερθεί, έχουν προταθεί ορισμένες κατηγοριοποιήσεις που θα εξεταστούν στη συνέχεια.

Μια παραδοσιακή κατηγοριοποίηση των συστημάτων ανίχνευσης επιθέσεων είναι αυτή των συστημάτων ανίχνευσης ανωμαλιών (anomaly detection systems) και των συστημάτων ανίχνευσης κακής χρήσης (misuse detection systems).

Το μοντέλο των συστημάτων ανίχνευσης ανωμαλιών επινοεί μια σειρά από στατιστικές μετρήσεις για τη μοντελοποίηση της συμπεριφοράς μιας οντότητας, όπως ένας χρήστης, μια ομάδα χρηστών ή ένα υπολογιστικό σύστημα. Το προφίλ ενός χρήστη για παράδειγμα, μπορεί να περιλαμβάνει πληροφορίες όπως η μέση χρονική διάρκεια των συνδέσεων TELNET και FTP που πραγματοποιεί, το πλήθος των bytes που μεταφέρει προς τις δύο κατευθύνσεις, την ώρα και τα τερματικά από τα οποία συνήθως συνδέεται, κ.ο.κ.

Το προφίλ ενός υπολογιστικού συστήματος από την άλλη, μπορεί να διαθέτει τη μέση χρησιμοποίηση της κεντρικής μονάδας επεξεργασίας (CPU), το μέσο αριθμό συνδεδεμένων χρηστών, κλπ. Το σύστημα παρακολουθεί τη λειτουργία ενός υπολογιστικού συστήματος και συνεχώς συγκρίνει το προφίλ μιας οντότητας, π.χ. ενός χρήστη, με αυτό που βρίσκεται αποθηκευμένο στη βάση δεδομένων του.

Στην περίπτωση που διαπιστωθεί «μεγάλη» απόκλιση από την κανονική συμπεριφορά σημαίνει συναγερμό στον υπεύθυνο ασφαλείας. Το μέγεθος της «μεγάλης» απόκλισης ορίζεται σαν ένα κατώφλι που έχει καθοριστεί από το σύστημα ή από τον υπεύθυνο ασφαλείας. Συνήθως τα αποθηκευμένα προφίλ ανανεώνονται περιοδικά για να προσαρμοστούν στις αλλαγές της συμπεριφοράς του χρήστη ή του συστήματος. Ένα από τα βασικά προβλήματα αυτού του μοντέλου είναι ο μεγάλος αριθμός λανθασμένων θετικών ανιχνεύσεων (false positives) που δημιουργεί,

θεωρώντας λανθασμένα νόμιμες χρήσεις των συστημάτων σαν παράνομες (McAfee, 2017).

Ένα άλλο γεγονός είναι ότι αντανακλούν την πολωμένη άποψη αυτού που θέτει τα κατώφλια σήμανσης συναγερμού. Μιας και αυτό το μοντέλο λειτουργεί ψάχνοντας για αποκλίσεις από την ομαλή λειτουργία του συστήματος, αποκαλείται μοντέλο ανίχνευσης ανωμαλιών. Το μοντέλο των συστημάτων ανίχνευσης κακής χρήσης από την άλλη, λειτουργεί αναζητώντας ίχνη γνωστών επιθέσεων που έχουν αποθηκευτεί στη βάση δεδομένων του. Η γνώση των επιθέσεων είναι κωδικοποιημένη σαν ένα σύνολο από υπογραφές (signatures), οι οποίες είναι ουσιαστικά πρότυπα ή ίχνη (patterns) που εμφανίζονται κάθε φορά που πραγματοποιείται μια επίθεση. Ο τρόπος με τον οποίο μια επίθεση αναπαρίσταται μέσα στο σύστημα είναι ένα σημαντικό χαρακτηριστικό της λειτουργίας του. Μερικά συστήματα χρησιμοποιούν διάφορα είδη γράφων, άλλα χρησιμοποιούν κανονικές εκφράσεις, κ.ά.

Ο τρόπος λειτουργίας του μοντέλου αυτού είναι παρεμφερής με αυτόν των προγραμμάτων καταπολέμησης ιών (anti-virus scanners). Η υλοποίηση ενός τέτοιου IDS συνήθως περιλαμβάνει ένα έμπειρο σύστημα που πραγματοποιεί τον έλεγχο των δεδομένων ανίχνευσης με βάση το αποθηκευμένο σύνολο κανόνων. Μια προφανής δυσκολία σε αυτή την αρχιτεκτονική είναι η ανάγκη για συνεχή ενημέρωση του συνόλου κανόνων ανίχνευσης, καθώς ανακαλύπτονται νέα είδη επιθέσεων. Μια και το μοντέλο λειτουργεί ψάχνοντας για ίχνη που αναπαριστούν γνωστές επιθέσεις, αποκαλείται μοντέλο ανίχνευσης κακής χρήσης.

3.5. Συστήματα ανίχνευσης βασισμένα στο υπολογιστικό σύστημα (Host και Network-based detection systems)

Τα συστήματα ανίχνευσης βασισμένα στο υπολογιστικό σύστημα, παρακολουθούν την δραστηριότητα σε ένα υπολογιστικό σύστημα, ή σε ένα δίκτυο υπολογιστών (McAfee, 2017).

Στην πρώτη περίπτωση έχουμε τα συστήματα ανίχνευσης βασισμένα στο υπολογιστικό σύστημα (Host-based detection systems), ενώ στη δεύτερη έχουμε τα συστήματα ανίχνευσης βασισμένα στο δίκτυο (Network-based detection systems). Τα πρώτα συστήματα που κατασκευάστηκαν εξέταζαν τα δεδομένα ανίχνευσης σε ένα μηχάνημα και έβγαζαν τα συμπεράσματά τους με βάση αποκλειστικά αυτή την πληροφορία. Κατά συνέπεια δεν μπορούσαν να εντοπίσουν επιθέσεις που προέρχονταν από πολλές πηγές ή επιθέσεις που κατευθύνονταν σε πολλαπλά μηχανήματα σε ένα δίκτυο. Επίσης, τα συστήματα ανίχνευσης βασισμένα στο υπολογιστικό σύστημα στηρίζονται ιδιαίτερα στα αρχεία καταγραφής που παρέχει το λειτουργικό σύστημα του υπολογιστή. Αυτό είναι κάτι που τα καθιστά άμεσα εξαρτώμενα από το συγκεκριμένο λειτουργικό σύστημα (architecture-dependent) και πιο ευάλωτα σε επιθέσεις άρνησης υπηρεσίας (Denial of Service attacks, DoS) ενάντια στο σύστημα ανίχνευσης, καθώς ο επιτιθέμενος μπορεί να κατορθώσει να καθυστερήσει το μηχανισμό καταγραφής ή να τον απενεργοποιήσει εντελώς.

Ένα άλλο πρόβλημα που προκύπτει είναι το επιπλέον φορτίο που δημιουργούν στο υπό παρακολούθηση σύστημα. Μια αποτελεσματική λύση σε αυτά τα προβλήματα παρέχεται από τα συστήματα ανίχνευσης βασισμένα στο δίκτυο. Αυτά καθώς παρακολουθούν παθητικά το δίκτυο για ύποπτη δραστηριότητα, είναι ουσιαστικά ανεξάρτητα από τα λειτουργικά συστήματα των υπολογιστών που προστατεύουν και μπορούν να επιβλέψουν ετερογενή δίκτυα χωρίς δυσκολία. Ούτως ή άλλως με το σημερινό επίπεδο δικτύωσης του κόσμου, πρακτικά κάθε επίθεση πραγματοποιείται μέσω του δικτύου. Το κυριότερο πρόβλημα τους, είναι η ραγδαίες μεταβολές στην ταχύτητα των δικτύων, που καθιστά δύσκολη την απορρόφηση όλων των δεδομένων που κυκλοφορούν. Τα σύγχρονα συστήματα χειρίζονται με άνεση φορτίο σε ασύρματα τοπικά δίκτυα (Wireless Area Networks) και τα ενσύρματα τοπικά δίκτυα (Local Area Networks) μέχρι τα 100Mbps, ενώ πολλά αντέχουν ακόμη και σε ταχύτητες 1000Mbps. Τα σύγχρονα όμως δίκτυα της κατηγορίας

Gigabit Ethernet στο Gbps είναι εξαιρετικά δύσκολο να παρακολουθηθούν αποτελεσματικά.

Εκτός από τα συστήματα που ανήκουν στις προηγούμενες κατηγορίες, έχουν προταθεί και άλλα τα οποία δεν μπορούν να ενταχθούν άμεσα σε κάποια από αυτές. Τα συστήματα αυτά δημιουργήθηκαν είτε για να προσφέρουν μια λύση σε αδυναμίες των προηγουμένων, είτε για να αντιμετωπίσουν το πρόβλημα από μια εντελώς διαφορετική οπτική γωνία. Στην πρώτη κατηγορία ανήκει το σύστημα ανίχνευσης εισβολής με βάση το γράφημα (Graph-Based Intrusion Detection System, GrIDS), που κατασκευάστηκε από την ομάδα «Computer Security Research Group» του «University of California at Davis». Σκοπός του ήταν η ανίχνευση επιθέσεων μεγάλης κλίμακας, μέσω του συγκερασμού φορτίων σε διάφορες δικτυακές συνδέσεις. Το GrIDS χρησιμοποιεί εσωτερικά μια δομή γραφήματος για την αναπαράσταση της κατάστασης του δικτύου. Οι κόμβοι αναπαριστούν υπολογιστικά συστήματα, ενώ οι ακμές αντιστοιχούν σε δικτυακές συνδέσεις Για την προσέγγιση αυτή θα γίνει εκτενέστερη αναφορά και στα επόμενα κεφάλαια.

ΚΕΦΑΛΑΙΟ 4- ΧΡΗΣΗ ΤΩΝ FIREWALLΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΒΙΟΜΗΧΑΝΙΚΟΥ ΕΛΕΓΧΟΥ

4.1. Εισαγωγή

Όταν σχεδιάζεται μια αρχιτεκτονική δικτύου για την ανάπτυξη ενός συστήματος βιομηχανικού ελέγχου (Industrial Control System, ICS), συνίσταται ο διαχωρισμός του δικτύου ICS από το εταιρικό δίκτυο. Η φύση της κυκλοφορίας δικτύου σε αυτά τα δύο δίκτυα είναι διαφορετική: η πρόσβαση στο Internet, το FTP (File Transfer Control), το ηλεκτρονικό ταχυδρομείο και η απομακρυσμένη πρόσβαση θα επιτρέπονται συνήθως στο εταιρικό δίκτυο αλλά δεν θα πρέπει να επιτρέπονται στο δίκτυο ICS (Bailey et al., 2013).

Οι αυστηρές διαδικασίες ελέγχου αλλαγών για τον εξοπλισμό του δικτύου, τη διαμόρφωση και τις αλλαγές λογισμικού μπορεί να μην υπάρχουν στο εταιρικό δίκτυο. Εάν η κυκλοφορία δικτύου ICS μεταφέρεται στο εταιρικό δίκτυο, μπορεί να παρεμποδιστεί ή να υποβληθεί σε επιθέσεις DoS (Denial Of service) ή επιθέσεις ενδιάμεσου χρήστη (Man in the Middle). Με τη δημιουργία ξεχωριστών δικτύων, τα προβλήματα ασφάλειας και απόδοσης στο εταιρικό δίκτυο δεν θα πρέπει να επηρεάζουν το δίκτυο ICS. Οι πρακτικές εκτιμήσεις, όπως το κόστος εγκατάστασης του ICS ή η διατήρηση μιας ομοιογενούς υποδομής δικτύου, συνήθως σημαίνει ότι απαιτείται η σύνδεση μεταξύ του ICS και των εταιρικών δικτύων. Αυτή η σύνδεση αποτελεί σημαντικό κίνδυνο για την ασφάλεια ολόκληρου του δικτύου της επιχείρησης και θα πρέπει να προστατεύεται από συσκευές οι οποίες είναι ευάλωτες σε επιθέσεις (Bailey et al., 2013).

Εάν τα δίκτυα πρέπει να είναι συνδεδεμένα, συνιστάται να επιτρέπονται μόνο ελάχιστες (αν αυτό είναι εφικτό) συνδέσεις και η σύνδεση

να γίνεται μέσω ενός τείχους προστασίας (Firewall) και ενός DMZ (demilitarized zone). Ένα DMZ είναι ένα ξεχωριστό τμήμα του δικτύου που συνδέεται απευθείας με το τείχος προστασίας. Οι διακομιστές που περιέχουν τα δεδομένα από το ICS που πρέπει να έχουν πρόσβαση από το εταιρικό δίκτυο τοποθετούνται σε αυτό το τμήμα δικτύου. Μόνο αυτά τα συστήματα πρέπει να είναι προσβάσιμα από το εταιρικό δίκτυο. Με οποιεσδήποτε εξωτερικές συνδέσεις, θα πρέπει να επιτρέπεται η ελάχιστη πρόσβαση μέσω του τείχους προστασίας, συμπεριλαμβανομένου του ανοίγματος μόνο των θυρών (ports) που απαιτούνται για την συγκεκριμένη επικοινωνία (Boyer et al., 2010).

4.2. Τοποθέτηση και διαχωρισμός δικτύων

Αυτή η ενότητα πραγματεύεται την κατάτμηση του ICS σε τομείς ασφαλείας και τον διαχωρισμό του ICS από άλλα δίκτυα, όπως το εταιρικό δίκτυο, και παρουσιάζει επεξηγηματική αρχιτεκτονική ασφαλείας. Πρέπει να διεξάγεται ανάλυση επιχειρησιακού κινδύνου για τον προσδιορισμό των κρίσιμων τμημάτων κάθε δικτύου και λειτουργίας του ICS και να καθορίζεται ποια τμήματα του ICS πρέπει να κατατμηθούν. Ο κατακερματισμός του δικτύου περιλαμβάνει το διαχωρισμό του δικτύου σε μικρότερα δίκτυα (Boyer et al., 2010).

Ο κατακερματισμός και ο διαχωρισμός δικτύων είναι μια από τις πιο αποτελεσματικές αρχιτεκτονικές έννοιες που μπορεί να εφαρμόσει μία βιομηχανική επιχείρηση για την προστασία των συστημάτων του. Η τμηματοποίηση δημιουργεί τομείς ασφαλείας, οι οποίοι τυπικά ορίζονται ως διαχειριζόμενοι από την ίδια αρχή, επιβάλλοντας την ίδια πολιτική και έχοντας ένα ενιαίο επίπεδο εμπιστοσύνης. Η τμηματοποίηση μπορεί να ελαχιστοποιήσει τη μέθοδο και το επίπεδο πρόσβασης σε ευαίσθητες πληροφορίες, την επικοινωνία ICS και τη διαμόρφωση του εξοπλισμού και μπορεί να εμποδίσει ή να δυσκολέψει μια ενδεχόμενη επίθεση από κάποιο

κακόβουλο χρήστη του κυβερνοχώρου. Ο στόχος της κατάτμησης και του διαχωρισμού του δικτύου είναι η ελαχιστοποίηση της πρόσβασης σε ευαίσθητες πληροφορίες για τα μη εξουσιοδοτημένα άτομα, διασφαλίζοντας παράλληλα την ομαλή και αποτελεσματική λειτουργία της επιχείρησης. Αυτό μπορεί να επιτευχθεί με τη χρήση πολλών τεχνικών και τεχνολογιών, ανάλογα με την αρχιτεκτονική και τη διαμόρφωση του δικτύου (Boyer et al., 2010).

Ο διαχωρισμός του δικτύου συνεπάγεται στην ανάπτυξη και την επιβολή ενός συνόλου κανόνων που ελέγχει ποιες επικοινωνίες επιτρέπονται μέσω των ορίων. Οι κανόνες τυπικά βασίζονται στην ταυτότητα προέλευσης και προορισμού και στον τύπο ή το περιεχόμενο των δεδομένων που μεταφέρονται. Όταν εφαρμόζεται σωστά ο κατακερματισμός και ο διαχωρισμός του δικτύου, τότε ελαχιστοποιείται η πρόσβαση σε ευαίσθητες πληροφορίες από χρήστες που δεν πρέπει να έχουν πρόσβαση. Αυτό μπορεί να επιτευχθεί χρησιμοποιώντας μια ποικιλία τεχνολογιών και μεθόδων. Ανάλογα με την αρχιτεκτονική και τη διαμόρφωση του δικτύου της επιχείρησης, ορισμένες από τις κοινές τεχνολογίες και μέθοδοι που χρησιμοποιούνται περιλαμβάνουν (Knapp, 2011):

- Λογικό διαχωρισμό δικτύων που επιβάλλεται από κρυπτογράφηση ή διαχωρισμό που επιβάλλεται από συσκευές δικτύου.
    - Εικονικά τοπικά δίκτυα (VLANS).
    - Κρυπτογραφημένα εικονικά ιδιωτικά δίκτυα (VPN) χρησιμοποιούν κρυπτογραφικούς μηχανισμούς για να διαχωρίζουν την κυκλοφορία σε ένα δίκτυο.
    - Μονο-κατευθυντικές πύλες, οι οποίες περιορίζουν τις επικοινωνίες μεταξύ των συνδέσεων σε μία μόνο κατεύθυνση, επομένως, την κατάτμηση του δικτύου.
- Διαχωρισμός φυσικού δικτύου για την πλήρη αποτροπή οποιασδήποτε διασύνδεσης της κυκλοφορίας μεταξύ τομέων.
- Φιλτράρισμα της κίνησης των δεδομένων στο δίκτυο που μπορεί να

χρησιμοποιεί μια ποικιλία τεχνολογιών σε διάφορα επίπεδα δικτύου για την επιβολή των απαιτήσεων ασφαλείας και των τομέων.

- Φιλτράρισμα στρώματος δικτύου που περιορίζει τα συστήματα που είναι σε θέση να επικοινωνούν με άλλους στο δίκτυο βάσει πληροφοριών IP και διαδρομής.
- Φίλτρο που βασίζεται στην κατάσταση, το οποίο περιορίζει τα συστήματα που είναι σε θέση να επικοινωνούν με άλλους στο δίκτυο με βάση την προβλεπόμενη λειτουργία τους ή την τρέχουσα κατάσταση λειτουργίας τους.
- Φιλτράρισμα επιπέδου θύρας και / ή πρωτοκόλλου που περιορίζει τον αριθμό και τον τύπο των υπηρεσιών που μπορεί να χρησιμοποιεί κάθε σύστημα για να επικοινωνεί με άλλους στο δίκτυο.
- Φιλτράρισμα εφαρμογών, που συνήθως φιλτράρει το περιεχόμενο επικοινωνιών μεταξύ συστημάτων στο επίπεδο εφαρμογής. Αυτό περιλαμβάνει τα τείχη προστασίας σε επίπεδο εφαρμογής, τους διακομιστές μεσολάβησης και το φίλτρο βάσει περιεχομένου.

4.3. Firewalls επιχειρησιακής τεχνολογίας

Τα τείχη προστασίας δικτύων (firewalls) είναι συσκευές ή συστήματα που ελέγχουν τη ροή της κίνησης δικτύου μεταξύ των δικτύων που χρησιμοποιούν διαφορετικά επίπεδα ασφαλείας. Στις περισσότερες σύγχρονες εφαρμογές, τα firewalls και τα περιβάλλοντα τείχους προστασίας συζητούνται στο πλαίσιο της σύνδεσης του διαδικτύου και των πρωτοκόλλου UDP (User Datagram Protocol) και IP. Ωστόσο, τα τείχη προστασίας έχουν δυνατότητα εφαρμογής σε περιβάλλοντα δικτύου που δεν περιλαμβάνουν ούτε απαιτούν σύνδεση στο διαδίκτυο (Forrest, 2012).

Για παράδειγμα, πολλά εταιρικά δίκτυα χρησιμοποιούν τείχη προστασίας για να περιορίσουν τη συνδεσιμότητα από και πρός εσωτερικά δίκτυα που εξυπηρετούν πιο ευαίσθητες λειτουργίες, όπως τα τμήματα λογιστικών ή ανθρώπινων πόρων. Περαιτέρω περιορίζουν τις ενδοεπιχειρησιακές επικοινωνίες ICS μεταξύ λειτουργικών υπό-δικτύων και συσκευών ασφαλείας. Χρησιμοποιώντας τείχη προστασίας για τον έλεγχο της σύνδεσης με αυτές τις περιοχές, μία επιχείρηση μπορεί να αποτρέψει την μη εξουσιοδοτημένη πρόσβαση στα αντίστοιχα συστήματα και πόρους μέσα στις πιο ευαίσθητες περιοχές (Forrest, 2012).

Υπάρχουν τρεις γενικές κατηγορίες τείχους προστασίας:

1. **Firewalls φίλτρων πακεταρίσματος**. Ο πιο βασικός τύπος τείχους προστασίας ονομάζεται φίλτρο πακέτων. Τα τείχη προστασίας φίλτρων πακέτων είναι ουσιαστικά συσκευές δρομολόγησης που περιλαμβάνουν λειτουργικότητα ελέγχου πρόσβασης για διευθύνσεις συστήματος και συνεδρίες επικοινωνίας. Ο έλεγχος πρόσβασης διέπεται από ένα σύνολο οδηγιών που συλλογικά αναφέρονται ως σύνολο κανόνων. Στην πιο βασική τους μορφή, τα φίλτρα πακέτων λειτουργούν στο επίπεδο 3 (δίκτυο) του μοντέλου ανοικτού συστήματος διασύνδεσης (OSI), ISO / IEC 7498. Αυτός ο τύπος τείχους προστασίας ελέγχει βασικές πληροφορίες σε κάθε πακέτο, όπως είναι οι διευθύνσεις IP, έναντι σειράς κριτηρίων πριν από την προώθηση του πακέτου. Ανάλογα με το πακέτο και τα κριτήρια, το τείχος προστασίας μπορεί να αποβάλει το πακέτο, να το προωθήσει ή να στείλει ένα μήνυμα στον δημιουργό. Αυτός ο τύπος τείχους προστασίας μπορεί να προσφέρει υψηλό επίπεδο ασφάλειας, αλλά μπορεί να έχει ως αποτέλεσμα επιβαρύνσεις και καθυστερήσεις στην απόδοση του δικτύου.
2. **Τείχη προστασίας από επιθεωρήσεις (Statewatch firewalls).** Αυτός ο τύπος του firewall ελέγχου, περιλαμβάνει φίλτρα πακέτων

που ενσωματώνουν αυξημένη επίγνωση των δεδομένων μοντέλου OSI στο επίπεδο 4 (μεταφορά). Τα Statewatch firewalls ελέγχου, φιλτράρουν τα πακέτα στο επίπεδο δικτύου, καθορίζουν εάν τα πακέτα συνεδριών είναι νόμιμα και αξιολογούν τα περιεχόμενα των πακέτων στο επίπεδο μεταφοράς (π.χ. TCP, UDP). Ο καθολικός έλεγχος παρακολουθεί τις ενεργές περιόδους σύνδεσης και χρησιμοποιεί αυτές τις πληροφορίες για να προσδιορίσει εάν τα πακέτα πρέπει να προωθηθούν ή να αποκλειστούν. Προσφέρει υψηλό επίπεδο ασφάλειας και καλής απόδοσης, αλλά μπορεί να είναι πιο ακριβό και πολύπλοκο για τη διαχείριση.

3. **Τείχη προστασίας με ενδιάμεσο δρομολογητή (Firewalls Gateway Application-Proxy)**. Αυτή η κατηγορία τείχους προστασίας εξετάζει τα πακέτα στο επίπεδο εφαρμογής και φιλτράρει την επισκεψιμότητα με βάση συγκεκριμένους κανόνες εφαρμογής, όπως συγκεκριμένες εφαρμογές (π.χ. προγράμματα περιήγησης) ή πρωτόκολλα (π.χ. FTP). Τα τείχη προστασίας αυτού του τύπου μπορούν να είναι πολύ αποτελεσματικά στην αποτροπή επιθέσεων στις υπηρεσίες απομακρυσμένης πρόσβασης και διαμόρφωσης που παρέχονται από τα στοιχεία ICS. Προσφέρουν υψηλό επίπεδο ασφάλειας, αλλά θα μπορούσαν να έχουν επιβαρυντικές επιπτώσεις και καθυστερήσεις στην απόδοση του δικτύου, κάτι που μπορεί να είναι απαράδεκτο σε περιβάλλον ICS. Το NIST SP 800-41 Revision 1, οδηγίες για τα Τείχη προστασίας και την Πολιτική του Τείχους προστασίας παρέχει γενικές οδηγίες για την επιλογή των τείχους προστασίας και των πολιτικών τείχους προστασίας (NIST, 2011).

Σε ένα περιβάλλον ICS, τα τείχη προστασίας εντοπίζονται συχνότερα μεταξύ του δικτύου ICS και του εταιρικού δικτύου. Είναι κατάλληλα διαμορφωμένα, μπορούν να περιορίσουν σε μεγάλο βαθμό την ανεπιθύμητη πρόσβαση από και προς τους κεντρικούς υπολογιστές και τους ελεγκτές του

συστήματος ελέγχου, βελτιώνοντας έτσι την ασφάλεια. Μπορούν επίσης να βελτιώσουν την ανταπόκριση του δικτύου ελέγχου, εξαλείφοντας μη βασική κίνηση από το δίκτυο. Όταν σχεδιαστεί σωστά, διαμορφωθεί και διατηρηθεί, τα αποκλειστικά τείχη προστασίας υλικού μπορούν να συμβάλουν σημαντικά στην αύξηση της ασφάλειας των σημερινών περιβάλλοντος ICS (Forrest, 2012).

Τα τείχη προστασίας παρέχουν διάφορα εργαλεία για την επιβολή μιας πολιτικής ασφάλειας που δεν μπορεί να επιτευχθεί τοπικά με το τρέχον σύνολο συσκευών ελέγχου διαδικασιών που διατίθενται στην αγορά, συμπεριλαμβανομένης της δυνατότητας:

- Αποκλεισμός όλων των επικοινωνιών, με εξαίρεση τις ειδικές επικοινωνίες μεταξύ συσκευών στο μη προστατευμένο τοπικό δίκτυο προστατευμένα δίκτυα ICS. Ο αποκλεισμός μπορεί να βασίζεται, για παράδειγμα, σε ζεύγη διευθύνσεων IP προέλευσης και προορισμού, υπηρεσίες, θύρες, κατάσταση σύνδεσης και καθορισμένες εφαρμογές ή πρωτόκολλα που υποστηρίζονται από το τείχος προστασίας. Ο αποκλεισμός μπορεί να συμβεί και στα εισερχόμενα και εξερχόμενα πακέτα, κάτι που είναι χρήσιμο για τον περιορισμό των επικοινωνιών υψηλού κινδύνου όπως το ηλεκτρονικό ταχυδρομείο.
- Εφαρμογή ασφαλούς ελέγχου ταυτότητας όλων των χρηστών που επιθυμούν να έχουν πρόσβαση στο δίκτυο ICS. Υπάρχει ευελιξία να χρησιμοποιούνται ποικίλα επίπεδα προστασίας των μεθόδων ελέγχου ταυτότητας, όπως απλοί κωδικοί πρόσβασης, σύνθετοι κωδικοί πρόσβασης, τεχνολογίες επαλήθευσης πολλαπλών παραγόντων, μάρκες, βιομετρικά στοιχεία και έξυπνες κάρτες.
- Εφαρμογή εξουσιοδότησης προορισμού: Οι χρήστες μπορούν να περιοριστούν και να επιτραπεί η πρόσβαση μόνο στους κόμβους του δικτύου ελέγχου που είναι απαραίτητοι για τη δουλειά τους. Αυτό μειώνει το δυναμικό των χρηστών να έχουν πρόσβαση σκόπιμα ή

τυχαία και να ελέγχουν τις συσκευές για τις οποίες δεν είναι εξουσιοδοτημένες, αλλά αυξάνει την πολυπλοκότητα των εργαζομένων κατά τη διάρκεια της εκπαίδευσης ή της ενδοεπιχειρησιακής κατάρτισης.

- Καταγραφή ροής πληροφοριών για παρακολούθηση κυκλοφορίας, ανάλυση και ανίχνευση εισβολής.
- Εφαρμογή επιχειρησιακών πολιτικών, κατάλληλων για το ICS, (ίσως να μην είναι κατάλληλες σε ένα δίκτυο πληροφορικής), όπως η απαγόρευση λιγότερο ασφαλών επικοινωνιών όπως το ηλεκτρονικό ταχυδρομείο και η επιτρεπόμενη χρήση εύχρηστων ονομάτων χρηστών και ομάδων κωδικών πρόσβασης.
- Σχεδιασμός τεκμηριωμένων ελάχιστων (ενιαίων, αν είναι δυνατόν) συνδέσεων που επιτρέπουν την αποκοπή του δικτύου ICS από το εταιρικό δίκτυο σε περίπτωση σοβαρών περιστατικών στον κυβερνοχώρο. Άλλες πιθανές αναπτύξεις περιλαμβάνουν τη χρήση είτε τείχους προστασίας που βασίζονται σε κεντρικούς υπολογιστές είτε μικρά αυτόνομα τείχη προστασίας υλικού μπροστά ή μεμονωμένες συσκευές ελέγχου. Η χρήση τείχους προστασίας σε μεμονωμένες συσκευές μπορεί να δημιουργήσει σημαντικά έξοδα διαχείρισης, ειδικά στη διαχείριση αλλαγών των διαμορφώσεων του τείχους προστασίας, ωστόσο αυτή η πρακτική θα απλοποιήσει επίσης τα ατομικά σύνολα κανόνων. Υπάρχουν αρκετά ζητήματα που πρέπει να αντιμετωπιστούν κατά την ανάπτυξη τείχους προστασίας σε περιβάλλοντα ICS, ιδιαίτερα τα εξής (BCIT, 2015):

  Προσθήκη καθυστέρησης για τον έλεγχο των επικοινωνιών του συστήματος.Τα τείχη προστασίας απαιτούν συνεχή υποστήριξη, συντήρηση και δημιουργία αντιγράφων ασφαλείας. Τα σύνολα κανόνων πρέπει να επανεξεταστούν για να διασφαλιστεί ότι παρέχουν επαρκή προστασία υπό το πρίσμα των συνεχώς μεταβαλλόμενων απειλών κατά της ασφάλειας. Οι δυνατότητες του συστήματος (π.χ.

χώρος αποθήκευσης για τα αρχεία καταγραφής τείχους προστασίας) θα πρέπει να παρακολουθούνται ώστε να διασφαλίζεται ότι το τείχος προστασίας εκτελεί τις εργασίες συλλογής δεδομένων και μπορεί να εξαρτάται από την περίπτωση παραβίασης της ασφάλειας. Η παρακολούθηση σε πραγματικό χρόνο των firewall και άλλων αισθητήρων ασφαλείας απαιτείται για την ταχεία ανίχνευση και εκκίνηση της αντίδρασης (BCIT, 2015).

4.4. Πρακτικές ασφάλειας με χρήση Firewall

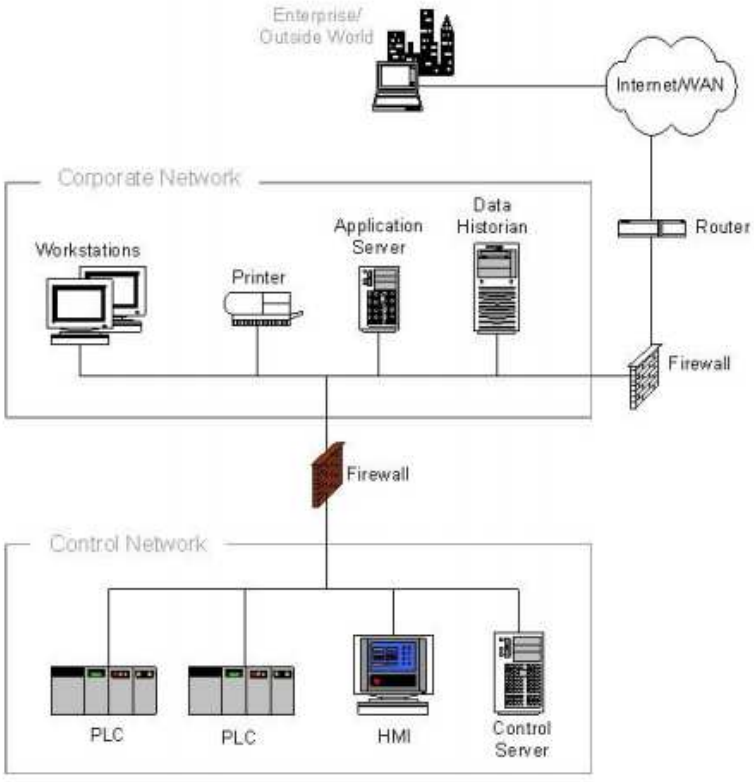
Οι αποτελεσματικές πρακτικές της εφαρμογής των συστημάτων firewall, συνήθως διαχωρίζουν τα δίκτυα των επιχειρήσεων με τέτοιο τρόπο ώστε να μειώνονται στο ελάχιστο οι κίνδυνοι και οι απειλές που δέχονται τα υπολογιστικά συστήματα.

Τα δίκτυα ICS και τα εταιρικά δίκτυα μπορούν να διαχωριστούν για να ενισχύσουν την ασφάλεια στον κυβερνοχώρο χρησιμοποιώντας διαφορετικές αρχιτεκτονικές. Αυτή η ενότητα περιγράφει διάφορες πιθανές αρχιτεκτονικές και εξηγήσει τα πλεονεκτήματα και τα μειονεκτήματα του καθενός.

4.4.1. Τείχος προστασίας μεταξύ δικτύου εταιρικού δικτύου και ελέγχου

Με την εισαγωγή ενός απλού τείχους προστασίας δύο θυρών μεταξύ των εταιρικών δικτύων και των δικτύων ελέγχου, όπως φαίνεται στην εικόνα 4.1., μπορεί να επιτευχθεί σημαντική βελτίωση της ασφάλειας. Η σωστή

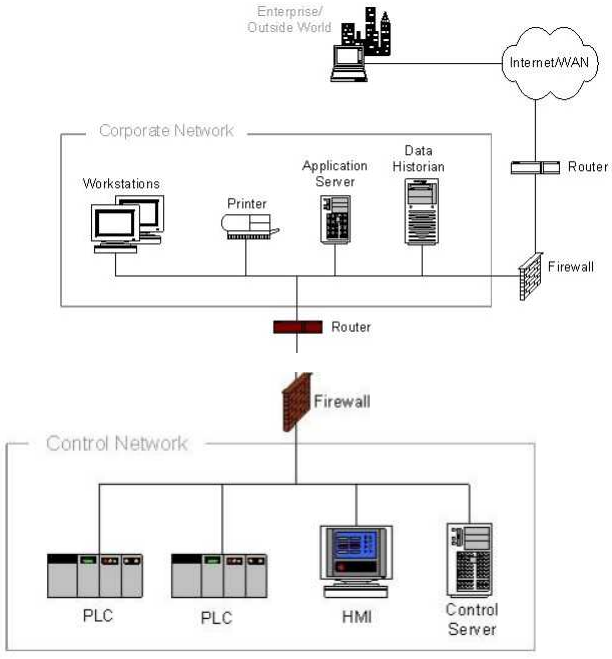
διαμόρφωση του τείχους προστασίας μειώνει σημαντικά την πιθανότητα μιας επιτυχημένης εξωτερικής επίθεσης στο δίκτυο ελέγχου. Δυστυχώς, εξακολουθούν να υπάρχουν δύο θέματα με αυτό το σχέδιο. Πρώτον, εάν ο ιστορικός δεδομένων βρίσκεται στο εταιρικό δίκτυο, το τείχος προστασίας πρέπει να επιτρέπει στον ιστορικό δεδομένων να επικοινωνεί με τις συσκευές ελέγχου στο δίκτυο ελέγχου. Ένα πακέτο που προέρχεται από κακόβουλο ή εσφαλμένα διαμορφωμένο κεντρικό υπολογιστή στο εταιρικό δίκτυο (που φαίνεται να είναι ο ιστορικός δεδομένων) θα διαβιβάζεται σε μεμονωμένα PLC / DCS.



Εικόνα 4.1- Τείχος προστασίας μεταξύ εταιρικού δικτύου και δικτύου ελέγχου

4.4.2. Τείχος προστασίας και δρομολογητή μεταξύ εταιρικού δικτύου και δικτύου ελέγχου

Ένας λίγο πιο εξελιγμένος σχεδιασμός, όπως φαίνεται στην εικόνα 4.2, είναι η χρήση ενός συνδυασμού δρομολογητή / τείχους προστασίας. Ο δρομολογητής κάθεται μπροστά από το τείχος προστασίας και προσφέρει βασικές υπηρεσίες φιλτραρίσματος πακέτων, ενώ το τείχος προστασίας χειρίζεται τα πιο περίπλοκα ζητήματα χρησιμοποιώντας είτε κρατικές επιθεωρήσεις είτε τεχνικές πληρεξούσιου. Αυτός ο τύπος σχεδίασης είναι πολύ δημοφιλής στα τείχη προστασίας που απευθύνονται στο Internet, επειδή επιτρέπει στον ταχύτερο δρομολογητή να χειρίζεται το μεγαλύτερο μέρος των εισερχόμενων πακέτων, ειδικά στην περίπτωση των επιθέσεων άρνησης υπηρεσίας και μειώνει το φορτίο στο τείχος προστασίας. Προσφέρει επίσης βελτιωμένη άμυνα σε βάθος επειδή υπάρχουν δύο διαφορετικές συσκευές που ένας αντίπαλος πρέπει να παρακάμψει (Thurman, 2011).

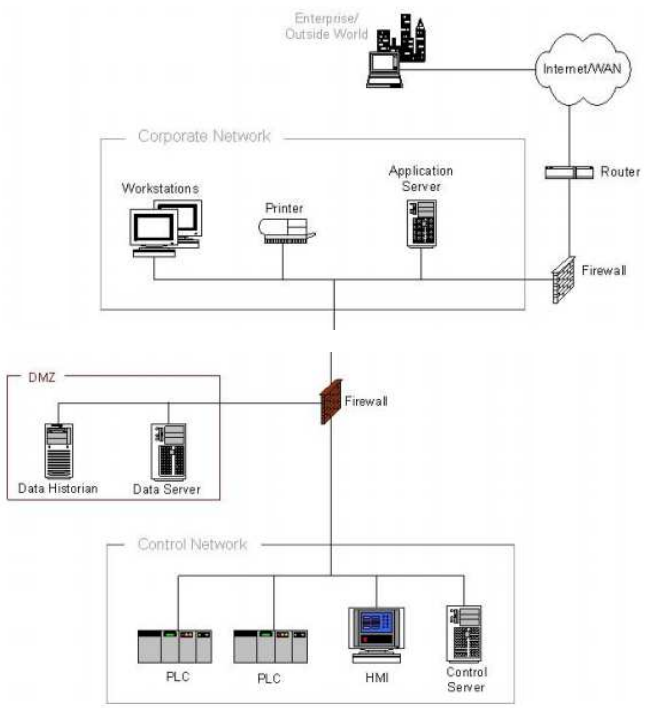


Εικόνα 4.2- Τείχος προστασίας και δρομολογητή μεταξύ εταιρικού δικτύου και δικτύου ελέγχου

4.4.3 Firewall με DMZ(demilitarized zone) μεταξύ εταιρικού δικτύου και δικτύου ελέγχου

Σημαντική βελτίωση στην ασφάλεια, αποτελεί η χρήση τείχους προστασίας με τη δυνατότητα δημιουργίας DMZ μεταξύ εταιρικών δικτύων και δικτύων ελέγχου. Κάθε DMZ περιέχει ένα ή περισσότερα κρίσιμα στοιχεία, όπως το ιστορικό δεδομένων, το σημείο ασύρματης πρόσβασης ή τα συστήματα πρόσβασης τρίτων μερών. Στην πραγματικότητα, η χρήση ενός τείχους προστασίας επιτρέπει τη δημιουργία ενός ενδιάμεσου δικτύου. Η δημιουργία ενός DMZ απαιτεί ότι το τείχος προστασίας προσφέρει τρεις ή περισσότερες διεπαφές, αντί για τις τυπικές δημόσιες και ιδιωτικές διεπαφές (Chapple, 2014).

Μία από τις διεπαφές συνδέεται με το εταιρικό δίκτυο, το δεύτερο με το δίκτυο ελέγχου και τις υπόλοιπες διεπαφές με τις κοινές ή ανασφαλείς συσκευές, όπως ο ιστορικός διακομιστής δεδομένων ή τα σημεία ασύρματης πρόσβασης στο δίκτυο DMZ. Η εφαρμογή συνεχούς παρακολούθησης της κυκλοφορίας εισόδου και εξόδου στο DMZ συνιστάται. Επιπλέον, συνιστώνται κανόνες κανόνων τείχους προστασίας που επιτρέπουν μόνο συνδέσεις μεταξύ του δικτύου ελέγχου και του DMZ που εκκινούν από συσκευές δικτύου ελέγχου. Στην εικόνα 4.3 παρέχει ένα παράδειγμα αυτής της αρχιτεκτονικής (Chapple, 2014).



Εικόνα 4.3- Firewall με DMZ(demilitarized zone) μεταξύ εταιρικού δικτύου και δικτύου ελέγχου

Με την τοποθέτηση εταιρικών προσπελάσιμων στοιχείων στο DMZ, δεν απαιτούνται άμεσες διαδρομές επικοινωνίας από το εταιρικό δίκτυο στο δίκτυο ελέγχου. κάθε πορεία τελικά τελειώνει στο DMZ. Τα περισσότερα τείχη προστασίας μπορούν να επιτρέψουν πολλαπλά DMZ και μπορούν να καθορίσουν ποιος τύπος κίνησης μπορεί να προωθηθεί μεταξύ των ζωνών. Όπως δείχνει η εικόνα 4.3., το τείχος προστασίας μπορεί να εμποδίσει την είσοδο αυθαίρετων πακέτων από το εταιρικό δίκτυο στο δίκτυο ελέγχου και μπορεί επίσης να ρυθμίσει την κυκλοφορία από τις άλλες ζώνες δικτύου συμπεριλαμβανομένου του δικτύου ελέγχου. Με καλά σχεδιασμένα σύνολα κανόνων, μπορεί να διατηρηθεί ένας σαφής διαχωρισμός μεταξύ του δικτύου ελέγχου και άλλων δικτύων, με ελάχιστη ή καθόλου κίνηση που μεταδίδεται

απευθείας μεταξύ των εταιρικών δικτύων και των δικτύων ελέγχου. Εάν πρόκειται να χρησιμοποιηθεί διακομιστής διαχείρισης ενημερώσεων κώδικα, διακομιστής προστασίας από ιούς ή άλλος διακομιστής ασφαλείας για το δίκτυο ελέγχου, θα πρέπει να βρίσκεται απευθείας στο DMZ (Thurman, 2011).

Και οι δύο λειτουργίες θα μπορούσαν να βρίσκονται σε ένα μόνο διακομιστή. Η κατοχή της διαχείρισης των ενημερώσεων κώδικα και της διαχείρισης ιών που είναι αφιερωμένη στο δίκτυο ελέγχου επιτρέπει ελεγχόμενες και ασφαλείς ενημερώσεις που μπορούν να προσαρμοστούν στις μοναδικές ανάγκες του περιβάλλοντος ICS. Μπορεί επίσης να είναι χρήσιμο εάν το προϊόν προστασίας από ιούς που επιλέγεται για προστασία ICS δεν είναι το ίδιο με το προϊόν προστασίας από ιούς που χρησιμοποιείται για το εταιρικό δίκτυο. Για παράδειγμα, αν εγκατασταθεί κακόβουλο λογισμικό και ένα προϊόν εντοπισμού ιών δεν μπορεί να το ανιχνεύσει ή να το σταματήσει, είναι κάπως πιθανό ότι ένα άλλο προϊόν μπορεί να έχει αυτή τη δυνατότητα.

ΚΕΦΑΛΑΙΟ 5 - ΑΣΦΑΛΕΙΑ ΜΕ ΤΗΝ ΧΡΗΣΗ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΒΙΟΜΗΧΑΝΙΚΟΥ ΑΥΤΟΜΑΤΟΥΕΛΕΓΧΟΥ ΚΑΙ ΤΗΛΕΜΕΤΡΙΑΣ (SCADA)

5.1. Εισαγωγή

Τα τελευταία χρόνια, με τους ιούς (viruses), τα σκουλήκια (worms), τους δούρειους ίππους (Trojan Horses) και τα αυξημένα επίπεδα δραστηριότητας των κακόβολων λογισμικών όπως το Blaster (γνωστό και ως MSBlast), αναγνωρίζεται ότι αυτά τα συστήματα που ήταν παλαιότερα ιδιόκτητα και απομονωμένα, σήμερα συνδέονται με εταιρικά δίκτυα και πολλά από αυτά περιέχουν σημεία σύνδεσης από το διαδίκτυο.

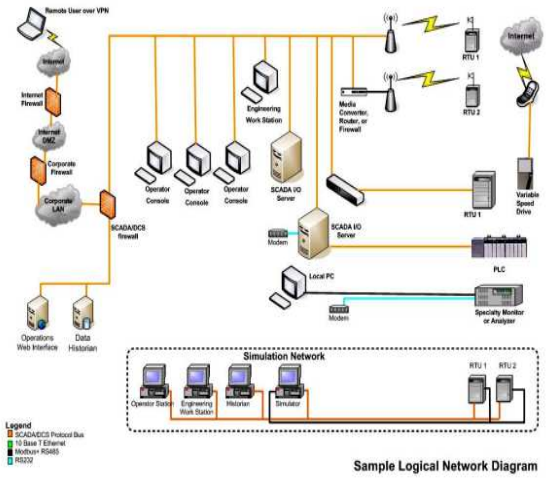
Επίσης, είναι γνωστό ότι ο ηλεκτρονικός εξοπλισμός που ελέγχει την κρίσιμη υποδομή είναι επιρρεπής σε αποτυχία μέσω της υπηρεσίας DoS (Denial of Service), των παραμορφωμένων πακέτων και του κακόβουλου κώδικα που προκαλείται από ιούς, δούρειους ίππους και σκουλήκια. Οι αξιολογήσεις ευπάθειας της ασφάλειας των δικτύων που εκτελούνται σε σύστημα βιομηχανικού αυτομάτου ελέγχου και τηλεμετρίας (Supervisory Control and Data Acquisition, SCADA) και έχουν δημιουργήσει ένα πρότυπο στην προσέγγιση που πολλές εταιρίες υιοθετούν για να εξασφαλίσουν τα κρίσιμα στοιχεία ενεργητικού τους. Πάνω από το 80% αυτών των επιχειρήσεων ηλεκτρικής ενέργειας, φυσικού αερίου και νερού ανέφεραν ότι ένα τείχος προστασίας (firewall) ή ισοδύναμη λύση στον κυβερνοχώρο μεταξύ του δικτύου εταιρικών δικτύων πληροφορικής και ελέγχου διαδικασιών ήταν επαρκής για τη διατήρηση της ασφάλειας των κρίσιμων στοιχείων του ενεργητικού τους υπό τον έλεγχο των SCADA και των συστημάτων ελέγχου διαδικασιών.

Αυτές οι εταιρίες θεωρούσαν συνήθως το δίκτυο ελέγχου διαδικασιών ως ένα μεγάλο μαύρο κουτί και τείνουν να προσεγγίζουν τη διασφάλιση αυτών

των περιβαλλόντων προσπαθώντας να απομονώσουν το περιβάλλον όσο το δυνατόν περισσότερο από οποιοδήποτε άλλο δίκτυο. Παρόλο που πρόκειται για μια καλή πρώτη προσπάθεια και μια κίνηση προς τη σωστή κατεύθυνση, υπάρχουν πρόσθετες λύσεις για την ασφάλεια στον κυβερνοχώρο, οι οποίες θα πρέπει να ληφθούν υπόψη λαμβάνοντας υπόψη τις σύγχρονες εξωτερικές και εσωτερικές απειλές που αντιμετωπίζουν αυτά τα συστήματα που συνδέονται μέσω πρωτοκόλλων Ethernet και Internet-routable. Στην συνέχεια, εμφανίζονται δύο διαγράμματα.

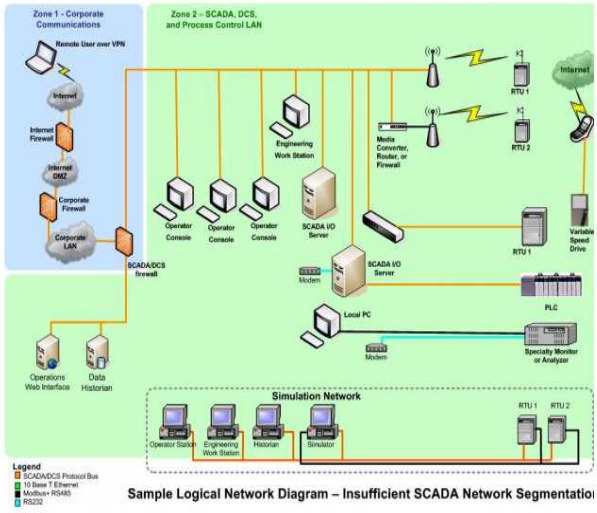
5.2. Αρχιτεκτονική συστημάτων SCADA

Η εικόνα 5.1 δείχνει το διάγραμμα λογικής δικτύου για το πώς ένα τυπικό σύστημα SCADA ή DCS είναι συνδεδεμένο στο δίκτυο προς το εταιρικό δίκτυο.



Εικόνα 5.1- Τυπική δομή ενός δικτύου που βασίζεται στο πρότυπο SCADA

Η εικόνα 5.2 δείχνει πώς οι περισσότερες εταιρίες βλέπουν την ασφάλεια των περιβαλλόντων ελέγχου σε πραγματικό χρόνο, συστηματα SCADA και διαδικασίες ελέγχου. Κατά κανόνα, τμηματοποιούν το δίκτυό τους σε δύο περιβάλλοντα, το ένα για την εταιρική / πληροφορική και το άλλο για τα συστήματα ελέγχου SCADA και διαδικασιών (Johnson, 2011).



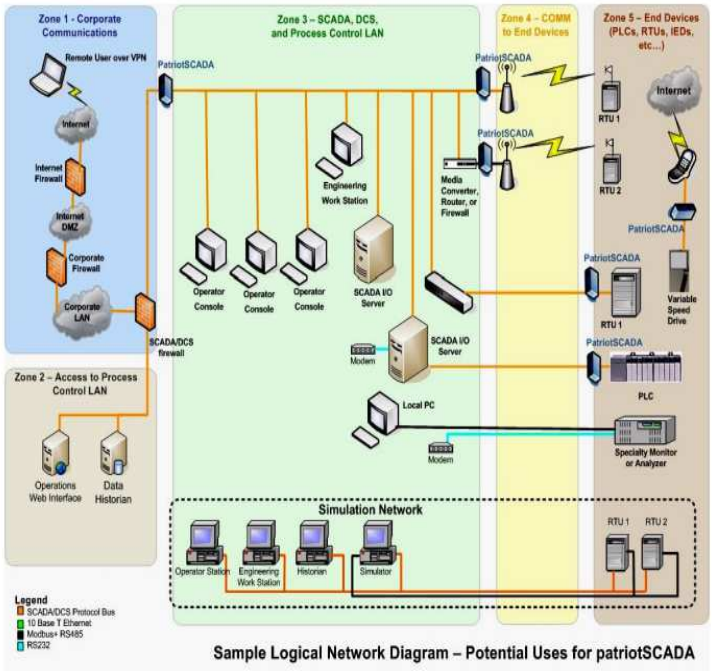
Εικόνα 5.2- Τμηματοποίηση σε 2 ζώνες

5.3. Προσαρμοσμένη προσέγγιση τείχους προστασίας

Η διατήρηση του περιβάλλοντος SCADA / DCS ξεχωριστά από το περιβάλλον εταιρικής πληροφορικής συνίσταται και για συσκευές όπως οι ευφυείς ηλεκτρονικές συσκευές (Intelligent Electronic Devices, IED) και οι προγραμματιζόμενοι λογικοί ελεγκτές (Programmable Logic Controller, PLCs), που ελέγχουν τον φυσικό εξοπλισμό και θα πρέπει να βρίσκονται σε διαφορετική ζώνη ασφαλείας με πρόσθετους ελέγχους πρόσβασης για περιορισμό της πρόσβασης σε αυτούς. Οι διακομιστές SCADA και οι

κονσόλες χειριστών πρέπει να βρίσκονται σε άλλη ζώνη ασφαλείας (Johnson, 2011).

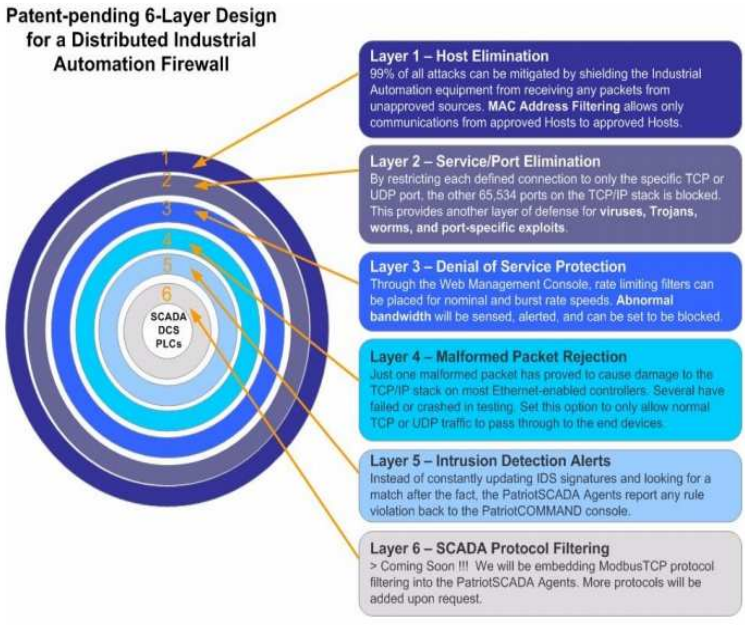
Έχει αποδειχθεί σε ερευνητικές μελέτες και στις δοκιμές διαχείρισης κρίσεων του κυβερνοχώρου που πραγματοποίησε η εταιρία PlantData στον εξοπλισμό SCADA ότι αυτοί οι ελεγκτές είναι επιρρεπείς σε συντριβή όταν το δίκτυο βρίσκεται σε υψηλό επίπεδο εύρους ζώνης ή εάν έχουν αποσταλεί πακέτα δικτύου με ακατάλληλη μορφή στο λογισμικό SCADA ή τον εξοπλισμό. Η εικόνα 5.3 δείχνει μια καλύτερη προσέγγιση για την κατάτμηση του περιβάλλοντος SCADA σε ζώνες ασφαλείας. Οι μικροί πράκτορες PatriotSCADA μπορούν να εγκατασταθούν σε όλο το περιβάλλον SCADA για να λειτουργήσουν ως κατανεμημένο τείχος προστασίας (McCallister, 2010).



Εικόνα 5.3- Τμηματοποίηση δικτύου SCADA σε ζώνες ασφαλείας (βελτιωμένη προσέγγιση)

5.4. Επίπεδα Ασφαλείας για την προστασία

Η εταιρία PlantData ανέπτυξε μια προσέγγιση πολλαπλών στρωμάτων για την εξασφάλιση συστημάτων ελέγχου σε πραγματικό χρόνο, λογισμικό, υλικό και εξοπλισμό εγκατάστασης με δυνατότητα Ethernet χωρίς να επηρεάζεται η ταχύτητα ή η απόδοση του δικτύου. Η εικόνα 5.4. περιγράφει κάθε αμυντικό στρώμα στο εσωτερικό του firmware που εκτελείται στους πράκτορες PatriotSCADA. Μεμονωμένα, αυτά τα αμυντικά στρώματα μπορεί να υπάρχουν σε μία ή περισσότερες τρέχουσες λύσεις ασφάλειας. Ωστόσο, το PatriotSCADA κατανεμημένο τείχος προστασίας είναι το πρώτο προϊόν στην αγορά που απευθύνεται ειδικά σε όλες αυτές τις εκτιμήσεις σε μια μικρή ενσωματωμένη μονάδα χωρίς κινητά εξαρτήματα (McCallister, 2010).



Εικόνα 5.4- Τα 6 επίπεδα ασφαλείας για τους κατανεμημένους πράκτορες firewall

ΚΕΦΑΛΑΙΟ 6 –ΑΣΦΑΛΕΙΑ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ ΣΤΙΣ ΕΠΙΧΕΙΡΗΣΕΙΣ ΚΑΙ ΣΤΙΣ ΒΙΟΜΗΧΑΝΙΕΣ

Η τεχνολογία ασύρματου LAN υπήρξε ένα ισχυρό κίνητρο για την πρόοδο της ασφάλειας του δικτύου. Με μεγαλύτερη ευκολία πρόσβασης μέσω ασύρματων συσκευών έρχεται μια μεγαλύτερη ανάγκη για ολοκληρωμένες λύσεις ασύρματης ασφάλειας.

Επίσης, η έλευση της τηλεφωνίας μέσω διαδικτύου (Voice over IP, VoIP) και όλες οι συνοδευτικές συσκευές και τεχνολογίες (IP τηλεφωνία), έχουν κάνει αρκετά βήματα προόδου στον τομέα της ασφάλειας. Ποιος θα ήθελε η τηλεφωνική κλήση τους να υποκλαπεί από κακόβουλους χρήστες; Αξίζει η περιγραφή των προγραμμάτων οδήγησης για εφαρμογές VoIP, τα στοιχεία που απαιτούνται σε δίκτυα VoIP, καθώς και θέματα υπηρεσιών VoIP. Η φυσική εξέλιξη είναι η διερεύνηση των επιπτώσεων της εφαρμογής των μέτρων ασφαλείας σε δίκτυα IP που μεταφέρουν φωνή.

Τα δίκτυα αποθήκευσης δεδομένων (Storage Area Networks, SANs) προσφέρουν μια λύση για την μείωση του κόστους του δικτύου και τη λύση των προβλημάτων στους δρομολογητές. Δεδομένου ότι ο σκοπός της ασφάλειας του δικτύου είναι η διασφάλιση των δεδομένων (συμπεριλαμβανομένης της φωνής και βίντεο), καθώς και το γεγονός ότι τα δεδομένα τώρα βρίσκονται συνήθως σ' ένα SAN, είναι σημαντικό το SAN να ασφαλιστεί.

Τα σύγχρονα δίκτυα επιχειρήσεων απασχολούν συνήθως ασύρματους ελεγκτές, σημεία πρόσβασης, καθώς και ένα ασύρματο σύστημα διαχείρισης για να προσφέρουν ολοκληρωμένη προστασία ενάντια στις ασύρματες επιθέσεις. Το ασύρματο περιβάλλον εξασφαλίζεται με ολοκληρωμένη Integrated Infrastructure προστασία από απειλές δηλαδή μια έγκυρη διαμόρφωση που συνδυάζει τους φυσικούς υπολογιστές, τους πόρους δικτύωσης και τους αποθηκευτικούς πόρους για να σχηματίσουν μια ενιαία λύση,

, προηγμένη ορατότητα στο περιβάλλον RF και ενσύρματη συνεργασία της ασφάλειας του δικτύου (Hong Liu & Mouchtaris,2010).

Μια integrated infrastructure προσέγγιση για την ολοκληρωμένη ασφάλεια ασύρματου δικτύου μειώνει το κόστος, ενώ εξορθολογίζει τις λειτουργίες ασφαλείας. Μια τέτοια λύση έχει μια σειρά από πλεονεκτήματα (Hong Liu & Mouchtaris, 2010):

1. Οι δυνατότητες ανίχνευσης εισβολής και προληπτικής απειλής ανιχνεύουν ασύρματες επιθέσεις και τις αποτρέπουν.
2. Η ολοκληρωμένη προστασία προστατεύει εμπιστευτικά δεδομένα και επικοινωνίες.
3. Μια ενιαία ταυτότητα του χρήστη και πολιτική απλοποιεί τη διαχείριση των χρηστών και προστατεύει από μη εξουσιοδοτημένη πρόσβαση.
4. Η συνεργασία με ενσύρματα συστήματα ασφαλείας ενεργοποιεί ένα υπερσύνολο των ασύρματων λειτουργιών ασφάλειας και προστασίας.

6.1. IP τηλεφωνία

Τα IP τηλέφωνα, IP Private Branch Exchanges (PBXs), φωνητικές πύλες, τα συστήματα φωνητικού ταχυδρομείου, καθώς και τα απαιτούμενα πρωτόκολλα είναι επίσης κοινά σε ένα εταιρικό δίκτυο. Αυτές οι τεχνολογίες και τα πρωτόκολλα ενισχύουν την παραγωγικότητα και τελικά σώζουν τον οργανισμό σχετικά με το κόστος τηλεφωνίας. Με τη χρήση ενός IP PBX, οι οργανισμοί μπορούν να εξαλείψουν την legacy PBX και να απολαύσουν τα οφέλη της IP τηλεφωνίας σ' ένα μόνο δίκτυο. Ένα IP PBX παρέχει λειτουργικότητα ελέγχου κλήσεων και, όταν χρησιμοποιείται σε συνδυασμό με τα IP σύνολα τηλέφωνο ή μια εφαρμογή του τηλεφώνου, μπορεί να παρέχει

λειτουργικότητα PBX σ' ένα κατανεμημένο και επεκτάσιμο τρόπο διαμόρφωσης (Udani, 2011).

Τα Cisco IP μοντέλα ανάπτυξης λύσεων τηλεφωνίας εμπίπτουν σε μία από αυτές τις κατηγορίες:

* Single-site deployment

* Centralized call processing with remote branches

* Distributed call processing deployment

* Clustering over the IP WAN

Η επιλογή του μοντέλου ανάπτυξης εξαρτάται από τις απαιτήσεις του οργανισμού, όπως το μέγεθος του δικτύου, τα χαρακτηριστικά και τη διαθεσιμότητα του WAN εύρους ζώνης.

Τα επιχειρησιακά δίκτυα χρησιμοποιούν επίσης τη δικτύωση αποθηκευτικού χώρου. Η δικτύωση αποθηκευτικού χώρου είναι κεντρικής σημασίας για τη σύγχρονη αρχιτεκτονική κέντρου δεδομένων, παρέχοντας μια πλατφόρμα δικτύωσης που βοηθά τα IT τμήματα να επιτύχουν χαμηλότερο συνολικό κόστος ιδιοκτησίας, αυξημένη ανθεκτικότητα και μεγαλύτερη ευελιξία. Οι δικτυακές λύσεις αποθήκευσης παρέχουν:

1. Ενσωματωμένη προστασία - Η πρώτη, δεύτερη, και τρίτη γενιά μπορούν να συνυπάρχουν σε ήδη υπάρχοντα σκελετό του πελάτη .
2. Εικονικότητα (Virtualization)- Οι διαχειριστές της τεχνολογίας των πληροφοριών μπορούν να παρέχουν τις υποδομές αποθήκευσής τους.
3. Ασφάλεια - Τα δεδομένα προστατεύονται όταν βρίσκονται σε κατάσταση ηρεμίας και ενώ μεταφέρονται και αναπαράγονται.

4. Ενοποίηση - Οι επαγγελματίες αποθήκευσης μπορούν να ενοποιήσουν τους πόρους επωφελούμενοι από τις εξαιρετικά επεκτάσιμες, έξυπνες πλατφόρμες SAN.
5. Διαθεσιμότητα - Η στιγμιαία πρόσβαση στα δεδομένα είναι διαθέσιμη από πολλαπλά επίπεδα για την αποκατάσταση των καταστροφών.

Τα ασύρματα τοπικά δίκτυα βασίζονται στην τεχνολογία ραδιοσυχνοτήτων (RF). Η RF τεχνολογία υπάρχει από τα τέλη του δέκατου ένατου αιώνα. Η τεχνολογία VoIP έγινε εμπορικά διαθέσιμη στη δεκαετία του 1990. Η τεχνολογία SAN δεν μπήκε επίσημα στην αγορά μέχρι τις αρχές της δεκαετίας του 2000. Η προσέγγιση ακολουθεί εδώ την ιστορική σειρά (Udani, 2011).

Τα πρώτα ασύρματα τοπικά δίκτυα (WLANs) εμφανίστηκαν το 1990. Αυτά τα WLANs ήταν εντελώς ανοικτά, χωρίς να απαιτείται έλεγχος ταυτότητας ή κρυπτογράφησης. Η πρώτη επιλογή ασφαλείας για WLANs ήταν ένα service set identifier (SSID). Οι επόμενες εφαρμογές επέτρεψαν τη χρήση των SSIDs χωρίς τα APs που εκπέμπουν τα SSIDs.

Το IEEE 802.11b πρότυπο προσδιόρισε το Wired Equivalent Privacy (WEP) πρωτόκολλο ασφαλείας για την κρυπτογράφηση δεδομένων μεταξύ των radio τερματικών σημείων. Για αρκετά χρόνια, οι εφαρμογές WEP ήταν το μόνο μέσο για την εξασφάλιση των WLANs. Οι αδυναμίες στο WEP οδήγησε στην ανάπτυξη νεότερων τεχνολογιών, με βάση πρωτόκολλα όπως το Temporal Key Integrity Protocol (TKIP) και αλγόριθμους κρυπτογράφησης, όπως το Advanced Encryption Standard (AES). Το Wi-Fi Protected Access (WPA) υλοποιεί το TKIP και είναι πιο ασφαλές από το WEP. Το WPA2 υλοποιεί το AES και είναι πιο ασφαλές από το WPA. Το WPA2, μια διαλειτουργική εφαρμογή του 802.11i, είναι σήμερα το state of the art στην ασύρματη ασφάλεια (Udani, 2011).

Στη πορεία, η πιστοποίηση προστέθηκε ως επιλογή για την ασφάλιση των WLANs και τώρα είναι ένα θεμελιώδες συστατικό της ασύρματης πολιτικής επιχειρήσεων. Η 802.11i αρχιτεκτονική καθορίζει το 802.1X για έλεγχο ταυτότητας, που συνεπάγεται με τη χρήση του EAP και ενός διακομιστή ελέγχου ταυτότητας.

Κατά το σχεδιασμό και τη χρήση ασύρματων δικτύων, οι ειδικοί της ασφάλειας του δικτύου των επιχειρήσεων θα πρέπει να διατηρούν το κατάλληλο επίπεδο της προστασίας. Τα ασύρματα δίκτυα είναι εξαιρετικά φιλόξενα για τους χάκερ.

Ευτυχώς, εάν ληφθούν μερικές προφυλάξεις, οι διαχειριστές του δικτύου μπορούν να μειώσουν τον κίνδυνο για τους ασύρματους χρήστες. Ο διαχειριστής του δικτύου πρέπει να κρατήσει πολλά ζητήματα κατά νου:

1. Τα ασύρματα δίκτυα που χρησιμοποιούν κρυπτογράφηση με αλγόριθμο Wired Equivalent Privacy (WEP) ή Temporal Key Integrity Protocol (TKIP) δεν είναι πολύ ασφαλής και είναι ευάλωτα σε επιθέσεις.
2. Τα ασύρματα δίκτυα που χρησιμοποιούν WPA2/AES θα πρέπει να έχουν μία φράση (κωδικό) τουλάχιστον 21 χαρακτήρων.
3. Εάν ένα εικονικό ιδιωτικό δίκτυο VPN (Virtual Private Network) είναι διαθέσιμο, καλό είναι να χρησιμοποιηθεί σε οποιοδήποτε δημόσιο ασύρματο LAN.
4. Εάν η ασύρματη πρόσβαση δεν χρειάζεται, απενεργοποιείται η ασύρματη επικοινωνία ή ο ασύρματος ελεγκτής διασύνδεσης δικτύου NIC (Network Interface Controller).

Ως επαγγελματίας της ασφάλειας του δικτύου, η ανάπτυξη μιας ασύρματης λύσης θα πρέπει απολύτως να απαιτεί τα WPA2/AES μαζί με έλεγχο ταυτότητας. Ο έλεγχος ταυτότητας θα πρέπει να γίνεται από έναν κεντρικό διακομιστή ελέγχου ταυτότητας.

6.2. Ασφάλεια VoIP Security

Το VoIP είναι η μετάδοση της κίνησης φωνής πάνω από IP-based δίκτυα. Το IP είχε αρχικά σχεδιαστεί για τη δικτύωση δεδομένων, αλλά η επιτυχία του στη δικτύωση των δεδομένων έχει οδηγήσει σε προσαρμογή του στην κίνηση φωνής

Το VoIP έχει γίνει δημοφιλές σε μεγάλο βαθμό λόγω της εξοικονόμησης κόστους σε σχέση με τα παραδοσιακά τηλεφωνικά δίκτυα. Στα παραδοσιακά τηλεφωνικά δίκτυα, οι περισσότεροι άνθρωποι πληρώνουν ένα σταθερό μηνιαίο τέλος για τις τοπικές τηλεφωνικές κλήσεις και χρέωση ανά λεπτό για τις υπεραστικές κλήσεις. Οι κλήσεις VoIP διατίθενται μέσω του Διαδικτύου, με τις περισσότερες συνδέσεις στο Διαδίκτυο να χρεώνονται ένα σταθερό μηνιαίο τέλος. Χρησιμοποιώντας τη σύνδεση στο Internet για κλήσεις τόσο της κυκλοφορίας δεδομένων, όσο και της φωνής επιτρέπει στους καταναλωτές να μειώσουν το μηνιαίο λογαριασμό του τηλεφώνου τους. Για διεθνείς κλήσεις, η χρηματική εξοικονόμηση μπορεί να είναι τεράστια (Rosenberg & Schulzrinne, 2013).

Το VoIP έχει μια σειρά από επιχειρηματικά πλεονεκτήματα:

1. Το χαμηλότερο κόστος κλήσεων είναι σημαντικό. Οι πάροχοι υπηρεσιών VoIP χρεώνουν έως και 50 τοις εκατό λιγότερο για την υπηρεσία σύνδεσης του τηλεφώνου από τις παραδοσιακές τηλεφωνικές εταιρίες.
2. Οι αυξήσεις της παραγωγικότητας με τη VoIP τηλεφωνική υπηρεσία μπορεί να είναι σημαντικές. Ορισμένες επιχειρήσεις

έχουν αναφέρει αυξήσεις της παραγωγικότητας έως και τρεις ώρες ανά εβδομάδα, ανά εργαζόμενο. Χαρακτηριστικά όπως find me/follow me, remote office, click-to-call, Outlook integration, unified voice mail, conference calling και collaboration tools επιτρέπουν την αύξηση της παραγωγικότητας.

3. Το συνεχιζόμενο κόστος συντήρησης και επισκευής μπορεί να είναι χαμηλότερο.
4. Πολλά συστήματα VoIP απαιτούν λίγη ή καθόλου εκπαίδευση για τους χρήστες.
5. Οι επιβαρύνσεις κινητής τηλεφωνίας μειώνονται καθώς οι εργαζόμενοι κάνουν κλήσεις μέσω του φορητού υπολογιστή τους, αντί του κινητού τους τηλεφώνου. Αυτές οι κλήσεις δικτύου αποτελούν μέρος των επιβαρύνσεων δικτύου και κοστίζουν μόνο το ποσό της ίδιας της σύνδεσης στο Internet.
6. Το κόστος τηλεφώνου τηλεργασίας μειώνεται και δεν υπάρχουν σημαντικά τέλη εγκατάστασης. Η φωνητική επικοινωνία πραγματοποιείται μέσω ευρυζωνικής σύνδεσης.
7. Το VoIP επιτρέπει ενιαία μυνηματα (unified messaging). Τα συστήματα πληροφοριών είναι ολοκληρωμένα.
8. Η κρυπτογράφηση των φωνητικών κλήσεων υποστηρίζεται.
9. Λιγότερο διοικητικό προσωπικό απαιτείται για να απαντά στα τηλέφωνα.
10. Ένα packet voice δίκτυο, ή δίκτυο που υποστηρίζει την κίνηση φωνής, έχει μια σειρά από πιθανές συνιστώσες:

- IP τηλέφωνα: Παρέχει IP φωνή στην επιφάνεια εργασίας.
- Gateway: Παρέχει μετάφραση μεταξύ VoIP και μη-VoIP δίκτυα, όπως το PSTN. Τα Gateways παρέχουν επίσης φυσική

πρόσβαση σε τοπικές αναλογικές και ψηφιακές συσκευές φωνής, όπως τηλέφωνα, συσκευές φαξ, βασικά σύνολα και PBXs.

- Μονάδα ελέγχου πολλαπλών σημείων (Multipoint control unit-MCU): Παρέχει σύνδεση σε πραγματικό χρόνο για τους συμμετέχοντες σε πολλαπλές τοποθεσίες για να παρακολουθήσουν την ίδια τηλεδιάσκεψη ή συνάντηση.
- Εξυπηρετητής τηλεφωνίας (Call agent): Παρέχει έλεγχο κλήσης για IP τηλέφωνα, CAC, το εύρος ζώνης ελέγχου και διαχείρισης, καθώς και τη μετάφραση διεύθυνσης.
- Δρομολογητές εφαρμογών (Application servers): Παρέχουν υπηρεσίες, όπως το φωνητικό ταχυδρομείο και unified messaging, όπως το Cisco Unity.
- Σταθμός τηλεδιάσκεψης (Video conference station) - Παρέχει πρόσβαση για τη συμμετοχή του τελικού χρήστη στη τηλεδιάσκεψη. Ο σταθμός τηλεδιάσκεψης περιέχει μια συσκευή καταγραφής βίντεο για την είσοδο βίντεο και ένα μικρόφωνο για είσοδο ήχου. Ο χρήστης μπορεί να δει ροές βίντεο και να ακούσει τον ήχο που προέρχεται σ'ένα απομακρυσμένο σταθμό χρήστη.
- VoIP επικοινωνία εμφανίζεται κατά τη διάρκεια του παραδοσιακού δικτύου δεδομένων. Αυτό σημαίνει ότι η εξασφάλιση της επικοινωνίας φωνής είναι άμεσα συνδεδεμένη με την διασφάλιση του δικτύου δεδομένων.

6.3. Μη εξουσιοδοτημένη πρόσβαση στους πόρους φωνής

Οι κακόβουλοι χρήστες μπορούν να παραποιούν τα συστήματα φωνής, την ταυτότητα των χρηστών, και τις διαμορφώσεις τηλεφώνου και να διακόπτουν voice-mail μηνύματα. Αν οι επιτιθέμενοι αποκτήσουν πρόσβαση

στο σύστημα φωνητικού ταχυδρομείου, μπορούν να αλλάξουν τον χαιρετισμό φωνητικού ταχυδρομείου, το οποίο μπορεί να έχει αρνητικό αντίκτυπο στην εικόνα και τη φήμη της εταιρίας. Ένας κακόβουλος χρήστης που αποκτά πρόσβαση στο PBX ή στη φωνητική πύλη μπορεί να κλείσει τις θύρες φωνής ή να αλλάξει τις παραμέτρους του δρομολογητή, επηρεάζοντας τη πρόσβαση φωνής μέσα και μέσω του δικτύου (Rosenberg & Schulzrinne, 2013).

Ο στόχος ενός ασφαλούς δικτύου είναι να διασφαλίσει ότι οι εφαρμογές, οι διαδικασίες και οι χρήστες μπορούν αξιόπιστα και με ασφάλεια να λειτουργούν χρησιμοποιώντας τους κοινόχρηστους πόρους του δικτύου. Επειδή η κοινή υποδομή δικτύου μεταφέρει φωνή και δεδομένα, η ασφάλεια και η πρόσβαση σε υποδομή δικτύου είναι ζωτικής σημασίας για τη διασφάλιση των φωνητικών λειτουργιών. Επειδή τα IP φωνητικά συστήματα είναι εγκατεστημένα σ'ένα δίκτυο δεδομένων, είναι πιθανοί στόχοι για τους κακόβουλους χρήστες οι οποίοι προηγουμένως είχαν ως στόχο μόνο υπολογιστές, δρομολογητές και εφαρμογές δεδομένων. Οι κακόβουλοι χρήστες βοήθησαν στην αναζήτησή τους για τα τρωτά σημεία των IP φωνητικών συστημάτων από τα ανοικτά και γνωστά πρότυπα και πρωτόκολλα που χρησιμοποιούνται από τα IP δίκτυα.

Υποκλοπές

Οι υποκλοπές περιλαμβάνουν, την παράνομη υποκλοπή των πακέτων φωνής ή RTP media streams. Οι υποκλοπές εκθέτουν εμπιστευτικές ή αποκλειστικές πληροφορίες που λαμβάνονται από την παρακολούθηση και την επανασυναρμολόγηση πακέτων σ'ένα voice stream. Οι χάκερ χρησιμοποιούν μια ποικιλία εργαλείων για την υποκλοπή (Houle, 2011).

6.4. Επιθέσεις DoS

Οι επιθέσεις DoS ορίζονται ως η κακόβουλη επίθεση ή υπερφόρτωση του call-processing εξοπλισμού να αρνηθεί την πρόσβαση στις υπηρεσίες από τους νόμιμους χρήστες. Οι περισσότερες επιθέσεις DoS εμπίπτουν σε μία από τις τρεις κατηγορίες (SANS, 2015):

1. Υπερφόρτωση των πόρων δικτύου περιλαμβάνει την υπερφόρτωση ενός πόρου δικτύου που απαιτείται για την εύρυθμη λειτουργία της υπηρεσίας. Ο πόρος του δικτύου είναι τις περισσότερες φορές το εύρος ζώνης. Η επίθεση DoS χρησιμοποιεί όλο το διαθέσιμο bandwidth, προκαλώντας εξουσιοδοτημένους χρήστες να μην είναι σε θέση να έχουν πρόσβαση στις απαιτούμενες υπηρεσίες.
2. Host resource starvation περιλαμβάνει τη χρήση κρίσιμων πόρων του host. Όταν η χρήση των πόρων αυτών μεγιστοποιείται από την επίθεση DoS, ο διακομιστής δεν μπορεί πλέον να ανταποκριθεί στα νόμιμα αιτήματα παροχής υπηρεσιών.
3. Out-of-bounds επίθεση περιλαμβάνει τη χρήση παράνομης δομής του πακέτου και απρόσμενων δεδομένων, το οποίο μπορεί να οδηγήσει το λειτουργικό σύστημα του απομακρυσμένου συστήματος στην συντριβή. Ένα παράδειγμα αυτού του τύπου της επίθεσης είναι η χρήση παράνομων συνδυασμών των TCP flags. Οι περισσότερες TCP/IP στοίβες αναπτύχθηκαν για να ανταποκριθούν στην κατάλληλη χρήση δεν έχουν αναπτυχθεί για ανωμαλίες. Όταν η στοίβα λαμβάνει παράνομα δεδομένα, μπορεί να μην ξέρει πώς να χειριστεί το

πακέτο, προκαλώντας κατάρρευση του συστήματος. (Houle, 2011)

Το Spam over Internet Telephony (SPIT), ή VoIP spam, είναι αυτόκλητα και ανεπιθύμητα μαζικά μηνύματα που μεταδίδονται μέσω VoIP στους τελικούς χρήστες ενός δικτύου της επιχείρησης. Εκτός του ότι είναι ενοχλητικές, οι υψηλής έντασης μαζικές κλήσεις μπορούν να επηρεάσουν σημαντικά τη διαθεσιμότητα και την παραγωγικότητα των τερματικών σημείων. Επειδή οι μαζικές κλήσεις είναι επίσης δύσκολο να εντοπιστούν, μπορούν να χρησιμοποιηθούν για απάτη, μη εξουσιοδοτημένη χρήση, καθώς και ιδιωτικές παραβιάσεις.

Το SPIT θα μπορούσε να παραχθεί με παρόμοιο τρόπο για το email spam με την χρήση συστημάτων κακόβουλων προγραμμάτων στοχεύοντας εκατομμύρια VoIP χρήστες από προσβεβλημένους υπολογιστές. Το αυτόκλητα εμπορικό και κακόβουλο email spam κάνει τώρα την πλειοψηφία των email σ'όλο τον κόσμο. Υπάρχει μια ανησυχία ότι το VoIP θα έχει την ίδια τύχη με το email (Houle, 2011).

Μια άλλη ανησυχία για το SPIT είναι ότι οι email anti-spam μέθοδοι δεν θα λειτουργήσουν. Η φύση των φωνητικών κλήσεων σε πραγματικό χρόνο κάνει την ενασχόληση με το SPIT πιο δύσκολη από ότι το email spam. Νέες μέθοδοι πρέπει να εφευρεθούν για την αντιμετώπιση των SPIT προβλημάτων.

6.5. VoIP Security Solutions

Πολλές IP λύσεις ασφαλείας μπορούν να εφαρμοστούν μόνο σε Layer 3 συσκευές. Λόγω της αρχιτεκτονικής του πρωτοκόλλου, το Layer 2 προσφέρει πολύ λίγη ή καμία εγγενή ασφάλεια. Η κατανόηση και η θέσπιση τομέων εκπομπής είναι μία από τις θεμελιώδεις έννοιες της σχεδίασης ασφαλών IP δικτύων. Πολλές απλές αλλά και επικίνδυνες επιθέσεις μπορούν να ξεκινήσουν εάν η επιτιθέμενη συσκευή κατοικεί εντός του ίδιου τομέα

εκπομπής, όπως το σύστημα στόχος. Για το λόγο αυτό, τα IP τηλέφωνα, τα VoIP gateways και οι θέσεις διαχείρισης του δικτύου θα πρέπει πάντα να είναι στο δικό τους υποδίκτυο, ξεχωριστά από το υπόλοιπο δίκτυο δεδομένων και από κάθε άλλο δίκτυο (Thalhammer, 2015).

Για να εξασφαλιστεί η προστασία της ιδιωτικής ζωής και της ακεραιότητας των επικοινωνιών, τα voice media streams πρέπει να προστατεύονται από υποκλοπές και παραβιάσεις. Οι data-networking τεχνολογίες όπως τα VLANs μπορούν να χωρίσουν τη κίνηση φωνής από την κίνηση των δεδομένων, εμποδίζοντας την πρόσβαση στο VLAN φωνής από το VLAN δεδομένων. Χρησιμοποιώντας ξεχωριστά VLANs για φωνή και δεδομένα αποτρέπει κάθε εισβολέα ή επιτιθέμενη εφαρμογή από την υποκλοπή και τη σύλληψη άλλης VLAN κίνησης, καθώς διασχίζει το φυσικό σύρμα. Με τη διασφάλιση ότι κάθε συσκευή συνδέεται στο δίκτυο χρησιμοποιώντας μια υποδομή μεταγωγής, τα packet-sniffing εργαλεία μπορούν επίσης να καταστούν λιγότερο αποτελεσματικά για την καταγραφή της επισκεψιμότητας των χρηστών (Thalhammer, 2015).

Η εκχώρηση της κίνησης φωνής σε συγκεκριμένα VLANs σε λογικά τμήμα κίνησης φωνής και δεδομένων είναι μια industry-wide συνιστώμενη πρακτική. Οι συσκευές οι οποίες προσδιορίζονται ως συσκευές φωνής θα πρέπει όσο το δυνατόν περισσότερο να περιορίζονται σε ειδικά VLANs φωνής. Η προσέγγιση αυτή διασφαλίζει ότι μπορούν να επικοινωνούν μόνο με άλλους πόρους φωνής. Το πιο σημαντικό, η κίνηση της φωνής διατηρείται μακριά από το γενικό δίκτυο δεδομένων, όπου θα μπορούσε πιο εύκολα να υποκλαπεί ή να αλλοιωθεί. Έχοντας ένα VLAN σχετικό με τη φωνή το καθιστά ευκολότερο στην εφαρμογή λιστών ελέγχου πρόσβασης VLAN (VACLs) για την προστασία της κίνησης φωνής (Thalhammer, 2015).

Με την κατανόηση των πρωτοκόλλων που χρησιμοποιούνται μεταξύ των συσκευών του VoIP δικτύου, αποτελεσματικά ACLs μπορούν να εφαρμοστούν στα VLANs φωνής. Τα IP τηλέφωνα στέλνουν μόνο RTP κίνηση

μεταξύ τους και ποτέ δεν έχουν λόγο να στείλουν TCP ή ICMP κίνηση το ένα στο άλλο. Τα IP τηλέφωνα στέλνουν μερικά πρωτόκολλα TCP και UDP για να επικοινωνήσουν με τους διακομιστές. Πολλές από τις επιθέσεις του IP τηλεφώνου μπορούν να διακοπούν με τη χρήση των ACLs στα VLANs φωνής για να παρεμποδίσουν αποκλίσεις από τις αρχές αυτές (Kuhn et al., 2014).

Τα τείχη προστασίας επιθεωρούν τα πακέτα και τα ταιριάζουν με τους διαμορφωμένους κανόνες με βάση τις θύρες που προσδιορίζονται. Είναι δύσκολο να προσδιοριστεί εκ των προτέρων ποιες θύρες θα χρησιμοποιηθούν σε μια φωνητική κλήση, επειδή οι θύρες διαπραγματεύονται δυναμικά κατά τη διάρκεια της εγκατάστασης κλήσης.

Τα VPNs χρησιμοποιούνται ευρέως για την παροχή ασφαλών συνδέσεων στο εταιρικό δίκτυο. Οι συνδέσεις μπορεί να προέρχονται από ένα υποκατάστημα, ένα μικρό γραφείο/home office (SOHO), ένα telecommuter, ή ένα χρήστη περιαγωγής. Το Internet Protocol Security (IPsec) μπορεί να χρησιμοποιηθεί για τις υπηρεσίες πιστοποίησης και εμπιστευτικότητας. Για να διευκολυνθεί η απόδοση, συνιστάται τα VPN τούνελ να τερματίζουν μέσα από ένα τείχος προστασίας. Το τείχος προστασίας χρησιμοποιείται για να επιθεωρήσει και να προστατεύσει τα πρωτόκολλα απλού κειμένου (Kuhn et al., 2014).

Κατά την ανάπτυξη των VPNs μέσω του Internet ή ενός δημόσιου δικτύου, είναι σημαντικό να εξεταστεί η απουσία του Quality of Service (QoS). Όπου είναι δυνατόν, το QoS θα πρέπει να αντιμετωπιστεί με τον πάροχο μέσω μιας συμφωνίας επιπέδου υπηρεσιών (SLA). Ένα SLA είναι ένα έγγραφο που περιγράφει λεπτομερώς τις αναμενόμενες QoS παραμέτρους για τα πακέτα που περνούν μέσω του δικτύου του φορέα παροχής.

Οι φωνητικές επικοινωνίες δεν λειτουργούν καλά (ή μερικές φορές καθόλου) με λανθάνουσα κατάσταση. Επειδή τα ασφαλή VPNs κρυπτογραφούν τα δεδομένα, μπορούν να δημιουργήσουν μια δυσχέρεια

απόδοσης κατά την επεξεργασία των πακέτων μέσω του αλγόριθμου κρυπτογράφησης τους. Το πρόβλημα συνήθως επιδεινώνεται όσο αυξάνεται η ασφάλεια (Kuhn et al., 2014).

Το VoIP και είτε η DES ή η 3DES κρυπτογραφήσεις είναι πλήρως συμβατές μεταξύ τους όσο το VPN προσφέρει την απαραίτητη απόδοση. Σε διεθνές επίπεδο, οι επιχειρήσεις ενδέχεται να αντιμετωπίσουν άλλα θέματα που επηρεάζουν την φωνητική επικοινωνία. Το Υπουργείο Εμπορίου των ΗΠΑ θέτει περιορισμούς στην εξαγωγή ορισμένης τεχνολογίας κρυπτογράφησης. Συνήθως, η DES είναι εξαγώγιμη ενώ η 3DES δεν είναι. Ωστόσο, οι κανονισμοί παίρνουν πολλές μορφές, από το σύνολο των αποκλεισμών των εξαγωγών που εφαρμόζονται σε ορισμένες χώρες, να επιτρέπουν την 3DES εξαγωγή σε συγκεκριμένους κλάδους και χρήστες. Οι περισσότερες εταιρίες με VPNs που εκτείνονται εκτός των Ηνωμένων Πολιτειών θα πρέπει να μάθουν αν ο πάροχος του VPN τους έχει εξαγώγιμα προϊόντα και πώς οι κανονισμοί εξαγωγών επηρεάζουν τα δίκτυα δημιουργημένα με τα εν λόγω προϊόντα (Kuhn et al., 2014).

Κατά την ασφάλιση της κίνησης φωνής, μην ξεχάσετε να ασφαλίσετε τους διακομιστές εφαρμογών φωνής. Οι νεότερες εκδόσεις του Cisco Unified Communications Manager απενεργοποιούν περιττές υπηρεσίες, απενεργοποιούν προεπιλεγμένα ονόματα χρηστών, επιτρέπουν μόνο υπογεγραμμένες εικόνες που πρόκειται να εγκατασταθούν και υποστηρίζουν ασφαλή πρωτόκολλα διαχείρισης.

Με το συνδυασμό της ασφάλειας των μεταφορών, που παρέχεται από ασφαλή LANs, τείχη προστασίας και VPNs με τα χαρακτηριστικά ασφάλειας των εφαρμογών και διαθέσιμα με το Cisco Unified Communications Manager και τα Cisco IP τηλέφωνα, είναι δυνατό να έχουμε ένα εξαιρετικά ασφαλές περιβάλλον IP τηλεφωνίας (Dhamankar, 2014).

6.6. Λύσεις ασφάλειας SAN

Ένα SAN (Storage Area Network) είναι ένα εξειδικευμένο δίκτυο που επιτρέπει τη γρήγορη και αξιόπιστη πρόσβαση στους δρομολογητές και τους εξωτερικούς πόρους αποθήκευσης. Σ'ένα SAN, μια συσκευή αποθήκευσης δεν είναι αποκλειστική ιδιοκτησία του κάθε διακομιστή. Αντίθετα, οι συσκευές αποθήκευσης μοιράζονται μεταξύ όλων των εξυπηρετητών του δικτύου ως ομότιμοι πόροι. Ακριβώς όπως ένα LAN μπορεί να χρησιμοποιηθεί για τη σύνδεση πελατών στους διακομιστές, ένα SAN μπορεί να χρησιμοποιηθεί για να συνδέσει τους δρομολογητές στην αποθήκευση, τους servers μεταξύ τους και την αποθήκευσης στην αποθήκευση.

Ένα SAN δεν χρειάζεται να είναι ξεχωριστό δίκτυο. Μπορεί να είναι ένα ειδικό υποδίκτυο που μεταφέρει εμπιστευτικά δεδομένα μεταξύ των δρομολογητών και των συσκευών αποθήκευσης. Ένα SAN, για παράδειγμα, δεν θα μεταφέρει κυκλοφορία γενικής χρήσης όπως το ηλεκτρονικό ταχυδρομείο ή άλλες εφαρμογές τερματικού χρήστη. Θα πρέπει να περιορίζεται στην I/O κυκλοφορία, όπως η ανάγνωση ενός αρχείου από έναν δίσκο ή η εφαρμογή ενός αρχείου σ'ένα δίσκο. Αυτή η προσέγγιση δικτύου βοηθά να αποφευχθεί ο απαράδεκτος συμβιβασμός και η μειωμένη απόδοση που συνυπάρχει όταν ένα ενιαίο δίκτυο χρησιμοποιείται για όλες τις εφαρμογές.

Ο χρόνος των συστημάτων εκτός λειτουργίας (downtime) του δικτύου και του διακομιστή κοστίζει στις εταιρίες μεγάλα χρηματικά ποσά στις ζημίες παραγωγικότητας. Ταυτόχρονα, η ποσότητα των πληροφοριών που πρέπει να διαχειρίζεται και να αποθηκεύεται αυξάνεται δραματικά κάθε χρόνο.

Τα SANs προσφέρουν μια απάντηση στον αυξανόμενο όγκο των δεδομένων που πρέπει να αποθηκευτεί σ'ένα εταιρικό περιβάλλον δικτύου.

Με την εφαρμογή ενός SAN, οι χρήστες μπορούν να απαλλαγούν από την κυκλοφορία αποθήκευσης, από τις καθημερινές λειτουργίες του δικτύου και να δημιουργήσουν μια άμεση σχέση μεταξύ των μέσων αποθήκευσης και των δρομολογητών.

Τα SANs σε υποδομές επιχείρησης εξελίσσονται ραγδαία ώστε να ανταποκριθούν στις τρεις κύριες επιχειρηματικές απαιτήσεις:

1. Τη μείωση κεφαλαίου και λειτουργικών εξόδων.
2. Την αύξηση της ευελιξίας για την υποστήριξη μεταβαλλόμενων επιχειρηματικών προτεραιοτήτων, τις απαιτήσεις της εφαρμογής και την αύξηση των εσόδων.
3. Τη βελτίωση αντιγραφής μεγάλης απόστασης, δημιουργία αντιγράφων ασφαλείας και ανάκτησης για να πληροί τις κανονιστικές απαιτήσεις και τις βέλτιστες πρακτικές του κλάδου.

Όλες οι μεγάλες τεχνολογίες μεταφοράς SAN είναι βασισμένες στο μοντέλο επικοινωνίας SCSI (Small Computer System Interface). Ενα SAN μπορεί να περιγραφεί ως η συγχώνευση του SCSI και της δικτύωσης. Το SCSI πρωτόκολλο εντολής είναι το de facto πρότυπο που χρησιμοποιείται ευρέως σε εφαρμογές αποθήκευσης υψηλής απόδοσης. Το μέρος εντολής του SCSI μπορεί να μεταφερθεί πάνω από ένα Fibre Channel SAN ή έγκλειστο σε IP και να μεταφερθεί σε όλα τα IP δίκτυα.

Υπάρχουν τρεις κύριες τεχνολογίες μεταφοράς SAN:

1. Fibre Channel - Αυτή η τεχνολογία είναι η κύρια SAN μεταφοράς για τον host προς συνδέσεις SAN. Παραδοσιακά, τα SANs απαιτούσαν ξεχωριστή ειδική υποδομή για τη διασύνδεση των hosts και των συστημάτων αποθήκευσης. Το κύριο πρωτόκολλο

μεταφοράς για τη διασύνδεση αυτή υπήρξε το Fibre Channel. Τα Fibre Channel δίκτυα προσφέρουν μια σειριακή μεταφορά για το πρωτόκολλο SCSI.

2. iSCSI - Καθορίζει το SCSI πάνω από το TCP/IP. Αυτό είναι ένα άλλο host to SAN μοντέλο σύνδεσης που χρησιμοποιείται συνήθως στο LAN. Ένα iSCSI αξιοποιεί μια επένδυση σε υφιστάμενα IP δίκτυα, για να δημιουργήσει και να επεκτείνει τα SANs. Αυτό επιτυγχάνεται χρησιμοποιώντας το πρωτόκολλο TCP/IP για τη μεταφορά εντολών SCSI, δεδομένων και τη κατάσταση μεταξύ hosts ή μυητών και συσκευών αποθήκευσης ή στόχους, όπως τα υποσυστήματα αποθήκευσης και συσκευές ταινίας.
3. FCIP. Δημοφιλές SAN to SAN μοντέλο σύνδεσης που χρησιμοποιείται συχνά στο WAN ή MAN (μητροπολιτικό δίκτυο περιοχής). Οι SAN σχεδιαστές μπορούν να χρησιμοποιήσουν το πρωτόκολλο ανοικτών προτύπων FCIP για να σπάσει το φράγμα απόστασης από τις τρέχουσες Fibre Channel λύσεις και να επιτρέψει τη διασύνδεση των SAN islands πάνω από μεγάλες αποστάσεις.

Στην αποθήκευση υπολογιστή, ένα αριθμός λογικής μονάδας (LUN) είναι μια 64-bit διεύθυνση για ένα μεμονωμένο δίσκο και, κατ 'επέκταση, η συσκευή δίσκου η ίδια. Ο όρος χρησιμοποιείται στο πρωτόκολλο SCSI ως ένας τρόπος για να διαφοροποιήσει επιμέρους δίσκους μέσα σε μια κοινή συσκευή προορισμού SCSI, όπως μια συστοιχία δίσκων.

Το LUN masking είναι μια διαδικασία εξουσιοδότησης που κάνει ένα LUN διαθέσιμο σε ορισμένους hosts και μη διαθέσιμο σε άλλους hosts και εφαρμόζεται κυρίως στο host bus adapter (HBA) επίπεδο. Το LUN masking που υλοποιείται σ'αυτό το επίπεδο είναι ευάλωτο σε οποιαδήποτε επίθεση που θέτει σε κίνδυνο τον HBA.

Τα οφέλη για την ασφάλεια του LUN masking είναι περιορισμένα, διότι, με πολλά HBAs, είναι δυνατή η πλαστογράφηση διευθύνσεων πηγής. Το LUN masking είναι κυρίως ένας τρόπος για την προστασία έναντι διακομιστών εσφαλμένης συμπεριφοράς που διαφθείρουν δίσκους που ανήκουν σε άλλους διακομιστές.

Για παράδειγμα, οι Windows servers που συνδέονται μ'ένα SAN μερικές φορές διαφθείρουν τα non-Windows volumes προσπαθώντας να γράψουν τις Windows volume ετικέτες σ'αυτούς. Με την απόκρυψη των LUNs των non-Windows volumes απ'το διακομιστή των Windows, αυτό μπορεί να προληφθεί, επειδή ο διακομιστής των Windows δεν συνειδητοποιεί καν ότι υπάρχουν non-Windows volumes.

Ένα world wide name (WWN) είναι μια διεύθυνση 64-bit που τα δίκτυα Fibre Channel χρησιμοποιούν για την αποκλειστική αναγνώριση κάθε στοιχείου σ'ένα δίκτυο Fibre Channel.

Το zoning (η διαμέριση σε μικρότερα υποσύνολα), μπορεί να χρησιμοποιήσει τα WWNs ώστε να εκχωρήσουν δικαιώματα ασφαλείας. Το zoning μπορεί επίσης να χρησιμοποιήσει name servers στους διακόπτες οι οποίοι είτε θα επιτρέψουν, είτε θα αποκλείσουν την πρόσβαση σε συγκεκριμένα Fabric Assigned WWNs.

Η χρήση των WWNs για λόγους ασφαλείας είναι εγγενώς ανασφαλής, διότι το WWN μιας συσκευής είναι μια παράμετρος ρυθμιζόμενη από το χρήστη. Το zoning χρησιμοποιεί WWNs που είναι ευπαθή σε μη εξουσιοδοτημένη πρόσβαση, επειδή η ζώνη μπορεί να παρακαμφθεί εάν ένας επιτιθέμενος είναι σε θέση να ξεγελάσει το WWN ενός εξουσιοδοτημένου host προσαρμογέα διαύλου (HBA). Ενας HBA είναι ένας I/O προσαρμογέας που βρίσκεται μεταξύ του διαύλου του κεντρικού υπολογιστή και του Fibre Channel βρόχου και διαχειρίζεται τη μεταφορά των πληροφοριών μεταξύ των δύο καναλιών (Grance, 2012).

ΣΥΜΠΕΡΑΣΜΑΤΑ

Στην παρούσα εργασία, μελετήθηκαν οι τεχνολογίες του τείχους προστασίας (firewall), για την προστασία των επιχειρήσεων και των συστημάτων που χρησιμοποιούνται στον βιομηχανικό τομέα.

Οι επιχειρήσεις προσπαθούν να αποφύγουν και να αντιμετωπίσουν σε καθημερινή βάση, διάφορες απειλές για την επίτευξη των επιχειρηματικών στόχων τους. Οι απειλές αυτές μπορεί να περιλαμβάνουν τον οικονομικό κίνδυνο, τον κίνδυνο αποτυχίας του εξοπλισμού και τον κίνδυνο της ασφάλειας του προσωπικού. Συνεπώς, οι επιχειρήσεις πρέπει να αναπτύξουν διαδικασίες για την αξιολόγηση των κινδύνων που σχετίζονται με την επιχείρησή τους και να αποφασίσουν πώς να αντιμετωπίσουν αυτούς τους κινδύνους με βάση τις οργανωτικές προτεραιότητες και τους εσωτερικούς και εξωτερικούς περιορισμούς. Ιδιαίτερα, στον τομέα των δικτύων θα πρέπει να εξασφαλίσουν την ακεραιότητα των δεδομένων και των ευαίσθητων πληροφοριών των ίδιων αλλά και των πελατών τους.

Για αυτό το λόγο, έχουν δημιουργηθεί κατάλληλα πρότυπα εκτιμήσεων των επιπέδων ασφαλείας και θα πρέπει να ενσωματώνονται στις κανονιστικές απαιτήσεις των επιχειρήσεων. Ένα από τα πρώτα εργαλεία για την ασφάλεια των δικτύων των επιχειρήσεων είναι το σύστημα ανίχνευσης εισβολής (Intrusion Detection Systems, IDS), το οποίο παρέχει σε πραγματικό χρόνο ανίχνευση ορισμένων τύπων επιθέσεων. Αυτή η ανίχνευση επιτρέπει στους επαγγελματίες της ασφάλειας δικτύων, την γρήγορη καταπολέμηση των αρνητικών επιπτώσεων από αυτές τις επιθέσεις σε συσκευές δικτύου και στους χρήστες. Οι συσκευές IDS επιτρέπουν την ανίχνευση της κακόβουλης δραστηριότητας και έχουν την ικανότητα να μπλοκάρουν αυτόματα την επίθεση σε πραγματικό χρόνο.

Εκτός από τις λύσεις των συστημάτων ανίχνευσης και πρόληψης εισβολών, η τεχνολογία του «τείχους προστασίας» (firewall) αναπτύχθηκε για να αποτρέψει την ανεπιθύμητη κυκλοφορία από την είσοδο που προβλέπονται στις περιοχές εντός ενός δικτύου, παρέχοντας έτσι περιμετρική ασφάλεια. Γενικά, υπάρχουν τρία είδη Firewalls:

1)τα Firewalls φιλτραρίσματος πακέτων, τα οποία ελέγχουν κάθε πακέτο σε απομόνωση χωρίς να εξετάσουν αν ένα πακέτο είναι μέρος μιας υπάρχουσας σύνδεσης

2)τα Firewalls ελέγχου κατάστασης (stateful firewalls), τα οποία χρησιμοποιούν προκαθορισμένους κανόνες για τη χορήγηση ή την απόρριψη της κυκλοφορίας

3)τα τείχη προστασίας με ενδιάμεσο δρομολογητή (Firewalls Gateway Application-Proxy). Αυτή η κατηγορία τείχους προστασίας εξετάζει τα πακέτα στο επίπεδο εφαρμογής και φιλτράρει την επισκεψιμότητα με βάση συγκεκριμένους κανόνες εφαρμογής, όπως συγκεκριμένες εφαρμογές (π.χ. προγράμματα περιήγησης) ή πρωτόκολλα (π.χ. FTP). Τα τείχη προστασίας αυτού του τύπου μπορούν να είναι πολύ αποτελεσματικά στην αποτροπή επιθέσεων στις υπηρεσίες απομακρυσμένης πρόσβασης και διαμόρφωσης που παρέχονται από τα στοιχεία ICS.

Τα κύρια πλεονεκτήματα της χρήσης των firewalls είναι η προστασία από ευπαθείς υπηρεσίες, η ελεγχόμενη πρόσβαση και η συγκεντρωμένη ασφάλεια. Στα συστήματα βιομηχανικού αυτόματου ελέγχου και τηλεμετρίας (Supervisory Control And Data Acquisition, SCADA) που χρησιμοποιούνται στον τομέα της βιομηχανίας είναι απαραίτητο να αξιολογούνται για ευπάθειας της ασφάλειας. Η χρήση των firewalls, στα συστήματα βιομηχανικού αυτόματου ελέγχου και τηλεμετρίας, τμηματοποιούν το δίκτυό της επιχείρησης σε δύο περιβάλλοντα, το ένα για την εταιρική / πληροφορική και το άλλο για τα συστήματα ελέγχου SCADA και διαδικασιών.

ΤΟ ΜΕΛΛΟΝ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ FIREWALL

Η βιομηχανία ασφάλειας στον κυβερνοχώρο φαίνεται να αλλάζει καθημερινά, αλλά ένα πράγμα παραμένει το ίδιο, οι επιτιθέμενοι είναι όλο και περισσότεροι και είναι σε θέση να παραβιάζουν όλες τις εταιρίες, ανεξαρτήτου μεγέθους.

Σύμφωνα με την εταιρία, Palo Alto Networks, τα τείχη προστασίας θα επικεντρωθούν σε πληροφορίες ανώτερου επιπέδου για να κατανοήσουν την κατάσταση. Θα γίνουν πιο δυναμικά για να προσαρμοστούν στις αλλαγές των απειλών κατά τη διάρκεια του χρόνου και θα καταστούν περισσότερο ικανά να χωρίσουν το δίκτυο χωρίς να διαταράξουν την επικοινωνία των μηχανημάτων. Ο Michael Kiefer της εταιρίας BrandProtect πιστεύει ότι ενώ τα τείχη προστασίας είναι απαραίτητα στην περιμετρική ασφάλεια, πρέπει να ενισχυθούν όσο αναφορά την παρακολούθηση εξωτερικών απειλών. Οι ειδικοί της ασφάλειας, θα πρέπει, αντί να επικεντρωθούν αποκλειστικά στο τι υπάρχει μέσα στο τείχος προστασίας, να εστιάσουν στην ασφάλεια εκτός της περιφερειακής άμυνας των firewall έξω από την περίμετρο.

Ο Jonathan Sander, της εταιρίας Lieberman Software, θεωρεί ότι ο τρόπος της εφαρμογής των firewall θα αλλάξει στο μέλλον. Στο μέλλον, η ανθρώπινη παρέμβαση, για την λήψη αποφάσεων, κατά την εμφάνιση των απειλών δεν θα είναι αναγκαία. Η εξέλιξη της μηχανικής μάθησης θα επιτρέψει στα τείχη προστασίας να αναλάβουν αυτόματα τους επιτιθέμενους και να ενεργούν χωρίς την βοήθεια του ανθρώπου.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. American Gas Association, AGA Report No. 12 (2006), Cryptographic Protection of SCADA Communications, Part 1: Background, Policies and Test Plan, September, March 14, 2006
2. Axelsson, S.(1999)," Research in intrusion detection systems: a survey". Technical Report TR 98-17 (revised in 1999). Chalmers University of Technology, Goteborg, Sweden (1999)
3. Avishai Wool (2004), A Quantitative Study of Firewall Configuration Errors. Computer, 37(6):62–67
4. Bailey, David, and Edwin Wright (2013), Practical SCADA for Industry, Vancouver: IDC Technologies, 2013.
5. Boyer, Stuart, SCADA (2010), Supervisory Control and Data Acquisition. 4th ed. Research Triangle Park, North Carolina: International Society of Automation
6. British Columbia Institute of Technology- BCIT (2005), "Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks (Prepared for National Infrastructure Security Coordination Centre)", National Infrastructure Security Co-ordination Centre (NISCC), February 2005. Available at: http://www.cpni.gov.uk/docs/re-20050223-00157.pdf
7. Carpenter,B. Brim,S., Middleboxes (2002): Taxonomy and Issues, RFC 3234,
8. Chapple M.(2014), . Four Tips for Securing a Network DMZ. 18 May 2012. 11
9. Collin Jackson, Adam Barth, Andrew Bortz, Weidong Shao, and Dan Boneh (2009), Protecting browsers from dns rebinding attacks. ACM Trans. Web, 3(1):2:1–2:26
10. Dorothy E.(1986) Denning.An intrusion detection model. In Proceedings of the IEEE Symposium on Security and Privacy, pages 118
11. Galbally J & Marcel S (2014) Face anti-spoofing based on general image quality assessment. Proc. Proc. IAPR/IEEE Int. Conf. on Pattern Recognition, ICPR, 1173–1178.

12. Gao X, Ng TT, Qiu B & Chang SF (2010) Single-view recaptured image detection based on physics-based features. Proc. IEEE International Conference on Multimedia & Expo (ICME), 1469–1474
13. Government Accountability Office (GAO), GAO-15-6 (2014), Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems
14. FORE Systems (1999), Firewall Switching Agent White Paper
15. Forrest, K. I. (2012, 02 1). A History and Survey of Network Firewalls. Retrieved from University of New Mexico: http://www.cs.unm.edu/~treport/tr/02-12/firewall.pdf
16. Ginter, A. (2012). UTC. Retrieved from UTC.org: http://www.utc.org/sites/default/files/public/UTC_Public_files/Stronger%20than%20Fire walls%20and%20Cheaper%20Too.pdf
17. Grance, Tim, et al.(2012), NIST SP 800-61, Revision 2, Computer Security Incident Handling Guide, 2012
18. Hong Liu, Mouchtaris,(2010), Voice over IP signaling: H.323 and beyond, P., IEEE Communications Magazine, Vol.: 38 Issue: 10
19. Industrial Automation Open Networking Association (IAONA)(2005), The IAONA Handbook for Network Security, Version 1.3, http://www.iaona.org/pictures/files/1122888138-IAONA_HNS_1_3-reduced_050725.pdf
20. Johnson, Arnold (2011) NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems
21. Joint Task Force Transformation Initiative (2014) Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans
22. Johann Thalhammer (2015). Security in voip - telephony systems. Master's thesis, Institute for Applied Information Processing and Communications, Graz University of Technology, Graz, Austria
23. Jingmin Zhou, Mark Heckman, Brennan Reynolds, Adam Carlson, and Matt Bishop (2007), Modelling Network Intrusion Detection Alerts for Correlation. ACM Transactions on Information and System Security (TISSEC), 10(1),
24. Knapp, Eric, Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, Waltham,
25. Kevin. J. Houle and George. M. Weaver (2011), "Trends in Denial of Service Attack Technology," CERT Advisory, v1.0, Oct. 2011

26. McCallister E.(2010), NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), April 2010
27. Misherghi G., Lihua Yuan, Zhendong Su, Chen-Nee Chuah, and Hao Chen (2008), A general framework for benchmarking firewall optimization techniques. IEEE Trans. on Netw. and Serv. Manag., 5(4):227–238, December 2008.
28. Michael, C. (2009, August). Computer Viruses Slow African Expansion. Guardian. Retrieved from https://www. theguardian.com/technology/2009/aug/12/ethiopia-computer-virus
29. McAfee. (2017, April). McAfee Labs Threat Report: April 2017 (Rep.) Retrieved from https://www.mcafee.com/ca/ security-awareness/articles/mcafee-labs-threats-report-mar-2017.aspx
30. NIST. (2011, 6). NIST 800-82: Guide to Industrial Control System (ICS) Security. Retrieved from NIST.Gov: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf
31. NIST. (2013, 4). Security and Privacy Controls for Federal Information Systems and Organizations. Retrieved from NIST: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
32. Olivier Hersent, David Gurle, and Jean-Pierre Petit (2011) IP Telephony, volume 54. Addison Wesley Longman (Singapore) Pte. Ltd
33. Richard Kuhn, Thomas J. Walsh, and Steffen Fries (2014) Security considerations for voice over ip systems. Computer Security
34. Rosenberg and H. Schulzrinne (2013), “SIP Traversal through Residential and Enterprise NATs and Firewalls”. Internet Draft, Internet Engineering Task Force
35. Robert Marmorstein and Phil Kearns (2005). A Tool for Automated iptables Firewall Analysis. In USENIX Annual Technical Conference
36. Sihyung Lee, Tina Wong, and Hyong S. Kim (2008). Improving Dependability of Network Configuration through Policy Classification. In IEEE/IFIP Conference on Dependable Systems and Networks
37. Rohit Dhamankar (2014) Intrusion Prevention: The Future of VoIP Security
38. SANS Institute. (2015). Infrastructure Security Architecture for Effective Security Monitoring. (Publication) Retrieved from https://www.sans.org/reading-room/whitepapers/bestprac/infrastructure-security-architectureeffective-security-monitoring-36512

39. Thurman, M. (2011), . Security Manager's Journal: Keeping the DMZ safe.
40. Udani O. (2011), Voice over IP, Mehta, P.; IEEE Potentials, Vol.: 20 Issue: 4
41. Vijayakumar, G. Jakka, S. Rueda, J. Schiffman, and T. Jaeger (2012), Integrity walls: Finding attack surfaces from mandatory access control policies. In ASIACCS
42. William Stallings (2011). Cryptography and Network Security: Principles and Practice. Pearson Education, 5th edition