ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΜΜΕ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΜΕΛΕΤΗ ΚΑΙ ΑΝΑΛΥΣΗ ΤΕΧΝΙΚΩΝ ΚΑΙ ΜΕΘΟΔΩΝ ΕΙΣΒΟΛΗΣ ΣΕ ΛΟΓΙΣΜΙΚΑ ΓΙΑ ΤΗ ΔΙΑΤΗΡΗΣΗ ΤΩΝ ΕΠΙΠΕΔΩΝ ΑΣΦΑΛΕΙΑΣ ΤΟΥΣ

ΣΤΑΥΡΟΠΟΥΛΟΣ ΠΑΝΑΓΙΩΤΗΣ

ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ: ΦΕΡΕΝΤΙΝΟΣ ΒΗΣΣΑΡΙΩΝ

ΠΥΡΓΟΣ, 2018

ΠΙΣΤΟΠΟΙΗΣΗ

Πιστοποιείται ότι η πτυχιακή εργασία με θέμα:

«ΜΕΛΕΤΗ ΚΑΙ ΑΝΑΛΥΣΗ ΤΕΧΝΙΚΩΝ ΚΑΙ ΜΕΘΟΔΩΝ ΕΙΣΒΟΛΗΣ ΣΕ ΛΟΓΙΣΜΙΚΑ ΓΙΑ ΤΗ ΔΙΑΤΗΡΗΣΗ ΤΩΝ ΕΠΙΠΕΔΩΝ ΑΣΦΑΛΕΙΑΣ ΤΟΥΣ»

Του φοιτητή του Τμήματος ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΜΜΕ

ΣΤΑΥΡΟΠΟΥΛΟΥ Δ. ΠΑΝΑΓΙΩΤΗ

παρουσιάστηκε δημόσια και εξετάσθηκε στο Τμήμα ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΜΜΕ στις

_____ / _____ / _____

Ο ΕΠΙΒΛΕΠΩΝ

(ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΕΠΙΒΛΕΠΟΝΤΑ)

Ο ΠΡΟΕΔΡΟΣ ΤΟΥ ΤΜΗΜΑΤΟΣ

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ ΠΕΡΙ ΜΗ ΛΟΓΟΚΛΟΠΗΣ

Βεβαιώνω ότι είμαι συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Ακόμα δηλώνω ότι αυτή η γραπτή εργασία προετοιμάστηκε από εμένα προσωπικά και αποκλειστικά και ειδικά για την συγκεκριμένη πτυχιακή εργασία και ότι θα αναλάβω πλήρως τις συνέπειες εάν η εργασία αυτή αποδειχθεί ότι δεν μου ανήκει.

ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΣΠΟΥΔΑΣΤΗ **ΑΜ** **ΥΠΟΓΡΑΦΗ**

ΣΤΑΥΡΟΠΟΥΛΟΣ Δ. ΠΑΝΑΓΙΩΤΗΣ

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα πτυχιακή εργασία αποτελεί απόρροια και εκπλήρωση της πορείας της φοίτησης μου στο Τμήμα Πληροφορικής και Μέσων Μαζικής Ενημέρωσης του Τ.Ε.Ι Δυτικής Ελλάδος που εδρεύει στον Πύργο. Τόσο οι σπουδές μου, όσο και η πρακτική άσκηση, μου έδωσαν τα απαραίτητα εφόδια για τη μελλοντική μου επαγγελματική πορεία, αλλά εκτός τούτου συνέβαλαν σημαντικά στη διαμόρφωση της αντιληπτικής μου ικανότητας και στη βελτίωση της προσωπικότητάς μου. Θα ήθελα να ευχαριστήσω θερμά όλους τους καθηγητές μου και ειδικά τον κύριο Φερεντίνο Βησσαρίωνα για την επίβλεψη και περάτωση αυτής της πτυχιακής εργασίας. Επίσης, θα ήθελα να ευχαριστήσω τους γονείς μου για την σημαντική τους ηθική και οικονομική στήριξη, καθώς και την εμπιστοσύνη τους σε εμένα καθ' όλη τη διάρκεια των σπουδών μου. Τέλος, θα ήθελα να ευχαριστήσω τους φίλους και συμφοιτητές μου για τις όμορφες στιγμές που μοιραστήκαμε κατά τη διάρκεια της φοίτησής μας στον Πύργο.

ΠΡΟΛΟΓΟΣ

Το θέμα της παρούσας εργασίας σχετίζεται με τα Συστήματα Ανίχνευσης Εισβολών (Intrusion Detection Systems) καθώς και τα Συστήματα Πρόληψης Εισβολών (Intrusion Prevention Systems), μια τεχνολογία που έχει γνωρίσει σημαντική διάδοση τα τελευταία χρόνια, διότι τη σημερινή εποχή η ανάγκη προστασίας και ασφάλειας των υπολογιστικών συστημάτων είναι αυξημένη αλλά και επιτακτική. Η διατήρηση των επιπέδων ασφαλείας του λογισμικού των υπολογιστικών συστημάτων αποτελεί βασικό αντικείμενο έρευνας και κρίσιμο τεχνολογικό ζήτημα της εποχής μας συγχρόνως. Η καθολικότητα χρήσης του διαδικτύου και η ραγδαία εξέλιξη των τεχνολογικών μέσων έχουν ως επακόλουθο την ταυτόχρονη ανάπτυξη των κακόβουλων λογισμικών, τα οποία προσπαθούν να εισβάλουν σε θωρακισμένα και καλά διαφυλαγμένα δεδομένα ευαίσθητου περιεχομένου πληροφοριών. Η εξέλιξη αυτή συνεπώς, αναπόφευκτα οδήγησε στην ανάπτυξη στοχευμένων μεθόδων άμυνας, ικανών να αντιμετωπίζουν νέα μοντέλα εισβολών και να αναγνωρίζουν-προλαμβάνουν άγνωστες διαδικτυακές απειλές. Στόχος της εργασίας είναι να περιγραφεί εκτενώς, πρώτιστα ο τρόπος ‘αντίληψης’ και αντιμετώπισης των Συστημάτων Ανίχνευσης αλλά και Πρόληψης Εισβολών, σε περίπτωση παραβίασης της ασφάλειας ενός υπολογιστικού συστήματος και κατ’επέκταση ενός δικτύου, από ανεπιθύμητες επιθέσεις. Αναφέρονται και αναπτύσσονται οι θεωρητικοί τύποι, η αρχιτεκτονική και τα μοντέλα ανίχνευσης στα Συστήματα Ανίχνευσης/ Πρόληψης Εισβολών ώστε να διερευνηθούν οι μηχανισμοί εκείνοι που θα μπορούσαν να οδηγήσουν στην ομαλή λειτουργία των δικτύων. Ένα από τα πλέον δημοφιλή, ευρέως διαδεδομένα και αποτελεσματικά Συστήματα Ανίχνευσης/ Πρόληψης Εισβολών είναι και το λογισμικό Snort (Martin Roesch,1998.), που αναφέρεται ως παράδειγμα εφαρμογής στην εργασία αυτή. Παρ’ολο που υπάρχουν και άλλα αντίστοιχα πακέτα λογισμικών, καταλήξαμε σε αυτή την επιλογή για το λόγο ότι είναι ένα ελεύθερο, *“open source”* λογισμικό που διατίθεται δωρεάν.

ΠΕΡΙΛΗΨΗ

Τα Συστήματα Ανίχνευσης και Πρόληψης δικτυακών Εισβολών έχουν σαν κύρια αποστολή την έγκαιρη ανίχνευση αλλά και την αποτροπή των διάφορων επιθέσεων που απειλούν στις μέρες μας όλα τα δίκτυα υπολογιστών. Η ανάπτυξη της τεχνολογίας αυτών των συστημάτων έχει καταγράψει μεγάλη πρόοδο τα τελευταία χρόνια και συνεπώς τείνουν να γίνουν απαραίτητο κομμάτι κάθε ολοκληρωμένης αρχιτεκτονικής ασφάλειας των δικτύων. Εστιάζοντας λοιπόν στην ανάγκη αυτή, στην παρούσα εργασία επιχειρείται μια διεξοδική μελέτη των συστημάτων αυτών. Πιο συγκεκριμένα, γίνεται μια περιγραφή των Συστημάτων Ανίχνευσης Εισβολών και των δύο σημαντικών κατηγοριών τους, NIDS και HIDS, και αναλύονται οι τεχνικές και οι μηχανισμοί που χρησιμοποιούνται προς ανίχνευση πιθανών επιθέσεων. Εν συνεχεία, γίνεται και μια αναφορά των προιόντων και πιο συγκεκριμένα του Snort , ενός software Συστήματος Ανίχνευσης/ Πρόληψης Εισβολών, που είναι βασισμένο κυρίως πάνω στο δίκτυο υπολογιστών.

ABSTRACT

Intrusion detection and prevention systems have as their primary task the early detection and prevention of the various attacks that are currently threatening all computer networks. The development of the technology of these systems has made great progress in recent years and tends to become an indispensable part of any integrated network security architecture. Focusing on this need, this study attempts a thorough study of these systems. In particular, a description of the Intrusion Detection Systems of both major categories, NIDS and HIDS, is made and the techniques and mechanisms used to detect possible attacks are analyzed. Then a detailed description of Snort, a free and open source Network Intrusion Prevention System and Network-Based Intrusion Detection System (NIDS) is made.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ

Σύστημα Ανίχνευσης Εισβολών (ΣΑΕ) - IDS:Intrusion Detection System, HIDS:Host Intrusion Detection System, NIDS:Network Intrusion Detection System, Σύστημα παρεμπόδισης εισβολών - IPS:Intrusion Prevention System, Μηχανική Μάθηση - Machine learning, Snort.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΥΡΕΤΗΡΙΟ ΕΙΚΟΝΩΝ

ΕΥΡΕΤΗΡΙΟ ΠΙΝΑΚΩΝ

ΕΙΣΑΓΩΓΗ

Η παρούσα πτυχιακή εργασία ως στόχο έχει τη μελέτη και καταγραφή των μηχανισμών των Συστημάτων Ανίχνευσης Εισβολών (IDS) και κατ'επέκταση των Συστημάτων Πρόληψης Εισβολών (IPS) ομοίως, με σκοπό τη διατήρηση της ασφάλειάς, και την υποκλοπή δεδομένων ή την παράκαμψη των επιπέδων ασφαλείας τους και της αυθεντικότητάς τους. Θα αναλυθούν περαιτέρω λογισμικά υποβοήθησης εισβολής και εφαρμογές αναγνώρισης απειλών και θα καταγραφούν οι λειτουργίες τους αποδίδοντας παραδείγματα και μετρώντας τον βαθμό επιτυχίας αυτών.

Αναλυτικότερα, το παρόν κείμενο δομείται από εφτά κεφάλαια τα οποία συμπυκνώνουν σε γενικές γραμμές το σύνολο των γνώσεων που συγκεντρώθηκαν και χρησιμοποιήθηκαν για την υλοποίηση της εργασίας αυτής και των όσων πραγματεύεται. Στο πρώτο κεφάλαιο, ως εισαγωγικό που είναι, πραγματοποιείται μια ιστορική αναδρομή ως προς την εξέλιξη και ανάπτυξη της ανίχνευσης εισβολών των υπολογιστικών συστημάτων, λόγω της αναγκαιότητας ασφάλειας, που έχουν καταγραφεί τόσο τα τελευταία χρόνια όσο και σε πραγματικές εισβολές που έχουν συμβεί από αρχαιοτάτων χρόνων ως παραλληρισμός των σύγχρονων προγραμματιστικών εισβολών. Στο δεύτερο κεφάλαιο παρατίθεται μια πιο θεωρητική ανάλυση των θεμελειωδών εννοιών που αφορούν την ασφάλεια των υπολογιστικών συστημάτων, με ό,τι αυτή περιλαμβάνει. Παρακάτω, το τρίτο κεφάλαιο αποτελεί μία εμπεριστατωμένη αναφορά του χώρου των ψηφιακών εγκλημάτων λόγω αδυναμίας ασφάλειας, μέσω επιθέσεων διαφόρων τύπων. Διαχωρίζονται οι βασικές έννοιες του hacking και cracking και περιγράφεται η διαδικασία του να σαμποτάρει κανείς ένα λογισμικό για να το 'σπάσει.'. Στο τέταρτο κεφάλαιο, εν συνεχεία, περιγράφονται οι πιο διαδεδομένοι αλγόριθμοι μηχανικής μάθησης,, όπου στηρίχθηκε η ανάπτυξη γνωστών εφαρμογών και αναλύονται τα μέτρα αξιολόγησης, τα οποία καθορίζουν το ποσοστό επιτυχίας ενός μοντέλου στην επίλυση ενός προβλήματος. Έπειτα, στο πέμπτο κεφάλαιο αναλύονται τα Συστήματα Ανίχνευσης Εισβολών που είναι ουσιαστικά οι μηχανισμοί εποπτίας και ελέγχου για την προστασία των υπολογιστικών συστημάτων. Αναπτύσσεται η αρχιτεκτονική τους, τα μοντέλα και η κατηγοριοποίησή τους βάσει συγκεκριμένων κριτηρίων, καθώς και ο τρόπος απόκρισής τους στις όποιες εισβολές. Στο έκτο κεφάλαιο εξετάζουμε τα Συστηματα Πρόληψης Εισβολών και τον τρόπο εφαρμογής και λειτουργίας τους καθώς και τη σύγκρισή τους σε σχέση με τα Συστήματα Ανίχνευσης Εισβολών. Ακόμη, παρουσιάζονται τέτοια λογισμικά και εκτενέστερα το ελεύθερα διαθέσιμο λογισμικό Snort και μερικές εφαρμογές του. Τέλος, παρατίθενται τα συμπεράσματα που προέκυψαν από την εργασία αυτή και προτείνονται κατευθύνσεις προς τις οποίες μπορεί το θέμα που πραγματεύεται να επεκταθεί.

1 ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ ΣΕ ΥΠΟΛΟΓΙΣΤΙΚΑ ΣΥΣΤΗΜΑΤΑ

1.1 ΑΝΑΓΚΑΙΟΤΗΤΑ ΥΠΑΡΞΗΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ/ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Η έννοια της ασφάλειας (τόσο των εδαφικών εκτάσεων όσο και πληροφοριών) καθώς και της ασφαλούς εισβολής και υποκλοπής απασχολούσε τους ανθρώπους από την αρχαιότητα ακόμη. Ένα τέτοιο αξιοσημείωτο χαρακτηριστικό παράδειγμα αποτελεί ο Δούρειος Ίππος που ήταν μια ξύλινη κατασκευή, που προσφέρθηκε ως δώρο από τους Αχαιούς στους Τρώες, ύστερα από πρόταση του πολυμήχανου Οδυσσέα. Οι Έλληνες, προσποιούμενοι ότι εγκαταλείπουν την πολιορκία και αναχωρούν, άφησαν έξω από τα τείχη της πόλης τον Δούρειο Ίππο, ως προσφορά για την ασφαλή επιστροφή στην πατρίδα τους. Ο γιγάντιος ξύλινος ίππος αυτός λοιπόν, με οπλισμένους πολεμιστές στο εσωτερικό του, αφού μεταφέρθηκε από τους ίδιους τους Τρώες μέσα στην πόλη τους, συνέβαλε στην άλωση και κατάληψη της Τροίας (1194-1184 π. Χ.).

Εικόνα 1-1 Ο Δούρειος Ίππος [37].

Με αυτόν τον παραλληλισμό ξεκινώντας, θα μιλήσουμε κατ’ επέκταση για την έννοια της ασφάλειας δικτύων όπου αναφερόμαστε σ’ ένα πολυσύνθετο κομμάτι, το οποίο αποτελείται από διάφορους κανόνες, πολιτικές ασφάλειας, ενέργειες αλλά και εξοπλισμό(software/hardware). Με τον όρο «ασφάλεια» λοιπόν, υποδηλώνεται ένα πλήθος από έννοιες, όπως είναι η εμπιστευτικότητα (confidentiality), δηλαδή η προστασία της πληροφορίας από μη εξουσιοδοτημένη πρόσβαση, η ακεραιότητα (integrity), δηλαδή η προστασία της πληροφορίας από μη εξουσιοδοτημένη

τροποποίησή της και τέλος η διαθεσιμότητα (availability), όπου τα δεδομένα υπάρχουν στη θέση, στο χρόνο και στη μορφή που ο χρήστης τα χρειάζεται. Άλλες εκφάνσεις της εμπιστευτικότητας είναι: η ιδιωτικοποίηση (privacy), δηλαδή η προστασία των προσωπικών δεδομένων καθώς και η μυστικότητα (secrecy), δηλαδή η προστασία δεδομένων που ανήκουν σε μία εταιρεία. Δίνοντας λοιπόν, μεγάλη βαρύτητα στην ίδια την ασφάλεια αλλά και την διαχείρισης γεγονότων της ασφάλειας των δικτύων αποτρέπουμε τυχόν επιθέσεις που μπορεί να έχουν ως αντίκτυπο οικονομικές απώλειες ή και πιθανή σπατάλη πολύτιμου χρόνου τόσο για την αποκατάσταση του εκάστοτε συστήματος που δέχτηκε επίθεση, όσο και την αποφυγή ενδεχόμενου καίριου πλήγματος στο κύρος και την αξιοπιστία του συστήματος.

Εικόνα 1-2 Χαρακτηριστικά της Ασφάλειας των Πληροφοριών [38].

Στις μέρες μας η αύξηση των απειλών και επιθέσεων σε ένα υπολογιστικό σύστημα εξέλιξαν και έκαναν απαραίτητα για την ασφάλεια τα Συστήματα Ανίχνευσης Εισβολών. Η ανίχνευση εισβολών είναι η διαδικασία παρακολούθησης των γεγονότων που συμβαίνουν σε ένα σύστημα ή ένα δίκτυο υπολογιστών και με σκοπό την ανάλυση τους για σημάδια πιθανών περιστατικών, τα οποία αποτελούν παραβιάσεις ή επικείμενες απειλές παραβίασης για τις πολιτικές ασφάλειας υπολογιστών, τις πολιτικές χρήσης ή τις συνήθεις πρακτικές ασφαλείας. Έπειτα από τις τεράστιες τεχνολογικές εξελίξεις τα τελευταία χρόνια αναπτύχθηκαν γι’ αυτό τον λόγο τα Συστήματα Ανίχνευσης Εισβολών (Intrusion Detection Systems-IDS) τα οποία βέβαια έκαναν την εμφάνισή τους γύρω στο 1980 και απασχολούν τα τελευταία 40 χρόνια.[8],[21],[47].

1.2 ΑΝΑΠΤΥΞΗ ΤΗΣ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ – ΕΞΕΛΙΞΗ ΤΕΛΕΥΤΑΙΩΝ 40 ΕΤΩΝ

Ένα έγγραφο του USAF (United States Air Force) που δημοσιεύθηκε τον Οκτώβριο του 1972 από τον James P. Anderson περιγράφει το γεγονός ότι η USAF είχε όλο και μεγαλύτερη επίγνωση των προβλημάτων ασφάλειας υπολογιστών. Αυτά τα προβλήματα ήταν αισθητά σχεδόν σε όλες τις πτυχές της λειτουργίας και της διοίκησης των ΗΠΑ. Κατά τη διάρκεια αυτού του χρονικού διαστήματος, το USAF είχε την υποχρέωση παροχής κοινής χρήσης στα συστήματα ηλεκτρονικών υπολογιστών τους, τα οποία περιείχαν διάφορα επίπεδα ταξινομήσεων σε μια ανάγκη γνώσης περιβάλλοντος με μια βάση χρηστών που κατέχει διάφορα επίπεδα ασφαλείας. Τριάντα χρόνια πριν, αυτό δημιούργησε ένα σοβαρό πρόβλημα που εξακολουθεί να είναι μαζί μας σήμερα. Το πρόβλημα παραμένει και ορίζεται ως τον τρόπο ασφαλούς διασφάλισης ξεχωριστών τομέων ταξινόμησης στο ίδιο δίκτυο χωρίς αμφιβολίες για την ασφάλεια. Το 1980, ο James P. Anderson δημοσίευσε μια μελέτη που περιγράφει τους τρόπους βελτίωσης του υπολογιστή στον έλεγχο ασφαλείας και στην επιτήρηση σε χώρους πελατών. Η αρχική ιδέα βρισκόταν πίσω από την αυτοματοποίηση των Σ.Α.Ε. για την αναγνώριση της ταυτότητας του χρήστη, με βάση το έγγραφό του στην εφημερίδα: Πώς να χρησιμοποιήσετε τα αρχεία για τον εντοπισμό χρηστών με μη εξουσιοδοτημένη πρόσβαση [36].

Αυτή η μελέτη ταυτότητας άνοιξε το δρόμο ως μια μορφή ανίχνευσης κακής συμπεριφοράς σε μεμονωμένα δίκτυα. Το πρώτο καθήκον ήταν να καθοριστούν οι απειλές που υπήρχαν. Πριν σχεδιάσει ένα IDS, ήταν απαραίτητο να κατανοήσουμε τους τύπους απειλών και επιθέσεων που θα μπορούσαν να δεχθούν τα συστήματα ηλεκτρονικών υπολογιστών και πώς να τα αναγνωρίσουν σε δεδομένα ελέγχου. Στην πραγματικότητα, αναφερόταν στην πιθανότητα αναγνώρισης και την ανάγκη ενός σχεδίου αξιολόγησης κινδύνου για την κατανόηση της απειλής (ποιοι είναι οι κίνδυνοι, ποια η ικανότητα τους ή τα τρωτά σημεία ενός συστήματος, ποιες είναι οι επιθέσεις ή ποια είναι τα μέσα διείσδυσης), ακολουθώντας έτσι τον σχεδιασμό μιας πολιτικής ασφάλειας με σκοπό την προστασία των υπολογιστικών συστημάτων .Μεταξύ του 1984 και του 1986, η επιστήμων Dorothy Denning, με την επικύρωση και βοήθεια του Peter Neumann, πρότεινε ένα σύστημα ανίχνευσης εισβολών, το οποίο αποτέλεσε τη βάση για την σημερινή μετέπειτα εξέλιξη.

Το μοντέλο αυτό χρησιμοποιούσε ένα αφηρημένο πρότυπο χαρακτηριστικών, τα οποία χαρακτηριστικά αυτά αν δεν πληρούν τα πληροφοριακά συστήματα, τότε υπάρχει σημαντική πιθανότητα να δέχονται κάποια μορφή απειλής. Ερεύνησαν και ανέπτυξαν το πρώτο μοντέλο IDS σε πραγματικό χρόνο. Αυτό το πρωτότυπο μοντέλο ονομάστηκε Σύστημα Ανίχνευσης Εισβολής Εμπειρογνωμόνων (IDES). Το IDES ήταν αρχικά ένα σύστημα εμπειρογνωμόνων βασισμένο σε κανόνες που εκπαιδεύτηκε στον γνωστό τρόπο ανίχνευσης κακόβουλης δραστηριότητας. Το ίδιο σύστημα έχει βελτιωθεί και συνεχίζει να βελτιώνεται έχοντας γίνει το γνωστό σήμερα Σύστημα Ανίχνευσης Εισβολής Εμπειρογνωμόνων νέας γενιάς (NIDES). Η έκθεση η οποία δημοσίευσε ο James P. Anderson και οι μελέτες σχετικά με το IDES ήταν η αρχή για το μεγάλο μέρος της έρευνας για τα IDS σε όλη τη δεκαετία του 1980 και του 1990. Κατά τη διάρκεια αυτής της περιόδου, η κυβέρνηση των ΗΠΑ χρηματοδότησε το μεγαλύτερο μέρος αυτής της έρευνας. Εργασίες όπως το

Discovery, το Haystack, το MIDAS, το NADIR αναπτύχθηκαν όλα για να ανιχνεύσουν εισβολές [4].

Μεταξύ άλλων το 1988, υπήρξαν άλλες σημαντικές πρόοδοι που σημειώθηκαν στο εργαστήριο Lawrence Livermore του Πανεπιστημίου Devis της Καλιφόρνια. Το 1988, το έργο Haystack στο Lawrence Livermore Labs κυκλοφόρησε μια άλλη έκδοση ανίχνευσης εισβολών για την Πολεμική Αεροπορία των ΗΠΑ. Το έργο αυτό παρήγαγε ένα IDS το οποίο ανέλυε τα δεδομένα ελέγχου, συγκρίνοντάς το με τα προκαθορισμένα πρότυπα. Σε μια τηλεφωνική συνέντευξη με τον συγγραφέα, ο Crosby Marks, πρώην μέλος της ομάδας Haystack Project και ο εργαζόμενος Haystack Labs, δήλωσε ότι «η αναζήτηση αυτού του μεγάλου όγκου δεδομένων για μια συγκεκριμένη κακή χρήση ήταν ισοδύναμη με την αναζήτηση μιας βελόνας μέσα σε άχυρα». [5]

Επίσης το Computer Watch, όπου αναπτύχθηκε στο εργαστήριο AT&TBell Labs,στο Murray Hill του New Jersey χρησιμοποιούσε και αυτό στατιστικές και κανόνες για την μείωση ελέγχου των δεδομένων και την ανίχνευση εισβολών [34]. Στη συνέχεια, το 1991, οι ερευνητές του ΠανεπιστημίουDavis της Καλιφόρνια, δημιούργησαν ένα πρωτότυπο πρότυπο κατανεμημένου συστήματος ανίχνευσης εισβολών (DIDS), το οποία ήταν επίσης κι αυτό ένα έμπειρο σύστημα. Την ίδια χρονιά, στο εργαστήριο τουLos Alamos National Laboratory των Η.Π.Α. αναπτύχθηκε ξανά ένα πρωτότυπο σύστημα ανίχνευσης εισβολών, το επονομαζόμενο ως Network Anomaly Detection and Intrusion Reporter (NADIR) [7]. Αυτό ήταν βασισμένο σε μεγάλο βαθμό στο έργο των Dennnig και Lunt [9].

Από το 1995 κι έπειτα ωστόσο, άρχισαν να εμφανίζονται οι πρώτες εμπορικές εκδόσεις των Συστημάτων Ανίχνευσης Εισβολών, τα οποία χρησιμοποιήθηκαν κυρίως από τις στρατιωτικές υπηρεσίες πληροφοριών. Το Lawrence Berkeley National Laboratory της Καλιφόρνια, το 1998, ανακοίνωσε επίσημα το λογισμικό Bro. Ήταν ένα προγραμματισμένο λογισμικό το οποίο ακολουθούσε μία γλώσσα κανόνων με σκοπό την συλλογή των πακέτων από την βιβλιοθήκη δεδομένων, Libpcap [2].

Αξίζει να σημειωθεί ότι από το 2000 κι έπειτα, στη γενιά των «millenials», υποστηρίζεται η τεράστια σημασία των Συστημάτων Ανίχνευσης αλλά και Πρόληψης-Παρεμπόδισης Εισβολών σε υπολογιστικά συστήματα αφού η ολοένα αυξανόμενη πληροφορία συνεπάγεται και την αυξημένη ευθύνη προστασίας αυτής προκειμένου να διασφαλιστεί η ακεραιότητα των διαχειριζόμενων δεδομένων ενός ατόμου, μιας εταιρείας ή ενός οργανισμού. Έκτοτε, είναι αρκετές οι εταιρείες υπηρεσιών πληροφορικής και τηλεπικοινωνιών που ιδρύθηκαν και δραστηριοποιούνται, με έργα στον δημόσιο και ιδιωτικό τομέα, προσφέροντας ενοποιημένες λύσεις ασφάλειας πληροφοριακών συστημάτων με μηχανισμούς ασφαλείας κάθε επιπέδου (π.χ. η εταιρία Netbull).

.

2 ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Όπως προαναφέρθηκε και στο πρώτο κεφάλαιο, καθώς τα υπολογιστικά/πληροφοριακά συστήματα είναι αρκετά ευάλωτα στις μέρες μας ενώ παράλληλα οι κακόβουλες εισβολές έχουν αυξηθεί τόσο σε αριθμό όσο και σε ποσοστό επικινδυνότητας, η εγκατάσταση και εφαρμογή ενός ολοκληρωμένου συστήματος αναγνώρισης επιθέσεων είναι απαραίτητο στις σύγχρονες επιχειρηματικές δραστηριότητες. Τέτοια συστήματα δίνουν τη δυνατότητα στους χρήστες τους να διαφυλάξουν τα συστήματά τους ένα άρτια στημένο σύστημα ανίχνευσης εισβολών επιτρέπει σε οργανισμούς/εταιρείες να προστατέψουν τα συστήματά τους τα προσωπικά τους στοιχεία από τυχόν κινδύνους.

2.1 ΥΠΗΡΕΣΙΕΣ ΑΣΦΑΛΕΙΑΣ

Η ασφάλεια των πληροφοριών είναι μια συνεχής και επαναλαμβανόμενη διαδικασία που στηρίζεται στη συνεχή, αδιάκοπη διαχείριση των σχετικών κινδύνων. Η αποτελεσματικότητά της είναι αποτέλεσμα του τρόπου υλοποίησης των τεχνικών και διαχειριστικών δικλείδων ασφαλείας και της συνεχούς διαδικασίας ελέγχου, παρακολούθησης και επιθεώρησης τους. Η διασφάλιση της αξιοπιστίας των πληροφοριών αφορά στη διαχείριση των κινδύνων που σχετίζονται με τη χρήση, την επεξεργασία, την αποθήκευση και διαβίβαση των πληροφοριών όπως και των συστημάτων που χρησιμοποιούνται για τους σκοπούς αυτούς. Βασικός στόχος λοιπόν της ασφάλειας των πληροφοριών, είναι και παραμένει η διαφύλαξη της, εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας όλων των συστατικών της μερών όπως αναφέραμε παραπάνω.

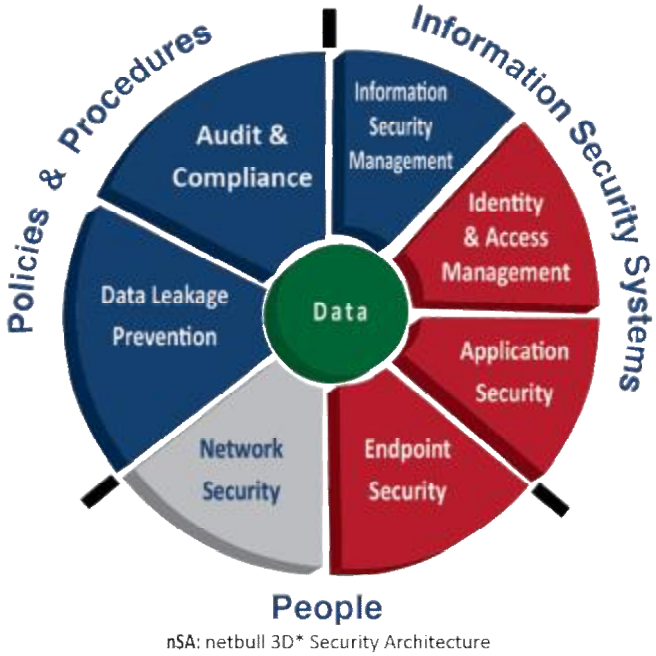
Άλλες συνιστώσες που αφορούν και εμπεριέχονται στις υπηρεσίες Ασφάλειας είναι εξίσου και οι ακόλουθες:

1) ο Έλεγχος (control),

2) η Καταγραφή (audit),

3) η Σταθερότητα (consistency).

Αν και όλες οι παραπάνω μορφές Ασφάλειας είναι εξίσου απαραίτητες και σημαντικές διαφορετικοί οργανισμοί /εταιρείες δίνουν διαφορετική προτεραιότητα διότι αντιμετωπίζουν διαφορετικού είδους απειλές ανά περιβάλλον όπου βρίσκονται ή εκπροσωπούν [32]. Για παράδειγμα, σε ένα ακαδημαϊκό περιβάλλον όπως είναι το Πανεπιστήμιο, πιο σημαντικά θεωρούνται η διαθεσιμότητα και η ακεραιότητα της πληροφορίας, ενώ σε ένα περιβάλλον που σχετίζεται με θέματα Εθνικής Ασφάλειας ή με θέματα Υγείας και Ιατρικού απορρήτου, η εμπιστευτικότητα είναι πολύ σημαντικότερη από τη διαθεσιμότητα.



Εικόνα 2-1 Παράδειγμα Υπηρεσιών Συστημάτων Ασφάλειας Πληροφοριών μιας εταιρείας (Πολιτικές & Διαδικασίες) [39].

2.2 ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ

Ο κίνδυνος που αφορά την ασφάλεια πληροφοριών, είτε χρησιμοποιούνται ποσοτικά, είτε ποιοτικά κριτήρια, ως έννοια της επικινδυνότητας (risk) δανεισμένη από τον κλάδο της χρηματοοικονομικής διοίκησης μπορεί να προσδιοριστεί και να οριστεί μαθηματικά από το γινόμενο της πιθανότητας εκδήλωσης μιας απειλής επί την επίδραση της απειλής αυτής.

Κίνδυνος = (Πιθανότητα της Εκδήλωσης Απειλής) X (Επίδραση της Απειλής)

Ως Απειλή (Threat) ασφάλειας πληροφοριών ορίζουμε την πιθανότητα εκμετάλλευσης μιας αδυναμίας ασφάλειας των υπολογιστικών συστημάτων ή των διαδικασιών διαχείρισης της ασφάλειας πληροφοριών από μια συγκεκριμένη εστία απειλών, ικανή να υποκινήσει την εκδήλωση μιας αδυναμίας ασφάλειας και να εκμεταλλευθεί το αποτέλεσμα της. Σύμφωνα με τον παραπάνω ορισμό, η απειλή ασφάλειας είναι αποτέλεσμα της εκμετάλλευσης των εκάστοτε κενών-αδυναμιών ασφάλειας. Πιο απλά, μπορούμε να πούμε ότι είναι ένα σύνολο γεγονότων, η εκδήλωση των οποίων μειώνει τη δυνατότητα ενός οργανισμού να πετύχει τους στόχους του, όπως είναι η μη εξουσιοδοτημένη πρόσβαση ή η μη εξουσιοδοτημένη τροποποίηση των δεδομένων που διαχειρίζεται.

Ως Αδυναμία Ασφάλειας Πληροφοριών (Information Security Vulnerability) ορίζεται η οποιαδήποτε ανεπάρκεια, ευπάθεια ή αδύναμο σημείο των υφιστάμενων διαδικασιών διαχείρισης ασφάλειας, των υφιστάμενων διαδικασιών ασφάλειας που ακολουθεί ένα πληροφοριακό σύστημα, του σχεδιασμού και των εσωτερικών

δικλείδων ασφαλείας του πληροφοριακού συστήματος, της αποτελεσματικότητας των υφισταμένων τεχνικών και οργανωτικών δικλείδων ασφαλείας και της εναρμόνισης με νομικές και θεσμικές απαιτήσεις.

Η πλέον διαδεδομένη μεθοδολογία που χρησιμοποιείται για τη διασφάλιση ενός συστήματος είναι αυτή όπου ακολουθείται αξιολόγηση, προσδιορισμός και διαχείριση των κινδύνων και των απαιτήσεων. Το αποτέλεσμα της παραπάνω διεργασίας αποσκοπεί στη χάραξη στρατηγικής και θέτει τις απαιτήσεις και τις προτεραιότητες που αφορούν την προστασία, εντός αποδεκτών όρων.

2.3 ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ

Πρωτίστως, βασικό παράγοντα αποδοτικής επίτευξης ασφάλειας είναι η δρομολόγηση μιας πολιτικής ικανής να προσδιορίσει επαρκώς τον τρόπο που θα εφαρμοστεί ένα σύστημα ανίχνευσης εισβολής. Η προαναφερθείσα πολιτική είναι πλέον διεθνών προδιαγραφών. Προς διάθεση υφίσταται πλήθος προτύπων, διεθνούς βεληνεκούς, όπως για παράδειγμα το πρότυπο ISO 27002, το οποίο αποσαφηνίζει με κάθε λεπτομέρεια τα πεδία που πρέπει να προστατευτούν ώστε να πιστοποιηθεί η ασφάλεια του περιβάλλοντος εφαρμογής. Στο σημείο αυτό είναι κρίσιμο να αναφερθούν τα πιο κρίσιμα πεδία που εφαρμόζονται τα εν λόγω πρότυπα [34]:

i. Η αξιολόγηση της ασφαλούς λειτουργίας των πεδίων που συντελούν το host, δηλαδή όλα τα πεδία δικτύου αλλά και υπολογιστών. Αυτό είναι κρίσιμο να επιδιωχθεί προκειμένου να λειτουργήσει σα δεύτερο στάδιο προστασίας, στη περίπτωση που κάποια εισβολή «ξεφύγει» από το πρώτο στάδιο ελέγχου και καταφέρει τελικά να εισχωρήσει τελικά στο σύστημα.
ii. Η υλοποίηση του ολοκληρωμένου μοντέλου Ανίχνευσης Επιθέσεων είναι δυνατόν να ενημερώσει με ακρίβεια και σε σύντομο χρονικό διάστημα τους υπεύθυνους για ενδεχόμενη εμφάνιση κακόβουλης δραστηριότητας στο σύστημα. Παράλληλα, το σύστημα αυτό είναι σε θέση να αντιμετωπίζει ενδεχόμενες εισβολές ακολουθώντας ένα προκαθορισμένο πρωτόκολλο. Πιο αναλυτικά, τα επικείμενα πρότυπα δύνανται να αναλύσουν μια πιθανή εισβολή και σε πραγματικό χρόνο, που συνεπάγεται το προτέρημα που έχουν να εκτελούν εσωτερικές επιβλέψεις και προλήψεις στο δίκτυο που εγκαθίστανται.
iii. Τα ορθώς καταρτισμένα πρότυπα εξουσιοδότησης καθώς και έλεγχου πρόσβασης που παρέχουν αξιοπιστία ενώ είναι και σε θέση να αξιολογήσουν κάθε τύπο που επιδιώκει την είσοδό του στο περιβάλλον εφαρμογής αυτών καθώς και στις υπηρεσίες που αυτά προσφέρουν.
iv. Τα ολοκληρωμένα εφεδρικά συστήματα που δύνανται να αποθηκευτούν και παράλληλα να αποκαθιστούν τις επιπτώσεις που ενδέχεται να προκαλέσει μια επιτυχημένη κακόβουλη δραστηριότητα σε ένα σύστημα.
v. Η διαρκώς αναπτυσσόμενη και ταυτόχρονα αξιόπιστη μέθοδος κρυπτογράφησης, η οποία στοχεύει στην επίτευξη ασφαλέστερων επικοινωνιών μεταξύ των κόμβων του συστήματος, είτε των εσωτερικών είτε των εξωτερικών [34].

2.4 ΑΡΧΙΤΕΚΤΟΝΙΚΕΣΑΣΦΑΛΕΙΑΣ

Η υλοποίηση μιας ορθώς δομημένης ασφάλειας δικτύου απαιτεί, πέραν τη διενέργεια των ανωτέρω διεργασιών, την εφαρμογή επιπρόσθετων τεχνικών που είναι ικανές να αναβαθμίσουν τα επίπεδα ασφάλειας, δεδομένων των ορθολογικών χειρισμών και της σωστής τους εγκατάστασης. Έτσι, κρίνεται αναγκαία η εφαρμογή κρυπτογραφικών τεχνικών, ώστε να επιτευχθεί ασφαλέστερη διαβίβαση πληροφοριών ανάμεσα στα συστήματα καθώς επίσης και να καταστήσει αδύνατη τη δυνατότητα υποκλοπής. Οι εν λόγω τεχνικές είναι εφαρμόσιμες σε διάφορες φάσεις ανίχνευσης κακόβουλης ενέργειας, όπως για παράδειγμα η φάση μεταφοράς.

Ακολούθως τα αντίγραφα ασφαλείας, είναι ικανά να αποκαταστήσουν ένα περιβάλλον που έχει υποστεί εισβολή (και τις επιπτώσεις αυτής) σε σύντομο χρονικό διάστημα και με όσο το δυνατόν μικρότερες απώλειες για το σύστημα. Επίσης, το σύστημα προβλέπει την ανάκτηση των υπαρχουσών πληροφοριών, που αποκτήθηκαν σε προγενέστερη φάση . Άλλη μια αρχιτεκτονική που προβλέπεται προς ανίχνευση επιθέσεων είναι η εφαρμογή του λογισμικού απομάκρυνσης, το οποίο δύναται να αξιολογήσει σε πραγματικό χρόνο κάθε τύπο πληροφορίας που εισέρχεται στο υπό εξέταση περιβάλλον.

Η προσαρμογή του τοίχους προστασίας είτε με τη μορφή λογισμικού είτε με τη μορφή συσκευής, επιμελείται την αποδοχή ή τον αποκλεισμό του συνόλου δεδομένων που διαβιβάζονται από το ένα δίκτυο στο άλλο. Η τεχνολογία αυτή, ουσιαστικά αποσκοπεί στη διαφύλαξη του υπό εξέταση συστήματος από ενδεχόμενες απειλές. Έτσι, αποκλείονται οι συνδέσεις που δεν αφορούν το διαχειριστή του προγράμματος. Οι πρόσφατες εξελίξεις ώθησαν στη δημιουργία ενός τοίχους προστασίας τέταρτης γενιάς, το οποίο εμπεριέχει και λειτουργικό σύστημα που υποδηλώνει την επίτευξη μεγαλύτερων ποσοστών ακρίβειας και αποδοτικότητας. Είναι σημαντικό, ωστόσο, να γίνει κατανοητό ότι καμία από τις ανωτέρω τεχνολογίες δεν αποφέρει επιθυμητά αποτελέσματα, δηλαδή όσο δυνατόν καλύτερη διαφύλαξη ασφάλειας, αν δε χρησιμοποιηθεί συνδυαστικά[18].

Μπορεί να διαπιστωθεί από προηγούμενες υποενότητες ότι ορθολογική ρύθμιση των παραμέτρων του τοίχου συνεπάγεται την επίτευξη πρώτου επιπέδου άμυνας για το υπό εξέταση δίκτυο. Ωστόσο, ενδέχεται μια κακόβουλη ενέργεια να καταφέρει να προσπελάσει το πρώτο αυτό επίπεδο και για αυτό κρίνεται αναγκαία η εφαρμογή επιπρόσθετων μέτρων ασφαλείας, όπως για παράδειγμα οι Λίστες Ελέγχου Πρόσβασης (Access Control Lists). Έτσι, με την εφαρμογή επιπρόσθετης φάσης άμυνας, θωρακίζεται η διαφύλαξη του δικτύου με αποτελεσματικό και βέλτιστο τρόπο. Η μέθοδος που υλοποιεί πολλαπλά επίπεδα ασφάλειας προκειμένου για αποτελεσματικότερη δράση, ορίζεται ως Άμυνα εις Βάθος (Defense of Depth). Αποδεκτή και ορθολογική λύση κατά τη διενέργεια ελέγχου δεύτερης φάσης θεωρείται η υλοποίηση ενός συστήματος που είναι ικανό να ανιχνεύσει πιθανά κακόβουλα στοιχεία που εισήλθαν στο εσωτερικό του δικτύου. Έτσι καθίσταται αναγκαία, σημαντική και απαραίτητη η δημιουργία ενός Συστήματος Ανίχνευσης και Διαχείρισης- Πρόληψης Εισβολών.

Τα Συστήματα Πρόληψης-Παρεμπόδισης Εισβολών (IPS), τα οποία χαρακτηρίζονται και ως αντιδραστικά συστήματα, είναι το επόμενο επίπεδο,

παραπάνω άμυνας από τα Συστήματα Ανίχνευσης εισβολών αφού τα συστήματα αυτά δεν εμμένουν στην ανίχνευση της επίθεσης αλλά προχωρούν και στην αντιμετώπισή της χρησιμοποιώντας ένα μεγάλο αριθμό κανόνων και πρακτικών που ανανεώνονται σε διαρκή ρυθμό. Μάλιστα η αντιμετώπιση αυτή είναι καλό να γίνει χωρίς την ανθρώπινη παρέμβαση για να ελαχιστοποιηθεί έτσι, ο χρόνος αντίδρασης στην επίθεση. Συχνά ένα IPS αποτελεί μέρος ενός IDS και δεν αποτελεί ξεχωριστή οντότητα από μόνο του. Αυτό συμβαίνει επειδή το IDS είναι αυτό που ανιχνεύει μια επίθεση, οπότε αυτό πρέπει να πάρει και την πρωτοβουλία για να την σταματήσει. Στην ουσία ένα IPS, συνδυάζει τα χαρακτηριστικά ενός Firewall και ενός IDS, καθώς μπορεί και μπλοκάρει την ανεπιθύμητη κίνηση έχοντας την βοήθεια ανίχνευσης των κακόβουλων πακέτων που προσφέρει ένα IDS. Η διαφορά του από το firewall είναι ότι έχει καλύτερη και πιο ολοκληρωμένη πληροφορία. Αυτό οφείλεται στην ύπαρξη του IDS, το οποίο και παρακολουθεί όλη την δικτυακή κίνηση που συμβαίνει [10,33].

3 ΕΠΙΘΕΣΕΙΣ / ΕΙΣΒΟΛΕΣ, ΧΡΗΣΗ ΣΥΣΤΗΜΑΤΩΝ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ

Η διαρκής αναβάθμιση των τεχνολογιών στο κλάδο της πληροφορικής επιφέρει αρνητικές συνέπειες στην δημιουργία και εξέλιξη καινοτόμων και άγνωστων μορφών δικτυακών εισβολών. Έτσι, η υλοποίηση των Συστημάτων Ανίχνευσης Εισβολών αποσκοπεί στην εύρεση όλων των ενδείξεων που υποδηλώνουν την εμφάνιση κακόβουλων δραστηριοτήτων. Στις προαναφερθείσες δραστηριότητες συγκαταλέγονται οι διαδικασίες παρεμπόδισης της εμπιστευτικότητας, της ακεραιότητας καθώς και της διαθεσιμότητας των πόρων που προστατεύονται [18]. Στο σημείο αυτό είναι καλό να προσδιοριστούν και ορισμένες από τις σημαντικότερες έννοιες και ορολογίες που αφορούν τόσο τους ίδιους τους εισβολείς όσο και τις επιθέσεις αυτών στα υπολογιστικά/ πληροφοριακά συστήματα.

3.1 ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ ΤΩΝ ΟΡΩΝ “HACKING” , “CRACKING” ΚΑΙ ΔΙΑΦΟΡΟΠΟΙΗΣΗ ΤΟΥΣ

Ο όρος “hacking” πηγάζει από μικρά εργαλεία κοπής (προγράμματα) που υλοποιούνταν κατά κύριο λόγιο τα πρώτα χρόνια δημιουργίας των υπολογιστών, όπου και ο προγραμματισμός ήταν σε αρκετά πρώιμο στάδιο και για λίγους, εμπειρογνώμονες του κλάδου. Οι υπεύθυνοι των προγραμμάτων αυτών, οι λεγόμενοι “hackers”, ανέπτυξαν τις εντολές “hacking” προκειμένου να διευκολύνουν την επίπονη ρουτίνα που έπρεπε να φέρουν εις πέρας, αναφορικά με τις διαδικασίες προγραμματισμού. Συνεπώς, στη τρέχουσα περίοδο ο προαναφερθέν όρος αναφέρεται σε αξιόλογους και ικανότατους φανατικούς του κλάδου της πληροφορικής που επιτίθενται και προκαλούν επιπτώσεις σε συστήματα.

Οι πραγματικοί hackers δεν χαίρουν του χαρακτηρισμού τους από τους υπολοίπους και επιδιώκουν την διαφοροποίησή τους από τους κακόβουλους hackers, ή, όπως αλλιώς ονομάζονται, crackers οι οποίοι εστιάζουν στη πρόκληση καταστροφών στο σύστημα που εισέρχονται. Με τον όρο hacker χαρακτηρίζεται το άτομο που κατέχει πολλές τεχνικές γνώσεις υπολογιστών καθώς και προγραμματισμού και συνεπώς είναι σε θέση να αναγνωρίσει με ευκολία τις αδυναμίες των εκάστοτε συστημάτων. Παράλληλα, ο ίδιος είναι σε θέσει να συνεργάζεται με συναδέλφους του και να παρέχει αξιόπιστες και αποτελεσματικές λύσεις σε τυχόν προβλήματα και εφαρμογές, χωρίς να προκαλεί βλάβες. Σε όλες τις περιπτώσεις (εκτός από τους Script Kiddies) οι hackers είναι συνήθως άτομα με αυξημένο δείκτη νοημοσύνης.

Οπτική Απεικόνιση ενός Hacker [40].

3.1.1 ΚΑΤΗΓΟΡΙΕΣ HACKERS:

- **White-hat hackers:**

Άτομα που τους αρέσει να "σπάνε" την ασφάλεια συστημάτων για μη κακόβουλους σκοπούς. Τους αρέσει η γνώση, το να κατανοούν πώς λειτουργεί κάποιο πρόγραμμα ή μηχανισμός.

- **Crackers ή Blackhat hackers:**

Οι crackers (criminal hackers) είναι εκείνοι που αποσκοπούν στη πρόκληση σοβαρών ζημιών σε ένα σύστημα υπολογιστή και για το λόγο αυτό επιδιώκουν να επιτεθούν σε συστήματα που δεν έχουν εξουσιοδότηση. Οι τύποι αυτοί παραβιάζουν τα δεδομένα ασφαλείας κάθε συστήματος, αλλοιώνουν ή και καταστρέφουν δικτυακούς τόπους και αναπτύσσουν ιούς στα περιβάλλοντα εισβολής τους, υποδεικνύοντας σε κάθε περίπτωση τη ταυτότητά τους.

- **Script Kiddies:**

Είναι άτομα χωρίς πολλές γνώσεις, που χρησιμοποιούν έτοιμα προγράμματα για να κάνουν επιθέσεις ή και απλά φιγούρα στους φίλους τους. Είναι άτομα που, καλά-καλά, δε χαρακτηρίζονται ως hackers.

- **Gray-hat hackers ή Hacktivists ή νέο-hackers:**

Είναι άτομα που χρησιμοποιούν τις γνώσεις τους με σκοπό να πουν ή να προωθήσουν μια κοινωνική, ιδεολογική, θρησκευτική ή πολιτική γνώμη. Στις περισσότερες περιπτώσεις καταστρέφουν την κεντρική σελίδα από γνωστά sites ή τα αλλάζουν με σκοπό να γελοιοποιήσουν τον ιδιοκτήτη. Πιο σπάνια, χρησιμοποιούν τις γνώσεις τους και στο όνομα της διαδικτυακής τρομοκρατίας.

Συνοπτικά λοιπόν, ο cracker κάνει ό, τι και ο hacker, αλλά δημιουργεί ζημιά και παραβιάζει τους νόμους. Για παράδειγμα, αν κάποιος καταφέρει και βρει -"σπάσει" τους κωδικούς από μία ιστοσελίδα, αποκτώντας πρόσβαση στα πάντα, και μείνει εκεί χωρίς να συνεχίσει, τότε ονομάζεται hacker.Αν όμως προχωρήσει και

κάνει μεταβολές στο περιεχόμενο εν αγνοία του ιδιοκτήτη της ιστοσελίδας, ή και δημιουργήσει ζημιά, τότε αυτός είναι cracker! Τέλος, αξίζει να σημειώσουμε το αυτονόητο: όλοι οι crackers είναι και hackers, αλλά το αντίθετο δεν ισχύει. [21,38]

3.1.2.ΠΩΣ ΛΕΙΤΟΥΡΓΟΥΝ ΟΙ HACKERS ΓΙΑ ΝΑ ΑΠΟΣΠΑΣΟΥΝ ΠΛΗΡΟΦΟΡΙΕΣ, ΜΕ ΠΟΙΟΥΣ ΤΡΟΠΟΥΣ ΚΑΝΟΥΝ ΕΠΙΘΕΣΗ

Ανεξάρτητα με το σκοπό τους, hackers και crackers λειτουργούν με παρόμοιους τρόπους. Βέβαια, δεν υπάρχει κάποια σχολή hackers, ο καθένας μαθαίνει μόνος του και οι γνώσεις τους ποτέ δεν είναι οι ίδιες. Ανεξαρτήτως των γνώσεων των προαναφερθέντων σε τεχνικά και προγραμματιστικά ζητήματα, οι ίδιοι εμφανίζουν και αρκετές κοινωνικές δεξιότητες, ούτως ώστε να μην γίνονται εύκολα αντιληπτοί ως προς το τομέα ειδίκευσής τους.

Ο πιο δημοφιλής hacker, ο Mitnick (2001), στο βιβλίο του «The art of deception» επισημαίνει ότι ένα άτομο είναι ικανό να εκλάβει τις πληροφορίες που χρειάζεται με το να παρατηρεί και να εφαρμόζει μεθόδους κοινωνικής μηχανικής στα συστήματα ενδιαφέροντος. Προστασία από τους hackers δεν μας προσφέρει μόνο ένα καλό firewall, ούτε ένα ισχυρό antivirus. Ο πραγματικός hacker θα φτιάξει τα εργαλεία που θα κάνει επίθεση μόνος του και θα προσπαθήσει να τα κάνει μη ανιχνεύσιμα στα προγράμματα ασφάλειας[10].

3.2 ΠΑΡΑΓΟΝΤΕΣ ΠΙΘΑΝΟΤΗΤΑΣ ΜΙΑΣ ΕΠΙΘΕΣΗΣ

Η σπουδαιότητα ενός προγράμματος ασφάλειας έγκειται στη διαφύλαξη των συστημάτων εφαρμογής τους από ιούς και άλλα σχετιζόμενα κακόβουλα προγράμματα ή προγραμματιστές. Σπουδαία είναι και η συμβολή των χρηστών, οι οποίοι συχνά παραβλέπουν τις ειδοποιήσεις των συστημάτων ανίχνευσης επιθέσεων και έτσι αυξάνουν το ενδεχόμενο εμφάνισης μιας τέτοιας ενέργειας [22]. Οι παράγοντες που μπορούν να οδηγήσουν σε μια υφιστάμενη επίθεση αναλύονται ως εξής:

Οι αδύναμοι κωδικοί πρόσβασης, είτε ως επιλογή των χρηστών είτε ως επιλογή των διαχειριστών. Τα κλειδιά αυτά ασφαλείας εφαρμόζοντας ως κωδικοί εισόδου σε δοθέν σύστημα ενώ αναγνωρίζεται μοναδικά από το άτομο που τα δημιούργησε. Ωστόσο, η αδυναμία αυτών έγκειται στο γεγονός ότι πολλές φορές η πληροφορία αυτή είναι αναμενόμενη και συνεπώς εύκολα μπορεί να αποκρυπτογραφηθεί (ημερομηνία γέννησης κλπ).

Η μη ορθή εγκατάσταση ή και ρύθμιση ενός δικτυακού συστήματος, ενδέχεται να επιτρέψει στον επιτιθέμενο να εισέρθει στο σύστημα ενδιαφέροντός του χωρίς, ορισμένες φορές, να γίνεται αντιληπτός. Οι επιπτώσεις, δε, των δραστηριοτήτων των εισβολέων σε ένα σύστημα ποικίλλουν ως προς τον αντίκτυπο που θα προκαλέσουν στο διαχειριστή ή/ και το χρήστη. Ειδικότερα, είτε θα είναι σχετικά μικρή η επίπτωση της δράσεις του επιτιθέμενου είτε θα αφορά παραβίαση προσωπικών δεδομένων και σχετικών απόρρητων δεδομένων και πληροφοριών [22]..

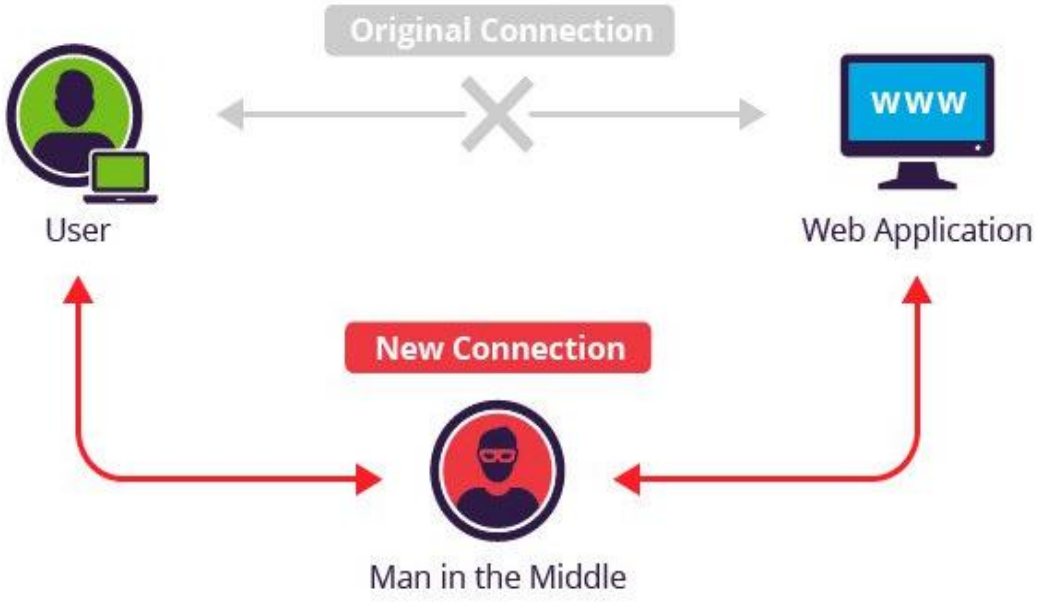
Επιπροσθέτως, η διατήρηση προγενέστερων εκδόσεων σε συνδυασμό με την εμφάνιση λαθών στο κώδικα ή ακόμη και κακός χειρισμός κατά την επεξεργασία των ιδιοτήτων των εν λόγω προτύπων, αναμένεται να αποτελέσουν ακρογωνιαίους λίθους για την υλοποίηση κακόβουλων δραστηριοτήτων [22].. Αξίζει ακόμη να σημειωθεί ότι η άγνοια χρήσης ενός συστήματος είτε λόγω κακών πολιτικών ασφαλείας είτε λόγω αδιαφορίας ως προς την εκμάθηση του τρόπου διαχείρισης αυτών, διευκολύνει τον εισβολέα, αφού καθιστά το σύστημα ενδιαφέροντος ευάλωτο [22].

3.3 ΤΥΠΟΙ ΕΠΙΘΕΣΕΩΝ

Υπάρχουν διάφορες μορφές βασικών εισβολών που δύνανται να συμβούν σε ποικίλα πληροφοριακά συστήματα δικτύων, προκαλώντας είτε αμελητέες είτε σοβαρές συνέπειες. Η εισβολή ιών σε ένα πληροφοριακό σύστημα είναι η πιο διαδεδομένη μορφή επίθεσης. Η εμφάνιση ενός ιού συνεπάγεται μεταβολή του λειτουργικού συστήματος ή ακόμη και του λογισμικού, σε βαθμό καταστροφικό και για τις δύο μορφές μεταβολών [20,33]. Επιπλέον, οι Δούρειοι Ίπποι επιτυγχάνουν να πραγματοποιούν κακόβουλες δραστηριότητες εντός του δικτύου, χωρίς όμως να είναι δυνατή η ανίχνευσή τους από τα λογισμικά ασφαλείας.

Η επιτυχία αποδοτικής επικοινωνίας μεταξύ ενός πελάτη και ενός εξυπηρετητή συνεπάγεται την ορθολογική αξιοποίηση ενός πρωτοκόλλου (TCP/IP), το οποίο έγκειται σε τρεις βασικές παραμέτρους [33]: Η πρώτη παράμετρος αφορά την λειτουργία του πελάτη, ο οποίος αποστέλλει ένα μήνυμα συγχρονισμού (SYN) στον server. Ο τελευταίος παρακρατεί τους πόρους που απαιτούνται για την εγκατάσταση και κατά συνέπεια ολοκλήρωση της εισόδου και αποστέλλει απαντητικό μήνυμα ανακοίνωσης της διεργασίας στον πελάτη (SYN/ACK). Η τελευταία παράμετρος αφορά την τελική επιβεβαίωση του πελάτη για έναρξη της διαδικασίας σύνδεσης (SCK). Αξιοσημείωτο είναι ότι οι hackers αναγνωρίζοντας το πρωτόκολλο αυτό, επιδιώκουν τη δέσμευση των πόρων αποστέλλοντας πληθώρα μηνυμάτων SYN από μη υπαρκτές διευθύνσεις ταυτότητας [20,33]. Έτσι, το τελικό response δεν έχει πραγματικό δέκτη και συνεπώς δεν επιτυγχάνεται η σύνδεση ενώ αν παράλληλα κάποιο φυσικό πρόσωπο επιχειρήσει την είσοδό του σε ένα δίκτυο, ο αντίστοιχος εξυπηρετητής θα αρνηθεί (επίθεση Dos).

Επιπλέον, ευρέως διαδεδομένη είναι και η τεχνική υποκλοπής δεδομένων, η ονομαζόμενη τεχνική του «μεσάζοντα» (Man in the Middle). Η μέθοδος αυτή προβλέπει τον εισβολέα να εισχωρεί στην επικοινωνία μεταξύ εξυπηρετητή και πελάτη και να εξαπατά τον δεύτερο, προσποιούμενος ότι είναι τμήμα του πληροφοριακού συστήματος ενός δικτύου. Έτσι, είναι δυνατόν να αποσπάσει απόρρητες προσωπικές πληροφορίες και να καταχραστεί τα δικαιώματα του «ανήξερου» πελάτη [20,33].



Εικόνα 3-1Μέθοδος του Μεσάζοντα (Man-In-The-Middle) [41].

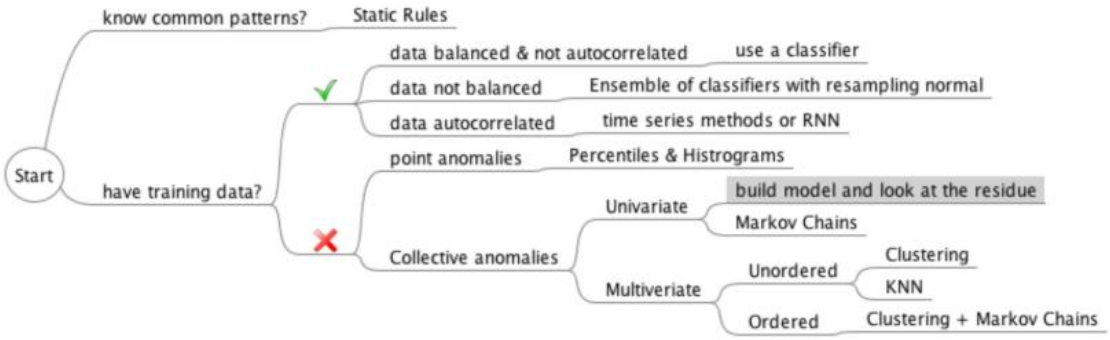
Αξίζει ακόμη να επισημανθεί ότι τα λογισμικά «σκουλήκια», είναι επίσης υπεύθυνα για κλοπές ή και καταστροφές στα πλαίσια των επιπέδων ενός δικτύου, αφού το μέγεθός τους είναι τεράστιο. Τα λογισμικά αυτά δύνανται να αναπτύσσονται και να εξαπλώνονται αυτοβούλως, γεγονός που συνεπάγεται την αύξηση του ποσοστού δραστηριοποίησης σε ένα δοθέν δίκτυο και τελικώς να μεταβάλλουν τη δυναμική του ολοκληρωτικά. Η απόσπαση, ακόμη, χρήσιμων πληροφοριών προσεγγίζοντας, ο επιτιθέμενος, ανήξερους χρήστες, αποτελεί τη μέθοδο «κοινωνικών μέσων». Η μέθοδος αυτή, ουσιαστικά, αφορά την αξιοποίηση τηλεφωνικών μέσων ή και μηνύματα ηλεκτρονικού ταχυδρομείου, προκειμένου για αμεσότερη προσέγγιση.

3.4 ΧΡΗΣΗ ΕΝΟΣ ΣΥΣΤΗΜΑΤΟΣ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ

Τα Συστήματα Ανίχνευσης Εισβολών εκπροσωπούν ένα εξελιγμένο σκεπτικό και μεθοδολογία στην οποία εμπλέκονται πάρα πολλές τεχνολογίες. Είναι λογισμικό ή συνδυασμός λογισμικού και υλικού το οποίο πραγματοποιεί την άμεση ανίχνευση περίεργης δικτυακής κίνησης καθώς και την γρήγορη αντίδραση σε έναν υπολογιστή μεμονωμένα στο δίκτυο. Αναπτύχθηκαν προκειμένου να παρέχουν έγκαιρη προειδοποίηση για τις εισβολές παρακολουθώντας τις εξελίξεις των γεγονότων, ώστε αφενός να ληφθούν τα κατάλληλα αμυντικά μέτρα κατά του επιτιθέμενου, αφετέρου να διεξαχθούν χρήσιμα συμπεράσματα [19].

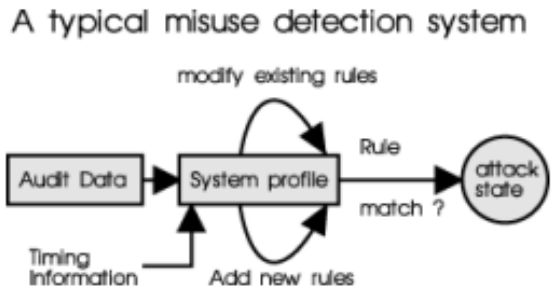
Η λειτουργία των Συστημάτων Ανίχνευσης Εισβολών είναι παθητική, που σημαίνει ότι ασχολείται μόνο με την ανίχνευση κακόβουλων δραστηριοτήτων και την παροχή λύσεων στους υπεύθυνους σχετικά με τους τρόπους διαχείρισης αυτών. Ακόμη, τέτοια μοντέλα αξιοποιούν στατιστικές τεχνικές προκειμένου για παρατήρηση κακόβουλων ενεργειών. Μέσω στατιστικής λοιπόν, εδραιώνεται ένα

προκαθορισμένο προφίλ ενεργειών, κατά τον οποίο το σύνολο των εισβολών είναι κακόβουλες ανωμαλίες αν παρεκκλίνουν από το προκαθορισμένο προφίλ που έχε οριοθετηθεί. για την ανίχνευση είτε τον τρόπο στατιστικής διαταραχών είτε την παρατήρηση κακής συμπεριφοράς.



Εικόνα 3-2 Σύστημα Στατιστικής Αναγνώρισης Διαταραχών [42].

Η ανίχνευση κακής συμπεριφοράς (misuse detection), από την άλλη, βασίζεται στο ότι υπάρχουν κάποια προκαθορισμένα σχέδια επίθεσης, που ονομάζονται πρότυπα ή υπογραφές (signatures). Αν το σύστημα ανιχνεύσει κάποιο από τα πρότυπα, τότε το ίδιο συμπεραίνει ότι δέχεται επίθεση. Ο τρόπος αυτός είναι ο συνηθέστερος στα περισσότερα IDS.



Εικόνα 3-3 Ανίχνευση Κακής Συμπεριφοράς [43].

Πιο αναλυτικά, προκειμένου να αναλυθούν οι στόχοι των προαναφερθέντων συστημάτων, παρατίθενται τα ακόλουθα:

- Η αναγνώριση πλήθους επιθέσεων, οι οποίες είναι δυνατόν να προέρχονται από εσωτερικούς και εξωτερικούς παράγοντες ενός πληροφοριακού συστήματος. Επιπλέον, τα τελευταίας τεχνολογίας συστήματα αναγνώρισης διαθέτουν τεχνικές που τους επιτρέπουν να αντιμετωπίζουν αποτελεσματικά άγνωστους τύπους κακόβουλων δραστηριοτήτων. Ωστόσο, το πλεονέκτημα αυτό απαιτεί την υλοποίηση ενός τύπου μάθησης ή συγκεκριμένες τροποποιήσεις από τους υπεύθυνους.

- Η αναγνώριση των κακόβουλων δραστηριοτήτων σε χρονικό διάστημα που συνεπάγεται την άμεση άμβλυνση του προβλήματος. Ουσιαστικά, δεν είναι αναγκαία η ταυτοποίηση μιας απειλής σε πραγματικό χρόνο αλλά η αναγνώριση ενός κινδύνου σε πλαίσιο που ο αποκλεισμός αυτού είναι εφικτός.
- Η παροχή έγκυρων πληροφοριών. Αναμφίβολα, η μετάδοση ενός ψευδώς θετικού μηνύματος, δηλαδή η λανθασμένη ενημέρωση για ύπαρξη εισβολής, συνεπάγεται ελάττωση της αξιοπιστίας ενός συστήματος αλλά και ταυτόχρονη αύξηση της απαιτούμενης διεργασίας προκειμένου για περαιτέρω ανάλυση αυτής της πληροφορίας. Όμοια, η εμφάνιση ενός ψευδώς αρνητικού μηνύματος, σημαίνει ότι το μοντέλο ανίχνευσης δεν είναι σε θέση να ενημερώσει για μια αληθινή επίθεση, ενώ η τελευταία υφίσταται και απαιτείται επιπλέον χρόνος προκειμένου για διαπίστωση της πραγματικής τρέχουσας κατάστασης στο σύστημα.
- Η υλοποίηση απλουστευμένης και εύληπτης τεχνικής επίλυσης προβλημάτων. Είναι απαραίτητο, οι λύσεις που δίνονται στο χρήστη να είναι εύληπτες και κατά συνέπεια αποτελέσματα δυαδικής μεταβλητής. Όμως, αυτό δεν είναι πραγματοποιήσιμο, δοθείσας της πολυπλοκότητας των ενεργειών εισβολής σε ένα σύστημα. Η αποτελεσματικότητα, παρόλα αυτά, από την επικοινωνία του υπεύθυνου ασφαλείας με το σύστημα πρέπει να διεξάγεται με τρόπο που δύναται να επιτευχθεί η βέλτιστη λύση.

4 ΕΠΙΣΤΗΜΗ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ ΚΑΙ ΑΛΓΟΡΙΘΜΩΝ

Τα Μοντέλα Ανίχνευσης Διαταραχών χρησιμοποιούν του αλγορίθμους της Τεχνητής Νοημοσύνης (Artificial Intelligent), με σκοπό την αναγνώριση τύπων εισβολών που δεν υπάγονται στις υπογραφές κακής συμπεριφοράς που αναφέρθηκε σε προηγούμενες ενότητες.. Πιο συγκεκριμένα, οι τεχνικές που χρησιμοποιούνται εντάσσονται στο πεδίο της Μηχανικής Μάθησης, η οποία ξεκίνησε να αναπτύσσεται ως επιστήμη από τη δεκαετία του 1950 ακόμα, και διερευνά τη μελέτη και την κατασκευή αλγορίθμων, οι οποίοι στοχεύουν στην πρόβλεψη άγνωστων καταστάσεων, χρησιμοποιώντας συγκεκριμένους μηχανισμούς. Στο παρόν κεφάλαιο πραγματοποιείται μία μικρή εισαγωγή στον τομέα της μηχανικής μάθησης, εξετάζοντας τις κατηγορίες στις οποίες διακρίνεται, και τους τύπους των προβλημάτων που επιλύει. Επιπλέον, περιγράφονται οι πιο διαδεδομένοι αλγόριθμοι μηχανικής μάθησης, με αναφορά στη χρήση των τεχνητών νευρωνικών δικτύων, στα οποία στηρίχθηκε η ανάπτυξη γνωστών Συστημάτων Ανίχνευσης Εισβολών. Τελικό βήμα είναι η καταγραφή των μέτρων αξιολόγησης που λαμβάνονται υπόψη κατά την εφαρμογή ενός μοντέλου επίλυσης.

4.1 ΜΗΧΑΝΙΚΗ ΜΑΘΗΣΗ

Η Μηχανική Μάθηση αποσκοπεί στην κατασκευή προγραμμάτων, που δύνανται να αναβαθμίζονται αυτόματα και αναλόγως την αποκτηθείσα εμπειρία από το χρονικό περιθώριο εκπαίδευσης. Η προαναφερθείσα αξιοποιεί δεδομένα από διάφορα επιστημονικά πεδία και με μεγαλύτερο ποσοστό από τη θεωρία της πληροφορίας, τη στατιστική και τη τεχνητή νοημοσύνη. Ήδη από τις αρχές του 1950, ο Samuel όρισε τη Μηχανική Μάθηση (Machine Learning) «*το πεδίο μελέτης που δίνει στις υπολογιστικές μηχανές την ικανότητα να μαθαίνουν χωρίς να έχουν προγραμματιστεί για αυτό*» [24].

Ο Mitchell, ομοίως, προσδιόρισε τον όρο τονίζοντας ότι «τα *32 προγράμματα υπολογιστών δύνανται να μάθουν την εμπειρία (E), όσον αφορά μερικές τάξεις έργων T (tasks) και μέτρων απόδοσης P (performance measures), αν οι αποδόσεις P τους στα έργα T βελτιώνονται με την εμπειρία E*». [18] Με βάση τα ανωτέρω, μπορεί να υποδειχθεί ότι το ποσοστό των ορθώς αναγνωρισμένων ενεργειών σε μια διαδικασία ανίχνευσης εισβολών αποτελεί μέτρο αξιολόγησης. Οι ενέργειες, μάλιστα, αφορούν σύνολα δεδομένων που είναι ήδη γνωστά πριν την έναρξη της διαδικασίας,

4.2 ΚΑΤΗΓΟΡΙΕΣ ΜΗΧΑΝΙΚΗΣ ΜΑΘΗΣΗΣ

Τέσσερις είναι οι βασικές κατηγορίες της Μηχανικής Μάθησης, όπως παρατίθενται και αναλύονται ακολούθως:

· **Επιβλεπόμενη ή επιτηρούμενη μάθηση:** Η διενέργεια αυτού του τύπου μάθησης αποσκοπεί στην παραγωγή ενός μοντέλου που είναι σε θέσει να προβλέψει ένα σύνολο παρατηρούμενων χαρακτηριστικών σε ένα σύνολο άγνωστων αντικειμένων. Η ικανότητα πρόβλεψης παρέχεται από τη χρήση ενός σώματος εκπαίδευσης, δηλαδή παραδειγμάτων, στα οποία τα προαναφερθέντα χαρακτηριστικά είναι γνωστά. Αναλυτικότερα, η επιτηρούμενη μάθηση χρησιμοποιεί ένα προκαθορισμένο σύνολο εκπαίδευσης προκειμένου να κατηγοριοποιήσει τα προς εξέταση αντικείμενα. Έτσι, είναι ικανό να λαμβάνει καλύτερες αποδόσεις και συνεπώς η μέθοδος ενδείκνυται για την βελτίωση και υλοποίηση ενός μοντέλου εισβολών.

· **Μη επιβλεπόμενη μάθηση**: Η μέθοδος αυτή κάνει χρήση των τεχνικών ομαδοποίησης και εκτίμησης παραμέτρων, προκειμένου για εκπαίδευση του υπό εξέταση αντικειμένου. Πιο ειδικά, η ομαδοποίηση (clustering) αφορά την διαδικασία δημιουργίας ομάδων από αντικείμενα με κοινά χαρακτηριστικά, με χρήση σχετικού αλγορίθμου ομαδοποίησης [7]. Όμοια, η εκτίμηση παραμέτρων (parameter estimation) αφορά την δημιουργία ενός στατιστικού μοντέλου, των οποίων οι παράμετροι πρέπει να υπολογιστούν βάσει ενός αλγορίθμου μάθησης. Ο αλγόριθμος αυτός προσεγγίζει τις τιμές των παραμέτρων χρησιμοποιώντας αντιπροσωπευτικά δεδομένα.

· **Ημι-επιβλεπόμενη μάθηση**: Η μέθοδος αυτή αξιοποιεί τόσο προ-ταξινομημένα όσο και μη ταξινομημένα παραδείγματα προκειμένου για ενδυνάμωση των εκβάσεων της διαδικασίας της μάθησης. Σκοπός, βέβαια, είναι η χρήση όσο το δυνατών λιγότερων προ-ταξινομημένων συνόλων δεδομένων.

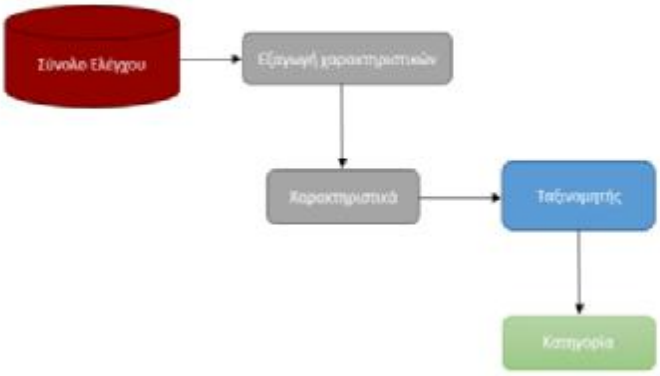
· **Ενισχυτική μάθηση:** Ο συγκεκριμένος τύπος μεταχειρίζεται παρατηρημένες ειδικές αναδράσεις, αποσκοπώντας στη μάθηση βελτιστοποιημένων πολιτικών. Ουσιαστικά, η ενισχυτική μάθηση εφαρμόζεται, ως επί το πλείστον σε προβλήματα Σχεδιασμού (Planning), όπως για παράδειγμα για τον έλεγχο κίνησης ενός ρομπότ και τη βελτιστοποίηση εργασιών σε εργοστασιακούς χώρους. Βελτιστοποιημένη πολιτική θεωρείται εκείνη η πολιτική που είναι ικανή να μεγιστοποιήσει την προβλεπόμενη συνολική ανταμοιβή και να οδηγήσει σε υψηλές αποδόσεις.

4.3 ΤΑΞΙΝΟΜΗΣΗ

Η ταξινόμηση των προβλημάτων έγκειται στο γεγονός ότι δύναται η εφαρμογή εναλλακτικών τεχνικών μηχανικής μάθησης, βάσει του τύπου πρόβλεψης. Δεδομένου όμως ότι η ενότητα αυτή αφορά την αξιολόγηση του προβλήματος της ταξινόμησης, θα αναλυθούν οι αλγόριθμοι της επιβλεπόμενης μηχανικής μάθησης. Αξίζει να τονιστεί ότι η ταξινόμηση ενδείκνυται σε περιπτώσεις μάθησης μιας συνάρτησης-στόχο, η οποία είναι σε θέση κατανέμει άγνωστα αντικείμενα σε προκαθορισμένες κατηγορίες. Συνεπώς, οι αλγόριθμοι μάθησης που εφαρμόζονται στη ταξινόμηση στοχεύουν στην ανάπτυξη ενός μοντέλου που θα προβλέψει τις κατηγορίες αυτών των άγνωστων αντικειμένων (test sets), βασιζόμενο σε ορισμένα γνωστά χαρακτηριστικά (features). Είσοδος (input) των αλγορίθμων μάθησης είναι τα χαρακτηριστικά των άγνωστων αντικειμένων αλλά και το σύνολο εκπαίδευσης αυτών. Οι προαναφερόμενοι αλγόριθμοι ονομάζονται ταξινομητές και οι κυριότεροι

εξ’ αυτών είναι τα Τεχνητά Νευρωνικά Δίκτυα (Artificial Neural Networks), τα Δέντρα Απόφασης (Decision Trees) και οι Μηχανές Διανυσμάτων Υποστήριξης (SVM). Στα παρακάτω σχήματα απεικονίζονται οι διαδικασίες εκπαίδευσης και πρόβλεψης του ταξινομητή.

Εικόνα 4-1Διαδικασία Εκπαίδευσης του ταξινομητή [44].



Εικόνα 4-2 Διαδικασία Πρόβλεψης του ταξινομητή [44].

4.4 ΤΕΧΝΗΤΑ ΝΕΥΡΩΝΙΚΑ ΔΙΚΤΥΑ

Ένα παρακλάδι της Τεχνητής Νοημοσύνης (AI) αποτελούν τα Τεχνητά Νευρωνικά Δίκτυα (ANN). Απαρτίζονται στην ουσία από ένα σύνολο απλών προσαρμοστικών και διασυνδεδεμένων μονάδες, το σύνολο των οποίων αποτελεί ένα πολύπλοκο υπολογιστικό μοντέλο. Το πεδίο εφαρμογής τους είναι αρκετά διευρυμένο, δεδομένου ότι αξιοποιούνται προκειμένου για εύρεση λύσεων σε προβλήματα ταξινόμησης στην ιατρική, φυσική, πληροφορική κλπ. Τα Τεχνητά Νευρωνικά Δίκτυα είναι ένα σχετικά καινοτόμο πεδίο που «γεννήθηκε» στις αρχές της δεκαετίας του 1980 και έκτοτε εξελίσσεται αδιάκοπα. Χαρακτηριστικό παράδειγμα αποτελεσματικής εφαρμογής του ανωτέρου πεδίου είναι η ανάπτυξη του εργαλείου Network Neural Toolbox, διαθέσιμο από το λογισμικό Matlab.

.

4.4.1 ΕΚΠΑΙΔΕΥΣΗ ΤΕΧΝΗΤΩΝ ΝΕΥΡΩΝΙΚΩΝ ΔΙΚΤΥΩΝ

Η εκπαίδευση των Τεχνητών Νευρωνικών Δικτύων συνεπάγεται το καθορισμό των τιμών, των πολώσεων, των συνοπτικών βαρών καθώς και του συνόλου των κρυφών επιπέδων (συμπεριλαμβανομένων και των επιπέδων εξόδου). Ο λόγος της απαίτησης όλων των ανωτέρω δεδομένων έγκειται στο γεγονός ότι προσδοκάται επίτευξη μεγάλου ποσοστού επιτυχίας κατά τη κατηγοριοποίηση των υπό εξέταση αντικειμένων σε ένα πρόβλημα.

Ως εκ τούτου, η εφαρμογή ενός αλγορίθμου εκπαίδευσης σε ένα Τεχνητό Νευρωνικό Δίκτυο, αφορά το προσδιορισμό ενός διανύσματος συνοπτικών βαρών *w*, το οποίο είναι ικανό να ελαχιστοποιήσει το ολικό τετραγωνικό σφάλμα, όπως ορίζεται στην εξίσωση (4-3) που παρατίθεται ακολούθως. Η μεταβλητή t_i ορίζει την έξοδο για το σύνολο εκπαίδευσης και η μεταβλητή y_i προσδιορίζει την πιο πρόσφατη έξοδο, όπως αυτή υπολογίστηκε από την εφαρμογή του αντίστοιχου αλγορίθμου.

$$E(w) = \frac{1}{2} \sum_{i=1}^{N} (t_i - y_i)^2 \qquad \textbf{(4-3)}$$

Αρκετές μελέτες έχουν διενεργηθεί προκειμένου για την ανάπτυξη αλγορίθμων μάθησης στα Τεχνητά Νευρωνικά Δίκτυα, όμως, δεν συστήνεται κάποιος συγκεκριμένος προς επίτευξη μεγαλύτερου ποσοστού ακρίβειας. Ειδική κατηγορία που αξίζει να σημειωθεί στο σημείο αυτό είναι οι κατηγορία αλγορίθμων βαθμωτής κατάβασης. Ειδικότερα, σε περίπτωση που η συνάρτηση ενεργοποίησης που χρησιμοποιείται σε αυτή τη μέθοδο είναι μη γραμμική, η τεχνική της βαθμωτής κατάβασης ενδέχεται να μην αποδώσει τα αναμενόμενα, αφού θα εγκλωβιστεί σε κάποιο τοπικό ελάχιστο όριο. Εκτός αυτού, οι αλγόριθμοι της βαθμωτής κατάβασης δεν είναι ικανοί να υπολογίσουν τα βάρη των κρυφών νευρώνων, στις περιπτώσεις όπου οι είσοδοι των δεδομένων εκπαίδευσης δεν περιλαμβάνουν τις τιμές των κρυφών νευρώνων.

Προς επίλυση των ανωτέρω αδυναμιών στη μέθοδο βαθμωτής κατάβασης, αναπτύχθηκε ο αλγόριθμος οπισθοδιάδοσης του σφάλματος. Μπορεί να διαπιστωθεί ότι ο αλγόριθμος αυτός αποτελεί θεμέλιο για την ανάπτυξη αναβαθμισμένων σύγχρονων αλγορίθμων στο πεδίο της Τεχνητής Νοημοσύνης και ειδικότερα στα Τεχνητά Νευρωνικά Δίκτυα.

4.4.2 ΤΕΧΝΗΤΑ ΝΕΥΡΩΝΙΚΑ ΔΙΚΤΥΑ ΚΑΙ ΑΝΙΧΝΕΥΣΗ ΕΙΣΒΟΛΩΝ

Οι κυριότερες αδυναμίες των διαρκών αναπτυσσόμενων Συστημάτων Ανίχνευσης Εισβολών είναι η ανικανότητα ταυτοποίησης των άγνωστων και κακόβουλων λογισμικών αλλά και η εμφάνιση υψηλών ποσοστών εσφαλμένων

ειδοποιήσεων. Βασική αιτία πρόκλησης των ανωτέρω είναι η δυναμικότητα της φύσης τόσο των νευρικών δικτύων όσο και των ίδιων των συστημάτων.

Οι ερευνητές έχουν επιδείξει ότι η αξιοποίηση των τεχνητών νευρωνικών δικτύων προκειμένου για ανίχνευση εισβολών, είναι μια αρκετά προσοδοφόρα λύση που δύναται να αντιμετωπίσει κάθε είδους αδυναμίας. Με αφορμή, δε, τις ιδιότητες πρόβλεψης και κατηγοριοποίησης των δεδομένων εισόδου που εμφανίζουν, οι ίδιοι επιδιώκουν όλο και περισσότερο τη μελέτη των αντίστοιχων ερευνητικών μοντέλων [28, 29, 30]. Μια ευρέως γνωστή κατηγορία τεχνητών νευρωνικών δικτύων, που άπτεται στα πλαίσια της ανίχνευσης εισβολών, είναι τα επονομαζόμενα τεχνικά νευρωνικά δίκτυα πολλών επιπέδων Perceptron.

Αρχικό πεδίο έρευνας αποτέλεσε η εφαρμογή των δικτύων Perceptron σε προβλήματα ανίχνευσης ενδεχόμενων διαταραχών, που είναι άγνωστες. Η περεταίρω εξέλιξη και μελέτη αυτών τους επέτρεψε να χρησιμοποιηθούν σε προβλήματα κακής συμπεριφορά και πιο συγκεκριμένα για τη κατηγοριοποίηση μιας εισβολής σε ένα τύπο επίθεσης που είναι ήδη γνωστός. Η πρόσφατη βιβλιογραφία επί του θέματος, παρουσιάζει το μη εποπτευόμενο μοντέλο εκπαίδευσης προκειμένου για εντόπιση των εισβολών. Αναλυτικότερα, οι ερευνητές υποδεικνύουν τη χρήση των αυτό-οργανούμενων τεχνητών δικτύων (Self Organizing Map) προκειμένου πέραν της ταυτοποίησης, να ερευνηθεί και η συμπεριφορά του ίδιου του χρήστη [31, 32].

4.5 ΜΕΤΡΑ ΑΞΙΟΛΟΓΗΣΗΣ

Ένας αλγόριθμος ταξινόμησης στοχεύει στην ορθή κατηγοριοποίηση του συνόλου των δεδομένων εισόδου στο σύστημα. Βάσει αυτού, είναι απαραίτητο στην υποενότητα αυτή να εξεταστούν οι μετρικές, οι οποίες δύνανται να αξιολογήσουν την εξαγόμενη πληροφορία, όπως προκύπτει από τον εφαρμοζόμενο αλγόριθμο ταξινόμησης. Πιο ειδικά, παρατίθενται ακολούθως το σύνολο των εξισώσεων αλλά και οι πιθανές λύσεις που προκύπτουν από την επίλυση ενός προβλήματος κατηγοριοποίησης δυαδικής ταξινόμησης.

· **TP (True Positive):** Η λύση TP προσδιορίζει το σύνολο των περιπτώσεων ενός θετικού παραδείγματος όπου η κατηγοριοποίηση επιτεύχθηκε σωστά. Ειδικεύοντας στο πρόβλημα ανίχνευσης εισβολών, ο τύπος αυτής της λύσης αφορά το σύνολο των περιπτώσεων ορθής κατηγοριοποίησης μιας επιθετικής δραστηριότητας. Το θετικό παράδειγμα, στη προκειμένη, είναι οι ενέργειες μη φυσιολογικής συμπεριφοράς.

· **TN (True Negative):** Η λύση TN προσδιορίζει το σύνολο των περιπτώσεων ενός αρνητικού παραδείγματος όπου η κατηγοριοποίηση επιτεύχθηκε σωστά. Ομοίως, ειδικεύοντας στο πρόβλημα ανίχνευσης εισβολών, ο τύπος αυτής της λύσης αφορά το σύνολο των περιπτώσεων ορθής κατηγοριοποίησης μιας μη επιθετικής δραστηριότητας. Το αρνητικό παράδειγμα, στη προκειμένη, είναι οι ενέργειες φυσιολογικής συμπεριφοράς.

· **FP (False Positive):** Η λύση FP προσδιορίζει το σύνολο των περιπτώσεων ενός αρνητικού παραδείγματος όπου η κατηγοριοποίηση δεν επιτεύχθηκε σωστά. Πιο συγκεκριμένα, στο πρόβλημα ανίχνευσης εισβολών, ο τύπος της λύσης FP σχετίζεται με το σύνολο των περιπτώσεων εσφαλμένης κατηγοριοποίησης μιας επιθετικής δραστηριότητας. Το αρνητικό παράδειγμα, στη προκειμένη, είναι οι ενέργειες φυσιολογικής συμπεριφοράς.

· **FN (False Negative):** Η λύση FN προσδιορίζει το σύνολο των περιπτώσεων ενός θετικού παραδείγματος όπου η κατηγοριοποίηση δεν επιτεύχθηκε σωστά. Πιο συγκεκριμένα, στο πρόβλημα ανίχνευσης εισβολών, ο τύπος της λύσης FN σχετίζεται με το σύνολο των περιπτώσεων εσφαλμένης κατηγοριοποίησης μιας μη επιθετικής δραστηριότητας. Το θετικό παράδειγμα, στη περίπτωση αυτή, είναι οι ενέργειες φυσιολογικής συμπεριφοράς.

4.5.1 ΑΚΡΙΒΕΙΑ

Ο υπολογισμός της ακρίβειας, δηλαδή ο υπολογισμός των ορθών προβλέψεων αναλογικά με το σύνολο των προβλέψεων, δίνεται από τον τύπο που παρουσιάζεται ακολούθως: Ως ακρίβεια (accuracy) ορίζεται η αναλογία των συνολικών προβλέψεων που ήταν ορθές:

$$\text{Ακρίβεια} = \frac{\text{Σύνολο ορθών προβλέψεων}}{\text{Σύνολο προβλέψεων}} \tag{4-4}$$

Στη περίπτωση ενός προβλήματος ταξινόμησης με δυαδικές λύσεις (όπως παρουσιάστηκε στη προηγούμενη υποενότητα), η ακρίβεια (accuracy) υπολογίζεται από τον τύπο:

$$\text{Ακρίβεια} = \frac{TP+TN}{TP+TN+FP+FN} \tag{4-5}$$

4.5.2 ΟΡΘΟΤΗΤΑ

Η ορθότητα (precision) των αποτελεσμάτων ή αλλιώς ο υπολογισμός της δεσμευμένης πιθανότητας, στη περίπτωση ταύτισης της προβλέψιμης κλάσης με το στιγμιότυπο της πραγματικής κλάσης , δίνεται από την εξίσωση:

$$\text{Ορθότητα} = \frac{\text{Σύνολο ορθών προβλέψεων κλάσης } c}{\text{Σύνολο προβλέψεων κλάσης } c} \quad (4\text{-}6)$$

Στη περίπτωση επίλυσης προβλημάτων με δυαδικές λύσεις, η ορθότητα υπολογίζεται από τις σχέσεις που παρατίθενται ως εξής:

$$\text{Ορθότητα}_P = \frac{TP}{TP+FP}$$

$$\text{Ορθότητα}_N = \frac{TN}{TN+FN} \quad (4\text{-}7)$$

4.5.3 ΑΝΑΚΛΗΣΗ

Η ανάκληση (recall) αντιπροσωπεύει τη δεσμευμένη πιθανότητα, σε περίπτωση που αξιολογηθεί ότι ένα στιγμιότυπο ανήκει σε μια συγκεκριμένη κατηγορία, η οποία έχει ορθώς ταυτοποιηθεί από τον αλγόριθμο ταξινόμησης που χρησιμοποιήθηκε. Ο τύπος της ανάκλησης είναι ο ακόλουθος:

$$\text{Ανάκληση} = \frac{\text{Σύνολο προβλέψεων κλάσης } c}{\text{Δεδομένα κλάσης } c} \quad (4\text{-}8)$$

Ειδικότερα, σε προβλήματα ταξινόμησης με δυαδικές λύσεις, ο αντίστοιχοι τύποι υπολογισμού της ανάκλησης είναι:

$$\text{Ανάκληση}_P = \frac{TP}{TP+FN}$$

$$\text{Ανάκληση}_N = \frac{TN}{TN+FP} \quad (4\text{-}9)$$

4.5.4 ΜΕΤΡΟ F

Προκειμένου για συνδυαστικό υπολογισμό των μετρικών ορθότητας και ανάκλησης προτείνεται η εφαρμογή ενός επιπρόσθετου μέτρου, της συνάρτησης F (F-score), η οποία δίδεται ως εξής:

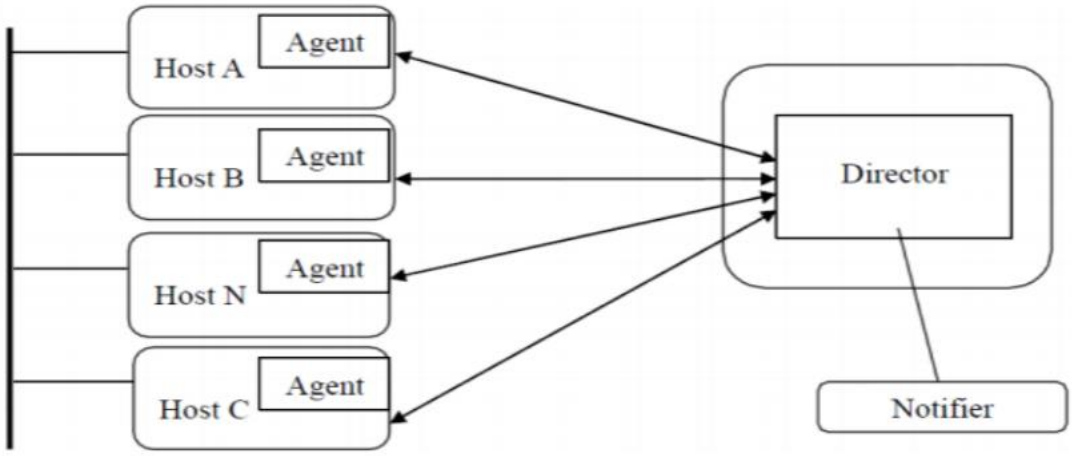
$$F_c = \frac{2 \times \text{Ορθότητα}_c \times \text{Ανάκληση}_c}{\text{Ορθότητα}_c + \text{Ανάκληση}_c} \quad (4\text{-}10)$$

5 ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ (IDS)

Όπως αναφέραμε και προηγουμένως, ταIDSμε ειδικά ανεπτυγμένους αλγορίθμους παρακολουθούν και αναλύουν σε συνεχή βάση συμβάντα και πληροφορίες που ανταλλάσσονται μέσα στο δίκτυο ενός υπολογιστικού συστήματος προκειμένου να εντοπίσουν προσπάθειες εισβολής και τυχόν παραβίαση της ασφάλειας του συστήματός του. Παρακάτω, παρουσιάζονται οι μηχανισμοί για την προστασία των συστημάτων, η αρχιτεκτονική των λογισμικών αυτών και οι κατηγορίες που αυτά χωρίζονται. Επίσης, αναπτύσσονται οι βασικές αρχές για ένα περιβάλλον ανίχνευσης εισβολών και αναλύονται τα μοντέλα εισβολών. Περιγράφεται τέλος, η πρόληψη και ο χειρισμός περιστατικών ασφάλειας-εισβολών.

5.1 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΣΥΣΤΗΜΑΤΩΝ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ

Τρία μέρη συντελούν τον μηχανισμό παρακολούθησης καθώς και ελέγχου των συστημάτων ανίχνευσης των εισβολών. Τα μέρη αυτά αφορούν την ύπαρξη ενός (ή περισσότερων) αντιπροσώπων (agent-s), την ύπαρξη ενός διευθυντή (director) και τέλος την ύπαρξη ενός αγγελιοφόρου (notifier). Στο σχήμα 5-1 που φαίνεται παρακάτω, αποτυπώνεται γραφικά η αρχιτεκτονική ενός τέτοιου συστήματος.



Εικόνα 5-1Αρχιτεκτονική Συστήματος Ανίχνευσης Εισβολών [45].

5.1.1 ΑΝΤΙΠΡΟΣΩΠΟΣ (AGENT)

Ο αντιπρόσωπος σε ένα σύστημα ανίχνευσης εισβολών αποσκοπεί στη συλλογή πληροφοριών που είναι σημαντικές προς εξαγωγή συμπερασμάτων. Τις συλλεγόμενες πληροφορίες τις επεξεργάζονται καταλλήλως και στη συνέχεια τις

μεταβιβάζουν στο διευθυντή. Η συλλογή τους, πιο ειδικά, πραγματοποιείται από είτε εφαρμογές είτε δεδομένα του αυτούσιου λειτουργικού συστήματος ή από δεδομένα καταγραφής συμβάντων (log files). Επιπρόσθετα, η τοπολογία του εκάστοτε συστήματος καθορίζει και τον αριθμό αντιπροσώπων που θα επιστρατευτούν, προκειμένου να επιτευχθεί όσο το δυνατών μεγαλύτερη ακρίβεια. Μπορεί να συμπεραθεί, λοιπόν, ότι οι διαφορετικές πηγές πληροφοριών (τοπολογία) που παρέχονται στο σύστημα μπορούν να διαχωριστούν σε επίπεδο δικτύου και επίπεδο συστήματος και κατ' επέκταση να δημιουργήσουν τις αντίστοιχες κλάσεις των μηχανισμών ανίχνευσης εισβολών, που θα αναλυθούν σε επόμενες υποενότητες.

5.1.2 ΔΙΕΥΘΥΝΤΗΣ (DIRECTOR)

Η βασική λειτουργία του διευθυντή στο σύστημα έγκειται στην ενασχόλησή του με τα δεδομένα που έχουν συλλεχθεί από τους αντιπροσώπους, ώστε να προσδιοριστεί το ενδεχόμενο εξέλιξης μιας επίθεσης ή και ενός προδρόμου μιας επίθεσης. Πιο ειδικά, ο διευθυντής αξιοποιεί μια μηχανή ανάλυσης, που έχει τη δυνατότητα να λάβει υπόψη πλήθος προτύπων ταυτοποίησης εισβολών. Τα προαναφερθέντα διασαφηνίζουν την ύπαρξη απειλητικής ενέργειας, με βάση δεδομένους κανόνες και αντίστοιχων μεθόδων τεχνητής νοημοσύνης.

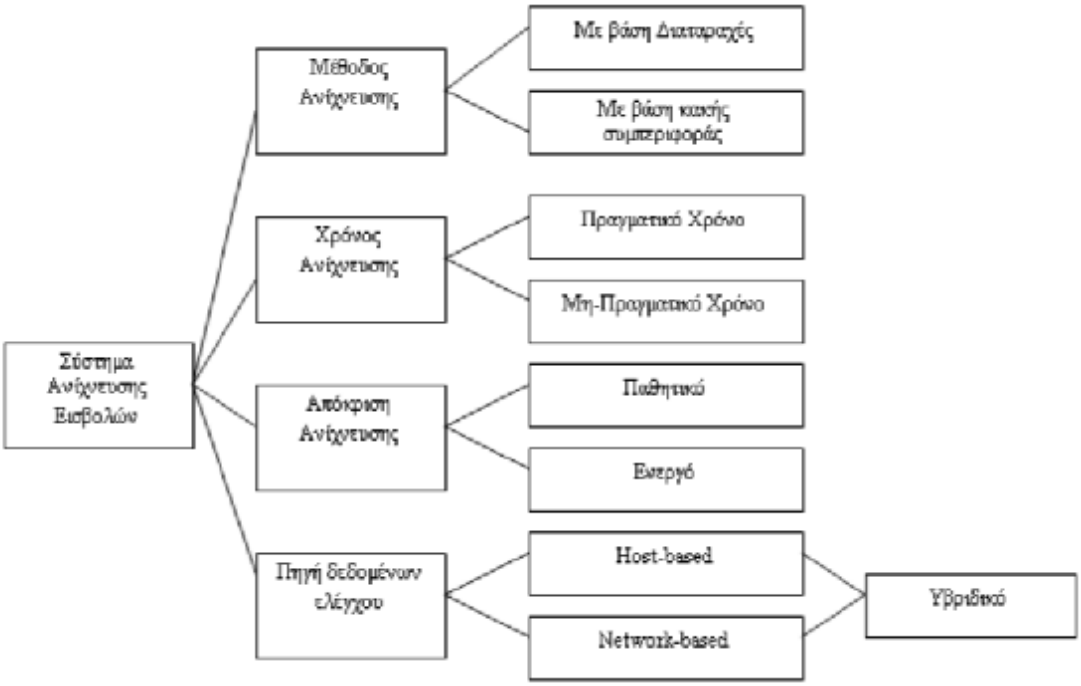
Εκτός αυτού, ο διευθυντής δύναται να αποστείλει δεδομένο πλήθος οδηγιών στους αντιπροσώπους ώστε οι τελευταίοι να συλλέξουν επιπρόσθετες πληροφορίες, σχετικές με συγκεκριμένο τύπο ενεργειών. Παράλληλα, η λειτουργία του εν λόγω μέρους του μηχανισμού ανίχνευσης, προτιμάται να διενεργείται σε εξωτερικό σύστημα, λόγω της κρισιμότητας του ρόλου του σε αυτό.

5.1.3 ΑΓΓΕΛΕΙΟΦΟΡΟΣ (NOTIFIER)

Η ύπαρξη του αγγελιοφόρου σε ένα σύστημα ανίχνευσης αποσκοπεί στην ενημέρωση του υπεύθυνου ασφαλείας αυτού, αναφορικά με τις εκβάσεις των μηχανών ανάλυσης του διευθυντή. Αξίζει να σημειωθεί ότι η λειτουργία του αγγελιοφόρου ποικίλλει, ανάλογα με τον προγραμματισμό του συστήματος. Έτσι, ο αγγελιοφόρος «απαντάει» στις επιθέσεις είτε αποστέλλοντας ειδοποίηση στο διαχειριστή του συστήματος είτε προβαίνοντας σε σύνολο διαφοροποιημένων συγκεκριμένων ενεργειών.

5.2 ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗ ΤΩΝ ΣΑΕ (IDS)

Τα Συστήματα Ανίχνευσης Εισβολών σύμφωνα με τον τρόπο που επιλέγουμε να τα κατηγοριοποιήσουμε, αναλόγως χωρίζονται στις εξής κατηγορίες όπως φαίνεται στο επόμενο σχήμα και παρουσιάζονται αναλυτικότερα παρακάτω. Πρώτα, αναλύονται οι τρείς κατηγορίες που προκύπτουν με βάση την πηγή δεδομένων ελέγχου:



Εικόνα 5-2 Κατηγοριοποίηση των Συστημάτων Ανίχνευσης Εισβολών [45].

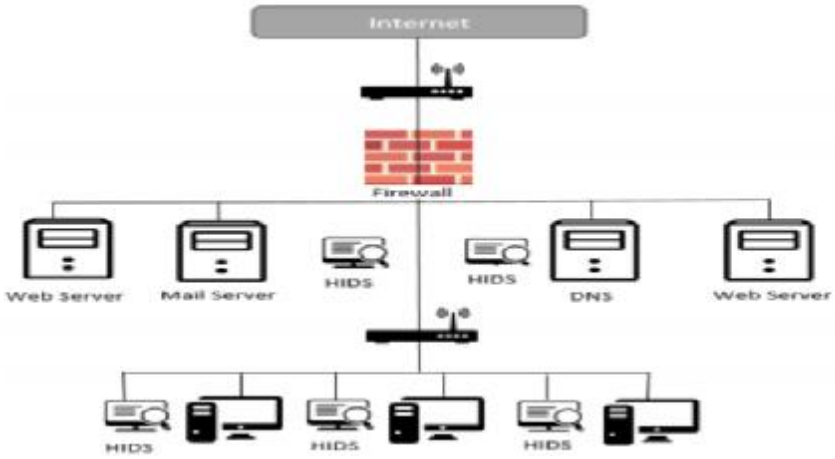
5.2.1 ΣΥΣΤΗΜΑ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ ΜΕΜΟΝΩΜΕΝΟΥ ΣΥΣΤΗΜΑΤΟΣ (Host-Based IDS - HIDS)

Η λειτουργία των Συστημάτων Ανίχνευσης Εισβολών Μεμονωμένου Συστήματος (HIDS) έγκειται στη χρήση συλλεγόμενων πληροφοριών από ένα μοναδικό σύστημα, το οποίο και προστατεύουν. Το σύνολο των πληροφοριών αυτών αφορά αρχεία καταγραφής ενός μεμονωμένου συστήματος, όχι μόνο τις διεργασίες αλλά και τις εφαρμογές του εν λόγω συστήματος. Πιο συγκεκριμένα, λειτουργούν παρακολουθώντας για ασυνήθιστη δραστηριότητα που περιορίζεται στον τοπικό υπολογιστή, όπως παράξενη πρόσβαση στα αρχεία ή μετατροπές σε δικαιώματα του συστήματος. Επειδή υπάρχει κάθε χρονική στιγμή εικόνα των συμβάντων του συστήματος, ο συγκεκριμένος τύπος ανίχνευσης θεωρείται αρκετά ισχυρός. Στη περίπτωση εμφάνισης δραστηριότητας που προκαλεί δυσλειτουργία σε ένα υπολογιστή, το εν λόγω σύστημα, την κατηγοριοποιεί ως επίθεση.

Τα συστήματα HIDS εμφανίζουν μικρότερο ποσοστό λανθασμένων ειδοποιήσεων (False Positive), εν συγκρίσει με τα συστήματα NIDS, δεδομένου ότι η πληθώρα των εντολών που εκτελούν είναι αρκετά μικρότερη και κατά συνέπεια η πολυπλοκότητά τους είναι σαφώς μικρότερη. Επίσης, τα συστήματα HIDS μένουν ανεπηρέαστα από τιε συνδεσμολογίες ή τα κρυπτογραφημένα πακέτα που χρησιμοποιούν ως βάσει μεταγωγούς καθώς τα προαναφερθέντα υπόκειται σε επεξεργασία μετά τη διαδικασία αποκρυπτογράφησης και εισαγωγής στο σύστημα.

Στα μειονεκτήματα των συγκεκριμένων τεχνικών ανίχνευσης συγκαταλέγεται η απαίτηση εγκατάστασης αυτών σε κάθε συσκευή που επιδιώκει τη προστασία της.

Σε περίπτωση, για παράδειγμα, που η συσκευή είναι ένας διακομιστής δικτύου, τότε αναμένεται να προκληθεί ζήτημα χωρητικότητας, κατά την εγκατάσταση του συστήματος HIDS ή/ και ζήτημα ασφάλειας, καθώς ενδέχεται οι διαχειριστές να μην είναι σε θέση να εισέλθουν στο σύστημα. Εν γένει, η φύση του εν λόγω λογισμικού είναι δυσκολεύει τη χρήση τους. Επιπλέον, τέτοια συστήματα καθιστούν ευάλωτα τα συστήματα που εγκαθίστανται, σε επιθέσεις, αν ληφθεί υπόψη το ποσό χρόνου που πρέπει να σπαταληθεί προκειμένου για ανάλυση των βλαβών. Ειδικότερα, ο χρόνος αυξάνεται γραμμικά, ανάλογα με τον αριθμό των συσκευών που λαμβάνουν χώρα και συνεπώς αν απαιτείται χρόνος t για την ανάλυση ενός συμβάντος. Απαιτείται χρόνος k_t για πλήθος k συσκευών. Στο σχήμα 5-3 φαίνεται ένα παράδειγμα εφαρμογής του λογισμικού HIDS.



Εικόνα 5-3Παράδειγμα Host-Based IDS–HIDS [42].

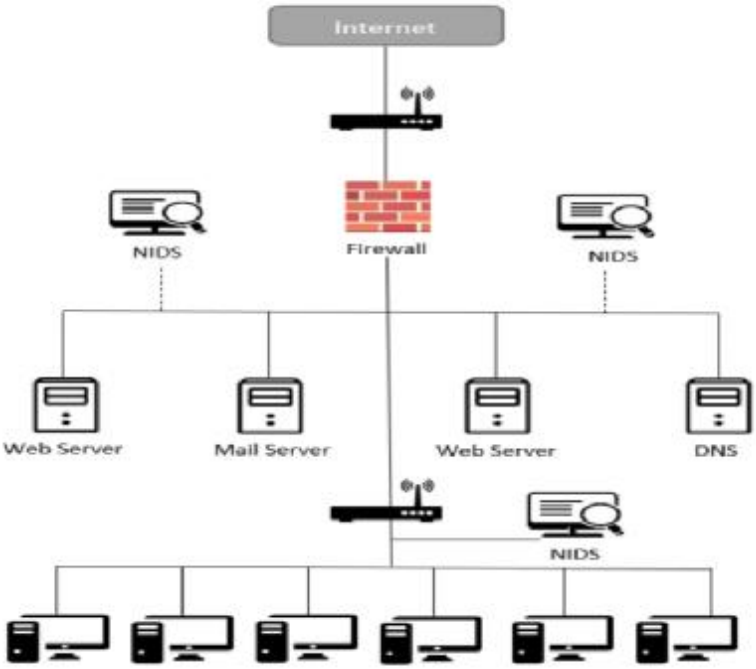
5.2.2 ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ ΔΙΚΤΥΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ (Network-Based IDS – NIDS)

Η λειτουργία των Συστημάτων Ανίχνευσης των Εισβολών ενός Δικτυακού Συστήματος (NIDS), βασίζεται στο σύνολο των πληροφοριών, όπως αυτές προκύπτουν από την γενικής δικτυακή δραστηριότητα. Αναλυτικότερα, στόχος των προαναφερθέντων είναι η παρακολούθηση της συνολικής δικτυακής κίνησης ενός υπολογιστικού συστήματος, με την προϋπόθεση ότι δεν προβαίνουν σε επιπρόσθετη επεξεργασία πληροφοριών [20,33]. Για του λόγου το αληθές, τα συστήματα NIDS απαρτίζονται από αισθητήρες, οι οποίοι εγκαθίστανται σε δεδομένα σημεία του δικτύου και είναι ικανοί να αξιολογήσουν κάθε πακέτο της δικτυακής κίνησης. Στην ουσία, οι αισθητήρες είναι πληροφοριακά συστήματα με εξαιρετική δυναμική επεξεργασίας αλλά και δικτύωσης, γεγονός που τα καθιστούν ικανότατα μέσα καταγραφής της αξιολόγησης ενός δικτύου. Η καταγραφή δε, πραγματοποιείται σε χώρους αποθήκευσης, τοπικούς ή απομακρυσμένους.

Παράλληλα, τα συστήματα δύνανται να αποκρύψουν τη παρουσία τους στους επιτιθέμενους και έτσι να μην ταυτοποιούνται ως προς την ύπαρξη ή και τη θέση τους. Μια κάρτα δικτύου, για παράδειγμα, είναι σε θέση να δέχεται δικτυακά πακέτα που προορίζονται ,μόνο για προσωπική διεύθυνση και συνεπώς, βάσει του ορισμού των NIDS, η κάρτα αυτή είναι απαραίτητο να τεθεί σε λειτουργία παρακολούθησης προκειμένου για αντίληψη της ολικής δραστηριότητας στο δίκτυο[33]. Το σχήμα 5-4 αποτυπώνει τον τρόπο λειτουργίας ενός δικτύου που αξιοποιεί 3 συστήματα ανίχνευσης NIDS.

Τα συστήματα NIDS είναι τα συστήματα που ενδείκνυνται περισσότερο για τη παρακολούθηση της ολικής κίνησης ενός δικτύου ή ενός τμήματος ενός δικτύου αναφορικά με την ύπαρξη ιχνών εισβολών. Επιπλέον, τα προαναφερθέντα έχουν καλύτερες αποδόσεις εν συγκρίσει με τα HIDS, αφού δεν είναι απαραίτητη η εξουσιοδότηση για την πρόσβασή τους σε ένα δίκτυο και συνεπώς μπορούν να παρακολουθούν χωρίς επιπτώσεις τη κίνηση ευαίσθητων αντικειμένων[20,33]. Παράλληλα, το λογισμικό αυτό δεν απαιτεί περαιτέρω επεξεργασία κατά την εγκατάστασή του σε μια δικτυακή συσκευή, που ενδεχομένως να προκαλούσε ζητήματα λειτουργικότητας ή χωρητικότητας σε αυτό.

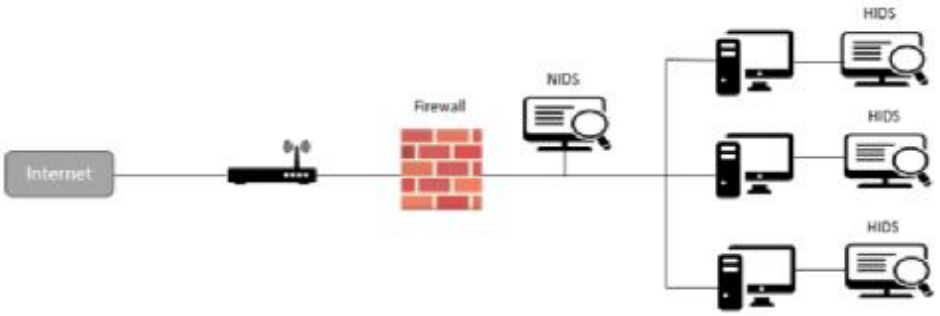
Ένα μειονέκτημα του network-based λογισμικού είναι η ανικανότητα που εμφανίζει στην αναγνώριση μιας επίθεσης που προκαλείται από διαφορετικό δίκτυο από αυτό που καλούνται να προστατέψουν, γεγονός που συνεπάγεται την επένδυση μεγάλου χρηματικού ποσού προκειμένου να εγκατασταθεί σε περιβάλλον με πολλαπλές Ethernet δικτυώσεις. Πέραν αυτού, τα εν λόγω συστήματα αδυνατούν να αντιμετωπίσουν με ευκολία επιθέσεις με κρυπτογραφημένες πληροφορίες ενώ ο τρόπος συνδεσμολογίας τους δε τους επιτρέπει να ελέγξουν το σύνολο των πακέτων που κινούνται στο δίκτυο που είναι εγκατεστημένα [33].



Εικόνα 5-4Παράδειγμα Network-Based IDS–NIDS [43].

5.2.3 ΣΥΝΔΥΑΣΤΙΚΗ ΛΥΣΗ ΣΥΣΤΗΜΑΤΩΝ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ ΥΒΡΙΔΙΚΑ (Hybrid IDS)

Στη πραγματικότητα, ο αποτελεσματικότερος τρόπος ασφάλειας στα δίκτυα των υπολογισμών, σε περιπτώσεις αναγνώρισης εισβολών είναι η συνδυαστική αξιοποίηση των μοντέλων HIDS και NIDS. Ουσιαστικά, ο μηχανισμός που ενδείκνυται για αποδοτικότερη μεταχείριση των προβλημάτων αναγνώρισης εισβολών είναι ο συνδυαστικός τρόπος μεταχείρισης των προηγουμένως αναλυόμενων μοντέλων. Η μέθοδος αυτή αντιμετωπίζει σωρεία προβλημάτων βάσει του μηχανισμού NIDS (δηλαδή δίκτυα μεταγωγών και συστήματα κρυπτογραφημένων επικοινωνιών) και είναι σε θέση να ανταποκριθεί σε οποιοδήποτε επίπεδου ενός δικτύου εφαρμοστεί, παρέχοντας υψηλά ποσοστά επιτυχίας, αφού οι λύσεις που παρέχουν είναι σαφέστερες και κατ' επέκταση ακριβέστερες ως προς την ανίχνευση ενδεχόμενων εισβολών. Ωστόσο, στα Υβριδικά Συστήματα Ανίχνευσης η συγκεκριμένη λύση, απαιτεί ιδιαίτερο φόρτο εργασίας κατά την εγκατάσταση και τη μάθηση του τρόπου διαχείρισής του. Ακολούθως παρατίθενται η εικόνα 5-5, που αποτυπώνει ένα Υβριδικό Σύστημα Ανίχνευσης.



Εικόνα 5-5 Συνδυασμός HIDS –NIDS [44].

5.3 ΜΟΝΤΕΛΑ ΕΙΣΒΟΛΩΝ

Σε προγενέστερες ενότητες της παρούσας εργασίας αναφέρθηκε ότι ο διευθυντής ενός Συστήματος Ανίχνευσης Εισβολών αξιοποιεί τα μοντέλα εισβολών με σκοπό την αξιολόγηση των πληροφοριών που του παρέθεσαν οι αντιπρόσωποι. Έπειτα, ταξινομεί τις παρεχόμενες πληροφορίες σε δύο κατηγορίες: «καλές», δηλαδή δεν υπάρχει το ενδεχόμενο εισβολής, και «κακές», δηλαδή υπάρχει το ενδεχόμενο εισβολής. Βάσει αυτών των ενεργειών, ορίζονται τρεις βασικές ταξινομήσεις στα μοντέλα αναγνώρισης πιθανών εισβολών: Κακής Συμπεριφοράς, Ανίχνευσης Διαταραχών καθώς και ανίχνευσης Διαταραχών Πρωτοκόλλων.

Σε κάθε κατηγορία, ακόμη, είναι δυνατή η εμφάνιση προσαρμοστικότητας, δηλαδή επαναπροσδιορισμός της συμπεριφοράς, βάσει των ενεργειών των συστημάτων, καθώς και η εμφάνιση στατικότητας, δηλαδή ο μηχανισμός τους να

παραμένει ανεξάρτητη από τις ενέργειες του συστήματος στο οποίο εφαρμόζονται. Στις υποενότητες που ακολουθούν, αναλύεται κάθε μοντέλο εμφάνισης.

5.3.1 ΜΟΝΤΕΛΟ ΚΑΚΗΣ ΣΥΜΠΕΡΙΦΟΡΑΣ

Τα πρότυπα Κακής Συμπεριφοράς είναι από τα πιο διαδεδομένα χρησιμοποιούμενα μοντέλα στο πεδίο ανίχνευσης εισβολών. Ουσιαστικά, ο τρόπος λειτουργίας του έγκειται στην αντιστοίχιση των συμβάντων που πραγματοποιούνται σε ένα πληροφοριακό σύστημα, με τις υπογραφές, δηλαδή με σύνολα προτύπων εισβολών που έχουν καθοριστεί σε πρότερη φάση. Η περίπτωση πλήρους αντιστοίχισης συνεπάγεται ότι το ενδεχόμενο εισβολής βρίσκεται σε εξέλιξη.

Επομένως, προκειμένου για έγκυρη ταυτοποίηση κακής συμπεριφοράς σε ένα σύστημα, είναι απαραίτητη η γνώση του συνόλου των (δυνητικών) ευπαθειών που δύνανται να λάβουν υπόψη οι επιτιθέμενοι [32]. Παρά τα υψηλά ποσοστά αξιοπιστίας που προσφέρει η εφαρμογή του εν λόγω μοντέλου σε ένα πληροφοριακό σύστημα, η ανικανότητα ανίχνευσης ενδεχόμενων εισβολών, που δεν είναι γνωστές στα σύνολα υπογραφών, αποτελεί σοβαρό μειονέκτημα.

5.3.2 ΜΟΝΤΕΛΑ ΑΝΙΧΝΕΥΣΗΣ ΔΙΑΤΑΡΑΧΩΝ

Η μη προσδοκώμενη συμπεριφορά ενός πληροφοριακού συστήματος αποτελεί αποδεικτικό στοιχείο για την παρουσία εισβολής, στα μοντέλα Ανίχνευσης Διαταραχών. Η υλοποίηση ενός τέτοιου μοντέλου, προϋποθέτει αρχικά τη συλλογή δεδομένων, συμπεριλαμβανομένων και των πληροφοριών των στατιστικών μέτρων αναφορικά με τη μη φυσιολογικής συμπεριφοράς αυτών. Δοθέντων αυτών, ακολουθεί η ενημέρωση του διαχειριστή και στη συνέχεια η διαταραχή ενεργοποιείται. Αξίζει να σημειωθεί ότι ο υπολογισμός των στατιστικών μέτρων αποτελεί το πολυπλοκότερο μέρος της διαδικασίας ενεργοποίησης των μοντέλων ανίχνευσης, δεδομένης της αυξημένης διακύμανσης που εμφανίζει η δραστηριότητα ενός πληροφοριακού συστήματος.

Απτόμενοι από αυτή τη συμπεριφορά, οι Lankewicz & Benard (2003), μελέτησαν την αξιοποίηση στατιστικών μοντέλων που βασίζονται σε μη παραμετρικές στατιστικές τεχνικές [15]. Η τεχνική των προαναφερθέντων ερευνητών ορίζεται ως ανάλυση κατά συστάδες και προϋποθέτει την ύπαρξη υπάρχουσας γνώσης (σύνολο δεδομένων), η οποία προέρχεται από τη παρακολούθηση, για συγκεκριμένο χρόνο, ενός συστήματος. Η μέθοδος των Lankewicz & Benard (2003), ακόμη, περιλαμβάνει την ομαδοποίηση σε υποσύνολα ή ομάδες των δεδομένων βάσει ορισμένων χαρακτηριστικών. Ανεξαρτήτως του γεγονότος ότι το προαναφερόμενο μοντέλο παρουσιάζει μικρότερο ποσοστό ακρίβειας, εν συγκρίσει με το μοντέλο Κακής Συμπεριφοράς, ενδείκνυται για χρήση αφού είναι ικανό να ταυτοποιήσει άγνωστες επιθέσεις [15].

5.4 ΟΡΓΑΝΩΣΗ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ

Λαμβάνοντας υπόψη τόσο τους τρόπους παρακολούθησης ενός πληροφοριακού συστήματος αλλά και του μοντέλου που θα εφαρμοστεί σε αυτό, προκειμένου για αναγνώριση δυνητικών εισβολών, κρίνεται σημαντική η οργάνωση του τελευταίου. Υπάρχουν διάφοροι τρόποι οργάνωσης ενός συστήματος ανίχνευσης, εκ των οποίων τρεις προσεγγίσεις θα αναλυθούν στις υποενότητες που ακολουθούν.

5.4.1 ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΤΗΣ ΚΥΚΛΟΦΟΡΙΑΣ ΣΤΟ ΔΙΚΤΥΟ – NSM

Το σύστημα όπου ο διευθυντής κάνει συνδυαστική χρήση των μοντέλων Ανίχνευσης Διαταραχών και Κακής Συμπεριφοράς ονομάζεται σύστημα Παρακολούθησης Κυκλοφορίας Δικτύου (Network Security Monitor) [36]. Στην αρχική του έκδοση, το σύστημα εκπαιδευόταν από ένα συγκεκριμένο σύνολο ενεργειών που έχουν καθοριστεί από προγενέστερη φάση και υποδηλώνουν φυσιολογική συμπεριφορά του υπό εξέταση δικτύου. Το εν λόγω σύστημα στην ουσία στηριζόταν στα δεδομένα εκπαίδευσης που ορίζουν τη δικτυακή κίνηση μεταξύ μιας ορισμένης πηγής και ενός προορισμού.

Παράλληλα, η μηχανή ανάλυσης (ταυτότητα σύνδεσης) που εφαρμοζόταν προσδιόριζε το τύπο συνδέσεων, υπό το πρίσμα εμφάνισης ή όχι μιας εισβολής. Στην ουσία, η μηχανή που θέτονταν σε λειτουργία σύγκρινε τις προσδοκώμενες τιμές των δεδομένων εκπαίδευσης με το σύνολο των πακέτων ανά σύνδεση και αν παρουσιάζονταν τιμές εκτός του προσδοκώμενου πεδίου τιμών, τότε οριζόταν μια ενδεχόμενη εισβολή. Στη πρώτη αξιολόγησή του, το σύστημα NSM χαρακτηρίστηκε από τους μελετητές ως χρονικά δαπανηρό. Προκειμένου για μείωση του παραγόμενου όγκου πληροφοριών και κατά συνέπεια του χρόνου ανίχνευσης, προτάθηκε η ομαδοποίηση των δικτυακών κινήσεων, αναφορικά με τον προορισμό και τη πηγή. Η αναβάθμιση του προαναφερθέντος συστήματος είχε ως αποτέλεσμα την ανάπτυξη κανόνων (υπογραφών), που θεωρήθηκαν ακρογωνιαίοι λίθοι για την περεταίρω βελτίωσή του.

5.4.2 ΣΥΝΔΥΑΣΜΕΝΗ ΠΡΟΣΕΓΓΙΣΗ: DIDS

Το σύστημα Ανίχνευσης Κατανεμημένων Εντολών (Distributed Instruction Detection System) κάνει συνδυαστική χρήση των Μεμονωμένων συστημάτων ανίχνευσης και του Δικτυακού συστημάτων [28]. Ειδικότερα, αξιοποιεί τις λειτουργίες του συστήματος NSM αλλά σε περιβάλλοντα μεμονωμένων συστημάτων ενώ διαφοροποιείται ως προς το σύνολο ταυτοτήτων δικτύου που αποδίδονται σε κάθε χρήστη, αφού αποδίδονται περισσότερες από μια. Ο λόγος διαφοροποίησης έγκειται στην ανικανότητα των αντιπροσώπων του συστήματος να αναγνωρίζουν τις περιπτώσεις μετακίνησης των εισβολέων μεταξύ των συστημάτων. Κατά τη λειτουργία του εν λόγω συστήματος, τα δεδομένα εκπαίδευσης συλλέγονται από τους αντιπροσώπους σε μια διαδικασία 5 επιπέδων που περιγράφεται ως εξής:

1. Συλλογή των δεδομένων εκπαίδευσης από τους αντιπροσώπων των μεμονωμένων συστημάτων αλλά και των συστημάτων δικτύου.
2. Αντιστοίχιση των χρηστών, όπως αναγνωρίστηκαν από τους αντιπροσώπους του δικτύου, με τα υποκείμενα και παράλληλα καταχώρηση ταυτότητας και αντίστοιχων ενεργειών για κάθε χρήστη.
3. Ανάλυση πληροφοριών που σχετίζονται με τη χρονική διάρκεια χρήσης, συχνότητα και στοιχεία ομοιότητας κατά τις συνδέσεις των χρηστών στο σύστημα, ώστε να αποφανθεί η ύπαρξη ύποπτης συμπεριφοράς.
4. Εποπτεία των απειλών που παρουσιάζονται στο δίκτυο, συμπεριλαμβανομένων και των συνδυασμών αυτών. Αξίζει να αναφερθεί ότι η απειλή προσδιορίζεται ως η κακή συμπεριφορά, που δύναται να καταπατήσει την πολιτική ασφάλειας που εφαρμόζει το υπό εξέταση σύστημα, χωρίς όμως να καταφέρει να το τροποποιήσει. Όμοια, μια απειλεί ορίζεται ύποπτη στις περιπτώσεις που δεν καταχράται τη πολιτική ασφαλείας που εφαρμόζεται σε ένα σύστημα αλλά υποδεικνύει το ενδεχόμενο εμφάνισης μιας επίθεσης.
5. Αξιολόγηση των συνθηκών ασφαλείας ενός δικτύου, με γνώμονα τις απειλές που πραγματοποιήθηκαν σε προγενέστερη φάση.

Κρίνεται, ακόμη, απαραίτητο να αναφερθεί ότι κάθε κανόνας σε ένα σύστημα DIDS αποσαφηνίζεται από μια αξία, η οποία κατ' επέκταση αξιοποιείται προκειμένου για υπολογισμό της βαθμολογίας ανά σύστημα. Ειδικότερα, ο υπεύθυνος ασφάλειας δίνει αναφορά στο σύστημα ανάλυσης και σε περιπτώσεις ψευδών ειδοποιήσεων η αξία, δηλαδή ο δείκτης του αντίστοιχου κανόνα, ελαττώνεται.

5.5 ΑΠΟΚΡΙΣΗ ΣΤΙΣ ΕΙΣΒΟΛΕΣ

Το επόμενο ζήτημα έρευνας, ύστερα από την ανάλυση της διαδικασίας ανίχνευσης εισβολών, αποτέλεσε η δημιουργία αυτόματων μηχανισμών άμυνας, στόχος των οποίων είναι η αντιμετώπιση των αποπειραθέντων επιθέσεων με συγκεκριμένο τρόπο έτσι ούτως ώστε να ελαχιστοποιούνται οι επιπτώσεις της εκάστοτε επίθεσης, όπως αυτές ορίζονται στην πολιτική ασφάλειας του εκάστοτε συστήματος.

5.5.1 ΕΝΕΡΓΕΣ ΑΠΟΚΡΙΣΕΙΣ

Εξ ορισμού οι ενεργές αποκρίσεις συντελούν αυτοματοποιημένες ενέργειες, οι οποίες είναι σε θέση να υλοποιούνται από τα συστήματα αναγνώρισης εισβολών. Σκοπός των ενεργειών αυτών είναι η άμεση διαχείριση της ενδεχόμενης επίθεσης και προς επίτευξη αυτού προβαίνει σε μια σειρά δραστηριοτήτων, όπως επεξηγείται ακολούθως:

- Συγκέντρωση επιπρόσθετων δεδομένων εκπαίδευσης: Στη φάση αυτή προσδιορίζονται οι επιπρόσθετες πληροφορίες που ενδέχεται να οδηγήσουν στην ύπαρξη πιθανής εισβολής, αποσκοπώντας στην αύξηση της ακρίβειας ως

προς την κατανόηση του τύπου εισβολής. Η τελική απόφαση του συστήματος, εξαρτάται από το περιεχόμενο των δεδομένων εκπαίδευσης που θα αποκτηθούν.

- Παρακώλυση του επιτιθέμενου: Η φάση αυτή συνεπάγεται με τη παρακώλυση ή τερματισμό της εισβολής στο υπό εξέταση σύστημα. Για το λόγο αυτό απαιτείται η επαναξιολόγηση των πολιτικών ασφαλείας και των δρομολογητών του εν λόγω συστήματος, ώστε να προβούν σε άμεση απόκλιση της IP του εισβολέα.
- Ανταπόδοση επίθεσης: Η φάση αυτή διακρίνεται σε δύο τύπους. Ο πρώτος τύπος αφορά τη δραστηριοποίηση στα πλαίσια του νομικού πλαισίου σε συναρμογή με τα αποδεικτικά στοιχεία εμφάνισης πιθανής επίθεσης, προκειμένου να αποσαφηνιστεί αν η εισβολή είναι υπαρκτή ή ψευδής. Ο δεύτερος τύπος σχετίζεται με την εφαρμογή μιας νέας μεθόδου επίθεσης που αποσκοπεί στο τερματισμό της υφιστάμενης επίθεσης αλλά και στην επίτευξη ανικανότητας αυτής να πραγματοποιήσει μελλοντική επίθεση. Ωστόσο, η τελευταία μεθοδολογία δεν ενδείκνυται, καθώς ενδέχεται να προκαλέσει πληθώρα επιπτώσεων και παρενεργειών σε «αθώα» συστήματα.

5.5.2 ΠΑΘΗΤΙΚΕΣ ΑΠΟΚΡΙΣΕΙΣ

Οι παθητικές αποκρίσεις αποσκοπούν στην ενημέρωση του υπεύθυνου ασφαλείας για το ενδεχόμενο υλοποίησης μιας εισβολής. Η ενημέρωση, ειδικότερα, δύναται να εμφανίζει κυμαινόμενο ρυθμό στις λεπτομέρειες που παρέχει ενώ εμφανίζεται με ποικίλους τρόπους (αναδυόμενο παράθυρο, σε ειδικό χώρο αναγνώρισης εισβολών κλπ). Είναι επίσης εφικτή για κάποια συστήματα, η αποστολή των παραγόμενων ειδοποιήσεων μέσω ενός ειδικού πρωτοκόλλου, του SNNP.

Η συναθροισμένη αποθήκευση των εν λόγω ειδοποιήσεων προέρχεται όχι μόνο από πληθώρα συστημάτων αναγνώρισης εισβολών αλλά και από δεδομένα που εξάγονται από εναλλακτικές τεχνικές ασφαλείας. Έτσι, απλουστεύεται η διαδικασία αντιστοίχισης των αποτελεσμάτων και κατά συνέπεια επιτυγχάνονται μεγαλύτερα ποσοστά ακρίβειας σχετικά με τη ταυτοποίηση των εισβολών σε ένα σύστημα.

6 ΣΥΣΤΗΜΑΤΑ ΠΡΟΛΗΨΗΣ ΕΙΣΒΟΛΩΝ (IPS)

Τα Συστήματα Πρόληψης Εισβολών -IPS είναι ένας εξελιγμένος και ευφυής τρόπος ελέγχου των εισβολών, αποτελούν δηλαδή το επόμενο βήμα εξέλιξης των Συστημάτων Ανίχνευσης Εισβολών (IDS), στοχεύοντας στην αντιμετώπιση των επιθέσεων πριν αυτές προλάβουν να ολοκληρωθούν. Χρησιμοποιούνται πολλές τεχνικές προκειμένου να εξασφαλιστεί το βέλτιστο επίπεδο ασφάλειας.

6.1 ΟΡΙΣΜΟΣ

Η τεχνολογία των Συστήματα Πρόληψης Εισβολής έγκειται στην αναγνώριση της ύποπτης κακόβουλης κίνησης σε ένα δίκτυο καθώς και στη πρόληψη ενδεχόμενης κακόβουλης συμπεριφοράς σε αυτό. Οι βασικότερες δραστηριότητες που λαμβάνουν χώρα σε ένα τέτοιο σύστημα αφορούν την καταγραφή πληροφορικών που αφορούν την ύποπτη κακόβουλη κίνηση προκειμένου για αποκλεισμό αυτής [8]. Ειδικότερα τα συστήματα IPS είναι σε θέση να μειώσουν τις ψευδώς θετικά υπογραφές εισβολής και παράλληλα να αναβαθμίσουν τα ποσοστά ακρίβειας των ορθώς υπολογισμένων επιθέσεων. Το τελευταίο επιτυγχάνεται με την υλοποίηση εφαρμογών μόνο σε μέρη κίνησης που έχει προσδιοριστεί από το αντίστοιχο πρωτόκολλο, στην αναγνώριση μιας εισβολής. Στόχος της εν λόγω τεχνολογίας αποτελεί η άμεση αυτόματη διακοπή της εισβολής, χωρίς την παρέμβαση του ανθρώπινου παράγοντα, προκειμένου να ελαχιστοποιηθεί η χρονική διάρκεια εξέλιξης της επίθεσης.

6.2 ΛΕΙΤΟΥΡΓΙΑ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΠΡΟΛΗΨΗΣ ΕΙΣΒΟΛΩΝ

Τα Συστήματα Πρόληψης Εισβολών (Intrusions Prevention Systems-IPS) εφευρέθηκαν για να επιλύσουν τις ασάφειες στον παθητικό έλεγχο των δικτύων. Τα προαναφερθέντα διαφέρουν ως προς το σύστημα firewall ως προς την ικανότητα ελέγχου της προσβασιμότητας, η οποία βασίζεται στο τύπο της εκάστοτε εφαρμογής και όχι στην IP [10]. Μερικά από τα IPS συστήματα μπορούν επίσης να αποτρέψουν την χρήση επιθέσεων που δεν έχουν ακόμα ανακαλυφθεί (Zero Day Exploit) που προκαλούνται από Buffer Overflow.

Οι κύριες λειτουργίες τους είναι ο καθορισμός των κακεντρεχών δραστηριοτήτων, η καταγραφή των δεδομένων που υποδεικνύουν την ύπαρξη κακόβουλης δραστηριότητας καθώς και οι ενέργειας τερματισμού αυτών. Τα συστήματα IPS λαμβάνουν διαδοχικές θέσεις στο περιβάλλον εφαρμογής τους και εστιάζουν στην ενεργή προστασία του περιβάλλοντός τους από κάθε κακεντρεχή ενέργεια (hackers). Η τεχνολογία που εφαρμόζεται είναι η εξελιγμένη μορφή της τεχνολογίας IDS, δεδομένου ότι τα προαναφερθέντα είναι σε θέση να στείλουν τις απαραίτητες ειδοποιήσεις ή να επαναπροσδιορίσουν μια σύνδεση ή, τέλος, να αποκλείσουν πιθανή εισβολή [39, 40].

Είναι αναμφισβήτητα λοιπόν, το επόμενο επίπεδο τεχνολογίας όσον αφορά την ασφάλεια καθώς το σύστημα εξασφαλίζει την ασφάλεια σε κάθε φάση του συστήματος, δηλαδή από τον πυρήνα έως τα πακέτα δεδομένων. Εκτός αυτού, τα εν

λόγω συστήματα αφήνουν το χρήστη να ορίζει την τελική ενέργεια όταν ενημερώνεται για την ύπαρξη κακόβουλης εισβολής. Κατά συνέπεια, όταν το πρότυπο IPS αντιληφθεί ότι υπόκεινται σε ύποπτες ενέργειες, προβαίνει σε ενέργειες τερματισμού, και πιο ειδικά, σε αποτροπή των υπογραφών εισβολής όχι μόνο αυτών που είναι ήδη γνωστές αλλά και ορισμένων άγνωστων, βάσει της συνολικής τους δραστηριότητας κατά την υλοποίηση της εισβολής.

Τα IPS εκτελούν εκτενή καταγραφή των δεδομένων που σχετίζονται με συμβάντα που εντοπίζονται. Περιλαμβάνουν αξιολογήσεις κωδίκων και δικτύων καθώς και ανάλυσης της κυκλοφορίας αυτού. Ακόμη, οι λειτουργίες τους αφορούν τον έλεγχο στο μοντέλο παρακολούθησης και της διαδικασίας συνολικά. Αξίζει ακόμη να αναφερθεί ότι παρέχουν ευρεία προστασία σε: Web, Mail, Windows, Linux, BSD, UNIX, Routers και Firewalls και βάσεις δεδομένων όπως DB2, Oracle, MySQL, MSsql και Postgresql.

6.3 ΨΕΥΔΩΣ ΘΕΤΙΚΑ ΚΑΙ ΑΡΝΗΤΙΚΑ IPS

Στο πλαίσιο της πρόληψης εισβολής, ψευδώς θετικό είναι ένα IPS που δηλώνει καλή κυκλοφορία ως κακή, με αποτέλεσμα είτε έναν ψευδή συναγερμό (αν τοIPS είναι σε παθητική λειτουργία ανίχνευσης) ή διακοπή της υπηρεσίας (αν το IPS είναι σε υπό-έλεγχο λειτουργίας πρόληψης). Ένα ψευδώς θετικό (False Positive) συνήθως προκαλείται από ένα αναποτελεσματικό κανόνα IPS ή αναποτελεσματική υπογραφή. Μια εσφαλμένη θετική επίθεση όμως δεν θα πρέπει να συγχέεται με μια «πραγματική» επίθεση που είναι αναποτελεσματική ενάντια στο λειτουργικό σύστημα ή την εφαρμογή που στοχεύει.

Το αντίθετο πρόβλημα είναι με ένα ψευδώς αρνητικό (False Negative) και υφίσταται όταν το σύστημα IPS δεν είναι σε θέσει να ανιχνεύσει την ύπαρξη εισβολής ή παρεμφερούς ενέργειας στα πλαίσια ασφάλειας. Αυτό τις περισσότερες φορές είναι αποτέλεσμα λανθασμένης ενημέρωσης αναφορικά με τους κανόνες ή και απουσία ενημέρωσης από τον υπεύθυνο παροχής του λογισμικού. Πιο αναλυτικά, η είσοδος μιας ψευδώς αρνητικής άδειας, είναι δυνατό να επιφέρει απώλειες στα συστήματα και κατ’ επέκταση μείωση της παραγωγικότητας και της κερδοφορίας σε μια επιχείρηση.

6.4 ΒΑΣΙΚΟΙ ΤΥΠΟΙ ΣΥΣΤΗΜΑΤΩΝ IPS

Αναλόγως το τόπο εφαρμογής αλλά και το είδος συστημάτων που καλούνται να προστατέψουν, τα Συστήματα IPS, διακρίνονται σε αρκετούς τύπους, με κυριότερους εξ αυτών τα συστήματα Πρόληψης Εισβολής που βασίζονται σε Κεντρικούς Υπολογιστές (Host-Based Intrusion Prevention Systems), τα συστήματα Πρόληψης Εισβολής Δικτύου (Network Intrusion Prevention Systems) καθώς και τα Ασύρματα Συστήματα Πρόληψης Εισβολής (Wireless Intrusion Prevention Systems) [8].

6.4.1 Host-Based Intrusion Prevention Systems (HIPS)

Τα συστήματα HIPS αξιολογούν τις ενέργειες που πραγματοποιούνται εντός του υπό μελέτη ξενιστή προκειμένου να αντιληφθούν μια ύποπτη ενέργεια. Ακόμη, είναι δυνατή η προστασία του περιβάλλοντος στο οποίο εφαρμόζονται σε κάθε επίπεδο λειτουργία του. Για παράδειγμα, η οποιαδήποτε μεταβολή που υφίσταται στο σύστημα, είτε από την είσοδο ενός κακόβουλου λογισμικού είτε από την εισβολή ενός hacker, συνεπάγεται ότι το λογισμικό θα αδρανοποιηθεί προσωρινά και θα ενημερώσει τον υπεύθυνο ώστε από κοινού να αποφανθούν για τη καλύτερη δυνατή λύση.

Αξίζει ακόμη να σημειωθεί η διαφορετικότητα λειτουργίας του συστήματος HIPS, εν συγκρίσει με τη δραστηριότητα των anti-virus καθώς και των firewalls, έγκειται στη προσέγγιση που θα λάβει για να καταπολεμήσει μια εφαρμογή [10]. Αναλυτικότερα, το σύστημα ελέγχει ολικά την εφαρμογή, φιλτράροντας όλη τη κυκλοφορία μιας συγκεκριμένης υποδοχής (αντί να αντιστοιχίζει τις υπογραφές), παρεμποδίζοντας έτσι τις κακόβουλες απόπειρες εισβολής. Επιπρόσθετα, μια εφαρμογή τελευταίας τεχνολογίας για το εν λόγω λογισμικό αποτελεί η δυνατότητα που παρέχουν στους χρήστες τους να εξατομικεύουν τα συστήματά τους με δικούς τους κανόνες ή πρόσθετες εφαρμογές.

6.4.2 Network-Based Intrusion Prevention Systems (NIPS)

Το Σύστημα Ανίχνευσης Πρόληψης (IPS) άπτεται σε δίκτυα που αποσκοπούν στη σάρωση των πακέτων δεδομένων καθώς και στην αξιολόγηση της κυκλοφορίας, εισερχόμενων και εξερχόμενων ενεργειών, ούτως ώστε να αποκλείσει οποιαδήποτε ύποπτη κακόβουλη ενέργεια. Τα παράγωγα του προτύπου NIPS, δραστηριοποιούνται σε σειρά, γεγονός που υποδηλώνει ότι το λογισμικό αυτό αποτελεί ένα τείχος προστασίας για το περιβάλλον εφαρμογής του. Ακόμη, το NIPS αποδέχεται πακέτα που στη συνέχεια αξιολογεί προκειμένου να αποφανθεί για το αν πρέπει να απορριφθούν ή να συνεχίζουν να υφίστανται στο δίκτυο

Πέραν αυτού, η διάρθρωση ενός τέτοιου μοντέλου ενδείκνυνται για την ταυτοποίηση ορισμένων εισβολών πριν ακόμη επηρεάσουν το δίκτυο στο οποίο εισήλθαν. Η πλειοψηφία των λογισμικών NIPS αξιοποιούν συνδυαστικά τις τεχνικές υπογραφών και ανάλυσης αλλά και των πολιτικών που εφαρμόζονται σε άλλα μοντέλα (πχ E-mails, Web Servers), προκειμένου να αναγνωρίσουν ήδη γνώριμες συμπεριφορές και συνεπώς να επιτύχουν σωστά αποτελέσματα. Η χρήση των NIPS έγκειται στην αναγνώριση διάφορων τύπων κακόβουλων ενεργειών ενώ δύναται και η ταυτοποίηση εκ μέρους τους και συγκεκριμένων τύπων malwares (worms).

Ακόμη, ένα σύστημα NIPS είναι ικανό να εντοπίζει και να εκτοπίζει πληθώρα γνωστών απειλών, βάσει του πρωτοκόλλου εφαρμογής και συνεπώς να αυξάνει την ακρίβεια απόδοσής του. Επιπλέον, τα συστήματα αυτά έχουν την ιδιότητα υπερβολικής προσαρμογής στο δίκτυό τους με αποτέλεσμα μέσα σε μικρό χρονικό διάστημα να επιτυγχάνεται η δημιουργία πολλαπλών υπογραφών και συνεπώς να γίνουν λάθη, όπως ψευδώς αληθείς υπογραφές που θα πλήξουν τη διαδικασία

συνολικά. Παρόλα αυτά, το πρότυπο NIPS δεν είναι σε θέση να αποκλείσει τη δραστηριότητα κακόβουλων ενεργειών που πηγάζουν από κινητή συσκευή ή εναλλακτικά από Trojan Horses.

6.4.3 Wireless Intrusion Prevention Systems (WIPS)

Τα Ασύρματα Συστήματα Πρόληψης Εισβολής είναι πρότυπα που δύνανται να σαρώνουν την ασύρματη κίνηση των εισερχόμενων και εξερχόμενων δεδομένων, με απώτερο σκοπό την αποτροπή της μη εξουσιοδοτημένης εισόδου ή της πιθανότητας εισβολής σε ένα δίκτυο ή εναλλακτικά σε άλλους πόρους που επίσης κάνουν χρήση της ασύρματης σύνδεσης στο Internet. Μπορεί να επισημανθεί στο σημείο αυτό ότι ένα τέτοιο σύστημα ελέγχει το ράδιο φάσμα προκειμένου να εντοπιστεί ενδεχόμενη εισβολή ή ύποπτα μέσα εισόδου στο δίκτυο.

Έτσι, μόλις γίνει αντιληπτή η παρουσία ενός μη εξουσιοδοτημένου σημείου εισόδου, το σύστημα WIPS ενημερώνει τον χρήστη ή το δίκτυο για τα τεκταινόμενα. Η λειτουργία του προαναφερθέντος βασίζεται στην δημιουργία αισθητήρων που διαθέτουν ενσωματωμένες κεραίες και ραδιόφωνα, των οποίων πρωταρχικός ρόλος είναι η αποτύπωση των κινήσεων που πραγματοποιούνται. Επόμενο βήμα είναι η σάρωση των λαμβανόμενων, από τους αισθητήρες, πληροφοριών.

6.5 ΔΙΑΦΟΡΕΣ IDS ΚΑΙ IPS ΣΥΣΤΗΜΑΤΩΝ

Προκειμένου να εντοπιστούν οι διαφοροποιήσεις μεταξύ των IDS και IPS συστημάτων, σημειώνεται ότι τα πρώτα αρχικώς προοριζόταν για την αναγνώριση κακόβουλων δραστηριοτήτων σε ένα μέρος του δικτύου, ενώ τα δεύτερα στην αναγνώριση τέτοιων δραστηριοτήτων προκειμένου να τα αποκλείσει. Ωστόσο, και τα δύο συστήματα υλοποιούν ίδιου βελληνεκούς ενέργειες, όπως ο έλεγχος και η αξιολόγηση των δεδομένων που εισέρχονται, ο επαναπροσδιορισμός του επιπέδου TCP καθώς και η συνάρμοση με το πρωτόκολλο και τη διαδικασία των υπογραφών. Η διαφορετικότητα εκτείνεται και στον τρόπο που δραστηριοποιούνται προκειμένου για την αντιμετώπιση μιας εισβολής. Το IDS είναι ένα παθητικό μοντέλο παρακολούθησης ενώ αντίθετα το σύστημα IPS είναι ένα ενεργό μοντέλο πρόληψης.

Ειδικότερα, τα πρώτα είναι σε θέση να αποδώσουν σε πραγματικό χρόνο ενημερώσεις για πιθανή εισβολή και έτσι εγκαίρως να επιλύσουν το πρόβλημα ενώ τα δεύτερα μοντέλα αποδίδουν ανά τακτά χρονικά διαστήματα ενημερώσεις της κατάστασης του δικτύου προκειμένου για να εγγυηθεί η προστασία τους από κάθε κακόβουλη δραστηριότητα. Μπορεί να διαπιστωθεί ότι τα συστήματα IPS λαμβάνουν όλες τις πληροφορίες που καταγράφηκαν, από το σύνολο των δικτύων που τίθενται υπό έλεγχο, αξιοποιώντας μια κονσόλα διαχείρισης. Κατά αυτό τον τρόπο, ταυτοποιούνται εισβολές που δεν δύνανται να αναγνωριστούν από τα συστήματα IPS.

Όμως τα συστήματα IPS έχουν και κάποια μειονεκτήματα στη λειτουργία τους, όπως το ότι είναι λιγότερο αποδοτικά. Δεν μπορούν να ανιχνεύσουν μικρότερες εκδηλώσεις του δικτύου επιπέδου. Επίσης, δεν μπορούν να εξετάσει καμία

κρυπτογραφημένη κίνηση. Τα πρότυπα IPS δεν θα πρέπει να χρησιμοποιούνται με πολλαπλά λειτουργικά συστήματα. Αντιθέτως, είναι αναγκαίο να έχουν αισθητήρες σφαλμάτων, διαφορετικά δημιουργούν αρνητικές επιπτώσεις στη κίνηση του δικτύου. Το λογισμικό μπορεί να δημιουργήσει ένα μεγάλο αριθμό λανθασμένων συναγερμών. Αυτοί οι ψευδείς συναγερμοί αυξάνονται σε δίκτυα όπου υπάρχει μεγάλος αριθμός χρηστών. Για την αποφυγή ψευδών συναγερμών, οι επαγγελματίες πρέπει να λαμβάνουν εκτενή κατάρτιση, έτσι ώστε να μπορούν να αναγνωρίζουν ποιος είναι ο ψευδής συναγερμός και ποιος δεν είναι. Η δαπάνη για την ολοκλήρωση αυτής της εκπαίδευσης είναι ένα άλλο μειονέκτημα του λογισμικού Πρόληψης Εισβολών.

6.6 ΠΑΡΟΥΣΙΑΣΗ ΠΡΟΪΟΝΤΩΝ IDS και IPS

Η έρευνα προκειμένου για περεταίρω ανάπτυξη των Συστημάτων Ανίχνευσης και Πρόληψης Εισβολών την τελευταία δεκαετία παρουσίασε αρκετά βιώσιμα συστήματα-προϊόντα [21, 35]. Κάποια από τα πιο κορυφαία λογισμικά που υπάρχουν στην αγορά ή διατίθενται δωρεάν, αναφέρονται στους παρακάτω πίνακες με λίγο αναλυτικότερη και εκτενέστερη παρουσίαση αυτής του SNORT.

Snort	Είναι ένα ελαφρύ δωρεάν σύστημα ανίχνευσης εισβολών, ικανό να εκτελεί σε πραγματικό χρόνο ανάλυση της κυκλοφορίας και καταγραφής πακέτων σε IP δίκτυα.
Bro	Bro είναι μια ανοιχτή πηγή, Unix-based σύστημα ανίχνευσης εισβολών που παρακολουθεί παθητικά την κυκλοφορία του δικτύου και ψάχνει για ύποπτη δραστηριότητα.
Sguil	Sguil είναι μια συλλογή των ελεύθερων συστατικών λογισμικού για παρακολούθηση ασφάλειας δικτύου και την περίπτωση με γνώμονα την ανάλυση των IDS ειδοποιήσεις.

Πίνακας6-1Κορυφαία Συστήματα Ανίχνευσης Εισβολών [45].

Ossec	Είναι ένα δωρεάν σύστημα πρόληψης εισβολής. Εκτελεί ανάλυση καταγραφής, ελέγχου της ακεραιότητας, παρακολούθησης μητρώου των Windows, ανίχνευσης rootkit, χρόνο προειδοποίησης, και την ενεργό
	ανταπόκριση. Παρέχει ανίχνευσης πρόληψης για τα περισσότερα λειτουργικά συστήματα, όπως το Linux, OpenBSD, FreeBSD, Mac OS X, Solaris και Windows .
Suricata	Είναι ένα ανοιχτού κώδικα σύστημα πρόληψης εισβολής. Αναπτύχθηκεαπότην Open Information Security Foundation (OISF).

Πίνακας6-2Κορυφαία Συστήματα Πρόληψης Εισβολών [45].

6.7 ΣΥΝΤΟΜΗ ΠΑΡΟΥΣΙΑΣΗ ΤΟΥ SNORT

Το Snort είναι ένα δωρεάν λογισμικό ανοιχτού κώδικα (Open Source), πρόληψης και ανίχνευσης εισβολών (Network Intrusion Prevention System–NIPS καθώς και ένα “ελαφρύ” NIDS, όπως ακόμη και ένα εργαλείο ανάλυσης πακέτων. Ο δημιουργός του Snort είναι ο Martin Roesch ο οποίος ξεκίνησε την ανάπτυξη του, το 1998, κώδικά σε γλώσσα προγραμματισμού C, ενώ σήμερα ένας μεγάλος αριθμός ατόμων έχει εμπλακεί σε αυτήν την διαδικασία, με απώτερο στόχο την προσθήκη νέων λειτουργιών στο Snort και την βελτίωση των δυνατοτήτων του [50]. Σημαντικό ρόλο για το γεγονός αυτό παίζει ότι το Snort είναι ένα Open Source λογισμικό, το οποίο διατίθεται κάτω από την GNU General Public License (GPL) που καθιστά ελεύθερη την χρήση και ανάπτυξη του κώδικά του από τον καθένα. Ο όρος 'ελαφρύ' έχει δύο έννοιες. Η μία έχει να κάνει με την εφαρμογή του σε σχετικά μικρά δίκτυα,

ενώ η δεύτερη έχει να κάνει με το μικρό μέγεθος του και την ευκολία εφαρμογής και χρήσης του. Όμως εκτός από την λειτουργία του σαν NIDS μπορεί να δουλέψει και σαν ένας απλός sniffer ή σαν ένας sniffer που καταγράφει (Iogging) τα πακέτα που λαμβάνει σε αρχεία. Έχει τρεις τρόπους (mode) λειτουργίας :

1. **Sniffer** mode : Σε αυτό τον τρόπο λειτουργίας το Snort έχει την ικανότητα να διαβάζει τα πακέτα που περνούν από το δίκτυο, να τα αποκωδικοποιεί και να τα εμφανίζει στην οθόνη σε μορφή φιλική προς τον χρήστη.

2. **Packet** logger mode: Σε αυτό το τρόπο λειτουργίας το Snort αποθηκεύει στο δίσκο τα πακέτα που διαβάζει από το δίκτυο, αντί απλά να τα εμφανίζει στην οθόνη. Η διαδικασία αυτή είναι αρκετά σημαντική στην περίπτωση που απαιτείται τα πακέτα αυτά να εξεταστούν με λεπτομέρεια σε επόμενο στάδιο.

3. **NIDS** mode:Αυτή είναι η κύρια λειτουργία του Snort. Όπως αναφέρθηκε προηγουμένως, το Snort είναι ένα ΣΑΕ το οποίο ενεργεί σε επίπεδο δικτύου, δηλαδή τα γεγονότα που παρακολουθεί και εξετάζει για την εμφάνιση μίας πιθανής επίθεσης, αφορούν την δραστηριότητα που παρατηρείται σε ένα δίκτυο. Το Snort έχει την ικανότητα να ανιχνεύει ένα μεγάλο φάσμα από γνωστές δικτυακές επιθέσεις, όπως port scans, buffer overflows, OS fingerprints και πολλά άλλα. Η τεχνική που χρησιμοποιεί το Snort για την διαδικασία αυτή είναι κατά κύριο λόγο η Misuse Detection σε συνδυασμό, ωστόσο με την αξιοποίηση των Signatures ενός βλαβερού πακέτου. Παρόλα αυτά, η τελευταία αναβάθμιση στο Snort, του επέτρεψε να συναρμόζει τις ενέργειες αξιολόγησης των δραστηριοτήτων που σχετίζονται με τις διαδικασίες ανίχνευσης απειλών, με τις πρακτικές του Protocol Anomaly Detection και του Anomaly Detection. Οι μηχανισμοί αυτοί υλοποιούνται κατά κύριο λόγο από τους preprocessors αλλά και από το νέο του μηχανισμό να συντάσσει τα rules σε κατηγορίες.

Τα βασικότερα επίπεδα λειτουργίας του λογισμικού Snort παρατίθενται ως εξής:

1. Βιβλιοθήκη συλλογής πακέτων (Packet Capture Library-Libpcap)
2. Τον αποκωδικοποιητή πακέτων (Packet Decoder)
3. Τον προ-επεξεργαστή (Preprocessor)
4. Την μηχανή ανίχνευσης (Detection Engine)
5. Πακέτα λογισμικού αποτύπωσης εξόδου (Output Plug-ins)

Εντρυφώντας στις παραπάνω φάσεις λειτουργίας του λογισμικού, αξίζει να σημειωθεί ότι χρησιμοποιούνται αρχεία με υπογραφές που ταιριάζουν σε κάποια χαρακτηριστικά μιας συγκεκριμένης επικοινωνίας. Οι υπογραφές του Snort ονομάζονται και κανόνες (Rules), δεδομένου ότι αναλύουν τα στοιχεία ενός πακέτου που ενδέχεται να αποτελεί τμήμα γνωστής κακόβουλης δραστηριότητας, καθώς και την ενέργεια που πρόκειται να εφαρμοστεί προκειμένου για ανίχνευση αυτής. Κάθε

πακέτο που εντοπίζεται από το Snort, ελέγχεται για το αν έχει τα ίδια χαρακτηριστικά με αυτά που περιγράφονται από κάποιο κανόνα. Το Snort επιτρέπει την ενσωμάτωση ξεχωριστών υποπρογραμμάτων στον κώδικά του με κομμάτια κώδικα που ονομάζονται ‘plug-ins’. Τα plug-ins επιτρέπουν την επέκταση των δυνατοτήτων του Snort χωρίς να χρειάζεται αλλαγή το κύριο σώμα του κώδικά του. Τα plug-ins έχουν σαν κύριο στόχο να επεκτείνουν τις δυνατότητες του Snort.

Τα preprocessor plug-ins για παράδειγμα προσθέτουν δυνατότητες ανίχνευσης ανώμαλης συμπεριφοράς. Οι preprocessors είναι σαν μία συμπληρωματική μηχανή του Snort όπου χωρίς αυτούς ορισμένα είδη επιθέσεων δεν θα μπορούσαν να εντοπιστούν. Οι Preprocessors του Snort μπορούν να προσφέρουν την δυνατότητα στο Snort να εντοπίζει ακόμα και επιθέσεις που δεν έχουν γίνει ακόμα κανόνες. Το εν λόγω λογισμικό είναι ενσωματωμένο με περισσότερους από 2500 έτοιμους κανόνες, που υλοποιούνται προκειμένου για εντοπισμό των ήδη γνωστών κακόβουλων ενεργειών. Τέλος, για την ανάπτυξη καινοτόμων κανόνων, το λογισμικό προσφέρει πληθώρα χαρακτηριστικών τα οποία ο χρήστης έχει τη δυνατότητα να αξιοποιήσει και συνεπώς να αυξήσει με αυτό τον τρόπο την ευελιξία του, αναφορικά με τον τρόπο δράσης σε περίπτωση ανίχνευσης μιας εισβολής.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Σύμφωνα με όσα μελετήσαμε παραπάνω, συμπερασματικά, στη σύγχρονη εποχή της συνεχούς εξελισσόμενης τεχνολογίας που βιώνουμε, παρόλο που η αρχιτεκτονική ασφάλειας έχει φτάσει σε πολύ υψηλά επίπεδα, ολοένα και αυξάνονται οι κίνδυνοι και οι απειλές της ασφάλειας των πληροφοριακών συστημάτων, είτε αυτό αποβαίνει επιβλαβές σε προσωπικό επίπεδο, είτε επιφέρει τεράστια πρόκληση ζημιάς σε επιχειρήσεις, εταιρείες, τράπεζες, οργανισμούς κλπ. , πλήττοντας έτσι το κύρος και την αξιοπιστία τους. Η ραγδαία αυτή ανάπτυξη των απειλών καθιστά αναπόφευκτα αναγκαία την εξέλιξη και ενδυνάμωση των Συστημάτων Ανίχνευσης/ Πρόληψης Εισβολών για την αντιμετώπιση αυτών. Πιο συγκεκριμένα, συνδυάζοντας όλη την τεχνογνωσία, εφόσον τα ΣΑΕ από μόνα τους δεν ήταν επαρκή για την αντιμετώπιση του όγκου απειλών-επιθέσεων, με τους μηχανισμούς και πολιτικές ασφαλείας , στόχος είναι να επιτευχθει η μέγιστη βελτίωση του ποσοστού ακρίβειας ορθών προβλέψεων με το να συλλαμβάνονται απειλές για αυτά άγνωστες, εκτός των κανόνων τους και τον προκαθορισμένων μοντέλων τους με σκοπό τη μείωση των ψευδών συναγερμών και του χαμένου πραγματικού χρόνου. Ωστόσο, ένα τέτοιο σύστημα ποτέ δε θα κατέχει τον απόλυτο βαθμό αξιοπιστίας όσο κι αν πληροί τις προϋποθέσεις ασφάλειας σε υψηλά επαρκή βαθμό σε όλα τα επίπεδα.

Βέβαια, είναι επόμενο με την αύξηση των νέων σχεδιαζόμενων απειλών να μην υπάρχει ακόμα το επιθυμητό αποτέλεσμα στον εντοπισμό και παρεμπόδιση αυτών από τα Συστήματα Ανίχνευσης και Πρόληψης Εισβολών. Σαφώς η εμφάνιση των IPS σε συνδυασμό πάντα με τα IDS, αφού τα IPS από μόνα τους δεν υφίστανται, έχει προσφέρει αρκετά κερδοφόρα αποτελέσματα, όχι μόνο στον εντοπισμό αλλά και στην εξουδετέρωση των επιθέσεων, εφόσον έχουν τη δυνατότητα να αντιδράσουν, ακόμα και να αντιπιτεθούν εάν ο χρήστης το επιθυμεί. Τα συστήματα αυτά, έχουν τη δυνατότητα να λειτουργούν, είτε μεμονωμένα, είτε σε μικρά δίκτυα, είτε σε ευρύτερα γεωγραφικά, πολλαπλά δίκτυα, προσφέροντας αρκετά αξιόπιστη προστασία σε πραγματικό χρόνο.

Σα συμπέρασμα που καταλήγουμε εντέλει, από την προκείμενη εργασία, είναι το γεγονός ότι οι τύποι επιθεσεων και τεχνικών εισβολής στα πληροφοριακά συστήματα εξελίσσονται παράλληλα με την τεχνολογία της παρεμπόδισης αυτών, βρίσκοντας πάντα κερκόπορτες και κενά στην ασφάλεια δικτύου οποιουδήποτε επιπέδου χωρίς να υπάρχει κάποιο τέλος στο ‘ανελέητο κυνήγι’ αυτό, κ ίσως να μην υπάρξει ούτε στο μέλλον αφού ακόμη κι αν ο επιτεθέμενος αποτύχει θα εφεύρει νέα εργαλεία. Αναγκαία λοιπόν καθίσταται η σωστή εκμάθηση και άρτια εκπαίδευση-κατάρτηση του εκάστοτε χρήστη, επαγγελματία ή μη ενός υπολογιστικού συστήματος, με στόχο την βέλτιστη αποτελεσματικότερη και άμεση αντίδρασή και συνεπώς πρόληψη εισβολής που γίνεται αντιληπτή από τη χρήση του λογισμικού που διαχειρίζεται ο ίδιος ως γνώστης χρήσης αυτού. Ως επέκταση μελλοντική θα μπορούσε να προταθεί η ευρεία διάδοση και χρήση των Συστημάτων Πρόληψης Εισβολών από τους Δημόσιους φορείς εκπαίδευσης ώστε να γίνεται η κατάλληλη εισαγωγή και εκπαίδευση από μικρή ηλικία προκειμένου να είναι όλοι εξοικειωμένοι με τη χρήση τέτοιων λογισμικών και γνώσης των κανόνων τους καθώς και η παιδεία

πάνω στην πολιτική απορρήτου και κανόνων πρωτοκόλλων που προστατεύουν και διαφυλλάτουν την ακεραιότητα πληροφοριών. Αφού κανένα λογισμικό δεν είναι δυνατό να προσφέρει τη μέγιστη απόδοση ασφάλειας σε ένα δίκτυο , εμείς οι ίδοι οι χρήστες καλούμαστε να συμμορφωνόμαστε με υγιείς συμπεριφορές και συνετή ,σοφή διαχείριση των παροχών της τεχνολογίας.

7 ΒΙΒΛΙΟΓΡΑΦΙΑ

7.1 ΞΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

[1]Ashoor, A., & Gore, S. (2011). Intrusion Detection System (IDS) & Intrusion Prevention System (IPS): Case Study. *International Journal of Scientific and Engineering Research* , σσ. 1-3.

[2]Cannady, J. (1998). Artificial neural networks for misuse detection. *National information systems security conference* , 368-381.

[3]Chakrabarti, S., Mukhopadhyay, I., & Chakraborty, M. (2010). Study of snort-based IDS. *Proceedings of the ICWET '10 International Conference & Workshop on Emerging Trends in Technology* (σσ. 43-47). Mumbai: ICWET 2010.

[4]Cohen, F. (1987). Computer viruses: Theory and experiments. *Computers & Security* , σσ. 22-35.

[5]Denning, D. (1987). An Intrusion-Detection Model. *IEEE Transactions on Software Engineering* , σσ. 222 - 232.

[6]Dowell, C., & Ramstedt, P. (1990). The ComputerWatch Data Reduction Tool. *Proceedings of the 13th National Computer Security Conference* (σσ. 99-108). Washington: IEEE.

[7]Duda, R. O., & Stork, D. G. (2012). *Pattern Classification.* NY: John Wiley & Sons.

[8]Dulanović, N., Hinić, D., & Simić, D. (2008). An Intrusion Prevention System as a Proactive Security Mechanism in Network Infrastucture. *Yugoslav Journal of Operations Research* , σσ. 109-122.

[9]Ghosh, A. K., & Schwartzbard, A. (1999). A Study in Using Neural Networks for Anomaly and Misuse Detection. *Proceedings of the 8th USENIX Security Symposium* (σσ. 141-152). Washington: IEEE.

[10]Hartmann, B., & Symhony, B. (1997). Firewall Software [Data Sheet]. USA.

[11]Hochberg, J., Jackson, K., Stallings, C., McClary, J., DuBois, D., & Ford, J. (1993). NADIR: An automated system for detecting network intrusion and misuse. *Computers & Security* , σσ. 235-248.

[12]Hoglund, A. J., Hatonen, K., & Sorvari, A. S. (2000). A computer host-based user anomaly detection system using the selforganizing map. *Proceedings of the IEEEINNS-ENNS International Joint Conference on Neural Networks* (σσ. 411-416). Finland: IEEE.

[13]Jones, A., & Sielken, R. (2000). Computer System Intrusion Detection: A survey. *Computer Science Technical Report* , σσ. 1-25.

[14]Kruegel, C., Valeur, F., & Vigna, G. (2005). *Intrusion Detection and Correlation - Challenges and Solutions.* Advances in Information Security Springer.

[15]Lankewicz, L., & Benard, M. (1991). Real-time anomaly detection using a nonparametric pattern recognition approach. *Proceedings Seventh Annual Computer Security Applications Conference* (σσ. 80-89). IEEE.

[16]Lichodzijewski, P., Zincir-Heywood, A. N., & Heywood, M. I. (2002). Host-Based Intrusion Detection Using Self-Organizing Maps. *Proceedings of the 2002 International Joint Conference on Neural Networks.* (σσ. 1714-1719). Canada: IEEE.

[17]Lunt, T. (1998). Detecting Intruders in Computer Systems. *Sixh Annual Symposium and Technical Displays on Physical and Electronic Security* (σσ. 17-19).IEEE.

[18]Mitchell, T. M. (1997). *Machine Learning.* NY: McGraw-Hill Science/Engineering/Math.

[19]Mukherjee, B., Heberlein, L., & Levitt, K. (1994). Network intrusion detection. *IEEE Network* , σσ. 26-41.

[20]Northcutt, S., & Novak, J. (2002). *Network Intrusion Detection (3rd Edition).* New Riding Publishing.

[21]Paxson, V. (1998). Bro: A System for Detecting Network Intruders in Real-Time. *Proceedings of the 7th USENIX Security Symposium* (σσ. 2435-2463). Texas: IEEE.

[22]Piper, S. (2016). *IntrusionPrevention Systems for Dummies.* Wiley Publishing Inc.

[23]Ryan, J., Lin, M. J., & Miikkulainen, R. (1998). Intrusion detection with neural networks. *Advances in Neural Information Processing Systems* , σσ. 943-949.

[24]Samuel, A. L. (1959). Some studies in machine learning using the game of checkers. *IBM Journal of Research and Development* , σσ. 210-229.

[25]Scarfone, K., & Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS).* NIST Special Publication 800-94 .

[26]Sebring, M. M., & Whitehurst, R. A. (1988). "Expert Systems in Intrusion Detection: A Case Study. *The 11th National Computer Security Conference.* IEEE.

[27]Snapp, S. R., Brentano, J., Dias, G. V., Goan, T. L., Heberlein, L. T., Ho, C.-l., και συν. (1991). DIDS (distributed intrusion detection system)—motivation, architecture, and an early prototype. *In Proceedings of the 14th National Computer Security Conference* (σσ. 167-176). IEEE.

[28]Theodoridis, S., & Koutroumbas, K. (1999). *Pattern Recognition.* NY: Academic Press.

[29]Vaccaro, H., & Liepins, G. (1989). Detection of anomalous computer session activity. *The 1989 IEEE Symposium on Security and Privacy.* IEEE.

[30]Winkeler, J. (1990). "A UNIX Prototype for Intrusion and Anomaly Detection in Secure Networks. *The Thirteenth National Computer Security Conference* , σσ. 115-124.

[31]Zhang, Y., & Lee, W. (2000). Intrusion detection in wireless ad-hoc networks. *MobiCom '00 Proceedings of the 6th annual international conference on Mobile computing and networking* (σ. MobiCom '00 Proceedings of the 6th annual international conference on Mobile computing and networking). Boston: IEEE.

7.2 ΕΛΛΗΝΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

[32]Γκρίτζαλης, Σ., Κάτσικας, Σ., & Δ. Γκρίτζαλης. (2003). *Ασφάλεια Δικτύων Υπολογιστών.* Αθήνα : Εκδόσεις Παπασωτηρίου.

[33]Κομνηνός, Θ., & Σπυράκης, Π. (2002). *Ασφάλεια Δικτύων & Υπολογιστικών Συστημάτων Αναχαιτίστε τους εισβολείς*. Αθήνα: Εκδόσεις Ελληνικά Γράμματα.

[34]Πάγκαλος, Γ., & Ι. Μαυρίδης. (2002). *Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων*. Θεσσαλονίκη: Εκδόσεις ΑΝΙΚΟΥΛΑ.

[35]Πρίτσος, Δ. (2003). ***SLAB HACK:** Βασικές Έννοιες & Προγραμματισμός του **Snort 2.0**.* Αθήνα: Τεχνολογικό Ιδρυμα Αθήνας.

7.3 ΔΙΑΔΙΚΤΥΟ

[36]Anderson, J. P. (1980). *COMPUTER SECURITY THREAT MONITORING AND SURVEILLANCE*. Ανάκτηση 2018, από Computer Security Resource Center: https://csrc.nist.gov/csrc/media/publications/conferencepaper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ande80.pdf

[37]Google1. (n.d.). *Trojan Horse*. Ανάκτηση από GreekBoston.com: http://www.greekboston.com/culture/mythology/odysseus-trojan-horse/

[38]Google2. (n.d.). *Key Elements Information Security*. Ανάκτηση 2018, από InfosecInstitute.com: https://resources.infosecinstitute.com/key-elements-information-security-policy/

[39]Google3. (n.d.). *Ενοποιημένες Λύσεις Ασφάλειας Πληροφοριακών Συστημάτων*. Ανάκτηση 2018, από Netbull.gr: http://www.netbull.gr/default.aspx?lang=el-GR&page=2

[40]Google4. (n.d.). *Διαφορά Hacker- Cracker*. Ανάκτηση 2018, από Coolweb.gr: http://coolweb.gr/diafora-hacker-cracker

[41]Google5. (n.d.). *MAN IN THE MIDDLE (MITM) ATTACK*. Ανάκτηση 2018, από Incapsula.com: https://www.incapsula.com/web-application-security/man-in-the-middle-mitm.html

[42]Google6. (n.d.). *Introduction to Anomaly Detection: Concepts and Techniques*. Ανάκτηση 2018, από Wordpress.com.

https://iwringer.wordpress.com/2015/11/17/anomaly-detection-concepts-and-techniques/

[43Google7. (n.d.). *Intrusion Detection in Wireless Ad-Hoc Networks*. Ανάκτηση 2018, από SemanticcSholar.org: https://pdfs.semanticscholar.org/4613/90a85d48b8b37f625d7788b8dab0e044637d.pdf

[44]Google8. (n.d.). *ΚΕΦΑΛΑΙΟ 4 - Μηχανική Μάθηση*. Ανάκτηση 2018, από Kallipos.gr: http://repfiles.kallipos.gr/html_books/93/04a-main.html

[45]Google9. (n.d.). *Συστήματα Ανίχνευσης Εισβολών*. Ανάκτηση 2018, από Evdoxos.unipi.gr: https://evdoxos.ds.unipi.gr/modules/document/file.php/DS168/BOOK_NetSec_08_IntrusionDetectSys.pdf

[46]Kohlenberg, T. (2007). *Snort IDS and IPS Toolkit.* Ανάκτηση 2018, από Syngress: http://index-of.es/Networking/Snort%20IDS%20and%20IPS%20Toolkit.pdf

[47]Sukhai, N. B. (2005). *Hacking And Cybercrime* . Ανάκτηση 2018, από CiteSeerX: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.470.3895&rep=rep1&type=pdf