Τ.Ε.Ι. ΑΡΤΑΣ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ
ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΑΝΑΛΥΣΗ ΑΔΥΝΑΜΙΩΝ

ΟΝΟΝΑΤΕΠΩΝΥΜΟ ΦΟΙΤΗΤΗ
ΚΩΣΤΑΡΑ ΑΝΝΑ ΑΜ 9189
ΣΚΑΖΑ ΠΑΥΛΙΝΑ – ΠΑΡΑΣΚΕΥΗ ΑΜ 9298

ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΕΠΙΒΛΕΠΟΝΤΑ ΚΑΘΗΓΗΤΗ
ΣΑΚΚΑΣ ΛΑΜΠΡΟΣ

ΑΡΤΑ, 2015

ΔΗΛΩΣΗ ΠΕΡΙ ΛΟΓΟΚΛΟΠΗΣ

Η παρούσα εργασία αποτελεί προϊόν αποκλειστικά δικής μου προσπάθειας. Όλες οι πηγές που χρησιμοποιήθηκαν περιλαμβάνονται στη βιβλιογραφία και γίνεται ρητή αναφορά σε αυτές μέσα στο κείμενο όπου έχουν χρησιμοποιηθεί.

ΕΙΣΑΓΩΓΗ

Το πρόβλημα της ασφάλειας στα δίκτυα υπολογιστών απασχολεί τα τελευταία χρόνια έντονα πληθώρα κοινωνικών ομάδων, όπως είναι απλοί χρήστες του διαδικτύου έως και μεγάλοι εμπορικοί και μη οργανισμοί. Τα θέματα της ασφάλειας του διαδικτύου λόγω της ιδιαίτερης σημασίας που έχουν κινητοποιήσει σε μεγάλο βαθμό την επιστημονική κοινότητα αλλά και τις εταιρείες κατασκευής λογισμικού και υλικού, οδηγώντας τες προς την κατεύθυνση της κατανόησης, ανάλυσης και εύρεσης μεθόδων βελτίωσης.

Στην παρούσα εργασία σκοπός είναι να παρουσιαστούν τα κύρια σημεία στα οποία τίθενται ζητήματα ασφάλειας σε σχέση με τον τομέα των δικτύων των υπολογιστών αλλά επιπλέον και να εξηγηθούν και αναλυθούν οι αδυναμίες εκείνες οι οποίες δημιουργούν τα εν λόγω ζητήματα ασφάλειας.

Πιο συγκεκριμένα στο πρώτο κεφάλαιο γίνεται μια εισαγωγή στο αναγκαίο θεωρητικό υπόβαθρό στο οποίο στηρίζεται όλη η εργασία. Το υπόβαθρο αυτό περιλαμβάνει αναφορές σε είδη και κατηγορίες δικτύων υπολογιστών. Κατά καιρούς πολλοί είναι οι τρόποι με τους οποίους έχουν κατηγοριοποιηθεί τα δίκτυα υπολογιστών. Κάθε ένα από τα κριτήρια αυτά είναι εξίσου σημαντικό με τα υπόλοιπα. Ωστόσο μπορούμε να πούμε ότι μια κοινώς αποδεκτή κατηγοριοποίηση γίνεται με βάση δύο κριτήρια, την τεχνολογία μετάδοσης και την κλίμακα.

Στην συνέχεια στο δεύτερο κεφάλαιο περνάμε στο κυρίως θέμα της εργασίας το οποίο έχει να κάνει με την ανάλυση των αδυναμιών, από τις οποίες ανακύπτουν τα θέματα ασφάλειας. Παρόμοιας σημαντικότητας είναι και οι επιθέσεις που γίνονται ως αποτέλεσμα αυτών των τρωτών σημείων των δικτύων.

Τέλος στο 3^{ο} και τελευταίο κεφάλαιο κάνουμε λόγο για τις διάφορες τεχνικές οι οποίες έχουν προταθεί κατά καιρούς για να δώσουν λύση στο θέμα της ασφαλείας. Τέτοιες μέθοδοι είναι η κρυπτογραφία, η χρήση τείχους προστασίας, τα πρωτόκολλα ασφάλειας, κα. Ωστόσο καταλήγουμε στο συμπέρασμα ότι πότε καμία μέθοδος και τεχνική δεν θα είναι 100% ασφαλής, λόγω του ασύμφορου κόστους ανάπτυξης ενός τέτοιου συστήματος. Πιστεύουμε πως η ασφάλεια των δικτύων είναι ένα θέμα που χρειάζεται συνεχή παρακολούθηση και ενασχόληση για όσους ενδιαφέρονται στην πράξη για τέτοια θέματα.

Περιεχόμενα

Κεφάλαιο 1ο 6
Δίκτυα Υπολογιστών 6
1.1.Εισαγωγή 6
1.2. Εταιρικά και Επιχειρησιακά Δίκτυα Υπολογιστών 8
1.3. Πολυπλοκότητα Δικτύων Υπολογιστών 10
1.4 Οικιακά Δίκτυα Υπολογιστών 11
1.5. Κατηγορίες Δικτύων 13
1.5.1. Τεχνολογίες Μετάδοσης 13
1.5.2. Κλίμακα Δικτύων Υπολογιστών 15
Κεφάλαιο 2ο 19
Αδυναμίες Δικτύων Υπολογιστών - Επιθέσεις 19
2.1. Η Σημαντικότητα της Ασφάλειας 19
2.2. Ιστορικό Επιθέσεων σε Δίκτυα 22
2.3. Είδη Επιθέσεων 25
2.4. Υποκλοπή Προσωπικών Δεδομένων 37
2.5. Ανάλυση Αδυναμιών 38
2.5.1. Αδυναμίες στο Σχεδιασμό του Λογισμικού 38
2.5.2. Αδυναμίες στην Υλοποίηση του Λογισμικού 39
2.5.3. Αδυναμίες στην Διαμόρφωση Συστημάτων και Δικτύων 40
2.6. Προετοιμασία και Υλοποίηση της Επίθεσης 41
Κεφάλαιο 3ο 45
Μεθοδολογίες Βελτίωσης της Ασφάλειας 45
3.1. Γενική Μεθοδολογία Ασφάλειας 45
3.2. Αποτίμηση Κινδύνου 47
3.3. Πολιτικές Ασφάλειας 50
3.4. Κανόνες Ασφαλείας Δικτύων 54
3.5. Ασφάλεια με Τείχος Προστασίας 58
3.6. Υπηρεσίες για την Ασφάλεια 66

3.7. Πρωτόκολλα για την Ασφάλεια 71
3.8. Ενίσχυση της Ασφάλειας 77
3.9. Κρυπτογραφία 78
3.9.1. Συμμετρική Κρυπτογράφηση 79
3.9.2. Ασύμμετρη Κρυπτογράφηση 79
3.9.3. Αλγόριθμοι Κατακερματισμού 80
Βιβλιογραφία 84

Κεφάλαιο 1^{ο}

Δίκτυα Υπολογιστών

1.1.Εισαγωγή

Δίκτυο στην επιστήμη των επικοινωνιών αποτελεί ένα σύστημα το οποίο συνδέει κυρίως τερματικές συσκευές διαφόρων ειδών, είτε είναι απλές («χαζά» τερματικά) είτε είναι κανονικοί υπολογιστές. Ο σκοπός της δομής του δε είναι τέτοιος που επιτρέπει την επικοινωνία μεταξύ αυτών των δικτύων. Ένα δίκτυο συνήθως αποτελείται από τα συστατικά του στοιχεία, τα οποία είναι κόμβοι σύνδεσης, συσκευές τηλεπικοινωνιών αλλά και μέσα σύνδεσης /διέλευσης πληροφοριών, προκειμένου οι χρήστες του να αποκτήσουν κοινή χρήση στους υπάρχοντες πόρους, δηλαδή κοινή πρόσβαση στις διάφορες συσκευές υλικού όπως εκτυπωτές και σαρωτές, το λογισμικό όπως προγράμματα και τα δεδομένα - αρχεία που διαθέτει.

Τα δίκτυα υπολογιστών όπως θα δούμε και στη συνέχεια προσφέρουν την δυνατότητα ανάμιξης της πληροφορίας, των επικοινωνιών και της διασκέδασης. Τα

δίκτυα υπολογιστών αυξάνονται εκρηκτικά με το πέρασμα των χρόνων. Πριν από τρείς δεκαετίες περίπου, ελάχιστοι ήταν αυτοί που είχαν πρόσβαση σε έναν δίκτυο. Σήμερα η επικοινωνία των υπολογιστών έχει γίνει απαραίτητο μέρος της υποδομής μας. Η δικτύωση χρησιμοποιείται σχεδόν σε κάθε δραστηριότητα των επιχειρήσεων – δημόσιων και ιδιωτικών – όπως στην διαφήμιση, την παραγωγή, την διεκπεραίωση, τον σχεδιασμό, την κοστολόγηση και την λογιστική [9].

Αυτός είναι άλλωστε και ο βασικός λόγος για τον οποίο τα μελετάμε. Η συνεχιζόμενη ανάπτυξη του παγκόσμιου διαδικτύου επίσης, δηλαδή το Διαδίκτυο (Internet), είναι ένα από τα πιο ενδιαφέροντα και εντυπωσιακά φαινόμενα της δικτύωσης. Πριν από είκοσι περίπου χρόνια, το διαδίκτυο ήταν ένα ερευνητικό έργο που περιλάμβανε μερικές δεκάδες τοποθεσίες. Σήμερα, έχει εξελιχθεί σε ένα σύστημα επικοινωνίας που χρησιμοποιείται στην παραγωγή, το οποίο φτάνει σε εκατομμύρια άτομα από όλες τις κατοικημένες χώρες του κόσμου.

Σε πολλές χώρες του κόσμου, και στην Ελλάδα, το διαδίκτυο συνδέει επιχειρήσεις, κολέγια και πανεπιστήμια, καθώς και κρατικές, περιφερειακές και τοπικές δημόσιες υπηρεσίες και οργανισμούς όπως σχολεία. Ακόμα οι ιδιωτικές κατοικίες έχουν πρόσβαση στο διαδίκτυο σήμερα, διαμέσω του τηλεφωνικού συστήματος που διαθέτουν και επιτυγχάνουν υψηλές ταχύτητες μέσω του κατάλληλου εξοπλισμού όπως καλωδιακά μόντεμ, δορυφόρων και ασύρματων τεχνολογιών [11].

Η μεγάλη αύξηση της δικτύωσης έχει και οικονομικές επιπτώσεις. Τα δίκτυα μετάδοσης δεδομένων έχουν κάνει εφικτές τις συναλλαγές από απόσταση για μεμονωμένα άτομα, και έχουν αλλάξει τις επαγγελματικές επικοινωνίες. Ακόμα έχει αναδυθεί μια ολόκληρη βιομηχανία η οποία αναπτύσσει δικτυακές τεχνολογίες, προϊόντα και υπηρεσίες. Η δημοτικότητα και η σημασία της δικτύωσης των υπολογιστών έχει δημιουργήσει σε όλες τις εργασίες, ισχυρή ζήτηση για άτομα με περισσότερες γνώσεις δικτύωσης [2]. Οι επιχειρήσεις χρειάζονται άτομα που να μπορούν να σχεδιάζουν, να προμηθεύονται, να εγκαθιστούν, να λειτουργούν και να

διαχειρίζονται τα συστήματα υλικού και λογισμικού που αποτελούν τα δίκτυα και τα διαδίκτυα υπολογιστών. Ακόμα ο προγραμματισμός υπολογιστών δεν περιορίζεται πλέον σε μεμονωμένους υπολογιστές – αναμένεται από τους προγραμματιστές να σχεδιάζουν και να υλοποιούν λογισμικό εφαρμογών που να μπορεί να επικοινωνεί με λογισμικό που βρίσκεται σε άλλους υπολογιστές.

1.2. Εταιρικά και Επιχειρησιακά Δίκτυα Υπολογιστών

Στα πλαίσια του όλο και συνεχώς αυξανόμενου ανταγωνισμού των σημερινών επιχειρήσεων και οργανισμών, η καθιέρωση της χρήσης ηλεκτρονικών υπολογιστών απαιτεί επιτακτική ανάγκη για την βιωσιμότητα τους. Πολλές είναι οι επιχειρήσεις σήμερα που διαθέτουν έναν αρκετά μεγάλο αριθμό ηλεκτρονικών υπολογιστών σε λειτουργία, οι οποίοι βρίσκονται τόσο σε μικρή απόσταση όσο επίσης και σε μεγάλες αποστάσεις μεταξύ τους. Για παράδειγμα, μια επιχείρηση η οποία έχει πολλά εργοστάσια, μπορεί να εγκαθιστά και να λειτουργεί έναν υπολογιστή σε κάθε μέρος προκειμένου να διατηρεί αρχεία που έχουν να κάνουν με τα αποθέματα, με την παρακολούθηση και τον έλεγχο της παραγωγικότητας των εργαζομένων της και με την διεκπεραίωση να διαφόρων εργασιών όπως είναι η τοπική μισθοδοσία.

Τα πρώτα πρότυπα υπολογιστικών συστημάτων τα οποία χρησιμοποίησαν οι επιχειρήσεις, ο κάθε υπολογιστής μέρος του υπολογιστικού συστήματος μπορούσε να αξιοποιείται ξεχωριστά από τους υπόλοιπους. Όμως με την πάροδο των χρόνων αλλά και την ανάπτυξη της πληροφορικής και των τηλεπικοινωνιών, οι επιχειρήσεις και οι λοιποί οργανισμοί, άρχισαν να αποκτούν άμεση πρόσβαση στην πληροφορία. Υπό αυτές τις συνθήκες προέκυψε και το πρόβλημα του ορθού καταμερισμού των πόρων [1].

Οι επιχειρήσεις τότε αποφάσισαν να προβούν στην διασύνδεση όλων των υπολογιστών που διέθεταν με στόχο γα γίνουν κοινόχρηστα όλα τα προγράμματα και το υλικό και κυρίως τα δεδομένα και τα αρχεία σε οποιονδήποτε έκανε χρήση του δικτύου, ανεξάρτητα από την χωρική θέση των πόρων και των χρηστών. Επιπλέον με την διασύνδεση των υπολογιστών τους δίνονταν η δυνατότητα να εξάγουν και να συσχετίζουν πληροφορίες οι οποίες προέρχονταν από διάφορους υπολογιστές του οργανισμού.

Επιπρόσθετα, ένα πλεονέκτημα για την λειτουργία της επιχείρησης η οποία κάνει χρήση δικτύων υπολογιστών, είναι και η ασφάλεια που παρέχει στην διατήρηση των δεδομένων της, παρέχοντας έτσι υψηλή αξιοπιστία. Αυτό πραγματοποιείται μέσω εναλλακτικών πηγών τροφοδοσίας με αποτέλεσμα στις περιπτώσεις που κάποια μονάδα επεξεργασίας τεθεί εκτός λειτουργίας, οι υπόλοιπες να είναι σε θέση να αναλάβουν την εργασία της, η ακόμα και αν λειτουργήσουν ανεξάρτητα από αυτή [9].

Πολύ σημαντικό ρόλο έπαιξε εδώ είναι και ο παράγοντας της εξοικονόμησης οικονομικών πόρων τόσο για τις επιχειρήσεις, των οποίων ο κερδοσκοπικός χαρακτήρας επιβάλει μια τέτοια τακτική όσο και για έναν οργανισμό ο οποίος έχει μεγάλο αριθμό εργαζομένων και κατά συνέπεια μεγάλο αριθμό υπολογιστικών μονάδων. Είναι βέβαιο ότι οι μικροί υπολογιστές έχουν πολύ καλύτερο λόγο κόστους προς επίδοση από τους μεγαλύτερους. Από την άλλη πλευρά τα μεγάλα υπολογιστικά συστήματα δουλεύουν με μεγαλύτερες ταχύτητες από τους προσωπικούς υπολογιστές αλλά το μειονέκτημα τους είναι ότι κοστίζουν πολύ περισσότερο.

Λόγω της παραπάνω ανισορροπίας οι σχεδιαστές δικτύων κατασκεύασαν συστήματα τα οποία αποτελούνταν από πολλούς προσωπικούς υπολογιστές. Στο επίκεντρο των προσωπικών βρίσκονταν ένας ή περισσότεροι κοινόχρηστοι εξυπηρετητές αρχείων, οι οποίοι διατηρούν και συντηρούν τα δεδομένα του

συστήματος. Το σύστημα αυτό είναι το πολύ γνωστό σε όλους μας μοντέλο πελάτη-εξυπηρετητή στο οποίο η επικοινωνία πραγματοποιείται με την ανταλλαγή μηνυμάτων αίτησης από τον πελάτη στον εξυπηρετητή. Ο εξυπηρετητής πραγματοποιεί και ολοκληρώνει την εργασία και αποστέλλει πίσω την απάντηση.

Ένας ακόμα στόχος της δικτύωσης των υπολογιστών αποτελεί και η ικανότητα σταδιακής αύξησης της επίδοσης του όλου συστήματος, αφού πολλαπλασιάζει το φορτίο, κάνοντας πρόσθεση περισσοτέρων επεξεργαστών. Στην περίπτωση δε των μεγάλων υπολογιστικών συστημάτων, αν αυτά εξαντλήσουν τις δυνάμεις τους, απαιτείται να αντικατασταθούν από άλλα μεγαλύτερα, τα οποία έχουν και αυξημένο κόστος και δημιουργούν ακόμα περισσότερη αναστάτωση στους χρήστες τους. [12]

Εν τέλει ένα επιπλέον όφελος που απολαμβάνει μια επιχείρηση ή ένας οργανισμός κάνοντας χρήση δικτύων υπολογιστών στους χώρους δραστηριοποίησής της, είναι η διευκόλυνση της άμεσης επικοινωνίας μεταξύ των εργαζόμενων της ακόμα και σε περιπτώσει που βρίσκονται σε μεγάλες γεωγραφικές αποστάσεις αλλά και η εκπόνηση ομαδικών εργασιών οι οποίες απαιτούν ομαδική συμβολή και προσπάθεια στην επίτευξη των στόχων της επιχείρησης και που σε αντίθετη περίπτωση είναι χρονοβόρες και πολλές φορές μη αποδοτικές. [2]

1.3. Πολυπλοκότητα Δικτύων Υπολογιστών

Η δικτύωση των υπολογιστών είναι ένα πολύπλοκο θέμα. Υπάρχουν πολλές τεχνολογίες και η κάθε τεχνολογία έχει τα δικά της χαρακτηριστικά τα οποία την κάνουν να ξεχωρίζει από άλλες. Πολλοί οργανισμοί έχουν δημιουργήσει πρότυπα δικτύωσης ανεξάρτητα, τα οποία δεν είναι όλα συμβατά. Πολλές επιχειρήσεις έχουν

δημιουργήσει εμπορικά προϊόντα και υπηρεσίες δικτύωσης τα οποία χρησιμοποιούν τις τεχνολογίες με μη συμβατικούς τρόπους. Η δικτύωση επίσης είναι πολύπλοκη επειδή υπάρχουν πολλές τεχνολογίες οι οποίες μπορούν να χρησιμοποιηθούν για την διασύνδεση δύο η περισσότερων δικτύων. Συνεπώς υπάρχουν πολλοί πιθανοί συνδυασμοί [9].

Η δικτύωση μπορεί να προκαλέσει ιδιαίτερα μεγάλη σύγχυση σε έναν αρχάριο, επειδή δεν βασίζεται σε μια ενιαία θεωρία που να εξηγεί την σχέση μεταξύ όλων των τμημάτων. Είναι αλήθεια ότι οι διάφοροι οργανισμοί και ερευνητικές ομάδες έχουν προσπαθήσει να ορίσουν εννοιολογικά μοντέλα που να μπορούν να χρησιμοποιηθούν για να εξηγήσουν τις διαφορές και τις ομοιότητες μεταξύ των δικτυακών συστημάτων υλικού και λογισμικού. Δυστυχώς το σύνολο των τεχνολογιών είναι ετερογενές και γρήγορα μεταβαλλόμενο, τα μοντέλα είναι είτε τόσο απλουστευτικά που δεν διακρίνουν τις λεπτομέρειες, είτε τόσο πολύπλοκα που δεν βοηθούν στην απλούστευση του θέματος.

Η έλλειψη μιας υποκειμενικής θεωρίας δημιουργεί ακόμα μια δυσκολία για τους αρχάριους. Δεν υπάρχει απλή και ενιαία ορολογία για τις έννοιες της δικτύωσης. Επειδή είναι πολλοί οι οργανισμοί που ορίζουν τεχνολογίες και διάφορα πρότυπα δικτύωσης, υπάρχουν και πολλοί όροι για μια δεδομένη έννοια. Έτσι εκτός από ένα ευρύ σύνολο όρων και ακρωνύμων το οποίο περιέχει πληθώρα συνωνύμων, η ειδική ορολογία της δικτύωσης περιέχει και όρους που είναι συντμήσεις , χρησιμοποιούνται λανθασμένα, η συνδέονται με προϊόντα. [9]

1.4 Οικιακά Δίκτυα Υπολογιστών

Οι επιχειρήσεις όπως προαναφέραμε χρησιμοποιούν δίκτυα υπολογιστών για την διευκόλυνση των εργασιών που καλούνται να διεκπεραιώσουν ενώ ο απώτερος

σκοπός χρήσης τους είναι τα τεχνολογικά και οικονομικά κίνητρα που τα δίκτυα τους δίνουν. Όμως η χρήση δικτύων τις περισσότερες φορές απαιτεί την χρήση μεγάλων υπολογιστικών συστημάτων, ιδιαίτερα σε επιχειρήσεις οι οποίες διέθεταν υποκαταστήματα σε διαφορετικές πόλεις ή ακόμα και χώρους του κόσμου. Προφανώς αυτού του είδους τα συστήματα έχουν μεγάλο κόστος αγοράς και συντήρησης.

Αντίθετα τα οικιακά δίκτυα δίνουν το όφελος του μικρού κόστους, αφού οι μόνες τεχνολογίες οι οποίες χρησιμοποιούν είναι απλοί προσωπικοί υπολογιστές. Κατά την εμφάνιση τους έγιναν ιδιαίτερα δημοφιλή, ενώ δεν μπορεί να αμφισβητηθεί και το γεγονός ότι γενικά τα οικιακά δίκτυα αποτέλεσαν την αιτία να γίνουν γνωστά σε πολύ κόσμο οι τεχνολογίες δικτύων υπολογιστών. Η εμφάνιση των τοπικών οικιακών δικτύων συντελέστηκε στις αρχές της δεκαετίας του 90, ακολουθούμενη από σειρά σημαντικών παρεχόμενων υπηρεσιών, οι οποίες είχαν να κάνουν με την πρόσβαση των χρηστών των δικτύων σε απομακρυσμένες πληροφορίες, με την επικοινωνία πρόσωπο με πρόσωπο καθώς και την διασκέδαση με αλληλεπίδραση[2].

Αποτελεί πραγματικότητα ότι πληθώρα ανθρώπων στις μέρες μας πραγματοποιούν τις τραπεζικές τους συναλλαγές καθώς και τις αγορές τους με ηλεκτρονικό τρόπο ενώ οι κατάλογοι των προϊόντων και των υπηρεσιών που μπορεί κανείς να βρει μέσω του διαδικτύου εμπλουτίζονται διαρκώς και γίνονται πιο δελεαστικοί. Η έγκαιρη ενημέρωση και πληροφόρηση για θέματα ενδιαφέροντος έχει αποδειχθεί ευκολότερη από ποτέ, κυρίως μέσω του ηλεκτρονικού τύπου, ενώ παραδοσιακές συνήθειες όπως το ψάξιμο ενός βιβλίου σε ένα βιβλιοπωλείο και το παραδοσιακό ταχυδρομείο έχουν αντικατασταθεί πλέον από την σύνθετη αναζήτηση (μέσω θέσπισης κριτηρίων) μεταξύ εκατομμυρίων τίτλων και την γρήγορη του τίτλου που μας ενδιαφέρει στα ράφια ενός εικονικού βιβλιοπωλείου και την αποστολή μηνυμάτων μέσω ηλεκτρονικού ταχυδρομείου [12].

1.5. Κατηγορίες Δικτύων

Η γιγαντιαία ανάπτυξη της διάδοση των δικτύων υπολογιστών τα τελευταία χρόνια απαιτεί την ανάγκη ταξινόμηση τους όχι μόνο με βάση τις εφαρμογές τους αλλά και με βάση τα τεχνικά τους χαρακτηριστικά. Σε γενικές γραμμές μπορούμε να πούμε ότι βάσει της μελέτης της διεθνούς βιβλιογραφίας δεν προκύπτει μια κοινώς αποδεκτή ταξινόμηση στην οποία θα μπορούν να εμπίπτουν όλα τα δίκτυα. Ωστόσο, υπάρχουν δύο χαρακτηριστικά τα οποία είναι κοινά για όλα τα δίκτυα υπολογιστών, και τα οποία μας βοηθάνε στην ταξινόμηση τους. Τα χαρακτηριστικά αυτά είναι η τεχνολογία μετάδοσης και η κλίμακα – γεωγραφική θέση.

1.5.1. Τεχνολογίες Μετάδοσης

Δύο είναι οι τύποι τεχνολογίας μετάδοσης στα δίκτυα υπολογιστών, τα Δίκτυα Εκπομπής και τα Δίκτυα Σημείου προς Σημείου, τα οποία θα δούμε περιληπτικά παρακάτω.

Δίκτυα Εκπομπής

Τα δίκτυα υπολογιστών ανεξάρτητα από το είδος στο οποίο ανήκουν διαθέτουν έναν ή πολλούς δίαυλους προκειμένου να επικοινωνούν μεταξύ τους. Στα δίκτυα εκπομπής τα οποία μελετάμε στην παρούσα παράγραφο χρησιμοποιείται αποκλειστικά ένας δίαυλο επικοινωνίας ο οποίος είναι κοινός για όλους τους υπολογιστές του δικτύου, και διατίθεται για την μεταξύ τους επικοινωνία. Οι υπολογιστές που ανήκουν σε δίκτυα εκπομπής επικοινωνούν με τους υπόλοιπους, στέλνοντας τους μηνύματα και πληροφορίες με την μορφή πακέτων δεδομένων. Πάνω σε κάθε ένα από τα πακέτα δεδομένων υπάρχει ένα πεδίο διεύθυνσης στο

οποίο αναγράφεται ένας κωδικός ο οποίος δηλώνει τον αποστολέα του πακέτου, ούτως ώστε όταν ένα υπολογιστής του δικτύου παραλάβει το πακέτο να είναι σε θέση να ελέγξει τον κωδικό του πεδίου διεύθυνσης για να διαπιστώσει αν το πακέτο απευθύνεται στον ίδιο. Αφού λοιπόν ο υπολογιστής λάβει το πακέτο και διαπιστώσει ότι προοριζόταν για τον ίδιο, το επεξεργάζεται, σε διαφορετική περίπτωση το αγνοεί.

Επίσης στα δίκτυα εκπομπής εκτός από την παραπάνω περίπτωση της επικοινωνίας μεταξύ δύο μόνο υπολογιστών του δικτύου, υπάρχει και η περίπτωση της αποστολής ενός πακέτου δεδομένων από ένα υπολογιστή, σε όλους τους υπόλοιπους. Σε αυτήν την περίπτωση στο πεδίο της διεύθυνσης του προς αποστολή πακέτου χρησιμοποιείται κατάλληλος κωδικός, προκειμένου όλοι οι υπολογιστές - παραλήπτες του συγκεκριμένου δικτύου να έχουν τη δυνατότητα να επεξεργαστούν την ίδια πληροφορία.

Δίκτυα Σημείο προς Σημείο

Στην δεύτερη κατηγορία έχουμε τα δίκτυα σημείου προς σημείο. Στην περίπτωση αυτή υπάρχουν πολλές συνδέσεις, οι οποίες πάντα υφίστανται μεταξύ δύο μόνο υπολογιστών. Κάθε κανάλι επικοινωνίας (π.χ. ένα μισθωμένο κύκλωμα δεδομένων), συνδέεται σε ακριβώς δύο υπολογιστές, και είναι διαθέσιμο αποκλειστικά σε αυτούς τους υπολογιστές. Η μέθοδος αυτή καλείται δίκτυο σημείου προς σημείο ή δίκτυο πλέγματος και έχει τις εξής τρείς χρήσιμες ιδιότητες:

1. Επειδή η κάθε σύνδεση εγκαθίσταται ανεξάρτητα μπορεί να χρησιμοποιηθεί κατάλληλο υλικό. Για παράδειγμα η χωρητικότητα μετάδοσης (δηλαδή το εύρος ζώνης) του υποκείμενου κυκλώματος και τα μόντεμ που χρησιμοποιούνται δεν χρειάζεται να είναι ίδια για όλες τις συνδέσεις.

2. Επειδή οι συνδεδεμένοι υπολογιστές έχουν αποκλειστική πρόσβαση, μπορούν να αποφασίζουν πως ακριβώς θα στέλνουν δεδομένα μέσω της σύνδεσης. Μπορούν να επιλέξουν μια μορφή πλαισίου, έναν μηχανισμό ανίχνευσης σφαλμάτων, και ένα ανώτατο μέγεθος πλαισίου. Το σημαντικότερο, επειδή η κάθε σύνδεση είναι ανεξάρτητη από τις υπόλοιπες, οι λεπτομέρειες αυτές μπορούν να αλλάζουν όποτε οι ιδιοκτήτες των συνδεδεμένων υπολογιστών συμφωνήσουν να κάνουν μια αλλαγή.

3. Επειδή μόνο δύο υπολογιστές έχον πρόσβαση στο κανάλι, είναι εύκολο να εξασφαλιστεί η ασφάλεια και το προσωπικό απόρρητο. Κανένας άλλος υπολογιστής δεν χειρίζεται τα δεδομένα και κανένας άλλος υπολογιστής δεν μπορεί να αποκτήσει πρόσβαση.

Φυσικά αυτό το είδος δικτύων έχει και μειονεκτήματα . Το κύριο μειονέκτημα γίνεται φανερό όταν χρειάζεται να επικοινωνούν μεταξύ τους περισσότεροι από δύο υπολογιστές. Σε ένα δίκτυο σημείου προς σημείο που διαθέτει ένα ξεχωριστό κανάλι επικοινωνίας για το κάθε ζεύγος υπολογιστών, ο αριθμός των συνδέσεων αυξάνεται γρήγορα καθώς αυξάνεται το μέγεθος του συνόλου.

1.5.2. Κλίμακα Δικτύων Υπολογιστών

Όπως αναφέραμε και παραπάνω ένα ακόμη κριτήριο ταξινόμησης των δικτύων είναι η κλίμακά – γεωγραφική θέση τους. Με βάση αυτή την ταξινόμηση έχουμε τις παρακάτω τέσσερις κατηγορίες [9].

Τοπικά Δίκτυα LAN (Local Area Network)

Όπως προκύπτει και από το όνομα τους τα δίκτυα αυτά καλύπτουν ανάγκες διασύνδεσης υπολογιστών οι βρίσκονται σε μικρές γεωγραφικές αποστάσεις. Τα δίκτυα αυτά σχεδιάστηκαν ως εναλλακτική μέθοδος αντί για τις δαπανηρές αποκλειστικές συνδέσεις σημείου προς σημείο και η σχεδίαση τους διαφέρει ριζικά από τα δίκτυα μεγάλων αποστάσεων τα οποία θα μελετήσουμε στην συνέχεια, επειδή βασίζονται στον μερισμό του δικτύου.

Κάθε τοπικό δίκτυο αποτελείται από ένα και μόνο μεριζόμενο μέσο μετάδοσης, συνήθως ένα καλώδιο, στο οποίο συνδέονται πολλοί υπολογιστές. Οι υπολογιστές χρησιμοποιούν ένας-ένας με την σειρά το μέσο για να στέλνουν πακέτα. Επειδή ο μερισμός εξαλείφει την επανάληψη, έχει μια σημαντική οικονομική επίπτωση στην δικτύωση η οποία έγκειται στο ότι μειώνει το κόστος. Για αυτό και οι τεχνολογίες τοπικών δικτύων που επιτρέπουν σε ένα σύνολο υπολογιστών να μοιράζονται ένα μέσο μετάδοσης έχουν γίνει πολύ διαδεδομένες.

Δίκτυα Ευρείας Περιοχής WAN (Wide Area Network)

Τα δίκτυα ευρείας περιοχής επεκτείνονται σε τοποθεσίες που βρίσκονται σε πολλές πόλεις, χώρες ή ηπείρους. Το βασικό σημείο που διαχωρίζει ένα δίκτυο WAN από ένα LAN είναι η προσαρμοστικότητα μεγέθους. Ένα δίκτυο ευρείας περιοχής πρέπει να έχει την δυνατότητα να μεγαλώνει όσο χρειάζεται για να συνδέει πολλές τοποθεσίες που βρίσκονται σε μεγάλες γεωγραφικές αποστάσεις, με κάθε τοποθεσία να έχει υπολογιστές. Για παράδειγμα ένα δίκτυο ευρείας περιοχής θα πρέπει να δίνει την δυνατότητα διασύνδεσης όλων των υπολογιστών μιας μεγάλη εταιρείας με γραφεία ή εργοστάσια σε δεκάδες τόπους, οι οποίοι είναι διάσπαρτοι σε χιλιάδες

τετραγωνικά χιλιόμετρα. Επιπλέον ένα δίκτυο για να μπορεί να θεωρηθεί ως δίκτυο ευρείας περιοχής (WAN) θα πρέπει να είναι σε θέση, να παρέχει την απόδοση που απαιτούν αυτού του είδους τα μεγάλα δίκτυα. Στην πράξη δηλαδή ένα δίκτυο WAN δεν αρκεί να συνδέει απλώς πολλούς υπολογιστές σε πολλές τοποθεσίες – πρέπει να υπάρχει αρκετά μεγάλη χωρητικότητα για αν μπορούν οι υπολογιστές να επικοινωνούν ταυτόχρονα.

Δίκτυα Μητροπολιτικής Περιοχής MAN (Metropolitan Area Network)

Τα δίκτυα μητροπολιτικής περιοχής ή αλλιώς μητροπολιτικά δίκτυα εκτείνονται σε μεγαλύτερη απόσταση από ότι τα τοπικά, και σε μικρότερη από ότι τα δίκτυα ευρείας περιοχής. Για παράδειγμα μητροπολιτικά δίκτυα αποτελούν αυτά τα οποία εκτείνονται σε μια πόλη. Τα μητροπολιτικά δίκτυα χρησιμοποιούνται για να καλύψουν ανάγκες διασύνδεσης υπολογιστών σε μεσαίες αποστάσεις. Μια επιχείρηση για παράδειγμα που διαθέτει υποκαταστήματα σε διαφορετικά σημεία της ίδιας πόλης χρησιμοποιεί μητροπολιτικά δίκτυα. Τέλος αυτού του είδους τα δίκτυα δύναται αν είναι είτε ιδιωτικά είτε δημόσια, ενώ υποστηρίζουν και την μεταφορά πολυμεσικών δεδομένων όπως ήχο, φωνή, εικόνα. Για την επικοινωνία των υπολογιστών αυτών των δικτύων χρησιμοποιούνται ένας ή δύο δίαυλοι επικοινωνίας.

Διαδίκτυο

Το διαδίκτυο έγκειται σε έναν επιμέρους συνδυασμό των παραπάνω μορφών δικτύων που περιγράψαμε. Παρά τις ασυμβατότητες μεταξύ των τεχνολογιών του

διαδικτύου, οι ερευνητές επινόησαν μια μέθοδο για να παρέχεται οικουμενική εξυπηρέτηση μεταξύ ετερογενών δικτύων. Η μέθοδος αυτή λέγεται διαδικτύωση και χρησιμοποιεί υλικό και λογισμικό. Πρόσθετα συστήματα υλικού χρησιμοποιούνται για την αλληλοσύνδεση ενός συνόλου φυσικών δικτύων. Έπειτα λογισμικό, σε όλους τους διασυνδεδεμένους υπολογιστές παρέχει οικουμενική εξυπηρέτηση. Το σύστημα διασυνδεδεμένων φυσικών δικτύων καλείται διαδίκτυο.

Η διαδικτύωση είναι μια πολύ γενική μέθοδος και δεν φέρει περιορισμούς στον αριθμό των φυσικών που θα συνδεθούν μεταξύ τους, ούτε του αριθμού των υπολογιστών που κάθε δίκτυο θα διαθέτει. Για το λόγο αυτό μπορεί να συναντήσουμε διαδίκτυα τα οποία αποτελούν διασύνδεση είτε δεκάδων δικτύων, είτε εκατοντάδων δικτύων, είτε χιλιάδων δικτύων. Όσο αφορά του υπολογιστές που ανήκουν στα διασυνδεδεμένα δίκτυα, ο αριθμός αυτών δύναται αν διαφέρει σημαντικά από διαδίκτυο σε διαδίκτυο, ενώ υπάρχουν και περιπτώσεις δικτύων, τα οποία δεν διαθέτουν κανένα συνδεδεμένο υπολογιστή.

Για την επίτευξη της διαδικτύωσης των επιμέρους φυσικών δικτύων χρησιμοποιούνται από σειρά από τεχνολογίες και συσκευές τηλεπικοινωνιών όπως γέφυρες (bridges), πύλες(gateways), αναδιαμορφωτές(repeaters), δρομολογητές(routers), κλπ.

Κεφάλαιο 2^{ο}

Αδυναμίες Δικτύων Υπολογιστών - Επιθέσεις

2.1. Η Σημαντικότητα της Ασφάλειας

Ένα σύστημα είναι ασφαλές τόσο, όσο οι άνθρωποι που το χρησιμοποιούν. Κανείς δεν νοιάζεται για την ασφάλεια ενός συστήματος που λειτουργεί συνεχώς και έχει τα απαραίτητα backup για να επανέλθει στην κανονική λειτουργία του, αν συμβεί πρόβλημα στο υλικό.

Το πρόβλημα προκύπτει όταν μία λειτουργική ανάγκη (όπως η εμπιστευτικότητα) πρέπει να υλοποιηθεί. Από την στιγμή που θα αρχίσουν η υλοποιήσεις συστημάτων ασφαλείας, δεν υπάρχει ορατό τέλος στην βελτίωση της ασφάλειας. Όποιος δεν έχει προσπέλαση στο σύστημα, θα προσπαθεί να βρει τρωτό σημείο στην ασφάλεια. Επειδή στην συνέχεια θα αναφερθούμε ιδιαίτερα στην τρωτότητα καλό είναι να δώσουμε τον ορισμό τη.

Τρωτό θεωρούμαι ένα αδύναμο σημείο (στην συγκεκριμένη περίπτωση ενός υπολογιστικού συστήματος) το οποίο αξιοποιούν προς όφελος τους αυτοί που ενδιαφέρονται να επινοήσουν ένα τρόπο να εισβάλλουν σε ένα σύστημα, χωρίς φυσικά να έχουν τα απαραίτητα δικαιώματα Όταν λοιπόν κάποιος χρησιμοποιεί ακούσια τα τρωτά σημεία ενός δικτύου ή ενός υπολογιστικού δικτύου τότε κάνουμε

λόγο για περιστατικό παραβίασης της ασφάλειας. Τα τρωτά σημεία οφείλονται κατά κύριο λόγο σε σχεδιαστικά και κατασκευαστικά λάθη.

Στις μέρες μας πλέον είναι εξαιρετικά εύκολο μη εξουσιοδοτημένοι χρήστες να αποκτήσουν πρόσβαση σε δεδομένα, και αυτό συμβαίνει λόγω της τρωτότητας των υπολογιστικών συστημάτων και δικτύων στην οποία αναφερθήκαμε παραπάνω. Υπάρχουν δηλαδή σε πολλά συστήματα χαλαρές δικλείδες ασφαλείας με αποτέλεσμα να πραγματοποιούνται επιθέσεις , οι οποίες τις περισσότερες φορές δεν είναι εύκολο να γίνουν άμεσα αντιληπτές..

Ακόμα και η πιο «αθώα» πληροφορία, όπως τι προγράμματα τρέχουν οι υπολογιστές, τι πρωτόκολλα χρησιμοποιούνται είναι πολύ σημαντικά στοιχεία για τους hackers. Με τη γνώση αυτή μπορούν να δοκιμάσουν γνωστά τρωτά σημεία τους και να αποκτήσουν πρόσβαση σε σημαντικές πληροφορίες.

Το διαδίκτυο είναι ένα μέσο διάδοσης πληροφοριών. Αυτό όμως ισχύει και για τους hackers που μεταδίδουν πληροφορίες για τις αδυναμίες που βρίσκουν σε λειτουργικά συστήματα, πρωτόκολλα και εφαρμογές. Στο διαδίκτυο υπάρχει ένας ανταγωνισμός ταχύτητας, ανάμεσα στο πόσο γρήγορα θα αντιδράσουν οι κατασκευαστές και οι διαχειριστές των υπολογιστικών συστημάτων για να διορθώσουν ένα νέο αδύνατο σημείο στο σύστημα τους, πριν δεχθούν εισβολή και των hackers που θέλουν να εκμεταλλευτούν το αδύνατο σημείο για να εισβάλουν στο σύστημα. Σύμφωνα με στοιχεία του CERT/CC και τα καθημερινά κρούσματα επιθέσεων, κανένας στο διαδίκτυο δεν μπορεί να θεωρηθεί ασφαλής.

Τα αποτελέσματα μίας παραβίασης στην ασφάλεια ενός υπολογιστικού συστήματος ή ενός δικτύου μπορεί να είναι ο χρόνος που χάθηκε για την ανάκτηση της λειτουργικότητας των υπολογιστικών συστημάτων, η οικονομική απώλεια αλλά και η απώλεια αξιοπιστίας, τυχόν ανακύπτοντα νομικά προβλήματα, και πολλά άλλα.

Συνήθως οι περιπτώσεις επίθεσης έχουν σκοπό την επίθεση κατά της αξιοπιστίας, της φήμης και της λειτουργικότητας ίων οργανισμών με αποτέλεσμα την άμεση ή έμμεση χρηματική επιβάρυνση.

Επιθέσεις έχουν παρουσιαστεί και σε sites του Ελληνικού χώρου κύρια σε κρατικούς οργανισμούς με σκοπό την δυσφήμηση τους. Οι πιο γνωστοί από αυτούς του οργανισμού αποτελούν η βιβλιοθήκη του Κογκρέσου στις ΗΠΑ, επιθέσεις στην ΝΑΣΑ, επιθέσεις στην εταιρεία κατασκευής δικτυακού λογισμικού IPSwitch, στο Purdue, το Γεωδυναμικό Ινστιτούτο, την εταιρεία παροχής διασύνδεσης ISP, στις ιστοσελίδες του υπουργείου παιδείας, και σε πολλά άλλα.

Πολλά από τα πρωταρχικά δικτυακά πρωτόκολλα, που τώρα αποτελούν μέρος της υποδομής του διαδικτύου, δεν σχεδιάστηκαν έχοντας κατά νου την ασφάλεια. Χωρίς την απαραίτητη ασφαλή υποδομή, δυσχεραίνεται η άμυνα του δικτύου. Επιπλέον, το διαδίκτυο αποτελεί ένα περιβάλλον με δυναμικό χαρακτήρα, όσο αφορά τις τεχνολογίες κατασκευής του αλλά και την τοπολογία του .

Κατά τα αρχικά στάδια δημιουργίας των IP, σκοπός ήταν η δημιουργία ενός πρωτοκόλλου το οποίο θα μπορούσε να διασύνδεει ετερογενή δίκτυα με τρόπο τέτοιο που ο κάθε ένας υπολογιστής θα είχε μια μοναδική ταυτότητα. Έτσι θα γινόταν ευκολότερη η ανταλλαγή και μετάδοση δεδομένων μεταξύ συγκεκριμένων υπολογιστών και δει παραληπτών. Τα διασυνδεόμενα δίκτυα αρχικά αφορούσαν πανεπιστήμια ή ερευνητικά ιδρύματα και στόχος ήταν η διαπανεπιστημιακή συνεργασία. Για αυτόν το λόγο ουδέποτε τέθηκε θέμα ασφάλειας στο σχεδιασμό του IP. Με μοιραίο τρόπο λοιπόν οι απαραίτητες δικλείδες ασφαλείας δεν υπάρχουν, παρ ότι αναγκαίες. Όταν αργότερα με την τεράστια εξάπλωση του διαδικτύου και τη χρήση του για εμπορικούς σκοπούς εμφανίστηκε το θέμα της ασφάλειας, έπρεπε αναγκαστικά να αντιμετωπιστεί σε ένα υψηλότερο επίπεδο, όπως στο επίπεδο εφαρμογής ή σπανιότερα στο επίπεδο μεταφοράς. Για παράδειγμα το πρωτόκολλο Secure Sockets Layer (SSL) λειτουργεί στο επίπεδο

μεταφοράς, ενώ το πρωτόκολλο Secure HTTP (SHTTP) λειτουργεί στο επίπεδο εφαρμογής.

Εξαιτίας λοιπόν της φύσης του ανοικτού περιβάλλοντος του διαδικτύου αλλά και του τρόπου με τον οποίο αρχικά σχεδιάστηκαν τα πρωτόκολλα, οι επιθέσεις καταστάθηκαν εύκολες, μη όντας δυνατό να ανιχνευτούν έγκαιρα. Ο εισβολέας δεν χρειάζεται να είναι παρών στο site που επιτίθεται, αλλά αντίθετα μπορεί να βρίσκεται οπουδήποτε στον κόσμο και μάλιστα είναι δυνατό να αποκρυφτεί και το σημείο που βρίσκεται.

Μία σημαντική τακτική ή μέθοδος για την ενίσχυση της ασφάλειας στα δίκτυα η οποία έκανες την εμφάνιση της τα τελευταία χρόνια είναι η δημιουργία και χρήση ιδεατών ιδιωτικών δικτύων (VPNs) με χρήση κατάλληλου λογισμικού η υλικού. Ο βασικός άξονας λειτουργίας της μεθόδου αυτής είναι η κωδικοποίηση του πακέτου που πρόκειται να μεταδοθεί και στην συνέχεια η ενσωμάτωσή του σε ένα άλλο καινούργιο πακέτο το οποίο αποστέλλεται στον προορισμό. Παρά το γεγονός της επιτυχίας των μεθόδων ενίσχυσης της ασφάλειας που έχουν προταθεί, σοβαρά προβλήματα εξακολουθούν να υφίστανται.

2.2. Ιστορικό Επιθέσεων σε Δίκτυα

Το πρώτο σημαντικό περιστατικό ασφάλειας παρουσιάστηκε στο διαδίκτυο το 1988. Ονομάστηκε Morris worm [16], από το όνομα του φοιτητή του Cornell University, Robert Morris, που έγραψε ένα πρόγραμμα που μπορούσε να συνδεθεί σε έναν άλλο υπολογιστή, να αντιγραφεί σε αυτόν και να αρχίσει να κάνει το ίδιο με τον επόμενο υπολογιστή στο δίκτυο. Αυτό το αυτόματα αναπαραγόμενο πρόγραμμα προκάλεσε μία γεωμετρική έκρηξη επιθέσεων στο διαδίκτυο.

Το πρόγραμμα χρησιμοποιούσε τόσους πολλούς πόρους από το σύστημα που βρισκόταν, ώστε τελικά έπαυε να είναι λειτουργικό. Το αποτέλεσμα ήταν το 10% των υπολογιστών που ήταν συνδεμένοι στο ARPANET (σε σύνολο 88,000) να σταματήσουν την λειτουργία τους την ίδια ώρα. Το δίκτυο που θα μπορούσε να ήταν το μέσο που θα Βοηθούσε στην επίλυση του προβλήματος, είχε πάψει να είναι λειτουργικό. Επιπλέον οι διαχειριστές πολλών sites από φόβο μήπως «μολυνθούν» τα συστήματα τους, σταματούσαν την επικοινωνία τους με το δίκτυο για να αντιμετωπίσουν την κατάσταση, με αποτέλεσμα να γίνονται περισσότεροι οι κόμβοι που δεν ήταν συνδεμένοι.

Ήταν τόσο μεγάλη η αίσθηση που προκάλεσε το Morris worm, που το Υπουργείο Άμυνας αποφάσισε την χρηματοδότηση μίας ομάδας άμεσης αντίδρασης σε προβλήματα ασφάλειας, που τώρα ονομάζεται CERT Coordination Center. Το CERT/CC πρόκειται για ένα καλά οργανωμένο ινστιτούτο ασφάλειας στο διαδίκτυο που παρέχει ενημέρωση, τεχνική υποστήριξη και κάλυψη γενικότερα σε χρήστες του διαδικτύου. Διαθέτει βάσεις δεδομένων με τα περισσότερα περιστατικά επιθέσεων στο διαδίκτυο, ομάδες εκπαίδευσης και ανάπτυξης λογισμικού και γενικότερα τεχνικών θωράκισης του διαδικτύου και των δικτύων γενικότερα.

Υπάρχουν και άλλοι οργανισμοί και ινστιτούτα όπως το CERT/CC, μικρότερης όμως εμβέλειας. Στο σύνολο τους αποτελούν το FIRST (Forum of Incident Response and Security Teams), μια μορφή κοινότητας που παρακολουθεί και επινοεί τρόπους άμυνας απέναντι σε επιθέσεις στο διαδίκτυο. Το FIRST αριθμούσε το 1996, τα 57 μέλη με δράση στον κυβερνητικό, εμπορικό και ακαδημαϊκό τομέα και με σημαντική συμβολή στην ασφάλεια του διαδικτύου.

Από την πρώτη σημαντική εμφάνιση μαζικής επίθεσης, μέχρι σήμερα η ίδια η εξέλιξη του internet είναι τέτοια που το έχει κάνει ένα μέσο διακίνησης τεράστιων ποσοτήτων πληροφορίας σχετικές με τα τρωτά του. Έχει καταφέρει να ενώσει ανθρώπους σε ομάδες που δεν γνωρίζονται προσωπικά, αλλά έχουν κοινά

ενδιαφέροντα και επιδιώξεις. Η διακίνηση της πληροφορίας είναι ελεύθερη και φτάνει ταχύτατα σε κάθε σημείο του πλανήτη. Οι νέοι μαθαίνουν από τους γνώστες νέους τρόπους επιθέσεων, τροφοδοτούνται με εργαλεία, εκπαιδεύονται σε μεθόδους, γίνονται έμπειροι στην ανακάλυψη νέων τρωτών σημείων και όλοι μαζί προσπαθούν να γίνουν γνωστοί στην ομάδα κρυμμένοι πίσω από το ψευδώνυμο τους κάνοντας όμως αισθητή την παρουσία τους στον κόσμο.

Είναι δύσκολο να χαρακτηρίσεις τους ανθρώπους που προκαλούν περιστατικά παραβίασης ασφάλειας. Ένας εισβολέας μπορεί να είναι ένας έφηβος που αναρωτιέται τι μπορεί να κάνει στο διαδίκτυο, ή ένας φοιτητής που κατασκεύασε ένα νέο εργαλείο ή υλοποίησε μία ιδέα που είχε σε ένα πρόγραμμα, ή κάποιος που προσπαθεί να έχει ίδιο όφελος ή ένας πληρωμένος κατάσκοπος που προσπαθεί να κλέψει πληροφορίες για ανταγωνιστές από εταιρίες ακόμα και από κράτη. Μπορεί ακόμα να είναι ένας απολυμένος ή δυσαρεστημένος υπάλληλος. Μπορεί να το κάνει για την διασκέδαση, τον διανοητικό ανταγωνισμό, την αίσθηση της ισχύος, την πολιτική παρουσία ή το χρηματικό όφελος.

Για τον έλεγχο της τρωτότητας σε συστήματα, έχουν γίνει πολλές προσπάθειες οι περισσότερες με χρηματοδότηση του υπουργείου άμυνας των ΗΠΑ, με στόχο κόμβους στρατιωτικών υπηρεσιών και υπηρεσιών ασφάλειας. Σε μια τέτοια έρευνα επιστήμονες της DISA (Defense Information Systems Agency) έκαναν επιθέσεις σε υπολογιστές στρατιωτικών υπηρεσιών στο διάστημα από το 1992 ως το 1995. Σύμφωνα με τα αποτελέσματα της έρευνας πραγματοποιήθηκαν 38. 000 επιθέσεις από τις οποίες οι 13.300 αποκρούστηκαν, οι 27.400 ήταν επιτυχείς, οι 988 ανακαλύφθηκαν, οι 23.712 πέρασαν απαρατήρητες [17].

Σύμφωνα με εκτιμήσεις της DISA τα συστήματα του Υπουργείου Άμυνας, πρέπει να έχουν δεχθεί 250,000 επιθέσεις από το 1992- 1995 [19]. Υποθέτοντας πως τα

συστήματα αυτά αποτελούν το 10% του συνόλου του διαδικτύου εκτιμούν πως 2.5 εκατομμύρια επιθέσεις έγιναν στο διαδίκτυο μόνο το διάστημα 1992-1995. Επίσης συμπεράνουν πως 1 στις 140 επιθέσεις ανακοινώνονται.

2.3. Είδη Επιθέσεων

Επιθέσεις σε Ιστοσελίδες

Οι ιστοσελίδες του διαδικτύου αποτελούσαν πάντα τον εύκολο στόχο για επιθέσεις από hackers. Αυτό συνέβαινε γιατί οι δικλείδες ασφαλείας που είχαν και έχουν δεν ήταν πάντα αρκετά ικανοποιητικές ώστε να απωθήσουν τέτοιου είδους εισβολές. Η επίθεση σε αυτή την περίπτωση πραγματοποιείται αλλάζοντας το λινκ της κεντρικής σελίδας και ορίζοντας το να δείχνει σε κάποια άλλη κακόβουλη τοποθεσία. Δεν είναι λίγες οι περιπτώσεις που οργανισμοί έχουν δει την φήμη τους να πληγώνεται από τέτοιες επιθέσεις. Μεγάλες εταιρίες, κυβερνητικοί οργανισμοί, στρατιωτικά προγράμματα είναι οι κύριοι στόχοι.

Επίθεση στην υπηρεσία ονοματολογίας (DNS)

Ένας άλλος τρόπος για να τροποποιηθούν σι ιστοσελίδες ενός site που βλέπουν οι χρήστες είναι να αλλάξει η IP διεύθυνση που υποτίθεται πως έχει από την υπηρεσία ονοματολογίας (Domain Name Service) ο κόμβος. Για παράδειγμα αν η IP διεύθυνση του κόμβου www.victim.com μεταφραζόταν σε 13.42.111.33, η επίθεση θα είχε ωα αποτέλεσμα την αλλαγή των κατάλληλων στοιχείων της βάσης δεδομένων του DomainNameServer και η σελίδα να παραπέμπει σε μια άλλη ιστοσελίδα, κακόβουλη, όπως π.χ. πορνογραφικού περιεχομένου. Ο Eugene

Kashpureff, στέλεχος της AlterNIC, άλλαξε τα στοιχεία της βάσης δεδομένων που κρατά τα Domain Names και τις IP διευθύνσεις, έτσι ώστε όσοι προσπαθούσαν να πάνε στην σελίδα του InterNIC, οδηγούνταν στις σελίδες του AlterNIC. Από εκεί οι χρήστες μπορούσαν με ένα κλικ να πάνε στην πραγματική σελίδα [18]. Η επίθεση έγινε ένα Σαββατοκύριακο του Ιουλίου του 1997, σαν διαμαρτυρία για το μονοπώλιο που πέτυχε το InterNIC για την διαχείριση του DNS πρώτου επιπέδου για τους δημοφιλείς κόμβους .com, .org, .net αποφέροντάς του έτσι κέρδη των $78 εκατομμυρίων. Ο Kashpureff τελικά συνελήφθη στον Καναδά με ένταλμα του FBI και δικάστηκε σε 2 χρόνια επιτήρηση και $100 (εκατό δολάρια) πρόστιμο μετά από συμφωνία με την Network Solutions που είχε την διαχείριση του InterNIC και την δημόσια συγγνώμη του.

Επίθεση με Δουρείους Ίππους

Οι Δούρειοι Ίπποι (trojan horses) αποτελούν κακόβουκα προγράμματα τα οποία προσποιούνται ότι διαθέτουν διαφορετικές λειτουργίες από αυτές που πραγματικά έχουν –από εκεί άλλωστε προκύπτει και το όνομα τους. Συνήθως αποτελούν μέρος άλλων προγραμμάτων, αλλά είναι δυνατό να δρούν και μεμονωμένα.

Επίθεση με «σκουλήκια»

Τα «σκουλήκια» (worms) είναι προγράμματα που δρουν αυτόνομα και «σέρνονται» (έτσι προκύπτει το όνομα «σκουλήκι») από site σε site εκμεταλλευόμενα τρύπες του συστήματος. Σε κάθε ιστοσελίδα τα σκουλήκια δρούν αυτόνομα και χωρίς την χρήση ή την ενσωμάτωση τους σε άλλα προγράμματα. Το πιο «διάσημο» σκουλήκι όλων των εποχών ήταν το Internet Worm, το οποίο το 1988, μπόρεσε να διασπάσει το Διαδίκτυο στην Αμερική, προκαλώντας αντιδράσεις πανικού σε όλο τον κόσμο.

Επίθεση με Ιούς

Οι Ιοί αποτελούν τα πιο γνωστά μέσα επίθεσης στην ασφάλεια του διαδικτύου. Οι τεχνικές που χρησιμοποιούν είναι ως επι το πλείστον πονηρές και δόλιες. Σκοπός τους είναι να εγκατασταθούν σε υπολογιστικά συστήματα χωρίς φυσικά την συγκατάβαση του ιδιοκτήτη και να πλήξουν την ακεραιότητα του συστήματος. Οι τρόποι που χρησιμοποιούν για να το πετύχουν είναι άλλες φορέα ανώδυνοι, αλλα στις περισσότερες περιπτώσεις είναι επώδυνοι αφού προκαλούν απώλεια δεδομένων, ή οδηγούν το όλο σύστημα σε διαμόρφωση.

Επίθεση με «Ανιχνευτές»

Οι ανιχνευτές δικτυακής κίνησης συνήθως αποτελούν προγράμματα τα οποία χρησιμοποιούνται προκειμένου να επιτευχθεί ο έλεγχος της ασφάλειας των υπολογιστικών συστημάτων. Το όνομα τους προκύπτει από το γεγονός ότι έχουν γνώση για όλα τα πιθανά εξωτερικά σημεία τα οποία θα μπορούσε να εκμεταλλευτεί ένας hacker προκειμένου να πλήξει την ασφάλεια του συστήματος. Παρότι λοιπόν αρχικά η δημιουργία τους συντελέστηκε για καλό σκοπό, αργότερα ο τρόπος λειτουργίας τους έγινε αντικείμενο εκμετάλλευσης από τους επίδοξους hacker. Τέτοιου είδους προγράμματα είναι το ISS, το TCPdump, το Nmap, το SATAN αλλά και πολλά άλλα. Το ποσοστό της χρήσης τους είναι 14.3% του συνολικού των εργαλείων.

Επίθεση στο πρωτόκολλο TFTP

Το πρωτόκολλο TFTP (Trivial File Transfer Protocol) σχεδιάστηκε εξαρχής για την άνευ δίσκου εκκίνηση «πελατών». Παρ' όλα αυτά, δεν δόθηκε η απαραίτητη προσοχή στα σημεία πρόσβασης συγκεκριμένων καταλόγων του συστήματος, κάτι

το οποίο είχε ως αποτέλεσμα κάποιος να είναι σε θέση αντιγράψει κι άλλα αρχεία, όπως για παράδειγμα, το αρχείο κωδικών πρόσβασης.

Επίθεση σιη Δικτυακή Υπηρεσία Πληροφοριών (NIS)

Πρόκειται για την υλοποίηση της Sun Microsystems «Κίτρινων Σελίδων» (Yellow Pages) για κατανεμημένη διαχείριση δικτυακών πληροφοριών (όπως αρχεία κωδικών πρόσβασης, χάρτες του δικτύου κλπ.). Παρ' όλα αυτά, αυτές οι πληροφορίες διέρχονταν πάνω από το δίκτυο και έτσι ο οποιοσδήποτε ήταν σε θέση να τα παρακολουθήσει και να τα υποκλέψει. Το NIS (Network Information Service) στην συνέχει αντικαταστάθηκε από το NIS+ (από την Sun Microsystems και πάλι) το οποίο πλέον έκανε χρήση κρυπτογραφικών μεθόδων για την εκτέλεση της ασφαλούς μεταφοράς ευαίσθητων πληροφοριών.

Επίθεση στο πρωτόκολλο μεταφοράς αρχείων (FTP)

Το FTP είναι το πρωτόκολλο ασφαλούς μεταφοράς αρχείων μέσω του διαδικτύου όπως προκύπτει και από το όνομα του (File Transfer Protocol). Μέσω αυτού του πρωτόκολλου μεταφοράς αρχείων και συναμα μιας λανθασμένης διαμόρφωσης ο οποιοσδήποτε είναι σε θέση να υποκλέψει αρχεία ενός υπολογιστικού συστήματος.

Επίθεση στο Σύστημα Δικτυακής Αρχειοθέτησης (NFS)

Το NFS (Network File System) είναι ένα σύστημα δικτυακής αρχειοθέτησης και αποτέλεσε πρωτοποριακή υλοποίηση από την Sun Microsystems. Ωστόσο, κάνοντας χρήση λάθος διαμόρφωσης, μπορεί να «μοιράσει» τα δικτυακώς

αποθηκευμένα αρχεία σε κακόβουλους χρήστες που δεν έχουν την απαραίτητη εξουσιοδότηση.

Επίθεση στο πρωτόκολλο ηλεκτρονικού ταχυδρομείου (SMTP)

Το πρωτόκολλο SMTP (Simple Mail Transfer Protocol) πρόκειται για το TCP/IP πρωτόκολλο επικοινωνίας των MTA (Mail Transfer Agents) της υπηρεσίας του ηλεκτρονικού ταχυδρομείου. Το κυριότερο πρόγραμμα που χρησιμοποιείται και αποτελεί πηγή του προβλήματος (10.4%) είναι το sendmail (σε Berkeley UNIX συστήματα). Πιο πρόσφατα, νέα προγράμματα με μεγαλύτερη ασφάλεια έχουν εμφανιστεί, τόσο για πλατφόρμες UNIX (π.χ. qmail) όσο και για πλατφόρμες Windows (Exchange Server).

Επίθεση στο ηλεκτρονικό ταχυδρομείο

Πρόκειται για ένα ακόμα είδος πολύ συχνά εμφανιζόμενων επιθέσεων, τα οποία ανακύπτουν λόγω της προβληματικής και ελλιπούς χρήσης του SMTP. Τέτοια είναι το mail spoofing (απόκρυψη αποστολέα ή αλλαγή διεύθυνσής του), mail bombs (μεγάλος όγκος μηνυμάτων σε συγκεκριμένο παραλήπτη), binmail, mailrace, mail abuse. Ένα πιο σύγχρονο δε είδος επίθεσης σε λογαριασμούς ηλεκτρονικού ταχυδρομείου είναι το πολύ γνωστό σε όλους μας spamming, δηλαδή η μαζική μηνυμάτων ηλεκτρονικού ταχυδρομείου με περιεχόμενο ακατάλληλο ή ασήμαντος.

Επίθεση με «έμπιστους υπολογιστές»

Το πρόβλημα της επίθεση με έμπιστους υπολογιστές αρχικά παρουσιάζεται σε υπολογιστικά συστήματα με λογισμικό UNIX. Ο όρος των «έμπιστων υπολογιστών» (trusted hosts) έγκειται στη διευκόλυνση των χρηστών οι οποίοι διατηρούσαν πολλούς λογαριασμούς σε διαφορετικά υπολογιστικά συστήματα και έπρεπε να έχουν άμεση πρόσβαση δίχως την καθυστέρηση για ταυτοποίηση μέσω κωδικών πρόσβασης.

Επίθεση από εύρεση των κωδικών πρόσβασης

Η αδυναμία και ευαισθησία των κωδικών πρόσβασης αποτελεί την πιο συχνή μορφή επίθεσης σε ασφάλεια από όλες όσες μελετήσαμε μέχρι τώρα. Η αποκάλυψη του κωδικού πρόσβασης ενός χρήστη σε τρίτους είναι δυνατό να πραγματοποιηθεί με πολλούς και διάφορους τρόπους οι πιο γνωστοί από τους οποίους είναι οι παρακάτω:

1. Αρχικά αντιγραφή του αρχείου διατήρησης κωδικού και στην συνέχεια επεξεργασία αυτού,

2. «Σπάσιμο» του κωδικού πρόσβασης (password cracking) κάνοντας χρήση ειδικών προγραμμάτων τα οποία προσπαθούν να μαντέψουν τους κωδικούς χρησιμοποιώντας σύνηθες λέξεις,

3. «Αδύνατοι κωδικοί» (weak passwords). Εδώ έχουμε τους κωδικούς τους οποίους κάποιος μπορεί να βρει με ευκολία, δεδομένου ότι γνωρίζει το άτομο στο οποίο ανήκει ο λογαριασμός (χρήση του ονόματος, διεύθυνσης, τηλεφώνου κλπ.).

Επίθεση με «σπαστήρια» κωδικών

Τα «σπαστήρια κωδικών» (password cracks) είναι προγράμματα τα οποία με είσοδο ένα αρχείο κωδικών πρόσβασης (password file) και με χρήση ενός λεξικού συνηθισμένων λέξεων που χρησιμοποιούνται για κωδικοί, προσπαθούν να ανακαλύψουν όσο το δυνατό περισσότερους κωδικούς για πρόσβαση σε κάποιο σύστημα. Ενδεικτικά εδώ μπορούμε να πούμε σε ένα υπολογιστικό σύστημα με λειτουργικό Unix το οποίο έχει 1000 περίπου χρήστες, και με την προϋπόθεση ότι οι χρήστες του συστήματος δεν είναι εκπαιδευμένοι στο να επιλέγουν δύσκολους κωδικούς, ένα «σπαστήρι» κωδικών είναι σε θέση να προσπελάσει με ευκολία ένα ποσοστό 40% των συνολικών κωδικών.

Επίθεση με «ωτακουστές»

Οι «Ωτακουστές» πακέτων (packet sniffers) αποτελούν ειδικά προγράμματα τα οποία δύναται να παρακολουθούν την κίνηση μέσα σε ένα δίκτυο σε επίπεδο IP πακέτων. Με τις τεχνικές που αναπτύσσουν τους δίνεται η δυνατότητα να διαφοροποιούν τα μηνύματα που λαμβάνουν αλλά ταυτόχρονα να κάνουν αναγνώριση των πρωτοκόλλων που περνούν διαμέσω του δικτύου. Οι packet sniffers χρησιμοποιούνται για επιθέσεις συνήθως σε τοπικά δίκτυα και σπάνε κωδικούς πρόσβασης, μέσω παρακολούθησης της πληκτρολόγησης του ατόμου από εκάστοτε συγκεκριμένους σταθμούς εργασίας.

Με του ειδικούς μηχανισμούς που διαθέτουν διαφοροποιούν τα πακέτα μηνυμάτων τα οποία τις περισσότερες φορές περιέχουν χρήσιμη πληροφορία δίχως ωστόσο να επηρεάζουν το περιεχόμενο τους.

Από την άλλη βέβαια η χρήση των ωτακουστών μπορεί να έχει και θετικά αποτελέσματα για την διαχείριση δικτύου και υπολογιστικών συστημάτων, όμως και σε αυτήν την περίπτωση είναι σημαντικό τέτοιες τεχνολογίες να μην χρησιμοποιούντα με κακόβουλο τρόπο. Η χρήση ενός ωτακουστή τις περισσότερες φορές απαιτεί προνόμια διαχειριστή , αν και σήμερα, ο καθένας είναι

«διαχειριστής» του προσωπικού του συστήματος και μάλιστα με σύνδεση στο διαδίκτυο. Για τον λόγο αυτό. η ασφάλεια από τα sniffers θα πρέπει να εξασφαλίζεται στο επίπεδο παρόχου υπηρεσιών δικτύου (ISP).

Επίθεση με πλαστογράφηση της IP διεύθυνσης

Η τεχνική της πλαστογράφησης της IP διεύθυνσης στηρίζεται στη δυνατότητα που δύναται να έχει ένας κόμβος και να ισχυρίζεται πως έχει την IP διεύθυνση ενός άλλου. Από την στιγμή που πληθώρα συστημάτων καθορίζουν ποια είναι τα πακέτα τα οποία επιτρέπονται και ποια όχι να εισέλθουν σε ένα δίκτυο ανάλογα με την IP διεύθυνση του αποστολέα, αυτό αποτελεί μία χρήσιμη τεχνική στα χέρια ενός hacker. Έτσι είναι εφικτό να διασφαλιστεί η προσπέλαση σε υπηρεσίες που επιτρέπονται σε κόμβους με συγκεκριμένες IP διευθύνσεις. Επίσης μπορεί να σταλεί από ένα εξωτερικό δίκτυο ένα πακέτο δεδομένων που να φαίνεται πως έχει σταλεί από εσωτερικό κόμβο ενός προφυλαγμένου δικτύου, δίνοντας έτσι την δυνατότητα να εκτελεστούν εντολές, που επιτρέπονται να εκτελεστούν μόνο από εσωτερικούς κόμβους.

Η πλαστογράφηση της IP διεύθυνσης αποτελεί μια σημαντική τεχνική επίθεσης σε δικτυωμένους υπολογιστές. Για να αποκτήσουν πρόσβαση, οι hackers δημιουργούν πακέτα με πλαστές IP διευθύνσεις. Αυτό εκμεταλλεύεται τις εφαρμογές που χρησιμοποιούν ταυτοποίηση (authentication) που βασίζεται στην IP διεύθυνση του αποστολέα και μπορεί να οδηγήσει ακόμα και στην απόκτηση πρόσβασης διαχειριστή στο σύστημα στόχο (για παράδειγμα στις περιπτώσεις χρήσης του /etc/hosts.equiv ή .rhosts). Οι επιθέσεις αυτές μπορούν να εμποδιστούν μέσω τείχων προστασίας τα οποία τσεκάρουν τις διευθύνσεις IP προτού μπουν στο τοπικό, έμπιστο (trusted) δίκτυο.

Οι επιθέσεις με πλαστογράφηση IP διεύθυνσης είναι σε γενικές γραμμές δύσκολο να εντοπιστεί, αφού η πρώτη εντύπωση είναι ότι η επίθεση έχει προέλθει από την πλαστή διεύθυνση. Η επαλήθευση τις περισσότερες φορές καθυστερεί και αυτή η καθυστέρηση επιτρέπει στον hacker να δρα ανενόχλητος για κάποιο διάστημα.

Επίθεση με «πειρατεία» IP σύνδεσης

Πρόκειται για μία σύνθετη επίθεση η οποία περιγράφηκε για πρώτη φορά από τον Steve Bellovin. Με αυτό το είδος της επίθεσης ένας hacker είναι σε θέση να καταλάβει την σύνδεση ενός χρήστη με έναν εξυπηρετητή (γνωστή και σαν man in the middle) και να εκτελεί εντολές που έχει δικαίωμα ο χρήστης. Επιπλέον μπορεί να βλέπει χι γράφει ο χρήστης. Για παράδειγμα αν ο χρήστης γράφει ένα mail τότε ο hacker μπορεί να διαβάσει το mail του, ενώ αν στέλνει στοιχεία της πιστωτικής του κάρτας μπορεί να τα δει.

Αρχική Αντιμετώπιση: Με την δημιουργία κωδικοποιημένης σύνδεσης του χρήστη με τον εξυπηρετητή, μπορούμε να εμποδίσουμε το διάβασμα των στοιχείων, δεδομένων ή εντολών καθώς και την χρήση της σύνδεσης από τον hacker που μη έχοντας το κλειδί κρυπτογράφησης του χρήστη βλέπει μόνο «σκουπίδια».

Επίθεση με παραποίηση IP διεύθυνσης

Αυτό το είδος επίθεσης εμφανίστηκε για πρώτη φορά το 1998. Βασίζεται στην τεχνική του IP spoofing την οποία περιγράψαμε παραπάνω, αφού εκμεταλλεύεται αδυναμίες της υλοποίησης των IP και ICMP (Internet Control Message Protocol) πρωτοκόλλων σε δικτυακές συσκευές.

Το smurf είναι ένα ειδικό πρόγραμμα, το οποίο προσποιείται ότι στέλνει πακέτα από άσχετο αποστολέα (εδώ χρησιμοποιούνται οι τεχνικές του IP spoofing). Τα

πακέτα αυτά είναι του πρωτοκόλλου ICMP, το οποίο και χρησιμοποιείται από βασικές λειτουργίες του δικτύου (π.χ. τις υπηρεσίες ping και traceroute). Στέλνοντας ένα ping πακέτο στην διεύθυνση εκπομπής (broadcast address) ενός δικτύου, ο αποστολέας δέχεται απάντηση από κάθε έναν από τους κόμβους που δέχθηκαν το ICMP ping πακέτο (δηλαδή όλους του κόμβους του δικτύου).

Αν και το ping πακέτο δεν είναι μεγάλο σε μέγεθος, εντούτοις ο παράγοντας της ενίσχυση είναι ίσος με τον αριθμό των μηχανημάτων. Σε ένα μεγάλο B-class δίκτυο όπου λ.χ. χρησιμοποιείται το ένα τέταρτο του πεδίου διευθύνσεων, η απάντηση είναι ίση με περίπου 16.000 πακέτα. Είναι προφανές ότι με μερικές εκατοντάδες πακέτα ping μπορούν να κάνουν άχρηστο το δίκτυο, δημιουργώντας μία κατάσταση άρνησης εξυπηρέτησης (Denial-of- Service).

Επίθεση με υπερχείλιση προσωρινής μνήμης

Οι μέθοδοι επίθεσης όπως είδαμε είναι πολλές και διάφοροι, άλλες πιο πολύπλοκες και άλλες πιο απλές. Η παρούσα μέθοδος είναι αρκετά ιδιαίτερη γιατί σε αυτή την περίπτωση οι hackers εισβάλουν σε υπολογιστικά συστήματα, χωρίς να εισάγουν τα αντίστοιχα στοιχεία σύνδεσης. Η εισβολή γίνεται ωστόσο με την χρήση ενός προγράμματος το οποίο ήδη εκτελείται στον υπολογιστή και μέσω αυτού οι hackers εκτελούν εντολές του συστήματος.

Προκειμένου να γίνει αυτό εφικτό κατασκευάζουν ένα μεγάλο κομμάτι χαρακτήρες το οποίο περιέχει τις εντολές που όπως προαναφέραμε θέλουν να εκτελέσουν. Το κομμάτι αυτό χρησιμοποιείται ως παράμετρος εισόδου στο πρόγραμμα. Σε κανονικές συνθήκες το πρόγραμμα που διαθέτει ο υπολογιστής δεν τρέχει τον κώδικα ο οποίος περνιέται σαν παράμετρος. Εάν ωστόσο το μήκος (length) του κειμένου (σειρά χαρακτήρων) της παραμέτρου ξεπερνά το μήκος το οποίο έχει δοθεί σαν διαθέσιμος χώρος για το πέρασμα της παραμέτρου, τότε ένα τμήμα

αυτού περνά στον χώρο του εκτελέσιμου προγράμματος και εκτελείται (Buffer overflow). Από όλη την διαδικασία προκύπτει και το όνομα της μεθόδου.

Επίθεση μέσω άρνησης παροχής υπηρεσιών (DoS)

Οι επιθέσεις μέσω άρνησης παροχής υπηρεσιών θεωρούνται από τις πιο μοχθηρές, και για το λόγο αυτό υπάρχει μεγάλη δυσκολία στην αντιμετώπιση τους. Η έννοια μοχθηρές αναφέρεται στο γεγονός ότι δύσκολα έως καθόλου γίνονται αντιληπτές.

Η μεθοδολογία αυτού του είδους της επίθεσης είναι απλή και περιγράφεται παρακάτω: αν σταλούν στον server ενός δικτύου, αιτήσεις περισσότερες σε μέγεθος από όσες δύναται σε κανονικές συνθήκες να εξυπηρετήσει, τότε οι λειτουργίες που ορίζουν και συνεπώς επιβάλλουν οι αιτήσεις αυτές, χρησιμοποιούν πόρους του υπολογιστικού συστήματος. Αυτό έχει ως αποτέλεσμα, μετά την παρέλευση κάποιου χρονικού διαστήματος, ο server να μην μπορεί να εξυπηρετήσει τους πελάτες του λόγω έλλειψης πόρων για την εκτέλεση των διεργασιών αυτών. [13]

Κατανεμημένη επίθεση άρνησης παροχής υπηρεσιών (DDoS)

Πρόκειται για μια μεθοδολογία παρόμοια με αυτή που αναπτύξαμε παραπάνω. Ωστόσο η διαφορά τους εντοπίζεται στην συνδυασμένη προσπάθεια προσβολής σε ένα κόμβο από πολλούς διαφορετικούς επιτιθέμενους. Η κατανεμημένη επίθεση

άρνησης παροχής υπηρεσιών έχει ως στόχο να ξεγελάσει τα υπολογιστικά συστήματα τα οποία παρακολουθούν το δίκτυο για επιθέσεις. Τα εργαλεία που χρησιμοποιούνται είναι εξειδικευμένα και έχουν αποδείξει πως τα Intrusion Detection Systems δεν τα καταφέρνουν καλά σε αυτές τις επιθέσεις. Χαρακτηριστικά παραδείγματα τέτοιων επιθέσεων αποτελούν οι επιθέσεις στο Yahoo, e-Bay, Amazon, e-Trade οι οποίες πραγματοποιήθηκα το 2000.

Επίθεση με «μοχθηρό κώδικα» (Malicious Code)

Ο μοχθηρός κώδικας αναφέρεται σε ένα σύνολο από εντολές οι οποίες φαίνεται ότι πραγματοποιούνται από χρήστες του δικτύου, όμως στην πράξη σκοπό έχουν να συλλέξουν και να εκμεταλλευτούν ευαίσθητα δεδομένα όπως είναι για παράδειγμα οι κωδικοί πρόσβασης. Στην κατηγορία αυτή των επιθέσεων εντάσσονται οι προσπάθειες για σύνδεση μέσω του προγράμματος login, μέσω συνδέσεων http και telnet.

Επίθεση με εκμετάλλευση κοινωνικών σχέσεων

Αυτοί οι οποίοι πραγματοποιούν τις επιθέσεις ψάχνουν να βρουν εκείνα τα στοιχεία τα οποία θα τους δώσουν την δυνατότητα να εισβάλουν σε ένα υπολογιστικό σύστημα κάνοντας χρήση κοινωνικών σχέσεων και αναπαριστόντας πως είναι κάποιοι άλλοι. Αυτό το είδος της αναζήτησης πληροφοριών μπορεί να γίνει σε μεγάλους οργανισμούς που οι υπάλληλοι δεν γνωρίζονται μεταξύ τους. Για παράδειγμα μπορούν να παραστήσουν πως είναι νέοι τεχνικοί ή σύμβουλοι ασφάλειας που χρειάζονται ένα password για να φτιάξουν κάτι. Υπολογίζεται πως το 20% των εισβολών προέρχεται από πληροφορίες από social engineering36.

Σε μία περίπτωση έχει αναφερθεί πως ο hacker κατάφερε να πάρει πληροφορίες και Passwords, μοιράζονται leaflets σε μία εταιρία για την αλλαγή του τηλεφώνου του help desk. Μόνο που το τηλέφωνο ήταν του σπιτιού του.

2.4. Υποκλοπή Προσωπικών Δεδομένων

Υποκλοπή προσωπικών δεδομένων στο διαδίκτυο αποτελεί η διαδικασία της εξαπάτησης ενός χρήστη με σκοπό να δώσει τις προσωπικές του πληροφορίες σε έναν «πλαστό» διαδικτυακό τόπο όπως είναι η διεύθυνση του, ο αριθμό ταυτότητας του, οι αριθμοί τραπεζικών λογαριασμών κ.α..μια τέτοια δραστηριότητα επιτρέπει σε έναν απατεώνα να υποκλέψει ή ακόμα και να πλαστογραφήσει τα στοιχεία ενός χρήστη προκειμένου να κερδίσει παράνομη πρόσβαση στα δεδομένα του, όπως προσωπικούς λογαριασμούς, συνδρομές, e-mail, κωδικούς ασφαλείας, κ.λπ [4]. Σε αυτήν την κατηγορία μπορούμε να εντάξουμε και τις Απάτες (Scams), αν και συνήθως αυτοί που τις επιδιώκουν δεν ενδιαφέρονται για τις προσωπικές πληροφορίες των χρηστών όπως αυτές που αναφέραμε παραπάνω, αλλά προσπαθούν να προκαλέσουν τον οίκτο για τον ανθρώπινο πόνο ώστε να κάνουν τους χρήστες να προσφέρουν χρήματα για να συνδράμουν σε ένα δήθεν καλό σκοπό. Ενδεικτικό παράδειγμα εδώ είναι το γεγονός ότι σχεδόν σε κάθε μεγάλη καταστροφή όπως σεισμός, πλημμύρες, πείνα, πόλεμος, έχουν προκαλέσει πολυάριθμες ηλεκτρονικές απάτες, μηνύματα σε ιστοσελίδες που ζητούν από τους χρήστες τους να προσφέρουν χρηματικά ποσά προκειμένου να βοηθήσουν για κάποιο καλό σκοπό. Όλα τα παραπάνω παραβιάζουν την ιδιωτική ζωή των χρηστώ του διαδικτύου και επίσης εκμεταλλεύονται δεδομένα που έχουν υποκλαπεί όπως συνθηματικά ή στοιχεία από πιστωτικές κάρτες για εμπορικό κέρδος ή δολιοφθορά.

Η υποκλοπή προσωπικών δεδομένων μπορεί να πραγματοποιηθεί μέσω ηλεκτρονικών μηνυμάτων (e-mail) που εξαπατούν έναν χρήστη ώστε να στην συνέχεια να επισκεφτεί πλαστές ιστοσελίδες, ή κατά την διάρκεια του φυλλομετρήματος οποιασδήποτε ηλεκτρονικής ιστοσελίδας, η οποία είναι

μολυσμένη από ίο. Ακόμα μέσω της περιήγησης σε ιστότοπους με αναληθή προϊόντα και πληροφορίες. Επιπλέον σε πιο εξειδικευμένες περιπτώσεις υποκλοπή προσωπικών δεδομένων μπορεί να πραγματοποιηθεί κατά την περιήγηση ενός χρήστη σε έναν ισότοπο, που είναι μολυσμένος με προγράμματα που καταγράφουν προσωπικές και οικονομικές πληροφορίες, τις οποίες χρησιμοποίησε ο χρήστης σε επισκέψεις του σε σελίδες που του τις ζητούν.

2.5. Ανάλυση Αδυναμιών

Η ακόλουθη ταξινόμηση είναι χρήσιμη για να καταλάβουμε τους τεχνικούς λόγους, πίσω από επιτυχείς τεχνικές παραβίασης της ασφάλειας και να βοηθήσει τους ειδικούς να προσδιορίσουν γενικές λύσεις για τον ίδιο τύπο προβλημάτων.

2.5.1. Αδυναμίες στο Σχεδιασμό του Λογισμικού

Τα πρωτόκολλα ασφαλείας είναι αυτά τα οποία καθορίζουν κανόνες και μεθόδους που χρησιμοποιούνται για την αποτελεσματική επικοινωνία των υπολογιστών σε ένα οποιοδήποτε δίκτυο – από το πιο απλό τοπικό μέχρι το διαδίκτυο. Για το λόγο αυτό ο τρόπος με τον οποίο θα σχεδιαστεί ένα πρωτόκολλο είναι σημαντικός. Αν δηλαδή σχεδιαστεί με λάθος τρόπο, τότε η χρήση του δεν θα είναι ασφαλής και οι κακόβουλοι hackers πάντα θα ενδιαφέρονται για τα τρωτά σημεία του και θα προσπαθούν να τα εκμεταλλεύονται.

Ένα τέτοιο παράδειγμα είναι το Network File System (NFS), που επιτρέπει στα συστήματα να μοιράζουν αρχεία το οποίο δεν παρέχει έναν σαφή τρόπο πιστοποίησης, προκειμένου οι χρήστες όταν συνδέονται να πιστοποιούνται. Για το λόγο αυτό οι NFS servers είναι στόχος για την κοινότητα των εισβολέων.

Μπορεί φυσικά η ασφάλεια του λογισμικού να ενισχυθεί στην πορεία από τους σχεδιαστές του με τις κατάλληλες διορθωτικές ενέργειες. Ωστόσο κάποιες φορές αυτό μπορεί να αποδειχθεί μάταιο καθώς το επιπλέον κομμάτι της ασφάλειας δεν είναι βέβαιο ότι θα αλληλεπιδράσει με τον σωστό τρόπο με το υπόλοιπο λογισμικό. Για αυτό είναι κρίσιμο το κάθε λογισμικό να σχεδιάζεται εξαρχής με την απαιτούμενη ασφάλεια, ανάλογα πάντα και με την χρήση για την οποία προορίζεται.

2.5.2. Αδυναμίες στην Υλοποίηση του Λογισμικού

Ακόμα και σε περιπτώσεις που ένα πρωτόκολλο έχει σχεδιαστεί με τον σωστό τρόπο δύναται να διαθέτει τρωτά σημεία ως προς τον τρόπο υλοποίησής του. Για παράδειγμα, ένα πρωτόκολλο για ηλεκτρονικό ταχυδρομείο, μπορεί να υλοποιηθεί με τέτοιο τρόπο που να επιτρέπει την σύνδεση στο mail port του συστήματος που θα γίνει η επίθεση και να ζητήσει να εκτελέσει συγκεκριμένες εντολές. Έτσι ο εισβολέας μπορεί να γράψει στο πεδίο «Προς:», αντί την σωστή διεύθυνση ηλεκτρονικού ταχυδρομείου, συγκεκριμένες εντολές και να ζητήσει το password file του συστήματος, χωρίς να χρειάζεται καν λογαριασμός στο σύστημα.

Το οποιοδήποτε λογισμικό δύναται να έχει χαλαρά σημεία – τα οποία το καθιστούν τρωτό, επειδή αυτά δεν εντοπίστηκαν πριν την τελική έκδοση. Οι εισβολείς αναζητούν και καταλήγουν εν τέλει να βρουν τα ελαττώματα που το λογισμικό έχει με δικά τους εργαλεία. Για παράδειγμα ψάχνουν για ελαττώματα σε περιπτώσεις όπως [4]:

1. Ανταγωνιστικές καταστάσεις στην προσπέλαση αρχείων Ανυπαρξία ελέγχων για το περιεχόμενο και το μέγεθος των δεδομένων

2. Ανυπαρξία ελέγχων για την αντιμετώπιση εσωτερικών λαθών

3. Αδυναμία προσαρμογής σε εξάντληση πόρων

4. Ελλιπή έλεγχο του λειτουργικού περιβάλλοντος

5. Ανάρμοστη χρήση κλήσεων του συστήματος

6. Χρήση τμημάτων του λογισμικού για άλλο σκοπό από αυτό που σχεδιάστηκαν.

Κάνοντας χρήση αδυναμιών στο λογισμικό οι εισβολείς μπορούν να αποκτήσουν πρόσβαση σε πόρους, χωρίς να χρειάζονται την απαραίτητη εξουσιοδότηση από το σύστημα

2.5.3. Αδυναμίες στην Διαμόρφωση Συστημάτων και Δικτύων

Τρωτά σημεία σε αυτή την κατηγορία δεν προέρχονται από προβλήματα στα πρωτόκολλα ή το λογισμικό. Αντίθετα τα προβλήματα αυτά πηγάζουν από την τακτική με την οποία τα δομικά αυτά στοιχεία, εγκαθίστανται και χρησιμοποιούνται. Τα προϊόντα στις περισσότερες περιπτώσεις παραδίδονται και εγκαθίστανται με συγκεκριμένες παραμέτρους, οι οποίες αποτελούν μέσο εκμετάλλευσης των κακόβουλων εισβολέων. Οι διαχειριστές των υπολογιστικών συστημάτων και των δικτύων, καθώς και οι χρήστες συνήθως δεν προβαίνουν στην αλλαγή των προκαθορισμένων παραμέτρων, κάτι το οποίο έχει ως αποτέλεσμα το σύστημα να εμφανίζει τρωτά σημεία. Ένα χαρακτηριστικό παράδειγμα λανθασμένης διαμόρφωσης το οποίο συνήθως αποτελεί αντικείμενο εκμετάλλευσης από τους εισβολείς είναι η ανώνυμη χρήση της υπηρεσίας File Transfer Protocol (FTP).

Οι τρέχουσες μέθοδοι δημιουργίας λογισμικού δεν έχουν να επιδείξουν αξιόλογα επιτεύγματα, σε ότι αφορά θέματα ασφάλειας. Τις περισσότερες φορές το θέμα τις ασφάλειας είναι μεταγενέστερο του βασικού σχεδιασμού του λογισμικού. Η δημιουργία ασφαλών λογισμικών, πρέπει να έχει την δυνατότητα να επιδεικνύει το λογισμικό συμπεριφορά που συνεισφέρει στην ικανότητα επιβίωσης του συστήματος παρά τις επιθέσεις που δέχεται.

Σαν ικανότητα επιβίωσης, ορίζεται η ικανότητα ενός συστήματος να συνεχίζει να εκτελεί τις κρίσιμες λειτουργίες, με τον χρονοπρογραμματισμό που έχει οριστεί, ακόμα και αν μέρος των πόρων του συστήματος έχουν δεχτεί επίθεση ή έχουν βλάβη. Ο όρος σύστημα έχει ευρεία έννοια και περιλαμβάνει και συστάδες από συστήματα και δίκτυα.

Αν και οι αρχές και μέθοδοι που έχουν να κάνουν με την ικανότητα επιβίωσης είναι χαρακτηριστικά των έμβιων όντων, μπορούν να υλοποιηθούν με παραδοσιακές τεχνικές της περιοχής της δημιουργίας λογισμικού και των υπολογιστικών συστημάτων, όπως αξιοπιστία, αντιμετώπιση σφαλμάτων, επιβεβαίωση ορθότητας, απόδοση και ασφάλεια συστημάτων. Η έρευνα κατευθύνεται σε δημιουργία μεθόδων ανοσοποίησης που θα διακινούν αυτόματα τις διορθώσεις των τρωτών, σε ένα ολόκληρο δίκτυο, για να διαφυλαχτούν όλα τα συστήματα από ένα νέο πρόβλημα ασφάλειας. Η έννοια της ανοσοποίησης μπορεί να γενικευθεί ώστε να συμπεριλάβει προσαρμόσιμα δίκτυα, που αποτελούνται από κατανεμημένα συνεργαζόμενα δικτυακά στοιχεία, που ανταλλάσσουν πληροφορίες για προβλήματα ασφάλειας και δραστικά αλλάζουν και προσαρμόζονται σαν αντίδραση απειλών εναντίον της ασφάλειας.

2.6. Προετοιμασία και Υλοποίηση της Επίθεσης

Η μεθοδολογία που χρησιμοποιείται από κάποιον που προετοιμάζει μία επίθεση είναι απλή. Μαθαίνει από το διαδίκτυο για τα τελευταία τρωτά στα συστήματα. Ανιχνεύει το δίκτυο ενός ιστότπου, για να βρεθεί ένα τέτοιο τρωτό σημείο. Αν

βρεθεί αρχίζει η προσπάθεια εκμετάλλευσής του. Οι έμπειροι hackers προσπαθούν να αποκρύψουν την πραγματική IP address του συστήματος τους. Χρησιμοποιούν συστήματα που έχουν καταλάβει και από κει επιτίθενται στους επόμενους στόχους τους. Οι πιο έμπειροι θα δοκιμάσουν επιθέσεις από κόμβους που έχουν προσπέλαση μέσω τηλεφώνου.

Τα περισσότερα εργαλεία που χρησιμοποιούνται είναι αυτοματοποιημένα ώστε να μην χρειάζονται παρέμβαση του χρήστη. Το εργαλείο ξεκινά και μετά από αρκετές μέρες συγκεντρώνονται τα αποτελέσματα. Τα εργαλεία, αν και είναι πολλά και διαφορετικά, χρησιμοποιούν την ίδια στρατηγική:

- Δημιουργούν βάσεις δεδομένων με τα προσπελάσιμα συστήματα
- Βρίσκουν το λειτουργικό σύστημα και τις υπηρεσίες που προσφέρουν
- Προσδιορίζουν το τρωτό σημείο και το εκμεταλλεύονται

Παρόλο που φαίνεται πως το ψάξιμο είναι κάτι που εύκολα εντοπίζεται τα αποτελέσματα δείχνουν το αντίθετο. Πολλοί διαχειριστές δεν παρακολουθούν το δίκτυο τους, αλλά και οι hackers δεν ψάχνουν πάντα στο κενό. Βρίσκουν ένα σύστημα και αφού καταφέρουν να «μπουν» το χρησιμοποιούν σαν όχημα. Μπορούν είτε να συνεχίσουν στο εσωτερικό δίκτυο, είτε να ξεκινήσουν την αναζήτηση μεγάλου μέρους του διαδικτύου. Αν τυχόν και ο ανιχνευτής τους ανακαλυφτεί, θα κατηγορηθεί ο διαχειριστής του συστήματος από το οποίο ξεκινά η επίθεση. Τυχόν νέες ανακαλύψεις μοιράζονται με άλλους hackers, αυξάνοντας κατά πολύ την δραστικότητά τους.

Για να γίνει μία επίθεση αρκεί κανείς:

⇒ Να ανατρέξει μετά την συγκέντρωση αυτών των πληροφοριών στις βάσεις δεδομένων που υπάρχουν στο διαδίκτυο (αρκεί μία μηχανή αναζήτησης, όπως astalavista, neworder), με στοιχεία των τρωτών ανά σύστημα και έκδοση, ώστε να βρει μεθόδους επίθεσης και να τις εφαρμόσει στο σύστημα-στόχο.

⇒ Να κατεβάσει το απαραίτητο λογισμικό για τον συγκεκριμένο τρόπο επίθεσης στο σύστημα και αν χρειάζεται, να κάνει compile τον κώδικα.

⇒ Να κάνει την επίθεση ώστε να πετύχει προσπέλαση με προνόμια διαχειριστή, ανάλογα με το σύστημα ασφάλειας που υπάρχει. Σε περίπτωση που υπάρχει firewall ή αυτόματο σύστημα ανίχνευσης επιθέσεων (Intrusion Detection System -IDS) εφαρμόζονται μέθοδοι για να ξεπεραστούν όπως για παράδειγμα η μέθοδος του firewalking.

⇒ Να εγκαταστήσει κερκόπορτες για μεταγενέστερη χρήση.

⇒ Να στήσει sniffers για το δίκτυο.

⇒ Να εγκαταστήσει DoS-Trojan (π.χ. TrinOO, TFN, TFN2K κ.ά.)

⇒ Να καλύψουν τα ίχνη τους από τα system logs. Υπάρχουν εργαλεία για την διαγραφή των στοιχείων από τα logs. Τέτοια εργαλεία είναι ομαδοποιημένα σε σουίτες προγραμμάτων που λέγονται και rootkits (π.χ. Irk4). Τα rootkits έχουν σαν σκοπό να παρέχουν ένα ολοκληρωμένο περιβάλλον για την επίθεση, μέχρι και να αποκρύψουν τις ενέργειες του hacker (π.χ. ps, netstat), να καθαρίσουν τα logs (π.χ. clean), να αφήσουν κερκόπορτες (π.χ. σαν login, inetd) και να καταγράψουν τις ενέργειες του διαχειριστή (π.χ. linsniffer).

⇒ Να συνεχίσει τις επιθέσεις του από τον κόμβο αυτό. Αν πρόκειται για προσπάθεια DDoS, μπορεί σε κάθε 20 συστήματα να εγκαθιστά ένα master

control πρόγραμμα για τον συντονισμό της επίθεσης προς τον υπολογιστή στόχο.

Τα εργαλεία που χρησιμοποιούνται από τους hackers είναι συνήθως εξαιρετικά απλά και πλήρως αυτοματοποιημένα. Ένα τυπικό πακέτο εργαλείων περιλαμβάνει ανιχνευτές δικτύου (network scanners), εργαλεία εύρεσης λέξεων συνθηματικών (password cracking tools), «ωτακουστές» πακέτων (packet sniffers), δούρειους ίππους (trojan horses) «καθαριστές» εγγραφών συστήματος (log cleaners), ανιχνευτές ενεργειών στα συστήματα. Ο σκοπός τους είναι η απόκτηση δικαιωμάτων root με τον ευκολότερο και ταχύτερο τρόπο. Συνήθως Βασίζονται στην υπόθεση πως υπάρχει τρωτό σημείο και δοκιμάζουν καταρχήν τα γνωστά. Ο πόλεμος διαχειριστών-hackers κρίνεται στα διαθέσιμα εργαλεία, την συνεχή πληροφόρηση, την ταχύτητα αντίδρασης για ίο κλείσιμο των τρωτών και στο διαθέσιμο χρόνο για αυτή την δουλειά. Οι επιθέσεις γίνονται όλες τις ώρες κύρια όμως τις πρώτες πρωινές.

Κεφάλαιο 3ο

Μεθοδολογίες Βελτίωσης της Ασφάλειας

3.1. Γενική Μεθοδολογία Ασφάλειας

Η ανάγκη για την διασφάλιση της ασφάλειας στα τοπικά δίκτυα και άλλα και στα δίκτυα ευρείας ζώνης, κάνει όλο και πιο εκτεταμένη την ανάγκη για δημιουργία των εμποδίων εκείνων που είναι απαραίτητα στην φυσική προσπέλαση του εξοπλισμού, το δίκτυο, αλλά και τις εφαρμογές. Την δεδομένη χρονική στιγμή δεν υπάρχει κάποιο σύστημα ασφαλείας δικτύων το οποίο είναι στο 100% και το πιο πιθανό μάλιστα είναι ένα τέτοιο σύστημα να μην κατασκευαστεί λόγω του ασύμφορου κόστους που εσωκλείει [5].

Για το λόγο αυτό οι περισσότεροι επιδιώκουν να κατασκευάσουν απλώς ένα ασφαλές σύστημα του οποίου το κόστος υλοποίησης θα είναι οριακά μεγαλύτερο από το κόστος μια κακόβουλης επίθεσης. Για την κατασκευή ενός τέτοιου συστήματος όποιο και αν είναι το κόστος του απαιτούνται μια σειρά από ενέργειες, οι οποίες είναι οι ενέργειες για την δημιουργία ενός λογισμικού ή μιας μονάδας υλικού. Οι ενέργειες αυτές είναι η ανάλυση απαιτήσεων, ο σχεδιασμός, η υλοποίηση, η δοκιμή και η τελική λειτουργία. Πιο αναλυτικά λοιπόν έχουμε τις παρακάτω ενέργειες:

1. Πρέπει να γίνει ανάλυση απαιτήσεων , δηλαδή από την μία λεπτομερής ανάλυση των κινδύνων οι οποίοι είναι πιθανό να εμφανιστούν στην πορεία και από την άλλη η καταγραφή των πόρων τους οποίους θέλουμε να διαφυλάξουμε από επιθέσεις. Όσο αφορά την καταγραφή των κινδύνων είναι αναγκαία η καλή γνώση των εργαλείων και των μεθόδων με τις οποίες πραγματοποιούνται οι κακόβουλες επιθέσεις.

2. Πρέπει να προσδιοριστεί και να οριοθετηθεί η πολιτική ασφαλείας που θα επιλέξουμε να ακολουθήσουμε.

3. Πρέπει να γίνει σχεδιασμός του συστήματος ασφάλειας που θα φτιάξουμε. Μιλώντας για σχεδιασμό , εννοούμε την αρχιτεκτονική

4. Το λογισμικό ή υλικό που θα κατασκευαστεί θα πρέπει να περιέχει και υπηρεσίες ασφαλείας οι οποίες θα πρέπει να αποφασισθούν εξαρχής και πριν την υλοποίηση του.

5. Να έχουμε σχεδιάσει τον τρόπο αντιμετώπισης ενός περιστατικού επίθεσης να ενημερώνουμε τους χρήστες μας

6. Να ήμαστε πάντα ενημερωμένοι για τα πιο πρόσφατα νέα σε σχέση με την ασφάλεια.

Για να επιτύχουμε λοιπόν έχουμε ένα ικανοποιητικό επίπεδο ασφάλειας πρέπει να αναλύσουμε τα παραπάνω για να ικανοποιήσουμε την ύπαρξη έξι βασικών σημείων της ασφάλειας:

1. Την εμπιστευτικότητα της πληροφορίας: διασφαλίζοντας πως η πληροφορία είναι προσπελάσιμη από τους σωστούς χρήστες (π.χ. τα σχέδια για το νέο προϊόν είναι προσπελάσιμα σε ορισμένους μόνο χρήστες)

2. Την πιστοποίηση αυθεντικότητας: επαληθεύοντας την αυθεντικότητα ενός χρήστη ή υπολογιστικού συστήματος (π.χ. πως είναι πράγματι ο χρήστης που ζητά προσπέλαση)

3. Την αποφυγή άρνησης πράξεων: εξασφαλίζοντας πως οι χρήστες δεν μπορούν να αρνηθούν τις ηλεκτρονικές πράξεις τους (π.χ. ότι αντέγραψαν ένα αρχείο)

4. Την ακεραιότητα των δεδομένων: διασφαλίζοντας πως τα δεδομένα δεν έχουν αλλάξει και είναι τα ίδια με αυτά που αρχικά τοποθετήθηκαν (π.χ. τα περιεχόμενα της μελέτης δεν έχουν αλλάξει από κάποιο τρίτο)

5. Τον έλεγχο προσπέλασης: διασφαλίζοντας πως οι πόροι βρίσκονται κάτω από τον αποκλειστικό έλεγχο εξουσιοδοτημένων χρηστών, βεβαιώνοντας πως ο χρήστης που ζητά την προσπέλαση έχει την άδεια να το κάνει (π.χ. η αλλαγή στο αρχείο ενός υπαλλήλου επιτρέπεται μόνο σε εξουσιοδοτημένα άτομα)

6. Την διαθεσιμότητα των πόρων: εξασφαλίζοντας πως τα δεδομένα οι υπηρεσίες και οι εξυπηρετητές είναι διαθέσιμα όποτε ζητηθούν (π.χ. άμεση αποκατάσταση δεδομένων και υπηρεσιών μετά από επίθεση).

3.2. Αποτίμηση Κινδύνου

Είναι πολύ σημαντικό να καταλάβουμε πως στην υλοποίηση της ασφάλειας δεν μπορεί κανείς να κάνει την ερώτηση «ποιο είναι το καλύτερο firewall, να το εγκαταστήσω». Υπάρχουν δύο άκρα: απόλυτη ασφάλεια και απόλυτη ελευθερία πρόσβασης. Μία καλή προσέγγιση προς την απόλυτη ασφάλεια έχουμε όταν ο υπολογιστής μας δεν είναι συνδεμένος με το δίκτυο, δεν είναι συνδεμένος στο ηλεκτρικό ρεύμα, είναι κλειστός, κλειδωμένος σε ένα χρηματοκιβώτιο, κτισμένο με τεράστιες ποσότητες τσιμέντου σε πολύ μεγάλο βάθος, με μοναδική είσοδο που φυλάσσεται από ακριβοπληρωμένους φρουρούς [4]. Δυστυχώς έτσι δεν είναι και τόσο χρήσιμος.

Από την άλλη πλευρά ένας υπολογιστής με πλήρη ελευθερία πρόσβασης είναι μεν τρομερά εύχρηστος, αλλά μπορεί να καταλήξει άχρηστος αφού χωρίς κανόνες χρήσης ο καθένας μπορεί να κάνει ότι θέλει καταστρέφοντας την λειτουργικότητά του είτε εσκεμμένα, είτε από άγνοια.

Οι περισσότεροι άνθρωποι έχουν μία εικόνα για το ανεκτό επίπεδο κινδύνου για κάθε ενέργειά τους (όσο και αν είναι προσιτό δεν πηδάμε από το παράθυρο του σπιτιού μας για να κατέβουμε γρήγορα στο δρόμο να προλάβουμε το λεωφορείο για την δουλειά, ενώ μπορεί να το επιχειρήσουμε αν κινδυνεύει η ζωή μας).

Ο κάθε οργανισμός λοιπόν πρέπει να αποφασίσει για τα συστήματά του, το σημείο που χρειάζεται να βρίσκεται, ανάμεσα στην απόλυτη ασφάλεια και την απόλυτη ευκολία προσπέλασης. Μία πολιτική ασφάλειας πρέπει να προσδιορίσει τους πόρους που έχουν αξία για τον οργανισμό, τις πιθανές απειλές και κατόπιν να προτείνει την κατάλληλη πολιτική ασφάλειας για το πως θα διασφαλιστούν οι πόροι από τις πιθανές απειλές [5].

Όπως αναφέραμε και σε προηγούμενο κεφάλαιο είναι σημαντικό να προσδιοριστούν όλοι οι πόροι που θα πρέπει να προστατευθούν. Η κατηγοριοποίηση των πόρων που θα προστατευθούν έχει ως εξής:

1. Υλικό: Κεντρική Μονάδα Επεξεργασίας, τερματικοί σταθμοί εργασίας, προσωπικοί υπολογιστές, εκτυπωτές, δίσκοι, γραμμές επικοινωνίας, εξυπηρετητές, δρομολογητές.

2. Λογισμικό: Πηγαίος κώδικας, αντικείμενος κώδικας, εργαλεία, διαγνωστικά προγράμματα, λειτουργικά συστήματα, προγράμματα επικοινωνίας.

3. Δεδομένα: Αρχειοθετημένα off-line, αποθηκευμένα on-line, κατά την διάρκεια της επεξεργασίας τους, αντίγραφα ασφαλείας.

4. Ανθρώπινο δυναμικό: Χρήστες, διαχειριστές, τεχνικοί κ.λπ.

5. Τεκμηρίωση: Προγραμμάτων, υλικού, συστημάτων, τοπικών διαδικασιών διαχείρισης.

6. Υλικό Υποστήριξης: Δημοσιεύσεις, φόρμες, μαγνητικά μέσα κ.α.

Αφού καταγραφούν οι πόροι που πρέπει να προστατευτούν θα πρέπει να προσδιοριστούν πιθανές απειλές τους. Κλασικές απειλές που μπορεί να δεχθεί ένα σύστημα είναι οι ακόλουθες [5]:

1. Σκόπιμη απειλή (Hacking, Denial of Service, κατασκοπία)

2. Απροσχεδίαστη απειλή (π.χ. λανθασμένη αποστολή με mail κρίσιμων στοιχείων σε μια ομάδα αποδεκτών)

3. Φυσικές περιβαλλοντικές απειλές (σεισμός)

4. Μη φυσικές απειλές (εμπρησμός, διακοπή ρεύματος)

5. Μη εξουσιοδοτημένη προσπέλαση των μέσων και / ή της πληροφορίας.

6. Αγνώστου ταυτότητας και / ή μη εξουσιοδοτημένη αποκάλυψη της πληροφορίας.

7. Κατάργηση / άρνηση των προσφερόμενων υπηρεσιών.

Η εμπιστοσύνη παίζει σημαντικό ρόλο στην υλοποίηση της πολιτικής ασφάλειας. Το πρώτο βήμα είναι να αποφασιστεί ποιος έχει προσπέλαση, σε ποιους πόρους, τι είδους (διαχειριστή, απλού χρήστη, χειριστή) και να περιγραφεί το μοντέλο υλοποίησης με ομάδες χρηστών.

3.3. Πολιτικές Ασφάλειας

Η πολιτική ασφάλειας είναι το σύνολο των κανόνων που ρυθμίζουν την πρόσβαση που έχει κάθε χρήστης στα πληροφοριακά συστήματα ενός οργανισμού. Χωρίς την ύπαρξη πολιτικής ασφάλειας δεν υπάρχει ένα γενικό πλαίσιο για την ασφάλεια. Με την πολιτική ορίζουμε ποια συμπεριφορά είναι επιτρεπόμενη μέσα στον οργανισμό ως προς την χρήση των προσφερόμενων υπηρεσιών, μέσα από διαδικασίες που πρέπει να ακολουθηθούν από όλους [4].Η πολιτική ασφάλειας είναι μία καλή μέθοδος για την δημιουργία συναντίληψης ανάμεσα στα στελέχη του οργανισμού.

Οι χρήστες αντιμετωπίζουν τις πολιτικές σαν ένα φρένο της παραγωγικότητας ή ένα τρόπο να ελέγχεται η συμπεριφορά των εργαζομένων, αρνούμενοι να υποκύψουν στην παρακολούθηση.

Οι αποφάσεις που λαμβάνονται για την ασφάλεια ενός δικτύου από τον διαχειριστή του, καθορίζουν το πόσο ασφαλές είναι ένα δίκτυο καθώς και την ευκολία στη χρήση του. Καταρχήν θα πρέπει να αποφασιστεί τι είναι σκόπιμο να διαφυλαχτεί. Όταν γίνει αυτό θα πρέπει να οριστούν οι περιορισμοί που θα πρέπει να τεθούν ώστε να έχουμε το επιθυμητό αποτέλεσμα.

Οι στόχοι καθορίζονται από τους ακόλουθους παράγοντες [5]:

1. Προσφερόμενες υπηρεσίες σε σχέση με την ασφάλεια του δικτύου. Υπάρχουν περιπτώσεις που η χρήση κάποιων υπηρεσιών αυξάνει τον κίνδυνο για την άρση της ασφάλειας ενός δικτύου, με αποτέλεσμα το κόστος των υπηρεσιών αυτών να είναι μεγαλύτερο από τα οφέλη τους. Σε τέτοιες περιπτώσεις είναι προτιμότερη η κατάργηση της υπηρεσίας.

2. Ευκολία χρήσης σε σχέση με τη προσφερόμενη ασφάλεια. Το ευκολότερο σύστημα στη χρήση είναι αυτό που προσφέρει άμεση πρόσβαση χωρίς την ύπαρξη συνθηματικών. Παρόλα αυτά ένα τέτοιο σύστημα δεν προσφέρει καμία απολύτως ασφάλεια. Με την χρήση συνθηματικών (password) το σύστημα γίνεται λίγο πιο δύσκολο αφού κάθε χρήστης θα πρέπει να θυμάται τον κωδικό του, αλλά ταυτόχρονα γίνεται και πιο ασφαλές.

3. Κόστος ασφάλειας ενάντια στον κίνδυνο απώλειας. Υπάρχουν διάφορα είδη που προσδιορίζουν το κόστος της ασφάλειας όπως:

4. Κόστος αγοράς υλικού ή λογισμικού, όπως firewalls και on-time password generators

5. Απόδοση (η κωδικοποίηση και η αποκωδικοποίηση χρειάζονται κάποιο χρόνο) καθώς και ευκολία στην χρήση.

Υπάρχουν επίσης διάφορα επίπεδα κινδύνου όπως:

1. Αρση του απορρήτου (π.χ. ανάγνωση πληροφορίας από τρίτους),

2. Απώλεια δεδομένων (διαγραφή δεδομένων) ή

3. Απώλεια υπηρεσιών (χρήση ίων πηγών του δικτύου, άρνηση πρόσβασης στο δίκτυο κ.α.).

Για την υλοποίηση της ασφάλειας του δικτύου θα πρέπει να ληφθούν υπόψη όλα τα παραπάνω.

Μια πολιτική ασφάλειας για να είναι κατάλληλη για τον οργανισμό θα πρέπει να είναι αποδεκτή από όλους τους εργαζομένους. Επίσης θα πρέπει να υπάρχει υποστήριξη της πολιτικής και από τη διεύθυνση του οργανισμού ώστε να επιτύχει στους στόχους της. Οι ομάδες εργαζομένων που εμπλέκονται σε μια πολιτική ασφάλειας είναι:

1. Οι απλοί χρήστες, οι οποίοι είναι και οι πρώτοι και κυριότεροι που πρέπει να την κατανοήσουν γιατί σε αυτούς απευθύνεται.

2. Προσωπικό υποστήριξης - είναι αυτοί που θα υλοποιήσουν και θα υποστηρίξουν την πολιτική ασφάλειας

3. Διοικητικό προσωπικό - καθορίζουν το Βαθμό προστασίας των περισσότερων δεδομένων και αναλαμβάνουν το οικονομικό κόστος της πολιτικής που θα υλοποιηθεί

4. Νομικοί σύμβουλοι - που ενδιαφέρονται για την φήμη και την νομική κάλυψη του οργανισμού

Τέλος μια πολιτική ασφάλειας θα πρέπει να έχει τα παρακάτω χαρακτηριστικά:

1. Υλοποιήσιμη: Να υπάρχουν ρεαλιστικοί κανόνες διαχείρισης των συστημάτων για κάθε τμήμα του οργανισμού, οδηγίες χρήσης των διάφορων πόρων, εγκατεστημένα συστήματα ασφάλειας.

2. Θα πρέπει να ακολουθείται απ' όλους: Οι χρήστες θα πρέπει να κατανοήσουν πως δε γίνονται παρακάμψεις για τη διευκόλυνση τους. Θα πρέπει οι ίδιοι να προσαρμόσουν τις καθημερινές δραστηριότητές τους στους κανόνες ασφάλειας. Δεν θα πρέπει όμως να είναι και υπερβολικά αυστηροί γιατί τότε οι χρήστες θα προσπαθούν να βρουν τρόπους για να ξεπεράσουν τους κανόνες

3. Ευέλικτη: Για να είναι βιώσιμη μια πολιτική ασφάλειας θα πρέπει να εξαρτάται από το υλικό και το λογισμικό που υπάρχει, ώστε να μπορεί να αναπροσαρμόζει τους κανόνες της σύμφωνα με τις προδιαγραφές τους. Επίσης θα πρέπει να αναγνωρίζει τις εξαιρέσεις που είναι δυνατό να γίνουν στους κανόνες ασφάλειας ανάλογα με τις ανάγκες που θα παρουσιαστούν. Για παράδειγμα ο διαχειριστής ενός συστήματος μπορεί να χρειαστεί τον κωδικό πρόσβασης κάποιου χρήστη για ένα σύστημα.

4. Θα πρέπει να ισοσταθμίζει την προστασία του οργανισμού με την παραγωγικότητα. Αν οι κανόνες είναι πολύ αυστηροί οι χρήστες θα βρουν τρόπους να μην τους εφαρμόζουν. Οι τεχνικοί έλεγχοι δεν είναι πάντα εφικτοί

5. Αναβαθμίσιμη: Οι κανόνες που τίθενται θα πρέπει να αναπροσαρμόζονται και να ακολουθούν την εξέλιξη του οργανισμού.

3.4. Κανόνες Ασφαλείας Δικτύων

Η πολιτική ασφάλειας για το δίκτυο καθορίζει:

⇒ Ποιος εγκαθιστά καινούριες συσκευές στο δίκτυο

⇒ Ποιος ειδοποιείται για κάθε τέτοια εγκατάσταση

⇒ Πώς τεκμηριώνεται μια τέτοια αλλαγή

⇒ Ποιες είναι οι αλλαγές στο «χάρτη» του δικτύου

⇒ Ποιες οι νέες απαιτήσεις σε ασφάλεια

⇒ Πώς αντιμετωπίζονται μη ασφαλείς συσκευές

Επιπλέον η πολιτική ασφάλειας για την προστασία των δεδομένων - πληροφοριών του οργανισμού, καθορίζει τα εξής:

⇒ Επίπεδα κρισιμότητας των πληροφοριών που κυκλοφορούν

⇒ Ποιος έχει πρόσβαση σε ευαίσθητες πληροφορίες

⇒ Τα επίπεδα πρόσβασης σε τέτοιες πληροφορίες που έχουν οι ομάδες των χρηστών

⇒ Πώς αποθηκεύεται και μεταδίδεται τέτοιου είδους πληροφορία

⇒ Σε ποια συστήματα αποθηκεύεται τέτοια πληροφορία

⇒ Σε ποια συστήματα εκτυπώνονται τέτοια δεδομένα

Από πλευρά των χρηστών η πολιτική ασφαλείας θα πρέπει να καθορίζει τα παρακάτω:

1. Την ευθύνη των χρηστών για την προστασία των δεδομένων που έχουν στους προσωπικούς λογαριασμούς τους

2. Αν οι χρήστες μπορούν διαβάζουν και να αντιγράφουν αρχεία που δεν τους ανήκουν αλλά έχουν πρόσβαση

3. Αν οι χρήστες μπορούν να μεταβάλλουν αρχεία που δεν τους ανήκουν αλλά έχουν δικαίωμα εγγραφής σ' αυτά

4. Αν οι χρήστες μπορούν να πάρουν αντίγραφα βασικών αρχείων (configuration files) από τα βασικά συστήματα του οργανισμού

5. Αν οι χρήστες μπορούν να μοιράζουν αρχεία για κοινή χρήση

6. Αν οι χρήστες μπορούν να δημιουργούν αντίγραφα νόμιμα αγορασμένου λογισμικού

7. Το επίπεδο χρήσης του Mail, Web, News από τους χρήστες ή από ομάδες χρηστών

Η πολιτική ασφάλειας για τους λογαριασμούς των χρηστών θα πρέπει να καθορίζει:

1. Ποιος έχει τη δικαιοδοσία να δέχεται αιτήσεις ανοίγματος λογαριασμών

2. Ποιος επιτρέπεται να κάνει χρήση των πόρων του οργανισμού

3. Αν οι χρήστες μοιράζονται το λογαριασμό τους με άλλους ή αν έχουν περισσότερους από έναν λογαριασμούς σε συστήματα του οργανισμού

4. Τα δικαιώματα και τις υπευθυνότητες των χρηστών για τη χρήση των πόρων που τους διατίθενται

5. Πότε ο λογαριασμός ενός χρήστη απενεργοποιείται

6. Τους κανόνες που ακολουθούν οι κωδικοί πρόσβασης των χρηστών

Η πολιτική ασφάλειας για την απομακρυσμένη πρόσβαση θα πρέπει να καθορίζει [5]:

1. Ποιος έχει το δικαίωμα της απομακρυσμένης πρόσβασης (Authentication)

2. Ποιες είναι οι επιτρεπόμενες μέθοδοι για απομακρυσμένη πρόσβαση

3. Αν επιτρέπονται dial-out modems

4. Αν θα υπάρχει καταγραφή των χρηστών που χρησιμοποιούν την υπηρεσία αυτή

5. Αν θα δίνεται η δυνατότητα για callback

6. Σε ποια δεδομένα επιτρέπεται η απομακρυσμένη πρόσβαση

Η πολιτική ασφάλειας στη διαδικασία του configuration management καθορίζει:

1. Πώς ελέγχεται και εγκαθίσταται καινούριο υλικό και λογισμικό στα συστήματα του οργανισμού

2. Πώς τεκμηριώνονται οι αλλαγές σε υλικό και λογισμικό

3. Ποιος ενημερώνεται για τυχόν αλλαγές σε υλικό και λογισμικό

4. Ποιος έχει τη δικαιοδοσία να κάνει αλλαγές στο υλικό ή το λογισμικό των συστημάτων του οργανισμού

5. Με ποια διαδικασία μπορεί να υπάρξει εξαίρεση σε ένα κανόνα για ορισμένο χρονικό διάστημα

6. Πως γίνεται η διαχείριση των firewalls, πως ζητούνται αλλαγές και πως εγκρίνονται

Η πολιτική ασφάλειας στην περίπτωση που παρουσιαστεί κάποιο πρόβλημα (εισβολή) καθορίζει:

1. Διαδικασία άμεσης υποστήριξης από εξειδικευμένο προσωπικό

2. Τις πρώτες, άμεσες ενέργειες που πρέπει να γίνουν

3. Τον τρόπο που θα αντιμετωπιστεί μια εισβολή

4. Ποιες πληροφορίες θα πρέπει να καταγραφούν για να χρησιμοποιηθούν αργότερα

5. Ποιος θα πρέπει να ενημερωθεί και πότε

Τέλος η πολιτική ασφάλειας για τη διαδικασία του backup καθορίζει:

1. Ποια είναι τα αρχεία τα οποία παίρνονται backup (αρχεία συστήματος, αρχεία χρηστών)

2. Πόσο συχνά πραγματοποιείται η διαδικασία του backup

3. Αν υπάρχει Disaster Recovery το όποιο είναι άμεσα εκτελέσιμο μετά από κάποια δυσλειτουργία.

4. Που φυλάγονται τα μαγνητικά μέσα.

3.5. Ασφάλεια με Τείχος Προστασίας

Η σύνδεση ενός συστήματος στο διαδίκτυο παρέχει την δυνατότητα πλήρους αμφίδρομης επικοινωνίας με αυτό. Αυτή η δυνατότητα δεν μπορούμε να πούμε ότι

είναι σε όλες τις περιπτώσεις επιθυμητή αφού δεν είναι λίγες οι περιπτώσεις όπου εμπιστευτικές πληροφορίες οι οποίες βρίσκονταν στα συστήματα ενός οργανισμού διέρρευσαν.

Για να υπάρξει ένα είδος διαχωρισμού ανάμεσα στο Internet του οργανισμού και το Internet υπάρχει μία ομάδα συστημάτων που δημιουργεί έναν τοίχο ασφαλείας ανάμεσα στα δύο δίκτυα. Η χρήση τους βέβαια βοηθά την ενίσχυση της ασφάλειας, αλλά δεν την εγγυάται. Ο σωστός σχεδιασμός της περιμέτρου και της διαμόρφωσης των συστημάτων είναι απαραίτητος για την σωστή λειτουργία τους.

Ένα τείχος προστασίας μπορεί να προσφέρει:

1. Ένα σημείο εφαρμογής των αποφάσεων που αφορούν την ασφάλεια
2. Ένα μέσο για την εφαρμογή της πολιτικής ασφάλειας
3. Έναν τρόπο καταγραφής της δικτυακής κίνησης
4. Ένα φράγμα σε ανεπιθύμητες επιθέσεις

Αντίθετα ένα firewall δεν μπορεί να μας προφυλάξει από:

1. Εσωτερικούς χρήστες που σκοπεύουν να επιτεθούν
2. Συνδέσεις που δεν περνούν από αυτό
3. Εντελώς νέους τύπους απειλών-επιθέσεων

4. Ιούς, αποδοτικά

5. Λάθη στην διαμόρφωση

Παρόλα αυτά ούτε με τη χρήση firewall μπορούμε να έχουμε απόλυτη ασφάλεια στο δίκτυο. Όταν μιλάμε για ασφάλεια θα πρέπει να λάβουμε υπόψη μας το κόστος που απαιτείται για την προστασία, το βαθμό πολυπλοκότητας του συστήματος μας καθώς και την ευκολία στη χρήση. Το firewall αλληλεπιδρά με το internet και χρειάζεται ιδιαίτερη προσοχή στην εγκατάστασή του και την σωστή διαμόρφωσή του.

Τείχος Προστασίας λοιπόν, είναι ένας μηχανισμός που χρησιμοποιείται για να ελέγχει την πρόσβαση από και προς το δίκτυο με απώτερο σκοπό την προστασία του δικτύου. Ένα firewall λειτουργεί σαν μία πύλη από την οποία περνάει όλη η κίνηση από και προς το εξωτερικό δίκτυο. Με την χρήση ενός Firewall περιορίζεται η επικοινωνία ανάμεσα στο προστατευόμενο δίκτυο και ένα οποιοδήποτε άλλο δίκτυο. Γενικά ένα firewall θα μπορούσαμε να το παρομοιάσουμε με έναν τοίχο ανάμεσα στο εσωτερικό δίκτυο και ένα εξωτερικό δίκτυο (π.χ. το Διαδίκτυο).

Το βασικό χαρακτηριστικό αυτού του τοίχου είναι να βρεθούν οι δρόμοι - πύλες από τους οποίους θα μπορεί να περάσει συγκεκριμένη πληροφορία. Το πιο κρίσιμο κομμάτι για την υλοποίηση του firewall είναι η εύρεση των κριτηρίων που θα προσδιορίσουν ποια πακέτα επιτρέπεται και ποια όχι να περάσουν μέσα από αυτές τις πύλες. Ένα τείχος προστασίας μπορεί να είναι ο συνδυασμός δρομολογητών (routers), υποδικτύων (network segments) και υπολογιστών που έχουν ρόλο host.

Ανάλογα με τον τρόπο λειτουργίας της συσκευής υπάρχουν διαφορετικού είδους εγκαταστάσεις. Παρακάτω αναφέρουμε μερικά στοιχεία των firewalls [5]:

1. Bastion host: Ένας υπολογιστής γενικού σκοπού που χρησιμοποιείται για να ελέγξει την προσπέλαση ανάμεσα στο εσωτερικό (ιδιωτικό) δίκτυο (intranet) και το Internet. Συνήθως το λειτουργικό τους σύστημα είναι της κατηγορίας Unix που έχει τροποποιηθεί, αφαιρώντας συγκεκριμένες εντολές και υπηρεσίες, ώστε να ελαττωθούν οι δυνατότητές του στις ελάχιστες απαραίτητες για την υποστήριξη των υπηρεσιών που επιτρέπονται.

2. Δρομολογητής (Router): Ένας υπολογιστικό σύστημα ειδικού σκοπού, που διασυνδέει δύο δίκτυα. Διαχειρίζεται τα πακέτα που διακινούνται ανάμεσα στα δίκτυα, δρομολογώντας την κυκλοφορία στα κατάλληλα δίκτυα.

3. Ελεγκτής Λίστας Προσπέλασης (Access Control List-ACL): Πολλοί δρομολογητές έχουν την δυνατότητα να επεξεργάζονται τα πακέτα που δρομολογούν και να επιτρέπουν (ή όχι) την κυκλοφορία τους ανάλογα με το αν πληρούν (ή όχι) ορισμένες συνθήκες. Αυτές συμπεριλαμβάνουν την διεύθυνση του αποστολέα, του παραλήπτη, το port που απαντά η υπηρεσία κλπ. Έτσι μπορούν να δημιουργηθούν λίστες με κανόνες που πρέπει να ικανοποιούνται για να μπορεί να γίνει προσπέλαση ενός εξυπηρετητή ή μιας υπηρεσίας.

4. Η αποστρατικοποιημένη ζώνη (Demilitarized Zone-DMZ): είναι ένα κρίσιμο συστατικό του δικτύου που βρίσκεται ανάμεσα στο ιδιωτικό δίκτυο που προφυλάσσει το firewall και το διαδίκτυο. Είναι μία περιοχή που ανήκει μεν στην εσωτερική δομή του δικτύου μας, αλλά οι κόμβοι του δεν απολαμβάνουν την εμπιστοσύνη που έχουν οι κόμβοι του υπόλοιπου δικτύου. 0 σκοπός της ζώνης αυτής είναι στρατηγικής σημασίας για την ασφάλεια του δικτύου μας και επιτρέπει στην ουσία την προσπέλαση σε κόμβους και υπηρεσίες του εσωτερικού δικτύου. Οι εξωτερικοί χρήστες του διαδικτύου μπορούν να προσπελάσουν μόνο τους κόμβους της ζώνης αυτής, ενώ αυτοί μπορούν να προσπελάσουν και κόμβους του εσωτερικού δικτύου.

Σε περίπτωση επίθεσης ο hacker θα πρέπει να αντιμετωπίσει και δεύτερο «τείχος» άμυνας.

5. Proxy**:** Όταν ένας εξυπηρετητής δρα σαν να ήταν κάποιος άλλος. Για παράδειγμα ένας κόμβος που μπορεί να φέρει μία σελίδα από το διαδίκτυο πρέπει να στηθεί σαν proxy server και ένας κόμβος που ζητά την σελίδα αυτή αλλά βρίσκεται στο εσωτερικό του δικτύου πρέπει να στηθεί σαν proxy client. Με τον τρόπο αυτό όταν ένας κόμβος από το εσωτερικό μας δίκτυο ζητά μία σελίδα από το διαδίκτυο, ο proxy server την ζητά για λογαριασμό του client και την παραδίδει σε αυτόν. Με τον τρόπο αυτό μόνο οι proxy servers έρχονται σε επικοινωνία με το διαδίκτυο, ενισχύοντας την ασφάλεια του εσωτερικού μας δικτύου.

Η καταλληλότερη στο πρόβλημα της ασφάλειας σπάνια είναι μία μόνο τεχνολογία ή μία συσκευή. Συνήθως αποτελείται από προσεκτική επιλογή και συνδυασμό διαφορετικών τεχνολογιών και συσκευών που επιλύουν διαφορετικά προβλήματα [5].

Η λειτουργία των firewalls μπορεί να είναι ένα ή περισσότερα από τα ακόλουθα: Packet-filtering router, Application-level gateway (ή proxy server).

Δρομολογητές φιλτραρίσματος πακέτων (Packet-Filtering Routers)

Αυτό που γίνεται αντιληπτό πιο εύκολα σε ένα firewall είναι η λειτουργία που σχετίζεται με ένα filtering router. Ένας δρομολογητής κινεί δεδομένα από και προς ένα ή περισσότερα δίκτυα. Ένας κανονικός δρομολογητής παίρνει ένα πακέτο από ένα δίκτυο «Α» και το δρομολογεί προς τον προορισμό του ένα δίκτυο «Β». Ένας δρομολογητής φιλτραρίσματος (filtering router) κάνει ακριβώς το ίδιο με ένα απλό δρομολογητή, επιπλέον όμως αποφασίζει για το αν θα δρομολογήσει ή όχι ένα πακέτο. Αυτό επιτυγχάνεται με την εγκατάσταση κάποιων φίλτρων βάση των

οποίων ο δρομολογητής αποφασίζει για το τι θα κάνει με οποιοδήποτε πακέτο φτάνει σε αυτόν.

Επιπλέον στοιχεία που θα πρέπει να λαμβάνονται υπόψη, ώστε να κατασκευάσουμε ένα ασφαλές filtering πλάνο, είναι αν ο δρομολογητής επαναπροσδιορίζει τις εντολές φιλτραρίσματος και αν είναι δυνατή η εφαρμογή φίλτρων για εισερχόμενα ή εξερχόμενα πακέτα σε κάθε διεπαφή (interface). Ένα άλλο σημαντικό θέμα είναι η ικανότητα ανάπτυξης φίλτρων που βασίζονται σε επιλογές του IP header και στον τεμαχισμό των πακέτων. Η κατασκευή ενός καλού φίλτρου είναι πολύ δύσκολη και απαιτείται η πλήρης κατανόηση των πρωτοκόλλων που θέλουμε να φιλτράρουμε.

Ένας δρομολογητής φιλτραρίσματος πακέτων παίρνει αποφάσεις για το αν θα περάσει ή όχι το κάθε πακέτο. Ο δρομολογητής εξετάζει το κάθε datagram για να αποφασίσει αν ταιριάζει με κάποιον από τους κανόνες φιλτραρίσματος των πακέτων. Οι πληροφορίες είναι η IP αποστολέα, IP παραλήπτη, (TCP, UDP, ICMP, ή IPTunnel), το TCP/UDP port προέλευσης, το TCP/UDP port προορισμού. [8]

Πύλες εφαρμογών (Application level gateways)

Οι πύλες εφαρμογών επιτρέπουν στον διαχειριστή, να υλοποιήσει μία αυστηρότερη πολιτική ασφάλειας. Στο σύστημα εγκαθίστανται proxies των εφαρμογών που επιτρέπουν την προσπέλαση σε εξωτερικούς χρήστες μόνο μέσα από αυτές, ενώ κάθε άλλη χρήση αποτρέπεται από το firewall. Οι χρήστες επιτρέπεται να προσπελαύνουν τις υπηρεσίες του gateway αλλά δεν επιτρέπεται να κάνουν Login σε αυτόν. Για την καλύτερη ασφάλεια του δικτύου τα φίλτρα περιορίζουν την πρόσβαση δυο συνδεδεμένων δικτύων σε ένα μόνο host ο οποίος λέγεται bastion host. Για να φτάσει κάποιο πακέτο στο δευτερεύον δίκτυο θα πρέπει να περάσει από το bastion host. Έτσι περιορίζεται ο αριθμός των άμεσα προσπελάσιμων κόμβων των δικτύων με αποτέλεσμα να επιτυγχάνεται περισσότερη ασφάλεια. Στην περίπτωση αυτή οι υπηρεσίες προωθούνται ξανά από τον bastion host

Οι proxy servers χρησιμοποιούνται προκειμένου να έχουμε πρόσβαση στα δεδομένα με ασφαλή τρόπο. Διάφορες εφαρμογές συγκεντρώνονται σε μια μηχανή, η μηχανή αυτή αποτελεί το βασικό κόμβο (bastion host) που λειτουργεί σαν proxy server για διάφορες υπηρεσίες όπως (Telnet, SMTP, FTP, HTTP κ.α.). Παρόλα αυτά είναι δυνατό να χρησιμοποιούνται διαφορετικοί host για καθεμία από τις παραπάνω υπηρεσίες. Σε αυτή την περίπτωση ο πελάτης αντί να συνδέεται απευθείας με έναν εξωτερικό server συνδέεται με τον proxy server, ο οποίος με τη σειρά του συνδέεται με τον εξωτερικό server.

Από τη χρήση ενός proxy server είναι δυνατό να αποκομιστούν σημαντικά οφέλη. Καταρχήν είναι δυνατή η προσθήκη μιας λίστας ελέγχου προσπέλασης (access control list) για τις διάφορες υπηρεσίες, απαιτώντας από τους χρήστες και τα συστήματα κάποια μορφή πιστοποίησης (authentication) προ ιού τους επιτραπεί πρόσβαση σε κάποια από τις υπηρεσίες. Υπάρχουν επίσης και οι «έξυπνοι» proxy servers που λέγονται Application Layer Gateways (ALGs), οι οποίοι μπορούν να μπλοκάρουν συγκεκριμένα τμήματα (subsections) ενός πρωτοκόλλου. Για παράδειγμα ένας ALG για FTP μπορεί να διαχωρίζει την εντολή "put" από την εντολή "get". Έτσι ένας οργανισμός μπορεί να επιτρέπει στους χρήστες του να «κατεβάζουν» αρχεία αλλά να μην αφήνει τους έξω να παίρνουν τα αρχεία των δικών του συστημάτων.

Επίσης, οι proxy servers μπορούν να διαμορφωθούν με τέτοιο τρόπο ώστε να κωδικοποιούνται οι ροές των δεδομένων με βάση διάφορες παραμέτρους. Τέτοιες δυνατότητες μπορούν να χρησιμοποιηθούν από οργανισμούς για να επιτύχουν ασφαλή διασύνδεση των sites τους μέσω του Διαδικτύου.

Τα πλεονεκτήματα αυτού του τύπου είναι η μεγαλύτερη ασφάλεια αφού τα συστήματα αυτά «τρέχουν» μειωμένο σετ εφαρμογών και ένα ασφαλές λειτουργικό σύστημα. Η προσπέλαση στα εσωτερικά συστήματα γίνεται μόνο από τον proxy εμποδίζοντας έτσι την απευθείας σύνδεση. Οι κανόνες φιλτραρίσματος είναι αρκετά

πιο εύκολοι να υλοποιηθούν και να εξακριβωθούν για την ορθότητά τους. Το μεγαλύτερο μειονέκτημα είναι πως πρέπει οι χρήστες να αλλάξουν την συμπεριφορά τους ή να στηθεί εξειδικευμένο λογισμικό που θα δίνει μεγαλύτερη ευελιξία στους εσωτερικούς χρήστες χωρίς να μειώνεται η προσφερόμενη ασφάλεια.

Υβριδικά Συστήματα

Ο συνδυασμός ίων δύο περιπτώσεων οδηγεί σε καλύτερα αποτελέσματα και συνήθως η υλοποίηση περιλαμβάνει και packet filtering και proxy applications. Τα firewalls εκτός από την ιδιότητα που έχουν να διαφυλάσσουν ένα δίκτυο από διάφορους τρίτους δίνουν δυνατότητα πρόσβασης από απόσταση στους νόμιμους χρήστες του. Το καλύτερο firewall σε ένα δίκτυο επιτυγχάνεται με το συνδυασμό δυο screening routers με ένα ή περισσότερους proxy servers που τοποθετούνται ανάμεσα στους δυο routers. Με την μέθοδο αυτή ο εξωτερικός router εμποδίζει την μη εξουσιοδοτημένη πρόσβαση σε επίπεδο IP (IP spoofing, source routing, packet fragments) ενώ επιτρέπει στον proxy server να παρέχει ασφάλεια στα πρωτόκολλα υψηλότερων επιπέδων. Ο σκοπός του εσωτερικού router είναι να μπλοκάρει όλη την κίνηση εκτός από αυτή του proxy server.

Πολλά firewalls είναι δυνατό να κρατάνε log file για την ενημέρωση των διαχειριστών. Πολλές φορές οι εισβολείς προσπαθούν να παραποιήσουν τα log file. Είναι λοιπόν σκόπιμο να διαφυλάσσονται αυτές οι πληροφορίες. Για το σκοπό αυτό υπάρχουν διάφορες μέθοδοι όπως:

- Μονή εγγραφή (Write-once)

- Μονή εγγραφή-πολλαπλή ανάγνωση (WORM drives)

- Paper logs

- Κεντρικός έλεγχος του logging μέσα από χρήσιμα εργαλεία όπως το syslog.

Διαφύλαξη της πληροφορίας που κρατείται μέσω log με την σύνδεση μέσω σειριακής θύρας σε ένα υπολογιστή που κρατά το Log σε αρχείο.

3.6. Υπηρεσίες για την Ασφάλεια

Προκειμένου να ασφαλιστεί ένα δίκτυο υπάρχουν κάποια βασικά σημεία τα οποία θα πρέπει να μελετηθούν και να υλοποιηθούν. Θα πρέπει να καταβάλλεται προσπάθεια για την προστασία όλων των κρίσιμων στοιχείων του δικτύου. Πολλοί διαχειριστές ασχολούνται μόνο με την ασφάλεια των κόμβων. Προτιμάται να προστατεύονται μόνο οι κόμβοι για δύο λόγους:

1. είναι κάτι που μπορεί να επιτευχθεί εύκολα

2. οι hosts είναι τα «στοιχεία» του δικτύου που δέχονται τις περισσότερες επιθέσεις

Παρόλα αυτά είναι εξίσου σημαντική η προστασία όλων των συσκευών του δικτύου. Αν το δίκτυο είναι «ανοιχτό» σε τρίτους, μπορεί κάποιος να αλλάξει την δρομολόγηση των πακέτων και να υποκλέψει κρίσιμη πληροφορία (π.χ. passwords). Μπορεί επίσης να έχει πρόσβαση στο σύστημα διαχείρισης του δικτύου ή σε διάφορες υπηρεσίες του όπως (DNS, NFS, NTP, WWW).

Ένας άλλος παράγοντας που θα πρέπει να λαμβάνεται υπόψη είναι το ανθρώπινο λάθος. Κάποιος διαχειριστής μπορεί να μην κάνει σωστή διαμόρφωση ενός κόμβου, με αποτέλεσμα η προβληματική λειτουργία να επηρεάζει τους χρήστες που

χρησιμοποιούν τον συγκεκριμένο host. Το πρόβλημα αυξάνεται όταν γίνει λάθος configuration σε κάποια βασική συσκευή (π.χ. router), όπου επηρεάζονται άμεσα όλοι οι χρήστες του δικτύου.

Υπάρχουν κάποια κλασικά προβλήματα τα οποία κάνουν τρωτό ένα δίκτυο. Ένα από αυτά είναι η μη διαθεσιμότητα της υπηρεσίας μετά από κάποια επίθεση. Στην περίπτωση αυτή δεν είναι δυνατή η μεταφορά δεδομένων. Ένα δίκτυο έρχεται στην κατάσταση αυτή με δύο τρόπους:

1. Επίθεση στους δρομολογητές.

2. Συμφόρηση (flooding) του δικτύου.

Στο σημείο αυτό θα πρέπει να επισημανθεί ότι με τον όρο δρομολογητής εκτός από τις κλασσικές συσκευές δρομολόγησης εννοούνται και «στοιχεία» όπως firewalls, proxy servers κ.α. Η επίθεση σε ένα δρομολογητή έχει σκοπό τη διακοπή της μεταφοράς των πακέτων ή την προώθηση τους σε λάθος σημείο. Σε αυτήν την κατάσταση μπορεί να βρεθεί ένας δρομολογητής όταν δεν έχει σωστό configuration ή όταν Βομβαρδίζεται με πακέτα που δεν προλαβαίνει να δρομολογήσει με αποτέλεσμα να μειώνεται σταδιακά η απόδοσή του.

Η συμφόρηση ενός δικτύου διαφέρει από αυτή του δρομολογητή γιατί τα πακέτα απευθύνονται σε όλες τις συσκευές του δικτύου (broadcast). Η «ιδανική» συμφόρηση επιτυγχάνεται όταν ένα πακέτο πηγαίνει σε όλους τους κόμβους του δικτύου οι οποίοι το στέλνουν πάλι ή δημιουργούν προβληματικά πακέτα τα οποία συλλέγονται από τους hosts που με τη σειρά τους τα προωθούν ξανά.

Ένα άλλο κλασικό πρόβλημα είναι αυτό του spoofing (υποκλοπή της πληροφορίας). Στην περίπτωση του spoofing τα πακέτα, προτού φτάσουν στον παραλήπτη, περνούν από κάποιον ενδιάμεσο host. Η διάγνωση του spoofing είναι

γενικά δύσκολη, γιατί τις περισσότερες φορές η πληροφορία που φτάνει στον παραλήπτη *δεν* αλλοιώνεται.

Για την επίλυση των προαναφερόμενων προβλημάτων χρησιμοποιούνται γνωστά πρωτοκόλλα όπως το RIP-2 και το OSPF.

Με τη χρήση password επιτυγχάνεται η ελάχιστα απαιτούμενη προστασία του δικτύου αφού δεν είναι δυνατή η άμεση πρόσβαση στους πόρους του από κάποιον τρίτο. Υπάρχουν τα ακόλουθα επίπεδα προστασίας:

- Clear text password
- Cryptographic checksum
- Encryption

Με τη χρήση συνθηματικών δεν επιβαρύνονται η CPU και το bandwidth. Με τον έλεγχο ισοτιμίας (checksum) δεν είναι δυνατό να περάσουν πακέτα που δεν ανήκουν στο δίκτυο ακόμη και όταν ο εισβολέας έχει άμεση πρόσβαση στους πόρους του δικτύου. Η καλύτερη προστασία του δικτύου επιτυγχάνεται με την κρυπτογράφηση όλης της πληροφορίας καθώς και των routing updates. Με τον τρόπο αυτό ένας εισβολέας είναι δύσκολο να καταλάβει την τοπολογία του δικτύου. Το μειονέκτημα της κρυπτογράφησης είναι το overhead που έχουμε κατά την διαδικασία των updates.

Τόσο το RIP-2 όσο και το OSPF υποστηρίζουν την χρήση των συνθηματικών (clear text password). Ορισμένες φορές είναι δυνατόν να υποστηρίζουν και MD5 κρυπτογράφηση. Δυστυχώς δεν υπάρχει ακόμη σίγουρη προστασία σε περιπτώσεις συμφόρησης του δικτύου. Το θετικό στην περίπτωση αυτή είναι ότι η συμφόρηση είναι άμεσα εμφανής και μπορεί να αντιμετωπιστεί με σχετικά απλούς τρόπους.

Σε περίπτωση που μας ενδιαφέρει η διασύνδεση επιχειρήσεων, οργανισμών, καταναλωτών και πελατών πρέπει να υπάρχει ένα είδος συνεννόησης για τα standards που θα χρησιμοποιηθούν στην επέκταση του επιχειρηματικού δικτύου μέχρι τον πελάτη. Τα standards που έχουν συμφωνηθεί αφορούν διαμορφώσεις των firewalls, μηχανισμούς ψηφιακής πιστοποίησης, πρακτικές διακίνησης εφαρμογών και δομές για την ανταλλαγή δεδομένων. Όλο και περισσότερες εταιρίες εγκαταλείπουν τα ιδιόκτητα κλειστά πρωτόκολλα και εφαρμογές και υιοθετούν τα συνήθη ανοικτά πρωτόκολλα του Internet, με τα οποία μπορούν να παρέχουν σελίδες στο διαδίκτυο, δυνατότητα ηλεκτρονικού ταχυδρομείου για συνεργασία με τους πελάτες τους, να κάνουν χρήση client-server εφαρμογών.

Προσπαθώντας να οδηγήσουμε το δίκτυο στο επόμενο επίπεδο ασφάλειας, έχουμε σαν σύμμαχους την τεχνολογία του διαδικτύου και τα ανοικτά πρωτόκολλα. Επιπλέον υπάρχουν πολλά είδη υπηρεσιών που προσφέρονται καθεμία με τις δικές της απαιτήσεις για ασφάλεια. Για παράδειγμα μία υπηρεσία που χρησιμοποιείται μόνο εσωτερικά σε ένα site (π.χ. NFS) μπορεί να απαιτεί διαφορετικούς μηχανισμούς προστασίας από μια άλλη που χρησιμοποιείται για πρόσβαση από εξωτερικούς χρήστες.

Πολλές φορές ο αποκλεισμός των εξωτερικών προσπελάσεων σε ένα εξυπηρετητή μπορεί λόγω της φύσης της προσφερόμενης υπηρεσίας να αρκεί. Παρόλα αυτά ένας εξυπηρετητής παγκόσμιου ιστού (Web Server), ο οποίος είναι προσπελάσιμος από όλο τον κόσμο, απαιτεί εσωτερική προστασία. Αυτό σημαίνει ότι η υπηρεσία, τα πρωτόκολλα επικοινωνίας και ο εξυπηρετητής πρέπει να προστατεύονται με τέτοιο τρόπο ώστε να αποφεύγεται οποιαδήποτε μη επιτρεπτή πρόσβαση και τροποποίηση των αρχείων από τα οποία αντλείται η προς δημοσίευση πληροφορία.

Από τα παραπάνω φαίνεται ότι οι υπηρεσίες που παρέχονται εσωτερικά πρέπει να διαφοροποιούνται από αυτές που παρέχονται εξωτερικά, γιατί έχουν διαφορετικές απαιτήσεις προστασίας. Αυτό σημαίνει ότι οι δύο αυτοί τύποι των υπηρεσιών

πρέπει να είναι εγκατεστημένες ανεξάρτητα σε διαφορετικούς εξυπηρετητές. Ορισμένες φορές, προκειμένου να επιτευχθεί καλύτερο επίπεδο ασφάλειας, σε κάποια sites ορίζονται ακόμη και διαφορετικά υποδίκτυα -άλλα προσβάσιμα από τους εσωτερικούς χρήστες και άλλα προ- σβάσιμα από οποιονδήποτε- για την παροχή των υπηρεσιών αυτών. Στις περιπτώσεις αυτές, πολλές φορές υπάρχει κάποιο firewall το οποίο ενώνει τα διαφορετικά υποδίκτυα. Ιδιαίτερη προσοχή πρέπει να δοθεί στην κατάλληλη λειτουργία του firewall.

Σε μεγάλους οργανισμούς παρατηρείται το φαινόμενο να υπάρχει αυξανόμενο ενδιαφέρον για τη χρήση intranets, μέσω των οποίων επιτυγχάνεται η διασύνδεση διαφορετικών τμημάτων ενός οργανισμού (π.χ. τομείς μιας εταιρείας). Μολονότι υπάρχει μία γενική διαφοροποίηση ανάμεσα σε εξωτερικές και εσωτερικές υπηρεσίες, τα sites, που χρησιμοποιούν intranets θα πρέπει να λαμβάνουν υπόψη ότι πρόκειται για μία υπηρεσία που δε θα είναι δημόσια, ούτε τόσο αποκλειστικά ιδιωτική. Επομένως, μια τέτοια υπηρεσία χρειάζεται το δικό της σύστημα για να την υποστηρίζει, το οποίο θα είναι διαφοροποιημένο από τα συστήματα υποστήριξης των εξωτερικών και εσωτερικών υπηρεσιών.

Ένας τύπος εξωτερικών υπηρεσιών που χρήζει ιδιαίτερης αναφοράς, είναι αυτός των υπηρεσιών που επιτρέπουν ανώνυμη πρόσβαση. Τέτοιες υπηρεσίες είναι το ανώνυμο ftp και η μη- πιστοποιημένη πρόσβαση. Είναι εξαιρετικά σημαντικό να διασφαλιστεί ότι οι εξυπηρετητές αυτών των υπηρεσιών είναι προσεκτικά απο- μονωμένοι από τους υπόλοιπους εξυπηρετητές και ότι στα συστήματα αρχείων δε θα πρέπει να έχουν πρόσβαση εξωτερικοί χρήστες.

Επίσης, ιδιαίτερη μνεία χρειάζεται να γίνει για τις υπηρεσίες ανώνυμης πρόσβασης που δίνουν δικαιώματα εγγραφής στους χρήστες. Επειδή το site που φιλοξενεί μια υπηρεσία είναι υπεύθυνο για το περιεχόμενο των πληροφοριών που δημοσιεύει, απαιτείται προσεκτική παρακολούθηση της πληροφορίας που εισάγουν οι ανώνυμοι χρήστες.

Οι πιο δημοφιλείς υπηρεσίες στην κοινωνία των δικτύων και του Διαδικτύου είναι οι: name service, password key service, authentication / proxy server, electronic mail, www, file transfer & NFS. Εφόσον αυτές είναι οι πιο συχνά χρησιμοποιούμενες υπηρεσίες είναι και τα πιο προφανή σημεία επίθεσης. Επιπλέον, πρέπει να τονιστεί ότι μία επιτυχημένη επίθεση σε μία από αυτές τις υπηρεσίες μπορεί να επιφέρει γενικότερα προβλήματα.

3.7. Πρωτόκολλα για την Ασφάλεια

IPsec

Ο αρχικός σχεδιασμός του IPv4 δεν είχε λάβει υπόψη ίου κανένα θέμα ασφάλειας λόγω της φύσης του δικτύου (επιδίωκε να συνδέσει ακαδημαϊκά ιδρύματα). Μετά την τεράστια εξάπλωση όμως που γνώρισε το διαδίκτυο και τη σημασία που απέκτησε στον τομέα των επιχειρήσεων και του ηλεκτρονικού εμπορίου η ασφάλεια έγινε ένα από τα πιο απαιτητικές ανάγκες στο διαδίκτυο. Για να καλύψει τις ανάγκες αυτές η IETF δημιούργησε το IP Security Working Group με στόχο να σχεδιάσει μία αρχιτεκτονική ασφαλείας και τα αντίστοιχα πρωτόκολλα ώστε να παρέχεται ασφάλεια βασισμένη στην κρυπτογραφία για το IPv6 πρωτόκολλο. Η αρχιτεκτονική αυτή είναι γνωστή και ως IPsec και περιγράφεται στο RFC 182565.

Η ασφάλεια επιτυγχάνεται αν έχουν επιτευχθεί οι παρακάτω στόχοι:

1. Πιστοποίηση παραλήπτη: Αφορά τη δυνατότητα ελέγχου των δεδομένων και της πιστοποίησης ότι ο αποστολέας που μετέδωσε αυτά τα δεδομένα είναι αυτός που φαίνεται στο αντίστοιχο πεδίο του πακέτου.

2. Ακεραιότητα δεδομένων: Αφορά τη δυνατότητα ελέγχου των δεδομένων και πιστοποίησης ότι αυτά δεν έχουν αλλαχθεί κατά τη μετάδοσή τους από τον αποστολέα στον παραλήπτη.

3. Δυνατότητα απορρήτου: Αφορά τη δυνατότητα μετάδοσης των δεδομένων με τέτοιο τρόπο ώστε να μπορούν να διαβαστούν μόνο από τον ορισμένο παραλήπτη και όχι από τους ενδιάμεσους κόμβους στο μονοπάτι από τον αποστολέα στον παραλήπτη.

Η πιστοποίηση και η ακεραιτότητα είναι συχνά στενά συνδεμένες ενώ η δυνατότητα του απορρήτου της μηνύματος επιτυγχάνεται με χρήση κωδικοποίησης με δημόσια κλειδιά, μία μέθοδο με την οποία εξασφαλίζεται ταυτόχρονα και η πιστοποίηση του αποστολέα.

Το πιο σημαντικό πρόβλημα με την ασφάλεια στο διαδίκτυο είναι το γεγονός ότι πρόκειται για ένα εντελώς ανοιχτό δίκτυο, όπου τα πακέτα θα πρέπει να περάσουν από διάφορους κόμβους για τους οποίους κανείς δεν μπορεί να εγγυηθεί. Έτσι πιθανά είναι να υπάρχουν διάφοροι ανιχνευτές - υποκλοπείς πακέτων (packet sniffers). Ένα τέτοιο περιβάλλον είναι πολύ δύσκολο να ασφαλιστεί έστω και με τη χρήση κωδικοποιήσεων και ψηφιακών υπογραφών. Η ασφάλεια θα πρέπει να αντιμετωπίζει και θέματα όπως οι επιθέσεις τύπου Denial Of Service, όπου στόχος είναι η δέσμευση όλων των διαθέσιμων πόρων μίας υπηρεσίας ώστε αυτή να μην μπορεί να δοθεί σε άλλους χρήστες, ή οι επιθέσεις τύπου Spoofing, όπου έχει γίνει αλλαγή της διεύθυνσης του αποστολέα ενός πακέτου.

Το IPsec πρότυπο καθορίζει τα πρότυπα ασφάλειας τα οποία μπορούν να χρησιμοποιηθούν από το IP πρωτόκολλο ανεξαρτήτως έκδοσης ώστε να επιτυγχάνεται ασφάλεια στο επίπεδο δικτύου. Ένα σύστημα χρησιμοποιεί το IPsec για να απαιτήσει από τους κόμβους που επικοινωνεί να κάνουν χρήση συγκεκριμένων

αλγορίθμων και πρωτοκόλλων ασφαλείας.Οι υπηρεσίες που μπορούν να θεωρηθούν μέρος του IPsec περιλαμβάνουν [8]:

1. Έλεγχο πρόσβασης: Η πρόσβαση σε οποιαδήποτε υπηρεσία ή σύστημα απαιτεί τον κατάλληλο κωδικό. Υπάρχουν διάφορα πρωτόκολλα ασφάλειας που μπορούν να χρησιμοποιηθούν για να ορίσουν μία ασφαλή ανταλλαγή κλειδιών.

2. Ακεραιότητα δεδομένων: Είναι δυνατή η πιστοποίηση ακεραιότητας ενός οποιουδήποτε IP πακέτου χωρίς την ανάγκη να ελεγχθεί άλλο πακέτο πριν ή μετά από το πακέτο που πρέπει να ελεγχθεί. Αυτό μπορεί να επιτευχθεί με χρήση τεχνικών hashing.

3. Πιστοποίηση ίου αποστολέα: Είναι δυνατή η πιστοποίηση του αποστολέα με χρήση των κατάλληλων αλγορίθμων ψηφιακών υπογραφών.

4. Προστασία εναντίον επιθέσεων τύπου packet replay: Παρέχονται μηχανισμοί προστασίας του κόμβου αποστολέα από επιθέσεις όπου ο επιτιθέμενος προσπαθεί να βλάψει τη διαθεσιμότητα του συστήματος, υποκλέπτοντας ένα πακέτο και στέλνοντάς το πολλές φορές στον αποστολέα.

5. Κωδικοποίηση ίων δεδομένων: Παρέχονται μηχανισμοί κωδικοποίησης για να εξασφαλιστεί το απόρρητο των δεδομένων.

6. Εξασφάλιση απορρήτου της ροής ίων δεδομένων. Παρέχονται μηχανισμοί προστασίας της ροής των πακέτων ώστε ο επιτιθέμενος να μην μπορεί να βγάλει συμπεράσματα παρακολουθώντας ένα προς ένα τα πακέτα (που μπορεί να είναι κωδικοποιημένα).

Εξυπηρετητής Ονοματολογίας DNS

Στο Διαδίκτυο η υπηρεσία DNS χρησιμοποιείται για την αντιστοίχηση διευθύνσεων στο δίκτυο IP σε ονόματα υπολογιστών. Οι υπηρεσίες NIS και NIS+ δε χρησιμοποιούνται στο Διαδίκτυο, αλλά υπόκεινται στους ίδιους κινδύνους με αυτούς ενός DNS εξυπηρετητή. Η αντιστοίχηση ενός ονόματος σε μία διεύθυνση είναι κρίσιμη για την ασφαλή λειτουργία ενός δικτύου. Ένας εισβολέας που μπορεί να ελέγξει επιτυχώς ή να απενεργοποιήσει ένα DNS εξυπηρετητή (DNS spoofing), μπορεί να επαναδρομολογήσει τη ροή των πακέτων και να υπονομεύσει τους μηχανισμούς ασφαλείας. Για παράδειγμα η κίνηση ενός δρομολογητή μπορεί να εκτραπεί προς ένα ξένο σύστημα ή οι χρήστες μπορούν να εξαπατηθούν και να παρέχουν πληροφορίες πιστοποίησης.

Ένας οργανισμός θα πρέπει να δημιουργεί προστατευμένους κόμβους στα sites για να ενεργούν σαν δευτερεύοντες name servers και να προστατεύουν τους βασικούς DNS servers από επιθέσεις με τη χρήση filtering routers. Μια υπηρεσία DNS γενικά είναι δύσκολο να προστατευτεί και το αποτέλεσμα σε μια αίτηση δεν είναι δυνατόν να ελεγχθεί αν έχει τροποποιηθεί ή αλλοιωθεί από κάποιον τρίτο. Μια μέθοδος για την προστασία των DNS υπηρεσιών είναι η ενσωμάτωση ψηφιακών υπογραφών (digital signature) στο πρωτόκολλο, που όταν εφαρμόζεται επιτρέπει τον έλεγχο της ακεραιότητας της πληροφορίας χρησιμοποιώντας κρυπτογράφηση [8].

Παγκόσμιος Ιστός (www)

Υπάρχει μία εκθετική αύξηση των εξυπηρετητών παγκόσμιου ιστού που οφείλεται στην ευκολία της χρήσης τους καθώς και στην ικανότητα που έχουν να συγκεντρώνουν υπηρεσίες παροχής πληροφοριών. Ορισμένοι χρήστες που προσπελαύνουν αυτούς τους εξυπηρετητές είναι δυνατό να εκτελέσουν κάποιες λειτουργίες όπως για παράδειγμα όταν επιθυμούν να κάνουν μία αίτηση, ο

εξυπηρετητής για να ανταποκριθεί στις απαιτήσεις της αίτησης πρέπει εκτελέσει κάποιο πρόγραμμα. Ορισμένοι προγραμματιστές που υλοποιούν αυτά τα προγράμματα δε λαμβάνουν τα απαιτούμενα μέτρα ασφαλείας γι' αυτές τις περιπτώσεις, με αποτέλεσμα να κάνουν το σύστημα ευάλωτο σε εξωτερικές επιθέσεις. Όταν κάποιος υπολογιστής φιλοξενεί έναν εξυπηρετητή παγκόσμιου ιστού, δε θα πρέπει να φυλάσσονται απόρρητες πληροφορίες σε αυτό το μηχάνημα.

Σε πολλά sites χρησιμοποιείται ο ίδιος υπολογιστής σαν FTP εξυπηρετητής ή WWW εξυπηρετητής. Στην περίπτωση αυτή θα πρέπει ο FTP εξυπηρετητής να απαντά μόνο σε «get» αιτήσεις, διαφορετικά (αιτήσεις put) είναι δυνατό να αντικαταστήσουν αρχεία του εξυπηρετητή web.

Μεταφορά Αρχείων (File transfer, FTP, TFTP)

Το FTP όπως και το TFTP προσφέρουν υπηρεσίες μεταφοράς αρχείων. Το FTP απαιτεί πιστοποίηση (authentication), ενώ το TFTP όχι. Για το λόγο αυτό είναι καλό να αποφεύγεται το TFTP. Οι FTP εξυπηρετητές που δεν έχουν σωστή διαμόρφωση (configuration), δίνουν την δυνατότητα σε εισβολείς να αντιγράφουν, να αντικαθιστούν ή να σβήνουν αρχεία του υπολογιστή που φιλοξενεί την εν λόγω υπηρεσία. Από τα πιο συνηθισμένα φαινόμενα που μπορεί να παρουσιαστούν σε έναν εξυπηρετητή με λάθος διαμόρφωση είναι η πρόσβαση σε κρυπτογραφημένα αρχεία password και ιδιωτικά αρχεία, καθώς και η εισαγωγή Δούρειων Ίππων (Trojan Horses).

Μία βασική αρχή για την ασφάλεια ενός δικτύου είναι ότι «Οι υπηρεσίες που προσφέρονται εσωτερικά σε ένα site δε θα πρέπει να συνυπάρχουν με τις υπηρεσίες που προσφέρονται εξωτερικά». Το TFTP δεν παρέχει καμία απολύτως ασφάλεια, είναι μία υπηρεσία για εσωτερική και μόνο χρήση και θα πρέπει να είναι πολύ καλά ορισμένη (μέσω του TFTP εξυπηρετητή να επιτρέπεται πρόσβαση μόνο σε

προκαθορισμένα αρχεία). Ένας TFTP εξυπηρετητής χρησιμοποιείται κυρίως για να γίνονται download τα αρχεία για τη διαμόρφωση των Δρομολογητών

Δικτυακές Υπηρεσίες Αρχειοθέτησης NFS

Το NFS (Network File Service) δίνει τη δυνατότητα σε διάφορους hosts να διαμοιράζονται κοινούς δίσκους. Το NFS χρησιμοποιείται συχνά από υπολογιστές οι οποίοι δεν έχουν σκληρούς δίσκους αλλά εξαρτώνται από κάποιο disk server. Το NFS δεν έχει ενσωματωμένο σύστημα ασφάλειας. Ένας εξυπηρετητής συνιστάται να είναι προσπελάσιμος μόνο από τους υπολογιστές που χρησιμοποιούν τις υπηρεσίες του. Αυτό μπορεί να επιτευχθεί με τον προσδιορισμό του υπολογιστή του οποίου το σύστημα αρχείων είναι προσπελάσιμο και με ποια δικαιώματα, (π.χ. read-only, read-write κ.α.). Η διαμοίραση των συστημάτων αρχείων είναι μια υπηρεσία που πρέπει να προσφέρεται μόνο εσωτερικά σε ένα δίκτυο. Γενικά, η εξωτερική πρόσβαση στο διαμοιραζόμενο σύστημα αρχείων μπορεί να περιοριστεί με τη χρήση Firewalls.

LDAP (Lightweight Directory Access Protocol)

Αυτό το πρότυπο δίνει την δυνατότητα για την καταχώρηση, αποθήκευση και διανομή πληροφοριών επικοινωνίας (contact information), ψηφιακής πιστοποίησης (digital certification), δεδομένων διαμόρφωσης συσκευών (configuration data), κατάσταση εξυπηρετητών (server state information). Με την χρήση αυτού του πρωτοκόλλου είναι δυνατή η προσπέλαση των χρηστών σε εφαρμογές και υπολογιστές, μέσω του διαδικτύου με πιστοποίηση της ταυτότητάς του. Τα κύρια πλεονεκτήματα του είναι τα παρακάτω:

1. Οι χρήστες μπορούν να αναζητήσουν πληροφορίες για επικοινωνία με στελέχη επιχειρήσεων με τον ίδιο τρόπο που το κάνουν οι εργαζόμενοι στην επιχείρηση.

2. Υπάρχει τυποποιημένος τρόπος για την αποθήκευση και ανταλλαγή στοιχείων και δεδομένων όπως των X.509 ψηφιακών πιστοποιητικών και των S/MIME πληροφοριών.

3. Υπάρχει η δυνατότητα για την ασφαλή αντιγραφή των πληροφοριών και σε άλλους εξυπηρετητές συνεργαζόμενων δικτύων.

4. Επιτρέπει οι εφαρμογές extranet να μπορούν με ένα αξιόπιστο και ταχύ τρόπο να κάνουν ερωτήσεις σε δομημένη πληροφορία.

3.8. Ενίσχυση της Ασφάλειας

Μια κλασική διαδικασία που εφαρμόζεται σε υπολογιστικά συστήματα είναι αυτή της λήψης αντιγράφων ασφαλείας. Για να είναι σωστός ο σχεδιασμός που γίνεται για την ασφάλεια ενός site, η διαδικασία λήψης αντιγραφών θα πρε'πει να αποτελεί αναπόσπαστο κομμάτι του. Κατά την δημιουργία αντιγράφων ασφαλείας θα πρέπει να λαμβάνονται υπόψη τα ακόλουθα:

1. Να είναι δυνατή η δημιουργία αντιγράφων ασφαλείας.

2. Τα αντίγραφα θα πρέπει να αποθηκεύονται off-site. Ο αποθηκευτικός χώρος θα πρέπει να επιλέγεται προσεκτικά σύμφωνα με τα ακόλουθα κριτήρια: την ασφάλεια και τη διαθεσιμότητα του.

3. Προκειμένου να έχουμε επιπρόσθετη ασφάλεια τα αντίγραφα θα πρέπει να κρυπτογραφούνται. Η ανάκτηση της πληροφορίας θα πρέπει να είναι δυνατή από οποιαδήποτε σημείο οποιαδήποτε στιγμή. Επίσης άμεσα διαθέσιμα θα πρέπει να είναι και τα προγράμματα αποκρυπτογράφησης.

4. Τα αντίγραφα ασφαλείας ενδεχομένως να μην περιέχουν τη σωστή πληροφορία. Πολλές φόρες μπορεί να γίνεται η λήψη ενός αντιγράφου ενώ η πληροφορία έχει υποστεί αλλοίωση.

5. Τα αντίγραφα θα πρέπει να ελέγχονται ανά τακτά χρονικά διαστήματα τόσο για την ορθότητα όσο και για την πληρότητα τους.

3.9. Κρυπτογραφία

Η κρυπτογραφία χρησιμοποιείται ευρέως σήμερα ως ένα πολύ χρήσιμο εργαλείο στην ασφάλεια της μεταφοράς πληροφοριών, προκειμένου να προστατευτούν προσωπικά δεδομένα ως προς την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητά τους. Σε νομικό και κοινωνικό επίπεδο, εδώ και πολλά χρόνια θέτονται ζητήματα προστασίας απορρήτου σε όλες τις δυνατές εκδοχές μιας δικτυακής συναλλαγής όπως είναι η λήψη και αποστολή email, οι διαφόρων ειδών εμπορικές συναλλαγές, η τήρηση του τραπεζικού και ιατρικού απορρήτου, κ.α. και γενικότερα ζήτημα προστασίας προσωπικών δεδομένων των χρηστών του διαδικτύου [1].

Από την στιγμή που ξεκίνησαν να μεταφέρονται πληροφορίες μέσω διαδικτύου, γεννήθηκε και η ιδέα της κρυπτογράφησης ή του κώδικα προκειμένου να ασφαλιστούν όλα τα μεταφερόμενα μηνύματα. Με άλλα λόγια η κρυπτογράφηση εξασφαλίζει, με τρόπους που θα δούμε στην συνέχεια το απόρρητο των μεταφερόμενων προσωπικών πληροφοριών εντός διαδικτύου. Σκόπιμο είναι προτού

αναφερθούμε σε αυτές τις μεθόδους να δώσουμε κάποιους βασικούς ορισμούς, ξεκινώντας από αυτόν της κρυπτογράφησης.

Κρυπτογράφηση(encryption) λοιπόν ονομάζεται η διαδικασία μετασχηματισμού ενός μηνύματος με τέτοιο τρόπο ώστε αυτό να μην είναι δυνατό να διαβαστεί από κανέναν, παρά μόνο από τον νόμιμο παραλήπτη του. Η αντίστροφη διαδικασία κατά την οποία από το κρυπτογραφημένο κείμενο παράγεται το αρχικό μήνυμα ονομάζεται αποκρυπτογράφηση (decryption). Αρχικό μήνυμα είναι αυτό που αποτελεί την είσοδο σε μια διεργασία κρυπτογράφησης. Αντίθετα κρυπτογραφημένο κείμενο είναι το αποτέλεσμα από την εφαρμογής ενός κρυπτογραφικού αλγόριθμου που πραγματοποιείται πάνω στο αρχικό κείμενο.

3.9.1. Συμμετρική Κρυπτογράφηση

Στην συμμετρική κρυπτογράφηση ο αποστολέας της πληροφορίας ή του μηνύματος χρησιμοποιεί ένα κλειδί, προκειμένου να κρυπτογραφήσει το μήνυμα του ή την πληροφορία που θέλει να αποστείλει και εν συνεχεία ο παραλήπτης χρησιμοποιεί το ίδιο κλειδί προκειμένου να πραγματοποιήσει την αποκρυπτογράφηση. Δηλαδή στην περίπτωση της συμμετρικής κρυπτογραφίας χρησιμοποιείται το ίδιο κλειδί και κατά την κρυπτογράφηση και κατά την αποκρυπτογράφηση της πληροφορίας

3.9.2. Ασύμμετρη Κρυπτογράφηση

Στην ασύμμετρη κρυπτογράφηση, σε αντίθεση με την συμμετρική, χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση τα οποία είναι αντίστοιχα το δημόσιο (public) και το ιδιωτικό (private) κλειδί. Τα κλειδιά αυτά δημιουργούνται με τρόπο ώστε να έχουν τις εξής ιδιότητες:

- ✓ Το κρυπτογραφημένο μήνυμα ή η πληροφορία, του οποίου η κρυπτογράφηση έχει γίνει με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί και αντίστροφα.
- ✓ Το δημόσιο κλειδί δεν μπορεί να προκύψει από το ιδιωτικό κλειδί με απλό τρόπο και αντίστροφα.

3.9.3. Αλγόριθμοι Κατακερματισμού

Η τελευταία κατηγορία αλγορίθμων κρυπτογράφησης είναι οι αλγόριθμοι κατακερματισμού (hash functions). Σε αυτό το είδος, ο αλγόριθμος παίρνοντας σαν είσοδο το αρχικό προς μεταφορά μήνυμα ή πληροφορία, το μετατρέπει σε μια καθορισμένου μήκους συνάρτηση κατακερματισμού (hash value), και με αυτόν τον τρόπο δεν γίνεται χρήση κάποιου κλειδιού όπως στις προηγούμενες περιπτώσεις με την χρήση των αλγορίθμων κατακερματισμού το περιεχόμενο αλλά και το μέγεθος του αρχικού μηνύματος/πληροφορίας είναι αδύνατο να ανακτηθούν από το αντίστοιχο κρυπτογραφημένο, ενώ ακόμα αδύνατο παραμένει το γεγονός δύο διαφορετικές πληροφορίες θα έχουν την ίδια τιμή κατακερματισμού [6].

ΣΥΜΠΕΡΑΣΜΑΤΑ

Το πρόβλημα της ασφάλειας στα δίκτυα υπολογιστών απασχολεί τα τελευταία χρόνια έντονα πληθώρα κοινωνικών ομάδων, όπως είναι απλοί χρήστες του διαδικτύου έως και μεγάλοι εμπορικοί και μη οργανισμοί. Τα θέματα της ασφάλειας του διαδικτύου λόγω της ιδιαίτερης σημασίας που έχουν, έχουν κινητοποιήσει σε μεγάλο βαθμό την επιστημονική κοινότητα αλλά και τις εταιρείες κατασκευής λογισμικού και υλικού, οδηγώντας τες προς την κατεύθυνση της κατανόησης, ανάλυσης και εύρεσης μεθόδων βελτίωσης.

Στην παρούσα εργασία σκοπός παρουσιάσαμε τα βασικά σημεία της ασφάλειας στον τομέα των δικτύων υπολογιστών και επιπλέον και αναλύσαμε τις αδυναμίες εκείνες οι οποίες δημιουργούν τα εν λόγω ζητήματα ασφάλειας.

Δίκτυο στην επιστήμη των επικοινωνιών αποτελεί ένα σύστημα το οποίο συνδέει κυρίως τερματικές συσκευές διαφόρων ειδών, είτε είναι απλές («χαζά» τερματικά) είτε είναι κανονικοί υπολογιστές. Ο σκοπός της δομής του δε είναι τέτοιος που

επιτρέπει την επικοινωνία μεταξύ αυτών των δικτύων. Σήμερα η επικοινωνία των υπολογιστών έχει γίνει απαραίτητο μέρος της υποδομής μας. Η δικτύωση χρησιμοποιείται σχεδόν σε κάθε δραστηριότητα των επιχειρήσεων – δημόσιων και ιδιωτικών – όπως στην διαφήμιση, την παραγωγή, την διεκπεραίωση, τον σχεδιασμό, την κοστολόγηση και την λογιστική [9]. Αυτός είναι άλλωστε και ο βασικός λόγος για τον οποίο τα μελετάμε. Η συνεχιζόμενη ανάπτυξη του παγκόσμιου διαδικτύου επίσης, δηλαδή το Διαδίκτυο (Internet), είναι ένα από τα πιο ενδιαφέροντα και εντυπωσιακά φαινόμενα της δικτύωσης.

Επιπλέον, μαζί με την ανάπτυξη των δικτύων και συνάμα την ραγδαία αύξηση του διαδικτύου η ανάγκη για την διασφάλιση της ασφάλειας έχει γίνει όλο και πιο εκτεταμένη. Την δεδομένη χρονική στιγμή δεν υπάρχει κάποιο σύστημα ασφαλείας δικτύων το οποίο είναι στο 100% και το πιο πιθανό μάλιστα είναι ένα τέτοιο σύστημα να μην κατασκευαστεί λόγω του ασύμφορου κόστους που εσωκλείει.

Για το λόγο αυτό οι περισσότεροι επιδιώκουν να κατασκευάσουν απλώς ένα ασφαλές σύστημα του οποίου το κόστος υλοποίησης θα είναι οριακά μεγαλύτερο από το κόστος μια κακόβουλης επίθεσης.

Όσοι διαθέτουν δίκτυα υπολογιστών είτε σε προσωπικό είτε σε επιχειρηματικό επίπεδο θα πρέπει να θέτουν τις κατάλληλες πολιτικές ασφαλείας δηλαδή ένα σύνολο κανόνων που θα ρυθμίζουν την πρόσβαση που έχει ο κάθε χρήστης. Επιπλέον πληθώρα τεχνολογιών έχουν αναπτυχθεί σήμερα προκειμένου να γίνεται ασφαλέστερη η χρήση δικτύων υπολογιστών ακόμα για απλούς χρήστες. Τέτοιες τεχνολογίες είναι τα λεγόμενα πρωτόκολλα ασφαλείας, οι κρυπτογραφικές μέθοδοι, κ.α.

Πιστεύουμε πως η ασφάλεια των δικτύων είναι ένα θέμα που χρειάζεται συνεχή παρακολούθηση και ενασχόληση για όσους ενδιαφέρονται στην πράξη για τέτοια

θέματα. Ευελπιστούμε δε η παρούσα εργασία να είναι απόλυτα κατατοπιστική πάνω στα θέματα που μελετάει.

Βιβλιογραφία

Ελληνική

[1] Γλαμπεδακης Μ. (2001), Εφαρμογες Τοπικών δικτύων. Με Windows 95, 98, 2000, Εκδόσεις Ιων, Αθήνα

[2] Αλεξόπουλος Α., Λαγογιάννης Γ. (2009), Τηλεπικοινωνίες και Δίκτυα Υπολογιστών, Εκδόσεις Γιαλός, Αθήνα

[3] Βούκαλης Δ.,(2007) Εφαρμοσμένη Κρυπτογραφία, Εκδόσεις Σύγχρονη Εκδοτική, Αθήνα

[4] Γκριτζάλης Δ.,Γκριτζάλης Σ., Κάτσικας Σ. Ασφάλεια Δικτύων Υπολογιστών, Εκδόσεις Παπασωτηρίου, Αθήνα

[5] Κομνηνός Θ., Σπυράκης Π. (2002), Ασφάλεια Δικτύων και Υπολογιστικών Συστημάτων, Εκδόσεις Ελληνικά Γράμματα, Αθήνα

[6] Κάτος Β., Στεφανίδης Γ., Τεχνικές κρυπτογραφίας και Κρυπτανάλυσης, Εκδόσεις Ζυγός, Αθήνα

[7] Πομπόρτσης Α. (1997), Εισαγωγή Στις Νέες Τεχνολογίες Επικοινωνιών, Εκδόσεις Τζιόλα, Θεσσαλονίκη

[8] Σιάχος Γ. (2000), Μελέτη και προτάσεις Βελτιστοποίησης απόδοσης των μηχανισμών που προτείνει το IPv6 για την εξάλειψη των περιορισμών του IPv4, Μεταπτυχιακή διπλωματική εργασία.

[9] Comer D. (2004), Δίκτυα και Διαδίκτυα Υπολογιστών και Εφαρμογές τους στο Internet, Εκδόσεις Κλειδάριθμος, Αθήνα

[10] McClure S., Scambray J., Kurtz G. (2009), Ασφάλεια Δικτύων, Εκδόσεις Γκιούρδας, Αθήνα

[11] Stallings W. (2007), Ασύρματες Επικοινωνίες και Δίκτυα, Εκδόσεις Τζιόλα, Αθήνα

[12] Tanenbaum A. (2000), Δίκτυα Υπολογιστών, Εκδόσεις Παπασωτηρίου, Αθήνα

Ξένη

[13] Adler M. (2002), Tradeoffs in Probabilistic Packet Marking for IP TraceBack, Procceedings of the 34th ACM Symposium on Theory of Computing

[14] Bellovin S. (1989), Security Problems in the TCP/IP Protocol Suite, Compouter Communication Review Vol.19

[15] Collin B.,(1997), Extranet security: What happens if your partner turns against you?, Computer Security Institute

[16] Denning J. (1990), Computers Under Attack: Intruders, Worms and Viruses, ACM Press, Addison – Wesley.

[17] GAO (1996), Information Security: Compouter Attacks at Department of Defense Pose Increasing Risks, Government Accounting Office.

[18] Macavinta C. (1997), AlterNIC takes oner InterNIC Traffic

[19] Nikoletseas S., Prasinos G., Spirakis P., Zaroliagkis C. (2001), Attack Propagation in Network, Procceedings of the 13th Annual ACM symposium on Parallel Algorithms and Architectures, ACM Press

[20] Tanenbaum A.,(1989), Computer Networks, Prentice Hall, New Jersey