Πανεπιστήμιο Πειραιώς

Τμήμα Ψηφιακών Συστημάτων

Μεταπτυχιακό Πρόγραμμα Σπουδών

Τεχνοοικονομίκη Διοίκηση & Ασφάλεια Ψηφιακών Συστημάτων

Κατεύθυνση: Ασφάλεια Ψηφιακών Συστημάτων

Μεταπτυχιακή Διπλωματική Εργάσια: Συστηματα Ανίχνευσης Εισβολών σε Περιβάλλον Υπολογιστικού Νέφους

Παντελής Σκαμάγκας ΜΤΕ 1130

Επιβλέπων : Λαμπρινουδάκης Κωνσταντίνος

Ακαδημαϊκό Έτος 2012-2013

Ευχαριστίες

Θα ήθελα να ευχαριστήσω ιδιαίτερα τον καθηγητή μου κ. Λαμπρινουδάκη Κωνσταντίνο για την άψογη συνεργασία που είχα μαζί του.

Ευχαριστώ, επίσης, όλους τους ακαδημαϊκούς του μεταπτυχιακού προγράμματος για την προσφορά των γνώσεών τους στο πεδίο της ασφάλειας των ψηφιακών συστημάτων.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένειά μου για την συμπαράσταση και τη στήριξή της κατά τη διάρκεια των σπουδών μου.

Περίληψη

Η τεχνολογία του cloud computing, αν και σχετικά νέα, συναντά μεγάλη ανταπόκριση και από πλευράς Οργανισμών, αλλά και από την πλευρά των απλών χρηστών. Επειδή είναι νέα τεχνολογία, συναντά πολλές φορές διάφορες δυσκολίες. Μία από αυτές είναι και το θέμα της ασφάλειας. Μένει, λοιπόν, να δούμε αν οι παραδοσιακοί τρόποι ασφάλειας μπορούν να προστατεύσουν εταιρείες και χρήστες που χρησιμοποιούν ένα τέτοιο περιβάλλον. Σε αυτή την εργασία θα εφαρμόσουμε ένα δικτυακό εργαλείο ανίχνευσης εισβολών ως παραδοσιακό τρόπο ασφάλειας σε ένα περιβάλλον cloud και θα δούμε εάν μπορεί να ανταπεξέλθει στις απαιτήσεις ενός τέτοιου περιβάλλοντος.

Abstract

Cloud computing technology is somewhat new, and used by many businesses and users. The fact that this technology is new, results into having numerous challenges, including security. We need to see if traditional ways of securing a system are capable of protecting organizations and users of the cloud environment. We will use a network intrusion detection system in order to see if it is capable of that purpose.

Λίστα Ακρωνυμίων

NIST – National Institute of Standard and Technology

ACL – Access Control Lists

IDS- Intrusion Detection System

NIDS - Network-based Intrusion Detection System

HIDS – Host-based Intrusion Detection Systems

CCDC - Cloud Computing Data Center

LC - local controllers

LIDB- Local Intrusion Data Base

LA- local analyzer

GIDB- Global Intrusion Data Base

DIDS- distributed intrusion detection system

IDMEF- Intrusion Detection Message Exchange Format

TCP – Transmition control protocol

DOS – Denial of service

Περιεχόμενα

1. Εισαγωγή

Η τεχνολογία του Cloud Computing έχει επιτυχημένα διαφημιστεί ως το πιο αναπτυσσόμενο μοντέλο υπηρεσίας στο διαδίκτυο. Πολλοί πάροχοι μεγάλης κλίμακας, όπως η IBM [1] και η Amazon [2], μοιράζουν τα κέντρα δεδομένων τους μέσω ενός σχεδίου εικονικών υπηρεσιών για ευρεία κατανάλωση των υπολογιστικών τους πόρων. Ως αποτέλεσμα, οι χρήστες του cloud μπορούν να μετριάσουν τα έξοδά τους και να αυξήσουν τη διαθεσιμότητα των υπηρεσιών που βρίσκονται στο cloud.

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST – National Institute of Standard and Technology) ορίζει την τεχνολογία του Cloud Computing ως ένα μοντέλο που δίνει εύκολη δικτυακή πρόσβαση σε διαμοιραζόμενους υπολογιστικούς πόρους (π.χ. δίκτυα, εφαρμογές, αποθηκευτικό χώρο και υπηρεσίες) με την ελάχιστη προσπάθεια διαχείρισης.

Με τον αυξανόμενο ρυθμό επιθέσεων εναντίον των μέσων κοινωνικής δικτύωσης και μεγάλων διαδικτυακών επιχειρήσεων, οι οργανισμοί προβληματίζονται για την ασφάλεια της υπολογιστικής τους περιουσίας σε περίπτωση που την μετακινήσουν στο cloud [3].

Οι παραδοσιακοί μηχανισμοί ασφάλειας αντιμετωπίζουν νέες δυσκολίες στο cloud, όπως εισβολές σε εικονικές μηχανές και κακόβουλες ενέργειες χρηστών. Αυτή τη στιγμή οι πάροχοι υπηρεσιών cloud εφαρμόζουν κρυπτογράφηση δεδομένων για υπηρεσίες αποθήκευσης, εικονικά firewalls και λίστες ελέγχου πρόσβασης (ACL – Access Control Lists).

Ένας από αυτούς τους παραδοσιακούς μηχανισμούς είναι η χρήση εργαλείων ανίχνευσης εισβολών (IDS- Intrusion Detection System). Αυτά τα εργαλεία ασφάλειας είναι ζωτικά για την ασφάλεια πολλών δικτυακών υποδομών. Ελέγχουν την κίνηση του δικτύου για το σύστημα που παρακολουθείται, ώστε να ανιχνεύσουν απειλές ασφάλειας. Ο ορισμός μιας απειλής έχει να κάνει είτε με λογικούς κανόνες γνωστών επιθέσεων ή ως την απόκλιση της

συμπεριφοράς ενός συστήματος από αυτή που θεωρείται φυσιολογική. Εάν η κίνηση του δικτύου και ο ορισμός μιας απειλής ταιριάζουν, τότε δημιουργείται μια ειδοποίηση. Έπειτα ο διαχειριστής ασφάλειας του συστήματος λαμβάνει δράση βασισμένη σε ένα προκαθορισμένο σχέδιο δράσης. Γενικά, αποθηκεύονται οι πληροφορίες του συστήματος για περαιτέρω ανάλυση αργότερα.

1.1 Στόχος διπλωματικής εργασίας

Ο στόχος της έρευνας σε αυτή τη διπλωματική εργασία έχει να κάνει με την εφαρμογή ενός δικτυακού IDS σε ένα περιβάλλον cloud και πώς αυτό ανταποκρίνεται σε επιθέσεις που ξεκινούν από μία εικονική μηχανή μέσα στο cloud και έχουν ως στόχο άλλες εικονικές μηχανές. Στο πλαίσιο, λοιπόν, αυτής της εργασίας θα προσομοιωθούν διαφόρων τύπων επιθέσεις και θα εξετάσουμε εάν το IDS, όντας παραδοσιακός μηχανισμός ασφάλειας, μπορεί να χρησιμοποιηθεί, επιτυχημένα, σε ένα τέτοιο περιβάλλον ανιχνεύοντας αυτές τις επιθέσεις ή οποιαδήποτε άλλη ασυνήθιστη συμπεριφορά του συστήματος.

2 . Cloud Computing

Σε αυτό το κεφάλαιο δίνουμε μια γενική περιγραφή για τα μοντέλα, τις κατηγορίες και τα κύρια χαρακτηριστικά του Cloud Computing. Επίσης θα δούμε θέματα ασφάλειας και απειλές στο Cloud.

2.1 Ορισμός

Η νεφοϋπολογιστική (cloud computing), είναι αρκετά δύσκολο να οριστεί και αυτό διότι εξελίσσεται διαρκώς, με αποτέλεσμα να αλλάζουν κάθε φορά και τα χαρακτηριστικά της. Σε αυτή την ενότητα θα προσπαθήσουμε να την ορίσουμε περιγραφικά, παραθέτοντας τον ορισμό του NIST (National Institute of Standards Technology) [4] καθώς και τα κύρια χαρακτηριστικά της.

Ο συγκεκριμένος ορισμός ξεκινάει με δύο σημειώσεις. Αρχικά υπογραμμίζει ότι το «νέφος» εξελίσσεται διαρκώς. Ορισμοί που σχετίζονται με αυτό, περιπτώσεις χρήσεις, υποκείμενες τεχνολογίες, κίνδυνοι και οφέλη θα τελειοποιηθούν μέσα από διάλογο με δημόσιους και ιδιωτικούς φορείς. Αυτοί οι ορισμοί και τα χαρακτηριστικά θα αλλάζουν και θα εξελίσσονται με την πάροδο του χρόνου. Ενώ έπειτα σημειώνει ότι, η βιομηχανία του «νέφους» αντιπροσωπεύει ένα μεγάλο σύστημα από πολλά μοντέλα, πωλητές – κατασκευαστές και εξειδικευμένα τμήματα αγοράς. Ο παρών ορισμός προσπαθεί να συμπεριλάβει τις ποικίλες προσεγγίσεις του cloud.

Το cloud αποτελεί, λοιπόν, ένα μοντέλο που επιτρέπει την κατά-ζήτηση (on-demand) πρόσβαση μέσω δικτύου σε μια κοινόχρηστη δεξαμενή διαμορφώσιμων υπολογιστικών πόρων (δίκτυα, εξυπηρετητές, μνήμη, εφαρμογές και υπηρεσίες) που μπορούν να προσφερθούν με ελάχιστη προσπάθεια διαχείρισης ή αλληλεπίδραση με τον πάροχο της υπηρεσίας. Αυτό το μοντέλο προωθεί την διαθεσιμότητα, και αποτελείται από πέντε απαραίτητα χαρακτηριστικά, τρία μοντέλα υπηρεσιών και τέσσερα μοντέλα ανάπτυξης.

2.2 Χαρακτηριστικά

Κατά-ζήτηση αυτό-εξυπηρέτηση (on-demand self-service): Ο χρήστης μπορεί μονομερώς να χρησιμοποιεί υπολογιστικούς πόρους, όπως το χρόνο του εξυπηρετητή και αποθηκευτικούς πόρους δικτύου αυτόματα, ανάλογα με τις ανάγκες του, χωρίς να απαιτείται διάδραση με τον εκάστοτε πάροχο της συγκεκριμένης υπηρεσίας.

Ευρεία δικτυακή πρόσβαση (ubiquitous network access) : Οι πόροι είναι διαθέσιμοι μέσα από το δίκτυο στο οποίο μπορεί κανείς να έχει πρόσβαση μέσα από γνωστούς μηχανισμούς, οι οποίοι προωθούν την χρήση ετερογενών τερματικών συσκευών στην πλευρά του τελικού χρήστη (όπως έξυπνα τηλέφωνα, φορητοί υπολογιστές κτλ.).

Διάθεση των πόρων (resource pooling) : Οι υπολογιστικοί πόροι του παρόχου είναι συγκεντρωμένοι έτσι ώστε να μπορούν να εξυπηρετήσουνε παράλληλα πολλούς πελάτες χρησιμοποιώντας το μοντέλο πολλών-χρηστών (multi-tenant), με διαφορετικούς φυσικούς και εικονικούς πόρους να έχουν αντιστοιχηθεί δυναμικά ανάλογα με την ζήτηση του κάθε πελάτη. Ο χρήστης δε έχει τον έλεγχο ή την γνώση για την ακριβή τοποθεσία των παρεχόμενων πόρων, αλλά μπορεί να έχει την δυνατότητα να καθορίσει σε σχετικά αφηρημένο επίπεδο την ακριβή τοποθεσία (όπως χώρα, περιοχή κτλ.). Οι πόροι μπορεί να είναι αποθηκευτικός χώρος, υπολογιστική ισχύ, μνήμη, εύρος ζώνης και εικονικές μηχανές (virtual machines).

Ταχεία ελαστικότητα (rapid elasticity) : Οι πόροι αυτοί μπορούν με πολύ ευέλικτο τρόπο να αυξηθούν πολύ γρήγορα, σε πολλές περιπτώσεις με αυτόματο τρόπο, έτσι ώστε να μην υπάρχει διάδραση με τον πάροχο της συγκεκριμένης υπηρεσίας, με σκοπό την παράκαμψη χρονοβόρων διαδικασιών.

Μετρούμενη υπηρεσία (measured service) : Τα cloud συστήματα έχουν την δυνατότητα αυτόματα να ελέγχουν και να βελτιώνουν τους διαθέσιμους πόρους χρησιμοποιώντας ένα μηχανισμό μέτρησης, ανάλογα με τον τύπο της προσφερόμενης υπηρεσίας. Οι χρησιμοποιούμενοι πόροι μπορούν να ελέγχονται και να παρακολουθούνται χωρίς να γίνονται αντιληπτοί τόσο στον πάροχο όσο και στον χρήστη της χρησιμοποιούμενης υπηρεσίας.

Ελαστική επεκτασιμότητα (elastic scalability) : Οι χρήστες του Cloud έχουν τη δυνατότητα να τροποποιούν το μέγεθος των πόρων που χρησιμοποιούν, ανάλογα με τις εκάστοτε απαιτήσεις. Έτσι, οι χρήστες που χρειάζονται να επεξεργαστούν μεγάλο όγκο δεδομένων, μπορούν να μοιράζουν σε κομμάτια αυτά τα δεδομένα και στη συνέχεια τα κομμάτια αυτά θα μοιραστούν σε πολλαπλές διεργασίες, τις οποίες θα διαχειριστούν πόροι στο Cloud.

Υψηλή διαθεσιμότητα (high availability) : Για ένα σύνθετο περιβάλλον, όπως το Cloud, όπου υπάρχει μεγάλος αριθμός εικονικών πόρων, υπάρχει και η ανάγκη για μία σταθερή και προσβάσιμη υπηρεσία. Το Cloud υπόσχεται προσβασιμότητα ακόμη και αν διακοπεί η λειτουργία κάποιων πόρων. Για παράδειγμα, μπορεί να διακοπεί η λειτουργία κάποιων υπηρεσιών για κάποιο αριθμό χρηστών, αλλά συνολικά το σύστημα συνεχίζει να λειτουργεί για μια άλλη ομάδα χρηστών.

Υπηρεσία βασισμένη στη χρησιμότητα **(utility-based service)**: Οι χρήστες του Cloud “πληρώνουν ό,τι χρησιμοποιούν”. Τα κόστη του κτισίματος ενός server, της πρόσληψης διαχειριστή συστήματος και της εγκατάστασης διαφόρων αναγκαίων εφαρμογών είναι ελάχιστα. Επιπλέον, οι πάροχοι του Cloud μπορούν να ειδοποιήσουν τους χρήστες εάν υπερβούν κάποιο όριο επεξεργασίας δεδομένων ή χρόνου χρήσης της υπηρεσίας.

2.3 Μοντέλα Υπηρεσιών

Νέφος λογισμικού ως μια υπηρεσία (Cloud Software as a Service, SaaS) : Η δυνατότητα που παρέχεται στον χρήστη είναι να μπορεί να χρησιμοποιήσει τις εφαρμογές του παρόχου σε μια υποδομή «νέφους». Οι εφαρμογές είναι προσβάσιμες μέσα από διεπαφές ή εργαλεία όπως οι φυλλομετρητές διαδικτύου (web browsers). Ο χρήστης δεν έχει την δυνατότητα να διαχειρίζεται ή να ελέγχει την υποδομή που μπορεί να αποτελείται από το δίκτυο, τους εξυπηρετητές, λειτουργικά συστήματα, αποθηκευτικοί χώροι ή ακόμα και ειδικές δυνατότητες εφαρμογής για τον συγκεκριμένο χρήστη. Ένα τέτοιο παράδειγμα είναι η εφαρμογή του ηλεκτρονικού ταχυδρομείου (e-mail). Ο τελικός χρήστης δεν χρειάζεται να κατανοήσει και να μπορεί να υποστηρίζει την φιλοσοφία της υπηρεσίας αλλά μόνο να μπορεί να τη χρησιμοποιήσει μέσα από τη διεπαφή που διαθέτει (πχ. ενός φυλλομετρητή).

Νέφος πλατφόρμας ως μια υπηρεσία (Cloud Platform as a Service, PaaS): Το συγκεκριμένο μοντέλο, προσφέρει στον καταναλωτή τη δυνατότητα να αναπτύξει πάνω στην δομή του «νέφους», εφαρμογές ή και αποκτηθείσες εφαρμογές χρησιμοποιώντας γλώσσες προγραμματισμού και εργαλεία που υποστηρίζονται από τον πάροχο. Ο καταναλωτής δεν διαχειρίζεται ή ελέγχει την υποκείμενη υποδομή, συμπεριλαμβανομένου του δικτύου, των εξυπηρετητών, των λειτουργικών συστημάτων και της μνήμης, αλλά έχει τον έλεγχο στις αναπτυσσόμενες εφαρμογές και πιθανώς σε εφαρμογές που φιλοξενούν διαμορφώσεις περιβάλλοντος.

Νέφος υποδομής ως μια υπηρεσία (Cloud Infrastructure as a Service, IaaS) : Αναφέρεται στην δυνατότητα που παρέχεται στο χρήστη να έχει τον έλεγχο βασικών υπολογιστικών πόρων και εφαρμογών. Ο χρήστης της υπηρεσίας δεν έχει την δυνατότητα να ελέγχει την υποδομή του «νέφους», αλλά έχει την δυνατότητα να ελέγχει το λειτουργικό σύστημα, τον αποθηκευτικό χώρο, καθώς επίσης και τις αναπτυσσόμενες εφαρμογές και πιθανόν να έχει και περιορισμένο έλεγχο σε κάποιους διαδικτυακού πόρους, όπως για παράδειγμα σε τοίχο προστασίας (firewall).

2.4 Μοντέλα Ανάπτυξης

Ιδιωτικό «νέφος» (private cloud) : Η υποδομή του «νέφους» λειτουργεί αποκλειστικά για έναν οργανισμό. Μπορεί να διαχειρίζεται από τον ίδιο τον οργανισμό ή από κάποιον τρίτο και μπορεί να βρίσκεται στις κτηριακές υποδομές του οργανισμού. Σε αντίθεση με το δημόσιο «νέφος», το ιδιωτικό είναι εσωτερικά φιλοξενούμενο. Η σφραγίδα ενός ιδιωτικού «νέφους», συνήθως αφιερώνεται σε οργανισμούς. Οι οργανισμοί στην προσπάθεια να αναπτύξουν το ιδιωτικό «νέφος», εφαρμόζουν εικονοποίηση μέσα στα δικά τους κέντρα δεδομένων. Αν και τα ιδιωτικά «νέφη» είναι ικανοποιητικά, κάποιες από τις ανησυχίες ασφάλειας που ισχύουν στα δημόσια δεν ισχύουν. Ακριβώς όμως επειδή είναι ιδιωτικά δε σημαίνει ότι είναι και πιο ασφαλή. Στο ιδιωτικό «νέφος», εκτιμήσεις όπως εξασφάλιση του εικονικού περιβάλλοντος (που είναι το λογισμικό και το φυσικό υλικό) γίνονται από τον πελάτη, εν αντίθεση με το το δημόσιο, που όλα τα αναλαμβάνει ο πάροχος υπηρεσίας. Κατά συνέπεια, σε συγκρίσεις του ιδιωτικού με το κοινό «νέφος», είναι δύσκολο να κάνουν γενικεύσεις για το πιο είναι ασφαλέστερο από τα δύο. Ένα ιδιωτικό «νέφος» προσφέρει τη δυνατότητα να επιτύχουμε μεγαλύτερη ασφάλεια. Το πραγματικό πλεονέκτημα ενός ιδιωτικού «νέφος» είναι ότι ο πάροχος έχει το ενδιαφέρον για να κάνει το περιβάλλον της διεπαφής να βρίσκεται περισσότερο κοντά στις ανάγκες του εκμισθωτή.

Κοινοτικό «νέφος» (community cloud) : Η υποδομή του «νέφους» είναι διαμοιρασμένη σε διάφορους οργανισμούς και υποστηρίζει προκαθορισμένες κοινότητες που μπορεί να έχουν κοινές απαιτήσεις, σε επίπεδο ασφάλειας, λειτουργικότητας, αποστολής. Μπορεί να διαχειρίζεται είτε από έναν οργανισμό είτε από κάποιον εξωτερικό πάροχο και μπορεί να βρίσκεται στις κτηριακές υποδομές του οργανισμού. Η υπόσχεση του κοινοτικού «νέφους» είναι ότι επιτρέπει πολλαπλές ανεξάρτητες οντότητες να συνυπάρχουν.

Δημόσιο «νέφος» (public cloud) : Η υποδομή του «νέφους» μπορεί να είναι διαθέσιμη στο κοινό ή σε μια μεγάλη ομάδα από οργανισμούς/επιχειρήσεις και να ανήκει σε έναν οργανισμό που διαχειρίζεται υπηρεσίες «νέφους». Στην απλούστερη εκδοχή του ένα δημόσιο «νέφος» είναι διαθέσιμο εξωτερικά στον

τελικό χρήση με μικρό περιορισμό για το ποιός μπορεί να γίνει χρήστης της υπηρεσίας με πληρωμή. Οι πιο κοινές μορφές του δημόσιου «νέφους», είναι αυτές που είναι προσβάσιμες μέσω του διαδικτύου. Τα τελευταία χρόνια έχει υπάρξει τεράστια ανάπτυξη του δημόσιου «νέφους», με αποτέλεσμα νε υπάρχει μεγάλη προσφορά σε υπηρεσίες Iasi από εταιρίες, όπως η Amazon με την υπηρεσίας EC2 και την IBM Blue Cloud. Άλλες μορφές προσφοράς δημόσιου «νέφους», σε υπηρεσίες PaaS γίνονται από την Google με το AppEngine και το Windows Azure, από την Microsoft. Στο βασικό επίπεδο, το δημόσιο «νέφος», έχει μοναδικά στοιχεία ασφάλειας και κριτήρια αξιολόγησης σε σχέση με το ιδιωτικό cloud. Το δημόσιο cloud, επίσης, μπορεί να διαμορφωθεί από τους παρόχους υπηρεσιών που θέλουν μια υποδομή μεγάλης δυναμικότητας και ένα ευρύ φάσμα πελατών. Ως αποτέλεσμα τα δεδομένα μπορούν να αποθηκευτούν σε κοινά μέσα αποθήκευσης, κάτι που καθιστά απαραίτητη την κωδικοποίηση των δεδομένων για μεγαλύτερη ασφάλεια.

Υβριδικό «νέφος» (hybrid cloud) : Η υποδομή του hybrid cloud είναι μια σύνθεση δύο ή περισσοτέρων «νεφών» (ιδιωτικό, κοινοτικό ή δημόσιο) που παραμένουν μοναδικές οντότητες, αλλά συνδέονται μεταξύ τους με τυποποιημένη ή ιδιόκτητη τεχνολογία που επιτρέπει φορητότητα σε δεδομένα και εφαρμογές.

3. Θέματα ασφάλειας στο Cloud Computing

3.1 Εισαγωγή

Η ασφάλεια αποτελεί αναγκαία συνθήκη και είναι απαραίτητη, σε συνδυασμό με τις άλλες βασικές προϋποθέσεις λειτουργίας όπως η ποιότητα και η απόδοση, για την εξασφάλιση της καλής λειτουργίας μιας επιχείρησης ή ενός οργανισμού. Η έννοια της ασφάλειας ενός Δικτύου Υπολογιστών σχετίζεται με την ικανότητα μιας επιχείρησης ή ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Σχετίζεται επίσης με την ικανότητά του να παρέχει ορθές και αξιόπιστες πληροφορίες, οι οποίες είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες κάθε φορά που τις αναζητούν. Η ικανότητα αυτή στηρίζεται στη λήψη μέτρων τα οποία διασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, καθώς και την συνεχή λειτουργία του δικτύου.

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

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

Εμπιστευτικότητα: Εμπιστευτικότητα σημαίνει πρόληψη μη εξουσιοδοτημένης αποκάλυψης πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη

ανάγνωση. Επομένως, σημαίνει ότι τα δεδομένα που διακινούνται μεταξύ των υπολογιστών ενός δικτύου, αποκαλύπτονται μόνο σε εξουσιοδοτημένα άτομα. Αυτό αφορά όχι μόνο την προστασία από μη εξουσιοδοτημένη αποκάλυψη των δεδομένων αυτών καθαυτών αλλά ακόμη και από το γεγονός ότι τα δεδομένα απλώς υπάρχουν. Έτσι για παράδειγμα, το γεγονός ότι κανείς έχει φάκελο εγκληματία είναι συχνά το ίδιο σημαντικό όπως και οι λεπτομέρειες για το έγκλημα που διαπράχθηκε. Άλλες εκφάνσεις της εμπιστευτικότητας είναι: Η ιδιωτικότητα, προστασία των δεδομένων προσωπικού χαρακτήρα, δηλαδή αυτών που αφορούν συγκεκριμένα πρόσωπα και η μυστικότητα, προστασία των δεδομένων που ανήκουν σε έναν οργανισμό ή μια επιχείρηση.

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

Μη αποποίηση της ευθύνης: Μη αποποίηση της ευθύνης σημαίνει ότι ένας χρήστης δεν μπορεί να αρνηθεί την εκτέλεση μιας λειτουργίας, και κανένα από τα συναλλασσόμενα μέρη δεν έχει την δυνατότητα να αρνηθεί την συμμετοχή του σε μια συναλλαγή.

Εξουσιοδότηση: Η εξουσιοδότηση περιλαμβάνει τον έλεγχο πρόσβασης σε συγκεκριμένες πληροφορίες και υπηρεσίες όταν η ταυτότητα του χρηστή εξακριβωθεί. Η εξουσιοδότηση στην ουσία περιορίζει τις ενέργειες ή τις λειτουργίες που τα εξουσιοδοτημένα μέλη μπορούν να πραγματοποιήσουν, όπως για παράδειγμα εκτέλεση συναλλαγών, μεταφορά χρημάτων από ένα λογαριασμό σε άλλο ή αύξηση του πιστωτικού ορίου κάποιου πελάτη.

Αυθεντικοποίηση: Η διαδικασία της αυθεντικοποίησης αποσκοπεί στην εξακρίβωση της ταυτότητας, την οποία ισχυρίζεται ότι έχει ένας πελάτης της εφαρμογής. Όσον αφορά λοιπόν την ασφάλεια, θα την χωρίσουμε σε δύο υπό-

ενότητες. Η πρώτη ασχολείται με θέματα ασφάλειας που προκύπτουν από την παροχή υπηρεσιών από τρίτους, ενώ η δεύτερη εστιάζει σε σύγχρονους κινδύνους διάθεσης υπηρεσιών cloud computing.

3.2 Παροχή υπηρεσιών από τρίτους

Η παροχή “outsourced” υπηρεσιών υφίσταται εδώ και πολλά χρόνια ως επιχειρησιακή και λειτουργική διαδικασία η οποία έχει μελετηθεί εκτενώς ενώ οι όποιοι εγγενείς κίνδυνοι υπάρχουν, έχουν αναλυθεί και αναγνωρισθεί από τους ειδικούς ασφάλειας. Είναι προφανές ότι η πλειοψηφία αυτών των απειλών, αφορούν τη διακύβευση της εμπιστευτικότητας και ακεραιότητας ανάμεσα στις σχέσεις του πελάτη και του παρόχου. Ωστόσο δεν απουσιάζουν και κίνδυνοι οι οποίοι έχουν να κάνουν με το βαθμό διάθεσης της υπηρεσίας. Μερικοί κίνδυνοι από το σύνολο των εγγενών απειλών της παροχής υπηρεσιών από “third party” εταιρείες παρουσιάζονται παρακάτω:

- Διαφωνίες σχετικά με την απόδοση ευθύνης σε περιπτώσεις περιστατικών ασφάλειας.
- Αδυναμία του παρόχου να ευθυγραμμίσει τις διαδικασίες του με την πολιτική ασφάλειας του πελάτη.
- Η υφιστάμενη υπηρεσία που παρέχεται δεν συμβαδίζει με τις λειτουργικές απαιτήσεις του πελάτη.
- Η υφιστάμενη υπηρεσία που παρέχεται δεν ανταποκρίνεται στις επιχειρησιακές προσδοκίες του πελάτη.
- Κενά ανάμεσα στους επιχειρησιακούς στόχους και τις πολιτικές Πληροφοριακών Συστημάτων.
- Διαφορές στον τρόπο αναγνώρισης και επίλυσης περιστατικών ασφάλειας
- Ανεπαρκής αναγνώριση βελτίωσης των λειτουργιών
- Αυξημένη εξάρτηση του πελάτη από υπαλλήλους "κλειδιά" του παρόχου της υπηρεσίας.
- Η γνώση και η εμπειρία που αποκτάται κατά τη διάθεση της υπηρεσίας, παραμένει στον πάροχο.

- Ανεπάρκεια ικανοτήτων, γνώσεων και πόρων με αποτέλεσμα η διακύβευση κρίσιμων επιχειρησιακών έργων.

3.3 Κίνδυνοι στο Cloud

Μέχρι αρκετά πρόσφατα, η αναγνώριση και ανάλυση των κινδύνων που αφορούν τις υπηρεσίες Cloud, γινόταν αποκλειστικά βάσει προτύπων που είχαν να κάνουν με την ανάληψη/διάθεση “outsourced” υπηρεσιών. Ωστόσο, τα ελκυστικά οικονομικά οφέλη του *Cloud Computing*, δεν άργησαν να το καθιερώσουν ως μία ξεχωριστή τεχνολογική μορφή διάθεσης υπολογιστικών υπηρεσιών. Ταυτόχρονα τα θέματα ασφάλειας που το πλαισιώνουν τέθηκαν υπό ξεχωριστό πρίσμα μελέτης βάσει της δυναμικότητάς του *Cloud Computing* και των τεχνολογιών που αξιοποιούνται για την ασφαλή λειτουργία και εκμετάλλευση των υπηρεσιών και των πόρων αντίστοιχα.

Στο σημείο αυτό θα αναλυθούν μερικές από τις σημαντικότερες απειλές που προκύπτουν από τη διάθεση υπηρεσιών νέφους, έτσι όπως έχουν εντοπιστεί και αναγνωρισθεί καθώς και οι σχετικές προτάσεις υλοποίησης αντιμέτρων [5] [6] [7] [8].

3.3.1 Εσωτερικές Απειλές

Η απειλή για κακόβουλες επιθέσεις από το εσωτερικό είναι πάντα πιθανή και μπορεί να αφορά όλα τα μοντέλα υπηρεσιών που θίξαμε σε παραπάνω ενότητα. Οι insiders, δεν αναφέρονται αποκλειστικά και μόνο στους υπαλλήλους μιας επιχείρησης, αλλά σε οποιοδήποτε εργάζεται με τον έναν ή με τον άλλον τρόπο στην επιχείρηση. Για παράδειγμα μπορεί να αφορά τους συμβούλους της επιχείρησης, τους συνεταίρους κτλ. Οι επιθέσεις αυτές συμβαίνουν όταν ένας εξουσιοδοτημένος χρήστης πραγματοποιεί ενέργειες οι οποίες δεν συμπεριλαμβάνονται στις αρμοδιότητές του. Το φαινόμενο αυτό γίνεται πιο εμφατικό όταν δεν έχει ξεκαθαριστεί εντός της επιχείρησης ο ρόλος και οι αρμοδιότητες για τον κάθε εργαζόμενο. Οι πιθανές αιτίες για μια τέτοιου

είδους επίθεση μπορεί να είναι τρεις. Αρχικά μπορεί να συμβεί τυχαία, εξαιτίας κάποιου ακούσιου λάθους ενός εργαζομένου. Επιπλέον, όταν ένα άτομο προσπαθεί να κάνει κάτι που βρίσκεται εντός του αντικειμένου της δουλειάς του, αλλά δεν έχει το προνόμιο να το κάνει. Τέλος, μπορεί να συμβεί από ηθελημένη κακόβουλη επίθεση. Σε αυτή την περίπτωση ο insider προσπαθεί να αποκτήσει πρόσβαση σε δεδομένα, για τα οποία δεν έχει καμία εξουσιοδότηση. Στις περιπτώσεις αυτές, αντιλαμβανόμαστε την επίθεση εκ των υστέρων. Το πρόβλημα και ταυτόχρονα η πρόκληση σε αυτού του είδους την επίθεση πηγάζει από το γεγονός ότι τις περισσότερες φορές δεν είναι σαφές τι εννοούμε με τον όρο φυσιολογική συμπεριφορά του εργαζομένου, ποιες ενέργειες είναι μη φυσιολογικές, και πότε ένα άτομο πραγματοποιεί ενέργεια για την οποία δεν έχει εξουσιοδότηση. Επιπλέον τίθεται στο προσκήνιο ένα θέμα που αφορά τον τρόπο επιλογής των εργαζομένων. Διότι αν αυτός είναι χαλαρός, τότε μπορεί κάλλιστα να αποτελέσει ευκαιρία για έναν κακόβουλο ώστε να οργανώσει μία στοχευόμενη επίθεση εναντίον ενός συγκεκριμένου πελάτη του παρόχου με ελάχιστη ή ανύπαρκτη πιθανότητα εντοπισμού.

Οι πιθανότητες για τους πελάτες του cloud αυξάνονται, διότι είναι συγκεντρωμένοι σε έναν πάροχο χωρίς να είναι σίγουροι για την πλήρη εφαρμογή των πρωτόκολλων ασφάλειας και για των έλεγχο των ατόμων που έχουν φυσική πρόσβαση στα δεδομένα τους. Για την ακρίβεια, ο πάροχος εάν δεν του ζητηθεί, δεν πρόκειται να αποκαλύψει στους πελάτες του τη διαδικασία με την οποία αποκτούν φυσική ή λογική πρόσβαση οι εργαζόμενοί του στους πληροφοριακούς πόρους που παρέχει, τη διαδικασία επίβλεψης του προσωπικού του ή τον τρόπο με τον οποίο ελέγχει εάν οι πολιτικές του τηρούνται.

Ο αντίκτυπος μιας τέτοιας επίθεσης είναι αρκετά αξιοσημείωτος, δεδομένου ότι δίνεται η δυνατότητα πρόσβασης και αλλαγής στα αρχεία ενός οργανισμού. Αυτό, με τη σειρά του μπορεί να επιφέρει ως αποτέλεσμα την δυσφήμηση του οργανισμού, οικονομικές επιπτώσεις και πολλά άλλα. Καθώς λοιπόν οι οργανισμοί υιοθετούν την νέα τεχνολογία του cloud computing, το ανθρώπινο στοιχείο αποκτάει όλο και μεγαλύτερη βαρύτητα. Για αυτό το λόγο επιβάλλεται οι πελάτες των υπηρεσιών νέφους να έχουν πλήρη επίγνωση των μεθόδων

μέσω των οποίων οι πάροχοι ανιχνεύουν και αμύνονται εναντίον εσωτερικών κακόβουλων απειλών.

3.3.2 Απώλεια Ελέγχου Λογαριασμού ή Υπηρεσίας

Η απειλή που σαν αποτέλεσμα έχει την απώλεια ελέγχου λογαριασμού ή υπηρεσίας δεν είναι κάτι καινούργιο. Η χρήση μεθόδων phishing, social engineering και vulnerability exploitation χρησιμοποιούνται εδώ και πολλά χρόνια από κακόβουλους για αυτό τον σκοπό. Ειδικά στις περιπτώσεις όπου κωδικοί και λοιπά credentials χρηστών χρησιμοποιούνται για πολλές υπηρεσίες, οι επιπτώσεις ενός τέτοιου κινδύνου αυξάνονται δραματικά.

Στην εποχή του *Cloud Computing* το φαινόμενο αυτό γίνεται πιο επικίνδυνο διότι αν ο επιτιθέμενος καταφέρει να αποσπάσει credentials για της υπηρεσίες του χρηστή τότε θα έχει τη δυνατότητα να χαρτογραφήσει τις κινήσεις και τις συναλλαγές του, να αλλοιώσει δεδομένα που τον αφορούν, να του δώσει ψευδείς πληροφορίες ή να τον αποπροσανατολίσει οδηγώντας τον σε διάφορες ιστοσελίδες. Επιπλέον, ο λογαριασμός του χρήστη μπορεί να αποτελέσει τη «βάση» του κακόβουλου για περεταίρω παράνομες δραστηριότητες, εισάγοντας επιπλέον κινδύνους με πιθανές επιπτώσεις δυσφήμησης. Να σημειώσουμε ότι αυτή η απειλή αφορά όλα τα μοντέλα ανάπτυξης του cloud computing.

Ο αντίκτυπος μιας τέτοιας επίθεσης είναι ιδιαίτερης σημασίας. Ο επιτιθέμενος μπορεί να αποκτήσει με αυτό τον τρόπο πρόσβαση σε «κρίσιμα» δεδομένα υπηρεσιών clouding. Για αυτό το σκοπό πρέπει οι οργανισμοί να είναι ενήμεροι με τους τρόπους που χρησιμοποιούν οι κακόβουλοι, έτσι ώστε να παρέχουν μηχανισμούς άμυνας ενάντια στην απειλή.

<u>Ανάλυση όρων</u>

Το **phishing** (αγγλικός νεολογισμός βασιζόμενος στη λέξη fishing=ψάρεμα) είναι ένας τρόπος οικονομικής εξαπάτησης ανυποψίαστων πελατών, οι οποίοι

λαμβάνουν μηνύματα από «αξιόπιστες» πηγές (τράπεζες, εταιρείες κ.λπ.) που τους ζητούν προσωπικά τους στοιχεία (συνήθως αριθμούς πιστωτικών καρτών, αριθμούς λογαριασμών τραπέζης, κωδικούς πρόσβασης κ.α.), προκειμένου να διεκπεραιώσουν μία συναλλαγή. Η πλειοψηφία των Phishing μηνυμάτων επικαλείται κάποιο επείγον πρόβλημα ή κάποια «μοναδική ευκαιρία» και ζητά από τον ανυποψίαστο παραλήπτη να απαντήσει άμεσα, είτε για να αποκατασταθεί το πρόβλημα είτε για να επωφεληθεί της ευκαιρίας. Οι τεχνικές εξαπάτησης που χρησιμοποιούνται είναι ποικίλες. Είτε υπάρχει μια παραποιημένη διεύθυνση url μέσα στο περιεχόμενο του μηνύματος, η οποία, εκ πρώτης όψεως, φαίνεται σωστή, όταν όμως επιλεγεί από τον χρήστη οδηγεί σε σελίδες ακατάλληλου περιεχομένου. Είτε χρησιμοποιούνται εντολές JavaScript ώστε να μπερδευτεί η γραμμή διευθύνσεων και να οδηγήσει σε διαφορετικό ιστοχώρο, είτε χρησιμοποιούνται τα ίδια τα scripts των τραπεζών ή των εταιρειών και σε αυτήν την περίπτωση οι χρήστες λαμβάνουν ένα μήνυμα που φαίνεται γνήσιο και τους ζητά να επιβεβαιώσουν το λογαριασμό τους ακολουθώντας ένα σύνδεσμο που δείχνει να αντιστοιχεί σε αυθεντικό δικτυακό τόπο.

Το **social engineering** (κοινωνική μηχανική) αποτελεί τη μη εξουσιοδοτημένη πρόσβαση σε ένα υπολογιστικό σύστημα, με την φυσική-ανθρώπινη παρέμβαση, συνήθως χωρίς σχεδόν οποιασδήποτε χρήσης τεχνικών μέσων. Αποτελεί με απλά λόγια την ανθρώπινη πλευρά στην παραβίαση ενός πληροφοριακού δικτύου ή απλά ενός τερματικού, συνήθως με στόχο τη λήψη συγκεκριμένων στοιχείων ή πληροφοριών. Ακόμη και εταιρείες που διαθέτουν αυστηρές πολιτικές αυθεντικοποίησης, ισχυρά firewall, VPN και monitoring ολόκληρου του εταιρικού δικτύου, γίνονται αντικείμενο εκμετάλλευσης με χρήση επιτυχών μεθόδων κοινωνικής μηχανικής.

Το **SLA** (συμφωνία επιπέδων εξυπηρέτησης) είναι ένας επίσημος ορισμός της σχέσης που υπάρχει μεταξύ ενός φορέα παροχής υπηρεσιών και του πελάτη του ,σύμφωνα με τον Dinesh Verma. Τα Service Level Agreements (SLA) 1 αποτελούν συμβολαιοποιημένες συμφωνίες μεταξύ μιας επιχείρησης και ενός τρίτου παρόχου, που καθορίζουν με τι είδους υπηρεσίες και σε ποιο επίπεδο θα προμηθεύει ο πάροχος την επιχείρηση-πελάτη, κατά τη διάρκεια μιας

μακροχρόνιας συνεργασίας.

3.3.3 Απώλεια ή Διαρροή Δεδομένων

Η απώλεια ή διαρροή των δεδομένων αποτελεί έναν από τους σπουδαιότερους κινδύνους που απειλεί τις εταιρείες/οργανισμούς με τεράστιες άμεσες ή έμμεσες οικονομικές επιπτώσεις, είτε σε επίπεδο απώλειας αγαθών είτε σε επίπεδο δυσφήμησης. Δεν είναι λίγοι οι τρόποι με τους οποίους ένας οργανισμός μπορεί να χάσει ευαίσθητα ή κρίσιμα δεδομένα. Η διαγραφή ή αλλαγή δεδομένων χωρίς την ύπαρξη μεθόδου λήψης backup, η αποθήκευση σε μη αξιόπιστα μέσα, η απώλεια ενός κλειδιού κωδικοποίησης και τέλος η φυσική ή λογική πρόσβαση σε κάποιον μη εξουσιοδοτημένο αποτελούν αδιαίρετα κομμάτια του κινδύνου απώλειας/διαρροής δεδομένων. Όπως είναι προφανές, οι κίνδυνοι απώλειας/διαρροής δεδομένων αυξάνονται κατά την χρήση του cloud λόγω της μεγαλύτερη έκθεσης των δεδομένων σε τρίτους.

Η συγκεκριμένη απειλή αναφέρεται σε όλα τα μοντέλα υπηρεσιών του cloud computing. Είναι ήδη κατανοητό ότι μια ενδεχόμενη απώλεια ή διαρροή δεδομένων μπορεί να έχει ένα καταστρεπτικό αντίκτυπο για την επιχείρηση. Μπορεί να στοιχήσει στην φήμη του παρόχου, και την εμπιστοσύνη όχι μόνο από τους πελάτες αλλά και από τους υπαλλήλους, τους συνέταιρους και όλων όσων συνεργάζονται με τον εκάστοτε πάροχο. Στην περίπτωση, που τα δεδομένα που χαθούν ή διαρρεύσουν έχουν να κάνουν με τον τρόπο λειτουργίας του παρόχου τότε θα χάσει αρκετό έδαφος στον ανταγωνισμό με τους υπόλοιπους παρόχους, κάτι το οποία θα προκαλέσει και οικονομικές ζημιές. Στην χειρότερη περίπτωση αν τα δεδομένα που διαρρεύσουν είναι «κρίσιμα» και έχει δεσμευτεί ο πάροχος για την ακεραιότητα τους, τότε μπορεί να του επιβληθούν νομικές κυρώσεις.

Κάποια από τα αίτια που μπορούν να οδηγήσουν σε απώλεια ή διαρροή δεδομένων είναι αναποτελεσματική αυθεντικοποίηση, ασυνεπής χρήση κρυπτογράφησης και λογισμικών «κλειδιών», αναξιοπιστία των κέντρων δεδομένων, λειτουργικές αποτυχίες, ανυπαρξία σχεδιασμού ανάκαμψης από

κάποια καταστροφή.

Στο σημείο αυτό θα παραθέσουμε ένα παράδειγμα που έχει να κάνει με απώλεια δεδομένων στο νέφος. Συγκεκριμένα αποτελεί, την κατά πολλούς, μεγαλύτερη καταστροφή που συνέβη στην ιστορία του Cloud Computing, αφού είχε σαν αποτέλεσμα 800.000 χρήστες έξυπνων τηλεφώνων της εταιρίας Danger Hiptop (Sidekick), συνδεδεμένοι στο κυψελωτό δίκτυο της T-Mobile να χάσουν προσωρινά, όλα τα προσωπικά τους στοιχεία, όπως e-mails, διευθύνσεις επαφών, φωτογραφίες κτλ. Η συγκεκριμένη εταιρία κινητής τηλεφωνίας είχε εξαγοραστεί από την Microsoft νωρίτερα, τον Φεβρουάριο του 2007. Από εκείνο το σημείο η Microsoft ανέλαβε την διαχείριση των δεδομένων στα δικά της κέντρα δεδομένων που βρισκόντουσαν στην περιοχή βόρεια του Seattle στην Washington. Το Σεπτέμβριο του 2009 οι χρήστες των συγκεκριμένων κινητών τηλεφώνων που εξυπηρετούνται από τον τηλεπικοινωνιακό πάροχο της T-Mobile, παρατήρησαν απώλεια των δεδομένων τους. Μετά από δύο εβδομάδες ήρθε και η επίσημη ανακοίνωση από την T-Mobile που επικύρωσε την απώλεια. Τα αίτια σύμφωνα με την Microsoft ήταν μια αποτυχία του συστήματος που είχε σαν αποτέλεσμα την απώλεια των δεδομένων στον πυρήνα της κύριας και back up βάσης δεδομένων. Το θέμα οδηγήθηκε στα δικαστήρια όπου Microsoft και η T-Mobile κατηγορήθηκαν για τον τρόπο προστασίας των δεδομένων, που όπως ειπώθηκε δεν ακολουθούσαν καν τις βασικές αρχές. Παρόλα αυτά η Microsoft κατάφερε να επαναφέρει τα δεδομένα, παίρνοντας κατάλληλα μέτρα ώστε να μην συμβεί κάτι αντίστοιχο στο μέλλον. Να επισημάνουμε ότι αυτό δεν ήταν το μοναδικό περιστατικό απώλειας δεδομένων, απλά θεωρείται αξιοσημείωτο, διότι ενεπλάκη μια μεγάλη εταιρία παροχής υπηρεσιών cloud computing, η Microsoft, και διότι εκείνη την στιγμή εκφράστηκε ένας σκεπτικισμός σχετικά με το μέλλον της συγκεκριμένης τεχνολογίας.

3.3.4 Επισφαλείς διεπαφές/APIs

Οι πάροχοι cloud computing προσφέρουν μια κατάλληλη διεπαφή (API), στους πελάτες τους με στόχο την καλύτερη αλληλεπίδραση με τις υπηρεσίες νέφους. Η συνδυαστική αλληλεπίδραση και η ενορχήστρωση των cloud υπηρεσιών που παρέχονται στους χρήστες γίνεται με τις αντίστοιχες διεπαφές. Είναι προφανές ότι το επίπεδο ασφάλειας των cloud υπηρεσιών που προσφέρονται έχουν άμεση εξάρτηση από το επίπεδο ασφάλειας των APIs που χρησιμοποιούνται για αυτές. Το πρόβλημα έγκειται στο γεγονός ότι τα APIs συχνά εμπλουτίζονται με νέα εργαλεία από την στιγμή έκδοσής τους προς εξυπηρέτηση των πελατών, ώστε να προσφέρουν επιπρόσθετες υπηρεσίες. Αυτό έχει σαν αποτέλεσμα την αύξηση της πολυπλοκότητας των υφιστάμενων διεπαφών καθώς και την ύπαρξη κενών ασφάλειας.

Η συγκεκριμένη απειλή αναφέρεται σε όλα τα μοντέλα υπηρεσιών του cloud computing. Παρόλο που οι περισσότεροι πάροχοι προσπαθούν να εξασφαλίσουν ότι η ασφάλεια θα είναι ενσωματωμένη σε όλο το μοντέλο, είναι εξίσου σημαντικό οι πελάτες να μπορούν να καταλάβουν τη σημασία της ασφάλειας με την χρήση, την διαχείριση, την ενορχήστρωση και την επίβλεψη των υπηρεσιών cloud computing. Έτσι όταν οι διεπαφές είναι «ασθενής», εκθέτουν τον πάροχο σε αρκετά ζητήματα ασφάλειας που έχουν να κάνουμε την εμπιστευτικότητα την ακεραιτότητα, την διαθεσιμότητα και την υπευθυνότητα.

Μερικά από τα αίτια της συγκεκριμένης απειλής είναι η δυνατότητα ανώνυμης πρόσβασης, η επαναχρησιμοποίηση κωδίκων, λάθος χειρισμός του ελέγχου πρόσβασης, εσφαλμένη εξουσιοδότηση χρηστών κτλ.

3.3.5 Προβλήματα Διαμοιρασμού

Όπως αναφέρθηκε στην εισαγωγή, οι πάροχοι IaaS, προσφέρουν υπολογιστική και δικτυακή υποδομή. Συχνά, τα στοιχεία που περιλαμβάνονται σε αυτή την υποδομή (για παράδειγμα επεξεργαστές, κάρτες γραφικών κτλ.)

δεν είναι κατασκευασμένα έτσι ώστε να είναι απομονωμένα σε *"multitenant"* αρχιτεκτονικές. Για αυτό το σκοπό χρησιμοποιείται από τον πάροχο του cloud ένας εικονικός hypervisor, ο όποιος ελέγχει τη διανομή των πόρων στα λειτουργικά μηχανήματα των πελατών. Ωστόσο έχουν εντοπιστεί προβλήματα στους hypervisors μέσω των οποίων μπορεί να επιτραπεί στα εικονικά μηχανήματα των πελατών να αποκτήσουν αυξημένο έλεγχο στην υποδομή ή ακόμα και να επηρεάζουν την λειτουργία της. Έτσι κρίνεται απαραίτητη μια στρατηγική άμυνας κατά την οποία υπολογιστική δύναμη, αποθηκευτική δυνατότητα και ασφάλεια θα επιβλέπονται. Επίσης, θα υπάρχει ισχυρός διαχωρισμός τμημάτων, έτσι ώστε να εξασφαλιστεί ότι οι χρήστες του cloud δεν θα έχουν πρόσβαση στα δεδομένα και στην υποδομή άλλων χρηστών στο ίδιο cloud.

Υπάρχουν αρκετές επιθέσεις τα τελευταία χρόνια βασισμένες στο πρόβλημα του διαμοιρασμού. Αυτό εξαιτίας του γεγονότος ότι στοιχεία, όπως επεξεργαστές, κάρτες γραφικών κτλ, δεν έχουν σχεδιαστεί για να λειτουργούν χωρισμένα σε τμήματα. Ως αποτέλεσμα, ο επιτιθέμενες εστιάζει στο πως θα επηρεάσει τις ενέργειες άλλων πελατών του ίδιου cloud, και πως θα αποκτήσεις πρόσβαση σε δεδομένα για τα οποία δεν έχει εξουσιοδότηση.

3.3.6 Κακόβουλη και άσκοπη χρήση

Οι πάροχοι IaaS προσφέρουν στους πελάτες τους την ψευδαίσθηση ότι διαθέτουν ανεξάντλητους υπολογιστικούς και αποθηκευτικούς πόρους, τους οποίους μπορούν να τους αποκτήσουν με μια εγγραφή στον αντίστοιχο πάροχο η οποία απαιτεί μόνο έναν έγκυρο αριθμό πιστωτικής κάρτας. Πολλοί πάροχοι επίσης προσφέρουν, τις λεγόμενες «περιόδους δοκιμής», κατά τις οποίες μπορεί ένας χρήστης για ένα συγκεκριμένο χρονικό διάστημα να χρησιμοποιεί δωρεάν τις υπηρεσίες του παρόχου. Η ανωνυμία αυτή μπορεί να εκμεταλλευτεί από κακόβουλους χρηστές ώστε να χρησιμοποιούν τις υπηρεσίες που παρέχονται είτε για την αποστολή spam αλληλογραφίας είτε για την ανάπτυξη κακόβουλου κώδικα και άλλων παρανομών πράξεων. Επίσης, οι

πάροχοι PaaS αντιμετωπίζουν το ίδιο πρόβλημα. Κάποιες λοιπόν από τις ενδεχόμενες απειλές είναι το σπάσιμο κλειδιών, επιθέσεις DoS, την κατασκευή rainbow tables, την επίλυση CAPTCHA καθώς και τον έλεγχο botnets.

Οι κακόβουλοι συνεχίζουν να εκμεταλλεύονται νέες τεχνολογίες για να βελτιώσουν την δράση τους, αποφεύγοντας να γίνουν αντιληπτοί και βελτιώνοντας την απόδοση των ενεργειών τους. Τα νέφη υπολογιστών αποτελούν στόχος των κακόβουλων, διότι αφενός οι πάροχοι έχουν ελαχιστοποιήσει τα στοιχεία αυθεντικοποίησης κατά την διάρκεια εγγραφής ενός πελάτη και αφετέρου γιατί η ικανότητά τους να εντοπίσουν κακόβουλη συμπεριφορά είναι περιορισμένη.

Παράδειγμα μιας τέτοιας απειλής αποτελεί το Zeus Botnet. Ερευνητές διαπίστωσαν ότι το botnet Zeus διέθετε κέντρο ελέγχου στο EC2, την υποδομή cloud computing της Amazon. Είναι η πρώτη φορά που η υπηρεσία αυτή χρησιμοποιήθηκε για μια τέτοια παράνομη δραστηριότητα, σύμφωνα με τον Don DeBolt, ερευνητή της εταιρείας HCL Technologies.Οι hackers "εγκαταστάθηκαν" στο EC2 αφού παραβίασαν ένα website που φιλοξενούνταν στους servers της Amazon. Άλλο παράδειγμα αποτελεί το InfoStealer trojan. Τέλος ένα άλλο παράδειγμα αποτελεί το spam, που είναι πολύ συχνό φαινόμενο στις περιπτώσεις cloud. Για αυτό το λόγο υπάρχουν μαύρες λίστες με διευθύνσεις IaaS.

Ανάλυση όρων

Οι επιθέσεις του τύπου **DoS (Denial of Service)**, που είναι γνωστές και ως επιθέσεις άρνησης υπηρεσίας, αποτελούν μια από τις σοβαρότερες επιθέσεις που μπορούν να εκδηλωθούν σ' ένα Web site ή σ' ένα δίκτυο υπολογιστών. Οι επιθέσεις αυτές είναι καταστροφικές για τις εταιρείες και έχουν μεγάλο οικονομικό κόστος. Το κόστος αφορά στις χαμένες ώρες λειτουργίας μιας επιχείρησης αλλά και στο κόστος που απαιτείται για τον εντοπισμό και την αντιμετώπιση αυτών των επιθέσεων. Ουσιαστικά μια τέτοια επίθεση έχει ως αποτέλεσμα την αδυναμία της εταιρείας να εξυπηρετήσει τους πελάτες της. Η επίθεση συνίσταται στην εκδήλωση χιλιάδων αιτήσεων σύνδεσης σ' έναν

server και σε διάστημα μερικών ημερών, με απώτερο στόχο τον κατάρρευση του server από την αδυναμία του να ανταποκριθεί σ' έναν τόσο μεγάλο αριθμό αιτήσεων.

Rainbow Tables λέγονται οι λίστες οι οποίες μαντεύουν την κρυπτογραφημένη εκδοχή του κωδικού (ή hash) αντί για τον ίδιο τον κωδικό. Ο κακόβουλος σε αυτήν την περίπτωση χρησιμοποιεί ένα πρόγραμμα το οποίο δημιουργεί κωδικούς και ταυτόχρονα τους κρυπτογραφεί.

Το σύστημα CAPTCHA είναι αυτή τη στιγμή ο πλέον διαδεδομένος τρόπος για να ξεχωρίζει ένα site αν έχει απέναντί του έναν άνθρωπο ή ένα bot. Βέβαια, η εμπειρία έχει δείξει ότι πολλές φορές το CAPTCHA δημιουργεί περισσότερα προβλήματα από όσα λύνει. Το CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) επινοήθηκε το 2000 από ερευνητές του Carnegie Mellon University. Ο χρήστης βλέπει μια εικόνα που περιλαμβάνει με λιγότερη ή περισσότερη παραμόρφωση μία ή περισσότερες λέξεις. Σε περίπτωση που ο χρήστης πληκτρολογήσει σωστά τις λέξεις, μπορεί να συνεχίσει στην ενέργεια που θέλει να κάνει. Εκείνη την εποχή, το σύστημα CAPTCHA ήταν αρκετά αποτελεσματικό και κάποιοι έσπευσαν να προβλέψουν το τέλος των bots. Με τον καιρό, όμως, τα άυλα ρομποτάκια έγιναν πιο “έξυπνα” και άρχισαν να ανταποκρίνονται στις απαιτήσεις του CAPTCHA, διαβάζοντας τις λέξεις. Για να αντιμετωπιστεί αυτή η εξέλιξη, οι παραμορφωμένες λέξεις έγιναν ακόμα πιο παραμορφωμένες, με αποτέλεσμα σε πολλές περιπτώσεις να είναι ουσιαστικά αδύνατη η ανάγνωσή τους. Έτσι, το σύστημα άρχισε να κρατά μακριά ακόμα και τους ανθρώπους. Η εταιρεία Are You A Human είναι ένα αμερικάνικο startup που έχει αναπτύξει ένα νέο σύστημα υποδοχής. Το νέο μοντέλο αντικαθιστά το CAPTCHA με ένα mini game. Έτσι, ο χρήστης καλείται π.χ. να διακρίνει ποια από τα πέντε εμφανιζόμενα αντικείμενα είναι εργαλεία και να τα βάλει σε ένα κουτί. Πρόκειται για tasks που είναι πολύ απλά για τους ανθρώπους, αλλά πολύ δύσκολα για τις μηχανές - τουλάχιστον σε αυτή τη φάση.

Ως **botnet** ορίζεται ένα δίκτυο υπολογιστών, το οποίο ελέγχεται εξ αποστάσεως από τον λεγόμενο botmaster χωρίς τη γνώση ή την έγκριση των

κατόχων των μεμονωμένων υπολογιστών. Οι υπολογιστές που είναι μέλη του δικτύου αυτού ονομάζονται *ζόμπι*. Ο botmaster μπορεί να χρησιμοποιεί αυτούς τους υπολογιστές-ζόμπι για διάφορους παράνομους σκοπούς. Καθώς μπορεί να έχει πρόσβαση στον κάθε υπολογιστή-ζόμπι σαν να βρισκόταν ο ίδιος μπροστά σε αυτόν, είναι δυνατή τόσο η πρόσβαση στα αρχεία του συστήματος όσο και η χρήση της σύνδεσης δικτύου του υπολογιστή, χωρίς να το αντιληφθεί ο ιδιοκτήτης του. Αυτό του δίνει αμέτρητες δυνατότητες. Πέρα από την υποκλοπή δεδομένων, η πρόσβαση στους υπολογιστές-ζόμπι επιτρέπει και την απόκρυψη της ταυτότητας του δράστη, καθώς ως διακομιστής μεσολάβησης χρησιμοποιείται ο υπολογιστής του θύματος. Ανάλογα με το μέγεθος του botnet, ο δράστης μπορεί να αλλάζει σε ορισμένες εξαιρετικές περιπτώσεις τη διεύθυνση IP του ακόμη και ανά δευτερόλεπτο, ώστε να μπορεί να προβαίνει σε παράνομες ενέργειες μέσω των συνδέσεων των θυμάτων του. Επιπλέον, ο εξ αποστάσεως έλεγχος των υπολογιστών εξυπηρετεί ιδανικά τη μετάδοση του κακόβουλου κώδικα bot ή τη μαζική αποστολή spam.

Στην επιστήμη υπολογιστών ο **δούρειος ίππος** (trojan horse ή απλά trojan) είναι ένα κακόβουλο πρόγραμμα που ξεγελάει τον χρήστη και τον κάνει να πιστεύει ότι εκτελεί κάποια χρήσιμη λειτουργία ενώ στα κρυφά εγκαθιστά στον υπολογιστή του άλλα κακόβουλα προγράμματα. Η τακτική που χρησιμοποιούν οι δούρειοι ίπποι είναι παρόμοια με την τακτική που χρησιμοποίησε ο Οδυσσέας (στην Ηλιάδα του Ομήρου), οπότε πήραν και αυτήν την ονομασία. Συγκεκριμένα, κρύβουν μέσα τους κακόβουλο κώδικα ο οποίος μπορεί να μολύνει τον υπολογιστή. Εξωτερικά μοιάζουν με προγράμματα τα οποία εκτελούν χρήσιμες λειτουργίες, είναι ενδιαφέροντα και δίνουν την εντύπωση στον χρήστη ότι είναι ακίνδυνα. Όταν όμως ο χρήστης εκτελέσει αυτό το πρόγραμμα, τότε ενεργοποιείται ο κακόβουλος κώδικας με αποτέλεσμα ο υπολογιστής να μολυνθεί. Συνήθως αποτέλεσμα της μόλυνσης από δούρειο ίππο είναι η εγκατάσταση κάποιου προγράμματος που επιτρέπει σε μη εξουσιοδοτημένους χρήστες να έχουν πρόσβαση στον μολυσμένο υπολογιστή και να τον χρησιμοποιούν για να ξεκινήσουν άλλες επιθέσεις προς άλλους υπολογιστές του διαδικτύου. Σε αντίθεση με τους ιούς, οι δούρειοι ίπποι δε μεταδίδονται μολύνοντας αρχεία.

3.3.7 Δυσκολία εντοπισμού των κινδύνων

Όπως ειπώθηκε ήδη, βασικό πλεονέκτημα του *Cloud Computing* είναι η δυνατότητα που δίνει σε έναν οργανισμό να αφοσιωθεί στις επιχειρησιακές του λειτουργίες αφού η διαχείριση των πληροφοριακών του συστημάτων περνάει στα χέρια ενός τρίτου. Αυτό έχει σαν αποτέλεσμα σημαντικό οικονομικό όφελος, το οποίο όμως είναι αντιστρόφως ανάλογο με την ασφάλεια των δεδομένων και των λοιπών αγαθών και υπηρεσιών που παρέχονται. Κάποια βασικά πράγματα για την εκτίμηση του πόσο ασφαλής είναι τα δεδομένα ενός πελάτη αποτελούν, ο έλεγχος για νέες εκδόσεις και ενημερώσεις λογισμικού, η ύπαρξη μηχανισμού αναφοράς και καταγραφής ύποπτων ενεργειών, η σχεδίαση της ασφάλειας κτλ. Επίσης, σημαντικές πληροφορίες έχουν να κάνουν με το ποίος άλλος διαμοιράζεται την υποδομή σου. Δεν αποκλείεται, σε περίπτωση παραβίασης, οι οικονομικές επιπτώσεις να είναι μεγαλύτερες από το όφελος που προσφέρεται από το Cloud Computing.

Ο κάθε πελάτης μια υπηρεσίας cloud είναι σαφώς ενημερωμένος για τη λειτουργικότητα και τα χαρακτηριστικά του παρόχου. Όμως δεν δίνεται τις περισσότερες φορές σημασία σε ότι έχει να κάνει με την ασφάλεια που του παρέχει. Για παράδειγμα κάποια ερωτήματα όπως, ποιος άλλος έχει πρόσβαση στα δεδομένα, ή σε περίπτωση μια επίθεσης τι δεδομένα μπορεί να διαρρεύσουν, δεν έχουν μια διευκρινιστική απάντηση ή απλά παραλείπεται η απάντηση τους, αφήνοντας τους πελάτες με το ρίσκο της απειλής μιας ενδεχόμενης επίθεσης. Μάλιστα, αυτό το ρίσκο είναι δύσκολο ακόμα και να το οριοθετήσουν.

Ένα παράδειγμα για αυτή την περίπτωση, αποτελεί η άρνηση της Amazon για το νέφος EC2, όταν της ζητήθηκε από την IRS η πραγματοποίηση C&A. Η τελευταία αποτελεί μια διαδικασία για την καταγραφή των επιπέδων ασφάλειας. Είναι μια συστηματική διενέργεια με σκοπό την αποτίμηση, καταγραφή, έλεγχο και εξουσιοδότηση συστημάτων αφότου ή πριν το σύστημα τεθεί σε λειτουργία.

Άλλο ένα παράδειγμα, αποτελεί αυτό της εταιρίας Heartland Payment το 2008. Η εταιρία αυτή παρέχει κάρτες χρεωστικές , πιστωτικές κτλ. Η εταιρία αυτή

εξυπηρετούσε πάνω από 100 εκατομμύρια συνδιαλλαγές με κάρτες μηνιαία που ανήκαν σε πάνω από 250 χιλιάδες επιχειρήσεις. Εκείνη την εποχή έπεσε θύμα κακόβουλου, ο οποίος κατάφερε μέσα από παρακολούθηση των πακέτων που προορισμό είχα τα υπολογιστικά κέντρα της εταιρίας να αποσπά όλα τα στοιχεία των δικαιούχων των καρτών. Το επόμενο βήμα ήταν να δημιουργήσει αντίγραφα τον καρτών, και με λιγότερο από ένα δολάριο να τσεκάρουν αν η κάρτα είναι ενεργή και στην περίπτωση που ήταν να πραγματοποιήσουν συνδιαλλαγές προς το συμφέρον τους. Το κόστος από αυτή την επίθεση ήταν τεράστιο. Ενώ θεωρείται ακόμα απαράδεκτο το γεγονός ότι η εταιρία έκανε ακριβώς ότι έλεγε ο νόμος (σε πολλές πολιτείες που ανήκαν θύματα δεν υπήρχε τίποτα σχετικό με τον τρόπο αντιμετώπισης παρόμοιων καταστάσεων), και δεν μπήκε στην διαδικασία να ενημερώσει τον κάθε πελάτη περί της κλοπής της κάρτας του, ανεξάρτητα από το ότι δεν το επίτασσε ο νόμος.

3.3.8 Μεγάλος βαθμός εξάρτησης και vendor lock-in

Με τις διαστάσεις που έχει πάρει το *Cloud Computing* τα τελευταία χρόνια, δεν είναι λίγοι οι οργανισμοί που επιλέγουν να εναποθέσουν το σύνολο των πληροφοριακών τους υπηρεσιών στα χέρια των Cloud παρόχων. Σε περιπτώσεις σαν και αυτές, ο βαθμός εξάρτησης όλων των υπηρεσιών του οργανισμού από κάποιο τρίτο, εισάγει πλήθος κινδύνων, όπως τη συσσώρευση των δεδομένων του οργανισμού σε ένα data center ή την αδυναμία διαθεσιμότητας των υπηρεσιών από τον πάροχο για οποιοδήποτε λόγο. Επιπλέον υφίσταται και ο κίνδυνος του «εγκλωβισμού» (lock-in) του οργανισμού σε ένα συγκεκριμένο Cloud πάροχο. Η ανάκτηση και η μεταστέγαση των δεδομένων και των υπηρεσιών δεν είναι ποτέ μία εύκολη και απλή διαδικασία καθώς το συνεπαγόμενο κόστος μπορεί να αποτελέσει εμπόδιο. Συγκεκριμένα, η απουσία θέσπισης προτύπων μορφοποίησης δεδομένων (data formats) και APIs ώστε να επιτρέπεται η διαλειτουργικότητα μεταξύ των υποδομών, μπορεί να μετατρέψει τη μετακίνηση των υπηρεσιών σε άλλο πάροχο σε μία περίπλοκη και δαπανηρή υπόθεση. Εκτός από τις πιθανές συμφωνημένες κυρώσεις που μπορούν να υπάρχουν κατά τη διάλυση μίας

συνεργασίας και του υφιστάμενου συμφώνου, οι οργανισμοί θα πρέπει να επιβαρυνθούν τόσο για τη μετατροπή των formats όσο και για τη διαδικασία μεταφοράς ενώ μπορεί να υπάρχουν και επιπλέον χρεώσεις για τη χρήση bandwidth. Συνολικά αυτά τα κόστη μπορούν να ανέλθουν σε ασύμφορα για τον οργανισμό ποσά, υποχρεώνοντάς τον να διατηρήσει τη διάθεση των υπηρεσιών του στον ίδιο πάροχο.

3.3.9 Πολυπλοκότητα συμμόρφωσης προς τη διεθνή νομοθεσία

Από την προοπτική του Διεθνούς Δικαίου, η βασική διαφορά μεταξύ των παραδοσιακών IT outsourced υπηρεσιών και του *Cloud Computing*, είναι το «που» βρίσκονται ή επεξεργάζονται τα δεδομένα των πελατών αφού στην ουσία υπάρχει η δυνατότητα να είναι διασκορπισμένα σε διάφορα data centers σε ολόκληρο τον κόσμο. Επιπλέον η χρήση μίας Cloud πλατφόρμας μπορεί στη πράξη να οδηγήσει στη δημιουργία πολλών αντιγράφων των δεδομένων που χρησιμοποιούνται και που αποθηκεύονται σε διαφορετικές τοποθεσίες. Αυτό μπορεί να ισχύει και κατά τη χρήση ενός ιδιωτικού νέφους (Private Cloud) το οποίο χρησιμοποιείται από έναν και μόνο πελάτη.

Η τοποθεσία που βρίσκεται το data center από το οποίο εκτελούνται οι cloud υπηρεσίες, δεν μπορεί να είναι γνωστό για το εάν αντιμετωπίζουν απειλές από φυσικές καταστροφές ή άλλους ανθρώπινους παράγοντες. Επίσης, η νομοθεσία που διέπει τη δικαιοδοσία της εκάστοτε τοποθεσίας μπορεί να αφήνει περιθώρια ύπαρξης διαφωνιών σχετικά με κινδύνους παραβίασης προσωπικών δεδομένων, απαγορεύοντας στο πελάτη να εφαρμόσει τα δικαιώματα που του παρέχει το συμβόλαιο που έχει υπογράψει. Επίσης η διακίνηση της πληροφορίας, δεν υπόκειται κάτω από την ίδια νομοθεσία διεθνώς, με αποτέλεσμα κάποια δεδομένα τα οποία θεωρούνται ευαίσθητα στη δικαιοδοσία ενός κράτους, να μην έχουν κανένα μέτρο διαβάθμισης στη δικαιοδοσία ενός άλλο.

3.3.10 Εξάρτηση από το Διαδίκτυο ως τον κύριο δίαυλο επικοινωνίας

Η επικοινωνία μεταξύ του οργανισμού-πελάτη και των δεδομένων και των υποδομών που δέχεται ως υπηρεσία από το Διαδίκτυο, εισάγει όλους τους σχετικούς κινδύνους εμπιστευτικότητας, ακεραιότητας και αυθεντικότητας που υπάρχουν σε ένα περιβάλλον δημόσιας χρήσης. Στην ουσία, όλες οι απειλές που σχετίζονται με την Ασφάλεια Υπηρεσιών Διαδικτύου κληρονομούνται αυτόματα στο *Cloud Computing*. Επίσης, εισάγεται και ένας επιπλέον κίνδυνος ο οποίος σχετίζεται με την εξάρτηση από έναν ISP για πρόσβαση προς το Διαδίκτυο.

3.4 Επιθέσεις που σχετίζονται με το Cloud

Οι επιθέσεις που μπορούν να γίνουν μέσα στο cloud είναι κοινές με αυτές που μπορεί να συμβούν σε ένα οποιοδήποτε πληροφοριακό σύστημα. Παρόλα αυτά υπάρχει ένα τύπος επίθεσης που σχετίζεται μόνο με το cloud. Αυτή είναι η επίθεση VM escape. Με άλλα λόγια ο επιτιθέμενος προσπαθεί να ξεφύγει από την απομωνομένη εικονική μηχανή του, ώστε να επιτεθεί σε άλλες εικονικές μηχανές.

4. Intrusion Detection Systems

4.1 Γενικά

Η ανίχνευση εισβολής (intrusion detection) είναι η διαδικασία της παρακολούθησης των γεγονότων που συμβαίνουν σε ένα υπολογιστικό σύστημα ή δίκτυο και της ανάλυσής τους για πιθανά συμβάντα τα οποία είναι παραβιάσεις ή απειλές παραβίασης των πολιτικών ασφάλειας ενός υπολογιστή, των πολιτικών ασφάλειας αποδεκτής χρήσης ή καθιερωμένων πρακτικών ασφάλειας. Τα γεγονότα αυτά μπορεί να πηγάζουν από πολλές αιτίες, όπως, για παράδειγμα, κακόβουλο λογισμικό (worms, spyware κλπ), επιτιθέμενους οι οποίοι λαμβάνουν μη εξουσιοδοτημένη πρόσβαση στο σύστημα, ενώ οι ίδιοι βρίσκονται εκτός συστήματος και εξουσιοδοτημένους χρήστες που χρησιμοποιούν τα δικαιώματά τους με κακόβουλο τρόπο ή προσπαθούν να λάβουν επιπλέον δικαιώματα για τα οποία δεν είναι εξουσιοδοτημένοι. Αν και πολλά από τα συμβάντα είναι κακόβουλα από τη φύση τους, πολλά άλλα δεν είναι. Για παράδειγμα, ένας χρήστης μπορεί να δώσει λάθος κωδικό πρόσβασης. Αυτό δεν σημαίνει ότι είναι κακόβουλος χρήστης, αλλά έκανε λάθος τη συγκεκριμένη στιγμή. Τα εργαλεία με τα οποία μπορούμε να ανιχνεύσουμε εισβολές ονομάζονται εργαλεία ανίχνευσης εισβολών (Intrusion Detection Systems).

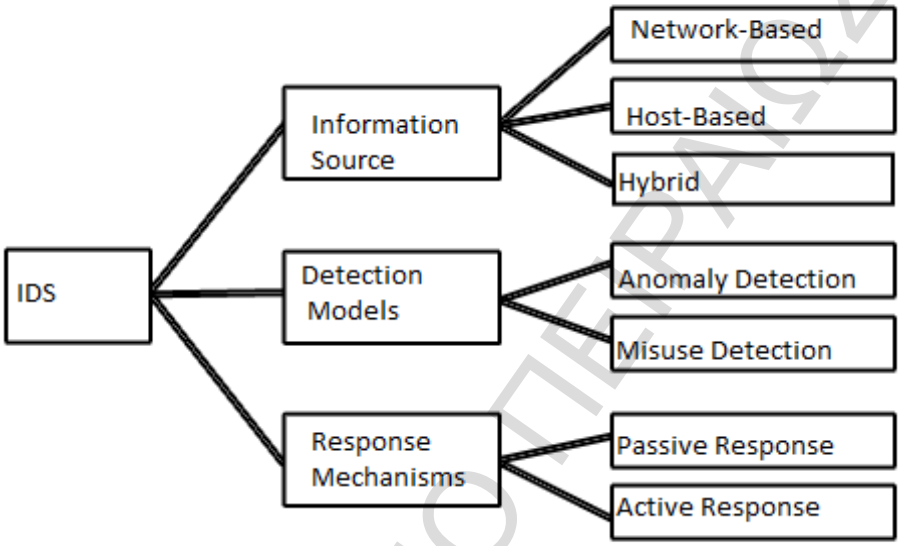
4.2 Κατάταξη των IDS

Ένα εργαλείο ανίχνευσης εισβολής (IDS) είναι ένα λογισμικό που αυτοματοποιεί τη διαδικασία ανίχνευσης απειλών. Αυτό το επιτυγχάνει παρακολουθώντας τα γεγονότα που συμβαίνουν σε ένα υπολογιστικό σύστημα ή δίκτυο και τα αναλύει προκειμένου να εντοπίσει σημάδια εισβολής.

Τα IDS μπορούν να ταξινομηθούν με βάση τρεις παράγοντες:

- την πηγή από την οποία συγκεντρώνουν την πληροφορία για ανάλυση

- το μηχανισμό ανίχνευσης από τον οποίο τα συγκεντρωμένα δεδομένα αναλύονται ώστε να ανιχνευθούν πιθανές εισβολές
- τους μηχανισμούς απάντησης οι οποίοι εκτελούνται ως αποτέλεσμα των ειδοποιήσεων που έχουν συγκεντρωθεί.



Εικόνα 4.1: Κατάταξη των IDS

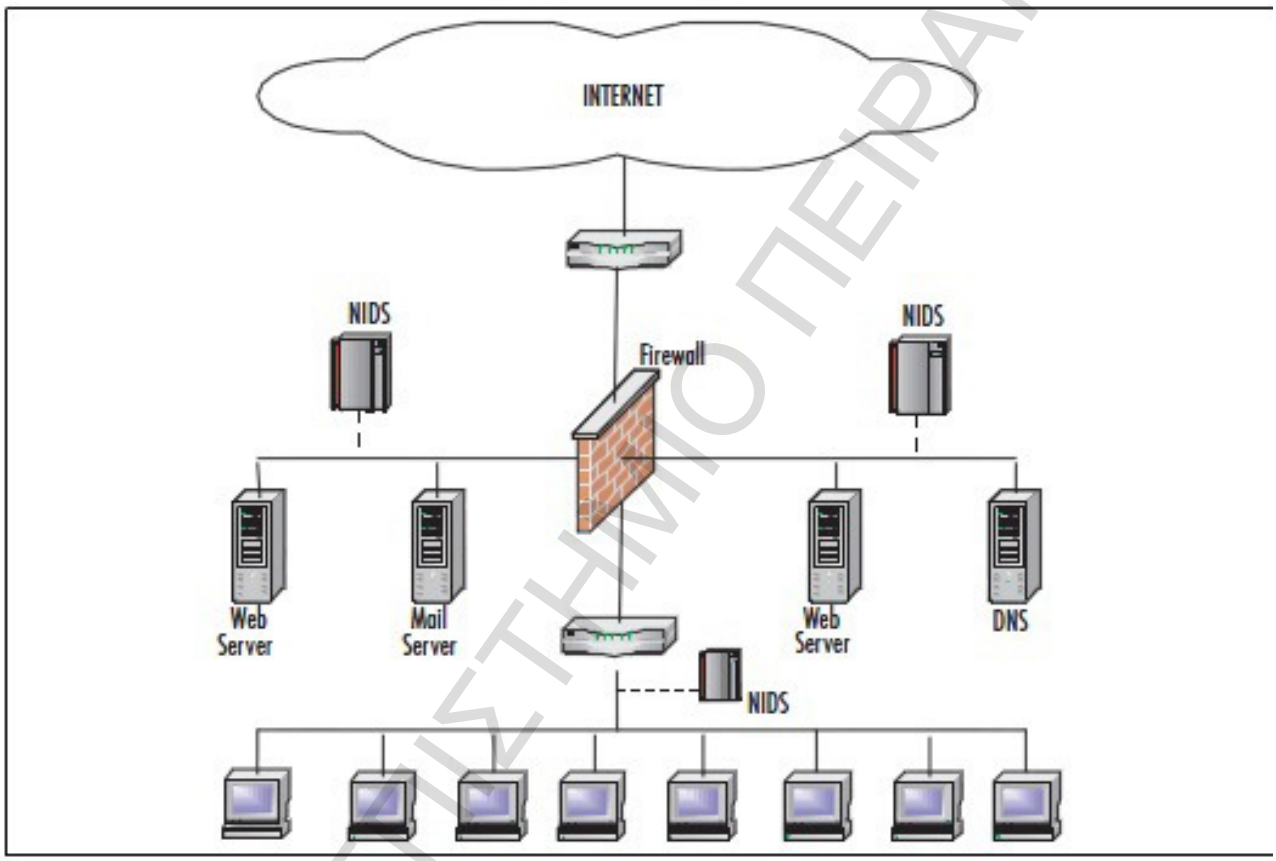
4.2.1 Ταξινόμηση με βάση την πηγή

Τα δεδομένα μπορούν να συλλεχθούν από δικτυακή κίνηση, από γεγονότα σε έναν υπολογιστή ή από δραστηριότητες διαφόρων εφαρμογών. Σύμφωνα με αυτό έχουμε τρεις διαφορετικές κατηγορίες IDS.

- ***εργαλείο ανίχνευσης εισβολής βασισμένο στο δίκτυο*** **(NIDS - Network-based Intrusion Detection System)**: Η συγκεκριμένη κατηγορία IDS εξετάζει την κίνηση στο δίκτυο. Τα IDS ανιχνεύουν και αναλύουν συμβάντα που γίνονται σε ένα πληροφοριακό σύστημα ώστε να αναλύσουν την κίνηση του δικτύου. Συνήθως αποτελούνται από ένα σύνολο αισθητήρων που δίνουν αναφορά σε μια κεντρική κονσόλα διαχείρισης. Ένας τέτοιου τύπου IDS αναλύει πακέτα του δικτύου

ψάχνοντας για επιθέσεις. Παίρνει όλα τα πακέτα ενός τομέα του δικτύου και προσεκτικά επαναδημιουργεί την κίνηση ούτως ώστε να την αναλύσει για μοτίβα κακόβουλης συμπεριφοράς.

Τα περισσότερα NIDS έχουν τη δυνατότητα να καταγράφουν τις δραστηριότητές τους και να αναφέρουν ή να ειδοποιούν για ύποπτα συμβάντα.



Εικόνα 4.2: NIDS

Πλεονεκτήματα των NIDS:

1. Με τη χρήση σχετικά μικρού αριθμού NIDS μπορούμε να επιβλέπουμε ένα σχετικά μεγάλο δίκτυο και να προστατεύσουμε ένα σχετικά μεγάλο αριθμό υπολογιστών ή άλλων συσκευών που βρίσκονται μέσα σε αυτό.
2. Ένα NIDS μπορεί να επιβλέπει συσκευές και λειτουργικά συστήματα που

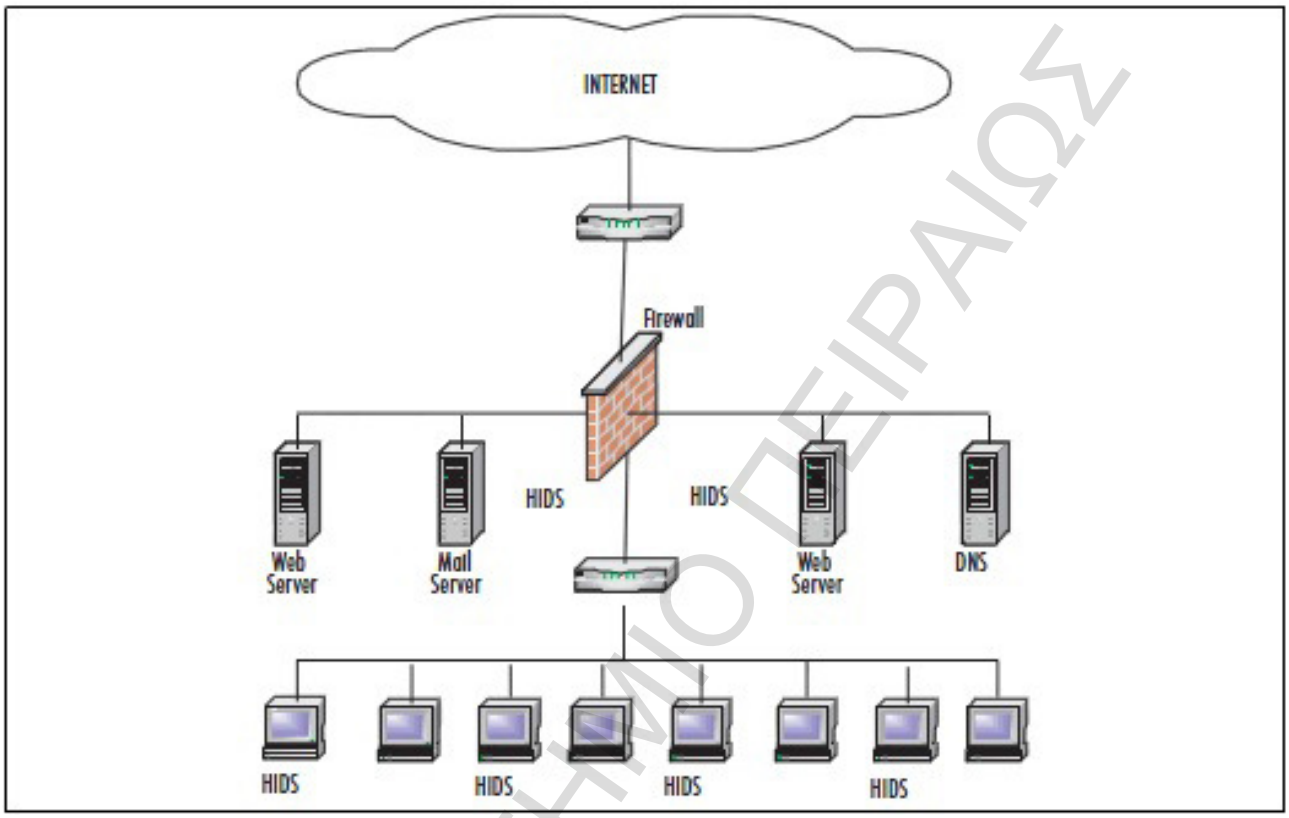
είναι διαφορετικά μεταξύ τους.

3. Μπορεί να είναι αρκετά προστατευμένο κατά τη διάρκεια μιας επίθεσης, ακόμα και αόρατο στον εκάστοτε επιτιθέμενο.

Μειονεκτήματα των NIDS:

1. Ένα NIDS μπορεί να αντιμετωπίσει δυσκολία στην ανάλυση επιθέσεων μέσα σε ένα φορτωμένο δίκτυο και αυτό έχει ως αποτέλεσμα να οδηγείται σε αποτυχία ανίχνευσης επιθέσεων.
2. Η ανάγκη να αναλυθούν τα πακέτα όσο πιο γρήγορα γίνεται, πολλές φορές έχει ως αποτέλεσμα τον εντοπισμό λιγότερων επιθέσεων.
3. Ένα NIDS δεν μπορεί να αναλύσει κρυπτογραφημένη πληροφορία.
4. Τα switch-based δίκτυα μπορεί να περιορίσουν την πρόσβαση ενός NIDS σε κίνηση δικτύου.

Εργαλείο ανίχνευσης εισβολής βασισμένο στη συσκευή **(HIDS – Host-based Intrusion Detection Systems):** Ένα HIDS χρησιμοποιεί αρχεία καταγραφής του συστήματος. Συνήθως είναι σχεδιασμένο για να υποστηρίζει μία κεντρική διαχείριση, όπως επίσης και μία κεντρική δομή αναφοράς. Ένα τέτοιου είδους εργαλείο, συνήθως, χρειάζεται λογισμικό που θα είναι εγκατεστημένο στο σύστημα και θα εποπτεύει όλους τους πόρους της συσκευής για κάθε είδους δραστηριότητα. Καταγράφει τις δραστηριότητες της συσκευής σε μία ασφαλή βάση δεδομένων και ελέγχει εάν τα γεγονότα που έχουν καταγραφεί ταιριάζουν με οποιοδήποτε κακόβουλο γεγονός το οποίο υπάρχει σε μια γνωσιακή βάση.



Εικόνα 4.3: HIDS

Πλεονεκτήματα των HIDS:

1. Ένα HIDS μπορεί να αναλύσει δραστηριότητες με μεγάλη αξιοπιστία και ακρίβεια ως αποτέλεσμα της μεγάλης ποσότητας πληροφορίας που μπορεί να συλλέξει από ένα σύστημα.
2. Ένα HIDS μπορεί να προβλέψει το αποτέλεσμα μιας επίθεσης.
3. Ένα HIDS μπορεί να ανταπεξέλθει απέναντι στο πρόβλημα που δημιουργούν κρυπτογραφημένα περιβάλλοντα.
4. Δεν επηρεάζεται από switch-based δίκτυα

Μειονεκτήματα των HIDS:

1. Ο μεγάλος αριθμός των συσκευών που παρακολουθούνται συντελεί στην αύξηση της δυσκολίας διαχείρισής τους.
2. Ένα HIDS μπορεί να γίνει στόχος επίθεσης και ο επιτιθέμενος να το βγάλει εκτός λειτουργίας.
3. Ένα HIDS δεν είναι κατάλληλο για τον εντοπισμό επιθέσεων που έχουν στόχο ολόκληρο το δίκτυο (όπως, για παράδειγμα, επιθέσεις σάρωσης του δικτύου).
4. Χρειάζεται επιπλέον πόρους αποθήκευσης στο σύστημα.
5. Επιβαρύνουν με ένα κόστος απόδοσης το σύστημα που παρακολουθείται.

Υβριδικά / κατανεμημένα εργαλεία ανίχνευσης εισβολής **(Hybrid**/ **Distributed Intrusion Detection Systems)**: Αποτελούνται από ένα συνδυασμό HIDS και NIDS.

4.2.2 Μοντέλα ανίχνευσης

Η τεχνολογία των IDS χρησιμοποιεί πολλές μεθοδολογίες ώστε να εντοπίσει συμβάντα και πολλές από αυτές επίσης χρησιμοποιούν πολλές μεθοδολογίες, είτε ξεχωριστά είτε ταυτόχρονα, ώστε να επιτύχουν πιο ακριβή αποτελέσματα. Παρακάτω θα αναφερθούν οι δύο πιο σημαντικές μεθοδολογίες.

α. ***Εντοπισμός βασισμένος σε ανωμαλία*** **(Anomaly Detection)**: Αυτή η μεθοδολογία βασίζεται στο συμπέρασμα ότι η κακόβουλη συμπεριφορά θα διαφέρει από μία φυσιολογική συμπεριφορά του συστήματος. Είναι,

λοιπόν, η διαδικασία σύγκρισης του τι θεωρείται φυσιολογικό με ο,τιδήποτε αποκλίνει από μία φυσιολογική συμπεριφορά.

β. ***Εντοπισμός βασισμένος στην υπογραφή*** **(Signature- based Detection)**: Αυτή η μεθοδολογία βασίζεται στη σύγκριση μιας δραστηριότητας του συστήματος που περιγράφει μία γνωστή επίθεση. Αλλιώς ονομάζεται εντοπισμός κακόβουλης χρήσης ή εντοπισμός βασισμένος σε κανόνες. Αυτού του τύπου τα IDS αναλύουν τη συσκευή ή το δίκτυο και συγκρίνουν τη δραστηριότητα με γνωστή δραστηριότητα από επιθέσεις, ψάχνουν, δηλαδή, για γνωστές υπογραφές ή αλλιώς μοτίβα. Με αυτό τον τρόπο μπορούν να εντοπίσουν πιθανές επιθέσεις. Αυτή η μεθοδολογία είναι πολύ αποδοτική στο να εντοπίζει γνωστές επιθέσεις, αλλά όχι να εντοπίζει άγνωστες επιθέσεις που χρησιμοποιούν τεχνικές αποφυγής εντοπισμού.

4.2.3 Μηχανισμοί απόκρισης

Αυτοί οι μηχανισμοί περιγράφουν την αντίδραση ενός IDS σε περίπτωση επίθεσης ή εισβολής.

α. Παθητικός μηχανισμός απόκρισης: Αυτού του είδους οι μηχανισμοί έχουν ως σκοπό να ενημερώνουν για ένα συμβάν χωρίς να προβαίνουν σε περαιτέρω δράσεις.

β. Ενεργητικός μηχανισμός απόκρισης: Αυτού του είδους οι μηχανισμοί μπορούν να απαντήσουν στο γεγονός αναλαμβάνοντας δράση ανάλογα με την περίπτωση.

5. IDS στο Cloud

Σε ένα περιβάλλον cloud ένα IDS είναι επίσης σημαντικό. Οι χρήστες του cloud δεν μπορούν πάντα να εξαρτώνται από τους παρόχους σε θέματα υποδομής στην ασφάλεια. Μπορεί να χρειαστεί να παρακολουθήσουν και να προστατέψουν τις ενέργειές τους στο cloud χρησιμοποιώντας ένα IDS παράλληλα με άλλες τεχνολογίες διαδικτυακής ασφάλειας, όπως firewalls, μεθόδους ελέγχου πρόσβασης και κρυπτογράφηση δεδομένων.

Ως αποτέλεσμα, οι χρήστες του cloud, χρειάζεται να είναι ικανοί να εφαρμόζουν συστήματα ανίχνευσης μέσα στα εικονικά τους όρια.

Το IDS στο Cloud έχει τις παρακάτω απαιτήσεις:

- Το IDS θα πρέπει να παρακολουθεί πολλαπλές εικονικές μηχανές ταυτόχρονα.

- Οι χρήστες του cloud θα πρέπει να έχουν στα χέρια τους τη διαχείριση του IDS.

- Ένα IDS που είναι βασισμένο στο cloud θα πρέπει να είναι ικανό να ενσωματώνει προσαρμοσμένους κανόνες (υπογραφές σεναρίων επίθεσης). Αυτοί οι προσαρμοσμένοι κανόνες θα μπορούν να συντεθούν από έναν υπεύθυνο ασφάλειας.

- Οι χρήστες του cloud θα πρέπει να έχουν τη δυνατότητα να κλιμακώσουν την κάλυψη ασφάλειας των εφαρμογών τους, με βάση τον όγκο και την τοποθεσία των δεδομένων που αναλύονται.

5.1 Ανίχνευση εισβολών σε περιβάλλον Cloud

Η αρχιτεκτονική ανίχνευσης εισβολών που βασίζεται σε περιβάλλον cloud (IDCC), αναπτύχθηκε ώστε να επιτευχθεί ένας τρόπος παγκόσμιας επίβλεψης πόρων κάποιου δικτύου και να βοηθήσει στην ανακάλυψη συγχρονισμένων επιθέσεων. Αυτή η αρχιτεκτονική αποτελείται από δύο κύρια μέρη, την τοπική σύνδεση και την παγκόσμια σύνδεση.

Για το παγκόσμιο μέρος χρησιμοποιούμε την ονομασία Κέντρο Δεδομένων Υπολογιστικών Νεφών (Cloud Computing Data Center – CCDC). Κάθε μέρος έχει το δικό του αναλυτή με επιμέρους βάσεις δεδομένων. Κάθε τοπική σύνδεση αποτελείται από πολλαπλούς αισθητήρες ώστε να συλλέγεται κίνηση δικτύου ανάμεσα στους τοπικούς κόμβους. Αυτοί οι αισθητήρες παράγουν αρχεία καταγραφής από πηγές όπως αυτόνομα IDS, firewalls ή από οποιοδήποτε σύστημα το οποίο μπορεί να παράγει αρχεία καταγραφής.

Γενικά οι τοπικοί ελεγκτές (local controllers- LC), σε κάθε τοπική δικτύωση, διαμορφώνουν τα αρχεία καταγραφής που παράγονται από τους αισθητήρες και τα αποθηκεύουν σε μια τοπική βάση δεδομένων (Local Intrusion Data Base – LIDB). Εάν υπάρχουν πολλοί τοπικοί ελεγκτές, ένας κύριος τοπικός ελεγκτής (master LC) χρησιμοποιείται ώστε να συντονίζει τους υπόλοιπους.

Με τον ίδιο τρόπο ένας τοπικός αναλυτής (local analyzer- LA) χρησιμοποιείται για την ανάλυση των δεδομένων που συλλέγονται στην LIDB και παράγει ειδοποιήσεις που βασίζονται στους προκαθορισμένους κανόνες. Ο τοπικός αναλυτής συνδυάζει παρόμοιες ειδοποιήσεις και τις στέλνει σε μια παγκόσμια βάση δεδομένων (Global Intrusion Data Base – GIDB) στο CCDC για περαιτέρω ανάλυση. Δηλαδή, η GIDB χρησιμοποιείται σαν μια μεγάλη βάση δεδομένων για τις ειδοποιήσεις που παράγονται από τις τοπικές πηγές.

Ο παγκόσμιος αναλυτής (GA) αναλύει τις ειδοποιήσεις που συγκεντρώνονται στην GIDB και ψάχνει για σύνθετα μοτίβα επιθέσεων που πραγματοποιούνται εναντίον των τοπικών πηγών. Όταν ανιχνευθεί μία απειλή από τον παγκόσμιο αναλυτή, ο τοπικός υπεύθυνος ασφάλειας ενημερώνεται ώστε να προβεί στις

απαραίτητες δράσεις, όπως να συμπεριλάβει την πηγή της επίθεσης σε μία μαύρη λίστα.

Η προτεινόμενη αρχιτεκτονική ταιριάζει περισσότερο σε ιδιωτικά clouds που είναι σχεδιασμένα με αυτό τον τύπο υποδομής λόγω της ικανότητας επικοινωνίας μεταξύ τοπικών και παγκόσμιων πηγών. Αυτό έχει σαν αποτέλεσμα, οι χρήστες ενός τέτοιου cloud να είναι πιο εξαρτημένοι από τους παρόχους σε θέματα διαχείρισης IDS.

5.2 Συνεργαζόμενα κατανεμημένα συστήματα ανίχνευσης εισβολών

Ο κύριος στόχος ενός συνεργαζόμενου κατανεμημένου συστήματος ανίχνευσης εισβολών (distributed intrusion detection system – DIDS), είναι να μειωθούν οι επιπτώσεις που θα δημιουργούνταν από μια επίθεση άρνησης υπηρεσίας (DOS) ή μια επίθεση κατανεμημένης άρνησης υπηρεσίας (DDOS), μέσω του διαμοιρασμού ειδοποίησεων μεταξύ πολλαπλών IDS, τα οποία βρίσκονται σε διαφορετικές περιοχές του cloud [11].

Εάν κάποιο σύστημα βρίσκεται σε κατάσταση επίθεσης άρνησης υπηρεσίας, μπορεί να διαμοιράσει πληροφορία και να ενημερώσει και άλλα συστήματα τα οποία βρίσκονται στο cloud, πριν ο επιτιθέμενος καταφέρει να πλημμυρίσει με πακέτα και τα υπόλοιπα συστηματα. Ως αποτέλεσμα, τα υπόλοιπα συστήματα μπορούν να αποφύγουν μια τέτοια επίθεση, λαμβάνοντας μέτρα όπως τον αποκλεισμό της πηγής που ανέφερε την επίθεση.

Τα μηνύματα μεταξύ των IDS ανταλλάσονται σε μορφή XML με το πρωτόκολλο ανταλλαγής μυνημάτων ανίχνευσης εισβολών (Intrusion Detection Message Exchange Format- IDMEF). Αυτή η μέθοδος επικοινωνίας μεταξύ των κόμβων των IDS βοηθάει στην διαδικασία αφομοίωσης νέων IDS στην υπάρχουσα διάταξη των IDS.
Κάθε IDS έχει τη δυνατότητα να επαληθεύει την αυθεντικότητα μιας ειδοποίησης, η οποία έχει σταλεί από ένα συνεργαργαζόμενο IDS. Για να

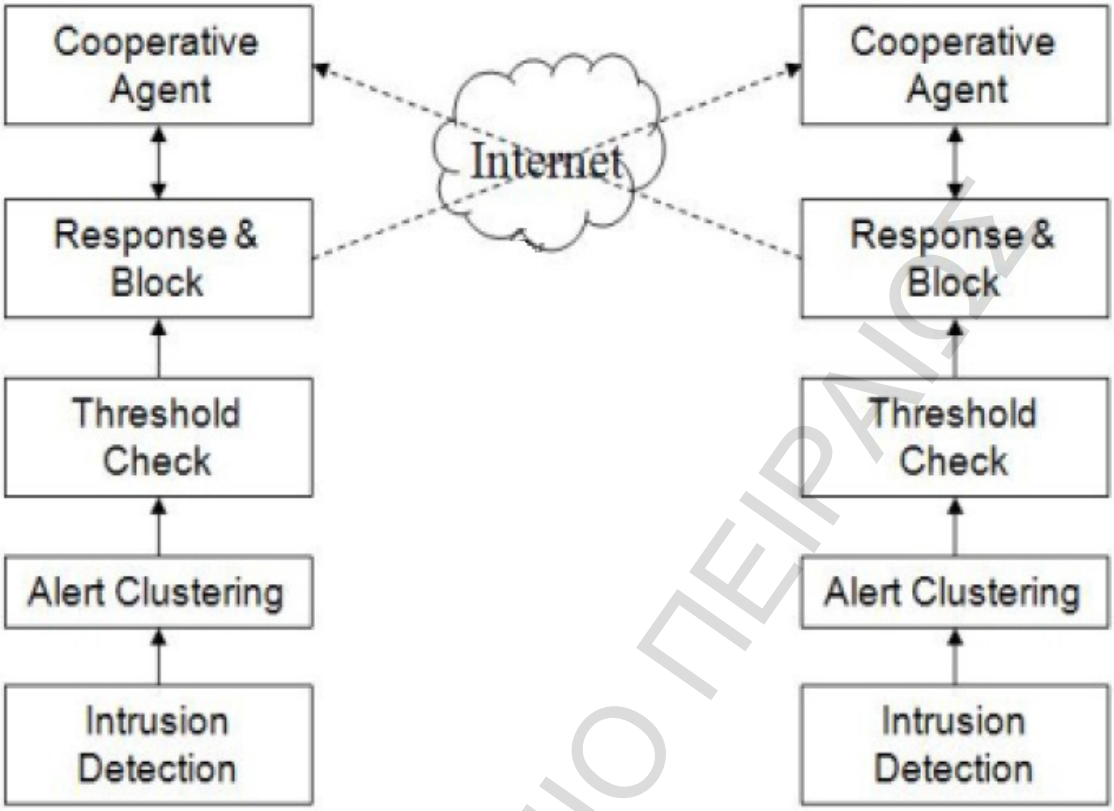
επιτευχθεί αυτός ο σκοπός το κάθε συνεργαζόμενο IDS χρησιμοποιεί τη διαδικασία ψήφου πλειοψηφίας, ώστε να κρίνει την εγκυρότητα των ειδοποιήσεων που εκπέμπονται από άλλα IDS και να δημιουργήσει ένα νέο κανόνα αποκλεισμού στη βάση δεδομένων τοπικών κανόνων, σε περίπτωση που η ειδοποίηση είναι έγκυρη. Εάν μια ειδοποίηση αποτύχει να περάσει τη δοκιμασία της διαδικασίας ψήφου πλειοψηφίας, το τοπικό IDS την αγνοεί.

Όπως βλέπουμε στην παρακάτω εικόνα το συνεργαζόμενο κατανεμημένο σύστημα ανίχνευσης εισβολών έχει πέντε κύρια συστατικά:

- Ανίχνευση εισβολής (Intrusion Detection): Το μέρος της ανίχνευσης εισβολής υλοποιείται με τη χρήση ενός NIDS που είναι βασισμένο σε κανόνες, ώστε να συλλέγεται κίνηση δικτύου.
- Συσταδοποίηση ειδοποιήσεων (Alert Clustering): Αυτό το μέρος χρησιμοποιείται ώστε να ομαδοποιεί παρόμοιες ειδοποιήσεις και να αποφασίζει εάν χρειάζεται να απορριφθούν ύποπτα πακέτα δικτύου.
- Έλεγχος κατωφλίου (Threshold Check): Παίρνει τη σκυτάλη από τη συσταδοποίηση ειδοποιήσεων σε περίπτωση ύποπτων πακέτων και πραγματοποιεί επιπλέον έρευνες σε αυτά, σύμφωνα με προκαθορισμένους κανόνες κατωφλίου.

Στα δύο παραπάνω μέρη, έχουμε απόρριψη όλων των πακέτων που δημιουργούν ειδοποιήσεις οι οποίες είναι πολύ σοβαρές. Επιπλέον, η πηγή που παρήγαγε αυτά τα πακέτα προστίθεται σε μία μαύρη λίστα ή πιο επίσημα έναν πίνακα αποκλεισμού.

- Απάντηση και αποκλεισμός (Response and Block): Η κύρια λειτουργία αυτού του μέρους είναι να μην επιτρέπει τη ροή μη επιθυμητών πακέτων στο τοπικό δίκτυο, όπως επίσης να εκπέμπει ειδοποιήσεις προς άλλα IDS.
- Συνεργαζόμενος πράκτορας (Cooperative agent): Είναι υπεύθυνος να στέλνει και να λαμβάνει ειδοποιήσεις, και να εφαρμόζει τον αλγόριθμο της διαδικασίας ψήφου πλειοψηφίας ώστε να επικυρώνει την αυθεντικότητα μιας ειδοποίησης.



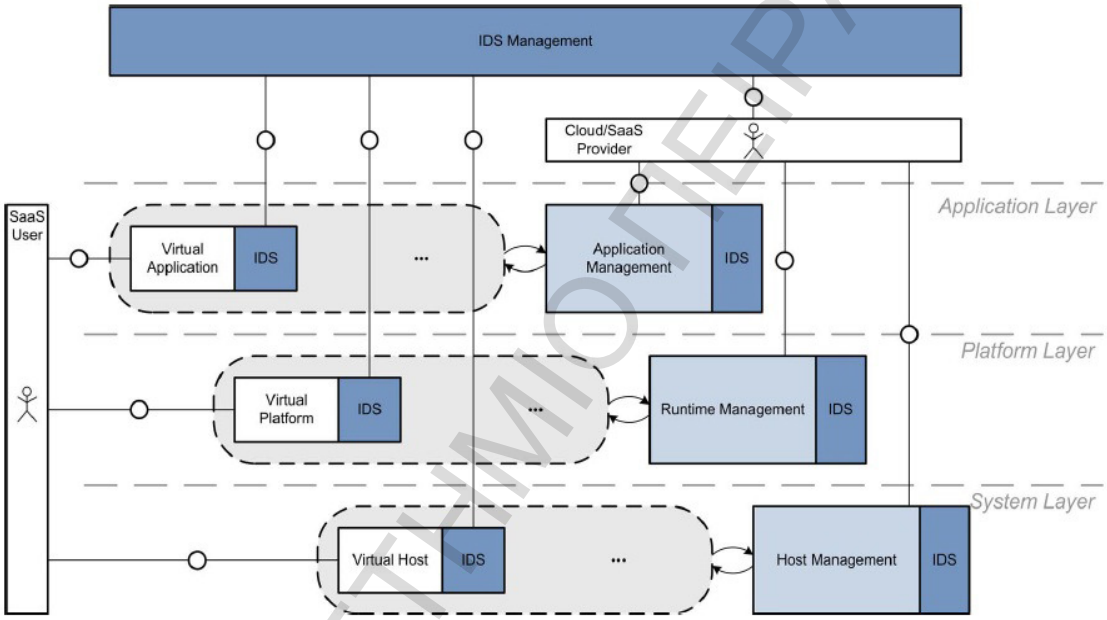
Εικόνα 5.1: DIDS

Ο κύριος σκοπός μιας επίθεσης άρνησης υπηρεσίας είναι να αναστείλει την πρόσβαση σε ένα υπολογιστικό σύστημα μέσω της υπερφόρτωσης των πόρων του με τη χρήση άσκοπων αιτημάτων. Αυτός ο τύπος ξαφνικής επίθεσης στα δίκτυα-θύματα μπορεί να προκαλέσει σημαντικές οικονομικές ζημιές σε σχέση με άλλες επιθέσεις [12].

Ένα συνεργαζόμενο κατανεμημένο σύστημα ανίχνευσης εισβολών είναι σχεδιασμένο επακριβώς ώστε να αντιτίθεται σε μια τέτοια επίθεση. Παρόλα αυτά η χρήση του συνεργαζόμενου πράκτορα και το σύστημα ψήφου πλειοψηφίας προσθέτουν επιπλέον πολυπλοκότητα στο υπάρχον σύστημα. Ως αποτέλεσμα ένα συνεργαζόμενο κατανεμημένο σύστημα ανίχνευσης εισβολών μπορεί να έχει μικρότερη απόδοση σε θέματα χρόνου υπολογισμού και ανίχνευσης διαφορετικών τύπων επιθέσεων από την άρνηση υπηρεσίας.

5.3 Ανίχνευση εισβολών στο Cloud (IDC)

Η ανάγκη για διαχείριση των IDS από τους πελάτες του cloud είναι μία από τις πιο σημαντικές απαιτήσεις που υπάρχουν κατά την υλοποίηση ενός IDS στο cloud. Στο σύγγραμμα Intrusion Detection In The Cloud (IDC) [13] προτείνεται η ιδέα μίας μερικής διαχείρισης του IDS από τους χρήστες του Cloud. Στην παρακάτω εικόνα βλέπουμε την προτεινόμενη αρχιτεκτονική.



Εικονα 5.2 : Partial user administration

Αυτή η αρχιτεκτονική αποτελείται από αρκετούς αισθητήρες και μία μονάδα κεντρικής διαχείρισης. Αυτή η ιδέα ενός κατανεμημένου IDS υλοποιείται και στα τρία επίπεδα του cloud (Επίπεδο εφαρμογής, επίπεδο πλατφόρμας, επίπεδο συστήματος), η οποία συμπεριλαμβάνει ένα συνδυασμό από αισθητήρες HIDS και NIDS.

Το HIDS περιλαμβάνεται σε κάθε VM που ξεκινάει κάποιος χρήστης. Από την άλλη οι αισθητήρες των NIDS τοποθετούνται σε κάθε επίπεδο του cloud ώστε να είναι δυνατή η παρακολούθηση του κάθε στρώματος. Στη μονάδα της κεντρικής διαχείρισης, οι ειδοποιήσεις όλων των στρωμάτων του cloud μπορούν να συνδυαστούν και να αναλυθούν. Επιπλέον οι πελάτες του cloud

έχουν τη δυνατότητα να επιλέξουν ποιους κανόνες θέλουν να χρησιμοποιήσουν, σύμφωνα με τις ανάγκες των εφαρμογών τους. Το πρωτόκολλο IDMEF χρησιμοποιείται για την επικοινωνία μεταξύ διαφορετικών τύπων αισθητήρων, ώστε να γίνεται η ανταλλαγή μυνημάτων ειδοποιήσεων.

Ένα από τα κύρια ζητήματα που δημιουργούνται με αυτή την προσέγγιση, είναι ο μεγάλος βαθμός εξάρτησης των χρηστών από τον πάροχο του cloud. Ο πάροχος είναι αυτός που θα υλοποιήσει τα κύρια μέρη του περιβάλλοντος του IDS, όπως τη μονάδα κεντρικής διαχείρισης, το HIDS για κάθε VM, την βάση δεδομένων υπογραφών και τα κανάλια επικοινωνίας μεταξύ των VM και της κεντρικής μονάδας διαχείρισης.

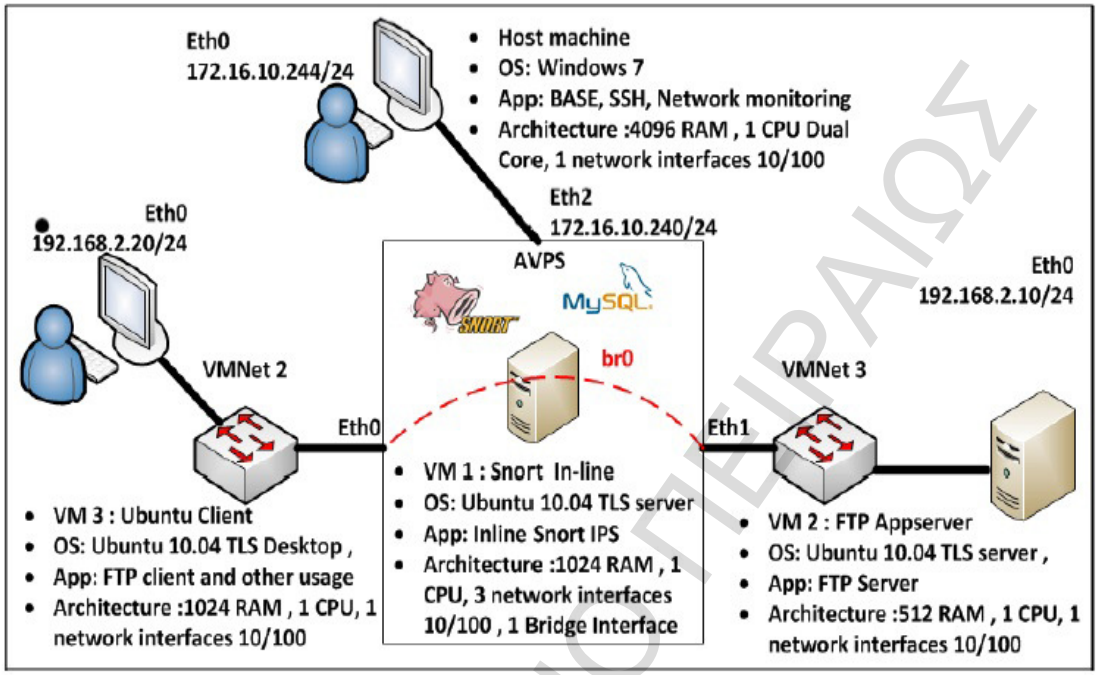
Οι χρήστες του cloud βασίζονται εξ ολοκλήρου στην υποδομή του παρόχου, αλλά έχουν ένα μερικό έλεγχο πάνω στην κεντρική μονάδα διαχείρισης. Αυτό γίνεται με τη δημιουργία και χρήση προσαρμοσμένων κανόνων, ώστε να παρακολουθούν τις εφαρμογές τους. Επιπλέον, δημιουργούνται και θέματα ιδιωτικότητας από την ενσωμάτωση μερών του IDS, τα οποία εγκαθιστά ο πάροχος, σε κάθε εικονική μηχανή.

5.4 Αυτόνομο σύστημα πρόληψης παραβίασης (AVPS)

Στην πλειοψηφία της η προτεινόμενη έρευνα πάνω σε θέματα IDS σε περιβάλλοντα cloud, επικεντρώνεται στην παροχή μηχανισμών ανίχνευσης εισβολών για συγκεκριμένα ζητήματα ασφάλειας. Το αυτόνομο σύστημα πρόληψης παραβίασης (AVPS) [14] επικεντρώνεται στην προστασία από την παραβίαση πολιτικών ασφάλειας που προέρχεται από χρήστες με πολλά προνόμια στο σύστημα. Η προστασία αυτή επιτυγχάνεται με τη συνεχή παρακολούθηση της κίνησης του δικτύου για παραβιάσεις των πολιτικών του συστήματος.

Στο σχεδιασμό ενός αυτόνομου συστήματος πρόληψης, χρησιμοποιούνται κανόνες γεγονότων-προϋποθέσεων-δράσεων (Events-Conditions-Actions rules

– ECA) [15]. Η επόμενη εικόνα περιγράφει την δομή του δικτύου για ένα τέτοιο περιβάλλον.

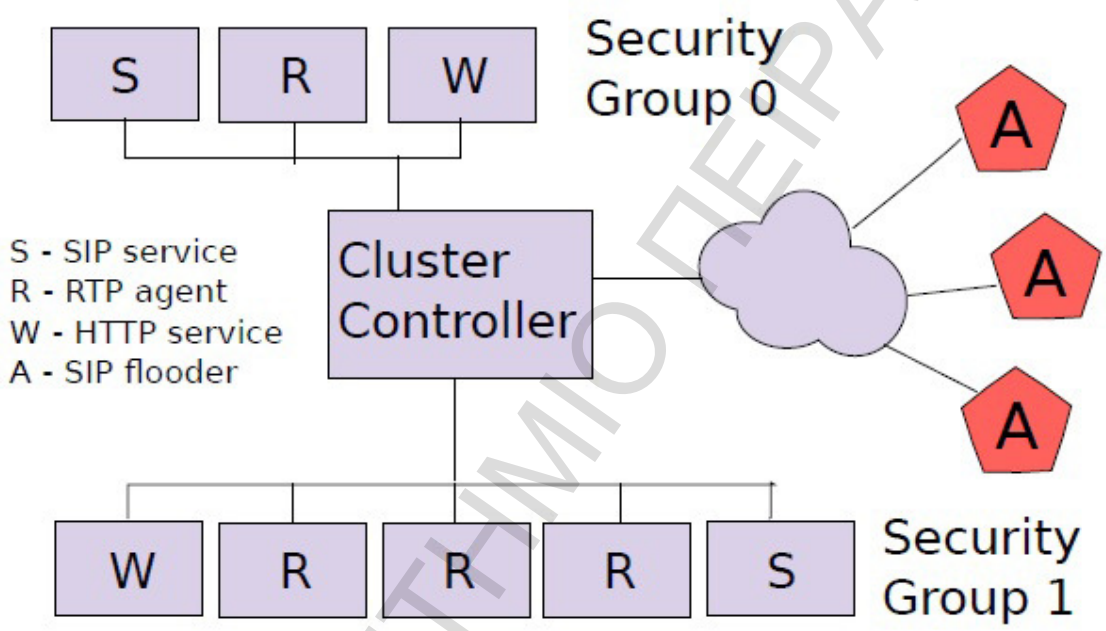


Εικονα 5.3: AVPS

Οι δημιουργοί του AVPS προτείνουν πως μπορεί να χρησιμοποιηθεί σε εικονικά περιβάλλοντα όπως το cloud. Όμως το AVPS δεν έχει διαμορφωθεί ώστε να πληροί αρκετά κριτήρια που είναι αναγκαία για ένα περιβάλλον cloud. Για παράδειγμα, χρειάζεται κλιμάκωση του συστήματος για πολλαπλούς κόμβους IDS ώστε να είναι δυνατή η σωστή λειτουργία του και για να μπορεί να ανταπεξέλθει στο μεγάλο αριθμό αιτημάτων. Επιπλέον δεν καλύπτει την ανάγκη υποστήριξης της κατανεμημένης φύσης του cloud, δηλαδή την προστασία πολλαπλών εφαρμογών σε διαφορετικές τοποθεσίες.

5.5 Ενσωματώνοντας ενα δικτυακό σύστημα ανίχνευσης εισβολών σε περιβάλλον cloud

Άλλη μια ιδέα για την εφαρμογή ενός IDS σε περιβάλλον cloud [16] είναι τοποθέτηση πολλαπλών υπαρχόντων IDS κοντά σε κάθε φυσικό ελεγκτή του cloud, που παρακολουθούν ένα μικρό μέρος της κίνησης του δικτύου για μία ομάδα εικονικών μηχανών. Στην παρακάτω εικόνα βλέπουμε τη γενική δομή αυτής της προσέγγισης.



Εικόνα 5.4 : Cluster Controller IDCS

Η γενική δομή αυτής της προσέγγισης απαιτεί μεγάλη αλλαγή των φυσικών εφαρμογών των πόρων του cloud, που έχει ως αποτέλεσμα τη μεγάλη εξάρτηση μεταξύ των μερών του IDS και της υποδομής των παρόχων του cloud. Ως αποτέλεσμα, η διαδικασία διαχείρισης του IDS από τους χρήστες περιορίζεται από την έλλειψη παραμετροποίησης.

6. Snort

Το snort είναι ένα IDS ανοιχτού κώδικα. Συνδυάζει τα ωφέλη των μεθόδων εντοπισμού μέσω υπογραφών και ανωμαλιών. Μπορεί να παραμετροποιηθεί ώστε να τρέξει με τρεις διαφορετικούς τρόπους.

1. Κατάσταση ανίχνευσης (Sniffer mode): Όταν εκτελείται με αυτό τον τρόπο διαβάζει τα πακέτα του δικτύου και τα προβάλλει σε συνεχή ροή στην οθόνη.
2. Κατάσταση καταγραφής πακέτου (Packet Logger mode): Καταγράφει τα πακέτα που διαβάζει στο δίσκο.
3. Κατάσταση εντοπισμού εισβολής στο δίκτυο (Network Intrusion Detection System mode): Είναι ο πιο πολύπλοκος τρόπος να εκτελεστεί το εργαλείο αυτό, το οποίο επιτρέπει στο snort να αναλύσει την κίνηση του δικτύου και να τη συγκρίνει με ένα σύνολο κανόνων και να εκτελέσει αρκετές δράσεις βασισμένες στο τι βλέπει.

6.1 Αρχιτεκτονική του snort

Το snort αποτελείται από πέντε κύρια μέρη: τον αποκωδικοποιητή πακέτου, τον προεπεξεργαστή, τη μηχανή εντοπισμού, την καταγραφή αρχείων και την ειδοποίηση.

Πριν εξηγήσουμε, αναλυτικά, την λειτουργία αυτών των μερών, θα περιγράψουμε τη ζωή ενός πακέτου μέσα στο snort. Τα εισερχόμενα πακέτα αρχικά αποκωδικοποιούνται από τον αποκωδικοποιητή πακέτου. Εάν το snort τρέχει σε κατάσταση ανίχνευσης, τα αποκωδικοποιημένα δεδομένα θα διαμορφωθούν για προβολή και θα προβληθούν στην οθόνη. Εάν τρέχει σε κατάσταση καταγραφής πακέτου, τα δεδομένα θα καταγραφούν είτε σε διαμόρφωση ASCII είτε σε ένα δυαδικό αρχείο. Εάν τρέχει ως NIDS, αφού

αναλυθεί το εισερχόμενο πακέτο από τον αποκωδικοποιητή, τότε τα δεδομένα στέλνονται προς οποιοδήποτε προεπεξεργαστή έχει ενεργοποιηθεί στο αρχείο παραμετροποίησης του snort. Τα δεδομένα στέλνονται στη μηχανή εντοπισμού που τα συγκρίνει με τους κανόνες που έχουν επιλεχθεί ως ενεργοί στο αρχείο παραμετροποίησης του snort. Οι επιτυχημένες συγκρίσεις στέλνονται στα μέρη του snort που ευθύνονται για τις ειδοποιήσεις και την καταγραφή, τα οποία θα καταγράψουν τα δεδομένα ή θα δημιουργήσουν ειδοποιήσεις αναλόγως με την παραμετροποίησή τους.

I. Αποκωδικοποιητής πακέτου

Η κύρια λειτουργία του αποκωδικοποιητή πακέτων είναι να διαχωρίζει ποιο πρωτόκολλο επικοινωνίας χρησιμοποιείται για κάθε εισερχόμενο πακέτο και να συγκρίνει τα δεδομένα με επιτρεπόμενη συμπεριφορά για πακέτα αυτού του πρωτοκόλλου. Επίσης, ο αποκωδικοποιητής πακέτων, μπορεί να δημιουργεί ειδοποιήσεις εάν εντοπίσει δύσμορφες κεφαλίδες πρωτοκόλλων, πολύ μεγάλα πακέτα ή ασυνήθιστες και λανθασμένες επιλογές TCP. Ο διαχειριστής του συστήματος μπορεί να ενεργοποιήσει ή να απενεργοποιήσει επιλογές ειδοποιήσεων από το αρχείο παραμέτρων του snort.

ii. Προεπεξεργαστής

Η κύρια λειτουργία του προεπεξεργαστή είναι να αναλύει εισερχόμενα δεδομένα σε τρόπους που μπορεί να είναι χρήσιμα. Τα δεδομένα φτάνουν στον προεπεξεργαστή αφού φύγουν από τον αποκωδικοποιητή πακέτου. Το snort έχει αρκετούς προεπεξεργαστές και μπορούν, για παράδειγμα, να εντοπίσουν σαρώσεις θυρών και να ακολουθήσουν ροές δεδομένων ώστε να εντοπίσουν συγκαλυμένη δραστηριότητα.

iii. Μηχανή εντοπισμού

Η μηχανή εντοπισμού είναι το κύριο κομάτι του snort. Κύρια λειτουργία της είναι να λαμβάνει δεδομένα από τον αποκωδικοποιητή πακέτων και τους προεπεξεργαστές και να τα συγκρίνει με τους κανόνες που έχουν δημιουργηθεί

στο αρχείο παραμέτρων. Είναι σημαντικό να γνωρίζουμε ότι το snort μπορεί να προβεί σε πολλαπλές συγκρίσεις και να δημιουργήσει πολλαπλές ειδοποιήσεις ερευνώντας ένα και μόνο πακέτο.

iv. Ειδοποιήσεις και αρχεία καταγραφής

Το τελευταίο βήμα του ταξιδιού ενός πακέτου στο snort είναι η δημιουργία ειδοποίησης και η καταγραφή. Ο μηχανισμός καταγραφής αρχείων θα αρχειοθετήσει τα πακέτα που ταιριάζουν με τους κανόνες που έχει δημιουργήσει ο χρήστης για το snort. Ο μηχανισμός ειδοποίησης χρησιμοποιείται για να ενημερώσει τον αναλυτή ότι ένας κανόνας έχει βρει μια επιτυχημένη σύγκριση. Το snort μας δίνει τη δυνατότητα να επιλέξουμε με ποιο τρόπο θα λαμβάνουμε τις ειδοποιήσεις και πώς να καταγράφουμε τα δεδομένα των πακέτων. Για παράδειγμα, ειδοποιήσεις μπορεί να στέλνονται σε κινητό τηλέφωνο μέσω γραπτού μηνύματος.

6.2 Κανόνες στο snort

Το snort είναι ένα IDS το οποίο χρησιμοποιεί περιγραφή κανόνων που είναι ελαφρά και ισχυρή. Ένας κανόνας αποτελείται από δύο λογικές οντότητες, την επικεφαλίδα και τις επιλογές των κανόνων. Η επικεφαλίδα περιέχει την δράση του κανόνα, το πρωτόκολο για το οποίο ενεργοποιείται και τις θύρες πηγής και προορισμού τις οποίες ελέγχει. Μια επιλογή κανόνα περιέχει μηνύματα ειδοποιήσεων και πληροφορίες για το ποιο κομμάτι ενός πακέτου θα πρέπει να ελεγχθεί, ωστε να αποφασιστεί αν κάποιος κανόνας θα πρέπει να αναλάβει δράση.

6.2.1 Επικεφαλίδα κανόνα

Η επικεφαλίδα κανόνα περιέχει την πληροφορία που καθορίζει τι θα γίνει στην περίπτωση που εμφανιστεί ένα πακέτο με όλες τις ιδιότητες που καθορίζονται στον κανόνα. Χωρίζεται σε πέντε κατηγορίες.

- Δράση του κανόνα
- Πρωτόκολλο
- Πληροφορία πηγής
- Πληροφορία προορισμού
- Κατεύθυνση

Δράση κανόνα

Όταν το snort εντοπίζει ένα πακέτο το οποίο ταιριάζει στα κριτήρια ενός κανόνα λαμβάνονται κάποιες δράσεις. Αυτές είναι οι ακόλουθες:

- Ειδοποίηση (alert): δημιουργείται μια ειδοποίηση χρησιμοποιώντας τη μέθοδο που έχει επιλεχθεί και ακολουθεί καταγραφή του πακέτου.
- Καταγραφή του πακέτου (log): γίνεται καταγραφή του πακέτου σε αρχείο.
- Ενεργοποίηση (activate): δημιουργείται μια ειδοποίηση και ύστερα ενεργοποιείται κάποιος άλλος δυναμικός κανόνας.
- Δυναμική δράση (dynamic): παραμονή σε ανενεργή φάση μέχρι να γίνει ενεργοποίηση από κάποιον κανόνα.
- Απόρριψη (drop): Μπλοκάρισμα και καταγραφή του πακέτου.
- S-Απόρριψη (sdrop): Μπλοκάρισμα και μη καταγραφή του πακέτου.

Πρωτόκολλο

Το snort μπορεί να αναλύσει ύποπτη συμπεριφορά για τέσσερα πρωτόκολλα: TCP, UDP, ICMP, IP.

Πληροφορία Πηγής – Πληροφορία Προορισμού

οι Πληροφορίες Πηγής και Προορισμού αποτελούνται από δύο μέρη, τη διεύθυνση IP και τη θύρα. Το πεδίο για τη διεύθυνση IP μπορεί να

περιλαμβάνει ένα από τα παρακάτω:

- Any: οποιαδήποτε διεύθυνση
- Μία συγκεκριμένη διεύθυνση
- Ένα ολόκληρο δίκτυο

Το μέρος που έχει να κάνει με τη θύρα μπορεί να καθοριστεί με διάφορους τρόπους, όπως: συμπεριλαμβάνοντας οποιαδήποτε θύρα (any), μία συγκεκριμένη θύρα, ένα εύρος αριθμού θυρών ή εξαίρεση κάποιων θυρών.

Κατεύθυνση

Το σύμβολο της κατεύθυνσης (->) δηλώνει τον προσανατολισμό ή την κατεύθυνση της κίνησης στην οποία αναφέρεται ένας κανόνας. Η διεύθυνση IP και ο αριθμός θύρας στην αριστερή πλευρά του συμβόλου θεωρείται ως η κίνηση που έρχεται από την πηγή.

6.2.2 Επιλογές κανόνα

Άλλο ένα σημαντικό μέρος ενός κανόνα στο snort είναι αυτό της επιλογής ενός κανόνα. Υπάρχουν τέσσερις κύριες κατηγορίες:

- Γενικές επιλογές: Παρέχουν πληροφορίες για τον κανόνα αλλά δεν παίζουν κάποιο ρόλο κατά τη διαδικασία της ανίχνευσης.
- Επιλογές φορτίου: Ελέγχουν για δεδομένα μέσα στο φορτίο ενός πακέτου.
- Επιλογές μη φορτίου: Ελέγχουν για δεδομένα στο υπόλοιπο πακέτο.
- Επιλογές μετά την ανίχνευση: Χρησιμοποιούνται ώστε να πυροδοτήσουν κανόνες ύστερα από την ενεργοποίηση ενός προηγούμενου κανόνα.

Για κάθε κατηγορία θα παραθέσουμε κάποια παραδείγματα.

Α. Γενικές επιλογές

- Msg: Αυτή η λέξη κλειδί δηλώνει στη μηχανή καταγραφής και ειδοποίησης ποιο μήνυμα θα εμφανίσουν κατά την καταγραφή του πακέτου.
- Reference: Αυτή η λέξη κλειδί επιτρέπει στους κανόνες να συμπεριλαμβάνουν αναφορές σε εξωτερικά συστήματα αναγνώρισης επιθέσεων.
- Gid: Χρησιμοποιείται ώστε να αναγνωριστεί ποιο μέρος του snort δημιουργεί το γεγονός όταν ενεργοποιείται ένας συγκεκριμένος κανόνας.
- Sid: Χρησιμοποιείται ώστε να αναγνωρίζεται ξεχωριστά κάθε κανόνας του snort.
- Classtype: Χρησιμοποιείται ώστε να κατηγοριοποιηθεί από έναν κανόνα μια επίθεση η οποία είναι μέρος μιας πιο γενικής ομάδας επιθέσεων.
- Priority: Αυτή η λέξη κλειδί δηλώνει το βαθμό επικινδυνότητας της επίθεσης για την οποία έχει δημιουργηθεί ο κανόνας.
- Metadata: Επιτρέπει στο δημιουργό του κανόνα να συμπεριλάβει περισσότερες πληροφορίες για τον κανόνα.

Β. Επιλογές σχετικές με το φορτίο του πακέτου

- Content: Αυτή η επιλογή επιτρέπει στο χρήστη να δημιουργήσει κανόνες που ψάχνουν για συγκεκριμένο περιεχόμενο στο φορτίο του πακέτου και να ενεργοποιήσουν απαντήσεις βασισμένες στα δεδομένα.
- Rawbytes: Επιτρέπει στους κανόνες να ψάξουν στα δεδομένα του πακέτου αγνωώντας οποιαδήποτε κωδικοποίηση έχει γίνει από τους

προεπεξεργαστές.

- Depth: Επιτρέπει στο χρήστη να δημιουργήσει κανόνες, στους οποίους μπορεί να οριστεί πόσο βαθιά μέσα στο πακέτο θα πρέπει να ψάξει το snort για ένα συγκεκριμένο μοτίβο.
- Offset: Επιτρέπει στο χρήστη να δημιουργήσει κανόνες, στους οποίους μπορεί να οριστεί πόσο βαθιά μέσα στο πακέτο θα ξεκινήσει να ψάχνει το snort για ένα συγκεκριμένο μοτίβο.

Γ. Επιλογές μη σχετικές με το φορτίο του πακέτου

- Flow: Αυτή η λέξη κλειδί επιτρέπει στους κανόνες να εφαρμόζονται σε συγκεκριμένες κατευθύνσεις της ροής των δεδομένων.
- Flags: Χρησιμοποιείται για να ελέγξει εάν υπάρχουν κάποια συγκεκριμένα bits που σχετίζονται με τα TCP flags.
- Ttl: Χρησιμοποιείται για να ελέγξει την τιμή ttl (χρόνος ζωής ενός πακέτου).
- Ack: Χρησιμοποιείται για να ελέγξει την τιμή ACK (δηλώνει ότι έχει ληφθεί ένα πακέτο σύμφωνα με το πρωτόκολλο TCP).
- Window: Χρησιμοποιείται για να ελέγξει την τιμή Window size (όγκος δεδομένων σε συγκεκριμένο χρόνο).

Δ. Επιλογές μετά την ανίχνευση

- Logto: Αυτή η λέξη κλειδί επισημαίνει στο snort να καταγράψει όλα τα πακέτα που ενεργοποιούν αυτόν τον κανόνα σε ένα ξεχωριστό αρχείο καταγραφής.
- session: Χρησιμοποιείται για να εξάγει δεδομένα χρήστη από συνόδους TCP.
- React: Δίνει τη δυνατότητα να κλείνει η σύνδεση όταν ένας συγκεκριμένος

κανόνας του snort ενεργοποιείται.

- tag: Επιτρέπει την καταγραφή περισσότερων του ενός πακέτων που ενεργοποίησαν τον κανόνα.
- Activated by: Επιτρέπει στο δημιουργό κανόνων να ενεργοποιεί δυναμικά έναν κανόνα, όταν ένας συγκεκριμένος κανόνας με τη λέξη κλειδί activate ενεργοποιείται.

6.2.3 Τεχνικές για τη δημιουργία σωστών κανόνων

Εάν θέλουμε να έχουμε ένα αποδοτικό NIDS, ο αναλυτής πρέπει να γράψει σωστούς κανόνες. Ο αναλυτής πρέπει να φτιάξει τους κανόνες όσο το δυνατόν πιο ισχυρούς και ακριβείς.

Πρώτα από όλα ένας σωστός κανόνας πρέπει να είναι συγκεκριμένος, ακριβής και σαφής. Δημιουργεί ειδοποιήσεις σε σχετικά δεδομένα που είναι απειλή για το δίκτυο και το κάνει αυτό με ενδεδειγμένο τρόπο. Με αυτό το τρόπο, ο αναλυτής έχει την πληροφορία που χρειάζεται ώστε να αποφασίσει εάν πρέπει να δράσει έχοντας δει κάποια ειδοποίηση ή να την αγνοήσει. Επίσης, ένας σωστός κανόνας πρέπει να δημιουργεί όσο το δυνατόν λιγότερες λανθασμένες ειδοποιήσεις, αλλά επίσης να δημιουργεί ειδοποιήσεις καθέ φορά που χρειάζεται. Να περιέχει μια ακριβή περιγραφή της επίθεσης, και αναφορές για περαιτέρω έρευνα.

Για να ελαχιστοποιηθεί ο αριθμός των λανθασμένων ειδοποιήσεων, θα πρέπει να ληφθεί σοβαρά υπόψη το κύριο μέρος του κανόνα, και πιο συγκεκριμένα, το περιεχόμενο της υπογραφής των επιθέσεων. Συγκεκριμένα, ένα από τα σημαντικότερα βήματα που ο αναλυτής πρέπει να κάνει, είναι να δημιουργήσει το σωστό περιεχόμενο του κανόνα, όπως επίσης να καθορίσει τις σωστές δράσεις για τους κανόνες.

Σε αυτό το στάδιο, ο αναλυτής έχει δύο επιλογές, την καταγραφή και την ειδοποίηση. Το πρώτο βήμα ώστε να επιλεχθεί η σωστή δράση είναι να

αποφασιστεί σε ποιά κατηγορία ανήκει ο κανόνας. Ο αναλυτής πρέπει να αποφασίσει εάν η επίθεση επηρρεάζει κρίσιμα μέρη του συστήματος ή εάν θέτει ευθέως σε κίνδυνο το σύστημα. Εάν η απάντηση είναι θετική, τότε η δράση του κανόνα είναι στην κατηγορία της ειδοποίησης. Σε άλλη περίπτωση, μπορεί να γίνει απλά μία καταγραφή.

Γενικά, τα δεδομένα καταγράφονται όταν μπορούν να χρησιμοποιηθούν για να αναγνωριστεί ένας επιτιθέμενος ή για να χρησιμοποιηθούν νομικά εναντίον ενός επιτιθέμενου. Επίσης τα καταγεγραμμένα δεδομένα, παρέχουν επιπλέον πληροφορία για τις επιθέσεις.

Επίσης, πρέπει να λάβουμε υπόψη μας, ότι όταν δηλώνουμε υπομάσκες δικτύου μέσα στους κανόνες, χρησιμοποιούμε πόρους της CPU. Αυτό σημαίνει πως εάν συγχωνευθούν υπομάσκες δικτύου, χρησιμοποιούμε λιγότερους πόρους και μεγαλώνουμε την χρησιμότητα του IDS. Η συγχώνευση των υπομασκών δικτύου είναι μία διαδικασία η οποία προκαθορίζεται εκτός του περιβάλλοντος του snort.

Τελικά, το πιο σημαντικό πράγμα κατά την συγγραφή κανόνων είναι η αποφυγή δημιουργίας πολύ γενικών κανόνων, οι οποίοι θα έχουν ως αποτέλεσμα τη δημιουργία πολλών λανθασμένων ειδοποιήσεων ή θα έχουν ως αποτέλεσμα την παράλειψη καταγραφής ή ειδοποίησης για γεγονότα που είχαν σχεδιαστεί να πιάσουν.

7. Εφαρμογή ενός NIDS σε προσομοιωμένο περιβαλλον Cloud

7.1 Γενικά

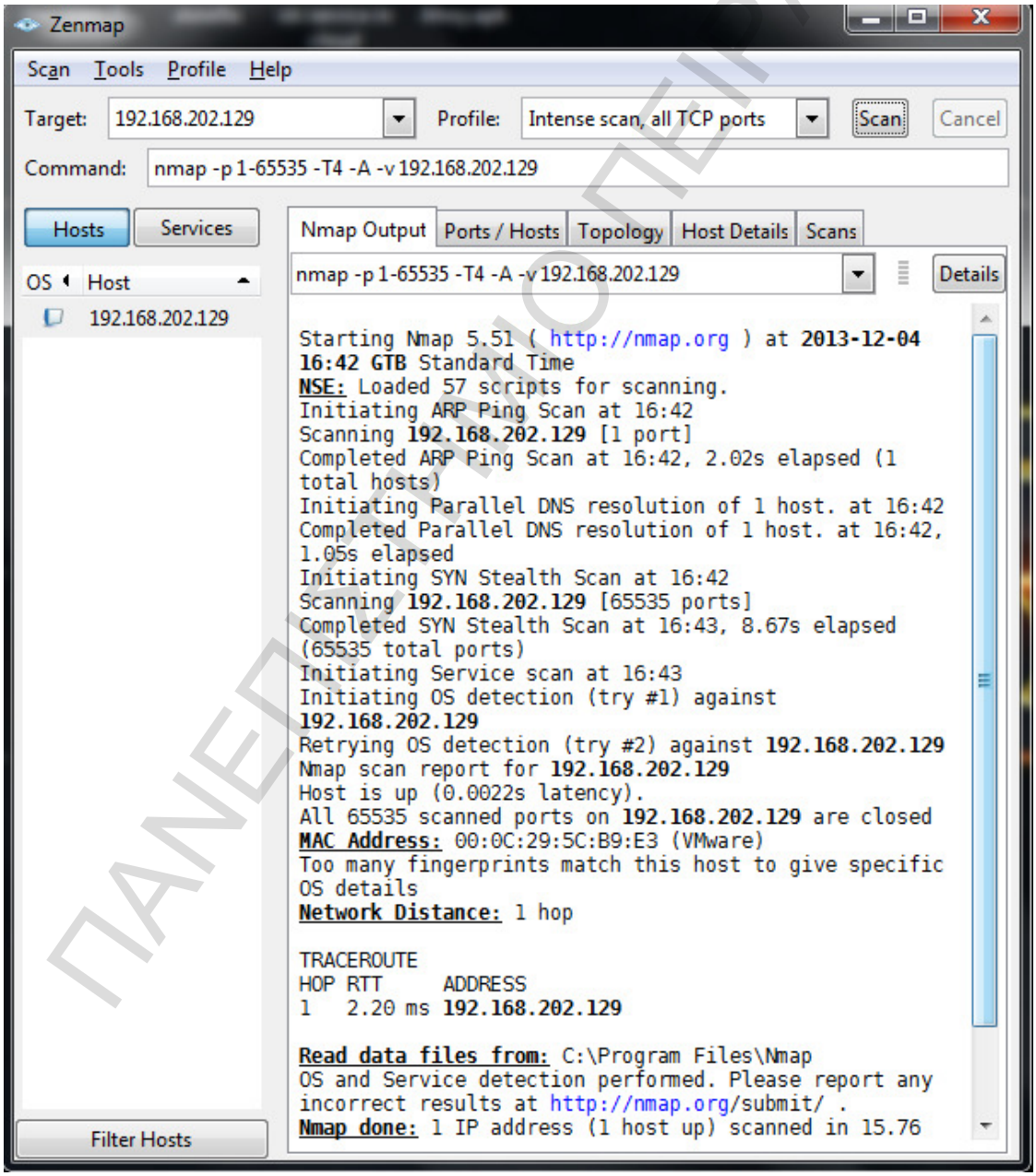
Όπως αναφέραμε, παραπάνω, ως στόχο έχουμε ορίσει να δούμε εάν ένα εργαλείο ασφάλειας, όπως ένα IDS, μπορεί να ανταπεξέλθει στις ανάγκες ασφάλειας ενός περιβάλλοντος cloud, αντιμετωπίζοντας διάφορους τύπους επιθέσεων.

Για αυτό το λόγο, λοιπόν, έγινε προσομοίωση ενός περιβάλλοντος cloud με τη χρήση εικονικών μηχανών οι οποίες δημιουργήθηκαν με τη βοήθεια του εργαλείου Vmware workstation. Επίσης, α χρησιμοποιήθηκε το NIDS snort για τις ανάγκες του intrusion detection, το οποίο εγκαταστάθηκε στο host λειτουργικό σύστημα, και όχι μέσα σε κάποια εικονική μηχανή. Με αυτόν τον τρόπο ο υπολογιστής έχει τις ιδιότητες ενός server στον οποίο τρέχουν οι εικονικές μηχανές, ανεξάρτητα η μία από την άλλη, και το IDS παρακολουθεί τη δικτυακή κίνηση από και προς τις εικονικές μηχανές, καθώς και του κεντρικού λειτουργικού.

Με αυτή τη δομή έγινε προσομοίωση διαφόρων τύπων επιθέσεων από τη μία εικονική μηχανή στην άλλη. Σε αυτό το κεφάλαιο θα παρουσιαστούν τα σενάρια που υλοποιήθηκαν.

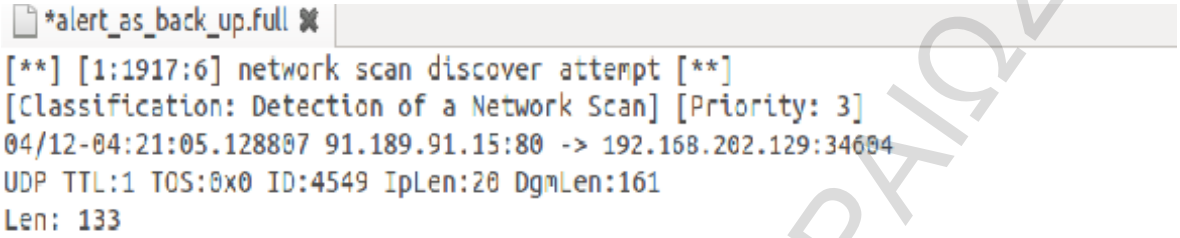
7.2 Επίθεση χαρτογράφησης δικτύου

Το πρώτο βήμα ενός επιτιθέμενου εναντίον ενός συστήματος είναι η χαρτογράφηση του δικτύου, ώστε να γνωρίζει τι μηχανές τρέχουν και τι υπηρεσίες και θύρες είναι ενεργές. Μια τέτοια επίθεση είναι πιθανή και στο cloud. Αρχικά έγινε προσπάθεια, από την πλευρά του επιτιθέμενου, να χαρτογραφηθεί το δίκτυο (local machine) και αφού εντοπίστηκε κάποια εικονική μηχανή έγινε προσπάθεια πιο βαθιάς χαρτογράφησης αυτής της μηχανής.



Εικόνα 7.1: zenmap scan

Από την άλλη μεριά, το IDS θα πρέπει να μπορεί να εντοπίζει μια τέτοια επίθεση, ακόμα και αν δεν υπάρχουν έτοιμοι κανόνες, μπορεί να γίνει παραμετροποίηση. Στην περίπτωση αυτή το snort έχει έτοιμους κανόνες και μπορεί να εντοπίσει αυτή την επίθεση. Παρακάτω, φαίνεται το πώς εντόπισε επιτυχημένα το snort αυτή την επίθεση και κατέγραψε το γεγονός.



Εικόνα 7.2: Snort scan alert

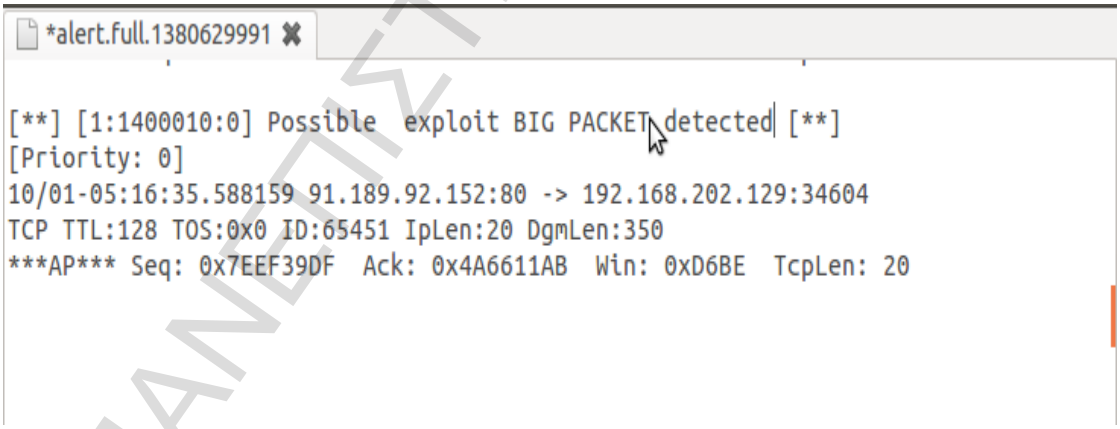
7.3 Εντοπισμός ασυνήθιστου μεγέθους πακέτων

Υπό κάποιες συνθήκες ένα πακέτο το οποίο υπερβαίνει ένα συγκεκριμένο μέγεθος μπορεί να θεωρηθεί κακόβουλο. Για παράδειγμα, ο επιτιθέμενος αφού γνωρίζει τι υπηρεσίες τρέχουν σε μια μηχανή και τι μέγεθος buffer χρησιμοποιεί, μπορεί να στείλει πακέτα μεγαλύτερα από αυτά που μπορεί να διαχειριστεί ο buffer και να προκαλέσει segmentation fault.

Με κατάλληλη παραμετροποίηση μπορεί να προστεθεί ένας κανόνας στο snort, που να ελέγχει τα πακέτα ως προς το μέγεθός τους και να δημιουργεί ειδοποιήσεις όταν χρειάζεται. Παραδειγματικά δημιουργήθηκε ο παρακάτω κανόνας που έχει ως στόχο να δημιουργεί ειδοποιήσεις εάν το μέγεθος του πακέτου είναι μεγαλύτερο από 1000 bytes:

Alert tcp any any → 192.168.202.129 any (dsize: >1000; msg: “Possible exploit BIG PACKET detected”; sid:1400010;)

Το snort εντοπίζει και καταγράφει πακέτα που ταιριάζουν στον παραπάνω κανόνα.

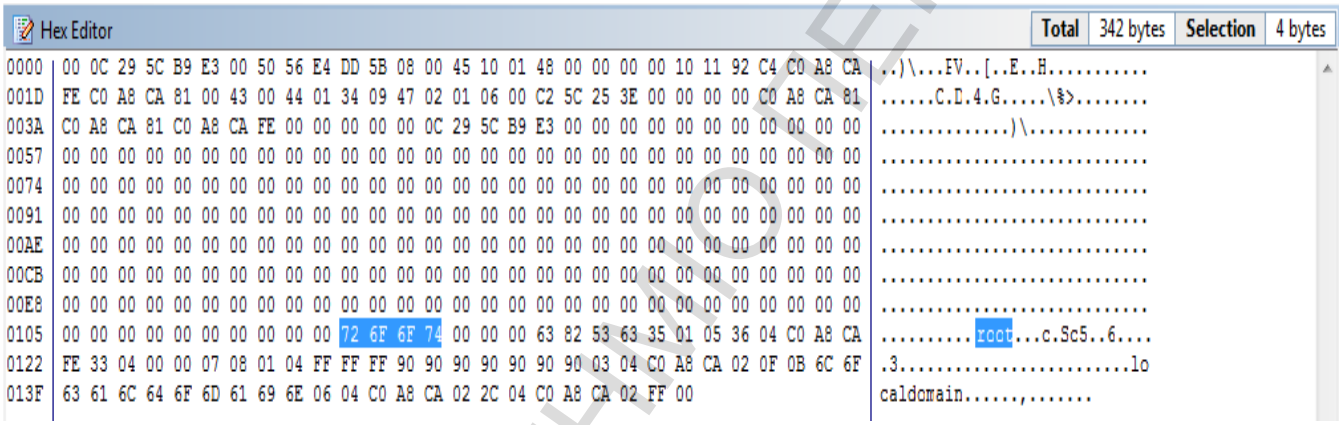


Εικόνα 7.3: Snort big packet alert

7.4 Εντοπισμός Περιεχομένου πακέτων

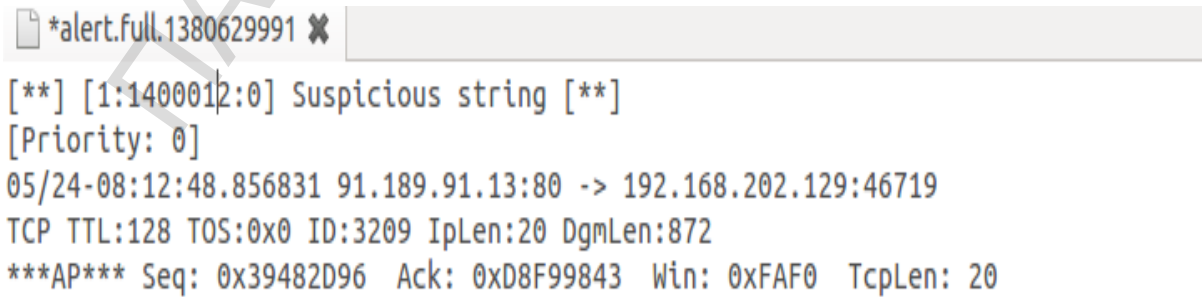
7.4.1 Εντολές

Ο επιτιθέμενος μπορεί να στείλει πακετα από μία εικονική μηχανή σε άλλη, τα όποια περιέχουν κακόβουλες εντολές. Για παράδειγμα στο παρακάτω πακέτο, που στέλνει η εικονική μηχανή από τη μεριά του επιτιθέμενου, φαίνεται η λέξη root, όπως λέγεται αλλιώς ο διαχειριστής σε συστήματα Linux. Μπορεί λοιπόν να προσπαθεί να αποκτήσει δικαιώματα σε μια εικονική μηχανή για τα οποία δεν έχει εξουσιοδότηση.



Εικόνα 7.4 : packet content root keyword

Με τη δημιουργία και χρήση κανόνων από πλευράς snort που στοχεύουν στον έλεγχο του περιεχομένου πακέτων με βάση λέξεις κλειδιά μπορεί να εντοπιστεί και να καταγραφεί μια τέτοια κακόβουλη συμπεριφορά όπως φαίνεται παρακάτω:



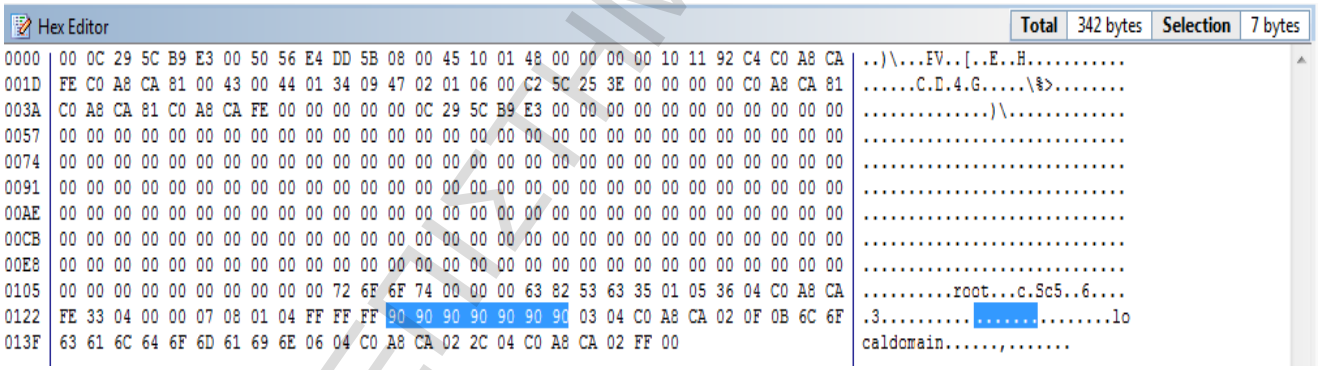
Εικόνα 7.5 : packet content keyword alert

Ο κανόνας που χρησιμοποίηθηκε φαίνεται παρακάτω:

Alert tcp any any → 192.168.202.129 any (msg: “Suspicious string”; content:”root”; sid:1400012;)

7.4.2 Υπογραφές

Ο επιτιθέμενος μπορεί να στείλει πακετα από μία εικονική μηχανή σε άλλη, τα όποια περιέχουν κακόβουλο κώδικα ή κακόβουλο λογισμικό. Για παράδειγμα στο παρακάτω πακέτο, που στέλνει η εικονική μηχανή από τη μεριά του επιτιθέμενου, φαίνεται πως στα bytes υπάρχουν επαναλαμβανόμενα “no operation bytes” (0x90) τα οποία χρησιμοποιούνται σε επίθεσεις με τεχνικές buffer overflow.



Εικόνα 7.6: packet content NOPS

Το snort μπορεί να παραμετροποιηθεί ώστε να εξετάζει τα bytes των πακέτων με κατάλληλους κανόνες. Για αυτήν την περίπτωση δημιουργήθηκε και χρησιμοποιήθηκε ο παρακάτω κανόνας:

Alert tcp any any → 192.168.202.129 any (msg: “Possible exploit NOP byte found”; content: ”|90|”; rawbytes; sid:1400001;)

Εφόσον το περιεχόμενο ταιριάζει με τον κανόνα, το snort δημιουργεί μια ειδοποίηση και την καταγράφει.

```
[**] [1:1400001:0] Possible  exploit NOP byte found   [**]
[Priority: 0]
06/03-08:31:48.785450 91.189.92.184:80 -> 192.168.202.129:57093
TCP TTL:128 TOS:0x0 ID:132 IpLen:20 DgmLen:1500
***A**** Seq: 0x6D2B071A  Ack: 0x16CA386  Win: 0xFAF0  TcpLen: 20
```

Εικόνα 7.7 : packet content raw bytes alert

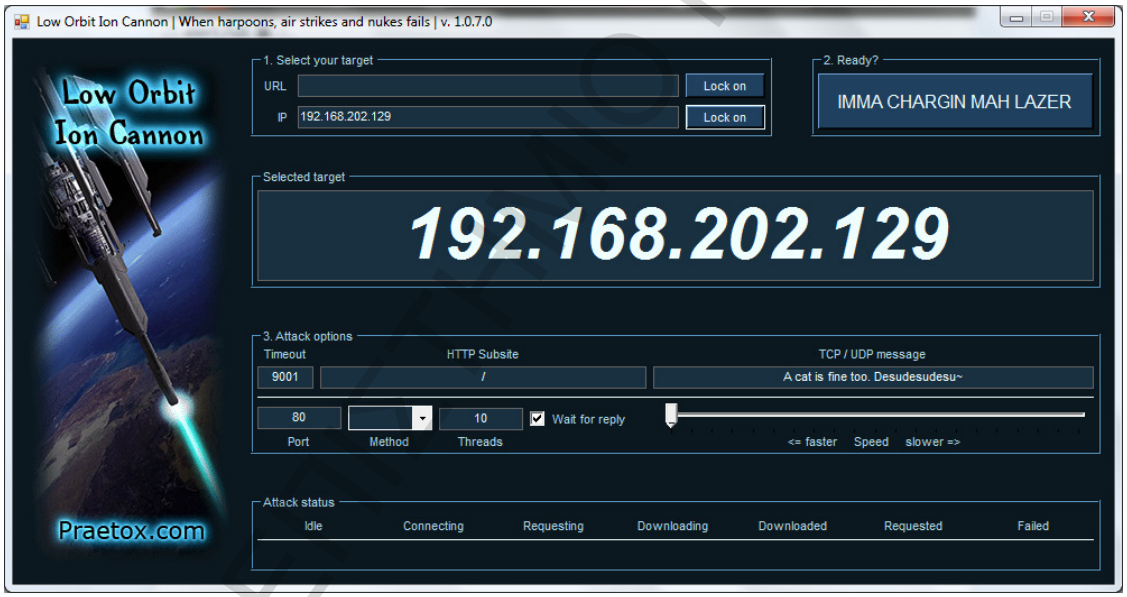
Η διαφορά με την προηγούμενη περίπτωση είναι ότι τώρα το snort εξετάζει τα bytes του πακέτου για υπογραφές. Με τον ίδιο τρόπο μπορεί να εντοπίσει και κακόβουλο λογισμικό.

7.5 Επιθέσεις άρνησης της υπηρεσίας (DOS) και άλλη ανεπιθύμητη εισερχόμενη κίνηση

7.5.1 DoS

Σε αυτή την περίπτωση ο επιτιθέμενος στέλνει στον στόχο υπερβολικά μεγάλο αριθμό από αιτήματα, τα οποία δεν είναι δυνατόν να διαχειριστεί και δημιουργείται “πλημμύρα” (flooding), με αποτέλεσμα ο νόμιμος χρήστης της εικονικής μηχανής να μην έχει πρόσβαση στην υπηρεσία.

Με τη χρήση του LOIC, το οποίο είναι εργαλείο προσομοίωσης DoS επιθέσεων, έγινε προσπάθεια DoS από τη μία εικονική μηχανή στην άλλη.



Εικόνα 7.8 : LOIC Interface

Στο snort μπορούν να προστεθούν κανόνες με τους οποίους ο διαχειριστής ειδοποιείται για τέτοιου τύπου επιθέσεις, όπως για παράδειγμα :

alert udp any any -> 192.168.202.129 any (threshold:type threshold, track by_src, count 100, seconds 5; sid:1234590; rev:1; msg:"SLR - LOIC DoS Tool(UDP Mode)";

Έτσι όταν μέσα σε ένα χρονικό πάραθυρο, ο αριθμός πακέτων από μία η

περισσότερες πηγές υπερβεί κάποιο όριο, το snort δημιουργεί και καταγράφει μια ειδοποίηση.

```
[**] [1:1234590:0] SLR - LOIC DoS Tool(UDP Mode) [**]
[Priority: 0]
10/01-05:16:42.935293 91.189.91.15:80 -> 192.168.202.129:56971
UDP TTL:128 TOS:0x0 ID:9205 IpLen:20 DgmLen:40
***A**** Seq: 0x32650E66   Win: 0x0  TcpLen: 20
```

Εικόνα 7.9 : DoS attack alert

7.5.2 Άλλη ανεπιθύμητη εισερχόμενη κίνηση

Υπάρχει περίπτωση να εντοπιστεί ανεπιθύμητη εισερχόμενη κίνηση από μία εικονική μηχάνη προς άλλη (π.χ worm self propagation). Μπορούμε να παραμετροποιήσουμε το snort ώστε να μας ειδοποιεί για τέτοιου είδους κίνηση. Παρακάτω βλέπουμε ένα από τα πολλά πακέτα που στέλνονται από μία ύποπτη εικονική μηχανή:

```
[**] [1:1400000:0] ciao [**]
[Priority: 0]
10/01-05:16:35.587052 91.189.91.14:80 -> 192.168.202.129:57700
TCP TTL:128 TOS:0x0 ID:65448 IpLen:20 DgmLen:40
***A**** Seq: 0x38D2177D  Ack: 0x21D6049D  Win: 0xCE3A  TcpLen: 20
```

Εικόνα 7.10: Suspicious traffic

7.5.3 Το snort ως IDPS

Παρακάτω θα δούμε πως το snort μπορεί να δράσει ως IDPS (Intrusion detection-prevention system) και να σταματήσει επιθέσεις σαν τις παραπάνω, αφού τις εντοπίσει, με συνδυασμό κανόνων. Με τον κανόνα που ακολουθεί δεν επιτρέπεται η επικοινωνία από την πηγή στον προορισμό:

alert udp any any -> 192.168.202.129 any (resp: icmp_port,icmp_host; msg: "Inbound connection blocked"; sid:1400014;)

Έτσι για παράδειγμα αν συνδυάσουμε αυτόν τον κανόνα με αυτόν του 7.5.1 το snort αφού εντοπίσει μια DoS επίθεση θα σταματήσει την σύνδεση μεταξύ της επιτιθέμενης εικονικής μηχανής και του στόχου, θα δημιουργήσει μια ειδοποίηση και θα καταγράψει το γεγονός.

```
[**] [1:1400014:0] Inbound connection blocked [**]
[Priority: 0]
12/04-06:08:07.352635 192.168.202.2:53 -> 192.168.202.129:2510
UDP TTL:128 TOS:0x0 ID:39311 IpLen:20 DgmLen:206
Len: 178

[**] [1:399:6] ICMP Destination Unreachable Host Unreachable [**]
[Classification: Misc activity] [Priority: 3]
12/04-06:08:07.372064 192.168.202.129 -> 192.168.202.2
ICMP TTL:64 TOS:0x0 ID:59947 IpLen:20 DgmLen:56
Type:3  Code:1  DESTINATION UNREACHABLE: HOST UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
192.168.202.2:53 -> 192.168.202.129:2510
UDP TTL:128 TOS:0x0 ID:39311 IpLen:20 DgmLen:206
Len: 178  Csum: 58990
** END OF DUMP
```

Εικόνα 7.11 : Inbound connection block alert

7.6 Επιθέσεις τύπου proxy

Ο επιτιθέμενος μπορεί να χρησιμοποιεί μια εικονική μηχανή η οποία δεν του ανήκει ως ενδιάμεση για να πραγματοποιήσει άλλες επιθέσεις, όπως πραγματοποιήθηκαν επιθέσεις DoS μέσα απο εικονικές μηχανές του Cloud της Amazon. Με τον παρακάτω κανόνα μπορούμε να απαγορεύσουμε κίνηση από μια εικονική μηχανή προς κάποιο προορισμό:

alert tcp any any <> 192.168.202.129 any (msg: "unauthorized outbound connection detected"; react: block; sid:1400013;)

Παρακάτω βλέπουμε τι καταγράφει το snort:

```
[**] [1:1400013:0] unauthorized outbound connection detected [**]
[Priority: 0]
10/01-05:16:35.587052 91.189.91.14:80 -> 192.168.202.129:57700
TCP TTL:128 TOS:0x0 ID:65448 IpLen:20 DgmLen:40
***A**** Seq: 0x38D2177D  Ack: 0x21D6049D  Win: 0xCE3A  TcpLen: 20
```

Εικόνα 7.12 : Outbound connection block alert

8. Επίλογος

Σ' αυτή την εργασία περιγράψαμε τα βασικά στοιχεία του cloud, καθώς και διάφορες απειλές που αντιμετωπίζει. Επίσης, αναφέραμε τις κατηγορίες των IDS, τα πλεονεκτήματα και τα μειονεκτήματά τους, όπως επίσης και διάφορα μοντέλα εφαρμογής τους σε περιβάλλον cloud.

Ειδικότερα, αναλύθηκε το εργαλείο snort, το οποίο χρησιμοποιήθηκε και στην εφαρμογή μας. Με βάση αυτό το εργαλείο μελετήσαμε πώς ένα δικτυακό IDS μπορεί να αναποκριθεί σε ανίχνευση επιθέσεων σε cloud περιβάλλοντα. Είδαμε ότι, τουλάχιστον, στις επιθέσεις στις οποίες προσομοιώθηκαν, από μία εικονική μηχανή προς άλλη, το snort έχοντας τους απαραίτητους παραμετροποιημένους κανόνες, κατάφερε να ανιχνεύσει αυτές τις επιθέσεις.

Μελλοντικά, ανοίγεται ο δρόμος ώστε να υπάρξει μια τάση παροχής του IDS ως υπηρεσία (IDSAAS) που θα δίνει τη δυνατότητα στους χρήστες του cloud να παραμετροποιούν ένα τέτοιο εργαλείο, είτε μόνοι τους είτε με τη συνεργασία των παρόχων, σύμφωνα με τις δικές τους ανάγκες.

Βιβλιογραφία

[1] Amazon Web Services, Amazon Elastic Compute Cloud, (Amazon EC2). http://aws.amazon.com/ec2/.

[2] IBM, IBM Smart Cloud. http://www.ibm.com/cloud-computing/us/en/index.html.

[3] C. Burns: Public cloud security remains MISSION IMPOSSIBLE, 2011

[4] NIST: http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

[5] Cloud Security Alliance, 2009 http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

[6] ISACA. (2011). *IT Control Objectives for Cloud Computing.* IL: ISACA.

[7] Cloud Security Alliance, 2010 http://www.cloudsecurityalliance.org/topthreats

[8] ENISA, 2009: Cloud Computing: Benefits, risks and recommendations for U: ENISA.information security.

[9] Tim Mather , Subra Kumaraswamy , Shahed Latif: Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice) .

[10] R. Srinivasa: Cloud computing: an overview, 2009

[11] C. Lo, C. Huang, and J. Ku: A cooperative intrusion detection system framework for cloud computing networks, 2010.

[12] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, Denial-of-service attack-detection techniques," IEEE Internet Computing, 2006.

[13] S. Roschke, F. Cheng, and C. Meinel, Intrusion detection in the cloud, 2009.

[14] F. Sibai and D. Menasce, Defeating the insider threat via autonomic network capabilities, 2011.

[15] M. N. Bennani and D. A. Menasce, Resource allocation for autonomic data centers using analytic performance models, June 2005.

[16] C. M. R. Bifulco and R. Canonic, Integrating a network ids into an open source cloud computing environment, 2010.

[17] Chirag Modi, Dhiren Patel, Hiren Patel, Bhavesh Borisaniya, Avi Patel, Muttukrishnan Rajarajan: A survey of intrusion detection techniques in Cloud, 2012

[18] P. Skrobanek : Intrusion detection systems, 2011

[19] Snort 2.1 Intrusion Detection, 2nd Edition (2004)