Ασφάλεια Δικτύων και Συστημάτων με την βοήθεια Τειχων Προστασίας

Η σελίδα είναι σκόπιμα λευκή

ΑΝΩΤΑΤΟ ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΗΠΕΙΡΟΥ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ:

«Ασφάλεια Δικτύων και Συστημάτων με την βοήθεια Τειχων Προστασίας»

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:

ΑΡΤΑ, 2014

Περιεχόμενα

1.0 Εισαγωγή 7

1.1 Τι σημαίνει Ασφάλεια Δικτύων 8

1.2 Δίκτυα και Ασφάλεια 15

1.3 Το μοντέλο αναφοράς δικτύων ISO/OSI 17

1.4 Ασφάλεια στο Μοντέλο Αναφοράς ISO/OSI 20

1.5 Προβλήματα Ασφαλείας Δικτύων 21

1.6 Αναγκαιότητα και Σκοπιμότητα της Ασφάλειας 22

1.7 Υπηρεσίες Ασφάλειας και Μηχανισμοί Ασφάλειας 23

1.8 Επιθέσεις Ασφάλειας Δικτύων 27

2.0 Εξέλιξη πληροφοριακών Συστημάτων 30

2.1 Βασικές αρχές Πληροφοριακών Συστημάτων 31

2.2 Ασφάλεια Πληροφοριακών Συστημάτων 32

2.3 Σχεδιασμός πολιτικής ασφαλείας 33

2.4 Σκοποί επιθέσεων σε Πληροφοριακά Συστήματα 36

2.4.1 Οι «εχθροί» των Πληροφοριακών Συστημάτων 36

2.5 Ασφάλεια Λειτουργικών Συστημάτων 37

2.5.1 Προστασία Λειτουργικών Συστημάτων 37

2.5.2 Απειλές και ζητήματα Ασφάλειας 39

2.5.3 Μηχανισμοί ασφάλειας Λειτουργικών Συστημάτων 40

3.0 Εισαγωγή στα Τείχη Προστασίας (Firewalls) 41

3.1 Λειτουργία Τειχών Προστασίας 42

3.2 Τι κάνουν τα Τείχη Προστασίας 43

3.2.1 Διαχείριση και έλεγχος την κίνησης στο δίκτυο 43

3.3 Επικύρωση πρόσβασης 46

3.4 Η αποστρατικοποιημένη ζώνη (DMZ) 47

3.5 Τα firewall ελέγχου καταστάσεων (stateful inspection) 49

3.6 Πολιτικές ασφάλειας 50

3.7 Τείχη Προστασίας και εμπιστοσύνη 51
3.8 Κατηγοριοποίηση Τειχών Προστασίας..... 52
3.9 Διαφανείς Τείχη Προστασίας..... 57
4.0 Εικονικά Τείχη Προστασίας..... 58
4.1 Τείχη προστασίας ανοικτού και κλειστού κώδικα 58
4.2 Ασφάλεια δικτύων με τη βοήθεια Τειχών Προστασίας 59
4.3 Γενικά στοιχεία ασφαλείας..... 60
4.4 Άμυνα δικτύου 61
4.5 Ασφάλεια πρωτοκόλλων 63
4.6 Υπηρεσίες ασφαλείας OSI 64
4.7 Μηχανισμοί ασφαλείας OSI 65
4.8 Ασύρματα δίκτυα 66
4.9 Ασφάλεια στα ασύρματα δίκτυα 67
4.9.1 Ο μηχανισμός προστασίας ασύρματης πρόσβασης WPA 71
4.9.2 Ο μηχανισμός αυτοδύναμης ασφάλειας δικτύων RSN..... 73
5.0 Συμπεράσματα..... 74
6.0 Βιβλιογραφία 75

Περίληψη

Οι απαιτήσεις ασφάλειας στις μέρες μας είναι τουλάχιστον δεδομένες σε κάθε κοινωνία. Η ιδιωτικότητα, εμπιστευτικότητα, αυθεντικοποίηση, ακεραιότητα, είναι μερικές από τις λέξεις οι οποίες ακούγονται ολοένα και συχνότερα στη καθημερινότητα μας. Η εξέλιξη του Διαδικτύου, των ηλεκτρονικών συναλλαγών και γενικότερα των νέων τεχνολογιών δημιουργεί συνεχώς νέα ζητήματα ασφάλειας και προστασίας της ιδιωτικότητας σε όλους τους τομείς.

Όπως είναι φυσικό δε θα μπορούσαν να αποτελούν εξαίρεση τα ζητήματα ασφάλειας και προστασίας που δημιουργούνται στα Δίκτυα και στα Πληροφοριακά Συστήματα. Γενικότερα θα μπορούσε να πει κανείς ότι αποτελούν γεννήτορα ζητημάτων και προβλημάτων για τους υπόλοιπους τομείς αλλά αυτό είναι κάτι που ξεφεύγει από τα όρια αυτής της εργασίας. Τα θέματα ασφάλειας σε δικτυακές υποδομές και συστήματα μπορούμε να πούμε ότι είναι στοιχεία τα οποία μπορούν να επηρεάσουν συνολικά την πορεία, την εξέλιξη αλλά και την επιχειρησιακή στρατηγική ενός οργανισμού ή μια επιχείρησης. Συνεπώς μπορεί να γίνει κατανοητό το μέγεθος της σημασίας μιας όσο το δυνατόν ασφαλέστερης τεχνολογικής υποδομής σε ένα οποιοδήποτε περιβάλλον.

Τα Δίκτυα και τα Πληροφοριακά Συστήματα αναπτύσσονται συνεχώς μέσα σε ένα πολυσύνθετο περιβάλλον διαφορετικών μεταβλητών και παραγόντων. Η τάση για τεχνολογική εξέλιξη των συστημάτων αυτών δημιουργεί μεγαλύτερη πολυπλοκότητα στα θέματα ασφάλειας που τα αφορούν. Πλέον τα κενά ασφάλειας δεν είναι εμφανή και ο εκάστοτε υπεύθυνος ασφάλειας θα έχει σίγουρα πολύ περισσότερα να σκεφτεί από έναν απλό και τυπικό έλεγχο ασφάλειας.

Λέξεις κλειδιά: ασφάλεια, πληροφοριακά συστήματα, δίκτυα

Abstract

The safety requirements nowadays are given at least every society. The privacy, confidentiality, authentication, integrity, are some of the words that are heard more and more often in our daily lives. The evolution of the Internet, electronic transactions and general new technologies constantly creates new security issues and privacy protection in all areas.

Naturally they could be exceptional safety issues and protection generated in Networks and Information Systems. General could be said to constitute generator issues and problems for other sectors but this is something that goes beyond the limits of this work. Security issues in network infrastructure and systems can be said to be elements which can affect overall progress, development and business strategy of an organization or a business. Thus can be understood the magnitude of the importance of a possible safer technological infrastructure in any environment.

Networks and Information Systems are constantly being developed within a complex environment of different variables and factors. The tendency for technological development of these systems creates greater complexity in security issues affecting them. Most security holes are not obvious and each security officer will certainly have much more to think about than a simple and typical screening.

Keywords: security, information systems, networks

1.0 Εισαγωγή

Την περίοδο 1965-1975 άρχισαν οι κεντρικοί υπολογιστές να γίνονται πιο ισχυροί και ο αριθμός των χρηστών που συνδεόταν σε αυτούς έφτασαν τις χιλιάδες, το θέμα της υπευθυνότητα έγινε πιο σημαντικό. Η εισβολή εκείνη την εποχή ήταν σε επίπεδο φημών, περί κακόβουλων προγραμματιστών, που έκαναν παράνομες ενέργειες όπως να γράφουν κώδικα που έπαιρνε τα δεκαδικά ψηφία τραπεζικών συναλλαγών και τα κατέθετε στο δικό τους λογαριασμό ή να γράφουν συστήματα πίσω «πόρτας» στον κώδικά τους για να μπορούν να μπαίνουν σε συστήματα.

Η έλλειψη πραγματικής ασφάλειας εμφανίστηκε στην περίοδο 1975-1985, όταν οι εταιρείες άρχισαν να παρέχουν απομακρυσμένη προσπέλαση σε χρήστες τερματικών, μέσω μόντεμ που εργαζόταν χρησιμοποιώντας το δημόσιο τηλεφωνικό δίκτυο. Το 1969 η Defense Advanced Research Projects Agency (DARPA) ξεκίνησε ένα έργο για να μελετήσει τα δίκτυα δρομολόγησης πακέτων, όπου μεμονωμένα μικρά μηνύματα μπορούσαν να μεταδίδονται ανάμεσα σε δύο τερματικά συστήματα και να δρομολογούνται από ενδιάμεσα συστήματα με ένα χαλαρά ιεραρχικό τρόπο, επιτρέποντας έτσι σε οποιονδήποτε βρισκόταν στο δίκτυο να επικοινωνεί με τους άλλους. Αυτές οι ερευνητικές προσπάθειες άρχισαν να αποδίδουν καρπούς στα τέλη της δεκαετίας του '70. Η IBM ανέπτυξε τον αλγόριθμο Data Encryption Standard (DES) για την κυβέρνηση των Η.Π.Α το 1975. Σχεδόν ταυτόχρονα, οι Whitfield Diffie και Martin Hellman ανέπτυξαν την έννοια της κωδικοποίησης δημόσιου κλειδιού (Public Key Encryption, PKE), η οποία επέλυσε το πρόβλημα της ασφαλούς ανταλλαγής κλειδιού. Το 1977, οι Rivest, Shamir και Adelman υλοποίησαν την PKE στον ιδιοταγή αλγόριθμο κρυπτογράφησης RSA, που ήταν τα θεμέλια της σημερινής ασφάλειας δικτύων. Ωστόσο,το πρόσφατο ενδιαφέρον για την ασφάλεια τροφοδοτήθηκε από το έγκλημα του Kevin Mitnick. Ο Κέβιν Μίτνικ διέπραξε το μεγαλύτερο έγκλημα σε Ιστορίας των Ηνωμένων Πολιτειών το 1979. Οι απώλειες ήταν ογδόντα εκατομμυρίων δολάρια στις ΗΠΑ και την πνευματική ιδιοκτησία του πηγαίου κώδικα από μια ποικιλία των εταιρειών. Από τότε, ασφάλεια των πληροφοριών ήρθε στο προσκήνιο.

1.1 Τι σημαίνει Ασφάλεια Δικτύων

Το πρόβλημα της ασφάλειας των πληροφοριών είναι ιδιαίτερα σημαντικό στα σύγχρονα δίκτυα υπολογιστών. Η χρησιμοποίηση όλο και πιο προχωρημένων τεχνικών και τεχνολογιών όπως για παράδειγμα οι σύγχρονες βάσεις δεδομένων και τα σύγχρονα δίκτυα, προσφέρει αναμφισβήτητα σημαντικά πλεονεκτήματα και δυνατότητες, αυξάνει όμως ταυτόχρονα σημαντικά τα προβλήματα τα σχετικά με την προστασία και τη διαθεσιμότητα των πληροφοριών.

Η ασφάλεια αποτελεί αναγκαία συνθήκη και είναι απαραίτητη, σε συνδυασμό με τις άλλες βασικές προϋποθέσεις λειτουργίας όπως η ποιότητα και η απόδοση, για την εξασφάλιση της εύρυθμης λειτουργίας μιας επιχείρησης ή ενός οργανισμού. Αυτό είναι ιδιαίτερα σημαντικό σήμερα όπου πολύ συχνά το σύνολο των παρερχομένων υπηρεσιών μιας επιχείρησης στηρίζεται στην πληροφορική (π.χ. πάνω από το 80% των υπηρεσιών μιας τράπεζας).

Η έννοια της ασφάλειας ενός Δικτύου Υπολογιστών σχετίζεται με την ικανότητα μιας επιχείρησης ή ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Σχετίζεται επίσης με την ικανότητά του να παρέχει ορθές και αξιόπιστες πληροφορίες, οι οποίες είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες κάθε φορά που τις αναζητούν. Η ικανότητα αυτή στηρίζεται στη λήψη μέτρων τα οποία διασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, καθώς και την αδιάλειπτη λειτουργία του δικτύου.

Σύμφωνα με τον προηγούμενο ορισμό της ασφάλειας, η ασφάλεια στα δίκτυα υπολογιστών έχει να κάνει με την πρόληψη και ανίχνευση μη εξουσιοδοτημένων ενεργειών των χρηστών του δικτύου καθώς και την λήψη μέτρων. Ποιο συγκεκριμένα η ασφάλεια στα δίκτυα υπολογιστών σχετίζεται με:

Πρόληψη (prevention): Την λήψη δηλαδή μέτρων για να προληφθούν φθορές των μονάδων ενός δικτύου υπολογιστών.

Ανίχνευση (detection): Την λήψη μέτρων για την ανίχνευση του πότε, πώς και από ποιον προκλήθηκε φθορά σε μία από τις παραπάνω μονάδες.

Αντίδραση (reaction): Την λήψη δηλαδή μέτρων για την αποκατάσταση ή ανάκτηση των συστατικών ενός δικτύου.

Η ασφάλεια δικτύων και πληροφοριών μπορεί ακόμη να οριστεί ως η δυνατότητα ενός δικτύου ή συστήματος πληροφοριών να αντισταθεί, σε δεδομένο επίπεδο αξιοπιστίας, σε τυχαία συμβάντα ή κακόβουλες ενέργειες που θέτουν σε κίνδυνο τη διάθεση, την επαλήθευση ταυτότητας, την ακεραιότητα και την τήρηση του απορρήτου των δεδομένων που έχουν αποθηκευτεί ή μεταδοθεί καθώς και τις συναφείς υπηρεσίες που παρέχονται είτε είναι προσβάσιμες μέσω των δικτύων και συστημάτων αυτών.

Η προστασία ενός δικτύου το οποίο συνδέεται και με το Internet είναι ένα θέμα που καλούνται να αντιμετωπίσουν οι σύγχρονες επιχειρήσεις και οργανισμοί. Είναι γενικά αποδεκτό σήμερα ότι η έννοια της ασφάλειας των δικτύων υπολογιστών αλλά και των πληροφοριακών συστημάτων γενικότερα, συνδέεται στενά με τρεις βασικές έννοιες:

- Διαθεσιμότητα {Availability}
- Εμπιστευτικότητα {Confidentiality}
- Ακεραιότητα {Integrity}

Οι γενικές απαιτήσεις ασφάλειας δικτύων και συστημάτων πληροφοριών μπορούν να διατυπωθούν με τα εξής τέσσερα, αλληλένδετα χαρακτηριστικά:

α) Διαθεσιμότητα :

Διαθεσιμότητα ονομάζεται η ιδιότητα του να είναι προσπελάσιμες και χωρίς αδικαιολόγητη καθυστέρηση οι υπηρεσίες ενός δικτύου υπολογιστών όταν τις χρειάζεται μια εξουσιοδοτημένη οντότητα. Με τον όρο διαθεσιμότητα εννοούμε ότι δηλαδή ότι τα δεδομένα είναι προσβάσιμα και οι υπηρεσίες λειτουργούν, παρά τις όποιες τυχόν διαταραχές, όπως διακοπή τροφοδοσίας, φυσικές καταστροφές, ατυχήματα ή επιθέσεις. Αυτό σημαίνει ότι οι εξουσιοδοτημένοι χρήστες των υπολογιστικών συστημάτων και των υπολογιστών του δικτύου δεν αντιμετωπίζουν προβλήματα άρνησης εξυπηρέτησης (denial of service) όταν επιθυμούν να προσπελάσουν τους πόρους του δικτύου.

Για τους σκοπούς της ασφάλειας, μας απασχολεί βασικά η παρεμπόδιση κακόβουλων επιθέσεων που αποσκοπούν στο να παρακωλύσουν την πρόσβαση των νόμιμων χρηστών σε ένα πληροφοριακό σύστημα. Αυτές οι επιθέσεις ονομάζονται επιθέσεις άρνησης παροχής υπηρεσιών. Η άρνηση παροχής υπηρεσιών σημαίνει παρεμπόδιση της εξουσιοδοτημένης προσπέλασης πληροφοριών και πόρων ή πρόκληση καθυστέρησης των λειτουργιών που είναι κρίσιμες στο χρόνο. Η αντιμετώπισή τους αποσκοπεί στο να υπερνικήσει την σκόπιμη, που προκαλείται από κακόβουλα μέρη, παρά τυχαία απώλεια της διαθεσιμότητας. Ένα παράδειγμα επίθεσης άρνησης παροχής υπηρεσιών είναι οι

επιθέσεις «πλημμύρας» στο διαδίκτυο, όπου ο επιτιθέμενος κατακλύζει έναν εξυπηρετητή στέλνοντάς του έναν τεράστιο αριθμό αιτήσεων σύνδεσης.

Παρόλο που η διαθεσιμότητα συχνά αναδεικνύεται στο πλέον σημαντικό χαρακτηριστικό της ασφάλειας, εντούτοις λίγοι μηχανισμοί υπάρχουν για να βοηθήσουν στην υποστήριξή της.

β) Εμπιστευτικότητα :

Σε πολλές περιπτώσεις της καθημερινής ζωής οι έννοιες της ασφάλειας και της εμπιστευτικότητας σχεδόν ταυτίζονται, όπως για παράδειγμα στα στρατιωτικά περιβάλλοντα όπου η ασφάλεια έχει τη σημασία του να κρατούνται μυστικές οι πληροφορίες.

Η εμπιστευτικότητα σημαίνει πρόληψη μη εξουσιοδοτημένης αποκάλυψης πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη ανάγνωση. Επομένως, σημαίνει ότι τα δεδομένα που διακινούνται μεταξύ των υπολογιστών ενός δικτύου, αποκαλύπτονται μόνο σε εξουσιοδοτημένα άτομα. Αυτό αφορά όχι μόνο την προστασία από μη εξουσιοδοτημένη αποκάλυψη των δεδομένων αυτών καθαυτών αλλά ακόμη και από το γεγονός ότι τα δεδομένα απλώς υπάρχουν. Έτσι για παράδειγμα, το γεγονός ότι κανείς έχει φάκελο εγκληματία είναι συχνά το ίδιο σημαντικό όπως και οι λεπτομέρειες για το έγκλημα που διαπράχθηκε.

Άλλες εκφάνσεις της εμπιστευτικότητας είναι:

- **Η ιδιωτικότητα:** προστασία των δεδομένων προσωπικού χαρακτήρα, δηλαδή αυτών που αφορούν συγκεκριμένα πρόσωπα και
- **Η μυστικότητα:** προστασία των δεδομένων που ανήκουν σε έναν οργανισμό ή μια επιχείρηση.

γ) Ακεραιότητα:

Πρόκειται για την επιβεβαίωση ότι τα δεδομένα που έχουν αποσταλεί, παραληφθεί ή αποθηκευτεί είναι πλήρη και δεν έχουν υποστεί αλλοίωση. Η ακεραιότητα μπορεί να οριστεί γενικότερα ως η απαίτηση να είναι τα πράγματα όπως πρέπει να είναι. Στην πληροφορική, ακεραιότητα σημαίνει πρόληψη μη εξουσιοδοτημένης μεταβολής πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη εγγραφή ή διαγραφή, συμπεριλαμβανομένης και της μη εξουσιοδοτημένης δημιουργίας δεδομένων.

Επομένως, σημαίνει ότι η μετατροπή, διαγραφή και δημιουργία των δεδομένων ενός υπολογιστικού συστήματος, γίνεται μόνο από εξουσιοδοτημένα μέρη.

Ένας γενικός ορισμός της ασφάλειας δικτύων μπορεί να κατασκευαστεί ορίζοντας τα δύο συστατικά του, ασφάλεια και δίκτυα. Σαν ασφάλεια μπορεί να δοθεί ένα πλήθος ορισμών. Σύμφωνα με το λεξικό Oxford, ασφάλεια είναι «η ελευθερία από τον κίνδυνο και την ανησυχία». Η ασφάλεια μπορεί επίσης να οριστεί σαν:

Μία κατάσταση χωρίς κίνδυνο, χωρίς καμία αίσθηση απειλής:

- Η αποτροπή του κινδύνου ή της απειλής
- Η εγγύηση της αίσθησης εμπιστοσύνης και βεβαιότητας.

Σύμφωνα με την παραδοσιακή θεωρεία της πληροφορίας η ασφάλεια περιγράφεται διαμέσου της επιτυχίας μερικών βασικών ιδιοτήτων της, όπως είναι η εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα της πληροφορίας.

Εμπιστευτικότητα (confidentiality), είναι η ιδιότητα της προστασίας του περιεχομένου της πληροφορίας από όλους τους χρήστες εκτός από εκείνους που έχει εγκρίνει ο νόμιμος κάτοχος της πληροφορίας. Οι μη εγκεκριμένοι χρήστες συνήθως καλούνται μη εξουσιοδοτημένοι χρήστες. Άλλοι όροι, όπως η ιδιωτικότητα (privacy), χρησιμοποιούνται σχεδόν συνώνυμα με την εμπιστευτικότητα. Παρόλα αυτά, ο όρος ιδιωτικότητα αναπαριστά μία ανθρώπινη ιδιότητα (και όχι μία ιδιότητα της πληροφορίας) η οποία συνήθως δεν είναι εύκολα μετρήσιμη. Ακεραιότητα (integrity) είναι η ιδιότητα της προστασίας της πληροφορίας από την τροποποίησή της από μη εξουσιοδοτημένους χρήστες. Διαθεσιμότητα (availability) είναι η ιδιότητα της προστασίας της πληροφορίας από μη εξουσιοδοτημένη, προσωρινή ή μόνιμη, παρακράτησή της. Άλλες βασικές ιδιότητες ασφάλειας είναι η αυθεντικοποίηση και η μη αποποίηση. Η αυθεντικοποίηση (authentication) χωρίζεται σε αυθεντικοποίηση οντότητας (entity authentication) και σε αυθεντικοποίηση προέλευσης δεδομένων (data origin authentication). Η αυθεντικοποίηση οντότητας είναι η ιδιότητα της διασφάλισης της ταυτότητας μίας οντότητας (γνωστή και ως υποκείμενο – subject), η οποία μπορεί να είναι ένας άνθρωπος, μία μηχανή ή ένα πρόγραμμα λογισμικού. Η αυθεντικοποίηση προέλευσης δεδομένων είναι η ιδιότητα της διασφάλισης της πηγής της πληροφορίας. Τέλος, η μη αποποίηση (non-repudiation) είναι η ιδιότητα της διασφάλισης ότι υποκείμενα τα οποία έχουν δεσμευτεί με μία πράξη, δεν μπορούν σε μελλοντικό χρόνο να αρνηθούν αυτή την δέσμευση. Λεπτομερείς ορισμοί των ιδιοτήτων ασφάλειας μπορούν να βρεθούν σε γνωστά πρότυπα ασφάλειας, όπως τα ISO/IEC (International Organization for Standardization/International Engineering

Consortium) 7498-2 και ITU-T (International Telecommunication Union) X.800 . Κατά μία πρακτική προσέγγιση, η ασφάλεια πληροφοριακών συστημάτων περιλαμβάνει την προστασία των πληροφοριακών αγαθών ή παγίων (information assets) από απειλές ασφάλειας. Με βάση τις μεθοδολογίες ανάλυσης πληροφοριακής επικινδυνότητας, πληροφοριακό αγαθό είναι κάθε αντικείμενο ή πόρος, ο οποίος είναι αρκετά «σημαντικός» ώστε να προστατευτεί. Τα αγαθά μπορεί να είναι φυσικά (υπολογιστές, στοιχεία δικτυακής υποδομής, κτήρια και εγκαταστάσεις που φιλοξενούν εξοπλισμό), δεδομένα (ηλεκτρονικά αρχεία, ηλεκτρονικές βάσεις/βιβλιοθήκες δεδομένων), ή λογισμικό (λογισμικά προγράμματα, αρχεία διαμόρφωσης). Η προστασία των αγαθών μπορεί να επιτευχθεί μέσα από διάφορους μηχανισμούς ασφάλειας (security mechanisms), οι οποίοι μπορεί να στοχεύουν στην πρόληψη (protection), την ανίχνευση (detection) ή την ανάκαμψη (recovery) των αγαθών από απειλές ασφάλειας και αδυναμίες.

Μία απειλή ασφάλειας (security threat) είναι κάθε γεγονός που μπορεί να βλάψει ένα αγαθό. Όταν μία απειλή ασφάλειας εκδηλώνεται, το σύστημα ή το δίκτυο είναι «υπό επίθεση». Ο επιτιθέμενος ή φορέας της επίθεσης (attacker, threat agent) είναι κάθε υποκείμενο ή οντότητα που προκαλεί την επίθεση. Η συνέπεια (impact) της απειλής μετράει την έκταση της απώλειας που θα προκληθεί στο αγαθό ή στον ιδιοκτήτη του αγαθού, εφόσον η απειλή πραγματοποιηθεί εναντίον του αγαθού.

Αδυναμία της ασφάλειας (vulnerability) είναι κάθε χαρακτηριστικό σε ένα σύστημα που κάνει ένα αγαθό περισσότερο ευάλωτο σε μία ή περισσότερες απειλές. Ο συνδυασμός αγαθών, απειλών και αδυναμιών, παρέχει μια ποσοτική ή/και ποιοτική μέτρηση της πιθανοφάνειας (likelihood) εκδήλωσης των απειλών, καθώς και της συνέπειας που δημιουργείται από την εκδήλωση της απειλής. Αυτή η μέτρηση είναιγνωστή ως επικινδυνότητα ή κίνδυνος (security risk). Συνεπώς, οι μηχανισμοί ασφάλειας παρέχουν δυνατότητες που μειώνουν την επικινδυνότητα σε ένα σύστημα. Σημειώστε ότι, η ασφάλεια δεν βασίζεται μονομερώς σε τεχνικούς μηχανισμούς ασφάλειας. Σχεδόν σε κάθε σύστημα πληροφοριών και δικτύων, απαιτούνται επιπλέον διαδικαστικά και οργανωτικά μέτρα ασφάλειας επιπροσθέτως των τεχνικών μηχανισμών, ώστε να επιτευχθούν οι επιθυμητοί στόχοι της ασφάλειας.

Ένα δίκτυο υπολογιστών (computer network), ή απλά ένα δίκτυο, είναι κάθε συλλογή διασυνδεδεμένων υπολογιστών. Δύο ή περισσότερα συστήματα υπολογιστών θεωρούνται συνδεδεμένα εάν μπορούν να στείλουν και να λάβουν μεταξύ τους δεδομένα, διαμέσου ενός κοινόχρηστου μέσου πρόσβασης. Τα μέρη της επικοινωνίας σε ένα δί-

κτυο υπολογιστών είναι γνωστά ως οντότητες, υποκείμενα, ή κόμβοι. Αυτές οι οντότητες μπορούν να διαιρεθούν περαιτέρω σε χρήστες (users) οικοδεσπότες (hosts), και διεργασίες (processes):

- Ένας χρήστης (user) είναι μια ανθρώπινη οντότητα αρμόδια για τις ενέργειές του σε ένα δίκτυο υπολογιστών.
- Ένας οικοδεσπότης ή ξενιστής (host) είναι μια προσπελάσιμη οντότητα μέσα σε ένα δίκτυο υπολογιστών. Κάθε οικοδεσπότης έχει έναν μοναδικό διεύθυνση μέσα σε ένα δίκτυο.
- Μια διεργασία (process) είναι ένα στιγμιότυπο ενός εκτελέσιμου προγράμματος. Ο όρος διαδικασία χρησιμοποιείται στο μοντέλο επικοινωνίαςπελάτη-εξυπηρετητή (client-server) προκειμένου να διακρίνονται οι διεργασίες του πελάτη και οι διεργασίες του εξυπηρετητή:
  - Η διεργασία πελάτη είναι εκείνη η διεργασία η οποία είναι υπεύθυνη να υποβάλλει αιτήματα χρήσης μιας δικτυακής υπηρεσίας.
  - Η διεργασία εξυπηρετητή είναι η διεργασία η οποία είναι υπεύθυνη να παρέχει μια δικτυακή υπηρεσία, παραδείγματος χάριν, μία διεργασία η οποία τρέχει διαρκώς στο υπόβαθρο για να προσφέρει μία δικτυακή υπηρεσία.

Ένα δίκτυο θεωρείται ενσύρματο ή σταθερό (wired or fixed), εάν το μέσο πρόσβασης είναι κάποιο είδος φυσικής σύνδεσης καλωδίων μεταξύ των υπολογιστών, όπως ένα χάλκινο καλώδιο ή ένα καλώδιο οπτικών ινών. Αντίστοιχα, ένα δίκτυο θεωρείται ως ασύρματο δίκτυο (wireless network) εάν η πρόσβαση στο μέσο στηρίζεται σε εναέρια σηματοδοσία, όπως η επικοινωνία με ραδιοσυχνότητα (RF). Ένα δίκτυο μπορεί επίσης να διαιρεθεί σύμφωνα με τη γεωγραφική κάλυψή του. Ανάλογα με το μέγεθός του, ένα δίκτυο μπορεί να είναι ένα προσωπικό δίκτυο περιοχής (Personal Area Network – PAN), ένα δίκτυο τοπικής περιοχής (Local Area Network – LAN), ένα δίκτυο μητροπολιτικής περιοχής (Metropolitan Area Network –MAN), ή ένα δίκτυο ευρείας περιοχής ((Wide Area Network – WAN).

Ανεξάρτητα από το μέσο πρόσβασης και την κάλυψη ενός δικτύου, η ασφάλεια δικτύων (network security) μπορεί να εξετάζεται μέσω της επίτευξης δύο στόχων ασφάλειας: την ασφάλεια υπολογιστικών συστημάτων (computer systems security) και την ασφάλεια επικοινωνίας (communication security):

- Ο στόχος της ασφάλειας υπολογιστικών συστημάτων είναι η προστασία των πληροφοριακών αγαθών από μη εξουσιοδοτημένη ή κακόβουλη χρήση, καθώς

επίσης και η προστασία των πληροφοριών που αποθηκεύονται στα υπολογιστικά συστήματα από μη εξουσιοδοτημένη αποκάλυψη, τροποποίηση, ή καταστροφή.

- Ο στόχος της ασφάλειας επικοινωνίας είναι η προστασία των πληροφοριών κατά τη διάρκεια της μετάδοσής τους διαμέσου ενός μέσου επικοινωνίας, από την μη εξουσιοδοτημένη αποκάλυψη, τροποποίηση, ή καταστροφή.

1.2 Δίκτυα και Ασφάλεια

Ένα δίκτυο υπολογιστών (computer network), ή απλά ένα δίκτυο, είναι κάθε συλλογή διασυνδεδεμένων υπολογιστών. Δύο ή περισσότερα συστήματα υπολογιστών θεωρούνται συνδεδεμένα εάν μπορούν να στείλουν και να λάβουν μεταξύ τους δεδομένα, διαμέσου ενός κοινόχρηστου μέσου πρόσβασης. Τα μέρη της επικοινωνίας σε ένα δίκτυο υπολογιστών είναι γνωστά ως οντότητες, υποκείμενα, ή κόμβοι. Αυτές οι οντότητες μπορούν να διαιρεθούν περαιτέρω σε χρήστες (users) οικοδεσπότες (hosts), και διεργασίες (processes):

- Ένας χρήστης (user) είναι μια ανθρώπινη οντότητα αρμόδια για τις ενέργειές του σε ένα δίκτυο υπολογιστών.
- Ένας οικοδεσπότης (host) είναι μια προσπελάσιμη οντότητα μέσα σε ένα δίκτυο υπολογιστών. Κάθε οικοδεσπότης έχει μια μοναδική διεύθυνση μέσα σε ένα δίκτυο.
- Μια διεργασία (process) είναι ένα στιγμιότυπο ενός εκτελέσιμου προγράμματος. Ο όρος διαδικασία χρησιμοποιείται στο μοντέλο επικοινωνίας πελάτη-εξυπηρετητή (client-server) προκειμένου να διακρίνονται οι διεργασίες του πελάτη και οι διεργασίες του εξυπηρετητή:
  - ✓ Η διεργασία πελάτη είναι εκείνη η διεργασία η οποία είναι υπεύθυνη να υποβάλλει αιτήματα χρήσης μιας δικτυακής υπηρεσίας.
  - ✓ Η διεργασία εξυπηρετητή είναι η διεργασία η οποία είναι υπεύθυνη να παρέχει μια δικτυακή υπηρεσία, παραδείγματος χάριν, μία διεργασία η οποία τρέχει διαρκώς στο υπόβαθρο για να προσφέρει μία δικτυακή υπηρεσία.

Ένα δίκτυο θεωρείται ενσύρματο ή σταθερό (wired or fixed), εάν το μέσο πρόσβασης είναι κάποιο είδος φυσικής σύνδεσης καλωδίων μεταξύ των υπολογιστών, όπως ένα χάλκινο καλώδιο ή ένα καλώδιο οπτικών ινών. Αντίστοιχα, ένα δίκτυο θεωρείται ως ασύρματο δίκτυο (wireless network)εάν η πρόσβαση στο μέσο στηρίζεται σε εναέρια σηματοδοσία, όπως η επικοινωνία με ραδιοσυχνότητα (RF). Ένα δίκτυο μπορεί επίσης να διαιρεθεί σύμφωνα με τη γεωγραφική κάλυψή του. Ανάλογα με το μέγεθός του, ένα

δίκτυο μπορεί να είναι ένα προσωπικό δίκτυο περιοχής (Personal Area Network – PAN), ένα δίκτυο τοπικής περιοχής (Local Area Network – LAN), ένα Δίκτυο Μητροπολιτικής Περιοχής (Metropolitan Area Network – MAN), ή ένα Δίκτυο Ευρείας Περιοχής (Wide Area Network – WAN). Ανεξάρτητα από το μέσο πρόσβασης και την κάλυψη ενός δι-

κτύου, η ασφάλεια δικτύων (network security) μπορεί να εξετάζεται μέσω της επίτευξης δύο στόχων ασφάλειας: την ασφάλεια υπολογιστικών συστημάτων (computer systems security) και την ασφάλεια επικοινωνίας (communication security):

- ✓ Ο στόχος της ασφάλειας υπολογιστικών συστημάτων είναι η προστασία των πληροφοριακών αγαθών από μη εξουσιοδοτημένη ή κακόβουλη χρήση, καθώς επίσης και η προστασία των πληροφοριών που αποθηκεύονται στα υπολογιστικά συστήματα από μη εξουσιοδοτημένη αποκάλυψη, τροποποίηση, ή καταστροφή.
- ✓ Ο στόχος της ασφάλειας επικοινωνίας είναι η προστασία των πληροφοριών κατά τη διάρκεια της μετάδοσής τους διαμέσου ενός μέσου επικοινωνίας, από την μη εξουσιοδοτημένη αποκάλυψη, τροποποίηση, ή καταστροφή.

1.3 Το μοντέλο αναφοράς δικτύων ISO/OSI

Προκειμένου να υπάρξει μια βαθιά κατανόηση του τρόπου που εκτελείται η δικτύωση, έχουν αναπτυχθεί μοντέλα αναφοράς δικτύων (network reference models) τα οποία ομαδοποιούν ομοειδείς λειτουργίες σε αφηρημένα επίπεδα, γνωστά ως στρώματα ή επίπεδα (layers). Οι λειτουργίες κάθε επιπέδου σε έναν κόμβο του δικτύου (host), μπορούν να επικοινωνήσουν με τις λειτουργίες του ίδιου επιπέδου σε έναν άλλο δικτυακό κόμβο. Στον ίδιο κόμβο, οι λειτουργίες κάθε επιπέδου διαθέτουν διεπαφές επικοινωνίας με τα επίπεδα που βρίσκονται ακριβώς πάνω και κάτω από το συγκεκριμένο επίπεδο. Αυτή η αφαιρετική προσέγγιση απλοποιεί την επικοινωνία εφόσον ορίζει συγκεκριμένες και διακριτές ενέργειες για την επικοινωνία σε κάθε δικτυακό επίπεδο.

Το μοντέλο αναφοράς δικτύων ISO Open Systems Interconnection (OSI) ορίζει επτά επίπεδα δικτύου καθώς και τις αντίστοιχες διεπαφές τους (interfaces).

Κάθε επίπεδο εξαρτάται από τις παρεχόμενες υπηρεσίες από το αμέσως χαμηλότερο επίπεδό του, μέχρι το φυσικό επίπεδο και την καλωδίωση. Κατόπιν, παρέχει τις υπηρεσίες του στο άμεσο ανώτερο επίπεδό του, μέχρι την εκτελούμενη εφαρμογή. Πρέπει να διευκρινιστεί ότι δεν περιλαμβάνουν όλα τα δικτυακά μοντέλα αναφοράς και τα επτά στρώματα. Η δημοφιλέστερη σουίτα πρωτοκόλλων δικτύωσης, το γνωστό πρωτόκολλο ελέγχου μετάδοσης/πρωτόκολλο διαδικτύου (TCP/IP), ορίζει πέντε επίπεδα. Δεν ορίζει επίπεδο παρουσίασης και επίπεδο συνόδου και οι λειτουργίες αυτών των επιπέδων ενσωματώνονται στα ανώτερα και κατώτερα επίπεδα.

Τα επτά επίπεδα του προτύπου αναφοράς ISO/OSI περιγράφονται συνοπτικά ακολούθως, ακολουθώντας τη σειρά από το υψηλότερο προς το χαμηλότερο επίπεδο:

- ✓ **Επίπεδο 7:** Επίπεδο εφαρμογής (Application Layer). Αυτό το επίπεδο εξετάζει τα ζητήματα επικοινωνίας των εφαρμογών. Εντοπίζει και εγκαθιστά τη διαθεσιμότητα των επικοινωνούντων, ενώ είναι επίσης αρμόδιο και για τη διεπαφή με το χρήστη. Παραδείγματα διαδεδομένων πρωτοκόλλων επιπέδου εφαρμογής αποτελούν το πρωτόκολλο έναρξης συνόδου (Session Initiation Protocol – SIP), το πρωτόκολλο μεταφοράς υπερκειμένου (Hyper-Text Transfer Protocol – HTTP), το πρωτόκολλο μεταφοράς αρχείων (File Transfer Protocol – FTP), το πρωτόκολλο απλής μεταφοράς ταχυδρομείου (Simple Mail Transfer Protocol – SMTP), και το πρωτόκολλο απομακρυσμένης διασύνδεσης Telnet.

- ✓ **Επίπεδο 6:** Επίπεδο παρουσίασης (Presentation Layer). Αυτό το επίπεδο είναι αρμόδιο για την παρουσίαση των δεδομένων στο ανώτερο επίπεδο της εφαρμογής. Ουσιαστικά, μεταφράζει τα δεδομένα και εκτελεί εργασίες όπως η συμπίεση και η αποσυμπίεση και η κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων. Μερικά από τα γνωστά πρότυπα και πρωτόκολλα αυτού του επιπέδου αποτελούν η κωδικοποίηση χαρακτήρων ASCII, το πρωτόκολλο συμπίεσης ZIP, η κωδικοποιήσεις αρχείων εικόνας JPEG και TIFF, το RTP, και η κωδικοποίηση ήχου MIDI.
- ✓ **Επίπεδο 5:** Επίπεδο συνόδου (Session Layer). Αυτό το επίπεδο είναι αρμόδιο για την έναρξη της επαφής μεταξύ δύο κόμβων και την εξασφάλιση της γραμμής επικοινωνίας. Μορφοποιεί τα δεδομένα για τη μεταφορά και διατηρεί τη σύνδεση από-άκρο-σε-άκρο (end-to-end). Δύο παραδείγματα πρωτοκόλλων του επιπέδου συνόδου είναι το πρωτόκολλο κλήσης απομακρυσμένης σύνδεσης (Remote Procedure Call – RPC) και το πρωτόκολλο ασφαλούς υποδοχής (Secure Socket Layer – SSL).
- ✓ **Επίπεδο 4:** Επίπεδο μεταφοράς (Transport Layer). Αυτό το επίπεδο καθορίζει τον τρόπο που αναφέρονται οι φυσικές θέσεις του δικτύου, εγκαθίστανται οι συνδέσεις μεταξύ των κόμβων, και ανταλλάσσονται τα μηνύματα εντός του δικτύου. Διατηρεί επίσης την ακεραιότητα της συνόδου από άκρο-σε-άκρο και παρέχει τους μηχανισμούς για να υποστηρίξει την καθιέρωση συνόδου για τα ανώτερα στρώματα. Το πρωτόκολλο ελέγχου μεταφοράς (Transmission Control Protocol – TCP) και το πρωτόκολλο δεδομένων χρήστη (User Datagram Protocol – UDP) είναι τα ευρύτατα γνωστά πρωτόκολλα αυτού του επιπέδου, ενώ ένα αναπτυσσόμενο πρωτόκολλο αυτού του επιπέδου είναι το πρωτόκολλο ελέγχου μετάδοσης ροής (Strea Control Transmission Protocol – SCTP).
- ✓ **Επίπεδο 3:** Επίπεδο δικτύου (Network Layer). Αυτό το επίπεδο είναι αρμόδιο για τη δρομολόγηση και την αναμετάδοση των δεδομένων μεταξύ των κόμβων του δικτύου. Η βασική λειτουργία του είναι να στείλει τα τεμάχια/τμήματα των δεδομένων τα οποία είναι γνωστά και ως πακέτα δεδομένων (data packets) από μια πηγή σε έναν κόμβο προορισμού. Περιλαμβάνει επίσης τη διαχείριση της ανίχνευσης σφαλμάτων, τη δρομολόγηση μηνυμάτων, και τον έλεγχο της κίνησης. Το πρωτόκολλο διαδικτύου (Internet Protocol – IP) ανήκει σε αυτό το επίπεδο.

- ✓ **Επίπεδο 2:** Επίπεδο ζεύξης δεδομένων (Data Link Layer). Αυτό το επίπεδο καθορίζει τους όρους που πρέπει να ακολουθηθούν από έναν κόμβο προκειμένου να ‘εχει πρόσβαση στο δίκτυο. Εγκαθιστά τη σύνδεση μεταξύ των κόμβων πάνω από το φυσικό κανάλι. Εξασφαλίζει την παράδοση των μηνυμάτων στην κατάλληλη συσκευή και μεταφράζει τα μεταδιδόμενα bit για το χαμηλότερο φυσικό στρώμα. Το Ethernet και το Token Ring είναι χαρακτηριστικά παραδείγματα των πρωτοκόλλων που λειτουργούν σε αυτό το στρώμα.
- ✓ **Επίπεδο 1:** Φυσικό Επίπεδο (Physical Layer). Αυτό το επίπεδο ορίζει τη φυσική σύνδεση μεταξύ ενός κόμβου και ενός δικτύου. Η βασική του εργασία είναι η μετατροπή των δυαδικών ψηφίων (bit) σε ένα φυσικό σήμα κατάλληλο για μετάδοση, όπως για παράδειγμα σε ηλεκτρική τάση ή σε παλμούς φωτός. Οι οδηγοί συσκευών που χειρίζονται το υλικό δικτυακής επικοινωνίας (π.χ. κάρτες Ethernet, ασύρματες κάρτες κ.λπ.) λειτουργεί σε αυτό το στρώμα. Η σύσταση X.200 [6] του διεθνούς οργανισμού τηλεπικοινωνιών ITU-T ευθυγραμμίζεται με το πρότυπο ISO/IEC 7498-1.

Εικόνα 1: Τα επίπεδα του OSI

1.4 Ασφάλεια στο Μοντέλο Αναφοράς ISO/OSI

Σύμφωνα με το πρότυπο ISO/IEC 7498-1 , κάθε επίπεδο πρωτοκόλλου αποτελείται από τρία λειτουργικά πλάνα (functional planes): το επίπεδο χρηστών, το επίπεδο της σηματοδοσίας και ελέγχου, και το επίπεδο διαχείρισης. Για τη διασφάλιση των δικτυακών επικοινωνιών θα πρέπει να επιτευχθούν οι κατάλληλοι στόχοι ασφάλειας σε κάθε επίπεδο πρωτοκόλλων και σε κατάλληλο λειτουργικό πλάνο. Το πρότυπο ISO/IEC 7498-2 και η αρχιτεκτονική ασφάλειας ITU-T X.800 για τη διασύνδεση ανοικτών συστημάτων, βασίζονται και επεκτείνουν το πρότυπο ISO/OSI 7498-1, για να καλύψουν τις πτυχές ασφάλειας των δικτύων. Η σύσταση X.800 παρέχει μία γενική περιγραφή των υπηρεσιών και των σχετικών μηχανισμών ασφάλειας, τα οποία παρέχονται από το πρότυπο αναφοράς. Επίσης καθορίζει τις θέσεις μέσα στο μοντέλο αναφοράς, όπου οι υπηρεσίες και οι μηχανισμοί μπορούν να παρασχεθούν.

Με βάση τα πρότυπα και οι στόχοι ασφάλειας επιτυγχάνονται μέσω πολιτικών ασφάλειας (security policies) και υπηρεσιών ασφάλειας (security services). Μια πολιτική ασφάλειας είναι το σύνολο κριτηρίων το οποίο ορίζει την παροχή υπηρεσιών ασφάλειας. Υπηρεσία ασφάλειας είναι μία υπηρεσία η οποία παρέχεται από ένα επίπεδο δικτύου, προκειμένου να εξασφαλιστεί η επαρκής προστασία των συστημάτων ή των μεταδιδόμενων δεδομένων. Οι υπηρεσίες ασφάλειας υλοποιούνται μέσω μηχανισμών ασφάλειας (security mechanisms), οι οποίοι είναι γενικά μηχανισμοί που μπορούν να χρησιμοποιηθούν για να επιβάλουν τεχνικά την εφαρμογή μια υπηρεσίας ασφάλειας.

1.5 Προβλήματα Ασφαλείας Δικτύων

Ένα δικτυωμένο σύστημα είναι επιρρεπές σε ένα αριθμό απειλών που προέρχονται και από νόμιμους χρήστες του συστήματος αλλά και κυρίως από επίδοξους εισβολείς. Κάθε κόμβος του δικτύου είναι ένα υπολογιστικό σύστημα με όλα τα γνωστά προβλήματα ασφάλειας. Σε αυτά, έρχεται το δίκτυο να προσθέσει το πρόβλημα της επικοινωνίας μέσω ενός πολύ εκτεθειμένου μέσου και της προσπέλασης από μακρινές τοποθεσίες μέσω πιθανώς μη-έμπιστων υπολογιστικών συστημάτων. Μερικοί λόγοι για τους οποίους αποκτούν ιδιαίτερη σημασία τα θέματα ασφάλειας δικτύων υπολογιστών είναι οι εξής :

- Η αυξημένη περιπλοκότητα περιορίζει το αίσθημα εμπιστοσύνης για την ασφάλεια των δικτύων.
- Υπάρχει αύξηση στον αριθμό των διαύλων επικοινωνίας και άρα των πιθανών σημείων επίθεσης, τα οποία πρέπει να οχυρωθούν κατάλληλα.
- Έχουν γίνει ασαφή τα όρια των δικτύων και οι διακρίσεις μεταξύ των τμημάτων μιας επιχείρησης. Κάθε κόμβος οφείλει να είναι ικανός να αντιδράσει σωστά στη παρουσία ενός νέου και μη-έμπιστου κόμβου. Από την άλλη, κάθε κόμβος μπορεί να ανήκει ταυτόχρονα σε περισσότερα από ένα δίκτυα, με αποτέλεσμα να μην είναι ξεκάθαρη η εικόνα των νομίμων χρηστών του κάθε δικτύου.
- Η δυνατότητα ανωνυμίας ενός χρήστη απαιτεί ισχυρούς μηχανισμούς πιστοποίησης μεταξύ των υπολογιστών, που συνήθως είναι διαφορετικοί από αυτούς που πιστοποιούν τους χρήστες στα υπολογιστικά συστήματα.
- Υπάρχει αδυναμία ελέγχου της δρομολόγησης των δεδομένων που διακινούνται μέσω των δικτύων.

1.6 Αναγκαιότητα και Σκοπιμότητα της Ασφάλειας

Είναι γεγονός ότι, παρά την προφανή της χρησιμότητα, η λήψη των απαραίτητων μέτρων ασφάλειας δημιουργεί πολλές φορές κάποια πρόσθετη επιβάρυνση στην απόδοση και το κόστος λειτουργίας του δικτύου υπολογιστών μιας επιχείρησης. Θα πρέπει ακόμη να αποδεχτούμε το κόστος της ασφάλειας και ως κόστος χρόνου και ως κόστος χρήματος. Συνεπώς, μπορεί να θεωρηθεί ότι η ασφάλεια βρίσκεται σε σχέση αντιστρόφως ανάλογη με την αποδοτικότητα του δικτύου υπολογιστών μιας επιχείρησης. Αυτό όμως δεν είναι σωστό γιατί η ασφάλεια είναι κόστος αναγκαίο για την ομαλή και εύρυθμη λειτουργία του.

Το συγκεκριμένο κόστος για την ασφάλεια των δικτύων μιας επιχείρησης εξαρτάται και προκύπτει από την εκάστοτε ακολουθούμενη πολιτική ασφάλειας. Απαιτείται συνεπώς μια πολιτική ασφαλείας η οποία θα πρέπει να εξισορροπεί το κόστος εισαγωγής ασφάλειας από την μία πλευρά και το κόστος ζημιών από πιθανολογούμενο κίνδυνο από την άλλη. Επίσης, θα πρέπει να δημιουργούνται τέτοιες συνθήκες ασφάλειας ώστε να μη παρεμποδίζεται η ευελιξία και η ανάπτυξη της επιχείρησης.

Η αναγκαία πολιτική ασφάλειας καθορίζεται από μία δυναμική εκτίμηση του κόστους των μέτρων ασφάλειας σε σχέση με τις συνέπειες που θα έχει για τον οργανισμό οποιαδήποτε πρόκληση δυσλειτουργίας. Ο βασικός αυτός κανόνας ισχύει για όλους τους τομείς και όλα τα επίπεδα ασφάλειας. Έτσι, σε κάθε περίπτωση όπου απαιτείται η λήψη κάποιου μέτρου ασφάλειας, πρέπει να εξετάζεται η πιθανότητα να συμβεί κάποιο πρόβλημα ασφάλειας, σε σχέση με τις συνέπειες που αυτό θα δημιουργήσει. Εάν η τιμή των δύο αυτών παραμέτρων είναι υψηλή, τότε πρέπει απαραίτητα να ληφθούν μέτρα, ανεξάρτητα από το κόστος πρόληψης.

Τέλος, πρέπει να σημειωθεί ότι η ασφάλεια χαρακτηρίζεται από την φύση της ως δυναμική παράμετρος και όχι στατική, καθώς η τεχνολογία, ο ανταγωνισμός, η πολυπλοκότητα των πληροφοριακών συστημάτων και η ολοένα βελτιούμενη επιτηδειότητα των 'επιτιθέμενων', απαιτούν τη λήψη νέων και συνεχώς αυστηρότερων μέτρων ασφάλειας. Συνεπώς, η ακολουθούμενη πολιτική ασφαλείας θα πρέπει να επανεξετάζεται τακτικά και να διορθώνεται όπου αυτό κρίνεται απαραίτητο.

1.7 Υπηρεσίες Ασφάλειας και Μηχανισμοί Ασφάλειας

Όπως περιγράφεται στα πρότυπα οι βασικές υπηρεσίες ασφάλειας στις επικοινωνίες του μοντέλου αναφοράς OSI περιλαμβάνουν τα παρακάτω:

1. Αυθεντικοποίηση (Authentication). Αυτή η υπηρεσία μπορεί να χρησιμοποιηθεί από μία οντότητα του δικτύου, α) είτε ως αυθεντικοποίηση οντότητας 2. Έλεγχος πρόσβασης (Access Control). Αυτή η υπηρεσία μπορεί να χρησιμοποιηθεί για να προστατεύσει τα πληροφοριακά αγαθά και τους πόρους που είναι διαθέσιμοι μέσω του δικτύου από μη εξουσιοδοτημένη πρόσβαση. Η υπηρεσία μπορεί να εφαρμοστεί για διάφορους τύπους πρόσβασης όπως προσπέλαση ανάγνωσης, εγγραφής, εκτέλεσης ή οποιουδήποτε συνδυασμού των ανωτέρω. Η πρόσβαση στους πόρους μπορεί να ελεγχθεί μέσω των διάφορων πολιτικών πρόσβασης, όπως είναι οι πολιτικές κανόνων (rule-based policies) ή οι πολιτικές ταυτότητας (identity-based policies). Οι υπηρεσίες ελέγχου πρόσβασης θα πρέπει να συνεργάζονται με τις υπηρεσίες αυθεντικοποίησης, εφόσον η χορήγηση της πρόσβασης σε κάποιο πληροφοριακό πόρο απαιτεί την προγενέστερη αυθεντικοποίηση της οντότητας που ζητά την πρόσβαση.
2. Εμπιστευτικότητα Δεδομένων (Data Confidentiality). Αυτή η υπηρεσία προστατεύει τα δεδομένα από την αποκάλυψή τους σε μη εξουσιοδοτημένες οντότητες. Σύμφωνα με τη σύσταση X.800, παραλλαγές αυτής της υπηρεσίας περιλαμβάνουν: α) την εμπιστευτικότητα σύνδεσης (connection confidentiality), όταν η υπηρεσία παρέχεται σε όλα τα επίπεδα (layers) της επικοινωνίας, β) την εμπιστευτικότητα χωρίς σύνδεση (connectionless confidentiality), όταν η εμπιστευτικότητα παρέχεται μόνο σε ένα επίπεδο, γ) την επιλεκτική εμπιστευτικότητα (selective field confidentiality), όταν προστατεύει μόνο ορισμένα πεδία των δεδομένων, και δ) την εμπιστευτικότητα κυκλοφοριακής ροής (traffic flow confidentiality), όταν προστατεύει την πληροφορία που ενδεχομένως θα μπορούσε να εξαχθεί από την παρατήρηση της κυκλοφοριακής ροής των δεδομένων).
3. Ακεραιότητα δεδομένων (Data Integrity). Αυτή η υπηρεσία εξασφαλίζει ότι κατά τη διάρκεια της μετάδοσής τους τα δεδομένα δεν έχουν τροποποιηθεί από μη εξουσιοδοτημένες οντότητες. Αυτή η υπηρεσία μπορεί να έχει διάφορες μορφές:

    α)Η ακεραιότητα σύνδεσης με αποκατάσταση (connection integrity with recovery) παρέχει την ακεραιότητα των δεδομένων και επίσης ανιχνεύει πιθανή

τροποποίηση, εισαγωγή, διαγραφή, και επανάληψη των δεδομένων. β) Η ακεραιότητα σύνδεσης χωρίς αποκατάσταση (connection integrity without recovery), σε αντίθεση με την προηγούμενη περίπτωση, δεν προσπαθεί την αποκατάσταση της ακεραιότητας. γ) Η επιλεκτική ακεραιότητα σύνδεσης (connection field integrity) παρέχει ακεραιότητα για μόνο σε ορισμένα πεδία δεδομένων σε μια σύνδεση. Αντίστοιχα, μπορούν να χρησιμοποιηθούν και οι χωρίς σύνδεση εκδόσεις των ανωτέρω υπηρεσιών.

4. Μη αποποίηση (non-repudiation). Αυτή η υπηρεσία εξασφαλίζει ότι μία οντότητα δεν μπορεί να αρνηθεί τη μετάδοση ή η παραλαβή ενός μηνύματος. Μπορεί να πάρει τη μία ή και τις δύο από τις παρακάτω μορφές. α) Με την μη αποποίηση με απόδειξη προέλευσης (non-repudiation with proof of origin) παρέχεται στον παραλήπτη των δεδομένων μία απόδειξη της προέλευσής τους, έτσι ώστε ο αποστολέας δεν μπορεί αργότερα να αρνηθεί ότι απέστειλε τα συγκεκριμένα δεδομένα. Με την μη αποποίηση με απόδειξη παράδοσης (non-repudiation with proof of delivery) παρέχεται στον αποστολέα των δεδομένων μία απόδειξη της παράδοσής τους, έτσι ώστε ο παραλήπτης δεν μπορεί αργότερα να αρνηθεί την λήψη των συγκεκριμένων δεδομένων.

Η εφαρμογή των υπηρεσιών ασφάλειας παρέχεται μέσω των μηχανισμών ασφάλειας. Αυτοί μπορούν επίσης να διαιρεθούν σε διάφορες κατηγορίες:

1. Μηχανισμοί Κρυπτογράφησης (Encipherment Mechanisms). Αυτοί οι μηχανισμοί παρέχουν τις υπηρεσίες εμπιστευτικότητας δεδομένων, μετασχηματίζοντας τα δεδομένα σε μορφές οι οποίες δεν είναι αναγνώσιμες από τις μη εξουσιοδοτημένες οντότητες. Οι μηχανισμοί κρυπτογράφησης μπορούν επίσης να χρησιμοποιηθούν και ως συστατικό στοιχείο άλλων μηχανισμών ασφάλειας. Οι αλγόριθμοι κρυπτογράφησης διακρίνονται: α) στους συμμετρικούς ή μυστικού κλειδιού (symmetric or secret-key encipherment), όπου το ίδιο μυστικό κλειδί χρησιμοποιείται και για κρυπτογράφηση και για αποκρυπτογράφηση, και β) στους ασύμμετρους ή δημόσιου κλειδιού (asymmetric or public-key encipherement), όπου χρησιμοποιούνται δύο κλειδιά τα οποία συνδέονται με κάποια μαθηματική σχέση. Το ιδιωτικό κλειδί (public key) χρησιμοποιείται για την κρυπτογράφηση και το δημόσιο κλειδί (public key) για αποκρυπτογράφηση. Η γνώση του δημόσιου κλειδιού δεν οδηγεί στη γνώση του μυστικού κλειδιού.

Και στις δύο κατηγορίες αλγορίθμων κρυπτογράφησης υπάρχουν ζητήματα σχετικά με τη διαχείριση των κλειδιών. Παραδείγματα αλγορίθμων συμμετρικής κρυπτογράφησης είναι οι αλγόριθμοι AES, Twofish, και RC5, ενώ παραδείγματα ασύμμετρης κρυπτογράφησης είναι οι αλγόριθμοι RSA και ElGamal. Αυτοί περιγράφονται λεπτομερέστερα στο Παράρτημα Α. Πολλά διαδεδομένα πρωτόκολλα ασφάλειας δικτύων όπως το SSL (Secure Socket Layer), το TLS (Transport Layer Security) και το IPSec που αναλύονται στο κεφάλαιο 5, αλλά και επίσης μηχανισμούς ασφάλειας όπως τα ιδεατά ιδιωτικά δίκτυα (Virtual Private Networks – VPNs)

2. Ψηφιακές υπογραφές (Digital Signatures). Οι ψηφιακές υπογραφές είναι το ηλεκτρονικό αντίστοιχο των συνηθισμένων υπογραφών για τα ηλεκτρονικά δεδομένα. Οι μηχανισμοί αυτοί κατασκευάζονται συνήθως χρησιμοποιώντας κατάλληλους αλγόριθμους ασύμμετρης κρυπτογράφησης. Η αποκρυπτογράφηση μιας ακολουθίας δεδομένων με τον ιδιωτικό το κλειδί μιας οντότητας αντιστοιχεί στη 3. Μηχανισμοί Ελέγχου Πρόσβασης (Access Control Mechanisms). Οι μηχανισμοί ελέγχου πρόσβασης χρησιμοποιούνται για να παρέχουν την αντίστοιχη υπηρεσία ελέγχου πρόσβασης. Αυτοί οι μηχανισμοί μπορούν να χρησιμοποιήσουν την επικυρωμένη ταυτότητα μιας οντότητας από κάποια υπηρεσία αυθεντικοποίησης ή άλλες πληροφορίες που αφορούν μια οντότητα π.χ., ιδιότητα μέλους (group membership), δικαιώματα (permissions), ή ικανότητες της οντότητας (capabilities), προκειμένου να καθοριστούν και να επιβληθούν τα δικαιώματα πρόσβασης της οντότητας. Οι μηχανισμοί ελέγχου πρόσβασης μπορούν επίσης να αναφέρουν προσπάθειες μη εξουσιοδοτημένης πρόσβασης. Παραδείγματα των μηχανισμών ελέγχου πρόσβασης είναι τα Τείχη Προστασίας (Firewalls)και τα προνόμια πρόσβασης χρηστών των λειτουργικών συστημάτων.
3. Μηχανισμοί Ακεραιότητας Δεδομένων (Integrity Mechanisms). Αυτοί οι μηχανισμοί παρέχουν τις υπηρεσίες ακεραιότητας δεδομένων, επισυνάπτοντας κάποια αθροίσματα ελέγχου (checksums) μνήμης στα δεδομένα τα οποία και μπορούν να αποδείξουν πιθανή τροποποίηση των δεδομένων. Η ακεραιότητα δεδομένων μπορεί να αφορά μια ενιαία μονάδα ή ένα πεδίο δεδομένων, ή μία ροή δεδομένων ή πεδίων δεδομένων. Γενικά, η παροχή ακεραιότητας σε μία ροή δεδομένων, προϋποθέτει την παροχή ακεραιότητας σε κάθε μεμονωμένο πεδίο ή τμήμα δεδομένων. Οι κώδικες αυθεντικοποίησης μηνύματος (Message Authentication Codes – MACs) και οι ψηφιακές υπογραφές μπορεί να χρησιμοποιηθούν ως μηχανισμοί ακεραιότητας δεδομένων.

4. Μηχανισμοί Αυθεντικοποίησης (Authentication Mechanisms). Αυτοί οι μηχανισμοί παρέχουν τις υπηρεσίες επιβεβαίωσης της ταυτότητας μίας οντότητας. Οι μηχανισμοί αυθεντικοποίησης μπορεί να βασίζονται στη χρήση κωδικών πρόσβασης, κρυπτογραφικών τεχνικών (π.χ ψηφιακών υπογραφών) ή βιομετρικών χαρακτηριστικών. Οι κρυπτογραφικοί μηχανισμοί αυθεντικοποίησης μπορούν επίσης να στηρίζονται σε υποδομές εμπιστοσύνης όπως είναι οι Υποδομές Δημόσιου Κλειδιού (Public Key Infrastructures – PKI).
5. Μηχανισμοί Προστασίας Κίνησης (Traffic-Padding). Αυτοί οι μηχανισμοί παρέχουν προστασία από επιθέσεις ανάλυσης κίνησης. Διάφορα πρωτόκολλα δικτύων και μηχανισμοί ασφάλειας περιλαμβάνουν μηχανισμούς προστασίας κίνησης για να προστατεύσουν την επικοινωνία. Για να είναι αποτελεσματικοί οι μηχανισμοί προστασίας κίνησης απαιτείται συνήθως η συνεργασία με την υπηρεσία εμπιστευτικότητας για την κρυπτογράφηση της επικοινωνίας.
6. Μηχανισμοί Ελέγχου Δρομολόγησης (Routing Control Mechanisms). Αυτοί οι μηχανισμοί επιτρέπουν την επιλογή μίας συγκεκριμένης διαδρομής για τα δεδομένα επικοινωνίας, είτε δυναμικά είτε στατικά μέσω προσχεδιασμένων διαδρομών. Επιπλέον, με την εφαρμογή κατάλληλων πολιτικών ασφάλειας, τα δεδομένα τα οποία φέρουν συγκεκριμένες ετικέτες ασφάλειας (security labels) μπορούν να δρομολογηθούν διαμέσου συγκεκριμένων υποδικτύων, αναμεταδόσεων, ή συνδέσεων. Οι ευπάθειες των πρωτοκόλλων δρομολόγησης γίνονται συχνά στόχος των ιών, και άλλων κακόβουλων προγραμμάτων, προκειμένου να εφαρμοστούν επιθέσεις ασφάλειας δικτύων.
7. Μηχανισμοί «Συμβολαιογράφου» (Notarization Mechanisms). Τέλος, οι μηχανισμοί «συμβολαιογράφου» χρησιμοποιούνται για την διασφάλιση της ακεραιότητας, της πηγή ή του προορισμού, και του χρόνου αποστολής ή παράδοσης των μεταδιδόμενων δεδομένων. Τέτοιοι μηχανισμοί μπορούν να αποτελούν μέρος των πρωτοκόλλων δικτύωσης ή να παρέχονται από μία έμπιστη Τρίτη οντότητα η οποία μπορεί να χρησιμοποιηθεί για να βεβαιώσει την συνέπεια και την μη αποποίηση της επικοινωνίας.

1.8 Επιθέσεις Ασφάλειας Δικτύων

Είναι προφανές ότι οι επιθέσεις και οι απειλές ασφάλειας μπορούν να αφορούν οποιοδήποτε επίπεδο δικτύου, από το φυσικό επίπεδο μέχρι το επίπεδο εφαρμογής. Επιπρόσθετα, είναι πιθανό μια επιτυχής επίθεση η οποία εκδηλώθηκε σε ένα δικτυακό επίπεδο να παρακάμψει τα μέτρα ασφάλειας που λαμβάνονται στα άλλα επίπεδα. Μερικές βασικές επιθέσεις ασφάλειας δικτύων περιγράφονται παρακάτω:

- Επιθέσεις Ωτακουστή (Eavesdropping Attacks). Οι επιθέσεις αυτής της κατηγορίας περιλαμβάνουν την τη εξουσιοδοτημένη υποκλοπή της επικοινωνίας και την αποκάλυψη της ανταλλασσόμενης πληροφορίας. Τέτοιες επιθέσεις μπορεί να εκδηλωθούν σε διάφορα επίπεδα. Για παράδειγμα, στο επίπεδο δικτύου μέσω της υποκλοπής (sniffing) των ανταλλασσόμενων πακέτων, ή στο φυσικό στρώμα με φυσική παγίδευση (wiretapping) του ενσύρματου μέσου πρόσβασης.
- Επιθέσεις Εξαπάτησης (Spoofing Attacks). Η επίθεση εξαπάτησης αφορά την περίπτωση όπου μία οντότητα αποκτά παράνομα μία ταυτότητα (π.χ. όνομα χρήστη, IP διεύθυνση, κτλ) – username), για την οποία δεν έχει κανένα δικαίωμα χρήσης. Μια απλή περίπτωση αυτού του τύπου επιθέσεων είναι το IP spoofing, κατά την οποία μία δικτυακή οντότητα εξαπατάται ώστε να θεωρεί ότι επικοινωνεί με μία γνωστή οντότητα. Ο επιτιθέμενος στέλνει ένα πακέτο με τροποποιώντας το πεδίο της IP διεύθυνσης προέλευσης (source IP address) στο επίπεδο μεταφοράς (transport layer). Ο παραλήπτης μπορεί να εξαπατηθεί και να δεχτεί το τροποποιημένο πακέτο όπως έγκυρο.
- Επιθέσεις Εισβολής (Intrusion Attacks). Αυτοί οι τύποι επιθέσεων αφορούν την μη εξουσιοδοτημένη πρόσβαση εξωτερικών χρηστών σε ένα δίκτυο. Μια τέτοια επίθεση εκμεταλλεύεται συνήθως γνωστές ευπάθειες των δικτυακών πόρων. Παραδείγματος χάριν, μια χαρακτηριστική επίθεση εισβολής στο διαδίκτυο είναι η επίθεση υπερχείλισης ενδιάμεσης μνήμης (buffer overflow attack), η οποία εμφανίζεται όταν μια υπηρεσία Ιστού λαμβάνει περισσότερα δεδομένα από όσα είναι προγραμματισμένη να χειριστεί και συνεπώς αντιδρά με απρόβλεπτους και μη αναμενόμενους τρόπους.
- Επιθέσεις Πειρατείας (Hijacking Attacks). Αυτές οι επιθέσεις περιλαμβάνουν προσπάθειες ανάκτησης μη εξουσιοδοτημένης πρόσβασης σε ένα σύστημα, με την χρήση μίας ήδη υπάρχουσας σύνδεσης από κάποια εξουσιοδοτημένη οντότητα. Παραδείγματος χάριν, στο επίπεδο συνόδου (session layer), εάν ένας

χρήστης εγκαταλείψει ανοικτή μία σύνοδο, αυτή μπορεί να υποπέσει θύμα πειρατείας από έναν επιτιθέμενο. Ένα παράδειγμα της πειρατείας συνόδου είναι η επίθεση ακολουθίας αριθμού TCP (TCP sequence number attack). Αυτή η επίθεση εκμεταλλεύεται τη σύνοδο επικοινωνίας που καθιερώθηκε μεταξύ ενός εξυπηρετητή-στόχου και μίας νόμιμης οντότητας που εκκίνησε τη συγκεκριμένη σύνοδο. Ο επιτιθέμενος μπορεί να υποκλέψει τη σύνοδο του νόμιμου οικοδεσπότη, εφόσον προβλέψει τον αριθμό ακολουθίας TCP που χρησιμοποίησε ο νόμιμος οικοδεσπότης.

- Επιθέσεις Κατάχρησης Σύνδεσης (Logon Abuse Attacks). Μια επιτυχής επίθεση κατάχρησης σύνδεσης αφορά την χρήση μίας ενεργής δικτυακής σύνδεσης που έχει εγκατασταθεί με νομότυπο τρόπο μεταξύ δύο οντοτήτων από κάποιον μη εξουσιοδοτημένο χρήστη. Με αυτό τον τρόπο θα παρέκαμπτε τους μηχανισμούς αυθεντικοποίησης και ελέγχου πρόσβασης.
- Επιθέσεις Άρνησης Υπηρεσίας (Denial-of-Service – DOS). Αυτές οι επιθέσεις προσπαθούν να εξαντλήσουν το δίκτυο ή τους πόρους εξυπηρετητών, προκειμένου να αποτρέψουν την επικοινωνία των νόμιμων χρηστών. Μία πιο εξελιγμένη μορφή είναι οι κατανεμημένες επιθέσεις άρνησης υπηρεσιών (Distributed DoS), όπου ο επιτιθέμενος χρησιμοποιεί τους πόρους από ένα κατανεμημένο περιβάλλον ενάντια σε έναν εξυπηρετητή στόχο. Μερικοί γνωστοί τύποι επιθέσεων DOS είναι οι ακόλουθες:
  - ✓ Ping θανάτου (Ping of Death). Αποτελεί μία πρώιμη επίθεση τύπου DOS στην οποία ένας επιτεθείς στέλνει ένα αίτημα ping που είναι μεγαλύτερο από 65.536 bytes, το οποίο είναι το μέγιστο επιτρεπόμενο μέγεθος για το πρωτόκολλο IP. Αυτό προκαλούσε κατάρρευση ή επανέναρξη στο σύστημα. Τέτοιες επιθέσεις δεν εφαρμόζονται σήμερα, δεδομένου ότι τα περισσότερα λειτουργικά συστήματα έχουν εφαρμόσει κατάλληλα μέτρα προστασίας.
  - ✓ Επίθεση SYN (SYN Attack). Σε μια επίθεση SYN, ο επιτιθέμενος εκμεταλλεύεται την αδυναμία μίας διεργασίας ενός εξυπηρετητή να διαχειριστεί τα μη ολοκληρωμένα αιτήματα σύνδεσης. Ο επιτιθέμενος υπερχειλίζει την διεργασία του εξυπηρετητή με αιτήματα σύνδεσης, και στη συνέχεια δεν αποκρίνεται στις αντίστοιχες απαντήσεις (ACK) των αιτημάτων SYN. Αυτό οδηγεί τον εξυπηρετητή σε κατάρρευση, κατά την αναμονή μεγάλου αριθμού απαντήσεων ACK) των αρχικών αιτημάτων.

- Επιθέσεις στο Επίπεδο Εφαρμογής (Application-Level Attacks). Αυτές οι επιθέσεις ασχολούνται με την εκμετάλλευση αδυναμιών στο επίπεδο εφαρμογής και κυρίως περιλαμβάνουν επιθέσεις εισβολής. Για παράδειγμα μπορεί να εκμεταλλεύονται αδυναμίες του εξυπηρετητή διαδικτύου (web server), αδυναμίες μίας συγκεκριμένης τεχνολογίας η οποία χρησιμοποιείται, αδυναμίες ασφάλειας στον κεντρικό υπολογιστή δικτύου, στην συγκεκριμένη τεχνολογία που χρησιμοποιείται σε έναν ιστοχώρο, ή ελλιπείς ελέγχους φιλτραρίσματος (filetering) στα ορίσματα εισόδου από την πλευρά του εξυπηρετητή. Παραδείγματα τέτοιων επιθέσεων περιλαμβάνουν τις κακόβουλες επιθέσεις λογισμικού (ιοί, Δούρειοι Ίπποι, κτλ), επιθέσεις κατά των εξυπηρετητών διαδικτύου (web server attacks), απομακρυσμένη εκτέλεση εντολής (remote command execution), έγχυση ερωτημάτων SQL (SQL injection), και επιθέσεις cross-site scripting (XSS).

2.0 Εξέλιξη πληροφοριακών Συστημάτων

Η ασφάλεια πληροφοριακών συστημάτων μελετήθηκε για πρώτη φορά στις αρχές της δεκαετίας του 1970. Η πρώτη σχετική δημοσίευση, από την Ομάδα Εργασίας του Συμβουλίου Αμυντικής Επιστήμης του υπουργείου Άμυνας των ΗΠΑ, εξέτασε το πρόβλημα της χρήσης υπολογιστών εξ αποστάσεως (μέσω τερματικών). Προηγουμένως, η πρόσβαση στους υπολογιστικούς πόρους προϋπέθετε την φυσική παρουσία και πρόσβαση του χρήστη ή του διαχειριστή στον κεντρικό υπολογιστή. Η προσέγγιση στην λύση των προβλημάτων ασφάλειας μέχρι τότε βασιζόταν στην φυσική απομόνωση και προστασία του κεντρικού υπολογιστή καθώς και στον έλεγχο πρόσβασης σε αυτόν. Ένα από τα συμπεράσματα στην αναφορά της Ομάδας Εργασίας ήταν ότι ο χρήστης δεν θα έπρεπε να δημιουργήσει το δικό του κωδικό πρόσβασης, μια πρόταση που ποτέ δεν υιοθετήθηκε ευρέως. Άλλες καινοτόμες ιδέες που εκφράστηκαν στην ανάλυση είχαν μεγαλύτερη απήχηση. Για παράδειγμα, αναγνωρίστηκε από τους ερευνητές η αρχή της ισορροπίας μεταξύ της ευκολίας της εργασίας του χρήστη και της προστασίας των πληροφοριών και σήμερα έχει καταλήξει θεμέλιος λίθος στη δημιουργία πολιτικών ασφάλειας.

Ο πρώτος ιός, ο Creeper, εμφανίστηκε επίσης στις αρχές της δεκαετίας του 1970 στο ARPANET, και το πρώτο δικτυακό «σκουλήκι» (worm), το σκουλήκι Morris, κυκλοφόρησε το 1998. Εκτιμάται ότι 6.000 συστήματα προσβλήθηκαν από το «σκουλήκι». Το 2007 ανακαλύφθηκαν περισσότεροι από 711.000 καινούργιοι ιοί.

Παρόλο που ο πρώτος υπολογιστής με το λειτουργικό σύστημα Multics εγκαταστάθηκε το 1967 με κωδικό πρόσβασης για χρήστες και με άλλα μέτρα ασφάλειας στο σχεδιασμό του, και δύο από τους δημιουργούς του, ο Ken Thompson και ο Dennis Ritchie, έπαιξαν κρίσιμο ρόλο στην ανάπτυξη του Unix, η πρώτη έκδοση του Unix δεν διέθετε κωδικούς. Η λειτουργία αυτή προστέθηκε αργότερα, το 1973. Σήμερα η χρήση αδύναμων κωδικών πρόσβασης παραμένει μία από τις κυριότερες δυσκολίες που αντιμετωπίζει ο επαγγελματίας στον τομέα.[13] Χρησιμοποιούνται και άλλες μέθοδοι αυθεντικοποίησης, για παράδειγμα οι έξυπνες κάρτες, αλλά μόνο σε συγκεκριμένους τομείς.

2.1 Βασικές αρχές Πληροφοριακών Συστημάτων

Η ασφάλεια πληροφοριακών συστημάτων στηρίζεται σε τρεις βασικές ιδέες:

Ακεραιότητα

Η ακεραιότητα αναφέρεται στη διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μια γνωστή κατάσταση χωρίς ανεπιθύμητες τροποποιήσεις, αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα, καθώς και την αποτροπή της πρόσβασης ή χρήσης των υπολογιστών και δικτύων του συστήματος από άτομα χωρίς άδεια.

Για παράδειγμα, μια εφημερίδα που δημοσιεύει τα άρθρα της και στο Διαδίκτυο θα ήθελε αυτά τα άρθρα να είναι ασφαλή από μετατροπές ενός χάκερ που επιθυμεί να εισάγει λανθασμένες πληροφορίες στα κείμενα.

Διαθεσιμότητα

Η διαθεσιμότητα των δεδομένων και των υπολογιστικών πόρων είναι η εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα θα είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους.

Μία τυπική απειλή που αντιμετωπίζουν τα σύγχρονα πληροφοριακά συστήματα είναι η επίθεση άρνησης υπηρεσιών (DOS attack), που έχει ως σκοπό να τεθούν εκτός λειτουργίας οι στοχευμένοι πόροι είτε προσωρινά, είτε μόνιμα. Η άρνηση υπηρεσιών δεν προκαλείται αναγκαία από εχθρική επίθεση. Το φαινόμενο Slashdot, κατά το οποίο ένας σύνδεσμος προς μια ιστοσελίδα φιλοξενούμενη σε διακομιστή με σύνδεση χαμηλής χωρητικότητας δημοσιεύεται σε δημοφιλή ιστότοπο, με συνέπεια εκατοντάδες χιλιάδες αναγνώστες να υπερφορτώσουν τη σύνδεση της αναφερομένης ιστοσελίδας, προκαλεί το ίδιο αποτέλεσμα.

Εμπιστευτικότητα

Η εμπιστευτικότητα σημαίνει ότι ευαίσθητες πληροφορίες δεν θα έπρεπε να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα.

Η διαρροή ευαίσθητων πληροφοριών μπορεί να γίνει με πιο παραδοσιακές μεθόδους από την ψηφιακή υποκλοπή, π.χ. με την κλοπή φορητών υπολογιστών από το κατάλληλο τμήμα μιας εταιρίας. Το 2006 μια μελέτη με τη συνεργασία 480 εταιριών έδειχνε ότι 80% των εταιριών είχε πρόβλημα με διαρροή πληροφοριών λόγο κλοπής φορητού.

2.2 Ασφάλεια Πληροφοριακών Συστημάτων

Το εύρος της ασφάλειας Πληροφοριακών Συστημάτων, πιθανές απειλές σε Πληροφοριακό Σύστημα (ΠΣ) καθώς και νέες τάσεις και τεχνολογίες που χρησιμοποιούνται στην επίτευξη των στόχων ασφάλειας σε κάποιο Ολοκληρωμένο Πληροφοριακό Σύστημα κάποιας επιχείρησης ή οργανισμού.

Αρχικά είναι σημαντικό για την εξέλιξη της ενότητας αυτής να δοθεί ένας ορισμός του Πληροφοριακού Συστήματος αλλά και στο τι εννοούμε ως ασφάλεια Πληροφοριακού Συστήματος. Ως Πληροφοριακό Σύστημα μπορούμε να ορίσουμε ένα οργανωμένο σύνολο από πέντε στοιχεία (άνθρωποι, λογισμικό, υλικό, διαδικασίες και δεδομένα), τα οποία αλληλεπιδρούν μεταξύ τους και με το περιβάλλον, με σκοπό την παραγωγή και διαχείριση πληροφορίας, για την υποστήριξη ανθρώπινων δραστηριοτήτων, στα πλαίσια του οργανισμού.

Ως ασφάλεια Πληροφοριακού Συστήματος μπορούμε να ορίσουμε εκείνο το οργανωμένο πλαίσιο εννοιών, αντιλήψεων, αρχών, πολιτικών, διαδικασιών, τεχνικών και μέτρων που απαιτούνται για να προστατευθούν τα στοιχεία του Πληροφοριακού Συστήματος αλλά και το σύστημα ολόκληρο, από κάθε σκόπιμη ή τυχαία απειλή.

2.3 Σχεδιασμός πολιτικής ασφαλείας

Ο σχεδιασμός ασφαλών πολιτικών στα πληροφοριακά συστήματα, συνδέεται άμεσα τόσο με τεχνικές, διαδικασίες και διοικητικά μέτρα όσο και με ηθικό-κοινωνικές αντιλήψεις, αρχές και παραδοχές, προφυλάσσοντας από κάθε είδους απειλή τυχαία ή σκόπιμη. Οι διαδικασίες σχεδιασμού πολιτικών ασφαλείας, δεν θα πρέπει να παρεμβαίνουν στην απρόσκοπτη λειτουργία των πληροφοριακών συστημάτων, ενώ οφείλουν να τηρούν την αρχή της αποκέντρωσης, της ύπαρξης αντικατάστασης και την αρχή της άμυνας σε βάθος. Ως βάση μπορεί να οριστεί ο εντοπισμός, η αξιολόγηση και στη συνεχεία η διαμόρφωση ενός θεωρητικού πλαισίου για το σχεδιασμό πολιτικών σχεδιασμού ασφάλειας.

Το πιο βασικό σημείο στη διαδικασία σχεδιασμού ασφαλών πολιτικών, είναι ο εντοπισμός και χαρακτηρισμός ως εμπιστευτικών των πληροφοριών που πρόκειται να χρησιμοποιηθούν και να προστατευθούν. Εκτός από τις αρχές της Ακεραιότητας Πληροφοριών, την Εμπιστευτικότητα και τη Διαθεσιμότητα Πληροφοριών οι πολιτικές ασφάλειας θα πρέπει να εμπεριέχουν και τους όρους αυθεντικότητα, εγκυρότητα, μοναδικότητα και μη αποποίηση.

Ωστόσο, οι πολιτικές ασφάλειας προϋποθέτουν την ύπαρξη μίας δέσμης βασικών αρχών, εκφρασμένων με σαφήνεια η οποία να περιλαμβάνει τους σχεδιαστικούς στόχους των λειτουργικών συστημάτων. Κάθε αντικείμενο του συστήματος θα πρέπει να μπορεί να αναγνωρισθεί μονοσήμαντα και να συνοδεύεται από μία ένδειξη του βαθμού εμπιστευτικότητας. Επιπλέον, η ισχύς των ασφαλιστικών μηχανισμών δεν θα πρέπει να βασίζονται στην άγνοια των χρηστών, σχετικά με τις τεχνικές ασφαλείας οι οποίες χρησιμοποιούνται. Αλλά στην αποτελεσματική τους σχεδίαση.

Στόχος ενός συστήματος πολιτικής ασφάλειας είναι ο περιορισμός επικινδυνότητας σε αποδεκτό επίπεδο. Το σύστημα περιλαμβάνει αξιολόγηση της επικινδυνότητας και περιορισμό του αποδεκτού επιπέδου ασφαλείας, ανάπτυξη και εφαρμογή μιας πολιτικής ασφαλείας καθώς και δημιουργία κατάλληλου οργανωτικού πλαισίου και εξασφάλιση των απαιτούμενων πόρων για την εφαρμογή της πολιτικής ασφάλειας. Η πολιτική ασφάλεια μαζί με το σύνολο των μέτρων προστασίας αποτελούν το σχέδιο ασφαλείας (security plan) για τα πληροφοριακά συστήματα ενός οργανισμού διότι χρειαζόμαστε ένα ολοκληρωμένο πλαίσιο με την καθοδήγηση των μέτρων ασφαλείας να λειτουργεί ως μέσο επικοινωνίας των εμπλεκομένων στα ζητήματα ασφαλείας.

Επιπλέον θεμελιώνεται η σημασία της ασφάλειας του πληροφοριακού συστήματος για τα μέλη του οργανισμού, δημιουργείται μια κουλτούρα ασφαλείας καθώς πολλές φορές αποτελεί νομική υποχρέωση και αποτελεί παράγοντα εμπιστοσύνης μεταξύ οργανισμού και πελατών. Τα είδη των πολιτικών ασφαλείας είναι α)τα τεχνικά (computer oriented) συστήματα πληροφοριών, λειτουργικά συστήματα και δίκτυα υπολογιστών β)τα οργανωτικά (human oriented) και γ)τα ατομικά (individual security policies). Περιλαμβάνει αποσπασματική διαχείριση της ασφάλειας πληροφοριακών συστημάτων και μεγάλη πολυπλοκότητα στη συντήρηση ενώ αποτελεσματική σε αυτόνομες εφαρμογές κ υπολογιστικά συστήματα που δεν συνδέονται μεταξύ τους.

Σε ένα ενιαίο έγγραφο μη εύχρηστο λόγω όγκου και με πληροφορίες γενικού επιπέδου αναφέρονται όλα τα υπολογιστικά συστήματα, οι εφαρμογές και η διαδικασία του πληροφοριακού συστήματος.

Τις απαιτήσεις για την ασφάλεια του πληροφοριακού συστήματος πρέπει να την ικανοποιεί η πολιτική ασφάλεια που προέρχονται από όλους τους εμπλεκόμενους στη χρήση κ στη λειτουργία του πληροφοριακού συστήματος ενός οργανισμού που είναι οι χρήστες κ οι διαχειριστές του πληροφοριακού συστήματος, η διοίκηση του οργανισμού, οι πελάτες του οργανισμού, οι νομικές και κανονιστικές διατάξεις που διέπουν την λειτουργία τους.

Ο καθορισμός της πολιτικής ασφάλειας του πληροφοριακού συστήματος θα πρέπει να καλύπτουν οι ακόλουθες κατηγορίες:

- Ζητήματα προσωπικού
- Φυσική ασφάλεια
- Έλεγχος πρόσβασης στο πληροφοριακό σύστημα
- Διαχείριση υλικών και λογισμικών
- Νομικές υποχρεώσεις
- Διαχείριση της πολιτικής ασφάλειας
- Οργανωτική δομή
- Σχέδιο συνέχισης λειτουργίας

Όταν εφαρμόζουμε μια πολιτική ασφαλείας επιδιώκουμε:

- ❖ οι οδηγίες και τα μέτρα προστασίας οφείλουν να καλύπτουν το σύνολο των αγαθών και όλες τις λειτουργίες(πληρότητα)
- ❖ να λάβουμε υπόψη τις τρέχουσες τεχνολογικές εξελίξεις (επικαιρότητα)

- με κάποιες τροποποιήσεις ή προσθήκες να μπορεί η πολιτική να καλύπτει μικρές αλλαγές ή επεκτάσεις στο πληροφοριακό σύστημα (γενικευσιμότητα). Επιπλέον πρέπει να υπάρχει σαφήνεια κ εύκολη κατανόηση, τεχνολογική ανεξαρτησία και καταλληλότητα ανάλογα με τον οργανισμό που απευθύνεται.

Για να είναι επιτυχές ένα σύστημα πολιτικής ασφάλειας οφείλει να υποστηρίζει τους επιχειρηματικούς στόχους, να συμμετέχει η διοίκηση, να είναι κατάλληλη για το περιβάλλον που εφαρμόζεται, οι χρήστες να εκπαιδεύονται κατάλληλα, να υπάρχει αξιολόγηση και η πρόσβαση να είναι εύκολη και άμεση για όλους τους χρήστες του πληροφοριακού συστήματος. Τέλος το περιεχόμενο και οι εφαρμογές πρέπει να ανανεώνονται τακτικά.

2.4 Σκοποί επιθέσεων σε Πληροφοριακά Συστήματα

Αν μπορούσαμε να κατηγοριοποιήσουμε τις σκόπιμες ενέργειες με πρόθεση την παραβίαση των απαιτήσεων ασφάλειας του ΠΣ (επιθέσεις), με βάση το στόχο τους και το σκοπό τους μπορούμε να πούμε ότι είναι σε θέση να προκαλέσουν τα παρακάτω:

- Εισαγωγή ή Μετατροπή δεδομένων στο σύστημα (αφαίρεση, μεταβολή, διαγραφή, πρόσθεση ψευδών στοιχείων κλπ).
- Μείωση της αξιοπιστίας των δεδομένων και κατά συνέπεια της επιχείρησης ή του οργανισμού.
- Παρεμπόδιση λειτουργίας συστήματος και υπηρεσιών.
- Εισβολή και Παραβίαση Δικαιωμάτων, είτε του δημιουργού, είτε των νόμιμων δικαιούχων είτε πληροφοριακού υλικού.

2.4.1 Οι «εχθροί» των Πληροφοριακών Συστημάτων

Έχει σημασία να δει κανείς ποιοι είναι αυτοί οι οποίοι απειλούν ένα Πληροφοριακό Σύστημα. Οι επιτιθέμενοι θα μπορούσαν να χωριστούν σε 2 μεγάλες κατηγορίες, στους εσωτερικούς (πχ. Υπάλληλοι, στελέχη κλπ) και τους εξωτερικούς (hackers, ανταγωνιστές κλπ). Περνώντας στα στατιστικά στοιχεία που συνήθως λένε την αλήθεια

μπορεί κανείς να βρεθεί σε μια μεγάλη αλήθεια. Σε παλιότερη έρευνα στις Ηνωμένες Πολιτείες ανακαλύφθηκε ότι οι περισσότερες επιθέσεις έρχονται από το εσωτερικό περιβάλλον παρά από το εξωτερικό περιβάλλον. Πιο αναλυτικά φαίνεται ότι το 55% των παραβιάσεων έγινε από υπαλλήλους του οργανισμού, 38% από χάκερς και το 7% από ανταγωνιστές (Μπόζιος Ε., 2004). Αυτή η έρευνα θέτει σοβαρά ζητήματα στο πως εξετάζουν πλέον οι επιχειρήσεις την ασφάλεια του συστήματος τους αλλά βέβαια και το πως μπλέκεται ο ανθρώπινος παράγοντας στην ασφάλεια.

Τέλος διαπιστώθηκε ότι στόχοι των χάκερς είναι κυρίως τράπεζες, κυβερνητικοί οργανισμοί και συστήματα, τηλεπικοινωνιακοί φορείς αλλά και επιχειρήσεις διαφορετικής φύσεως.

2.5 Ασφάλεια Λειτουργικών Συστημάτων

Σύμφωνα με τον ορισμό του American Standards Institute (ANSI), Λειτουργικό Σύστημα (Λ.Σ.) (Operating System) ενός υπολογιστή ονομάζεται το προϊόν λογισμικού που ελέγχει την εκτέλεση των προγραμμάτων του υπολογιστή και παρέχει υπηρεσίες χρονοκατανομής (time sharing), αποσφασλμάτωσης (debugging), ελέγχου εισόδου εξόδου (I/O control), μεταγλώττισης (compilation), διαχείρισης μνήμης και δεδομένων, καθώς και άλλες υπηρεσίες. Το Λειτουργικό Σύστημα παρέχει τους μηχανισμούς επικοινωνίας των τελικών εφαρμογών με το υλικό του συστήματος.

Η ασφάλεια του ΛΣ θεωρείται κρίσιμη για την ασφαλή λειτουργία του υπολογιστικού συστήματος, διότι το ΛΣ είναι αυτό που μπορεί να διασφαλίσει τα παρακάτω :

- Τα χαρακτηριστικά ασφάλειας των ίδιων των υπηρεσιών που παρέχει.
- Την καταστολή των απειλών που προέρχονται από τα υψηλότερα επίπεδα.
- Την απομόνωση των απειλών που προέρχονται από τα χαμηλότερα επίπεδα, έτσι ώστε να μην επηρεαστεί η λειτουργία των τελικών εφαρμογών (Κάτσικας κ.α. 2004).

2.5.1 Προστασία Λειτουργικών Συστημάτων

Τα Λειτουργικά Συστήματα τα οποία εξυπηρετούν ανάγκες σύγχρονων πολυεπεξεργαστικών συστημάτων έχουν σύνθετες και αυξημένες απαιτήσεις ασφάλειας των μερών τους και των στοιχείων τους.

Τέτοια στοιχεία είναι τα παρακάτω :

- Δεδομένα που βρίσκονται σε μνήμες (RAM, σκληροί δίσκοι κλπ)
- Εκτελέσιμα προγράμματα και διεργασίες (processes)
- Συσκευές εισόδου εξόδου και δικτύου
- Διεργασίες και δεδομένα του ΛΣ

Είναι σημαντικό βέβαια τα παραπάνω στοιχεία και μέρη του Λειτουργικού Συστήματος να προστατεύονται ασφαλώς προκειμένου να τηρούνται οι παρακάτω προϋποθέσεις και απαιτήσεις:

- Ευχρηστία (usability)
- Αποδοτικότητα (efficiency)
- Ακεραιότητα (integrity)
- Εμπιστευτικότητα (confidentiality)
- Αυθεντικότητα (authenticity)
- Διαθεσιμότητα (availability)
- Ευκινησία (capacity)
- Ανιχνευσιμότητα (detectability)

2.5.2 Απειλές και ζητήματα Ασφάλειας

Όπως αναφέρθηκε και παραπάνω σε ένα Λειτουργικό Σύστημα (ΛΣ) υπάρχει σημαντικός κίνδυνο για απώλεια, αλλοίωση και καταστροφή δεδομένων όπως επίσης και για αποκάλυψη τους. Επίσης υπάρχει και το ενδεχόμενο της μη εξουσιοδοτημένης πρόσβασης του συστήματος από μη δικαιούχες οντότητες που έχουν σκοπό την εκμετάλλευση αυτού η των πόρων του.

Κίνητρα κακόβουλων χρηστών μπορεί να είναι η περιέργεια, το άμεσο ή έμμεσο οικονομικό όφελος, η πρόκληση δυνατοτήτων του κακόβουλου χρήστη ή τέλος η βιομηχανική κατασκοπία η οποία σύμφωνα με έρευνες έχει εκτιναχθεί στα ύψη τη τελευταία δεκαετία.

Όπως αναφέραμε και πριν το ΛΣ γίνεται συχνά στόχος τέτοιων επιθέσεων και κακόβουλων ενεργειών και απειλών. Μερικές απ' αυτές τις απειλές παρουσιάζονται παρακάτω (Gritzalis and Spinellis, 1997):

Αποκάλυψη κωδικών-συνθηματικών: Η πλέον συνήθης απειλή σε ένα ΛΣ. Οι κακόβουλοι χρήστες αποκτούν πρόσβαση στο σύστημα με αυτό το τρόπο και πολλές φορές φτάνουν να έχουν δικαιώματα διαχειριστή (administrator, superuser κλπ).

Μη εξουσιοδοτημένη εκτέλεση λογισμικού: Λογισμικό το οποίο έχει εγκατασταθεί παράνομα στο σύστημα από μη εξουσιοδοτημένους χρήστες και μπορεί να προκαλέσει ζημιές και απώλειες στο υπολογιστικό σύστημα. Άρνηση Υπηρεσίας: Κατασπατάληση των πόρων του συστήματος σε μέγιστο βαθμό, τέτοιο ώστε να γίνεται αδύνατη η προσπέλαση και η χρήση της υπηρεσίας από τους άμεσα ενδιαφερόμενους.

Κακόβουλες ενέργειες: Τέτοιες ενέργειες, όπως η τροποποίηση δεδομένων, η καταστροφή αρχείων συστήματος (system files) ή και φυσική καταστροφή ακόμα.

Συμπτωματικές ασυνέπειες και σφάλματα: Προέρχονται από κατασκευαστικές και προγραμματιστικές ατέλειες και ασάφειες και από την αμέλεια του διαχειριστή να παρακολουθήσει τις προσθήκες και τις επιδιορθώσεις που ανακοινώνει ο κατασκευαστής του συστήματος

Ιομορφικό Λογισμικό: Οποιασδήποτε μορφής πρόγραμμα που μπορεί να προκαλέσει ζημιές ή και βλάβες στο σύστημα (πχ. Trojan horses, viruses, worms κλπ).

Κερκόπορτα (backdoor): Διάταξη στο κώδικα κάποιου προγράμματος η οποία επιτρέπει παράκαμψη ασφάλειας.

Ανθρώπινος παράγοντας: Ένα σύνθετο και συνήθως δύσκολα αντιμετωπίσιμο πρόβλημα στην ασφάλεια υπολογιστών. Η δυσκολία του έγκειται στο στοιχείο του απρόβλεπτου λόγω τις μεγάλης γκάμας αντιδράσεων των χρηστών σε υπολογιστικά συστήματα.

2.5.3 Μηχανισμοί ασφάλειας Λειτουργικών Συστημάτων

Όπως έγινε αντιληπτό και από τα παραπάνω τα Λειτουργικά Συστήματα έχουν κάποιες απαιτήσεις ασφάλειας οι οποίες πρέπει να διαφυλαχθούν. Για να επιτευχθεί αυτό επιστρατεύονται διάφοροι μηχανισμοί ασφάλειας που εξυπηρετούν διαφορετικούς σκοπούς προκειμένου τελικά να υπάρξει το ζητούμενο επίπεδο ασφάλειας (Tanenbaum, 2008). Μερικοί από τους παρακάτω μηχανισμούς είναι οι παρακάτω :

- Μηχανισμοί Αυθεντικοποίησης Χρηστών
- Μηχανισμοί Ελέγχου Προσπέλασης
- Μηχανισμοί Διαθεσιμότητας Συστήματος
- Μηχανισμοί Ακεραιότητας Λογισμικού και Δεδομένων
- Μηχανισμοί Καταγραφής και Παρακολούθησης
- Μηχανισμοί Εμπιστευτικότητας Ευαίσθητων Δεδομένων Είναι κατανοητό βέβαια πως αυτοί οι μηχανισμοί υλοποιούνται με συγκεκριμένα μέτρα και ενέργειες στα οποία θα γίνει ανάλυση αν χρειαστεί κατά τα παρακάτω κεφάλαια και στην εφαρμογή πρακτικών θεμάτων.

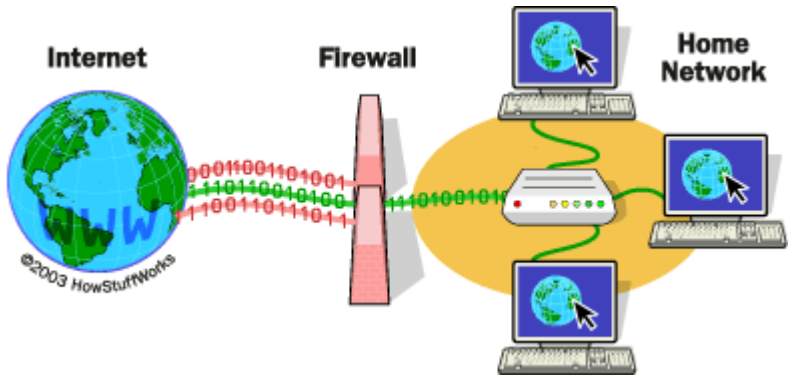
3.0 Εισαγωγή στα Τείχη Προστασίας (Firewalls)

α) Τι είναι Τείχος Προστασίας;

Όταν οι περισσότεροι άνθρωποι ακούν τον όρο firewall, σκέφτονται μια συσκευή που υπάρχει στο δίκτυο και ελέγχει τα δεδομένα που περνούν από ένα δίκτυο υπολογιστών σε ένα άλλο. Ωστόσο, τα τείχη προστασίας μπορούν επίσης να εφαρμοστούν και στα ίδια τα συστήματα υπολογιστών, όπως το Microsoft Internet Connection Firewall (ICF). Σε αυτή την περίπτωση είναι γνωστές ως host-based firewalls. Και οι δύο τύποι αντιπυρικών ζωνών έχουν τον ίδιο στόχο:

- Να παρέχουν μια μέθοδο που θα ενισχύει την πολιτική ελέγχου πρόσβασης. Στον απλούστερο ορισμό, τα τείχη προστασίας δεν είναι τίποτα περισσότερο από σημεία επιβολής πολιτικής ελέγχου πρόσβασης.

Στην επιστήμη των υπολογιστών ο όρος firewall ή τείχος προστασίας χρησιμοποιείται για να δηλώσει κάποια συσκευή ή πρόγραμμα που είναι έτσι ρυθμισμένο ούτως ώστε να επιτρέπει ή να απορρίπτει πακέτα δεδομένων που περνούν από ένα δίκτυο υπολογιστών σε ένα άλλο.



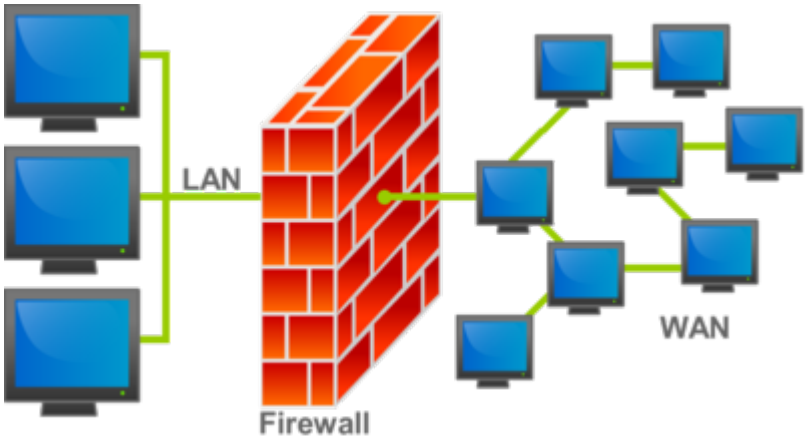
Εικόνα 2: Firewall

Τα Τείχη Προστασίας επιτρέπουν να καθορίσουμε μια απαίτηση ελέγχου πρόσβασης και να εξασφαλίσουμε ότι μόνο η κίνηση (traffic) που πληρεί την απαίτηση μπορεί να διαπεράσει την αντιπυρική ζώνη (στην περίπτωση ενός network-based firewall) ή να έχει πρόσβαση στο προστατευμένο σύστημα (στην περίπτωση του host-based firewall).

3.1 Λειτουργία Τειχών Προστασίας

Η κύρια λειτουργία ενός firewall είναι η ρύθμιση της κυκλοφορίας δεδομένων ανάμεσα σε δύο δίκτυα υπολογιστών. Συνήθως τα δύο αυτά δίκτυα είναι το Διαδίκτυο και το τοπικό/εταιρικό δίκτυο. Ένα firewall παρεμβάλλεται ανάμεσα σε δύο δίκτυα που έχουν διαφορετικό επίπεδο εμπιστοσύνης. Το Διαδίκτυο έχει μικρό βαθμό εμπιστοσύνης (low level of trust), ενώ το εταιρικό δίκτυο ή το οικιακό δίκτυο διαθέτουν τον μέγιστο βαθμό εμπιστοσύνης. Ένα περιμετρικό δίκτυο (perimeter network) ή μία Demilitarized Zone (DMZ) διαθέτουν μεσαίο επίπεδο εμπιστοσύνης.

Ο σκοπός της τοποθέτησης ενός firewall είναι η πρόληψη επιθέσεων στο τοπικό δίκτυο και η αντιμετώπισή τους. Παρόλα αυτά όμως, ένα firewall μπορεί να αποδειχθεί άχρηστο εάν δεν ρυθμιστεί σωστά. Η σωστή πρακτική είναι το firewall να ρυθμίζεται ούτως ώστε να απορρίπτει όλες τις συνδέσεις εκτός αυτών που επιτρέπει ο διαχειριστής του δικτύου (default-deny). Για να ρυθμιστεί σωστά ένα firewall θα πρέπει ο διαχειριστής του δικτύου να έχει μία ολοκληρωμένη εικόνα για τις ανάγκες του δικτύου και επίσης να διαθέτει πολύ καλές γνώσεις πάνω στα δίκτυα υπολογιστών. Πολλοί διαχειριστές δεν έχουν αυτά τα προσόντα και ρυθμίζουν το firewall ούτως ώστε να δέχεται όλες τις συνδέσεις εκτός από εκείνες που ο διαχειριστής απαγορεύει (default-allow). Η ρύθμιση αυτή καθιστά το δίκτυο ευάλωτο σε επιθέσεις από εξωτερικούς χρήστες.



Εικόνα 3: Διάταξη Firewall

3.2 Τι κάνουν τα Τείχη Προστασίας

Όλα τα Τείχη Προστασίας μοιράζονται μερικά κοινά γνωρίσματα και λειτουργίες που καθορίζουν τι μπορεί μια αντιπυρική ζώνη να κάνει. Οι αντιπυρικές ζώνες πρέπει να είναι σε θέση να εκτελέσουν τις ακόλουθους εργασίες:

1. Διαχείριση και έλεγχο την κίνησης στο δίκτυο
2. Επικύρωση πρόσβασης
3. Λειτουργία μεσολαβητή
4. Προστασία πόρων
5. Καταγραφή και αναφορά συμβάντων

3.2.1 Διαχείριση και έλεγχος την κίνησης στο δίκτυο

Η πρώτη και θεμελιώδης λειτουργία που όλα τα Τείχη Προστασίας πρέπει να εκτελέσουν είναι να διαχειρίζονται και να ελέγχουν την κίνηση που επιτρέπεται να έχει πρόσβαση στο προστατευμένο δίκτυο ή υπολογιστή. Τα Τείχη Προστασίας επιτυγχάνουν αυτό με την επιθεώρηση των πακέτων και των έλεγχο των συνδέσεων που πραγματοποιούνται. Φιλτράρουν τις συνδέσεις συμφώνα με τα αποτελέσματα της επιθεώρησης πακέτων (packet-inspection) και των συνδέσεων.

Επιθεώρηση πακέτων: Είναι η διαδικασία της επεξεργασίας των δεδομένων σε ένα πακέτο με στόχο να καθορίσει εάν πρέπει να επιτραπεί ή απαγορευτεί σύμφωνα με την προκαθορισμένη πολιτική πρόσβασης.

Η επιθεώρηση πακέτων μπορεί να εξετάσει ένα ή όλα τα ακόλουθα στοιχεία:

- IP διεύθυνση πηγής (Source IP address)
- Θύρα πηγής (Source port)
- IP διεύθυνση προορισμού (Destination IP address)
- Θύρα προορισμού (Destination port)
- IP πρωτόκολλο (IP protocol)
- Πληροφορίες επικεφαλίδας πακέτων (Packet header information)

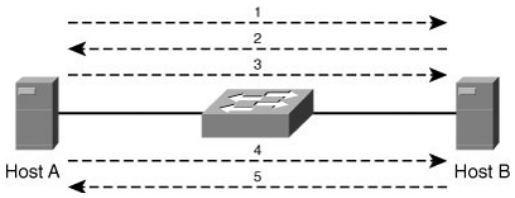
Ένα σημαντικό γεγονός είναι ότι για την επιθεώρηση πακέτων είναι ότι για να πάρουν τα τείχη προστασίας μια απόφαση φιλτραρίσματος, πρέπει να επιθεωρήσει κάθε πακέτο

σε κάθε κατεύθυνση και σε όλες τις διεπαφές. Επίσης, για κάθε πακέτο που θα επιθεωρηθεί πρέπει να υπάρξουν κανόνες ελέγχου πρόσβασης. Αυτή η απαίτηση μπορεί να παρουσιάσει πρόβλημα όταν έρχεται η σειρά που πρέπει να καθοριστεί ένας κανόνας ελέγχου πρόσβασης για να εξεταστεί η επιστρεφόμενη κυκλοφορία από ένα επιτρεπόμενο αίτημα.

Συνδέσεις και κατάσταση: Για να επικοινωνήσουν δύο TCP/IP hosts πρέπει πρώτα να καθιερώσουν κάποια σύνδεση. Οι συνδέσεις εξυπηρετούν δύο σκοπούς. Καταρχήν, μπορούν να χρησιμοποιήσουν τη σύνδεση για να προσδιοριστούν εκατέρωθεν. Ο προσδιορισμός εξασφαλίζει ότι τα συστήματα δεν παραδίδουν ακούσια τα στοιχεία στους hosts που δεν περιλαμβάνονται στη σύνδεση. Τα τείχη προστασίας μπορούν να χρησιμοποιήσουν αυτές τις πληροφορίες σύνδεσης για να καθορίσουν τις συνδέσεις που επιτρέπονται μεταξύ των hosts από την πολιτική ελέγχου πρόσβασης και έτσι να καθορίζουν εάν τα στοιχεία πρέπει να επιτραπούν ή να απορριφτούν.

Στη συνεχεία, οι συνδέσεις χρησιμοποιούνται για να καθορίσουν τον τρόπο με τον οποίο δύο hosts θα επικοινωνήσουν μεταξύ τους. Για το πρωτόκολλο ελέγχου μεταφοράς (TCP), αυτός ο τύπος σύνδεσης είναι γνωστός ως σύνοδος προσανατολισμένη προς τη σύνδεση (connection-oriented session). Για το πρωτόκολλο διαγραμμάτων δεδομένων χρηστών (UDP) και το πρωτόκολλο μηνυμάτων ελέγχου διαδικτύου (ICMP), αυτός ο τύπος σύνδεσης είναι γνωστός ως σύνοδος χωρίς σύνδεση (connectionless session).

Η προκαθορισμένη δομή μιας σύνδεσης μπορεί να χρησιμοποιηθεί για να καθορίσει την κατάσταση των επικοινωνιών μεταξύ δύο hosts. Για παράδειγμα όταν ο host A προσπαθεί να επικοινωνήσει με τον host B, ο A ξεκινά ένα αίτημα σύνδεσης. Έπειτα ο host B ανταποκρίνεται στο αίτημα σύνδεσης προσδιορίζοντας με αυτό τον τρόπο πώς οι δύο hosts θα γνωρίζουν τα δεδομένα που πρέπει να σταλούν καθώς και το πότε πρέπει να σταλούν. Το παρακάτω σχήμα δείχνει αυτή τη διαδικασία:



Εικόνα 4: Διαδικασία επικοινωνίας μεταξύ δυο host

1. Ο Host A αρχίζει μια σύνδεση προς το Host B.
2. Ο Host B ανταποκρίνεται στο αίτημα σύνδεσης από το Host A.
3. Ο Host A οριστικοποιεί τη σύνδεση με το Host B, επιτρέποντας τη μεταφορά των δεδομένων.
4. Ο Host A αρχίζει να μεταδίδει τα απαραίτητα δεδομένα στο Host B.
5. Ο Host B αποκρίνεται όπως απαιτείται, είτε με τα ζητούμενα δεδομένα, είτε για να αναγνωρίσει περιοδικά την παραλαβή των στοιχείων από το Host A.

Τα τείχη προστασίας μπορούν να παρακολουθήσουν τις πληροφορίες κατάστασης σύνδεσης για να καθορίσουν εάν θα επιτρέψουν ή θα αρνηθούν την κυκλοφορία. Παραδείγματος χάριν, όταν η αντιπυρική ζώνη βλέπει το πρώτο αίτημα σύνδεσης από το Host A (βήμα 1), γνωρίζει ότι το επόμενο στοιχείο που πρέπει να δει είναι η αναγνώριση του αιτήματος σύνδεσης από το Host B (βήμα 2). Αυτό γίνεται με τη χρήση ενός πίνακα κατάστασης (state table) που διατηρεί την κατάσταση όλων των συνομιλιών που διαπερνούν την αντιπυρική ζώνη. Με τον έλεγχο της κατάστασης συνομιλίας, η αντιπυρική ζώνη μπορεί να καθορίσει εάν τα δεδομένα που διακινούνται αναμένονται από το Host A. Εάν τα δεδομένα που περνούν δεν ταιριάζουν με την κατάσταση της συνομιλίας (όπως καθορίζεται από τον πίνακα κατάστασης), ή εάν το στοιχείο δεν είναι στον πίνακα, τα απορρίπτει. Αυτή η διαδικασία είναι γνωστή ως stateful inspection.

Stateful Packet Inspection (SPI): Η διαδικασία που τα τείχη προστασίας συνδυάζουν την stateful επιθεώρηση με την επιθεώρηση πακέτων, είναι γνωστή ως stateful επιθεώρηση πακέτων. Είναι στην ουσία η επιθεώρηση των πακέτων βασισμένη όχι μόνο στη δομή τους και τα δεδομένα που περιλαμβάνονται σε αυτά, αλλά βασισμένη και στην κατάσταση που είναι η συνομιλία μεταξύ των hosts. Κατά συνέπεια η επιθεώρηση επιτρέπει στα τείχη προστασίας να φιλτράρουν χρησιμοποιώντας όχι μόνο το περιεχόμενο του πακέτου, αλλά και τη σύνδεση ή τη κατάσταση στην οποία η θα είναι η σύνδεση στην συγκεκριμένη περίοδο. Παρέχει έτσι μια πιο ευέλικτη, συντηρήσιμη, και εξελικτική λύση φιλτραρίσματος.

3.3 Επικύρωση πρόσβασης

Το να θεωρηθεί η επιθεώρηση της IP διεύθυνσης προέλευσης και θύρας ως το ίδιο με την επικύρωση, ένα κοινό λάθος που γίνεται κατά την αξιολόγηση των τειχών προστασίας. Κάνοντας spoof μια IP διεύθυνση, κάποιο host θα μπορούσε να εμφανιστεί σαν να είναι εξ ολοκλήρου διαφορετικός host, παραμερίζοντας έτσι την επιθεώρηση ασφάλειας που θα ήταν βασισμένη στη διεύθυνση προέλευσης και θύρας. Για να αποβάλουν αυτό τον κίνδυνο, τα τείχη προστασίας πρέπει να παρέχουν επίσης και ένα μέσο επικύρωσης πρόσβασης. Το TCP/IP στηρίχτηκε στην προϋπόθεση των ανοικτών επικοινωνιών. Εάν δύο hosts γνωρίζουν εκατέρωθεν τις διευθύνσεις IP και συνδέονται ο ένας με τον άλλον, τότε μπορούν να επικοινωνήσουν. Αν και αυτό ήταν ένα ευγενές σχέδιο, στο σημερινό κόσμο μπορεί να μην θελήσουμε ο καθένας να είναι σε θέση να επικοινωνεί με τα συστήματα πίσω από τα τείχη προστασίας.

Τα τείχη προστασίας μπορούν να υποστηρίξουν την επικύρωση χρησιμοποιώντας διάφορους μηχανισμούς. Κατ' αρχάς, τα τείχη προστασίας μπορούν να απαιτήσουν την εισαγωγή ενός ονόματος χρήστη και ενός κωδικού πρόσβασης (γνωστό ως εκτεταμένη επικύρωση ή xauth). Χρησιμοποιώντας την xauth, ο χρήστης που προσπαθεί να αρχίσει μια σύνδεση προτρέπεται για ένα όνομα χρήστη και έναν κωδικό πρόσβασης πριν η τα τείχη προστασίας επιτρέψουν σε μια σύνδεση να καθιερωθεί. Έτσι, αφού η σύνδεση έχει επικυρωθεί και εξουσιοδοτηθεί από την πολιτική ασφάλειας, ο χρήστης δεν προτρέπεται πλέον για επικύρωση για την ιδία σύνδεση. Ένας άλλος μηχανισμός για την επικύρωση των συνδέσεων είναι μέσω της χρήσης πιστοποιητικών (certificates) και δημόσιων κλειδιών (public keys). Το όφελος των πιστοποιητικών σε σχέση με τη xauth είναι η διαδικασία επικύρωσης, η οποία μπορεί να γίνει χωρίς την επέμβαση χρηστών. Προϋπόθεση για το τελευταίο είναι οι hosts να έχουν διαμορφωθεί με τα αντίστοιχα πιστοποιητικά και μαζί με την αντιπυρική ζώνη να χρησιμοποιούν μια κατάλληλα διαμορφωμένη υποδομή δημόσια κλειδιού (public key infrastructure). Ένα όφελος αυτής της προσέγγισης είναι ότι μπορεί να κλιμακωθεί πολύ καλύτερα για μεγάλες εφαρμογές.

Επιπλέον, η επικύρωση μπορεί να αντιμετωπιστεί μέσω της χρήσης των προ-μοιραζόμενων κλειδιών (pre-shared keys PSK). Τα PSK είναι λιγότερο σύνθετα για να εφαρμόσουν από τα πιστοποιητικά, επιτρέποντας συγχρόνως στη διαδικασία επικύρωσης να γίνει χωρίς την επέμβαση των χρηστών. Με τα PSK, στον host παρέχεται ένα προκαθορισμένο κλειδί που χρησιμοποιείται για τη διαδικασία επικύρωσης. Ένα μειονέκτημα

αυτού του συστήματος είναι ότι το PSK αλλάζει σπάνια και πολλές οργανώσεις χρησιμοποιούν το ίδιο κλειδί σε μεγάλο αριθμό host, υπονομεύοντας κατά συνέπεια την ασφάλεια της διαδικασίας επικύρωσης. Με την εφαρμογή της επικύρωσης, τα τείχη προστασίας έχουν μια πρόσθετη μέθοδο για να καθορίσει εάν μια σύνδεση πρέπει να επιτραπεί. Ακόμα και όταν θα επιτρεπόταν το πακέτο βάσει στην επιθεώρηση της κατάσταση σύνδεσης, εάν ο host δεν μπορέσει να επικυρωθεί επιτυχώς με τα τείχη προστασίας, τότε το πακέτο θα απορριφθεί.

3.4 Η αποστρατικοποιημένη ζώνη (DMZ)

Η αποστρατικοποιημένη ζώνη (Demiliterized Zone – DMZ) είναι ένα ειδικό μέρος του δικτύου που απολαμβάνει μερική μόνο προστασία από το firewall. Αυτό επιτρέπει στο διαχειριστή του δικτύου να καθιερώσει ένα ειδικό σύνολο πολιτικών για τους δικτυακούς κόμβους που βρίσκονται στη ζώνη DMZ. Για παράδειγμα, ενώ η κύρια πολιτική ασφάλειας μπορεί να απαγορεύει στους εσωτερικούς εξυπηρετητές (servers) να επικοινωνούν με το εξωτερικό δίκτυο, μια ειδική πολιτική DMZ μπορεί να επιτρέψει εξαιρέσεις έτσι ώστε:

- ένας Web server που βρίσκεται μπορεί στη ζώνη DMZ να είναι προσπελάσιμος από το εξωτερικό δίκτυο στη θύρα 80 μέσω του πρωτοκόλλου TCP ή
- ένας εξυπηρετητής ηλεκτρονικού ταχυδρομείου που βρίσκεται μπορεί στη ζώνη DMZ να είναι προσπελάσιμος από το εξωτερικό δίκτυο στη θύρα 25 η οποία αντιστοιχεί στο πρωτόκολλο απλού ταχυδρομείου (Simple Mail Transfer Protocol – SMTP)

Η τοποθέτηση των δικτυακών κόμβων στη ζώνη DMZ τους καθιστά πιο ευάλωτους σε επιθέσεις ασφάλειας. Για αυτό το λόγο ρυθμίζονται συνήθως με κατάλληλη διαμόρφωση ενίσχυσης της ασφάλειάς τους. Οι εξυπηρετητές οι οποίοι βρίσκονται στην ζώνη DMZ αναφέρονται επίσης και ως εξυπηρετητές έπαλξης (bastion hosts). Οι bastion hosts, είναι κατάλληλα διαμορφωμένοι υπολογιστές οι οποίοι έχουν ρυθμιστεί να εκτελούν μόνο τις οριζόμενες υπηρεσίες και τίποτα περισσότερο. Μερικές φορές, αυτές οι μηχανές τρέχουν με στατικά ορισμένες παραμέτρους λειτουργίας (π.χ. χρησιμοποίηση του αρχείου "/etc/hosts" για την επίλυση ονόματος (name resolution) αντί για την υπηρεσία Domain Name System –DNS). Αυτό γίνεται ώστε να ελαχιστοποιηθεί ο κίνδυνος ένας επιτιθέμενος ο οποίος καταφέρνει να διεισδύσει στον εξυπηρετητή έπαλξης να χρησιμοποιήσει ταυτόχρονα και μία υπηρεσία ανεξάρτητη από τη λειτουργία του

εξυπηρετητή. Επιπλέον, το λειτουργικό σύστημα που εγκαθίσταται στους εξυπηρετητές έπαλξης είναι συνήθως ένα υποσύνολο της τυποποιημένης διανομής (π.χ., μπορεί να μην έχει μεταγλωττιστές, εργαλεία ελέγχου δικτύων, κτλ) έτσι ώστε ένας πιθανός εισβολέας να μην είναι σε θέση να χρησιμοποιήσει τον εξυπηρετητή έπαλξης για να εκτελέσει νέες επιθέσεις σε άλλους κόμβους του δικτύου.

Μία καλή τακτική είναι οι διαχειριστές δικτύου να μεταχειρίζονται τους κόμβους που βρίσκονται στη ζώνη DMZ ως δυνητικά μη έμπιστους κόμβους και να έχουν προετοιμάσει κατάλληλες στρατηγικές και τεχνικές αποκατάστασης. Τέτοιες στρατηγικές μπορούν να περιλάβουν βήματα για τη συγκέντρωση αποδείξεων πιθανών εισβολών ή πληροφοριών για τον επιτιθέμενο, περιορισμού των συνεπειών της επίθεσης κτλ.. Ανεξάρτητα από την υιοθετούμενη στρατηγική αποκατάστασης, ο διαχειριστής των συστημάτων πρέπει να είναι σε θέση να αποκαταστήσει την υπηρεσία σε κάθε δικτυακό κόμβο το συντομότερο δυνατόν. Αυτό υπονοεί ότι ολόκληρη η διαμόρφωση των συστημάτων (λειτουργικού συστήματος, υπηρεσίας κτλ) έχει διατηρηθεί σε εφεδρικό αρχείο ασφαλείας και υπάρχουν διαδικασίες για την επαναφορά του μολυσμένου κόμβου και την αποκατάσταση της διαμόρφωσης και των σχετικών δεδομένων.

Εάν η μέθοδος επίθεσης δεν είναι δυνατό να προσδιοριστεί επακριβώς, η επαναφορά του κόμβου με μία καθαρή διαμόρφωση δεν είναι αρκετή. Ο επιτιθέμενος θα επαναλάβει απλώς το ίδιο μοτίβο επίθεσης για να επιτύχει και πάλι το ίδιο αποτέλεσμα. Η ανίχνευση και η κατανόηση της επίθεσης είναι την ευπάθεια που επέτρεψε στην επίθεση να πραγματοποιηθεί και να την αντιμετωπίσουμε, προτού να μπορέσει η μηχανή να συνδεθεί στο δίκτυο. Ο προσδιορισμός της αδυναμίας ή των αδυναμιών που χρησιμοποίησε ο επιτιθέμενος και η ανίχνευση και κατανόηση της επίθεσης ενάντια στους κόμβους που βρίσκονται στη ζώνη DMZ ή το εσωτερικό δίκτυο, είναι μια σημαντική πτυχή της διαμόρφωσης του firewall. Ο έλεγχος της κίνησης (traffic monitoring) και η καταγραφή των γεγονότων (event logging) είναι βασικά εργαλεία του διαχειριστή του δικτύου. Επιπλέον είναι δυνατό να εγκατασταθούν στη ζώνη DMZ συστήματα ανίχνευσης παρείσφρησης (IDSs) ώστε να ελέγχουν (και μερικές φορές να αντιδρούν) στις επιθέσεις.

3.5 Τα firewall ελέγχου καταστάσεων (stateful inspection)

Αρχικά, τα firewall σχεδιάστηκαν για να εξετάσουν κάθε πακέτο χωριστά, και αποφάσιζαν εάν θα επιτρέπει τη διέλευση σε ένα πακέτο κατευθείαν, μόνο βάσει των πληροφοριών που περιλήφθηκαν μέσα σε εκείνο το πακέτο. Αυτό δημιούργησε δυσκολίες με τα πρωτόκολλα που στηρίζονταν σε δευτερεύουσες συνδέσεις για την ανταλλαγή πρόσθετων πληροφοριών (π.χ., FTP). Δεδομένου ότι το firewall δεν μπορεί να ξέρει εάν το (δευτεροβάθμιο) αίτημα σύνδεσης προήλθε από μια υπάρχουσα σύνδεση ή εάν δημιουργήθηκε ανεξάρτητα, το firewall αναγκαζόταν να το απορρίψει.

Τα firewall ελέγχου καταστάσεων, χρησιμοποιούν μηχανές καταστάσεων για να διατηρήσουν πληροφορίες της κατάστασης των ήδη εγκατεστημένων συνδέσεων πρωτοκόλλου. Οι αποφάσεις λαμβάνονται βάσει των πληροφοριών στο πακέτο συν την κατάσταση της σύνδεσης που διατηρείται από την αντιπυρική ζώνη. Κατά συνέπεια, ένα πακέτο TCP με καθαρή σημαία SYN, θα απορριφθεί εκτός αν ανήκει σε μια ήδη υπάρχουσα σύνδεση. Ακόμη και σε περιπτώσεις όπου οι πληροφορίες ανταλλάσσονται χωρίς πραγματοποίηση σύνδεσης (επικοινωνίες χωρίς σύνδεση όπως εκείνες που χρησιμοποιούν το πρωτόκολλο UDP), το firewall μπορεί να κάνει μια σημείωση ότι ένα πακέτο αιτήματος έχει περάσει την έξοδο του προστατευμένου δικτύου και επιτρέπει έτσι την απάντηση κατευθείαν (π.χ., μια ερώτηση SNMP από έναν εσωτερικό σταθμό διαχείρισης δικτύου σε έναν πράκτορα (agent) που βρίσκεται στο DMZ).

Πρόσθετες υπηρεσίες Τειχών Προστασίας

Σε πολλές περιπτώσεις, τα firewall παρέχουν επίσης διάφορες πρόσθετες υπηρεσίες που ενώ δεν αποτελούν αυστηρά μέρος της εργασίας τους, έχουν ρησιμοποιηθεί τόσο ευρέως ώστε να θεωρούνται πλέον αναπόσπαστο τμήμα τους.

3.6 Πολιτικές ασφάλειας

Τα τείχη προστασίας δεν είναι τίποτα περισσότερο από τα σημεία πολιτικής επιβολής ελέγχου πρόσβασης. Συνεπώς, τα τείχη προστασίας είναι τόσο αποτελεσματικά όσο η πολιτική ασφάλειας (security policy) που θα υπαγορεύει το πώς θα χρησιμοποιηθούν τα τείχη προστασίας. Το πρώτο βήμα σε μια πετυχημένη πολιτική ασφάλειας είναι η ανάλυση κινδύνου (risk analysis), η οποία και θα καθορίσει τις απειλές για το προστατευμένο σύστημα. Μετά από αυτό, μπορεί να αναπτυχθεί η στρατηγική και η πολιτική για την προστασία του συστήματος από τα τείχη προστασίας για τις αντίστοιχες απειλές.

Ένα βασικό στοιχειό που θα πρέπει να γίνει αντιληπτό κατά την ανάπτυξη της στρατηγικής είναι ότι μπορεί να μην είμαστε σε θέση να προστατευτούμε ή να αποτρέψουμε όλες τις επιθέσεις. Οι λόγοι ξεκινούν από τους τεχνολογικούς περιορισμούς και φτάνουν στους πρακτικούς και οικονομικούς περιορισμούς. Κατά συνέπεια, το θέμα θα πρέπει να εξεταστεί από την προοπτική της επιδίωξης να ελαχιστοποιηθεί ο κίνδυνος που συνδέεται με την απειλή. Σε μερικές περιπτώσεις, αυτό σημαίνει ότι ο κίνδυνος μπορεί να μειωθεί στο μηδέν . Σε άλλες περιπτώσεις, μπορούμε μόνο να μειώσουμε τον κίνδυνο σε ένα επίπεδο που θα είναι αποδεκτό για το δίκτυο.

3.7 Τείχη Προστασίας και εμπιστοσύνη

Με την λήψη απόφασης που επιτρέπει την κυκλοφορία μέσω των τειχών προστασίας, ο διαχειριστής έχει λάβει και την απόφαση (σκόπιμη ή όχι) να εμπιστευθεί την κυκλοφορία αυτή. Η παρούσα απόφαση είναι μέρος του καθορισμού ενός αποδεκτού επιπέδου κινδύνου. Τα τείχη προστασίας δεν υπάρχουν για να σταματήσουν όλη την κυκλοφορία, αλλά για να επιτρέψει κάποια κυκλοφορία σταματώντας κάποια άλλη. Αυτό δεν σημαίνει ότι με μια απόφαση που επιτρέπει κάποια κυκλοφορία αφαιρούμε την ασφάλεια που μπορεί να παρέχει ένα τείχος προστασίας.

Στη συνεχή αναζήτηση της ελαχιστοποίησης του κινδύνου, το τείχος προστασίας μπορεί να διαμορφωθεί ώστε να επικυρώνει τις συνδέσεις που έχουν πρόσβαση στον εμπιστευόμενο σύστημα η πώρο. Να εξασφαλιστεί έτσι ότι προτού χορηγηθεί κάποια πρόσβαση στον προστατευμένο πόρο, το σύστημα που κάνει την αίτηση πρέπει να επικυρωθεί ως νόμιμος και έγκυρος χρήστης του τελικού συστήματος . Μια άλλη επιλογή είναι να χρησιμοποιηθεί το τείχος προστασίας ως proxy, λειτουργώντας ως ένας μεσάζων για την παροχή της πρόσβασης στον προστατευμένο σύστημα. Το σημείο που θα πρέπει να αποτελέσει και κανόνα για τα τείχη προστασίας και την εμπιστοσύνη είναι ότι όσο και να εμπιστευόμαστε την πρόσβαση που χορηγείται, αύτη θα πρέπει να περάσει από τα τείχη προστασίας πριν αποκτήσει έλεγχο στον προστατευμένο σύστημα.

3.8 Κατηγοριοποίηση Τειχών Προστασίας

α) Ταξινόμηση Τειχών Προστασίας

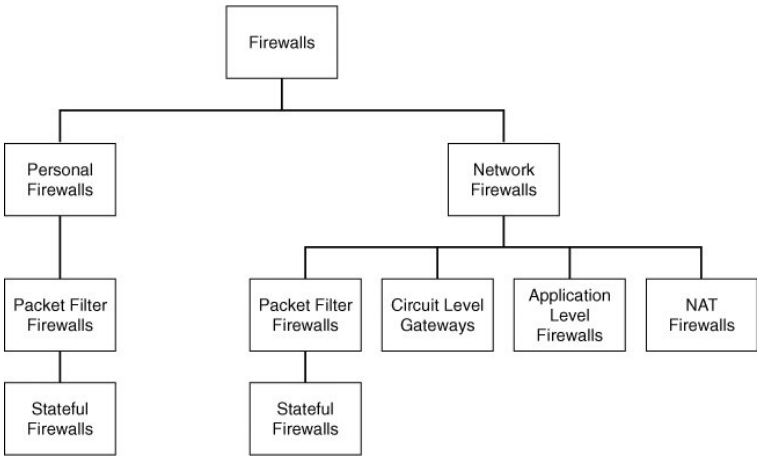
Τα τείχη προστασίας μπορούν να ταξινομηθούν κάτω από δύο γενικούς τύπους:

1. Προσωπικά τείχη προστασίας (Personal firewalls)
2. Τείχη Προστασίας Δικτύων (Network firewalls)

Η αρχική διαφορά μεταξύ αυτών των δύο τύπων τειχών προστασίας είναι στον αριθμό των υπολογιστών που προστατεύει το τείχος προστασίας.

- Στα Τείχη Προστασίας Δικτύων, συμπεριλαμβανομένων οι παρακάτω τύποι:
- Τείχη Προστασίας φιλτραρίσματος πακέτων (Packet-filtering firewalls)
- Πύλες επιπέδου συνόδου (Circuit-level gateways)
- Πύλες επιπέδου εφαρμογής (Application-level gateways)

Η παραπάνω ταξινόμηση περιγράφει τις γενικές κατηγορίες τειχών προστασίας. Πολλά Τείχη Προστασίας δικτύων χρησιμοποιούν υβριδικές τεχνικές και έχουν χαρακτηριστικά που τις τοποθετούν σε περισσότερες από μια ταξινομήσεις. Το παρακάτω σχήμα παρουσιάζει μια ανάλυση των διάφορων τύπων τειχών προστασίας, που υπάρχουν σήμερα διαθέσιμα, με κριτήριο τους δύο αρχικούς τύπους: Προσωπικά Τείχη Προστασίας και Τείχη Προστασίας δικτύων.



Εικόνα 5: Ταξινόμηση Firewall

β) Προσωπικά Τείχη Προστασίας

Τα προσωπικά Τείχη Προστασίας σχεδιάζονται για να προστατεύσουν ένα host. Μπορούν να αντιμετωπισθούν ως το περίβλημα προστασίας γύρω από το σύστημα, όπου το σύστημα μπορεί να είναι ένας κεντρικός υπολογιστής, ένας υπολογιστής γραφείου ή ένα laptop. Στα προσωπικά τείχη προστασίας η εξερχόμενη κυκλοφορία επιτρέπετε ενώ η εισερχόμενη κυκλοφορία απαιτεί επιθεώρηση. Συνήθως τα Προσωπικά Τείχη Προστασίας περιλαμβάνουν διάφορα προφίλ τα οποία προσαρμόζουν τη κυκλοφορία που θα δεχτεί ένα σύστημα. Ένας σημαντικός παράγοντας είναι η συγκεντρωτική διαχείριση. Το σημαντικότερο εμπόδιο στην επέκταση των Προσωπικών Τειχών Προστασίας ότι σε κάθε σύστημα είναι υπάρχει η ανάγκη για συγκεντρωτική διαχείριση, έτσι ώστε οι πολιτικές ασφάλειας να μπορούν να αναπτυχθούν και να εφαρμοστούν στα απομακρυσμένα συστήματα. Οι μεγάλες επιχειρήσεις είναι διστακτικές στο να υιοθετήσουν την προσωπική τεχνολογία τειχών προστασίας για τα συστήματά τους λόγω της δυσκολίας για μια συνεπής πολιτική τειχών προστασίας σε ολόκληρη την επιχείρηση.

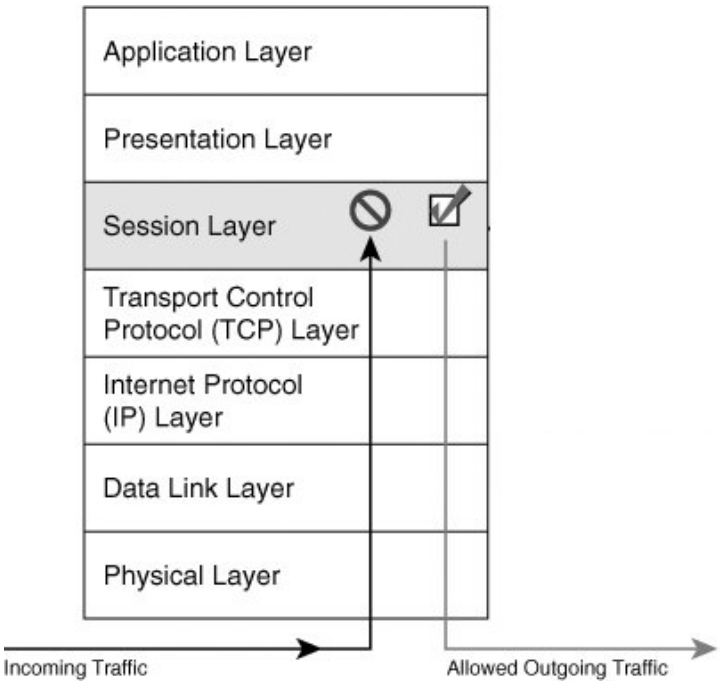
γ) Τείχη Προστασίας NAT

Ένα άλλο τείχος προστασίας, που υπήρξε για μια μικρή χρονική περίοδο, είναι το τείχος προστασίας μεταφράσεων διευθύνσεων δικτύων. Στη σημερινή αγορά του Τείχος Προστασίας NAT αποτελεί μέρος σχεδόν κάθε διαθέσιμου προϊόντος τειχών προστασίας. Το Τείχος Προστασίας NAT παρέχουν αυτόματα την προστασία στα συστήματα πίσω από το τείχος προστασίας επειδή επιτρέπουν μόνο τις συνδέσεις που προέρχονται από το εσωτερικό της. Ο βασικός σκοπός του NAT είναι να κάνει πολυπλεξία της κυκλοφορίας στο εσωτερικό δίκτυο ώστε να την παρουσιαστεί στο ευρύτερο δίκτυο (δηλαδή το Διαδίκτυο) σαν να προερχόταν από μια διεύθυνση IP ή μια μικρή σειρά από διευθύνσεις IP.

Το Τείχος Προστασίας NAT δημιουργεί έναν πίνακα που περιέχει τις πληροφορίες για όλες της συνδέσεις που έχουν δημιουργηθεί. Αυτός ο πίνακας χαρτογραφεί τις διευθύνσεις των εσωτερικών συστημάτων σε μια εξωτερική διεύθυνση. Η δυνατότητα να τοποθετηθεί ένα ολόκληρο δίκτυο πίσω από μια διεύθυνση IP είναι βασισμένη στη χαρτογράφηση των αριθμών θύρας από το NAT τείχος προστασίας.

δ) Τείχη Προστασίας επιπέδου συνόδου

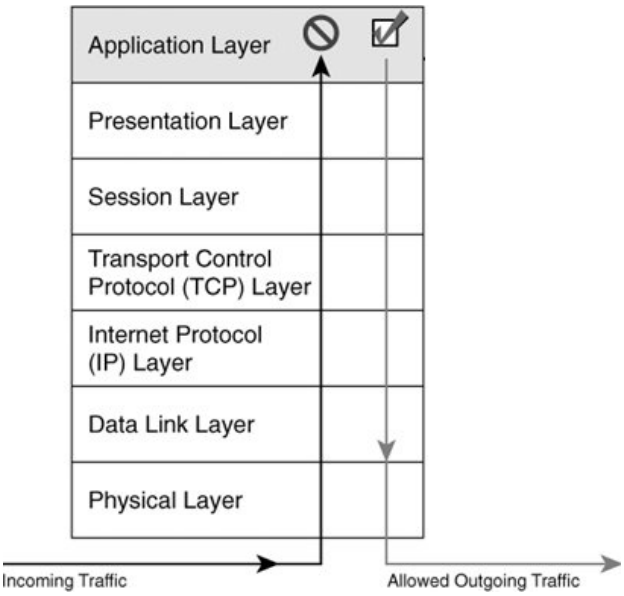
Τα τείχη προστασίας επιπέδου συνόδου λειτουργούν στο στρώμα συνόδου του μοντέλου OSI. Για να αποφασίσουν εάν η κυκλοφορία είναι νόμιμη, ελέγχουν τις διαδικασίες ανταλλαγείς (handshaking) μεταξύ των πακέτων. Η κυκλοφορία προς έναν απομακρυσμένο υπολογιστή τροποποιείται κατά τέτοιο τρόπο ώστε να εμφανιστεί σαν να προήλθε από το ίδιο τείχος προστασίας. Αυτή η τροποποίηση καθιστά τείχος προστασίας επιπέδου συνόδου ιδιαίτερα χρήσιμο στο κρύψιμο των πληροφοριών για ένα προστατευμένο δίκτυο. Το μειονέκτημα της υλοποίησης του τείχους προστασίας επιπέδου συνόδου στέκεται στο γεγονός ότι δεν φιλτράρει τα μεμονωμένα πακέτα σε μια δεδομένη σύνδεση. Το παρακάτω σχήμα παρουσιάζει το παράδειγμα ενός τείχους προστασίας επιπέδου συνόδου, δείχνοντας την εισερχόμενη κυκλοφορία, τον έλεγχο στο επίπεδο συνόδου και την επιτρεπόμενη εξερχόμενη κυκλοφορία.



Εικόνα 6: Circuit-Level Firewall

ε) Τείχη Προστασίας πληρεξούσιου

Ένα τείχος προστασίας πληρεξούσιου ενεργεί ως μεσάζων μεταξύ δύο συστημάτων, παρόμοια με τις πύλες επιπέδου συνόδου. Ωστόσο, στην περίπτωση ενός τείχος προστασίας πληρεξούσιου, η αλληλεπίδραση ελέγχεται στο στρώμα εφαρμογής με τον καταναγκασμό και των δύο πλευρών να διεξάγουν την επικοινωνία μέσω του πληρεξούσιου. Η λειτουργία αυτή επιτυγχάνεται στο τείχος προστασίας με τη δημιουργία και εκτέλεση μιας διαδικασίας που αντανακλά μια υπηρεσία όπως αυτή θα έτρεχε σε ένα απομακρυσμένο σύστημα. Για να υποστηρίξει τις διάφορες υπηρεσίες, τείχος προστασίας πληρεξούσιου πρέπει να έχει μια υπηρεσία που τρέχει για κάθε πρωτόκολλο: ένα απλό πληρεξούσιο πρωτοκόλλου μεταφορών ταχυδρομείου (SMTP) για το ηλεκτρονικό ταχυδρομείο, ένα πληρεξούσιο πρωτοκόλλου μεταφοράς αρχείων (FTP) για τις μεταφορές αρχείων, και ένα πληρεξούσιο πρωτοκόλλου μεταφοράς υπερκειμένων (HTTP) για τις υπηρεσίες Ιστού. Το παρακάτω σχήμα παρουσιάζει το παράδειγμα ενός τείχους προστασίας πληρεξούσιου.

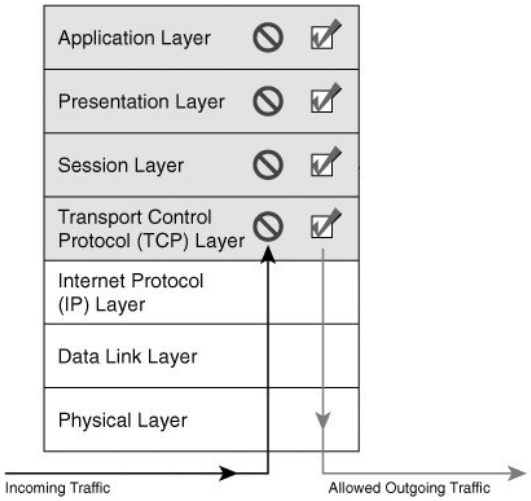


Εικόνα 7: Proxy Firewall

στ) Τείχη Προστασίας Stateful

Τα σύγχρονα stateful τείχη προστασίας συνδυάζουν σε ένα σύστημα τις πτυχές και τις ικανότητες των τειχών προστασίας NAT, επιπέδου συνόδου και πληρεξούσιου. Το φιλτράρισμα της κυκλοφορίας βασίζεται αρχικά στα χαρακτηριστικά των πακέτων αλλά περιλαμβάνει και ελέγχους σε επίπεδο συνόδου για να σιγουρευτεί ότι επιτρέπεται μια συγκεκριμένη σύνοδος.

Αντίθετα από τα άλλα τείχη προστασίας, σχεδιάζονται για να είναι πιο διάφανης. Ωστόσο, περιλαμβάνουν τις πτυχές φιλτραρίσματος που έχει ένα πληρεξούσιο με το να επιθεωρήσουν ξανά τα στοιχεία σε επίπεδο εφαρμογής, μέσω της χρήσης των συγκεκριμένων υπηρεσιών. Σχεδόν όλες τα σύγχρονα τείχη προστασ είναι stateful και αντιπροσωπεύουν τη βασική γραμμή για την ασφάλεια στα σημερινά δίκτυα. Η παρακάτω εικόνα απεικονίζει το παράδειγμα τειχών προστασίας stateful.



Εικόνα 8: Stateful Firewall

3.9 Διαφανείς Τείχη Προστασίας

Τα διαφανείς τείχη προστασίας (γνωστά ως bridging firewalls) δεν είναι μια νέα τείχη προστασίας αλλά μάλλον ένα υποσύνολο των stateful τειχών προστασίας. Ενώ σχεδόν όλα τα τείχη προστασίας λειτουργούν στο στρώμα IP και πάνω, τα διαφανείς τείχη προστασίας λειτουργούν στο δεύτερο στρώμα, το στρώμα ζεύξης δεδομένων (data link layer) και ελέγχουν την κυκλοφορία για τα ανώτερα στρώματα.

Επιπλέον, τα διαφανείς τείχη προστασίας μπορούν να εφαρμόσουν κανόνες φιλτραρίσματος πακέτων όπως και ένα stateful τείχος προστασίας και να εμφανιστεί στον τελικό χρήστη σαν αόρατη. Στην πραγματικότητα, μια το διαφανής τείχος προστασίας ενεργεί ως γέφυρα, φιλτράροντας τα πακέτα μεταξύ δύο τμημάτων δικτύου. Αντιπροσωπεύει έναν άριστο τρόπο για εγκατάσταση πολιτικής ασφάλειας στη μέση ενός τμήματος δικτύων, χωρίς να πρέπει να εφαρμοστεί κάποιο φίλτρο NAT.

Τα οφέλη των διαφανών τειχών προστασίας χωρίζονται σε τρεις γενικές κατηγορίες:

- Μηδενική διαμόρφωση (Zero configuration)
- Απόδοση (Performance)
- Μυστικότητα (Stealth)

Τα διαφανείς τείχη προστασίας δεν απαιτούν καμία τροποποίηση στο υπάρχων δίκτυο, επειδή είναι ευθύγραμμος συνδεδεμένη (in-line plugged) με το δίκτυο που προστατεύει. Επειδή λειτουργεί στο στρώμα ζεύξης δεδομένων, δεν απαιτείται καμία αλλαγή διευθύνσεων IP. Επειδή τείνουν να είναι απλούστερες, έχουν χαμηλότερα φόρτο επεξεργασίας, γεγονός που τις επιτρέπει να παρέχουν την καλύτερη απόδοση καθώς επίσης και τη βαθύτερη επιθεώρηση πακέτων. Τέλος, η μυστικότητά τους προέρχεται άμεσα από το γεγονός ότι είναι συσκευές που λειτουργούν στο δεύτερο στρώμα. Οι διεπαφές δικτύων δεν έχουν καμία διεύθυνση IP (εκτός από τη διεπαφή διαχείρισης) και επομένως είναι αόρατες σε έναν επιτιθέμενο. Δεν μπορεί κάποιος να επιτεθεί επειδή εναντίον της, γιατί απλά δεν μπορεί να την προσεγγίσει.

4.0 Εικονικά Τείχη Προστασίας

Τα εικονικά τείχη προστασίας είναι πολλά λογικά τείχη προστασίας που τρέχουν σε μια ενιαία φυσική συσκευή. Αυτή η ρύθμιση επιτρέπει σε πολλά δίκτυα να προστατεύονται από ένα μοναδικό τείχος προστασίας που τρέχει μια μοναδική πολιτική ασφάλειας σε μια φυσική συσκευή. Ένας φορέας υπηρεσιών (service provider) μπορεί να παρέχει υπηρεσίες τειχών προστασίας σε πολλούς πελάτες, ασφαλίζοντας και διαχωρίζοντας την κυκλοφορία, ενώ η διαχώριση θα γίνεται σε μια συσκευή. Αυτό υλοποιείται με την δημιουργία ξεχωριστών περιοχών ασφάλειας για κάθε πελάτη, όπου κάθε περιοχή θα ελέγχεται από ένα διαφορετικό λογικό εικονικό τείχος προστασίας.

4.1 Τείχη προστασίας ανοικτού και κλειστού κώδικα

Μια άλλη κατηγοριοποίηση που μπορεί να γίνει είναι στα τείχη προστασίας ανοικτού και κλειστού κώδικα (Open and Closed Source Firewalls). Στις ανοιχτού κώδικα ανήκουν οι Linux's IPTables, OpenBSD's pf, και Solaris IPF. Άλλες, όπως τα Cisco PIX, ASA, Juniper's ScreenOS, Check Point's firewall είναι κλειστού κώδικα. Τα περισσότερες εμπορικά τείχη προστασίας επιτρέπουν δυνατότητες VPN για τους απομακρυσμένους χρήστες καθώς επίσης και επιθεώρηση πακέτων μέσα στα ίδια τείχη προστασίας. Τα τείχη προστασίας ανοικτού κώδικα τείνουν να εστιάσουν στις ικανότητες φιλτραρίσματος παρά την ενσωμάτωση άλλων εφαρμογών.

4.2 Ασφάλεια δικτύων με τη βοήθεια Τειχών Προστασίας

α) Firewalls και Ασφάλεια Δικτύου

Ως firewall (τείχος προστασίας), ορίζεται το λογισμικό ή το υλικό (hardware) που επιτρέπει σε ορισμένους εξωτερικούς χρήστες με συγκεκριμένα χαρακτηριστικά να έχουν πρόσβαση σε ένα προστατευμένο δίκτυο ή δικτυακό τόπο (site). Στην τυπική του μορφή, ένα τέτοιο προστατευτικό τείχος επιτρέπει στους έσω να έχουν πλήρη και χωρίς περιορισμούς πρόσβαση σε υπηρεσίες έξω από το συγκεκριμένο δίκτυο, ενώ παραχωρεί την άδεια πρόσβασης εκ των έξω επιλεκτικά, με βάση κωδικούς πρόσβασης, ονόματα χρηστών, διευθύνσεις του διαδικτύου (Internet IP address) ή ονομασίες περιοχών (domain name).

Η κύρια λειτουργία ενός firewall είναι η ρύθμιση της κυκλοφορίας δεδομένων ανάμεσα σε δύο δίκτυα υπολογιστών. Συνήθως τα δύο αυτά δίκτυα είναι το Διαδίκτυο (Internet) και το τοπικό/ εταιρικό δίκτυο. Ένα firewall παρεμβάλλεται ανάμεσα σε δύο δίκτυα που έχουν διαφορετικό επίπεδο εμπιστοσύνης. Το διαδίκτυο έχει μικρό βαθμό εμπιστοσύνης (low level of trust), ενώ το εταιρικό δίκτυο ή το οικιακό δίκτυο διαθέτουν τον μέγιστο βαθμό εμπιστοσύνης. Ένα περιμετρικό δίκτυο (perimeter network) διαθέτει μεσαίο επίπεδο εμπιστοσύνης.

Ο σκοπός της τοποθέτησης ενός firewall είναι η πρόληψη επιθέσεων στο τοπικό δίκτυο και η αντιμετώπισή τους. Παρόλα αυτά όμως, ένα firewall μπορεί να αποδειχθεί άχρηστο εάν δεν ρυθμιστεί σωστά. Η σωστή πρακτική, είναι το firewall να ρυθμίζεται ούτως ώστε να απορρίπτει όλες τις συνδέσεις εκτός αυτών που επιτρέπει ο διαχειριστής του δικτύου (default-deny). Για να ρυθμιστεί σωστά ένα firewall θα πρέπει ο διαχειριστής του δικτύου να έχει μία ολοκληρωμένη εικόνα για τις ανάγκες του δικτύου και επίσης να διαθέτει πολύ καλές γνώσεις πάνω στα δίκτυα υπολογιστών. Πολλοί διαχειριστές δεν έχουν αυτά τα προσόντα και ρυθμίζουν το firewall ούτως ώστε να δέχεται όλες τις συνδέσεις εκτός από εκείνες που ο διαχειριστής απαγορεύει (default- allow). Η ρύθμιση αυτή καθιστά το δίκτυο ευάλωτο σε επιθέσεις από εξωτερικούς χρήστες.

4.3 Γενικά στοιχεία ασφαλείας

Πριν την έλευση των μεταγωγεών (switches), τα δίκτυα μπορούσαν να παραβιαστούν με την παρακολούθηση της κίνησης του δικτύου μέσα από ένα διανομέα (hub). Με την έλευση των switches, οι υποκλοπές έχουν γίνει πιο δύσκολες. Πολλά switches επιτρέπουν την παρακολούθηση της κίνησης του δικτύου, με την τοποθέτηση μιας από τις πόρτες του switch σε κατάσταση παρακολούθησης. Η κατάσταση παρακολούθησης, είναι ένα νόμιμο μέσο επίλυσης προβλημάτων του δικτύου, αλλά ταυτόχρονα κάνει ευάλωτο το δίκτυο σε οποιονδήποτε έχει πρόσβαση στο switch.

Είναι επίσης πιθανή η υποκλοπή σε δίκτυα οπτικών ινών, με τη δημιουργία μιας εκτροπής στην κίνηση πολλαπλής λειτουργίας του δικτύου. Η εκτροπή επιτρέπει σε αρκετό φως να φεύγει από την οπτική ίνα, με αποτέλεσμα να είναι πιθανές οι υποκλοπές στο δίκτυο. Τα ασύρματα δίκτυο έχουν γίνει υπέρ- κυρίαρχα στην πρόσβαση στο διαδίκτυο, χρησιμοποιώντας το ασύρματο μέσο σαν πρώτο κρίκο.

Ιστορικά, τα ασύρματα δίκτυα άντεχαν μικρότερη ασφάλεια και μπορούσαν εύκολα να παρακολουθηθούν από κάποιον μέσα στην εμβέλεια του ασύρματου σημείου πρόσβασης. Τα τελευταία χρόνια, μια ολόκληρη σουίτα από ασύρματα πρότυπα ασφαλείας έχουν εισαχθεί και καθιερωθεί ευρέως. Προσφέρουν πιστοποίηση και εμπιστευτικότητα δεδομένων σε ασύρματες επικοινωνίες, από μια δοσμένη συσκευή στο άμεσο Επίπεδο 2 (Layer 2) των γειτόνων. Αυτά τα πρότυπα, καθιερώθηκαν από την IEEE. Ένα από τα κυρίαρχα πρότυπα ασφαλείας, είναι το 802.11i με πολλά παρελκόμενα παράγωγα πρότυπα που έχουν ήδη οριστεί. Αυτά τα πρότυπα προσφέρουν επιπρόσθετες υπηρεσίες ασφαλείας στα ασύρματα δίκτυα

Το λογισμικό το οποίο υποστηρίζει την επικοινωνία δεδομένων σε κάθε μια από τις διάφορες συσκευές σε οποιαδήποτε διαδρομή δεδομένων στο Internet, οργανώνεται σε στρώματα. Κάθε στρώμα εκτελεί μια διαφορετική λειτουργία, ή μεταβάλλει τα δεδομένα καθώς περνούν μέσα από τις στοίβες των επιπέδων. Αν κάποιος εισβολέας, μπορεί να πάρει κάποιο κομμάτι από αυτό το κακόβουλο λογισμικό που έχει εισαχθεί ανάμεσα σε αυτά τα στρώματα, ο εισβολέας μπορεί παρακολουθεί ή ακόμα να εισάγει κακόβουλα προγράμματα σε άλλα συστήματα, κατά μήκος του καναλιού επικοινωνίας.

4.4 Άμυνα δικτύου

Η άμυνα ενάντια σε αυτές τις απειλές ρυθμίζεται σήμερα με την εγκατάσταση πολυάριθμων τεχνολογιών ασφαλείας, όπως τον έλεγχο πρόσβασης δικτύου (NAC) και τα αντί-υιικά προγράμματα σε πλατφόρμες αλλά και εντός του δικτύου. Στο δίκτυο, οι επιχειρήσεις σήμερα εγκαθιστούν συσκευές σε κάποιο σημείο της υπάρχουσας υποδομής, έτσι ώστε να διαχωρίσουν την εξωτερική μη αξιόπιστη περιοχή του δικτύου, μέσα σε αυτήν και το διαδίκτυο (Internet), από την αξιόπιστη εσωτερική, που προφυλάσσεται φυσικά σαν τμήμα του δικτύου. Αυτές οι συσκευές, ανιχνεύουν και εμποδίζουν επιθέσεις από το διαδίκτυο, σαρώνουν εισερχόμενα πακέτα για ιούς και άλλο κακόβουλο λογισμικό και αμύνονται ενάντια στις επιθέσεις άρνησης υπηρεσίας. Αυτή η άμυνα με συσκευές λειτουργεί λιγότερο αποτελεσματικά για πολλούς λόγους. Αρχικά, πολλές επιθέσεις έρχονται εσωτερικά από την αμυντική περίμετρο, από πηγές που θεωρητικά θα έπρεπε να είναι έμπιστες, συμπεριλαμβανομένων των υπαλλήλων και των εργολάβων για παράδειγμα. Στη συνέχεια, είναι όλο και πιο κοινό να ανοιχτούν πόρτες μέσα από την περίμετρο ασφαλείας, ώστε να παρέχεται πρόσβαση σε συγκεκριμένους τύπους ρευμάτων κίνησης, όπως το πρωτόκολλο μεταφοράς υπερκειμένου (HTTP), πρωτόκολλο μεταφοράς αρχείων (FTP) κλπ. Έτσι σχεδιάζονται οι επιθέσεις, με στόχο να διαπερνούν αυτά τα κενά στα συστήματα. (Kent, S. 2005).

Σαν αποτέλεσμα αυτών, η προστατευμένη περίμετρος κινείται πιο κοντά στα συστήματα που έχει σχεδιαστεί για να προστατεύει, όπως οι εξυπηρετητές (servers) και οι αποθηκευτικές συσκευές (storage media). Η αυξανόμενη πρόσβαση, ακόμα και μέσα από τον οργανισμό, δρομολογείται μέσα από συσκευές έλεγχου εισβολής, ανίχνευσης και απαγόρευσης. Έτσι, το στρώμα ασφαλείας ανάμεσα στην περίμετρο ασφαλείας και τα συστήματα, γίνεται λεπτότερο. Η λογική επέκταση ασφαλείας, είναι ο ορισμός της περιμέτρου ακριβώς δίπλα στους ίδιους τους εξυπηρετητές. Αυτό όμως θα σήμαινε ότι δημιουργήθηκε μια άμυνα σε βάθος για κάθε εξυπηρετητή. Μια τέτοια λύση, δεν είναι πρακτική στη σημερινή υπολογιστική, δεδομένου του υπάρχοντος οικονομικού βάρους στους οργανισμούς. Οι πόροι οι οποίοι μεταφέρονται από την παραγωγική εργασία στα συστήματα ασφαλείας, είναι ακόμα περισσότερο αντιοικονομικοί από οτιδήποτε άλλο.

Μια εναλλακτική λύση για να μειωθεί το κόστος αμυντικής λειτουργίας σε κάθε εξυπηρετητή, είναι να δημιουργηθεί το ίδιο επίπεδο προστασίας στα πρωτοκόλλα επικοινωνίας, επιτρέποντας στα δεδομένα να προστατεύονται καθώς κινούνται εντός του οργανισμού αλλά και κατά μήκος του διαδικτύου. Κατά μια έννοια, η μερική προστασία

αυτού του τύπου χρησιμοποιείται σε μεγάλο βαθμό σήμερα. Τα Ιδιωτικά Εικονικά Δίκτυα (VPN) δημιουργούν ένα προστατευτικό τούνελ στο οποίο, τα δεδομένα κρυπτογραφούνται καθώς κινούνται μεταξύ οργανισμών και των απομακρυσμένων υπολογιστών που λειτουργούν στο διαδίκτυο. Τα VPN's χρησιμοποιούνται με μεγάλο αποτέλεσμα τα τελευταία χρόνια , αλλά ακόμα δεν προστατεύουν από υπερχειλίσεις απροστάτευτων δεδομένων μέσα στην αμυντική περίμετρο που υπάρχει, και συχνά είναι ακατάλληλα για χρήση από χρήστες σε απομακρυσμένους υπολογιστές.

4.5 Ασφάλεια πρωτοκόλλων

Η ασφάλεια πρωτοκόλλων είναι ένας γενικός όρος, που χρησιμοποιείται για να περιγράψει τις υπηρεσίες κρυπτογράφησης που παρέχονται στα πακέτα δεδομένων του δικτύου. Η ροη δεδομένων μέσα σε ένα δίκτυο μπορεί να πάρει πολλές μορφές και μπορεί να διαφοροποιηθεί από τις παρεχόμενες υπηρεσίες εντός του δικτύου. Αυτές μπορεί να ποικίλουν, από πρωτόκολλα επικοινωνίας που διαχειρίζονται υπηρεσίες δικτύων, άμεση ανταλλαγή μηνυμάτων ανάμεσα σε διαφορετικούς κόμβους του δικτύου, εγκατάσταση απομακρυσμένων συνεδριών και ροών ανάμεσα σε δυο ή περισσότερους κόμβους του δικτύου για το σκοπό της επικοινωνίας δεδομένων ανάμεσα σε αυτούς τους κόμβους, καθώς επίσης και για έναν μεγάλο αριθμό από άλλες εργασίες του δικτύου. Πολλές από αυτές τις υπηρεσίες μπορούν να χαρτογραφηθούν σε διαφορετικά στρώματα του μοντέλου OSI.

Το μοντέλο OSI, ξεχωρίζει την αρχιτεκτονική του δικτύου σε πολλαπλά επίπεδα, όπου το κάθε επίπεδο πραγματοποιεί μια λογική λειτουργία και αλληλεπιδρά με τα επίπεδα που βρίσκονται πάνω και κάτω. Τα ανώτερα επίπεδα σε αυτό το μοντέλο βασίζονται σε υπηρεσίες που παρέχονται από τα κατώτερα επίπεδα, με μια εγγύηση του τι είδους είναι αυτές οι υπηρεσίες, χωρίς να χρειάζεται να κατανοήσουν με ποιον τρόπο μπορεί να παρέχονται αυτές οι υπηρεσίες. Ένα παράδειγμα αυτού του μοντέλου φαίνεται στο πως το πρωτόκολλο μεταφοράς (TCP) παρέχει υπηρεσίες προσανατολισμένης σύνδεσης σε ανώτερα επίπεδα, ενώ βασίζεται σε υπηρεσίες δικτύου από το πρωτόκολλο IP που βρίσκεται σε επίπεδο κατώτερο. Το επίπεδο πρωτοκόλλου διαδικτύου (IP), βασίζεται στο επίπεδο συνδέσμου δεδομένων και στα φυσικά επίπεδα πιο κάτω για να παρέχει επιπλέον υπηρεσίες. Αυτές οι υπηρεσίες μπορεί να είναι εξαρτημένες από υποκείμενα μέσα επικοινωνίας, χωρίς να χρειάζονται επιπλέον πληροφορίες σε αυτό το υποκείμενο μέσο.

4.6 Υπηρεσίες ασφαλείας OSI

Υπάρχουν 8 υπηρεσίες ασφαλείας σχετικές με το μοντέλο OSI:

- **Αναγνώριση:** ομότιμες οντότητες πρέπει να αναγνωρίζονται.
- **Πιστοποίηση:** παρέχει πιστοποίηση για την ταυτότητα των οντοτήτων που επικοινωνούν ή της προέλευσης των δεδομένων.
- **Έλεγχος πρόσβασης:** υπάρχουν κανόνες για την προστασία ενάντια στην μη εξουσιοδοτημένη πρόσβαση και χρήση πηγών στο OSI. Για να προστατεύουν πολύτιμα δεδομένα, αυτοί οι κανόνες καθορίζουν υποχρεωτικούς ελέγχους πρόσβασης.
- **Εμπιστευτικότητα δεδομένων:** παρέχει προστασία ενάντια στη μη εξουσιοδοτημένη γνωστοποίηση.
- **Ακεραιότητα επικοινωνίας:** επιτυγχάνει ακριβή μετάδοση δεδομένων από την πηγή στον προορισμό.
- **Διαθεσιμότητα υπηρεσίας:** επιτυγχάνει τη μικρότερη αποδεκτή, συνεχόμενη και παρεχόμενη υπηρεσία.
- **Ευθύνη:** ανιχνεύει δραστηριότητες που επηρεάζουν την υπεύθυνη οντότητα.
- **Μη αποκήρυξη:** στόχος της είναι να προστατεύσει τον αποστολέα και/ ή τον παραλήπτη ενάντια σε χρηστή που λαθεμένα αρνείται την αποδοχή ή μετάδοση των δεδομένων.

4.7 Μηχανισμοί ασφαλείας OSI

I. Μηχανισμοί ελέγχου δρομολόγησης: διαλέγει τα πιο ασφαλή υπό-δίκτυα και συνδέσμους.
II. Μηχανισμοί ακεραιότητας δεδομένων: αποτελούνται από κώδικες μπλοκαρίσματος και κρυπτογραφικό έλεγχο λειτουργιών.
III. Κρυπτογράφηση: μπορεί να παρέχει εμπιστευτικότητα δεδομένων και δεδομένα ροής της κυκλοφορίας.
IV. Μηχανισμοί ψηφιακής υπογραφής: μέρος κρυπτογραφίας ως διαδικασία υπογραφής.
V. Μηχανισμοί πιστοποίησης συναλλαγών: κωδικοί και κρυπτογραφικές μέθοδοι.
VI. Μηχανισμοί κίνησης: προστασία ενάντια στην ανάλυση κίνησης.

4.8 Ασύρματα δίκτυα

Η κυριότερη διαφορά μεταξύ ενσύρματων και ασύρματων δικτύων είναι ο τρόπος με τον οποίο μεταδίδονται τα δεδομένα. Όσο αφορά τα προβλήματα ασφαλείας, η κύρια διαφορά ανάμεσα σε αυτά τα δυο είδη δικτύων είναι ο τρόπος με τον οποίο γίνεται η πρόσβαση στα μεταδιδόμενα δεδομένα. Στα ενσύρματα δίκτυα, αυτό γίνεται με υποκλοπή του μέσου (καλώδιο) που χρησιμοποιείται για την επικοινωνία του δικτύου. Στα ασύρματα δίκτυα, το μέσο επικοινωνίας είναι ο αέρας. Η μεταδιδόμενη πληροφορία, μέσα από τη συχνότητα μετάδοσης, μπορεί να γίνει διαθέσιμη από διάφορους εξοπλισμούς, οι οποίοι βρίσκονται εύκολα, γρήγορα και φθηνά στην αγορά. Από τα πρώτα στάδια ανάπτυξης των ασύρματων δικτύων, η ασφάλειά τους θα έπαιζε μεγάλο ρόλο, σύμφωνα με τους ειδικούς. Τα ασύρματα δίκτυα είναι παραδοσιακά λιγότερο ασφαλή σε σχέση με τα ενσύρματα, από τη στιγμή που η μετάδοση της πληροφορίας γίνεται μέσω του αέρα και ο καθένας μπορεί να έχει πρόσβαση σε αυτήν. (Bulbul, H. & Batmaz, I. & Ozel, M, 2008)

4.9 Ασφάλεια στα ασύρματα δίκτυα

Υπάρχουν τρία είδη ασύρματης ασφάλειας, κάθε ένα από τα οποία χρησιμοποιεί τον ομώνυμο αλγόριθμο, που παρέχει την απαιτούμενη κρυπτογράφηση της μεταδιδόμενης πληροφορίας. Αυτά είναι: η Ισοδύναμη ενσύρματη ασφάλεια (Wired Equivalent Privacy ή WEP), η Ασύρματη προστατευόμενη πρόσβαση (Wi-fi Protected Access ή WPA) και το Δίκτυο αυτοδύναμης ασφάλειας (Robust Security Network ή RSN).

α) Ο μηχανισμός ασφαλείας WEP

Ο WEP αρχικά προοριζόταν στο να δώσει στους χρήστες την αίσθηση ότι βρίσκονται σε ενσύρματα δίκτυα με την αντίστοιχη ασφάλεια. Ο κύριος προορισμός του WEP δεν ήταν να παρέχει ένα επίπεδο ασφαλείας υψηλότερο από αυτό που υπήρχε στα ενσύρματα δίκτυα, αλλά ένα επίπεδο ασφαλείας ιδίου μεγέθους. Παρόλα αυτά, η πρακτική του χρήση έδειξε ότι ο WEP ήταν αρκετά υποδεέστερος από την ασφάλεια των ενσύρματων δικτύων. (Wong, S, 2003)

Όταν ο WEP είναι ενεργός, κάθε 802.11 πακέτο κρυπτογραφείται ξεχωριστά με ένα Rivest Cipher 4 (RC4) κύμα και παράγεται ένα κλειδί των 64-bit. Αυτό το κλειδί αποτελείται από 24-bit διάνυσμα αρχικοποίησης (Initialization Vector ή IV) και ένα κλειδί WEP των 40-bit. Το κρυπτογραφημένο πακέτο παράγεται με αποκλειστική διάζευξη του αρχικού πακέτου και του κύματος RC4. Το IV επιλέγεται από τον αποστολέα και μπορεί να αλλαχθεί περιοδικά, έτσι ώστε κάθε πακέτο να μην κρυπτογραφείται με το ίδιο κύμα RC4. Όπως αναφέρθηκε πριν, ο WEP χρησιμοποιεί το RC4 κύμα κρυπτογράφησης με ένα διάνυσμα αρχικοποίησης των 24-bit για κρυπτογράφηση. Η σχεδίαση του WEP αφήνει το σύστημα ευάλωτο σε πολλές περιοχές, και ένα από τα πιο ευάλωτα μέρη είναι το διάνυσμα αρχικοποίησης των 24- bit, το οποίο μπορεί να οδηγήσει σε επαναχρησιμοποίηση του κλειδιού κρυπτογράφησης. (Wong, S, 2003)

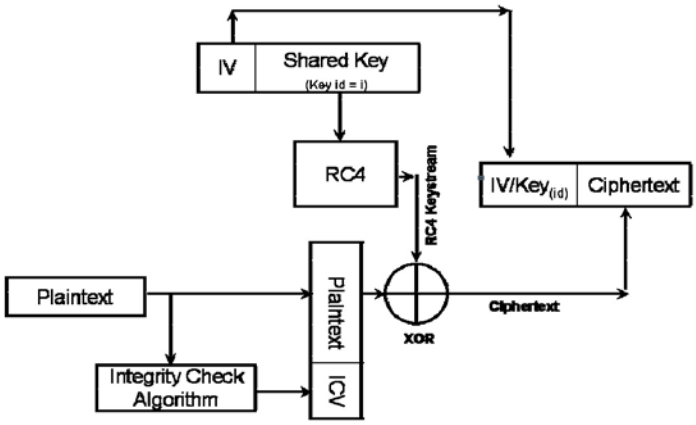


Figure -1 WEP Encryption

Εικόνα 9: Μηχανισμός ασφαλείας WEP

β) Οι αδυναμίες του WEP

Η χρήση κύριων κλειδιών άμεσα: Από την κρυπτογραφική άποψη, η χρήση κύριων κλειδιών κρυπτογράφησης άμεσα δεν συνίσταται. Τα κύρια κλειδιά πρέπει μόνο να χρησιμοποιούνται για την παραγωγή προσωρινών κλειδιών.

Μικρό μέγεθος κλειδιού: Το μέγεθος κλειδιού για τον WEP είναι 40-bit, το οποίο έχει καταταγεί σα μια από τις μεγαλύτερες αδυναμίες του. Την προηγούμενη 10ετία, τα κλειδιά των 40-bit, θεωρούνταν αξιόπιστα για μερικές εφαρμογές, όπως την προστασία από απλή παρακολούθηση των δεδομένων. Το πρότυπο 802.11 δεν καθορίζει κάποια αλλά κλειδιά διαφορετικού μεγέθους, παρά μόνο τα υπάρχοντα των 40-bit. Οι περισσότεροι πωλητές χρησιμοποιούν κλειδιά με μέγεθος που κυμαίνεται στα 104-232 bit, τα όποια είναι πιο ανθεκτικά σε επιθέσεις.

Έλλειψη διαχείρισης κλειδιού: Η διαχείριση κλειδιού δεν καθορίζεται συγκεκριμένα στο WEP. Από τη στιγμή λοιπόν που δεν καθορίζονται, τότε τα κλειδιά δεν θα ανανεώνονται, θα είναι μεγάλης διάρκειας ζωής και χαμηλής ποιότητας. Τα περισσότερα ασύρματα δίκτυα τα οποία χρησιμοποιούν ασφάλεια WEP, μοιράζονται το ίδιο κλειδί για κάθε κόμβο του δικτύου. Τα σημεία πρόσβασης και οι σταθμοί των πελατών πρέπει να προγραμματίζονται με το ίδιο κλειδί. Από τη στιγμή που η αλλαγή κλειδιών είναι μια δύσκολη διαδικασία, τα κλειδιά παραμένουν τα ιδία για μεγάλο χρονικό διάστημα και δεν ανανεώνονται από τους διαχειριστές των δικτύων.

Η χρήση του RC4: Η εφαρμογή του RC4 θωρείται ότι έχει αδύναμα κλειδιά, που σημαίνει ότι υπάρχει μεγαλύτερη συσχέτιση μεταξύ του κλειδιού και του τελικού αποτελέσματος, σε αντίθεση με αυτό που πρέπει να γίνεται. Είναι εύκολο να προσδιοριστεί,

ποια πακέτα έχουν κρυπτογραφηθεί με το αδύναμο κλειδί. Από τη στιγμή που τα τρία πρώτα bit λαμβάνονται από το IV, το οποίο στέλνεται χωρίς κρυπτογράφηση στο κάθε πακέτο, αυτή η αδυναμία μπορεί να «αξιοποιηθεί» από διάφορες παθητικές επιθέσεις.

Επαναχρησιμοποιούμενα και μικρού μεγέθους IV: Ανεξάρτητα από το μέγεθος του κλειδιού, το μέγεθος του IV το οποίο είναι 24-bit, μπορεί να παράγει 16.777.216 διαφορετικά RC4 κύματα κρυπτογράφησης για ένα δοσμένο κλειδί. Σε ένα σχετικά απασχολημένο δίκτυο, αυτός ο αριθμός μπορεί εύκολα να ξεπεραστεί μέσα σε μερικές ώρες και η επαναχρησιμοποίηση τους γίνεται αναπόφευκτη. Αν με κάποιο τρόπο ,μπορεί να βρεθεί το κύμα κρυπτογράφησης RC4, κάποιος εισβολές μπορεί να αποκρυπτογραφήσει μεταγενέστερα πακέτα, που είχαν κρυπτογραφηθεί με το ίδιο IV. Από τη στιγμή που υπάρχουν το πολύ 16.777.216 τιμές, ο τρόπος με τον οποίο επιλέγεται το IV κάνει τη διαφορά. Δυστυχώς, ο WEP δεν προκαθορίζει τον τρόπο επιλογής, δηλαδή το πόσο συχνά πρέπει να αλλάζουν τα IV. Μερικές εγκαταστάσεις ξεκινούν το IV από το μηδέν και το αυξάνουν σταδιακά για κάθε πακέτο, μέχρις ότου περάσουν οι 16.777.216 τιμές και ξαναφτάσουμε στο 0. Με μια τυχαία επιλογή του IV, υπάρχει 50% μικρότερη πιθανότητα επαναχρησιμοποίησης μετά από περίπου 5000 πακέτα. (Boland, H., & Mousavi, H, 2004)

Η αδυναμία του αλγορίθμου: Ο WEP ICV βασίζεται στον κυκλικό έλεγχο πλεονασμού CRC-32, έναν αλγόριθμο που μπορεί να ανιχνεύει το θόρυβο και τα κοινά λάθη στη μετάδοση. Ο CRC-32 είναι πολύ καλός για τον έλεγχο της ακεραιότητας και για την εύρεση λαθών, αλλά δεν είναι καλή επιλογή από κρυπτογραφική σκοπιά. Ο CRC-32 ICV, είναι μια γραμμική λειτουργία του μηνύματος που σημαίνει ότι ένας εισβολέας μπορεί εύκολα να μεταβάλει ένα κρυπτογραφημένο μήνυμα ώστε το ICV να δείχνει αυθεντικό, μετά από αυτή την αλλαγή. Οποίος είναι ικανός να μεταβάλει κρυπτογραφημένα πακέτα, μπορεί να προκαλέσει μια σειρά από επιθέσεις. Αυτός που κάνει την επίθεση, μπορεί να κάνει το ασύρματο σημείο πρόσβασης του θύματος, να κρυπτογραφεί τα πακέτα για αυτόν.

Αυτό γίνεται πολύ εύκολα, με την κυρίευση ενός κρυπτογραφημένου πακέτου, αλλάζοντας τη διεύθυνση προορισμού του κάθε πακέτου, ώστε να είναι η IP διεύθυνση του εισβολέα. Εύκολη σφυρηλάτηση των μηνυμάτων πιστοποίησης: Το 802.11 στάνταρ, καθορίζει 2 τύπους πιστοποίησης , την πιστοποίηση ανοιχτού συστήματος (Open System) και την πιστοποίηση κοινόχρηστου κλειδιού (Shared Key). Η πιστοποίηση μαζί με τη WEP ασφάλεια, στην πραγματικότητα μειώνει την συνολική ασφάλεια του δι-

κτύου, αφού κάνει πιο εύκολο σε εισβολείς , να μαντεύουν το WEP κλειδί. Η πιστοποίηση κοινόχρηστου κλειδιού περιλαμβάνει τη κρυπτογράφηση του δημοσίου κλειδιού με την κρυπτογράφηση μιας πρόκλησης. Το πρόβλημα εδώ είναι, ότι κάποιος μπορεί να παρακολουθεί την κρυπτογραφημένη απάντηση. Αυτοί λοιπόν,

μπορούν να προσδιορίσουν το κύμα RC4 που χρησιμοποιείται στην κρυπτογράφηση της απάντησης, και χρησιμοποιούν αυτό το κύμα ώστε να κρυπτογραφήσουν οποιοδήποτε πρόκληση λάβουν στο μέλλον. Έτσι, παρακολουθώντας μια επιτυχημένη πιστοποίηση, αυτός που κάνει την επίθεση μπορεί να πλαστογραφήσει μια πιστοποίηση. Το μόνο πλεονέκτημα της πιστοποίησης κοινόχρηστου κλειδιού είναι ότι μειώνει την ικανότητα του επιτιθέμενου να δημιουργεί επιθέσεις άρνησης υπηρεσίας, με την αποστολή πακέτων σκουπιδιών.

4.9.1 Ο μηχανισμός προστασίας ασύρματης πρόσβασης WPA

Ο WPA σχεδιάστηκε ώστε να βελτιώνει τα προβλήματα ασφαλείας που παρουσιάστηκαν στο WEP. Η τεχνολογία σχεδιάστηκε ώστε να δουλεύει με τα υπάρχοντα προϊόντα ασύρματης πρόσβασης που έχουν λειτουργήσει με WEP ασφάλεια. Οι κύριες βελτιώσεις της νέας ασφάλειας είναι οι εξής:

- Βελτιωμένη κωδικοποίηση δεδομένων μέσα από το πρωτόκολλο ακεραιότητας προσωρινού κλειδιού (TKIP). Αυτό το πρωτόκολλο ανακατεύει τα κλειδιά, χρησιμοποιώντας έναν αλγόριθμο κατακερματισμού, προσθέτοντας ένα στοιχείο ελέγχου ακεραιότητας και βεβαιώνοντας ότι τα κλειδιά δεν έχουν μετριαστεί. Το TKIP είναι μια λειτουργιά κατακερματισμού προσωρινού κλειδιού, η οποία είναι εναλλακτική του WEP, ώστε να διορθώνει όλα τα προβλήματα ασφαλείας και δεν χρειάζεται αλλαγή υλικού (hardware). Το TKIP χρησιμοποιείται το ίδιο RC4 κύμα κρυπτογράφησης με το WEP. Το κλειδί σε αυτή την περίπτωση είναι 128-bit και ονομάζεται προσωρινό κλειδί. Το TKIP χρησιμοποιεί ένα διάνυσμα αρχικοποίησης των 48- bit, το οποίο χρησιμοποιείται σα μετρητής. Ακόμα και αν το προσωρινό κλειδί μοιράζεται, όλες οι σχετικές οντότητες παράγουν ένα διαφορετικό κλειδί RC4. Από τη στιγμή που οι επικοινωνούντες οντότητες εκτελούν παραγωγή κλειδιού δύο φάσεων, ενός μοναδικού πακέτου που ονομάζεται «Κλειδί πακέτου», αυτό είναι το κλειδί που χρησιμοποιείται για το ρεύμα RC4.

- Πιστοποίηση χρήστη, η οποία λείπει από τον WEP μηχανισμό, μέσα από το πρωτόκολλο εκτεταμένης πιστοποίησης (EAP). Ο WEP μεθοδεύει την πρόσβαση σε ένα ασύρματο δίκτυο, σε μια συγκεκριμένη διεύθυνση ελέγχου της πρόσβασης των μέσων (MAC Address) του υλικού του δικτύου, που είναι σχετικά απλό να κλαπεί. Το EAP δημιουργείται πάνω σε μια κωδικοποίηση πιο ασφαλούς δημόσιου κλειδιού, για να μπορέσει να επιβεβαιώσει ότι μόνο τα πιστοποιημένα δίκτυα μπορούν να προσπελάσουν το υπάρχων δίκτυο.
- Ακεραιότητα, ένας νέος μηχανισμός, χρησιμοποιείται για την ακεραιότητα, ο οποίος ονομάζεται κώδικας ακεραιότητας μηνυμάτων (MIC). Ο κώδικας ακεραιότητας μηνυμάτων χρησιμοποιείται στο να ανακαλύπτει λάθη σε περιεχόμενα

δεδομένων, είτε λόγω λαθών μετάδοσης είτε πιθανών αλλαγών από εισβολείς. (Potter, B, 2003)

4.9.2 Ο μηχανισμός αυτοδύναμης ασφάλειας δικτύων RSN

Η αυτοδύναμη ασφάλεια δικτύων χρησιμοποιεί δυναμική διαπραγμάτευση της πιστοποίησης και αλγόριθμους κρυπτογράφησης ανάμεσα στα σημεία πρόσβασης και στις φορητές συσκευές. Τα σχήματα πιστοποίησης που βρίσκονται στο σχέδιο αυτό βασίζονται στο 802.1X και στο πρωτόκολλο επεκτάσιμης πιστοποίησης (EAP). Ο αλγόριθμος κρυπτογράφησης είναι ο AES (Advanced Encryption Standard). Η δυναμική διαπραγμάτευση της πιστοποίησης και οι αλγόριθμοι κρυπτογράφησης, επιτρέπουν στην RSN να εξελιχθεί. Η χρήση δυναμικής διαπραγμάτευσης καθώς και των EAP- AES δίνει στην RSN τα πρωτεία ασφαλείας σε σχέση με τα WEP- WPA.

Ωστόσο, ο RSN δε λειτουργεί σωστά σε κληροδοτημένες συσκευές. Δυστυχώς, μόνο οι τελευταίες συσκευές έχουν την απαιτούμενη δυνατότητα να επιταχύνουν τους αλγόριθμους σε πελάτες και σημεία πρόσβασης, παρέχοντας την αναμενόμενη απόδοση των σημερινών προϊόντων ασύρματων δικτύων.

5.0 Συμπεράσματα

Όπως περιγράψαμε παραπάνω, η ασφάλεια δικτύων αποκτά όλο και μεγαλύτερη σημασία, εν όψει των διάφορων επιθέσεων, που καθιστούν την περίμετρο ασφαλείας λιγότερο αποτελεσματική αλλά και ταυτόχρονα πολύ ευάλωτη. Αναφέραμε ένα μεγάλο είδος απειλών σε συστήματα, οι οποίες μπορούν να αντιμετωπιστούν με την χρήση του τοίχους προστασίας (firewall) αλλά και της ασφάλειας που παρέχουν τα πρωτόκολλα επικοινωνίας.

Παρ' όλα αυτά, λόγω της ραγδαίας εξέλιξης των επικοινωνιών, αλλά κυρίως των ασύρματων δικτύων, η ανάγκη για συνεχόμενη ασφάλεια στα νέα δίκτυα είναι επιβεβλημένη. Οι υπάρχοντες μηχανισμοί ασύρματης ασφαλείας, ξεκινώντας από τον παλαιότερο WEP έως τον πιο πρόσφατο RSN, παρέχουν ένα είδος ασφαλείας που σε πολλές περιπτώσεις απωθεί τις επιθέσεις από εισβολείς, οι οποίες περιλαμβάνουν από την πιο απλή περίπτωση την παρακολούθηση της κίνησης του δικτύου, έως τις πιο περίπλοκες όπως την μεταβολή και υποκλοπή δεδομένων της ασύρματης επικοινωνίας.

Το προσωπικό ασφαλείας που διαχειρίζεται τα ασύρματα δίκτυα, πρέπει να μπορεί να είναι σε θέση να κατανοεί και να αντιλαμβάνεται τέτοιες επιθέσεις. Παρόλα αυτά, τα ευάλωτα σημεία των μηχανισμών αυτών είναι γνωστά και πρέπει να μπορούν να αντιμετωπιστούν μέσα από την υπάρχουσα υποδομή και τεχνολογία. Η καλή εφαρμογή των αλγορίθμων ασφαλείας πρέπει να ληφθεί πολύ σοβαρά υπ' όψιν, γιατί το κόστος υποκλοπής δεδομένων υπολογίζεται ότι θα είναι πολύ μεγάλο. Για το λόγο αυτό, η προσαρμογή και συνεχόμενη εξέλιξη των ήδη υπαρχόντων μηχανισμών θεωρείται επιβεβλημένη, ώστε να μπορεί να λειτουργεί σωστά, αποδοτικά και αξιόπιστα το δίκτυο.

6.0 Βιβλιογραφία

1. A. Carasik-Henmi, T. W. S. C. A. R. J. S. D. L. S., 2003. *Best damn firewall book period.* s.l.:Syngress Publishing.
2. A. Henmi, M. L. A. S. C. C., 2006. *Firewall Policies and VPN Configurations.* s.l.:Syngress Publishing.
3. Bellovin, W. R. C. a. S. M., n.d. *Firewalls and Internet Security: Repelling the.* s.l.:Addison-Wesley.
4. E. Zwicky, S. C. D. B. C. D. R., 2000. *Building Internet Firewalls.* 2η Έκδοση επιμ. s.l.:O'Reilly.
5. G. Bastien, C. D., 2003. *CCSP Cisco Secure PIX Firewall Advanced Exam Certification Guide.* s.l.:Cisco Press.
6. G. Schudel, D. J. S., 2008. *Router Security Strategies: Securing IP Network Traffic Planes.* s.l.:Cisco Press.
7. J. Frahim, O. S., 2005. *Cisco ASA: All-in-One Firewall, IPS, and VPN Adaptive Security Appliance.* s.l.:Cisco Press.
8. Pepelnjak, I., 2007. *Deploying Zone-Based Firewalls.* s.l.:Digital Shortcut.
9. W. Noonan, I. D., 2006. *Firewall Fundamentals.* s.l.:Cisco Press.
10. W. R. Cheswick, S. M. B. D. R., 2003. *Firewalls and Internet Security: Repelling the Wily Hacker.* 2 Έκδοση επιμ. s.l.:Addison-Wesley Professional Computing Series.
11. Β., Χ., 1997. *Ασφάλεια Πληροφοριακών Συστημάτων.* Πειραιάς: Σημειώσεις Διδασκαλείας .
12. Δημήτρης Γκριτζαλης, Σ. Γ. Σ. Κ., 2003. *Ασφάλεια Δικτύων υπολογιστών.* Αθήνα: Παπασωτηριου.
13. Πομπόρτσης Ανδρέας, Π. Γ., 2003. *Ασφάλεια Δικτύων Υπολογιστών.* Αθήνα: Τζιόλα.
14. Πουλάκης, Δ. Μ., 2005. *Κρυπτογραφία, η επιστήμη της ασφαλούς επικοινωνίας.* Αθήνα: Ζήτη.