ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Πολυτεχνική Σχολή

Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων

Καρλόβασι, Σάμος

Διδακτορική Διατριβή

Ψηφιακή Εγκληματολογία Στο Υπολογιστικό Νέφος

Νικόλαος Μαραγγός

Ιούλιος 2023

Υπεύθυνη Δήλωση

Είμαι ο αποκλειστικός συγγραφέας της υποβληθείσας Διδακτορικής Διατριβής με τίτλο «Ψηφιακή Εγκληματολογία στο Υπολογιστικό Νέφος». Η συγκεκριμένη Διδακτορική Διατριβή είναι πρωτότυπη και εκπονήθηκε αποκλειστικά για την απόκτηση του Διδακτορικού διπλώματος του Τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων. Κάθε βοήθεια, την οποία είχα για την προετοιμασία της, αναγνωρίζεται πλήρως και αναφέρεται επακριβώς στην εργασία. Επίσης, επακριβώς αναφέρω στην εργασία τις πηγές, τις οποίες χρησιμοποίησα, και μνημονεύω επώνυμα τα δεδομένα ή τις ιδέες που αποτελούν προϊόν πνευματικής ιδιοκτησίας άλλων, ακόμη κι εάν η συμπερίληψή τους στην παρούσα εργασία υπήρξε έμμεση ή παραφρασμένη. Γενικότερα, βεβαιώνω ότι κατά την εκπόνηση της Διδακτορικής Διατριβής έχω τηρήσει απαρέγκλιτα όσα ο νόμος ορίζει περί διανοητικής ιδιοκτησίας και έχω συμμορφωθεί πλήρως με τα προβλεπόμενα στο νόμο περί προστασίας προσωπικών δεδομένων και τις αρχές Ακαδημαϊκής Δεοντολογίας.

Τριμελής Επιτροπή

Λίλιαν Μήτρου, Καθηγήτρια, Επιβλέπουσα
Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων
Πανεπιστήμιο Αιγαίου

Στέφανος Γκρίτζαλης, Καθηγητής, Μέλος
Τμήμα Ψηφιακών Συστημάτων
Πανεπιστήμιο Πειραιώς

Παναγιώτης Ριζομυλιώτης, Αναπληρωτής Καθηγητής, Μέλος
Τμήμα Πληροφορικής & Τηλεματικής
Χαροκόπειο Πανεπιστήμιο

Εξεταστική Επιτροπή

Λίλιαν Μήτρου, Καθηγήτρια, Επιβλέπουσα
Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων
Πανεπιστήμιο Αιγαίου

Στέφανος Γκρίτζαλης, Καθηγητής, Μέλος
Τμήμα Ψηφιακών Συστημάτων
Πανεπιστήμιο Πειραιώς

Παναγιώτης Ριζομυλιώτης, Αναπληρωτής Καθηγητής, Μέλος
Τμήμα Πληροφορικής & Τηλεματικής
Χαροκόπειο Πανεπιστήμιο

Κωνσταντίνος Λαμπρινουδάκης, Καθηγητής, Μέλος
Τμήμα Ψηφιακών Συστημάτων
Πανεπιστήμιο Πειραιά

Σπυρίδων Κοκολάκης, Καθηγητής, Μέλος
Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων
Πανεπιστήμιο Αιγαίου

Μαρία Καρύδα, Καθηγήτρια, Μέλος
Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων
Πανεπιστήμιο Αιγαίου

Γεώργιος Στεργιόπουλος, Επίκουρος Καθηγητής, Μέλος
Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων
Πανεπιστήμιο Αιγαίου

Ευχαριστίες

Έχοντας ολοκληρώσει την παρούσα διατριβή, αισθάνομαι την ανάγκη να ευχαριστήσω όλους όσους βοήθησαν στην πραγματοποίησή της. Αρχικά, είμαι ευγνώμων για τους καθηγητές της τριμελους επιτροπής, την κ. Λίλιαν Μήτρου, τον κ. Στέφανο Γκρίτζαλη και τον κ. Παναγιώτη Ριζομυλιώτη για τις εύστοχες υποδείξεις και για τον χρόνο που μου αφιέρωναν καθ' όλη την πορεία της μελέτης. Ειδικότερα, θα ήθελα να ευχαριστήσω την κ. Λίλιαν Μήτρου, επιβλέπουσα, για την εμπιστοσύνη που μου έδειξε, αναθέτοντάς μου την εκπόνηση της συγκεκριμένης διατριβής.

Επίσης, θα ήθελα να ευχαριστήσω το Ίδρυμα Κρατικών Υποτροφιών (Ι.Κ.Υ.) για την υποτροφία που μου χορήγησε με σκοπό την πραγματοποίηση της συγκεκριμένης διατριβής.

Αθήνα, Ιούλιος 2023

Νίκος Μαραγγός

Περιεχόμενα

Κεφάλαιο Δέκατο

Κ Ε Φ Α Λ Α Ι Ο Π Ρ Ω Τ Ο

Εισαγωγή

1.1. Εισαγωγή

Σε αυτό το κεφάλαιο περιγράφονται οι στόχοι της παρούσας έρευνας, διατυπώνονται και αναλύονται τα ερευνητικά ερωτήματα, τα οποία καλείται να απαντήσει η συγκεκριμένη διατριβή, και παρουσιάζεται ο τρόπος με τον οποίο δομήθηκε η διαδικασία της απάντησής τους. Τέλος, αναφέρεται περιληπτικά η δομή συγγραφής της διατριβής, η οποία διαρθρώνεται με τέτοιο τρόπο αποσκοπώντας στην

πλήρη κατανόηση τόσο των προβλημάτων που αναδεικνύει, όσο και των ενεργειών που πραγματοποιούνται για την επίλυσή τους.

1.2. Ερευνητικά ερωτήματα – στόχοι

Η συγκεκριμένη διατριβή στοχεύει να αναδείξει τα προβλήματα που προκύπτουν κατά την διάρκεια μας εγκληματολογικής έρευνας στο υπολογιστικό νέφος εφαρμόζοντας κλασικές μεθόδους ψηφιακών εγκληματολογικών ερευνών στο περιβάλλον του υπολογιστικού νέφους. Επισημαίνει πόσο σημαντικά είναι τα αρχεία καταγραφής συμβάντων για τη διεξαγωγή μιας έρευνας και διερευνά κατά πόσο τα υπάρχοντα περιβάλλοντα υπολογιστικού νέφους ελέγχουν τον συγχρονισμό του χρόνου των επιμέρους συστημάτων τους, από το οποίο προκύπτουν οι χρονοσφραγίδες στα αρχεία καταγραφής συμβάντων.

1.3. Συμβολή της διατριβής

Η έρευνα της συγκεκριμένης διατριβής ξεκίνησε μελετώντας εκτενώς τις ήδη υπάρχουσες μεθοδολογίες ψηφιακής εγκληματολογικής έρευνας σε ένα κλασικό περιβάλλον [01]. Ακολούθως, δημιουργήθηκε ένα γενικό πλαίσιο μεθοδολογίας μιας ψηφιακής εγκληματολογικής έρευνας, στο οποίο ενσωματώσαμε τα βασικά βήματα των επιμέρους μεθοδολογιών, εξετάσαμε κατά πόσο αυτό μπορεί να ανταπεξέλθει αποδοτικά σε μια έρευνα στο υπολογιστικό νέφος, τι είδους προβλήματα προκύπτουν και ποιες διαδικασίες πρέπει να τροποποιηθούν. Το γενικό πλαίσιο της μεθοδολογίας μας αποτελούνταν από τρεις βασικές φάσεις: τη φάση της προετοιμασίας, τη φάση της έρευνας και τη φάση της παρουσίασης.

Η φάση της προετοιμασίας έχει τρία διακριτά βήματα. Το πρώτο βήμα είναι η αναγνώριση, μέσω της οποίας ο ερευνητής αναγνωρίζει από επιμέρους ενδείξεις το περιστατικό ασφάλειας και καθορίζει τον τύπο του. Ένα περιστατικό ασφάλειας μπορεί να γίνει αντιληπτό από μια ειδοποίηση από το τείχος ασφαλείας του οργανισμού (firewall - IDS) ή

από την ασυνήθιστη συμπεριφορά μιας εφαρμογής ή ενός διακομιστή. Το επόμενο βήμα είναι η προετοιμασία, κατά την οποία ο ερευνητής προετοιμάζει τα εργαλεία και καταστρώνει ένα σχέδιο για τις τεχνικές που θα χρησιμοποιήσει. Τα εργαλεία που θα χρησιμοποιήσει εξαρτώνται σε μεγάλο βαθμό από το είδος του λειτουργικού συστήματος του υπόπτου. Κατόπιν, αιτείται από τον αρμόδιο εισαγγελέα ένταλμα για έρευνα. Χωρίς κατάλληλο ένταλμα έρευνας, όλα τα στοιχεία που έχουν συλλεχθεί είναι στην πραγματικότητα ανώφελα, καθώς η συλλογή και οιαδήποτε αποτελεσματική χρήση τους προϋποθέτει απόλυτη νομιμότητα, και επιπλέον ελλοχεύει ο κίνδυνος και ίδιος ο ερευνητής να κατηγορηθεί για παράνομη απόκτηση δεδομένων ή παράνομη πρόσβαση σε δεδομένα. Το τελευταίο βήμα της φάσης της προετοιμασίας είναι η στρατηγική προσέγγισης της έρευνας. Σε αυτό το βήμα ο ερευνητής πρέπει να προσδιορίσει μια προσέγγιση με βάση τις πιθανές επιπτώσεις στο θύμα. Στόχος του συγκεκριμένου βήματος είναι να μεγιστοποιηθεί η δυνατότητα συλλογής ψηφιακών αποδεικτικών στοιχείων, και παράλληλα να ελαχιστοποιηθούν οι επιπτώσεις της ψυφιακής εγκληματολογικής έρευνας για το θύμα.

Η φάση της έρευνας αποτελείται από πέντε βασικά βήματα. Αρχικά έχουμε το βήμα της διατήρησης των ψηφιακών αποδεικτικών στοιχείων. Σε αυτό το βήμα ο ερευνητής θα πρέπει να απομονώσει, να ασφαλίσει και να διατηρήσει σε ακέραιη κατάσταση τα ψηφιακά αποδεικτικά στοιχεία. Αυτό επιτυγχάνεται αρχικά με το να μην έχουν πρόσβαση άλλα άτομα στις συσκευές που έχουν τα ψηφιακά αποδεικτικά στοιχεία και σε δεύτερο επίπεδο με τη χρήση συναρτήσεων κατακερματισμού (hash functions), μέσω των οποίων ο ερευνητής μπορεί να τεκμηριώσει την ακρίβεια και τη μη τροποποίηση των στοιχείων. Το επόμενο βήμα είναι το βήμα της συλλογής. Ο ερευνητής αντιγράφει όλα τα ψηφιακά αποδεικτικά στοιχεία που έχει στη διάθεσή του. Από αυτό το σημείο και έπειτα τα αρχικά ψηφιακά στοιχεία παραμένουν άθικτα και ο ερευνητής δουλεύει με το αντίγραφο. Η συλλογή των ψηφιακών αποδεικτικών στοιχείων ακολουθεί μια αυστηρά προδιαγεγραμμένη σειρά συλλογής, η οποία ονομάζεται σειρά μεταβλητότητας. Το βήμα της τεκμηρίωσης είναι καθοριστικό για την επιτυχία μιας εγκληματολογικής έρευνας, καθώς διασφαλίζει ότι οι

αποδείξεις που συγκεντρώνονται είναι νόμιμες, ολοκληρωμένες και αξιόπιστες, επιτρέποντας έτσι τη διεξαγωγή δίκαιης και αξιόπιστης δικαστικής διαδικασίας. Ακολουθεί το βήμα της εξέτασης, κατά το οποίο ο ερευνητής εξετάζει όλα τα ψηφιακά μέσα για ψηφιακά αποδεικτικά στοιχεία που σχετίζονται με το έγκλημα, για το οποίο κατηγορείται ο ύποπτος. Θα πρέπει να τονιστεί ότι ο ερευνητής αναζητά ψηφιακά αποδεικτικά στοιχεία και σε περιοχές όπου υπό κανονικές συνθήκες δεν υπάρχουν δεδομένα, όπως για παράδειγμα σε κατεστραμμένους τομείς ενός δίσκου. Στο βήμα της ανάλυσης ο ερευνητής αναλύει τα δεδομένα που προέκυψαν από την έρευνα και αναδημιουργεί το συμβάν βασισμένος στα στοιχεία που ανακάλυψε. Τις περισσότερες φορές αυτό το βήμα αποτελείται από πολλούς βρόχους, προκειμένου να επιτευχθεί η συλλογή όλων των αποδεικτικών στοιχείων, ώστε να υποστηρίζεται πλήρως η θεωρία του ερευνητή για το συμβάν.

Τέλος, έχουμε την φάση της παρουσίασης. Στο πρώτο βήμα αυτής της φάσης είναι η παρουσίαση των αποτελεσμάτων στο δικαστήριο. Τα αποτελέσματα πρέπει να εμφανίζονται ολοκληρωμένα, αλλά χωρίς πολλές τεχνικές λεπτομέρειες. Ακολουθεί το βήμα της αναφοράς, το οποίο επιτελείται σε όλα τα επιμέρους βήματα όλων των φάσεων, αλλά σε αυτό το σημείο θα πρέπει να προσκομιστεί στην δικαστική αίθουσα. Ο ερευνητής θα πρέπει να τηρεί λεπτομερές αρχείο των πράξεών του επί των αποδεικτικών στοιχείων και θα πρέπει να είναι σε θέση να αποδείξει στο δικαστήριο με ποιους τρόπους έκανε την συλλογή των ψηφιακών αποδεικτικών στοιχείων, καθώς και με ποιους τρόπους τα χειρίστηκε αναφορικά με την αυθεντικότητα και την ακεραιότητά τους κατά τη διαδικασία της έρευνας. Το τελευταίο βήμα αυτής της φάσης είναι η επιστροφή των αποδεικτικών στοιχείων στον νόμιμο ιδιοκτήτη τους και η καταστροφή όλων των δεδομένων που είχαν δημιουργηθεί κατά τις προηγούμενες φάσεις.

Στη συνέχεια αναλύσαμε για κάθε επιμέρους βήμα της προηγούμενης μεθοδολογίας κατά πόσο αυτό είναι εφικτό να εφαρμοστεί ή όχι σε καθένα από τα τρία βασικά μοντέλα υπηρεσιών του υπολογιστικού νέφους. Δυστυχώς, το καθένα από τα τρία βασικά μοντέλα υπηρεσιών του υπολογιστικού νέφους προσφέρει εντελώς

διαφορετική ποσότητα ψηφιακών αποδεικτικών στοιχείων. Επίσης, ανάλογα με το μοντέλο, ο χρήστης έχει εντελώς διαφορετικά δικαιώματα και ελέγχους πρόσβασης στην υποκείμενη υποδομή, με λιγότερα στο SaaS, μετά στο PaaS και τέλος στο IaaS, όπου ο χρήστης έχει τα περισσότερα δικαιώματα. Αυτό με την σειρά του έχει αντίκτυπο στην συλλογή ψηφιακών αποδεικτικών στοιχείων. Από την έρευνά μας προέκυψε ότι αρκετά από τα προηγούμενα βήματα μιας ψηφιακής εγκληματολογικής έρευνας, μπορούν να εφαρμοστούν απευθείας σε περιβάλλοντα υπολογιστικού νέφους. Ωστόσο, υπάρχουν αρκετά και κρίσιμα βήματα που θα πρέπει να επαναπροσαρμοστούν λόγω των ιδιαίτερων χαρακτηριστικών του υπολογιστικού νέφους.

Πιο συγκεκριμένα, εκτός από τη φάση της παρουσίασης των αποτελεσμάτων της ψηφιακής εγκληματολογικής έρευνας, η οποία μπορεί να ανταπεξέλθει πλήρως και σε περιβάλλοντα υπολογιστικού νέφους, τα περισσότερα από τα βήματα των φάσεων της προετοιμασίας και της έρευνας δεν μπορούν να υλοποιηθούν αυτούσια σε περιβάλλοντα υπολογιστικού νέφους. Η φάση της προετοιμασίας, εάν εξαιρεθεί το μοντέλο IaaS, εξαρτάται αποκλειστικά από την διαθεσιμότητα του παρόχου να προσκομίσει τα αντίστοιχα δεδομένα των βημάτων.

Η φάση της έρευνας είναι η φάση στην οποία αναδεικνύονται εμφανώς οι ελλείψεις των κλασικών ψηφιακών ερευνών σε περιβάλλοντα υπολογιστικού νέφους. Στο βήμα της διατήρησης ο ερευνητής πρέπει να ασφαλίσει και να διατηρήσει αναλλοίωτη την σκηνή του εγκλήματος. Σε μια τυπική ψηφιακή εγκληματολογική έρευνα αυτό επιτελείται μεταφέροντας τις ψηφιακές συσκευές στο εργαστήριό του. Σε περιβάλλοντα υπολογιστικού νέφους ο ερευνητής μπορεί να μην γνωρίζει καν που βρίσκονται αποθηκευμένα τα δεδομένα. Επιπλέον, ακόμη και αν καταφέρει με κάποιον τρόπο να βρει τον φυσικό σκληρό δίσκο των δεδομένων, θεωρείται απίθανο ο δίσκος αυτός να μην έχει δεδομένα και άλλων χρηστών, μη σχετιζόμενων με την έρευνα. Αντίστοιχα, στο βήμα της εξέτασης οι ήδη υπάρχουσες τεχνικές δεν μπορούν να λειτουργήσουν σε περιβάλλοντα πολλαπλών χρηστών. Αυτό έχει ως συνέπεια ο ερευνητής να εξαρτάται πλήρως από τον εκάστοτε

πάροχο, προκειμένου εκείνος να του παράσχει τυχόν αποδεικτικά στοιχεία για τον ύποπτο.

Τέλος, αναδείξαμε τα προβλήματα που προκύπτουν σε νομικό επίπεδο. Είναι γεγονός ότι ένας ερευνητής έρχεται αντιμέτωπος με νομικές προκλήσεις κατά τον εντοπισμό, την επισήμανση, την καταγραφή και την απόκτηση των ψηφιακών αποδεικτικών στοιχείων στο υπολογιστικό νέφος. Ο ερευνητής θα πρέπει πρωτίστως, ανάλογα με το μοντέλο του υπολογιστικού νέφους, να τροποποιήσει κατάλληλα τα εργαλεία και τις διαδικασίες που ακολουθεί. Η ταυτοποίηση των ψηφιακών αποδεικτικών στοιχείων είναι προφανώς πολύ πιο δύσκολη σε ένα δημόσιο υπολογιστικό νέφος σε σχέση με ένα ιδιωτικό. Επίσης, σοβαρό πρόβλημα αποτελεί η ταυτοποίηση του υπόπτου και ο διαχωρισμός των αποδεικτικών στοιχείων σε σχέση με τους άλλους χρήστες του νέφους, ώστε να μην παραβιάζεται η ιδιωτικότητα των υπόλοιπων χρηστών. Ένα άλλο σοβαρό πρόβλημα που αναδείχτηκε στο υπολογιστικό νέφος είναι το ζήτημα της πολυνομοθεσίας. Ενώ το υπολογιστικό νέφος δεν έχει σύνορα, η έρευνα και η δίωξη ενός εγκλήματος λαμβάνουν χώρα αυστηρά εντός των ορίων ενός κράτους ή μιας ομάδας κρατών. Για παράδειγμα, ο ύποπτος μπορεί να διαμένει στην Ελλάδα, τα δεδομένα του να είναι αποθηκευμένα σε ένα δημόσιο υπολογιστικό νέφος στις ΗΠΑ και η επεξεργασία αυτών να γίνεται σε διακομιστές που εδρεύουν στην Κίνα. Συνεπώς, ένταλμα έρευνας μόνο στην Ελλάδα δεν θα αποφέρει κάποιο αποτέλεσμα. Επιπροσθέτως θα πρέπει να συνυπολογιστεί ότι υπάρχει περίπτωση μια πράξη που θεωρείται εγκληματική στη χώρα που κατοικεί ο ύποπτος, να μην είναι εγκληματική στη χώρα που τη διέπραξε ο ύποπτος. Αξίζει να σημειωθεί ότι οργανισμοί όπως ο ENISA αναφέρουν ρητά ότι για την αποδοτικότητα μιας έρευνας σε περιβάλλοντα υπολογιστικού νέφους θα πρέπει να υπάρχει συνεργασία των χωρών τόσο σε τεχνικό όσο και σε νομικό επίπεδο.

Στο δεύτερο σκέλος της διατριβής, αρχικά αναδείξαμε την σημαντικότητα των αρχείων καταγραφής συμβάντων για την αποδοτική διεξαγωγή μιας ψηφιακής εγκληματολογικής έρευνας [02]. Πιο συγκεκριμένα, σε περιβάλλοντα υπολογιστικού νέφους προκύπτουν

κάποιες προκλήσεις αναφορικά με τα αρχεία καταγραφής συμβάντων. Στην αρχή ερευνήσαμε τι είδους περιεχόμενα θα πρέπει να έχει ένα αρχείο καταγραφής συμβάντων, ώστε να αποφέρει τα μέγιστα σε μια ψηφιακή εγκληματολογική έρευνα. Δεύτερο στάδιο της έρευνάς μας ήταν ο τρόπος του προσδιορισμού της πηγής των δεδομένων ενός αρχείου καταγραφής συμβάντων και κατά πόσο αυτή είναι αξιόπιστη. Ακολούθως μελετήθηκε η περίοδος διατήρησης των αρχείων καταγραφής συμβάντων και το εάν η αποθήκευσή τους είναι αποδοτικότερο να γίνεται σε ένα κεντροποιημένο σύστημα ή σε ένα κατανεμημένο σύστημα αποθήκευσης αρχείων καταγραφής συμβάντων. Επίσης, εξετάστηκε λεπτομερώς η πολιτική πρόσβασης στα αρχεία καταγραφής συμβάντων. Τέλος, εξετάσαμε τον χρόνο στον οποίο καταγράφονται τα συμβάντα.

Πέραν των υπόλοιπων δεδομένων που μπορεί να περιλαμβάνει ένα αρχείο καταγραφής συμβάντων, καθώς και τους τρόπους με τους οποίους διαφυλάσσεται η ακεραιότητά του, ασχοληθήκαμε εκτενώς με τον χρόνο κατά τον οποίο καταγράφονται τα συμβάντα. Έγινε μελέτη της τρέχουσας κατάστασης αναφορικά με τους τρόπους διασφάλισης της ακεραιότητας του χρόνου. Σε περιβάλλοντα υπολογιστικού νέφους έχουμε δύο διακριτές περιπτώσεις: στην πρώτη περίπτωση, ο πάροχος υπηρεσιών υπολογιστικού νέφους είναι υπεύθυνος για τον συγχρονισμό του ρολογιού των διακομιστών του, ενώ στη δεύτερη το ίδιο το εικονικό μηχάνημα είναι υπεύθυνο για τον συγχρονισμό. Στη συνέχεια ερευνήσαμε εκτενώς τις ήδη υπάρχουσες τεχνικές για τη διατήρηση της ακεραιότητας του χρόνου και προσδιορίστηκαν τα θετικά και τα αρνητικά σημεία της κάθε μίας από αυτές.

Ως αποτέλεσμα της έρευνας, προτάθηκαν λύσεις για τον επιτυχή συγχρονισμό του χρόνου στα υποσυστήματα του υπολογιστικού νέφους και καταλήξαμε στην εισαγωγή της έννοιας της ορθότητας του χρόνου μέσω της καταγραφής όλων των συμβάντων συγχρονισμού του ρολογιού. Αναφορικά με τον επιτυχή συγχρονισμό του χρόνου, ερευνήθηκαν όλα τα πρωτόκολλα συγχρονισμού του χρόνου σε περιβάλλον υπολογιστικού νέφους και αναδείξαμε τα πλεονεκτήματα και τα μειονεκτήματά τους. Μέσω της έρευνας εισάγαμε την έννοια της

καταγραφής σε αρχεία καταγραφής συμβάντων όλων των επιμέρους βημάτων του συγχρονισμού του χρόνου σε περιβάλλοντα υπολογιστικού νέφους, ώστε ο ερευνητής να είναι σε θέση να αναπαράξει, εάν χρειαστεί, τα προβλήματα που υπήρχαν αναφορικά με τον χρόνο στη σκηνή του εγκλήματος.

1.4. Δομή της διατριβής

Η διατριβή είναι δομημένη ως εξής: Αρχικά, παρουσιάζεται και εξηγείται η έννοια του υπολογιστικού νέφους, αναφέρεται ο τρόπος δημιουργίας του και εν συνεχεία καταγράφεται η εξέλιξή του μέχρι τη σημερινή του μορφή. Στο τρίτο κεφάλαιο αναλύεται η υφιστάμενη τεχνολογία του υπολογιστικού νέφους. Στη συνέχεια, περιγράφονται τα βασικά μοντέλα του υπολογιστικού νέφους. Το πέμπτο κεφάλαιο αναφέρεται στις τεχνολογίες ασφάλειας που παρέχονται στο υπολογιστικό νέφος από κακόβουλους χρήστες, τόσο σε επίπεδο παρόχου/υπηρεσιών, όσο και σε επίπεδο πελάτη/χρήστη. Στο επόμενο κεφάλαιο γίνεται εκτενής αναφορά στα νομικά ζητήματα που καλείται να αντιμετωπίσει ένας ερευνητής στο περιβάλλον του υπολογιστικού νέφους. Το έβδομο κεφάλαιο αναδεικνύει τα προβλήματα και τις ελλείψεις που προκύπτουν σε κάθε ένα από τα τρία βασικά μοντέλα του υπολογιστικού νέφους, σε κάθε διακριτό βήμα μιας ψηφιακής εγκληματολογικής έρευνας. Στο όγδοο κεφάλαιο περιγράφονται και αναλύονται τα δομικά στοιχεία μιας ψηφιακής εγκληματολογικής έρευνας. Αναλύεται ο τρόπος αποθήκευσης των αρχείων καταγραφής συμβάντων, καθώς και τα σοβαρά προβλήματα που προκύπτουν από τον μη συγχρονισμό του ρολογιού στα συστήματα. Αναφέρονται, συγκρίνονται και αξιολογούνται τα πρωτόκολλα συγχρονισμού του ρολογιού. Τέλος, εισάγεται η έννοια της ορθότητας του χρόνου σε ένα σύστημα μέσω καταγραφής όλων των συμβάντων συγχρονισμού του ρολογιού. Το επόμενο κεφάλαιο είναι ο επίλογος της διατριβής και στο τελευταίο κεφάλαιο αναφέρονται οι πηγές οι οποίες χρησιμοποιήθηκαν για την εκπόνησή της.

Κ Ε Φ Α Λ Α Ι Ο Δ Ε Υ Τ Ε Ρ Ο

Υπολογιστικό νέφος

2.1. Εισαγωγή

Στα επόμενα κεφάλαια της συγκεκριμένης ενότητας θα αναφερθούμε λεπτομερώς σε μερικά από τα πιο βασικά επιμέρους στοιχεία του υπολογιστικού νέφους, τα οποία είναι απαραίτητα ώστε αυτό να είναι υλοποιήσιμο. Κρίσιμος παράγοντας για την ευρεία υιοθέτηση του μοντέλου υπολογιστικού νέφους θεωρείται η τυποποίηση, και υπάρχουν πολλά διαφορετικά πρότυπα τα οποία πρέπει

να ολοκληρωθούν πριν το υπολογιστικό νέφος γίνει αναπόσπαστο κομμάτι της δραστηριότητας των χρηστών. Τα πρότυπα αυτά έχουν να κάνουν με την υλοποίηση και την χρήση του υπολογιστικού νέφους, τη διαχείριση της υποδομής τους, καθώς και τις νομικές διαστάσεις που προκύπτουν από αυτή τη νέα διάσταση στο χώρο της πληροφορικής.

2.2. Το υπολογιστικό νέφος

Ιστορικά, ο όρος υπολογιστικό νέφος (Cloud Computing) χρησιμοποιήθηκε ως συνώνυμο του διαδικτύου (Internet). Αυτό οφείλεται στο ότι στα διαγράμματα δικτύων το διαδίκτυο απεικονιζόταν ως το περίγραμμα ενός σύννεφου, το οποίο αναπαριστούσε τη μεταφορά των δεδομένων μεταξύ παρόχων μεταφοράς δεδομένων, οι οποίοι είχαν στην κατοχή τους το υπολογιστικό νέφος, σε μια τελική τοποθεσία στην άλλη μεριά του νέφους. Η συγκεκριμένη έννοια χρονολογείται από το 1961, όταν ο καθηγητής J. McCarthy σκέφτηκε και πρότεινε ότι η τεχνολογία διαμοιρασμού χρόνου και των πόρων των υπολογιστών θα μπορούσε να οδηγήσει μελλοντικά σε υπολογιστικά μοντέλα και εφαρμογές που θα πωλούνται μέσω ενός εταιρικού δικτύου. Η συγκεκριμένη ιδέα αν και έγινε ιδιαίτερα δημοφιλής στα τέλη του 1960, περιθωριοποιήθηκε στα μέσα της δεκαετίας 1970, όταν έγινε σαφές ότι οι τότε υπάρχουσες τεχνολογίες υπολογιστών δεν θα μπορούσαν να υποστηρίξουν ένα τόσο φουτουριστικό μοντέλο υπολογιστών. Ωστόσο, με την αρχή της νέας χιλιετίας, ο συγκεκριμένος όρος άρχισε να επαναχρησιμοποιείται. Αυτήν τη χρονική εποχή άρχισε να εμφανίζεται και ο όρος υπολογιστικό νέφος σε όσους δραστηριοποιούνταν στον χώρο της τεχνολογίας.

Η παροχή υπολογιστικής ισχύος (Utility Computing - UC) μπορεί να οριστεί ως η παροχή υπολογιστικών και αποθηκευτικών πόρων σε μια μετρήσιμη υπηρεσία, παρόμοια με τις υπηρεσίες κοινής ωφέλειας, οι οποίες παρέχουν κάποιο αγαθό σε ένα μετρήσιμο μέγεθος [03]. Αυτού του είδους η παροχή υπολογιστικής ισχύος αυξάνεται σε δημοτικότητα προσφέροντας σε εταιρείες την δυνατότητα να παρέχουν υπολογιστική ισχύ επί πληρωμή σε άλλες εταιρείες ή απλούς χρήστες, οι οποίοι με τη

σειρά τους κάνουν χρήση ακριβώς όσων υπολογιστικών πόρων χρειάζονται ανά πάσα στιγμή. Σε πρώιμο στάδιο, διάφορες εταιρείες έκαναν χρήση αυτής της παροχής υπολογιστικής ισχύος για μη βασικές λειτουργίες της εταιρείας τους, αλλά αυτό σταδιακά άλλαξε από την στιγμή που επιλύθηκαν θέματα αξιοπιστίας και εμπιστευτικότητας.

Αρκετοί από τους επιστήμονες είχαν την πεποίθηση ότι το υπολογιστικό νέφος θα είναι το επόμενο μεγάλο ορόσημο στο κόσμο της πληροφορικής. Άλλοι πίστευαν ότι είναι απλώς μια παραλλαγή του UC, η οποία επαναεμφανίστηκε ως κάτι νέο και ενδιαφέρον. Ωστόσο, δεν είναι μόνο ο όρος υπολογιστικό νέφος ο οποίος προκαλεί σύγχυση στο ευρύ κοινό. Το γεγονός ότι από την μια μεριά οι πάροχοι υπολογιστικού νέφους (Cloud Service Provider - CSP) στην ουσία εξασκούνται πάνω σε αυτού του είδους την τεχνολογία και από την άλλη κάθε αναλυτής και ερευνητής ορίζει διαφορετικά το τι είναι υπολογιστικό νέφος, είχε επιφέρει μια σύγχυση για το τι πραγματικά σημαίνει ο όρος υπολογιστικό νέφος. Ακόμα και σε αυτούς που πίστευαν ότι έχουν κατανοήσει πλήρως την έννοια του υπολογιστικού νέφους, η απόδοση ενός ορισμού διαφέρει και οι περισσότεροι από αυτούς τους ορισμούς είναι ασαφείς. Από τη στιγμή που η παρούσα διατριβή ασχολείται ενδελεχώς με το υπολογιστικό νέφος θεωρείται πρωτίστης σημασίας το ξεκαθάρισμα των ασαφειών και η όσο το δυνατόν αποσαφήνιση της έννοιας. Οπότε, στις επόμενες παραγράφους θα προσπαθήσουμε να βοηθήσουμε τον αναγνώστη να κατανοήσει σε γενικές γραμμές τι σημαίνει το υπολογιστικό νέφος, πόσο ευεργετικό η προβληματικό είναι για μια επιχείρηση και τέλος ποια είναι τα πλεονεκτήματα και μειονεκτήματα που έχει.

Όπως προαναφέρθηκε, ο όρος υπολογιστικό νέφος χρησιμοποιήθηκε στο παρελθόν ως συνώνυμο του διαδικτύου και ενδεχομένως έγινε πρότυπο. Ωστόσο, όταν ο όρος συνδυάζεται με το Computing, προκαλεί σύγχυση. Αναλυτές της αγοράς και ερευνητές τείνουν να ορίσουν το νέφος αρκετά περιορισμένα και γενικά, ως ένα νέο τύπο UC ο οποίος χρησιμοποιεί εικονικούς διακομιστές (Virtual Servers), οι οποίοι είναι διαθέσιμοι σε πελάτες μέσω του διαδικτύου. Άλλοι ορίζουν τον όρο κάνοντας χρήση μιας αρκετά ευρείας και

ολοκληρωμένης εικονικής εφαρμογής [04, 05]. Υποστηρίζουν ότι οτιδήποτε εκτός της περιμέτρου του τείχους προστασίας (firewall) της εταιρείας ανήκει στο Cloud. Τέλος, ένας πιο αόριστος ορισμός θεωρεί ότι υπολογιστικό νέφος είναι ο διαμοιρασμός υπολογιστικών πόρων από μία τοποθεσία διαφορετική από αυτήν που εμφανίζεται το αποτέλεσμα της επεξεργασίας [05].

Για την παρούσα διατριβή κρίνεται σκόπιμο ως ορισμός για το υπολογιστικό νέφος να δοθεί ο ορισμός που του έχει αποδοθεί από NIST [06]. Πιο συγκεκριμένα υπολογιστικό νέφος είναι ένα μοντέλο το οποίο παρέχει συνεχώς και μέσω ζήτησης, πρόσβαση σε μια διαμοιραζόμενη δεξαμενή από ρυθμιζόμενους υπολογιστικούς πόρους, για παράδειγμα δίκτυα, διακομιστές, αποθηκευτικό χώρο, εφαρμογές και υπηρεσίες, το οποίο μπορεί να κατοχυρωθεί και να απελευθερωθεί από τον χρήστη με ελάχιστη διαχειριστική προσπάθεια ή συμβολή του παρόχου. Το υπολογιστικό νέφος απαρτίζεται από πέντε χαρακτηριστικά, τρία, βασικά, μοντέλα υπηρεσιών και τέσσερα μοντέλα ανάπτυξης.

Το υπολογιστικό νέφος δεν έχει σύνορα και ως εκ τούτου μετέτρεψε τον κόσμο σε μια «ψηφιακή γειτονιά». Το διαδίκτυο είναι μεν παγκόσμιας εμβέλειας αλλά λειτουργεί μόνο με εδραιωμένα και στατικά μονοπάτια επικοινωνίας και μέσω αυτού άνθρωποι από οπουδήποτε μπορούν να έχουν επικοινωνία με άτομα από οπουδήποτε αλλού. Από την άλλη μεριά, η παγκοσμιοποίηση των υπολογιστικών πόρων θεωρείται πως είναι η μεγαλύτερη συνεισφορά του υπολογιστικού νέφους. Για αυτόν τον λόγο το υπολογιστικό νέφος είναι αντικείμενο πολλών και περίπλοκων γεωπολιτικών ζητημάτων. Οι πάροχοι υπηρεσιών υπολογιστικού νέφους - Cloud Service Providers (CSPs) θα πρέπει να επιλύουν εκατοντάδες ρυθμιστικά προβλήματα ούτως ώστε να μπορούν να παρέχουν τις υπηρεσίες τους σε μια παγκόσμια αγορά. Όταν το διαδίκτυο ήταν σε πρώιμο στάδιο, πολλοί πίστευαν ότι ο κυβερνοχώρος ήταν ένα ξεχωριστό περιβάλλον το οποίο χρειάζονταν νομοθεσία ειδικά φτιαγμένη για αυτό. Οι υπολογιστές των πανεπιστημιακών μονάδων καθώς και το ARPANET [07] ήταν τα μόνα περιβάλλοντα στα οποία υπήρχε το διαδίκτυο, ενώ χρειάστηκε αρκετός

χρόνος για να διαδοθεί η ιδέα του διαδικτύου στον ευρύτερο χώρο και ειδικά στον επιχειρησιακό.

Το υπολογιστικό νέφος είναι πλέον καθημερινό γεγονός στη ζωή μας, όπως ήταν πριν μερικά χρόνια το internet. Υπάρχει ένα συνονθύλευμα από παρόχους υπολογιστικού νέφους, μικρούς και μεγάλους, οι οποίοι παρέχουν υπηρεσίες ευρείας κλίμακας. Για παράδειγμα, υπάρχει πληθώρα εφαρμογών όπως υπηρεσίες υποστηρικτικές, ηλεκτρονικού ταχυδρομείου, αποθηκευτικές και πολλές άλλες. Οι τεχνικοί της πληροφορικής έμαθαν να υποστηρίζουν μερικές από τις υπηρεσίες που παρέχει το υπολογιστικό νέφος ως αποτέλεσμα της ανάγκης για βελτιώσεις στις επιχειρήσεις που εργάζονται. Ωστόσο, συνεχίζουν και πληθαίνουν οι πάροχοι, οι οποίοι παρέχουν πακέτα προϊόντων και υπηρεσιών με μόνο μια απλή είσοδο στο υπολογιστικό νέφος τους.

Η ιδέα του υπολογιστικού νέφους γίνεται πολύ πιο κατανοητή όταν κάποιος αρχίζει να σκέφτεται τι χρειάζεται ένα μοντέρνο πληροφοριακό σύστημα. Τους τρόπους, δηλαδή, για να αυξήσει τη χωρητικότητά του ή να προσθέτει δυνατότητες στην υπάρχουσα υποδομή με δυναμικό τρόπο, χωρίς να χρειάζεται να επενδύσει χρήματα για την αγορά νέας υποδομής και χωρίς να απαιτείται η κατάρτιση του προσωπικού και η αγορά άδειας για κάθε νέο λογισμικό. Μια ήδη υπάρχουσα λύση για τις προαναφερθείσες ανάγκες είναι το υπολογιστικό νέφος και τα μοντέλα που παρέχει μέσω σταθερής συνδρομής ή μέσω πληρωμής σύμφωνα με τη χρήση. Με αυτόν τον τρόπο όλες οι προηγούμενες ανάγκες καλύπτονται στο ακέραιο. Αξίζει να αναφερθεί ό,τι πολλοί χρήστες διαπίστωσαν ότι η συγκεκριμένη προσέγγιση παρέχει απόδοση της επένδυσης πολύ μεγαλύτερη από αυτή που θα περίμεναν οι διαχειριστές των εκάστοτε εταιρειών.

Το υπολογιστικό νέφος, επιπλέον, παρουσιάζεται ως μια συνεχής παροχή υπολογιστικών πόρων ως υπηρεσία για εικονικά κέντρα δεδομένων, αλλά θα πρέπει να γίνει ξεκάθαρο ότι υπολογιστικό νέφος και εικονικά κέντρα δεδομένων είναι δύο εντελώς διαφορετικές έννοιες. Ας πάρουμε για παράδειγμα το γνωστό S3 (Simple Storage Service) της Amazon, το οποίο είναι ένα εικονικό κέντρο δεδομένων σχεδιασμένο για

χρήση στο διαδίκτυο ή και στο υπολογιστικό νέφος και έχει κατασκευαστεί με σκοπό την παροχή ευκολότερης δημιουργία διαδικτυακών εφαρμογών για τους προγραμματιστές [08]. Σύμφωνα με την ίδια την Amazon: «*Το S3 παρέχει μια απλή διεπαφή μέσω διαδικτύου, η οποία μπορεί να χρησιμοποιηθεί για την αποθήκευση και την ανάκτηση οποιουδήποτε μεγέθους δεδομένων, οποιαδήποτε ώρα, από οπουδήποτε στο διαδίκτυο. Επιτρέπει στους προγραμματιστές να έχουν πρόσβαση στην ίδια φθηνή, αξιόπιστη, γρήγορη και ευέλικτη, σε θέματα επεκτασιμότητας, υποδομή αποθήκευσης δεδομένων που χρησιμοποιεί και η Amazon για να τρέχει το ιδιωτικό της δίκτυο από ιστοσελίδες. Η υπηρεσία στοχεύει να μεγιστοποιήσει τα οφέλη της διαβάθμισης των πόρων και να περάσει αυτά τα οφέλη στους προγραμματιστές*» [08].

Είναι γεγονός ότι η Amazon έχει παίξει πρωταρχικό και ζωτικό ρόλο στην ανάπτυξη του υπολογιστικού νέφους. Εκμοντερνίζοντας τα κέντρα δεδομένων της μετά την έκρηξη του διαδικτύου το 2001, ανακάλυψε ότι η νέα αρχιτεκτονική νέφους (Cloud Architecture) που υλοποίησε, οδήγησε σε ορισμένες πολύ σημαντικές βελτιώσεις στην εσωτερική της αποδοτικότητα. Ως εκ τούτου, η Amazon παρέχοντας σε άλλους χρήστες πρόσβαση μέσω των συστημάτων της δηλαδή μιας φιλοσοφίας UC, την Amazon Web Services (AWS) [09], η οποία θεσπίστηκε το 2002, ξεκίνησε η επανάσταση του υπολογιστικού νέφους. Η AWS ξεκίνησε την υλοποίηση του μοντέλου της, ενοικιάζοντας υπολογιστικούς κύκλους (computing cycles) ως υπηρεσία στις διευθύνσεις διαδικτύου διαφόρων πελατών της, οπουδήποτε στον πλανήτη βρίσκονταν η συγκεκριμένη διεύθυνση. Αυτή η προσέγγιση εκμοντέρνισε το ύφος της πληροφορικής ενώ παράλληλα, δυνατότητες σχετικές με την πληροφορική θα μπορούσαν να παρέχονται στους χρήστες – πελάτες της ως υπηρεσία (as-a-Service). Επιτρέποντας στους χρήστες να έχουν πρόσβαση σε τεχνολογικές υπηρεσίες στο υπολογιστικό νέφος, χωρίς να γνωρίζουν την ύπαρξή του, αφενός εξειδικεύτηκε, αφετέρου έλεγχε τη λειτουργία της τεχνολογικής υποδομής, η οποία παρείχε αυτές τις υπηρεσίες. Με αυτό τον τρόπο, η Amazon άλλαξε ριζικά την προσέγγιση για την υπολογιστή ισχύ (computing). Αυτή η προσέγγιση, η οποία σήμερα ονομάζεται Λογισμικό-ως-Υπηρεσία (Software as a Service – SaaS) [10], μετασχημάτισε το υπολογιστικό νέφος σε ένα παράδειγμα όπου τα

δεδομένα είναι μόνιμα αποθηκευμένα σε απομακρυσμένους διακομιστές, προσβάσιμους μόνο μέσω διαδικτύου και, όταν και εφόσον ζητηθεί, αποθηκεύεται προσωρινά μέρος τους στις συσκευές των χρηστών της, οι οποίες μπορεί να είναι σταθεροί ή φορητοί υπολογιστές, smartphones, tablets κτλ. Στις επόμενες παραγράφους θα αναλυθεί εκτενέστερα πώς λειτουργεί σήμερα η συγκεκριμένη προσέγγιση.

Αξίζει να αναφερθεί ότι αρκετοί, ακόμα και μέσα από τους κύκλους των επιστημόνων της πληροφορικής, συγχέουν το υπολογιστικό νέφος με το Grid Computing (GC) [11]. Το GC είναι ένας τύπος κατανεμημένων υπολογιστικών πόρων οι οποίοι υλοποιούν ένα εικονικό υπερυπολογιστή. Ο συγκεκριμένος υπερυπολογιστής δημιουργείται από ένα σύμπλεγμα δικτυωμένων υπολογιστών είτε μέσω δικτύου ή μέσω του διαδικτύου και λειτουργεί στο σύνολό του ως ένας υπολογιστής, ο οποίος είναι σε θέση να επιτελέσει μεγάλες, σε υπολογιστικούς πόρους, εφαρμογές. Πολλές από τις υλοποιήσεις υπολογιστικού νέφους σήμερα τροφοδοτούνται μέσω εφαρμογών GC και χρεώνονται ως υπηρεσίες, αλλά θα πρέπει να γίνει κατανοητό ότι το υπολογιστικό νέφος είναι απαραίτητο να θεωρείται ως ένα εξελιγμένο ή επόμενο βήμα της παροχής υπηρεσιών του GC. Υπάρχει μια ραγδαίως αναπτυσσομένη λίστα από παρόχους, οι οποίοι χρησιμοποιούν επιτυχώς αρχιτεκτονικές νέφους με λιγοστή έως ανύπαρκτη κεντρική υποδομή ή σύστημα πληρωμών, όπως για παράδειγμα το δίκτυο peer-to-peer BitTorrent και η εθελοντική υπολογιστική ισχύς του SETI@home.

Οι πλατφόρμες παροχής υπηρεσιών πωλήσεων μπορεί να θεωρηθούν επίσης ως μια ακόμη παραλλαγή του SaaS. Αυτού του είδους το υπολογιστικό νέφος παρέχει έναν κεντρικό κόμβο πάνω στον οποίο τρέχει η υπηρεσία με την οποία αλληλεπιδρούν οι χρήστες. Επί του παρόντος, η πιο συχνά χρησιμοποιούμενη εφαρμογή της συγκεκριμένης πλατφόρμας βρίσκεται σε περιβάλλοντα σχετικά με τον τομέα των χρηματοπιστωτικών συναλλαγών ή σε συστήματα τα οποία επιτρέπουν στους χρήστες να παραγγέλνουν διάφορα αγαθά όπως ταξίδια ή προσωπικές υπηρεσίες από μια κοινή πλατφόρμα η οποία έχει σαν σκοπό τη διασφάλιση τιμής και της παροχής της υπηρεσίας σύμφωνα με

τις προδιαγραφές που καθορίστηκαν από τον χρήστη. Τυπικά παραδείγματα των παραπάνω είναι τα expedia.com και hotels.com.

Μία από τις βασικότερες ανησυχίες των χρηστών σχετικά με το υπολογιστικό νέφος, συνεχίζει να είναι η αξιοπιστία του. Η πλειοψηφία των σημερινών υποδομών υπολογιστικού νέφους αποτελείται από υπηρεσίες οι οποίες έχουν ελεγχθεί τόσο χρονικά όσο και σε θέματα αξιοπιστίας. Είναι χτισμένες πάνω σε διακομιστές οι οποίοι ποικίλλουν σε επίπεδο εικονικών τεχνολογιών και παραδίδονται στους χρήστες μέσω κέντρων δεδομένων τα οποία λειτουργούν με γραπτές συμφωνίες εγγύησης συνεχούς λειτουργίας 99.999% ή μεγαλύτερη. Οι εμπορικές προσφορές έχουν εξελιχθεί ούτως ώστε να ανταποκρίνονται στις απαιτήσεις των πελατών σχετικά με τη διασφάλιση της ποιότητας (Quality of Service - QoS) των προσφερόμενων υπηρεσιών και τυπικά προσφέρουν τα προηγούμενα μέσω συμβολαίων – Service Level Agreements (SLAs) που υπογράφονται και από τις δύο πλευρές. Από τη μεριά των χρηστών, το υπολογιστικό νέφος φαίνεται ως ένα μοναδικό σημείο μέσω του οποίου έχουν πρόσβαση σε όλες τις υπολογιστικές τους ανάγκες. Αυτού του είδους οι υπηρεσίες μέσω του υπολογιστικού νέφους είναι προσβάσιμες από τους χρήστες οπουδήποτε ανά την υφήλιο εφόσον υπάρχει σύνδεση στο διαδίκτυο. Αξίζει να σημειωθεί ότι τα ελεύθερα πρότυπα και το λογισμικό ανοικτού κώδικα είναι επίσης σημαντικοί παράγοντες στην ανάπτυξη του νέφους , θέματα τα οποία θα συζητηθούν εκτενέστερα.

Επειδή οι πελάτες δεν έχουν στην ιδιοκτησία τους την υποδομή που χρησιμοποιείται από το υπολογιστικό νέφος, απαλλάσσονται από τις δαπάνες αγοράς εξοπλισμού και καταναλώνουν πόρους ως υπηρεσία, πληρώνοντας μόνο για ο,τι χρησιμοποιούν ανά μονάδα χρόνου, όπως ακριβώς γίνεται και σε όλες τις άλλες υπηρεσίες κοινής ωφέλειας, π.χ. ΔΕΗ. Σχεδόν όλοι οι πάροχοι υπηρεσιών υπολογιστικού νέφους έχουν υιοθετήσει το UC και είτε ένα μοντέλο πληρωμών, όπως περιγράφηκε και πριν, ή χρεώνουν τους χρήστες τους μια μηνιαία συνδρομή. Με τον διαμοιρασμό υπολογιστικών πόρων μεταξύ πολλών χρηστών, τα ποσοστά χρήσης τους βελτιώνονται αρκετά, επειδή οι διακομιστές του υπολογιστικού νέφους δεν είναι ποτέ ανενεργοί ή σε αδράνεια. Αυτός

και μόνο ο παράγοντας από μόνος του μπορεί να μειώσει σημαντικά το κόστος της υποδομής από τη μία, και να αυξήσει την ταχύτητα της ανάπτυξης εφαρμογών από την άλλη.

Μια ευεργετική παράμετρος της χρήσης του συγκεκριμένου μοντέλου είναι ότι η υπολογιστική χωρητικότητα αυξάνεται δραματικά, από τη στιγμή που οι πελάτες δεν είναι υποχρεωμένοι να κατασκευάζουν την εφαρμογή τους για τις ώρες αιχμής, όταν δηλαδή τα φορτία επεξεργασίας είναι στο μέγιστο επιτρεπτό βαθμό. Τέλος, βασικός παράγοντας της υιοθέτησης του μοντέλου υπολογιστικού νέφους ήταν η μεγαλύτερη δυνατότητα αυξημένης ταχύτητας σύνδεσης στο διαδίκτυο. Με τη διεύρυνση της χρήσης του υπολογιστικού νέφους προέκυψαν άλλα ζητήματα τα οποία θα πρέπει να εξεταστούν, βασικότερα των οποίων είναι τα νομικά ζητήματα.

Το τι συμβαίνει με το νομικό πλαίσιο και τα νομικά ζητήματα γενικότερα στα μοντέλα του υπολογιστικού νέφους συνεχίζει να είναι ένα φλέγον ζήτημα, μιας και είχε φέρει στην επιφάνεια νέες διαστάσεις και προκλήσεις στη νομοθεσία, αρκετές από τις οποίες δεν έχουν ακόμα επιλυθεί. Στο παρελθόν έγιναν μερικές προσπάθειες για τη δημιουργία και ενοποίηση ενός νομικού περιβάλλοντος ειδικά για το υπολογιστικό νέφος. Για παράδειγμα, η νομοθεσία Safe Harbor μεταξύ των Η.Π.Α. και της Ε.Ε. παρέχει ένα πλαίσιο επτά σημείων για τις εταιρείες που έχουν έδρα τις Η.Π.Α και ενδέχεται να χρησιμοποιούν δεδομένα από άλλα μέρη του κόσμου, όπως για παράδειγμα την Ε.Ε [12]. Το συγκεκριμένο πλαίσιο ορίζει το πώς οι εταιρείες μπορούν να συμμετέχουν και να πιστοποιούν την τήρηση συγκεκριμένων κανόνων και αυτός ο τρόπος ορίζεται λεπτομερώς στις ιστοσελίδες του Υπουργείου Εμπορίου των Η.Π.Α. Εν περιλήψει, η συμφωνία επιτρέπει στις περισσότερες εταιρείες των Η.Π.Α να πιστοποιήσουν ότι έχουν προσχωρήσει σε μια οργάνωση αυτορρύθμισης, σχετική με τα επτά σημεία ή έχουν υλοποιήσει δικές τους πολιτικές ασφαλείας, οι οποίες συμμορφώνονται με τις ακόλουθες αρχές:

1. Ειδοποίηση των χρηστών σχετικά με τους σκοπούς για τους οποίους συλλέγονται οι εκάστοτε πληροφορίες, καθώς και τον τρόπο που χρησιμοποιούνται.

2. Εκχώρηση στους χρήστες του δικαιώματος επιλογής αν θέλουν και πόσο να κοινοποιηθούν σε τρίτους οι πληροφορίες τους.
3. Διασφάλιση ότι αν γίνει μεταφορά προσωπικών πληροφοριών χρηστών σε τρίτους, ο τελικός αποδέκτης θα παρέχει επίσης το ίδιο επίπεδο προστασίας της ιδιωτικότητας των χρηστών.
4. Ελεύθερη πρόσβαση από τους χρήστες στις προσωπικές τους πληροφορίες.
5. Λήψη απαραίτητων και εύλογων προφυλάξεων ασφαλείας για την προστασία των δεδομένων που συλλέγονται από απώλεια, κακή χρήση ή αποκάλυψη.
6. Λήψη απαραίτητων και εύλογων μέτρων για την εξασφάλιση την ακεραιότητας των δεδομένων που συλλέγονται, και
7. Εγκατάσταση επαρκούς μηχανισμός επιβολής.

Οι σημαντικότεροι πάροχοι υπηρεσιών, όπως για παράδειγμα η AWS, απευθύνονται σε μια παγκόσμια αγορά, όπως για παράδειγμα στις Η.Π.Α, την Ιαπωνία, την Ε.Ε., με την ανάπτυξη τοπικών υποδομών σε αυτές τις περιοχές και δίνοντας τη δυνατότητα στους χρήστες να επιλέγουν μόνοι τους τις ζώνες διαθεσιμότητας. Παρ' όλα αυτά, εξακολουθούν να υπάρχουν ανησυχίες σχετικά με την ασφάλεια και την ιδιωτικότητα τόσο σε επίπεδο χρηστών όσο και σε επίπεδο κυβερνητικών οργανισμών. Πρωταρχικό μέλημα είναι ο επονομαζόμενος USA PATRIOT ACT από τη μία και ο Electronic Communications Privacy Act's Stored Communications Act από την άλλη [13, 14]. Ο πρώτος είναι ένα νομοθέτημα του Κογκρέσου των Η.Π.Α. το οποίο προσυπέγραψε ο πρόεδρος W. Bush τον Οκτώβριο του 2001 και προέρχεται από τα αρχικά «Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001». Ο συγκεκριμένος νόμος επέκτεινε τον ήδη υπάρχοντα νόμο περί τρομοκρατίας ούτως ώστε να περιλαμβάνει και την εγχώρια τρομοκρατία, διευρύνοντας έτσι τον αριθμό των δραστηριοτήτων στις οποίες θα μπορούσαν να εφαρμοστούν οι υπηρεσίες επιβολής του νόμου. Πιο συγκεκριμένα, ενίσχυσε τη δυνατότητα των υπηρεσιών επιβολής του νόμου να είναι σε θέση να εποπτεύουν – παρακολουθούν τις τηλεφωνικές κλήσεις, τα e-mail, τις ιατρικές, οικονομικές και κάθε άλλου είδους επικοινωνίες – συναλλαγές. Επιπρόσθετα, οι υπηρεσίες

επιβολής καθώς και οι υπηρεσίες σχετικά με τους μετανάστες, έχουν μεγαλύτερη ευχέρεια παρακολούθησης αλλοδαπών που κρατούνταν και απελαύνονταν ή σχετίζονταν με τρομοκρατικές ή συναφείς πράξεις. Επίσης, μείωσε τους περιορισμούς για συλλογή πληροφοριών για άλλες χώρες οι οποίες συγκεντρώνονται εντός των Η.Π.Α. Τέλος, επέκτεινε την υπηρεσία «Secretary of the Treasury's» ώστε να είναι σε θέση να ρυθμίζει χρηματοπιστωτικές συναλλαγές οι οποίες περιελάμβαναν ξένους ιδιώτες και επιχειρήσεις.

Ο δεύτερος νόμος συνοψίζεται στα ακόλουθα. Αδικήματα που διαπράττονται στο πλαίσιο του προηγούμενου νόμου περιλαμβάνουν την εκούσια πρόσβαση χωρίς άδεια σε μια εγκατάσταση μέσω της οποίας παρέχεται μια ηλεκτρονική υπηρεσία επικοινωνίας ή τη σκόπιμη υπέρβαση της άδειας χρήσης για απόκτηση πρόσβασης στην υπηρεσία προκειμένου να αποκτήσει, μεταβάλει ή να εμποδίσει την εξουσιοδοτημένη πρόσβαση σε μια ενσύρματη η ηλεκτρονική επικοινωνία, ενώ το σύστημα είναι κατασκευασμένο για το αντίθετο. Τα άτομα που καταδικάζονται με βάση τον συγκεκριμένο νόμο, μπορούν να τιμωρηθούν αν το αδίκημα διαπράχθηκε για λόγους εμπορικού πλεονεκτήματος, για κακόβουλη καταστροφή ή ζημιά, ή ιδιωτικό εμπορικό κέρδος, ή στο πλαίσιο της προώθησης κάποιας ενδεχόμενης ποινικής ή ζημιογόνας πράξης, σε παραβίαση των νόμων των Η.Π.Α. ή κάποιας επιμέρους πολιτείας με πρόστιμο ή φυλάκιση ή και τα δύο, αλλά όχι για παραπάνω από πέντε χρόνια στην περίπτωση αδικήματος που διαπράχθηκε για πρώτη φορά. Για διάπραξη δεύτερης φοράς ή κατά συρροή οι ποινές γίνονται πολύ πιο αυστηρές τόσο σε πρόστιμα όσο και σε φυλάκιση, η οποία δεν πρέπει να ξεπερνά τα δέκα χρόνια και για τα δύο.

Υπάρχει μια σειρά από βασικά χαρακτηριστικά σχετικά με το περιβάλλον του υπολογιστικού νέφους. Προσφορές σχετικές με τις παρεχόμενες υπηρεσίες είναι συνήθως διαθέσιμες σε συγκεκριμένους πελάτες και μικρές εταιρείες, οι οποίοι βλέπουν τη χρήση του υπολογιστικού νέφους ως πλεονέκτημα λόγω της μείωσης των κεφαλαιούχων δαπανών. Αυτό εξυπηρετεί στη μείωση των ενστάσεων σχετικά με την είσοδο των εταιρειών στο υπολογιστικό νέφος, από τη

στιγμή που η υποδομή που χρησιμοποιείται για να παρέχει τις προσφορές ανήκει στον πάροχο και δεν υπάρχει λόγος αγοράς από τον πελάτη. Επίσης, με δεδομένο ότι οι χρήστες δεν είναι υποχρεωμένοι να συνδέονται με μια συγκεκριμένη συσκευή, το μόνο που χρειάζονται είναι η δυνατότητα πρόσβασης στο διαδίκτυο, και επειδή το διαδίκτυο εξασφαλίζει την πρόσβαση από οποιαδήποτε περιοχή, η χρήση των υπηρεσιών του υπολογιστικού νέφους επιτρέπει στους πελάτες των παρόχων να έχουν πρόσβαση στις υπηρεσίες ανεξάρτητα από το που μπορεί να βρίσκονται ή τι είδους συσκευή χρησιμοποιούν.

Η πολλαπλή μίσθωση (multitenancy) των πόρων επιτρέπει την κοινή χρήση τους καθώς και τον διαμοιρασμό του κόστους μεταξύ μιας μεγάλης ομάδας χρηστών [15]. Τα γενικά οφέλη μιας προσέγγισης πολλαπλής μίσθωσης περιλαμβάνουν:

- Συγκέντρωση της υποδομής σε ένα μέρος και με μικρότερο κόστος
- Αυξημένη ανταπόκριση σε φορτία κατά τη διάρκεια μιας μεγάλης ζήτησης
- Βελτίωση της απόδοσης των συστημάτων τα οποία συχνά υποχρησιμοποιούνται
- Δυναμική κατανομή της κεντρικής μονάδας επεξεργασίας (Central Processing Unit – CPU), των αποθηκευτικών μέσων και του εύρους ζώνης του δικτύου
- Σταθερή απόδοση που παρακολουθείται από τον πάροχο της υπηρεσίας

Επίσης, ως πλεονέκτημα προστίθεται στα περιβάλλοντα υπολογιστικού νέφους η αξιοπιστία, επειδή οι πάροχοι υπηρεσιών αξιοποιούν πλεονάζουσες θέσεις. Αυτό είναι ιδιαίτερα ελκυστικό στις επιχειρήσεις καθώς εξασφαλίζει από τη μία την συνεχή λειτουργία και από την άλλη ανάκαμψη μετά από κάποια καταστροφή. Από την άλλη πλευρά όμως, βασικό μειονέκτημα είναι ότι οι διαχειριστές των εκάστοτε πληροφοριακών συστημάτων δεν μπορούν να κάνουν σχεδόν τίποτα στην περίπτωση που συμβεί μια διακοπή.

Ένα άλλο πλεονέκτημα το οποίο καθιστά τις υπηρεσίες νέφους ακόμα πιο αξιόπιστες, είναι η δυνατότητα διαβάθμισης (scalability) [16].

Η δυνατότητα διαβάθμισης είναι η λειτουργία που προσφέρει το υπολογιστικό νέφος, ώστε η υπολογιστική ισχύς που παρέχεται στο χρήστη να μπορεί να αλλάζει δυναμικά ανάλογα με τις απαιτήσεις του. Επειδή ο πάροχος υπολογιστικού νέφους διαχειρίζεται την αναγκαία υποδομή, η όλη ασφάλεια του συστήματος είναι σημαντικά βελτιωμένη. Σαν αποτέλεσμα της συγκέντρωσης των δεδομένων σε ένα σύστημα, υπάρχει ένα αυξημένο ενδιαφέρον για την προστασία των πόρων του πελάτη που τηρείται από τον φορέα παροχής υπηρεσιών. Για να διαβεβαιωθούν οι πελάτες ότι τα δεδομένα τους είναι ασφαλή, οι πάροχοι υπηρεσιών σπεύδουν να επενδύσουν σε ειδικό προσωπικό ασφαλείας. Ίσως σε μεγάλο βαθμό το προηγούμενο να θεωρείται επωφελές για τους χρήστες, δημιουργεί, παρόλα αυτά, ανησυχίες σχετικά με την απώλεια ελέγχου των ευαίσθητων δεδομένων από τους χρήστες. Συνήθως, η πρόσβαση στα δεδομένα καταγράφεται λεπτομερώς, αλλά η πρόσβαση στα αρχεία καταγραφής συμβάντων (audit logs) μπορεί να είναι από δύσκολη έως αδύνατη για τους πελάτες.

Η λειτουργία των κέντρων δεδομένων, των ηλεκτρονικών υπολογιστών, και γενικότερα όλης της συναφούς υποδομής που απαιτείται για την υποστήριξη του υπολογιστικού νέφους, καταναλώνει μεγάλα ποσά ενέργειας. Η βιωσιμότητα του υπολογιστικού νέφους επιτυγχάνεται με την αξιοποίηση βελτιώσεων στη χρήση των πόρων και την υλοποίηση πιο αποδοτικών ενεργειακά συστημάτων. Από το 2007 η Google [17], η IBM [18] και ένας μεγάλος αριθμός πανεπιστημίων, είχαν ξεκινήσει να εργάζονται σε ένα ερευνητικό πρόγραμμα σχετικό με μεγάλα μεγέθους υπολογιστικού νέφους συστήματα. Μέχρι το καλοκαίρι του 2008 είχαν προγραμματιστεί σχετικά λίγες εκδηλώσεις πάνω στο υπολογιστικό νέφος. Η πρώτη ετήσια συνδιάσκεψη για το υπολογιστικό νέφος είχε προγραμματιστεί να υλοποιηθεί με την μορφή τηλεδιάσκεψης από τις 20 έως τις 24 Απριλίου του 2009. Σύμφωνα με την επίσημη ιστοσελίδα: «*η συγκεκριμένη τηλεδιάσκεψη είναι η κορυφαία εκδήλωση του υπολογιστικού νέφους ανά την υφήλιο, καλύπτοντας έρευνα, ανάπτυξη και καινοτομίες για τον κόσμο του υπολογιστικού νέφους. Το συγκεκριμένο πρόγραμμα αντικατοπτρίζει το υψηλότερο επίπεδο επιτευγμάτων στην κοινότητα του υπολογιστικού νέφους, ενώ οι προσκεκλημένοι ομιλητές περιλαμβάνουν ένα εξαιρετικό σύνολο*

παρουσιάσεων. Τα πάνελ, τα σεμινάρια και τα μαθήματα επιλέχθηκαν ώστε να καλύπτουν μια σειρά από τα πιο καυτά θέματα του υπολογιστικού νέφους » [19].

Μπορεί να φαίνεται ότι όλος ο κόσμος ενθουσιάστηκε σχετικά με τις δυνατότητες του υπολογιστικού νέφους, παρόλα αυτά αρκετοί σύμβουλοι ή στελέχη επιχειρήσεων στόχευσαν στο να μάθουν για το ποια θα είναι η ευκαιρία της αγοράς για τη συγκεκριμένη τεχνολογία καθώς και το τι μέλλει γενέσθαι στο ενδεχόμενο μακροχρόνιας χρήσης του, μιας και στις αρχές της προηγούμενης δεκαετίας ήταν ακόμα σε πολύ πρώιμο στάδιο. Έρευνες και δεδομένα διεξήχθησαν, μέσω οποίων εξάχθηκαν αρκετά συμπεράσματα πάνω στα προηγούμενα. Σήμερα, και οι χρήσεις του υπολογιστικού νέφους είναι πολλαπλές. Ως μια γενική και αφηρημένη άποψη μπορεί να θεωρηθεί ότι το υπολογιστικό νέφος μπορεί να φέρει τις δυνατότητες των υπερυπολογιστών στους απλούς ανθρώπους και γενικότερα στον οποιοδήποτε. Εταιρείες όπως η Yahoo [20], η Google [17], η Microsoft [21], η IBM [18] και άλλες, ασχολούνται με τη δημιουργία και παροχή υπηρεσιών υπολογιστικού νέφους για να είναι σε θέση να δίνουν στους χρήστες τους ακόμα καλύτερα πρόσβαση στα δεδομένα και να βοηθήσουν σε ζητήματα καθημερινότητας, όπως υγειονομική περίθαλψη, ασφάλιση και χρηματοπιστωτικές συναλλαγές.

Οι μεγαλύτερες προκλήσεις που αντιμετωπίζουν όλες οι εταιρείες παροχής υπηρεσιών υπολογιστικού νέφους είναι η ασφαλής αποθήκευση των δεδομένων, οι συνδέσεις υψηλών ταχυτήτων πρόσβασης στο διαδίκτυο, που δυστυχώς ακόμα δεν είναι ευρεία, και, τέλος, η τυποποίηση. Η αποθήκευση μεγάλου όγκου δεδομένων, η οποία απαιτείται να είναι προσανατολισμένη στην ιδωτικότητα του χρήστη, στην ταυτότητά του και στις συγκεκριμένες προτιμήσεις που έχει σχετικά με τις εφαρμογές που χρησιμοποιεί, έχει ως αποτέλεσμα την εμφάνιση πολλών ανησυχιών σχετικά με την προστασία των δεδομένων. Οι προηγούμενοι προβληματισμοί, με τη σειρά τους, οδηγούν σε σειρά ερωτήσεων σχετικά με το νομικό πλαίσιο που θα πρέπει να εφαρμοστεί σε ένα περιβάλλον υπολογιστικού νέφους. Μια άλλη πρόκληση για το υπολογιστικό νέφος είναι το γεγονός ότι η διείσδυση της ευρυζωνικότητας, μέσω γραμμών DSL (Digital Subscriber Line), στις

Η.Π.Α. υπολείπεται σε σχέση με άλλες χώρες της Ευρώπης και της Ασίας, αν και έχουν γίνει αρκετά και γενναία βήματα προς την ευρυζωνικότητα σε επίπεδο απλών χρηστών. Το υπολογιστικό νέφος δεν μπορεί να λειτουργήσει αποδοτικά χωρίς συνδέσεις υψηλών ταχυτήτων, ενσύρματες ή ασύρματες. Στην περίπτωση που δεν υπάρχουν συνδέσεις υψηλών ταχυτήτων, οι υπηρεσίες που προσφέρει το υπολογιστικό νέφος δεν μπορούν να είναι προσβάσιμες.

Πέρα από τις προκλήσεις που αναφέρθηκαν στην προηγούμενη παράγραφο, ένα αμφιλεγόμενο θέμα στους κύκλους της πληροφορικής που ανέκυψε πρόσφατα είναι η αξιοπιστία του υπολογιστικού νέφους. Εξαιτίας της δημόσιας διάθεσης του περιβάλλοντος του υπολογιστικού νέφους, προβλήματα που συμβαίνουν σε αυτό τείνουν να λάβουν τεράστια δημοσιότητα στο ευρύ κοινό. Σε αντίθεση με τα προβλήματα που εμφανίζονται σε περιβάλλοντα επιχειρήσεων, τα οποία τις περισσότερες φορές αντιμετωπίζονται χωρίς να λάβει δημοσιότητα το γεγονός, στην περίπτωση του υπολογιστικού νέφους ακόμα και λίγοι χρήστες αν έχουν έστω ένα πρόβλημα, γίνονται πρωτοσέλιδα στον Τύπο.

Ιστορικά, τον Οκτώβριο του 2008, η Google δημοσιοποίησε ένα άρθρο στο οποίο ανέφερε τα συμπεράσματα από τη φιλοξενία άνω του ενός εκατομμυρίου εταιρικών πελατών στο δικό της υπολογιστικό νέφος [17]. Το προσωπικό της Google μέτρησε τη διαθεσιμότητα ως προς το ποσοστό του χρόνου λειτουργίας ανά χρήστη βασισμένο στα ποσοστά σφαλμάτων που καταγράφηκαν στους διακομιστές της. Πίστευαν ότι αυτή η αξιόπιστη μέτρηση επιτρέπει τη βέλτιστη σύγκριση με άλλες λύσεις υπολογιστικού νέφους. Οι μετρήσεις τους για κάθε αίτημα στο διακομιστή και για κάθε χρήστη, σημειώθηκαν οποιαδήποτε στιγμή της ημέρας, καταγράφοντας ακόμα και καθυστέρηση 1 msec. Η Google ανέλυσε τα δεδομένα που συνέλεξε κατά τη διάρκεια ενός έτους και βρέθηκε ως αποτέλεσμα ότι η SaaS υπηρεσία Gmail ήταν διαθέσιμη στον οποιοδήποτε περισσότερο από 99.99% του χρόνου.

Κάποιος θα μπορούσε να αναρωτηθεί για τον τρόπο με τον οποίο το 99.99% που προέκυψε από τις μετρήσεις θα μπορούσε να συγκριθεί με τις συμβατικές μεθόδους που χρησιμοποιούνταν για τη λήψη και αποστολή email. Σύμφωνα με την εταιρεία ερευνών Radicati Group,

εταιρείες με εφαρμογές e-mail εγκατεστημένες σε τοπικούς δικούς τους διακομιστές είχαν κατά μέσο όρο από 30 έως 60 λεπτά απρογραμμάτιστων και επιπλέον 36 έως 90 λεπτά προγραμματισμένων διακοπών λειτουργίας σε περίοδο χρήσης ενός μήνα, σε σύγκριση με τα 10 έως 15 λεπτά χρόνου διακοπής από το Gmail [22]. Η Google, με βάση την ανάλυση αυτών των ευρημάτων, ισχυρίστηκε ότι για απρογραμμάτιστες διακοπές, το Gmail είναι διπλάσια αξιόπιστο από τη λύση του Novell GroupWise [23] και τέσσερις φορές περισσότερο αξιόπιστο από τη λύση Microsoft Exchange-Based [24]. Αξίζει να σημειωθεί ότι και οι δύο προηγούμενες εφαρμογές προϋποθέτουν τη διατήρηση και συντήρηση εξοπλισμού εντός των ορίων τους. Θεωρείται αυτονόητο ότι μεγαλύτερη αξιοπιστία θα μεταφραστεί σε αύξηση της παραγωγικότητας των εργαζομένων της εταιρείας. Επίσης, σε άλλη έρευνα που διεξήγε η Google, ανακάλυψε ότι το Gmail είναι 10 φορές πιο αξιόπιστο από τη λύση Exchange-Based στην περίπτωση που ο παράγοντας των προγραμματισμένων διακοπών είναι εγγενής στην εσωτερική λειτουργία ανταλλαγής e-mail [25].

Η Google, βασισμένη στα προηγούμενα ευρήματα, είχε αρκετή αυτοπεποίθηση για να ανακοινώσει δημοσίως, τον Οκτώβριο του 2008, ότι η συμφωνία σε επίπεδο συνεχούς λειτουργίας 99.99% που πρόσφερε στους εταιρικούς της πελάτες, οι οποίοι χρησιμοποιούσαν το Gmail θα επεκτείνονταν στα Google Calendar [26], Google Docs [27], Google Sites [28] και Google Voice [29]. Από τη στιγμή που περισσότερες από ένα εκατομμύριο εταιρείες χρησιμοποιούν τις εφαρμογές της Google (Google Apps) [30] για να υποστηρίζουν τη μηχανοργάνωσης της εταιρείας τους, η Google προχώρησε σε μια σειρά από δεσμεύσεις για τη βελτίωση της επικοινωνίας με τους πελάτες της κατά τη διάρκεια τυχόν διακοπών και στο να καταστήσει όλα τα ζητήματα ορατά και διαφανή μέσω των ανοικτών ομάδων χρηστών. Το ισχυρότερο επιχείρημά της ήταν ότι από τη στιγμή που η ίδια η Google τρέχει πάνω στην πλατφόρμα των εφαρμογών της, δίνει εξέχουσα βαρύτητα σε αυτό το κομμάτι της πληροφορικής, το θεωρεί εξαιρετικά αξιόπιστο και έχει μεγάλη ισχύ η δέσμευση που έχει αναλάβει να υλοποιήσει. Κλείνοντας, αξίζει να αναφερθεί ότι η Google οδήγησε τη βιομηχανία της πληροφορικής,

εξελίσσοντας έτσι το υπολογιστικό νέφος, ώστε να είναι μέρος του Web 3.0 [31], την επόμενη γενιά του διαδικτύου.

ΚΕΦΑΛΑΙΟ ΤΡΙΤΟ

Η τεχνολογία του υπολογιστικού νέφους

3.1. Εισαγωγή

Στο συγκεκριμένο κεφάλαιο θα αναπτύξουμε τη τεχνολογία που υφίσταται για την λειτουργία του υπολογιστικού νέφους. Θα αναφέρουμε ότι αφορά την υποδομή από το μέρος του πελάτη, του παρόχου και του δικτύου διασύνδεσης αυτών των δύο.

3.2. Υλικό και υποδομή από μέρους του πελάτη

Η τελική υποδομή του υπολογιστικού νέφους είναι αυτή που βρίσκεται στα γραφεία των τελικών χρηστών, οι οποίοι αλληλεπιδρούν με το νέφος. Σε αυτή την ενότητα θα αναφέρουμε τους διάφορους τύπους χρηστών.

Υπάρχουν διάφοροι τύποι χρηστών που μπορούν να συνδεθούν στο υπολογιστικό νέφος, καθένας από τους οποίους προσφέρει διαφορετικό τρόπο αλληλεπίδρασης μεταξύ των δεδομένων και των εφαρμογών. Ανάλογα με τις ανάγκες της εταιρείας, μπορεί να υπάρξει συνδυασμός τύπων χρηστών και συσκευών. Ο τρόπος αλληλεπίδρασης με τα δεδομένα με βάση τους χρήστες, εξαρτάται από ένα σύνολο παραγόντων, όπως ποιες είναι οι ανάγκες των χρηστών και της εταιρείας, σε συνδυασμό με τα πλεονεκτήματα και τα μειονεκτήματα του κάθε τύπου.

3.2.1. Χρήστες φορητών συσκευών

Οι χρήστες φορητών συσκευών χρησιμοποιούν μια πληθώρα από συσκευές, όπως φορητούς υπολογιστές, tablets και έξυπνα τηλέφωνα (smartphones). Είναι δεδομένο ότι δεν είναι δυνατόν να χρησιμοποιηθεί μια ιδιαίτερα ισχυρή εφαρμογή σε ένα tablet ή σε ένα έξυπνο τηλέφωνο, αντίθετα σε φορητούς υπολογιστές μπορεί να υπάρξει πλήρης πρόσβαση στο υπολογιστικό νέφος, όπως ακριβώς συμβαίνει και με τους υπολογιστές γραφείου.

Οι χρήστες φορητών συσκευών έχουν, επίσης, θέματα και με την ασφάλεια και την ταχύτητα. Επειδή οι χρήστες αυτοί συνδέονται στο υπολογιστικό νέφος από ποικίλες τοποθεσίες, οι οποίες είναι πιθανό να μην έχουν την καλύτερη δυνατή ταχύτητα, όπως σε ένα ξενοδοχείο, δεν γίνεται να λειτουργεί το υπολογιστικό νέφος όπως θα λειτουργούσε σε ένα σταθερό υπολογιστή σε ένα γραφείο. Παρόλα αυτά, αξίζει να σημειωθεί ότι δεν χρειάζονται όλες οι εφαρμογές δυνατές συνδέσεις στο διαδίκτυο, μιας και οι χρήστες δεν σκοπεύουν να εισάγουν ή να εξάγουν μεγάλο ποσό δεδομένων από το υπολογιστικό νέφος. Επιπλέον, από τη

στιγμή που η εταιρεία έχει την ευχέρεια να δημιουργήσει τις δικές της εφαρμογές στο υπολογιστικό νέφος, αυτές θα μπορούσαν να υλοποιηθούν έχοντας ως παράμετρο και τη χρήση τους από φορητές συσκευές. Για παράδειγμα, ίσως ένας χρήστης να μην εισάγει μεγάλο όγκο δεδομένων σε μια βάση δεδομένων στο υπολογιστικό νέφος, θα μπορεί όμως μέσω της εφαρμογής να έχει πρόσβαση στα δεδομένα, ή σε μέρος αυτών.

Η ασφάλεια, που είναι ο βασικότερος παράγοντας, είναι ένα θέμα με δύο όψεις. Από τη μια μεριά είναι πολύ εύκολο να χαθεί η να κλαπεί μια φορητή συσκευή, οπότε να θέσει σε κίνδυνο έκθεσης τα δεδομένα που είναι αποθηκευμένα σε αυτή. Από την άλλη πλευρά, αν ο χρήστης έκανε χρήση των υπηρεσιών του υπολογιστικού νέφους, τότε στη συσκευή του θα υπήρχαν από λίγα έως καθόλου δεδομένα, ενώ παράλληλα δεν θα επιτρεπόταν η σύνδεση της συγκεκριμένης συσκευής στο υπολογιστικό νέφος, για να μην υπάρξει περαιτέρω πρόσβαση στα δεδομένα της εταιρείας. Βέβαια, εδώ ανακύπτει και το ζήτημα του τρόπου πρόσβασης, καθώς, αν ο χρήστης μπαίνει από δημόσια δίκτυα, όπως αυτό το ξενοδοχείου, θα μπορεί εύκολα ένας κακόβουλος χρήστης να εισέλθει στα δεδομένα του στο υπολογιστικό νέφος. Τη συγκεκριμένη παράμετρο θα την αναλύσουμε περαιτέρω σε επόμενο κεφάλαιο.

3.2.2. Συσκευές περιορισμένων δυνατοτήτων

Συσκευές περιορισμένων δυνατοτήτων (thin clients) ονομάζονται οι συσκευές, οι οποίες δεν έχουν σκληρό δίσκο, δεν έχουν μονάδα DVD-ROM και απλώς εμφανίζουν στην οθόνη τους ό,τι υπάρχει στον διακομιστή με τον οποίο είναι συνδεδεμένοι [22]. Κλασικά παραδείγματα μπορεί να θεωρηθούν τα smartphones και τα tablets.

Οι συσκευές περιορισμένων δυνατοτήτων ενδεχομένως να έχουν υπόσταση σε μια εταιρεία, μόνο στην περίπτωση που αυτή έχει εσωτερικά ένα δικό της υπολογιστικό νέφος. Φυσικά, αυτό εξαρτάται από το είδος των εφαρμογών και των υπηρεσιών στις οποίες η εταιρεία έχει πρόσβαση στο υπολογιστικό νέφος. Αν ο τελικός χρήστης χρειάζεται μόνο να έχει πρόσβαση στις υπηρεσίες υπολογιστικού νέφους ή σε έναν

εικονικό διακομιστή, τότε οι συσκευές περιορισμένων δυνατοτήτων είναι η βέλτιστη δυνατή λύση. Είναι φθηνότεροι από τις συσκευές πολλαπλών δυνατοτήτων στην αγορά, στη συντήρηση και καταναλώνουν σαφώς λιγότερη ενέργεια. Επίσης, προσφέρουν μεγάλο βαθμό ασφάλειας, επειδή δεν έχουν χώρο να αποθηκεύουν δεδομένα. Όλα τα δεδομένα είναι πάνω στο νέφος, οπότε ο κίνδυνος της φυσικής παραβίασής τους είναι μηδενικός.

3.2.3. Συσκευές πολλαπλών δυνατοτήτων

Συσκευές πολλαπλών δυνατοτήτων (thick clients) ονομάζονται τα υπολογιστικά μηχανήματα που χρησιμοποιούν οι χρήστες, για να συνδεθούν στις εφαρμογές τους στο υπολογιστικό νέφος [32, 33]. Είναι υπολογιστές που έχουν αποθηκευτικό χώρο και εγκατεστημένες εφαρμογές, τις οποίες μπορούν να χρησιμοποιήσουν χωρίς να είναι συνδεδεμένοι στο νέφος. Αυτά τα μηχανήματα μπορούν επίσης να συνδέονται σε έναν εικονικό διακομιστή όπως ακριβώς και οι συσκευές περιορισμένων δυνατοτήτων. Επίσης, είναι καλή επιλογή, αν οι χρήστες θέλουν να διατηρούν αρχεία στον υπολογιστή τους και να λειτουργούν εφαρμογές, οι οποίες δεν είναι στο υπολογιστικό νέφος.

Αναφορικά με την ασφάλεια, οι συσκευές πολλαπλών δυνατοτήτων είναι πιο ευάλωτες σε επιθέσεις από ό,τι οι συσκευές περιορισμένων δυνατοτήτων. Από τη στιγμή που υπάρχουν δεδομένα αποθηκευμένα στον σκληρό του υπολογιστή τοπικά, τότε σε περίπτωση κλοπής του υπολογιστή, τα δεδομένα θα παραβιαστούν. Επιπλέον, τα μηχανήματα αυτά θα πρέπει να διαθέτουν όλες εκείνες τις δικλείδες ασφαλείας που επιβάλλεται να έχει ένα υπολογιστικό σύστημα, όπως για παράδειγμα πρόγραμμα εύρεσης ιών, τείχος προστασίας κτλ. Επίσης, υπάρχει και το ζήτημα της αξιοπιστίας. Αν χαλάσει μια συσκευή πολλαπλών δυνατοτήτων και ο χρήστης δεν έχει πάρει αντίγραφα ασφαλείας, τότε θα χαθούν όλα τα δεδομένα που ήταν αποθηκευμένα σε αυτή. Επιπλέον, θα πάρει χρόνο για να ρυθμιστεί το νέο μηχάνημα με το λειτουργικό του σύστημα, τις εφαρμογές και τις συνδέσεις που θα έχει και τέλος, με τις ρυθμίσεις του χρήστη που θα το χρησιμοποιεί.

3.3. Ασφάλεια από μέρους του πελάτη

Η ασφάλεια είναι ο πρωταρχικός παράγοντας στο υπολογιστικό νέφος. Από τη στιγμή που κάποιος τρίτος αποθηκεύει τα δεδομένα του χρήστη – πελάτη, ο πελάτης δεν γνωρίζει τι συμβαίνει με αυτά. Είναι εύκολο λοιπόν ο πελάτης να αναρωτηθεί τους κινδύνους σχετικά με την ασφάλεια των δεδομένων του αντιμετωπίζει στο υπολογιστικό νέφος, αλλά να δει και τα οφέλη στην ασφάλεια που θα έχει από τη χρήση του υπολογιστικού νέφους.

3.3.1. Διαρροή δεδομένων

Το μεγαλύτερο πλεονέκτημα που προσφέρει το υπολογιστικό νέφος είναι η συγκέντρωση των δεδομένων σε ένα χώρο. Όλες οι εταιρείες έχουν προβλήματα με την ασφάλεια των δεδομένων τους, επειδή αυτά είναι αποθηκευμένα σε πολλά σημεία, όπως φορητοί υπολογιστές, smartphones και σταθεροί υπολογιστές.

Οι συσκευές πολλαπλών δυνατοτήτων μπορούν να κατεβάσουν αρχεία και να τα διατηρούν στον τοπικό σκληρό δίσκο. Οι φορητοί υπολογιστές, οι οποίοι είναι πολύ εύκολο να κλαπούν, έχουν, αν όχι όλο, το μεγαλύτερο ποσοστό των δεδομένων τους μη-κρυπτογραφημένο. Η χρήση των συσκευών περιορισμένων δυνατοτήτων παρέχει μια πρώτης τάξεως ευκαιρία για συγκέντρωση και αποθήκευση των δεδομένων σε ένα χώρο, και ως εκ τούτου η πιθανότητα να κλαπούν δεδομένα ελαχιστοποιείται. Η συγκέντρωση των δεδομένων σε ένα χώρο, επίσης, παρέχει τη δυνατότητα για καλύτερη παρακολούθηση, καθώς η διαδικασία ελέγχου τους καθίσταται πολύ πιο εύκολη.

3.3.2. Μείωση του κόστους – χρόνου εργασίας

Ένα ακόμα πλεονέκτημα ασφάλειας, το οποίο δεν έχει σχέση τόσο με την τεχνολογία, είναι το γεγονός ότι ο διαχειριστής του συστήματος δεν επιβαρύνεται με πολλά πράγματα για την ασφάλεια της υποδομής του νέφους, την οποία επιφορτίζεται εξ ολοκλήρου ο πάροχος

υπηρεσιών του υπολογιστικού νέφους. Επίσης ο πάροχος, σε γενικές γραμμές, προσφέρει περισσότερα εργαλεία ασφάλειας και είναι 24/7 σε εγρήγορση.

Το γεγονός ότι υπάρχει μια πληθώρα χρηστών οι οποίοι πληρώνουν για υπηρεσίες υπολογιστικού νέφους, επιτρέπει στον πάροχο υπηρεσιών υπολογιστικού νέφους να παρέχει σε αυτούς αποτελεσματικότερη ασφάλεια, απλώς και μόνο λόγω της οικονομικής κλίμακας που εμπλέκονται. Αυτό σημαίνει ότι, από τη στιγμή που υπάρχουν πολλοί πελάτες ανεβαίνουν οι χρηματικές απολαβές του παρόχου, οπότε και αυτός με τη σειρά του είναι σε θέση να παρέχει καλύτερες υπηρεσίες.

3.3.3. Αρχεία καταγραφής συμβάντων

Τα αρχεία καταγραφής συμβάντων στις υπηρεσίες υπολογιστικού νέφους είναι επίσης βελτιωμένα, αναφορικά με τον όγκο. Στην περίπτωση όπου μια εταιρεία έχει το πληροφοριακό της σύστημα εντός των φυσικών της ορίων και σε δική της υποδομή, ο αποθηκευτικός χώρος για τα αρχεία καταγραφής συμβάντων είναι περιορισμένος. Αντίθετα, στην περίπτωση του υπολογιστικού νέφους, ο χώρος για την αποθήκευση των αρχείων καταγραφής συμβάντων μπορεί να είναι οσοδήποτε μεγάλος τον θέλει ο χρήστης με το μικρότερο δυνατό κόστος για αυτόν.

3.4. Δίκτυο

Σε γενικές γραμμές η πρόσβαση στις υπηρεσίες του υπολογιστικού νέφους γίνεται μέσω διαδικτύου. Με σκοπό όμως την καλύτερη παροχή υπηρεσιών από τους παρόχους προς τους πελάτες τους, υπάρχουν διάφορα επίπεδα σύνδεσης, όταν αυτό απαιτείται.

Έρευνα που δημοσιεύτηκε στο περιοδικό Gartner [34] αναγνώρισε τέσσερα διαφορετικά επίπεδα πρόσβασης. Στην έρευνα αυτή υποστηρίχθηκε ότι διαφορετικές εταιρείες και μεμονωμένοι πελάτες

έχουν διαφορετικές απαιτήσεις από το υπολογιστικό νέφος και ως εκ τούτου θα πρέπει να συνδέονται σε αυτό με διαφορετικούς τρόπους. Επομένως, ό,τι λειτουργεί αποδοτικά σε επίπεδο σύνδεσης σε μια εταιρεία, ενδεχομένως να μην λειτουργεί το ίδιο αποδοτικά σε μια άλλη ή σε ένα μεμονωμένο χρήστη.

3.4.1. Βασικό δημόσιο διαδίκτυο

Η πρώτη επιλογή πρόσβασης είναι η σύνδεση που έχουμε όλοι μας στο γραφείο ή στο σπίτι μας και είναι η απλή σύνδεση διαδικτύου που μας παρέχει κάποιος πάροχος υπηρεσιών διαδικτύου και συνδεόμαστε μέσω τηλεφωνικής γραμμής σε δίκτυο ADSL ή VDSL. Η συγκεκριμένη επιλογή είναι η βασικότερη και απλούστερη επιλογή που έχει ο χρήστης για να συνδεθεί στο νέφος.

Παρόλα αυτά, το βασικό διαδίκτυο είναι αυτό ακριβώς που περιγράφει ό όρος. Δεν περιέχει τίποτα παραπάνω, όπως επιτάχυνση του πρωτοκόλλου TCP [36] ή προηγμένη συμπίεση δεδομένων μεταφοράς, εκτός από τη βασική σύνδεση.

Στα πλεονεκτήματα της βασικής σύνδεσης στο διαδίκτυο είναι ο μεγάλος αριθμός πελατών, η δυνατότητα επιλογής μεταξύ πολλών παρόχων και η χρήση του πρωτοκόλλου SSL [37] πάνω από το HTTP [38], με σκοπό την παροχή εμπιστευτικότητας. Τέλος, η βασική σύνδεση στο διαδίκτυο είναι αρκετά φθηνή σε σχέση με άλλου είδους συνδέσεις.

Στον αντίποδα, η βασική σύνδεση δεν παρέχει εγγυημένη ποιότητα παρεχόμενων υπηρεσιών (Quality of Service - QoS) και αυτό έχει ως αποτέλεσμα τη δυσκολία επίτευξης των όσων έχουν συμφωνηθεί μεταξύ παρόχου του υπολογιστικού νέφους και πελάτη. Επίσης, έχει παρατηρηθεί ότι σε περιόδους μεγάλου φόρτου το δίκτυο αρχίζει να έχει καθυστερήσεις, οι οποίες, σε μερικές περιπτώσεις, είναι απογοητευτικές.

Υλοποιώντας αυτή τη μέθοδο ως τρόπο σύνδεσης με τον πάροχο του υπολογιστικού νέφους, η εταιρεία θα πρέπει να συνδεθεί με όποιο πάροχο διαδικτύου της προσφέρει καλύτερη ταχύτητα σε σχέση με τον

πάροχο υπολογιστικού νέφους. Καλό θα ήταν η εταιρεία να έχει παραπάνω από μία γραμμές σύνδεσης στο διαδίκτυο, από διαφορετικό πάροχο η καθεμία, ώστε αφενός να έχει μεγαλύτερη ταχύτητα, αφετέρου να έχει καλύτερη αξιοπιστία.

3.4.2. Γρήγορο διαδίκτυο

Ο πελάτης, κάνοντας χρήση των προηγμένων δυνατοτήτων μερικών εφαρμογών παροχής σύνδεσης στο διαδίκτυο μπορεί να ωφελήσει τόσο τον πάροχο υπολογιστικού νέφους, όσο και τον ίδιο. Οι προσφερόμενες υπηρεσίες του νέφους μπορεί να βελτιωθούν από 20% έως 50% σε σχέση με το βασικό διαδίκτυο.

Ο τερματισμός του πρωτοκόλλου SSL [37] και η αποδοτικότερη διαχείριση του πρωτοκόλλου TCP [36] αφαιρούν ένα σημαντικό κομμάτι επεξεργασίας από τους διακομιστές σύνδεσης στο διαδίκτυο. Επιπρόσθετα, η συμπίεση των δεδομένων στο δίκτυο και η μεταφορά περισσότερων δεδομένων από αυτά που ζητά ο χρήστης, όπως δηλαδή γίνεται και στην περίπτωση της λανθάνουσας μνήμης του υπολογιστή, έχει επιφέρει αποτελέσματα που αγγίζουν το 50% σε καλύτερη αποδοτικότητα στους τελικούς χρήστες.

Η συγκεκριμένη μέθοδος πρόσβασης είναι προσανατολισμένη περισσότερο προς τους παρόχους υπηρεσιών υπολογιστικού νέφους, αλλά στο τέλος επωφελούνται οι τελικοί χρήστες. Οι εταιρείες που ενδιαφέρονται για τη συγκεκριμένη μέθοδο πρόσβασης θα πρέπει να επικοινωνήσουν με τον πάροχο υπηρεσιών νέφους αρχικά και κατόπιν να ζητήσουν να συμπεριληφθεί στο συμβόλαιο που προσυπογράφουν η συγκεκριμένη μέθοδος ως τρόπος πρόσβασης του πελάτη στον πάροχο.

Από πλευράς παρόχου, η εφαρμογή της συγκεκριμένης μεθόδου απαιτεί την εγκατάσταση ενός επιπλέον ειδικού διακομιστή και από μεριάς πελάτη απαιτείται η εγκατάσταση ενός συγκεκριμένου λογισμικού στον υπολογιστή του, μέσω του οποίου θα συνδέεται στις υπηρεσίες του υπολογιστικού νέφους.

3.4.3. Βελτιστοποιημένη πρόσβαση μέσω διαδικτύου

Η βελτιστοποιημένη πρόσβαση μέσω του διαδικτύου επιτρέπει στους πελάτες να έχουν πρόσβαση στις υπηρεσίες υπολογιστικού νέφους μέσω του διαδικτύου, αλλά υπάρχουν εφαρμογές ενίσχυσης της ταχύτητας από μεριάς του παρόχου του υπολογιστικού νέφους. Οι εφαρμογές ενίσχυσης της ταχύτητας συνοψίζονται παρακάτω. Αρχικά, γίνεται επιλογή της βέλτιστης δυνατής διαδρομής για το πρωτόκολλο TCP [36]. Αυτό βοηθάει στην αποφυγή καθυστερήσεων που οφείλονται στους δρομολογητές. Επιπλέον, σταματάει η χρήση του πρωτοκόλλου SSL [37] και τα δεδομένα κρυπτογραφούνται με άλλους τρόπους, τους οποίους έχει προεπιλέξει ο πάροχος. Από την άλλη πλευρά όμως, η συγκεκριμένη μέθοδος απομονώνει τον πελάτη από τη δυνατότητα αλλαγής παρόχου και τίθεται θέμα ασφάλειας της όλης υποδομής, αν διαρρεύσει ο τρόπος κρυπτογράφησης των δεδομένων από τον πάροχο.

3.4.4. Χρήση VPN από τον πάροχο στον χρήστη

Η τέταρτη επιλογή πρόσβασης είναι η σύνδεση στην παρεχόμενη υπηρεσία υπολογιστικού νέφους απευθείας με τη χρήση ενός ιδιωτικού δικτύου ευρείας περιοχής, όπως για παράδειγμα το Virtual Private Network (VPN) [39]. Η συγκεκριμένη σύνδεση εξασφαλίζει εμπιστευτικότητα των δεδομένων μαζί με την εγγυημένη ταχύτητα πρόσβασης. Τα VPNs επίσης είναι σε θέση να έχουν εναλλασσόμενες ταχύτητες μεταφοράς δεδομένων, ώστε και να παρέχεται η απαιτούμενη ποιότητα των υπηρεσιών (Quality of Service – QoS) αλλά και να μην γίνεται άσκοπη χρήση των πόρων του δικτύου.

3.4.5. Πάροχοι υπηρεσιών νέφους

Οι πάροχοι υπηρεσιών υπολογιστικού νέφους που έχουν τις υπηρεσίες τους διανεμημένες εντός του υπολογιστικού νέφους, χρειάζονται μια σταθερή μέθοδο σύνδεσης. Τα ιδιωτικά δίκτυα μέσω VPN διασφαλίζουν το εύρος ταχύτητας και γενικότερα την απόδοση του

δικτύου. Επιπρόσθετα, ένα άλλο πλεονέκτημά τους είναι ότι παρέχουν κρυπτογράφηση και ισχυρή αυθεντικοποίηση.

Οι πάροχοι που επεκτείνουν το δίκτυο τους και τις υπηρεσίες τους ενδεχομένως να έρθουν αντιμέτωποι με μεγάλα κόστη στην τιμολόγηση του δικτύου που χρησιμοποιούν, καθώς από τη στιγμή που μεγαλώνουν οι απαιτήσεις του δικτύου τόσο σε ταχύτητα όσο και σε όγκο δεδομένων, οι χρεώσεις αυξάνονται. Η κίνηση αυτή προέρχεται τόσο από τους παρόχους προς τους πελάτες τους και το αντίστροφο, όσο και μεταξύ των παρόχων ή μεταξύ των διαφόρων υπηρεσιών τους. Οι μεγάλοι πάροχοι, όπως για παράδειγμα η Google [17] ή η Microsoft [21], μπορούν να παρακάμψουν αυτές τις χρεώσεις χτίζοντας το δικό τους δίκτυο, με αρκετά σημεία διανομής μέσω διαφόρων παρόχων υπηρεσιών διαδικτύου ανά τον κόσμο. Παρόλα αυτά, αρκετοί πάροχοι υπηρεσιών υπολογιστικού νέφους δεν είναι σε θέση να πράξουν κάτι αντίστοιχο.

Η απόδοση μπορεί να βελτιωθεί και τα κόστη προς τους παρόχους υπηρεσιών διαδικτύου να μειωθούν, αν οι πάροχοι υπηρεσιών υπολογιστικού νέφους κάνουν χρήση της ασύμμετρης βελτιστοποίησης. Για τη λειτουργία της συγκεκριμένης τεχνικής απαιτείται η εγκατάσταση μιας εφαρμογής τόσο από μέρος του παρόχου όσο και από μέρους του πελάτη. Με τη χρήση της συγκεκριμένης μεθόδου μπορεί να μειωθεί ο χρόνος απόκρισης έως και 70%, καθώς και το εύρος χρήσης του δικτύου έως και 80%.

3.4.6. Χρήστες υπηρεσιών νέφους

Οι μεγάλες εταιρείες και οι οργανισμοί μπορούν να κατασκευάσουν το δικό τους υπολογιστικό νέφος μέσω των κέντρων δεδομένων τους, των διακομιστών τους και της ήδη υπάρχουσας υποδομής στο δίκτυό τους, αν είναι αρκετά γρήγορη. Αυτό όμως προϋποθέτει ένα αρκετά μεγάλο κονδύλιο τόσο για την κατασκευή της όλης υποδομής όσο, κυρίως, για τη συντήρησή της. Οπότε, με την εμφάνιση του υπολογιστικού νέφους, οι εταιρείες και οι οργανισμοί μετέφεραν την υποδομή τους εκεί, έχοντας σημαντικά χρηματικά οφέλη.

Η πλειοψηφία των πελατών έχει πρόσβαση στις υπηρεσίες υπολογιστικού νέφους μέσω του διαδικτύου. Επίσης, κάποιοι άλλοι προτιμούν τις συνδέσεις VPN για τα πλεονεκτήματα που προσφέρουν. Γενικότερα, οι συνδέσεις VPN θεωρούνται ο καλύτερος δυνατός τρόπος επικοινωνίας σήμερα.

3.4.7. Εύρος ζώνης

Εύρος ζώνης (bandwidth) ονομάζεται η ταχύτητα λήψης και αποστολής δεδομένων μέσω μιας σύνδεση διαδικτύου [40]. Παρόλα αυτά, η αντικειμενική μέτρηση της ταχύτητας μπορεί να είναι δύσκολη και να μην είναι σωστή από τη στιγμή που ανά πάσα χρονική στιγμή η μικρότερη ταχύτητα που έχει κάποιος από τους δρομολογητές των πακέτων IP είναι και η ταχύτητα που έχει το δίκτυο.

Υπάρχουν τρεις παράγοντες, οι οποίοι είναι εκτός ελέγχου των πελατών, όταν χρειάζονται αρκετά μεγάλο εύρος ζώνης. Ο πρώτος είναι το εύρος ζώνης μεταξύ του παρόχου υπηρεσιών νέφους και του παρόχου υπηρεσιών διαδικτύου, ο δεύτερος είναι ο χρόνος που απαιτείται για να έρθουν τα δεδομένα από τον πάροχο στον πελάτη και ο τρίτος είναι ο χρόνος απόκρισης του νέφους.

Ένας άλλος παράγοντας που πρέπει να ληφθεί υπόψη σχετίζεται με το αν η σύνδεση θα είναι συμμετρική ή ασύμμετρη. Σε περίπτωση που η σύνδεση είναι συμμετρική, αυτό σημαίνει ότι ο πελάτης λαμβάνει και στέλνει δεδομένα με την ίδια ταχύτητα. Αν η σύνδεση είναι ασύμμετρη, σημαίνει ότι η ταχύτητα λήψης είναι διαφορετική από την ταχύτητα αποστολής δεδομένων και συνήθως μεγαλύτερη. Για παράδειγμα, οι συνδέσεις ADSL (Asymmetric Digital Subscriber Line) στέλνουν και λαμβάνουν δεδομένα με διαφορετικές ταχύτητες. Ανάλογα με το είδος της σύνδεσης (2, 4, 8, 24 Mbps) έχουμε εντελώς διαφορετικές ταχύτητες στη λήψη και αποστολή δεδομένων και συνήθως η ταχύτητα αποστολής είναι ένα κλάσμα της ταχύτητας λήψης. Σε περίπτωση που μια εταιρεία θέλει να συνδεθεί στο υπολογιστικό νέφος και να μεταφέρει εκεί όλη την υποδομή της, μια απλή σύνδεση ADSL δεν αρκεί, οπότε θα πρέπει να αποκτήσει ένα άλλος είδος σύνδεσης και κατά προτίμηση συμμετρική.

Επίσης, θα πρέπει να ληφθούν υπόψη και οι αλλαγές στο διαδίκτυο από τη μια στιγμή στην άλλη, οι οποίες είναι αδύνατο να προβλεφθούν. Τα δεδομένα μετακινούνται μεταξύ διαφόρων δρομολογητών και δικτύων, οπότε η τελική ταχύτητα ποικίλλει από στιγμή σε στιγμή. Αυτό μπορεί μεν να μην είναι αισθητό στον απλό χρήστη, παρόλα αυτά παρουσιάζει διακυμάνσεις. Οπότε, ακόμα και αν ο χρήστης – πελάτης έχει πληρώσει για γραμμή τύπου Τ1, μπορεί να δει μεγάλες διαφορές στην τελική του ταχύτητα. Γενικότερα, κανόνας είναι ότι, αν ο χρήστης επιτυγχάνει το 85% της ονομαστικής ταχύτητας, τότε έχει αποτελεσματικό πάροχο.

Το πόση ταχύτητα χρειάζεται κάποιος που θέλει να έχει πρόσβαση σε υπηρεσίες του υπολογιστικού νέφους, είναι περίπλοκη ερώτηση. Αρχικά, θα πρέπει να δει τον όγκο των δεδομένων που ανεβάζει και κατεβάζει από το υπολογιστικό νέφος σε καθημερινή, σε εβδομαδιαία και σε μηνιαία βάση. Εκτός από τον μέσο όσο που θα προκύψει από τις μετρήσεις, θα βρεθεί τόσο η ελάχιστη όσο και η μέγιστη τιμή του ποσού των δεδομένων, οπότε ανάλογα θα επιλέξει το είδος της σύνδεσης που χρειάζεται. Επίσης, θα πρέπει να καταστεί σαφές ότι όσο αυξάνονται οι απαιτήσεις του από το υπολογιστικό νέφος σχετικά με τα δεδομένα, τόσο θα αυξάνεται και ο φόρτος του δικτύου, οπότε επιβάλλεται η βελτίωση της γραμμής σύνδεσης.

Τέλος, απαραίτητο γεγονός είναι η ασφάλιση του εύρους ζώνης στο συμβόλαιο με τον πάροχο υπηρεσιών υπολογιστικού νέφους. Αυτό εξασφαλίζει όχι μόνο ότι ο πελάτης έχει την ταχύτητα που χρειάζεται αλλά, επίσης, αν ο πάροχος υπηρεσιών διαδικτύου αποτύχει να εξασφαλίσει τη συγκεκριμένη ταχύτητα, ίσως υπάρξει κάποιο είδος αποκατάστασης και βελτιωθεί το είδος της γραμμής με ανώδυνο τρόπο για τον πελάτη.

3.4.8. Εφεδρικά συστήματα

Κατά τη διαμόρφωση των υποδομών του υπολογιστικού νέφους, ο πελάτης θα πρέπει να εξετάσει το ζήτημα της αξιοπιστίας και του χρόνου

απόκρισης και να ζητήσει από τον πάροχό του να ρυθμίσει την υποδομή ώστε να παρέχει αντίγραφα ασφαλείας και να έχει εφεδρικά συστήματα.

Στο τοπικό του δίκτυο, η έννοια των εφεδρικών συστημάτων σημαίνει ο πελάτης να έχει άλλον ένα ή δύο εφεδρικούς διακομιστές σε περίπτωση που προκύψει κάποιο πρόβλημα στον λειτουργικό διακομιστή. Στη σημερινή εποχή, τα εφεδρικά συστήματα είναι μια πολύ εύκολη υπόθεση λόγω των υπηρεσιών που παρέχει το υπολογιστικό νέφος, κατά τις οποίες μπορεί και κλωνοποιεί ένα ολόκληρο εικονικό μηχάνημα μέσα σε μερικά δευτερόλεπτα.

3.5. Υπηρεσίες

Υπάρχουν διαφορετικές υπηρεσίες που πρέπει να τρέχει ο πελάτης, οι οποίες εξαρτώνται τόσο από τον πάροχο όσο και από το τι ζητά η εταιρεία – πελάτης. Επίσης, αυτές οι υπηρεσίες θα επηρεάσουν τον τρόπο ανάπτυξης της υποδομής του υπολογιστικού νέφους στο πελάτη.

3.5.1. Ταυτότητα

Ανεξάρτητα από το αν μια εφαρμογή τρέχει εντός της εταιρείας ή στο υπολογιστικό νέφος, θα πρέπει αυτή να γνωρίζει για τους χρήστες που την χρησιμοποιούν ανά πάσα στιγμή. Για να επιτευχθεί αυτό, η εφαρμογή συνήθως ζητά μια ψηφιακή ταυτότητα, ένα σύνολο από bytes δηλαδή, από τον χρήστη. Βασισμένη σε αυτή την πληροφορία, η εφαρμογή είναι σε θέση να καθορίσει ποιος είναι ο χρήστης και ποια δικαιώματα έχει πάνω στην εφαρμογή.

Για την παροχή των παραπάνω πληροφοριών, οι εφαρμογές που βρίσκονται εντός της εταιρείας βασίζονται σε υπηρεσίες, όπως το AD (Active Directory) [41] των Windows [42]. Σε επίπεδο υπολογιστικού νέφους, ωστόσο, θα πρέπει να θεσπιστεί τρόπος υπηρεσιών αναγνώρισης ταυτοτήτων των χρηστών. Για παράδειγμα, αν ένας χρήστης εισέλθει στις υπηρεσίες νέφους της Amazon [43], θα πρέπει να

δώσει ως διαπιστευτήρια τα στοιχεία εισόδου, όνομα χρήστη και κωδικό πρόσβασης, που έχει λάβει από την Amazon. Αντίστοιχα για την Google ή για την Microsoft θα πρέπει να δώσει άλλα διαπιστευτήρια.

Οι υπηρεσίες ταυτότητας δεν θα πρέπει να είναι ιδιόκτητες. Το πρότυπο OpenID [44], είναι ένα ανοικτό, μη-κεντροποιημένο πρότυπο, το οποίο επιτρέπει στους χρήστες να εισέρχονται σε πολλές και διαφορετικές υπηρεσίες με τη χρήση της ίδιας ψηφιακής ταυτότητας. Το πρότυπο αυτό λειτουργεί ως μια φόρμα στην οποία ο χρήστης εισάγει το όνομά του και τον κωδικό του. Με αυτό τον τρόπο αυθεντικοποιεί τον εαυτό του για κάποια υπηρεσία στην οποία κατευθύνεται αμέσως μετά. Πολλοί από τους πάροχους υπολογιστικού νέφους υποστηρίζουν το πρότυπο OpenID και μεταξύ αυτών οι Google, IBM, Microsoft και Yahoo!.

3.5.2. Επικοινωνία εφαρμογών

Στις μέρες μας, η επικοινωνία μεταξύ των εφαρμογών είναι ένα καθημερινό φαινόμενο. Οι πάροχοι υπηρεσιών υπολογιστικού νέφους έχουν όλων των ειδών τις υποδομές για να υποστηρίξουν αυτή την επικοινωνία. Οι υποδομές αυτές ποικίλλουν από τεχνολογίες για απλή ανταλλαγή μηνυμάτων μέσω ουράς μέχρι περίπλοκους διακομιστές προώθησης μηνυμάτων.

Για παράδειγμα, η Amazon έχει θεσπίσει την τεχνολογία SQS [45] (Simple Queue Service), η οποία παρέχει στις εφαρμογές την δυνατότητα να επικοινωνούν μεταξύ τους μέσω εικονικών ουρών που βρίσκονται αποθηκευμένες στο νέφος της. Μέσω της συγκεκριμένης τεχνολογίας, καθεμία από τις εφαρμογές έχει πρόσβαση σε όσες ουρές έχουν μηνύματα σχετικά με εκείνη, προστατεύοντας έτσι την ιδιωτικότητα και την ασφάλεια των δεδομένων, καθιστώντας και τις εφαρμογές πιο γρήγορες.

3.6. Πρόσβαση στο υπολογιστικό νέφος

Ο τρόπος αλληλεπίδρασης του χρήστη με το υπολογιστικό νέφος είναι συνάρτηση πολλών παραγόντων μέσα στους οποίους συγκαταλέγεται και ο πάροχος που έχει επιλέξει να συνεργάζεται. Υπάρχει πληθώρα από εργαλεία ανάπτυξης κώδικα, τα οποία επιτρέπουν στους χρήστες να χτίζουν τις δικές τους εφαρμογές, καθώς και πολλές επιλογές από τα προγράμματα περιήγησης που επιτρέπουν την πρόσβαση σε αυτές τις εφαρμογές.

Στις επόμενες παραγράφους θα δούμε περιληπτικά τα εργαλεία που χρησιμοποιούνται για να συνδεθεί κάποιος χρήστης στο υπολογιστικό νέφος.

3.6.1. Πλατφόρμες

Πλατφόρμα ονομάζεται ο τρόπος με τον οποίο διανέμονται στον χρήστη – πελάτη οι υπηρεσίες υπολογιστικού νέφους [06]. Σε αυτή την ενότητα θα αναφερθούμε στον τρόπο με τον οποίο δημιουργείται το υπολογιστικό νέφος και διανέμεται στους χρήστες του.

Ένα πλαίσιο εφαρμογών διαδικτύου (web application framework) χρησιμοποιείται για να υποστηρίξει την ανάπτυξη δυναμικών ιστοσελίδων, διαδικτυακών εφαρμογών και υπηρεσιών διαδικτύου [46]. Το βασικό στοιχείο ενός τέτοιου πλαισίου είναι η μείωση της επιβάρυνσης στην ανάπτυξη μιας εφαρμογής η οποία επιτυγχάνεται μέσω συγκεκριμένων διαδικασιών. Για παράδειγμα, ένα πλαίσιο παρέχει ένα σύνολο από βιβλιοθήκες, οι οποίες επειδή είναι ήδη γραμμένες, δίνουν το πλεονέκτημα στον προγραμματιστή να μην γράψει από την αρχή τον βασικό κώδικα κάθε φορά που δημιουργεί μια διαδικτυακή εφαρμογή.

Στα πρώιμα στάδια του διαδικτύου, ο μοναδικός τρόπος συγγραφής διαδικτυακών εφαρμογών ή αλλιώς ιστοσελίδων ήταν η γλώσσα HTML (Hypertext Markup Language) [47]. Η HTML δεν είχε τη δυνατότητα ενσωμάτωσης δυναμικών εφαρμογών, οπότε με την πάροδο

του χρόνου θεσπίστηκαν διάφορα επιπλέον πρότυπα με βάση τα οποία επεκτάθηκε την HTML.

Το AJAX (Asynchronous JavaScript & XML) [48] είναι ένα σύνολο από τεχνικές ανάπτυξης για τη δημιουργία διαδραστικών διαδικτυακών εφαρμογών. Με τη χρήση του AJAX οι εφαρμογές μπορούν να ανακτούν δεδομένα από τους διακομιστές με ασύγχρονο τρόπο. Λόγω του ότι όλη η διαδικασία συμβαίνει στο παρασκήνιο, δεν επηρεάζει τη μορφή της ιστοσελίδας.

Ένα επίσης δημοφιλές πλαίσιο ανάπτυξης διαδικτυακών εφαρμογών είναι το Python Django [35]. Το Django είναι γραμμένο στη γλώσσα προγραμματισμού Python. Αρχικά, είχε κατασκευαστεί για να διαχειρίζεται ειδησεογραφικές ιστοσελίδες, αλλά από τον Ιούνιο του 2005 και μετά διατέθηκε στο σύνολο των προγραμματιστών. Τον Ιούνιο του 2008 ανακοινώθηκε το ίδρυμα Django Software Foundation [49], το οποίο πήρε στην κατοχή του το Django.

Από τη στιγμή που θα κατασκευαστεί η εφαρμογή και τα δεδομένα της, χρειάζεται μια υπηρεσία, η οποία θα φιλοξενεί τόσο την ίδια την εφαρμογή, όσο και τα δεδομένα. Αυτή ακριβώς είναι η ανάγκη που καλύπτεται από το υπολογιστικό νέφος, με το οποίο δίνεται η δυνατότητα στους χρήστες – προγραμματιστές να ανεβάζουν τις εφαρμογές τους και τα δεδομένα τους. Από τους πιο γνωστούς παρόχους υπηρεσιών υπολογιστικού νέφους είναι το EC2 [39] της Amazon και το Microsoft Azure [51, 52].

Από την άλλη πλευρά υπάρχει ένα σύνολο παρόχων υπηρεσιών υπολογιστικού νέφους, οι οποίοι δεν φιλοξενούν ανοικτά πρότυπα, όπως το AJAX ή το Django, αλλά παρέχουν τις δικές τους μεθόδους για σύνδεση και για δημιουργία εφαρμογών στο υπολογιστικό νέφος. Η Microsoft και η Force.com είναι δύο χαρακτηριστικά παραδείγματα εταιρειών, οι οποίες έχουν σχεδιάσει τις δικές τους υποδομές για εφαρμογές στο υπολογιστικό νέφος.

Σε ό,τι αφορά την Microsoft υπάρχει η λύση που ονομάζεται Azure [40], όπως αναφέρθηκε και ανωτέρω. Το Azure είναι μια πλατφόρμα, η οποία επεκτείνει την υλοποίηση του υπολογιστικού νέφους σε ένα

κέντρο δεδομένων. Επιπρόσθετα, μπορεί να διανείμει το περιεχόμενο σε υπολογιστές, στο δίκτυο και στα έξυπνα κινητά τηλέφωνα. Η συγκεκριμένη πλατφόρμα συνδυάζει δυνατότητες αποθήκευσης, επεξεργασίας και υποδομές δικτύου στο υπολογιστικό νέφος της. Οι διακομιστές που παρέχουν την υποδομή αυτή είναι οι διακομιστές της Microsoft ανά την υφήλιο.

Η Force.com παρέχει μια δική της πλατφόρμα για δημιουργία και ανάπτυξη εφαρμογών [53]. Προσφέρει απλότητα σε σχέση με άλλες πλατφόρμες ανάπτυξης και συνδυάζεται με αρκετά εργαλεία, τα οποία δίνουν στον προγραμματιστή τη δυνατότητα να αναπτύξει ταχύτατα τον κώδικά του.

3.6.2. Διαδικτυακές εφαρμογές

Αν κάποιος χρήστης ή εταιρεία προτίθεται να εισέλθει στο υπολογιστικό νέφος, υπάρχει μια πληθώρα από εφαρμογές σε αυτό. Επιπλέον, ο πάροχος υπηρεσιών υπολογιστικού νέφους καλό θα ήταν να ενημερώσει κατάλληλα τους χρήστες του για τις εφαρμογές που του παρέχει και ανάλογα ο χρήστης να μπορεί να επιλέξει. Στη τρέχουσα παράγραφο θα αναφερθούμε εν συντομία στις επιλογές που έχει κάποιος χρήστης σχετικά με τις ήδη υπάρχουσες εφαρμογές του νέφους.

Ο χρήστης έχει πολλαπλές επιλογές, όταν πρόκειται για εύρεση διαδικτυακών εφαρμογών στο υπολογιστικό νέφος. Ο πάροχος, επίσης, διαθέτει συνήθως στο χρήστη τις πιο διαδεδομένες και σταθερές εφαρμογές. Για παράδειγμα, η Microsoft ή η Google προσφέρουν ένα σύνολο εφαρμογών, οι οποίες είναι προσανατολισμένες προς την παραγωγικότητα του χρήστη.

Επιπλέον, θεωρείται δεδομένο ότι κάποιος άλλος έχει δημιουργήσει στο υπολογιστικό νέφος την εφαρμογή που αναζητά ο χρήστης. Έτσι, αρκετοί από τους παρόχους υπολογιστικού νέφους παρέχουν την δυνατότητα στους χρήστες να χρησιμοποιούν εφαρμογές άλλων χρηστών, σαφώς με την συγκατάθεσή τους.

Τέλος, στην περίπτωση που ο χρήστης δεν καταφέρει να βρει την εφαρμογή που χρειάζεται, μπορεί να απευθυνθεί στον πάροχό του. Συνήθως οι πάροχοι έχουν επιπλέον εφαρμογές εκτός δικτύου, οι οποίες δεν είναι διαδεδομένες, ή μπορούν να κατευθύνουν το χρήστη στο πού θα βρει ακριβώς αυτό που έχει ανάγκη.

Συνοψίζοντας τα προηγούμενα μπορούμε να πούμε ότι όλοι οι πάροχοι προσφέρουν στους πελάτες τους εφαρμογές γραφείου, εφαρμογές επεξεργασίας εικόνας και βίντεο, υπηρεσίες ηλεκτρονικού ταχυδρομείου και ηλεκτρονικές ατζέντες.

3.6.3. Διεπαφές προγραμματισμού εφαρμογών

Κατά τη διάρκεια του προγραμματισμού αρκετοί χρήστες κάνουν χρήση των διεπαφών προγραμματισμού εφαρμογών (API – Application Programming Interface). Υπάρχουν πολλά και διαφορετικά APIs και η χρήση οποιουδήποτε από αυτά εξαρτάται από τις γνώσεις του προγραμματιστή και τις ανάγκες της εταιρείας. Επίσης, διαφορετικοί πάροχοι υπηρεσιών νέφους προσφέρουν και διαφορετικά APIs.

API είναι το σύνολο από εντολές προγραμματισμού και πρότυπα, τα οποία παρέχουν πρόσβαση σε ένα διαδικτυακό πρόγραμμα [54]. Εταιρείες λογισμικού διαθέτουν τα APIs τους ελεύθερα, έτσι ώστε άλλοι προγραμματιστές να σχεδιάζουν προϊόντα που λειτουργούν σύμφωνα με τα APIs τους. Για παράδειγμα, η Amazon έχει ελεύθερα τα δικά της APIs, ώστε οι προγραμματιστές να μπορούν να έχουν εύκολα πρόσβαση στα δεδομένα που είναι αποθηκευμένα στο υπολογιστικό της νέφος.

Επίσης, τα APIs προσφέρουν τη δυνατότητα της επικοινωνίας μεταξύ των εφαρμογών [54]. Παρόλα αυτά, δεν θα πρέπει να μπερδεύονται με τις διεπαφές των χρηστών. Με τη χρήση των APIs, οι εφαρμογές μπορούν να επικοινωνούν μεταξύ τους χωρίς τη διαμεσολάβηση των χρηστών. Για παράδειγμα, όταν κάποιος προβαίνει σε αγορά κάποιου προϊόντος από την Amazon και εισάγει τα δεδομένα της πιστωτικής του κάρτας, η Amazon χρησιμοποιεί ένα API για να στείλει τα δεδομένα της κάρτας σε μια απομακρυσμένη εφαρμογή, η οποία

πιστοποιεί την ορθότητα εισαγωγής των δεδομένων. Από τη μεριά του χρήστη, το μόνο που βλέπει στην οθόνη του είναι το μέρος στο οποίο εισήγαγε τα δεδομένα, αγνοώντας ότι στο παρασκήνιο το API παίρνει τα δεδομένα του και τα στέλνει στη συγκεκριμένη εφαρμογή.

Τα APIs μπορεί να παρομοιαστούν με τις εφαρμογές-ως-υπηρεσία, επειδή οι προγραμματιστές δεν χρειάζεται να ξεκινήσουν από το μηδέν μια εφαρμογή, αλλά επιλέγουν από ήδη έτοιμες εφαρμογές που επιτελούν διάφορες εργασίες και τις συνδέουν κατάλληλα για να κάνουν την επιπρόσθετη εργασία στην νέα εφαρμογή που κατασκευάζουν.

Με τη βοήθεια των APIs, οι υπηρεσίες διαδικτύου διαχειρίζονται όλες οι κλήσεις από και προς τις εφαρμογές. Οι υπηρεσίες διαδικτύου είναι μια συλλογή από πρότυπα συμπεριλαμβανομένης της XML (Extensible Markup Language) [55], τη γλώσσα προγραμματισμού που επιτρέπει την επικοινωνία των εφαρμογών μέσω του διαδικτύου. Η XML είναι μια γλώσσα προγραμματισμού γενικού σκοπού, η οποία περιγράφει δομημένα δεδομένα με τέτοιο τρόπο, ώστε τόσο ο άνθρωπος όσο και οι εφαρμογές να μπορούν να γράψουν και να διαβάσουν.

Το API είναι ένα κομμάτι κώδικα γραμμένο ως XML μήνυμα. Οι προγραμματιστές μπορούν να χρησιμοποιούν ήδη υπάρχοντα APIs ή να προγραμματίζουν νέα, ανάλογα με τις εφαρμογές που θέλουν να κατασκευάσουν. Για παράδειγμα, αν κάποιος θέλει να κάνει μια εφαρμογή ηλεκτρονικού ταχυδρομείου στο υπολογιστικό νέφος, μπορεί να χρησιμοποιήσει ένα API που αυτόματα θα στέλνει τα ηλεκτρονικά μηνύματα από τον αποστολέα στον παραλήπτη ή να τα αποθηκεύει σε ένα εφεδρικό αρχείο στο υπολογιστικό νέφος.

Αν και υπάρχουν πολλών ειδών APIs, παρόλα αυτά κρίνεται σκόπιμο να μην αναφερθούμε περαιτέρω σε αυτά. Για περισσότερα σχετικά με τα APIs ο αναγνώστης μπορεί να ανατρέξει στο [54].

3.6.4. Προγράμματα περιήγησης

Το πιο απλό και διαδεδομένο εργαλείο σύνδεσης σε ένα υπολογιστικό νέφος είναι το πρόγραμμα περιήγησης (web browser). Ένα

πρόγραμμα περιήγησης είναι λογισμικό που επιτρέπει στον χρήστη του να προβάλλει και να αλληλεπιδρά με κείμενα, εικόνες, βίντεο, μουσική, παιχνίδια και άλλες πληροφορίες, συνήθως αναρτημένες σε μια ιστοσελίδα [56], της οποίας ο κώδικας είναι γραμμένος σε HTML [47].

Σήμερα υπάρχουν αρκετά προγράμματα περιήγησης, τα οποία σε γενικές γραμμές είναι ίδια. Τα πιο γνωστά από αυτά είναι ο Microsoft Edge [57], ο Google Chrome [58], ο Mozilla Firefox [59] και ο Safari [60]. Η επιλογή κάποιου συγκεκριμένου προγράμματος έχει να κάνει με τις προτιμήσεις του χρήστη, καθώς και τα επιπλέον χαρακτηριστικά που προσφέρει μέσω πρόσθετων το καθένα από τα προγράμματα περιήγησης.

3.7. Πρότυπα

Τα πρότυπα είναι ο βασικός παράγοντας που λειτουργεί το WWW (World Wide Web) [56] και κατ' επέκταση είναι επίσης πολύ σημαντικά για το υπολογιστικό νέφος. Τα πρότυπα είναι ο λόγος που καθίσταται δυνατή η σύνδεση στο υπολογιστικό νέφος και δίνουν τη δυνατότητα για την ανάπτυξη και την παροχή υπηρεσιών.

Σε αυτή την ενότητα θα εξετάσουμε περιληπτικά όλα τα διαδεδομένα πρότυπα, τα οποία καθιστούν δυνατή την ύπαρξη του υπολογιστικού νέφους, και επίσης τα είδη των προτύπων που χρησιμοποιούνται για την ανάπτυξη εφαρμογών στο νέφος.

3.7.1. Εφαρμογές

Μια εφαρμογή υπολογιστικού νέφους είναι μια αρχιτεκτονική λογισμικού, την οποία χρησιμοποιεί το υπολογιστικό νέφος, για να εξαλείψει την ανάγκη εγκατάστασης και λειτουργίας λογισμικού στον υπολογιστή του πελάτη. Με αυτό τον τρόπο μπορούν να λειτουργήσουν πολλές εφαρμογές, αν και επιβάλλεται να υπάρχει ένας πρότυπος τρόπος σύνδεσης μεταξύ του πελάτη και του υπολογιστικού νέφους. Στη

συνέχεια, θα αναφερθούμε στα πρωτόκολλα που χρησιμοποιούνται για τη διαχείριση της σύνδεσης μεταξύ των συμμετεχόντων.

Όπως είναι γνωστό, οι υπολογιστές χρειάζονται ένα κοινό τρόπο για να συνομιλούν. Αυτό θα μπορούσαμε να το παρομοιάσουμε με δύο άτομα που μιλούν στο τηλέφωνο και ο ένας μιλάει μόνο αγγλικά ενώ ο δεύτερος μόνο ελληνικά. Δεν υπάρχει τρόπος να επιτευχθεί η επικοινωνία μεταξύ τους. Ο ένας μπορεί να υποθέτει κάποια από τα λεγόμενα του άλλου, αυτό όμως σε καμία περίπτωση δεν θεωρείται επικοινωνία. Σε ό,τι αφορά τους υπολογιστές η κατάσταση είναι πιο δύσκολη, γιατί δεν μπορούν να μαντέψουν ούτε μια λέξη, οπότε δεν υπάρχει επικοινωνία.

Για να δει μια ιστοσελίδα από τον πάροχο υπηρεσιών υπολογιστικού νέφους, ο χρήστης χρησιμοποιεί το πρωτόκολλο HTTP (Hypertext Transfer Protocol) [38], ως μηχανισμό για τη μεταφορά δεδομένων μεταξύ του παρόχου και του ιδίου.

Το πρωτόκολλο HTTP είναι ένα πρωτόκολλο επικοινωνίας που θεωρεί την κάθε αίτηση σαν μοναδική και δεν ενδιαφέρεται για προηγούμενες ή επόμενες αιτήσεις (stateless protocol), οπότε έχει ως πλεονέκτημα ότι αφενός δεν απαιτεί τη διατήρηση της συνόδου από τον διακομιστή και αφετέρου δε χρειάζεται πληροφορίες σχετικές με τις αιτήσεις του χρήστη. Παρόλα αυτά, σε περιπτώσεις που επιβάλλεται η συνεχής σύνδεση, οι προγραμματιστές επιφορτίζονται με τη θέσπιση μεθόδων για να την διατηρήσουν ενεργή. Για παράδειγμα, όταν ένας διακομιστής θέλει να μεταβάλει το περιεχόμενο μιας ιστοσελίδας για ένα συγκεκριμένο χρήστη, η διαδικτυακή εφαρμογή θα πρέπει να γραφεί με τέτοιο τρόπο ώστε να καταγράφει την πρόοδο του χρήστη από σελίδα σε σελίδα και η πιο κοινή μέθοδος για να γίνει κάτι τέτοιο είναι η αποστολή και η λήψη cookies [61]. Το πρωτόκολλο HTTP είναι η γλώσσα που χρησιμοποιεί το υπολογιστικό νέφος και οι υπολογιστές για να επικοινωνούν. Η συγκεκριμένη γλώσσα δεν είναι δύσκολη τόσο στην κατανόηση όσο και στη συγγραφή της από τους προγραμματιστές.

Ο επόμενος ακρογωνιαίος λίθος στο οικοδόμημα του υπολογιστικού νέφους είναι το πρωτόκολλο XMPP (Extensible Messaging

& Presence Protocol) [62]. Το βασικό πρόβλημα του υπολογιστικού νέφους είναι ότι οι υπηρεσίες μέσω του HTTP εξασφαλίζουν μόνο τη μονόδρομη μεταφορά δεδομένων. Αυτό συνεπάγεται ότι το υπολογιστικό νέφος δεν μπορεί να λειτουργήσει αποδοτικά και σε πραγματικό χρόνο. Αντίθετα, το πρωτόκολλο XMPP επιτρέπει την αμφίδρομη επικοινωνία και εξαλείφει το προηγούμενο πρόβλημα. Το XMPP υπογράφηκε από κοινού από τις Google [17], Apple [63], AOL [64], IBM [18] και LiveJournal [65]. Παρόλο όμως που έχει υπογραφεί από κολοσσούς του υπολογιστικού νέφους δεν χρησιμοποιείται ευρέως και από άλλους παρόχους. Ο κύριος λόγος για αυτό είναι ότι μέσω του XMPP μπορεί να δημιουργηθεί πρόβλημα, το γνωστό polling [62]. Οι άλλοι πάροχοι υπολογιστικού νέφους αναλογιζόμενοι το πρόβλημα το οποίο ενδεχομένως θα προκληθεί έχουν προχωρήσει ήδη σε άλλου είδους υλοποιήσεις.

Η ασφάλιση της συνόδου μεταξύ χρήστη και υπολογιστικού νέφους είναι εξαιρετικά σημαντική, από τη στιγμή που η ασφάλεια γενικότερα είναι ένας από τους βασικότερους λόγους, για τους οποίους οι εταιρείες δεν έχουν μεταφέρει την υποδομή τους στο υπολογιστικό νέφος. Η ασφάλιση των συνόδων μπορεί να επιτευχθεί μέσω της κρυπτογράφησης και της αυθεντικοποίησης. Τα πιο διαδεδομένα μέσα διαδικτυακής κρυπτογράφησης υπάρχουν ως πρότυπα σε όλα τα προγράμματα περιήγησης. Το δεύτερο θέμα είναι η αυθεντικοποίηση, η οποία παρέχει πολλές επιλογές για τους χρήστες. Τα πιο ευρέως διαδεδομένα πρωτόκολλα αυθεντικοποίησης και κρυπτογράφησης στο υπολογιστικό νέφος είναι τα OpenID [44], SSL [37] (Secure Sockets Layer) και Transport Layer Security (TLS) [66].

Όταν κάποιος θέλει να αγοράσει κάτι από το διαδίκτυο και χρησιμοποιεί την πιστωτική του κάρτα, όλες οι σχετικές με αυτή πληροφορίες κρυπτογραφούνται με τη χρήση του πρωτοκόλλου TLS, του οποίου η τελευταία έκδοση είναι η 1.3. Το TLS είναι πρότυπο για την εγκαθίδρυση μιας ασφαλούς σύνδεσης μεταξύ ενός διακομιστή και ενός προγράμματος περιήγησης. Μέσω του TLS διαβεβαιώνεται ότι τα δεδομένα που ανταλλάσσουν ο διακομιστής και το πρόγραμμα περιήγησης είναι ασφαλή. Για τη δημιουργία μιας σύνδεσης TLS σε ένα

διακομιστή απαιτείται ένα πιστοποιητικό SSL/TLS. Όταν ο πάροχος υπηρεσιών νέφους ξεκινήσει μια σύνοδο TLS, θα ζητηθεί από τον χρήστη να ολοκληρώσει μια σειρά από ερωτήματα σχετικά με την ταυτότητα της εταιρείας και την ιστοσελίδα του. Έπειτα, οι υπολογιστές του παρόχου παράγουν δύο κρυπτογραφικά κλειδιά, ένα δημόσιο και ένα ιδιωτικό. Το δημόσιο κλειδί δεν είναι μυστικό και τοποθετείται σε ένα αρχείο που ονομάζεται CSR (Certificate Signing Request). Αυτό το αρχείο, στο οποίο εμπεριέχονται όλες οι λεπτομέρειες του χρήστη, υποβάλλεται στον πάροχο. Κατά τη διάρκεια της διαδικασίας πιστοποίησης του TLS, μια έμπιστη οντότητα θα επικυρώσει τα στοιχεία του χρήστη και, αν είναι σωστά, θα εκδώσει ένα πιστοποιητικό SSL/TLS, το οποίο θα περιέχει λεπτομέρειες σχετικά με τον χρήστη και θα του επιτρέπει να κάνει χρήση του TLS. Κατόπιν, ο πάροχος υπηρεσιών υπολογιστικού νέφους θα ταιριάζει το πιστοποιητικό που εκδόθηκε για τον χρήστη με το ιδιωτικό του κλειδί και το πρόγραμμα περιήγησης θα μπορεί να εγκαθιδρύσει μία κρυπτογραφημένη σύνδεση μεταξύ του υπολογιστή του χρήστη και του παρόχου του υπολογιστικού νέφους. Η όλη διαδικασία είναι αρκετά βελτιστοποιημένη και λειτουργεί στο παρασκήνιο. Η μόνη διαφορά που είναι πιθανό να αντιληφθεί ο χρήστης είναι ότι η σελίδα καθυστερεί λίγο περισσότερο από το κανονικό για να φορτώσει, λόγω της υλοποίησης του πρωτοκόλλου. Ένα τυπικό πιστοποιητικό SSL θα περιέχει το όνομα του παρόχου του υπολογιστικού νέφους, το όνομα της εταιρείας, την πλήρη διεύθυνσή της και τη χώρα που ανήκει. Επίσης, θα περιέχει την ημερομηνία λήξης του πιστοποιητικού, καθώς και λεπτομέρειες σχετικά με την έμπιστη οντότητα που το εξέδωσε. Όταν το πρόγραμμα περιήγησης θα προσπαθήσει να συνδεθεί με ασφαλή τρόπο στο υπολογιστικό νέφος, θα λάβει το πιστοποιητικό SSL/TLS, θα ελέγξει αν ισχύει ακόμα και αν η οντότητα που το εξέδωσε είναι έμπιστη. Όταν ισχύουν όλα τα προηγούμενα, προβαίνει σε ασφαλή σύνδεση ενώ σε αντίθετη περίπτωση ενημερώνεται ο χρήστης ότι δεν υπάρχει ασφαλής σύνδεση μέσω TLS.

Όπως αναφέρθηκε και σε προηγούμενη παράγραφο, για την επίλυση του προβλήματος ενός μοναδικού ονόματος και κωδικού ανά χρήστη μεταξύ των πολλών εφαρμογών, έχει θεσπιστεί το πρότυπο OpenID [44]. Μέσω του συγκεκριμένου προτύπου, ο χρήστης έχει τη

δυνατότητα να επιλέξει τον πάροχο OpenID που επιθυμεί και εμπιστεύεται. Επιπλέον, το συγκεκριμένο πρότυπο είναι δωρεάν και παρέχει πολύ καλή και εύκολη διαχείριση των λογαριασμών των χρηστών. Το OpenID υιοθετήθηκε από μεγάλα ονόματα στον χώρο του υπολογιστικού νέφους, όπως για παράδειγμα η AOL [64], η Microsoft [21] και η Oracle Solaris [67]. Είναι προϊόν ανοικτού κώδικα και κατάφερε να επιλύσει προβλήματα, τα οποία με την υπάρχουσα υποδομή ήταν αδύνατο να επιλυθούν, αφού μπορεί να ταυτοποιεί χρήστες σε υπηρεσίες με την ίδια τεχνολογία που ταυτοποιούνται και οι ιστοσελίδες σε ένα διακομιστή. Τέλος, αξίζει να σημειωθεί ότι οποιοσδήποτε μπορεί να είναι χρήστης ή πάροχος OpenID εντελώς δωρεάν.

3.7.2. Χρήστες

Όταν κάποιοι χρήστες συνδέονται στο υπολογιστικό νέφος, χρειάζεται να εκτελούν συγκεκριμένα προγράμματα στους υπολογιστές τους. Κατά κύριο λόγο θα είναι ένα πρόγραμμα περιήγησης ή μια παρόμοια εφαρμογή που επιτρέπει τη σύνδεση του χρήστη με το υπολογιστικό νέφος. Τα προγράμματα περιήγησης χρησιμοποιούν αρκετούς τρόπους για να αποθηκεύουν και να εμφανίζουν τα δεδομένα, με γνωστότερο όλων τη χρήση της γλώσσας HTML [47].

Από τη στιγμή που το μεγαλύτερο μέρος του υπολογιστικού νέφους είναι βασισμένο στη σύνδεση μέσω του www, θα αναφέρουμε μερικά κύρια στοιχεία του επικοινωνιακού φορέα, δηλαδή της γλώσσας HTML. Η γλώσσα HTML (Hypertext Markup Language) είναι υπό συνεχή αναθεώρηση με στόχο τη βελτίωση της χρηστικότητας και της λειτουργικότητάς της και η τελευταία της έκδοση είναι η HTML5 [68]. Ο οργανισμός W3C (World Wide Web Consortium) είναι επιφορτισμένος με τον σχεδιασμό και τη συντήρηση της γλώσσας. Όταν κάποιος πατήσει με το ποντίκι του ένα σύνδεσμο σε μια ιστοσελίδα, έχει πρόσβαση στην HTML με τη μορφή ενός υπερσυνδέσμου, ο οποίος με τη σειρά του μεταφέρει τον χρήστη σε μια άλλη ιστοσελίδα. Η συγγραφή HTML είναι μια αλληλουχία σύντομου κειμένου που εισάγουμε σε ένα αρχείο κειμένου και αποθηκεύουμε με την κατάληξη .html. Τα αυτοτελή αυτά

κείμενα ονομάζονται ετικέτες (tags). Για να δούμε την ιστοσελίδα μας, απλώς επιλέγουμε να ανοίξουμε το συγκεκριμένο αρχείο με ένα πρόγραμμα περιήγησης. Το πρόγραμμα περιήγησης διαβάζει το κείμενο – κώδικα που έχουμε γράψει και μεταφράζει το κείμενο στην μορφή που έχει ζητήσει ο συγγραφέας της σελίδας. Σήμερα υπάρχει και μια παραλλαγή της HTML, η DHTML (Dynamic HTML), η οποία παρέχει μεγαλύτερο έλεγχο στα στοιχεία της HTML, επιτρέποντας αλλαγές χωρίς να απαιτείται αίτηση επιστροφής στο διακομιστή.

Παρόλα αυτά, η HTML επιτελεί μόνο το βασικό ρόλο σε μια ιστοσελίδα. Από τη στιγμή που κάποιος θέλει να καταστήσει λειτουργική την ιστοσελίδα του θα πρέπει να εισάγει σε αυτή και κώδικα JavaScript [69]. Η λειτουργία της JavaScript είναι απλή. Μέσω αυτής γράφονται συναρτήσεις, οι οποίες ενσωματώνονται στην HTML και αλληλεπιδρούν με τον χρήστη της ιστοσελίδας. Για παράδειγμα, μέσω JavaScript ο προγραμματιστής μπορεί να δημιουργήσει νέα παράθυρα στην ιστοσελίδα, τα οποία αναδύονται, όταν ζητηθεί κάτι από τον χρήστη, μπορεί να επικυρώνει τις τιμές που έχει εισάγει ο χρήστης σε μία φόρμα εισαγωγής δεδομένων εξασφαλίζοντας ότι αυτές θα γίνουν αποδεκτές από τον διακομιστή πριν γίνει η υποβολή τους σε αυτόν. Επιπλέον, έχει την ευχέρεια να αλλάζει τη μορφή και το περιεχόμενο των εικόνων τη στιγμή που το ποντίκι διέρχεται πάνω από αυτές. Η JavaScript είναι μια γλώσσα δέσμης ενεργειών, η οποία χρησιμοποιείται για την ανάπτυξη διαδικτυακών εφαρμογών από την πλευρά του χρήστη – πελάτη. Επηρεάστηκε από πολλές γλώσσες προγραμματισμού και σχεδιάστηκε να μοιάζει με την Java [70], αλλά να είναι πολύ πιο εύκολη από αυτή και να μπορούν και μη-προγραμματιστές Java να την χρησιμοποιούν. Παρόλο που η JavaScript είναι περισσότερο γνωστή για τη χρήση της στις ιστοσελίδες, χρησιμοποιείται επίσης για την ενεργοποίηση της εκτέλεσης κώδικα σε αντικείμενα τα οποία είναι ενσωματωμένα σε διάφορες εφαρμογές. Παρά το όνομά της, δεν έχει κληρονομήσει πολλά μόνο από την Java, αλλά είναι ένα συνονθύλευμα της C και της Java σε ό,τι αφορά τη σύνταξη και τα είδη μεταβλητών που περιέχει. Η JavaScript, αντί να τρέχει στον διακομιστή, τρέχει τοπικά στο πρόγραμμα περιήγησης του χρήστη και έτσι ανταποκρίνεται γρηγορότερα στις αιτήσεις του. Επιπλέον, μπορεί να ανιχνεύει ενέργειες του χρήστη που δεν μπορεί η

HTML, όπως για παράδειγμα συνδυασμό κουμπιών από το πληκτρολόγιο.

3.7.3. Υποδομή

Η υποδομή είναι το μέσο για την παροχή των υπηρεσιών νέφους από τους παρόχους μέσω της εικονικοποίησης (virtualization) [71]. Η εικονικοποίηση μπορεί να βρίσκεται στο διαδίκτυο, όπου κάποια συστήματα τρέχουν σε ένα απομακρυσμένο διακομιστή και εμφανίζονται σαν να είναι εντός της εταιρείας του πελάτη. Επίσης, μπορεί να υφίσταται και τοπικά, όπου οι εφαρμογές τρέχουν σε ένα διακομιστή εντός της εταιρείας και εμφανίζονται στις οθόνες των χρηστών. Σε αυτή την ενότητα θα μιλήσουμε για το πώς η εικονικοποίηση τυποποιείται και το πώς οι μεγάλοι πάροχοι υπηρεσιών υπολογιστικού νέφους εργάζονται μαζί για την αποδοτική λειτουργία της εικονικοποίησης.

Κάθε φορά που ανακαλύπτεται κάτι νέο στον χώρο της πληροφορικής, οι ανταγωνιστές συναγωνίζονται μεταξύ τους για να θεωρηθεί ως πρότυπο η υλοποίηση που έχει κάνει ο καθένας από αυτούς. Αυτό δεν συνέβη όμως και με την εικονικοποίηση, για την οποία οι κύριοι παίκτες συνεργάστηκαν για τη δημιουργία του προτύπου. Η VMware [72], η AMD [73], η BEA Systems [74] , η BMC Software [75], η Broadcom [76], η Cisco [77], η Dell [78], η HP [79], η IBM [18], η Intel [80] η Red Hat [81] και άλλες, οι οποίες δεν υπάρχουν πια στην αγορά, εργάστηκαν από κοινού για τη δημιουργία και την προώθηση ανοικτών προτύπων πάνω στην εικονικοποίηση.

Η VMware προσέφερε στους εταίρους πρόσβαση στον πηγαίο κώδικα του ESX Server [82] και σε διεπαφές μιας εφαρμογής, η οποία ονομάστηκε VMware Community Source [83]. Η συγκεκριμένη εφαρμογή σχεδιάστηκε για να βοηθήσει τους εταίρους να επηρεάσουν τις κατευθυντήριες γραμμές δημιουργίας των προτύπων της εικονικοποίησης μέσω της ομαλής συνεργασίας.

Η εικονικοποίηση κέρδισε την ευρεία υιοθέτηση από τους παρόχους υπηρεσιών υπολογιστικού νέφους λόγω των αναμφισβήτητων οφελών προς τους πελάτες τους. Είναι μια περιοχή πλούσια σε ευκαιρίες και η όλη υποδομή θα αναπτυχθεί καλύτερα και πληρέστερα μέσω των ανοικτών προτύπων. Όπως δήλωσε και η τέως πρόεδρος της VMware, Diane Greene, «*όλα τα εμπορικά προϊόντα της VMware καθώς και τα API της είναι διαθέσιμα σε όλους τους εταίρους τόσο ως εφαρμογές όσο και ως πηγαίος κώδικας για την ομαλή υιοθέτηση της εικονικοποίησης από όλους με απώτερο σκοπό από τη μία τη διεύρυνση των εταίρων και από την άλλη την πλήρη αποδοχή της εικονικοποίησης από τους χρήστες*» [84].

Όλες αυτές οι πρωτοβουλίες αποσκοπούσαν στο να επωφεληθούν οι τελικοί χρήστες. Αρχικά, μέσω των προτύπων και του πηγαίου κώδικα που διέθεσε η VMware, οι άλλες εταιρείες θα μπορούν να δημιουργήσουν εφαρμογές όχι από την αρχή, αλλά ενσωματώνοντας τα ήδη δοκιμασμένα API της VMware, καθώς και να ανακαλύψουν νέες λύσεις πάνω στην εικονικοποίηση. Τα πρότυπα πάνω στα οποία έχουν χτιστεί οι hypervisors αναμένεται να επιτρέψουν τη διαλειτουργικότητα μεταξύ των πελατών σε ετερογενή εικονικά περιβάλλοντα. Τέλος, οι εταίροι μέσω της ήδη υπάρχουσας υποδομής σε εφαρμογές μπορούν να αναπτύξουν νέες ταχύτερες και καλύτερες έχοντας κοινή βάση με την υπάρχουσα υποδομή.

Ο hypervisor είναι ο θεμελιώδης λίθος της εικονικής υποδομής και επιτρέπει την κατάτμηση του υπολογιστικού συστήματος [85-88]. Το ανοικτό πρότυπο πάνω στους Hypervisors ωφέλησε τους χρήστες δίνοντάς τους τη δυνατότητα να μετακινούνται μεταξύ των παρόχων υπηρεσιών υπολογιστικού νέφους.

Ως αρχικό βήμα, η VMware προσέφερε ένα υπάρχον πλαίσιο από διεπαφές, με ονομασία VMHI (Virtual Machine Hypervisor Interfaces) [88], στο οποίο είναι βασισμένα τα εικονικά προϊόντα της, ώστε να διευκολύνει την ανάπτυξη των προτύπων αυτών σε βιομηχανικό επίπεδο. Η συνεπής υιοθέτηση ανοικτών διεπαφών αναμένεται να διευκολύνει τη διαλειτουργικότητα και τη δυνατότητα υποστήριξης σε ετερογενή εικονικά περιβάλλοντα.

Το πρόγραμμα CS (Community Source) παρέχει στους βιομηχανικούς εταίρους τη δυνατότητα να έχουν πρόσβαση στον πηγαίο κώδικα του διακομιστή VMware ESXi. Οι εταίροι μπορούν να συνεισφέρουν με δημιουργία νέου κώδικα ή APIs, ώστε να επεκταθεί η διαλειτουργικότητα μέσω ολοκληρωμένων λύσεων. Τόσο ο κώδικας όσο και τα APIs είναι διαθέσιμα μέσω του προγράμματος CS σε όλους τους εταίρους. Η βασική ιδέα πίσω από αυτό είναι να συνδυαστούν τα καλύτερα σημεία τόσο των προγραμμάτων ελεύθερου κώδικα όσο και των εμπορικών εφαρμογών. Επίσης, τα μέλη της κοινότητας μπορούν να συμμετέχουν και να επηρεάζουν τη διαχείριση του διακομιστή VMware ESXi μέσω μιας κονσόλας εντολών. Η συγκεκριμένη προσέγγιση θα συμβάλει στην προώθηση της ανοικτής συνεργασίας, ενώ παράλληλα διατηρεί την δυνατότητα των εταίρων να κατασκευάζουν διαφορετικές και ιδιόκτητες εφαρμογές, αν το επιθυμούν.

Σε ό,τι αφορά τους πελάτες, η προηγούμενη φιλοσοφία τους προσέφερε ένα μεγαλύτερο εύρος από λύσεις μεταξύ των παρόχων που εφαρμόζουν την υποδομή VMware ή κάποιο από τα εικονικά προϊόντα της VMware. Σε ό,τι αφορά τα μέλη της κοινότητας, η πρόσβαση στον πηγαίο κώδικα αφενός τους επιτρέπει να παραδίδουν στους πελάτες τους ολοκληρωμένες λύσεις σε μικρό χρονικό διάστημα και αφετέρου τους δίνει τη δυνατότητα να προσφέρουν καλύτερες υπηρεσίες στους πελάτες τους μέσω της ίδιας υποδομής.

Το αποτέλεσμα της συνεργασίας των παραπάνω εταιρειών στον τομέα της εικονικοποίησης ήταν να δημιουργηθεί ένα πρότυπο με όνομα OVF (Open Virtualization Format) [89]. Το συγκεκριμένο πρότυπο περιγράφει λεπτομερώς τον τρόπο με τον οποίο οι εικονικές συσκευές θα μπορούν να κατασκευάζονται οπουδήποτε και από οποιονδήποτε πάροχο, ενώ παράλληλα θα είναι σε θέση να τρέξουν σε οποιονδήποτε hypervisor. Το πρότυπο είναι ανεξάρτητο από την πλατφόρμα υλοποίησης, είναι επεκτάσιμο και παρέχει τη δυνατότητα προσθήκης νέων Hypervisors στην ήδη υπάρχουσα υποδομή.

Το OVF δίνει στους χρήστες και στους προγραμματιστές την ευκαιρία να επιλέξουν οποιοδήποτε Hypervisor θέλουν, βασιζόμενοι στην τιμή, στις προτιμήσεις τους ή στην λειτουργικότητά του, χωρίς να

είναι υποχρεωμένοι να τον χρησιμοποιούν για πάντα. Το συγκεκριμένο πρότυπο θεωρήθηκε ότι ήταν καταλυτικός παράγοντας στην ευρεία υιοθέτηση των εικονικών συσκευών από το ευρύ κοινό.

Η VMware ανέλαβε ηγετικό ρόλο στην ανάπτυξη του προτύπου OVF, καθώς ήταν η κυρίαρχη δύναμη στον κόσμο της εικονικοποίησης. Είναι, επίσης, ενθαρρυντικό το γεγονός ότι έδωσαν τον πηγαίο κώδικα των εφαρμογών τους στους εταίρους, ώστε να υιοθετηθεί το πρότυπο και από τη βιομηχανία εφαρμογών.

3.7.4. Διαδικτυακές υπηρεσίες

Σύμφωνα με το W3C (World Wide Web Consortium) μια διαδικτυακή υπηρεσία είναι ένα σύστημα λογισμικού σχεδιασμένο να υποστηρίζει τη διαλειτουργική αλληλεπίδραση μιας υπολογιστικής μηχανής με κάποια άλλη μέσω ενός δικτύου [90]. Σε επίπεδο υπολογιστικού νέφους αυτό συνεπάγεται την επικοινωνία μίας υπηρεσίας ή ενός αντικειμένου με ένα άλλο. Συνήθως, οι διαδικτυακές υπηρεσίες είναι APIs, τα οποία μπορεί να προσπελαστούν μέσω ενός δικτύου, όπως το διαδίκτυο, και να εκτελεστούν σε ένα απομακρυσμένο σύστημα, το οποίο φιλοξενεί τις αιτηθείσες υπηρεσίες.

Στη συνέχεια θα αναφέρουμε μερικές από τις πιο διάσημες διαδικτυακές υπηρεσίες, όπως την REST [91], την SOAP [92] και την JSON [93].

Τα δεδομένα μπορούν να υποστούν επεξεργασία και να εμφανιστούν στον χρήστη με αρκετούς μηχανισμούς και δύο από τους πιο γνωστούς είναι οι JSON και XML. Και οι δύο αυτοί μηχανισμοί είναι βασισμένοι σε δύο ηγετικά πρότυπα της βιομηχανίας, την HTML και την JavaScript, με σκοπό τη διανομή και παρουσίαση των δεδομένων.

Το JSON (JavaScript Object Notation) [93] είναι μια μορφή ανταλλαγής δεδομένων, η οποία χρησιμοποιείται για να μεταδίδει δομημένα δεδομένα μέσω μιας σύνδεσης δικτύου κατά τη διάρκεια μιας διαδικασίας που ονομάζεται διαδοχή (serialization). Συχνά χρησιμοποιείται ως εναλλακτικό του XML. Βασίζεται σε ένα υποσύνολο

εντολών της γλώσσας JavaScript και συνήθως χρησιμοποιείται μαζί με αυτή τη γλώσσα. Παρόλα αυτά, το JSON θεωρείται ένα πρότυπο ανεξάρτητο από γλώσσα προγραμματισμού και υπάρχει διαθέσιμος μεταγλωττιστής για μεταγλώττιση και δημιουργία εκτελέσιμου κώδικα JSON σε αρκετές γλώσσες προγραμματισμού. Το γεγονός αυτό είναι που καθιστά και το JSON έναν καλό αντικαταστάτη της XML, όταν έχουμε να κάνουμε με ανταλλαγή δεδομένων.

Στον αντίποδα έχουμε το XML (Extensible Markup Language) [55]. Το XML είναι ένα πρότυπο, το οποίο προσφέρει έναν αυτοπεριγραφικό τρόπο κωδικοποίησης του κειμένου και των δεδομένων, έτσι ώστε το περιεχόμενο να μπορεί να προσεγγιστεί με πολύ μικρή ανθρώπινη αλληλεπίδραση και αποστέλλεται σε μια ευρεία γκάμα υλικού, λειτουργικών συστημάτων και εφαρμογών. Το XML παρέχει ένα προτυποποιημένο τρόπο για αναπαράσταση τόσο του κειμένου όσο και των δεδομένων σε μια μορφή που μπορεί να χρησιμοποιηθεί από πολλές πλατφόρμες. Επίσης, μπορεί να χρησιμοποιηθεί από μεγάλο εύρος εργαλείων προγραμματισμού. Το XML μοιάζει με την HTML επειδή και τα δύο πηγάζουν από τη γλώσσα προγραμματισμού SGML, η οποία υπάρχει από το 1986. Όσοι είναι γνώστες της HTML μπορούν πολύ εύκολα να χρησιμοποιήσουν το XML. Οι βασικές διαφορές των δύο συνοψίζονται στο ότι η HTML διαφοροποιεί τη μορφή από το περιεχόμενο, ενώ το XML ενδιαφέρεται μόνο για το περιεχόμενο. Άλλη βασική διαφορά είναι ότι το XML είναι επεκτάσιμο.

Το XML καθιστά τη χρήση των βάσεων δεδομένων ακόμα πιο εύκολη για μια εταιρεία. Οι σχεσιακές βάσεις δεδομένων δεν μπορούν να ανταποκριθούν στις απαιτήσεις των ηλεκτρονικών επιχειρήσεων, επειδή επεξεργάζονται τα δεδομένα ανεξάρτητα από το περιεχόμενό τους. Επίσης, οι σχεσιακές βάσεις δεδομένων δεν γίνεται να χειριστούν δεδομένα ήχου, εικόνας, βίντεο η εμφωλευμένες δομές δεδομένων, στοιχεία τα οποία είναι ευρέως διαδεδομένα στο υπολογιστικό νέφος. Οι παραδοσιακές βάσεις δεδομένων, για να καταφέρουν να ανταπεξέλθουν στα δεδομένα του υπολογιστικού νέφους, αναγκάζονται να μετατρέψουν τα δεδομένα τους σύμφωνα με το πρότυπο XML. Αυτή η διαδικασία μετατροπής είναι επιρρεπής σε λάθη, έχει μεγάλα ποσοστά

αστοχίας, αυξάνει την πολυπλοκότητα του όλου σχήματος και γι' αυτούς τους λόγους δημιουργήθηκαν οι βάσεις δεδομένων XML [94]. Οι συγκεκριμένες βάσεις εξομαλύνουν αυτή τη διαδικασία, επειδή είναι κατασκευασμένες να αποθηκεύουν εγγενώς δεδομένα XML σε δομημένη, ιεραρχική δομή. Τα ερωτήματα σε βάσεις δεδομένων XML μπορεί να απαντηθούν πολύ γρηγορότερα σε σχέση με τις παραδοσιακές βάσεις δεδομένων, επειδή δεν υπάρχει ανάγκη μετατροπής των δεδομένων σε XML από τη σχεσιακή βάση.

Σε επίπεδο υπολογιστικού νέφους, οι διαδικτυακές υπηρεσίες περιγράφουν τη διαδικασία μεταφοράς των δεδομένων από τον διακομιστή στον πελάτη – χρήστη. Τα βασικότερα πρωτόκολλα σε αυτό τον τομέα είναι τα REST και SOAP.

Το πρωτόκολλο REST (Representational state transfer) παρέχει ένα τρόπο για να λαμβάνει ο χρήστης το περιεχόμενο των πληροφοριών από μια ιστοσελίδα, η οποία περιέχει ένα αρχείο XML που περιγράφει και περιλαμβάνει το επιθυμητό περιεχόμενο [91]. Για παράδειγμα το REST θα μπορούσε να χρησιμοποιηθεί από τον πάροχο υπολογιστικού νέφους για να παρέχει ενημερωμένες πληροφορίες σχετικά με τη χρέωση του πελάτη. Ανά τακτά χρονικά διαστήματα ο πάροχος θα μπορούσε να προετοιμάσει μια ιστοσελίδα, η οποία να είχε ως περιεχόμενο δηλώσεις XML. Οι πελάτες, γνωρίζοντας την ακριβή διεύθυνση της συγκεκριμένης ιστοσελίδας, θα μπορούσαν μέσω ενός προγράμματος περιήγησης να διαβάζουν το περιεχόμενο και να το εμφανίζουν στην οθόνη τους. Το REST ήταν η εκπόνηση της διδακτορικής διατριβής του Roy Fielding [95], στην οποία το ονόμασε αρχιτεκτονικό στυλ. Στη διατριβή αυτή ο Fielding αναφέρει ότι το REST αξιοποιεί στο έπακρο την υπάρχουσα τεχνολογία και τα πρωτόκολλα του διαδικτύου μεταξύ των οποίων τα HTTP και XML. Σε επίπεδο λειτουργικότητας το REST είναι παρόμοιο με το SOAP (Simple Object Access Protocol), αλλά αρκετά ευκολότερο στη χρήση. Το SOAP απαιτεί την χρήση ενός προγράμματος σε ένα διακομιστή δεδομένων και ενός προγράμματος στον υπολογιστή του χρήστη. Παρόλα αυτά, το SOAP προσφέρει περισσότερες δυνατότητες. Για παράδειγμα, αν κάποιος ήθελε να παρέχει μια περίληψη περιεχομένου από τις ιστοσελίδες του παρόχου του, θα έπρεπε υποχρεωτικά να κάνει χρήση του SOAP, από τη

στιγμή που αυτό μόνο προσφέρει την μέγιστη δυνατή αλληλεπίδραση μεταξύ διακομιστή και πελάτη. Τέλος, αξίζει να σημειωθεί ότι το REST χρησιμοποιεί την ίδια μέθοδο παρουσίασης με το RSS (RDF Site Summary) .

Το πρωτόκολλο SOAP (Simple Object Access Protocol) [92] είναι ένας τρόπος για κάποιο πρόγραμμα που τρέχει σε ένα συγκεκριμένο λειτουργικό σύστημα, όπως για παράδειγμα τα Windows 7 [42], να επικοινωνεί με ένα άλλο πρόγραμμα που τρέχει σε ίδιο ή άλλο λειτουργικό σύστημα, όπως για παράδειγμα το Ubuntu Linux [96], με τη χρήση των HTTP και XML ως εργαλεία για ανταλλαγή πληροφοριών [38, 55]. Λόγω του ότι τα HTTP και XML είναι ήδη εγκατεστημένα και διαθέσιμα για χρήση σχεδόν σε όλα τα λειτουργικά συστήματα, παρέχουν μια εύκολη λύση στο πρόβλημα της επικοινωνίας των προγραμμάτων που τρέχουν σε διαφορετικά λειτουργικά συστήματα. Το πρωτόκολλο SOAP περιγράφει επακριβώς το πώς θα κωδικοποιηθεί μια κεφαλίδα HTTP και ένα αρχείο XML, έτσι ώστε ένα πρόγραμμα από έναν υπολογιστή να μπορεί να καλέσει ένα άλλο πρόγραμμα σε ένα δεύτερο υπολογιστή και να του περάσει δεδομένα. Επίσης, εξηγεί το πώς ένα κληθέν πρόγραμμα μπορεί να επιστρέψει απάντηση στην κλήση του καλούντος. Ένα από τα πλεονεκτήματα του SOAP είναι ότι οι κλήσεις των προγραμμάτων μπορούν να διαπεράσουν τα τείχη προστασίας, που δεν θα ήταν εφικτό υπό άλλες συνθήκες, όπως στην περίπτωση που τα προγράμματα από μόνα τους προσπαθούσαν να κάνουν κάτι τέτοιο. Ο λόγος που συμβαίνει αυτό είναι ότι οι αιτήσεις HTTP επιτρέπονται εξ ορισμού να διαπερνούν τα τείχη προστασίας, οπότε και η επικοινωνία μέσω SOAP δεν αντιμετωπίζει πρόβλημα.

Τα πρότυπα είναι εξαιρετικά σημαντικά και κάτι που θεωρούμε δεδομένο στις μέρες μας. Για παράδειγμα, δεν θεωρούμε πρόβλημα να στείλουμε ή να λάβουμε ένα έγγραφο του Microsoft Word [97] μέσω του ηλεκτρονικού ταχυδρομείου μας και να μπορούμε να το επεξεργαστούμε. Πριν τυποποιηθούν τα αρχεία τύπου .doc και .txt, ήταν πολύ συνηθισμένο για αρχεία που γίνονταν σε κάποιον υπολογιστή να μην είναι αναγνώσιμα σε άλλον υπολογιστή.

Στο κεφάλαιο αυτό μιλήσαμε για τα πρότυπα και τα πρωτόκολλα που θα συναντήσει ο χρήστης κατά την ενασχόλησή του με το υπολογιστικό νέφος, καθώς και για το πώς συνδυάζονται, ώστε να λειτουργούν αποδοτικά.

Κ Ε Φ Α Λ Α Ι Ο Τ Ε Τ Α Ρ Τ Ο

Μοντέλα του υπολογιστικού νέφους

4.1. Εισαγωγή

Σε αυτό το κεφάλαιο θα εξετάσουμε μερικές από τις διαδικτυακές υπηρεσίες ή αλλιώς μοντέλα, που παρέχονται από το υπολογιστικό νέφος, θα αναλύσουμε την Επικοινωνία-ως-Υπηρεσία (Communication-as-a-Service – CaaS) [98], καθώς επίσης και τα πλεονεκτήματα που έχει σε σχέση με τις συμβατικές τεχνολογίες. Η υποδομή (infrastructure) παρέχεται επίσης ως υπηρεσία στο νέφος και αξίζει να αναφερθεί ότι

υπάρχουν πολλές εναλλακτικές λύσεις για το πώς γίνεται η διαχείρισή της. Όταν οι πάροχοι του υπολογιστικού νέφους αναθέτουν την υποδομή-ως-υπηρεσία (Infrastructure-as-a-Service – IaaS) [99], βασίζονται κυρίως στα πολύ γρήγορα δίκτυα επικοινωνιών και στη μοντέρνα τεχνολογία βάσει της οποίας γίνεται ζήτηση και κατανάλωση ακριβώς όσων πόρων χρειάζεται ο κάθε χρήστης. Επίσης, υπάρχουν πάροχοι οι οποίοι παρέχουν Εφαρμογές-ως-υπηρεσία (Software-as-a-Service – SaaS) [99, 100], μέσω των οποίων δίνεται η δυνατότητα στους χρήστες να έχουν το καλύτερο δυνατό επίπεδο σε μια εφαρμογή που χρησιμοποιούν. Τέλος, υπάρχει η δυνατότητα από τους παρόχους παροχής μιας ολόκληρης Πλατφόρμας-ως-υπηρεσία (Platform-as-a-Service – PaaS) [99, 100], πάνω στην οποία οι χρήστες μπορούν να χτίσουν δικές τους εφαρμογές και είτε να τις μεταπωλήσουν ως SaaS σε άλλους χρήστες, ή να τις χρησιμοποιούν αποκλειστικά ως επιχειρησιακό κομμάτι της εταιρείας τους.

Καθώς η τεχνολογία αναβαθμίζεται από το κλασσικό μοντέλο πληροφορικής στο νέο μοντέλο του υπολογιστικού νέφους, οι παροχές προσφερόμενων υπηρεσιών εξελίσσονται σε καθημερινή βάση. Στο συγκεκριμένο κεφάλαιο έχουμε ως σκοπό να ερμηνεύσουμε κάποιες βασικές έννοιες για το πεδίο του υπολογιστικού νέφους σχετικά με τη λειτουργία του.

Οι παρεχόμενες υπηρεσίες διαδικτύου έχουν συχνά μια σειρά από κοινά χαρακτηριστικά, όπως για παράδειγμα χαμηλό επίπεδο εισόδου στην αγορά, ειδικά για υπηρεσίες οι οποίες προσφέρονται συγκεκριμένα για μεμονωμένους καταναλωτές ή μικρές επιχειρηματικές οντότητες. Συχνά σε αυτές τις περιπτώσεις, από τη μεριά του πελάτη, απαιτείται ελάχιστη υποδομή. Παρόλο που η δυνατότητα μαζικής επεκτασιμότητας είναι κοινή σε αυτά τα είδη προσφορών, αυτό δεν είναι πάντα απαραίτητο να συμβαίνει. Πολλοί από τους παρόχους υπηρεσιών υπολογιστικού νέφους δεν έχουν αξιοποιήσει την προηγούμενη δυνατότητα γιατί δεν απαιτείται κάτι τέτοιο, βάσει των χρηστών τους. Η πολλαπλή μίσθωση επιτρέπει τον διαμοιρασμό των πόρων αλλά και του κόστους μεταξύ της συνολικής βάσης των χρηστών. Με τον όρο βάση εννοούνται οι χρήστες οι οποίοι χρησιμοποιούν το υπολογιστικό νέφος

μόνο για τις βασικές – τυπικές υπηρεσίες του. Τέλος, η ανεξαρτησία τόσο από κάποια συγκεκριμένη συσκευή, όσο και από κάποιο συγκεκριμένο σημείο, επιτρέπει στους χρήστες να έχουν πρόσβαση στο σύστημα άσχετα από το πού βρίσκονται ή τι είδους συσκευή χρησιμοποιούν. Στη συνέχεια θα εξετάσουμε περιληπτικά μερικές από τις πιο κοινές και διαδεδομένες υπηρεσίες που προσφέρουν οι πάροχοι του υπολογιστικού νέφους.

4.2. Communication-as-a-Service

Το Communication-as-a-Service (CaaS) είναι η υπηρεσία που προσφέρει επικοινωνία στις επιχειρήσεις [98]. Οι πάροχοι αυτού του είδους της υπηρεσίας, είναι υπεύθυνοι για τη διαχείριση του υλικού και του λογισμικού που απαιτείται για τη μεταφορά μέσω δικτύων IP [101], φωνής (Voice over IP – VoIP) [102], άμεσων μηνυμάτων (Instant Messaging – IM) [103], καθώς και δυνατότητες τηλεδιάσκεψης (Video Conferencing – VC) [104] στους πελάτες της. Το συγκεκριμένο μοντέλο ξεκίνησε την εξελικτική του διαδικασία μέσα από τη βιομηχανία τηλεπικοινωνιών, σε αντίθεση με το μοντέλο SaaS το οποίο «ανέτειλε» από τον τομέα υπηρεσιών διανομής λογισμικού. Σε μια τυπική συναλλαγή, οι πάροχοι CaaS προσφέρουν εγγυημένη ποιότητα παρεχόμενων υπηρεσιών (Quality of Service - QoS) [105] μέσω ενός ειδικού συμβολαίου που στη γλώσσα του υπολογιστικού νέφους ονομάζεται συμβόλαιο σε επίπεδο υπηρεσιών (Service-Level Agreement - SLA) [106].

Ένα μοντέλο CaaS επιτρέπει στους εταιρικούς πελάτες των παρόχων να αναπτύσσουν επιλεκτικά τα χαρακτηριστικά των επικοινωνιών και των υπηρεσιών για την επιχείρησή τους με τη γνωστή τακτική της χρέωσης μέσω χρήσης. Το CaaS έχει σχεδιαστεί πάνω σε ένα οικονομικό μοντέλο πίστωσης, το οποίο παρέχει κατανοητά, ευέλικτα και εύκολα στην κατανόηση σχέδια υπηρεσιών.

Οι υπηρεσίες CaaS συχνά ομαδοποιούνται και μπορεί να περιλαμβάνουν ολοκληρωμένη πρόσβαση στη φωνή και τα δεδομένα,

προηγμένες ενοποιημένες τεχνικές επικοινωνίας, όπως βιντεοκλήση, διαδικτυακή συνεργασία, chat, παρουσιάσεις σε πραγματικό χρόνο, φωνητικό γραμματοκιβώτιο και τέλος, προηγμένα χαρακτηριστικά κλήσεων. Μια τυπική εφαρμογή CaaS περιλαμβάνει μεταγωγή κυκλώματος, δίκτυο, POP και μεταγωγή πακέτου καθώς και συγκεκριμένη στοχοποίηση των αναγκών των πελατών. Είναι αυτονόητο, ότι όλα τα στοιχεία του CaaS βρίσκονται σε διαφορετικές γεωγραφικά θέσεις, μέσα σε ασφαλή κέντρα δεδομένων με σκοπό να επιτυγχάνεται η συνεχής διαθεσιμότητα και η επιβιωσιμότητα.

Το μοντέλο CaaS παρέχει ευελιξία και κλιμακωτή διάθεση πόρων, στοιχεία τα οποία μικρές και μεσαίες επιχειρήσεις δεν θα μπορούσαν να έχουν, από οικονομικής άποψης. Οι πάροχοι του συγκεκριμένου μοντέλου είναι προετοιμασμένοι να χειρίζονται μεγάλα και απότομα πακέτα δεδομένων κατά τη διάρκεια των ωρών αιχμής, παρέχοντας υπηρεσίες ικανές για χρήση περισσότερων πόρων, όταν θεωρηθεί απαραίτητο. Η χωρητικότητα και οι δυνατότητες του δικτύου μπορούν να αλλάξουν δυναμικά, έτσι ώστε η λειτουργικότητα να συμβαδίζει με τη ζήτηση των καταναλωτών και παράλληλα να μην σπαταλώνται οι πόρου του παρόχου. Από την μεριά των καταναλωτών, υπάρχει μικρός σχεδόν κανένας κίνδυνος για λήψη παρωχημένης υπηρεσίας, από την στιγμή που μέσα στις ευθύνες του παρόχου είναι η τακτική αναβάθμιση ή αλλαγή του υλικού και του λογισμικού ώστε να είναι πάντα στην αιχμή της τεχνολογίας η εφαρμογή.

Το CaaS απαιτεί λίγη ή καθόλου εποπτεία της διαχείρισης από τους πελάτες. Επίσης, ελαχιστοποιεί τις ανάγκες των πελατών για κεφαλαιακές επενδύσεις σε υποδομή και εξαλείφει τις δαπάνες για συνεχή συντήρηση και γενικότερα τη λειτουργία των υποδομών. Μέσω μιας λύσης CaaS, οι πελάτες είναι σε θέση να αξιοποιούν τις υπηρεσίες επικοινωνίας των μεγάλων επιχειρήσεων χωρίς να χρειάζεται να κατασκευάσουν τίποτα παραπάνω, εκτός από τα βασικά, στον δικό τους χώρο. Αυτό επιτρέπει στους πελάτες να ανακατανέμουν τον προϋπολογισμό και τους ανθρώπινους πόρους της εταιρείας τους με σκοπό την καλύτερη και αποδοτικότερη λειτουργία τους.

4.2.1. Πλεονεκτήματα του CaaS

Από το τηλέφωνο που βρίσκεται στο γραφείο του κάθε υπαλλήλου μέχρι την εφαρμογή που τρέχει στον φορητό υπολογιστή του και μέχρι το ιδιωτικό δίκτυο VoIP, όλα τα στοιχεία που υπάρχουν τα διαχειρίζεται 24/7 ο πάροχος CaaS. Όπως αναφέρθηκε και προηγουμένως, το βάρος της διαχείρισης ενός κέντρου δεδομένων διαμοιράζεται σε όλη την πελατειακή βάση του παρόχου, κάνοντας σαφώς οικονομικότερη την υλοποίηση CaaS από την κατασκευή ενός ιδιωτικού VoIP δικτύου. Στη συνέχεια θα αναφερθούν μερικά από τα πλεονεκτήματα του CaaS.

Μερικά χρόνια νωρίτερα, η απομακρυσμένη διαχείριση υποδομών και υπηρεσιών που παρέχονταν από τρίτους, ήταν μια απαράδεκτη κατάσταση για τις περισσότερες, αν όχι για όλες τις επιχειρήσεις. Ωστόσο, κατά τη διάρκεια της τελευταίας δεκαετίας, λόγω της βελτίωσης τεχνολογίας στο υλικό και λογισμικό και ων νέων ταχυτήτων των δικτύων η συγκεκριμένη στάση έχει αλλάξει. Αυτό συμβαίνει, εν μέρει εξαιτίας των οικονομικών ωφελειών από τη χρήση των συγκεκριμένων υπηρεσιών. Σε αντίθεση με τις υπηρεσίες «εφάπαξ» που παρέχονται από ειδικούς παρόχους, το μοντέλο CaaS παρέχει μια πλήρη λύση επικοινωνίας, την οποία διαχειρίζεται εξ ολοκλήρου ο πάροχος. Τα χαρακτηριστικά όπως το VoIP, οι ενοποιημένες υπηρεσίες επικοινωνίας, η αναβάθμιση του πυρήνα των PBX με προηγμένες λειτουργίες, διαχειρίζονται από τους παρόχους, οι οποίοι είναι υπεύθυνοι για το σύνολο της ολοκλήρωσης και την παροχή υπηρεσιών στους χρήστες.

Με το μοντέλο CaaS ο πάροχος παρέχει πρόσβαση σε δεδομένα και φωνή, διαχειρίζεται το LAN/WAN, την ασφάλεια, τους δρομολογητές (routers), το ηλεκτρονικό ταχυδρομείο (e-mail), τα φωνητικά μηνύματα και τον αποθηκευτικό χώρο. Με τη διαχείριση του LAN/WAN ο πάροχος εγγυάται τη συνεχή ποιότητα των παρεχόμενων υπηρεσιών από το τερματικό ενός χρήστη στην άλλη άκρη του δικτύου και πίσω. Προηγμένες λειτουργίες ενοποιημένων επικοινωνιών, οι οποίες αποτελούν και μέρος του CaaS περιλαμβάνουν

- Chat
- Τηλεδιασκέψεις πολυμέσων

- Χρήση του Microsoft Outlook
- Παρουσιάσεις σε πραγματικό χρόνο
- Τηλέφωνα VoIP
- Βιντεοκλήσεις
- Ενοποιημένες τεχνικές αποστολής μηνυμάτων
- Φορητότητα

Οι πάροχοι προσφέρουν συνεχώς νέα προϊόντα, τόσο στην απόδοση όσο και στα χαρακτηριστικά, στις παρεχόμενες υπηρεσίες. Η διαδικασία ανάπτυξης και εισαγωγής νέων χαρακτηριστικών στις εφαρμογές είναι πολύ πιο εύκολη, γρήγορη και οικονομική από οποιαδήποτε προηγούμενη τεχνολογία. Αυτό συμβαίνει γιατί ο πάροχος εργάζεται έτσι ώστε να ωφελεί τους τελικούς χρήστες μέσω της υποδομής του. Οι υπηρεσίες προσφέρονται στους χρήστες με ένα εξαιρετικά ελκυστικό κόστος, εξαιτίας του γεγονότος ότι πολλοί τελικοί χρήστες διαμοιράζονται το κόστος, το οποίο από την πλευρά τους είναι πολύ μικρό σε σύγκριση με αυτό που θα αναλάμβαναν ατομικά από μόνοι τους.

Όταν μια επιχείρηση αναθέτει τις τηλεπικοινωνιακές της ανάγκες σε ένα πάροχο CaaS, αυτός της παρέχει μια ολοκληρωμένη λύση, η οποία ταιριάζει απόλυτα με τις ανάγκες της επιχείρησης. Οι πελάτες πληρώνουν ένα ποσό, το οποίο συνήθως χρεώνεται ως μια μηνιαία συνδρομή για τους πόρους και μόνο που χρησιμοποίησαν. Η επιχείρηση δεν χρειάζεται να αγοράσει εξοπλισμό, οπότε υπάρχει κέρδος σε ό,τι αφορά τις κεφαλαιακές δαπάνες. Επίσης, στους συγκεκριμένους τύπους υπηρεσιών συμπεριλαμβάνεται και το κόστος της συνεχούς συντήρησης και αναβάθμισης της υλικολογισμικής υποδομής, η οποία πραγματοποιείται από τον φορέα παροχής υπηρεσιών. Επιπλέον, η χρήση του μοντέλου CaaS δίνει την δυνατότητα στις επιχειρήσεις να είναι σε θέση να συνεργάζονται μεταξύ τους σε οποιονδήποτε χώρο εργασίας, καθώς χρησιμοποιούνται προηγμένα εργαλεία συνεργασίας για τη δημιουργία ασφαλών και υψηλής αποδοτικότητας χώρων εργασίας μέσω οποιουδήποτε οργανισμού. Αυτό επιτρέπει στους εργάτες, τους συνεργάτες, τους προμηθευτές και τους πελάτες μιας επιχείρησης να επικοινωνούν και να συνεργάζονται πιο αποτελεσματικά. Η καλύτερη

επικοινωνία επιτρέπει στις επιχειρήσεις να προσαρμόζονται γρήγορα στις αλλαγές της αγοράς και έτσι να οικοδομήσουν ένα ανταγωνιστικό πλεονέκτημα. Το μοντέλο CaaS μπορεί, επίσης, να επιταχύνει τη λήψη αποφάσεων εντός μιας επιχείρησης. Συμπερασματικά, οι καινοτόμες ενοποιημένες δυνατότητες επικοινωνίας συντελούν ώστε οι πληροφορίες να φτάνουν γρήγορα σε εκείνους που τις χρειάζονται.

Επίσης, όταν μια επιχείρηση αναθέτει τις υπηρεσίες επικοινωνιών της σε ένα πάροχο CaaS, πληρώνει για τα χαρακτηριστικά που χρειάζεται, όταν τα χρειάζεται. Ο πάροχος υπηρεσιών CaaS μπορεί να κατανείμει το κόστος των υπηρεσιών του σε μια πληθώρα πελατών – επιχειρήσεων. Όπως αναφέρθηκε και προηγουμένως, η συγκεκριμένη υλοποίηση καθιστά τη χρήση των κοινών χαρακτηριστικών αρκετά πιο οικονομική για τους πελάτες. Οι κλιμακωτές οικονομίες επιτρέπουν στους χρήστες αρκετή ευελιξία, ώστε να μην είναι υποχρεωμένοι να συνεργάζονται αποκλειστικά με έναν πάροχο, με αποτέλεσμα να είναι ελεύθεροι να επιλέξουν τον καλύτερο μεταξύ των πολλών παρόχων.

Η ραγδαία ανάπτυξη της τεχνολογίας, η οποία διατυπώθηκε πριν καιρό ως ο νόμος του Moore [107], έχει επιφέρει απαξίωση των προϊόντων σε όλο και μικρότερες χρονικές περιόδους. Ο νόμος του Moore περιγράφει την τάση που έχει η χρήση των ολοκληρωμένων κυκλωμάτων στο υλικό του υπολογιστή. Πιο συγκεκριμένα, από την ανακάλυψη του ολοκληρωμένου κυκλώματος το 1958, ο αριθμών των τρανζίστορ που μπορούν να τοποθετηθούν σε ένα ολοκληρωμένο κύκλωμα αυξάνεται εκθετικά, και διπλασιάζεται περίπου κάθε δύο χρόνια.

Σε αντίθεση με τα ολοκληρωμένα κυκλώματα, ο μέσος όρος ζωής ενός PBX, καθώς και των βασικών εξαρτημάτων που το πλαισιώνουν, κυμαίνεται από πέντε έως δέκα χρόνια. Η συνεχής εισαγωγή νεότερων μοντέλων για όλα τα είδη της τεχνολογίας, π.χ. υπολογιστές, κινητά τηλέφωνα, λογισμικό κτλ, επέφερε μικρότερο κύκλο ζωής στα μοντέλα και μερικές φορές μικρότερο από ένα έτος. Οι πάροχοι CaaS θα πρέπει να αντισταθμίσουν αυτό το μειονέκτημα για λογαριασμό των χρηστών με τη συνεχή αναβάθμιση του εξοπλισμού τους, ώστε να ανταποκρίνονται πλήρως στις μεταβαλλόμενες απαιτήσεις της αγοράς.

Οι πάροχοι CaaS φιλοξενούν όλο τον εξοπλισμό που απαιτείται για την παροχή των υπηρεσιών τους στους πελάτες τους, εξαλείφοντας ουσιαστικά την ανάγκη των πελατών να διατηρούν κέντρα δεδομένων και εγκαταστάσεις. Επίσης, δεν υπάρχει καμία επιπλέον δαπάνη για την κατανάλωση ρεύματος που θα απαιτούσε μια τέτοια υποδομή. Οι πελάτες καρπώνονται το όφελος των πολλών κέντρων δεδομένων σε πλήρη διάθεση, όταν απαιτείται, και όλα αυτά περιλαμβάνονται σε μία μηνιαία χρέωση, ανάλογα με τη χρήση που έγινε.

Τι θα γινόταν στην περίπτωση που ένα καταστροφικό συμβάν συνέβαινε σε μια επιχείρηση; Θα μπορούσε το σχέδιο ανάνηψης της επιχείρησης να επιτρέψει τη συνεχή και απρόσκοπτη λειτουργία της χωρίς διακοπές; Τι θα συνέβαινε στην περίπτωση που η εταιρεία έχανε τις επικοινωνίες της; Για πόσο καιρό θα μπορούσε να λειτουργήσει χωρίς επικοινωνία με τον έξω κόσμο; Για την πλειοψηφία των επιχειρήσεων η απάντηση είναι όχι για πολύ. Ο περιορισμός των κινδύνων με τη χρήση γεωγραφικά διεσπαρμένων κέντρων δεδομένων είναι από τα πλέον ασφαλή πρότυπα που υφίστανται σήμερα, καθώς μετριάζεται ο κίνδυνος και επιτρέπεται στις εταιρείες, στην περίπτωση που ένα από τα κέντρα της πληγεί από ένα καταστροφικό γεγονός, να ανακτήσει τη λειτουργία της το συντομότερο δυνατόν μέσω των υπολοίπων κέντρων δεδομένων. Η προαναφερθείσα διαδικασία, στην περίπτωση των επικοινωνιών, υλοποιείται από τους παρόχους CaaS, γιατί οι περισσότερες εταιρείες δεν είναι σε θέση να λειτουργήσουν ούτε μια εφεδρική γραμμή επικοινωνίας, αν συμβεί κάποια καταστροφή. Σε αντίθεση με την ακεραιότητα των δεδομένων, ο περιορισμός της καταστροφής σε κομβικά σημεία για ένα δίκτυο μεταφοράς φωνής είναι συνήθως απαγορευτικός λόγω του κόστους και της μεγάλης πολυπλοκότητας της εφαρμογής. Με το CaaS υπάρχουν πολλά επίπεδα ασφάλειας και κομβικά σημεία ενσωματωμένα στο μοντέλο, ώστε να μην υπάρχει περίπτωση αποτυχίας στην εκτέλεση της υπηρεσίας.

4.3. Infrastructure-as-a-Service

Ο γενικός ορισμός του όρου Υποδομή-ως-Υπηρεσία (Infrastructure-as-a-Service – IaaS) είναι η παροχή υποδομών πληροφορικής, η οποία γίνεται μέσω ενός εικονικού περιβάλλοντος ως υπηρεσία [99, 108, 109]. Το IaaS αξιοποιεί σημαντική και τελευταίας γενιάς τεχνολογία, υπηρεσίες καθώς και επενδύσεις σε κέντρα δεδομένων με σκοπό την παροχή υπηρεσιών πληροφορικής ως υπηρεσία στους πελάτες. Σε αντίθεση με το παραδοσιακό μοντέλο ανάθεσης, το οποίο απαιτεί εκτεταμένη επιμέλεια, χρονοβόρες διαπραγματεύσεις και πολύπλοκες συμβάσεις, το IaaS επικεντρώνεται αποκλειστικά στο μοντέλο παροχής υπηρεσιών κάνοντας χρήση προκαθορισμένων όρων, τυποποιημένης υποδομής, ειδικά βελτιστοποιημένης για τις εφαρμογές των πελατών. Οι απλοποιημένες καταστάσεις εργασίας και οι βαθμιδωτές επιλογές στην υπηρεσία κάνουν το IaaS ιδανικό, για την υλοποίηση λύσεων που ανταποκρίνονται ακριβώς σε αυτό που ζητά ο πελάτης και η εφαρμογή του. Οι πάροχοι IaaS διαχειρίζονται τη μεταφορά και τη φιλοξενία των συγκεκριμένων εφαρμογών στην υποδομή τους. Οι πελάτες διατηρούν την ιδιοκτησία και τη διαχείριση της εφαρμογής τους, ενώ παράλληλα οι λειτουργίες φόρτωσης και διαχείρισης της υποδομής της εφαρμογής ανήκουν στον πάροχο IaaS. Οι τυπικές υλοποιήσεις που ανήκουν στον πάροχο περιλαμβάνουν τα ακόλουθα πολυεπίπεδα συστατικά:

- Υλικό υπολογιστών, το οποίο είναι οργανωμένο σε μορφή πλέγματος για μαζική οριζόντια επεκτασιμότητα.
- Δίκτυο υπολογιστών, το οποίο περιλαμβάνει δρομολογητές, τείχη προστασίας (firewalls), διαχείριση και εξισορρόπηση του φόρτου κτλ.
- Σύνδεση με το διαδίκτυο, συχνά σε δίκτυα κορμού αρχιτεκτονικής οπτικής ίνας.
- Ένα ολοκληρωμένο εικονικό περιβάλλον πάνω στο οποίο τρέχουν τα εικονικά μηχανήματα του χρήστη.
- Συμβόλαια παροχής υπηρεσιών.
- Ειδικά συστήματα χρέωσης ανάλογα με τη χρήση.

Οι πελάτες έχουν το πλεονέκτημα να νοικιάζουν ουσιαστικά ως υπηρεσία μόνο τους συγκεκριμένους πόρους που χρειάζονται από κάποιο πάροχο, αντί να αγοράζουν κέντρα δεδομένων, διακομιστές, λογισμικό, εξοπλισμό δικτύου κτλ. Συνήθως η χρέωση της υπηρεσίας γίνεται σε μηνιαία βάση, όπως ακριβώς χρεώνει τους πελάτες της μια εταιρεία κοινής ωφέλειας. Αξίζει να αναφερθεί ξανά ότι ο πελάτης χρεώνεται μόνο για τους πόρους που έχει καταναλώσει. Στα κύρια οφέλη από τη χρήση της συγκεκριμένης υπηρεσίας συμπεριλαμβάνονται τα ακόλουθα:

- Έτοιμη πρόσβαση σε ένα ήδη εγκατεστημένο και προρυθμισμένο περιβάλλον, το οποίο πληροί όλες τις προϋποθέσεις.
- Χρήση εξοπλισμού τελευταίας τεχνολογίας.
- Ασφαλείς και μεμονωμένες υπολογιστικές πλατφόρμες, με την τεχνολογία sand-box, οι οποίες παρακολουθούνται συνεχώς για παραβιάσεις ασφαλείας.
- Μειωμένος κίνδυνος για κατοχή πόρων που διατηρούνται από τρίτους.
- Δυνατότητα διαχείρισης των ωρών αιχμής καθώς και το αντίθετο.
- Χαμηλότερο κόστος, το οποίο προκύπτει από τη μειωμένη χρέωση του κόστους των υπηρεσιών αντί της πραγματοποίησης επενδύσεων σε υλικοτεχνική υποδομή.
- Μειωμένος χρόνος, κόστος και πολυπλοκότητα στην πρόσθεση νέων λειτουργιών και δυνατοτήτων.

4.3.1. Υπολογιστική ισχύς κατά παραγγελία

Η υπολογιστική ισχύς κατά παραγγελία (on-demand) είναι ένα όλο και πιο δημοφιλές μοντέλο των επιχειρήσεων στο οποίο οι υπολογιστικοί πόροι είναι στη διάθεση των χρηστών, όταν και μόνο όταν απαιτείται [109]. Οι υπολογιστικοί πόροι που διατηρούνται από την πλευρά του χρήστη γίνονται όλο και λιγότεροι, ενώ αυξάνονται αυτοί που διατηρούνται από τη μεριά του παρόχου. Το μοντέλο κατά παραγγελία

εξελίχθηκε, για να ξεπεραστεί η πρόκληση της αποτελεσματικής διαχείρισης των ζητούμενων πόρων. Λόγω του ότι η ζήτηση για υπολογιστικούς πόρους μπορεί να διαφέρει δραματικά από τη μια στιγμή στην άλλη, η διατήρηση επαρκών πόρων για την κάλυψη των αναγκών σε περιόδους αιχμής είναι δαπανηρή. Από την άλλη, η επιλογή είναι να υπάρχουν μόνο οι ελάχιστοι υπολογιστικοί πόροι σε μια εταιρεία για να μειωθεί το κόστος είναι εξίσου αρνητική, μιας και θα οδηγήσει με μαθηματική ακρίβεια σε ανεπαρκείς υπολογιστικούς πόρους, όταν είναι ανάγκη, όταν δηλαδή υπάρχει μεγάλος φόρτος εργασίας. Έννοιες όπως υπολογιστική συστάδα (clustered computing), υπολογιστικό πλέγμα (grid computing), παροχή υπολογιστικής ισχύος (utility computing) κτλ, μπορεί να φαίνονται παρόμοιες με τον όρο υπολογιστική ισχύ κατά παραγγελία, παρόλα αυτά δεν σημαίνουν το ίδιο. Θα μπορούσαν να γίνουν όμως πιο κατανοητά, αν κάποιος τα θεωρούσε δομικούς λίθους, οι οποίοι στο πέρασμα του χρόνου και με την τεχνολογική επανάσταση βοήθησαν στην επίτευξη του μοντέλου υπολογιστικού νέφους, το οποίο χρησιμοποιούμε σήμερα.

Στην συνέχεια θα περιγράψουμε εν συντομία το EC2 (Elastic Compute Cloud) [50] του παρόχου Amazon με σκοπό την καλύτερη κατανόηση του όρου IaaS. Το EC2 είναι μια διαδικτυακή υπηρεσία, η οποία παρέχει υπολογιστική ισχύ δυναμικού μεγέθους στο υπολογιστικό νέφος. Σχεδιάστηκε ώστε να κάνει ευκολότερη την κλιμακωτή διάθεση πόρων στους προγραμματιστές και παρέχει πολλά πλεονεκτήματα στους πελάτες, όπως φαίνεται και ακολούθως:

- Είναι μια διαδικτυακή υπηρεσία, η οποία επιτρέπει στους πελάτες να αποκτήσουν και να ρυθμίσουν τη ζητούμενη υπολογιστική ισχύ με ελάχιστη προσπάθεια.
- Παρέχει στους χρήστες πλήρη έλεγχο των μισθωμένων υπολογιστικών πόρων τους και τους επιτρέπει να εκτελούν τις εφαρμογές τους σε ένα αξιόπιστο περιβάλλον.
- Μειώνει τον χρόνο που απαιτείται για την απόκτηση και εκκίνηση νέων στιγμιότυπων (instances) σε περίπου ένα λεπτό, επιτρέποντας στους πελάτες να αναβαθμίζουν

γρήγορα την υπολογιστή ισχύ ανάλογα με τις απαιτήσεις τους.

- Αλλάζει τις οικονομικές απαιτήσεις των υπολογιστών, επιτρέποντας στους πελάτες να πληρώνουν μόνο για την υπολογιστική ισχύ που πραγματικά χρησιμοποιούν.
- Παρέχει στους προγραμματιστές εργαλεία που απαιτούνται για να κατασκευάσουν εφαρμογές ανθεκτικές σε τυχόν αποτυχίες και τις απομονώνει από κοινά σενάρια αποτυχίας.

Το EC2 παρέχει ένα ρεαλιστικό εικονικό υπολογιστικό περιβάλλον, το οποίο επιτρέπει στους χρήστες να χρησιμοποιούν μια διαδικτυακή εφαρμογή, για να έχουν πρόσβαση και να διαχειρίζονται τις υπηρεσίες που χρειάζονται σε ένα ή περισσότερα στιγμιότυπα με ποικιλία από λειτουργικά συστήματα (Operating System - OS). Οι πελάτες μπορούν να φορτώνουν το περιβάλλον του λειτουργικού που θέλουν με τις δικές τους εφαρμογές. Μπορούν να διαχειρίζονται την πρόσβαση στο δίκτυο και, τέλος, να τρέχουν λίγα ή πολλά συστήματα ανάλογα με τις ανάγκες τους. Αποβλέποντας στη χρήση του EC2, οι χρήστες θα πρέπει πρώτα να δημιουργήσουν ένα Amazon Machine Image (AMI) [110]. Το AMI περιέχει τις εφαρμογές, τις βιβλιοθήκες, τα δεδομένα και τις σχετικές ρυθμίσεις διαμόρφωσης που χρησιμοποιούνται στο εικονικό υπολογιστικό περιβάλλον. Επίσης, η Amazon προσφέρει τη δυνατότητα χρήσης ήδη διαμορφωμένων περιβαλλόντων, σχεδιασμένα με πληθώρα προτύπων, με σκοπό την έναρξη και την άμεση λειτουργία τους. Από τη στιγμή που ο χρήστης έχει ορίσει και έχει ρυθμίσει το AMI του κάνοντας χρήση των εργαλείων του EC2 μπορεί να αποθηκεύσει το AMI στο Amazon S3 [08]. Το S3 είναι ένας αποθηκευτικός χώρος, ο οποίος παρέχει ασφαλή, αξιόπιστη και γρήγορη πρόσβαση στο AMI του πελάτη. Πριν ο πελάτης αρχίσει να χρησιμοποιεί το AMI, θα πρέπει πρώτα να χρησιμοποιήσει τη διαδικτυακή υπηρεσία του EC2 με σκοπό την διαμόρφωση της ασφάλειας και της πρόσβασης στο δίκτυο.

Κατά τη διάρκεια των ρυθμίσεων, ο χρήστης επιλέγει τι είδους στιγμιότυπο και λειτουργικό σύστημα θέλει να χρησιμοποιήσει. Υπάρχουν δύο διακριτές κατηγορίες στιγμιότυπων. Η βασική (standard)

κατηγορία και η υψηλής ΚΜΕ (high-CPU). Η πλειονότητα των εφαρμογών ταιριάζει καλύτερα σε βασικά στιγμιότυπα, τα οποία υπάρχουν σε μικρές, μεγάλες και πολύ μεγάλες πλατφόρμες. Τα στιγμιότυπα υψηλής ΚΜΕ έχουν αναλογικά περισσότερους πόρους ΚΜΕ από κεντρική μνήμη (Random Access Memory - RAM) και είναι κατάλληλα για εφαρμογές με υψηλές υπολογιστικές ανάγκες. Στην περίπτωση των στιγμιότυπων υψηλών ΚΜΕ υπάρχουν μεσαίες και πολύ μεγάλες πλατφόρμες υποστήριξης. Μετά από τον καθορισμό του στιγμιότυπου που θα χρησιμοποιηθεί, οι πελάτες μπορούν να ξεκινήσουν, να σταματήσουν και να παρακολουθούν όσα στιγμιότυπα θέλουν και χρειάζονται με τη χρήση διαδικτυακών διεπαφών προγραμματισμού εφαρμογών (Application Programming Interfaces - APIs) ή με ευρεία ποικιλία από άλλα εργαλεία διαχείρισης που παρέχονται από την υπηρεσία. Ο χρήστης έχει τη δυνατότητα να επιλέξει αν θέλει να τρέχει την εφαρμογή σε πολλαπλές τοποθεσίες, να χρησιμοποιεί στατικές IPs, ή να προσθέσει μόνιμο αποθηκευτικό χώρο σε κάποιο από τα στιγμιότυπα, και θα πληρώνει μόνο για όσα από τα προηγούμενα καταναλώνει. Επίσης, μπορεί να επιλέξει από μια βιβλιοθήκη από AMIs, τα οποία παρέχουν χρήσιμα στιγμιότυπα. Για παράδειγμα, αν το μόνο που χρειάζεται είναι ένας απλός διακομιστής που να τρέχει σε Linux, ο χρήστης μπορεί να επιλέξει μια τυπική διανομή AMI με Linux.

Επιπρόσθετα, υπάρχουν αρκετά χαρακτηριστικά του EC2, τα οποία παρέχουν σημαντικά οφέλη σε μια επιχείρηση. Πρώτα απ’ όλα, το EC2 παρέχει οικονομικά οφέλη. Εξαιτίας της μεγάλης πελατειακής βάσης και της δυνατότητας μαζικής λειτουργίας της Amazon, το EC2 είναι η πιο φθηνή λύση από άλλες πιθανές. Οι δαπάνες για τη δημιουργία και λειτουργία μιας εφαρμογής μοιράζεται από κοινού σε πολλούς πελάτες, καθιστώντας με αυτό τον τρόπο το συνολικό κόστος για τον καθένα από τους πελάτες πολύ χαμηλότερο από οποιαδήποτε άλλη εναλλακτική λύση. Οι πελάτες πληρώνουν ένα πολύ χαμηλό ποσοστό για την υπολογιστική ισχύ που πραγματικά καταναλώνουν. Επίσης, η ασφάλεια παρέχεται μέσω διαδικτυακών διεπαφών, οι οποίες επιτρέπουν τη ρύθμιση του τείχους ασφαλείας, τον έλεγχο για την πρόσβαση στο δίκτυο μεταξύ ομάδων ή στιγμιότυπων. Περισσότερα για την ασφάλεια θα αναφερθούν εκτενέστερα σε επόμενο κεφάλαιο. Τέλος, η Amazon

προσφέρει ένα πολύ αξιόπιστο περιβάλλον μέσα στο οποίο μπορούν να ανατροφοδοτηθούν αμέσως νέα στιγμιότυπα, έχοντας ανα πάσα στιγμή τις νέες ρυθμίσεις.

Το EC2 επιτρέπει στους χρήστες να αυξάνουν ή να μειώνουν την υπολογιστή ισχύ μέσα σε λίγα λεπτά. Οι χρήστες μπορούν να χρησιμοποιήσουν ένα στιγμιότυπο, εκατοντάδες ή ακόμα και χιλιάδες στιγμιότυπα ταυτόχρονα. Φυσικά, επειδή όλα αυτά είναι ελεγχόμενα από διαδικτυακές υπηρεσίες API, μια εφαρμογή μπορεί αυτόματα από μόνη της να αυξήσει η να μειώσει τις απαιτήσεις της σε πόρους ανάλογα με τις ανάγκες της. Αυτός ο τύπος της δυναμικής επεκτασιμότητας (dynamic scalability) είναι πολύ ελκυστικός για τους εταιρικούς πελάτες, επειδή τους επιτρέπει να αλληλεπιδρούν με τους πελάτες τους χωρίς να χρειάζεται να αναδομούν την υποδομή τους.

Οι χρήστες έχουν πλήρη έλεγχο στα στιγμιότυπά τους, καθώς έχουν πρόσβαση διαχειριστή σε καθένα από τα στιγμιότυπα και μπορούν να αλληλεπιδρούν μαζί τους, όπως θα έκαναν με ένα συμβατικό μηχάνημα στο γραφείο τους. Τα στιγμιότυπα μπορούν να επανεκκινηθούν εξ αποστάσεως μέσω διαδικτυακών υπηρεσιών API. Επίσης, οι χρήστες έχουν πρόσβαση στη γραμμή εντολών των στιγμιότυπων τους. Από τη στιγμή που ο χρήστης έχει ρυθμίσει τον λογαριασμό του και έχει ανεβάσει το AMI του στο S3 της Amazon, το μόνο που χρειάζεται να κάνει είναι να εκκινήσει ένα στιγμιότυπο.

Οι ρυθμίσεις διαμόρφωσης μπορεί να διαφέρουν σε μεγάλο βαθμό μεταξύ των χρηστών, καθώς έχουν την επιλογή πολλαπλών τύπων στιγμιότυπων, λειτουργικών συστημάτων και πακέτων λογισμικού. Το EC2 τους επιτρέπει να επιλέξουν μια διαμόρφωση για τη μνήμη, την ΚΜΕ καθώς και τον αποθηκευτικό χώρο των στιγμιότυπών τους, ούτως ώστε να είναι βέλτιστο για την επιλογή τους στο λειτουργικό σύστημα και τις εφαρμογές τους. Για παράδειγμα, η επιλογή του χρήστη για το λειτουργικό σύστημα μπορεί να περιλαμβάνει πολυάριθμες διανομές Linux, Microsoft Windows Server, OpenSolaris και όλα αυτά να τρέχουν σε εικονικούς διακομιστές.

Το EC2 λειτουργεί σε συνδυασμό με μια ποικιλία από άλλες διαδικτυακές υπηρεσίες της Amazon. Για παράδειγμα το S3 (Simple Storage Service), το SimpleDB, το SQS (Simple Queue Service) και το CloudFront είναι υπηρεσίες της Amazon, οι οποίες είναι ήδη ενσωματωμένες στο EC2 για να παρέχουν μια ολοκληρωμένη λύση στην πληροφορική, στην επεξεργασία επερωτήσεων σε βάσεις δεδομένων (query processing) και την αποθήκευση ενός ευρέους φάσματος εφαρμογών.

Πιο συγκεκριμένα, το S3 παρέχει διαδικτυακές υπηρεσίες, οι οποίες επιτρέπουν στους χρήστες να αποθηκεύουν και να ανακτούν οποιοδήποτε ποσό δεδομένων από το διαδίκτυο, οποιαδήποτε στιγμή και από οποιοδήποτε μέρος. Δίνει στους προγραμματιστές απευθείας πρόσβαση στην ίδια αποθηκευτική υποδομή που χρησιμοποιεί και η ίδια η Amazon για να τρέχει το ιδιωτικό της δίκτυο από ιστοσελίδες. Το S3 έχει σαν σκοπό να μεγιστοποιήσει τα οφέλη της κλιμάκωσης και να μεταφέρει αυτά τα οφέλη στους προγραμματιστές.

Η SimpleDB [111] είναι άλλη μια διαδικτυακή υπηρεσία, σχεδιασμένη να τρέχει σε πραγματικό χρόνο επερωτήσεις σε δομημένα δεδομένα, τα οποία είναι αποθηκευμένα στο S3. Η συγκεκριμένη υπηρεσία λειτουργεί σε συνδυασμό με το EC2, με στόχο την παροχή στους χρήστες της δυνατότητας να αποθηκεύουν, να επεξεργάζονται και να επερωτούν σύνολα δεδομένων εντός του περιβάλλοντος του υπολογιστικού νέφους. Παραδοσιακά, ο συγκεκριμένος τύπος λειτουργικότητας παρέχονταν με την χρήση συστάδας σχεσιακής βάσης δεδομένων (Clustered Relational DataBase – C-RDB) [112], γεγονός που θα απαιτούσε μια αξιοσέβαστη επένδυση. Όμως, τέτοιου είδους εφαρμογές επέφεραν μεγαλύτερη πολυπλοκότητα στο κέντρο δεδομένων μια εταιρείας και συχνά ήταν επιτακτική η συνδρομή ενός διαχειριστή στη βάση δεδομένων. Σε σύγκριση με τις παραδοσιακές προσεγγίσεις, το SimpleDB είναι πολύ εύκολο στη χρήση και παρέχει τη βασική λειτουργικότητα μιας βάσης δεδομένων, δηλαδή αναζήτηση σε πραγματικό χρόνο και επερωτήσεις επί των δομημένων δεδομένων, χωρίς να έχει συμπεριλάβει την επιχειρησιακή πολυπλοκότητα που εμπλεκόταν στις παραδοσιακές υλοποιήσεις. Επιπρόσθετα, δεν

απαιτείται μορφοποίηση στη βάση δεδομένων γιατί δεικτοδοτεί αυτόματα τα δεδομένα και παρέχει ένα απλό API τόσο για την αποθήκευση όσο και για την πρόσβαση σε αυτά. Αυτό εξαλείφει την ανάγκη των πελατών να εκτελούν καθήκοντα, όπως μοντελοποίηση των δεδομένων διατήρηση των δεικτών και βελτιστοποίηση των επιδόσεων.

Η υπηρεσία SQS [113] είναι μια αξιόπιστη ουρά για αποθήκευση μηνυμάτων όπως περνούν μεταξύ των υπολογιστών. Με την χρήση του SQS, οι προγραμματιστές είναι σε θέση να μετακινούν δεδομένα μεταξύ κατανεμημένων επιμέρους συστατικών των εφαρμογών, οι οποίες επιτελούν διαφορετικές εργασίες, χωρίς να χαθούν τα μηνύματα ή να χρειάζεται 100% διαθεσιμότητα για καθένα από τα συστατικά. Το SQS λειτουργεί με τη διάθεση ως υπηρεσία του συστήματος μηνυμάτων που χρησιμοποιεί η ίδια η Amazon. Οποιοσδήποτε υπολογιστής που είναι συνδεδεμένος στο διαδίκτυο μπορεί να προσθέτει ή να διαβάζει μηνύματα χωρίς την ανάγκη χρήσης ειδικού λογισμικού ή ειδικές ρυθμίσεις στο τείχος προστασίας του. Τα επιμέρους συστατικά των εφαρμογών που χρησιμοποιούν το SQS μπορούν να τρέχουν ανεξάρτητα το ένα από το άλλο και δεν είναι ανάγκη να βρίσκονται στο ίδιο δίκτυο, να έχουν γραφτεί με την ίδια τεχνολογία ή και να τρέχουν την ίδια στιγμή.

Η υπηρεσία CloudFront είναι μια διαδικτυακή υπηρεσία για διανομή δεδομένων [114]. Είναι ενσωματωμένη στις άλλες διαδικτυακές υπηρεσίες της Amazon με σκοπό τη διανομή δεδομένων στους τελικούς χρήστες με χαμηλή καθυστέρηση και υψηλές ταχύτητες μετάδοσης δεδομένων. Το CloudFront διανέμει τα δεδομένα κάνοντας χρήση ενός παγκόσμιου δικτύου από τοποθεσίες ως θέσεις. Οι αιτήσεις για αντικείμενα ή δεδομένα δρομολογούνται αυτόματα στον κοντινότερο διακομιστή θέσης ούτως ώστε το αποτέλεσμα της αίτησης να διανεμηθεί στο χρήστη με την καλύτερη δυνατή απόδοση. Ο διακομιστής θέσης παραλαμβάνει την αίτηση από τον υπολογιστή του χρήστη και δημιουργεί μια σύνδεση με έναν άλλο υπολογιστή, τον διακομιστή εκτέλεσης, όπου και παραμένει η αίτηση. Όταν ο διακομιστής ικανοποιήσει το αίτημα, αποστέλλει πίσω στον διακομιστή θέσης τα δεδομένα που προέκυψαν και αυτός με τη σειρά του τα προωθεί στον υπολογιστή του πελάτη που έκανε το αίτημα.

Ένα βασικό χαρακτηριστικό του EC2 είναι το EBS (Elastic Block Store) [115]. Το EBS παρέχει στους χρήστες ισχυρά χαρακτηριστικά για να χτίσουν εφαρμογές ανθεκτικές σε αποτυχίες. Προσφέρει σταθερό αποθηκευτικό χώρο για τα στιγμιότυπα EC2. Επίσης, έχει τη δυνατότητα για παροχή αποθηκευτικού χώρου εκτός του στιγμιότυπου, δηλαδή χώρο που συνεχίζει να υφίσταται και μετά το πέρας του στιγμιότυπου. Το EBS προσφέρει υψηλά επίπεδα διαθεσιμότητας και αξιοπιστίας και μπορεί να συνδεθεί σε ένα EC2 που λειτουργεί και να θεωρεί ως εξ ορισμού συσκευή αποθήκευσης σε κάποιο στιγμιότυπο. Επιπλέον, δίνει τη δυνατότητα στους παρόχους υπηρεσιών να δημιουργούν προσωρινά αντίγραφα των δεδομένων τους, τα οποία αποθηκεύονται μέσω του S3. Τα συγκεκριμένα αντίγραφα μπορούν να χρησιμοποιηθούν ως δεδομένα έναρξης για νέα στιγμιότυπα και έτσι να προστατεύονται πιο αποτελεσματικά τα δεδομένα του χρήστη.

Το EC2 παρέχει στους χρήστες τη δυνατότητα να τοποθετούν ένα ή περισσότερα στιγμιότυπα σε πολλαπλές τοποθεσίες. Οι τοποθεσίες του EC2 αποτελούνται από περιφέρειες (region), όπως για παράδειγμα Βόρεια Αμερική ή Ευρώπη, και ζώνες διαθεσιμότητας (availability zones). Οι περιφέρειες αποτελούνται από μία η περισσότερες ζώνες διαθεσιμότητας, είναι σε γεωγραφική διασπορά και βρίσκονται σε διαφορετικές γεωγραφικές περιοχές ή χώρες. Οι ζώνες διαθεσιμότητας είναι διακριτές τοποθεσίες, οι οποίες έχουν κατασκευαστεί, ώστε να διαχωρίζονται από αποτυχίες άλλων ζωνών διαθεσιμότητας και παρέχουν φθηνή και γρήγορη σύνδεση δικτύου με άλλες ζώνες διαθεσιμότητας στην ίδια περιφέρεια. Για παράδειγμα, η περιφέρεια της Βόρειας Αμερικής μπορεί να χωριστεί στις ακόλουθες ζώνες διαθεσιμότητας: Βορειοανατολική, Ανατολική, Νοτιοανατολική, Βορειοκεντρική, Κεντρική, Νοτιοκεντρική κτλ. Εκκινώντας στιγμιότυπα σε μία ή περισσότερες από τις επιμέρους ζώνες διαθεσιμότητας, ο χρήστης μπορεί να απομονώσει την εφαρμογή του από μοναδικά σημεία αποτυχίας. Το EC2 προσφέρει συμβόλαια παροχής υπηρεσιών, τα οποία παρέχουν μέχρι και 99.95% διαθεσιμότητα χρόνου λειτουργίας για κάθε ξεχωριστή περιφέρεια.

Οι ευέλικτες διευθύνσεις IP (Elastic IP - EIP) είναι στατικές διευθύνσεις IP, οι οποίες έχουν σχεδιαστεί για το υπολογιστικό νέφος. Καθώς μια EIP συνδέεται με ένα λογαριασμό και όχι με ένα συγκεκριμένο στιγμιότυπο, ο χρήστης ελέγχει τη συγκεκριμένη διεύθυνση μέχρι να αποφασίσει ο ίδιος να την αποδεσμεύσει. Σε αντίθεση με τις παραδοσιακές διευθύνσεις IP, οι διευθύνσεις EIP επιτρέπουν στους χρήστες να προλαμβάνουν τυχόν αποτυχίες με το να αναδρομολογούν την IP τους από το στιγμιότυπο που προέκυψε κάποιο πρόβλημα σε ένα άλλο, λειτουργικό. Αντί να περιμένουν κάποιο τεχνικό να αναριθμήσει ή το DNS να μεταδώσει σε όλους τους χρήστες του τη νέα IP, το EC2 επιτρέπει να γίνεται αναδρομολόγηση των διευθύνσεων EIP σε άλλο στιγμιότυπο. Το βασικότερο χαρακτηριστικό των διευθύνσεων EIP είναι ότι, όταν παραστεί ανάγκη, κάθε διεύθυνση IP μπορεί να επανεκχωρηθεί σε άλλο στιγμιότυπο, χωρίς να προκύψει κανένα απολύτως πρόβλημα στην όλη λειτουργία της εφαρμογής. Στη συνέχεια θα δούμε πώς λειτουργεί η διευθυνσιοδότηση EIP με τις υπηρεσίες του EC2.

Αρχικά, η Amazon επιτρέπει ως προεπιλογή στους χρήστες της να διαθέτουν μέχρι πέντε διευθύνσεις EIP ανά λογαριασμό. Καθεμία από τις πέντε EIPs μπορεί να ανατεθεί μόνο σε ένα στιγμιότυπο. Όταν συμβαίνει η αναδρομολόγηση, αντικαθιστάται η δυναμική IP που χρησιμοποιούνταν από το συγκεκριμένο στιγμιότυπο. Εξ ορισμού, κάθε στιγμιότυπο ξεκινά τη λειτουργία του με μια δυναμική IP, η οποία του παραχωρείται κατά την εκκίνησή του. Από τη στιγμή που κάθε στιγμιότυπο μπορεί να έχει μόνο μία εξωτερική διεύθυνση IP, αυτό ξεκινά κάνοντας χρήση της προεπιλεγμένης δυναμικής IP. Αν η EIP που χρησιμοποιείται έχει παραχωρηθεί σε άλλο στιγμιότυπο, τότε δίνεται στο νέο στιγμιότυπο μια νέα διεύθυνση IP. Για να γίνει η παραχώρηση ή η αναδρομολόγηση μιας EIP σε ένα στιγμιότυπο χρειάζονται μόνο μερικά λεπτά. Ο περιορισμός του σχεδιασμού μιας μοναδικής IP για όλα τα στιγμιότυπα του χρήστη συμβαίνει λόγω του τρόπου λειτουργίας του Network Address Translation (NAT) [116]. Αν δύο εξωτερικές διευθύνσεις IP τύχει να μεταφραστούν στην ίδια εσωτερική διεύθυνση IP, όλη η κίνηση σε μορφή πακέτων δεδομένων θα εκτελεστεί χωρίς κανένα πρόβλημα. Ωστόσο, η παραχώρηση των πακέτων εξόδου σε μια εξωτερική διεύθυνση IP θα ήταν πολύ δύσκολη, γιατί δεν θα ήταν

εφικτός ο καθορισμός της συγκεκριμένης εξωτερικής διεύθυνσης. Αυτός είναι και ο λόγος για τον οποίο οι κατασκευαστές έχουν επιβάλλει τον περιορισμό μιας μοναδικής εξωτερικής διεύθυνσης IP ανά στιγμιότυπο στη μονάδα του χρόνου.

4.4. Monitoring-as-a-Service

Ο έλεγχος-ως-υπηρεσία (Monitoring-as-a-Service – MaaS) είναι η εξωτερική τροφοδότηση ασφάλειας, κυρίως στις πλατφόρμες εκείνων των επιχειρήσεων, οι οποίες αξιοποιούν το διαδίκτυο για την άσκηση των δραστηριοτήτων τους [117]. Το MaaS είχε γίνει όλο και πιο δημοφιλές κατά την δεκαετία του 2000, ενώ με την έλευση του υπολογιστικού νέφους, η δημοτικότητα του αυξήθηκε ακόμα περισσότερο. Η παρακολούθηση της ασφάλειας περιλαμβάνει προστασία της επιχείρησης ή του κυβερνητικού οργανισμού από απειλές στον κυβερνοχώρο. Η ομάδα ασφάλειας διαδραματίζει καίριο ρόλο στη διασφάλιση και διατήρηση της εμπιστευτικότητας (Confidentiality), της ακεραιότητας (Integrity) και της διαθεσιμότητας (Availability) των υπολογιστικών στοιχείων. Ωστόσο, περιορισμοί στον χρόνο και στους πόρους εμποδίζουν τις λειτουργίες ασφάλειας και την αποτελεσματικότητά τους για τις περισσότερες εταιρείες. Αυτό απαιτεί συνεχή επαγρύπνηση πάνω στην υποδομή ασφάλειας για τα κρίσιμα υπολογιστικά στοιχεία της εταιρείας.

Πολλοί κανονισμοί που υπάρχουν σε βιομηχανικό επίπεδο απαιτούν από τις εταιρείες να ελέγχουν το περιβάλλον ασφάλειάς τους, τα αρχεία καταγραφής συμβάντων των διακομιστών, καθώς και άλλα υπολογιστικά στοιχεία, με σκοπό τη διασφάλιση της ασφάλειας των κρίσιμων υπολογιστικών στοιχείων της εταιρείας. Ωστόσο, η αποτελεσματική παρακολούθηση της ασφάλειας είναι ένα δύσκολο έργο, επειδή απαιτούνται προηγμένη τεχνολογία, ειδικευμένοι εμπειρογνώμονες ασφάλειας και κλιμακούμενες διαδικασίες, κανένα από τα οποία δεν είναι οικονομικό. Οι παροχές ασφάλειας του MaaS προσφέρουν παρακολούθηση της ασφάλειας σε πραγματικό χρόνο, εικοσιτέσσερις ώρες την ημέρα, επτά ημέρες την βδομάδα και σχεδόν

άμεση ανταπόκριση σε κάποιο συμβάν πάνω σε μια υποδομή ασφάλειας προστατεύοντας τα ευαίσθητα δεδομένα των πελατών. Πριν την έλευση των ηλεκτρονικών συστημάτων ασφαλείας, η παρακολούθηση της ασφάλειας, καθώς και της ανταπόκρισης ήταν σε μεγάλο βαθμό εξαρτώμενες από ανθρώπινους πόρους και ικανότητες, γεγονός που περιόριζε την ακρίβεια και την αποτελεσματικότητα των προσπαθειών παρακολούθησης της ασφάλειας. Κατά τις δύο τελευταίες δεκαετίες, η υιοθέτηση της πληροφορικής στα συστήματα ασφαλείας και η ικανότητά τους να συνδέονται με κέντρα λειτουργιών ασφάλειας (Security Operation Centers – SOCs) μέσω εταιρικών δικτύων [118], έχει αλλάξει σημαντικά αυτή την εικόνα. Αυτό σημαίνει δύο σημαντικά πράγματα. Αφενός, το συνολικό κόστος της ιδιοκτησίας των παραδοσιακών SOCs είναι πολύ μεγαλύτερο από τα μοντέρνα SOCs. Αφετέρου, η επίτευξη χαμηλότερου κόστους σε λειτουργικά θέματα ασφάλειας καθώς και η μεγαλύτερη αποτελεσματικότητα στην ασφάλεια σημαίνει ότι η σύγχρονη αρχιτεκτονική SOC θα πρέπει να χρησιμοποιήσει την τεχνολογία της πληροφορικής για την αντιμετώπιση των κινδύνων της ασφάλειας.

Οι υπηρεσίες ασφάλειας οι οποίες είναι βασισμένες σε SOC, μπορούν να βελτιώσουν την αποδοτικότητα της υποδομής ασφάλειας των πελατών με την ενεργή ανάλυση των αρχείων καταγραφής συμβάντων, καθώς και των προειδοποιήσεων από τις συσκευές της υποδομής σε πραγματικό χρόνο. Οι ομάδες ασφάλειας συσχετίζουν τις πληροφορίες από διάφορες συσκευές ασφάλειας, για να παρέχουν στους αναλυτές ασφάλειας τα δεδομένα που χρειάζονται για την εξάλειψη των ψευδών απειλών και την άμεση ανταπόκριση στις αληθείς απειλές ενάντια στον οργανισμό. Διασφαλίζοντας συνεπή πρόσβαση στις δεξιότητες που απαιτούνται, για να διατηρηθεί το επίπεδο των υπηρεσιών, μια εταιρεία έρχεται αντιμέτωπη με το τεράστιο θέμα της παρακολούθησης της ασφάλειας σε επίπεδο επιχείρησης. Η ομάδα ασφάλειας μπορεί να αξιολογήσει περιοδικά την απόδοση του συστήματος και να παρέχει συστάσεις για βελτιώσεις, όταν θεωρηθεί αναγκαίο. Στις παραγράφους που ακολουθούν θα αναφερθούν οι υπηρεσίες που παρέχονται από ένα τυπικό πάροχο MaaS.

Αρχικά, ο πάροχος MaaS διαθέτει την υπηρεσία άμεσης ανίχνευσης. Η συγκεκριμένη υπηρεσία εντοπίζει και αναφέρει τα νέα τρωτά σημεία που προκύπτουν στην ασφάλεια αμέσως μόλις εντοπιστούν. Σε γενικές γραμμές, οι απειλές αυτές συσχετίζονται με προγράμματα που προέρχονται από τρίτους και σε αυτή την περίπτωση καταγράφεται και αποστέλλεται μια έκθεση προειδοποίησης ή αναφορά στον πελάτη. Η συγκεκριμένη έκθεση αποστέλλεται συνήθως μέσω ηλεκτρονικού ταχυδρομείου στον υπεύθυνο ασφάλειας της εταιρείας. Οι εκθέσεις ασφάλειας σχετικά με τις ευπάθειες του πληροφοριακού συστήματος, εκτός από το να περιέχουν μια λεπτομερή περιγραφή της συγκεκριμένης ευπάθειας καθώς και τα επιμέρους συστήματα που επηρεάζονται, περιλαμβάνουν, επίσης, πληροφορίες σχετικές με τις επιπτώσεις που η συγκεκριμένη ευπάθεια θα μπορούσε να επιφέρει στα συστήματα πριν την εύρεση, την καταγραφή και την εξόντωσή της. Επίσης, τις περισσότερες φορές η έκθεση επισημαίνει συγκεκριμένες ενέργειες στις οποίες η εταιρεία θα πρέπει να προβεί για την ελαχιστοποίηση της επίδρασης της ευπάθειας.

Συνεχίζοντας, ο πάροχος MaaS προσφέρει την υπηρεσία ελέγχου της ασφάλειας, δηλαδή του γενικότερου ελέγχου της εφαρμογής και της υποδομής. Η υπηρεσία αυτή υλοποιείται μέσω μιας διεπαφής που προσφέρει, εκτός από λεπτομερή καταγραφή ανά πάσα στιγμή της κατάστασης των επιμέρους στοιχείων, τον γενικότερο έλεγχο της κατάστασης λειτουργίας όλης της πλατφόρμας. Αυτή είναι προσβάσιμη μέσω διαδικτύου, καθιστώντας έτσι δυνατή την απομακρυσμένη πρόσβαση στην υποδομή. Καθένα από τα λειτουργικά στοιχεία που ελέγχεται συνήθως παρέχει ένα δείκτη λειτουργικότητας, λαμβάνοντας υπόψη τον βαθμό επίδρασης του συγκεκριμένου στοιχείου σε όλη την υποδομή. Επίσης, η συγκεκριμένη υπηρεσία στοχεύσει στο να καθορίσει ποια στοιχεία λειτουργούν κοντά ή πάνω από τα όρια, σύμφωνα με τις δοθείσες παραμέτρους του συστήματος. Με τον προσδιορισμό και την αναγνώριση τέτοιου είδους προβλημάτων, είναι δυνατό να ληφθούν αποτρεπτικά μέτρα ώστε να αποφευχθεί η απώλεια λειτουργίας της εφαρμογής.

Μια ακόμα υπηρεσία του MaaS είναι η ευφυής συγκέντρωση και ανάλυση των δεδομένων από τα αρχεία καταγραφής συμβάντων. Μια τέτοιου είδους ανάλυση βοηθά στη δημιουργία μιας βάσης λειτουργικών επιδόσεων και παρέχει ένα δείκτη των πιθανών απειλών για την ασφάλεια, ανάλογα με τις παραμέτρους που υπάρχουν. Σε περίπτωση που κάποιο συμβάν ξεπεράσει τις δόκιμες επιδόσεις και οι παράμετροι εμπίπτουν σε κάποια κατηγορία απειλής, ειδοποιείται η ομάδα ασφάλειας, για να επιληφθεί της κατάστασης. Τα συγκεκριμένα εργαλεία χρησιμοποιούνται από ειδικούς στην ασφάλεια, οι οποίοι είναι υπεύθυνοι για την άμεση ανταπόκριση στην ευπάθεια που προκύπτει με σκοπό την εξουδετέρωσή της.

Η ανίχνευση και η διαχείριση της ευπάθειας επιβάλλει αυτοματοποιημένο έλεγχο και διαχείριση του επιπέδου ασφάλειας των πληροφοριακών συστημάτων. Η υπηρεσία αυτή, ανά τακτά χρονικά διαστήματα διεξάγει μια σειρά από αυτοματοποιημένα τεστ με σκοπό την ανίχνευση αδυναμιών του συστήματος, οι οποίες μπορούν να εκτίθενται και στο διαδίκτυο, συμπεριλαμβανομένων της πιθανότητας της μη εξουσιοδοτημένης πρόσβασης σε περιβάλλον διαχειριστή συστήματος, της ύπαρξης υπηρεσιών που δεν έχουν ενημερωθεί με τις νέες εκδόσεις τους και, τέλος, του προσδιορισμού ευπαθειών που έχουν να κάνουν με γενικές απειλές, όπως π.χ. phishing. Επίσης, η υπηρεσία αυτή εκτελεί περιοδικές παρακολουθήσεις των εργασιών που εκτελούνται από ειδικούς, οι οποίοι διαχειρίζονται την ασφάλεια του συστήματος και παρέχει αναφορές, οι οποίες μπορεί να χρησιμοποιηθούν για την εφαρμογή ενός σχεδίου με στόχο τη συνεχή βελτίωση του επιπέδου ασφάλειας του συστήματος.

Το θέμα της ασφάλειας είναι επιφορτισμένο με τη συνεχή επιδιόρθωση και αναβάθμιση τόσο του συστήματος όσο και των εφαρμογών του. Νέες αναβαθμίσεις στο λειτουργικό σύστημα είναι απαραίτητες, ώστε να διατηρείται η ασφάλεια σε επαρκή επίπεδα και να είναι σε θέση να υποστηρίξει νέες εκδόσεις των εγκατεστημένων εφαρμογών. Η παρακολούθηση όλων των αλλαγών στο λογισμικό και το υλικό απαιτεί μεθοδευμένη προσπάθεια, ώστε να είναι πάντα

ενημερωμένα και με αυτό τον τρόπο να καλύπτονται τα κενά ασφάλειας που προκύπτουν.

Όταν εντοπιστεί μια απειλή, η άμεση παρέμβαση είναι καίριας σημασίας για τη μείωση των επιπτώσεων της απειλής. Αυτό απαιτεί ειδικούς ασφάλειας με μεγάλη γνώση διάφορων τεχνολογιών και τη δυνατότητα να υποστηρίζουν εφαρμογές, καθώς και την υποδομή σε εικοσιτετράωρη βάση, επτά ημέρες την εβδομάδα. Το MaaS εξ ορισμού παρέχει τη συγκεκριμένη υπηρεσία στους πελάτες του. Όταν εντοπιστεί μια απειλή, αρχικά αναλύεται, συνήθως με τη βοήθεια ερευνητών εγκληματολογικών ερευνών, ώστε να καθοριστεί τι ακριβώς είναι, το πώς λειτουργεί και τι θα πρέπει να γίνει, ώστε να διορθωθεί το πρόβλημα το συντομότερο δυνατόν. Όταν προκύπτει ένα πρόβλημα, το πρώτο πράγμα που κάνει ο πελάτης είναι να πάρει τηλέφωνο τον διαχειριστή MaaS και να του ζητήσει βοήθεια. Υπάρχουν ειδικές υπηρεσίες για κάθε πάροχο MaaS, οι οποίες παρέχουν βοήθεια σε ερωτήσεις ή θέματα που προκύπτουν σχετικά με την ασφάλεια των συστημάτων και την άμεση εύρεση λύσης.

Οι υπηρεσίες ελέγχου της ασφάλειας μπορεί επίσης να βοηθήσουν τους πελάτες να συμμορφώνονται με τους γενικούς κανονισμούς ασφάλειας με την αυτοματοποιημένη συλλογή και υποβολή συγκεκριμένων συμβάντων που έχουν ενδιαφέρον, όπως για παράδειγμα αποτυχίες κατά την είσοδο με διαπιστευτήρια. Οι κανονισμοί και οι κατευθυντήριες γραμμές των γενικών κανονισμών ασφάλειας απαιτούν συχνά τον έλεγχο των αρχείων καταγραφής συμβάντων κρίσιμων διακομιστών για να διασφαλίζεται η ακεραιότητα και η εμπιστευτικότητα των δεδομένων.

4.5. Platform-as-a-Service

Το υπολογιστικό νέφος έχει επίσης εξελιχθεί, ώστε να περιλαμβάνει ειδικές πλατφόρμες για τη δημιουργία και λειτουργία διάφορων διαδικτυακών εφαρμογών, όρος γνωστός ως Πλατφόρμα-ως-υπηρεσία (Platform-as-a-Service – PaaS) [99, 117]. Σε αντίθεση με το IaaS,

ο πελάτης δεν έχει σχέση με την υποδομή καθώς και το υποκείμενο λειτουργικό που χρησιμοποιεί. Το μοντέλο PaaS είναι μια φυσική συνέχεια του μοντέλου SaaS. Το συγκεκριμένο μοντέλο παρέχει όλες τις λειτουργίες που απαιτούνται για την υποστήριξη του πλήρους κύκλου ζωής της δημιουργίας και παροχής μιας διαδικτυακής εφαρμογής, καθώς και υπηρεσιών διαθέσιμων αποκλειστικά από το διαδίκτυο. Όλα αυτά διαδραματίζονται χωρίς να απαιτείται λήψη ή εγκατάσταση κάποιου λογισμικού για τους διαχειριστές ή τους τελικούς χρήστες. Σε αντίθεση με το μοντέλο IaaS, στο οποίο οι προγραμματιστές δημιουργούν ένα στιγμιότυπο με ένα συγκεκριμένο λειτουργικό σύστημα και τις εφαρμογές που χρειάζονται, οι προγραμματιστές του μοντέλου PaaS ενδιαφέρονται μόνο για την ανάπτυξη της εφαρμογής και όχι με το είδος του λειτουργικού που χρησιμοποιείται. Οι υπηρεσίες που προσφέρει το PaaS επιτρέπουν στους προγραμματιστές να επικεντρωθούν στον προγραμματισμό αντί στις σύνθετες υποδομές και στα διαδικαστικά. Οι εταιρείες μπορούν να ανακατευθύνουν ένα σημαντικό μέρος του προϋπολογισμού τους για τη δημιουργία εφαρμογών, οι οποίες θα προσφέρουν πραγματική αξία στην εταιρεία αντί να ανησυχούν για θέματα υποδομών και λογισμικού κατασκευάζοντας ένα ιδιόκτητο πληροφοριακό σύστημα. Κατ' αυτόν τον τρόπο, το PaaS οδηγεί σε μια νέα εποχή μαζικής καινοτομίας δίνοντας στους προγραμματιστές ανά τον κόσμο τη δυνατότητα να έχουν πρόσβαση σε απεριόριστη υπολογιστική ισχύ. Ο οποιοσδήποτε που έχει μια σύνδεση στο διαδίκτυο μπορεί να δημιουργήσει ισχυρές εφαρμογές και να τις μεταπωλήσει ως υπηρεσία σε άλλους χρήστες παγκοσμίως.

Η παραδοσιακή προσέγγιση της κατασκευής και λειτουργίας κατά παραγγελία εφαρμογών (on premises) ήταν πάντα δύσκολη, ακριβή και είχε σημαντικό ρίσκο. Η δημιουργία μιας τέτοιας λύσης δεν προσφέρει καμιά εγγύηση επιτυχίας. Κάθε εφαρμογή σχεδιαζόταν για να καλύψει συγκεκριμένες απαιτήσεις των εταιρειών. Κάθε λύση απαιτούσε ένα σύνολο από υλικό, λειτουργικό σύστημα, βάση δεδομένων, διακομιστές ηλεκτρονικής αλληλογραφίας, διακομιστές παροχής διαδικτυακού περιεχομένου κτλ. Από τη στιγμή που διαμορφωνόταν το περιβάλλον από άποψης υλικού και λογισμικού, μια ομάδα από προγραμματιστές έπρεπε να κατασκευάσει περίπλοκες πλατφόρμες και πάνω σε αυτές να

δομήσουν τις εφαρμογές. Επιπροσθέτως, στην ομάδα έπρεπε να προστεθεί ειδικός για τη διαχείριση της βάσης δεδομένων, ειδικός για τη διαχείριση του δικτύου, καθώς και ειδικός ασφάλειας με σκοπό την ομαλή λειτουργία όλου του συστήματος. Αναπόφευκτα, η επιχείρηση κάποια στιγμή θα απαιτούσε από τους προγραμματιστές να κάνουν κάποια αλλαγή στην εφαρμογή. Η νέα εφαρμογή θα έπρεπε να ελεγχθεί από όλους τους προηγούμενους ειδικούς, ανά κλάδο, πριν διανεμηθεί προς χρήση. Επίσης, μεγάλες εταιρείες χρειάζονταν ειδικές εγκαταστάσεις για να τοποθετήσουν τα κέντρα δεδομένων τους. Ως εκ τούτου, δαπανώνταν τεράστιες ποσότητες ηλεκτρικής ενέργειας τόσο για τη λειτουργία των διακομιστών του πληροφοριακού συστήματος, όσο και για τη διατήρηση της θερμοκρασίας σε χαμηλά επίπεδα. Τέλος, όλα τα προηγούμενα απαιτούσαν τη δημιουργία εφεδρικού συστήματος ούτως ώστε να λειτουργήσει το συντομότερο δυνατόν και χωρίς απώλειες το πληροφοριακό σύστημα σε περίπτωση κάποιας καταστροφής.

Σε αντίθεση με όλα όσα αναφέρθηκαν στην προηγούμενη παράγραφο, το PaaS προσφέρει μια γρήγορη, οικονομική και αξιόπιστη πλατφόρμα για τη δημιουργία και διανομή μιας εφαρμογής. Το PaaS προσφέρει όλη την υποδομή που χρειάζεται, ώστε να τρέχουν οι εφαρμογές μέσω διαδικτύου. Παραδείγματα τέτοιων εφαρμογών είναι εταιρείες, όπως η Amazon [43], το eBay [119] , η Google [17], το iTunes [120], το YouTube [121] κτλ. Το συγκεκριμένο μοντέλο του υπολογιστικού νέφους κατέστησε δυνατή την παροχή των εν λόγω νέων δυνατοτήτων σε νέες αγορές μόνο μέσω του προγράμματος περιήγησης (browser). Το PaaS βασίζεται τόσο στο κλασικό μοντέλο κατανάλωσης πόρων, ώστε οι χρήστες να πληρώνουν μόνο ό,τι χρησιμοποιούν όσο και στη μηναία συνδρομή των χρηστών. Στις παροχές του PaaS περιλαμβάνονται τα σχεδιαγράμματα ροής δεδομένων για σχεδιασμό εφαρμογών, η ανάπτυξη, η εγκατάσταση, ο έλεγχος και ο διαμοιρασμός των εφαρμογών, όπως επίσης και οι υπηρεσίες ολοκληρωμένων εφαρμογών, όπως για παράδειγμα εικονικές εφαρμογές γραφείου, ομαδική εργασία και συνεργασία, ολοκλήρωση της βάσης δεδομένων, ασφάλεια, επεκτασιμότητα, αποθήκευση των δεδομένων και, τέλος, διαχείριση της εφαρμογής μέσω διαδικτύου.

Στα βασικά χαρακτηριστικά του PaaS περιλαμβάνονται οι υπηρεσίες για ανάπτυξη, ο έλεγχος, η παραμετροποίηση και η διανομή εφαρμογών με σκοπό την υποστήριξη του κύκλου ζωής της εφαρμογής. Διάφορα διαδικτυακά εργαλεία κατασκευής τυπικά παρέχουν ένα επίπεδο υποστήριξης για την απλοποίηση της δημιουργίας των διεπαφών των χρηστών και είναι βασισμένα είτε σε κοινά πρότυπα, όπως για παράδειγμα HTML και JavaScript ή σε άλλες νέες τεχνολογίες. Η υποστήριξη μιας αρχιτεκτονικής πολλαπλής μίσθωσης βοηθά στην εξάλειψη των ανησυχιών σχετικά με τη χρήση της εφαρμογής από πολλούς χρήστες ταυτόχρονα. Οι πάροχοι PaaS συχνά συμπεριλαμβάνουν υπηρεσίες για τη διαχείριση του συγχρονισμού της εφαρμογής, την επεκτασιμότητά της, την αντιμετώπιση τυχόν αποτυχιών που θα προκύψουν και, τέλος, για την ασφάλειά της.

Ένα άλλο χαρακτηριστικό του PaaS είναι η εύκολη ενοποίηση με διαδικτυακές υπηρεσίες και βάσεις δεδομένων. Η υποστήριξη του SOAP (Simple Object Access Protocol) [92] καθώς και άλλων διαθέσιμων τεχνικών επιτρέπουν στις εφαρμογές PaaS να δημιουργούν συνδυασμούς από διαδικτυακές υπηρεσίες, καθώς και να έχουν τη δυνατότητα να αποκτούν πρόσβαση σε βάσεις δεδομένων και σε άλλες υπηρεσίες που διατηρούνται στο εσωτερικό των ιδιωτικών δικτύων των εταιρειών.

Επίσης, η δυνατότητα συγγραφής, διαμόρφωσης και διαμοιρασμού κώδικα μέσω ομάδων διανομής κώδικα ενισχύει σημαντικά την παραγωγικότητα των προγραμματιστών PaaS. Οι ολοκληρωμένες λύσεις PaaS παρέχουν ευχέρεια στους προγραμματιστές να έχουν πολύ μεγαλύτερη διεισδυτικότητα στην εσωτερική λειτουργία των εφαρμογών και τη συμπεριφορά των χρηστών τους, με τη χρήση εργαλείων διαχείρισης μέσω των οποίων βλέπουν τις εσωτερικές διεργασίες της εφαρμογής που τρέχουν και διάφορες μετρήσεις, όπως η απόδοση, ο αριθμός των ταυτόχρονων προσβάσεων κτλ. Οι προηγούμενες μετρήσεις εκτός από τη βοήθεια που παρέχουν στους προγραμματιστές είναι και η βάση για το μοντέλο χρέωσης με βάση τη χρήση, το οποίο υιοθετείται από αρκετούς παρόχους PaaS.

4.6. Software-as-a-Service

Το παραδοσιακό μοντέλο διανομής λογισμικού, κατά το οποίο το λογισμικό αγοράζεται και εγκαθίσταται σε προσωπικούς υπολογιστές, ονομάζεται λογισμικό-ως-προϊόν (Software-as-a-Product). Το λογισμικό-ως-υπηρεσία (Software-as-a-Service – SaaS) [99, 117] είναι ένα μοντέλο διανομής λογισμικού κατά το οποίο οι εφαρμογές υπάρχουν σε ένα πάροχο και είναι διαθέσιμες στους πελάτες μέσω ενός δικτύου και γενικότερα μέσω του διαδικτύου. Το μοντέλο SaaS γίνεται ένα όλο και πιο διαδεδομένο μοντέλο παράδοσης, καθώς ωρίμασαν οι υποκείμενες τεχνολογίες που παρέχουν διαδικτυακές και SOA (Service Oriented Architectures) [122] υπηρεσίες και έγιναν δημοφιλείς νέες αναπτυξιακές μέθοδοι. Το SaaS συχνά συσχετίζεται με την καθ' οδόν πληρωμή συνδρομής για την άδεια χρήσης του μοντέλου, όπως ονομάζεται. Εν τω μεταξύ, η διαθεσιμότητα υπηρεσιών ευρυζωνικών δικτύων, που έχουν μπει στη καθημερινότητα των χρηστών, έδρασαν καταλυτικά στην ευρεία υιοθέτηση του SaaS.

Τα τεράστια άλματα που έγιναν από τους παρόχους διαδικτύου (Internet Service Provider - ISP) με σκοπό την αύξηση της ταχύτητας σύνδεσης και η συνεχής εισαγωγή ολοένα και ισχυρότερων μικροεπεξεργαστών σε συνδυασμό με τις φθηνές αποθηκευτικές συσκευές παρέχουν μια τεράστια πλατφόρμα για σχεδιασμό, ανάπτυξη και χρήση λογισμικού σε όλους τους τομείς των επιχειρήσεων και των προσωπικών υπολογιστών. Οι εφαρμογές του μοντέλου SaaS θα πρέπει επίσης να αλληλεπιδρούν με άλλα δεδομένα και εφαρμογές σε μια εξίσου μεγάλη ποικιλία από περιβάλλοντα και πλατφόρμες. Αξίζει να σημειωθεί ότι το SaaS είναι στενά συνδεδεμένο με τα μοντέλα του υπολογιστικού νέφους που έχουν περιγραφεί σε προηγούμενες παραγράφους. Η εταιρεία International Data Corporation (IDC) [123] ορίζει δύο ελαφρώς διαφορετικά μοντέλα SaaS. Το πρώτο ονομάζεται μοντέλο φιλοξενίας της διαχείρισης της εφαρμογής και είναι παρόμοιο με το μοντέλο παροχής υπηρεσιών εφαρμογών (Application Service Provider – ASP.NET) [124]. Σε αυτό το μοντέλο ένα ASP.NET φιλοξενεί εμπορικό λογισμικό για τους πελάτες του και τους το διανέμει μέσω διαδικτύου. Το δεύτερο μοντέλο ονομάζεται λογισμικό κατά παραγγελία

στο οποίο ο πάροχος δίνει μέσω διαδικτύου στους πελάτες του πρόσβαση σε ένα και μόνο αντίγραφο της εφαρμογής, η οποία έχει δημιουργηθεί αποκλειστικά και μόνο για διανομή μέσω SaaS.

Συχνά, το μοντέλο SaaS υλοποιείται, ώστε να παρέχει επαγγελματική λειτουργικότητα στους εταιρικούς πελάτες με το μικρότερο δυνατό κόστος, επιτρέποντας παράλληλα στους πελάτες να έχουν τα ίδια οφέλη με λογισμικό που έχουν αγοράσει επίσημα και λειτουργούν εντός της εταιρείας τους, χωρίς να χρειάζεται να το εγκαταστήσουν, να το διαχειρίζονται, να έχουν άδειες χρήσης και υψηλό αρχικό κόστος λειτουργίας. Η πλειονότητα των πελατών δεν γνωρίζουν το πως γίνεται η εγκατάσταση ή η παραμετροποίηση του λογισμικού, αλλά όλοι έχουν ανάγκη της χρήσης του στην εργασία τους. Πολλοί τύποι λογισμικού έχουν προσαρμοστεί αρκετά καλά στο μοντέλο SaaS, για παράδειγμα λογιστικά πακέτα, ηλεκτρονικό ταχυδρομείο, ασφάλεια εφαρμογών, διαχείριση περιεχομένου ιστοσελίδων κ.α. Η διάκριση μεταξύ SaaS και προηγούμενων εφαρμογών που διανέμονταν μέσω διαδικτύου είναι ότι οι λύσεις SaaS αναπτύχθηκαν για να λειτουργούν αποκλειστικά στο περιβάλλον του προγράμματος περιήγησης. Επίσης, η αρχιτεκτονική των εφαρμογών SaaS είναι σχεδιασμένη, ώστε να υποστηρίζει πολλούς χρήστες, μέσω της πολλαπλής μίσθωσης, ταυτόχρονα. Αυτή είναι και η μεγαλύτερη διαφορά μεταξύ των παραδοσιακών μοντέλων πελάτη/διακομιστή ή του ASP που προσέφεραν λύσεις οι οποίες απευθύνονταν σε ένα περιορισμένο κοινό και του SaaS. Από την άλλη μεριά, οι πάροχοι SaaS, προσφέρουν μεγάλα οικονομικά οφέλη για τη ρύθμιση, τη διαχείριση, την υποστήριξη και τη συντήρηση των υπηρεσιών που προσφέρουν.

Για την ανάπτυξη εφαρμογών SaaS χρησιμοποιούνται πολλά από τα συστατικά λογισμικού και πακέτα ανάπτυξης κώδικα. Κάνοντας χρήση της νέας τεχνολογίας που παρέχεται μέσα σε αυτά τα πακέτα μπορεί να μειωθεί δραματικά ο χρόνος μετατροπής των παραδοσιακών εφαρμογών σε προϊόντα SaaS. Σύμφωνα με την εταιρεία Microsoft [21], οι αρχιτεκτονικές SaaS μπορεί να ταξινομηθούν σε ένα από τα τέσσερα επίπεδα ωριμότητας, των οποίων τα βασικά χαρακτηριστικά είναι η ευκολία ρύθμισης, η δυνατότητα πολλαπλής μίσθωσης και η

κλιμακοποίηση. Καθένα από τα επίπεδα διακρίνεται από τα προηγούμενα με την προσθήκη ενός από τα τρία προηγούμενα χαρακτηριστικά. Τα επίπεδα που περιγράφονται από την Microsoft έχουν ως εξής:

- Πρώτο αρχιτεκτονικό επίπεδο ωριμότητας SaaS (ad-hoc/custom). Το πρώτο επίπεδο ωριμότητας είναι στην ουσία επίπεδο άνευ ωριμότητας. Κάθε πελάτης έχει μία μοναδική, προσαρμοσμένη έκδοση της εφαρμογής που φιλοξενείται. Η εφαρμογή τρέχει το δικό της στιγμιότυπο στους διακομιστές του παρόχου. Η μετεγκατάσταση μιας παραδοσιακής εφαρμογής δηλαδή μιας εφαρμογής που δεν λειτουργεί στο δίκτυο ή με μοντέλο πελάτη/διακομιστή σε αυτό το επίπεδο ωριμότητας SaaS, τυπικά απαιτεί τη λιγότερη προσπάθεια ανάπτυξης από την αρχή, γεγονός που συμφέρει μιας και θα μειωθεί το κόστος αφενός της λειτουργίας του υλικού της εταιρείας και αφετέρου της διαχείρισης της εφαρμογής εντός της εταιρείας.
- Δεύτερο επίπεδο ωριμότητας SaaS (configurability). Το δεύτερο επίπεδο ωριμότητας SaaS παρέχει ευελιξία στο πρόγραμμα μέσω της διαμόρφωσης των μεταδεδομένων (metadata). Σε αυτό το επίπεδο πολλοί πελάτες μπορούν να χρησιμοποιούν ξεχωριστά στιγμιότυπα της ίδιας εφαρμογής. Αυτό επιτρέπει στον πάροχο να καλύψει τις ποικίλες ανάγκες του κάθε πελάτη, χρησιμοποιώντας λεπτομερείς επιλογές ρύθμισης της εφαρμογής. Επίσης, επιτρέπει στον πάροχο να μειώσει το βάρος της συντήρησης, επειδή είναι σε θέση να ενημερώνει τον κώδικα σε μια κοινή βάση.
- Τρίτο επίπεδο ωριμότητας SaaS (δυνατότητα πολλαπλής μίσθωσης). Το τρίτο επίπεδο ωριμότητα προσθέτει την δυνατότητα πολλαπλής μίσθωσης στο προηγούμενο επίπεδο. Αυτό έχει ως αποτέλεσμα ένα και μόνο στιγμιότυπο του προγράμματος να είναι ικανό να εξυπηρετεί όλους τους πελάτες του παρόχου. Η συγκεκριμένη προσέγγιση επιτρέπει την πιο αποδοτική

χρήση των πόρων του διακομιστή χωρίς να φαίνεται κάποια διαφορά στον τελικό χρήστη, αλλά τελικά αυτό το επίπεδο περιορίζεται από τη μη ικανότητα μαζικής κλιμάκωσης.

- Τέταρτο επίπεδο ωριμότητας SaaS (κλιμάκωση). Στο τέταρτο και τελευταίο επίπεδο ωριμότητας SaaS προστίθεται η κλιμάκωση με τη χρήση μιας αντίστοιχης αρχιτεκτονικής. Η αρχιτεκτονική αυτή είναι ικανή να υποστηρίζει τον τρόπο διαχείρισης του φόρτου εργασίας ίδιων στιγμιότυπων μιας εφαρμογής, τα οποία τρέχουν σε μεταβλητό αριθμό διακομιστών, αριθμός ο οποίες μερικές φορές φτάνει τις εκατοντάδες ή ακόμα και χιλιάδες. Η χωρητικότητα του συστήματος μπορεί να αυξάνεται ή να μειώνεται δυναμικά ώστε να ταιριάζει με τον φόρτο εργασίας, προσθέτοντας ή αφαιρώντας διακομιστές, χωρίς την ανάγκη για περαιτέρω αλλαγή της αρχιτεκτονικής του λογισμικού της εφαρμογής.

Η ανάπτυξη εφαρμογών σε μια αρχιτεκτονική που βασίζεται στο μοντέλο ως-υπηρεσία είναι πιο δύσκολο πρόβλημα από την ανάπτυξη σε παραδοσιακά μοντέλα εφαρμογών. Ως αποτέλεσμα, οι εφαρμογές SaaS κοστολογούνται ανάλογα με τον αριθμό των χρηστών που μπορούν να έχουν παράλληλα πρόσβαση στην υπηρεσία. Συνήθως υπάρχουν επιπρόσθετες χρεώσεις για τη χρήση υπηρεσιών βοήθειας, επιπλέον ταχύτητας στο δίκτυο και αποθηκευτικού χώρο. Σε γενικές γραμμές η ροή εσόδων των παρόχων SaaS είναι συνήθως μικρότερη από τις παραδοσιακές άδειες χρήσης λογισμικού. Ωστόσο, σε μηνιαία βάση γίνονται νέες συζητήσεις για το τι χρήματα χρειάζονται για τις άδειες χρήσης και ανάλογα με τη ζήτηση που υπάρχει γίνεται και ο απαιτούμενος διακανονισμός. Οι μηνιαίες χρεώσεις στους πελάτες θα πρέπει να θεωρούνται ως έξοδα συντήρησης για το λογισμικό γενικότερα και για τις άδειες χρήσεις του. Τα βασικά χαρακτηριστικά του λογισμικού SaaS μπορούν να συνοψιστούν στα ακόλουθα:

- Διαχείριση και πρόσβαση μέσω δικτύου σε εμπορικά διαθέσιμο λογισμικό από κεντρικά σημεία παρά από τον χώρο του κάθε πελάτη, επιτρέποντάς του έτσι να έχει

πρόσβαση στις εφαρμογές του από απόσταση μέσω του διαδικτύου.

- Διανομή της εφαρμογής μέσω του μοντέλου μίας εφαρμογή για πολλούς χρήστες, ενός στιγμιότυπου σε αρχιτεκτονική πολλαπλής μίσθωσης, σε αντίθεση με το παραδοσιακό μοντέλο μιας εφαρμογής για έναν χρήστη.
- Κεντρική βελτίωση και αναβάθμιση της εφαρμογής, η οποία αποτρέπει την ανάγκη για λήψη και εγκατάσταση νέων ενημερώσεων από τον χρήστη.

Ο κύκλος ανάπτυξης των εφαρμογών εντός των εταιρειών ενδεχομένως να διαρκέσει χρόνια, να καταναλώσει τεράστιους πόρους και στο τέλος να μην δώσει ικανοποιητικά αποτελέσματα. Παρά το γεγονός ότι η απόφαση να απολέσει τον έλεγχο επί των δεδομένων είναι αρκετά δύσκολο να ληφθεί από μια εταιρεία, αυτή η απόφαση θα οδηγήσει σε βελτίωση της απόδοσής της, μικρότερους κινδύνους και μια γενναιόδωρη απόδοση στην επένδυση που θα κάνει. Ένας αυξανόμενος αριθμός εταιρειών θέλουν να χρησιμοποιήσουν το μοντέλο SaaS για εταιρικές εφαρμογές, όπως η διαχείριση των σχέσεων με τους πελάτες τους. Το μοντέλο SaaS βοηθά τις εταιρείες να διασφαλίσουν ότι όλα τα επιμέρους τμήματά τους χρησιμοποιούν τη σωστή έκδοση της εφαρμογής και, ως εκ τούτου, ότι η μορφή των δεδομένων που καταγράφονται και μεταφέρονται είναι συνεπής, συμβατή και ακριβής. Με την απόδοση της ευθύνης της εφαρμογής στον πάροχο SaaS, οι εταιρείες μπορούν να μειώσουν τις διοικητικές και διαχειριστικές επιβαρύνσεις που θα είχαν σε αντίθετη περίπτωση χρησιμοποιώντας δικές τους εταιρικές εφαρμογές. Το SaaS, επίσης συντελεί στην αύξηση της διαθεσιμότητας των εφαρμογών σε όλο τον κόσμο και εξασφαλίζει ότι όλες οι συναλλαγές καταγράφονται για τυχόν ελέγχους που θα προκύψουν σε ύστερο χρόνο. Τα πλεονεκτήματα του SaaS είναι ξεκάθαρα για τον πελάτη και είναι τα ακόλουθα:

- Βελτιωμένη διαχείριση.
- Αυτοματοποιημένες υπηρεσίες διαχείρισης και ενημέρωσης της εφαρμογής.

- Συμβατότητα των δεδομένων σε ολόκληρη την επιχείρηση από τη στιγμή που όλοι οι χρήστες έχουν την ίδια έκδοση λογισμικού.
- Διευκόλυνση της συνεργασίας μεταξύ των μελών της επιχείρησης.
- Παγκόσμια προσβασιμότητα.

Όπως επισημάνθηκε και πριν, η εικονικοποίηση των διακομιστών μπορεί να χρησιμοποιηθεί στις αρχιτεκτονικές SaaS, είτε σε αντικατάσταση των ήδη υπαρχόντων φυσικών διακομιστών ή ως πρόσθεση στην πολλαπλή μίσθωση. Το κύριο πλεονέκτημα της εικονικής πλατφόρμας είναι ότι μπορεί να αυξάνει τη χωρητικότητα του συστήματος χωρίς την ανάγκη περαιτέρω προγραμματισμού. Αντίθετα, απαιτείται ένα μεγάλο ποσό χρόνου από τον προγραμματισμό για την αποτελεσματική κατασκευή εφαρμογών που να υποστηρίζουν πολλαπλή μίσθωση. Η επίδραση του συνδυασμού της πολλαπλής μίσθωσης με την εικονική πλατφόρμα σε ένα μοντέλο SaaS παρέχει τη μέγιστη ευελιξία και απόδοση για τον τελικό χρήστη.

Κ Ε Φ Α Λ Α Ι Ο Π Ε Μ Π Τ Ο

Ασφάλεια στο υπολογιστικό νέφος

5.1. Εισαγωγή

Το βασικότερο πρόβλημα που υπάρχει στο υπολογιστικό νέφος και δεν έχει γίνει ακόμα καθολική η χρήση του τόσο από εταιρείες όσο και από μεμονωμένους χρήστες, είναι η ασφάλεια. Με το υπολογιστικό νέφος τα δεδομένα των χρηστών παύουν να είναι υπό την εποπτεία τους [125]. Αυτό σημαίνει ό,τι πλέον θα πρέπει να εμπιστεύονται τον πάροχό τους για την ασφαλή φύλαξη των δεδομένων τους. Στις επόμενες

ενότητες θα αναφερθούμε εκτενώς σε όλα τα ζητήματα ασφάλειας που προκύπτουν τόσο από την μεριά του παρόχου όσο και από την μεριά του χρήστη – πελάτη.

5.2. Ασφάλεια της υποδομής

Όταν αναφερόμαστε στην ασφάλεια της υποδομής σε επίπεδο δικτύου, είναι σημαντικό να γίνει διάκριση μεταξύ των δημόσιων και των ιδιωτικών υπολογιστικών νεφών. Στην περίπτωση των ιδιωτικών νεφών δεν υπάρχουν νέα είδη επιθέσεων, ευπαθειών ή αλλαγών τις οποίες θα πρέπει να αντιμετωπίζει το προσωπικό ασφάλειας. Παρόλο που η πληροφοριακή υποδομή μιας εταιρείας αλλάζει προς την υλοποίηση μιας υποδομής ιδιωτικού υπολογιστικού νέφους, η τρέχουσα τοπολογία του δικτύου δεν αλλάζει σημαντικά. Αν η εταιρεία, έχει ένα ιδιωτικό εσωτερικό δίκτυο, για παράδειγμα για υψηλούς πελάτες ή στρατηγικούς συνεργάτες, η τοπολογία για ένα ιδιωτικό νέφος είναι ήδη έτοιμη. Οι μελέτες και τα διάφορα εργαλεία ασφάλειας που ήδη διαθέτει η εταιρεία μπορούν να εφαρμοστούν και στην υποδομή του ιδιωτικού νέφους και είναι αναγκαίο να λειτουργήσουν με τον ίδιο τρόπο για την ασφάλεια του συστήματος.

Ωστόσο, στην περίπτωση που μια εταιρεία επιλέξει να χρησιμοποιήσει δημόσιες υπηρεσίες υπολογιστικού νέφους, οι μεταβαλλόμενες απαιτήσεις ασφάλειας θα επιβάλλουν αλλαγές στην τοπολογία του δικτύου της. Ως εκ τούτου, θα πρέπει να γίνει εκτενής αναφορά για τον τρόπο που η υπάρχουσα δικτυακή υποδομή αλληλεπιδρά με την τοπολογία του δικτύου του παρόχου νέφους. Σε αυτή την περίπτωση υπάρχουν τέσσερις βασικοί παράγοντες κινδύνου:

- Διασφάλιση της εμπιστευτικότητας και ακεραιότητας των δεδομένων της εταιρείας κατά την μεταφορά τους από και προς τον πάροχο νέφους
- Διασφάλιση κατάλληλου ελέγχου πρόσβασης, μέσω αυθεντικοποίησης, άδειας πρόσβασης και πλήρους καταγραφής όλων των συμβάντων, για οποιουσδήποτε

πόρους χρησιμοποιεί η εταιρεία από το δημόσιο υπολογιστικό νέφος

- Διασφάλιση της διαθεσιμότητας των πόρων του διαδικτύου, ώστε να μην υπάρχει διακοπή στην επικοινωνία με τον πάροχο του υπολογιστικού νέφους
- Αντικατάσταση του καθιερωμένου μοντέλου ζωνών και βαθμίδων του δικτύου με τομείς.

Στη συνέχεια θα αναλύσουμε κάθε έναν από τους προηγούμενους παράγοντες κινδύνου στις ενότητες που ακολουθούν.

5.2.1. Διασφάλιση της εμπιστευτικότητας και της ακεραιότητας των δεδομένων

Τόσο οι πόροι όσο και τα δεδομένα της εταιρείας που πριν ήταν περιορισμένα στον ιδιωτικό χώρο της εταιρείας, τώρα και εκτίθενται στο διαδίκτυο και διαμοιράζονται σε ένα δημόσιο δίκτυο, το οποίο ανήκει σε ένα πάροχο νέφους, δηλαδή έναν τρίτο. Ένα τυπικό παράδειγμα που σχετίζεται με το πρόβλημα που προκύπτει από τον συγκεκριμένο κίνδυνο είναι η ευπάθεια που είχε παρουσιαστεί στο AWS. Σε μια ανάρτηση ενός blog, ο συγγραφέας περιέγραψε λεπτομερώς μια ευπάθεια στον αλγόριθμο ψηφιακής υπογραφής, όταν γινόταν κάποιο αίτημα στο simpleDB, στο EC2 και στο SQS μέσω του πρωτοκόλλου HTTP. Παρόλο που η χρήση του HTTPS αντί το HTTP θα εξάλειφε τον κίνδυνο που προέκυπτε στην ακεραιότητα, οι χρήστες κάνοντας χρήση του HTTP αντί του HTTPS αντιμετώπιζαν τον κίνδυνο τροποποίησης των δεδομένων τους κατά τη διάρκεια της μεταφοράς από και προς τον πάροχο εν αγνοία τους.

5.2.2. Διασφάλιση κατάλληλου ελέγχου πρόσβασης

Από τη στιγμή που ένα υποσύνολο, ή ακόμα και στο σύνολό τους, οι πόροι εκτίθενται στο διαδίκτυο, μια εταιρεία που χρησιμοποιεί κάποιο δημόσιο υπολογιστικό νέφος, αντιμετωπίζει μια σημαντική αύξηση κινδύνου για τα δεδομένα της. Η δυνατότητα του ελέγχου των

λειτουργιών του δικτύου του παρόχου υπολογιστικού νέφους, ακόμα και μετά από ένα συμβάν είναι κατά πάσα πιθανότητα ανύπαρκτη. Ο χρήστης – πελάτης έχει μειωμένη πρόσβαση στα σχετικά αρχεία καταγραφής συμβάντων και στα δεδομένα του δικτύου, και περιορισμένη δυνατότητα διεξαγωγής έρευνας σε βάθος και συγκέντρωσης αποδεικτικών στοιχείων (forensic data).

Ένα παράδειγμα των προβλημάτων που σχετίζονται με τον δεύτερο παράγοντα επικινδυνότητας είναι το ζήτημα των επαναχρησιμοποιούμενων διευθύνσεων IP. Σε γενικές γραμμές, οι πάροχοι υπολογιστικού νέφους δεν διατηρούν τις διευθύνσεις IP σε περίπτωση που ο χρήστης δεν τις χρειάζεται πλέον [99]. Τέτοιες διευθύνσεις IP συνήθως κατοχυρώνονται ως κενές και επαναχρησιμοποιούνται από άλλους πελάτες μόλις γίνουν διαθέσιμες. Αυτό θεωρείται λογικό από την πλευρά των παρόχων υπολογιστικού νέφους, καθώς οι διευθύνσεις IP είναι μια πεπερασμένη ποσότητα και χρεώνονται επιπλέον για τους χρήστες που θέλουν μόνιμη και σταθερή διεύθυνση IP. Ωστόσο, και από την πλευρά των πελατών, η ύπαρξη διευθύνσεων IP που δεν χρησιμοποιούνται μπορεί να παρουσιάσει κάποιο πρόβλημα. Ο πελάτης δεν μπορεί να θεωρήσει ότι έχει τερματίσει η πρόσβαση στο δίκτυο στους πόρους του παρά μόνο όταν δεν υπάρχει κάποια IP. Υπάρχει μια απαραίτητη χρονική διάρκεια για την αλλαγή της διεύθυνσης στο DNS και τον καθαρισμό της συγκεκριμένης διεύθυνσης από τους προσωρινούς DNSes. Επίσης, υπάρχει μια παρόμοια χρονική διάρκεια όταν οι φυσικές διευθύνσεις (MAC) αλλάζουν στους πίνακες ARP και οι παλιές φυσικές διευθύνσεις καθαρίζονται και από την προσωρινή μνήμη, καθώς μια φυσική διεύθυνση παραμένει στους πίνακες ARP μέχρι να διαγραφεί. Αυτό σημαίνει ότι ακόμα και αν αλλάξουν κάποιες διευθύνσεις, οι παλιές διευθύνσεις είναι διαθέσιμες για λίγο χρόνο μετά την αλλαγή, και ως εκ τούτου εξακολουθούν να επιτρέπουν σε διάφορους χρήστες να έχουν πρόσβαση σε υποθετικά ανύπαρκτους πόρους. Αξίζει να αναφερθεί ότι υπήρξαν πολλές αναφορές για τέτοιου είδους προβλήματα με παλιές διευθύνσεις IP στο AWS, και αυτό ήταν και το βασικό ζήτημα για το οποίο η Amazon εισήγαγε το Elastic IP, από την αυγή του υπολογιστικού νέφους, κάπου τον Μάρτιο του 2008. Όπως αναφέρθηκε και σε προηγούμενο κεφάλαιο,

με το Elastic IP, οι πελάτες παίρνουν πέντε διευθύνσεις IP, πάνω στις οποίες έχουν πλήρη έλεγχο. Επιπλέον, σύμφωνα με τον S. Garfinkel "*ένα ξεχωριστό και νέο πρόβλημα με τις εφαρμογές φόρτωσης αρχείων προκαλεί το τερματισμό της σύνδεσης TCP/IP όταν το μέγεθος είναι* 2^{31} *Β. Αυτό σημαίνει ότι αντικείμενα μεγαλύτερα των 2GB θα πρέπει να αποθηκεύονται στο S3 σε πολλές μεμονωμένες συνδέσεις, καθεμία από τις οποίες θα μεταφέρει διαφορετικό κομμάτι του ίδιου αντικειμένου* ".

Ωστόσο, το ζήτημα των παλιών διευθύνσεων IP και της μη εξουσιοδοτημένης πρόσβασης στο δίκτυο καθώς και σε πόρους, δεν συμβαίνει μόνο σε δρομολογήσιμες διευθύνσεις IP, δηλαδή σε πόρους που πρόκειται να είναι διαθέσιμοι απευθείας μέσω διαδικτύου. Το συγκεκριμένο ζήτημα συμβαίνει και στο εσωτερικό δίκτυο των παρόχων που είναι για χρήση των πελατών τους και στην ανάθεση των μη δρομολογήσιμων διευθύνσεων IP. Παρόλο που οι πόροι ενός πελάτη μπορεί να μην είναι προσβάσιμοι μέσω διαδικτύου, για σκοπούς διαχείρισης, οι πόροι θα πρέπει να είναι προσβάσιμοι εντός του δικτύου του υπολογιστικού νέφους μέσω ιδιωτικών διευθύνσεων καθώς κάθε πόρος που είναι δημόσιος και φαίνεται στο δίκτυο έχει και δημόσια και ιδιωτική διεύθυνση. Άλλοι πελάτες του ίδιου παρόχου ενδεχομένως να μην έχουν καλές προθέσεις και μέσω του προηγούμενου να είναι σε θέση να έχουν πρόσβαση στους πόρους του πρώτου πελάτη εσωτερικά, κάνοντας χρήση του δικτύου του υπολογιστικού νέφους. Κατά το παρελθόν οι πάροχοι υπηρεσιών υπολογιστικού νέφους είχαν να αντιμετωπίσουν τέτοιου είδους παραβιάσεις μεταξύ των πόρων των πελατών του.

Για τη λύση του προβλήματος την επαναχρησιμοποίησης των διευθύνσεων IP, δημιουργήθηκαν αρκετά προϊόντα στην αγορά, αλλά αν δεν χρησιμοποιήσουν οι πάροχοι υπολογιστικού νέφους αυτά τα προϊόντα ως υπηρεσίες, οι πελάτες θα συνεχίζουν να πληρώνουν τρίτες εταιρείες για να λύσουν ένα πρόβλημα που πρακτικά έχει δημιουργηθεί από τους παρόχους υπολογιστικού νέφους και επηρεάζει αποκλειστικά τους πελάτες.

5.2.3. Διασφάλισης της σύνδεσης στο διαδίκτυο

Είναι γεγονός ότι η εξάρτηση από την ασφάλεια του δικτύου έχει αυξηθεί ραγδαία επειδή ένα όλο και αυξανόμενο ποσοστό από δεδομένα καθώς και χρήστες εξαρτώνται πλήρως από τους παρόχους τους και τους πόρους που έχουν σε αυτούς. Κατά συνέπεια, οι τρεις βασικοί παράγοντες κινδύνου που αναφέρονται στην προηγούμενη παράγραφο πρέπει να είναι αποδεκτοί από την εταιρεία που σκοπεύει να μεταφέρει το πληροφοριακό της σύστημα στο υπολογιστικό νέφος.

Η πειρατεία του προθέματος του πρωτοκόλλου BGP (Border Gateway Protocol) αποτελεί ένα καλό παράδειγμα των τριών αυτών συνιστωσών στην επικινδυνότητα. Η πειρατεία του προθέματος περιλαμβάνει την δημιουργία ενός αυτόνομου συστήματος διευθύνσεων, το οποίο ανήκει σε κάποιο χρήστη χωρίς την άδειά του. Τέτοιες καταστάσεις συχνά συμβαίνουν λόγω κάποιου λάθους στις ρυθμίσεις διαμόρφωσης, αλλά αυτό το λάθος ενδεχομένως να επηρεάζει την διαθεσιμότητα των πόρων της εταιρείας που είναι στο υπολογιστικό νέφος. Δυστυχώς, κάθε μήνα συμβαίνουν εκατοντάδες τέτοια λάθη στις ρυθμίσεις διαμόρφωσης των πελατών. Πιθανόν το καλύτερο παράδειγμα για τέτοιου είδους λάθος στις ρυθμίσεις διαμόρφωσης στο παρελθόν, όταν η Πακιστανική εταιρεία Telecom θέλοντας να κατεβάσει το YouTube από την επικράτεια του Πακιστάν λόγω κάποιων βλάσφημων βίντεο, ρύθμισε λάθος τους διακομιστές της και αυτό είχε ως αποτέλεσμα να μην είναι διαθέσιμο το YouTube για δύο ολόκληρες ώρες παγκοσμίως.

Σε αντίθεση με τα λάθη που γίνονται στις ρυθμίσεις, υπάρχουν επίσης και σκόπιμες επιθέσεις. Παρόλο που η προηγούμενη επίθεση είναι πολύ σπάνια σε περίπτωση κακόβουλων χρηστών, μπορεί να συμβεί και να προκαλέσει την άρνηση πρόσβασης στα δεδομένα των χρηστών. Σύμφωνα με την ίδια έρευνα που αναφέρθηκε στην προηγούμενη παράγραφο, τέτοιου είδους επιθέσεις συμβαίνουν λιγότερες από 100 σε ένα μήνα. Παρόλο που το συγκεκριμένο είδος επίθεσης δεν είναι καινούριο, ο αριθμός των επιθέσεων με αυτόν τον τρόπο θα κλιμακωθεί σημαντικά σε συνδυασμό με την αύξηση του υπολογιστικού νέφους. Καθώς διευρύνεται η χρήση του υπολογιστικού νέφους, η διαθεσιμότητα σε πόρους του υπολογιστικού νέφους

αυξάνεται σε αξία για τους πελάτες. Αυτή η αυξημένη αξία για τους πελάτες μεταφράζεται σε εντονότερο κίνδυνο απειλής από κακόβουλη δραστηριότητα με άμεσο αποτέλεσμα την απώλεια της διαθεσιμότητας.

Ένα άλλο παράδειγμα είναι οι επιθέσεις DNS [125, 126]. Στην πραγματικότητα υπάρχουν πολλές μορφές επιθέσεων DNS που θα πρέπει να ανησυχούν τους χρήστες του υπολογιστικού νέφους. Παρόλο που οι επιθέσεις DNS δεν είναι καινούριες και δεν σχετίζονται απ' ευθείας με τη χρήση του υπολογιστικού νέφους, το θέμα με τον DNS και το υπολογιστικού νέφος είναι μείζον. Ο λόγος για αυτό είναι ότι ο πελάτης δεν μπορεί να κάνει και πολλά με την αποτροπή του ή την ασφάλεια του DNS και επαφίεται εξ ολοκλήρου στην ασφάλεια δικτύου που του παρέχει ο πάροχος για να διασφαλίζει τους πόρους που χρησιμοποιεί από αυτόν.

Παρόλο που το γνωστό «Kaminsky Bug» ήταν αυτό που συγκέντρωσε το μεγαλύτερο μέρος της προσοχής της ασφάλειας των δικτύων σε προηγούμενα χρόνια και τα υπόλοιπα προβλήματα του DNS έχουν επίσης αντίκτυπο στο υπολογιστικό νέφος. Το πρόβλημα δεν είναι ότι υπάρχουν μόνο ευπάθειες τόσο στο ίδιο το πρωτόκολλο του DNS και στις υλοποιήσεις του, αλλά επίσης υπάρχουν αρκετά διαδεδομένες επιθέσεις DNS, poisoning attacks, όπως ονομάζονται, όπου ο διακομιστής DNS παραπλανιέται, ώστε να λαμβάνει ψεύτικες πληροφορίες [127]. Παρόλο που αρκετοί πιστεύουν ότι τέτοιου είδους επιθέσεις έχουν εξαλειφτεί εδώ και αρκετά χρόνια, κάτι τέτοιο δεν είναι αληθές, καθώς αυτές είναι ακόμα ένα πολύ μεγάλο πρόβλημα, ιδίως στο πλαίσιο του υπολογιστικού νέφους. Παραλλαγές της επίθεσης συμπεριλαμβάνουν ανακατεύθυνση του ονόματος του διακομιστή DNS που είναι στόχος, ανακατεύθυνση μιας εγγραφής σε άλλο διακομιστή και απάντηση για ορθή λήψη πριν την απάντηση του πραγματικού διακομιστή.

Ένα τελευταίο παράδειγμα προβλημάτων που συσχετίζονται με τους τρεις παράγοντες επικινδυνότητας είναι οι επιθέσεις αφενός της άρνησης εκτέλεσης υπηρεσίας (Denial of Service - DoS) και αφετέρου η κατανεμημένη άρνηση εκτέλεσης υπηρεσίας (Distributed Denial of Service - DDoS). Παρόλο που τόσο το DoS όσο και το DDoS δεν είναι νέα

είδη επίθεσης και δεν σχετίζονται άμεσα με τη χρήση του υπολογιστικού νέφους, το θέμα που προκύπτει από αυτές τις επιθέσεις είναι η αύξηση του βαθμού επικινδυνότητας σε επίπεδο δικτύου λόγω της αυξημένης χρήσης κάποιων πόρων του δικτύου. Για παράδειγμα, κυκλοφόρησαν φήμες ότι υπήρχαν συνεχείς επιθέσεις DDoS στο AWS της Amazon, στο Azure της Microsoft και στο Google Cloud Platform (GCP) της Google [128], καθιστώντας τις υπηρεσίες μη διαθέσιμες προς τους χρήστες για αρκετά μεγάλο χρονικό διάστημα. Στις αντίστοιχες περιπτώσεις, οι πάροχοι είτε δηλώνουν πρόβλημα στις υποδομές τους ή ότι δεν μπορούν να προσδιορίσουν τους λόγους διακοπής των υπηρεσιών τους και ότι δεν ξέρουν να πουν αν οφειλόταν σε επιθέσεις DDoS.

Ωστόσο, στην περίπτωση του IaaS, ο κίνδυνος μιας επίθεσης DDoS δεν ωφελείται μόνο σε εξωτερικούς παράγοντες. Υπάρχει εξίσου μεγάλος κίνδυνος εσωτερικά μέσω του τμήματος του δικτύου του παρόχου IaaS που χρησιμοποιείται από τους πελάτες και είναι ξεχωριστό από το εταιρικό δίκτυο του παρόχου IaaS. Το εσωτερικό δίκτυο των υπολογιστικών νεφών είναι ένας διαμοιραζόμενος πόρος ο οποίος χρησιμοποιείται από τους πελάτες για να έχουν πρόσβαση στα ιδιωτικά τους στιγμιότυπα καθώς και από τον ίδιο τον πάροχο για να διαχειρίζεται το δίκτυο και τους πόρους του, όπως για παράδειγμα τους φυσικούς διακομιστές. Για έναν κακοήθη πελάτη, τίποτα δεν θα υπήρχε για να τον αποτρέψει από το να χρησιμοποιήσει την πρόσβαση που του δίνεται από τον πάροχο ώστε να μπει στο δίκτυο, πόρο που δικαιούται, και να επιτεθεί σε άλλους πελάτες, ή στην υποδομή IaaS του παρόχου. Αξίζει να σημειωθεί ότι ο ίδιος ο πάροχος θα μπορούσε πιθανότατα να μην έχει καθόλου συστήματα ελέγχου για να μπορεί να ενημερώνεται σχετικά για τέτοιου είδους επιθέσεις. Τα μόνα αποτρεπτικά μέσα που θα μπορούσαν να χρησιμοποιήσουν οι άλλοι πελάτες ενάντια στον εσωτερικό επιτιθέμενο είναι η ρύθμιση όσο το δυνατόν καλύτερα και λεπτομερέστερα τα στιγμιότυπά τους.

5.2.4. Αντικατάσταση του καθιερωμένου μοντέλου ζωνών δικτύου και βαθμίδων με τομείς

Το κλασικό καθιερωμένο μοντέλο απομόνωσης των ζωνών του δικτύου και των βαθμίδων δεν υπάρχει πλέον στα δημόσια PaaS και IaaS [129]. Για πολλά χρόνια, η ασφάλεια δικτύου βασιζόταν στις ζώνες, όπως για παράδειγμα το intranet με το extranet και η ανάπτυξη με την παραγωγή, με σκοπό τον διαχωρισμό της κυκλοφορίας του δικτύου για βελτίωση της γενικής ασφάλειας. Το συγκεκριμένο μοντέλο βασίζεται στον αποκλεισμό, δηλαδή στο ότι μόνο συγκεκριμένα άτομα ή συστήματα που είχαν συγκεκριμένους ρόλους θα μπορούσαν να έχουν πρόσβαση σε συγκεκριμένες ζώνες. Αντίστοιχα, τα συστήματα που ήταν εντός μιας βαθμίδας είχαν πρόσβαση μόνο στο εσωτερικό της συγκεκριμένης βαθμίδας ή σε κάποια άλλη, πάλι αυστηρά καθορισμένη. Για παράδειγμα, τα συστήματα που ανήκουν στη βαθμίδα της παρουσίασης δεν επιτρέπεται να επικοινωνούν απευθείας με την αντίστοιχη της βάσης δεδομένων, αλλά τους επιτρέπεται να επικοινωνούν μόνο μέσω μιας εξουσιοδοτημένης εφαρμογής εντός της βαθμίδας των εφαρμογών. Τα SaaS που έχουν κατασκευαστεί πάνω σε δημόσια PaaS ή IaaS έχουν παρόμοια χαρακτηριστικά. Ωστόσο, ένα δημόσιο SaaS που κατασκευάστηκε πάνω σε ένα ιδιωτικό IaaS μπορεί να ακολουθεί το παραδοσιακό μοντέλο απομόνωσης, αλλά πληροφορίες σχετικές με την τοπολογία του δικτύου δεν γνωστοποιούνται στους πελάτες.

Στο υπολογιστικό νέφος το παραδοσιακό μοντέλο των ζωνών δικτύου και των βαθμίδων έχει αντικατασταθεί με ομάδες ασφαλείας (security groups), τομείς ασφαλείας (security domains) ή εικονικά κέντρα δεδομένων (virtual data centers), γεγονός το οποίο μπορεί να θεωρηθεί ως ένας λογικός διαχωρισμός βαθμίδων αλλά είναι λιγότερο ακριβή και παρέχουν μικρότερη προστασία από τον προηγούμενο μοντέλο [99]. Για παράδειγμα το χαρακτηριστικό των ομάδων ασφαλείας στο AWS επιτρέπει στις εικονικές μηχανές ενός πελάτη να έχουν πρόσβαση η μία με την άλλη με την χρήση εικονικού τείχους προστασίας το οποίο έχει την δυνατότητα να φιλτράρει την κίνηση με βάση την διεύθυνση IP, τα είδη των πακέτων, TCP, UDP και ICMP, και τις θύρες. Τα ονόματα των τομέων

χρησιμοποιούνται σε διάφορες περιπτώσεις του δικτύου καθώς και σε ονοματολογία των εφαρμογών για σκοπούς διευθυνσιοδότησης, με βάση το DNS. Για παράδειγμα, το App Engine της Google παρέχει μια λογική ομαδοποίηση των εφαρμογών η οποία βασίζεται στα ονόματα των τομέων όπως mytestapp.test.mydomain.com και myprodapp.prof.mydomain.com.

Στο καθιερωμένο μοντέλο των ζωνών δικτύου και των βαθμίδων, δεν ήταν μόνο λογικά ξεχωριστά τα συστήματα ανάπτυξης από τα συστήματα παραγωγής σε επίπεδο δικτύου, αλλά οι δύο ομάδες που υλοποιούσαν τα συστήματα αυτά ξεχωριστές και σε φυσικό επίπεδο, δηλαδή λειτουργούσαν σε φυσικώς διαφορετικούς διακομιστές και σε λογικά άλλες ζώνες δικτύου. Ωστόσο, αυτός ο διαχωρισμός παύει να υπάρχει στο υπολογιστικό νέφος, καθώς τα μοντέλα του υπολογιστικού νέφους παρέχουν μόνο λογικό διαχωρισμό σε και μόνο για λόγους διευθυνσιοδότησης. Δεν υπάρχει πλέον ο απαιτούμενος φυσικός διαχωρισμός, καθώς ο τομέας του ελέγχου και ο τομέας της παραγωγής ενδεχομένως να τρέχουν στον ίδιο φυσικό διακομιστή. Επιπλέον, παύει να υπάρχει ο λογικός διαχωρισμός στο δίκτυο, καθώς αυτός τώρα είναι στο επίπεδο του πελάτη επιτρέποντας και στους δύο τομείς να τρέχουν στον ίδιο φυσικό διακομιστή και να διαχωρίζονται λογικά μέσω των εικονικών μηχανημάτων.

5.2.5. Μετρίαση κινδύνων σε επίπεδο δικτύου

Λαμβάνοντας υπόψη τους παράγοντες που εξετάστηκαν στις προηγούμενες ενότητες, τι θα μπορούσε να γίνει ώστε να μετριαστούν οι αυξημένοι παράγοντες κινδύνου; Καταρχάς, να σημειωθεί ότι οι κίνδυνοι σε επίπεδο δικτύου υφίστανται ανεξάρτητα από το είδος της υπηρεσίας υπολογιστικού νέφους που χρησιμοποιείται, δηλάδη IaaS, PaaS και SaaS. Ο πρωταρχικός προσδιορισμός του επιπέδου επικινδυνότητας δεν σχετίζεται με το ποια υπηρεσία χρησιμοποιείται, αλλά αν η εταιρεία σκοπεύει να κάνει χρήση της υπηρεσίας δημόσια, ιδιωτικά ή σε υβριδική μορφή. Παρόλο που μερικοί πάροχοι IaaS παρέχουν εικονικές ζώνες δικτύου, δεν μπορεί να θεωρηθεί το ίδιο με ένα ιδιωτικό περιβάλλον

υπολογιστικού νέφους το οποίο εκτελεί συνεχή επιθεώρηση και άλλα μέτρα ασφάλειας πάνω στο δίκτυο.

Αν μια εταιρεία είναι αρκετά μεγάλη ώστε να μπορεί να αντέξει τους πόρους ενός ιδιωτικού υπολογιστικού νέφους, αυτό σημαίνει αυτόματα σημαντική μείωση των κινδύνων, από την στιγμή που θα έχει ένα πραγματικό περιβάλλον υπολογιστικού νέφους εντός του εσωτερικού της δικτύου. Σε μερικές περιπτώσεις, ένα ιδιωτικό υπολογιστικό νέφος, το οποίο βρίσκεται εντός των εγκαταστάσεων του παρόχου υπολογιστικού νέφους, μπορεί να βοηθήσει στη πραγματοποίηση των απαιτήσεων ασφάλειας αλλά εξαρτάται στις ικανότητες και την ωρίμανση του παρόχου.

Μια εταιρεία μπορεί να μειώσει τους κινδύνους εμπιστευτικότητας με την χρήση κρυπτογράφησης και πιο συγκεκριμένα με την χρήση πιστοποιημένων εφαρμογών για την κρυπτογράφηση των εν κινήσει δεδομένων [125]. Οι ασφαλείς ψηφιακές υπογραφές καθιστούν ακόμα πιο δύσκολο, αν όχι ακατόρθωτο, για κάποιον τρίτο να μπορέσει να μεταβάλει τα δεδομένα και αυτό εξασφαλίζει την ακεραιότητα των δεδομένων.

Τα προβλήματα διαθεσιμότητας σε επίπεδο δικτύου είναι πολύ πιο δύσκολο να μετριαστούν στο υπολογιστικό νέφος, εκτός και αν κάποια εταιρεία χρησιμοποιεί ένα ιδιωτικό υπολογιστικό νέφος, το οποίο βρίσκεται εσωτερικά στην τοπολογία του δικτύου της. Ακόμα και αν ένα ιδιωτικό υπολογιστικό νέφος είναι ιδιωτικό τοπολογικά και για τον πάροχο υπολογιστικού νέφους, δηλαδή οι πόροι του είναι αποκλειστικά για μία εταιρεία, θα υπάρχουν επίσης κίνδυνοι σε επίπεδο δικτύου. Εννοείται ότι ένα δημόσιο υπολογιστικό νέφος αντιμετωπίζει ακόμα μεγαλύτερο κίνδυνο.

Ακόμα και τεράστιες εταιρείες με σημαντικούς πόρους αντιμετωπίζουν αξιοσημείωτες προκλήσεις σχετικά με την ασφάλεια της υποδομής σε επίπεδο δικτύου. Οι κίνδυνοι που σχετίζονται με την χρήση του υπολογιστικού νέφους είναι μεγαλύτεροι από τους κινδύνους που αντιμετωπίζουν οι εταιρείες σήμερα; Ας συγκρίνουμε τα υπάρχοντα ιδιωτικά και δημόσια extranets και ας λάβουμε υπόψη τις συνδέσεις των

εταίρων, όταν θα κάνουμε αυτή την σύγκριση. Για μεγάλες εταιρείες χωρίς σημαντικούς πόρους, ή για μικρές έως μεσαίες εταιρείες, είναι ο κίνδυνος της χρήσης δημόσιου υπολογιστικού νέφους, θεωρώντας ότι δεν έχουν πόρους για να υλοποιήσουν ένα ιδιωτικό υπολογιστικό νέφος, είναι πραγματικά μεγαλύτερος από τους κινδύνους που αντιμετωπίζουν στις τρέχουσες υποδομές τους; Στις περισσότερες των περιπτώσεων η απάντηση είναι προφανώς όχι, δεν υπάρχει μεγαλύτερο ποσοστό κινδύνου στο υπολογιστικό νέφος.

5.3. Υποδομή ασφάλειας σε επίπεδο εξυπηρετητή (host)

Κατά την εξέταση της ασφάλειας του παρόχου και της εκτίμησης των κινδύνων, θα πρέπει να ληφθούν υπόψη τα μοντέλα του υπολογιστικού νέφους, PaaS, IaaS και SaaS, και ο τρόπος παροχής της υπηρεσίας, δημόσιος, ιδιωτικός και υβριδικός. Παρόλο που δεν υπάρχουν νέοι κίνδυνοι στους εξυπηρετητές που είναι συγκεκριμένα στο υπολογιστικό νέφος, προκλήθηκαν μερικοί κίνδυνοι σχετικά με την εικονικοποίηση των συσκευών, όπως για παράδειγμα στο VM, η λανθασμένη διαμόρφωση του συστήματος, και εσωτερικοί κίνδυνοι μέσω του πλημμελούς ελέγχου πρόσβασης στο hypervisor, γεγονός που συμβαίνει σε δημόσια περιβάλλοντα υπολογιστικού νέφους [126]. Η δυναμική φύση του νέφους μπορεί να επιφέρει νέες διαχειριστικές προκλήσεις από την πλευρά της διαχείρισης ασφάλειας. Το επιχειρησιακό μοντέλο παρακινεί την ταχεία παροχή υπηρεσιών και συνεχώς νέα στιγμιότυπα. Η διαχείριση των ευπαθειών και η διόρθωσή τους είναι πολύ πιο δύσκολη από ένα απλό έλεγχο, καθώς ο ρυθμός αλλαγής είναι πολύ υψηλότερος από ότι σε ένα παραδοσιακό κέντρο δεδομένων.

Επιπλέον, το γεγονός ότι το υπολογιστικό νέφος εκμεταλλεύεται την υπολογιστική δύναμη χιλιάδων υπολογιστικών κόμβων, σε συνδυασμό με την ομογενοποίηση των λειτουργικών συστημάτων που τρέχουν στους hosts, σημαίνει ότι οι απειλές μπορεί να επεκταθούν γρήγορα και εύκολα, πράγμα το οποίο αναφέρεται ως ο επονομαζόμενος παράγοντας ταχύτητας της επίθεσης (velocity of attack) στο

υπολογιστικό νέφος [130]. Το πιο σημαντικό είναι ότι θα πρέπει να κατανοηθεί πλήρως πιο είναι το όριο των έμπιστων πόρων καθώς και οι ευθύνες που αναθέτονται στον καθένα από τους εμπλεκόμενους για την ασφάλεια της υποδομής του εξυπηρετητή που διαχειρίζονται. Τέλος, θα πρέπει να θεωρηθεί ότι η ίδια ασφάλεια θα πρέπει να υφίσταται και από τη μεριά των υποδομών των εξυπηρετητών των παρόχων.

5.3.1. Ασφάλεια εξυπηρετητών SaaS και PaaS

Σε γενικές γραμμές, οι πάροχοι υπολογιστικού νέφους δεν διαμοιράζουν δημόσια πληροφορίες που σχετίζονται με τους εξυπηρετητές τους, τα λειτουργικά συστήματα των εξυπηρετητών και τις διαδικασίες που τηρούνται για την ασφάλεια των εξυπηρετητών, από την στιγμή που διάφοροι κάκοβουλοι χρήστες μπορούν να εκμεταλλευτούν αυτές τις πληροφορίες όταν προσπαθούν να εισβάλλουν σε κάποια υπηρεσία του υπολογιστικού νέφους. Ως εκ τούτου, στο πλαίσιο των μοντέλων SaaS και PaaS, η ασφάλεια του εξυπηρετητή είναι αδιαφανής ως προς τους πελάτες και η ευθύνη της ασφάλειας των εξυπηρετητών μετατίθεται στον πάροχο. Με σκοπό τη λήψη επιβεβαίωσης από τον πάροχο σχετικά με την ασφάλεια που έχει στους εξυπηρετητές του, θα πρέπει να ζητηθεί από τον πάροχο να την εξασφαλίζει στον πελάτη μέσω μιας εμπιστευτικής συμφωνίας (NDA Non-Disclosure Agreement) ή απλά να απαιτήσει από τον πάροχο να διοχετεύει τη συγκεκριμένη πληροφορία μέσω ενός πλαισίου αξιολόγησης ασφάλειας όπως για παράδειγμα το SysTrust ή το ISO27002 [131]. Από την σκοπιά των ελέγχων διασφάλισης της ασφάλειας, ο πάροχος υπηρεσιών υπολογιστικού νέφους θα πρέπει να εξασφαλίσει ότι υπάρχουν ειδικοί έλεγχοι τόσο αποτρεπτικού όσο και κατασταλτικού φάσματος σε θέσεις κλειδιά στο δίκτυό του και αυτό θα πρέπει επίσης να γίνεται μέσω κάποιου πλαισίου αξιολόγησης όπως και προηγούμενα.

Από τη στιγμή που η εικονικοποίηση είναι μια τεχνολογία κλειδί που βελτιώνει την αξιοποίηση των εξυπηρετητών που είναι στο υλικό, μεταξύ άλλων πλεονεκτημάτων, είναι πολύ κοινό για τους παρόχους υπηρεσιών υπολογιστικού νέφους να χρησιμοποιούν πλατφόρμες

εικονικοποίησης, συμπεριλαμβανομένου των Hyper-V [132] και VMware Hypervisors [88], στη δική τους αρχιτεκτονική. Τέλος, οι πελάτες θα πρέπει να καταλάβουν το πώς οι πάροχοι κάνουν χρήση της τεχνολογίας εικονικοποίησης με σκοπό την ασφάλιση του επιπέδου εικονικοποίησης.

Τόσο το PaaS όσο και το SaaS είναι αφηρημένα και κρύβουν το λειτουργικό σύστημα του εξυπηρετητή από τους τελικούς χρήστες μέσω ενός αφηρημένου επιπέδου εξυπηρέτησης. Μια κύρια διαφορά μεταξύ του PaaS και του SaaS είναι η πρόσβαση στο αφηρημένο επίπεδο το οποίο κρύβει τις υπηρεσίες του λειτουργικού συστήματος που χρησιμοποιούν οι εφαρμογές. Στην περίπτωση του SaaS, το αφηρημένο επίπεδο δεν είναι εμφανές στους χρήστες και είναι διαθέσιμο μόνο στους προγραμματιστές και τους διαχειριστές του παρόχου, ενώ στην περίπτωση του PaaS, οι χρήστες έχουν έμμεση πρόσβαση στο αφηρημένο επίπεδο εξυπηρέτησης με τη μορφή κάποιας διεπαφής προγραμματισμού εφαρμογών (Application Programming Interface - API) η οποία με τη σειρά της αλληλεπιδρά με το αφηρημένο επίπεδο του εξυπηρετητή. Με λίγα λόγια, αν κάποιος είναι πελάτης PaaS ή SaaS, βασίζεται αποκλειστικά στον πάροχο για να έχει μια ασφαλή πλατφόρμα εξυπηρετητή πάνω στην οποία θα αναπτυχθούν και θα τρέχουν οι διάφορες εφαρμογές από τους χρήστες ή τον πάροχο για τους χρήστες, αντίστοιχα.

Κλείνοντας την συγκεκριμένη υποενότητα, οι ευθύνες σχετικά με την ασφάλεια του εξυπηρετητή σε υπηρεσίες SaaS και PaaS μεταφέρονται αποκλειστικά στον πάροχο του υπολογιστικού νέφους. Το γεγονός ότι ο χρήστης δεν χρειάζεται να ανησυχεί για την προστασία των εξυπηρετητών από διάφορες απειλές είναι το μέγιστο πλεονέκτημα από πλευράς διαχείρισης ασφάλειας και κόστους. Ωστόσο, οι πελάτες είναι ακόμα υπεύθυνοι για τη διαχείριση της ασφάλειας των πληροφοριών που υπάρχουν στους εξυπηρετητές. Είναι ευθύνη τους να εξασφαλίσουν την απαιτούμενη ασφάλεια πάντα ανάλογα βέβαια με το πώς λειτουργεί σε θέματα ασφαλείας ο πάροχός τους.

5.3.2. Ασφάλεια του εξυπηρετητή IaaS

Σε αντίθεση με τα PaaS και SaaS, οι χρήστες του IaaS είναι κυρίως υπεύθυνοι για την ασφάλιση των εξυπηρετητών που υπάρχουν στο υπολογιστικό νέφος [129]. Θεωρώντας δεδομένο ότι όλες οι διαθέσιμες υπηρεσίες IaaS σήμερα εφαρμόζουν την εικονικοποίηση σε επίπεδο εξυπηρετητή, η ασφάλεια στον εξυπηρετητή θα μπορούσε να κατηγοριοποιηθεί στις ακόλουθες εξής δύο περιπτώσεις.

Στην πρώτη περίπτωση έχουμε την εικονική ασφάλεια του λογισμικού. Το επίπεδο του λογισμικού που είναι το μόνο που δουλεύει με πραγματικά μηχανήματα και όχι εικονικά, παρέχει στους πελάτες τη δυνατότητα να δημιουργούν και να καταστρέφουν εικονικά στιγμιότυπα. Η εικονικοποίηση σε επίπεδο εξυπηρετητή μπορεί να επιτευχθεί με τη χρήση ενός από τα μοντέλα εικονικοποίησης, συμπεριλαμβανομένων αυτής σε επίπεδο λειτουργικού συστήματος, σε επίπεδο μηχανημάτων, π.χ. Xen, VMware, Microsoft Hyper-V, και τέλος, έμμεσης εικονικοποίησης που είναι ο συνδυασμός τόσο πραγματικών μηχανημάτων όσο και εικονικών. Η ασφάλιση του επιπέδου που βρίσκεται μεταξύ του υλικού και των εικονικών διακομιστών θεωρείται πολύ σημαντική. Σε μια δημόσια υπηρεσία IaaS, οι πελάτες δεν έχουν πρόσβαση στο επίπεδο λογισμικού και η διαχείρισή του γίνεται αποκλειστικά από τον πάροχο του νέφους.

Στη δεύτερη περίπτωση εμπίπτει η ασφάλιση του λειτουργικού του χρήστη ή αλλιώς η ασφάλιση του εικονικού διακομιστή. Το εικονικό στιγμιότυπο ενός λειτουργικού συστήματος το οποίο είναι στην κορυφή του επιπέδου εικονικοποίησης, είναι ορατό από τους χρήστες μέσω του διαδικτύου και οι χρήστες έχουν πλήρη πρόσβαση σε αυτό.

5.3.3. Ασφάλεια του εικονικού λογισμικού

Από τη στιγμή που ο πάροχος υπολογιστικού νέφους διαχειρίζεται το λογισμικό εικονικοποίησης, το οποίο κάθεται ακριβώς πάνω από το υλικό, οι πελάτες δεν έχουν ούτε ορατότητα ούτε πρόσβαση σε αυτό. Η εικονικοποίηση του υλικού ή του λειτουργικού συστήματος επιτρέπει τον

διαμοιρασμό των πόρων του υλικού μεταξύ πολλών εικονικών μηχανημάτων χωρίς να παρεμβάλλονται μεταξύ τους, έτσι ώστε ο χρήστης να μπορεί να τρέχει διάφορα λειτουργικά συστήματα και εφαρμογές την ίδια χρονική στιγμή στον ίδιο υπολογιστή. Για λόγους απλότητας, θα κάνουμε την υπόθεση ότι οι υπηρεσίες IaaS χρησιμοποιούν τεχνολογίες εικονικοποίησης απευθείας πάνω στο υλικό, γνωστές και ως hypervisors τύπου I, όπως για παράδειγμα τα VMware ESXi, Xen, Oracle VM και Microsoft Hyper-V. Οι συγκεκριμένοι hypervisors υποστηρίζουν πολλά guest λειτουργικά συστήματα συμπεριλαμβανομένων των Microsoft Windows, διαφόρων εκδόσεων του Linux και το OpenSolaris της Sun.

Η εικονικοποίηση του hypervisor είναι το απαραίτητο συστατικό, το οποίο εγγυάται κατακερματισμό και απομόνωση για τα VMs των πελατών σε ένα περιβάλλον πολλαπλής μίσθωσης, μιας και είναι σημαντική η προστασία των hypervisors από μη εξουσιοδοτημένους χρήστες. Μια νέα κούρσα εξοπλισμών μεταξύ των κακόβουλων χρηστών και των αμυνόμενων, των παρόχων, στη σφαίρα της εικονικοποίησης είναι ήδη σε εξέλιξη. Από τη στιγμή που η εικονικοποίηση είναι πολύ σημαντική στην αρχιτεκτονική IaaS του υπολογιστικού νέφους, οποιαδήποτε επίθεση που θα μπορούσε να θέσει σε κίνδυνο την ακεραιότητα των επιμέρους στοιχείων, θα ήταν καταστροφική για ολόκληρη την πελατειακή βάση του υπολογιστικού νέφους. Ένα γεγονός που συνέβη πριν μερικά χρόνια σε μια μικρή εταιρεία στο Ηνωμένο Βασίλειο με όνομα vaserv.com, αποτελεί χαρακτηριστικό παράδειγμα των απειλών για την ασφάλεια του hypervisor. Με την αξιοποίηση μιας άγνωστης ευπάθειας (zero-day vulnerability) στο HyperVM μέσω μιας εικονικής εφαρμογής που κατασκευάστηκε από μια εταιρεία με την επωνυμία Lxlabs, οι κακόβουλοι χρήστες κατάφεραν να καταστρέψουν 100000 ιστοσελίδες που φιλοξενούνταν από το vaserv.com. Η συγκεκριμένη ευπάθεια έδωσε τη δυνατότητα σε κακόβουλους χρήστες να εκτελέσουν ευαίσθητες εντολές UNIX στο σύστημα, συμπεριλαμβανομένης της εντολής rm –rf, η οποία σημαίνει τη μόνιμη διαγραφή όλων των αρχείων του συστήματος. Αξίζει να σημειωθεί ότι λίγες μέρες πριν την εισβολή, ένας ανώνυμος χρήστης έγραψε σε μια ιστοσελίδα κακόβουλων χρηστών με το όνομα milw0rm μια μεγάλη λίστα

από ευπάθειες που δεν είχαν διορθωθεί στο Kloxo [133], ένα διαχειριστικό πακέτο που υπάρχει εντός του HyperVM. Η κατάσταση ήταν ακόμα χειρότερη για τους μισούς περίπου από τους πελάτες της εταιρείας vaserv οι οποίοι είχαν κάνει συμβόλαιο για απλή υπηρεσία, χωρίς πρόσθετη διαχείριση, γεγονός που σήμαινε ότι δεν υπήρχαν αντίγραφα ασφαλείας για τα δεδομένα τους. Με τα προαναφερθέντα δεδομένα παραμένει ασαφές αν οι ιδιοκτήτες αυτών των ιστοσελίδων θα είναι ποτέ σε θέση να ανακτήσουν πλήρως τα απολεσθέντα δεδομένα τους.

Από τα παραπάνω γίνεται φανερό, ότι οι πάροχοι υπολογιστικού νέφους θα πρέπει να θεσπίσουν απαραίτητους ελέγχους ασφαλείας, συμπεριλαμβανομένων του περιορισμού της φυσικής και λογικής πρόσβασης στον hypervisor, καθώς και σε άλλα μισθωτά επίπεδα εικονικοποίησης. Οι πελάτες IaaS θα πρέπει να αντιλαμβάνονται τις διαδικασίες τόσο σε τεχνολογικό όσο και σε επίπεδο ασφάλειας που έχουν συσταθεί από τον πάροχο υπηρεσιών υπολογιστικού νέφους με σκοπό την προστασία του hypervisor. Το γεγονός αυτό θα βοηθήσει τους πελάτες να κατανοήσουν την πλήρωση των κενών ασφαλείας σε σχέση με τα πρότυπα ασφάλειας του εξυπηρετητή, τις πολιτικές που ακολουθούνται και τέλος, τις ρυθμιστικές συμμορφώσεις. Ωστόσο, γενικά, οι πάροχοι χαρακτηρίζονται από έλλειψη διαφάνειας σε αυτό τον τομέα και ίσως οι πελάτες δεν έχουν άλλη επιλογή από την παροχή εμπιστοσύνης στους παρόχους ότι τους εξασφαλίζουν ένα απομονωμένο και ασφαλές εικονικό λειτουργικό σύστημα

5.3.3.1. Απειλές για τον hypervisor

Η ακεραιότητα και η διαθεσιμότητα του hypervisor είναι πρωτίστης σημασίας και είναι το κλειδί για την εγγύηση της ακεραιότητας και διαθεσιμότητας ενός δημόσιου υπολογιστικού νέφους, το οποίο έχει χτιστεί πάνω σε ένα εικονικό περιβάλλον.

Ένας hypervisor με ευπάθειες θα μπορούσε να καταστήσει όλους τους χρήστες ευάλωτους σε κακόβουλους χρήστες. Επιπροσθέτως, οι hypervisors είναι δυνητικά επιρρεπείς σε επιθέσεις ανατροπής

(subversion attacks) [134]. Για την επίδειξη ευπαθειών στο επίπεδο εικονικοποίησης, μέλη μιας ερευνητικής ομάδας ασφάλειας κατέδειξαν την επίθεση «blue pill» στον Xen Hypervisor, κατά τη διάρκεια των συνεδρίων Black Hat [135], τονίζοντας ότι υπάρχουν αρκετοί τρόποι για να εισχωρήσει κάποιος σε ένα επίπεδο εικονικοποίησης εντός του υπολογιστικού νέφους. Παρόλο που οι συγκεκριμένοι ερευνητές εντόπισαν αρκετά προβλήματα στις υλοποιήσεις του Xen, σε γενικές γραμμές είναι θετικοί σχετικά με την προσέγγιση του Xen. Η επίδειξη που έκαναν είχε σκοπό να δείξει στους παρευρισκόμενους την πολυπλοκότητα που υπάρχει στην περίπτωση ασφάλειας εικονικών συστημάτων και την ανάγκη για νέες προσεγγίσεις με στόχο την προστασία των hypervisors από τέτοιου είδους επιθέσεις.

Από τη στιγμή που τα επίπεδα εικονικοποίησης εντός των δημόσιων υπολογιστικών νεφών είναι ως επί το πλείστον ιδιόκτητα και κλειστού κώδικα, αν και ορισμένοι πάροχοι ενδεχομένως να χρησιμοποιούν λογισμικό ανοικτού κώδικα όπως είναι το Xen, ο πηγαίος κώδικας του λογισμικού που χρησιμοποιείται από τους παρόχους υπηρεσιών υπολογιστικού νέφους δεν είναι διαθέσιμος για έλεγχο από την ερευνητική κοινότητα της ασφάλειας.

5.3.4. Ασφάλεια του εικονικού διακομιστή

Οι πελάτες του IaaS έχουν πλήρη πρόσβαση στα εικονικά μηχανήματα τα οποία εξυπηρετούνται και είναι απομονωμένα μεταξύ τους μέσω της τεχνολογίας των hypervisor. Ως εκ τούτου, οι πελάτες είναι υπεύθυνοι για τη διασφάλιση και τη συνεχή διαχείριση της ασφάλειας των εικονικών μηχανημάτων.

Ένα δημόσιο IaaS, όπως για παράδειγμα το EC2 της Amazon, προσφέρει διαδικτυακές υπηρεσίες διεπαφών προγραμματισμού εφαρμογών για την εκτέλεση λειτουργιών διαχείρισης, όπως για παράδειγμα την πρόβλεψη του φόρτου εργασίας, με σκοπό την αντιγραφή ή τη διαγραφή εικονικών διακομιστών στην πλατφόρμα IaaS [99]. Αυτές οι λειτουργίες διαχείρισης του συστήματος, όταν είναι κατάλληλα ενορχηστρωμένες, μπορούν να παρέχουν ευελιξία στους

πόρους και ανάλογα με την υπολογιστική ζήτηση να τους αυξάνουν ή να τους μειώνουν. Ο δυναμικός κύκλος ζωής των εικονικών διακομιστών μπορεί να έχει ως αποτέλεσμα την πολυπλοκότητα, αν η διαδικασία για τη διαχείριση των εικονικών διακομιστών δεν είναι αυτοματοποιημένη με κατάλληλες διεργασίες. Από την πλευρά μιας επίθεσης, οι εικονικοί διακομιστές (Windows, Solaris, Linux) μπορεί να είναι προσβάσιμοι από τον οποιονδήποτε στο διαδίκτυο, οπότε θα πρέπει να ληφθούν κατάλληλα μέτρα σε επίπεδο δικτύου για να περιοριστεί η πρόσβαση στα εικονικά στιγμιότυπα. Τυπικά, ο πάροχος υπολογιστικού νέφους μπλοκάρει όλες τις θύρες για πρόσβαση στους εικονικούς διακομιστές και προτείνει στους πελάτες του να χρησιμοποιούν μόνο τη θύρα 22, δηλαδή τη θύρα Secure Shell - SSH, για τη διαχείριση των στιγμιότυπων των διακομιστών. Η διαχείριση του υπολογιστικού νέφους μέσω των διεπαφών προγραμματισμού εφαρμογών (APIs) προσθέτει ένα ακόμα στρώμα για επιθέσεις και πρέπει να συμπεριληφθεί στο πεδίο της εξασφάλισης των εικονικών διακομιστών σε ένα δημόσιο υπολογιστικό νέφος. Μερικές από τις νέες απειλές στον εξυπηρετητή που υφίστανται σε ένα δημόσιο IaaS περιλαμβάνουν:

- Κλοπή κωδικών που χρησιμοποιούνται για πρόσβαση στη διαχείριση των εξυπηρετητών
- Επίθεση σε ευπαθείς υπηρεσίες που λειτουργούν σε καθιερωμένες θύρες, για παράδειγμα FTP, NetBIOS, SSH
- Κλοπή λογαριασμών που δεν είναι ασφαλισμένοι σωστά, για παράδειγμα ασθενής κωδικός εισαγωγής
- Επίθεση σε συστήματα που δεν είναι ασφαλισμένα σωστά από το τείχος προστασίας του εξυπηρετητή
- Εισαγωγή δούρειων ίππων (Trojan horse) σε συστατικά του λογισμικού τόσο στο VM όσο και σε αντίγραφα του VM, δηλαδή στα εικονικά λειτουργικά συστήματα.

5.3.4.1. Ασφαλίζοντας τους εικονικούς διακομιστές

Η απλότητα της δημιουργίας νέων εικονικών διακομιστών, όταν θεωρηθεί αναγκαίο λόγω του φόρτου εργασίας, ενέχει επιπλέον

κινδύνους, μιας και ενδέχεται να δημιουργηθούν μη ασφαλείς εικονικοί διακομιστές. Άρα, θα πρέπει να εξασφαλίζονται οι εξ ορισμού ρυθμίσεις ασφάλειας, οι οποίες προσφέρουν τη μέγιστη δυνατή προστασία.

Η ασφάλιση των εικονικών διακομιστών στο υπολογιστικό νέφος απαιτεί ισχυρές λειτουργικές διαδικασίες ασφάλειας συνοδευόμενες από την αυτοματοποίηση των συγκεκριμένων διαδικασιών. Στη συνέχεια θα αναφερθούν επιγραμματικά μερικές προτάσεις για ασφάλεια.

Αρχικά, θα πρέπει να γίνεται χρήση μιας εξ ορισμού ασφαλούς ρύθμισης. Οι ρυθμίσεις θα πρέπει να είναι αρκετά αυστηρές τόσο στα διάφορα στιγμιότυπα όσο και στο λειτουργικό σύστημα που θα τρέχει στο δημόσιο υπολογιστικό νέφος. Μια καλή πρακτική για τις εφαρμογές που τρέχουν στο υπολογιστικό νέφος είναι να δημιουργηθούν αντίγραφα των VM, τα οποία να έχουν αποκλειστικά και μόνο τις δυνατότητες και τις υπηρεσίες που είναι απαραίτητες για τη λειτουργία της συγκεκριμένης εφαρμογής. Περιορίζοντας τις δυνατότητες των VM, όχι μόνο περιορίζεται το εύρος ζώνης των επιθέσεων που μπορεί να δεχτεί ο εξυπηρετητής, αλλά επίσης μειώνεται δραστικά ο αριθμός των διορθωτικών προγραμμάτων που θα πρέπει να γίνουν, ώστε η συγκεκριμένη εφαρμογή να είναι απόλυτα ασφαλής.

Επίσης, θα πρέπει να γίνεται λεπτομερής καταγραφή των αντιγράφων των VM, καθώς και των εκδόσεων των λειτουργικών συστημάτων, τα οποία είναι έτοιμα για να παρέχουν εξυπηρέτηση στο υπολογιστικό νέφος. Ο πάροχος IaaS παρέχει μερικά από αυτά τα αντίγραφα. Όταν χρησιμοποιείται ένα εικονικό μηχάνημα από τον πάροχο IaaS, θα πρέπει να έχει το ίδιο επίπεδο ασφάλειας με τους εξυπηρετητές εντός της εταιρείας. Μια καλή εναλλακτική λύση θα ήταν ο κάθε πελάτης να έχει αποκλειστικά τα δικά του αντίγραφα, τα οποία να έχουν το επιθυμητό επίπεδο ασφάλειας που θέλει ο πελάτης.

Επιπλέον, η ακεραιότητα τόσο των δεδομένων όσο και του εικονικού εξυπηρετητή θα πρέπει να προστατεύεται με τη δημιουργία δικλείδων ασφαλείας για την αποφυγή μη εξουσιοδοτημένης πρόσβασης. Αυτό σημαίνει ότι οτιδήποτε πλεονάζει σε σχέση με τους πόρους θα πρέπει να απενεργοποιείται. Επίσης, τα μυστικά κλειδιά που

απαιτούνται για να έχουν πρόσβαση οι εξυπηρετητές στο δημόσιο υπολογιστικό νέφος θα πρέπει να είναι καλά διαφυλαγμένα. Σε γενικές γραμμές, θα πρέπει να απομονωθούν τα κλειδιά κρυπτογράφησης από το υπολογιστικό νέφος και ειδικά από εκεί όπου είναι τα δεδομένα, εκτός και αν είναι απαραίτητα για την αποκρυπτογράφησή τους, και σε αυτή την περίπτωση θα πρέπει να υφίστανται μόνο κατά τη διάρκεια της πραγματικής διαδικασίας αποκρυπτογράφησης. Αν μια εφαρμογή χρειάζεται ένα κλειδί για να κρυπτογραφεί και να αποκρυπτογραφεί τη συνεχή επεξεργασία των δεδομένων, μπορεί να μην είναι δυνατή η προστασία του κλειδιού, δεδομένου ότι θα πρέπει να συνυπάρχει στο ίδιο χώρο με την εφαρμογή. Τέλος, δεν θα πρέπει να συμπεριλαμβάνονται διαπιστευτήρια αυθεντικοποίησης στα εικονικά αντίγραφα εκτός μόνο του κλειδιού για την αποκρυπτογράφηση του συστήματος αρχείων.

Σε ό,τι αφορά κρίσιμες εντολές, οι οποίες με την εκτέλεσή τους να προκαλέσουν κάποια καταστροφή ή κάποιο πρόβλημα, όπως για παράδειγμα η εντολή sudo, θα πρέπει να ζητείται επιπλέον κωδικός για ενεργοποίηση του συγκεκριμένου ρεπερτορίου εντολών. Επίσης, για πρόσβαση από εξωτερικές πηγές, θα πρέπει εκτός του κλασικών ονόματος και κωδικού να πιστοποιείται ο χρήστης και μέσω της συσκευής που χρησιμοποιεί, για να εισέλθει στο σύστημα.

Όπως αναφέρθηκε και σε προηγούμενη παράγραφο, χρυσός κανόνας της ασφάλειας είναι η ελαχιστοποίηση του εύρους των πιθανών εισβολών. Αυτό μπορεί να επιτευχθεί αφενός με τη χρήση κάποιου τείχους προστασίας, το οποίο να επιτρέπει μόνο σε συγκεκριμένες θύρες την πρόσβαση και να κόβει όλες τις υπόλοιπες και αφετέρου με την απεγκατάσταση όλων των υπηρεσιών που δεν χρησιμοποιούνται σε μια εφαρμογή. Για παράδειγμα, αν μια εφαρμογή δεν διαθέτει ως επιλογή την εκτύπωση κάποιων στοιχείων της, θα πρέπει να απεγκατασταθεί η υπηρεσία εκτύπωσης.

Κλείνοντας το συγκεκριμένο θέμα, συμπεραίνουμε ότι θα πρέπει να γίνει εγκατάσταση ενός σύγχρονου συστήματος IDS (Intrusion Detection System) και επιβάλλεται να γίνεται μέσω των ρυθμίσεων ακριβής καταγραφή στα αρχεία καταγραφής συμβάντων όλων των

προσβάσεων τόσο στις εφαρμογές όσο και στα δεδομένα μέσω των εφαρμογών. Τα αρχεία καταγραφής συμβάντων θα πρέπει να διαβάζονται τακτικά και να καταγράφονται τυχόν περίεργες συμπεριφορές τόσο από χρήστες όσο και από εφαρμογές. Όλα αυτά θα πρέπει να τηρούνται ξεχωριστά σε έναν απομονωμένο διακομιστή καταγραφής συμβάντων, στον οποίο θα επιτρέπεται η πρόσβαση μόνο από ειδικευμένα άτομα πάνω στην ασφάλεια ή στην αντιμετώπιση επιθέσεων.

5.4. Υποδομή ασφάλειας σε επίπεδο εφαρμογών

Η ασφάλεια των εφαρμογών ή του λογισμικού θα πρέπει να είναι βασικό στοιχείο του προγράμματος ασφάλειας του συστήματος. Οι περισσότερες εταιρείες με ειδικά προγράμματα ασφάλειας θα πρέπει να καθιερώσουν ένα επιπλέον πρόγραμμα ασφάλειας για να αντιμετωπίσουν το συγκεκριμένο ζήτημα. Ο σχεδιασμός και η υλοποίηση εφαρμογών που θα λειτουργούν στο υπολογιστικό νέφος θα απαιτήσει την εκ νέου αξιολόγηση των τρεχουσών πρακτικών και προτύπων σχετικά με τα υφιστάμενα προγράμματα ασφάλειας. Το φάσμα της ασφάλειας των εφαρμογών εκτείνεται από εφαρμογές για έναν και μόνο χρήστη μέχρι ειδικές και πολύπλοκες εφαρμογές ηλεκτρονικού εμπορίου που χρησιμοποιούνται από εκατομμύρια χρήστες. Οι διαδικτυακές εφαρμογές, όπως για παράδειγμα τα συστήματα διαχείρισης περιεχομένου, οι ηλεκτρονικοί πίνακες και τα φόρουμ συζητήσεων χρησιμοποιούνται τόσο από μικρές όσο και από μεγάλες εταιρείες. Επίσης, ένας μεγάλος αριθμός από εταιρείες αναπτύσσει και διατηρεί διαδικτυακές εφαρμογές κατά παραγγελία για τη λειτουργία τους κάνοντας χρήση ποικίλων διαδικτυακών πλαισίων, όπως για παράδειγμα PHP [136], .NET [137], Ruby on Rails [138], Python [139] κτλ. Σε αυτό το σημείο είναι σκόπιμο να αναφερθεί ότι συνήθως γίνονται λίγες επιθέσεις σε ευπάθειες που αφορούν ιστοσελίδες, επειδή οι κακόβουλοι χρήστες έχουν εστιάσει σε επιθέσεις που ή τους αποφέρουν χρήματα ή τους δίνουν πρόσβαση σε πληροφορίες. Ολοένα και περισσότερο, ωστόσο, οι εξελίξεις στην XSS (Cross Site Scripting) καθώς και άλλων όμοιων

επιθέσεων δείχνουν ότι οι εγκληματίες που αποσκοπούν οικονομικό κέρδος χρησιμοποιούν τις ευπάθειες που προκύπτουν από προγραμματιστικά λάθη στις ιστοσελίδες ως νέους τρόπους για να εισβάλουν σε μια εταιρεία. Σε αυτό το τμήμα, θα περιορίσουμε την ανάλυσή μας στην ασφάλεια των διαδικτυακών εφαρμογών και πιο συγκεκριμένα στις διαδικτυακές εφαρμογές του υπολογιστικού νέφους, τις οποίες οι χρήστες προσπελαύνουν μέσω προγραμμάτων περιήγησης, όπως για παράδειγμα Chrome, Firefox και Microsoft Edge, από οποιονδήποτε υπολογιστική συσκευή συνδεδεμένη στο διαδίκτυο.

Από τη στιγμή που τα προγράμματα περιήγησης έχουν αναδειχτεί ως το μέσο πρόσβασης του τελικού χρήστη σε εφαρμογές του υπολογιστικού νέφους, θεωρείται μείζονος σημασίας για τα προγράμματα ασφάλειας των εφαρμογών να συμπεριλάβουν την ασφάλεια του προγράμματος περιήγησης στο πλαίσιο της ασφάλειας των εφαρμογών. Ο συνδυασμός των προηγούμενων δύο συνιστωσών, καθορίζουν την αποτελεσματικότητα της ασφάλειας η οποία βοηθά στην εμπιστευτικότητα, στην ακεραιότητα και στη διαθεσιμότητα των πληροφοριών που αποτελούν αντικείμενο επεξεργασίας από τις υπηρεσίες υπολογιστικού νέφους.

5.4.1. Απειλές ασφάλειας σε επίπεδο εφαρμογών

Σύμφωνα με την εταιρεία SANS [140], οι ευπάθειες στις διαδικτυακές εφαρμογές τόσο ανοικτού κώδικα όσο και προσωπικές, αντιπροσωπεύουν σχεδόν το μισό του συνολικού αριθμού των ευπαθειών που εντοπίζονται σε περιβάλλοντα υπολογιστικών νεφών. Οι τρέχουσες απειλές εκμεταλλεύονται γνωστές ευπάθειες στις εφαρμογές, συμπεριλαμβανομένων των XSS, SQL injection, την εκτέλεση ύποπτων προγραμμάτων καθώς και άλλες ευπάθειες που προκύπτουν από σφάλματα στο προγραμματισμό ή ελαττώματα κατά τη διάρκεια του σχεδιασμού της εφαρμογής. Οι κακόβουλοι χρήστες, οπλισμένοι με γνώση και εργαλεία, σκανάρουν συνεχώς τις διαδικτυακές εφαρμογές αναζητώντας ευπάθειες, μιας και είναι προσβάσιμες μέσω διαδικτύου. Κατόπιν, εκμεταλλεύονται τις ευπάθειες που ανακαλύπτουν για ποικίλες

παράνομες πράξεις, μεταξύ των οποίων είναι η οικονομική απάτη, η κλοπή πνευματικής ιδιοκτησίας, η μετατροπή αξιόπιστων ιστοσελίδων σε κακόβουλες, οι οποίες εξαπατούν τους χρήστες και τέλος οι απάτες κλοπής διαπιστευτηρίων (phishing scam). Όλα τα διαδικτυακά πλαίσια και όλων των ειδών οι διαδικτυακές εφαρμογές διατρέχουν τον κίνδυνο ελαττωμάτων στην ασφάλεια, ο οποίος μπορεί να κυμαίνεται από ανεπαρκή ρύθμιση της εφαρμογής μέχρι λογικά σφάλματα.

Μια κοινή πρακτική ήταν η χρήση ενός συνδυασμού από περιμετρικούς ελέγχους ασφαλείας και αυστηρά ελεγχόμενη πρόσβαση, τόσο στο δίκτυο όσο και στον εξυπηρετητή, ώστε να προστατευθούν οι διαδικτυακές εφαρμογές που αναπτύσσονταν, τόσο για intranets όσο και για ιδιωτικά υπολογιστικά νέφη, από κακόβουλους χρήστες. Οι διαδικτυακές εφαρμογές που κατασκευάστηκαν για δημόσια υπολογιστικά νέφη θα αντιμετωπίζουν υψηλότερο κίνδυνο σε επίπεδο απειλών, επιθέσεων και πιθανόν να αξιοποιηθεί κάποιο κενό ασφαλείας από κακόβουλους χρήστες με σκοπό κάποια παράνομη δραστηριότητα.

5.4.2. DoS, DDoS και EDoS

Επιπρόσθετα, ο πελάτης θα πρέπει να έχει υπόψη του ότι οι επιθέσεις DoS και DDoS [141], σε επίπεδο εφαρμογών, μπορούν ενδεχομένως να παρεμποδίσουν τις υπηρεσίες του υπολογιστικού νέφους για αρκετά μεγάλο χρονικό διάστημα. Τυπικά, αυτού του είδους οι επιθέσεις προέρχονται από υπολογιστικά συστήματα που είναι συνδεδεμένα στο διαδίκτυο και έχουν παραβιαστεί από κακόβουλους χρήστες. Συνήθως, οι κακόβουλοι χρήστες εισβάλουν και ελέγχουν υπολογιστικά συστήματα που έχουν μολυνθεί από κάποιον ιό ή κάποιο δούρειο ίππο και αυτό σε μερικές περιπτώσεις μπορεί να φτάσει μέχρι πανίσχυρους διακομιστές οι οποίοι δεν είναι σωστά προστατευμένοι. Οι επιθέσεις DoS σε επίπεδο εφαρμογών ενδέχεται να εκδηλωθούν ως υψηλό ποσό όγκου επαναφόρτωσης διάφορων ιστοσελίδων, δημιουργία πολλαπλών αιτημάτων XML μέσω διαδικτυακών υπηρεσιών τόσο σε HTTP όσο και HTTPS, ή ειδικές αιτήσεις από πρωτόκολλα που υποστηρίζονται από την υπηρεσία του υπολογιστικού νέφους.

Δεδομένου ότι αυτές οι κακόβουλες αιτήσεις αναμιγνύονται με την κανονική κυκλοφορία δεδομένων στο δίκτυο, θεωρείται εξαιρετικά δύσκολο το επιλεκτικό φιλτράρισμα της κακόβουλης κυκλοφορίας, χωρίς να επηρεάζεται η υπηρεσία στο σύνολό της.

Εκτός από τη διακοπή των υπηρεσιών του υπολογιστικού νέφους, με αποτέλεσμα την κακή εμπειρία του χρήστη σχετικά με τις επιπτώσεις σε επίπεδο υπηρεσιών, μια στοχευμένη και πετυχημένη επίθεση DoS μπορεί να στεγνώσει τον προϋπολογισμό της εταιρείας σχετικά με τη χρήση του υπολογιστικού νέφους, μιας και θα γίνονται θηριώδεις καταναλώσεις πόρων σε πολύ μικρά διαστήματα. Οι επιθέσεις DoS σε εφαρμογές που μισθώνονται σύμφωνα με τη χρήση θα έχουν ως αποτέλεσμα τη δραματική αύξηση του χρηματικού ποσού που θα πρέπει να πληρώσει η εταιρεία στον πάροχο υπολογιστικού νέφους, μιας και θα υπάρχει αυξημένη χρήση στο δίκτυο, στην CPU και στην κατανάλωση αποθηκευτικών χώρων. Αυτού του είδους η επίθεση έχει χαρακτηριστεί ως Economic Denial of Service – EDoS [142].

Τα λιγότερα εμπόδια για τις μικρές και μεσαίου μεγέθους εταιρείες να υιοθετήσουν το υπολογιστικό νέφος για νόμιμη χρήση, βοηθούν επιπλέον τους κακόβουλους χρήστες να εκπληρώσουν τις προθέσεις τους. Με την χρήση κλεμμένων λογαριασμών υπολογιστικού νέφους, οι κακόβουλοι χρήστες θα μπορούν να ενώνουν υπολογιστικούς πόρους με σκοπό την επίτευξη μεγάλης υπολογιστικής ισχύος με μηδαμινό κόστος. Στο, όχι και τόσο, μακρινό μέλλον, θα γίνουμε μάρτυρες επιθέσεων DoS που ξεκινούν από IaaS ή PaaS νόμιμων χρηστών ενάντια σε άλλες υπηρεσίες του υπολογιστικού νέφους, με τους νόμιμους χρήστες να έχουν πλήρη άγνοια. Τέλος, αρχίζει να διαφαίνεται στον ορίζοντα ο ορισμός του σκοτεινού υπολογιστικού νέφους (Dark Cloud) που θεωρείται παρεμφερής με τον ορισμό του σκοτεινού διαδικτύου (Dark Internet) η αλλιώς (Deep Web) [143].

5.4.3. Ασφάλεια στον τελικό χρήστη

Ο τελικός χρήστης, ως πελάτης μιας υπηρεσίας υπολογιστικού νέφους, είναι υπεύθυνος για την υλοποίηση της ασφάλειας στο σύστημα

που χρησιμοποιεί για να εισέρχεται στο υπολογιστικό νέφος. Οφείλει να υλοποιήσει όλες τις διαδικασίες για να προστατεύσει το υπολογιστικό του σύστημα και επίσης θα πρέπει να μην χρησιμοποιεί το συγκεκριμένο σύστημα για μη ασφαλή πλοήγηση στο διαδίκτυο, δηλαδή σε περίεργες ιστοσελίδες. Στις διαδικασίες που θα πρέπει να υλοποιήσει συμπεριλαμβάνονται η χρήση λογισμικού για την ασφάλεια, αντιϊκό πρόγραμμα, τείχος προστασίας, συνεχής αναβάθμιση του λογισμικού και ένα σύστημα ανίχνευσης εισβολών. Η τάση που έχει επικρατήσει είναι ότι το πρόγραμμα περιήγησης είναι «το λειτουργικό σύστημα» και θέλει να περάσει στους χρήστες το μήνυμα ότι τα προγράμματα περιήγησης στο διαδίκτυο έχουν γίνει τα πανταχού παρόντα «λειτουργικά συστήματα» για κατανάλωση των υπηρεσιών του υπολογιστικού νέφους. Όλα τα προγράμματα περιήγησης στο διαδίκτυο έχουν ευπάθειες στο λογισμικό και αυτό καθιστά τους τελικούς χρήστες ευάλωτους σε επιθέσεις. Ως εκ τούτου, η καλύτερη σύσταση είναι ότι οι χρήστες του υπολογιστικού νέφους θα πρέπει να λάβουν όλα τα κατάλληλα μέτρα για να προστατεύουν τα προγράμματα περιήγησής τους από επιθέσεις. Για να επιτευχθεί ασφάλεια από τον πάροχο μέχρι τον τελικό χρήστη, είναι απαραίτητο για τους χρήστες να διατηρούν όσο το δυνατό πιο ασφαλές γίνεται το πρόγραμμα περιήγησης. Αυτό σημαίνει ότι το πρόγραμμα περιήγησης θα πρέπει να συνεχώς ενημερωμένο και δεν θα πρέπει να εγκαθίστανται αγνώστου προελεύσεως πρόσθετα. Επί του παρόντος, αν και κάποια πρόσθετα των προγραμμάτων περιήγησης σχετικά με την ασφάλεια δεν είναι διαθέσιμα στο εμπόριο, οι χρήστες θα πρέπει να ελέγχουν σε συχνή βάση τον κατασκευαστή του λογισμικού τους για ενημερώσεις ασφαλείας, να χρησιμοποιούν την επιλογής της αυτόματης ενημέρωσης και να εγκαθιστούν άμεσα τα τυχόν patches για να διατηρήσουν την ασφάλεια του τελικού χρήστη σε όσο το δυνατόν υψηλότερο επίπεδο.

5.4.4. Ποιος είναι υπεύθυνος για την ασφάλεια των διαδικτυακών εφαρμογών στο υπολογιστικό νέφος

Ανάλογα με το μοντέλο διάθεσης υπηρεσιών του υπολογιστικού νέφους και το συμβόλαιο παροχής υπηρεσιών, το πεδίο των

αρμοδιοτήτων της ασφάλειας πέφτει στους ώμους τόσο του πελάτη όσο και του παρόχου του υπολογιστικού νέφους. Το κλειδί για να καταλάβει κάποιος τι είδους ευθύνες έχει σχετικά με την ασφάλεια είναι σχετίζεται με τις ευθύνες που έχει ο πάροχος [125]. Στο πλαίσιο αυτό, πρόσφατες έρευνες σχετικά με την ασφάλεια τόνισαν το γεγονός ότι η έλλειψη διαφάνειας στους ελέγχους ασφαλείας και στις πρακτικές που χρησιμοποιούνται από τους παρόχους είναι ένα σοβαρό εμπόδιο για την ευρεία υιοθέτηση του υπολογιστικού νέφους.

Ξεκινώντας πρέπει να τονιστεί ότι οι πελάτες του υπολογιστικού νέφους δεν έχουν την απαιτούμενη διαφάνεια στον τομέα των ευπαθειών των εφαρμογών του υπηρεσιών του υπολογιστικού νέφους. Το γεγονός αυτό αποτρέπει τους πελάτες από τη διαχείριση των κινδύνων που μπορεί να επέλθει από τα ευπαθή σημεία. Επιπλέον, επειδή η λειτουργία του λογισμικού από τους παρόχους θεωρείται ως κάτι ιδιόκτητο, οι πάροχοι εμποδίζουν τους ερευνητές ασφάλειας να αναλύσουν το λογισμικό τους για διάφορα κενά ασφαλείας και ευπάθειες. Εννοείται ότι οι πάροχοι που χρησιμοποιούν λογισμικό ανοικτού κώδικα αποτελούν εξαίρεση στο προηγούμενο. Λόγω της έλλειψης διαφάνειας, οι πελάτες δεν έχουν άλλη επιλογή από το να εμπιστεύονται τους παρόχους τους ότι θα αποκαλύψουν και θα να διορθώσουν οποιαδήποτε νέα ευπάθεια μπορεί να προκύψει και θα επηρεάζει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα της εφαρμογής τους. Στις αρχές του υπολογιστικού νέφους, κανένας από τους γνωστούς παρόχους IaaS, PaaS και SaaS δεν συμμετείχε στο πρόγραμμα Common Vulnerability and Exposures (CVE) [144]. Το αποτέλεσμα, συγκεκριμένα για το AWS, είναι ότι χρειάστηκαν σχεδόν οκτώ μήνες για να διορθώσει μια ευπάθεια που είχε αποκαλυφθεί. Η συγκεκριμένη ευπάθεια ήταν μια κρυπτογραφική αδυναμία στον κώδικα εισόδου των χρηστών και επηρέαζε τις υπηρεσίες SimpleDB και EC2. Αξίζει να σημειωθεί ότι η ευπάθεια δεν δημοσιοποιήθηκε μέχρι να διορθωθεί. Ο ερευνητής που ανακάλυψε την ευπάθεια τόνισε ότι η Amazon πήρε πολύ σοβαρά το ζήτημα και ο μεγάλος χρόνος διόρθωσής του ήταν απλά λόγω του μεγάλου φόρτου εργασίας που έπρεπε να γίνει με σκοπό την διόρθωσή του.

Οι εταιρικοί πελάτες θα πρέπει να κατανοήσουν την πολιτική γνωστοποίησης των ευπαθειών των υπηρεσιών του υπολογιστικού νέφους και να το αξιολογήσουν κατάλληλα ανάλογα με τρόπο λειτουργίας του παρόχου τους σε τέτοια ζητήματα. Οι ακόλουθες παράγραφοι αναφέρονται σε γενικές γραμμές στην ασφάλεια των διαδικτυακών υπηρεσιών στο πλαίσιο των μοντέλων διάθεσης υπηρεσιών του υπολογιστικού νέφους.

5.4.5. Ασφάλεια εφαρμογών SaaS

Το μοντέλο SaaS υπαγορεύει ότι ο πάροχος διαχειρίζεται ολόκληρη τη σουίτα των εφαρμογών που διανέμονται στους χρήστες. Ως εκ τούτου, οι πάροχοι SaaS είναι σε μεγάλο βαθμό υπεύθυνοι για την ασφάλιση των εφαρμογών και στοιχείων που προσφέρουν στους πελάτες τους. Από την άλλη μεριά, οι πελάτες είναι συνήθως υπεύθυνοι για τις επιχειρησιακές λειτουργίες ασφάλειας, συμπεριλαμβανομένων των χρηστών και της διαχείρισης της πρόσβασης, όπως αυτή υποστηρίζεται από τον πάροχο. Μια κοινή πρακτική για τους υποψήφιους πελάτες είναι να ζητούν πληροφορίες σχετικές με τις πρακτικές ασφάλειας που ακολουθεί ο πάροχος. Μερικοί πελάτες προχωρούν σε πρόσληψη ανεξάρτητων παρόχων ασφάλειας για να διεξάγουν δοκιμές ευπάθειας των εφαρμογών SaaS που χρησιμοποιούν, με τη συγκατάθεση του παρόχου, με σκοπό τη λήψη ανεξάρτητων εγγυήσεων. Ωστόσο, οι δοκιμές ευπάθειας των εφαρμογών είναι δαπανηρές και ενδεχομένως ο πάροχος να μην συμφωνεί με αυτό το είδος της επαλήθευσης.

Ιδιαίτερη προσοχή πρέπει να δοθεί στα συστήματα ελέγχου πρόσβασης και αυθεντικοποίησης που προσφέρει ο πάροχος SaaS [126]. Συνήθως αυτό είναι και ο μοναδικός διαθέσιμος έλεγχος ασφάλειας για τη διαχείριση των κινδύνων στις πληροφορίες. Οι περισσότερες υπηρεσίες, συμπεριλαμβανομένων και αυτών από τις Saleforce.com και Google, προσφέρουν κάποια διεπαφή-εργαλείο μέσω διαδικτύου για τη διαχείριση του ελέγχου πρόσβασης και της αυθεντικοποίησης. Μερικές εφαρμογές SaaS, όπως για παράδειγμα οι Google Apps, έχουν ενσωματωμένα χαρακτηριστικά, τα οποία μπορούν να χρησιμοποιήσουν

οι χρήστες για να δώσουν δικαιώματα πρόσβασης, ανάγνωσης και γραφής, σε άλλους χρήστες. Ωστόσο, τα χαρακτηριστικά διαχείρισης των δικαιωμάτων μπορεί να μην είναι εξειδικευμένα, δεν περιορίζουν την πρόσβαση στις εφαρμογές και θα μπορούσαν να έχουν αδυναμίες, οι οποίες να μην είναι σύμφωνες με το πρότυπο ασφάλειας μιας εταιρείας. Ένα παράδειγμα που αισθητοποιεί το προηγούμενο ζήτημα είναι ο μηχανισμός που έχουν τα Google Docs [17] σχετικά με την διαχείριση των εικόνων που βρίσκονται προσαρτημένες μέσα σε κείμενα, όπως επίσης και τα δικαιώματα πρόσβασης σε παλιότερες εκδόσεις ενός εγγράφου. Προφανώς, οι ενσωματωμένες εικόνες που είναι αποθηκευμένες στα Google Docs δεν προστατεύονται με τον ίδιο τρόπο που προστατεύεται το έγγραφο μέσω δικαιωμάτων πρόσβασης. Αυτό σημαίνει ότι αν κάποιος χρήστης έχει διαμοιράσει κάποιο έγγραφο, το οποίο εμπεριέχει διάφορες εικόνες, οι άλλοι χρήστες, που τους είχε διαμοιραστεί το έγγραφο, θα έχουν την δυνατότητα να βλέπουν αυτές τις εικόνες ακόμα και αν ο χρήστης σταματήσει τον διαμοιρασμό. Το συγκεκριμένο τέχνασμα ελέγχου πρόσβασης πρωτοεμφανίστηκε σε ένα blog και έτσι έγινε γνωστό και στην ίδια την Google, η οποία παρόλο που ενημερώθηκε για το ζήτημα έδωσε ως απάντηση ότι αυτού του είδους οι ανησυχίες από μέρος των χρηστών δεν συνιστούν σημαντικό κίνδυνο για την ασφάλειά τους.

Ένα άλλο περιστατικό που σχετιζόταν με τα Google Docs ήταν μια δυσλειτουργία στην ιδιωτικότητα των χρηστών μέσω μη θεμιτής παροχής πρόσβασης σε τρίτους χρήστες, των εγγράφων κειμένου και παρουσίασης που είχαν αποθηκευτεί στην υπηρεσία αποθήκευσης των Google Docs. Αν και τα συγκεκριμένα έγγραφα διαμοιράστηκαν μόνο με χρήστες με τους οποίους οι συντάκτες των εγγράφων είχαν κοινόχρηστα αρχεία και όχι με όλο τον κόσμο του υπολογιστικού νέφους, το συγκεκριμένο πρόβλημα καταδεικνύει την ανάγκη για αξιολόγηση και κατανόηση των μηχανισμών ελέγχου πρόσβασης στο υπολογιστικό νέφος.

Οι πελάτες του υπολογιστικού νέφους θα πρέπει να κατανοήσουν τους μηχανισμούς ελέγχου πρόσβασης που παρέχονται, συμπεριλαμβανομένων της υποστήριξης για ισχυρό έλεγχο

αυθεντικοποίησης και της διαχείρισης των δικαιωμάτων που βασίζονται σε ρόλους και λειτουργίες, και να λάβουν τα απαιτούμενα μέτρα που είναι αναγκαία για την προστασία της πληροφορίας που είναι αποθηκευμένη στο υπολογιστικό νέφος. Επιπλέον, θα πρέπει να εφαρμόζονται έλεγχοι στη διαδικασία της πρόσβασης των διαχειριστών στο αντίστοιχο εργαλείο διαχείρισης του SaaS, και να επιβληθεί διαχωρισμός καθηκόντων για την προστασία της εφαρμογής από εσωτερικές απειλές. Σύμφωνα με τις πρακτικές των προτύπων ασφάλειας, οι πελάτες θα πρέπει να εφαρμόσουν μια πολιτική ισχυρών κωδικών, η οποία θα αναγκάζει τους χρήστες να επιλέγουν ισχυρούς κωδικούς πρόσβασης, όταν αυθεντικοποιούνται σε μια εφαρμογή.

Μια κοινή πρακτική για τους παρόχους SaaS είναι να αναμιγνύουν τα δεδομένα των πελατών τους, δομημένα και αδόμητα, σε έναν ενιαίο εικονικό αποθηκευτικό χώρο και να στηρίζονται μόνο σε κάποια στοιχεία, σε μορφή ετικέτας (tagging), για να μπορούν να επιτύχουν την απομόνωση των δεδομένων μεταξύ των πελατών τους [99]. Σε ένα μοντέλο αποθήκευσης δεδομένων πολλαπλής μίσθωσης, στο οποίο η κρυπτογράφηση ενδεχομένως να μην είναι δυνατή εξαιτίας προβλημάτων στη διαχείριση των κλειδιών ή σε άλλα σχεδιαστικά εμπόδια, εισάγεται μια ειδική ετικέτα (tag) στα δεδομένα μαζί με ένα μοναδικό αναγνωριστικό πελάτη. Αυτό το μοναδικό προσδιοριστικό σε συνδυασμό με την ετικέτα καθιστά δυνατή την επιβολή απομόνωσης μεταξύ των δεδομένων των πελατών κατά τη διάρκεια της επεξεργασίας των δεδομένων. Είναι κατανοητό ότι το σύστημα που επιβάλλει τη συγκεκριμένη απομόνωση των δεδομένων θα μπορούσε να γίνει ευπαθές κατά τη διάρκεια διάφορων αναβαθμίσεων στο λογισμικό που κάνει ο πάροχος του υπολογιστικού νέφους. Ως εκ τούτου, οι πελάτες θα πρέπει να κατανοήσουν την εικονική αρχιτεκτονική αποθήκευσης δεδομένων και τους μηχανισμούς πρόληψης που χρησιμοποιούν οι πάροχοι για να εγγυηθούν τη στεγανότητα και την απομόνωση των δεδομένων σε ένα εικονικό περιβάλλον πολλαπλής μίσθωσης.

Κοινός κανόνας είναι ότι οι γνωστοί πάροχοι SaaS, όπως για παράδειγμα οι Salesforce.com, Microsoft και Google, επενδύουν στην ασφάλεια του λογισμικού τους και στην πρακτική διασφάλισης της

ασφάλειας ως μέρος του κύκλου ζωής του λογισμικού που προσφέρουν. Ωστόσο, δεδομένου ότι δεν υπάρχει κάποιο βιομηχανικό πρότυπο για την αξιολόγηση της ασφάλειας του λογισμικού, είναι σχεδόν αδύνατο να τεθεί θέμα σύγκρισης μεταξύ των παρόχων για το επίπεδο ασφάλειας που προσφέρουν στο λογισμικό τους.

5.4.6. Ασφάλεια εφαρμογών PaaS

Σε γενικές γραμμές οι πάροχοι PaaS εμπίπτουν σε δύο κύριες κατηγορίες. Στην πρώτη είναι οι πάροχοι λογισμικού αποκλειστικά, όπως για παράδειγμα οι Bungee, Etelos, GigaSpaces και Eucalyptus, και στη δεύτερη είναι οι πάροχοι υπηρεσιών νέφους, όπως οι Google App Engine, Saleforce.com, Force.com και Microsoft Azure.

Οι εταιρείες που έχουν ένα ιδιωτικό νέφος μπορούν να χρησιμοποιήσουν το λογισμικό PaaS για να χτίσουν μια λύση για εσωτερική χρήση. Επί του παρόντος, δεν υπάρχουν δημόσια νέφη για τα οποία να είναι γνωστό ότι κάνουν χρήση προγραμμάτων ανοικτού κώδικα, όπως είναι το Eucalyptus [145], παρόλο που το ίδιο το Eucalyptus παρέχει ένα υποτυπώδες περιβάλλον νέφους για προγραμματιστές. Ως εκ τούτου, δεδομένου του πρώιμου σταδίου στην ανάπτυξη του PaaS, δεν θα αναφερθούμε στην ασφάλεια του αυτόνομου λογισμικού PaaS. Παρόλα αυτά, συνιστάται οι εταιρείες να αξιολογούν το λογισμικό PaaS, να εκτελούν ανάλυση κινδύνου και να εφαρμόζουν πρότυπα ασφάλειας παρόμοια με εκείνα που θα είχαν σε ένα κοινό λογισμικό στην εταιρεία τους.

Το PaaS εξ ορισμού προσφέρει ένα ολοκληρωμένο περιβάλλον για σχεδιασμό, ανάπτυξη, δοκιμή και υποστήριξη ποικίλων εφαρμογών, οι οποίες έχουν αναπτυχθεί στη γλώσσα που υποστηρίζει η πλατφόρμα. Η ασφάλεια των εφαρμογών PaaS περιλαμβάνει δύο επίπεδα. Το πρώτο επίπεδο αφορά την ασφάλεια της ίδιας της πλατφόρμας PaaS και το δεύτερο επίπεδο την ασφάλεια των εφαρμογών των χρηστών που έχουν αναπτυχθεί πάνω στη συγκεκριμένη πλατφόρμα.

Σε γενικές γραμμές οι πάροχοι PaaS, όπως για παράδειγμα οι Google, Microsoft και Force.com, είναι υπεύθυνοι για την ασφάλεια της όλης πλατφόρμας, πράγμα που σημαίνει ότι θα πρέπει να υπάρχει ασφάλεια τόσο στην πλατφόρμα όσο και στις εφαρμογές των χρηστών. Από τη στιγμή που οι εφαρμογές που υπάρχουν σε ένα PaaS μπορεί να χρησιμοποιούν και εφαρμογές τρίτων κατασκευαστών, καθένας από τους κατασκευαστές της κάθε εφαρμογής είναι υπεύθυνος για την ασφάλεια της εφαρμογής που κατασκευάζει. Συνεκδοχικά, οι πελάτες θα πρέπει να κατανοήσουν τη συνάφεια της εφαρμογής τους με όλες τις υπηρεσίες και να αξιολογήσουν όλους τους κινδύνους που αφορούν τις εφαρμογές από τρίτους. Σε πρώιμα στάδια του υπολογιστικού νέφους, οι πάροχοι ήταν απρόθυμοι να μοιραστούν πληροφορίες που αφορούν στην ασφάλεια της πλατφόρμας με το επιχείρημα ότι οι εν λόγω πληροφορίες σχετικά με την ασφάλεια θα έδινε ένα πλεονέκτημα για επιθέσεις σε κακόβουλους χρήστες. Ωστόσο, οι εταιρικοί πελάτες θα πρέπει να απαιτήσουν διαφάνεια από τους παρόχους τους και να αναζητήσουν πληροφορίες που είναι αναγκαίες για την εκτίμηση της επικινδυνότητας του συστήματος και της τρέχουσας διαχείρισης της ασφάλειάς του.

5.4.6.1. Διαχείριση των εφαρμογών μέσω PaaS

Στο μοντέλο πολλαπλής μίσθωσης του PaaS, οι βασικές αρχές ασφάλειας είναι ο περιορισμός και η απομόνωση των εφαρμογών μεταξύ των χρηστών. Στο συγκεκριμένο μοντέλο, η πρόσβαση στα δεδομένα θα πρέπει να περιορίζεται μόνο στους χρήστες της εταιρείας και στις εφαρμογές που έχει στην κατοχή της η εταιρεία. Το μοντέλο ασφάλειας που υπάρχει σε ένα PaaS είναι πνευματική περιουσία του παρόχου του υπολογιστικού νέφους, και θεωρείται απαραίτητο για την παροχή της αρχιτεκτονικής «sandbox» σε ένα περιβάλλον πολλαπλής μίσθωσης χρηστών [99]. Ως εκ τούτου, το χαρακτηριστικό «sandbox» που υπάρχει στο PaaS είναι πρωτίστης σημασίας για τη διατήρηση της εμπιστευτικότητας και της ακεραιότητας των εφαρμογών που υπάρχουν στο PaaS. Οι πάροχοι του νέφους είναι υπεύθυνοι για την παρακολούθηση νέων ευπαθειών και λαθών, τα οποία μπορεί να

εκθέσουν σε κίνδυνο την πλατφόρμα PaaS και να ξεφύγουν από την αρχιτεκτονική «sandbox». Αυτού του είδους η κατάσταση συνιστά το χειρότερο δυνατό σενάριο για μια υπηρεσία PaaS, από τη στιγμή που οι επιπτώσεις στα προσωπικά δεδομένα των πελατών είναι άγνωστες και ενδεχομένως να είναι επιζήμιες για τις επιχειρήσεις τους. Για τη σοβαρότητα του προηγούμενου, οι εταιρικοί πελάτες θα πρέπει να ζητούν πληροφορίες από τον πάροχο του νέφους σχετικές με την αρχιτεκτονική που χρησιμοποιεί για τον περιορισμό και την απομόνωση των εφαρμογών τους.

Επίσης, η παρακολούθηση του δικτύου και του εξυπηρετητή έξω από την πλατφόρμα PaaS είναι ευθύνη του παρόχου PaaS. Πιο συγκεκριμένα, ο πάροχος PaaS θα πρέπει να παρακολουθεί τους διαμοιραζόμενους πόρους, τόσο του δικτύου όσο και των υποδομών, που φιλοξενούν τις εφαρμογές του πελάτη. Οι πελάτες του PaaS θα πρέπει να κατανοήσουν τον τρόπο με τον οποίο οι πάροχοι PaaS διαχειρίζονται την πλατφόρμα τους σε θέματα ασφάλειας, συμπεριλαμβανομένου μεταξύ άλλων του ελέγχου των επιμέρους τμημάτων που την απαρτίζουν.

5.4.7. Διαχείριση της ασφάλειας από μέρους του χρήστη

Οι προγραμματιστές PaaS θα πρέπει να εξοικειωθούν με ειδικά API για την ανάπτυξη και διαχείριση των μονάδων λογισμικού που επιβάλλουν ελέγχους ασφαλείας. Επιπρόσθετα, έχοντας σαν δεδομένο ότι κάθε API είναι μοναδικό για μια υπηρεσία PaaS, οι προγραμματιστές θα πρέπει να εξοικειωθούν με συγκεκριμένα χαρακτηριστικά ασφάλειας της συγκεκριμένης πλατφόρμας, τα οποία είναι στη διάθεσή τους με τη μορφή αντικειμένων ασφάλειας και υπηρεσιών διαδικτύου με σκοπό τη ρύθμιση των λειτουργιών της αυθεντικοποίησης και του ελέγχου πρόσβασης στην εφαρμογή. Το γεγονός ότι μέχρι πρότινος δεν υπήρχε κάποιο πρότυπο για σχεδιασμό ενός API σε PaaS ή ότι δεν καταβλήθηκε προσπάθεια από τους παρόχους του υπολογιστικού νέφους να αναπτύξουν ένα ευρέως διαδεδομένο και συνεπές API μεταξύ των υπολογιστικών νεφών, είναι ο λόγος που καθιστά τη μεταφορά μιας

εφαρμογής από ένα υπολογιστικό νέφος σε ένα άλλο δύσκολο και χρονοβόρο έργο. Επί του παρόντος, η Google υποστηρίζει μόνο Python και Java, και η SalesForce.com αντίστοιχα υποστηρίζει μόνο τη δική της γλώσσα που την ονομάζει Apex [146]. Η γλώσσα Apex διαφέρει από τις άλλες γλώσσες προγραμματισμού όπως C++, java, .NET, γιατί έχει ένα πολύ συγκεκριμένο πεδίο εφαρμογής και αυτό είναι αποκλειστικά ο προγραμματισμός σε πλατφόρμες της SalesForce.com [147]. Στο πλαίσιο αυτό, οι υπηρεσίες του υπολογιστικού νέφους έχουν τη δυνατότητα να διατηρούν τους πελάτες τους πιο δυναμικά από ότι το παραδοσιακό μοντέλο αδειοδότησης λογισμικού. Εν κατακλείδι, πρέπει να γίνει κατανοητό ότι η απουσία ενός πρότυπου API έχει επιπτώσεις τόσο στην διαχείριση της ασφάλειας μιας εφαρμογής όσο και στη δυνατότητα μεταφοράς των εφαρμογών μεταξύ των παρόχων υπηρεσιών υπολογιστικών νεφών.

Οι προγραμματιστές θα πρέπει να περιμένουν από τους παρόχους PaaS να προσφέρουν ένα σύνολο από χαρακτηριστικά ασφάλειας για καθένα από τα API, συμπεριλαμβανομένων της αυθεντικοποίησης των χρηστών, της δυνατότητας καθολικής σύνδεσης (Single Sign On – SSO), τη δυνατότητα ελέγχου πρόσβασης μέσω κατάλληλων δικαιωμάτων πρόσβασης και τέλος την υποστήριξη των πρωτοκόλλων SSL και TLS. Επί του παρόντος, δεν υπάρχει κανένα πρότυπο σχετικά με τη διαχείριση ασφάλειας. Οι πάροχοι υπηρεσιών υπολογιστικών νεφών έχουν μοναδικά μοντέλα ασφάλειας, και τα χαρακτηριστικά ασφάλειας ποικίλλουν από πάροχο σε πάροχο. Στην περίπτωση της Google, ο προγραμματιστής μπορεί να χρησιμοποιήσει αντικείμενα Python η Java για να ρυθμίσει το προφίλ του χρήστη και να επιλέξει το HTTPS [38] ως πρωτόκολλο μεταφοράς δεδομένων. Παρόμοια, η SalesForce.com παρέχει ένα API μέσω του Apex για τη ρύθμιση των παραμέτρων ασφάλειας, τη διαχείριση των στιγμιότυπων και την ανάθεση σε ορισμένες θύρες TCP της δυνατότητας για απευθείας επικοινωνία μεταξύ των εφαρμογών με χρήση αντικειμένων Apex [146].

Με βάση την έως τώρα έρευνα του γράφοντος, στην πλειοψηφία των παρόχων PaaS τα χαρακτηριστικά ασφάλειας που είναι διαθέσιμα περιορίζονται στη ρύθμιση των πρωτοκόλλων SSL και TLS, στην

υποτυπώδη διαχείριση δικαιωμάτων και αυθεντικοποίηση των χρηστών με διάφορους τρόπους, ανάλογα με τον πάροχο. Σε λίγες μόνο περιπτώσεις, παρέχεται επιπλέον ασφάλεια μέσω της γλώσσας SAML (Security Assertion Markup Language) [148].

5.4.8. Ασφάλεια εφαρμογών IaaS

Οι πάροχοι IaaS, για παράδειγμα το Amazon EC2 και το Microsoft Azure, χειρίζονται τις εφαρμογές των πελατών τους σε εικονικά στιγμιότυπα ως ένα μαύρο κουτί και ως εκ τούτου είναι άγνωστες σε αυτούς οι λειτουργίες και η διαχείριση των εφαρμογών των πελατών τους. Ολόκληρη η υποδομή, δηλαδή οι εφαρμογές των πελατών, η πλατφόρμα εκτέλεσης κ.α., τρέχει στους εικονικούς διακομιστές του πελάτη και είναι αντικείμενο διαχείρισης αποκλειστικά από αυτούς. Για το λόγο αυτό, οι πελάτες έχουν την αποκλειστική και πλήρη ευθύνη για την ασφάλεια των εφαρμογών που αναπτύσσουν στο υπολογιστικό νέφος. Συνεπώς, οι πελάτες δεν θα πρέπει να περιμένουν καμία βοήθεια για την ασφάλεια της εφαρμογής τους από τους παρόχους, εκτός από τις βασικές κατευθύνσεις και τα χαρακτηριστικά που σχετίζονται με την πολιτική του τείχους προστασίας, η οποία μπορεί να επηρεάζει τη δυνατότητα επικοινωνίας μιας εφαρμογής με άλλες εφαρμογές, χρήστες ή υπηρεσίες εντός ή εκτός του υπολογιστικού νέφους.

Οι διαδικτυακές εφαρμογές που αναπτύσσονται σε ένα δημόσιο υπολογιστικό νέφος θα πρέπει να είναι σχεδιασμένες σύμφωνα με κάποιο μοντέλο ασφάλειας του διαδικτύου και να έχουν ενσωματωμένα κάποια πρότυπα ασφάλειας και καταστολής ενάντια στις γνωστές απειλές του διαδικτύου. Σε τήρηση των πρακτικών ανάπτυξης ασφάλειας, οι εφαρμογές θα πρέπει να ελέγχονται ανά τακτά χρονικά διαστήματα για ευπάθειες, και κυρίως, η ασφάλεια θα πρέπει να ενσωματωθεί μέσα στον κύκλο ανάπτυξης της εφαρμογής (Software Development Life Cycle - SDLC) [149]. Οι πελάτες είναι οι αποκλειστικοί υπεύθυνοι για την τήρηση της ασφάλειας τόσο των εφαρμογών τους, όσο και του περιβάλλοντος αυτών, για να προστατεύουν το σύστημα από κακόβουλους χρήστες, από ιούς καθώς και ευπάθειες, τις οποίες μπορεί

να ανακαλύψουν κάποιοι και να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση, τόσο στις εφαρμογές τους όσο και στα δεδομένα τους εντός του υπολογιστικού νέφους. Ιδιαίτερη μνεία γίνεται στο να σχεδιάζονται οι εφαρμογές μέσω ενός μοντέλου ελάχιστων δικαιωμάτων (least privileges), όπως ονομάζεται, δηλαδή η εφαρμογή να εκτελείται κάνοντας χρήση ενός μη προνομιακού λογαριασμού, όπως είναι ο διαχειριστής ή ο υπερχρήστης.

Οι προγραμματιστές που προγραμματίζουν εφαρμογές για IaaS θα πρέπει να υλοποιήσουν τα δικά τους χαρακτηριστικά, για να χειρίζονται την αυθεντικοποίηση και τον έλεγχο πρόσβασης των χρηστών. Σύμφωνα με τις πρακτικές διαχείρισης ταυτότητας των χρηστών των επιχειρήσεων, οι εφαρμογές του υπολογιστικού νέφους θα πρέπει να είναι σχεδιασμένες ώστε να αξιοποιούν χαρακτηριστικά αυθεντικοποίησης υπηρεσίας μέσω κάποιας εταιρείας παροχής ταυτότητας (Identity Provider), όπως οι OpenSSO [150], Oracle IAM [151], IBM [18], CA, μέσω παροχής ταυτότητας από τρίτο, όπως οι Ping Identity [152], Symplified [153], TriCipher. Οποιεσδήποτε άλλες υλοποιήσεις της αυθεντικοποίησης, του ελέγχου πρόσβασης και της τήρησης αρχείων καταγραφής (AAA – Authentication, Authorization, Accounting) μπορεί να είναι ο αδύναμος κρίκος στην αλυσίδα της ασφάλειας, αν δεν έχουν εφαρμοστεί σωστά και θα πρέπει να αποφεύγονται, όταν είναι εφικτό.

Συνοψίζοντας, η αρχιτεκτονική για εφαρμογές που λειτουργούν σε μοντέλο IaaS μοιάζει αρκετά με τις επιχειρηματικές εφαρμογές διαδικτύου κατανεμημένης αρχιτεκτονικής. Σε μια εταιρεία, οι κατανεμημένες εφαρμογές λειτουργούν με πολλά είδη ασφάλειας για την ασφάλιση τόσο του εξυπηρετητή όσο και του δικτύου που συνδέει τους εξυπηρετητές μεταξύ τους. Στο μοντέλο IaaS δεν υπάρχουν ανάλογα συστήματα ελέγχου και γι΄ αυτό θα πρέπει να προστεθούν στο δίκτυο, στην πρόσβαση των χρηστών και τέλος, στην ίδια την εφαρμογή. Οι πελάτες των IaaS είναι αποκλειστικά υπεύθυνοι για όλες τις πτυχές ασφάλειας των εφαρμογών τους και οφείλουν να λάβουν τα αναγκαία και απαραίτητα μέτρα ούτως ώστε, αφενός να προστατεύουν τις εφαρμογές τους, αφετέρου να προβλέψουν και να επιλύσουν τυχόν

ευπάθειες που ενδέχεται να δημιουργηθούν σε ένα δημόσιο περιβάλλον από πολλούς και διαφορετικούς χρήστες.

5.4.9. Περιορισμοί των δημόσιων υπολογιστικών νεφών στην ασφάλεια

Οι πελάτες που αξιολογούν το υπολογιστικό νέφος θα πρέπει να έχουν κατά νου ότι υπάρχει μια πληθώρα περιορισμών σε ένα δημόσιο υπολογιστικό νέφος, όσον αφορά την υποστήριξη διάφορων χαρακτηριστικών ασφάλειας. Οι απαιτήσεις ασφάλειας, όπως για παράδειγμα η χρήση τείχους ασφαλείας, η χρήση της κρυπτογραφίας, συσκευών που παρέχουν στιγμιαία κλειδιά με κάποιον αλγόριθμο, δεν παρέχονται στα δημόσια SaaS, PaaS και IaaS. Στο μέλλον, οι πάροχοι IaaS και PaaS ίσως να παράσχουν μερικά από αυτά τα εξεζητημένα χαρακτηριστικά ασφάλειας, ανάλογα με τη ζήτηση των πελατών τους. Σε γενικές γραμμές, κάθε είδους έλεγχος μέσω περιφερειακών συσκευών ασφάλειας σε δημόσια IaaS και PaaS δεν είναι εφικτός μέχρι την τρέχουσα χρονική στιγμή.

5.5. Ασφάλεια των δεδομένων

Όσον αφορά τα δεδομένα κατά τη μετάδοση, ο πρωταρχικός κίνδυνος είναι η χρήση ενός αλγορίθμου κρυπτογράφησης, ο οποίος να μην πιστοποιημένος και πλήρως ελεγμένος. Παρόλο που αυτό είναι προφανές για τους ειδικούς της πληροφορικής, δεν είναι το ίδιο προφανές για άλλους οι οποίοι δεν μπορούν να καταλάβουν τη συγκεκριμένη απαίτηση, όταν χρησιμοποιούν ένα δημόσιο υπολογιστικό νέφος, ανεξάρτητα αν είναι IaaS, PaaS ή SaaS. Είναι επίσης σημαντικό να διαβεβαιωθεί ότι το συγκεκριμένο πρωτόκολλο παρέχει τόσο εμπιστευτικότητα όσο και ακεραιότητα, για παράδειγμα το FTP πάνω από το TLS, το οποίο ονομάζεται FTPS [153], το HTTPS (Hypertext Transfer Protocol Secure) [38] και το SCP (Secure Copy Protocol) [155], ειδικά στην περίπτωση που το συγκεκριμένο πρωτόκολλο χρησιμοποιείται για μεταφορά δεδομένων στο διαδίκτυο. Μόνο η κρυπτογράφηση των

δεδομένων χωρίς τη χρήση ενός ασφαλούς πρωτοκόλλου μεταφοράς δεδομένων μπορεί μεν να παρέχει εμπιστευτικότητα, δεν εγγυάται όμως την ακεραιότητα των δεδομένων.

Παρόλο που η χρήση κρυπτογράφησης για την προστασία των αποθηκευμένων δεδομένων (data-at-rest) μπορεί να φαίνεται προφανής, η πραγματικότητα δεν είναι τόσο απλή. Αν κάποιος χρησιμοποιεί μια υπηρεσία υπολογιστικού νέφους IaaS, δημόσια ή ιδιωτική, απλώς για αποθήκευση των δεδομένων του, η κρυπτογράφηση των αποθηκευμένων δεδομένων είναι εφικτή και συστήνεται ανεπιφύλακτα. Παρόλα αυτά, η κρυπτογράφηση των αποθηκευμένων δεδομένων στα μοντέλα PaaS και SaaS, η οποία γίνεται με αλγόριθμους που έχουν τα ίδια τα μοντέλα ως επιπλέον μέτρο ασφάλειας, δεν είναι πάντα εφικτή. Τα αποθηκευμένα δεδομένα που χρησιμοποιούνται από μια εφαρμογή νέφους γενικώς δεν είναι κρυπτογραφημένα, επειδή η κρυπτογράφηση δεν θα επέτρεπε την δεικτοδότηση ή την αναζήτηση σε αυτά [125].

Σε γενικές γραμμές, σε ό,τι αφορά τα αποθηκευμένα δεδομένα, οι οικονομικοί αναλυτές των υπολογιστικών νεφών σε εφαρμογές PaaS και SaaS χρησιμοποιούν το μοντέλο πολλαπλής μίσθωσης. Με άλλα λόγια, τα δεδομένα, όταν μπαίνουν σε διαδικασία επεξεργασίας από μια εφαρμογή υπολογιστικού νέφους ή όταν αποθηκεύονται για να χρησιμοποιηθούν από μια εφαρμογή υπολογιστικού νέφους, αναμιγνύονται με δεδομένα άλλων χρηστών, τα οποία είναι επίσης αποθηκευμένα στο ίδιο φυσικό μέσο αποθήκευσης. Παρόλο που οι εφαρμογές είναι σχεδιασμένες έτσι ώστε να υποστηρίζουν χαρακτηριστικά δεικτοδότησης των δεδομένων με σκοπό την αδυναμία πρόσβασης στα δεδομένα άλλων χρηστών, η μη εξουσιοδοτημένη πρόσβαση στα δεδομένα εξακολουθεί να είναι δυνατή μέσω κάποιων ευπαθειών στην εφαρμογή που εκμεταλλεύονται κάποιοι. Παρόλο που αρκετοί πάροχοι υπολογιστικών νεφών έχουν δώσει σε τρίτους τις εφαρμογές τους για να επανεξεταστούν και να επαληθευτεί η σωστή λειτουργία τους μέσω εργαλείων ασφάλειας, τα δεδομένα ενδεχομένως να μην είναι αποθηκευμένα αποκλειστικά σε μια πλατφόρμα που ανήκει σε έναν πάροχο.

Παρόλο πού τα δεδομένα μια εταιρείας ή ενός οργανισμού μπορεί να είναι κρυπτογραφημένα κατά τη διάρκεια μεταφοράς τους από και προς τον πάροχο του υπολογιστικού νέφους και τα αποθηκευμένα δεδομένα να είναι επίσης κρυπτογραφημένα στην περίπτωση που ο χρήσης χρησιμοποιεί το υπολογιστικό νέφος αποκλειστικά και μόνο για την αποθήκευση των δεδομένων, τα συγκεκριμένα δεδομένα δεν είναι σίγουρα κρυπτογραφημένα αν υπόκεινται σε επεξεργασία από το υπολογιστικό νέφος, δημόσιο ή ιδιωτικό. Για να μπορεί μια οποιαδήποτε εφαρμογή να επεξεργάζεται κάποια δεδομένα, τα δεδομένα αυτά θα πρέπει οπωσδήποτε να μην είναι κρυπτογραφημένα. Μέχρι σήμερα, δεν υπάρχει καμία μέθοδος για την πλήρη επεξεργασία των κρυπτογραφημένων δεδομένων. Ως εκ τούτου, τα δεδομένα των χρηστών θα είναι αποκρυπτογραφημένα το ελάχιστο κατά την διάρκεια επεξεργασίας τους από το υπολογιστικό νέφος, εκτός και αν τα δεδομένα βρίσκονται στο υπολογιστικό νέφος αποκλειστικά κα μόνο για λόγους αποθήκευσης.

Είτε τα δεδομένα που έχει αποθηκεύσει ένας οργανισμός στο υπολογιστικό νέφος είναι κρυπτογραφημένα, είτε δεν είναι, είναι χρήσιμο και θα πρέπει να απαιτείται να γίνεται γνωστή η ακριβής τοποθεσία στην οποία αποθηκεύτηκαν αυτά τα δεδομένα εντός του υπολογιστικού νέφους. Για παράδειγμα, τα δεδομένα μπορεί να μεταφέρθηκαν σε έναν πάροχο υπολογιστικού νέφους, για παράδειγμα το AWS, την ημέρα x_1 και χρονική στιγμή y_1 και αποθηκεύτηκαν σε ένα χώρο με όνομα example1.s3.amazonaws.com. Κατόπιν, την ημέρα x_2 και την χρονική στιγμή y_2 έγιναν αντικείμενο επεξεργασίας από ένα στιγμιότυπο του EC2, το ex2-12-345-67-123.compute-1.amazonaws.com και αποθηκεύτηκαν στον χώρο example2.s3.amazonaws.com. Τέλος, τα δεδομένα επέστρεψαν στην εταιρεία για μόνιμη αποθήκευση σε έναν από τους εσωτερικούς της χώρους αποθήκευσης την ημέρα x_3 και την χρονική στιγμή y_3. Η παρακολούθηση της διαδρομής των δεδομένων, όπως ονομάζεται, είναι γνωστή ως διαδρομή δεδομένων (data lineage), και είναι πολύ σημαντική [99]. Ωστόσο, η παροχή διαδρομής δεδομένων στους πελάτες είναι αρκετά χρονοβόρα, ακόμα και στην περίπτωση που το περιβάλλον του υπολογιστικού νέφους τελεί αποκλειστικά κάτω από τον έλεγχο της εταιρείας. Η προσπάθεια της παροχής ακριβούς

αναφοράς σχετικά με την διαδρομή δεδομένων σε ένα δημόσιο υπολογιστικό νέφος είναι απλώς αδύνατη. Στο προηγούμενο παράδειγμα, στο οποίο τα δεδομένα αποθηκεύτηκαν σε ένα χώρο με το όνομα example1.s3.amazonaws.com, δεν μπορούμε να γνωρίζουμε την ακριβή τοποθεσία του χώρου αυτού, δεν μπορούμε να ξέρουμε ποια ήταν η κατάσταση πριν και μετά την αποθήκευση των δεδομένων μας και, τέλος, δεν μπορούμε να επιβεβαιώσουμε τις όποιες πληροφορίες μας δώσει ο ίδιος ο πάροχος, στην περίπτωσή μας, η Amazon.

Ακόμη και αν η διαδρομή των δεδομένων μπορεί να επιτευχθεί σε ένα δημόσιο υπολογιστικό νέφος, για μερικούς πελάτες υπάρχει μια ακόμα πιο προκλητική απαίτηση και ένα μείζον πρόβλημα: η απόδειξη της ακρίβειας των δεδομένων (data provenance), καθώς αυτή δεν προϋποθέτει μόνο την ακεραιότητα των δεδομένων αλλά απαιτεί πολύ πιο συγκεκριμένα στοιχεία και χαρακτηριστικά επί των δεδομένων. Υπάρχει μια βασική διαφορά μεταξύ των δύο παραπάνω εννοιών. Η ακεραιότητα των δεδομένων αναφέρεται στο γεγονός ότι τα δεδομένα δεν έχουν τροποποιηθεί με μη θεμιτό τρόπο ή από μη εξουσιοδοτημένο πρόσωπο. Η ακρίβεια των δεδομένων σημαίνει αφενός την ακεραιότητά τους, αφετέρου ότι είναι υπολογιστικά σωστά, δηλαδή ότι τα δεδομένα είναι υπολογισμένα χωρίς λάθη. Για παράδειγμα, ας θεωρήσουμε την επόμενη μαθηματική εξίσωση:

$$sum((((2*3)*4)/6)-2) = \$2.00$$

Στη συγκεκριμένη εξίσωση η αναμενόμενη απάντηση είναι $2.00. Αν η απάντηση ήταν διαφορετική, θα προέκυπτε πρόβλημα ακεραιότητας των δεδομένων. Φυσικά, γίνεται η υπόθεση ότι το 2.00 είναι σε δολάρια Η.Π.Α., αλλά αυτή η υπόθεση μπορεί να είναι λανθασμένη, αν γίνεται χρήση διαφορετικού είδους δολαρίου με τις ακόλουθες σχετικές υποθέσεις:

- Η εξίσωση ισχύει ειδικά για χώρα που δεν χρησιμοποιεί το δολάριο των ΗΠΑ και επίσης αναφέρεται η χώρα
- Η εξίσωση έχει δολάρια Η.Π.Α. τα οποία έχουν μετατραπεί από δολάρια άλλων χωρών.

- Χρησιμοποιείται η σωστή συναλλαγματική ισοτιμία, η μετατροπή υπολογίζεται σωστά και μπορεί να αποδειχτεί.

Στο συγκεκριμένο παράδειγμα, αν η εξίσωση ικανοποιεί τις συγκεκριμένες υποθέσεις έχει ακεραιότητα αλλά δεν έχει ακρίβεια. Υπάρχει πληθώρα από παραδείγματα στον πραγματικό κόσμο στα οποία η ακεραιότητα των δεδομένων δεν είναι επαρκής και για αυτό απαιτείται και η ακρίβεια των δεδομένων. Οι οικονομικοί και οι επιστημονικοί υπολογισμοί είναι δύο προφανή παραδείγματα. Οπότε, στην περίπτωση του υπολογιστικού νέφους, πώς θα μπορεί κάποιος να αποδείξει την ακρίβεια των δεδομένων από τη στιγμή που χρησιμοποιεί διαμοιραζόμενους πόρους; Οι συγκεκριμένοι πόροι δεν είναι υπό τον φυσικό ή ακόμα και τον λογικό έλεγχο της εταιρείας και η εταιρεία δεν έχει τη δυνατότητα να εντοπίζει τα συστήματα καθώς και τον χρόνο που χρησιμοποιήθηκαν από τα δεδομένα της, ακόμα και στην περίπτωση που ενδεχομένως γνωρίζει μερικά αναγνωρίσιμα στοιχεία τους, όπως για παράδειγμα την διεύθυνση IP ή τη γενική τοποθεσία αποθήκευσης, δηλαδή τη χώρα και όχι κάποιο συγκεκριμένο κέντρο δεδομένων.

Μια τελευταία πτυχή της ασφάλειας των δεδομένων είναι τα παραμένοντα δεδομένα (data remanence). Παραμένοντα δεδομένα ονομάζεται η υπολειμματική αναπαράσταση των δεδομένων, τα οποία έχουν διαγραφεί η αφαιρεθεί με νόμιμο τρόπο [156]. Αυτά τα υπολείμματα μπορεί να οφείλονται σε δεδομένα που έμειναν άθικτα μετά τη λειτουργία της διαγραφής ή μέσω των φυσικών ιδιοτήτων του μέσου αποθήκευσης. Τα παραμένοντα δεδομένα μπορεί να κάνουν δυνατή την ακούσια αποκάλυψη ευαίσθητων πληροφοριών στην περίπτωση που το μέσο αποθήκευσης κυκλοφορήσει σε ένα μη ελεγχόμενο περιβάλλον.

Ο μεγαλύτερος κίνδυνος από τα παραμένοντα δεδομένα σε όλες τις υπηρεσίες του υπολογιστικού νέφους είναι ότι τα δεδομένα της εταιρείας μπορεί να εκτεθούν ακούσια σε τρίτους, ανεξαρτήτως από το είδος του μοντέλου που χρησιμοποιείται. Ειδικότερα στην περίπτωση χρήσης των μοντέλων PaaS και SaaS, ο κίνδυνος είναι πλήρως ακούσιος, μιας και ο χρήστης δεν γνωρίζει το πώς είναι γραμμένο το πρόγραμμα που χρησιμοποιεί σε ό,τι αφορά τη διαγραφή των δεδομένων. Αυτό όμως

δεν σημαίνει ότι οι πελάτες θα πρέπει να μην ασχοληθούν με το ζήτημα. Οι πελάτες θα πρέπει να ενημερωθούν πλήρως για το τι είδους εργαλεία χρησιμοποιήθηκαν για να επικυρωθεί η ασφάλεια της εκάστοτε εφαρμογής που χρησιμοποιούν, καθώς και γενικότερα της πλατφόρμας του παρόχου τους.

Παρά την αυξανόμενη σημασία της ασφάλειας των δεδομένων, η προσοχή που δίνουν οι πάροχοι των υπηρεσιών υπολογιστικού νέφους στα παραμένοντα δεδομένα είναι ιδιαίτερα χαμηλή. Πολλοί από τους παρόχους δεν αναφέρουν καν τον τρόπο διαχείρισης των παραμενόντων δεδομένων στις υπηρεσίες τους. Στην περίπτωση που αναφερθεί κάτι σχετικά με τα παραμένοντα δεδομένα από τους χρήστες, τότε οι πάροχοι απλώς επικαλούνται ότι συμμορφώνονται πλήρως με την οδηγία SP800-88 του NIST [157].

5.5.1. Μείωση της ασφάλειας των δεδομένων

Αν οι μελλοντικοί πελάτες των υπηρεσιών του υπολογιστικού νέφους πιστεύουν ότι η ασφάλεια των δεδομένων τους ενδεχομένως να αποδυναμώσει την ασφάλεια όλης της υποδομής, από τη στιγμή που μέρος της υποδομής ασφάλειας των δεδομένων τους φεύγει από τον έλεγχό τους και η υποδομή ασφάλειας του παρόχου μπορεί να είναι λιγότερο καλή από το αναμενόμενο, τότε θα απογοητευτούν. Παρόλο που τα δεδομένα κατά τη διάρκεια της μεταφοράς είναι κρυπτογραφημένα, οποιαδήποτε χρήση από τις υπηρεσίες του υπολογιστικού νέφους, πέρα από την αποθήκευση, επιβάλλει τη μη κρυπτογράφηση των δεδομένων. Αυτό σημαίνει ότι κατά πάσα πιθανότητα τα δεδομένα θα είναι μη κρυπτογραφημένα στο περιβάλλον του υπολογιστικού νέφους. Επίσης, στην περίπτωση ενός δημόσιου υπολογιστικού νέφους, όπου ο χρήστης χρησιμοποιεί μοντέλα PaaS ή SaaS τα μη κρυπτογραφημένα δεδομένα του θα είναι στον ίδιο φυσικό χώρο με δεδομένα άλλων χρηστών. Σε αυτό το πρόβλημα θα πρέπει να προστεθούν τα προβλήματα στον καθορισμό της διαδρομής των δεδομένων, της ακρίβειας των δεδομένων, όπου αυτό κρίνεται απαραίτητο και τέλος η αδυναμία πολλών από τους παρόχους να

αντιμετωπίσουν επαρκώς τη βασική απαίτηση ασφάλειας όπως τα παραμένοντα δεδομένα. Όλα τα προηγούμενα συνηγορούν στο γεγονός ότι οι κίνδυνοι στην ασφάλεια των δεδομένων των χρηστών είναι σημαντικά μεγαλύτεροι από πριν.

Οπότε σε αυτήν την περίπτωση κάποιος εύκολα θα σκεφτόταν τρόπους για τον περιορισμό των προαναφερθέντων κινδύνων σχετικά με την ασφάλεια των δεδομένων. Η μόνη βιώσιμη επιλογή για τη μείωση των παραπάνω κινδύνων είναι να διασφαλιστεί ότι τα ευαίσθητα δεδομένα μιας επιχείρησης ή ενός οργανισμού σε καμιά περίπτωση δεν τοποθετούνται σε ένα δημόσιο υπολογιστικό νέφος, ή στην περίπτωση που διάφοροι λόγοι επιβάλλουν την αποθήκευσή τους, αυτό να γίνεται με κρυπτογράφηση πριν την αποθήκευση και να αποθηκεύονται απλώς στο υπολογιστικό νέφος, χωρίς να υπάρχει καμία δυνατότητα επεξεργασίας τους. Λαμβάνοντας υπόψη τις οικονομικές εκτιμήσεις του υπολογιστικού νέφους σήμερα, καθώς και τα υπάρχοντα όρια της κρυπτογραφίας, οι πάροχοι δεν προσφέρουν αρκετά αυστηρούς ελέγχους γύρω από την ασφάλεια των δεδομένων. Ενδεχομένως στο μέλλον οι οικονομικές εκτιμήσεις να αλλάξουν και να αυξηθούν, ώστε οι πάροχοι να είναι σε θέση να παρέχουν περιβάλλοντα, τα οποία θα χειρίζονται με ειδικούς και ασφαλείς τρόπους τα δεδομένα των χρηστών. Επί του παρόντος, όπως αναφέρθηκε και προηγουμένως, η καλύτερη λύση είναι να μην αποθηκεύονται ευαίσθητα δεδομένα σε περιβάλλον δημόσιου υπολογιστικού νέφους.

5.5.2. Δεδομένα του παρόχου και ασφάλεια

Σε αντίθεση με τα δεδομένα των χρηστών και τον τρόπο χειρισμού της ασφάλειάς τους από τους παρόχους, οι χρήστες θα πρέπει να ανησυχούν και για το τι είδους δεδομένα συλλέγει ο πάροχος καθώς και το πώς προστατεύει τα δεδομένα που συλλέγει. Συγκεκριμένα και αναφορικά με τα δεδομένα των χρηστών, τι είδους μεταδεδομένα (metadata) συλλέγει ο πάροχος σχετικά με αυτά, πώς επιτυγχάνει την ασφάλειά τους και τι είδους πρόσβαση μπορεί να έχει, αν έχει, ο πελάτης; Θα πρέπει να θεωρείται δεδομένο ότι καθώς αυξάνει το

μέγεθος των δεδομένων του πελάτη, αναλογικά θα αυξάνεται και το μέγεθος των μεταδεδομένων του.

Επιπρόσθετα, ο πάροχος θα πρέπει να συγκεντρώνει ένα μεγάλο ποσό από δεδομένα σχετικά με την ασφάλεια. Για παράδειγμα, σε επίπεδο δικτύου, ο πάροχος θα πρέπει να συλλέγει, να ελέγχει και να διατηρεί συστήματα ανίχνευσης εισβολών (Intrusion Detection System – IDS), συστήματα αποτροπής εισβολών (Intrusion Prevention System - IPS), διαχείριση των συμβάντων που προκύπτουν σχετικά με την ασφάλεια και τέλος, όλη την ροή του δρομολογητή. Σε επίπεδο εξυπηρετητή ο πάροχος οφείλει να συλλέγει τα αρχεία καταγραφής συμβάντων του συστήματος (system log files) και σε επίπεδο εφαρμογών SaaS ο πάροχος επιβάλλεται να συλλέγει τα αρχεία καταγραφής συμβάντων για τις εφαρμογές που χρησιμοποιούνται, δίνοντας ιδιαίτερη έμφαση στις πληροφορίες εισόδου των χρηστών και του ελέγχου πρόσβασης.

Τα είδη των δεδομένων καθώς και ο τρόπος ελέγχου των δεδομένων που συλλέγει ο εκάστοτε πάροχος είναι αρκετά σημαντικά για τον ίδιο σχετικά με τη δική του ασφάλεια. Επιπρόσθετα, όπως θα δούμε και παρακάτω, τα παραπάνω δεδομένα είναι ιδιαίτερα χρήσιμα σε περιπτώσεις forensics.

5.5.3. Αποθήκευση

Για τα δεδομένα που είναι αποθηκευμένα στο υπολογιστικοό νέφος, δηλαδή το μοντέλο αποθήκευση-ως-υπηρεσία (Storage-as-a-Service – StaaS), αναφερόμαστε στο μοντέλο IaaS και όχι στα δεδομένα που σχετίζονται με μια εφαρμογή που τρέχει στο υπολογιστικό νέφος μέσω των PaaS ή SaaS. Όπως και στην αποθήκευση των δεδομένων οπουδήποτε, έτσι και στο υπολογιστικό νέφος, τρεις είναι οι βασικοί παράμετροι ασφάλειας: η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα (Confidentiality, Integrity, Availability – CIA).

5.5.3.1. Εμπιστευτικότητα

Σε ό,τι αφορά την εμπιστευτικότητα των δεδομένων στο υπολογιστικό νέφος έχουμε δυο βασικές συνιστώσες. Η πρώτη έχει να κάνει με τον έλεγχο πρόσβασης επί των δεδομένων. Ο έλεγχος πρόσβασης αποτελείται από την πιστοποίηση και από την εξουσιοδότηση του χρήστη να έχει πρόσβαση στα δεδομένα. Δυστυχώς, στο υπολογιστικό νέφος χρησιμοποιούνται ασθενείς μηχανισμοί αυθεντικοποίησης χρηστών, δηλαδή μόνο όνομα χρήστη και κωδικός χρήστη και οι μηχανισμοί ελέγχου πρόσβασης επί των δεδομένων που είναι διαθέσιμοι στους χρήστες τείνουν να είναι αρκετά γενικοί και δεν είναι λεπτομερείς. Για μεγάλες επιχειρήσεις, αυτή η γενικότητα στην εξουσιοδότηση πρόσβασης παρουσιάζει από μόνη της σημαντικές ανησυχίες για την ασφάλεια. Συχνά, τα μόνα επίπεδα πρόσβασης που μπορεί να παρέχει το υπολογιστικό νέφος είναι σε επίπεδο διαχειριστή και χρήστη, χωρίς να υπάρχει κανένα άλλο επίπεδο πρόσβασης μεταξύ αυτών των δύο. Ο διαχειριστής είναι και ο ιδιοκτήτης του λογαριασμού, ενώ οι χρήστες ενδεχομένως να μην είναι ιδιοκτήτες του συγκεκριμένου λογαριασμού.

Η δεύτερη συνιστώσα έχει να κάνει με την ασφάλεια των αποθηκευμένων δεδομένων στο υπολογιστικό νέφος και την ασφάλεια που αυτό προσφέρει για να είναι προστατευμένα. Για πρακτικούς λόγους, η προστασία των αποθηκευμένων δεδομένων στο υπολογιστικό νέφος προϋποθέτει την χρήση κρυπτογράφησης.

Οπότε, είναι τα δεδομένα των χρηστών κρυπτογραφημένα όταν βρίσκονται αποθηκευμένα στο υπολογιστικό νέφος; Και αν η απάντηση στο προηγούμενο ερώτημα είναι καταφατική, τότε με τι είδους αλγόριθμο κρυπτογράφησης είναι κρυπτογραφημένα και ποιο είναι το εύρος του κλειδιού; Η απάντηση σε αυτό το ερώτημα ποικίλλει ανάλογα με το είδος του παρόχου που χρησιμοποιεί ο εκάστοτε χρήστης. Για παράδειγμα, η carbonite [158] κρυπτογραφεί υποχρεωτικα τα δεδομένα των χρηστών μέσω του αλγόριθμου Blowfish 128 bits [159] ενώ το AWS S3 της Amazon αφήνει τον χρήστη να επιλέξει αν θέλει η όχι κρυπτογράφηση των δεδομένων τους. Οι πελάτες, βέβαια μπορούν να

κρυπτογραφούν μόνοι τους τα δεδομένα τους πριν τα ανεβάσουν στο υπολογιστικό νέφος.

Αν ένας πάροχος όντως κρυπτογραφεί τα δεδομένα των πελατών του, η αμέσως επόμενη σκέψη που έρχεται στο νου αυτόματα έχει σχέση με τον αλγόριθμο κρυπτογράφησης που χρησιμοποιεί. Δεν είναι όλοι οι αλγόριθμοι κρυπτογράφησης ίδιοι και ίσοι. Από κρυπτογραφικής άποψης, πολλοί αλγόριθμοι δεν παρέχουν επαρκή ασφάλεια. Μόνοι οι κρυπτογραφικοί αλγόριθμοι που έχουν εξεταστεί δημοσίως από επίσημες εταιρείες ή οργανισμούς ή τουλάχιστον από την κοινότητα των κρυπτογράφων θα πρέπει να χρησιμοποιούνται. Οπωσδήποτε θα πρέπει να αποφεύγονται αλγόριθμοι που είναι ιδιωτικοί και δεν έχουν κοινοποιηθεί σε τρίτους. Να σημειώσουμε ότι σε επίπεδο υπολογιστικού νέφους μιλάμε αποκλειστικά και μόνο για αλγόριθμους συμμετρικής κρυπτογραφίας. Η συμμετρική κρυπτογραφία περιλαμβάνει τη χρήση ενός και μόνο μυστικού κλειδιού τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση των δεδομένων. Μόνο η συμμετρική κρυπτογραφία έχει την ταχύτητα και την αποδοτικότητα ώστε να είναι σε θέση να κρυπτογραφεί μεγάλο όγκο δεδομένων. Θα ήταν εξαιρετικά ασυνήθιστο να χρησιμοποιηθεί ασύμμετρος αλγόριθμος για την κρυπτογράφηση των δεδομένων στο υπολογιστικό νέφος.

Το επόμενο θέμα που θα πρέπει να απασχολήσει τον πελάτη είναι το μήκος του κλειδιού που χρησιμοποιείται. Στη συμμετρική κρυπτογράφηση, όσο μεγαλύτερο είναι το μήκος του κλειδιού, τόσο δυνατότερη θεωρείται η κρυπτογράφηση. Παρόλο που τα μεγάλα μήκη κλειδιού παρέχουν καλύτερη κρυπτογράφηση, είναι πολύ απαιτητικά σε υπολογιστικούς πόρους και ενδεχομένως να καταπονήσουν αρκετά τις δυνατότητες των κεντρικών μονάδων επεξεργασίας των υπολογιστών. Σε γενικές γραμμές, το μήκος του κλειδιού θα πρέπει να είναι το λιγότερο 168 bits για τον αλγόριθμο Triple Data Encryption Standard (tripleDES) [160] και 192 bits για τον αλγόριθμο Advanced Encryption Standard (AES) [161]. Αξίζει να σημειωθεί ότι και οι δύο προαναφερθέντες αλγόριθμοι κρυπτογράφησης είναι εγκεκριμένοι από τον οργανισμό NIST [162].

Τέλος, το τελευταίο ζήτημα που θα πρέπει να απασχολήσει τον πελάτη σχετικά με την εμπιστευτικότητα των δεδομένων του, είναι η

διαχείριση του κλειδιού κρυπτογράφησης. Θα πρέπει να γνωρίζει που αποθηκεύονται τα κλειδιά κρυπτογράφησης, καθώς και με ποιον τρόπο και ποιος θα μπορεί να έχει πρόσβαση σε αυτά. Επίσης, θα πρέπει να γνωρίζει, αν θα μπορεί ο ίδιος να διαχειρίζεται τα κλειδιά του. Η απάντηση στα προηγούμενα ερωτήματα είναι ότι ο χρήστης αποκλειστικά και μόνο διαχειρίζεται τα κλειδιά του. Δεν συνιστάται η ανάθεση της διαχείρισης των κλειδιών κρυπτογράφησης σε πάροχο υπολογιστικού νέφους, τουλάχιστον όχι σε αυτόν που έχει τα κρυπτογραφημένα δεδομένα. Αυτό σημαίνει ότι είναι αναγκαίοι επιπρόσθετοι πόροι και δυνατότητες. Κλείνοντας την παρούσα παράγραφο, θα πρέπει να καταστεί σαφές προς τον αναγνώστη ότι η σωστή διαχείριση των κλειδιών κρυπτογράφησης είναι ένα πολύπλοκο και ιδιαίτερα δύσκολο έργο.

Η διαχείριση των κλειδιών κρυπτογράφησης είναι πολύπλοκο και δύσκολο έργο για έναν πελάτη, όπως αναφέρθηκε και ανωτέρω, αλλά είναι ακόμα πιο πολύπλοκο και δύσκολο έργο για τους παρόχους. Ειδικά, η διαχείριση πολλαπλών κλειδιών από πολλούς πελάτες θεωρείται αδύνατη. Γι’ αυτό τον λόγο, σχεδόν όλοι οι πάροχοι υπολογιστικώμ νεφών δεν υποστηρίζουν διαχείριση των κλειδιών κρυπτογράφησης των πελατών τους. Για παράδειγμα, είναι σύνηθες για έναν πάροχο να κρυπτογραφεί όλα τα δεδομένα ενός πελάτη του με ένα και μόνο κλειδί. Σε ακόμα χειρότερη περίπτωση, έχει καταγραφεί πάροχος υπλογιστικού νέφους, ο οποίος κρυπτογραφεί τα δεδομένα όλων των πελατών του με ένα και μόνο κλειδί.

5.5.3.2. Ακεραιότητα

Εκτός από την εμπιστευτικότητα των δεδομένων, ο πελάτης θα πρέπει να ανησυχεί και για την ακεραιότητά τους. Η εμπιστευτικότητα δεν συνεπάγεται και την ακεραιότητα. Τα δεδομένα μπορεί να είναι κρυπτογραφημένα για σκοπούς εμπιστευτικότητας και παρόλα αυτά να μην είναι δυνατή η πιστοποίηση της ακεραιότητάς τους. Αυτό σημαίνει ότι η κρυπτογράφηση από μόνη της είναι αρκετή για την εμπιστευτικότητα των δεδομένων, παρόλα αυτά στην περίπτωση της

ακεραιότητας απαιτούνται επιπλέον κωδικοί ελέγχου της γνησιότητας του μηνύματος (Message Authentication Code - MAC) [163]. Ο πιο απλός τρόπος για να χρησιμοποιήσει κάποιος κωδικούς ελέγχου γνησιότητας ενός μηνύματος είναι να χρησιμοποιήσει έναν συμμετρικό αλγόριθμο τύπου block με λειτουργία CBC (Cipher Block Chaining) [164] και να συμπεριλάβει μια μονόδρομη συνάρτηση κατακερματισμού (one-way Hash Function) [165]. Σε τελική φάση, οι πελάτες θα πρέπει να ρωτήσουν και να ενημερωθούν από τον πάροχό τους σχετικά με τα προαναφερθέντα θέματα. Τα προηγούμενα στοιχεία δεν είναι μόνο σημαντικά για την ακεραιότητα των δεδομένων των πελατών, αλλά επίσης αποδεικνύουν πόσο περίπλοκο και αποδοτικό είναι το πρόγραμμα ασφάλειας που υλοποιεί ο πάροχος. Αξίζει να σημειωθεί, ωστόσο, ότι δεν κρυπτογραφούν όλοι οι πάροχοι τα δεδομένα των πελατών τους, ειδικά εκείνοι που έχουν υπηρεσίες PaaS και SaaS.

Μια άλλη εξίσου σημαντική πτυχή της ακεραιότητας των δεδομένων είναι ο τρόπος αποθήκευσης των δεδομένων στο υπολογιστικό νέφος, ειδικά στο μοντέλο IaaS. Από τη στιγμή που ο πελάτης έχει αρκετά GB ή και TB δεδομένων αποθηκευμένα στο υπολογιστικό νέφος θα πρέπει να υπάρχει τρόπος να ελέγχει την ακεραιότητά τους. Η μεταφορά των δεδομένων από το υπολογιστικό νέφος στον πελάτη και το αντίστροφο, ώστε να ελεγχθεί εκεί η ακεραιότητά τους, εκτός από χρονοβόρα, είναι και δαπανηρή. Αυτό που πραγματικά χρειάζεται ο πελάτης είναι ένας μηχανισμός, ο οποίος να πιστοποιεί την ακεραιότητα των δεδομένων του όσο εκείνα είναι αποθηκευμένα στο υπολογιστικό νέφος, χωρίς να χρειάζεται να τα κατεβάσει και μετά να τα ανεβάσει ξανά σε αυτό.

Η όλη εργασία καθίσταται πολύ πιο δύσκολη γιατί στην περίπτωση του υπολογιστικού νέφους όλα θα πρέπει να λειτουργήσουν χωρίς να είναι γνωστό το πλήρες σύνολο των δεδομένων. Οι πελάτες δεν ξέρουν σε ποια φυσικά μηχανήματα είναι αποθηκευμένα τα δεδομένα τους ή το που βρίσκονται αυτά τα μηχανήματα. Επιπρόσθετα, τα σύνολα των δεδομένων μπορεί να είναι δυναμικά και να αλλάζουν σε συχνή βάση. Αυτές οι συχνές μεταβολές καθιστούν αναποτελεσματικές τις παραδοσιακές τεχνικές σχετικά με την ακεραιότητα.

5.5.3.3. Διαθεσιμότητα

Θεωρώντας ότι τα δεδομένα ενός πελάτη διατηρούν την εμπιστευτικότητα και την ακεραιότητά τους, θα πρέπει επίσης να διατηρήσουν και τη διαθεσιμότητά τους. Επί του παρόντος, τρεις είναι οι σοβαρές απειλές σχετικά με τη διαθεσιμότητα των δεδομένων, εκ των οποίων καμία δεν είναι νέα στην επιστήμη της πληροφορικής, αλλά όλες τους έχουν μεγαλύτερη αξία στην περίπτωση του υπολογιστικού νέφους λόγω του ήδη αυξημένου κινδύνου.

Η πρώτη απειλή για τη διαθεσιμότητα είναι οι επιθέσεις πάνω στο δίκτυο, όπως έχουν προαναφερθεί και σε προηγούμενες παραγράφους.

Η δεύτερη απειλή αφόρα τη διαθεσιμότητα του παρόχου. Αυτό σημαίνει ότι ο πάροχος ενδέχεται για κάποιο χρονικό διάστημα να μην μπορεί να εξυπηρετήσει τους πελάτες του. Στη γλώσσα του υπολογιστικού νέφους το ποσοστό συνεχούς λειτουργίας μετριέται σε εννιάρια, για παράδειγμα αν έχουν 99.999% λέμε ότι ο πάροχος μπορεί και προσφέρει πέντε εννιάρια λειτουργίας. Συνήθεις τιμές είναι από τρία μέχρι έξι εννιάρια, που μπορεί για τον αναγνώστη να φαίνεται ως αμελητέα ποσότητα, όταν όμως αυτό το ποσοστό μεταφραστεί σε ώρες ενός έτους, τότε τα τρία εννιάρια σημαίνουν οκτώ ώρες και σαράντα πέντε λεπτά μη λειτουργίας, ενώ τα πέντε εννιάρια σημαίνουν πέντε λεπτά και δεκαπέντε δευτερόλεπτα μη λειτουργίας.

Είναι γεγονός ότι κατά καιρούς έχουν συμβεί υψηλής διάρκειας διακοπές σε αρκετούς παρόχους του νέφους. Ιστορικά, το S3 της Amazon στα αρχικά του στάδια υλοποίησης, ήταν για περισσότερο από 2.5 ώρες ανενεργό τον Φεβρουάριο του 2008 και γύρω στις οκτώ ώρες τον Ιούλιο του 2008 [32]. Σε αυτό πρέπει να προστεθεί το γεγονός ότι η Amazon θεωρούνταν η πιο πρωτοπόρος εταιρεία σε θέματα υπολογιστικού νέφους, οπότε από τη στιγμή που ακόμα και αυτή η εταιρεία είχε τέτοιου είδους προβλήματα, οδηγούμαστε στο να αναλογιστούμε τι προβλήματα θα αντιμετωπίζουν άλλες εταιρείες μικρότερου βεληνεκούς. Οι συγκεκριμένες διακοπές της Amazon ήταν ακόμα πιο εμφανείς λόγω του σχετικά μεγάλου αριθμού πελατών που υποστηρίζει η υπηρεσία S3, και

οι οποίοι απευθύνονται αποκλειστικά στη συγκεκριμένη υπηρεσία για τις δικές τους ενέργειες.

Εκτός από τις διακοπές λειτουργίας των υπηρεσιών του νέφους, σε ορισμένες περιπτώσεις τα δεδομένα που ήταν αποθηκευμένα στο υπολογιστικό νέφος, χάθηκαν. Για παράδειγμα, τον Μάρτιο του 2009, η Google κατέθεσε μήνυση εναντίον δύο παρόχων υλικού κατηγορώντας τους ότι προκάλεσαν αποτυχίες στα αντίγραφα ασφάλειας και αυτό είχε ως αποτέλεσμα η εταιρεία να χάσει δεδομένα για περίπου 7500 πελάτες της [17].

Συνεχίζοντας, οι πελάτες θα πρέπει να κατανοήσουν ότι οι πάροχοι του υπολογιστικού νέφους δεν είναι τίποτα περισσότερο από εταιρείες, οι οποίες μπορεί κάποια στιγμή να σταματήσουν να λειτουργούν. Για παράδειγμα, τον Φεβρουάριο του 2009, ο πάροχος CogHead ξαφνικά σταμάτησε να λειτουργεί, δίνοντας στους πελάτες του προθεσμία λιγότερες από ενενήντα μέρες για να μεταφέρουν τα δεδομένα από τους διακομιστές του ή αλλιώς να τα χάσουν ολοσχερώς [166].

Το θετικό κομμάτι στα προηγούμενα σοβαρά προβλήματα που αντιμετώπισαν οι πάροχοι υπηρεσιών υπολογιστικού νέφους είναι ότι σήμερα θεωρείται αρκετά δύσκολο να υπάρχει αστοχία σαν τις προαναφερόμενες. Όλοι οι πάροχοι έχουν πλέον την δυνατότητα να χρησιμοποιούν διπλές ή και σε μερικές περιπτώσεις τριπλές υποδομές για την φιλοξενία του ίδιου πόρου και είναι πλέον στην διάθεση του πελάτη για εφαρμόσει την πολλαπλή αποθήκευσή του, πάντα με το αντίστοιχο κόστος.

Τέλος, οι υποψήφιοι πελάτες του υπολογιστικού νέφους θα πρέπει να γνωρίζουν ακριβώς τι είδους υπηρεσίες τους προσφέρει ο μελλοντικός πάροχός τους. Η αποθήκευση των δεδομένων στο υπολογιστικό νέφος δεν προϋποθέτει ότι τα αποθηκευμένα δεδομένα είναι και σε αντίγραφα ασφαλείας μαζί με την παροχή αποθήκευσης. Ωστόσο, πολλοί από τους παρόχους προσφέρουν αντίγραφα ασφαλείας των δεδομένων με επιπλέον κοστολόγηση. Για παράδειγμα, τα δεδομένα που είναι αποθηκευμένα σε ένα από τα υπολογιστικά νέφη που προσφέρει η Amazon, βρίσκονται σε διαφορετικές φυσικές τοποθεσίες

για την αποφυγή απώλειάς τους, αυτό όμως δεν σημαίνει ότι υποστηρίζεται εγγενώς και η λειτουργία των αντιγράφων ασφαλείας.

Και οι τρεις προαναφερθείσες συνιστώσες, διαθεσιμότητα, εμπιστευτικότητα και ακεραιότητα, θα πρέπει να υπάρχουν στα συμβόλαια παροχής υπηρεσιών των παρόχων και να διαβάζονται λεπτομερώς από τους πελάτες. Παρόλα αυτά, τα συμβόλαια παροχής υπηρεσιών είναι αρκετά λιτά και στην ουσία δεν αξίζουν πολλά για εξυπηρετούν κατά βάση τους ίδιους τους παρόχους. Ακόμα και όταν ένας πάροχος θεωρείται ότι έχει ένα αξιόπιστο και τεκμηριωμένο συμβόλαιο δεν υπάρχουν τρόποι για τον πελάτη να αποδείξει τυχόν προβλήματα στην παροχή των υπηρεσιών, παρά μόνο με τη συγκατάθεση του παρόχου. Για όλους τους προηγούμενους λόγους, οι μέθοδοι ασφάλειας των δεδομένων και ο τρόπος που αυτά είναι αποθηκευμένα στο υπολογιστικό νέφος θα πρέπει να χρήζουν ιδιαίτερης προσοχής από τους πελάτες για μια ομαλή, και με όσο το δυνατόν λιγότερα προβλήματα, χρήση.

Κ Ε Φ Α Λ Α Ι Ο Ε Κ Τ Ο

Νομικά ζητήματα του υπολογιστικού νέφους

6.1. Εισαγωγή

Σε αυτό το κεφάλαιο θα αναφερθούμε στα βασικά νομικά ζητήματα που υπάρχουν στο υπολογιστικό νέφος. Είναι γεγονός ότι το υπολογιστικό νέφος δημιούργησε νέες καταστάσεις τόσο σε επίπεδο πληροφορικής όσο και σε νομικό επίπεδο. Το πιο χαρακτηριστικό παράδειγμα είναι ότι όλοι οι κλασικοί νόμοι θεωρούσαν ως δεδομένο την συνύπαρξη του κατόχου των δεδομένων και των δεδομένων, γεγονός

που δεν υπάρχει στο υπολογιστικό νέφος. Στις παραγράφους που ακολουθούν θα αναφερθούμε όσο πιο εμπεριστατωμένα και λακωνικά γίνεται στη νομοθεσία που περιβάλλει το υπολογιστικό νέφος.

6.2. Προστασία της πληροφορίας

6.2.1. Ιδιωτικότητα

Πληροφορίες σχετικές με τις υποχρεώσεις των παρόχων αναφορικά με την προστασία της ιδιωτικότητας υπάρχουν σε διάφορους οργανισμούς σχετικούς με το ζήτημα και ενδεχομένως να διαφέρουν ανάλογα με την ήπειρο στην οποία αυτές ισχύουν. Παρόλα αυτά, οι εταιρείες που σκέφτονται να μεταφέρουν την υπολογιστική υποδομή τους στο υπολογιστικό νέφος θα πρέπει να εξετάσουν και να συμβουλευτούν τις κατά τόπους υπηρεσίες, οι οποίες είναι σχετικές με την ιδιωτικότητα αφενός των δεδομένων τους και αφετέρου των χρηστών τους, πριν προβούν σε οποιαδήποτε συμφωνία με τον πάροχο του υπολογιστικού νέφους.

Εντούτοις, το υπολογιστικό νέφος δεν σημαίνει ότι θα πρέπει απαραιτήτως να εισβάλει στην ιδιωτικότητα των χρηστών, αλλά η μεταφορά των δεδομένων στο υπολογιστικό νέφος συνεπάγεται ότι τα δεδομένα θα είναι εκτός ελέγχου της εταιρείας και μπορεί, σε μερικές περιπτώσεις, να αποθηκεύονται και να επεξεργάζονται εκτός των γεωγραφικών ορίων της εταιρείας ή της χώρας που γεωγραφικά ανήκει η συγκεκριμένη εταιρεία. Για παράδειγμα, για μία εταιρεία που εδρεύει στην Ελλάδα και έχει τα δεδομένα της στο υπολογιστικό νέφος, υπάρχει περίπτωση τα δεδομένα της να είναι αποθηκευμένα σε κάποιον διακομιστή στις Η.Π.Α και να γίνεται η επεξεργασία τους από κάποιον υπολογιστή που βρίσκεται στην Ιαπωνία. Ως εκ τούτου, είναι δυνατόν να υπάρξουν διαφορετικά επίπεδα του έμμεσου ελέγχου των δεδομένων, ανάλογα με το είδος της υπηρεσίας υπολογιστικού νέφους καθώς και των νομικών περιορισμών που τέθηκαν εξαρχής από την εταιρεία.

Οι εταιρείες, και γενικότερα οι πελάτες του υπολογιστικού νέφους, οφείλουν να είναι ενημερωμένες σχετικά με τους περιορισμούς στην

ιδιωτικότητα και την ασφάλεια των δεδομένων τους, ειδικά όταν μεταφέρουν προσωπικές πληροφορίες στο περιβάλλον του υπολογιστικού νέφους. Σε περίπτωση που θέματα σχετικά με την ιδιωτικότητα δεν μπορούν να αντιμετωπιστούν επαρκώς, προτείνεται να μην μεταφερθούν οποιεσδήποτε προσωπικές πληροφορίες σε ένα δημόσιο υπολογιστικό νέφος [167].

Όλες οι εταιρείες που θέλουν να εισέλθουν στο υπολογιστικό νέφος είναι υποχρεωμένες να συνάψουν ειδικές συμβάσεις σχετικές με την παροχή των υπηρεσιών από τους παρόχους, με τις οποίες αφενός οι εταιρείες θα προστατεύουν με όποιο δυνατό τρόπο την παραβίαση της ιδιωτικότητας των δεδομένων και των χρηστών της εταιρείας και αφετέρου οι συνεργαζόμενοι πάροχοι με τον αντίστοιχο της εταιρείας, καθώς και ο ίδιος ο πάροχος της συγκεκριμένης εταιρείας δεν θα κάνουν οτιδήποτε, το οποίο θα επέφερε παραβίαση τόσο της ιδιωτικότητας των δεδομένων όσο και των χρηστών της εταιρείας.

Επιπλέον, οι πελάτες θα πρέπει να εξασφαλίζουν μέσω συμβολαίου ότι απαγορεύουν στον πάροχο να χρησιμοποιεί τα δεδομένα για ιδίους σκοπούς, όπως για παράδειγμα για διαφημίσεις ή άλλες εμπορικές υπηρεσίες, καθώς αυτό επίσης είναι αντιφατικό με την εξασφάλιση της ιδιωτικότητας των χρηστών και των δεδομένων.

6.2.2. Ασφάλεια

Η ασφάλεια των δεδομένων αποτελεί πρωταρχικό μέλημα τόσο των παρόχων υπηρεσιών υπολογιστικού νέφους, όσο, κυρίως, των χρηστών και των εταιρειών που κάνουν χρήση των συγκεκριμένων υπηρεσιών. Για αυτό τον λόγο πρωταρχικής σημασίας για οποιαδήποτε συμφωνία μεταξύ παρόχου και εταιρείας είναι η κατοχή και η προσπέλαση στο υπολογιστικό νέφος των δεδομένων της εταιρείας με ασφαλή τρόπο. Σε προηγούμενες παραγράφους έγινε αναλυτική παρουσίαση της ασφάλειας που θα πρέπει να παρέχει ο πάροχος, ώστε να μην υπάρξουν προβλήματα ή κενά. Σε ό,τι αφορά το νομικό κομμάτι, η ασφάλεια επικεντρώνεται στην διασφάλιση του απορρήτου των

προσωπικών πληροφοριών, τόσο της εταιρείας όσο και των υπαλλήλων της εταιρείας [167].

Αρχικά θα πρέπει να ζητηθεί και να καταστεί σαφές μέσω του συμβολαίου μεταξύ εταιρείας – πελάτη και παρόχου, η ακριβής περιοχή αποθήκευσης και επεξεργασίας των δεδομένων. Αν η πολιτική της εταιρείας απαγορεύει τη μεταφορά δεδομένων εκτός των γεωγραφικών ορίων της χώρας που ανήκει, τότε ο πάροχος θα πρέπει να συμμορφωθεί με αυτό και να παρέχει τις υπηρεσίες του μόνο με διακομιστές που βρίσκονται εντός των γεωγραφικών ορίων της χώρας που ανήκει η εταιρεία.

Ένα άλλο βασικό ζήτημα αποτελεί το προσωπικό που διαχειρίζεται το υπολογιστικό νέφος, καθώς και οι τρόποι, τους οποίους παρέχει ο πάροχος για να διασφαλίζει το απόρρητο των προσωπικών δεδομένων από τους ίδιους τους υπαλλήλους του [168]. Παρόλο που το προηγούμενο μπορεί να θεωρηθεί απλό σε επίπεδο συμβολαίου να επιτευχθεί, σε επίπεδο πραγματικής διαχείρισης είναι αρκετά δύσκολο, μιας και θα πρέπει να γίνεται λεπτομερής και σχεδόν καθημερινός έλεγχος στις όσες εργασίες επιτέλεσε ο καθένας από τους υπαλλήλους του υπολογιστικού νέφους σχετικά με τα δεδομένα των χρηστών.

Όπως συμβαίνει και σε ένα τυπικό υπολογιστικό μηχάνημα, έτσι και στο υπολογιστικό νέφος ενδέχεται να υποστεί ζημιά ένα από τα φυσικά μέσα αποθήκευσης δεδομένων που έχει. Σε αυτή την περίπτωση θα πρέπει να υπάρχουν ειδικές διαδικασίες για την ασφαλή καταστροφή του προβληματικού μέσου, οι οποίες να καταγράφονται λεπτομερώς στο συμβόλαιο μεταξύ παρόχου και εταιρείας και, όπου είναι εφικτό, να διασφαλίζεται μέσω μιας τρίτης ανεξάρτητης αρχής ότι έχει τηρηθεί κατά γράμμα ό,τι υπάρχει υπογεγραμμένο στο συμβόλαιο.

Τέλος, μετά το πέρας της συνεργασίας παρόχου και εταιρείας, θα πρέπει να υπάρχουν ειδικές ρήτρες, οι οποίες να υποχρεώνουν τον πάροχο να καταστρέφει όλα τα δεδομένα της εταιρείας που βρίσκονται αποθηκευμένα τόσο στους διακομιστές του, όσο και στα εφεδρικά μέσα αποθήκευσης.

6.2.3. Εμπιστευτικότητα

Μια εταιρεία ενδέχεται να είναι υποχρεωμένη, μέσω νομοθετημάτων, να έχει έμπιστα κάποια δεδομένα. Είναι λοιπόν σημαντικό αυτές οι υποχρεώσεις να διαβιβάζονται στον πάροχο και σε περιπτώσεις που ο πάροχος αποθηκεύσει τα συγκεκριμένα δεδομένα σε ένα τρίτο πάροχο, να διαβιβάζονται σε αυτόν και οι συγκεκριμένες υποχρεώσεις. Θα πρέπει δηλαδή να καταστεί σαφές ότι τα δεδομένα κληροδοτούν, ή μεταφέρουν κατά άλλους, τις ιδιαιτερότητές τους σχετικά με την ασφάλεια, την εμπιστευτικότητα και την ιδιωτικότητά τους, ανεξάρτητα από το μέσο και τον φορέα που είναι αποθηκευμένα [167].

Στις περισσότερες των περιπτώσεων, οι εταιρείες απαιτούν ο πάροχός τους να έχει το ελάχιστο επίπεδο εμπιστευτικότητας πάνω στα δεδομένα τους. Σε περιπτώσεις όμως που ο πάροχος θα έχει στη διάθεσή του ευαίσθητα δεδομένα, το επίπεδο προστασίας θα πρέπει να είναι σημαντικά ισχυρότερο. Αυτό θα πρέπει να αναφέρεται στο συμβόλαιο μεταξύ εταιρείας και παρόχου και απαιτείται να υπάρχει λεπτομερής περιγραφή για τους τρόπους προστασίας που θα παρέχει ο πάροχος για τα ευαίσθητα δεδομένα της εταιρείας. Αυτό θα πρέπει να συμβεί εκ των ων ουκ άνευ, έτσι ώστε σε περίπτωση κοινοποίησης των δεδομένων από τον πάροχο, η εταιρεία αφενός να είναι καλυμμένη νομικά σχετικά με τα δεδομένα που κοινοποιήθηκαν και αφετέρου να κινήσει νομικές διαδικασίες για την παραπομπή του παρόχου.

6.2.4. Διασφάλιση των υποχρεώσεων του παρόχου

Όλα όσα περιγράφηκαν ανωτέρω για τις υποχρεώσεις του παρόχου σχετικά με την προστασία των δεδομένων είναι άχρηστα, αν η εταιρεία δεν είναι σε θέση να επιβεβαιώσει ότι πραγματικά πληρούνται οι απαιτήσεις που επέβαλε μέσω του συμβολαίου. Για να γίνει εφικτό κάτι τέτοιο, θα πρέπει ο πάροχος του υπολογιστικού νέφους να παρέχει ελέγχους που να διασφαλίζουν και να αποδεικνύουν ότι τηρεί τις υποχρεώσεις του [169]. Τα αρχεία καταγραφής συμβάντων θα πρέπει να

είναι στη διάθεση του πελάτη, όταν τα ζητήσει από τον πάροχο και θα πρέπει να είναι όσο το δυνατό πληρέστερα γίνεται.

Μέσα στα αρχεία καταγραφής συμβάντων θα πρέπει να υπάρχει εκτενής αναφορά για τους τόπους αποθήκευσης των δεδομένων, τα άτομα που ήρθαν σε επαφή μαζί τους καθώς και τον τρόπο επαφής, π.χ. ανάγνωση, διαγραφή, τροποποίηση [99]. Σε περίπτωση που ο πάροχος συνεργάζεται με άλλο πάροχο και τα δεδομένα βρίσκονται στον δεύτερο, αφενός ο πελάτης θα πρέπει να ενημερωθεί για αυτή την αλλαγή και ο δεύτερος είναι υποχρεωμένος να παρέχει τα αρχεία καταγραφής συμβάντων στον πρώτο και ο πρώτος στον πελάτη.

6.2.5. Αποζημίωση για απώλεια ή παράνομη χρήση των δεδομένων

Μπορεί να θεωρείται απίθανο, είναι δυνατόν όμως τα δεδομένα μιας εταιρείας να χαθούν οριστικά από το υπολογιστικό νέφος. Αυτό μπορεί να συμβεί εξαιτίας ενός πλήθους περιπτώσεων, όπως κάποιο τεχνικό πρόβλημα, κάποιο λάθος κατά τη διαχείρισή τους, πυρκαγιά ή άλλες φυσικές καταστροφές. Επίσης, ελλοχεύει πάντα ο κίνδυνος παράνομης χρήσης των δεδομένων από επιτήδειους υπαλλήλους του παρόχου ή από τρίτους.

Αν και η πιθανότητα να συμβεί κάτι από τα παραπάνω θεωρείται μηδαμινή μιας και ο κάθε πάροχος έχει αρκετά αντίγραφα ασφαλείας για καθένα από τα δεδομένα, μέσω της συνεχούς συντήρησης του υλικού και τέλος μέσω της εκπαίδευσης των υπαλλήλων του, είναι σημαντικό για μια εταιρεία να εξετάσει πως θα μπορεί να αντιμετωπίσει την απώλεια των δεδομένων της ή της παράνομης χρήσης τους, στο συμβόλαιο που υπέγραψε με τον πάροχο. Αυτό ισχύει ιδιαίτερα στην περίπτωση όπου τα δεδομένα παρέχονται στην εταιρεία από τρίτους και, σε περίπτωση απώλειας ή κατάχρησής τους, φέρει και η ίδια νομική ευθύνη.

Στην περίπτωση που η εταιρεία μπορεί να επιλέξει μεταξύ των παρόχων, θα πρέπει προσδιορίζοντας τους πιθανούς κινδύνους που ελλοχεύουν στο υπολογιστικό νέφος, να επιλέξει τον πλέον κατάλληλο κρίνοντας αποκλειστικά με γνώμονα τους τρόπους διαχείρισης των

κινδύνων που προσφέρουν οι διάφοροι πάροχοι. Αρχικά η εταιρεία θα πρέπει να απαιτεί από τον πάροχο να είναι υπεύθυνος για έμμεσες ή συνεπακόλουθες απώλειες των δεδομένων της, ανεξαρτήτως αιτίας [167]. Σε περίπτωση που συμβεί απώλεια ή κακή χρήση των δεδομένων, είτε εσκεμμένα είτε κατά λάθος, ο πάροχος θα είναι υποχρεωμένος να καταβάλει ένα σεβαστό χρηματικό ποσό ως αποζημίωση.

Τέλος, κρίσιμο στοιχείο για την εξασφάλιση της προστασίας των δεδμένων μιας εταιρείας είναι να διασφαλιστεί στο συμβόλαιο με τον πάροχο, ότι σε περίπτωση τυχόν μεταφορών των δεδομένων της μεταξύ άλλων παρόχων, οι οποίοι ενδεχομένως να συνεργάζονται με τον πάροχο της εταιρείας, αυτοί θα υποχρεούνται επίσης να παρέχουν τις ίδιες απαιτήσεις απορρήτου και ιδιωτικότητας με τον αρχικό πάροχο [170]. Σε περίπτωση που δεν ισχύει κάτι τέτοιο, η εταιρεία μπορεί να διαπιστώσει ότι κάποια συστήματα ασφαλείας, τα οποία έχει διαπραγματευτεί με τον πάροχο και έχει έρθει σε συμφωνία μαζί του για αυτά, ίσως να μην ισχύουν στον τρίτο πάροχο και να μην είναι σε θέση να διεκδικήσει τα δικαιώματά της. Επίσης, η εταιρεία θα πρέπει να είναι γνώστης των παρόχων με τους οποίους συνεργάζεται ο πάροχός της, ώστε να γνωρίζει σε ποια άλλα συστήματα βρίσκονται τα δεδομένα της.

6.3. Ευθύνη

6.3.1. Περιορισμοί στην ευθύνη

Όπως συμβαίνει και με όλες τις παραδοσιακές συμφωνίες πάνω στην πληροφορική, οι πάροχοι υπηρεσιών υπολογιστικού νέφους προσπαθούν να ελαχιστοποιήσουν την ευθύνη που φέρουν για θέματα απώλειας των δεδομένων από την παροχή της υπηρεσίας [167]. Αρχικά προσπαθούν να μην αναγνωρίσουν ευθύνες για απώλειες που οφείλονται σε έμμεσους παράγοντες ή είναι αποτελέσματα άλλων παραγόντων, π.χ. καταστροφή ενός σκληρού δίσκου, ενώ ήταν μέσα στην εγγύηση. Στη συνέχεια κατασκευάζουν τα συμβόλαιά τους με τέτοιο τρόπο, ώστε να έχουν τη χαμηλότερη δυνατή ευθύνη και μόνο υπό κάποιες παραμέτρους. Για παράδειγμα, μπορεί σε κάποιο συμβόλαιο να

δηλώνεται ότι ο πάροχος φέρει ευθύνη για την απώλεια των δεδομένων μόνο για το πρώτο τρίμηνο της υπηρεσίας, ή ότι ο πάροχος δεν φέρει ευθύνη, αν προκύψει ελαττωματικό το εξάρτημα που προκάλεσε την απώλεια των δεδομένων.

Για την καλύτερη κατοχύρωσή τους, οι εταιρείες θα πρέπει να συμβουλεύονται τους νόμους του κράτους στο οποίο ανήκουν και είναι σχετικοί με το ζήτημα, καθώς και την Ευρωπαϊκή νομοθεσία που έχει θεσπιστεί ειδικά για τέτοια θέματα. Θεωρείται θετικό στοιχείο οι πάροχοι να δηλώνουν ότι συμμορφώνονται πλήρως με τα νομοθετήματα τόσο του κράτους του πελάτη τους όσο και γενικότερα, όπως π.χ. της Ευρωπαϊκής Ένωσης.

6.3.2. Παροχή αποζημιώσεων

Αποζημίωση θεωρείται η νομικά δεσμευτική υποχρέωση στην οποία ο ένας συμβαλλόμενος αναλαμβάνει την υποχρέωση να αποδεχτεί τον κίνδυνο απώλειας ή ζημιάς στοιχείων του άλλου συμβαλλόμενου [171]. Σε επίπεδο υπολογιστικού νέφους η αποζημίωση μπορεί να αφορά και τα δύο συμβαλλόμενα μέρη, δηλαδή και από τον πάροχο προς την εταιρεία – πελάτη καθώς και το αντίστροφο [168].

Από τη μία πλευρά, ο πάροχος μπορεί να ζητήσει αποζημίωση από την εταιρεία στην οποία παρέχει τις υπηρεσίες του, αν αποδειχθεί ότι η εταιρεία καταπάτησε τα πνευματικά του δικαιώματα επί των εφαρμογών του. Επίσης, στην περίπτωση που αποδειχτεί ότι καταστράφηκαν δεδομένα εξαιτίας λανθασμένων χειρισμών της εταιρείας, ο πάροχος έχει δικαίωμα και να μην επαναφέρει τα απολεσθέντα δεδομένα αλλά και να ζητήσει αποζημίωση. Τέλος, υπάρχει και η περίπτωση η εταιρεία να καταπατήσει κάποιον ή κάποιους από τους όρους τους συμβολαίου, οπότε και σε αυτή την περίπτωση ο πάροχος δικαιούται αποζημίωση.

Από την άλλη πλευρά, η εταιρεία – πελάτης δικαιούται αποζημίωση από τον πάροχο σε περίπτωση που ο δεύτερος αθετήσει με τη σειρά του κάποιον από τους κανόνες του συμβολαίου. Αν ο πάροχος απολέσει τα δεδομένα της εταιρείας, και η απώλεια δεν υπόκειται σε

κάποια από τις δικλείδες ασφαλείας του, τότε επίσης είναι υποχρεωμένος να πληρώσει αποζημίωση στην εταιρεία. Τέλος, σε περιπτώσεις όπου μέρος των δεδομένων βρεθεί εκτός παρόχου χωρίς τη συγκατάθεση της εταιρείας, ο πάροχος εκτός από αποζημίωση ενδεχομένως να έχει και νομικές συνέπειες.

6.4. Απόδοση ευθυνών

Όπως συμβαίνει και στα παραδοσιακά συμβόλαια παρόχων υπηρεσιών πληροφορικής και πελατών, οι πάροχοι υπηρεσιών υπολογιστικού νέφους αναζητούν να βρουν τρόπους ούτως ώστε να ελαχιστοποιήσουν τις ευθύνες που τους αναλογούν για οποιαδήποτε απώλεια δεδομένων που συμβαίνει στην υπηρεσία τους [167]. Αρχικά, οι πάροχοι αποποιούνται των ευθυνών τους σε περίπτωση που συμβεί μια έμμεση ή συνεπακόλουθη ζημιά, για παράδειγμα αν καταστραφεί ένα κέντρο δεδομένων που το έχουν αγοράσει από μια εταιρεία παροχής υλικού, τότε μεταθέτουν τις ευθύνες στην εταιρεία παροχής υλικού. Επίσης, στα συμβόλαια που συνάπτουν με τους πελάτες τους είτε υποστηρίζουν συγκεκριμένες απώλειες ή προβλήματα μόνο για ένα χρόνο, είτε, εσκεμμένα, δεν αναφέρουν τίποτα για ευθύνες στο συμβόλαιο. Τέλος, διατυπώνουν τα συμβόλαιά τους με τέτοιο τρόπο που να φαίνεται ότι δέχονται κάποια βασικά είδη ευθυνών αλλά με κάποιο όριο, χωρίς να ορίζουν τι σημαίνει η λέξη όριο ή ποιες είναι οι προϋποθέσεις.

Οι πελάτες των παρόχων υπηρεσιών υπολογιστικού νέφους θα πρέπει να ελέγξουν, αν ο πάροχός τους συμμορφώνεται με τα γενικότερα νομικά πλαίσια πάνω σε θέματα ευθυνών, τόσο στην περίπτωση της χώρας τους, όσο και σε γενικότερες περιπτώσεις, για παράδειγμα, αν ο πάροχος έχει νομική ισχύ στην Ευρωπαϊκή Ένωση. Όλες οι νομικές δικλείδες των επίσημων οργανισμών παρέχουν αντικειμενικά ποσοστά ευθύνης και στους παρόχους αλλά και στους πελάτες και συνήθως έχουν μια λίστα από τις υποχρεώσεις τόσο των πελατών όσο και των παρόχων για τις μεταξύ τους δοσοληψίες.

6.4.1. Αποζημίωση

Όπως αναφέρθηκε και σε προηγούμενη παράγραφο, αποζημίωση ονομάζεται η νομικά δεσμευτική υπόσχεση με την οποία ό ένας συμβαλλόμενος αναλαμβάνει την υποχρέωση να αποδεχθεί τον κίνδυνο απώλειας ή ζημίας που ο δεύτερος συμβαλλόμενος μπορεί να υποστεί [171]. Σε αρκετές από τις περιπτώσεις συμβολαίων στο υπολογιστικό νέφος, ο πάροχος ενδεχομένως να ζητήσει αποζημίωση από την εταιρεία που συνεργάζεται. Οι πιο συνηθισμένες περιπτώσεις για τις οποίες ο πάροχος ζητάει αποζημίωση από την εταιρεία είναι όταν ο πάροχος, μέσω της εταιρείας, επεξεργάζεται ή κατέχει παράνομα δεδομένα, όταν χάνονται πόροι τους εξαιτίας κακής χρήσης από την εταιρεία και τέλος, όταν η εταιρεία σπάσει το συμβόλαιό της.

Από την άλλη πλευρά και η εταιρεία με την οποία συνεργάζεται ο πάροχος και έχει συμβόλαιο μαζί του μπορεί να ζητήσει αποζημίωση. Οι εταιρείες παίρνουν αποζημιώσεις, όταν ο πάροχος μεταφέρει τα δεδομένα τους σε άλλο πάροχο χωρίς να τους ενημερώσει, όταν ο πάροχος δεν συμφωνεί με τα διεθνή πρότυπα και όταν ο πάροχος πάψει να παρέχει τις υπηρεσίες του για περισσότερο από τον χρόνο που έχει δηλώσει στο συμβόλαιο που έχει συνάψει μαζί της.

6.5. Διαχείριση της απόδοσης

6.5.1. Επίπεδα εξυπηρέτησης

Τα επίπεδα εξυπηρέτησης (service levels) είναι ένα ικανοποιητικός τρόπος για να διασφαλιστεί ότι ο πάροχος ικανοποιεί το επίπεδο διαλειτουργικότητας που αναμένεται από την εταιρεία. Αυτό είναι ιδιαίτερα σημαντικό στην περίπτωση που η υπηρεσία υπολογιστικού νέφους είναι κρίσιμη είτε για την λειτουργία της ίδιας της εταιρείας ή για τους πελάτες της εταιρείας. Υπάρχουν τρία στοιχεία τα οποία είναι κοινά σε ένα αποτελεσματικό επίπεδο υπηρεσιών. Το πρώτο από τα στοιχεία είναι ότι καθένα από τα επίπεδα υπηρεσιών πρέπει να έχει νόημα, δηλαδή, θα πρέπει να δηλωθεί ποια από τις υπηρεσίες είναι σημαντική για την εταιρεία και θα πρέπει να έχει τη βέλτιστη δυνατή απόδοση.

Επίσης, η αποδοτικότητα του παρόχου σε σχέση με τα επίπεδα παροχής υπηρεσιών θα πρέπει να αξιολογείται με μετρήσιμα μεγέθη, τα οποία θα υπόκεινται σε έλεγχο. Το τελευταίο από τα στοιχεία είναι η ύπαρξη κάποιου κινήτρου για να πληροί ο πάροχος τα επίπεδα των υπηρεσιών, το οποίο κίνητρο θα πρέπει να είναι επαρκές για τον πάροχο. Τα κίνητρα είναι συνήθως χρηματικές απολαβές ή απώλειες, δηλαδή στην περίπτωση που ο πάροχος δεν ικανοποιεί κάποιο από τα επίπεδα υπηρεσιών που έχει συμφωνήσει με την εταιρεία, θα πρέπει να της καταβάλει χρηματική αποζημίωση.

Δεν θα πρέπει να αποτελεί έκπληξη, αν κάποιος πάροχος προσφέρει κάλυψη μόνο σε επίπεδα υπηρεσιών που μπορεί να ανταπεξέλθει πλήρως, με σχεδόν μηδενική πιθανότητα δημιουργίας προβλήματος, οπότε η εκάστοτε εταιρεία θα πρέπει να συζητήσει εκτενώς τα επίπεδα εξυπηρέτησης που θέλει να της παρέχει ο πάροχος και να καταφέρει να τα εντάξει μέσα στο συμβόλαιο που συνάπτει μαζί του, με το λιγότερο δυνατό κόστος για εκείνη.

6.5.2. Χρόνος απόκρισης

Θα είναι πολύ σημαντικό για τον πελάτη, όταν συμβεί μια διακοπή σε μία ή σε περισσότερες από τις υπηρεσίες που παρέχει ο πάροχος στον πελάτη – εταιρεία, να έχει δεσμεύσει μέσω συμβολαίου τον πάροχο ώστε αρχικά να ερευνηθεί το συμβάν και στην περίπτωση που ευθύνεται ο πάροχος, να αποκατασταθεί η διακοπή το συντομότερο δυνατόν. Καλό θα ήταν ο πελάτης να είναι σε θέση να κατηγοριοποιήσει τους χρόνους απόκρισης του παρόχου με βάση τη σοβαρότητα της βλάβης.

6.5.3. Ευελιξία της υπηρεσίας

Ένα από τα βασικότερα πλεονεκτήματα των υπηρεσιών που προσφέρει το υπολογιστικό νέφος, είναι η ευελιξία των υπηρεσιών με τη δυνατότητα που παρέχει για εύκολη αναβάθμιση ή υποβάθμιση του απαιτούμενου επιπέδου υπηρεσιών, ανάλογα με τις ανάγκες του πελάτη [99]. Συνεπώς, είναι πολύ σημαντικό για τον πελάτη να εξετάσει τις

απαιτήσεις του πάνω στο θέμα αυτό. Καίριο θέμα προς εξέταση είναι η διασφάλιση ότι το μοντέλο τιμολόγησης είναι κατάλληλο και συμφέρει τον πελάτη σε σχέση με τη ζήτηση που έχει ανά μονάδα χρόνου. Επίσης, ο πελάτης οφείλει να ενημερωθεί αν η τιμολόγηση αλλάζει όταν υπάρχουν μεγάλες αυξομειώσεις στην ζήτηση από την πλευρά του. Επιπλέον, οι όποιες αλλαγές γίνονται στη ζήτηση από τον πελάτη μπορούν να εισαχθούν μέσα στο συμβόλαιο, ώστε να καλύπτεται νομικά σε περιπτώσεις μεγάλης αυξομείωσης.

6.5.4. Ανάκαμψη από καταστροφή

Η ανάκαμψη από καταστροφή είναι πρωτίστης σημασίας και σε όλες τις περιπτώσεις είναι βασική παράμετρος στα συμβόλαια μεταξύ των παρόχων και των πελατών τους. Ο πάροχος θα πρέπει να διαβεβαιώσει με γραπτά μέσα ότι είναι σε θέση να παρέχει στον πελάτη του απρόσκοπτη πρόσβαση στις υπηρεσίες του και στην περίπτωση καταστροφής, αν δεν είναι εφικτή η συνεχής πρόσβαση, να είναι δυνατή η πρόσβαση στο μικρότερο δυνατό χρόνο. Τα πιο κοινά είδη καταστροφών είναι η διακοπή στην επικοινωνία του δικτύου, η καταστροφή υλικού ή λογισμικού, η πτώση τάσης και κάποια φυσική καταστροφή, όπως για παράδειγμα φωτιά, καταιγίδα και σεισμός.

Οι πελάτες θα πρέπει να εντάξουν μέτρα μέσα στα συμβόλαια που συνάπτουν με τον πάροχο για να διασφαλίσουν την απρόσκοπτη λειτουργία της υπηρεσίας που θέλουν χωρίς διακοπές από καμία από τις προαναφερθείσες αιτίες. Για αυτό θα πρέπει να λάβουν υπόψη τους μια σειρά από παραμέτρους – μέτρα, τα οποία θα πρέπει να πληροί ο πάροχος. Αρχικά, ο πάροχος θα πρέπει να έχει σε διαφορετικές γεωγραφικές θέσεις ανά τον πλανήτη μονάδες ανάκαμψης από καταστροφή, δηλαδή αντίγραφα όλου του συστήματος και των υποδομών που παρέχει. Σε περίπτωση διακοπής της ηλεκτροδότησης, ο πάροχος θα πρέπει να έχει γεννήτριες, οι οποίες να παράγουν αρκετή ηλεκτρική ενέργεια, ώστε να συνεχίσει να λειτουργεί κανονικά η υποδομή του. Επίσης, στο συμβόλαιο που συνάπτει με τον πελάτη του θα πρέπει να παρέχει αναλυτικό πλάνο ανάκαμψης από καταστροφή,

καθώς επίσης και να δηλώνει τις ακριβείς ώρες κατά τις οποίες θα επιτελέσει διάφορες εργασίες επί των υποδομών του, για παράδειγμα εγκαταστάσεις ή ενημερώσεις.

Εκτός των συμβολαίων, οι πελάτες μπορεί να χρειαστεί να λάβουν επιπλέον μέτρα ασφαλείας. Αυτά τα μέτρα θα πρέπει να συμπεριλαμβάνουν εκείνους που τους παρέχουν υπηρεσίες δικτύου και να έχουν εφεδρικές μονάδες ηλεκτροδότησης της εταιρείας τους, σε περίπτωση διακοπής της ηλεκτροδότησης από τον πάροχο. Σε περίπτωση που συμβεί κάτι από τα παραπάνω και ο πελάτης δεν είναι σε θέση να το αντιμετωπίσει επιτυχώς, ο πάροχος υπηρεσιών υπολογιστικού νέφους ενδεχομένως να δικαιούται αποζημίωση για μη χρήση των υπηρεσιών του, ενώ τις έχει διακόψει ο πελάτης.

6.6. Τερματισμός της συμφωνίας

6.6.1. Τέλη τερματισμού

Όπως συμβαίνει με όλα τα συμβόλαια, σημαντικό είναι να εξεταστεί η ενσωμάτωση στο συμβόλαιο μιας ρήτρας πρόωρης καταγγελίας του συμβολαίου, μέσω της οποίας ο πελάτης θα είναι σε θέση είτε να λήξει το συμβόλαιο ή να το περιορίσει στο βαθμό που θέλει [167]. Όταν υπάρχει πρόβλεψη για πρόωρη λήξη του συμβολαίου, ο πελάτης θα πρέπει να εξετάσει τι είδους πληρωμές πρέπει να κάνει σχετικά με την πρόωρη καταγγελία. Ο πελάτης θα πρέπει να υπολογίσει αν πραγματικά τον συμφέρει η αποζημίωση που θα κληθεί να καταβάλει στον πάροχο, δηλαδή αν το κόστος της αποζημίωσης είναι μικρότερο από το κόστος των εξόδων που θα απαιτούνταν από τη χρήση της υπηρεσίας ή από την κάλυψη της απώλειας του κέρδους που θα επιφέρει στον ίδιο η διακοπή χρήσης του υπολογιστικού νέφους. Έχει παρατηρηθεί ότι το ποσό της αποζημίωσης που καλείται να δώσει ο πελάτης στον πάροχο για τη διακοπή ενός συμβολαίου είναι κατά πολύ μεγαλύτερο από το ποσό που θα πλήρωνε, αν είχε κάνει χρήση της υπηρεσίας μέχρι το καθορισμένο τέλος του συμβολαίου του και για αυτό τον λόγο πολλοί από τους πελάτες δεν προβαίνουν καθόλου σε τέτοιες διαδικασίες.

6.6.2. Τερματισμός λόγω μη τήρησης του συμβολαίου

Ο πελάτης θα πρέπει να έχει τη δυνατότητα να τερματίζει εξ ορισμού το συμβόλαιο που έχει συνάψει με τον πάροχό του, στην περίπτωση που ο δεύτερος δεν ικανοποιεί όσα αναγράφονται σε αυτό. Και σε αυτή την περίπτωση όμως ο πελάτης θα πρέπει να είναι ενήμερος σχετικά με τα τέλη τερματισμού και κατά πόσο ισχύουν.

Από την άλλη πλευρά, ο πάροχος έχει και αυτός τη δυνατότητα να τερματίσει το συμβόλαιο που έχει συνάψει με τον πελάτη του, στην περίπτωση που ο δεύτερος δεν είναι εντάξει στις υποχρεώσεις του απέναντί του. Ο βασικότερος λόγος για τερματισμό του συμβολαίου είναι η μη τήρηση του χρονοδιαγράμματος πληρωμής από τον πελάτη προς τον πάροχο. Παρόλα αυτά, ο πάροχος είναι υποχρεωμένος να ενημερώσει τον πελάτη του για τον τερματισμό του συμβολαίου αρκετά μεγάλο χρονικό διάστημα πριν προβεί στην πράξη αυτή, για να δώσει το δικαίωμα στον πελάτη του να απευθυνθεί σε άλλο πάροχο για τις υπηρεσίες του.

Κλείνοντας τη συγκεκριμένη παράγραφο, θα πρέπει να γίνει σαφές στον αναγνώστη ότι η καταγγελία οποιασδήποτε συμφωνίας είναι ένα πολύ σοβαρό θέμα και θα πρέπει να πραγματοποιείται μόνο, άσχετα με το πόσο σαφές είναι το κείμενο του συμβολαίου, με ειδικούς νομικούς συμβούλους.

6.6.3. Αποχώρηση – μεταφορά των υπηρεσιών

Η αποχώρηση από τον πάροχο υπηρεσιών υπολογιστικού νέφους μπορεί να είναι ένα βασικό πρόβλημα για ένα πελάτη από τη στιγμή που οι υπηρεσίες που του εξασφαλίζει ο πάροχος είναι πρωταρχικής σημασίας για τη λειτουργία της εταιρείας του. Από την άλλη πλευρά, αν οι υπηρεσίες που του παρέχει δεν είναι πρωταρχικής σημασίας και μπορεί να αποχωρήσει ομαλά, ή έχουν προβλεφθεί τρόποι για εύκολη μετάβαση από πάροχο σε πάροχο, το γεγονός αυτό μπορεί μακροπρόθεσμα να οδηγήσει σε μεγαλύτερο ανταγωνισμό και

χαμηλότερες τιμές μεταξύ των παρόχων υπηρεσιών υπολογιστικού νέφους.

Αν ο πελάτης θέλει να μεταφέρει την υποδομή του σε ένα νέο πάροχο υπηρεσιών υπολογιστικού νέφους ή να επιστρέψει στο παραδοσιακό μοντέλο πληροφορικής, στο οποίο η υποδομή είναι εντός της εταιρείας του, τότε θα ήταν σημαντικό για τον πελάτη να συμπεριλάβει τις ακόλουθες απαιτήσεις στο συμβόλαιό του με τον πάροχο. Σε πρώτη φάση, ο πάροχος θα πρέπει να είναι υποχρεωμένος να παρέχει οτιδήποτε χρειαστεί σε υπηρεσία για να γίνει η μεταφορά της υποδομής. Τα δεδομένα και οι εφαρμογές θα πρέπει να μετασκευαστούν σε τέτοια μορφή, ώστε ο πρώην πελάτης να μπορεί να τα επεξεργαστεί και στη νέα υποδομή. Επίσης, ο πάροχος θα πρέπει να αναγράφει λεπτομερώς στο συμβόλαιο που συνάπτει με τον πελάτη, ακριβές σχέδιο μεταφοράς τόσο της υποδομής, όσο, το βασικότερο, των δεδομένων του πελάτη σε όποιο μέρος – υποδομή επιθυμεί ο δεύτερος, και σε ό,τι αφορά τα δεδομένα του πελάτη που υπάρχουν στο υπολογιστικό νέφος, να μην μπορεί να τα διαγράψει μέχρι να υπάρχει γραπτή εντολή από τον πελάτη και, όταν συμβεί αυτό, τότε να διαγράψει το σύνολο των δεδομένων, συμπεριλαμβανομένων και των δεδομένων στα εφεδρικά συστήματα, καθώς και των στατιστικών που προέκυπταν από τη χρήση του υπολογιστικού νέφους από τον πελάτη.

6.7. Επίλυση διαφορών

Μια άλλη σημαντική παράμετρος που θα πρέπει να συμπεριλαμβάνεται στο συμβόλαιο μεταξύ παρόχου και πελάτη είναι ο τρόπος επίλυσης των ποικίλων διαφορών που ενδεχομένως προκύψουν κατά τη διάρκεια παροχής της υπηρεσίας. Ο πελάτης θα πρέπει κατ ελάχιστο να απαιτήσει να δηλωθεί από τον πάροχο πάνω σε ποια χώρα και νομοθεσία υπόκειται η υποδομή του και οι υπηρεσίες του [170]. Ο πελάτης θα πρέπει να γνωρίζει το ακριβές δικαστήριο που θα πρέπει να αποταθεί για να λύσει τη διαφορά που τυχόν θα προκύψει με τον πάροχό του. Σε μερικές χώρες λειτουργεί ένας εναλλακτικός μηχανισμός επίλυσης διαφορών, που λειτουργεί σαν μοντέλο διαιτησίας. Ο πελάτης

θα πρέπει να γνωρίζει, μέσω του συμβολαίου, αν ο πάροχος έχει υιοθετήσει ένα τέτοιο μοντέλο, καθώς και το κόστος που θα χρειαστεί για να απευθυνθεί σε αυτό.

Ακόμα και αν σε ένα συμβόλαιο περιλαμβάνονται προσεκτικά διατυπωμένες διατάξεις και οδηγίες, δεν αποκλείεται, όταν βρεθούν στη δικαστική αίθουσα, οι δικαστές να εφαρμόσουν διαφορετικές από τις αναγραφόμενες στο συμβόλαιο οδηγίες, από τη στιγμή που κρίνουν ότι δεν έχουν νομική ισχύ ή δεν έχουν νομική βαρύτητα στο πλαίσιο μιας συγκεκριμένης διαφωνίας μεταξύ πελάτη και παρόχου [167].

Η επιλογή των οδηγιών, ενδέχεται, επίσης, να μην έχει καμία επίδραση στα νομικά ζητήματα που προκύπτουν και δεν έχουν διατυπωθεί στο πλαίσιο της συμφωνίας, μέσω του συμβολαίου. Για παράδειγμα, ο πελάτης μπορεί να αναγράφει στο συμβόλαιο που σύναψε με τον πάροχό του ότι δεν θέλει, εξ ορισμού, να αποθηκεύονται τα δεδομένα κίνησης για έξι μήνες, όπως είναι υποχρεωμένος μέσω νόμου να το πράξει ο πάροχος. Αν ο πάροχος πράξει το αντίθετο και ο πελάτης βρεθεί στα δικαστήρια με τον πάροχο, τότε οι δικαστές θα αθωώσουν τον πάροχο από τη στιγμή που η πράξη που έκανε ήταν μέρος των νομικών διατάξεων της χώρας. Για αυτόν τον λόγο θεωρείται επιτακτικό ο πελάτης να συνοδεύεται νομικό σύμβουλο σε θέματα πληροφορικής, για να μπορεί να δημιουργήσει κανόνες στο συμβόλαιό του που από τη μια πλευρά δεν θα αντιβαίνουν τους νόμους και από την άλλη θα του εξασφαλίζει τη μεγαλύτερη δυνατή ασφάλεια.

Ο πελάτης θα πρέπει να εξετάσει προσεκτικά τις επιπτώσεις της επιλογής των διαφόρων διατάξεων του νόμου και των προτεινόμενων διαδικασιών επίλυσης των διαφορών, ιδιαίτερα όταν αυτές οι διαδικασίες είναι υποχρεωτικές [170]. Θεωρείται απαραίτητο για κάποιον πελάτη να λάβει νομικές συμβουλές από δικηγόρους σχετικά με τις διαδικασίες, συμπεριλαμβανομένου επίσης και του νομικού καθεστώτος που ισχύει στα γεωγραφικά όρια που υπάρχει η υπηρεσία που εκτελεί ο πελάτης. Μέσω του νομικού, ο πελάτης θα αποφύγει πιθανές επιπλέον δαπάνες που θα του προκύψουν στην πορεία και κρυφούς κινδύνους από λάθη στο συμβόλαιο.

6.8. Άλλα νομικά ζητήματα

Υπάρχει μια πληθώρα από άλλα νομικά ζητήματα, τα οποία μπορεί να ανακύψουν σε ένα συμβόλαιο παροχής υπηρεσιών υπολογιστικού νέφους. Στις επόμενες παραγράφους θα σας περιγράψουμε τα σημαντικότερα από αυτά.

6.8.1. Εισαγωγή επιβλαβούς κώδικα

Ένας πιθανός κίνδυνος για τα συστήματα και τα δεδομένα του πελάτη είναι η εισαγωγή επιβλαβούς κώδικα, όπως για παράδειγμα ένας ιός ή δούρειος ίππος. Σε ένα περιβάλλον υπολογιστικού νέφους, ο πελάτης θα πρέπει να βασίζεται στον πάροχο για να του παρέχει ασφάλεια ενάντια στην εισαγωγή επιβλαβούς κώδικα στα δεδομένα και στα συστήματά του, καθώς επίσης και στον τρόπο επικοινωνίας με τα τοπικά συστήματα του πελάτη [99]. Συνεπώς, ο πελάτης θα πρέπει να εξετάσει σε κάθε περίπτωση τους πιθανούς κινδύνους που ελλοχεύουν από την εισαγωγή επιβλαβούς κώδικα στα συστήματα και στα δεδομένα του, καθώς και τις σχετικές υποχρεώσεις που θα πρέπει να επιβληθούν στον πάροχο, ώστε να διασφαλίζονται κατά τον μέγιστο δυνατό τρόπο τα συστήματα και τα δεδομένα του.

6.8.2. Έλεγχος επί των δεδομένων και των εφαρμογών

Είναι πολύ σημαντικό για ένα πελάτη να γνωρίζει τι είδους δεδομένα και εφαρμογές θα έχει στο υπολογιστικό νέφος, από τη στιγμή που τόσο τα δεδομένα όσο και οι εφαρμογές αυτές θα είναι πλέον εκτός των στενών ορίων της εταιρείας του. Θα πρέπει επίσης να γνωρίζει που και πώς αποθηκεύει τα δεδομένα του ο πάροχος, καθώς και, αν μπορεί να έχει πρόσβαση στις εφαρμογές κάποιος άλλος εκτός από τον πελάτη. Για να είναι αποδοτικός και να έχει κάποια υπόσταση ο έλεγχος επί των δεδομένων και των εφαρμογών του πελάτη στο υπολογιστικό νέφος, θα πρέπει να συμπεριλάβει στο συμβόλαιο που συνάπτει με τον πάροχό του μια σειρά από μέτρα [167].

Ο πελάτης θα πρέπει να απαιτήσει να ενημερώνεται από τον πάροχο για την όποια αλλαγή στην αποθήκευση των κλειδιών κρυπτογράφησης μεταξύ των παρόχων, πριν κάτι τέτοιο εφαρμοστεί. Σε μια τέτοια περίπτωση ο πρώτος πάροχος από τη μεριά του θα πρέπει να εξασφαλίσει ότι ο νέος πάροχος πληροί τις προϋποθέσεις και τους όρους που έχουν υπογραφεί μεταξύ πελάτη και αρχικού παρόχου. Τέλος, θα πρέπει να υπάρχει η δυνατότητα εκ μέρους του πελάτη να μην επιτρέψει την αποθήκευση των κλειδιών κρυπτογράφησης σε κάποιο τρίτο πάροχο.

6.8.3. Αλλαγή των όρων υπό την διακριτική ευχέρεια του παρόχου

Μερικά από τα συμβόλαια στο υπολογιστικό νέφος, συνήθως εκείνα που είναι τυποποιημένα, ανήκουν στα δημόσια υπολογιστικά νέφη και είναι διαθέσιμα σε πολλούς πελάτες, περιλαμβάνουν ρήτρες, οι οποίες επιτρέπουν στον πάροχο να αλλάξει τους όρους της σύμβασης ανά πάσα στιγμή κατά τη διακριτική του ευχέρεια, δηλαδή χωρίς τη συμβολή του πελάτη. Από εμπορικής άποψης, είναι εύκολο να κατανοήσουμε τους λόγους για τους οποίους ο πάροχος μπορεί να συμπεριλαμβάνει μια τέτοια ρήτρα στο συμβόλαιό του, ιδίως όταν έχει πολλές χιλιάδες πελατών που χρησιμοποιούν τις υπηρεσίες του. Ωστόσο, η συγκεκριμένη ρήτρα, μπορεί να είναι σοβαρός κίνδυνος για ένα πελάτη, ειδικά στην περίπτωση που ο πελάτης έχει διαπραγματευτεί με τον πάροχο ώστε να εξασφαλίζει και σε αυτόν όλα τα είδη των ρητρών που περιλαμβάνει στα συμβόλαιά του. Ως εκ τούτου, ο πελάτης θα πρέπει αμέσως να διαγράψει τη συγκεκριμένη ρήτρα ή να ζητήσει να υπόκεινται στην έγκρισή του οποιεσδήποτε αλλαγές και αφετέρου να καταστήσει σαφές στον πάροχο, μέσω του συμβολαίου, ότι οποιεσδήποτε αλλαγές που ο δεύτερος επιφέρει στην υπηρεσία και δεν αναγράφονται στο συμβόλαιο θα δίνουν δικαίωμα στον πελάτη να τερματίσει, ανέξοδα, το συμβόλαιο με τον πάροχο.

6.8.4. Εφαρμογή άλλης νομοθεσίας και μεταφορά δεδομένων μεταξύ κρατών

Ο πελάτης, όταν προσυπογράφει ένα συμβόλαιο με τον πάροχο υπηρεσιών υπολογιστικού νέφους, θα πρέπει να γνωρίζει ότι τα δεδομένα του μπορεί να υποβληθούν σε επεξεργασία ή να αποθηκευτούν σε κάποιο διακομιστή που βρίσκεται σε άλλο κράτος, στο οποίο ενδεχομένως να ισχύουν διαφορετικοί νόμοι ως προς την ιδιωτικότητα και την προστασία των δεδομένων των χρηστών [169]. Επίσης, είναι δυνατόν, η εκάστοτε κυβέρνηση του κράτους που υπάρχουν τα δεδομένα να απαιτεί να έχει πλήρη πρόσβαση σε αυτά και ίσως να έχει και αντίγραφό τους.

Για αυτούς τους λόγους, οι πελάτες θα πρέπει να γνωρίζουν τη νομική ισχύ που πρόκειται να έχει σχέση με τα δεδομένα τους και να προβούν στις αντίστοιχες διαδικασίες εγκαίρως. Είναι δεδομένο ότι η νομική συμβολή κρίνεται απαραίτητη για να μην βρεθεί προ εκπλήξεων ο πελάτης. Τέλος, όλοι αυτοί οι κίνδυνοι που προκύπτουν για τον πελάτη μέσω των ξένων δικαιοδοσιών επί των δεδομένων τους, θα πρέπει να εξεταστεί στο πλαίσιο της φύσης των δεδομένων του πελάτη και ανάλογα αυτός να επιλέξει αν θέλει ή όχι να αποθηκεύσει συγκεκριμένα δεδομένα του στο υπολογιστικό νέφος.

6.9. Το πρόβλημα της πολυνομοθεσίας

Το θέμα που θίχτηκε στην αμέσως προηγούμενη παράγραφο είναι η κορυφή του παγόβουνου για ένα σοβαρό ζήτημα που έχει προκύψει από την παγκόσμια χρήση του διαδικτύου σε πρώτη φάση και του υπολογιστικού νέφους σε δεύτερη. Το ζήτημα αυτό έχει σχέση με το ότι οι χρήστες ή αλλιώς πελάτες του υπολογιστικού νέφους δεν εμπίπτουν στα γεωγραφικά όρια του κράτους που ανήκουν τόσο σαν φυσική όσο και σαν νομική υπόσταση και εισέρχονται σε άλλα κράτη με διαφορετικό νομοθετικό πλαίσιο, όχι ως φυσική παρουσία αλλά ως χρήστες κάποιων εφαρμογών ή υπηρεσιών. Για αυτό ακριβώς το ζήτημα θεσπίστηκε ο όρος πολυνομοθεσία.

Ο όρος πολυνομοθεσία (multijurisdiction) προσδιορίζει το πρόβλημα που προκύπτει, αν σε κάποια πράξη εμπλέκονται πάνω από μία νομοθεσίες, για παράδειγμα νομοθεσίες από δύο διαφορετικές χώρες, και γίνεται ιδιαίτερα αντιληπτό, όταν στη νομοθεσία της μιας χώρας η πράξη δεν έχει ποινικό αντίκτυπο, ενώ στην άλλη έχει [167, 172, 173]. Για να γίνει πιο αντιληπτό το προηγούμενο, θα δοθεί ένα θεωρητικό παράδειγμα. Έστω ότι έχουμε ένα πελάτη μιας υπηρεσίας ενός υπολογιστικού νέφους. Ο πελάτης αυτός κατά τη δήλωση των στοιχείων του, ανέφερε ότι είναι είκοσι ετών, άρα ενήλικος για το νομοθετικό πλαίσιο της Ελλάδας. Για τον πρώτο καιρό λειτουργούσε την υπηρεσία του στο υπολογιστικό νέφος χωρίς κανένα πρόβλημα, μιας και ο πάροχος είχε λίγους πελάτες και χρησιμοποιούσε τη δική του υποδομή, η οποία ήταν εντός Ελλάδας. Μετά από λίγους μήνες όμως, οι πελάτες του παρόχου αυξήθηκαν και αυτός αναζήτησε ένα δεύτερο πάροχο, ο οποίος βρισκόταν στις Η.Π.Α., ώστε να λειτουργεί ένα μέρος από την υποδομή του εκεί, όταν αυτό κρίνεται απαραίτητο. Ο αρχικός πελάτης, αν και ενήλικος για τα νομικά δεδομένα της Ελλάδας, ήταν ανήλικος για τα νομικά δεδομένα των Η.Π.Α. Στις Η.Π.Α., για να έχει υπόσταση κάποιος σε νομικές ρήτρες, θα πρέπει να έχει ενηλικιωθεί, αλλιώς υπογράφει κάποιος άλλος ως υπεύθυνος για τον πρώτο. Σε αυτή, λοιπόν, την περίπτωση, ο πελάτης δεν θα ήταν νομικά σωστός απέναντι στον πάροχο και ενδεχομένως ο πάροχος να είχει πρόβλημα με την νομοθεσία που ισχύει εκεί.

Στην πολυνομοθεσία μπορεί να προκύψουν τα εξής προβληματικά σενάρια. Ο πελάτης μπορεί να προβεί σε ενέργεια παράνομη σύμφωνα με τους νόμους της χώρας στην οποία κατοικεί, αλλά νόμιμη σύμφωνα με τους νόμους της άλλης χώρας στην οποία συνέβη το συμβάν. Το δεύτερο προβληματικό σενάριο είναι ακριβώς το αντίθετο από το προηγούμενο, δηλαδή ο πελάτης να κάνει κάτι ποινικά κολάσιμο σε μια χώρα, το οποίο να θεωρείται μη τιμωρητέο στη χώρα που βρίσκεται σαν φυσική υπόσταση.

Κ Ε Φ Α Λ Α Ι Ο Ε Β Δ Ο Μ Ο

Ψηφιακή εγκληματολογία στο υπολογιστικό νέφος

7.1. Εισαγωγή

Ως ψηφιακή εγκληματολογία (Digital Forensics – DF) ορίζεται η χρήση επιστημονικά τεκμηριωμένων μεθόδων για τη διατήρηση, τη συλλογή, την επικύρωση, την αναγνώριση, την ανάλυση, την ερμηνεία, την τεκμηρίωση και την παρουσίαση ψηφιακών αποδεικτικών στοιχείων τα οποία προέρχονται από ψηφιακά μέσα με σκοπό τη διευκόλυνση ή την αναδημιουργία γεγονότων που θεωρούνται αξιόποινα, ή την παροχή

βοήθειας στην πρόβλεψη μη εξουσιοδοτημένων ενεργειών, οι οποίες φαίνεται να είναι αποδιοργανωτικές σε κάποιες προγραμματισμένες λειτουργίες [174]. Το υπολογιστικό νέφος είναι ένα μοντέλο, το οποίο παρέχει μόνιμη, εύχρηστη και κατά παραγγελία πρόσβαση δικτύου σε μια διαμοιραζόμενη δεξαμενή από προσαρμόσιμους υπολογιστικούς πόρους, για παράδειγμα δίκτυα, διακομιστές, αποθηκευτικός χώρος, εφαρμογές και υπηρεσίες, οι οποίοι μπορούν να εκχωρηθούν η να αποσπαστούν από τον πελάτη – χρήστη με ελάχιστη διαχειριστική αλληλεπίδραση από τον πάροχο της υπηρεσίας [06]. Οπότε, η εγκληματολογία του υπολογιστικού νέφους μπορεί να οριστεί ως η χρήση επιστημονικά τεκμηριωμένων μεθόδων για τη διατήρηση, τη συλλογή, την επικύρωση, την αναγνώριση, την ανάλυση, την ερμηνεία, την τεκμηρίωση και την παρουσίαση ψηφιακών αποδεικτικών στοιχείων που προέρχονται από κατανεμημένα υπολογιστικά συστήματα με τρόπο που να διατηρεί την ακεραιότητά τους, ώστε να έχουν νομική ισχύ σε μια δικαστική αίθουσα.

7.2. Τα μοντέλα ανάπτυξης του υπολογιστικού νέφους και οι επιπτώσεις τους στις εγκληματολογικές έρευνες

Σύμφωνα με τον Liu [175] υπάρχουν τέσσερις τύποι μοντέλων ανάπτυξης του υπολογιστικού νέφους. Σε αυτή την ενότητα θα αναπτύξουμε τις επιπτώσεις των εγκληματολογικών ερευνών από την τεχνική, τη νομική και την οργανωτική διάσταση, σύμφωνα με το τρισδιάστατο μοντέλο που πρότεινε η Ruan [176].

7.2.1. Δημόσιο υπολογιστικό νέφος

Δημόσιο υπολογιστικό νέφος (public cloud) ονομάζεται το υπολογιστικό νέφος, του οποίου η υποδομή και οι υπολογιστικοί πόροι είναι διαθέσιμοι στο ευρύ κοινό μέσω ενός δημόσιου δικτύου. Ένα δημόσιο νέφος ανήκει σε μια εταιρεία ή έναν οργανισμό που πουλά υπηρεσίες νέφους και εξυπηρετεί ένα σύνολο από πελάτες [175]. Οι γνωστότεροι δημόσιοι πάροχοι SaaS είναι οι Salesforce, Gmail και

Dropbox. Οι αντίστοιχοι δημόσιοι πάροχοι PaaS είναι οι Force.com και Google App Engine [177] και, τέλος, οι πιο σημαντικοί δημόσιοι πάροχοι IaaS είναι οι AWS της Amazon και το Azure της Microsoft.

7.2.1.1. Πελάτες που έχουν πρόσβαση στο υπολογιστικό νέφος μέσω ενός δημόσιου δικτύου

Σε αυτή την περίπτωση, οι πελάτες είναι συχνά μικρές εταιρείες ή προσωπικοί χρήστες, οι οποίοι από μόνοι τους έχουν ελάχιστες ή καθόλου δυνατότητες διεξαγωγής εγκληματολογικών ερευνών, ή είναι μεγάλες εταιρείες ή κυβερνητικοί οργανισμοί οι οποίοι αναζητούν φθηνές λύσεις για αποθηκευτικό χώρο ή εφαρμογές για τις ασήμαντες υπηρεσίες τους.

Από τεχνικής πλευράς, το συγκεκριμένο μοντέλο ανάπτυξης συχνά επιτρέπει την εύκολη εγγραφή και την ανώνυμη χρήση, χαρακτηριστικά τα οποία θα μπορούσαν να αξιοποιηθούν από κακόβουλους χρήστες. Οι απλοί χρήστες χρειάζεται να δώσουν ιδιαίτερη προσοχή στον τρόπο που χρησιμοποιούνται, αποθηκεύονται και μεταφέρονται στο σύστημα του υπολογιστικού νέφους οι προσωπικές πληροφορίες αναγνώρισής τους (Personal Identifiable Information – PII) [178]. Οι πάροχοι χρειάζεται να προσφέρουν ισχυρές δυνατότητες στον διαχωρισμό των αποδεικτικών στοιχείων σε ένα περιβάλλον πολλαπλής μίσθωσης και αναζήτησης αποδεικτικών στοιχείων με τον πολλαπλασιασμό των τελικών πελατών. Από οργανωτικής άποψης, πολιτικές και διαδικασίες σχετικά με τις δυνατότητες και τις εφαρμογές των εγκληματολογικών ερευνών εξαρτώνται από την πλευρά του παρόχου υπηρεσιών του υπολογιστικού νέφους. Από νομικής πλευράς, το φαινόμενο της πολυνομοθεσίας είναι ένα πολύ δύσκολο σενάριο, το οποίο καλείται να λύσει ο ερευνητής. Επίσης, συχνά υπάρχουν καθιερωμένα συμβόλαια παροχής υπηρεσιών μεταξύ του παρόχου και του πελάτη, τα οποία δεν επιτρέπουν ούτε προσαρμογή στις ανάγκες του πελάτη αλλά ούτε και δυνατότητα διαπραγμάτευσης.

7.2.1.2. Πελάτες που έχουν πρόσβαση στο υπολογιστικό νέφος μέσω του δικτύου της εταιρείας τους

Σε αυτή την περίπτωση, οι πελάτες του υπολογιστικού νέφους είναι εταιρείες ή οργανισμοί, οι οποίοι έχουν αναπτύξει μη-κρίσιμες υπηρεσίες στο δημόσιο υπολογιστικό νέφος. Αυτού του είδους οι πελάτες, τυπικά, πριν μεταφερθούν στο υπολογιστικό νέφος, είχαν ένα επίπεδο υλοποίησης ψηφιακών εγκληματολογικών ερευνών.

Από τεχνικής πλευράς, το εξ ορισμού επίπεδο υλοποίησης ψηφιακών εγκληματολογικών ερευνών του παρόχου είναι μερικές φορές υψηλότερο από εκείνο των πελατών, έτσι ώστε η μεταφορά των εφαρμογών στο υπολογιστικό νέφος να έχει ως αποτέλεσμα την αναβάθμιση του επιπέδου υλοποίησης των ψηφιακών εγκληματολογικών ερευνών από τη μεριά του πελάτη. Επίσης, ένα επιπλέον επίπεδο αυθεντικοποίησης και ελέγχου πρόσβασης μπορεί να εισαχθεί εντός του δικτύου της εταιρείας. Από οργανωτικής πλευράς, ο πελάτης μπορεί να διαμοιράζεται μέρος των αρμοδιοτήτων του σχετικά με τις πολιτικές και τις διαδικασίες πάνω σε θέματα ψηφιακών εγκληματολογικών ερευνών. Τέλος, από νομικής πλευράς, ο πελάτης μπορεί να ορίζει το νομοθετικό πλαίσιο στο οποίο υπόκεινται τα δεδομένα του μέσω του συμβολαίου παροχής υπηρεσιών που συνυπογράφει με τον πάροχό του.

7.2.2. Ιδιωτικό νέφος

Ένα ιδιωτικό υπολογιστικό νέφος (private cloud) δίνει αποκλειστική πρόσβαση σε έναν πελάτη για τη χρήση της υποδομής του υπολογιστικού νέφους και των υπολογιστικών και αποθηκευτικών πόρων. Μπορεί να διευθύνεται είτε από τον ίδιο τον πελάτη, δηλαδή να είναι εντός του φυσικού χώρου της εταιρείας του ή να γίνεται ανάθεσή του σε μια τρίτη εταιρεία ή αλλιώς έναν πάροχο υπηρεσιών υπολογιστικού νέφους [175].

Οι γνωστότεροι πάροχοι σε αυτή την κατηγορία είναι οι Oracle Grid και IBM CLoudBurst από μεριάς IaaS, Oracle Fusion και Azure Functions

από μεριάς PaaS και Microsoft Office 365 και IBM LotusLive Notes από μεριάς SaaS.

7.2.2.1. Ιδιωτικό υπολογιστικό νέφος εντός της εταιρείας του πελάτη

Το συγκεκριμένο μοντέλο ανάπτυξης είναι παρόμοιο με την παραδοσιακή υποδομή ενός πληροφοριακού συστήματος μιας εταιρείας. Σε αυτή την περίπτωση, οι πελάτες είναι μεσαίες και μεγάλες εταιρείες ή οργανισμοί, οι οποίοι αναπτύσσουν τα σημαντικά τμήματα των υπηρεσιών τους εντός του ιδιωτικού υπολογιστικού νέφους. Αυτού του είδους οι πελάτες, σε γενικές γραμμές, πριν μεταφέρουν την υποδομή τους στο υπολογιστικό νέφος, είχαν μεγάλο επίπεδο υλοποίησης ψηφιακών εγκληματολογικών ερευνών.

Από τεχνικής πλευράς, όταν το επίπεδο υλοποίησης ψηφιακών εγκληματολογικών ερευνών της εταιρείας είναι ανώτερο από αυτό που προσφέρει ο πάροχος υπηρεσιών υπολογιστικού νέφους, η μεταφορά της υποδομής στο υπολογιστικό νέφος θα έχει ως αποτέλεσμα την υποβάθμιση του επιπέδου υλοποίησης των ψηφιακών εγκληματολογικών ερευνών από τη μεριά του πελάτη αν και ως αντάλλαγμα θα είναι το μειωμένο κόστος της πληροφοριακής του υποδομής. Ωστόσο, μια τέτοια αντιστάθμιση θα πρέπει να ληφθεί σοβαρά υπόψη εκ μέρους του πελάτη, πριν προβεί σε οποιαδήποτε ενέργεια. Από οργανωτικής πλευράς, θα πρέπει να καταβληθούν συλλογικές προσπάθειες από ειδικές εγκληματολογικές ομάδες τόσο από την πλευρά του παρόχου όσο και από την πλευρά του πελάτη με σκοπό να προσδώσουν σημαντικές δυνατότητες σε μια ψηφιακή εγκληματολογική έρευνα. Από νομικής πλευράς, από τη στιγμή που τα δεδομένα θα είναι εντός της εταιρείας, για αυτά θα ισχύει το ίδιο νομικό καθεστώς με τον πελάτη.

7.2.2.2. Ανάθεση του ιδιωτικού υπολογιστικού νέφους

Η ανάθεση του ιδιωτικού υπολογιστικού νέφους μιας εταιρείας σε έναν πάροχο είναι πολύ πιο φθηνή σε σύγκριση με την προηγούμενη

υλοποίηση, επειδή η συντήρηση και η υποδομή του υπολογιστικού νέφους γίνεται από τον πάροχο. Σε ό,τι αφορά τις επιπτώσεις σε μια ψηφιακή εγκληματολογική έρευνα, είναι οι ίδιες με την προηγούμενη υλοποίηση εκτός από το νομικό κομμάτι. Στην τρέχουσα υλοποίηση τα δεδομένα μπορεί να ανήκουν σε διαφορετική νομοθετική δικαιοδοσία από ό,τι ο πελάτης – κάτοχός τους.

7.2.3. Κοινοτικό υπολογιστικό νέφος

Ένα κοινοτικό υπολογιστικό νέφος (community cloud) εξυπηρετεί ένα σύνολο πελατών, οι οποίοι έχουν κοινά ενδιαφέροντα, όπως στόχους, ασφάλεια, ιδιωτικότητα και κοινή πολιτική, αντί να εξυπηρετεί μία μόνο εταιρεία ή οργανισμό, όπως γίνεται στην περίπτωση του ιδιωτικού νέφους [175]. Παρόμοια με το ιδιωτικό νέφος, το κοινοτικό νέφος μπορεί να είναι αντικείμενο διαχείρισης από τις εταιρείες που το χρησιμοποιούν ή από κάποιο πάροχο και μπορεί είτε να υλοποιείται εντός μιας από τις εταιρείες που το χρησιμοποιούν, ή να έχει ανατεθεί σε κάποιον πάροχο. Τα πιο γνωστά κοινοτικά υπολογιστικά νέφη είναι τα κυβερνητικά υπολογιστικά νεφη (government clouds) [179], τα οποία παρέχονται από τους παρόχους δημόσιων υπολογιστικών νεφών για υπηρεσίες δημοσίου τομέα και μόνο.

7.2.3.1. Κοινοτικό υπολογιστικό νέφος εντός της εταιρείας του πελάτη

Σε αυτή την περίπτωση το υπολογιστικό νέφος φιλοξενείται σε μία από τις εταιρείες που απαρτίζουν την κοινότητα και οι υπόλοιπες εταιρείες συνδέονται σε αυτή, για να έχουν πρόσβαση στις υπηρεσίες υπολογιστικού νέφους.

Από τεχνικής πλευράς, το επίπεδο υλοποίησης ψηφιακών εγκληματολογικών ερευνών γίνεται με κοινή προσπάθεια από όλες τις εταιρείες της κοινότητας. Επίσης, απαιτείται διαχωρισμός των ψηφιακών αποδεικτικών στοιχείων μεταξύ των διαφόρων εταιρειών και μεταξύ των διαφόρων χρηστών των εταιρειών, οι οποίοι χρησιμοποιούν τις υπηρεσίες του υπολογιστικού νέφους. Από οργανωτικής πλευράς,

πολιτικές και διαδικασίες υλοποίησης ψηφιακών εγκληματολογικών ερευνών διαμοιράζονται μεταξύ των εταιρειών της κοινότητας. Τέλος, από νομικής πλευράς, αφού τα δεδομένα μπορεί να είναι αποθηκευμένα σε διαφορετικό γεωγραφικό σημείο από κάποια εταιρεία, από τη στιγμή που η εταιρεία που φιλοξενεί το υπολογιστικό νέφος βρίσκεται σε άλλη χώρα από τις υπόλοιπες έχουμε και εδώ το πρόβλημα της πολυνομοθεσίας. Επίσης, σε αυτή την υλοποίηση προκύπτουν ζητήματα σχετικά με την πολλαπλή μίσθωση, καθώς κάθε εταιρεία θα έχει αρκετούς χρήστες που θα χρησιμοποιούν από κοινού τις υπηρεσίες και τους πόρους.

7.2.3.2. Ανάθεση του κοινοτικού υπολογιστικού νέφους

Στην περίπτωση της ανάθεσης ενός κοινοτικού υπολογιστικού νέφους πολλές εταιρείες που ανήκουν στην ίδια κοινότητα διαμοιράζονται ένα ιδιωτικό υπολογιστικό νέφος από ένα πάροχο υπηρεσιών υπολογιστικού νέφους και έχουν πρόσβαση στις υπηρεσίες του μέσω δικτύου. Αυτή η περίπτωση σαν λύση είναι φθηνότερη από την προηγούμενη για τους γνωστούς λόγους, της συντήρησης του νέφους και της υποδομής που ανήκει στον πάροχο.

Από τεχνικής πλευράς, το επίπεδο υλοποίησης των ψηφιακών εγκληματολογικών ερευνών διατέθεται τόσο από τον πάροχο του υπολογιστικού νέφους όσο και από τους συμμετέχοντες στο κοινοτικό υπολογιστικό νέφος. Επιπλέον, απαιτείται διαχωρισμός των ψηφιακών αποδεικτικών στοιχείων μεταξύ των διαφόρων χρηστών των εταιρειών. Από οργανωτικής πλευράς, οι πολιτικές και οι διαδικασίες σχετικά με τις ψηφιακές εγκληματολογικές έρευνες διαμοιράζονται μεταξύ του παρόχου από τη μία και των εταιρειών από την άλλη. Από νομικής πλευράς, τα δεδομένα μπορεί να βρίσκονται σε διαφορετική τοποθεσία από τις εταιρείες, οπότε και εδώ προκύπτει το πρόβλημα της πολυνομοθεσίας.

7.2.4. Υβριδικό υπολογιστικό νέφος

Υβριδικό υπολογιστικό νέφος (hybrid cloud) είναι η σύνθεση από δύο ή περισσότερα μοντέλα ανάπτυξης, τα οποία παραμένουν ως ξεχωριστές οντότητες αλλά είναι συνδεδεμένα μεταξύ τους με τυποποιημένες τεχνολογίες, οι οποίες επιτρέπουν τη φορητότητα των δεδομένων και των εφαρμογών [175].

Σύμφωνα με την εταιρεία Gartner [24], το υβριδικό υπολογιστικό νέφος είναι το πρώτο μεταξύ των πέντε τάσεων του υπολογιστικού νέφους και με το πέρασμα του χρόνου θα μπορούσε να οδηγήσει σε ένα ενοποιημένο μοντέλο ενός και μόνο υπολογιστικού νέφους που θα δημιουργείται από πολλές πλατφόρμες, εσωτερικές ή εξωτερικές, οι οποίες θα μπορούν να χρησιμοποιηθούν ως βάση για τις μελλοντικές και μεταβαλλόμενες απαιτήσεις των εταιρειών.

Δυστυχώς το υβριδικό υπολογιστικό νέφος είναι η πιο δύσκολη περίπτωση από τα μοντέλα του υπολογιστικού νέφους, γιατί ανάλογα με το ποσοστό των μοντέλων που το απαρτίζουν, υπάρχει και διαφορετικό αποτέλεσμα στο τρίπτυχο που προαναφέραμε. Το μόνο σίγουρο είναι ότι ακόμα και στην περίπτωση που στα υπόλοιπα μοντέλα επιλυθούν τα επιμέρους ζητήματα που προκύπτουν σε μια ψηφιακή εγκληματολογική έρευνα, στο υβριδικό μοντέλο θα συνεχίζουν να υπάρχουν άλυτα ζητήματα.

7.3. Σύγκριση κλασικών τεχνικών σε περιβάλλον υπολογιστικού νέφους

Ένα μοντέλο διαδικασίας ψηφιακής εγκληματολογίας παρέχει ένα πλαίσιο για τη διεξαγωγή εγκληματολογικών ερευνών. Ενώ δεν υπάρχει κάποιο συγκεκριμένο μοντέλο που να ταιριάζει απόλυτα για όλα τα είδη των ψηφιακών εγκληματολογικών ερευνών. Παρόλα αυτά, ένα γενικό μοντέλο μπορεί να εφαρμοστεί σε πολλούς τύπους εγκληματολογικών ερευνών ανεξάρτητα από την τεχνολογία που χρησιμοποιείται. Με τη βοήθεια ενός τέτοιου γενικού μοντέλου, του IDIPM (Integrated digital investigation process model) που έχει προταθεί από τους Carrier και

Spafford [180] θα εξετάσουμε όλα τα επιμέρους προβλήματα που θα προκύψουν κατά τη διάρκεια μας εγκληματολογικής έρευνας στο υπολογιστικό νέφος κάνοντας χρήση του συγκεκριμένου μοντέλου. Το μοντέλο IDIPM αποτελείται από πέντε διακριτές φάσεις: τη διατήρηση των ψηφιακών αποδεικτικών στοιχείων, την έρευνα, την αναζήτηση και συλλογή, την ανακατασκευή του συμβάντος και την παρουσίαση των αποτελεσμάτων.

7.3.1. Φάση διατήρησης

Η φάση της διατήρησης σε μια παραδοσιακή ψηφιακή εγκληματολογική έρευνα συνεπάγεται την ασφάλιση της ψηφιακής σκηνής του εγκλήματος και της διατήρησης των ψηφιακών αποδεικτικών στοιχείων. Αυτό περιλαμβάνει την απομόνωση του υπολογιστικού συστήματος από το δίκτυο, τη συλλογή των ευαίσθητων δεδομένων (volatile data), τα οποία θα μπορούσαν να χαθούν όταν το σύστημα κλείσει και τον προσδιορισμό των ύποπτων διεργασιών που τρέχουν στο σύστημα. Επίσης, θα πρέπει να ερευνηθούν όλοι οι ύποπτοι χρήστες, οι οποίοι έχουν πρόσβαση στο σύστημα. Τέλος, τα αρχεία καταγραφής συμβάντων περιέχουν πολύτιμα αποδεικτικά στοιχεία και θα πρέπει να ασφαλιστούν, αν υπάρχει έστω και μικρή πιθανότητα απώλειας, πριν γίνει αντιγραφή του συστήματος.

Στην περίπτωση της έρευνας σε περιβάλλον υπολογιστικού νέφους, η απευθείας διατήρηση περιορίζεται μόνο στο υπολογιστικό σύστημα του υπόπτου, αν και εφόσον και αυτό είναι διαθέσιμο. Οποιαδήποτε άλλη διατήρηση δεν είναι εφικτή, επειδή τα δεδομένα είναι αποθηκευμένα σε μια απομακρυσμένη εικονική συσκευή. Ο ερευνητής μπορεί να προσπαθήσει να διατηρήσει τα δεδομένα του υπόπτου στο υπολογιστικό νέφος με εισαγγελική εντολή προς τον πάροχο υπηρεσιών υπολογιστικού νέφους του υπόπτου. Ωστόσο, ο ερευνητής θα πρέπει να εμπιστευτεί τον πάροχο ότι θα ανακτήσει και θα διατηρήσει τα δεδομένα με εγκληματολογικά ορθό τρόπο, κάνοντας δηλαδή χρήση κάποιας από τις δοκιμασμένες μεθόδους ψηφιακής εγκληματολογίας. Αυτό σημαίνει ότι ο πάροχος θα πρέπει να έχει

κατανοήσει ότι πλέον τα δεδομένα θεωρούνται ψηφιακά αποδεικτικά στοιχεία και έχουν νομική υπόσταση.

7.3.2. Φάση έρευνας

Ο στόχος της φάσης της έρευνας είναι η αναγνώριση και ο εντοπισμός των αποδεικτικών στοιχείων και η ανάπτυξη μιας πρώτης θεωρίας για το συμβάν. Εύθραυστα αποδεικτικά στοιχεία, όπως για παράδειγμα το περιεχόμενο της μνήμης RAM, καταγράφονται και συλλέγονται αμέσως ούτως ώστε να αποτραπεί ενδεχόμενη ζημιά ή καταστροφή τους. Ο Carrier και ο Spafford [180] αναφέρουν μια υπόθεση εισβολής σε ένα διακομιστή στην οποία ο ερευνητής αναζήτησε προφανή σημάδια από εγκατάσταση rootkit, ανέλυσε τα αρχεία καταγραφής συμβάντων και έψαξε για τυχόν νέα αρχεία ρυθμίσεων. Σε ένα περιβάλλον υπολογιστικού νέφους, ο υπολογιστής του υπόπτου μπορεί να ελεγχθεί για αποδεικτικά στοιχεία, αλλά ο ερευνητής δεν θα μπορεί να έχει πρόσβαση στα εξωτερικά δεδομένα, επειδή η φυσική εξέταση των απομακρυσμένων διακομιστών δεν είναι εφικτή.

Το επίπεδο στο οποίο ο ερευνητής μπορεί να αναγνωρίσει πιθανά αποδεικτικά στοιχεία σε ένα περιβάλλον υπολογιστικού νέφους επηρεάζεται κατά πολύ από το μοντέλο παροχής υπηρεσιών αυτού, δηλαδή από το αν είναι εφαρμογή-ως-υπηρεσία (SaaS), πλατφόρμα-ως-υπηρεσία (PaaS) ή υποδομή-ως-υπηρεσία (IaaS).

Στο μοντέλο SaaS, ο πελάτης δεν έχει κανένα έλεγχο επί της κείμενης υποδομής, όπως για παράδειγμα το λειτουργικό σύστημα, τις εφαρμογές, τους διακομιστές με πιθανή εξαίρεση ελάχιστες ρυθμίσεις επί των εφαρμογών που χρησιμοποιεί. Σε αυτή την περίπτωση, η αναγνώριση πιθανών αποδεικτικών στοιχείων από την μεριά του διακομιστή καθίσταται πάρα πολύ δύσκολο έργο για τον ερευνητή. Αυτό συμβαίνει γιατί βασίζεται μόνο στα αρχεία καταγραφής συμβάντων των εφαρμογών και του συστήματος, τα οποία θα λάβει από τον πάροχο υπηρεσιών υπολογιστικού νέφους. Αυτό με την σειρά του είναι δυνατό, μόνο αν ο πάροχος έχει εγκατεστημένο κάποιο είδος μηχανισμού

δημιουργίας αρχείων καταγραφής συμβάντων και καθιστά διαθέσιμα τα δεδομένα από αυτά τα αρχεία.

Το μοντέλο IaaS προσφέρει τα πιο πολλά αποδεικτικά στοιχεία στον ερευνητή. Σε ένα περιβάλλον IaaS, ο πελάτης – χρήστης ελέγχει την εγκατάσταση των εικονικών μηχανών, το υποκείμενο λειτουργικό σύστημα, καθώς και τις εφαρμογές που χρησιμοποιεί. Ως εκ τούτου, υπάρχει η δυνατότητα να εγκαταστήσει προγράμματα καταγραφής συμβάντων και να παρακολουθεί τη δραστηριότητα όλων των χρηστών του, η οποία θα μπορούσε να βελτιώσει σε μεγάλο βαθμό την ποιότητα των εγκληματολογικών ερευνών, αλλά δυστυχώς αυτό δεν είναι ο κανόνας. Παρόλα αυτά, ένας ερευνητής μπορεί να έχει πρόσβαση σε περισσότερα πιθανά αποδεικτικά στοιχεία στο μοντέλο IaaS από ό,τι στα άλλα δύο μοντέλα υπηρεσιών του υπολογιστικού νέφους.

Στο μοντέλο PaaS, ο πελάτης μπορεί να συγγράψει και να αναπτύξει εφαρμογές που τις δημιουργεί κάνοντας χρήση γλωσσών προγραμματισμού, βιβλιοθηκών, υπηρεσιών και εργαλείων που υποστηρίζονται από το πάροχο υπηρεσιών υπολογιστικού νέφους. Ο πελάτης δεν διαχειρίζεται και δεν ελέγχει την υποκείμενη υποδομή του υπολογιστικού νέφους, συμπεριλαμβανομένων του δικτύου, των διακομιστών, του λειτουργικού συστήματος και του αποθηκευτικού χώρου, αλλά έχει τον πλήρη έλεγχο στις εφαρμογές που αναπτύσσει και τις ρυθμίσεις σχετικά με τις εφαρμογές αυτές στο περιβάλλον που θα τις φιλοξενεί [06]. Αυτό δυσχεραίνει σημαντικά τη δυνατότητα του ερευνητή να εντοπίσει ενδεχόμενα αποδεικτικά στοιχεία, δεδομένου ότι η έρευνά του περιορίζεται σε συγκεκριμένα αρχεία καταγραφής συμβάντων σχετικά με την εφαρμογή μόνο, και εφόσον υπάρχουν και αυτά.

Σε αυτό το σημείο αξίζει να σημειωθεί ότι η τεκμηρίωση δεν θεωρείται ότι είναι ξεχωριστή φάση κατά τη διεξαγωγή μιας ψηφιακής εγκληματολογικής έρευνας, καθώς οτιδήποτε εντοπίζεται από ψηφιακά αποδεικτικά στοιχεία, καταγράφεται την ίδια στιγμή. Η τελική έκθεση των αποδεικτικών στοιχείων λαμβάνει χώρα κατά τη φάση της παρουσίασης. Τα ψηφιακά αποδεικτικά στοιχεία θα πρέπει να καταγράφονται και να τεκμηριώνονται προσεκτικά. Για παράδειγμα, ένα αρχείο τεκμηριώνεται κάνοντας χρήση της πλήρους διαδρομής του, τους

τομείς του λειτουργικού συστήματος που χρησιμοποιούσε το συγκεκριμένο αρχείο και τους τομείς του σκληρού δίσκου πάνω στους οποίους ήταν γραμμένο. Επίσης, υπολογίζεται η τιμή της συνάρτησης κατακερματισμού (hash function) [165], ώστε να διασφαλιστεί η επαλήθευση της ακεραιότητας του. Σε περίπτωση που τα ψηφιακά αποδεικτικά στοιχεία θα πρέπει να παρουσιαστούν σε δικαστική αίθουσα, ο ερευνητής είναι υποχρεωμένος να κατασκευάσει και "chain of custody".

Τόσο η τεκμηρίωση όσο και η αντίστοιχη χρονολογική (chain of custody) είναι δύσκολες εργασίες στο περιβάλλον του υπολογιστικού νέφους. Όπως προαναφέρθηκε, το επίπεδο των ψηφιακών αποδεικτικών στοιχείων που είναι διαθέσιμα στον ερευνητή μπορεί να ποικίλλει, γεγονός που επηρεάζει άμεσα το βαθμό επιτυχούς τεκμηρίωσης των ψηφιακών αποδεικτικών στοιχείων. Για παράδειγμα, ο ερευνητής που θα έχει άμεση πρόσβαση σε μια εικονική μηχανή θα μπορεί να καταγράψει και να τεκμηριώσει τα αρχεία που βρήκε σε αυτή την μηχανή. Από την άλλη πλευρά, αν ο ερευνητής βασιστεί στον πάροχο υπηρεσιών υπολογιστικού νέφους για να την παροχή των αρχείων που θέλει, θα πρέπει δείξει εμπιστοσύνη στο πάροχο ότι θα συλλέξει τα αρχεία με εγκληματολογικά ορθό τρόπο, χωρίς να καταστρέψει δηλαδή την ακεραιότητα τους.

7.3.3. Φάση αναζήτησης και συλλογής

Η συγκεκριμένη φάση περιλαμβάνει μια διεξοδική ανάλυση του συστήματος για εύρεση ψηφιακών αποδεικτικών στοιχείων. Αυτή η φάση χρησιμοποιεί τα αποτελέσματα της προηγούμενης φάσης για τον προσδιορισμό των διαφόρων τύπων ανάλυσης που θα πρέπει να εκτελεστούν. Για παράδειγμα, μπορεί κατά τη διάρκεια αυτής της φάσης να γίνει μια αναζήτηση λέξεων – κλειδιών, με τις λέξεις αυτές να προσδιορίζονται από άλλα αποδεικτικά στοιχεία ή μπορεί να γίνει ένα χρονοδιάγραμμα χαμηλού επιπέδου για τη δραστηριότητα που έλαβε χώρα στα αρχεία με τελικό σκοπό τις δραστηριότητες των χρηστών.

Στη φάση της αναζήτησης και της συλλογής καταναλώνεται το μεγαλύτερο μέρος του χρόνου που δαπανάται για μια έρευνα, καθώς σε αυτή συλλέγεται οτιδήποτε μπορεί να έχει αποδεικτική αξία, συνήθως από κάποιο μέσο ψηφιακής συσκευής αποθήκευσης δεδομένων. Η μέθοδος συλλογής περιλαμβάνει τη λήψη αντιγράφων από τις αποθηκευτικές συσκευές, ώστε να μπορούν να εξεταστούν σε συνθήκες εργαστηρίου. Άλλες μέθοδοι συλλογής χρησιμοποιούνται για τη συλλογή δεδομένων που είναι αποθηκευμένα στη μνήμη του υπολογιστικού συστήματος και στους καταχωρητές. Το μεγαλύτερο μέρος της συγκεκριμένης φάσης σε ένα παραδοσιακό μοντέλο ψηφιακής εγκληματολογικής έρευνας διεξάγεται σε τοπικό επίπεδο, εκτός αν, για παράδειγμα, η ανάκτηση των αρχείων καταγραφής συμβάντων του δικτύου επιβάλλει τη χρήση του διακομιστή στον οποίο είναι αποθηκευμένα τα αρχεία αυτά.

Η κατανεμημένη υποδομή του υπολογιστικού νέφους δημιουργεί προκλήσεις όσον αφορά την αναζήτηση και τη συλλογή. Η διασκορπισμένη φύση των δεδομένων στο υπολογιστικό νέφος σημαίνει ότι ο ερευνητής πρέπει να προσαρμόσει παραδοσιακές τεχνικές στο νέο περιβάλλον. Ο ερευνητής οφείλει να καταλάβει τον τρόπο με τον οποίο είναι αποθηκευμένα τα δεδομένα στο υπολογιστικό νέφος και να καθορίσει το πώς μπορεί να ανακτηθούν διατηρώντας παράλληλα την ακεραιότητά τους.

Σε τοπικό επίπεδο, τα ψηφιακά αποδεικτικά στοιχεία μπορεί να συλλεγούν από το ιστορικό του προγράμματος περιήγησης, και αυτό συμβαίνει, επειδή η επικοινωνία μεταξύ του πελάτη και της υπηρεσίας του υπολογιστικού νέφους, τυπικά, γίνεται μέσω του προγράμματος περιήγησης. Άλλα ψηφιακά αποδεικτικά στοιχεία, όπως για παράδειγμα τα δεδομένα εισόδου του χρήστη, για να εισέλθει στο υπολογιστικ;ο νέφος ή τα άμεσα μηνύματα, θα πρέπει επίσης να εξαχθούν και να αποκρυπτογραφηθούν, μιας και αυτό θα δώσει στον ερευνητή πρόσβαση σε προηγούμενες επικοινωνίες που διενεργήθηκαν από τον πελάτη στο διαδίκτυο. Σε επίπεδο δικτύου, σε γενικές γραμμές δεν είναι δυνατή η ανάλυση της κίνησης, επειδή οι πάροχοι υπηρεσιών μπορεί να

μην παρέχουν δεδομένα καταγραφής από τα στοιχεία του δικτύου που χρησιμοποιούνται από τα στιγμιότυπα και τις εφαρμογές του πελάτη.

Αν γίνεται χρήση του μοντέλου IaaS, τότε μπορεί να είναι δυνατό για τον ερευνητή να λάβει ολόκληρη την εικόνα την εικονικής συσκευής και να την αναλύσει στο εργαστήριο, όπως συμβαίνει και στο παραδοσιακό μοντέλο με ένα κανονικό σύστημα. Η κατάσταση είναι κάπως πιο περίπλοκη στην περίπτωση του PaaS λόγω του ότι στον ερευνητή είναι διαθέσιμα δεδομένα σχετικά μόνο με την εφαρμογή και τίποτα άλλο. Ο ερευνητής θα πρέπει να προσκομίσει δικαστική εντολή, η οποία θα απαιτεί από τον πάροχο να εκτελέσει την έρευνα, να συλλέξει τα δεδομένα και να τα επιστρέψει στον ερευνητή. Ο ερευνητής θα πρέπει να θεωρήσει ότι ο πάροχος υπηρεσιών υπολογιστικού νέφους χρησιμοποιεί αξιόπιστες διαδικασίες και εργαλεία για να διεξάγει την αναζήτηση, καθώς και για να επανασυνδέσει και να καταγράψει τα δεδομένα. Σε περίπτωση που η συλλογή των αποδεικτικών στοιχείων δεν γίνει με ορθό τρόπο, αυτά δεν θα έχουν καμία νομική υπόσταση, δεν θα θεωρούνται αποδεικτικά στοιχεία, δηλαδή, στο δικαστήριο.

7.3.4. Φάση ανακατασκευής του συμβάντος

Η φάση της ανακατασκευής του συμβάντος περιλαμβάνει την οργάνωση των αποτελεσμάτων των αναλύσεων από τα ψηφιακά και φυσικά αποδεικτικά στοιχεία που έχουν συλλεχθεί, με σκοπό την ανάπτυξη μιας θεωρίας για το συμβάν. Δεδομένα τα οποία απαιτούν προηγμένες τεχνικές ανάλυσης, όπως για παράδειγμα τα εκτελέσιμα αρχεία ή τα αρχεία που είναι κρυπτογραφημένα, μπαίνουν στο μικροσκόπιο και σε αυτή την φάση χρησιμοποιούνται τα αποτελέσματα της έρευνας. Επιστημονικές μέθοδοι εφαρμόζονται στα ψηφιακά αποδεικτικά στοιχεία, για να δοκιμαστεί η θεωρία σχετικά με το συμβάν. Σε ορισμένες περιπτώσεις, ενδέχεται να επαναληφθεί η φάση της αναζήτησης, για να ληφθούν επιπρόσθετα ψηφιακά αποδεικτικά στοιχεία.

Σε μια ψηφιακή εγκληματολογική έρευνα στο υπολογιστικό νέφος, ο πάροχος υπηρεσιών υπολογιστικού νέφους ελέγχει τα δεδομένα που

δίνει στον ερευνητή και ως εκ τούτου η ποσότητα των δεδομένων που του δίνει ενδεχομένως να επηρεάσει την ορθή ανασυγκρότηση του συμβάντος. Επιπλέον, λόγω της αποθήκευσης των δεδομένων στο υπολογιστικό νέφος καθίσταται δύσκολη η τοποθέτησή τους σε μια σωστή χρονολογική σειρά από τον ερευνητή. Η κατάσταση αυτή μπορεί να επιδεινωθεί, αν λάβουμε υπόψη μας το γεγονός ότι τα δεδομένα είναι αποθηκευμένα σε διαφορετικές γεωγραφικές περιοχές και τα σχετικά ρολόγια των υπολογιστικών συστημάτων στα οποία είναι αποθηκευμένα, δεν είναι συγχρονισμένα. Τα συγκεκριμένα προβλήματα μπορεί να επηρεάσουν αρνητικά την αξιοπιστία των αποδεικτικών στοιχείων στη δικαστική αίθουσα.

7.3.5. Φάση παρουσίασης

Η συγκεκριμένη φάση είναι η τελική στη διαδικασία της εγκληματολογικής έρευνας. Κατά τη διάρκεια αυτής της φάσης, όλα τα φυσικά και τα ψηφιακά αποδεικτικά στοιχεία καταγράφονται και παρουσιάζονται στην δικαστική αίθουσα ή σε αυτόν για τον οποίο διεξάγεται η έρευνα. Σε αυτή την φάση θεωρείται ότι είναι οι εκθέσεις, οι παρουσιάσεις και όλη η εργασία του ερευνητή. Η επιμέρους τεκμηρίωση για την υποστήριξη της κάθε επιμέρους φάσης είναι ιδιαίτερα σημαντική γιατί βοηθά στην απόδειξη της χρονογραμμής των γεγονότων του συμβάντος.

Σε μια εγκληματολογική έρευνα, τα αποδεικτικά στοιχεία θα πρέπει να παραμείνουν αναλλοίωτα και ο ερευνητής θα πρέπει να είναι σε θέση να παρουσιάσει τα ευρήματα, εξηγώντας τη σημασία και τις επιπτώσεις όλων των ενεργειών που έκανε κατά την διάρκεια της έρευνας. Επιπλέον, για κάθε βήμα της έρευνάς του θα πρέπει να τηρεί πολύ αυστηρό αρχείο καταγραφής όλων των κινήσεών του. Σε ένα περιβάλλον υπολογιστικού νέφους, είναι δύσκολο, αν όχι αδύνατο, να διατηρηθεί ένα αυστηρό ιστορικό βημάτων της έρευνας, ειδικά στην περίπτωση που τα δεδομένα είναι αποθηκευμένα σε πολλαπλές τοποθεσίες και υπό τον έλεγχο διαφορετικών οντοτήτων.

7.3.6. Ελλείψεις

Από τα παραπάνω έγινε σαφές ότι συγκεκριμένες ελλείψεις κατά τη διάρκεια των διαφόρων φάσεων της έρευνας μπορεί να επηρεάσουν αρνητικά τόσο την ομαλή διεξαγωγή της έρευνας όσο, το κυριότερο, τα αποτελέσματα που εξήγε ο ερευνητής κατά τη διάρκεια της διεξαγωγής της. Αυτό θα μπορούσε να θέσει σε αμφισβήτηση την εγκυρότητα των ψηφιακών αποδεικτικών στοιχείων που παρουσιάζονται σε μια δικαστική αίθουσα.

Θα μπορούσαμε να συνοψίσουμε τις ελλείψεις που προκύπτουν λόγω του ιδιαίτερου περιβάλλοντος του υπολογιστικού νέφους που θα πρέπει να εργαστεί ο ερευνητής στις ακόλουθες προτάσεις. Αρχικά, έχουμε την αδυναμία του ερευνητή να διατηρήσει την ψηφιακή σκηνή του εγκλήματος, γεγονός που θα επηρεάσει δυσμενώς την ακεραιότητα των ψηφιακών αποδεικτικών στοιχείων που συλλέγονται. Επίσης, έχουμε απροθυμία ή αδυναμία από μέρους του παρόχου υπηρεσιών υπολογιστικού νέφους να παρέχει δεδομένα στον ερευνητή, όπως για παράδειγμα αρχεία καταγραφής συμβάντων των εφαρμογών και του δικτύου. Στα προηγούμενα θα πρέπει να προστεθεί το γεγονός της περιορισμένης πρόσβασης από τον ερευνητή στα δεδομένα του υπολογιστικού νέφους, το οποίο έχει ως αποτέλεσμα τη μη σφαιρική εξέταση των δεδομένων του συμβάντος. Τέλος, σε ένα περιβάλλον υπολογιστικού νέφους ο ερευνητής θα βρεθεί αντιμέτωπος με ανώνυμα δεδομένα καθώς και μεταδεδομένα που έχουν αλλοιωθεί είτε εσκεμμένα από τον πάροχο, είτε κατά λάθος.

7.4. Άλλα θέματα

Άλλα θέματα που σχετίζονται με τη διενέργεια μια ψηφιακής εγκληματολογικής έρευνας στο υπολογιστικό νέφος, μπορούν επίσης να επηρεάζουν την ποιότητα των ψηφιακών αποδεικτικών στοιχείων που ανακτώνται από τον ερευνητή. Αυτό, με τη σειρά του, θα μπορούσε να επηρεάσει την αξιοπιστία των στοιχείων αυτών στο δικαστήριο.

7.4.1. Πολλαπλή μίσθωση

Η πολλαπλή μίσθωση είναι μια από τις ιδιότητες του υπολογιστικού νέφους, η οποία επιτρέπει σε πολλαπλούς χρήστες – πελάτες να διαμοιράζονται τον ίδιο φυσικό διακομιστή και να χρησιμοποιούν υπηρεσίες που παρέχονται από κοινό υλικό και λογισμικό του παρόχου υπηρεσιών νέφους ταυτόχρονα. Σε μερικές περιπτώσεις, οι υποδομές πολλαπλής μίσθωσης δημιουργούν ανησυχία, επειδή η κατανομή των πόρων είναι εκτεταμένη, εμφανίζεται σε πολύ μεγάλη κλίμακα και περιλαμβάνει πολλαπλές και πιθανόν ευπαθείς διεπαφές [181]. Αυτό το περιβάλλον στο οποίο γίνεται διαμοιρασμός πόρων δημιουργεί επιπλέον προκλήσεις για τον ερευνητή, ο οποίος δεν χρειάζεται να ασχοληθεί μόνο με τις υπηρεσίες που χρησιμοποιούνται από ένα πελάτη, αλλά επίσης και με όλα εκείνα τα αντικείμενα που υπάρχουν σε ένα περιβάλλον πολλαπλής μίσθωσης, καθώς και τους πόρους που διαμοιράζεται με τους άλλους πελάτες. Οι πόροι που διαμοιράζονται όλοι οι πελάτες μεταξύ τους είναι επεξεργαστική ισχύ και μνήμη, προσωρινή και μόνιμη. Οι πάροχοι υπηρεσιών υπολογιστικού νέφους είναι συχνά απρόθυμοι να δώσουν πρόσβαση στον ερευνητή στην κοινή μνήμη, διότι ενδέχεται να περιέχει δεδομένα που ανήκουν και σε άλλους χρήστες και η ανάγνωση αυτών θα μπορούσε να παραβιάσει την εμπιστευτικότητα και το απόρρητο των συμφωνιών που έχουν υπογραφεί μεταξύ του παρόχου και των πελατών του.

7.4.2. Προέλευση των δεδομένων

Η προέλευση των δεδομένων καταδεικνύει τον ιδιοκτήτη και την επεξεργαστική ιστορία των δεδομένων, και ως εκ τούτου είναι εξέχουσας σημασίας για την ψηφιακή εγκληματολογική έρευνα [182, 183]. Η προέλευση των δεδομένων μπορεί να παρέχει πληροφορίες σχετικά με το ποιος ή τι δημιούργησε τα δεδομένα και επίσης ποιος ή τι τα τροποποίησε. Ο βαθμός στον οποίο η προέλευση των δεδομένων μπορεί να υλοποιηθεί σε ένα περιβάλλον υπολογιστικού νέφους εξαρτάται από τον τύπο του μοντέλου που χρησιμοποιείται. Σε μια υλοποίηση SaaS, η προέλευση των δεδομένων μπορεί να είναι δύσκολο να εντοπιστεί,

επειδή ο πάροχος υπηρεσιών υπολογιστικού νέφους δεν θα δώσει στον ερευνητή πρόσβαση στην εφαρμογή και στα αρχεία καταγραφής συμβάντων που δημιουργούνται. Σε περίπτωση παραβίασης ενός λογαριασμού χρήστη, ο πελάτης δεν έχει τη δυνατότητα να προσδιορίζει τα δεδομένα που διέρρευσαν ή προσπελάστηκαν από τον κακόβουλο χρήστη. Αυτό περιλαμβάνει τροποποίηση ή διαγραφή των δεδομένων από τον κακόβουλο χρήστη, τα οποία με τη σειρά του τα διαγράφει και ο πάροχος για λόγους διαχείρισης του αποθηκευτικού χώρου.

7.4.3. Θέματα πολυνομοθεσίας

Τα δεδομένα που είναι αποθηκευμένα σε ένα περιβάλλον υπολογιστικού νέφους συχνά είναι κατανεμημένα μεταξύ αρκετών διαφορετικών περιοχών, με σκοπό την ανοχή των σφαλμάτων αφενός και την αποτελεσματικότητα της πρόσβασης αφετέρου. Ωστόσο, η κατανομή των δεδομένων δημιουργεί το ζήτημα της νομικής δικαιοδοσίας, το οποίο με τη σειρά του παρουσιάζει προβλήματα σε τυχόν νομικές διαδικασίες. Σύμφωνα με τον Garrie [184], το δικαστήριο μπορεί να επιληφθεί ενός θέματος μόνο, αν έχει νομική δικαιοδοσία επί των μερών και του αντικειμένου της πράξης. Επιπλέον, οι διάφορες υπηρεσίες επιβολής του νόμου μπορούν να ασκούν τις αρμοδιότητές τους μόνο εντός της επικράτειας που ανήκουν.

Τα προβλήματα οξύνονται, όταν τα δεδομένα είναι αποθηκευμένα σε μια άλλη χώρα καθώς οι νόμοι σχετικά με την εμπιστευτικότητα και την ιδιωτικότητα διαφέρουν σημαντικά από χώρα σε χώρα. Για παράδειγμα, μερικές χώρες έχουν αυστηρούς νόμους σχετικά με το απόρρητο των τραπεζικών εγγράφων και ειδικές κυρώσεις για παραβίαση των νόμων αυτών, οι οποίες μπορεί να περιλαμβάνουν, μεταξύ άλλων, και ποινικές κυρώσεις. Σε τέτοιες περιπτώσεις, μπορεί να μην καταστεί δυνατή η ανάκτηση όλων των ψηφιακών αποδεικτικών στοιχείων πάνω σε ένα συμβάν. Ο Garrie [184] αναφέρει χαρακτηριστικά ότι τα θέματα που προκύπτουν από την πολυνομοθεσία στο υπολογιστικό νέφος είναι η κυριότερη πρόκληση που θα πρέπει να

αντιμετωπίσει ο ερευνητής κατά τη διάρκεια διεξαγωγής της ψηφιακής εγκληματολογικής έρευνας.

7.4.4. Χρονολογική τεκμηρίωση

Η εγκαθίδρυση της χρονολογικής τεκμηρίωσης (Chain of Custody) είναι πρωταρχικής σημασίας για κάθε εγκληματολογική έρευνα [185]. Αυτή βοηθά στο να διαθέτει ο ερευνητής ένα τεκμηριωμένο ιστορικό για την έρευνα και συγκεκριμένα για το τρόπο συλλογής, ανάλυσης και διατήρησης των αποδεικτικών στοιχείων, κατά τέτοιο τρόπο, ώστε να τα παρουσιάσει στο δικαστήριο χωρίς να υπάρχει κίνδυνος απόρριψής τους [186].

Σε μια παραδοσιακή εγκληματολογική έρευνα, η χρονολογική τεκμηρίωση ξεκινά όταν ο ερευνητής διαφυλάττει τα αποδεικτικά στοιχεία στη σκηνή του εγκλήματος και τελειώνει όταν τα αποδεικτικά στοιχεία παρουσιάζονται στη δικαστική αίθουσα. Η κατανεμημένη φύση του υπολογιστικού νέφους περιπλέκει σημαντικά το έργο της διατήρησης της κατάλληλης χρονολογικής τεκμηρίωσης. Τα ψηφιακά αποδεικτικά στοιχεία θα πρέπει να συλλεχθούν από απομακρυσμένους διακομιστές με ασφαλή και νόμιμο τρόπο ώστε να μπορούν να παρουσιάζονται ως αποδεικτικά στοιχεία στο δικαστήριο. Αν ο ερευνητής δεν μπορεί να έχει άμεση πρόσβαση στις υπηρεσίες του υπολογιστικού νέφους ή στο υλικό, είναι απαραίτητο να βασιστεί στον πάροχο του υπολογιστικού νέφους για να του δημιουργήσει αντίγραφα των δεδομένων του υπόπτου, μέσω των οποίων ο ερευνητής θα εξάγει τα ψηφιακά αποδεικτικά στοιχεία. Επιπρόσθετα, ο ερευνητής θα πρέπει να εξασφαλίσει τη συνεχή διατήρηση της χρονολογικής τεκμηρίωσης, ώστε τα δεδομένα από το υπολογιστικό νέφος, συμπεριλαμβανομένων και αυτών που συλλέχτηκαν από τρίτους, να μπορούν να παρουσιαστούν ως αποδεικτικά στοιχεία στο δικαστήριο.

7.4.5. Συμβόλαια παροχής υπηρεσιών

Όπως αναφέρθηκε και σε προηγούμενη ενότητα, ένα συμβόλαιο παροχής υπηρεσιών (Service Level Agreement - SLA) είναι ένα συμφωνητικό μεταξύ του παρόχου υπηρεσιών νέφους και του πελάτη των υπηρεσιών νέφους, το οποίο θέτει τους όρους χρήσης των πόρων του υπολογιστικού νέφους [187]. Τα περισσότερα συμβόλαια παροχής υπηρεσιών δεν έχουν λάβει μέριμνα σχετικά με τη διεξαγωγή ψηφιακών εγκληματολογικών ερευνών και την ανάκτηση ψηφιακών αποδεικτικών στοιχείων από το περιβάλλον του υπολογιστικού νέφους, όταν κάτι τέτοιο χρειαστεί. Θεωρείται απαραίτητο να υπάρχουν ειδικά εδάφια σχετικά με την ανάκτηση ψηφιακών αποδεικτικών στοιχείων από το περιβάλλον του υπολογιστικού νέφους τα οποία θα πρέπει να είναι ενσωματωμένα στα συμβόλαια παροχής υπηρεσιών. Μεταξύ άλλων θα πρέπει να περιλαμβάνουν τρόπους πρόσβασης στα δεδομένα κατά τη διάρκεια διεξαγωγής μια εγκληματολογικής έρευνας και διατάξεις που αφορούν έρευνα σε περιβάλλοντα πολλαπλής νομικής δικαιοδοσίας και πολλαπλής μίσθωσης, συμπεριλαμβανομένων των νομικών ρυθμίσεων σχετικά με την εμπιστευτικότητα και την προστασία της ιδιωτικότητας των χρηστών [176].

Προς το παρόν, οι όροι που υπάρχουν στα συμβόλαια παροχής υπηρεσιών είναι διατυπωμένοι με τέτοιο τρόπο, ώστε να προστατεύουν τον πάροχο και σε γενικές γραμμές είναι μη-διαπραγματεύσιμοι [188]. Έτσι, ο πελάτης δεν έχει άποψη όσον αφορά τα δεδομένα που ο πάροχος υπηρεσιών υπολογιστικού νέφους μπορεί και δεν μπορεί να αποκαλύψει. Σε τελική ανάλυση όμως, η ευθύνη βαρύνει αποκλειστικά τον πελάτη για να διαπραγματευτεί μια κατάλληλη συμφωνία με τον πάροχο υπηρεσιών υπολογιστικού νέφους στην οποία να αναφέρονται οι τρόποι ανάκτησης ψηφιακών αποδεικτικών στοιχείων από το υπολογιστικό νέφος, καθώς επίσης και προβληματικά ζητήματα, όπως είναι η πολυνομοθεσία, η κυριότητα των δεδομένων και η εγκαθίδρυση της χρονολογικής τεκμηρίωσης.

7.5. Υπάρχουσες λύσεις

Όπως έγινε κατανοητό και από τα προηγούμενα, προφανώς υπάρχουν πολλά άλυτα θέματα σχετικά με την ψηφιακή εγκληματολογική έρευνα σε περιβάλλοντα υπολογιστικού νέφους. Τα θέματα αυτά επιδεινώνονται από τη δυναμική και συνεχώς μεταβαλλόμενη φύση του υπολογιστικού νέφους. Στην παρούσα υποενότητα θα ασχοληθούμε με μερικές λύσεις που προτάθηκαν από άλλους ερευνητές και θα μπορούσαν να βοηθήσουν σε μια ψηφιακή εγκληματολογική έρευνα σε περιβάλλον υπολογιστικού νέφους.

7.5.1. Έλεγχος εργαλείων για εγκληματολογική έρευνα

Δυστυχώς δεν υπάρχουν εργαλεία ή σουίτες εργαλείων από την παραδοσιακή ψηφιακή εγκληματολογία που θα μπορούσαν αυτούσια να ανταπεξέλθουν στο περιβάλλον του υπολογιστικού νέφους. Έχουν γίνει κάποιες μελέτες αξιολόγησης που επικεντρώθηκαν στη χρήση των υφιστάμενων εργαλείων για την απόκτηση αποδεικτικών στοιχειών από το υπολογιστικό νέφος, οι οποίες ωφέλησαν την κοινότητα των ερευνητών σε περιβάλλοντα υπολογιστικού νέφους, αλλά δεν έχει επιτευχθεί ολοκληρωμένη λύση για δημιουργία εργαλείων που είναι ικανά να λειτουργήσουν αποδοτικά στο υπολογιστικό νέφος. Για παράδειγμα, χρειάζονται εργαλεία, τα οποία θα είναι σε θέση να εκτελέσουν live αναλύσεις στο δυναμικό περιβάλλον του υπολογιστικού νέφους. Σε πολλές περιπτώσεις, η live ανάλυση προσφέρει την ευκαιρία για συλλογή πολύτιμων δεδομένων από ένα σύστημα που λειτουργεί, όπως για παράδειγμα τα δεδομένα που είναι στη μνήμη ή στους καταχωρητές.

Ένα άλλο σημαντικό κενό αφορά τα σύνολα δεδομένων πάνω στα οποία τρέχουν τα διάφορα εργαλεία που χρησιμοποιούνται σε μια ψηφιακή εγκληματολογική έρευνα. Επίσης, ένα άλλο θέμα που προκύπτει σε περιβάλλοντα υπολογιστικού νέφους είναι η συσχέτιση των προσωρινών δεδομένων με τους χρήστες τους. Ο πελάτης του υπολογιστικού νέφους και ο πάροχος υπηρεσιών του υπολογιστικού

νέφους συχνά ανήκουν σε διαφορετικές ζώνες ώρας, γεγονός που θα μπορούσε να προκαλέσει προβλήματα στα μεταδεδομένα, όπως για παράδειγμα τον χρόνο δημιουργίας, τροποποίησης και τελευταίας πρόσβασης σε κάποια δεδομένα και αυτό να οδηγήσει σε λανθασμένα αποτελέσματα κατά τη διεξαγωγή της έρευνας. Εννοείται ότι υπάρχει και το χειρότερο σενάριο, στο οποίο τα διάφορα συστήματα δεν έχουν συγχρονισμένα τα ρολόγια τους, οπότε το έργο του ερευνητή γίνεται ακόμα πιο δύσκολο. Η ανάπτυξη μεθόδων για αυτοματοποίηση της συσχέτισης των δεδομένων αυτών θα είναι πολύ χρήσιμη, καθώς θα μειώσει, αν όχι θα εξαλείψει, την ανάγκη διεξαγωγής χειρωνακτικής έρευνας από τον ερευνητή.

7.5.2. Διαφάνεια των υπηρεσιών του νέφους και των δεδομένων

Η έλλειψη διαφάνειας σχετικά με την εσωτερική υποδομή ενός περιβάλλοντος υπολογιστικού νέφους δημιουργεί επιπλέον προκλήσεις στο πλαίσιο διεξαγωγής της έρευνας. Παρόλο που οι πληροφορίες σχετικά με τις εσωτερικές εργασίες είναι πολύτιμες για μια έρευνα, οι πάροχοι υπηρεσιών υπολογιστικού νέφους παρέχουν ελάχιστες σχετικά με το περιβάλλον στο οποίο αποθηκεύονται και επεξεργάζονται τα δεδομένων των χρηστών. Η έλλειψη διαφάνειας δημιουργείται από την ανάγκη για προστασία των ευαίσθητων δεδομένων των χρηστών. Επίσης, η κοινοποίηση πληροφοριών σχετικά με την εσωτερική υποδομή ενός υπολογιστικού νέφους θα μπορούσε να καταστήσει το υπολογιστικό νέφος ευάλωτο σε μια επίθεση [189]. Επιπρόσθετα, οι πάροχοι υπηρεσιών υπολογιστικού νέφους είναι απρόθυμοι να δώσουν πληροφορίες σχετικά με την υποδομή του υπολογιστικού νέφους τους, γιατί θα μπορούσαν αυτές να χρησιμοποιηθούν από τους ανταγωνιστές τους. Τέλος, οποιαδήποτε αρνητική πληροφορία που θα κυκλοφορούσε σχετικά με τις υπηρεσίες ή τις διεργασίες ενός υπολογιστικού νέφους θα μπορούσε να βλάψει τη φήμη του παρόχου του [190].

Ο Haaberlen πρότεινε ότι οι υπηρεσίες του υπολογιστικού νέφους θα πρέπει να είναι διαφανείς τόσο στον πελάτη όσο και στον πάροχο και ότι και τα δύο μέρη θα πρέπει να είναι σε θέση να ελέγχουν αν

λειτουργούν σωστά ή όχι οι υπηρεσίες που συμφωνήθηκαν μεταξύ τους [191]. Σε περίπτωση που δημιουργηθεί κάποιο πρόβλημα, τα συμβαλλόμενα μέρη θα πρέπει να είναι σε θέση να καθορίσουν ποιος από τους δύο ευθύνεται και να αποδείξει την ύπαρξη του προβλήματος σε κάποιο τρίτο, όπως το δικαστήριο. Η συγκεκριμένη πρόταση είναι επωφελής και για τις δύο πλευρές. Από τη μια πλευρά, ο πελάτης μπορεί να ελέγχει κατά πόσο ή όχι αυτά που υπογράφηκαν στο συμβόλαιο παρέχονται από τον πάροχο και από την άλλη πλευρά, ο πάροχος μπορεί να χειριστεί τυχόν καταγγελίες από τους πελάτες του και να επιλύσει τις διαφορές μαζί τους με μεγαλύτερη ευκολία.

7.5.3. Συμβόλαια παροχής υπηρεσιών

Τα συμβόλαια παροχής υπηρεσιών θα πρέπει να περιλαμβάνουν ξεκάθαρες και ακριβείς διαδικαστικές πληροφορίες για τον τρόπο διεξαγωγής μιας ψηφιακής εγκληματολογικής έρευνας τόσο από κάποιο ερευνητή όσο και από τον πάροχο των υπηρεσιών υπολογιστικού νέφους στην περίπτωση ενός συμβάντος. Θα πρέπει να γίνει ακριβής ορισμός των ρόλων και κάθε μέλος οφείλει να είναι πλήρως ενημερωμένο σχετικά με τις ευθύνες, τις δυνατότητες και τα όριά του. Επιπροσθέτως, στα συμβόλαια παροχής υπηρεσιών είναι αναγκαίο να αντιμετωπίζονται οι νομικές διαδικασίες διεξαγωγής της έρευνας σε ένα περιβάλλον πολλαπλής μίσθωσης και παράλληλα πολλών νομικών δικαιοδοσιών.

7.5.4. Εγκληματολογία-ως-Υπηρεσία

Στο μοντέλο εγκληματολογίας-ως-υπηρεσία (Forensics-as-a-Service – FaaS) [192], ο πάροχος υπηρεσιών υπολογιστικού νέφους θα πρέπει να είναι υπεύθυνος για την απόκτηση των ψηφιακών αποδεικτικών στοιχείων ή τουλάχιστον να παράσχει βοήθεια και μέσα στον ερευνητή, για να συλλέξει εκείνος τα ψηφιακά αποδεικτικά στοιχεία. Ο πάροχος υπηρεσιών υπολογιστικού νέφους είναι σε θέση να διατηρεί και να συλλέγει τα δεδομένα, επειδή ελέγχει την υποδομή του υπολογιστικού νέφους και όχι μόνο τις εικονικές μηχανές, αλλά επίσης

τους μηχανισμούς δημιουργίας αρχείων καταγραφής συμβάντων και τα αρχεία πληρωμών των πελατών του. Το συγκεκριμένο μοντέλο θα μπορούσε να υλοποιηθεί από τους παρόχους υπηρεσιών υπολογιστικού νέφους με πολύ μικρή αλλαγή στην υπάρχουσα υποδομή τους και θα παρείχε στους πελάτες τους τη διαβεβαίωση ότι μπορούν να διεξαχθούν υψηλής ποιότητας ψηφιακές εγκληματολογικές έρευνες σε περίπτωση που προκύψει κάποιο συμβάν. Αυτό με τη σειρά του θα είχε ως συνέπεια τη μεγαλύτερη αποδοχή των υπηρεσιών νέφους από περισσότερο κόσμο.

7.6. Εγκληματολογικά στοιχεία σε περιβάλλον υπολογιστικού νέφους

Ο NIST ορίζει ένα γενικό διάγραμμα για την αναπαράσταση των τριών τύπων συστατικών για την παροχή υπηρεσιών υπολογιστικού νέφους [193]. Οι τρεις αυτοί τύποι είναι το φυσικό επίπεδο πόρων, το επίπεδο απόκρυψης και το επίπεδο υπηρεσιών. Όπως και στο παραδοσιακό μοντέλο υπολογιστών, έτσι και στο υπολογιστικό νέφος θα πρέπει να οριστεί ο βαθμός ευαισθησίας των ψηφιακών εγκληματολογικών στοιχείων.

7.6.1. Φυσικό επίπεδο

Το φυσικό επίπεδο περιλαμβάνει πόρους υλικού, όπως κεντρικές μονάδες επεξεργασίας και μνήμη. Επίσης διαθέτει μέρη δικτύου, όπως για παράδειγμα δρομολογητές (routers) και μεταγωγείς (swithes) και αποθηκευτικά στοιχεία, όπως σκληροί δίσκοι. Τέλος, σε αυτό το επίπεδο περιλαμβάνονται άλλα φυσικά μέσα υποδομής, όπως θέρμανση, εξαερισμός, κλιματισμός, παροχή επικοινωνίας και παροχή ισχύος.

Στο συγκεκριμένο επίπεδο υπάρχει και η φυσική αποθήκευση των δεδομένων, λειτουργία που είναι υπό τον έλεγχο του παρόχου υπολογιστικού νέφους. Συνήθως αυτή είναι γεωγραφικά μακριά τόσο από τον καταναλωτή – πελάτη όσο και από το νομοθετικό πλαίσιο του

πελάτη. Τα ψηφιακά εγκληματολογικά στοιχεία σε επίπεδο υλικού περιλαμβάνουν τους σκληρούς δίσκους, τα αρχεία καταγραφής συμβάντων του δικτύου και τα αρχεία καταγραφής συμβάντων των δρομολογητών του δικτύου. Επίσης, σε αυτό το επίπεδο συγκαταλέγονται στοιχεία από τα κέντρα δεδομένων όπως για παράδειγμα αρχεία πρόσβασης, αρχεία δραστηριοτήτων, εσωτερικές και εξωτερικές κάμερες παρακολούθησης του χώρου, αρχείο επισκεπτών και πληροφορίες σχετικά με τους μόνιμους εργαζόμενους σε αυτό τον τομέα. Η φυσική πρόσβαση στο κτήριο του κέντρου δεδομένων για την επί τόπου διεξαγωγή έρευνας μπορεί εκτός από πολύ δαπανηρή στις περισσότερες των περιπτώσεων να είναι αδύνατη. Ως εκ τούτου, τα ψηφιακά αποδεικτικά στοιχεία από αυτό το επίπεδο θα πρέπει να συλλέγονται με τεχνικές απομακρυσμένης συλλογής ή από πάροχο σε πάροχο.

7.6.2. Επίπεδο απόκρυψης

Το συγκεκριμένο επίπεδο περιέχει τα συστατικά στοιχεία που χρησιμοποιεί ο πάροχος για την παροχή και τη διαχείριση της πρόσβασης των υπολογιστικών πόρων μέσω λογισμικού. Τα συστατικά μέρη του συγκεκριμένου επιπέδου περιλαμβάνουν στοιχεία λογισμικού, όπως για παράδειγμα εικονικά υπολογιστικά συστήματα, εικονικές αποθηκευτικές συσκευές και hypervisors.

Το συγκεκριμένο επίπεδο τελεί υπό τον έλεγχο του παρόχου υπηρεσιών υπολογιστικού νέφους και είναι αδιαφανές στον πελάτη. Ωστόσο, αυτό το επίπεδο είναι εξαιρετικά σημαντικό για τη διευθέτηση των θεμάτων των πολλών ταυτόχρονων χρηστών πάνω σε θέματα συλλογής ψηφιακών αποδεικτικών στοιχείων, καθώς και στον εντοπισμό των πραγματικών φυσικών υπολογιστικών πόρων από εικονικές πηγές του επιπέδου υπηρεσιών. Τα αρχεία καταγραφής συμβάντων των hypervisors και η αντιγραφή εικονικών υπολογιστικών συστημάτων περιλαμβάνονται στα ψηφιακά αποδεικτικά στοιχεία αυτού του επίπεδο.

7.6.3. Επίπεδο υπηρεσιών

Ως επίπεδο υπηρεσιών θεωρείται το σημείο όπου ο πάροχος υπηρεσιών υπολογιστικού νέφους ορίζει τις διεπαφές για τους χρήστες – πελάτες του, ώστε να έχουν πρόσβαση στις υπηρεσίες του. Η πρόσβαση σε καθένα από τα τρία μοντέλα του υπολογιστικού νέφους είναι διαφορετική και ελέγχεται μέσω αυτών των διεπαφών. Είναι δυνατόν, αν και όχι απαραίτητο, εφαρμογές SaaS να έχουν χτιστεί μέσω στοιχείων του PaaS, τα οποία στοιχεία να είναι μέρος μιας υποδομής IaaS.

Το επίπεδο υπηρεσιών είναι το σημείο που γίνεται ο διαχωρισμός των καθηκόντων μεταξύ του παρόχου του υπολογιστικού νέφους και του πελάτη μέσω των διεπαφών. Όσα ψηφιακά αποδεικτικά στοιχεία είναι πάνω από τη διεπαφή μπορούν και επιβάλλεται να συλλεχθούν από τον πελάτη χωρίς τη βοήθεια του παρόχου. Αναλόγως, όσα ψηφιακά αποδεικτικά στοιχεία είναι κάτω από τη διεπαφή μπορούν και επιβάλλεται να συλλεχθούν από τον πάροχο υπηρεσιών υπολογιστικού νέφους. Σε αυτό το σημείο αξίζει να αναφερθεί ότι η ενσωμάτωση ειδικών διεπαφών για εγκληματολογικές έρευνες σε αυτές θα αύξανε ραγδαία τη δυνατότητα συλλογής ψηφιακών αποδεικτικών στοιχείων τόσο από τη μεριά του πελάτη όσο και από τη μεριά του παρόχου.

7.6.3.1. Επίπεδο λειτουργικού συστήματος

Το επίπεδο IaaS ονομάζεται επίσης και επίπεδο λειτουργικού συστήματος, καθώς αυτό το επίπεδο παρέχει διεπαφές για πρόσβαση στο λειτουργικό σύστημα και σε συσκευές και είναι αδιαφανές για τους χρήστες SaaS και PaaS. Το συγκεκριμένο επίπεδο επιτρέπει την εκτέλεση πολλών και διαφορετικών λειτουργικών συστημάτων σε ένα φυσικό μηχάνημα. Σε γενικές γραμμές, οι πελάτες έχουν τη δυνατότητα να επιλέξουν μέσα από μια ευρεία γκάμα από λειτουργικά συστήματα που τους προσφέρει ο πάροχος υπηρεσιών υπολογιστικού νέφους. Οι πελάτες IaaS έχουν την πλήρη και αποκλειστική ευθύνη για το λειτουργικό σύστημα που χρησιμοποιούν, ενώ ο πάροχος υπολογιστικού νέφους ελέγχει το υποκείμενο λειτουργικό σύστημα του υπολογιστικού συστήματος [175].

Τα ψηφιακά αποδεικτικά στοιχεία αυτού του επιπέδου είναι παρόμοια με αυτά των εικονικών λειτουργικών συστημάτων, στα οποία συμπεριλαμβάνονται τα αρχεία καταγραφής του εικονικού λειτουργικού συστήματος, τα αρχεία ρυθμίσεων, τα αρχεία καταγραφής συμβάντων των προγραμμάτων προστασίας από κακόβουλο λογισμικό και, τέλος, τα αρχεία καταγραφής από τα συστήματα ανίχνευσης εισβολών (IDSes).

7.6.3.2. Ενδιάμεσο επίπεδο

Το επίπεδο PaaS ονομάζεται και ενδιάμεσο, καθώς αυτό το επίπεδο παρέχει όλα εκείνα τα εργαλεία, για παράδειγμα βιβλιοθήκες, βάσεις δεδομένων, μεταφραστές, τα οποία είναι απαραίτητα για ένα προγραμματιστή, ώστε να δημιουργήσει μια εφαρμογή στο υπολογιστικό νέφος. Το συγκεκριμένο επίπεδο χρησιμοποιείται από πελάτες – προγραμματιστές, ενώ η εγκατάστασή του, η διαχείρισή του και η συντήρησή του γίνεται από πελάτες IaaS ή παρόχους PaaS και είναι κρυφό για πελάτες SaaS [175].

Τα ψηφιακά αποδεικτικά στοιχεία αυτού του επιπέδου είναι παρόμοια με αυτά που υπάρχουν σε ένα τυπικό προγραμματιστικό περιβάλλον. Στα ψηφιακά αποδεικτικά στοιχεία περιλαμβάνονται ο πηγαίος κώδικας των εφαρμογών, τα αρχεία καταγραφής της απόδοσης μιας εφαρμογής, τα αρχεία καταγραφής λαθών μια εφαρμογής και τα αρχεία καταγραφής πρόσβασης στο περιβάλλον.

7.6.3.3. Επίπεδο εφαρμογών

Το επίπεδο αυτό είναι το SaaS στο οποίο υπάρχουν εφαρμογές που χρησιμοποιούν οι τελικοί χρήστες. Η εγκατάσταση, η διαχείριση και η συντήρηση των εφαρμογών αυτών γίνεται από πελάτες PaaS, IaaS και SaaS.

Τα ψηφιακά αποδεικτικά στοιχεία αυτού του επιπέδου είναι παρόμοια με αυτά που λαμβάνει ο ερευνητής από τις διάφορες εφαρμογές που είναι εγκατεστημένες σε ένα υπολογιστικό μηχάνημα.

Στα ψηφιακά αποδεικτικά στοιχεία αυτού του επιπέδου περιλαμβάνονται τα αρχεία καταγραφής συμβάντων της εφαρμογής και τα αρχεία καταγραφής πρόσβασης των χρηστών στην εφαρμογή. Η μόνη διαφορά είναι ότι το λογισμικό βρίσκεται σε γεωγραφική απόσταση από τον χρήστη του και ο χρήστης έχει πρόσβαση σε αυτό μέσω ενός προγράμματος περιήγησης, οπότε εξίσου σημαντικό ρόλο παίζουν και τα ψηφιακά αποδεικτικά στοιχεία που θα συλλέξει ο ερευνητής από τον προσωπικό υπολογιστή του χρήστη.

7.6.4. Απόκτηση αποδεικτικών στοιχείων στο υπολογιστικό νέφος

Με βάση την παραπάνω ανάλυση, αρκετοί ερευνητές καταλήγουν στο συμπέρασμα ότι για την απόκτηση ψηφιακών αποδεικτικών στοιχείων στο υπολογιστικό νέφος θα πρέπει να καταφύγουμε σε μια υβριδική προσέγγιση, στην οποία θα περιλαμβάνονται διάφοροι επιμέρους τομείς των ψηφιακών εγκληματολογικών ερευνών, όπως για παράδειγμα στοιχεία από το δίκτυο, από το τερματικό του χρήστη, από τη μνήμη RAM κοκ. Μέσω των επιμέρους τομέων θα συλλέγονται όσο το δυνατόν περισσότερα ψηφιακά αποδεικτικά στοιχεία και κατόπιν θα είναι δυνατό να συλλεχθούν όσα αποδεικτικά στοιχεία γίνεται από το περιβάλλον του υπολογιστικού νέφους. Καλό θα ήταν να δημιουργηθεί μια λίστα από βήματα στα οποία να καθορίζεται επακριβώς ο τρόπος με τον οποίο θα εξασφαλίζεται η ετοιμότητα του υπολογιστικού νέφους σε θέματα ψηφιακών εγκληματολογικών ερευνών. Επιπρόσθετα, θα πρέπει να θεσπιστεί ο τρόπος και η σειρά συλλογής των ψηφιακών αποδεικτικών στοιχείων από το υπολογιστικό νέφος, με σκοπό αφενός την εγκυρότητα των δεδομένων και αφετέρου τις μηδαμινές πιθανότητες απώλειας αποδεικτικών στοιχείων.

Κ Ε Φ Α Λ Α Ι Ο Ο Γ Δ Ο Ο

Δομικά στοιχεία ερευνών

8.1. Εισαγωγή

Από τα προηγούμενα έγινε κατανοητό ότι η εργασία του ερευνητή σε ότι αφορά την εξαγωγή ψηφιακών αποδεικτικών στοιχείων στο υπολογιστικό νέφος δεν είναι εύκολη. Επιπλέον, σε αντίθεση με την παραδοσιακή εγκληματολογία, ο ερευνητής οφείλει να συμπεριλάβει ένα σύνολο παραγόντων για να μπορεί να εξάγει αφενός αξιόπιστα ψηφιακά αποδεικτικά στοιχεία και αφετέρου να μην υποπέσει σε τυχόν

λάθη. Στο κεφάλαιο αυτό, θα προσδιορίσουμε επακριβώς τις επιμέρους δυσκολίες, αναλύοντας τις τεχνικές που θα πρέπει να χρησιμοποιηθούν με στόχο την αποτελεσματική διεξαγωγή της έρευνας.

8.2. Δομικά στοιχεία των ψηφιακών εγκληματολογικών ερευνών στο υπολογιστικό νέφος

Μία από τις κυριότερες λειτουργίες που υπάρχει σε κάθε εφαρμογή και γενικότερα στις υποδομές των πληροφοριακών συστημάτων, είναι η δημιουργία αρχείων καταγραφής συμβάντων από εγγραφές που προκύπτουν σχετικά με διάφορα γεγονότα που συμβαίνουν στην εφαρμογή. Οι διακομιστές, τα λειτουργικά συστήματα, οι βάσεις δεδομένων και αρκετά από τα πρωτόκολλα που υπάρχουν σε ένα δίκτυο, όλα τους περιλαμβάνουν διαδικασίες για την αποτελεσματική καταγραφή όλων των γεγονότων, όπως για παράδειγμα τυχόν βλάβες ή δυσλειτουργίες που προέκυψαν, καθώς και δεδομένα για την είσοδο και την έξοδο των χρηστών. Όλη αυτή η πληροφορία αποθηκεύεται σε ένα ειδικό αρχείο, το αρχείο καταγραφής συμβάντων, όπως αναφέρθηκε και ανωτέρω. Αρχείο καταγραφής συμβάντων ονομάζεται το αρχείο που έχει καταχωρημένες όλες τις ενέργειες που συνέβησαν σε μια υποδομή πληροφορικής [194]. Με τον όρο υποδομή πληροφορικής ονομάζουμε μια πληθώρα από στοιχεία που ποικίλλουν από μια εφαρμογή μέχρι ένα λειτουργικό σύστημα και από μια γέφυρα δικτύου μέχρι ένα διακομιστή.

Τα αρχεία καταγραφής συμβάντων αρχικά δημιουργήθηκαν από τους προγραμματιστές εφαρμογών ή και ολόκληρων λειτουργικών συστημάτων, με σκοπό την αποτελεσματική αποσφαλμάτωση των λειτουργιών μιας εφαρμογής. Με την πάροδο του χρόνου, τα αρχεία καταγραφής συμβάντων γίνονταν όλο και πιο χρήσιμα. Σήμερα, τα αρχεία καταγραφής συμβάντων, εκτός από τον αρχικό λόγο ύπαρξης, τηρούνται για επιχειρησιακούς λόγους, καθώς και για λόγους συμμόρφωσης με τη νομοθεσία. Επιπρόσθετα, βοηθούν τους διαχειριστές των πληροφοριακών συστημάτων να ανακαλύψουν πιθανά προβλήματα στην υποδομή που διαχειρίζονται, αναφέρουν το λόγο ενός

απρόβλεπτου τερματισμού μιας εφαρμογής και καταδεικνύουν τυχόν παράνομες ενέργειες στην εφαρμογή.

Στην ψηφιακή εγκληματολογική έρευνα, τα αρχεία καταγραφής συμβάντων είναι μια από τις κυριότερες πηγές άντλησης ψηφιακών αποδεικτικών στοιχείων από μια ύποπτη συσκευή [195-198]. Στη συντριπτική πλειοψηφία των περιπτώσεων τα αρχεία καταγραφής συμβάντων είναι το σημείο έναρξης μιας έρευνας.

Σε μια τυπική ψηφιακή εγκληματολογική έρευνα έχουμε δύο ειδών στρατηγικές προσέγγισης του στόχου: την επονομαζόμενη από πάνω προς τα κάτω (top – down) και την από κάτω προς τα πάνω (bottom – up) [199]. Κατά τη διάρκεια της πρώτης προσέγγισης ο ερευνητής ξεκινά την εργασία του μετά την εμφάνιση του συμβάντος και ελέγχει τα αρχεία καταγραφής συμβάντων των διαφόρων υποδομών που τον ενδιαφέρουν, με σκοπό την ανακάλυψη πιθανών αποδεικτικών στοιχείων σχετικά με το συμβάν. Στη δεύτερη προσέγγιση αυτόματα εργαλεία εξετάζουν ανά τακτά χρονικά διαστήματα τα αρχεία καταγραφής συμβάντων, με σκοπό την εύρεση πιθανών κινδύνων ή παραβιάσεις των πολιτικών της εταιρείας.

Και στις δύο προαναφερθείσες περιπτώσεις, ο ερευνητής συλλέγει όλα τα γεγονότα που συνέβησαν μέσω των αρχείων καταγραφής συμβάντων και δημιουργεί μια χρονογραμμή, η οποία περιέχει όλες τις ύποπτες ενέργειες που ως σύνολο περιγράφουν τη ροή με την οποία διαδραματίστηκε το συμβάν. Κατόπιν τούτου, ο ερευνητής εφαρμόζει μία από τις μεθόδους εύρεσης ψηφιακών εγκληματολογικών στοιχείων, με σκοπό αφενός την ακριβή τεκμηρίωση της όλης διαδικασίας και αφετέρου την απόκτηση ισχυρών στοιχείων που θα είναι αδιάσειστα σε μια δικαστική αίθουσα.

Η αποτελεσματικότητα και η αξιοπιστία μιας ψηφιακής εγκληματολογικής έρευνας εξαρτάται σε μεγάλο βαθμό από την πληρότητα των αρχείων καταγραφής συμβάντων, καθώς και από τους μηχανισμούς που υπάρχουν, με σκοπό την προστασία της ακεραιότητας και της εμπιστευτικότητάς τους. Ωστόσο, ο σχεδιασμός και η εφαρμογή ενός αξιόπιστου συστήματος καταγραφής συμβάντων είναι ένα αρκετά

δύσκολο έργο και σε περιβάλλον υπολογιστικού νέφους φτάνει στο σημείο να είναι πρόκληση, καθώς σε αυτό υπάρχουν κάποια χαρακτηριστικά, όπως η δυναμικότητά του και η πολλαπλή μίσθωση που δημιουργούν επιπλέον θέματα. Ένας κακόβουλος χρήστης του υπολογιστικού νέφους, από τη στιγμή που θα διαπράξει την παράνομη πράξη του μπορεί πολύ απλά να διαγράψει το εικονικό μηχάνημα που χρησιμοποίησε και μαζί με αυτό όλα τα πιθανά αποδεικτικά στοιχεία που πιστοποιούν την ενοχή του [200]. Ακόμα και αν η πολιτική του παρόχου του υπολογιστικού νέφους είναι για λόγους χρέωσης να μην διαγράφει αμέσως τα διάφορα στοιχεία των πελατών του, τα διαγράφει μετά από ένα ορισμένο χρονικό διάστημα, όπως άλλωστε είναι υποχρεωμένος μέσω της νομοθεσίας. Έτσι, λόγω της ασταθούς φύσης των εικονικών πόρων που έχει στη διάθεσή του ο κακόβουλος χρήστης, τα αρχεία καταγραφής συμβάντων είναι διαθέσιμα στον ερευνητή για ορισμένο χρονικό διάστημα. Το προηγούμενο είναι ένα μικρό αλλά χαρακτηριστικό παράδειγμα για τις δυσκολίες με τις οποίες θα έρθει αντιμέτωπος ο ερευνητής σε περιβάλλον υπολογιστικού νέφους.

Επιπρόσθετα, η χρήση πολλών παρόχων υπολογιστικών νεφών μπορεί να προκαλέσει προβλήματα διαλειτουργικότητας μεταξύ αυτών, γεγονός το οποίο επηρεάζει άμεσα τα αρχεία καταγραφής συμβάντων. Για παράδειγμα, ένας πελάτης μπορεί να έχει εγγραφεί σε ένα μοντέλο IaaS από έναν πάροχο, το οποίο να συνδυάζεται με ένα μοντέλο PaaS από ένα δεύτερο πάροχο και να χρειάζεται λειτουργικά κομμάτια SaaS από ένα τρίτο. Επίσης, η ποικιλία των ελέγχων στα τρία μοντέλα του υπολογιστικού νέφους έχει αντίκτυπο στο σύστημα καταγραφής συμβάντων. Αυτό συμβαίνει γιατί καθένα από τα τρία μοντέλα εκχωρεί διαφορετικά δικαιώματα στην υποκείμενη υποδομή και συνεπώς και στα αρχεία καταγραφής συμβάντων που τηρεί. Για παράδειγμα, ένα χρήστης του μοντέλου SaaS μπορεί να έχει πρόσβαση μόνο στα αρχεία καταγραφής συμβάντων της εφαρμογής που χρησιμοποιεί και αυτό μόνο αν ο πάροχός του του το επιτρέπει μέσω μιας διεπαφής. Αντίθετα, ένας χρήστης IaaS έχει πρόσβαση μέχρι και στα αρχεία καταγραφής του λειτουργικού συστήματος που χρησιμοποιεί στο μοντέλο που έχει, χωρίς να χρειάζεται άδεια από τον πάροχό του για αυτό.

Οι περισσότεροι από τους παρόχους υπηρεσιών υπολογιστικού νέφους προσφέρουν ειδικές εφαρμογές αρχικά για τη συλλογή και κατόπιν για την εμφάνιση των περιεχομένων των αρχείων καταγραφής συμβάντων. Για παράδειγμα, η Amazon με το CloudFront [114] προσφέρει το SolarWinds LogAnalyzer [201]. Με τη χρήση του συγκεκριμένου εργαλείου ο χρήστης είναι σε θέση να δημιουργεί αναφορές, οι οποίες να περιέχουν πληροφορίες σχετικά με διάφορα στοιχεία, όπως για παράδειγμα τη δημοτικότητα ενός αντικειμένου, την κίνηση στο δίκτυο και τις διευθύνσεις IP που έχουν καταχωρηθεί. Ωστόσο, αυτές οι εφαρμογές δεν είναι σε θέση να καλύψουν μια εγκληματολογική έρευνα, αν και σε αυτές τις εφαρμογές ακολουθούνται οι γενικοί κανόνες συλλογής συμβάντων [202-204]. Στις παραγράφους που ακολουθούν, θα αναφέρουμε τις βασικές τεχνικές δυσκολίες που αντιμετωπίζει ο σχεδιαστής του συστήματος καταγραφής συμβάντων, καθώς και τις απαιτήσεις ασφάλειας που θα πρέπει να πληροί ένα τέτοιο σύστημα.

8.2.1. Τεχνικές προκλήσεις

Ο κύκλος ζωής ενός αρχείου καταγραφής συμβάντων διαιρείται σε δύο φάσεις. Η πρώτη είναι η φάση δημιουργίας μιας εγγραφής του αρχείου και η δεύτερη είναι η φάση της διαχείρισης μιας εγγραφής του αρχείου. Κατά τη διάρκεια της πρώτης φάσης, ο σχεδιαστής θα πρέπει να αποφασίσει σχετικά με τα ακριβή πεδία της εγγραφής, τα οποία σχετίζονται με το ποια είδη γεγονότων καθώς και τι είδους πληροφορίες σχετικές με το καθένα από αυτά τα γεγονότα θα πρέπει να αποθηκεύονται. Κατόπιν, όλες αυτές οι πληροφορίες θα πρέπει να συμπληρώνονται με σημαντικά μεταδεδομένα (metadata) για μια ψηφιακή εγκληματολογική έρευνα, όπως για παράδειγμα τον ακριβή χρόνο που συνέβη ένα γεγονός. Επιπλέον, ο σχεδιαστής θα πρέπει να επιλέξει την τοποθεσία αποθήκευσης των αρχείων καταγραφής συμβάντων μεταξύ της συγκεντρωμένης και της κατανεμημένης αποθήκευσής τους.

Στη δεύτερη φάση, επιτελείται η διαχείριση της εγγραφής. Σε αυτή την φάση αποφασίζεται το πόσο θα είναι η περίοδος διατήρησης των εγγραφών των αρχείων καταγραφής συμβάντων, καθώς και η πολιτική πρόσβασης στα αρχεία αυτά, πράγμα που σημαίνει το ποιος θα έχει το δικαίωμα να διαβάσει τις εγγραφές ενός αρχείου, ποια πεδία από τις εγγραφές και τέλος τι είδους δικαιώματα επεξεργασίας έχει.

Αναλυτικότερα, οι τεχνικές προκλήσεις που έχει να αντιμετωπίσει ο σχεδιαστής του συστήματος καταγραφής συμβάντων αναφέρονται στις επόμενες παραγράφους.

8.2.1.1. Περιεχόμενα εγγραφής ενός αρχείου καταγραφής συμβάντων

Δεν υπάρχει κάποια τυποποιημένη περιγραφή των πεδίων που θα πρέπει να υπάρχουν σε μια εγγραφή και συνήθως τα περιεχόμενα των αρχείων καταγραφής συμβάντων διαφέρουν και εξαρτώνται από τον προγραμματιστή της εκάστοτε εφαρμογής. Παρόλα αυτά, ο γενικός κανόνας που ισχύει είναι ότι καθεμία από τις εγγραφές θα πρέπει να περιέχει απαντήσεις στα «ποιος», «τι», «πού», «γιατί» και «πώς» συνέβη κάποιο γεγονός [195]. Λόγω της δυναμικότητας που χαρακτηρίζει το υπολογιστικό νέφος, το «πού» θα πρέπει να απαντηθεί με τη μεγαλύτερη δυνατή λεπτομέρεια, καθώς μια εφαρμογή ή και ένα ολόκληρο εικονικό μηχάνημα μπορεί να μεταφερθεί από ένα φυσικό υπολογιστή σε έναν άλλο κατά τη διάρκεια χρήσης του. Σε γενικές γραμμές, μια εγγραφή ενός αρχείου καταγραφής συμβάντων θα πρέπει να περιλαμβάνει όσο το δυνατόν περισσότερα αναγνωριστικά [140]. Αυτά τα χαρακτηριστικά επιβάλλεται να προσδιορίζουν μοναδικά το άτομο για το οποίο δημιουργήθηκε η συγκεκριμένη εγγραφή και την τοποθεσία που βρίσκεται. Το αποτέλεσμα θα πρέπει να είναι αδιαμφισβήτητο και αξιόπιστο. Για παράδειγμα, στην περίπτωση του CloudFront της Amazon, τα πεδία x-edge-location, c-ip, cs (Host), cs (Referrer), cs (User Agent) και x-cf-client-id είναι πηγές άντλησης πληροφοριών σχετικά με την τοποθεσία, τη διεργασία και το άτομο το οποίο διενήργησε κάποιο γεγονός. Δυστυχώς όμως, τα προαναφερόμενα πεδία δεν είναι επαρκή, ώστε να καλύψουν πλήρως τα αναγνωριστικά που θα πρέπει να έχει μια

εγγραφή ενός αρχείου καταγραφής συμβάντων σε μια ψηφιακή εγκληματολογική έρευνα.

8.2.1.2. Προέλευση εγγραφής ενός αρχείου καταγραφής συμβάντων

Όσον αφορά την προέλευση των εγγραφών ενός αρχείου καταγραφής συμβάντων υπάρχουν δύο είδη δεδομένων. Το πρώτο είδος είναι τα δεδομένα που προέρχονται από το λειτουργικό σύστημα και το δεύτερο είναι τα αντίστοιχα που προέρχονται από το δίκτυο [199]. Τα δεδομένα που προέρχονται από το λειτουργικό σύστημα χωρίζονται και αυτά με τη σειρά τους στα δεδομένα συστήματος και στα δεδομένα εφαρμογών [205]. Οι εγγραφές που προέρχονται από δεδομένα συστήματος δημιουργούνται από το ίδιο το λειτουργικό σύστημα και συνήθως περιέχουν πληροφορίες σχετικές με τους χρήστες που απέκτησαν πρόσβαση στο υπολογιστικό σύστημα, τις αλλαγές στο υλικό του και τις διεργασίες που εκτελούνται ανά μονάδα χρόνου. Από την άλλη πλευρά, οι εγγραφές που προκύπτουν από δεδομένα εφαρμογών δημιουργούνται από τις εφαρμογές που φιλοξενεί το λειτουργικό σύστημα. Τα περιεχόμενα ενός τέτοιου αρχείου εξαρτώνται αποκλειστικά από τον εκάστοτε προγραμματιστή της κάθε εφαρμογής. Τέλος, τα δεδομένα του δικτύου δημιουργούνται από δρομολογητές, πρωτόκολλα δικτύου και τείχη προστασίας. Συνήθως, αυτά περιέχουν πληροφορίες σχετικά με τη συμπεριφορά μιας συγκεκριμένης συσκευής του δικτύου ή και πληροφορίες για τη γενική λειτουργία του δικτύου.

Στο περιβάλλον του υπολογιστικού νέφους, σε περίπτωση που χρησιμοποιούμε το μοντέλο IaaS, έχουμε τα αρχεία καταγραφής συμβάντων του λειτουργικού συστήματος του χρήστη, τα οποία δημιουργούνται από το ίδιο το λειτουργικό σύστημα, όπως και στο παραδοσιακό μοντέλο. Επίσης διαθέτουμε τα αρχεία καταγραφής συμβάντων των εφαρμογών που φιλοξενεί το λειτουργικό σύστημα του χρήστη και τέλος τα αρχεία καταγραφής των δρομολογητών και όλων των άλλων συσκευών που χρησιμοποιεί ο χρήστης. Αξίζει να αναφερθεί ότι όλα τα προηγούμενα δεν είναι φυσικές συσκευές αλλά λειτουργούν εικονικά. Από την άλλη πλευρά υπάρχουν τα αρχεία καταγραφής

συμβάντων των παρόχων. Τα συγκεκριμένα αρχεία δημιουργούνται από το λειτουργικό σύστημα που φιλοξενεί τα εικονικά συστήματα, από τις φυσικές συσκευές του παρόχου και από το λογισμικό διαχείρισης της υποδομής του παρόχου.

8.2.1.3. Χρονοσφραγίδα

Χρονοσφραγίδα (timestamp) ονομάζονται όλες εκείνες οι πληροφορίες που χρειάζονται για να προσδιοριστεί ο χρόνος που συνέβη ένα γεγονός. Καθεμία από τις εγγραφές θα πρέπει να έχει ένα τέτοιο πεδίο, με σκοπό τον προσδιορισμό του ακριβούς χρόνου δημιουργίας της συγκεκριμένης εγγραφής [200, 206]. Δυστυχώς, η ακρίβεια στο χρόνο δεν επιτυγχάνεται εύκολα στις υποδομές της πληροφορικής εξαιτίας ποικίλων λόγων, εκ των οποίων μερικοί μπορεί να είναι ότι οι διακομιστές έχουν λανθασμένες ρυθμίσεις σχετικά με την ώρα ή ότι τα ρολόγια των μηχανημάτων έχουν αποσυγχρονιστεί από λίγα δευτερόλεπτα έως και πολλές ώρες. Στη συνέχεια της συγκεκριμένης ενότητας θα αναπτύξουμε τον κρίσιμο ρόλο που παίζει η ακρίβεια του χρόνου σε μια ψηφιακή εγκληματολογική έρευνα και θα αξιολογήσουμε τις τρέχουσες καταστάσεις ορθής διατήρησης της ώρας στο υπολογιστικό νέφος.

8.2.1.4. Κατανεμημένη και συγκεντρωμένη αποθήκευση των αρχείων καταγραφής συμβάντων

Όπως αναφέρθηκε και ανωτέρω, ένα σύστημα καταγραφής συμβάντων όσον αφορά τον τρόπο αποθήκευσης των αρχείων, μπορεί να είναι είτε κατανεμημένο είτε συγκεντρωμένο. Στο κατανεμημένο μοντέλο τα αρχεία καταγραφής συμβάντων διατηρούνται στη φυσική τοποθεσία που δημιουργήθηκαν. Στη δεύτερη προσέγγιση, όλα τα αρχεία καταγραφής συμβάντων συλλέγονται μέσω ειδικών μηχανισμών και αποθηκεύονται σε ένα κοινό μέσο αποθήκευσης. Στη βιβλιογραφία υπάρχουν αρκετά συστήματα καταγραφής συμβάντων που υλοποιούν το συγκεντρωμένο μοντέλο [202, 207-210].

8.2.1.5. Περίοδος διατήρησης των εγγραφών

Στις περισσότερες των περιπτώσεων, η περίοδος διατήρησης των εγγραφών καθορίζεται από γενικούς κανόνες [199]. Ωστόσο, σχετικά με αυτό το θέμα, στο υπολογιστικό νέφος έχει προκύψει ένα σημαντικό νομικό κενό [200]. Παρόλα αυτά, σε γενικές γραμμές τα αρχεία καταγραφής συμβάντων καταστρέφονται όταν θεωρηθεί ότι η χρήση τους έχει ολοκληρωθεί.

Σε πρακτικό επίπεδο, τα αρχεία καταγραφής συμβάντων είναι ή σειριακά ή κυκλικά [211]. Στα σειριακά, ή αλλιώς γραμμικά, αρχεία καταγραφής συμβάντων κάθε γεγονός καταγράφεται είτε στην αρχή είτε στο τέλος του αρχείου. Αυτού του είδους η καταγραφή παρέχει πληροφορίες από την πρώτη μέρα λειτουργίας της πληροφοριακής υποδομής. Δυστυχώς όμως, το εξαιρετικά μεγάλο μέγεθός τους σε συνδυασμό με το γεγονός ότι οι παλαιότερες εγγραφές είναι συνήθως άχρηστες έχει αρνητικό αντίκτυπο σε αυτά τα αρχεία. Από την άλλη πλευρά, τα κυκλικά αρχεία καταγραφής συμβάντων έχουν ένα προκαθορισμένο μέγιστο μέγεθος. Όταν το αρχείο φθάνει στο μέγιστο επιτρεπτό μέγεθός του, γράφει τις νέες εγγραφές πάνω από τις παλαιότερες. Αυτού του είδους η καταγραφή μάς παρέχει αρχεία καταγραφής συμβάντων σχετικά μικρού μεγέθους, με μειονέκτημα όμως, την απώλεια των παλαιών γεγονότων. Φυσικά, η διαγραφή των εγγραφών των αρχείων καταγραφής συμβάντων υπόκειται σε νομικές δικλείδες σχετικά με τον χρόνο διατήρησης των εγγραφών και στην περίπτωση του κυκλικού μοντέλου θα πρέπει να υπάρξει ιδιαίτερη μέριμνα από τον προγραμματιστή του συστήματος καταγραφής συμβάντων για την αποφυγή νομικών κυρώσεων.

8.2.1.6. Πολιτική πρόσβασης

Η παροχή πρόσβασης στα αρχεία καταγραφής συμβάντων είναι ένα εξαιρετικά λεπτό ζήτημα. Τα αρχεία καταγραφής συμβάντων μπορεί να περιέχουν εμπιστευτικές ή ιδιωτικές πληροφορίες. Συνήθως, η πολιτική πρόσβασης στα αρχεία καταγραφής συμβάντων ορίζεται από τη γενικότερη πολιτική της εταιρείας και από το νομοθετικό πλαίσιο της

χώρας στην οποία ανήκει η εταιρεία αυτή. Κατόπιν, ανάλογα με την πολιτική που έχει θεσπιστεί, τα αρχεία καταγραφής συμβάντων, είτε σαν εγγραφές ή στο σύνολο τους, θεωρούνται εμπιστευτική πληροφορία, επιτρέποντας έτσι πρόσβαση μόνο σε κατάλληλα εξουσιοδοτούμενο προσωπικό. Ανάλογα με το λειτουργικό σύστημα που χρησιμοποιείται έχουν δημιουργηθεί και διάφορα εργαλεία για την πρόσβαση και την ανάγνωση των εγγραφών των αρχείων καταγραφής συμβάντων. Για παράδειγμα, τα λειτουργικά συστήματα της Microsoft έχουν τη εφαρμογή Event Viewer. Εξυπακούεται ότι όλα αυτά τα εργαλεία θα πρέπει να δίνουν πρόσβαση μόνο για ανάγνωση στα περιεχόμενα των αρχείων καταγραφής συμβάντων από τους χρήστες τους.

8.2.2. Απαιτήσεις ασφάλειας

Ένα σύστημα καταγραφής συμβάντων θα πρέπει να ικανοποιεί τουλάχιστον τρεις απαιτήσεις ασφάλειας. Αρχικά, επιβάλλεται να διασφαλίζεται η αυθεντικότητα των εγγραφών, γεγονός που σημαίνει ότι η πηγή των εγγραφών θα πρέπει να είναι έμπιστη και η εγγραφή θα πρέπει να αποθηκεύεται αναλλοίωτη, συμπεριλαμβανομένων και των μεταδεδομένων της, όπως για παράδειγμα οι χρονοσφραγίδες. Επιπλέον, θα πρέπει να προστατεύεται η ακεραιότητα τόσο των εγγραφών όσο και των αρχείων καταγραφής των συμβάντων και τέλος, η πρόσβαση σε αυτά απαιτείται να γίνεται με αυστηρά μέτρα προστασίας και σύμφωνα με την ισχύουσα πολιτική ασφάλειας της εταιρείας. Αναλυτικότερα, οι βασικές απαιτήσεις ασφάλειας που θα πρέπει να πληροί ένα σύστημα καταγραφής συμβάντων αναφέρονται στις επόμενες παραγράφους.

8.2.2.1. Αυθεντικότητα των εγγραφών

Μια εγγραφή για να έχει νομική ισχύ σε μια δικαστική αίθουσα θα πρέπει να είναι αυθεντική [194]. Αυτό σημαίνει ότι αφενός η πηγή της εγγραφής είναι έμπιστη και νόμιμη και αφετέρου ότι οι πληροφορίες που περιέχει η εγγραφή δεν τροποποιήθηκαν από την πηγή στο αρχείο που

αποθηκεύτηκε. Με σκοπό τη διαφύλαξη της αυθεντικότητας της πηγής θα πρέπει να υπάρχει ένας αδιαμφισβήτητος τρόπος με τον οποίο να συνδέεται η εγγραφή με τον δημιουργό της. Έτσι, αποφεύγονται οι ψεύτικες εγγραφές, τις οποίες μπορεί να κάνει κάποιος κακόβουλος χρήστης έχοντας ως πρόθεση την παραπλάνηση του ερευνητή. Τέλος, θα πρέπει να διασφαλίζεται η ακεραιότητα των περιεχομένων της εγγραφής, ώστε να αποφεύγονται τυχόν εσκεμμένες τροποποιήσεις της. Δυστυχώς, σε αρκετές περιπτώσεις, οι πηγές των εγγραφών δεν είναι ασφαλισμένες κατάλληλα και σε συνδυασμό με επισφαλείς τρόπους μεταφοράς των εγγραφών, το όλο σύστημα είναι επισφαλές και επιτρέπει τη μεταβολή ή ακόμα και τη διαγραφή είτε μεμονωμένων εγγραφών ή και ολόκληρων των αρχείων καταγραφής συμβάντων [212].

8.2.2.2. Ακεραιότητα των εγγραφών

Η προστασία της ακεραιότητας των εγγραφών θεωρείται υψίστης σημασίας και έχει μελετηθεί εκτενώς από τη βιβλιογραφία [195, 196, 199, 211, 213]. Οποιαδήποτε ένδειξη καταδεικνύει ότι το αρχείο έχει αλλοιωθεί ή τροποποιηθεί μπορεί να καταστήσει το περιεχόμενό του αναξιόπιστο και εντελώς άχρηστο για τον ερευνητή. Την ίδια μοίρα θα έχει και οποιαδήποτε έρευνα που βασίζεται σε ένα παραβιασμένο αρχείο καταγραφής συμβάντων. Δυστυχώς, παρά την εξέχουσα σημασία της προστασίας της ακεραιότητας των αρχείων καταγραφής συμβάντων, στις περισσότερες των περιπτώσεων αυτά δεν είναι επαρκώς προστατευμένα και δεν υπάρχει καμιά εγγύηση για την αξιοπιστία τους.

8.2.2.3. Ιδιωτικότητα των εγγραφών

Το σύστημα καταγραφής συμβάντων θα πρέπει να ακολουθεί την καθορισμένη πολιτική πρόσβασης από την εταιρεία. Η συγκεκριμένη απαίτηση δεν σχετίζεται άμεσα με τον ερευνητή, καθώς η παραβίαση της εμπιστευτικότητας ενός αρχείου καταγραφής συμβάντων δεν επιφέρει κάποιο πρόβλημα σε μια ψηφιακή εγκληματολογική έρευνα. Παρόλα

αυτά, η καταγραφή των ατόμων που είχαν πρόσβαση σε ένα αρχείο καταγραφής συμβάντων μπορεί να αποδειχτεί πολύτιμη πληροφορία.

8.3. Προβλήματα συγχρονισμού του ρολογιού στο περιβάλλον του νέφους

Ο συγχρονισμός του ρολογιού των συστημάτων θεωρείται ένα δύσκολο πρόβλημα για τις υποδομές πληροφορικής και εξελίσσεται σε πραγματικό εφιάλτη για τα εικονικά περιβάλλοντα. Υπάρχουν δύο διαφορετικές οπτικές γωνίες για την ανάλυση του προβλήματος σε περιβάλλον υπολογιστικού νέφους. Η πρώτη αφορά τον πάροχο των υπηρεσιών και η δεύτερη είναι του πελάτη των υπηρεσιών. Κατά την πρώτη περίπτωση, θα ερευνήσουμε το πρόβλημα των συγχρονισμένων χρονοσφραγίδων στα αρχεία καταγραφής συμβάντων του παρόχου και κατά τη δεύτερη περίπτωση το πρόβλημα των συγχρονισμένων χρονοσφραγίδων του πελάτη. Οι δύο αυτές περιπτώσεις έχουν σημαντικές διαφορές, αλλά ο αντίκτυπος που προκαλούν στον συγχρονισμό των ρολογιών είναι αθροιστικός.

8.3.1. Συγχρονισμός ρολογιού του παρόχου

Ο πάροχος υπηρεσιών υπολογιστικού νέφους έχει δύο στόχους. Επιθυμεί όλοι του διακομιστές να είναι συγχρονισμένοι και αυτό σημαίνει ότι όλα τα φυσικά μηχανήματα που διαθέτει να έχουν την ίδια ακριβώς ώρα και όλα τα εικονικά μηχανήματα που διαθέτει να έχουν ακριβώς την ίδια ώρα μεταξύ τους και με τα φυσικά μηχανήματα. Η διαδικασία συγχρονισμού του ρολογιού αντιμετωπίζει τα κλασικά προβλήματα ενός κατανεμημένου συστήματος. Η κύρια πρόκληση σχετίζεται με τη γεωγραφική απόσταση μεταξύ των φυσικών μηχανημάτων. Επειδή είναι πολύ πιθανό οι διακομιστές του παρόχου να βρίσκονται ακόμα και σε διαφορετικές ηπείρους, η καθυστέρηση του δικτύου να επηρεάσει ακόμα και ορισμένες από τις πιο σύγχρονες τεχνολογίες συγχρονισμού. Σε επόμενες παραγράφους θα αναφερθούμε

εκτενώς σε αυτό το πρόβλημα καθώς και στις τεχνικές που χρησιμοποιούνται σήμερα.

8.3.2. Συγχρονισμός των εικονικών μηχανημάτων

Σε ό,τι αφορά τον συγχρονισμό των εικονικών μηχανημάτων θα επικεντρωθούμε στο μοντέλο IaaS, αφενός γιατί δίνει περισσότερη ευχέρεια επιλογών στους χρήστες και αφετέρου γιατί μπορούμε να γνωρίζουμε καλύτερα τη συγκεκριμένη υποδομή.

Το λειτουργικό σύστημα που βρίσκεται πάνω από την υποδομή του παρόχου του υπολογιστικού νέφους αντιμετωπίζει τις ίδιες ακριβώς προκλήσεις με ένα τυπικό λειτουργικό σύστημα που λειτουργεί εγγενώς σε ένα φυσικό υπολογιστικό μηχάνημα. Αυτό σημαίνει ότι θα πρέπει να αρχικοποιήσει το ρολόι του στη σωστή ώρα και κατόπιν να το διατηρεί συνεχώς ενημερωμένο. Η διατήρηση του συγχρονισμού του ρολογιού έχει μελετηθεί εκτενώς για φυσικά υπολογιστικά συστήματα και οι τρέχουσες τεχνικές έχουν αποδειχτεί αρκετά ακριβείς. Ωστόσο, σε ένα εικονικό περιβάλλον, υπάρχει μια πληθώρα από λόγους, οι οποίοι καθιστούν δύσκολη τη διαδικασία συνεχούς ενημέρωσης του χρόνου. Οι περισσότερες από τις δυσκολίες πηγάζουν από την ίδια τη φύση του υπολογιστικού νέφους. Στις επόμενες παραγράφους θα αναφερθούμε στις τεχνικές που μπορούν να χρησιμοποιηθούν σε ένα εικονικό μηχάνημα και θα τις αξιολογήσουμε από τη σκοπιά του ερευνητή ψηφιακών εγκληματολογικών ερευνών. Στη συνέχεια θα αναφερθούμε στα βασικά χαρακτηριστικά του υπολογιστικού νέφους που επηρεάζουν τη διαδικασία συγχρονισμού του ρολογιού και θα πρέπει να ληφθούν υπόψη τόσο από τον πάροχο του υπολογιστικού νέφους για τη διατήρηση της σωστής ώρας, όσο και από τον ερευνητή για την εξαγωγή σωστών συμπερασμάτων στην έρευνά του.

Παραδοσιακά, τα λειτουργικά συστήματα μετρούν τον χρόνο με δύο διαφορετικούς τρόπους. Ο πρώτος γίνεται με καταμέτρηση του χρόνου και ο δεύτερος χωρίς καταμέτρηση του χρόνου. Κυρίαρχος τρόπος είναι ο πρώτος κατά τον οποίο το λειτουργικό σύστημα χρησιμοποιεί το ρολόι του υλικού μόνο για να αρχικοποιήσει το ρολόι

του λειτουργικού συστήματος κατά τη διάρκεια εκκίνησής του και κατόπιν διατηρεί τον χρόνο συγχρονισμένο με βάση ειδικές ρουτίνες πάνω στην καταμέτρηση των διακοπών του συστήματος. Επίσης, το λειτουργικό σύστημα υποθέτει την ύπαρξη μιας συσκευής, η οποία στέλνει, ανά τακτά χρονικά διαστήματα, σήματα διακοπών. Μετρώντας αυτές τις διακοπές, το λειτουργικό σύστημα είναι σε θέση να προσδιορίσει τον χρόνο που έχει παρέλθει.

Συνήθως το λειτουργικό σύστημα δεν καταλαβαίνει ότι τρέχει εικονικά πάνω σε κάποιον διακομιστή και ότι διαμοιράζεται τους πόρους και το υλικό με άλλα λειτουργικά συστήματα. Την εργασία απόκρυψης την επιτελεί ο hypervisor, ο οποίος είναι επιφορτισμένος να κρύβει τα επιμέρους λειτουργικά συστήματα μεταξύ τους και να τους δημιουργεί τη ψευδαίσθηση ότι έχουν την αποκλειστική χρήση του υλικού και των πόρων. Παρόλα αυτά, σε πρακτικό επίπεδο, η πολλαπλή μίσθωση ενός μηχανήματος επηρεάζει την επίδοση των ρουτινών που χρησιμοποιεί το λειτουργικό σύστημα του πελάτη, για να καταμετρά τον χρόνο και αυτό οδηγεί σε απώλεια δευτερολέπτων. Για παράδειγμα, τη στιγμή που δημιουργηθεί μια διακοπή από το λειτουργικό σύστημα του πελάτη, αυτή μπορεί να μην εκτελεστεί λόγω της χρήσης της εικονικοποίησης από τον hypervisor. Έτσι, το λειτουργικό σύστημα μένει πίσω στον χρόνο. Επίσης, το πρόβλημα αυξάνεται αθροιστικά σε περίπτωση πολλών λειτουργικών συστημάτων στον ίδιο hypervisor.

Συνήθως, τα εικονικά μηχανήματα των πελατών μπορεί να ανασταλεί η λειτουργία τους και αυτά να αποθηκευτούν. Όταν ένα λειτουργικό σύστημα που κάθεται πάνω σε ένα τέτοιο εικονικό μηχάνημα επανέλθει από την αναστολή λειτουργίας του, συνεχίζει τη λειτουργία του σαν να μην είχε σταματήσει ποτέ. Το λειτουργικό σύστημα δεν είναι σε θέση να κατανοήσει ότι κάτι συνέβη, δηλαδή ότι μεσολάβησε κάποιο χρονικό διάστημα, οπότε το ρολόι του αφενός παραμένει στην χρονική στιγμή που ξεκίνησε η αναστολή της λειτουργίας του και αφετέρου συνεχίζει τη μέτρηση του χρόνου με τον τρόπο που αναφέρθηκε ανωτέρω.

Ένα άλλο πρόβλημα που προκύπτει στο υπολογιστικό νέφος είναι η διαφορετική ώρα που ενδεχομένως έχει η εικονική μηχανή, την οποία

λειτουργεί ο χρήστης και αυτή που έχει ο hypervisor, λόγω της διαφοράς των ζωνών ωρών μεταξύ των κρατών. Οπότε, όταν μια εικονική μηχανή χρησιμοποιήσει, μέσω μιας συνάρτησης, το ρολόι του hypervisor για συγχρονισμό, δεν θα λάβει υπόψη της τη διαφορετική πιθανόν ζώνη ώρας του hypervisor με τη δική της και θα οδηγήσει σε λανθασμένα δεδομένα σχετικά με τον χρόνο. Το συγκεκριμένο πρόβλημα διογκώνεται, όταν ένας hypervisor μεταφέρεται από μια τοποθεσία σε μια άλλη με διαφορετική ζώνη ώρας.

Το λειτουργικό σύστημα του χρήστη μπορεί να εκτελέσει όλες εκείνες τις λειτουργίες που συνήθως επιτελούσε και όταν ήταν εγκατεστημένο σε ένα κανονικό υπολογιστικό μηχάνημα, για να διατηρεί την ώρα σωστά. Η πιο αποδοτική τεχνική είναι η χρήση ενός δικτυακού πρωτοκόλλου για συγχρονισμό ρολογιών μεταξύ των NTP (Network Time Protocol) [212] και W32TIME [215]. Ωστόσο, αυτό μπορεί να αποδειχτεί ανεπαρκές στην περίπτωση του υπολογιστικού νέφους. Για παράδειγμα, συνήθως το λειτουργικό σύστημα του πελάτη χρησιμοποιεί μια πηγή για αρχικοποίηση του ρολογιού του που στις περισσότερες των περιπτώσεων είναι διαφορετική από την πηγή που χρησιμοποιεί ο πάροχος. Οπότε, στην περίπτωση που ο hypervisor προσπαθήσει να επιβάλει τη δική του ώρα, αυτό ενδέχεται να μπερδέψει το λειτουργικό του πελάτη. Από την άλλη πλευρά, όταν ξεκινά ένα εικονικό μηχάνημα, υπάρχει η δυνατότητα να χρησιμοποιήσει για αρχικοποίηση και συγχρονισμό το ρολόι του hypervisor. Αυτό σημαίνει όμως ότι ο πελάτης εξαρτάται πλήρως από τον πάροχό του σχετικά με το αν έχει συγχρονισμένα τα ρολόγια των διακομιστών του με σωστά πρωτόκολλα. Συνεπώς, στην περίπτωση που ο πάροχος έχει λανθασμένη ώρα, το εικονικό μηχάνημα του χρήστη θα ξεκινήσει τη λειτουργία του με λανθασμένο χρόνο.

8.4. Ο συγχρονισμός του ρολογιού στην ψηφιακή εγκληματολογική έρευνα

Όλες οι ψηφιακές εγκληματολογικές έρευνες θα πρέπει να διεξάγονται σύμφωνα με τις διαδικαστικές απαιτήσεις της νομοθεσίας.

Τα ψηφιακά αποδεικτικά στοιχεία είναι αναγκαίο να είναι σχετικά με το αντικείμενο της έρευνας, αυθεντικά, αξιόπιστα και να αποδεικνύεται τόσο η ακεραιότητα αυτών όσο και η ακεραιότητα της διαδικασίας της έρευνας [216]. Τόσο η δίωξη όσο και η δικαστική απόφαση θα πρέπει να βασίζονται σε στοιχεία που αποδεικνύουν ότι ένα συγκεκριμένο άτομο σε ένα συγκεκριμένο τόπο και χρόνο διέπραξε μια παράνομη πράξη [217].

Με σκοπό την εδραίωση της εγκυρότητας μιας πηγής αποδεικτικών στοιχείων όταν προκύπτουν νομικές διαφορές στο δικαστήριο, επιβάλλεται η αναδημιουργία του συμβάντος που ερευνάται καθώς και το πού και το πότε έγινε και το συμβάν αλλά και η διαδικασία της έρευνας. Η συλλογή και η διατήρηση των ψηφιακών αποδεικτικών στοιχείων στο υπολογιστικό νέφος παρουσιάζει επιπρόσθετες προκλήσεις, τόσο σε τεχνικό όσο και σε νομικό επίπεδο, όχι μόνο με σύγκριση με την παραδοσιακή πληροφορική αλλά και σε σχέση με την ψηφιακή εγκληματολογική έρευνα.

Οι συγκεκριμένες προκλήσεις γεννιούνται από τα ειδικά χαρακτηριστικά του υπολογιστικού νέφους και κυρίως από την εφήμερη φύση του και από το γεγονός ότι τα δεδομένα είναι αποθηκευμένα «κάπου», το οποίο «κάπου» ενδεχομένως να σημαίνει μια άλλη χώρα ή πολλές άλλες χώρες [218]. Είναι προφανές ότι μεταδεδομένα, όπως η χρονική στιγμή δημιουργίας, τροποποίησης και πρόσβασης σε ένα αρχείο, παρέχουν μια πολύτιμη πηγή αποδεικτικών στοιχείων για τον ερευνητή. Ωστόσο, λόγω της φύσης του υπολογιστικού νέφους είναι δύσκολο να προσδιοριστεί η ακριβής τοποθεσία αποθήκευσης των δεδομένων σε κάποια συγκεκριμένη χρονική στιγμή [99]. Μια περαιτέρω αβεβαιότητα αφορά τη φύση του χρόνου σε περιβάλλοντα υπολογιστικού νέφους, καθώς όπως αναφέρεται και ο Grispos στο [219] «ο ερευνητής δεν είναι σε θέση να προσδιορίσει αν τα δεδομένα είχαν υποστεί κάποιου είδους επεξεργασία σε μια δεδομένη χρονική στιγμή στο υπολογιστικό νέφος».

Σε περιβάλλοντα υπολογιστικού νέφους η χωρική διάσταση είναι απόλυτα αλληλένδετη με τη χρονική διάσταση. Η δυσκολία πρόσβασης στα δεδομένα με σκοπό την έρευνά τους για την αναδημιουργία ενός

συμβάντος σε συνδυασμό με τη διαφορετική ώρα που θα έχουν μεταξύ τους οι διάφορες συσκευές, εικονικές ή φυσικές, οι οποίες εμπλέκονται στο συμβάν, δημιουργούν επιπρόσθετα εμπόδια για την ομαλή διεξαγωγή της έρευνας. Μεταξύ των άλλων, ο ερευνητής θα πρέπει να διαπιστώσει αν όλες αυτές οι συσκευές έχουν σωστή ώρα ή αν είναι συγχρονισμένες χρονικά, ώστε να μπορεί να χρησιμοποιήσει τα δεδομένα που θα εξάγει από αυτές σε σωστή χρονική βάση.

Ο ορισμός της ώρας και ο συγχρονισμός του χρόνου των εμπλεκόμενων συσκευών έχει αναγνωριστεί ότι είναι μια σημαντική πρόκληση για την αποκάλυψη και τη διατήρηση των ψηφιακών αποδεικτικών στοιχείων [220]. Η σωστή και αποδεκτή αποθήκευση των ψηφιακών αποδεικτικών στοιχείων απαιτεί έγκυρο χρόνο στις χρονοσφραγίδες, για παράδειγμα στα μεταδεδομένα ή στα αρχεία καταγραφής συμβάντων των συσκευών ενός συστήματος [219].

Ο ορισμός της ακριβούς ώρας που συνέβη το γεγονός που ερευνάται, καθώς και των συνεπακόλουθων γεγονότων με αυτό, είναι πρωταρχικής σημασίας για την ακεραιότητα της διαδικασίας της έρευνας. Στη βιβλιογραφία υπάρχουν αρκετά παραδείγματα στα οποία ο διαφορετικός χρόνος μεταξύ των διαφόρων συσκευών είχε ως αποτέλεσμα τη διεξαγωγή λανθασμένων συμπερασμάτων [221]. Τέλος, ο παράγοντας του σωστού χρόνου είναι καθοριστικής σημασίας ακόμα και για τον χαρακτηρισμό μας πράξης ως αξιόποινης ή όχι.

Ο συγχρονισμός του χρόνου στα αρχεία καταγραφής συμβάντων, ή αλλιώς χρονοσφραγίδα, είναι πρωταρχικής σημασίας ως πηγή αποδεικτικών στοιχείων κατά τη διεξαγωγή μιας έρευνας. Αυτή είναι μια απαίτηση, η οποία δεν είναι εύκολο να επιτευχθεί, ιδίως στο περιβάλλον του υπολογιστικού νέφους, όπου ο διακομιστής και ο πελάτης στις περισσότερες, αν όχι σε όλες, τις περιπτώσεις βρίσκονται σε διαφορετικές, γεωγραφικά, ζώνες ώρας. Σε περιβάλλοντα υπολογιστικού νέφους είναι δυνατόν όχι μόνο ο διακομιστής να βρίσκεται κατανεμημένος σε αρκετές γεωγραφικές περιοχές, οι οποίες βρίσκονται σε διαφορετικές γεωγραφικές ζώνες, αλλά και οι εικονικές υπηρεσίες που υπάρχουν σε αυτόν να είναι προσανατολισμένες στο να έχουν την ώρα που έχει ο πελάτης και όχι ο ίδιος. Μια ψηφιακή εγκληματολογική

έρευνα, η οποία δεν θα λάβει υπόψη το προηγούμενο θέμα με τον χρόνο, θεωρείται δεδομένο ότι δεν θα έχει σωστά αποτελέσματα και, εκτός αυτού, δεν θα μπορεί να τεκμηριώσει την ακεραιότητα, την αξιοπιστία και την αποδοχή των αποδεικτικών στοιχείων σε μια δικαστική αίθουσα.

Το υπολογιστικό νέφος θέτει μια σειρά από σημαντικές επιπλοκές στις ψηφιακές εγκληματολογικές έρευνες. Η ύπαρξη διασυνοριακών υπολογιστικών νεφών σε συνδυασμό με τις άγνωστες τοποθεσίες που αποθηκεύονται τα δεδομένα, εγείρουν σοβαρά ζητήματα σε νομικό επίπεδο, τα οποία αφορούν κυρίως τη νομική δικαιοδοσία [222]. Ενώ το υπολογιστικό νέφος εξ ορισμού είναι «ασύνορο», τόσο μια έρευνα όσο και η νομοθεσία έχουν ισχύ αυστηρά σε ένα συγκεκριμένο και καθοριζόμενο χώρο, συνήθως μέσω των συνόρων των χωρών. Η έρευνα, η συλλογή των ψηφιακών αποδεικτικών στοιχείων καθώς και η νομική διαδικασία υπόκεινται στην αντίστοιχη νομοθεσία και διαφέρουν από χώρα σε χώρα. Διαφορές στη νομοθεσία μεταξύ των χωρών τόσο στην εφαρμογή όσο και στην ισχύ ενός νόμου μπορούν επίσης να εμποδίσουν την επιβολή του νόμου, καθώς οι νομικές αρχές εξαρτώνται από τους παρόχους υπηρεσιών, για να αποκτήσουν πρόσβαση στα σχετικά με το συμβάν δεδομένα.

Παράλληλα, ακόμα και αν διάφορες χώρες ή οργανισμοί έχουν θεσπίσει κοινούς νόμους και διαδικασίες σχετικά με το ηλεκτρονικό έγκλημα, δεν έχει γίνει το ίδιο και για το περιβάλλον του υπολογιστικού νέφους, οπότε οι περισσότερες από αυτές τις διαδικασίες δεν εφαρμόζονται σε αυτό [223]. Ο εγγενώς παγκόσμιος χαρακτήρας τόσο της αποθήκευσης όσο και της επεξεργασίας των δεδομένων που παρέχει το υπολογιστικό νέφος, σε συνδυασμό με τις νομικές πολυπλοκότητες μεταξύ των χωρών, απαιτούν αυξημένο επίπεδο συνεργασίας μεταξύ των χωρών και μεγαλύτερη εναρμόνισή τους με το διεθνές δίκαιο. Ως πηγή νομοθετικών εντολών μπορεί να θεωρηθεί η Σύμβαση του Συμβουλίου της Ευρώπης σχετικά με το κυβερνοέγκλημα (Convention on Cybercrime) της Βουδαπέστης, η οποία έχει υπογραφεί από περισσότερες από πενήντα χώρες, συμπεριλαμβανομένων και χωρών εκτός της Ευρώπης, όπως για παράδειγμα τις Η.Π.Α., και έχει επικυρωθεί από την πλειοψηφία τους. Το νομικό κείμενο της Συνθήκης έχει ένα

μεγάλο και ευρύ πεδίο εφαρμογών παρέχοντας παράλληλα διαδικαστικές διεργασίες, όπως για παράδειγμα την έρευνα και την κατάσχεση δεδομένων που βρίσκονται σε μια ψηφιακή συσκευή, την υποκλοπή δεδομένων από ύποπτες επικοινωνίες και την διασυνοριακή πρόσβαση στα αποθηκευμένα δεδομένα, είτε με τη συγκατάθεση της χώρας που ανήκουν, ή χωρίς, αν είναι δημόσια, ή τέλος, την αμοιβαία συνδρομή για συλλογή δεδομένων κίνησης σε ένα δίκτυο σε πραγματικό χρόνο. Οι διατάξεις αυτές διευκολύνουν τη συνεργασία για τη διερεύνηση και τη δίωξη του εγκλήματος σε καθεστώς πολλών χωρών και νομοθεσιών [206]. Παρά το γεγονός ότι τόσο οι ορισμοί όσο και οι διατάξεις της επονομαζόμενης συνθήκης της Βουδαπέστης αντικατοπτρίζουν την κατάσταση της τεχνολογίας πριν από δεκαπέντε χρόνια, μπορεί να θεωρηθούν ως ενεργές και εφαρμόσιμες στο περιβάλλον του υπολογιστικού νέφους.

8.4.1. Παράδειγμα σχετικά με την ανακρίβεια του χρόνου στο υπολογιστικό νέφος

Με σκοπό να καταστεί σαφής η ακρίβεια του χρόνου σε μια εγκληματολογική έρευνα στο υπολογιστικό νέφος, θα αναφερθούμε σε ένα περιστατικό που συνέβη σε μια εγκληματολογική έρευνα που διεξήχθη σε ένα τυπικό υπολογιστικό μηχάνημα [224]. Το συγκεκριμένο περιστατικό, με πολύ λίγες τροποποιήσεις, μπορεί να μεταφερθεί και σε περιβάλλον υπολογιστικού νέφους.

Έναυσμα για την έρευνα ήταν ένα μήνυμα ηλεκτρονικού ταχυδρομείου ενός ατόμου που ήταν ύποπτος για διακίνηση υλικού παιδικής πορνογραφίας. Ως συνήθως, αφού εκδόθηκε ένταλμα διεξαγωγής έρευνας, οι αστυνομικές αρχές συνέλαβαν τον ύποπτο και όλος ο ψηφιακός εξοπλισμός του κατασχέθηκε. Μια σχετικά απλή ψηφιακή εγκληματολογική έρευνα προκειμένου να εντοπίσει τα ίχνη του σχετικού μηνύματος με το υλικό παιδικής πορνογραφίας θα διεξαγόταν στον υπολογιστή του υπόπτου. Σε περιβάλλον υπολογιστικού νέφους η κατάσχεση του εικονικού μηχανήματος ενός υπόπτου θα μπορούσε να γίνει με την αντιγραφή αυτού σε ένα δεύτερο διακομιστή.

Κατά τη διεξαγωγή της ανάκρισης, ο ύποπτος δεν κατάφερε να δώσει πειστικές απαντήσεις σχετικά με το πώς βρέθηκαν στον υπολογιστή του οι παράνομες εικόνες. Το μόνο που ισχυρίστηκε ήταν ότι δεν ήταν ένοχος. Κατόπιν τούτου, ορίστηκε κανονική δικάσιμος για το αδίκημα.

Εν τω μεταξύ, οι αστυνομικοί περίμεναν από τον ερευνητή, ο οποίος διεξήγαγε την ψηφιακή εγκληματολογική έρευνα, να τους δώσει τα αποτελέσματα σχετικά με τα στοιχεία που ανακάλυψε στον υπολογιστή του υπόπτου. Όταν ο ερευνητής τους προσκόμισε την αναφορά σχετικά με την έρευνά του, διαπίστωσαν ότι σε αυτή γινόταν λόγος για σοβαρές καταχρήσεις από τους αστυνομικούς επί των αποδεικτικών στοιχείων [225]. Η αναφορά ξεκινούσε λέγοντας ότι ο υπολογιστής του υπόπτου μπήκε στο διαδίκτυο μετά την κατάσχεσή του από τους αστυνομικούς. Πιο συγκεκριμένα, ανέφερε ότι έξι ώρες μετά την κατάσχεση του υπολογιστικού συστήματος εντοπίστηκαν γύρω στις επτακόσιες πενήντα αιτήσεις στο διαδίκτυο. Μεταξύ των αιτήσεων αυτών ήταν σελίδες του Hotmail, ειδησεογραφικές και, επίσης, πορνογραφικές ιστοσελίδες. Επιπλέον, μετά από την κατάσχεση είχε γίνει χρήση του οδηγού δισκετών για αντιγραφή αρχείων. Η αναφορά έκλεινε αναγράφοντας ότι ο υπολογιστής του υπόπτου δεν θεωρείται έγκυρη πηγή αποδεικτικών στοιχείων, καθώς είχαν τροποποιηθεί τα περιεχόμενά του μετά την κατάσχεσή του, καταδεικνύοντας ότι, για άγνωστο λόγο, κάποιοι από τους αστυνομικούς έβαλαν ψευδώς κάποια δεδομένα στον υπολογιστή, για να ενοχοποιήσουν τον ύποπτο και το δικαστήριο δεν θα έπρεπε να λάβει υπόψη του τα όσα ψηφιακά αποδεικτικά στοιχεία υπήρχαν, γιατί ενδεχομένως να έβγαζε εντελώς λανθασμένα συμπεράσματα.

Εξαιτίας της ιδιαίτερης σοβαρότητας των αποτελεσμάτων της έρευνας, ξεκίνησε μια δεύτερη έρευνα, εσωτερικής φύσης, για να αποκαλυφθεί ο υπαίτιος αστυνομικός που δημιούργησε όλο αυτό το ζήτημα. Αξίζει να σημειωθεί ότι όλοι οι αστυνομικοί που συμμετείχαν στην κατάσχεση των μηχανημάτων δήλωναν ότι ακολουθήθηκε πιστά η διαδικασία και ότι κανείς τους δεν είχε πρόσβαση στο υπολογιστικό σύστημα και στα δεδομένα του. Οπότε, δουλειά του δεύτερου ερευνητή

ήταν αφενός να προσδιορίσει τι ακριβώς συνέβη, πότε και από ποιον και αφετέρου να διαπιστώσει αν όντως ο ύποπτος ήταν ένοχος για αυτό που είχε κατηγορηθεί. Μετά από εκτενή και ενδελεχή εξέταση του υπολογιστικού μηχανήματος ο δεύτερος ερευνητής τελικά ανακάλυψε τι πραγματικά είχε συμβεί. Ο μοναδικός λόγος για όλο αυτό το μπέρδεμα που δημιουργήθηκε ήταν ο χρόνος. Ο ύποπτος είχε εσκεμμένα αλλάξει το ρολόι του υπολογιστή του και το είχε βάλει αρκετές ώρες μπροστά από το κανονικό, γεγονός που ο πρώτος ερευνητής δεν πρόσεξε και γι' αυτό τον λόγο κατέληξε σε λανθασμένα συμπεράσματα.

Σε περιβάλλον υπολογιστικού νέφους ο ύποπτος μπορεί να κατέχει παραπάνω από ένα εικονικά μηχανήματα. Ο ερευνητής θα πρέπει θα εξετάσει το καθένα από αυτά και να εξάγει τα αντίστοιχα ψηφιακά αποδεικτικά στοιχεία. Οποιαδήποτε διαφορά στον χρόνο μεταξύ των εικονικών μηχανημάτων του υπόπτου θα δημιουργήσει προβλήματα στον ερευνητή κατά τη διάρκεια συσχέτισης των γεγονότων μεταξύ τους. Ακόμα και δέκα ή είκοσι δευτερόλεπτα απόκλισης μπορούν να αποβούν μοιραία για την αλληλουχία των διαφόρων ενεργειών του υπόπτου. Επίσης, θεωρώντας ότι ο χρόνος στο υπολογιστικό νέφος μπορεί να είναι είτε μπροστά είτε πίσω σε σχέση με τον πραγματικό, χωρίς κάποιο δεδομένο μοτίβο, ο ερευνητής δεν δύναται να διορθώνει τον χρόνο ή να κάνει υποθέσεις σχετικά με διαφορετικές μεταξύ τους χρονικές στιγμές.

8.5. Υπάρχουσες τεχνολογίες συγχρονισμού για το υπολογιστικό νέφος

Υπάρχει μια μεγάλη ποικιλία από τεχνικές, οι οποίες προσφέρουν συγχρονισμό του ρολογιού στο υπολογιστικό νέφος. Στις παραγράφους που ακολουθούν, θα αναφέρουμε τις πιο βασικές από αυτές με περισσότερη λεπτομέρεια.

8.5.1 Συγχρονισμός ρολογιού από εξωτερική πηγή

Οι πάροχοι υπηρεσιών υπολογιστικού νέφους χρησιμοποιούν παραδοσιακές λύσεις, για να διατηρούν τους φυσικούς τους διακομιστές συγχρονισμένους και να έχουν τη σωστή ώρα. Πιο συγκεκριμένα, χρησιμοποιούνται ειδικοί διακομιστές στο δίκτυο, οι οποίοι συλλέγουν και διορθώνουν την ώρα των υπόλοιπων διακομιστών με τη χρήση αρκετών πρωτοκόλλων, μεταξύ των οποίων το NTP (Network Time Protocol) [214] και το αντίστοιχο της Microsoft, το W32TIME [215].

Το πρωτόκολλο NTP είναι ένα πρωτόκολλο δικτύου για συγχρονισμό των ρολογιών μεταξύ των υπολογιστικών συστημάτων σε ένα δίκτυο μεταγωγής πακέτων [214]. Το συγκεκριμένο πρωτόκολλο έχει σχεδιαστεί από τον D. Mills του Πανεπιστημίου του Delaware. Σκοπός του είναι να παρέχει συντονισμένη μόνο την παγκόσμια ώρα (UTC – Coordinated Universal Time). Αυτό συνεπάγεται ότι το NTP δεν παρέχει πληροφορίες για τις ζώνες ώρας ή για τη θερινή και τη χειμερινή ώρα. Παρέχει συγχρονισμό ακριβείας δέκα msec στο διαδίκτυο και ακριβείας ενός msec σε επίπεδο τοπικών δικτύων. Η τρέχουσα έκδοση του είναι η 4.0 και τα πλήρη χαρακτηριστικά του είναι στο [214].

Το NTP μπορεί να λειτουργεί με τρεις διαφορετικούς τρόπους και συγκεκριμένα ως αρχικός διακομιστής, ως δευτερεύων διακομιστής και ως πελάτης. Ο αρχικός διακομιστής είναι εκείνος που συγχρονίζεται απευθείας με το ρολόι αναφοράς. Δουλειά του δευτερεύοντος διακομιστή είναι να συγχρονίζει τους υπόλοιπους και τους πελάτες. Με σκοπό τη διατήρηση της σταθερότητας σε μεγάλα υποδίκτυα NTP, οι διακομιστές NTP θα πρέπει να είναι πλήρως συμβατοί με την έκδοση 4.0. Τέλος, το πρωτόκολλο NTP ως πελάτης μπορεί να συγχρονίζει μερικά είδη διακομιστών, αλλά δεν είναι σε θέση να συγχρονίζει άλλους πελάτες.

Δυστυχώς, ο διακομιστής NTP δεν είναι σχεδιασμένος να τρέχει μέσα σε μια εικονική μηχανή. Αυτό συμβαίνει, γιατί το NTP απαιτεί την ύπαρξη στο υλικό ενός υψηλής ακριβείας ρολογιού σε συνδυασμό με τους χρόνους απόκρισης για τις σχετικά με το ρολόι διακοπές που θα πρέπει να εξυπηρετούνται αμέσως, χαρακτηριστικά που, εξ ορισμού, δεν

μπορούν να υπάρχουν σε ένα εικονικό μηχάνημα [226]. Παρόλο όμως που ο διακομιστής NTP αντιμετωπίζει προβλήματα με την εικονικοποίηση, ο πελάτης NTP μπορεί να λειτουργήσει ομαλά σε εικονικό περιβάλλον. Όλοι οι πάροχοι υπηρεσιών υπολογιστικού νέφους γνωρίζουν το πρόβλημα συγχρονισμού των ρολογιών τους και για αυτόν τον λόγο σχεδόν όλοι τους προτείνουν τη χρήση ενός πελάτη NTP. Για παράδειγμα, η Amazon προτείνει στους δικούς της χρήστες IaaS να απενεργοποιήσουν το ρολόι του Hypervisor και να εφαρμόσουν την πολιτική του NTP στα συστήματά τους για βέλτιστη απόδοση.

Η έκδοση των Windows για το πρωτόκολλο NTP ονομάζεται W32TIME. Το W32TIME χρησιμοποιεί το πρωτόκολλο NTP και παρέχει μια απλοποιημένη στρατηγική πρόσβασης στο χρόνο, σε διακομιστές και πελάτες που δεν ενδιαφέρονται για την ακρίβεια που παρέχει το NTP. Το W32TIME είναι εξ ορισμού εγκατεστημένο σε όλα τα υπολογιστικά συστήματα που φέρουν λειτουργικό σύστημα Windows και χρησιμοποιεί επίσης το σύστημα της παγκόσμιας ώρας (UTC) ως αναφορά. Όλοι οι πάροχοι υπηρεσιών υπολογιστικού νέφους που έχουν ως λειτουργικό σύστημα τα Windows στους διακομιστές τους, χρησιμοποιούν το W32TIME ως πρωτόκολλο συγχρονισμού των ρολογιών τους. Επειδή, όπως και το NTP, το W32TIME είναι ανεξάρτητο από τη ζώνη ώρας ενός υπολογιστικού συστήματος, η ζώνη ώρας αποθηκεύεται στη μνήμη του συστήματος και προστίθεται στην ώρα του ρολογιού πριν αυτή εμφανιστεί στον χρήστη.

Το πρωτόκολλο W32TIME λειτουργεί ως υπηρεσία στα Windows και ξεκινά αυτόματα έχοντας σαν σκοπό την αρχικοποίηση του ρολογιού από τη στιγμή που ο υπολογιστής εισέλθει σε κάποιο δίκτυο. Μια υπηρεσία ειδικού σκοπού, η οποία ονομάζεται Net Logon, ερευνά στο δίκτυο για τον αυθεντικοποιημένο κόμβο με τον οποίο θα συγχρονίσει το ρολόι του υπολογιστή [224]. Όταν τον βρει, ξεκινά την επικοινωνία μαζί του, ανταλλάσσοντας πακέτα SNTP (Simple Network Time Protocol) [227], με σκοπό τον υπολογισμό αρχικά του χρόνου που απαιτείται για τη λήψη και αποστολή μηνυμάτων μεταξύ των δύο οντοτήτων. Στη συνέχεια, έχοντας πάρει τον χρόνο από τον κόμβο, προσθέτει τον χρόνο

που βρήκε από τη λήψη – αποστολή, για να εξάγει το σωστό αποτέλεσμα [227].

Κάθε 45 λεπτά το W32TIME συνδέεται με τον αυθεντικοποιημένο κόμβο με σκοπό τον έλεγχο του τοπικού ρολογιού του και τη διόρθωση τυχόν αποκλίσεων. Αυτό θα συμβεί τρεις φορές και σε περίπτωση που δεν βρεθεί απόκλιση, η επόμενη σύνδεση θα συμβεί μετά από οκτώ ώρες. Σε περίπτωση κάποιας αποτυχίας η όλη διαδικασία ξεκινά από την αρχή. Υπάρχουν τρεις διαφορετικές μέθοδοι ρύθμισης του W32TIME. Η πρώτη είναι ο συγχρονισμός με βάση την ιεραρχία, η δεύτερη είναι η χρήση μιας ανεξάρτητης πηγής για συγχρονισμό που την επιλέγει ο χρήστης και η τρίτη είναι ο μη συγχρονισμός του ρολογιού. Εξ ορισμού η πρώτη μέθοδος λειτουργεί σε κάθε μηχάνημα που έχει ως λειτουργικό σύστημα τα Windows.

Οι ίδιες τεχνικές μπορεί να υιοθετηθούν από το λειτουργικό σύστημα του χρήστη και σε ένα περιβάλλον υπολογιστικού νέφους. Για παράδειγμα, μια τέτοια προσέγγιση χρησιμοποιείται στον Hypervisor Xen. Ειδικότερα, καθένα από τα λειτουργικά συστήματα των χρηστών τρέχει το δικό του πρωτόκολλο συγχρονισμού και συγκεκριμένα το NTP. Αυτό σημαίνει ότι το λειτουργικό σύστημα του χρήστη συνδέεται στον δικό του διακομιστή χρόνου κάνοντας χρήση της γνωστής διαδικασίας σύνδεσης [228]. Η συγκεκριμένη υλοποίηση λειτουργεί αποδοτικά σε σχέση με τη χρήση των πόρων, αλλά δεν είναι η καλύτερη σε ό,τι αφορά την απόδοση. Αυτό συμβαίνει επειδή υπάρχουν επιπρόσθετες καθυστερήσεις σε ένα τέτοιο λειτουργικό σύστημα και αυτό ωθεί το NTP σε καταστάσεις αστάθειας [228]. Παρόλα αυτά, η ίδια μέθοδος μπορεί να χρησιμοποιηθεί, όταν ένα εικονικό μηχάνημα μεταφέρεται από ένα φυσικό μηχάνημα σε ένα άλλο. Θα πρέπει να ληφθεί υπόψη όμως, ότι οι πολλές και συνεχείς μεταφορές ενός εικονικού μηχανήματος προκαλούν προβλήματα στο χρόνο, της τάξεως των δευτερολέπτων, για αυτό και η χρήση της μεθόδου αυτής θεωρείται αναποτελεσματική.

8.5.2. Συγχρονισμός ρολογιού με τοπική πηγή

Το λειτουργικό σύστημα του χρήστη που τρέχει μέσα στους διακομιστές του παρόχου μπορεί να κρατά συγχρονισμένο το ρολόι του, ελέγχοντας ανά τακτά χρονικά διαστήματα το ρολόι του φυσικού μηχανήματος. Όλοι οι hypervisors προσφέρουν εφαρμογές για τον συγχρονισμό του ρολογιού, συνήθως με τη μορφή ρουτινών του συστήματος αλλά χωρίς να εξασφαλίζουν την ακεραιότητα του συγχρονισμού. Συνήθως, ελέγχουν το ρολόι του κάθε διακομιστή τους με το ρολόι του φυσικού μηχανήματος. Όταν βρίσκουν κάποια απόκλιση, ο hypervisor διορθώνει αυτόματα το ρολόι του διακομιστή χωρίς καμιά προειδοποίηση ή απλώς μέσω μιας ρουτίνας ενημερώνει το λειτουργικό σύστημα του διακομιστή. Επίσης, ο hypervisor αναλαμβάνει δράση σχετικά με τον χρόνο, όταν επανέρχεται σε λειτουργία ένα εικονικό μηχάνημα μετά από κάποια αναστολή. Στη συνέχεια θα αναλύσουμε με μεγαλύτερη λεπτομέρεια τους τέσσερις πιο γνωστούς hypervisors, οι οποίοι είναι ο Xen, ο VMWare, ο Hyper-V και ο KVM (Kernel-based Virtual Machine).

Σε ένα τυπικό εικονικό μηχάνημα τύπου Xen μόνο το Dom0 είναι σε θέση να τρέξει αλγόριθμο συγχρονισμού ρολογιού, οπότε σε αυτή την περίπτωση τα πακέτα του NTP των λειτουργικών συστημάτων των χρηστών επικοινωνούν, ανά τακτά χρονικά διαστήματα με το Dom0, για να ελέγξουν την ώρα τους [228]. Η επικοινωνία αυτή διεξάγεται μέσω μιας τροποποιημένης ρουτίνας του λειτουργικού συστήματος του χρήστη, η οποία χρησιμοποιεί το Xen Clocksource, για να καθορίσει τη σωστή τιμή του χρόνου.

Σύμφωνα με την εταιρεία που έχει κατασκευάσει το VMware υπάρχει μια εσωτερική συνάρτηση, εξαιτίας της οποίας μένει πίσω στο χρόνο και, όταν χρειαστεί, κάνει τις απαραίτητες διορθώσεις [229]. Ο λόγος που συμβαίνει αυτό, όπως αναγράφεται και στο σχετικό εγχειρίδιο χρήσης, είναι για να μην διαταράσσεται η ομαλή λειτουργία τόσο του διακομιστή του παρόχου όσο και των λειτουργικών συστημάτων των πελατών από ανωμαλίες στις χρονικές ενδείξεις.

Ο Hyper-V προσφέρει επίσης τις βασικές υπηρεσίες συγχρονισμού του ρολογιού [230]. Αυτό το επιτυγχάνει κάνοντας αναγνώσεις ρολογιού από το υφιστάμενο λειτουργικό σύστημα και στέλνοντας τις στο λειτουργικό σύστημα του πελάτη. Το λειτουργικό σύστημα του πελάτη από την πλευρά του, όταν λάβει αυτά τα δεδομένα, τα παραχωρεί στην υποδομή των Windows. Επίσης, τα συγκεκριμένα δεδομένα του χρόνου είναι προσαρμοσμένα σε όποιες διαφορές ζώνης ώρας υπάρχουν μεταξύ του λειτουργικού συστήματος διαχείρισης και του λειτουργικού συστήματος του χρήστη.

Τέλος, ο hypervisor KVM παρέχει ένα ημι-εικονικό ρολόι για τα λειτουργικά συστήματα των χρηστών του [231]. Ημι-εικονικές ονομάζονται οι συσκευές, οι οποίες χρησιμοποιούν στοιχεία υλικού και, για να λειτουργήσουν, απαιτείται να υπάρχει ο οδηγός τους στο λειτουργικό σύστημα [232]. Λόγω του ότι το λειτουργικό σύστημα του πελάτη αξιοποιεί απλώς έναν μετρητή για την ώρα, το οποίο μπορεί να προκαλέσει προβλήματα συγχρονισμού, ο KVM παρέχει το ημι-εικονικό ρολόι, ώστε να τους δίνει τη δυνατότητα να χρησιμοποιούν τα συστήματα συγχρονισμού που είχαν και σε ένα παραδοσιακό υπολογιστικό σύστημα.

8.6. Αξιόπιστες τεχνικές διατήρησης χρόνου στο νέφος

Όπως αναφερθήκαμε σε προηγούμενες παραγράφους, ο σωστός χρόνος σε ένα υπολογιστικό μηχάνημα είναι απαραίτητος τόσο για την εύκολη διεξαγωγή μιας ψηφιακής εγκληματολογικής έρευνας, όσο, το κυριότερο, για την εξαγωγή σωστών και ασφαλών συμπερασμάτων. Στη συνέχεια, θα αναφερθούμε στον ρόλο που έχει ο καθένας από τους εμπλεκόμενους στη διατήρηση του σωστού χρόνου σε ένα περιβάλλον υπολογιστικού νέφους.

8.6.1. Ο ρόλος του παρόχου υπολογιστικού νέφους

Σε πρακτικό επίπεδο, όλες οι προτεινόμενες λύσεις βασίζονται σε μεγάλο βαθμό στον πάροχο υπηρεσιών υπολογιστικού νέφους. Αυτό θεωρείται αναμενόμενο από τη στιγμή που όλοι οι πόροι, εικονικοί και κανονικοί, είναι υπό τον έλεγχό του. Με στόχο την καλύτερη εκτίμηση του αντίκτυπου αυτής της εξάρτησης, θα ορίσουμε δύο διαφορετικά μοντέλα ασφάλειας. Στο πρώτο μοντέλο, ο πάροχος υπηρεσιών υπολογιστικού νέφους είναι έντιμος και στο δεύτερο είναι κακόβουλος.

Στο πρώτο μοντέλο ο έντιμος πάροχος υπηρεσιών υπολογιστικού νέφους προσπαθεί να παρέχει τις καλύτερες δυνατές υπηρεσίες στους πελάτες του, κάνοντας χρήση μιας ή περισσοτέρων αξιόπιστων πηγών χρόνου και του καλύτερου πρωτόκολλου συγχρονισμού. Σε αυτό το σενάριο οι πελάτες μπορούν να δείξουν εμπιστοσύνη στον πάροχο για τον ακριβή χρόνο. Ωστόσο, θα πρέπει να εμπιστεύονται και την ικανότητα του παρόχου να έχει τα φυσικά του μηχανήματα συγχρονισμένα με τον σωστό χρόνο. Εννοείται ότι ο χρήστης οφείλει να θεωρεί τον πάροχό του αξιόπιστο από τη στιγμή που χρησιμοποιεί τις υποδομές του.

Στο δεύτερο μοντέλο δεν υπάρχει καμιά είδους προστασία για τον πελάτη. Ο πάροχος υπηρεσιών υπολογιστικού νέφους μπορεί να διαχειρίζεται τα εσωτερικά ρολόγια των διακομιστών του, όπως επίσης και όλων των εικονικών μηχανημάτων του. Ακόμα και αν ένας πελάτης χρησιμοποιεί μια εξωτερική πηγή για λήψη του χρόνου, ο hypervisor μπορεί να δημιουργεί τεχνητές καθυστερήσεις τυχαίας περιόδου μεταξύ του πελάτη και της εξωτερικής πηγής, ώστε το λειτουργικό του πελάτη να μην μπορεί να λειτουργήσει με τα γνωστά πρωτόκολλα.

8.6.2. Ο ρόλος του έμπιστου παρόχου χρόνου

Στις περισσότερες από τις τρέχουσες υλοποιήσεις υπάρχει μεγάλη εξάρτηση στους παρόχους χρόνου. Είτε ο πάροχος υπηρεσιών υπολογιστικού νέφους ή/και το λειτουργικό σύστημα του πελάτη χρησιμοποιούν ένα από τα πρωτόκολλα που προαναφέρθηκαν για να

συγχρονίσουν το ρολόι τους με ένα διακομιστή χρόνου. Η ορθότητα στον χρόνο εξαρτάται σε μεγάλο βαθμό από την αξιοπιστία της συγκεκριμένης υπηρεσίας. Η λήψη του χρόνου από πολλούς διακομιστές και η διατήρηση της κοινής τιμής χρόνου από αυτούς, θεωρείται ότι είναι η καλύτερη στρατηγική. Καλό θα είναι να αποφεύγονται οι διακομιστές χρόνου που βρίσκονται μακριά γεωγραφικά, επειδή τυχόν καθυστερήσεις που οφείλονται στη διαδρομή από και προς τον διακομιστή είναι ποικίλες και μη προβλέψιμες, οπότε δεν μπορεί να ληφθεί έγκυρος χρόνος.

8.6.3. Ο ρόλος του πελάτη υπηρεσιών υπολογιστικού νέφους

Η διατήρηση της ακρίβειας στον χρόνο είναι μια πολύ δύσκολη εργασία και τα περισσότερα από τα πρωτόκολλα απαιτούν πολύπλοκες διαδικασίες εγκατάστασης και ρυθμίσεων. Για παράδειγμα, η ακρίβεια του πρωτόκολλου NTP είναι κυμαινόμενη και εξαρτάται πλήρως από τις παραμέτρους που του έχουν δοθεί. Σε περίπτωση που η ακρίβεια θα πρέπει να είναι σε βαθμό msec αντί για sec η ρύθμιση είναι ιδιαίτερα πολύπλοκη. Επιπλέον, οι διάφορες ενέργειες μεταφοράς, όπως για παράδειγμα μεταφορά, αδρανοποίηση, αναστολή και επαναλειτουργία του εικονικού μηχανήματος, μπορεί να προκαλέσουν σοβαρές αλλαγές στον χρόνο. Από τα προηγούμενα είναι προφανές ότι το να αφεθεί ο συγχρονισμός του ρολογιού στα χέρια του πελάτη απαιτεί πολλές τεχνικές γνώσεις από μέρους του, τις οποίες θα πρέπει να τις εφαρμόζει ανά πάσα στιγμή.

8.6.4. Καταγραφή του συγχρονισμού του ρολογιού

Το ρολόι ενός λειτουργικού συστήματος, άσχετα αν μιλάμε για το λειτουργικό σύστημα του παρόχου ή το λειτουργικό σύστημα του πελάτη, είναι μία από τις πιο πολύτιμες πηγές για την εύρεση ψηφιακών αποδεικτικών στοιχείων. Για αυτό τον λόγο θα πρέπει να κρατούνται αρχεία καταγραφής σχετικά με το ρολόι και τον χρόνο γενικότερα, τα οποία θα συγκεντρώνουν πληροφορίες σχετικές με το πότε ελέγχθηκε το

ρολόι του συστήματος, ποιος έκανε τον έλεγχο, τι είδους πρωτόκολλο χρησιμοποιήθηκε και ποιο ήταν το αποτέλεσμα του ελέγχου αυτού. Όσες φορές βρεθεί ότι υπάρχει απόκλιση μεταξύ του ρολογιού του λειτουργικού συστήματος σε σχέση με τον πραγματικό χρόνο, θα πρέπει να καταγράφεται εκτενώς, όπως επίσης να γίνεται το ίδιο και με το ποσό της απόκλισης και με τον τρόπο διόρθωσης.

8.6.5. Απόδειξη της ορθότητας του χρόνου

Η αποδοχή των αποδεικτικών στοιχείων θα πρέπει να συνοδεύεται από τεχνολογικές αποδείξεις. Στις μέρες μας, η κρυπτογραφία προσφέρει όλα τα εργαλεία, τα οποία είναι απαραίτητα για την αποδοτική και αποδεκτή διαχείριση του ρολογιού. Οποιαδήποτε τροποποίηση του χρόνου, οποιαδήποτε εφαρμογή που χρησιμοποιεί πρωτόκολλα συγχρονισμού του χρόνου, μπορεί να θεωρηθεί έμπιστη με τη χρήση κρυπτογραφικών τεχνικών. Ωστόσο, η συντριπτική πλειονότητα των εργαλείων και των εφαρμογών της κρυπτογραφίας δεν υποστηρίζονται από τις ήδη υπάρχουσες τεχνικές συγχρονισμού.

8.6.6. Αξιολόγηση των πρωτοκόλλων συγχρονισμού

Τα NTP και W32TIME δεν είναι τα μόνα πρωτόκολλα συγχρονισμού του ρολογιού μέσω δικτύου. Ένα άλλο πρωτόκολλο για τον συγχρονισμό του ρολογιού είναι το PTP (Precision Time Protocol) [233] και, επίσης, προτάθηκε το RADclock (Robust Absolute & Difference Clock), το οποίο έχει κατασκευαστεί με προσανατολισμό στο υπολογιστικό νέφος και την επίλυση των δυσκολιών που προκύπτουν στα ήδη υπάρχοντα πρωτόκολλα.

Το PTP είναι ένα πρωτόκολλο συγχρονισμού του ρολογιού μέσω ενός δικτύου. Αρχικά είχε οριστεί από την IEEE, συγκεκριμένα στο πρότυπο 1588-2002, και δημοσιοποιήθηκε το 2002. Η τρέχουσα έκδοσή του είναι η 2.0, η οποία εμφανίστηκε το 2008. Το πρωτόκολλο PTP χρησιμοποιείται κυρίως για τον συγχρονισμό ρολογιών συσκευών ειδικού σκοπού, όπως για παράδειγμα οι αυτοματοποιημένες συσκευές

μιας βιομηχανίας [233]. Όλες οι συσκευές θα πρέπει να είναι συνδεδεμένες σε ένα τοπικό δίκτυο πάνω σε μεταγωγέα. Το PTP λειτουργεί πρωτίστως σε λειτουργία πολυεκπομπής (broadcast mode). Σε αυτή τη λειτουργία ο κύριος κόμβος παρέχει συγχρονισμό σε πολλούς κόμβους – πελάτες στο ίδιο τοπικό δίκτυο. Εκτός από τη λειτουργία πολυεκπομπής, το πρωτόκολλο PTP μπορεί να λειτουργήσει και σε λειτουργία κυρίου/δούλου (master/slave). Σε αυτή τη λειτουργία ο συγχρονισμός επιτυγχάνεται μέσω μηνυμάτων που ανταλλάσσονται μεταξύ των συμμετεχόντων στο τοπικό δίκτυο. Η ακρίβεια του PTP στον συγχρονισμό του ρολογιού είναι της τάξης των 100nsec και καθορίζεται αποκλειστικά και μόνο από τη σταθερότητα και την ακρίβεια του κεντρικού ρολογιού και του μετρητή [233].

Όπως προαναφέρθηκε, το RADClock είναι ένα πρωτόκολλο, το οποίο χρησιμοποιεί νέα αρχιτεκτονική και σχεδιάστηκε αποκλειστικά για εικονικά περιβάλλοντα και συγκεκριμένα για το Xen [228]. Επίσης, είναι χτισμένο με βάση έναν αλγόριθμο ανατροφοδότησης και θεωρείται ο απόγονος του NTP. Μέχρι στιγμής είναι διαθέσιμο σε συστήματα με λειτουργικό FreeBSD και Linux. Σε αυτό το πρωτόκολλο τα πακέτα χρόνου σηματοδοτούνται με την ακριβή ημερομηνία δημιουργίας τους. Η τελική τιμή του ρολογιού εκτιμάται από την ακριβή δημιουργία των πακέτων χρόνου σε συνδυασμό με την λήψη του χρόνου από τον διακομιστή χρόνου. Από τη στιγμή που για κάθε ξεχωριστό πακέτο εκτιμάται ο ακριβής χρόνος, το πρωτόκολλο αυτό έχει τη μέγιστη δυνατή ακρίβεια ακόμα και σε περιβάλλοντα υπολογιστικού νέφους.

8.6.6.1. Σύγκριση πρωτοκόλλων

Στη συγκεκριμένη παράγραφο θα εξετάσουμε όλα τα προαναφερόμενα πρωτόκολλα αναφορικά με την ακρίβεια που επιτυγχάνουν, την υποστήριξη του υλικού, τις αναμενόμενες προσδοκίες ακρίβειας και, τέλος, το πεδίο εφαρμογής τους. Η ανάλυσή μας απεικονίζεται στον ακόλουθο πίνακα. Τα NTP, W32TIME και RADClock δεν χρειάζονται ειδικό υλικό για να λειτουργήσουν, ενώ το PTP χρειάζεται. Το συγκεκριμένο στοιχείο είναι και ο βασικότερος λόγος για

τον οποίο το PTP δεν είναι τόσο δημοφιλές όσο τα υπόλοιπα. Το PTP χρησιμοποιείται πιο συχνά, για να συγχρονίζει ρολόγια συσκευών σε βιομηχανικό επίπεδο. Τέλος, το πρωτόκολλο NTP είναι το πιο συνηθισμένο πρωτόκολλο για τον συγχρονισμό υπολογιστικών συστημάτων και διακομιστών.

Σε ότι αφορά την ακρίβεια, το NTP δεν διακρίνεται για τη σταθερότητά του. Η ακρίβειά του εξαρτάται εξ ολοκλήρου από το υφιστάμενο υλικό και τις ρυθμίσεις του χρήστη. Από την άλλη πλευρά, η ακρίβεια στο PTP είναι της τάξης των 100 nsec, στο W32TIME υπολογίζεται σε 1 msec και, τέλος, στο RADClock υπολογίζεται σε 1 μsec. Σε ό,τι αφορά την κλίμακα του χρόνου, τα NTP και W32TIME αντιλαμβάνονται secs, το PTP αντίστοιχα nsecs και, τέλος, το RADClock msecs.

Όσον αφορά τη χρήση, τα πρωτόκολλα NTP, W32TIME και RADClock εμφανίζονται σε υπολογιστικά συστήματα με σκοπό τη διατήρηση του χρόνου συγχρονισμένου. Από την άλλη πλευρά, το PTP, λόγω της μεγάλης του ακρίβειας, χρησιμοποιείται σε μηχανές σε βιομηχανικό επίπεδο. Τέλος, σχετικά με την προσφερόμενη ασφάλεια όλα τα πρωτόκολλα που προαναφέρθηκαν προσφέρουν ακεραιότητα και αυθεντικότητα των μηνυμάτων που δημιουργούν.

	NTP	**PTP**	**RADClock**	**W32TIME**
Υποστήριξη από υλικό	Όχι	Ναι	Όχι	Όχι
Ακρίβεια	Όχι σταθερή	100 nsec	< 1μsec	Msec
Ασφάλεια	- Συμμετρική και δημοσίου κλειδιού - Αυθεντικοποίηση ακεραιότητας	- Συμμετρική - Αυθεντικοποίηση Ακεραιότητας	Μη διαθέσιμη	Μη διαθέσιμη
Πεδίο εφαρμογής	Συστήματα Η/Υ	Βιομηχανικοί αυτοματισμοί	Συστήματα Η/Υ	Συστήματα Η/Υ

8.7. Επίλογος – Συμπεράσματα

Η κλασική διαδικασία της ψηφιακής εγκληματολογικής έρευνας δεν είναι ικανή να λειτουργήσει αποδοτικά στο περιβάλλον του υπολογιστικού νέφους λόγω της ιδιαίτερης φύσης του. Ως εκ τούτου, θα πρέπει να θεσπιστεί και να συγκροτηθεί ένα νέο πλαίσιο πάνω στο οποίο

θα επιτελούνται οι ψηφιακές εγκληματολογικές έρευνες στο περιβάλλον του υπολογιστικού νέφους. Μία από τις βασικότερες παραμέτρους που θα πρέπει να επαναπροσδιοριστούν είναι ο συγχρονισμός των ρολογιών των επιμέρους συστημάτων, με σκοπό την ακριβή αναπαράσταση των ψηφιακών αποδεικτικών στοιχείων στον χρόνο. Για να θεωρηθεί επιτυχής ένας τρόπος συγχρονισμού, θα πρέπει να διεξάγεται με τέτοιο τρόπο, ώστε αφενός να αποφεύγεται η αλλοίωση των ψηφιακών αποδεικτικών στοιχείων και αφετέρου να αποδεικνύεται η εγκυρότητα του χρόνου που συγχρονίζεται. Είναι ευνόητο ότι οι τρεις απαιτήσεις ασφάλειας για τα αρχεία καταγραφής συμβάντων, οι οποίες ορίστηκαν ανωτέρω, θα πρέπει επίσης να ικανοποιούνται και στο σύστημα συγχρονισμού του ρολογιού.

Σε ό,τι αφορά την κατασκευή ενός συστήματος συγχρονισμού σε περιβάλλον υπολογιστικού νέφους, ο προγραμματιστής θα πρέπει να λάβει υπόψη του μερικές αναγκαίες και υποχρεωτικές συνθήκες. Αρχικά, θα πρέπει να δημιουργηθεί ένα πρωτόκολλο που θα δουλεύει αποκλειστικά και μόνο σε όλα τα περιβάλλοντα του υπολογιστικού νέφους. Αναγκαίο είναι να προβλεφτούν ασφαλιστικές δικλείδες που να προστατεύουν όλα τα εμπλεκόμενα μέρη, καθώς και τα αρχεία καταγραφής συμβάντων. Σε ό,τι αφορά τον χρόνο, όλες οι λειτουργίες επί του ρολογιού θα πρέπει να καταγράφονται λεπτομερώς σε ένα ξεχωριστό αρχείο καταγραφής συμβάντων. Επίσης, το πρωτόκολλο συγχρονισμού που θα κατασκευαστεί για το υπολογιστικό νέφος θα πρέπει να υποστηρίζει εγγενώς κρυπτογραφία, τόσο για τη μεταφορά όσο και για το περιεχόμενο των δεδομένων που θα δημιουργεί. Τέλος, θα πρέπει να θεσπιστούν πολιτικές ασφάλειας σχετικές με το ζήτημα του συγχρονισμού του ρολογιού και αυτές θα πρέπει να τηρούνται κατά γράμμα από όλα τα εμπλεκόμενα μέρη.

ΚΕΦΑΛΑΙΟ ΕΝΑΤΟ

Επίλογος και συμπεράσματα

9.1. Εισαγωγή

Η συγκεκριμένη διατριβή, αρχικά, αναλύει τα προβλήματα που προκύπτουν κατά τη διαδικασία μιας εγκληματολογικής έρευνας στο υπολογιστικό νέφος, υπό το πρίσμα γνωστών μεθόδων ψηφιακών ερευνών. Γίνεται λεπτομερής περιγραφή του ορισμού του υπολογιστικού νέφους καθώς και της υφιστάμενης τεχνολογίας του. Παράλληλα, επισημαίνονται οι ήδη υπάρχουσες τεχνικές ασφάλισης της υποδομής

του υπολογιστικού νέφους που παρέχονται από τους παρόχους με στόχο την προσπάθεια εκμηδενισμού των επιτυχών επιθέσεων προς αυτό. Στη συνέχεια αναλύονται οι ήδη γνωστές μεθοδολογίες ψηφιακών εγκληματολογικών ερευνών υπό το πρίσμα του υπολογιστικού νέφους και τέλος, αναδεικνύεται το πρόβλημα του συγχρονισμού του ρολογιού των επιμέρους συστημάτων και παρουσιάζεται μια λύση αναφορικά με την διασφάλιση της ακεραιότητας του χρόνου.

9.2. Ψηφιακές εγκληματολογικές μέθοδοι στο υπολογιστικό νέφος

Αρχικά μελετήθηκαν διεξοδικά οι πιο διαδεδομένες μέθοδοι ψηφιακών εγκληματολογικών ερευνών και στη συνέχεια έγινε ομαδοποίηση των επιμέρους βημάτων σε τρεις κύριες φάσεις: τη φάση της προετοιμασίας, τη φάση της έρευνας και της φάση της παρουσίασης.

Σε δεύτερο χρόνο, εξετάστηκε μεμονωμένα κάθε βήμα των φάσεων κατά πόσο μπορεί να ανταπεξέλθει σε περιβάλλοντα υπολογιστικού νέφους. Οι δυνατές τιμές που θα μπορούσε να πάρει ήταν οι εξής:

1) μη εφαρμόσιμο,
2) εφαρμόσιμο,
3) εξαρτάται από τον χρήστη και,
4) εξαρτάται από τον πάροχο.

Από τα αποτελέσματα προέκυψε ότι το σύνολο των βημάτων εξαρτώνται κατά κύριο λόγο από τον πάροχο και ανάλογα με το μοντέλο (SaaS, IaaS, PaaS), ο ερευνητής θα είναι σε θέση να εξάγει περισσότερα ή λιγότερα ψηφιακά αποδεικτικά στοιχεία. Πιο συγκεκριμένα, στο IaaS μοντέλο ο ερευνητής έχει περισσότερες επιλογές συλλογής στοιχείων, ενώ στο SaaS ο ερευνητής εξαρτάται κατά μεγάλο ποσοστό από τα στοιχεία που θα του διαθέσει ο πάροχος υπηρεσιών υπολογιστικού νέφους. Επίσης, οι παραδοσιακές μέθοδοι ψηφιακών εγκληματολογικών ερευνών δεν μπορούν να λειτουργήσουν σε περιβάλλοντα με πολλαπλούς χρήστες παράλληλα, γιατί ελλοχεύει ο κίνδυνος να προσπελάσουν δεδομένα

άλλων χρηστών. Τέλος, ενώ στις παραδοσιακές εγκληματολογικές μεθόδους είναι σημαντικό κομμάτι η έρευνα για διαγραμμένα δεδομένα στον σκληρό δίσκο του υπόπτου, σε περιβάλλον υπολογιστικού νέφους αυτό είναι πρακτικά αδύνατο να συμβεί, καθώς μόλις ο ύποπτος διαγράψει έναν όγκο δεδομένων, ο ελεύθερος χώρος θα δοθεί αμέσως στον επόμενο διαθέσιμο χρήστη.

9.3. Διασφάλιση της ακεραιότητας του χρόνου

Στη συγκεκριμένη ενότητα αναφέρεται ο λόγος που τα αρχεία καταγραφής συμβάντων αποτελούν δομικά στοιχεία κατά τη διεξαγωγή μιας ψηφιακής εγκληματολογικής έρευνας. Αναλύεται ο τρόπος αποθήκευσης των αρχείων καταγραφής συμβάντων, καθώς και τα σοβαρά προβλήματα που προκύπτουν από τον μη συγχρονισμό του ρολογιού στα συστήματα.

Ακολούθως, εξηγούνται οι δύο τεχνικές που χρησιμοποιούνται στο υπολογιστικό νέφος. Η πρώτη είναι ο συγχρονισμός, τόσο για τον hypervisor όσο και τα εικονικά μηχανήματα, να γίνεται από μια εξωτερική πηγή χρόνου, ενώ η δεύτερη είναι ο συγχρονισμός να γίνεται μεταξύ μιας εξωτερικής πηγής χρόνου με τον hypervisor και αυτός με την σειρά του να είναι πηγή χρόνου για τα εικονικά μηχανήματα που φιλοξενεί. Αναφορικά με την πρώτη περίπτωση, γίνεται χρήση των γνωστών πρωτοκόλλων συγχρονισμού και στη συνέχεια γίνεται αξιολόγησή τους αναφορικά με την ακρίβεια που έχουν, την ασφάλεια που προσφέρουν, εάν χρειάζεται ειδικό υλικό για να λειτουργήσουν και ποιες είναι οι εφαρμογές τους. Στη δεύτερη περίπτωση τον ρόλο των πρωτοκόλλων συγχρονισμού τον προσφέρει ο hypervisor, ο οποίος ελέγχει ανά τακτά χρονικά διαστήματα τον δικό του χρόνο σε σχέση με τον χρόνο που λαμβάνει από την εξωτερική πηγή και με τα εικονικά μηχανήματα που φιλοξενεί. Όταν εντοπίσει κάποια απόκλιση, είτε τροποποιεί άμεσα το ρολόι του εικονικού μηχανήματος χωρίς κάποια προειδοποίηση ή ενημερώνει το λειτουργικό σύστημα του εικονικού μηχανήματος, ώστε αυτό να προβεί στη διόρθωση του χρόνου.

Ανεξάρτητα από το σε ποια εκ των δύο περιπτώσεων συγχρονισμού του χρόνου αναφερόμαστε, στην παρούσα διατριβή θεωρήσαμε την ορθότητα του χρόνου μέρος των αρχείων καταγραφής συμβάντων. Πιο συγκεκριμένα, όλα τα συμβάντα αλλαγής του ρολογιού καταχωρίζονται σε συγκεκριμένο αρχείο καταγραφής συμβάντων, το οποίο έχει δημιουργηθεί για αυτόν ακριβώς τον σκοπό.

9.4. Μελλοντική έρευνα

Με εφαλτήριο την παρούσα έρευνα θα μπορούσε να εξεταστεί το επόμενο βήμα, εάν δηλαδή μπορεί να καταστεί εφικτή η συσχέτιση των δύο επιμέρους τρόπων συγχρονισμού του ρολογιού στα εικονικά υπολογιστικά συστήματα. Θα πρέπει να απαντηθούν ερωτήματα όπως τι θα συμβαίνει αν οι χρόνοι των δύο πηγών είναι διαφορετικοί ή αν συνεχώς υπάρχει σοβαρή απόκλιση μεταξύ του πραγματικού χρόνου και του χρόνου που υπάρχει στο εικονικό μηχάνημα.

Μελλοντική έρευνα, επίσης, θα μπορούσε να γίνει σχετικά με τα αρχεία καταγραφής συμβάντων αναφορικά με τον τρόπο και τον τόπο αποθήκευσής τους. Κάτι τέτοιο δεν είναι εύκολο, διότι θα πρέπει να ληφθεί υπόψη η διασφάλιση της ακεραιότητας των αρχείων καταγραφής συμβάντων και ιδεατά να μην γίνεται από τον πάροχο.

Τέλος, μια καλή ιδέα θα ήταν η δημιουργία – πρόταση ενός νέου πρωτοκόλλου συγχρονισμού του ρολογιού, ειδικά για εικονικά συστήματα. Ενός πρωτοκόλλου δηλαδή, που θα είναι σε θέση να αντιλαμβάνεται ότι λειτουργεί σε εικονική μηχανή και όχι σε φυσική.

Κ Ε Φ Α Λ Α Ι Ο Δ Ε Κ Α Τ Ο

Αναφορές

10.1. Εισαγωγή

Κρίνεται σκόπιμο να επισημανθεί ότι αρκετές από τις παραπομπές αναφέρονται σε κείμενα διαδικτύου και καθώς το περιεχόμενο του διαδικτύου αλλάζει σε καθημερινή βάση, ενδέχεται κάποιοι από τους συνδέσμους να μην παραπέμπουν στα κείμενα που αναφέρονται.

10.2. Αναφορές

1. N. Marangos, P. Rizomiliotis and L. Mitrou, "Digital Forensics in the Cloud Computing Era". IEEE GC'12 Workshop: First International workshop on Management and Security technologies for Cloud Computing, 2012
2. N. Marangos, P. Rizomiliotis, and L. Mitrou, "Time Synchronization: Pivotal Element in Cloud Forensics". Secur. Commun. Networks, 2014.
3. J. W. Ross and G. Westerman, "Preparing for utility computing: The role of IT architecture and relationship management". IBM Syst J, 43 pp. 5-19, 2004
4. H. Madsen , B. Burtschy, G. Albeanu and Fl. Popentiu-Vladicescu, "Reliability in the utility computing era: towards reliable Fog computing". Proc. 20th international conference on systems, signals, and image processing (IWSSIP), p. 43–6, 2013
5. Gong, J. Liu, Q. Zhang, H. Chen and Z. Gong, "The characteristics of cloud computing". 39th International Conference on Parallel Processing Workshops (ICPPW), pp. 275–279, 2010
6. P. Mell and T. Grance, “The NIST Definition of Cloud Computing”. NIST Special Publication 800-145, 2011
7. M. Hauben, "History of ARPANET". Site de l’Instituto Superior de Engenharia do Porto, vol. 17, pp. 1-20, 2007
8. Amazon S3, “Amazon Simple Storage Service User Guide”. Amazon Web Services, 2023
9. S. Mathew and J. Varia, "Overview of amazon web services". Amazon Whitepapers, 2014
10. T. Makila, A. Jarvi, M. Ronkko and J. Nissila, "How to Define Software-as-a-Service – An Empirical Study of Finnish SaaS Providers". Software Business (P. Tyrvainen, S. Jansen and M. A. Cusumano) Springer, Berlin, Heidelberg, 115-124, 2010
11. P. V. Coveney, "Scientific grid computing". Philos Transact A Math Phys Eng Sci 363(1833):1707–1713, 2005
12. B. Reingold et al., "Cloud Computing: Whose Law Governs the Cloud? (Part III)". LegalWorks, 2010
13. C. Doyle, "The USA PATRIOT Act: A legal analysis". Washington, DC: Congressional Research Service, 2002

14. Richard Thompson II and P. Cole, "Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA)". Congressional Research Service, 2015
15. H. AlJahdali, A. Albatli, P. Garraghan, P. Townend, L. Lau and J. Xu, "Multi-tenancy in cloud computing". Service Oriented System Engineering (SOSE), IEEE 8th International Symposium On, 344–351 IEEE, 2014
16. S. Lehrig, H. Eikerling and S. Becker, "Scalability, elasticity, and efficiency in cloud computing: A systematic literature review of definitions and metrics". Proceedings of the International ACM SIGSOFT Conference on Quality of Software Architectures, pp. 83–92, 2015
17. Google, http://www.google.com, accessed on Feb 2023
18. IBM, https://www.ibm.com/gr-en, accessed on Feb 2023
19. http://2009.cloudcom.org/, accessed on Feb 2023
20. Yahoo, http://www.yahoo.com, accessed on Feb 2023
21. Microsoft, http://www.microsoft.com, accessed on Feb 2023
22. Gmail, https://gmail.google.com, accessed on Feb 2023
23. GroupWise, https://www.microfocus.com/en-us/products/groupwise/overview, accessed on Feb 2023
24. Microsoft Exchange, https://mail.exchange.microsoft.com, accessed on Feb 2023
25. P. Resnick, "Internet Message Format". RFC-2822, The Internet Society, 2001
26. Google Calendar, https://calendar.google.com/, accessed on Feb 2023
27. Google Docs, https://docs.google.com/, accessed on Feb 2023
28. Google Sites, https://sites.google.com/, accessed on Feb 2023
29. Google Voice, https://voice.google.com/, accessed on Feb 2023
30. Google Apps, https://https://apps.google.com/, accessed on Feb 2023
31. S. Aghaei, M. A. Nematbakhsh, H. K. Farsani, "Evolution of the www: From the web 1.0 to the web 4.0". International Journal of Web & Semantic Technology (IJWesT) Vol.3, No.1, January 2012
32. J. Nieh, N. Novik, S. J. Yang, "A Comparison of Thin-Client Computing Architectures". Technical Report CUCS-022-00, New York: Network Computing Laboratory, Columbia University, December 2005

33. Ορισμός του thick client, διαθέσιμος στο http://techterms.com/definition/thickclient, accessed on Feb 2023
34. Gartner, http://www.gartner.com/, accessed on Feb 2023
35. J. Forcier, P. Bissex and W. Chun, "Python Web Development with Django". PRENTICE HALL COMPUTER, 2009
36. J. Postel, "Transmission Control Protocol (TCP)" RFC-793, 1981
37. A. Freier, P. Karlton, P. Kocher, "The Secure Sockets Layer (SSL) Protocol Version 3.0". RFC-6101, 2011
38. R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee, "Hypertext Transfer Protocol". RFC-2616, 1999
39. L. Andersson, T. Madsen, "Provider Provisioned Virtual Private Network (VPN) Terminology". RFC-4026, 2005
40. D. Comer, "Computer Networks and Internets". σελίδα 99 ff, Prentice Hall 2008
41. B. Desmond et al, "Active Directory: Designing, Deploying, and Running Active Directory". O'Reilly Media, Inc., 2008
42. Microsoft Windows, https://www.microsoft.com/en-us/windows, accessed on Feb 2023
43. Amazon, http://www.amazon.com/, accessed on Feb 2023
44. OpenID E. Eldon, "Single sign-on service OpenID getting more usage". venturebeat.com.
45. Amazon SQS, http://aws.amazon.com/sqs/, accessed on Feb 2023
46. R. R. Perkoski, "Introduction to Web Development". The Wall Street Journal's Managing Your Career 7-8
47. T. Berners-Lee, D. Connolly, "Hypertext Markup Language (HTML) - 2.0". RFC-1866, 1995
48. J. J. Garrett, "Ajax: A New Approach to Web Applications". AdaptivePath.com, 2005
49. Django Foundation, https://www.djangoproject.com/foundation/, accessed on Feb 2023
50. Amazon EC2, http://aws.amazon.com/ec2/, accessed on Feb 2023
51. M. Collier and R. Shahan, "Microsoft Azure Essentials-Fundamentals of Azure". Microsoft Press Books, Pearson Education, 2015
52. Microsoft Azure, https://azure.microsoft.com/, accessed on Feb 2023

53. Force.com, "Force.com: A Comprehensive Look at the World's Premier Cloud-Computing Platform". Whitepaper on force.com cloud computing
54. B. De, "API documentation". API Management: An Architect's Guide to Developing and Managing APIs for Your Organization, Springer, pp. 59–80, 2017
55. T. Bray, J. Paoli, C. M. Sperberg-McQueen, E. Maler and F. Yergeau, "Extensible Markup Language (XML) 1.0 (Fifth Edition)". W3C Recommendation, 2008
56. I. Jacobs, N. Walsh, "URI/Resource Relationships". Architecture of the World Wide Web, Volume One. World Wide Web Consortium, 2004
57. Microsoft Edge, https://www.microsoft.com/en-us/edge, accessed on Feb 2023
58. Google Chrome, https://www.google.com/chrome/, accessed on Feb 2023
59. Mozilla Firefox, https://www.mozilla.org/en-US/firefox/new/, accessed on Feb 2023
60. Safari, https://www.apple.com/safari/, accessed on Feb 2023
61. A. Penenberg, "Cookie Monsters". https://slate.com/technology/2005/11/why-web-surfers-love-to-hate-cookies.html, accessed on Feb 2023
62. P. Saint-Andre, "Extensible Messaging and Presence Protocol (XMPP): Core". RFC-6120, 2011
63. Apple, https://www.apple.com/, accessed on Feb 2023
64. AOL, http://www.aol.com/, accessed on Feb 2023
65. LiveJournal, http://www.livejournal.com/, accessed on Feb 2023
66. E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3". IETF Internet Draft, draft-ietf-tls-tls13, 2018
67. Oracle Solaris, https://www.oracle.com/solaris/solaris11/, accessed on Feb 2023
68. I. Hickson and D. Hyatt, "HTML5". W3C Working Draft, 2011
69. B. Hoehrmann, "Scripting Media Types". RFC-4329, 2006
70. J. Gosling, and H. McGilton,"The Java Language Environment". Whitepaper, May 1996

71. R. Kumar and S. Charu, "An importance of using virtualization technology in cloud computing". Global J. Comput. Technol. 1(2), 2015
72. VMWare, https://www.vmware.com/, accessed on Feb 2023
73. AMD, https://www.amd.com/en-gb, accessed on Feb 2023
74. BEA Systems, http://www.baesystems.com/home, accessed on Feb 2023
75. BMC Software, https://www.bmc.com/, accessed on Feb 2023
76. BroadCom, https://www.broadcom.com/, accessed on Feb 2023
77. Cisco, https://www.cisco.com/, accessed on Feb 2023
78. Dell, https://www.dell.com/, accessed on Feb 2023
79. HP, https://www.hp.com/us-en/home.html, accessed on Feb 2023
80. Intel, https://www.intel.com/content/www/us/en/homepage.html, accessed on Feb 2023
81. RedHat, http://www.redhat.com/en, accessed on Feb 2023
82. VMware, "VMware Infrastructure Architecture Overview". Whitepaper, 2008.
83. VMware Community Source, https://news.vmware.com/releases/community_source, accessed on Feb 2023
84. Διαθέσιμο στο: https://old.gigaom.com/2014/08/19/where-in-the-world-is-vmware-co-founder-diane-greene-here-are-some-hints/, accessed on Feb 2023
85. Z. Aalam, V. Kumar, and S. Gour, S. "A review paper on hypervisor and virtual machine security". Journal of Physics: Conference Series (Vol. 1950, No. 1, p. 012027), IOP Publishing, 2021
86. D. Revelle, "Hypervisors and Virtual Machines Implementation Insights on the x86 Architecture". login: VOL. 36, NO. 5,2011
87. Sun Microsystems, "Introduction to Cloud Computing architecture". Whitepaper, 1st Edition, 2009
88. VMware, "Understanding Full Virtualization, Paravirtualization, and Hardware Assist". Whitepaper, 2007
89. S. Crosby, R. Doyle, M. Gering, M. Gionfriddo, S. Grarup, S. Hand, M. Hapner, D. Hiltgen, M. Johanssen, L. J. Lamers, J. Leung, F. Machida, A. Maier, E. Mellor, J. Parchem, S. Pardikar, S. J. Schmidt, R. W. Schmidt, A. Warfield, M. D. Weitzel, and J. Wilson, "Open

Virtualization Format Specification (OVF)". Technical Report DSP0243, Distributed Management Task Force, Inc., 2009
90. W3C, https://www.w3.org/community/cloud/, accessed on Feb 2023
91. Z. Shelby, "Constrained RESTful Environments (CoRE) Link Format". RFC-6690, 2012
92. D. Box, D. Ehnebuske, G. Kakivaya, A. Layman, N. Mendelsohn, H. F. Nielsen, S. Thatte, D. Winer, "Simple Object Access Protocol (SOAP) 1.1". W3C Note, W3C, 2000
93. T. Bray, "The JavaScript Object Notation (JSON) Data Interchange Format". RFC-7159, 2014
94. A. Chaudhri, R. Zicari, and A. Rashid, "XML Data Management: Native XML and XML Enabled DataBase Systems". Addison-Wesley Longman, 2003
95. R. T, Fielding, "Architectural Styles and the Design of Network-based Software Architectures". PhD Thesis, University of California, Irvine, 2000
96. Ubuntu Linux, httpσ://www.ubuntu.com/, accessed on Feb 2023
97. Microsoft Office, https://www.office.com/, accessed on Feb 2023
98. M. Garai, S. Rekhis, and N. Boudriga, "Communication as a Service for Cloud VANETs". 20th IEEE Symposium on Computer and Communications (ISCC'15), IEEE, 2015
99. K. A. Jamsa, "Cloud Computing". Burlington, MA: Jones & Bartlett Publishers, 2022
100. J. W. Rittinghouse and J. F. Ransome, "Cloud Computing: Implementation, Management, and Security". Boca Raton, FL, USA: CRC Press, 2017
101. DARPA Internet Program, "Internet Protocol". Protocol Specification, RFC-791, 1981.
102. R. Jain, "Voice over IP". The Ohio State University, 2003
103. S. Aggarwal, G. Mohr and J. Vincent, "Instant Messaging / Presence Protocol Requirements". RFC-2779, 2000
104. R. Even, N. Ismail, "Conferencing Scenarios". RFC-4597, 2006
105. M. Jelassi, C. Ghazel, and L. A. Saïdane, "A survey on quality of service in cloud computing". Proc. 3rd Int. Conf. Frontiers Signal Process. (ICFSP), pp. 63–67, 2017

106. D. Serrano, S. Bouchenak, Y. Kouki, F. A. de Oliveira Jr, T. Ledoux, J. Lejeune, and P. Sens, "SLA guarantees for cloud services". Future Generation Computer Systems, 2015
107. G. E. Moore, "Cramming more components onto integrated circuits". Electronics Magazine, 1965
108. N. Serrano, G. Gallardo and J. Hernantes, "Infrastructure as a service and cloud technologies". Softw. IEEE 32 (2)30–36, 2015
109. G. Blokdyk , "Infrastructure As A Service IaaS A Complete Guide". Book, 5STARCooks, 2021
110. B. Beach, "Amazon Machine Images". Pro Powershell for Amazon Web Services, pp. 115-134. Apress, 2019
111. Amazon SimlpeDB, https://aws.amazon.com/simpledb/, accessed on Feb 2023
112. H. Tang and Z. Mei, "A simple methodology for database clustering". Proc. 5th Int. Conf. Comput. Eng. Netw., p. 019, 2015
113. Amazon SQS, https://aws.amazon.com/sqs/, accessed on Feb 2023
114. Amazon CloudFront, http://aws.amazon.com/cloudfront/, accessed on Feb 2023
115. Amazon Elastic Block Store, https://aws.amazon.com/ebs/, accessed on Feb 2023
116. P. Srisuresh, M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations". RFC-2663
117. M. J. Kavis, "Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS)". John Wiley and Sons, 2014
118. M. Vielberth, F. Bhm, I. Fichtinger and G. Pernul, "Security Operations Center: A Systematic Study and Open Challenges". IEEE Access, 8, 227756–227779, 2020
119. eBay, https://www.ebay.com/, accessed on Feb 2023
120. iTunes, https://www.apple.com/itunes/, accessed on Feb 2023
121. YouTube, https://www.youtube.com, accessed on Feb 2023
122. N. Niknejad, W. Ismail, I. Ghani, B. Nazari, M. Bahari, and A. R. B. C. Hussin, "Understanding service-oriented architecture (SOA): A systematic literature review and directions for further investigation". Inf. Syst. 91, 101–491, 2020
123. International Data Corporation, https://www.idc.com/, accessed on Feb 2023

124. ASP.NET, https://dotnet.microsoft.com/en-us/apps/aspnet, accessed on Feb 2023
125. J. R. Vacca, "Cloud Computing Security: Foundations and Challenges". CRC Press, ch-15, 2020
126. S. Carlin and K. Curran, "Cloud Computing Security". International Journal of Ambient Computing and Intelligence, 3(1):38–46, 2013
127. A. Ramdas and R. Muthukrishnan, "A Survey on DNS Security Issues and Mitigation Techniques". Proceedings of the International Conference on Intelligent Computing and Control Systems (ICCS), Madurai, India, pp. 781–784, 2019
128. Google Cloud Platform, https://cloud.google.com/, accessed on Feb 2023
129. C. Dotson, "Practical Cloud Security A Guide for Secure Design and Deployment". O'REILLY, 2019
130. L. Jie and F. Fawzi, "Research About Attacks Over Cloud Environment", International Journal of Scientific & Technology Research, Volume 6, issue 01, ISSN 2277-8616, 2017
131. A. Calder and S. Watkins, "IT Governance: an international guide to data security and ISO27001/ISO27002". Kogan Page Publishers, 2015
132. J. A. Kappel, A. Velte and Toby Velte, "Microsoft Virtualization with Hyper-V: Manage Your Datacenter with Hyper-V, Virtual PC, Virtual Server, and Application Virtualization". McGraw Hill Professional, 2009
133. Kloxo, https://kloxong.org/, accessed on Feb 2023
134. J. Lv, Y. Wang, J. Su, R. Chen and W. Wu "Security of auditing protocols against subversion attacks". Int. J. Found. Comput. Sci., vol. 31, no. 2, pp. 193–206, 2020
135. J. Rutkowska and A. Tereshkin, "Bluepilling the xen hypervisor". Black Hat USA, 2008
136. PHP, https://php.net/, accessed on Feb 2023
137. .NET, https://dotnet.microsoft.com/en-us/, accessed on Feb 2023
138. Ruby on Rails, https://rubyonrails.org/, accessed on Feb 2023
139. Python Software Foundation, "Python 3.4.3". 2015
140. SANS, https://www.sans.org/, accessed on Feb 2023
141. O. Osanaiye, K. Kr. Choo and M. Dlodlo, "Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud DDoS mitigation framework". J Netw Comput Appl 67:147–165, 2017

142. F.Z. Chowdhury, L.B.M. Kiah, M.A.M. Ahsan and M.Y.I.B. Idris, "Economic denial of sustainability (EDoS) mitigation approaches in cloud: analysis and open challenges". Proc. of Intl. Conf. on Electrical Engineering and Computer Science, pp. 206-211, 2017
143. K. Finklea, "Dark Web". Congressional Research Service CRS Report, 2017
144. P Mell, K Scarfone, S Romanosky, "Common vulnerability scoring system". Security & Privacy, IEEE, 2006
145. D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, "The Eucalyptus open-source cloud-computing system". In CCA ’08, 2009
146. Apex, https://apex.oracle.com/en/, accessed on Feb 2023
147. SalesForce.com, http://www.salesforce.com/eu/?ir=1, accessed on Feb 2023
148. P. Mishra et al, "Differences between OASIS Security Assertion Markup Language (SAML) V1.1 and V1.0 ". OASIS, 2003
149. B. S. Blanchard, W. J. Fabrycky, "Systems engineering and analysis (4th ed.)". New Jersey: Prentice Hall, 2006
150. Sun Microsystems, "Sun OpenSSO Enterprise 8.0 Technical Overview". Technical Specification, 2009
151. A. Shuiaat, "Introduction to Oracle Identity And Access Management (IAM)". ORACLE presentation, 2010
152. Ping Identity, https://www.pingidentity.com/en.html, accessed on Feb 2023
153. Symplified, http://symplifiedtech.com/, accessed on Feb 2023
154. P. Ford-Hutchinson, "Securing FTP with TLS". RFC-4217, 2005
155. J. Pechanec, "How the SCP protocol works". Jan Pechanec's weblog, 2010
156. S. Skorobogatov, "Data Remanence in Flash Memory Devices". Cryptographic Hardware and Embedded Systems Workshop (CHES 2005), LNCS, Vol. 3659, Springer-Verlag, pp 339–353, 2005
157. R. Kissel, M. Scholl, S. Skolochenko and X. Li, "NIST SP800-88 guidelines for media sanitization". NIST Special Publication 88, 2006
158. Carbonite, https://www.carbonite.com , accessed on Feb 2023
159. K. Valmik, M. Neha, and V. K. Kshirsagar, "Blowfish Algorithm". IOSR Journal of Computer Engineering (IOSR-JCE) 16.2, 2014

160. S. Kelly, "Security Implications of Using the Data Encryption Standard (DES)". RFC-4772, 2006
161. U. Blumenthal, F. Maino, K. McCloghrie, "The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model". RFC-3826, 2004
162. NIST, https://www.nist.gov/, accessed on Feb 2023
163. P. Gutmann, "Using Message Authentication Code (MAC) Encryption in the Cryptographic Message Syntax (CMS)". RFC-6476, 2012
164. NIST Computer Security Division's (CSD) Security Technology Group (STG), "Block cipher modes". Cryptographic Toolkit, NIST, 2013
165. C. Paar, J. Pelzl, "11: Hash Functions". Understanding Cryptography, A Textbook for Students and Practitioners, Springer, 2009
166. A. Scott, "Turning out the lights - Coghead". The Wall Street Journal, 2009
167. C. J. Millard, "Cloud Computing Law". London, U.K.: Oxford Univ. Press, 2021
168. H. Hourani, and M. Abdallah, "Cloud Computing: Legal and Security Issues". 8th International Conference on Computer Science and Information Technology (CSIT) (pp. 13-16), 2018
169. J. Kerr and K. Teng, "Cloud computing: legal and privacy issues". Journal of Legal Issues and Cases in Business, Vol. 1 No. 1, pp. 1-11, 2012
170. K. K. R. Choo, "Legal issues in the cloud". IEEE Cloud Comput., vol. 1, no. 3, pp. 94–96, 2014
171. Ορισμός της αποζημίωσης, https://el.thefreedictionary.com/, accessed on Feb 2023
172. E. Sweden, "Capitals in the Clouds Part III – Recommendations for Mitigating Risks: Jurisdictional, Contracting and Service Levels". NASCIO Cloud Computing Series, 2012
173. D. R. Rani and P. L. Sravani, "Challenges of digital forensics in cloud computing environment". Indian J. Sci. Technol., vol. 9, no. 17, pp. 90–100, 2016
174. G. Palmer, "A Road Map for Digital Forensic Research", Report from the First Digital Forensic Research Workshop, DFRWS Technical Report, DTR-T001-01 FINAL, Air Force Research Laboratory, Rome, New York, 2001

175. J. Liu, Q. Zhang, H. Chen, Z. Gong "The Characteristics of Cloud Computing". 39th International Conference on Parallel Processing Workshops, 2010
176. K. Ruan, J. Carthy, T. Kechadi, M. Crosbie, "Cloud Forensics". Chapter 3, Advances in Digital Forensics VII IFIP Advances in Information and Communication Technology Volume 361, pp 35-46, 2011
177. Google App Engine, https://cloud.google.com/appengine/, accessed on Feb 2023
178. E. McCallister, T. Grance, K. Scarfone, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)". NIST Special Publication, 2010
179. K. Irion, "Government Cloud Computing and National Data Sovereignty". Policy & Internet 4 (3–4), 40–71, 2012
180. B. Carrier and E. Spafford, “Getting physical with the digital investigation process”. International Journal of Digital Evidence, vol. 2(2), 2003
181. L. Badger, R. Bohn, S. Chu, M. Hogan, F. Liu, V. Kaufmann, J. Mao, J. Messina, K. Mills, A. Sokol, J. Tong, F. Whiteside, D. Leaf, "U.S. Government Cloud Computing Technology Roadmap”. Volume II, Release 1.0 (Draft), Useful Information for Cloud Adopters, NIST Special Publication 500-293, National Institute of Standards and Technology, Gaithersburg, Maryland, 2011
182. R. Lu, X. Lin, X. Liang, X. Shen, “Secure provenance: The essential of bread and butter of data forensics in cloud computing”. Proceedings of the Fifth ACM Conference on Computer and Communications Security, pp. 282-292, 2010
183. B. Lee, A. Awad and M. Awad, "Towards secure provenance in the cloud: A survey". Proc. IEEE/ACM 8th Int. Conf. Utility Cloud Comput. (UCC), pp. 577–582, 2015
184. D. Garrie, “Cloud computing and jurisdiction, Part 2: A primer”. Law and Forensics, Seattle, Washington (www.lawandforensics.com/ cloud-computing-jurisdiction-part-primer), 2012
185. Association of Chief Police Officers, "Good Practice Guide for Computer-Based Evidence". London, United Kingdom, 2012
186. J. Vacca, "Computer Forensics: Computer Crime Scene Investigation". Charles River Media, Hingham, Massachusetts, 2005

187. G. J. Mirobi and L. Arockiam, "Service level agreement in cloud computing: An overview". Proceedings of the 2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), pp. 753–758, 2015
188. W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing". NIST Special Publication 800-144, National Institute of Standards and Technology, Gaithersburg, Maryland, 2011
189. T. Ristenpart, E. Tromer, H. Schacham, S. Savage, “Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds”. Proceedings of the Sixteenth ACM Conference on Computer and Communications Security, pp 199–212, 2009
190. D. Birk, C. Wegener, “Technical issues of forensic investigations in cloud computing environments”. Proceedings of the Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, 2011
191. A. Haeberlen, “A case for the accountable cloud”. ACM SIGOPS Operating Systems Review, vol. 44(2), pp. 52–57, 2010
192. Y. Wen, X. Man, K. L and W. Shi, "Forensics-as-a-Service (FaaS): computer forensic workflow management and processing using cloud". Cloud Computing 2013, The Fourth International Conference on Cloud Computing, GRIDs, and Virtualization, 2013
193. NIST, "NIST Cloud Computing Standards Roadmap". NIST, 2013
194. R. Gerhards, "The Syslog Protocol", RFC-5424, 2009
195. E. Kenneally , "Digital logs – proof matters". Digital Investigation 2004, 1(2): 94–101. 2004
196. A. R. Arasteh, M. Debbabi, A. Sakha, M. Saleh, “Analyzing multiple logs for forensic evidence”. Digital Investigation, 4, 82–91, 2007
197. M. Saleh, A. R. Arasteh, A. Sakha, M. Debbabi, “Forensic analysis of logs: modeling and verification”. Knowledge-Based Systems, 671–682, 2007
198. D. Takahashi, Y. Xiao, “Complexity analysis of retrieving knowledge from auditing log files for computer and network forensics and accountability”. Proc. of IEEE ICC ‘08, 1474–1478, 2008
199. D. V. Forte, "The art of log correlation". Proceedings of the Information Security South Africa (ISSA), Enabling Tomorrow Conference 2004

200. R. Marty, "Cloud application logging for forensics". Symposium on Applied Computing ACM ‘11, TaiChung, Taiwan, 2011
201. Amazon SolarWinds LogAnalyzer, https://aws.amazon.com/marketplace/pp/prodview-7nox6la4i3f42, accessed on Feb 2023
202. R. K. L. Ko, P. Jagadpraman, B. S. Lee, "Flogger: a file-centric logger for monitoring file access and transfers within cloud computing environments". HP Labs Singapore,Tech. Rep., HPL-2011-119, 2011
203. S. Zawoad, A. K. Dutta, R. Hasan, "SecLaaS: secure logging-as-a-service for cloud forensics". Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, Asia CCS ’13,219–230, 2013
204. W. Wongthai, F. L. Rocha, A. V. Moorsel, "A generic logging support architecture for infrastructure as a service (IaaS) cloud". School of Computing Science, University of Newcastle upon Tyne, 2012
205. S. P. Peisert, "A model of forensic analysis using goaloriented logging". PhD thesis, Department of Computer Science and Engineering, University of California, San Diego, 2007
206. P. Balboni, E. Pelino, "Law enforcement agencies’ activities in the cloud environment: a European legal perspective". Information & Communications Technology, 22(2): 165–190, 2013
207. W. Zhou W, M. Sherr M, W. R. Marczak WR et al., "Towards a data centric view of cloud security". 2nd International Workshop on Cloud Data Management, 25–32, 2010
208. D. Kelley, "How data-centric protection increases security in cloud computing and virtualization". Security Curve, 2011
209. R. K. L. Ko, P. Jagadpramana, M. Mowbray, et al. "TrustCloud - a framework for accountability and trust in cloud computing". Proc. IEEE 2nd Cloud Forum for Practitioners, (IEEE ICFP ‘11), IEEE Computer Society, 1–5, 2011
210. R. K. L. Ko, B. S. Lee, S. Pearson, "Towards achieving accountability, auditability and trust in cloud computing". Proc. International workshop on Cloud Computing: Architecture, Algorithms and Applications (CloudComp2011) Athens, Greece, Springer, pp. 5, 2011
211. R. Accorci, "Safekeeping digital evidence with secure logging protocols state of the art and challenges". Proceedings IMF ‘09, 94–110, 2009

212. K. Kent, M. Souppaya, "Guide to computer security log management". Recommendations of the National Institute of Standards and Technology, 2006
213. B. Schneier, J. Kelsey, "Secure audit logs to support computer forensics". ACM Transactions on Information and System Security (TISSEC), 2(2): 159–176, 1999
214. D. Mills, U. Delaware, J. Martin, J. Burbank, W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification". RFC-5905, 2010
215. Microsoft Team, "Windows Time Service Technical Reference". Microsoft, 2011
216. M. Karyda, L. Mitrou, "Internet forensics: legal and technical issues". Digital Forensics and Incident Analysis, WDFIA 2007. Second International Workshop on. IEEE, 3–12, 2007
217. M. Taylor, J. Haggerty, D. Gresty, D. Lamb, "Forensic investigation of cloud computing systems". Network Security 2011; 4–10, 2011
218. D. Reilly, C. Wren, T. Berry, "Cloud computing: forensic challenges for law enforcement". Internet Technology and Secured Transactions (ICITST), 2010 International Conference for IEEE, 1–7, 2010
219. G. Grispos, T. Storer, W. B. Glisson, "Calm before the storm: the challenges of cloud". Emerging Digital Forensics Applications for Crime Detection, Prevention, and Security, 4: 28–48, 2013
220. K. Ruan, I. Baggili, J. Carthy, T. Kechadi, "Survey on cloud forensics and critical criteria for cloud forensic capability: a preliminary analysis". Proceedings of the 2011 ADFSL Conference on Digital Forensics, Security and Law, 2011
221. C. W. Adams "Legal issues pertaining to the development of digital forensic tools". Systematic Approaches to Digital Forensic Engineering, SADFE'08. Third International Workshop on. IEEE, 123–132, 2008
222. M. G. Porcedda, "Law enforcement in the clouds: is the EU data protection legal framework up to the task?". European Data Protection: In Good Health? Gutwirth S, Leenes R, De Hert P, Poullet Y (eds). Springer, 203–232, 2012
223. C. Hooper, B. Martini, K. K. C. Raymond, "cloud computing and its implications for cybercrime investigations". Australia Computer Law & Security Review, 29(2): 152–163, 2013

224. C. Boyd, P. Forster, "Time and date issues in forensic computing – a case study". Digital Investigation, 1: 18–23, 2004
225. S. Biggs, S. Vidalis, "Cloud computing: the impact on digital forensic investigations". Paper presented at the 4th International Conference for Internet Technology and Secured Transactions, London, United Kingdom, 2009
226. StackOverFlow, "How do I establish clock synchronization in the cloud (AWS, heroku, etc) across many nodes?". StackOverFlow, 2012
227. D. Mills, "Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI". RFC-4330, 2006
228. T. Broomhead, L. Cremean, J. Ridoux, D. Veitch, "Virtualize everything but time". Proc. OSDI '10, Vancouver, Canada, 2010
229. Timekeeping in VMware virtual machines. Information guide, VMWARE, 2010
230. B. Armstrong, "Time synchronization in hyper-V". Ben Armstrong Virtualization Blog, 2010
231. "KVM guest timing management". Fedora Documentation, Chapter 17
232. Para-virtualized devices, "Virtualization Getting Started Guide". RedHat Product Documentation
233. S. Rodrigues, "IEEE 1588 and synchronous Ethernet in telecom". Proceedings of the IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication ISPCS 2007, Gaderer G, Lee K (eds). IEEE: Vienna, Austria, 138–142, 2007
234. S. Simou, C. Kalloniatis, S. Gritzalis, and H. Mouratidis, "A survey on cloud forensics challenges and solutions". Security and Communication Networks, vol. 9, no. 18, pp. 6285-6314, 2016
235. B. Manral, G. Somani, K. R. Choo, M. Conti and M. S. Gaur, "A systematic survey on cloud forensics challenges, solutions, and future directions". ACM Comput. Surv. 52, 6, 124:1–124:38, 2020
236. S. Simou, C. Kalloniatis, S. Gritzalis, and V. Katos, "A framework for designing cloud forensic-enabled services (CFeS)". Requirements Eng., vol. 24, no. 3, pp. 403–430, 2019
237. S. Simou, C. Kalloniatis, S. Gritzalis, and V. Katos, "A revised forensic process for aligning the investigation process with the design of forensic-enabled cloud services". in S. Katsikas and V. Zorkadis,

(Eds.): E-Democracy – Safeguarding Democracy and Human Rights in the Digital Age, Cham, Springer; pp.161–177, doi: 10.1007/978-3-030-37545-4_11, 2020