ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

" Cloud Computing εφαρμογές μελλοντικής χρήσης και ασφάλεια δεδομένων "

Επιμέλεια / Συγγραφή

Δημήτρης Κόνσουλας ΑΜ: 0728

Επιβλέπων Καθηγητής

Βασίλης Τσακανίκας

Καθηγητής του Τμήματος Μηχανικών Πληροφορικής Τ.Ε. του ΑΤΕΙ Δυτικής Ελλάδας

ΑΝΤΙΡΡΙΟ, ΙΟΥΝΙΟΣ 2017

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

Αντίρριο, _ _ / _ _ / _ _ _ _

1. [Ονοματεπώνυμο, Υπογραφή]

2. [Ονοματεπώνυμο, Υπογραφή]

3. [Ονοματεπώνυμο, Υπογραφή]

Περίληψη

Το cloud computing ή αλλιώς on-demand computing (υπολογισμοί κατ' απαίτηση) είναι ένα είδος υπολογισμού βασισμένο στο Διαδίκτυο που παρέχει κοινούς επεξεργαστικούς πόρους και δεδομένα σε υπολογιστές και άλλες συσκευές κατ' απαίτηση.

Οι εφαρμογές του cloud computing χρησιμοποιούνται από εκατομμύρια ανθρώπους καθημερινά, σε πάρα πολλούς τομείς: από την ανάπτυξη εφαρμογών και προγραμμάτων σε εταιρίες παραγωγής λογισμικού μέχρι στα σχολεία και νοσοκομεία για εισαγωγή στοιχείων και προβολή αποτελεσμάτων σε μαθητές και ασθενείς αντίστοιχα.

Με την επεξεργασία σημαντικών δεδομένων όπως τα παραπάνω, αυξήθηκε η ασφάλεια στις εφαρμογές cloud computing. Χρησιμοποιώντας σύγχρονες μεθόδους ασφάλειας, όπως είναι η αναγνώριση χρηστών με βιομετρικούς τρόπους και η χρήση κρυπτογράφησης, τα δεδομένα των χρηστών πλέον είναι πιο ασφαλή.

Για περαιτέρω προστασία των δεδομένων των χρηστών δημιουργήθηκε ειδική νομοθεσία για δεδομένα που βρίσκονται στο cloud και που μπορούν να χρησιμοποιηθούν από οποιοδήποτε μέρος του κόσμου.

Abstract

Cloud computing or on-demand computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand.

Cloud computing applications are used by millions of people every day, in many areas: from developing applications and programs to software companies up to schools and hospitals to import data and deliver results to students and patients respectively.

By processing important data like the above, security has increased in cloud computing applications. Using modern security methods such as user identification with biometrics and the use of encryption, user data is now safer.

To further protect users' data, specific legislation has been created for cloud-based data that can be used anywhere in the world.

Περιεχόμενα

1. Ιστορική Αναδρομή

1.1 Εισαγωγή

Το cloud computing είναι ένας συνδυασμός τεχνολογιών και υπηρεσιών που προϋπήρχαν εδώ και δεκαετίες, από την δεκαετία του 1950, αλλά από τις αρχές του 2000, βλέπουμε να αξιοποιούνται και να προσφέρουν ικανοποιητικές ή και καλύτερες λύσεις στα προβλήματα των τελικών χρηστών, σε σχέση με άλλες υπηρεσίες. Σε αυτό το κεφάλαιο λοιπόν θα εξετάσουμε την ιστορική εξέλιξη του cloud computing και των τεχνολογιών από το οποίο αποτελείται και θα μάθουμε τι ακριβώς σημαίνει ο όρος cloud computing. (Cloud Computing 2016)

1.2 Ορισμός Cloud Computing

Το cloud computing ή αλλιώς on-demand computing (υπολογισμοί κατ' απαίτηση) είναι ένα είδος υπολογισμού βασισμένο στο Διαδίκτυο που παρέχει κοινούς επεξεργαστικούς πόρους και δεδομένα σε υπολογιστές και άλλες συσκευές κατ' απαίτηση. Είναι ένα μοντέλο που μπορεί και προσφέρει αδιάκοπα τις υπηρεσίες του, οπουδήποτε και να βρίσκεται ο χρήστης, έχοντας πρόσβαση σε μια κοινή ομάδα επεξεργαστικών πόρων (π.χ. δίκτυα, διακομιστές, αποθηκευτικό χώρο, εφαρμογές και υπηρεσίες) που μπορούν να δεσμευτούν και να αποδεσμευτούν αστραπιαία με ελάχιστη διαχείριση. Οι υπηρεσίες cloud computing και αποθήκευσης δεδομένων επιτρέπουν στους χρήστες και στις επιχειρήσεις να αποθηκεύσουν και να επεξεργαστούν τα δεδομένα τους σε data centers (κέντρα δεδομένων) τρίτων επιχειρήσεων. Στηρίζεται στο διαμοιρασμό πόρων για να έχει συνοχή και μειωμένο κόστος, όπως για παράδειγμα έχει το ηλεκτρικό δίκτυο.

Η προέλευση του όρου cloud computing είναι άγνωστη. Μπορεί να προέρχεται από τον όρο cloud που χρησιμοποιείται στην επιστήμη για να περιγράψει μια μεγάλη ομάδα αντικειμένων που από μακριά μοιάζουν με σύννεφο και οι λεπτομέρειες τους είναι κρυμμένες ή δεν έχουν ερευνηθεί. Μια δεύτερη εξήγηση του όρου μπορεί να προέρχεται από παλιά προγράμματα υπολογιστών που κατέβαζαν σχηματικές αναπαραστάσεις δικτύων, τα οποία συμβόλιζαν τους

servers (διακομιστές) με κύκλο. Μια ομάδα διακομιστών αποτελούνταν από κύκλους ο ένας πάνω από τον άλλο, μοιάζοντας με σύννεφο. (Cloud Computing 2016)

1.3 Η δεκαετία του 1950

Η ιστορία του cloud computing ξεκινάει πίσω στο μακρινό 1950, όταν οι άνθρωποι τότε δούλευαν σε χαζά τερματικά συνδεδεμένα σε ένα κεντρικό υπολογιστή. Η μόνη λειτουργία αυτών των τερματικών, ήταν να προσφέρουν πρόσβαση στον κεντρικό υπολογιστή, αλλά δεν ήταν πρακτικό. Δεν ήταν εφικτό για καμία επιχείρηση της εποχής να παρέχει ξεχωριστό υπολογιστή σε κάθε υπάλληλο, λόγω της υψηλής τιμής τους και συντήρησης τους. Επιπροσθέτως, η επεξεργαστική ισχύς και ο μεγάλος αποθηκευτικός χώρος του κεντρικού υπολογιστή δεν γίνονταν απευθείας διαθέσιμα στους χρήστες. Η λύση σε αυτό το πρόβλημα, ήταν η κοινή χρήση των πόρων του συστήματος. Η μέθοδος που χρησιμοποιήθηκε για την κοινή χρήση ήταν το time-sharing (καταμερισμός χρόνου).

Το σημερινό cloud computing μοιάζει πάρα πολύ με το παραπάνω μοντέλο. Τα τερματικά αντιστοιχούν στις συσκευές που χρησιμοποιούμε σήμερα (υπολογιστές, κινητά κ.ά.) και ο κεντρικός υπολογιστής αντιστοιχεί στη κεντρική πλατφόρμα του cloud. Και τα δύο κεντρικά συστήματα χειρίζονται από μια ομάδα που διαχειρίζονται την ασφάλεια, τους λογαριασμούς των χρηστών, τα αντίγραφα ασφαλείας, τις ενημερώσεις του συστήματος και την εξυπηρέτηση των χρηστών. (History of Cloud Computing 2016)

1.4 Η δεκαετία του 1960

Το 1969 ο J.C.R. Licklider, ένας Αμερικανός επιστήμονας υπολογιστών ανέπτυξε το ARPANET (Advanced Research Projects Agency Network), τον πρόγονο του σημερινού μας Διαδικτύου. Το όραμα του δημιουργού ήταν «όλοι οι άνθρωποι στον πλανήτη να είναι διασυνδεδεμένοι και να έχουν πρόσβαση σε προγράμματα και δεδομένα σε οποιαδήποτε ιστοσελίδα, από οποιοδήποτε μέρος». Το ARPANET ήταν μέρος ενός προγράμματος του Υπουργείου Αμύνης των Ηνωμένων

Πολιτειών της Αμερικής και ο σκοπός του ήταν η επικοινωνία και η κοινή χρήση υπολογιστικών πόρων, μεταξύ επιστημόνων σε συνδεδεμένα πανεπιστήμια και οργανώσεις με το δίκτυο. Τα δεδομένα στέλνονταν σε μικρά κομμάτια που ονομάζονταν πακέτα, τα οποία δρομολογούνταν μέσα στο δίκτυο, σε διαφορετικά μονοπάτια και συναρμολογούνταν ξανά στον προορισμό τους. (The evolution of cloud computing 2016)

1.5 Η δεκαετία του 1970

Τη δεκαετία αυτή γεννήθηκε η ιδέα των virtual machines – vm (εικονικές μηχανές). Η δημιουργία του VM λειτουργικού συστήματος από την IBM, κατέστησε δυνατή την λειτουργία πολλών λειτουργικών συστημάτων ταυτόχρονα, χρησιμοποιώντας ένα απομονωμένο περιβάλλον. Έτσι κατάφεραν να τρέξουν δύο εντελώς διαφορετικά λειτουργικά συστήματα, σε ένα υλικό υπολογιστή. Το vm θεωρείται ως η εξέλιξη της κοινής χρήσης ενός κεντρικού υπολογιστή μέσω τερματικών του 1950 και λειτούργησε σαν καταλύτης για την πρόοδο των τεχνολογιών των υπολογιστών και των τηλεπικοινωνιών. (History of Cloud Computing 2016)

1.6 Η δεκαετία του 1990

Με την εξέλιξη του vm και την αύξηση του εύρους ζώνης, ορισμένες εταιρίες τηλεπικοινωνιών άρχισαν να προσφέρουν ιδιωτικές εικονικές συνδέσεις δικτύου (VPN –virtual private networks) στους χρήστες τους. Πριν το vm, πρόσφεραν γραμμές δικτύου από χρήστη σε χρήστη. Οι καινούριες ιδιωτικές συνδέσεις, πρόσφεραν ένα εικονικό δίκτυο που παρείχε υπηρεσίες χαμηλού κόστους παρόμοιες με εκείνες των γραμμών από χρήστη σε χρήστη. Οι εταιρίες ήταν ικανές να προσφέρουν κοινή χρήση στην υποδομή του δικτύου τους, για να μπορούν να εξυπηρετούν περισσότερους χρήστες, χωρίς να κατασκευάσουν νέες υποδομές. Αυτή η αλλαγή έδωσε στις εταιρίες την δυνατότητα να αλλάζουν την τηλεπικοινωνιακή κίνηση στο δίκτυο για να είναι ισορροπημένο, χωρίς συμφορήσεις και πέτυχαν καλύτερο έλεγχο στην διαχείριση του εύρους ζώνης. Έτσι ο αριθμός των συνδεδεμένων υπολογιστών που μοιράζουν δεδομένα με μεγάλες ταχύτητες αυξήθηκε, οδηγώντας στο σημερινό Διαδίκτυο. (History of Cloud Computing 2016)

Σε αυτά τα αρχικά στάδια του cloud computing, ο όρος cloud αντιπροσώπευε τον υπολογιστικό χώρο μεταξύ του παρόχου και του τελικού χρήστη. Το 1997 όμως, ο καθηγητής Ramnath Chellapa του πανεπιστημίου Emory και του πανεπιστημίου της Νότιας Καλιφόρνιας, όρισε για πρώτη φορά το cloud computing «ως ένα υπολογιστικό μοντέλο που τα όρια του θα καθοριστούν από οικονομικούς λόγους, παρά από τεχνικά όρια μόνο».

Κατά τη διάρκεια του δεύτερου μισού της δεκαετίας, οι εταιρίες άρχισαν να καταλαβαίνουν καλύτερα το cloud computing και την χρησιμότητα του στο να προσφέρει ανώτερες λύσεις και υπηρεσίες στους καταναλωτές. Το 1999 η εταιρία Salesforce.com, έγινε μια από τις πρώτες εταιρίες που δραστηριοποιήθηκε στο χώρο, προσφέροντας καινοτόμες λύσεις εταιρικού επιπέδου σε τελικούς χρήστες μέσω του Διαδικτύου. (The History of Cloud Computing_2 2016)

1.7 Η δεκαετία του 2000

Μετά την επιτυχία της εταιρίας Salesforce.com, η προσοχή του τεχνολογικού κόσμου στράφηκε στο cloud computing. Το 2002 η γνωστή εταιρία ηλεκτρονικού εμπορίου, Amazon εγκαινίασε το Amazon Web Services, το οποίο πρόσφερε μια σουίτα υπηρεσιών cloud, μαζί με αποθηκευτικό χώρο και τεχνητή νοημοσύνη. Το 2006 διέθεσε στο κοινό το Elastic Compute Cloud (EC2), μια υπηρεσία που νοίκιαζε υπολογιστές σε μικρές εταιρίες και ελεύθερους επαγγελματίες, όπου μπορούσαν να τρέξουν τις δικές τους εφαρμογές.

Επίσης η Amazon ήταν η πρώτη μεγάλη οργάνωση που βελτίωσε τα data centers της, τα οποία χρησιμοποιούσαν μόνο το 10% της χωρητικότητας τους, πράγμα το οποίο ήταν συνηθισμένο φαινόμενο της εποχής, γιατί οι εταιρίες ανησυχούσαν για spikes (περίοδοι αυξημένης κίνησης) στην ζήτηση.

Στο δεύτερο μισό της δεκαετίας, η Google εξελίχθηκε σε έναν από τους κύριους παίχτες στο ηλεκτρονικό εμπόριο. Το 2006 η εταιρία παρουσίασε τις υπηρεσίες Google Docs, οι οποίες ένωσαν το cloud computing και τη διαμοίραση εγγράφων. (The History of Cloud Computing_2 2016)

Πολλές εταιρίες ιδρύθηκαν και δημιούργησαν τις δικές τους εφαρμογές με βάση το Διαδίκτυο. Το 2009 όμως ήρθε το Web 2.0, ιστοσελίδες του παγκόσμιου ιστού με μεγάλη έμφαση στο περιεχόμενο δημιουργημένο από χρήστες, στη χρηστικότητα και την διαλειτουργικότητα. Το Διαδίκτυο ξαφνικά έγινε πιο δυναμικό, χάρη στην αλληλεπίδραση με περιεχόμενο δημιουργημένο από τους χρήστες και στην ραγδαία αύξηση των ιστοσελίδων κοινωνικής δικτύωσης. Οι χρήστες ήθελαν περισσότερα από ότι μπορούσαν να τους προσφέρουν οι τότε υπηρεσίες, έτσι οι εταιρίες άρχισαν να προσφέρουν περισσότερες εφαρμογές που τρέχουν σε προγράμματα περιήγησης διαδικτύου.

Άλλες δημοφιλείς εφαρμογές που βοήθησαν στην εξέλιξη και αναγνωρισιμότητα του cloud computing είναι οι iCloud της Apple, Google Apps της Google και το Dropbox. (The History of Cloud Computing_1 2016)

1.8 2010 έως σήμερα

Με πλεονεκτήματα όπως: καλύτερα εργαλεία για συνεργασία, ανάκτηση δεδομένων σε περίπτωση καταστροφής και την ικανότητα εργασίας των υπαλλήλων από οπουδήποτε στον κόσμο, η χρήση του cloud computing αυξάνεται μέρα με τη μέρα. Εκτιμάται ότι 1 Exabyte (δηλαδή 1 δισεκατομμύριο Gigabytes) δεδομένων βρίσκονται αυτή τη στιγμή αποθηκευμένα στο cloud, με το 82% των εταιριών να αναφέρουν μείωση του κόστους μετά την αλλαγή.

Μερικά ενδιαφέροντα στατιστικά ακόμη αναφέρουν ότι, το 84% των εταιριών σημείωσαν μείωση του κόστους όταν μετέφεραν τις εφαρμογές τους στο cloud, το 75% των εταιριών χρησιμοποιούν μια μορφή cloud για ηλεκτρονικό ταχυδρομείο, αποθήκευση κ.ά. και τέλος το 86% των εταιριών χρησιμοποιούν πάνω από ένα είδος υπηρεσίας cloud, με τις περισσότερες να χρησιμοποιούν 4 διαφορετικές υπηρεσίες. (The History of the Cloud 2016)

Το 2010 η εταιρία Rackspace μαζί με τη NASA συνεργάστηκαν στην δημιουργία του OpenStack, μιας cloud πλατφόρμας ανοικτού κώδικα. Ο σκοπός του έργου ήταν να βοηθήσει οργανώσεις, προσφέροντας υπηρεσίες cloud μέσω data centers.

Το 2012 η Oracle ανακοίνωσε το Oracle Cloud. Ενώ πολλά κομμάτια του έργου είναι ακόμη σε ανάπτυξη, πρόκειται να είναι ένα από τα πρώτα που θα προσφέρει μια ολοκληρωμένη IT λύση, που θα συμπεριλαμβάνει εφαρμογές (SaaS), πλατφόρμες (PaaS) και υποδομές (IaaS).

Η ακόλουθη λίστα περιγράφει συνοπτικά την εξέλιξη του cloud computing:

- Grid computing: Επίλυση μεγάλων προβλημάτων με παράλληλη επεξεργασία
- Utility computing: Προσφορά επεξεργαστικών πόρων με χρέωση ανάλογα την χρήση
- Software as a service: Συνδρομές βασισμένες σε δίκτυο για εφαρμογές
- Cloud computing: Πρόσβαση οπουδήποτε, οποιαδήποτε στιγμή σε IT πόρους παραδιδόμενοι δυναμικά ως υπηρεσία

1.9 Μέλλον

Ειδικοί προβλέπουν ότι η χρήση του cloud θα συνεχίσει να μεγαλώνει με ραγδαίους ρυθμούς. Με την τεχνολογία να ωριμάζει και να γίνεται πιο στιβαρή, την ασφάλεια να βελτιώνεται διαρκώς, οι εταιρίες στρέφονται στο cloud, για το IT κομμάτι τους. Το 2015 οι τελικοί χρήστες ξόδεψαν για cloud υπηρεσίες 180 δισεκατομμύρια δολάρια.

Μερικά στατιστικά για το μέλλον προβλέπουν ότι μέσα σε πέντε με δέκα χρόνια το 50% των εταιριών information technology θα βρίσκονται στο cloud, ο εξοπλισμός cloud μέχρι το 2018 θα αξίζει 80 δισεκατομμύρια δολάρια και το ποσοστό των υβριδικών δικτύων θα είναι 43% μέσα στα επόμενα πέντε χρόνια, μεγαλύτερο από τα ιδιωτικά και δημόσια δίκτυα. (The History of the Cloud 2016)

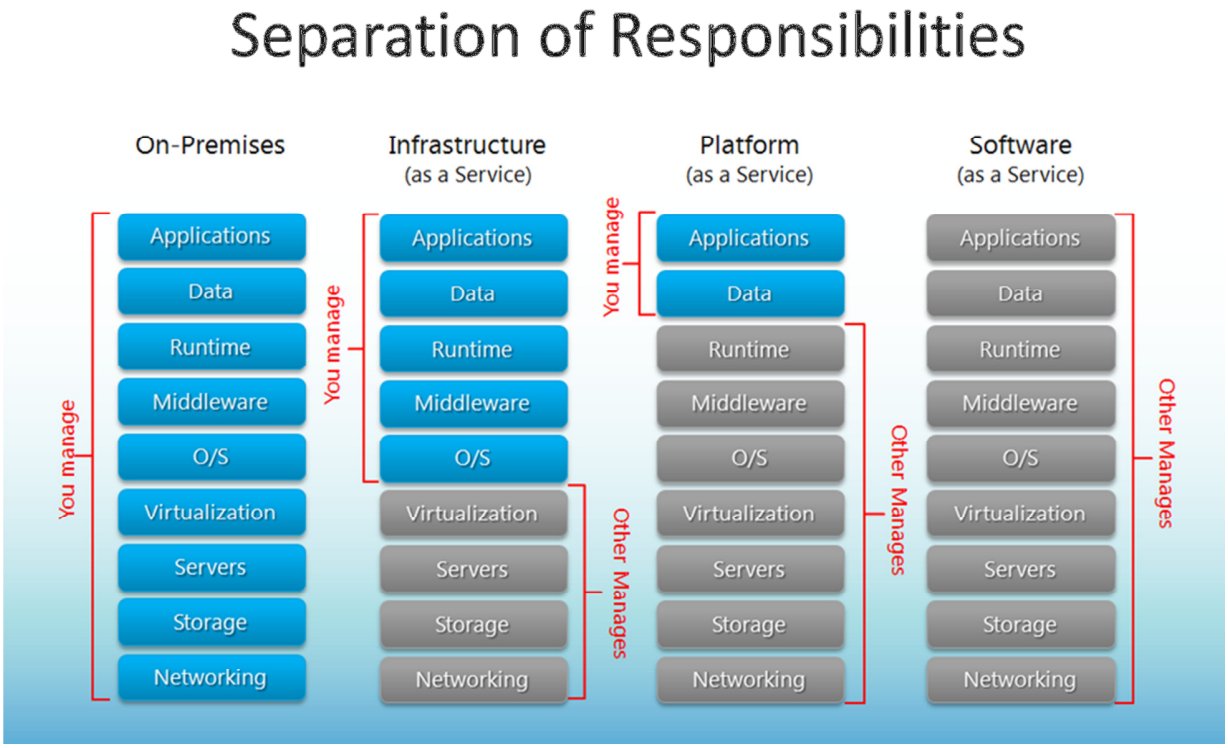
1.10 Τύποι cloud computing

Το cloud computing προσφέρει σε προγραμματιστές και τμήματα IT, την δυνατότητα να επικεντρώνονται στην δουλειά τους και να μην ανησυχούν με πράγματα όπως η συντήρηση και η

χωρητικότητα του δικτύου. Με την εξέλιξη του cloud, εμφανίστηκαν διάφορα μοντέλα και τρόποι ανάπτυξης που προσφέρουν διαφορετικά επίπεδα ελέγχου και διαχείρισης.

1.10.1 Κύρια μοντέλα cloud computing

Υπάρχουν τρία κύρια μοντέλα, με το κάθε μοντέλο να αναπαριστά διαφορετικό κομμάτι της στοίβας του cloud computing.



Εικόνα 1: Διαχωρισμός ευθυνών των μοντέλων cloud computing

1.10.1.1 Υποδομή ως υπηρεσία (Infrastructure as a Service - IaaS)

Η υποδομή ως υπηρεσία, περιέχει τα βασικά δομικά κομμάτια για ένα IT cloud και παρέχει πρόσβαση σε χαρακτηριστικά δικτύου, υπολογιστές (εικονικούς ή αυτόνομο υλικό) και χώρο

αποθήκευσης δεδομένων. Η υποδομή ως υπηρεσία παρέχει την μεγαλύτερη ευελιξία και διαχείριση στους IT πόρους και μοιάζει με τους υπολογιστικούς πόρους που χρησιμοποιούν σήμερα πολλοί προγραμματιστές και IT τμήματα.

1.10.1.2 Πλατφόρμα ως υπηρεσία (Platform as a Service - PaaS)

Η πλατφόρμα ως υπηρεσία, αφαιρεί την ανάγκη από τις επιχειρήσεις να διαχειρίζονται την υποδομή (συνήθως υλικό και λειτουργικά συστήματα), ώστε να εστιάσουν στην ανάπτυξη και διαχείριση των εφαρμογών τους. Έτσι η ανάπτυξη εφαρμογών γίνεται αποδοτικότερα, επειδή ο πάροχος των cloud υπηρεσιών φροντίζει για το διαμοιρασμό των πόρων, την χωρητικότητα των διακομιστών, την συντήρηση του λογισμικού, κ.ά..

1.10.1.3 Λογισμικό ως υπηρεσία (Software as a Service - SaaS)

Το λογισμικό ως υπηρεσία σου προσφέρει ένα πλήρες προϊόν, που εκτελείται και διαχειρίζεται από τον πάροχο της υπηρεσίας. Στις περισσότερες περιπτώσεις, οι άνθρωποι όταν αναφέρονται στο λογισμικό ως υπηρεσία, αναφέρονται στις εφαρμογές του χρήστη. Με μια τέτοια υπηρεσία δεν χρειάζεται να αναρωτιέσαι πως συντηρείται η υπηρεσία ή υποδομή από κάτω της. Το μόνο που σε νοιάζει είναι πως θα χρησιμοποιήσεις το λογισμικό. Ένα απλό παράδειγμα μιας SaaS υπηρεσίας είναι το διαδικτυακό ηλεκτρονικό ταχυδρομείο, όπου μπορείς να στείλεις και να λάβεις μηνύματα, χωρίς να χρειαστεί να διαχειριστείς τους διακομιστές ή τα λειτουργικά συστήματα στα οποία τρέχει η εφαρμογή. (Types of Cloud Computing 2016)

1.10.2 Δευτερεύοντα μοντέλα cloud computing

1.10.2.1 Δεδομένα ως υπηρεσία (Data as a Service - DaaS)

Αυτό το μοντέλο είναι μια υποκατηγορία του Software as a Service. Όπως όλα τα μοντέλα που ανήκουν στο SaaS, το DaaS προσφέρει υπηρεσίες (στην προκειμένη περίπτωση δεδομένα), κατ' απαίτηση στους χρήστες, ανεξαρτήτου περιοχής. Συνήθως χρησιμοποιείται μαζί με συγκεκριμένες εφαρμογές που αναπτύχθηκαν για να έχουν πρόσβαση στα δεδομένα για να τα επεξεργάζονται και να τα παρουσιάζουν σε μορφή που μπορεί να διαβαστεί από τον άνθρωπο. (Data as a service)

1.10.2.2 Mobile backend as a Service – MbaaS

Επίσης γνωστό και με το όνομα backend as a service (BaaS), το μοντέλο αυτό παρέχει στους προγραμματιστές διαδικτυακών και φορητών εφαρμογών, ένα τρόπο για να συνδέσουν τις εφαρμογές τους με το backend μιας υπηρεσίας αποθήκευσης στο cloud. Επίσης υποστηρίζει την σύνδεση με APIs και άλλα χαρακτηριστικά όπως είναι διαχείριση χρηστών, ειδοποιήσεις push και ενσωμάτωση υπηρεσιών κοινωνικών δικτύων. Το μοντέλο είναι σχετικά καινούριο στο χώρο του cloud (με εταιρίες να εμφανίζονται από το 2011 και μετά), αλλά οι υπηρεσίες του είναι δημοφιλείς με τους εταιρικούς πελάτες. (Mobile backend as a service 2016)

1.10.2.3 Δίκτυο ως υπηρεσία (Network as a Service – NaaS)

Το μοντέλο περιγράφει υπηρεσίες μεταφοράς δεδομένων σε δίκτυο και περιλαμβάνει την βελτιστοποίηση των κατανεμημένων πόρων, υπολογίζοντας τους υπολογιστικούς πόρους και τους πόρους του δικτύου ως ένα ενιαίο σύνολο. Μερικές υπηρεσίες του είναι τα εικονικά ιδιωτικά δίκτυα ή VPN, από την δημιουργία ενός τέτοιου δικτύου έως την συντήρηση του, εύρος

ζώνης κατ' απαίτηση, δηλαδή ο πάροχος ορίζει την χωρητικότητα του δικτύου ανάλογα με τις απαιτήσεις των πελατών. Η χωρητικότητα προσαρμόζεται ανάλογα με την κίνηση του δικτύου. (Network as a service 2016)

1.10.2.4 Ρομπότ ως υπηρεσία (Robot as a service – RaaS)

Το μοντέλο αυτό επιτρέπει την ενσωμάτωση ρομπότ και ενσωματωμένων συσκευών στο διαδίκτυο και σε περιβάλλοντα cloud. (Robot as a service 2016)

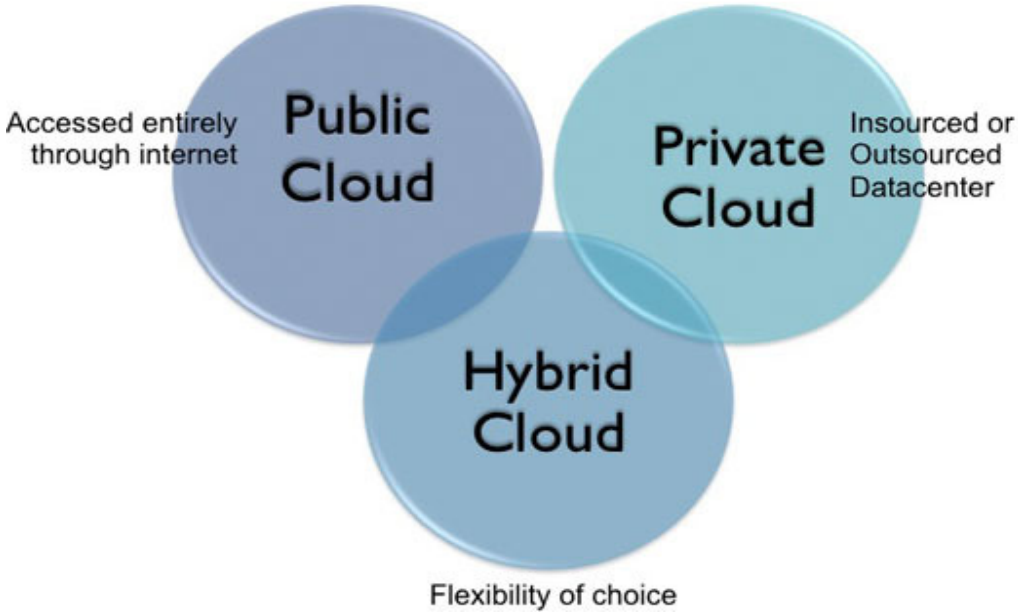
1.10.2.5 Επαναφορά ως υπηρεσία (Recovery as a service – RaaS)

Είναι ένα μοντέλο cloud που χρησιμοποιείται για την προστασία εφαρμογών και δεδομένων, από φυσικές ή ανθρώπινες καταστροφές ή διακοπή υπηρεσιών, κάνοντας πλήρη επαναφορά στο cloud. Το μοντέλο διαφέρει από άλλες υπηρεσίες επαναφοράς cloud, προσφέροντας περισσότερη χωρητικότητα και γρηγορότερη επαναφορά. Ένα μεγάλο πλεονέκτημα του είναι ότι ο πελάτης πληρώνει μόνο αν χρειαστεί να γίνει επαναφορά, επειδή οι πόροι δεν λειτουργούν συνέχεια, κάνοντας το πιο αποδοτικό σε σχέση με άλλες υπηρεσίες. (Recovery as a service 2016)

1.10.2.6 Αναζήτηση ως υπηρεσία (Search as a service – SaaS)

Ακόμη μια υποκατηγορία του Software as a Service, που επικεντρώνεται στην εταιρική αναζήτηση ή στη διαδικτυακή αναζήτηση συγκεκριμένης ιστοσελίδας. Συνήθως χρησιμοποιείται για αναζήτηση σε ιδιωτικούς πόρους μη ορατούς στο δημόσιο διαδίκτυο. Ο πελάτης χρησιμοποιεί το API του παρόχου για να στείλει τα δεδομένα του ή metadata των δεδομένων για την δημιουργία λιστών αναζήτησης από τον πάροχο. (Search as a service 2016)

1.10.3 Μοντέλα ανάπτυξης cloud computing



Εικόνα 2: Μοντέλα ανάπτυξης cloud computing

1.10.3.1 Δημόσιο cloud

Μια εφαρμογή βασισμένη στο cloud είναι ανεπτυγμένη στο cloud και όλα τα μέρη της τρέχουν στο cloud. Εφαρμογές στο cloud έχουν δημιουργηθεί στο cloud ή έχουν μετατραπεί από εφαρμογές σε προϋπάρχουσα υποδομή, ώστε να επωφεληθούν από τα πλεονεκτήματα του cloud computing. Οι εφαρμογές μπορούν να αναπτυχθούν σε κομμάτια υποδομής χαμηλού επιπέδου ή μπορούν να χρησιμοποιηθούν μεγαλύτερα επίπεδα υπηρεσιών, που προσφέρουν αφαίρεση από την διαχείριση, την αρχιτεκτονική και τις αυξανόμενες απαιτήσεις.

1.10.3.2 Υβριδικό cloud

Η υβριδική ανάπτυξη είναι ένας τρόπος να συνδέσουμε υποδομή και εφαρμογές μεταξύ cloud πόρων και υπαρχόντων πόρων που βρίσκονται εκτός cloud. Ο πιο συνηθισμένος υβριδικός τρόπος ανάπτυξης είναι μεταξύ του cloud και της τοπικής υποδομής, για επέκταση και αύξηση της υποδομής του οργανισμού στο cloud, ενώ παράλληλα συνδέουμε cloud πόρους στο σύστημα.

1.10.3.3 Ιδιωτικό cloud

Η χρησιμοποίηση τοπικών πόρων, χρησιμοποιώντας virtualization και διαχείριση πόρων, ονομάζεται ιδιωτικό cloud. Το ιδιωτικό cloud δεν προσφέρει πολλά από τα πλεονεκτήματα του δημόσιου cloud, αλλά προτιμάται επειδή προσφέρει ειδικούς πόρους. Στις περισσότερες περιπτώσεις η χρήση του ιδιωτικού cloud, είναι σαν να χρησιμοποιείς μια τοπική IT υποδομή, ενώ χρησιμοποιείς διαχείριση εφαρμογών και virtualization για αύξηση της αποδοτικότητας των πόρων.

1.10.3.4 Κοινοτικό cloud

Το κοινοτικό cloud είναι μια συνεργατική προσπάθεια στην οποία μοιράζεται η υποδομή μεταξύ κάποιων οργανώσεων, από μια συγκεκριμένη κοινότητα με κοινούς στόχους (όσον αφορά την ασφάλεια π.χ.). Η διαχείριση και η φιλοξενία του cloud μπορεί να γίνει εσωτερικά ή από τρίτη εταιρία. Με αυτή την προσπάθεια μειώνουν το κόστος, αφού μοιράζεται σε όλους τους οργανισμούς, κάνοντας το πιο οικονομικό από το δημόσιο cloud, αλλά και πάλι είναι πιο ακριβό από το ιδιωτικό cloud. (Types of Cloud Computing 2016)

1.11 Πλεονεκτήματα και μειονεκτήματα του cloud computing

1.11.1 Πλεονεκτήματα

1.11.1.1 Μειωμένο κόστος

Το cloud computing είναι η αποδοτικότερη μέθοδος χρήσης, συντήρησης και αναβάθμισης των IT πόρων μιας εταιρίας. Παραδοσιακό λογισμικό και υλικό που τρέχει τοπικά, είναι κατά πολύ ακριβότερο, αν συμπεριλάβουμε και τις άδειες λογισμικού που απαιτούνται. Το cloud όμως, παρέχει ευελιξία στις υπηρεσίες και τους τρόπους πληρωμής του. Μπορείς να αγοράσεις μια άδεια απεριόριστου χρόνου, να πληρώνεις ανάλογα με τη χρήση ή με μηνιαία συνδρομή.

1.11.1.2 Σχεδόν απεριόριστος αποθηκευτικός χώρος

Ο αποθηκευτικός χώρος στο cloud είναι σχεδόν απεριόριστος. Έτσι οι εταιρίες δεν ανησυχούν πλέον αν θα ξεμείνουν από αποθηκευτικό χώρο ή για την αγορά επιπλέον αποθηκευτικού χώρου.

1.11.1.3 Αντίγραφα ασφαλείας και επαναφορά

Αφού όλα τα δεδομένα της εταιρίας είναι αποθηκευμένα στο cloud, η δημιουργία αντιγράφων ασφαλείας και η επαναφορά τους, είναι ευκολότερη από ότι σε ένα φυσικό μέσο. Χάρη στις προηγμένες τεχνολογίες των cloud παρόχων, η διαδικασία είναι απλή και γρήγορη, σε σχέση με άλλα φυσικά μέσα.

1.11.1.4 Ευελιξία

Οι υπηρεσίες cloud είναι ιδανικές για εταιρίες με αυξανόμενο ή κυμαινόμενο εύρος ζώνης. Αν οι ανάγκες αυξηθούν, η χωρητικότητα του cloud αυξάνεται χρησιμοποιώντας περισσότερους απομακρυσμένους διακομιστές του παρόχου. Αν οι ανάγκες μειωθούν, τότε η χωρητικότητα μειώνεται. Αυτή η ευελιξία θεωρείται ως ο κύριος λόγος για την υιοθέτηση του cloud.

1.11.1.5 Αυτόματη αναβάθμιση λογισμικού

Ένα μεγάλο πλεονέκτημα του cloud είναι ότι οι διακομιστές βρίσκονται εκτός εταιρίας, στους παρόχους. Οι πάροχοι λοιπόν τους συντηρούν σε καθημερινή βάση, τους αναβαθμίζουν το υλικό και το λογισμικό, με σημαντικότερες τις αναβαθμίσεις ασφαλείας. Έτσι η εταιρία επικεντρώνεται στις υπηρεσίες ή τα προϊόντα της.

1.11.1.6 Αυξημένη συνεργασία

Όταν οι ομάδες μπορούν να έχουν πρόσβαση, να επεξεργάζονται και να μοιράζονται έγγραφα από οπουδήποτε, οποιαδήποτε στιγμή, μπορούν να κάνουν περισσότερα μαζί και να τα κάνουν καλύτερα. Εφαρμογές διαμοιρασμού αρχείων βοηθούν στην επεξεργασία πραγματικού χρόνου.

1.11.1.7 Εργασία από οπουδήποτε

Με το cloud computing αν έχεις πρόσβαση στο Διαδίκτυο, τότε μπορείς να εργαστείς. Με τις περισσότερες εφαρμογές να έχουν φορητές εφαρμογές, δεν υπάρχει περιορισμός συσκευών. (Cloud Computing and Is it Really All That Beneficial? 2016)

1.11.2 Μειονεκτήματα

1.11.2.1 Σύνδεση στο Διαδίκτυο

Για την πρόσβαση στις υπηρεσίες cloud computing, μια σύνδεση με το Διαδίκτυο είναι απαραίτητη.

1.11.2.2 Χαμηλό εύρος ζώνης

Με χαμηλό εύρος ζώνης, τα πλεονεκτήματα του cloud δεν μπορούν να χρησιμοποιηθούν. Μερικές φορές, ακόμη και μια δορυφορική σύνδεση μεγάλου εύρους ζώνης, μπορεί να είναι κακής ποιότητας λόγω της μεγάλης καθυστέρησης των δεδομένων (latency).

1.11.2.3 Σύγκριση τιμών και υπηρεσιών

Οι cloud υπηρεσίες μπορεί να φαίνονται πιο προσιτές από τις τοπικές, αλλά πάντα πρέπει να γίνεται σύγκριση υπηρεσιών και έρευνα αγοράς. Αλλιώς μια εταιρία μπορεί να χρησιμοποιεί υπηρεσίες που να μην διαθέτουν το βασικό λογισμικό που χρειάζονται ή να πληρώνουν παραπάνω για υπηρεσίες που δεν χρειάζονται.

1.11.2.4 Ασυμβατότητα

Μερικές φορές παρουσιάζονται προβλήματα συμβατότητας μεταξύ του λογισμικού του cloud και τις εφαρμογές ή εργαλεία ενός προσωπικού υπολογιστή.

1.11.2.5 Μη διαπραγματεύσιμες συμφωνίες

Μερικοί πάροχοι cloud computing προσφέρουν μη διαπραγματεύσιμες συμφωνίες, ένα μεγάλο μειονέκτημα για τις εταιρίες πελάτες. (11 Pros and Cons of Cloud Computing Everyone Should Know 2016)

Βιβλιογραφία

Cloud Computing, 2016. Διαθέσιμο από:
< https://en.wikipedia.org/wiki/Cloud_computing>. [28 Μαΐου 2016]

History of Cloud Computing, 2016. Διαθέσιμο από:
<http://saasaddict.walkme.com/history-cloud-computing>. [28 Μαΐου 2016]

The evolution of cloud computing, 2016. Διαθέσιμο από:
<http://blog.definityfirst.com/evolution-of-cloud-computing>. [28 Μαΐου 2016]

The History of Cloud Computing_1, 2016. Διαθέσιμο από:
<http://www.contegix.com/the-history-of-cloud-computing>. [28 Μαΐου 2016]

The History of Cloud Computing_2, 2016. Διαθέσιμο από:
<http://www.eci.com/cloudforum/cloud-computing-history.html>. [28 Μαΐου 2016]

The History of the Cloud, 2016. Διαθέσιμο από:
<https://onyx.net/history-of-the-cloud>. [28 Μαΐου 2016]

Types of Cloud Computing, 2016. Διαθέσιμο από:
<https://aws.amazon.com/types-of-cloud-computing>. [28 Μαΐου 2016]

11 Pros and Cons of Cloud Computing Everyone Should Know, 2016. Διαθέσιμο από:
<https://www.linkedin.com/pulse/11-pros-cons-cloud-computing-everyone-should-know-umesh-singh>. [28 Μαΐου 2016]

Cloud Computing and Is it Really All That Beneficial?, 2016. Διαθέσιμο από: <http://mobiledevices.about.com/od/additionalresources/a/Cloud-Computing-Is-It-Really-All-That-Beneficial.htm>. [28 Μαΐου 2016]

Data as a service, 2016. Διαθέσιμο από: <https://en.wikipedia.org/wiki/Data_as_a_service>. [28 Μαΐου 2016]

Mobile backend as a service, 2016. Διαθέσιμο από: <https://en.wikipedia.org/wiki/Mobile_backend_as_a_service>. [28 Μαΐου 2016]

Network as a service, 2016. Διαθέσιμο από: <https://en.wikipedia.org/wiki/Network_as_a_service>. [28 Μαΐου 2016]

Robot as a service, 2016. Διαθέσιμο από: <https://en.wikipedia.org/wiki/Robot_as_a_service>. [28 Μαΐου 2016]

Recovery as a service, 2016. Διαθέσιμο από: <https://en.wikipedia.org/wiki/Recovery_as_a_service>. [28 Μαΐου 2016]

Search as a service, 2016. Διαθέσιμο από: <https://en.wikipedia.org/wiki/Search_as_a_service>. [28 Μαΐου 2016]

2. Εφαρμογές

2.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα εξετάσουμε συνοπτικά τις σημαντικότερες και δημοφιλέστερες εφαρμογές και εταιρίες που δραστηριοποιούνται στο χώρο του cloud computing.

2.2 Οι σημαντικότερες εταιρίες cloud computing

2.2.1 SoftLayer

Η εταιρία SoftLayer ιδρύθηκε το 2005, και έχει ως έδρα το Ντάλας, Τέξας των Ηνωμένων Πολιτειών Αμερικής. Οι υπηρεσίες που προσφέρει είναι ενοικίαση διακομιστών, φιλοξενία ιστοσελίδων και υπηρεσίες cloud computing.

Το 2011 η εταιρία είχε αναφέρει ότι χρησιμοποιούσε περισσότερους από 81.000 διακομιστές, για την φιλοξενία ιστοσελίδων περισσότερων από 26.000 πελατών, σε περιοχές των Ηνωμένων Πολιτειών. Τον Ιούλιο του 2011 η εταιρία επεκτάθηκε στο Άμστερνταμ και τη Σιγκαπούρη, με την εταιρία να έχει στην κατοχή της 23 data centers σε 11 διαφορετικές χώρες μέχρι τον Μάϊο του 2015.

Τον Ιούνιο του 2013, η IBM ανακοίνωσε την εξαγορά της SoftLayer και δημιούργησε το τμήμα IBM Cloud Services. Τη στιγμή της εξαγοράς, η SoftLayer θεωρούνταν ο μεγαλύτερος ιδιωτικός πάροχος υποδομής cloud (IaaS) στο κόσμο.

2.2.2 Joyent

Η εταιρία Joyent ιδρύθηκε το 2004 από τον Καναδό επιχειρηματία Dean Allen, αλλά με το όνομα TextDrive. Τον πρώτο χρόνο λειτουργίας της πρόσφερε μόνο υπηρεσίες φιλοξενίας ιστοσελίδων. Το 2005 ενώθηκε με την εταιρία Joyent, και οι υπηρεσίες της επεκτάθηκαν στον τομέα του cloud computing.

Οι υπηρεσίες της εταιρίας, σχεδιασμένες να ανταγωνιστούν τις υπηρεσίες EC2 της Amazon περιλαμβάνουν υποδομή και πλατφόρμα ως υπηρεσία (IaaS και PaaS αντίστοιχα) για μεγάλες επιχειρήσεις.

Η εταιρία εξυπηρετεί πάνω από 30.000 πελάτες, συμπεριλαμβανομένου του LinkedIn και υποστηρίζεται από τις εταιρίες Intel, Dell, EMC και την Ισπανική τηλεφωνική εταιρία Telefonica.

2.2.3 Citrix

Η εταιρία Citrix ιδρύθηκε το 1989, στο Ρίτσαρντσον, Τέξας από τον Ed Iacobucci. Στα αρχικά της χρόνια ασχολούνταν με προϊόντα απομακρυσμένου ελέγχου για λειτουργικά συστήματα της Microsoft. Την δεκαετία του 1990, ήταν πρωτοπόρος στην δημιουργία thin client. Μετά την εξαγορά εταιριών την περίοδο 2005 έως 2012, εισήλθε στην αγορά του cloud computing.

Οι υπηρεσίες που προσφέρει είναι: προϊόντα για virtualization σε desktop και εφαρμογές, Desktop as a Service (DaaS) και την εφαρμογή CloudPlatform, η οποία χρησιμοποιεί σαν βάση το CloudStack της Apache για την δημιουργία cloud υποδομών.

Κύριοι ανταγωνιστές της είναι οι VMware και ο οργανισμός που αναπτύσσει το OpenStack, ένα λειτουργικό σύστημα cloud, ανοικτού κώδικα.

2.2.4 IBM

Η εταιρία ιδρύθηκε το 1911 στο Έντικοτ, Νέα Υόρκη από τον Charles Ranlett Flint. Στα αρχικά της χρόνια πουλούσε κάθε λογής μηχανήματα, από ζυγαριές και χρονομετρητές μέχρι μηχανήματα κοπής τυριού και κρέατος. Σήμερα είναι μια από τις μεγαλύτερες εταιρίες παγκοσμίως με πρωτεία στα κέρδη, τον αριθμό υπαλλήλων και το ερευνητικό της τμήμα.

Το εμπορικό όνομα του cloud της εταιρίας είναι IBM SmartCloud και περιλαμβάνει υπηρεσίες υποδομή ως υπηρεσία (IaaS), λογισμικό ως υπηρεσία (SaaS), πλατφόρμα ως υπηρεσία (PaaS), που προσφέρονται μέσω δημόσιων, ιδιωτικών και υβριδικών μοντέλων cloud, καθώς και τα υλικά που αποτελούν τα συγκεκριμένα cloud.

Κύριοι ανταγωνιστές της είναι οι VMware και η Citrix.

2.2.5 Rackspace

Η εταιρία ιδρύθηκε το 1998 από τους Richard Yoo, Dirk Elmendorf, Patrick Condon στο Γουίντκρεστ, Τέξας. Στα πρώτα χρόνια λειτουργίας πρόσφερε φιλοξενία ιστοσελίδων και ανάπτυξη διαδικτυακών εφαρμογών.

Οι υπηρεσίες που προσφέρει με την ονομασία Rackspace Cloud, περιλαμβάνουν φιλοξενία διαδικτυακών εφαρμογών, πλατφόρμα ως υπηρεσία (Cloud Sites), αποθήκευση αρχείων (Cloud Files), ιδιωτικούς εικονικούς διακομιστές (Cloud Servers), ισορροπιστές φορτίου, βάσεις δεδομένων, αντίγραφα ασφαλείας και λογισμικό παρακολούθησης.

Η εταιρία έγινε γνωστή χάρη στην δημιουργία του OpenStack σε συνεργασία με τη NASA. Ο λόγος που δημιουργήθηκε ήταν, επειδή η εταιρία δεν ήθελε να πληρώνει άλλες εταιρίες όπως η VMware για λογισμικό που δεν ήταν υπό τον έλεγχο της. Στη συνέχεια δημιούργησε έναν οργανισμό για την συνεισφορά προς τον ανοικτό κώδικα του OpenStack όπου ανταποκρίθηκαν 160 εταιρίες, ώστε να παραμείνει λειτουργικό και δωρεάν.

2.2.6 Google

Η εταιρία ιδρύθηκε το 1998 από τους Larry Page και Sergey Brin στο Μένλο Παρκ, Καλιφόρνια. Όμως το Google είχε γεννηθεί το 1996, σαν ερευνητικό έργο όταν οι ιδρυτές του ήταν ακόμη φοιτητές στο πανεπιστήμιο του Στάνφορντ. Η ιδέα πίσω από το έργο αυτό, ήταν η δημιουργία μιας καλύτερης μηχανής αναζήτησης.

Σήμερα έχει εξελιχθεί σε μια από τις μεγαλύτερες εταιρίες παγκοσμίως και προσφέρει υπηρεσίες ηλεκτρονικής διαφήμισης (απ' όπου προέρχονται τα περισσότερα έσοδα της), αναζήτησης, cloud computing και λογισμικού.

Η Google προσφέρει πάνω από 15 υπηρεσίες cloud computing με την ονομασία Google Cloud Platform. Μερικές από αυτές είναι η Google Compute Engine, μια υπηρεσία υποδομής ως υπηρεσία (IaaS), η Google Cloud Storage για αποθήκευση αρχείων και η Google Cloud SQL, μια πλήρης MySQL βάση δεδομένων στους διακομιστές cloud της Google.

2.2.7 Salesforce.com

Η εταιρία ιδρύθηκε το 1999 από τους Marc Benioff και Parker Harris, με έδρα το Σαν Φρανσίσκο, Καλιφόρνια. Από τα αρχικά της χρόνια, σκοπός της εταιρία είναι η προσφορά cloud υπηρεσιών με έμφαση στο λογισμικό ως υπηρεσία (SaaS).

Η εταιρία προσφέρει πάνω από 10 υπηρεσίες cloud computing. Μερικές από αυτές είναι η Force.com, μια υπηρεσία υποδομής ως υπηρεσία (IaaS) που ενσωματώνετε στις εφαρμογές της εταιρίας, η Desk.com, μια υπηρεσία εξυπηρέτησης πελατών και η Site.com, μια υπηρεσία που επιτρέπει την γρήγορη ανάπτυξη cloud εφαρμογών.

2.2.8 Microsoft

Η εταιρία ιδρύθηκε το 1975 από τους Paul Allen και Bill Gates, στην Αλμπουκέρκη, Νέο Μεξικό. Η σημερινή έδρα της βρίσκεται στο Ρέντμοντ, Ουάσιγκτον. Τα πρώτα της προϊόντα ήταν λογισμικό για υπολογιστές και τα λειτουργικά συστήματα MS-DOS και Windows. Σήμερα προσφέρει μια ποικιλία προϊόντων: υλικό και λογισμικό υπολογιστών, και ηλεκτρονικές συσκευές όπως το Surface και το Xbox.

Η πλατφόρμα cloud της Microsoft ονομάζεται Azure, για ανάπτυξη εφαρμογών και υπηρεσιών μέσω ενός παγκόσμιου δικτύου data centers. Περιλαμβάνει υπηρεσίες, πλατφόρμας ως υπηρεσία (PaaS) και υποδομής ως υπηρεσία (IaaS) και υποστηρίζει πολλές και διαφορετικές γλώσσες προγραμματισμού.

2.2.9 VMware

Η εταιρία ιδρύθηκε το 1998 από τους Diane Greene, Mendel Rosenblum, Scott Devine, Edward Wang και Edouard Bugnion στο Πάλο Άλτο, Καλιφόρνια. Η εταιρία ισχυρίζεται ότι ήταν η πρώτη που εφάρμοσε την τεχνολογία του virtualization σε x86 επεξεργαστές εμπορικά.

Η εταιρία προσφέρει μια σωρεία λογισμικού και υπηρεσίες cloud και virtualization. Μερικές από αυτές είναι το Workstation που επιτρέπει την παράλληλη εκτέλεση πολλαπλών λειτουργικών συστημάτων σε ένα υπολογιστή, το vCloud Air μια πλατφόρμα δημόσιου cloud, με τρείς τύπους συνδρομών υποδομής ως υπηρεσία (IaaS) και το VSAN (Virtual Storage Area Network) για αποθήκευση αρχείων.

2.2.10 Amazon

Η εταιρία ιδρύθηκε το 1994 από τον Jeff Bezos, στο Σιάτλ, Ουάσιγκτον. Ξεκίνησε να πουλάει βιβλία και αργότερα επεκτάθηκε και στους τομείς των CD, DVD, Blu-rays, MP3, audiobook,

λογισμικό, video games κ.ά.. Σήμερα προσφέρει υπηρεσίες cloud computing και είναι μια από τις μεγαλύτερες εταιρίες του χώρου.

Το τμήμα Amazon Web Services ασχολείται με τις cloud υπηρεσίες, οι οποίες είναι πάνω από 70 σε τομείς όπως επεξεργασία, αποθήκευση, δικτύωση, βάσεις δεδομένων κ.ά.. Μερικές από αυτές τις υπηρεσίες είναι οι Amazon Elastic Compute Cloud (EC2), που προσφέρει ιδιωτικούς εικονικούς διακομιστές, Amazon Simple Storage Service (S3), που προσφέρει αποθηκευτικό χώρο στο cloud και η Amazon DynamoDB, που προσφέρει μια βάση δεδομένων NoSQL τροφοδοτούμενη από SSDs. (The 10 Most Important Companies In Cloud Computing 2016)

2.3 Δημοφιλέστερες εφαρμογές cloud computing

Ολοένα και περισσότερες επιχειρήσεις στρέφονται στις cloud εφαρμογές, με μια πρόσφατη έρευνα να αναφέρει ότι κατά μέσο όρο, μικρές και μεγάλες επιχειρήσεις χρησιμοποιούν 16 cloud εφαρμογές.

2.3.1 Google Analytics

Μια δωρεάν υπηρεσία της Google, που μετράει και αναφέρει την κίνηση ιστοσελίδων. Επίσης ενσωματωμένη είναι και η υπηρεσία AdWords (διαφημίσεις). Οι χρήστες μπορούν να παρακολουθούν την ποιότητα της ιστοσελίδας τους και αν έχουν πετύχει συγκεκριμένους στόχους. Οι στόχοι μπορεί να είναι πωλήσεις, θεάσεις συγκεκριμένης σελίδας ή κατέβασμα συγκεκριμένου αρχείου. Το Google Analytics θεωρείται το καλύτερο και πιο διαδεδομένο εργαλείο για ανάλυση ιστοσελίδων στο Διαδίκτυο.

Λειτουργικό σύστημα: ανεξάρτητο λειτουργικού

2.3.2 Yammer

Το Yammer είναι ένα δωρεάν εταιρικό κοινωνικό δίκτυο που χρησιμοποιείται, για προσωπική επικοινωνία μέσα σε οργανισμούς. Η πρόσβαση καθορίζεται από το Internet domain, έτσι ώστε μόνο τα άτομα με εγκεκριμένες διευθύνσεις ηλεκτρονικού ταχυδρομείου να έχουν πρόσβαση. Μέσα από το κοινωνικό δίκτυο μπορούν να επικοινωνούν σαν ομάδες, να στέλνουν φωτογραφίες, έγγραφα, βίντεο και να επεξεργάζονται έγγραφα ομαδικά.

Λειτουργικό σύστημα: ανεξάρτητο λειτουργικού

2.3.3 NetSuite

Το NetSuite, μια σουίτα επαγγελματικών εφαρμογών, προσφέρει παρακολούθηση οικονομικών αποτελεσμάτων, διαχείριση πωλήσεων, εξυπηρέτηση πελατών και ηλεκτρονικό εμπόριο. Η πρόσβαση σε αυτές τις υπηρεσίες γίνεται, με μηνιαία συνδρομή. Κυρίως οι εφαρμογές αυτές απευθύνονται σε μεσαίες επιχειρήσεις.

Λειτουργικό σύστημα: ανεξάρτητο λειτουργικού

2.3.4 Jira

Το Jira που έχει πάρει το όνομα του από τη λέξη Gojira (το Ιαπωνικό όνομα του Godzilla), είναι ένα λογισμικό ανάπτυξης εφαρμογών που προσφέρει εντοπισμό σφαλμάτων και άλλων θεμάτων, καθώς και δυνατότητες διαχείρισης έργου. Αναπτύσσεται από την εταιρία Atlassian, από το 2002.

Λειτουργικό σύστημα: ανεξάρτητο λειτουργικού

2.3.5 Adobe Creative

Το Adobe Creative είναι μια cloud σουίτα, των γνωστών εφαρμογών της Adobe. Περιλαμβάνει εφαρμογές δημιουργίας γραφικών, επεξεργασίας βίντεο, ανάπτυξης ιστοσελίδων και φωτογραφίας. Όλες είναι διαθέσιμες με μια μηνιαία συνδρομή. Ο χρήστης κατεβάζει τις εφαρμογές από την ιστοσελίδα της εταιρία και τις χρησιμοποιεί μέχρι τη λήξη της συνδρομής.

Λειτουργικό σύστημα: Windows, OS X

2.3.6 WebEx

Μια εφαρμογή της Cisco που προσφέρει συνεργασία κατ' απαίτηση, ηλεκτρονικές συναντήσεις, τηλεδιάσκεψη μέσω διαδικτύου και τηλεδιάσκεψη με βίντεο.

Λειτουργικό σύστημα: Windows

2.3.7 DocuSign

Το DocuSign είναι μια εφαρμογή που σου επιτρέπει να υπογράφεις ηλεκτρονικά βοηθώντας τις εταιρίες να αντικαταστήσουν τις έντυπες φόρμες με ηλεκτρονικές. Επίσης προσφέρει υπηρεσίες ταυτοποίησης και διαχείρισης ταυτότητας χρήστη.

Λειτουργικό σύστημα: ανεξάρτητο λειτουργικού

2.3.8 Workday

Το Workday είναι μια σουίτα εφαρμογών για διαχείριση οικονομικών και διαχείριση του ανθρώπινου δυναμικού μιας επιχείρησης.

Λειτουργικό σύστημα: ανεξάρτητο λειτουργικού

2.3.9 Dropbox

Το Dropbox είναι μια εφαρμογή αποθήκευσης στο cloud, διαμοιρασμού αρχείων, συγχρονισμού και συνεργασίας. Επιτρέπει στους χρήστες να δημιουργήσουν ένα φάκελο, ο οποίος θα περιέχει τα ίδια δεδομένα ανεξάρτητα την συσκευή. Επίσης θα έχει πρόσβαση στο φάκελο και διαδικτυακά, από την ιστοσελίδα της εταιρίας.

Λειτουργικό σύστημα: ανεξάρτητο λειτουργικού

2.3.10 Zendesk

Το Zendesk είναι μια υπηρεσία cloud, για εξυπηρέτηση πελατών, που προσφέρει ευκολότερη αλληλεπίδραση μεταξύ εταιριών και πελατών.

Λειτουργικό σύστημα: Windows, OS X

2.3.11 Amazon Web Services

Μια από τις παλαιότερες cloud εφαρμογές. Η ιστοσελίδα τους επιτρέπει την φιλοξενία εφαρμογών, από τις εφαρμογές που έχει φτιάξει μια εταιρία, μέχρι εμπορικές εκδόσεις σχεδόν κάθε εφαρμογής που μπορείς να σκεφτείς.

Λειτουργικό σύστημα: ανεξάρτητο λειτουργικού

2.3.12 Concur

Το Concur, μια εφαρμογή της εταιρίας SAP, προσφέρει υπηρεσίες διαχείρισης ταξιδιού και εξόδων για επιχειρήσεις. Περιλαμβάνει κράτηση εισιτηρίων, ξενοδοχείου, αυτόματη αναφορά εξόδων, αποζημίωση, λογιστικό έλεγχο και ενσωμάτωση επαγγελματικής κάρτας.

Λειτουργικό σύστημα: Windows, OS X

2.3.13 Google Apps

Το Google Apps είναι μια σουίτα εφαρμογών, περισσότερη γνωστή για την συνεργατική επεξεργασία δεδομένων. Περιλαμβάνει εφαρμογές ηλεκτρονικού ταχυδρομείου (Gmail), επεξεργαστή κειμένου (Docs), λογιστικά φύλλα (Sheets), λογισμικό παρουσίασης (Slides), αποθήκευση στο cloud (Drive), ημερολόγιο (Calendar) κ.ά..

Λειτουργικό σύστημα: ανεξάρτητο λειτουργικού

2.3.14 Box

Το Box είναι μια εφαρμογή αποθήκευσης και διαμοιρασμού αρχείων στο cloud για εταιρίες. Επίσης υποστηρίζει διαχείριση περιεχομένου. Η υπηρεσία είναι δωρεάν και είναι διαθέσιμη και για απλούς χρήστες.

Λειτουργικό σύστημα: Windows, OS X

2.3.15 Salesforce

Το Salesforce είναι μια σουίτα εφαρμογών που χρησιμοποιείται συνήθως από τα τμήματα πωλήσεων και μάρκετινγκ, για παρακολούθηση πελατών και συμβολαίων (μια κατηγορία

προϊόντων γνωστή ως διαχείριση πελατειακών σχέσεων), καθώς και στην δημιουργία μάρκετινγκ εκστρατειών και στην εξυπηρέτηση πελατών.

Λειτουργικό σύστημα: ανεξάρτητο λειτουργικού

2.3.16 Microsoft Office 365

Το Office 365 είναι μια σουίτα εφαρμογών με μηνιαία συνδρομή. Για τους απλούς χρήστες περιλαμβάνει την χρήση των Office εφαρμογών (Word, Excel, PowerPoint, Access, Outlook, OneNote), αποθηκευτικό χώρο στο OneDrive και 60 λεπτά ομιλίας στο Skype. Για τις εταιρίες προσφέρει επιπλέον, ηλεκτρονικό ταχυδρομείο, υπηρεσίες κοινωνικού δικτύου μέσω Skype και Exchange Server και ενσωμάτωση με το Yammer.

Λειτουργικό σύστημα: Windows, OS X

2.3.17 iCloud

Η εφαρμογή cloud της Apple είναι από τις πιο διαδεδομένες στον επιχειρηματικό κόσμο. Παρέχει αποθηκευτικό χώρο και δημιουργία αντιγράφων ασφαλείας σε 320 εκατομμύρια χρήστες, ενώ μοιράζονται φωτογραφίες, μουσική και επιχειρηματικά έγγραφα.

Λειτουργικό σύστημα: Windows, OS X

2.3.18 Evernote

Το Evernote είναι μια δωρεάν εφαρμογή αποθήκευσης και οργάνωσης σημειώσεων. Οι σημειώσεις μπορεί να είναι ένα κομμάτι κειμένου, μια πλήρης ιστοσελίδα ή κομμάτι της, μια φωτογραφία, ένα ηχητικό μήνυμα ή ένα χειρόγραφο κείμενο.

Λειτουργικό σύστημα: ανεξάρτητο λειτουργικού

2.3.19 Microsoft Azure

Το Azure είναι η δημόσια πλατφόρμα cloud της Microsoft και προσφέρει υπηρεσίες υπολογισμού, ανάλυσης, αποθήκευσης και δικτύωσης. Οι χρήστες μπορούν να διαλέξουν από αυτές τις υπηρεσίες και να αναπτύξουν νέες εφαρμογές ή να τρέξουν δικές τους εφαρμογές στο cloud.

Λειτουργικό σύστημα: Windows, Linux (The 24 most popular cloud apps used at work 2016) (Most Used Cloud Apps in Enterprises 2016)

2.4 Cloud εφαρμογές ανοικτού κώδικα

2.4.1 Cloud Stack

Υπό την αιγίδα του Ιδρύματος λογισμικού Apache, το Cloud Stack περιγράφεται ως λογισμικό ανοικτού κώδικα το οποίο έχει σχεδιαστεί για να αναπτύξετε και να διαχειριστείτε μεγάλα δίκτυα εικονικών μηχανών, ως μια υποδομή υψηλής διαθεσιμότητας και υψηλής κλιμάκωσης, ως μια πλατφόρμα υποδομής ως υπηρεσία (IaaS). Γνωστοί χρήστες του είναι οι Cloudera, Citrix Systems, China Telecom, Dell, Disney, Huawei, Nokia, SAP, Verizon και άλλες οργανώσεις.

Λειτουργικό σύστημα: ανεξάρτητο λειτουργικού

2.4.2 OpenStack

Υποστηρίζεται από οργανώσεις όπως η Red Hat, SUSE, Rackspace, IBM, Intel, HP, Ubuntu και AT&T, το OpenStack τροφοδοτεί εκατοντάδες δημόσια και ιδιωτικά σύννεφα. Η ιστοσελίδα περιλαμβάνει online μαγαζί, για την αγορά σχετικών προϊόντων και υπηρεσιών.

Λειτουργικό σύστημα: ανεξάρτητο λειτουργικού

2.4.3 Synnefo

Χρηματοδοτημένο από την Ελλάδα και την Ευρωπαϊκή Ένωση, το Synnefo είναι μια σουίτα cloud ανοικτού κώδικα με βάση το Google Ganeti, Archipelago και Open Stack APIs. Η έκδοση 1.0 είναι ακόμα υπό ανάπτυξη.

Λειτουργικό σύστημα: ανεξάρτητο λειτουργικού

2.4.4 Oneye

Το Oneye βασίζεται στον ανοικτό πηγαίο κώδικα του eyeOS. Επιτρέπει στους χρήστες να δημιουργήσουν ένα cloud desktop με δικούς τους διακομιστές και να έχουν πρόσβαση από οποιαδήποτε συσκευή μέσω ενός προγράμματος περιήγησης.

Λειτουργικό σύστημα: Linux

2.4.5 ownCloud

Το παλαιό πρόγραμμα cloud desktop ownCloud βρίσκεται τώρα στην έκδοση 9.0. Βασικά χαρακτηριστικά περιλαμβάνουν κοινή χρήση, αγαπημένα, υποστήριξη metadata, εξαιρετική αναζήτηση και πολλά άλλα.

Λειτουργικό σύστημα: ανεξάρτητο λειτουργικού

2.4.6 AppScale

Χρηματοδοτημένο από Google, Ubuntu, Cloud Sherpas, Datastax, Canonical και Mirantis, το AppScale επιτρέπει στους χρήστες να δημιουργήσουν τη δική τους πλατφόρμα ως υπηρεσία που τρέχει Google App Engine εφαρμογές ενώ παρέχει πρόσθετη παρακολούθηση και εργαλεία

δημιουργίας αντιγράφων ασφαλείας. Πολλοί πελάτες το χρησιμοποιούν για να δημιουργήσουν το δικό τους υβριδικό cloud. Διατίθενται υπηρεσίες επί πληρωμή.

Λειτουργικό σύστημα: Linux

2.4.7 Cloud Foundry

Αυτό το πρόγραμμα ανοικτού κώδικα PaaS, έχει ένα τεράστιο κατάλογο εταιρικών χρηματοδοτών που περιλαμβάνει τις Pivotal, Cisco, Accenture, EMC, HP, IBM, Intel, SAP, Rackspace, VMware, ακόμη και την εκκλησία του Ιησού Χριστού των Τελευταίων Ημερών Αγίων. Έχει μια πολύ ενεργή κοινότητα προγραμματιστών με τακτικές δημοσιεύσεις σε blogs και επιμορφωτικές εκδηλώσεις.

Λειτουργικό σύστημα: ανεξάρτητο λειτουργικού

2.4.8 Cloud9 IDE

Το Cloud9 είναι ένας Ubuntu desktop υπολογιστής βασισμένος στο cloud, αλλά και ένα IDE βασισμένο σε πρόγραμμα περιήγησης. Μπορείτε να εγγραφείτε στη σελίδα του προγράμματος για να χρησιμοποιήσετε μια δωρεάν ή επί πληρωμή έκδοση της υπηρεσίας, ή μπορείτε να δημιουργήσετε το δικό σας βασισμένο στο cloud IDE, χρησιμοποιώντας τον πηγαίο κώδικα από το GitHub.

Λειτουργικό σύστημα: ανεξάρτητο λειτουργικού

2.4.9 Dirigible

Ιδιοκτησία της SAP, το Dirigible είναι ένα ολοκληρωμένο περιβάλλον ανάπτυξης ως υπηρεσία (IDEaaS) που υπόσχεται να βοηθήσει τους προγραμματιστές να απολαμβάνουν να γράφουν

κώδικα όπως ποτέ πριν. Το Dirigible είναι ακόμα σε δοκιμαστική περίοδο και μπορείτε να εγγραφείτε για να το χρησιμοποιήσετε δωρεάν από τη ιστοσελίδα του. Ο πηγαίος κώδικας βρίσκεται στο GitHub.

Λειτουργικό σύστημα: ανεξάρτητο λειτουργικού

2.4.10 Duplicati

Αυτό το πρόγραμμα δημιουργίας αντιγράφων ασφαλείας, αποθηκεύει αυτόματα τα δεδομένα του πελάτη σε μια υπηρεσία cloud. Λειτουργεί με AWS, Microsoft OneDrive, Google Drive, Rackspace και ιδιωτικά cloud. Διαθέτει κρυπτογράφηση AES-256 και τα αρχειοθετημένα αρχεία μπορούν επίσης να υπογραφούν με Gnu Privacy Guard.

Λειτουργικό σύστημα: ανεξάρτητο λειτουργικού

2.4.11 Ceph

Το Ceph προσφέρει μερική και ολική αποθήκευση, καθώς και ένα σύστημα αρχείων συμβατό με POSIX για κατανεμημένη αποθήκευση. Η διαχείριση του προγράμματος γίνεται από τη Red Hat, η οποία πουλάει προϊόντα που βασίζονται στο Ceph.

Λειτουργικό σύστημα: Linux

2.4.12 Gluster

Το Gluster υπό την διαχείριση της Red Hat, είναι ένα κατανεμημένο σύστημα αρχείων ανοικτού κώδικα, σχεδιασμένο για να χειριστεί petabytes (ή ακόμη και brontobytes) δεδομένων. Διαθέτει υψηλή επεκτασιμότητα, επιδόσεις και διαθεσιμότητα. Υποστήριξη με χρέωση και συμβουλευτικές υπηρεσίες διατίθενται από τρίτους συνεργάτες.

Λειτουργικό σύστημα: Linux, OS X, Free BSD

2.4.13 Docker

Αν και είναι μια αρκετά νέα τεχνολογία, το containerization του Docker ήδη αποσπά πολλή προσοχή από αναλυτές του κλάδου και επιχειρήσεις. Περιγράφετε ως μια ανοικτή πλατφόρμα για προγραμματιστές και sysadmins για να δημιουργήσουν, να φορτώσουν και να τρέξουν κατανεμημένες εφαρμογές.

Λειτουργικό σύστημα: Windows, Linux, OS X

2.4.14 Xen

Η ιστοσελίδα του το περιγράφει ως ένα hypervisor ανοικτού κώδικα σχεδιασμένο για cloud. Παρέχει τα θεμέλια για μερικά από τα μεγαλύτερα cloud στον κόσμο, συμπεριλαμβανομένου του Amazon Elastic Compute Cloud (EC2).

Λειτουργικό σύστημα: ανεξάρτητο λειτουργικού

2.4.15 Hadoop

Το Hadoop είναι τόσο διαδεδομένο έτσι ώστε να έχει γίνει σχεδόν συνώνυμο με δεδομένα μεγάλου όγκου. Είναι μια συλλογή από εργαλεία επεξεργασίας δεδομένων που μπορούν να χρησιμοποιηθούν σε κατανεμημένα υπολογιστικά περιβάλλοντα, συμπεριλαμβανομένων υπολογιστικών περιβαλλόντων cloud.

Λειτουργικό σύστημα: ανεξάρτητο λειτουργικού

2.4.16 Group-Office

Το Group-Office συνδυάζει λογισμικό συνεργασίας εταιρικού επιπέδου με μερική λειτουργικότητα CRM, και μπορεί να αναπτυχθεί ενδοεταιρικά ή στο cloud. Όλες οι βασικές λειτουργίες περιλαμβάνονται στην έκδοση κοινότητας ανοικτού κώδικα. Η επί πληρωμή επαγγελματική έκδοση προσθέτει helpdesk, καταγραφή χρόνου, φορητό συγχρονισμό και διαχείριση έργων. Η επεξεργασία εγγράφων με χρέωση και η αναζήτηση εγγράφου διατίθενται με ξεχωριστή χρέωση.

Λειτουργικό σύστημα: ανεξάρτητο λειτουργικού

2.4.17 opentaps

Χρησιμοποιείται από οργανώσεις όπως η Toyota και η Honeywell, το Opentaps ισχυρίζεται ότι είναι το πιο προηγμένο CRM πρόγραμμα ανοικτού κώδικα. Εκτός από τη δωρεάν έκδοση, η εταιρεία προσφέρει μια επαγγελματική έκδοση και υπηρεσίες επί πληρωμή, καθώς και μια έκδοση που τρέχει σε Amazon.

Λειτουργικό σύστημα: Windows, Linux

2.4.18 OrangeHRM

Με πελάτες όπως οι Lufthansa, Sandals, Red Hat και Stanley Black & Decker, το OrangeHRM υπερηφανεύεται ότι είναι το πιο δημοφιλές HR λογισμικό παγκοσμίως. Είναι διαθέσιμο σε εκδόσεις ανοικτού κώδικα, επαγγελματική και εταιρική, καθώς και έκδοση cloud.

Λειτουργικό σύστημα: Windows, Linux

2.4.19 OpenHAB

Το OpenHAB περιγράφει τον εαυτό του ως ένα προμηθευτή λογισμικού αυτοματισμού ανεξάρτητης τεχνολογίας ανοικτού κώδικα, για το σπίτι σας. Στόχος του είναι να επιτρέψει στους χρήστες να ελέγχουν μια ποικιλία διαφορετικών συσκευών από ένα ενιαίο πρόγραμμα.

Λειτουργικό σύστημα: ανεξάρτητο λειτουργικού (75 Open Source Cloud Computing Apps 2016)

Όνομα	Εταιρία ανάπτυξης	Είδος υπηρεσίας	Λειτουργικό σύστημα
Google Analytics	Google	SaaS	Ανεξάρτητο λειτουργικού
Yammer	Yammer	SaaS	Ανεξάρτητο λειτουργικού
NetSuite	NetSuite	SaaS	Ανεξάρτητο λειτουργικού
Jira	Atlassian	SaaS	Ανεξάρτητο λειτουργικού
Adobe Creative	Adobe Systems	SaaS	Windows, OS X
WebEx	Cisco WebEx	SaaS	Windows
DocuSign	DocuSign	SaaS	Ανεξάρτητο λειτουργικού
Workday	Workday, Inc.	SaaS	Ανεξάρτητο λειτουργικού
Dropbox	Dropbox, Inc.	SaaS	Ανεξάρτητο λειτουργικού
Zendesk	Zendesk, Inc.	SaaS	Windows, OS X
Amazon Web Services	Amazon.com, Inc.	SaaS, PaaS, IaaS	Ανεξάρτητο λειτουργικού
Concur	Concur Technologies	SaaS	Windows, OS X
Google Apps	Google	SaaS	Ανεξάρτητο λειτουργικού
Box	Box, Inc.	SaaS	Windows, OS X
Salesforce	Salesforce.com	SaaS, PaaS	Ανεξάρτητο λειτουργικού
Microsoft Office 365	Microsoft Corporation	SaaS	Windows, OS X
iCloud	Apple Inc.	SaaS	Windows, OS X
Evernote	Evernote Corporation	SaaS	Ανεξάρτητο λειτουργικού
Microsoft Azure	Microsoft Corporation	PaaS, IaaS	Windows, Linux

Πίνακας 1: Δημοφιλέστερες εφαρμογές cloud computing

Όνομα	Εταιρία ανάπτυξης	Είδος υπηρεσίας	Λειτουργικό σύστημα
Cloud Stack	Apache Software Foundation	IaaS	Ανεξάρτητο λειτουργικού
OpenStack	OpenStack Foundation	IaaS	Ανεξάρτητο λειτουργικού
Synnefo	GRNET	IaaS	Ανεξάρτητο λειτουργικού
Oneye	Κοινότητα	SaaS	Linux
ownCloud	OwnCloud Inc., Κοινότητα	SaaS	Ανεξάρτητο λειτουργικού
AppScale	Κοινότητα	PaaS	Linux
Cloud Foundry	VMware, Pivotal Software	PaaS	Ανεξάρτητο λειτουργικού
Cloud9 IDE	Cloud9 IDE, Inc.	SaaS	Ανεξάρτητο λειτουργικού
Dirigible	Κοινότητα	SaaS	Ανεξάρτητο λειτουργικού
Duplicati	Kenneth Skovhede	SaaS	Ανεξάρτητο λειτουργικού
Ceph	Canonical, Intel, Cisco, κ.ά.	SaaS	Linux
Gluster	Red Hat, Inc.	SaaS	Linux, OS X, Free BSD
Docker	Docker, Inc.	PaaS	Windows, Linux, OS X
Xen	Linux Foundation	Hypervisor	Ανεξάρτητο λειτουργικού
Hadoop	Apache Software Foundation	SaaS	Ανεξάρτητο λειτουργικού
Group-Office	Intermesh	SaaS	Ανεξάρτητο λειτουργικού
Opentaps	Open Source Strategies	SaaS	Windows, Linux
OrangeHRM	OrangeHRM Inc.	SaaS	Windows, Linux
OpenHAB	openHAB Foundation	SaaS	Ανεξάρτητο λειτουργικού

Πίνακας 2: Cloud εφαρμογές ανοικτού κώδικα

Βιβλιογραφία

The 10 Most Important Companies In Cloud Computing, 2016. Διαθέσιμο από: <http://www.businessinsider.com/10-most-important-in-cloud-computing-2013-4?op=1/#word-about-clouds-1>. [29 Μάϊου 2016]

The 24 most popular cloud apps used at work, 2016. Διαθέσιμο από: <http://www.businessinsider.com/the-most-popular-cloud-apps-used-at-work-2015-8/#no-24-google-analytics-afreemium-service-that-tracks-and-reports-website-and-mobile-website-traffic-1>. [29 Μάϊου 2016]

75 Open Source Cloud Computing Apps, 2016. Διαθέσιμο από: <http://www.datamation.com/cloud-computing/75-open-source-cloud-computing-apps-1.html>. [29 Μάϊου 2016]

Most Used Cloud Apps in Enterprises, 2016. Διαθέσιμο από: <https://www.rickscloud.com/most-used-cloud-apps-in-enterprises>. [29 Μάϊου 2016]

3. Ασφάλεια και αξιοπιστία δεδομένων

3.1 Εισαγωγή

Όσο αυξάνεται η χρήση του cloud computing, τόσο αυξάνεται και το ενδιαφέρον πιθανών επιθέσεων στις υπηρεσίες του από χάκερς ή άλλους εισβολείς για υποκλοπή δεδομένων ή άλλων βλαβερών επιθέσεων. Σε αυτό το κεφάλαιο θα εξετάσουμε τις πολιτικές και τεχνολογίες ασφάλειας που χρησιμοποιούνται για την ασφάλεια δεδομένων, εφαρμογών και γενικά της υποδομής του cloud computing.

3.2 Θέματα ασφάλειας που σχετίζονται με το cloud

Υπάρχουν πολλά θέματα ασφάλειας που σχετίζονται με το cloud. Μπορούμε όμως να τα χωρίσουμε σε δύο μεγάλες κατηγορίες: θέματα ασφάλειας που αντιμετωπίζουν οι πάροχοι cloud (οι οργανώσεις που προσφέρουν υπηρεσίες λογισμικού, πλατφόρμας και υποδομής) και στα θέματα ασφάλειας που αντιμετωπίζουν οι πελάτες (εταιρίες ή οργανισμοί που φιλοξενούν εφαρμογές ή αποθηκεύουν δεδομένα στο cloud). Και οι δύο πλευρές πρέπει να είναι προσεκτικές. Οι πάροχοι πρέπει να εξασφαλίζουν ότι η υποδομή τους είναι ασφαλής και τα δεδομένα και οι εφαρμογές των πελατών προστατεύονται επαρκώς. Οι πελάτες από την πλευρά τους πρέπει να ενισχύσουν την ασφάλεια των εφαρμογών τους, να χρησιμοποιούν δυνατούς κωδικούς και μέτρα πιστοποίησης.

Όταν μια οργάνωση επιλέγει να αποθηκεύσει τα δεδομένα της ή να φιλοξενήσει τις εφαρμογές της στο δημόσιο cloud, χάνει την δυνατότητα να έχει πρόσβαση στους διακομιστές που περιέχουν αυτή τη γνώση. Αυτό έχει σαν αποτέλεσμα, ευαίσθητα δεδομένα να βρίσκονται σε κίνδυνο από εσωτερικές επιθέσεις, την τρίτη μεγαλύτερη απειλή στο χώρο του cloud computing. Για να αποτραπούν τέτοιες επιθέσεις, οι πάροχοι πρέπει να πραγματοποιούν ελέγχους στους εργαζόμενους που έρχονται σε επαφή με τους διακομιστές και να υπάρχει συχνή παρακολούθηση για τυχόν ύποπτη δραστηριότητα.

Με σκοπό τη μείωση του κόστους, τη διατήρηση πόρων και την διατήρηση της παραγωγικότητας, οι πάροχοι συχνά αποθηκεύουν τα δεδομένα πολλών πελατών σε ένα διακομιστή. Αυτό έχει σαν αποτέλεσμα, να υπάρχει η δυνατότητα τα ιδιωτικά δεδομένα ενός πελάτη να είναι ορατά σε άλλους (ακόμη και ανταγωνιστών). Για να αποτραπούν τέτοιες καταστάσεις οι πάροχοι πρέπει να εξασφαλίζουν καλή απομόνωση δεδομένων και διαχωρισμό λογικής αποθήκευσης.

Η εκτεταμένη χρήση του virtualization στις υποδομές του cloud computing παρουσιάζει μοναδικά θέματα ασφάλειας για τους πελάτες του δημόσιου cloud. Το virtualization αλλάζει την σχέση μεταξύ του λειτουργικού συστήματος και του υλικού (υπολογιστικού, αποθηκευτικού ή δικτυακού). Προσθέτει ένα επιπλέον επίπεδο, που πρέπει να ρυθμιστεί, διαχειριστεί και ασφαλιστεί πολύ προσεκτικά. Υπάρχει η πιθανότητα (θεωρητική αλλά υπαρκτή) να πέσει υπό τον έλεγχο χάκερ το λογισμικό virtualization ή ο hypervisor. Αν συμβεί αυτό σε ένα σταθμό διαχειριστή με το λογισμικό διαχείρισης του virtualization, τότε ο εισβολέας μπορεί να γονατίσει το data center ή να το πάρει υπό τον έλεγχο του και να το χρησιμοποιήσει για τους δικούς του σκοπούς.

3.3 Έλεγχοι ασφάλειας cloud

Η αρχιτεκτονική ασφάλειας cloud είναι αποτελεσματική μόνο αν οι σωστές αμυντικές ρυθμίσεις είναι εγκατεστημένες. Μια αποδοτική ασφάλεια cloud πρέπει να αναγνωρίζει τα θέματα που προκύπτουν με σωστή διαχείριση ασφάλειας. Η διαχείριση ασφάλειας αντιμετωπίζει τα θέματα αυτά με ελέγχους ασφάλειας. Οι έλεγχοι αυτοί τοποθετούνται για να διασφαλίζουν τυχόν αδυναμίες στο σύστημα και για να μειώσουν το αποτέλεσμα μιας επίθεσης. Υπάρχουν πολλοί τύποι ελέγχων σε μια αρχιτεκτονική ασφάλειας cloud, αλλά συνήθως χωρίζονται σε μια από τις εξής κατηγορίες:

3.3.1 Αποτρεπτικοί έλεγχοι

Αυτοί οι έλεγχοι αποσκοπούν στην μείωση επιθέσεων σε ένα cloud σύστημα. Όπως μια προειδοποιητική πινακίδα σε ένα φράχτη, οι αποτρεπτικοί έλεγχοι μειώνουν τις απειλές, προειδοποιώντας τους πιθανούς εισβολείς ότι θα υπάρξουν δυσμενείς συνέπειες αν συνεχίσουν (μερικοί τις θεωρούν υποκατηγορία των προληπτικών ελέγχων).

3.3.2 Προληπτικοί έλεγχοι

Οι προληπτικοί έλεγχοι δυναμώνουν το σύστημα ενάντια σε συμβάντα, μειώνοντας ή εξαλείφοντας τρωτά σημεία. Δυνατή πιστοποίηση cloud χρηστών, για παράδειγμα, μειώνει τις πιθανότητες για είσοδο στο cloud σύστημα ανεξουσιοδότητων χρηστών και αυξάνει τις πιθανότητες για είσοδο σε εξουσιοδοτημένους χρήστες.

3.3.3 Ανιχνευτικοί έλεγχοι

Οι ανιχνευτικοί έλεγχοι αποσκοπούν στον εντοπισμό και την κατάλληλη αντίδραση σε συμβάντα που προκύπτουν. Στην περίπτωση μιας επίθεσης, ένας ανιχνευτικός έλεγχος θα ειδοποιήσει τον προληπτικό έλεγχο ή τον διορθωτικό έλεγχο για να επιλύσει το θέμα. Η παρακολούθηση συστήματος και δικτύου, συμπεριλαμβανομένης της ανίχνευσης εισβολών, χρησιμοποιούνται για την ανίχνευση επιθέσεων στα cloud συστήματα και την βοηθητική υποδομή επικοινωνίας.

3.3.4 Διορθωτικοί έλεγχοι

Οι διορθωτικοί έλεγχοι μειώνουν τις συνέπειες ενός συμβάντος, περιορίζοντας την ζημιά. Ενεργοποιούνται κατά τη διάρκεια ή μετά από ένα συμβάν. Η χρησιμοποίηση αντιγράφων

ασφάλειας για την επαναφορά ενός συστήματος σε κίνδυνο είναι ένα παράδειγμα ενός διορθωτικού ελέγχου.

3.4 Ασφάλεια και ιδιωτικότητα

3.4.1 Διαχείριση ταυτότητας

Κάθε εταιρία θα έχει το δικό της σύστημα διαχείρισης ταυτότητας για έλεγχο πρόσβασης σε πληροφορίες και υπολογιστικούς πόρους. Οι πάροχοι cloud είτε θα ενσωματώσουν το σύστημα διαχείρισης ταυτότητας στην δικιά τους υποδομή (χρησιμοποιώντας τις τεχνολογίες federation και SSO ή ένα βιομετρικό σύστημα αναγνώρισης), είτε θα προσφέρουν ένα δικό τους σύστημα διαχείρισης ταυτότητας. Το CloudID, για παράδειγμα, προσφέρει λύσεις βιομετρικής αναγνώρισης που διασφαλίζουν την ιδιωτικότητα και λειτουργούν σε πολλές και διαφορετικές εταιρίες. Συνδέει τις εμπιστευτικές πληροφορίες των χρηστών με τα βιομετρικά χαρακτηριστικά τους και τα αποθηκεύει κρυπτογραφημένα. Με την χρήση μιας κρυπτογραφημένης αναζήτησης, ο πάροχος cloud και πιθανοί εισβολείς δεν έχουν πρόσβαση σε ευαίσθητα δεδομένα, ούτε στα περιεχόμενα των αναζητήσεων.

3.4.2 Φυσική ασφάλεια

Οι πάροχοι υπηρεσιών cloud έχουν πάρει τα κατάλληλα μέτρα για να προστατεύσουν τα φυσικά μέσα και υλικά (π.χ. διακομιστές, routers, καλώδια κ.ά.), ενάντια σε μη εξουσιοδοτημένες εισόδους, παρεμβάσεις, κλοπές, πυρκαγιές, πλημμύρες και άλλες καταστροφές. Επίσης εξασφαλίζουν την συνεχή ροή προμηθειών (όπως είναι ο ηλεκτρισμός), για να ελαχιστοποιήσουν την πιθανότητα διακοπής των υπηρεσιών. Αυτό το πετυχαίνουν προσφέροντας τις υπηρεσίες τους από κορυφαία data centers (σχεδιασμένα, χτισμένα, διαχειριζόμενα, παρακολουθούμενα και συντηρούμενα από επαγγελματίες).

3.4.3 Ιδιωτικότητα

Οι πάροχοι εξασφαλίζουν ότι όλα τα κρίσιμα δεδομένα, όπως είναι οι αριθμοί πιστωτικών καρτών, είναι κρυπτογραφημένα ή μεταμφιεσμένα και μόνο εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στα αρχικά δεδομένα. Επιπροσθέτως, οι ψηφιακές ταυτότητες και τα διαπιστευτήρια πρέπει να προστατεύονται, όπως προστατεύονται οποιαδήποτε δεδομένα που ο πάροχος συλλέγει ή παράγει σχετικά με την δραστηριότητα του πελάτη στο cloud.

3.5 Ασφάλεια δεδομένων

Ο αριθμός των απειλών ασφάλειας που σχετίζονται με τις υπηρεσίες δεδομένων cloud είναι μεγάλος, από τις παραδοσιακές απειλές: υποκλοπές δικτύου, παράνομη εισβολή και άρνηση υπηρεσίας, μέχρι ειδικές απειλές που στοχεύουν τα cloud συστήματα: επιθέσεις side channel, τρωτά σημεία στο virtualization και κατάχρηση cloud υπηρεσιών. Για να καταπολεμήσουν αυτές τις απειλές , πρέπει να εφαρμοστούν τα παρακάτω μέτρα ασφάλειας σε μια υπηρεσία δεδομένων cloud.

3.5.1 Εμπιστευτικότητα δεδομένων

Η εμπιστευτικότητα δεδομένων ορίζεται ως η προστασία των περιεχομένων των δεδομένων από παράνομους χρήστες. Δεδομένα που έχουν ανατεθεί σε εξωτερικούς συνεργάτες είναι αποθηκευμένα στο cloud, μακριά από τον απευθείας έλεγχο του ιδιοκτήτη. Μόνο εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση στα ευαίσθητα δεδομένα, ενώ άλλοι μαζί με τους παρόχους, δεν πρέπει να συλλέξουν καμία πληροφορία από τα δεδομένα. Εντωμεταξύ οι ιδιοκτήτες των δεδομένων μπορούν να χρησιμοποιήσουν πλήρως τις υπηρεσίες δεδομένων cloud, όπως είναι η αναζήτηση δεδομένων, επεξεργασία δεδομένων και διαμοιρασμό δεδομένων, χωρίς να υπάρχει διαρροή δεδομένων σε παρόχους ή σε τρίτους.

3.5.2 Έλεγχος πρόσβασης δεδομένων

Έλεγχος πρόσβασης σημαίνει ότι ο ιδιοκτήτης δεδομένων μπορεί να επιλέξει μερικό περιορισμό πρόσβασης στα δεδομένα που έχουν ανατεθεί στο cloud. Νόμιμοι χρήστες μπορούν να πιστοποιηθούν από τον ιδιοκτήτη για να έχουν πρόσβαση στα δεδομένα, ενώ άλλοι δεν μπορούν να έχουν πρόσβαση χωρίς τα απαραίτητα δικαιώματα. Επίσης είναι επιθυμητό να επιβληθεί εξειδικευμένη πρόσβαση στα cloud δεδομένα. Διαφορετικοί χρήστες να έχουν διαφορετικά δικαιώματα πρόσβασης στα σχετικά κομμάτια δεδομένων. Η πιστοποίηση πρόσβασης πρέπει να χειρίζεται μόνο από τον ιδιοκτήτη σε μη έμπιστα περιβάλλοντα cloud.

3.5.3 Ακεραιότητα δεδομένων

Η ακεραιότητα δεδομένων απαιτεί την συντήρηση και εξασφάλιση της ακρίβειας και της πληρότητας των δεδομένων. Ένας ιδιοκτήτης δεδομένων αναμένει ότι τα δεδομένα του που βρίσκονται στο cloud μπορούν να αποθηκευτούν σωστά και αξιόπιστα. Αυτό σημαίνει ότι τα δεδομένα δεν έχουν αλλοιωθεί παράνομα, τροποποιηθεί εσφαλμένα, διαγραφτεί επίτηδες ή δεν έχουν επεξεργαστεί κακόβουλα. Αν κάποια μη επιθυμητή εργασία διαφθείρει ή διαγράψει τα δεδομένα, τότε ο ιδιοκτήτης πρέπει να είναι ικανός να εντοπίσει τη διαφθορά ή διαγραφή. Επίσης όταν ένα κομμάτι από τα δεδομένα έχει υποστεί διαφθορά ή έχει χαθεί, πρέπει να είναι δυνατή η επαναφορά τους από τους χρήστες των δεδομένων. (Cloud computing security 2016)

3.6 Χειρότερες απειλές ασφάλειας cloud

Συχνά οι χρήστες (ή ακόμη και ολόκληρα τμήματα εταιριών) υπηρεσιών cloud χρησιμοποιούν εφαρμογές και μεταφέρουν δεδομένα, χωρίς να υπολογίζουν τις συνέπειες τους στην ασφάλεια των υπηρεσιών αυτών. Αυτό ονομάζεται Shadow IT ή Stealth IT, όπου χρησιμοποιούνται υπολογιστικά συστήματα χωρίς την έγκριση των ανωτέρων μιας εταιρίας. Βέβαια μερικές φορές λειτουργούν σαν πρωτότυπα για νέες τεχνολογίες IT, αλλά τις περισσότερες φορές αποτελούν

κινδύνους για τον έλεγχο, τα έγγραφα, την αξιοπιστία και πάνω απ' όλα την ασφάλεια της εταιρίας.

Η Cloud Security Alliance, μια μη κερδοσκοπική οργάνωση, με αποστολή της την προώθηση της χρήσης καλών πρακτικών για την ασφάλεια cloud συστημάτων και γενικά την επιμόρφωση χρηστών για την ασφάλεια υπολογιστικών συστημάτων, έφτιαξε μια λίστα με τις κυριότερες και χειρότερες απειλές στο χώρο του cloud computing.

3.6.1 Ρήξη δεδομένων

Τα συστήματα cloud αντιμετωπίζουν πολλές από τις απειλές που απειλούν τα παραδοσιακά εταιρικά δίκτυα, αλλά χάρη στον μεγάλο όγκο δεδομένων που βρίσκεται αποθηκευμένος στους διακομιστές cloud, οι πάροχοι γίνονται ελκυστικοί στόχοι. Το μέγεθος της πιθανής ζημιάς εξαρτάται από πόσο ευαίσθητα είναι τα εκτεθειμένα δεδομένα. Μεγάλη δημοσιότητα παίρνουν οι προσωπικές οικονομικές πληροφορίες, αλλά οι ρήξεις που αφορούν πληροφορίες υγείας, επαγγελματικά μυστικά και πνευματική ιδιοκτησία είναι πιο καταστροφικά.

Όταν συμβεί μια ρήξη δεδομένων, οι εταιρίες μπορούν να τιμωρηθούν με πρόστιμο, ή μπορεί να οδηγηθούν σε αγωγές και ποινικές διώξεις. Οι έρευνες για την ρήξη και οι ειδοποιήσεις πελατών μπορούν να αυξήσουν παραπάνω τα κόστη. Έμμεσα αποτελέσματα όπως η καταστροφή του ονόματος και της αξιοπιστίας μιας εταιρίας, καθώς και η μείωση των κερδών είναι πολύ πιθανό να την ακολουθούν για χρόνια.

Οι πάροχοι cloud χρησιμοποιούν πολύπλοκα συστήματα ασφάλειας για να προστατεύσουν τις υπηρεσίες τους, αλλά τελικά οι οργανισμοί είναι υπεύθυνοι για την προστασία των δεδομένων τους στο cloud. Η Cloud Security Alliance προτείνει να εφαρμόζονται πολλαπλά επίπεδα ασφάλειας, πιστοποίησης και κρυπτογραφίας για προστασία απέναντι στις ρήξεις δεδομένων.

3.6.2 Κλεμμένα διαπιστευτήρια και χαλασμένη πιστοποίηση

Ρήξεις δεδομένων και άλλες επιθέσεις συχνά προέρχονται από χαλαρή πιστοποίηση, αδύναμους κωδικούς και φτωχή διαχείριση κλειδιών και πιστοποιητικών. Οι οργανώσεις συχνά δυσκολεύονται με την διαχείριση ταυτότητας, όταν προσπαθούν να διανέμουν τα κατάλληλα δικαιώματα σύμφωνα με την εργασία κάθε χρήστη. Πολύ σημαντικό, μερικές φορές ξεχνούν να αφαιρέσουν πρόσβαση σε κάποιο χρήστη μετά την αλλαγή εργασίας του ή όταν ο χρήστης φύγει από την οργάνωση.

Συστήματα πολλαπλών επιπέδων ασφάλειας όπως είναι κωδικοί μιας χρήσης, πιστοποίηση μέσω τηλεφώνου και έξυπνες κάρτες προστατεύουν τις υπηρεσίες cloud επειδή δυσκολεύουν το έργο των εισβολέων στο να έχουν πρόσβαση με κλεμμένους κωδικούς. Η ρήξη στην ασφαλιστική εταιρία Anthem, που είχε ως αποτέλεσμα την κλοπή περισσότερων από 80 εκατομμύρια αρχεία πελατών, προήλθε από κλεμμένα διαπιστευτήρια. Αυτό συνέβη επειδή η εταιρία δεν είχε εφαρμόσει ασφάλεια πολλαπλών επιπέδων, και μόλις πήραν στα χέρια τους τα διαπιστευτήρια οι εισβολείς, κανείς δεν μπορούσε να τους σταματήσει.

Πολλοί προγραμματιστές κάνουν το λάθος να ενσωματώνουν διαπιστευτήρια και κλειδιά κρυπτογραφίας σε πηγαίο κώδικα και να τον αφήνουν σε δημόσιες ιστοσελίδες, όπως είναι το GitHub. Τα κλειδιά πρέπει να φυλάσσονται προσεκτικά, και να υπάρχει μια προστατευμένη υποδομή δημόσιου κλειδιού. Επίσης τα κλειδιά πρέπει να αλλάζονται συχνά, για να δυσκολεύουν τους επιτιθέμενους να χρησιμοποιούν κλειδιά που πήραν χωρίς εξουσιοδότηση.

Οργανώσεις που σκοπεύουν να συνδέσουν ταυτότητες με κάποιο πάροχο, πρέπει να καταλάβουν τα μέτρα προστασίας που χρησιμοποιεί ο πάροχος για την προστασία της πλατφόρμας ταυτοτήτων. Η συγκέντρωση όλων των ταυτοτήτων σε ένα κεντρικό σημείο έχει ρίσκα.

3.6.3 Χακαρισμένες διεπαφές και APIs

Πρακτικά κάθε εφαρμογή και υπηρεσία cloud προσφέρει APIs. Ομάδες IT χρησιμοποιούν διεπαφές και APIs για να διαχειριστούν και να αλληλοεπιδράσουν με τις cloud υπηρεσίες, μαζί με αυτές που προσφέρουν τροφοδοσία, διαχείριση, ενοργάνωση και παρακολούθηση.

Η ασφάλεια και η διαθεσιμότητα των cloud υπηρεσιών, από πιστοποίηση και έλεγχο πρόσβασης μέχρι τη κρυπτογράφηση και την παρακολούθηση δραστηριοτήτων, εξαρτούνται από την ασφάλεια των APIs. Το ρίσκο αυξάνεται με την συνεργασία τρίτων εταιριών, που εξαρτούνται από τα APIs και τις διεπαφές, επειδή οι εταιρίες πρέπει να προσφέρουν περισσότερες υπηρεσίες και διαπιστευτήρια σε αυτές. Αδύναμες διεπαφές και APIs εκθέτουν τις οργανώσεις σε θέματα ασφάλειας που σχετίζονται με εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και ευθύνη.

Τα APIs και οι διεπαφές είναι τα πιο εκτεθειμένα κομμάτια του συστήματος, επειδή συνήθως είναι διαθέσιμα από το ανοιχτό Διαδίκτυο. Η Cloud Security Alliance προτείνει επαρκείς ελέγχους, σαν την πρώτη γραμμή άμυνας και ανίχνευσης. Εφαρμογές και συστήματα μοντέλων απειλών, μαζί με ροές δεδομένων και αρχιτεκτονική/σχεδιασμός, γίνονται σημαντικά κομμάτια του κύκλου ανάπτυξης. Επίσης η Cloud Security Alliance προτείνει αξιολογήσεις κώδικα με βάση την ασφάλεια και δοκιμές διείσδυσης στα συστήματα.

3.6.4 Αξιοποίηση τρωτών σημείων του συστήματος

Τα τρωτά σημεία ή εκμεταλλεύσιμα σφάλματα σε προγράμματα δεν είναι καινούρια, αλλά έχουν γίνει ένα μεγαλύτερο πρόβλημα με την έλευση των πολλών πελατών σε ένα διακομιστή στο χώρο του cloud computing. Οι οργανώσεις μοιράζονται μνήμη, βάσεις δεδομένων και άλλους πόρους σε μικρή απόσταση μεταξύ τους, δημιουργώντας νέες περιοχές επίθεσης.

Ευτυχώς, επιθέσεις σε τρωτά σημεία του συστήματος μπορούν να μετριαστούν με βασικές διαδικασίες IT, λέει η Cloud Security Alliance. Οι καλύτερες πρακτικές είναι η τακτική σάρωση τρωτών σημείων, η έγκαιρη εφαρμογή patch και οι γρήγορες διορθώσεις σε αναφορές που αφορούν απειλές συστήματος.

Σύμφωνα με την Cloud Security Alliance, το κόστος μετρίασης τρωτών σημείων του συστήματος είναι σχετικά μικρότερο σε σύγκριση με άλλες IT δαπάνες. Η δαπάνη τοποθέτησης IT διαδικασιών για ανακάλυψη και επιδιόρθωση τρωτών σημείων, είναι μικρότερη σε σχέση με τη πιθανή ζημιά. Ρυθμιζόμενες βιομηχανίες πρέπει να εφαρμόζουν patch όσο γρηγορότερα μπορούν, επιθυμητά σαν μέρος μιας αυτόματης και επαναλαμβανόμενης διαδικασίας. Διαδικασίες ελέγχου αλλαγής που εφαρμόζουν επείγοντα patch διασφαλίζουν ότι η αποκατάσταση των δραστηριοτήτων είναι σωστά τεκμηριωμένη και επανεξετάζεται από τεχνικές ομάδες.

3.6.5 Κλοπή λογαριασμού

Απάτες, επικίνδυνο λογισμικό και phishing είναι ακόμη επιτυχημένα και οι cloud υπηρεσίες προσθέτουν μια καινούρια διάσταση στην απειλή, επειδή εισβολείς μπορούν να κρυφακούσουν σε δραστηριότητες, να παραποιήσουν συναλλαγές και να τροποποιήσουν δεδομένα. Οι εισβολείς μπορεί να είναι ικανοί να χρησιμοποιήσουν την cloud εφαρμογή για να προωθήσουν και άλλες επιθέσεις.

Κοινές στρατηγικές προστασίας άμυνας-εις-βάθος μπορούν να περιορίσουν την ζημιά που προκλήθηκε από μια ρήξη. Οι οργανώσεις πρέπει να απαγορέψουν τον διαμοιρασμό διαπιστευτηρίων λογαριασμών μεταξύ χρηστών και υπηρεσιών, καθώς και να ενεργοποιήσουν πιστοποίηση πολλών επιπέδων όπου αυτό είναι δυνατό. Οι λογαριασμοί, ακόμη και οι λογαριασμοί υπηρεσιών, πρέπει να παρακολουθούνται έτσι ώστε κάθε συναλλαγή να μπορεί να εντοπιστεί σε ένα ανθρώπινο ιδιοκτήτη. Το κλειδί είναι η προστασία των διαπιστευτηρίων λογαριασμών από κλοπή.

3.6.6 Εσωτερικές απειλές

Η εσωτερική απειλή έχει πολλά πρόσωπα: ένας τωρινός ή πρώην εργαζόμενος, ένας διαχειριστής συστήματος, ένας εργολάβος ή ένας επαγγελματικός συνεργάτης. Τα κίνητρα τους είναι από

κλοπή δεδομένων μέχρι εκδίκηση. Σε ένα σενάριο cloud, μια εσωτερική απειλή μπορεί να καταστρέψει ολόκληρες υποδομές ή να τροποποιήσει δεδομένα. Συστήματα που εξαρτούνται πλήρως από την ασφάλεια του παρόχου υπηρεσιών cloud, όπως είναι η κρυπτογραφία, βρίσκονται στο μεγαλύτερο κίνδυνο.

Η Cloud Security Alliance προτείνει οι οργανώσεις να ελέγχουν τα κλειδιά και την διαδικασία κρυπτογράφησης, να διαχωρίζουν τα καθήκοντα και να μειώσουν την πρόσβαση στους χρήστες. Αποτελεσματικό σύστημα εισόδου, παρακολούθησης και τακτικοί έλεγχοι στις δραστηριότητες των διαχειριστών είναι επίσης κρίσιμες.

Όπως παρατηρεί η Cloud Security Alliance, είναι εύκολο κάποιος να παρεξηγήσει μια λανθασμένη προσπάθεια σε μια δουλειά ρουτίνας ως κακόβουλη εσωτερική επίθεση. Ένα παράδειγμα είναι ένας διαχειριστής που αντέγραψε κατά λάθος μια ευαίσθητη βάση δεδομένων ενός πελάτη σε ένα δημόσιο διακομιστή. Κατάλληλη εκπαίδευση και διαχείριση για αποφυγή τέτοιων λαθών γίνεται ακόμη πιο κρίσιμη στο cloud, χάρη στην μεγαλύτερη πιθανότητα έκθεσης.

3.6.7 Το παράσιτο APT

Η Cloud Security Alliance ορθώς καλεί τις προηγμένες επίμονες απειλές (advanced persistent threats - APTs), παρασιτικές μορφές επιθέσεων. Οι APTs διεισδύουν σε συστήματα για να εγκατασταθούν και μετά να μεταδίδουν στους δημιουργούς τους αθόρυβα δεδομένα και πνευματική ιδιοκτησία σε ένα μεγάλο διάστημα χρόνου.

Οι APTs τυπικά κινούνται πλευρικά μέσω του δικτύου και ανακατεύονται με την κανονική κίνηση, ώστε ο εντοπισμός τους να είναι δύσκολος. Οι κύριοι πάροχοι cloud εφαρμόζουν προηγμένες τεχνικές για να εμποδίσουν τις APTs να διεισδύσουν στην υποδομή τους, αλλά οι πελάτες πρέπει να είναι επιμελείς στον εντοπισμό APTs στους cloud λογαριασμούς τους, όπως πρέπει να είναι και στους λογαριασμούς της εταιρίας τους.

Κοινά σημεία εισόδου περιλαμβάνουν spear phishing, απευθείας επιθέσεις, μονάδες USB φορτωμένες με malware και μη ασφαλή δίκτυα τρίτων. Συγκεκριμένα, η Cloud Security Alliance προτείνει να εκπαιδευτούν οι χρήστες ώστε να μπορούν να αναγνωρίζουν τεχνικές phishing.

Τακτικά προγράμματα ενίσχυσης της ευαισθητοποίησης κρατούν τους χρήστες έτοιμους και μειώνουν την πιθανότητα εισόδου κάποιου APT στο δίκτυο. Επίσης τα τμήματα IT πρέπει να ενημερώνονται συνεχώς για τις τελευταίες προηγμένες επιθέσεις. Προηγμένοι έλεγχοι ασφάλειας, διαχείριση διαδικασιών, σχέδια ανταπόκρισης συμβάντων και εκπαίδευση του IT προσωπικού, όλα αυτά οδηγούν σε αυξημένους προϋπολογισμούς ασφάλειας. Οι οργανώσεις πρέπει να υπολογίσουν αν αξίζουν αυτά τα κόστη απέναντι σε μια πιθανή οικονομική ζημιά που έχει προέλθει από επιτυχημένες επιθέσεις APT.

3.6.8 Μόνιμη απώλεια δεδομένων

Όσο το cloud ωριμάζει, αναφορές για μόνιμη απώλεια δεδομένων εξαιτίας λάθους του παρόχου έχουν γίνει πολύ σπάνιες. Αλλά κακόβουλοι εισβολείς είναι ικανοί να διαγράψουν μόνιμα cloud δεδομένα για να βλάψουν εταιρίες και τα cloud data centers είναι ευάλωτα σε φυσικές καταστροφές όπως κάθε άλλη εγκατάσταση.

Οι πάροχοι cloud προτείνουν κατανεμημένα δεδομένα και εφαρμογές, σε διάφορες ζώνες για αυξημένη προστασία. Επαρκή μέτρα αντιγράφων ασφάλειας δεδομένων είναι ουσιώδες, όπως και η τήρηση μέτρων επαναφοράς σε περίπτωση καταστροφής και η συνέχιση των εργασιών της επιχείρησης. Η ημερήσια δημιουργία εφεδρικών δεδομένων και η αποθήκευση τους σε διαφορετικό μέρος παραμένουν σημαντικά σε cloud περιβάλλοντα.

Το βάρος της πρόληψης απώλειας δεδομένων δεν βρίσκεται μόνο στον πάροχο cloud υπηρεσιών. Αν ένας πελάτης κρυπτογραφεί δεδομένα πριν τα μεταφέρει στο cloud, τότε αυτός ο πελάτης πρέπει να είναι προσεκτικός στην προστασία του κλειδιού κρυπτογράφησης. Όταν θα χαθεί το κλειδί, τότε θα χαθούν και τα δεδομένα.

Πολιτικές συμμόρφωσης συνήθως συμφωνούν στην διάρκεια που οι οργανώσεις πρέπει να διατηρούν αρχεία ελέγχου και άλλα έγγραφα. Η απώλεια τέτοιων δεδομένων μπορεί να οδηγήσεις σε ρυθμιστικές συνέπειες. Οι νέοι κανόνες προστασίας δεδομένων της Ευρωπαϊκής Ένωσης επίσης μεταχειρίζονται την καταστροφή δεδομένων και τη διαφθορά των προσωπικών στοιχείων σαν ρήξεις δεδομένων που απαιτούν την κατάλληλη γνωστοποίηση. Γνωρίστε τους κανόνες για να αποφύγετε το πρόβλημα.

3.6.9 Ανεπαρκής επιμέλεια

Οι οργανώσεις που χρησιμοποιούν το cloud χωρίς να καταλαβαίνουν πλήρως το περιβάλλον και τους σχετικούς κινδύνους ενδέχεται να αντιμετωπίσουν μια μυριάδα εμπορικών, οικονομικών, τεχνικών και νομικών ρίσκων προειδοποιεί η Cloud Security Alliance. Δέουσα επιμέλεια χρειάζεται όταν μια οργάνωση προσπαθεί να μεταναστεύσει στο cloud ή να συγχωνευτεί (ή να συνεργαστεί) με άλλη εταιρία στο cloud. Για παράδειγμα, οργανώσεις που αποτυγχάνουν να διερευνήσουν ένα συμβόλαιο μπορεί να μην είναι ενήμερες για την ευθύνη του παρόχου σε περίπτωση απώλειας δεδομένων ή ρήξης δεδομένων.

Επιχειρησιακά και αρχιτεκτονικά θέματα προκύπτουν εάν η ομάδα ανάπτυξης μιας εταιρίας δεν είναι εξοικειωμένη με τις τεχνολογίες cloud, όπως εφαρμογές που αναπτύσσονται σε ένα συγκεκριμένο cloud. Η Cloud Security Alliance υπενθυμίζει στις οργανώσεις ότι πρέπει να είναι πολύ προσεκτικές στην κατανόηση των ρίσκων που υποθέτουν όταν γίνονται συνδρομητές σε κάθε cloud υπηρεσία.

3.6.10 Κατάχρηση cloud υπηρεσιών

Οι cloud υπηρεσίες μπορούν να επιταχθούν για να υποστηρίξουν αισχρές δραστηριότητες, όπως η χρησιμοποίηση επεξεργαστικών πόρων cloud για το σπάσιμο ενός κλειδιού κρυπτογράφησης, με σκοπό την προώθηση μιας επίθεσης. Άλλα παραδείγματα περιλαμβάνουν τις επιθέσεις άρνησης υπηρεσίας, αποστολή spam και phishing μηνυμάτων ηλεκτρονικού ταχυδρομείου και η φιλοξενία κακόβουλου περιεχομένου.

Οι πάροχοι πρέπει να αναγνωρίσουν τύπους κατάχρησης, όπως η εξέταση κίνησης για ανίχνευση επιθέσεων άρνησης υπηρεσίας, και άλλα εργαλεία για τους πελάτες να παρακολουθούν την κατάσταση των cloud περιβαλλόντων τους. Οι πελάτες πρέπει να σιγουρευτούν ότι οι πάροχοι προσφέρουν ένα μηχανισμό για αναφορά κατάχρησης. Αν και οι πελάτες μπορεί να μην είναι ο κύριος στόχος για κακόβουλες πράξεις, η κατάχρηση cloud υπηρεσιών μπορεί να έχει σαν αποτέλεσμα την μείωση της διαθεσιμότητας και απώλεια δεδομένων.

3.6.11 Επιθέσεις άρνησης υπηρεσίας

Οι επιθέσεις άρνησης υπηρεσίας υπάρχουν εδώ και χρόνια, αλλά απέκτησαν την προσοχή των εισβολέων ξανά, χάρη στην ικανότητα τους να επηρεάζουν την διαθεσιμότητα των cloud υπηρεσιών. Τα συστήματα μπορούν να επιβραδυνθούν σε σημείο συρσίματος ή απλά να ξεμείνουν από χρόνο. Βιώνοντας μια επίθεση άρνησης υπηρεσίας είναι σαν να έχεις κολλήσει σε κίνηση την ώρα αιχμής, υπάρχει ένας δρόμος για να πας στον προορισμό σου και δεν υπάρχει τίποτα που μπορείς να κάνεις για αυτό, παρά μόνο να περιμένεις, λέει μια αναφορά.

Οι επιθέσεις άρνησης υπηρεσίας καταναλώνουν μεγάλες ποσότητες επεξεργαστικής δύναμης, ένα λογαριασμό που τελικά θα τον πληρώσει ο πελάτης. Ενώ οι επιθέσεις άρνησης υπηρεσίας υψηλής έντασης είναι πολύ κοινές, οι οργανώσεις πρέπει να είναι ενήμερες για ασύμμετρες, επιπέδου εφαρμογής επιθέσεις άρνησης υπηρεσίας, οι οποίες έχουν σαν στόχο διακομιστές Διαδικτύου και τρωτά σημεία βάσεων δεδομένων.

Οι πάροχοι cloud τείνουν να είναι καλύτεροι στην αντιμετώπιση επιθέσεων άρνησης υπηρεσίας από τους πελάτες τους. Το κλειδί είναι η ύπαρξη ενός σχεδίου για τη μετρίαση της επίθεσης πριν αυτή συμβεί, έτσι ώστε οι διαχειριστές να έχουν πρόσβαση σε αυτούς τους πόρους όταν τους χρειαστούν.

3.6.12 Κοινή τεχνολογία, κοινοί κίνδυνοι

Τρωτά σημεία σε κοινή τεχνολογία είναι μια σημαντική απειλή για το cloud computing. Οι πάροχοι cloud υπηρεσιών μοιράζονται υποδομές, πλατφόρμες και εφαρμογές και αν ένα τρωτό σημείο εμφανιστεί σε κάποιο από αυτά τα επίπεδα, τότε τους επηρεάζει όλους. Ένα τρωτό σημείο ή μια λάθος ρύθμιση μπορεί να διακινδυνεύσει ολόκληρο το cloud ενός παρόχου, λέει μια αναφορά.

Εάν ένα αναπόσπαστο συστατικό τεθεί υπό κίνδυνο, όπως ένας hypervisor, ένα συστατικό μιας κοινής πλατφόρμας ή μια εφαρμογή, εκθέτει όλο το σύστημα σε κίνδυνο ρήξης. Η Cloud Security Alliance προτείνει μια στρατηγική άμυνας-εις-βάθος, που να περιλαμβάνει πιστοποίηση

πολλών επιπέδων σε όλους τους χρήστες, συστήματα ανίχνευσης εισβολών σε χρήστες και το δίκτυο, οι χρήστες να έχουν τα απολύτως απαραίτητα δικαιώματα και όχι παραπάνω, κατάτμηση του δικτύου και η επιδιόρθωση κοινών πόρων όταν χρειάζεται. (The dirty dozen: 12 cloud security threats 2016)

3.7 HTTPS (Hypertext Transfer Protocol Secure)

Το HTTPS είναι ένα πρωτόκολλο για ασφαλή επικοινωνία μέσω ενός δικτύου υπολογιστών, το οποίο χρησιμοποιείται ευρέως στο Διαδίκτυο. Το HTTPS είναι η επικοινωνία μέσω HTTP, διαμέσου μιας σύνδεσης κρυπτογραφημένη με TLS (Transport Layer Security) ή SSL (Secure Sockets Layer). Το κύριο κίνητρο για το HTTPS είναι η πιστοποίηση της ιστοσελίδας που έχουμε επισκεφτεί και η προστασία της ιδιωτικότητας και η ακεραιότητα των ανταλλασσόμενων δεδομένων.

Η ασφάλεια του HTTPS βασίζεται στο TLS, το οποίο τυπικά χρησιμοποιεί μακροπρόθεσμα δημόσια και ιδιωτικά κλειδιά για τη δημιουργία ενός βραχυπρόθεσμου κλειδιού συνεδρίας, το οποίο χρησιμοποιείται για την κρυπτογράφηση της ροής δεδομένων μεταξύ του πελάτη και του διακομιστή. Πιστοποιητικά X.509 χρησιμοποιούνται για να πιστοποιήσουν το διακομιστή (και μερικές φορές και τον πελάτη). Σαν αποτέλεσμα, αρχές έκδοσης πιστοποιητικών και πιστοποιητικά δημόσιου κλειδιού είναι απαραίτητα για την επαλήθευση της σχέσης μεταξύ του πιστοποιητικού και του ιδιοκτήτη του, όπως επίσης η παραγωγή, υπογραφή και παροχή της εγκυρότητας του πιστοποιητικού.

Μία ιστοσελίδα πρέπει να είναι φιλοξενημένη εξ ολοκλήρου σε HTTPS, χωρίς να έχει κομμάτια του περιεχομένου της φορτωμένα σε HTTP, για παράδειγμα μπορεί μερικά scripts να μην έχουν φορτωθεί με ασφάλεια, ή ο χρήστης θα είναι ευάλωτος σε κάποιες επιθέσεις και σε εξωτερική παρατήρηση. Επίσης έχοντας μόνο μια συγκεκριμένη σελίδα που περιέχει ευαίσθητα δεδομένα (όπως μια σελίδα εισόδου) μιας ιστοσελίδας φορτωμένη με HTTPS, ενώ η υπόλοιπη είναι φορτωμένη με απλό HTTP, θα εκθέσει το χρήστη σε επιθέσεις. Σε μια ιστοσελίδα που έχει ευαίσθητα δεδομένα σε κάποια σελίδα της, κάθε φορά που κάποιος έχει πρόσβαση στην ιστοσελίδα με HTTP αντί για HTTPS, ο χρήστης και η συνεδρία θα εκθέτονται σε κίνδυνο.

Παρόμοια, cookies σε μια ιστοσελίδα σερβιρισμένα μέσω HTTPS πρέπει να έχουν ενεργοποιημένη την ιδιότητα της ασφάλειας.

3.7.1 Διαφορές από το HTTP

Τα URLs του HTTPS ξεκινούν με https:// και χρησιμοποιούν ως προεπιλεγμένη την θύρα 443, ενώ του HTTP ξεκινούν με http:// και χρησιμοποιούν ως προεπιλεγμένη την θύρα 80.

Το HTTP δεν είναι κρυπτογραφημένο και είναι ευάλωτο σε επιθέσεις υποκλοπών και man in the middle, οι οποίες μπορούν να δώσουν πρόσβαση στους εισβολείς σε λογαριασμούς ιστοσελίδων και ευαίσθητα δεδομένα, οι οποίοι μπορούν να τροποποιήσουν ιστοσελίδες και να προσθέσουν malware ή διαφημίσεις. Το HTTPS είναι σχεδιασμένο για να αντέχει τέτοιες επιθέσεις και θεωρείται ασφαλές απέναντι σε αυτές (με την εξαίρεση παλαιότερων εκδόσεων του SSL).

3.7.2 Επίπεδα Δικτύου

Το HTTP λειτουργεί στο μεγαλύτερο επίπεδο του μοντέλου TCP/IP, το επίπεδο Εφαρμογής, όπως το πρωτόκολλο ασφάλειας TLS (λειτουργώντας σαν ένα μικρότερο υποεπίπεδο του ίδιου επιπέδου), το οποίο κρυπτογραφεί ένα HTTP μήνυμα πριν την μετάδοση και αποκρυπτογραφεί ένα μήνυμα όταν καταφτάνει. Ακριβολογώντας, το HTTPS δεν είναι ένα διαφορετικό πρωτόκολλο, αλλά αναφέρεται στη χρήση απλού HTTP διαμέσου μιας κρυπτογραφημένης σύνδεσης SSL/TLS.

Όλα σε ένα HTTPS μήνυμα είναι κρυπτογραφημένα, συμπεριλαμβανομένων των επικεφαλίδων, και το φόρτο request/response. Με την εξαίρεση της πιθανής κρυπτογραφικής επίθεσης CCA, ο εισβολέας μπορεί να γνωρίζει μόνο ότι μια σύνδεση είναι ενεργή μεταξύ των δύο πλευρών, τα domain names και τις διευθύνσεις IP. (HTTPS 2016)

3.8 Κρυπτογράφηση

Η κρυπτογράφηση είναι η διαδικασία κωδικοποίησης μηνυμάτων ή πληροφοριών με τέτοιο τρόπο που αναγνωρίζονται μόνο από εξουσιοδοτημένα άτομα. Η κρυπτογράφηση από μόνη της δεν αποτρέπει την υποκλοπή μηνυμάτων, αλλά προστατεύει το περιεχόμενο των μηνυμάτων. Στη διαδικασία της κρυπτογράφησης, το μήνυμα ή οι πληροφορίες που θέλουμε να στείλουμε, που ονομάζονται απλό κείμενο (plaintext), κρυπτογραφούνται με τη χρήση ενός αλγορίθμου κρυπτογράφησης, δημιουργώντας το κρυπτογραφημένο μήνυμα (ciphertext), το οποίο μπορεί να διαβαστεί αν αποκρυπτογραφηθεί. Για τεχνικούς λόγους, η διαδικασία της κρυπτογράφησης συνήθως χρησιμοποιεί ένα ψευδό-τυχαίο κλειδί κρυπτογράφησης που δημιουργείτε από έναν αλγόριθμο. Είναι πιθανόν κάποιος να αποκρυπτογραφήσει το μήνυμα χωρίς να έχει στην κατοχή του το κλειδί, αλλά για μια καλοσχεδιασμένη διαδικασία κρυπτογράφησης χρειάζονται μεγάλοι υπολογιστικοί πόροι. Ένας εξουσιοδοτημένος παραλήπτης μπορεί εύκολα να αποκρυπτογραφήσει το μήνυμα με το κλειδί που του έχει δώσει ο αποστολέας, αλλά όχι οι ανεπιθύμητοι εισβολείς.

Ο σκοπός της κρυπτογράφησης είναι η διασφάλιση ότι κάποιος που είναι εξουσιοδοτημένος να έχει πρόσβαση σε δεδομένα (π.χ. αρχείο κειμένου ή αρχείο), θα μπορεί να τα διαβάσει χρησιμοποιώντας το κλειδί αποκρυπτογράφησης.

3.8.1 Τύποι κρυπτογράφησης

3.8.1.1 Κρυπτογράφηση συμμετρικού κλειδιού

Σε διαδικασίες συμμετρικού κλειδιού, τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης είναι τα ίδια. Οι δύο πλευρές πρέπει να έχουν το ίδιο κλειδί για να έχουν επιτυχημένη επικοινωνία.

3.8.1.2 Κρυπτογράφηση δημόσιου κλειδιού

Στις διαδικασίες δημόσιου κλειδιού, το κλειδί κρυπτογράφησης είναι διαθέσιμο σε όλους για να το χρησιμοποιήσουν για κρυπτογράφηση. Αλλά μόνο ο παραλήπτης έχει πρόσβαση στο κλειδί αποκρυπτογράφησης, που του επιτρέπει να διαβάζει τα μηνύματα. Η κρυπτογράφηση δημόσιου κλειδιού περιγράφτηκε πρώτα σε ένα μυστικό κείμενο το 1973. Πριν όλες οι διαδικασίες κρυπτογράφησης ήταν συμμετρικού κλειδιού (αλλιώς λεγόταν ιδιωτικού κλειδιού). (Encryption 2016)

3.9 Secure Shell

Secure Shell (SSH) είναι ένα κρυπτογραφικό πρωτόκολλο δικτύου για χειρισμό υπηρεσιών δικτύου με ασφάλεια μέσω ενός μη ασφαλούς δικτύου. Η γνωστότερη εφαρμογή του είναι η απομακρυσμένη πρόσβαση σε υπολογιστές από χρήστες.

Το SSH παρέχει ένα ασφαλές κανάλι διαμέσου ενός μη ασφαλούς δικτύου σε αρχιτεκτονική πελάτη-διακομιστή, συνδέοντας ένα πελάτη SSH με ένα διακομιστή SSH. Κοινές εφαρμογές περιλαμβάνουν την απομακρυσμένη σύνδεση με γραμμή εντολών και απομακρυσμένη εκτέλεση εντολών, αλλά οποιαδήποτε υπηρεσία δικτύου μπορεί να ασφαλιστεί με SSH. Ο προσδιορισμός του πρωτοκόλλου διακρίνει μεταξύ δύο εκδόσεων, τις εκδόσεις SSH-1 και SSH-2.

Η πιο εμφανής εφαρμογή του πρωτοκόλλου είναι η πρόσβαση σε shell λογαριασμούς σε λειτουργικά συστήματα Unix, αλλά βλέπουμε μια μικρή χρήση στα λειτουργικά Windows.

3.9.1 Ορισμός

Το SSH χρησιμοποιεί κρυπτογράφηση δημόσιου κλειδιού για να πιστοποιήσει τον απομακρυσμένο υπολογιστή και να του επιτρέψει να πιστοποιήσει και τον χρήστη, αν χρειαστεί. Υπάρχουν πολλοί τρόποι να χρησιμοποιήσει κάποιος το SSH, ένας είναι να χρησιμοποιεί ζεύγη

κλειδιών δημόσιου κλειδιού που παράγονται αυτόματα για να κρυπτογραφεί απλές συνδέσεις δικτύου και μετά να χρησιμοποιεί κωδικούς πιστοποίησης για σύνδεση.

Ένας άλλος τρόπος είναι η χρησιμοποίηση ενός ζευγαριού δημόσιου κλειδιού που παράγεται από το χρήστη για να γίνει η πιστοποίηση, επιτρέποντας σε χρήστες και προγράμματα να συνδέονται χωρίς την χρήση κωδικού. Σε αυτό το σενάριο, οποιοσδήποτε μπορεί να παράγει ένα ζευγάρι διαφορετικών κλειδιών (δημόσιων και ιδιωτικών). Το δημόσιο κλειδί τοποθετείτε σε όλους τους υπολογιστές που πρέπει να επιτρέψουν πρόσβαση στο αντίστοιχο ιδιωτικό κλειδί (ο ιδιοκτήτης κρατάει το ιδιωτικό κλειδί μυστικό). Ενώ η πιστοποίηση βασίζεται στο ιδιωτικό κλειδί, το ίδιο το κλειδί δεν μεταφέρεται διαμέσου του δικτύου κατά τη διάρκεια της πιστοποίησης. Το SSH επαληθεύει αν το ίδιο πρόσωπο που προσφέρει το δημόσιο κλειδί, έχει στη κατοχή του το αντίστοιχο ιδιωτικό κλειδί. Σε όλες τις εκδόσεις του SSH είναι σημαντικό να επαληθεύουμε άγνωστα δημόσια κλειδιά, δηλαδή να συνδέσουμε τα δημόσια κλειδιά με ταυτότητες, πριν τα δεχτούμε σαν έγκυρα. Η αποδοχή ενός δημόσιου κλειδιού που ανήκει σε εισβολέα χωρίς νομιμοποίηση θα εξουσιοδοτήσει έναν εισβολέα σαν νόμιμο χρήστη.

3.9.2 Διαχείριση κλειδιών

Σε λειτουργικά συστήματα Unix, η λίστα πιστοποιημένων δημόσιων κλειδιών τυπικά βρίσκεται αποθηκευμένη στο φάκελο home του χρήστη που του επιτρέπεται να συνδέεται απομακρυσμένα, στο αρχείο /.ssh/authorized_keys. Αυτό το αρχείο είναι έγκυρο για το SSH μόνο αν είναι συνταγμένο από τον ιδιοκτήτη και το root. Όταν το δημόσιο κλειδί είναι παρόν στην απομακρυσμένη πλευρά και το αντίστοιχο ιδιωτικό κλειδί είναι παρόν στην τοπική πλευρά, η χρήση κωδικού δεν χρειάζεται πλέον. Ωστόσο, για περισσότερη ασφάλεια το ιδιωτικό κλειδί μπορεί να κλειδωθεί με κωδικό.

Το ιδιωτικό κλειδί μπορεί να βρεθεί σε συγκεκριμένα μέρη, και η πλήρης διαδρομή μπορεί να καθοριστεί από τη γραμμή εντολών (η επιλογή –i για ssh). Το ssh-keygen παράγει τα δημόσια και ιδιωτικά κλειδιά, πάντα σε ζευγάρια.

Το SSH επίσης υποστηρίζει πιστοποίηση με χρήση κωδικού που είναι κρυπτογραφημένη με αυτόματα παραγόμενα κλειδιά. Σε αυτήν την περίπτωση ο εισβολέας μπορεί να μιμηθεί την

πλευρά του νόμιμου διακομιστή, να ζητήσει τον κωδικό και να τον λάβει (man-in-the-middle attack). Ωστόσο, αυτό είναι πιθανόν μόνο αν οι δύο πλευρές δεν έχουν πιστοποιηθεί στο παρελθόν, επειδή το SSH θυμάται το κλειδί που είχε χρησιμοποιήσει ο διακομιστής. Ο πελάτης SSH αναρτά μια προειδοποίηση πριν δεχτεί το κλειδί ενός καινούριου άγνωστου διακομιστή. Η πιστοποίηση με χρήση κωδικού μπορεί να απενεργοποιηθεί.

3.9.3 Χρήση

Το SSH χρησιμοποιείται τυπικά για σύνδεση σε απομακρυσμένες μηχανές και για την εκτέλεση εντολών, αλλά επίσης υποστηρίζει tunneling, forwarding TCP ports και X11 συνδέσεις. Μπορεί να μεταφέρει αρχεία χρησιμοποιώντας το SSH file transfer (SFTP) ή secure copy (SCP) πρωτόκολλο. Το SSH χρησιμοποιεί το μοντέλο πελάτη-διακομιστή.

Η θύρα TCP 22 έχει ανατεθεί για την επικοινωνία SSH διακομιστών.

Ένα πρόγραμμα πελάτη SSH χρησιμοποιείται για την ίδρυση συνδέσεων σε ένα SSH daemon που δέχεται απομακρυσμένες συνδέσεις. Και τα δύο είναι συνήθως παρόν στα περισσότερα σύγχρονα λειτουργικά συστήματα, συμπεριλαμβανομένου του Mac OS X, τις περισσότερες διανομές GNU/Linux, OpenBSD, FreeBSD, NetBSD, Solaris και OpenVMS. Ιδιαίτερα το Windows είναι ένα από τα λίγα μοντέρνα λειτουργικά συστήματα που δεν περιλαμβάνει SSH.

Το SSH είναι σημαντικό στο cloud computing για την επίλυση προβλημάτων σύνδεσης, αποτρέποντας τα θέματα ασφάλειας που θα προκύπταν αν μια εικονική μηχανή cloud εκθέτονταν απευθείας στο Διαδίκτυο. Ένα SSH tunnel μπορεί να προσφέρει ένα ασφαλές μονοπάτι μέσω του Διαδικτύου, διαμέσου ενός firewall σε μια εικονική μηχανή. (Secure Shell 2016)

3.10 Firewall

Το firewall είναι ένα σύστημα ασφάλειας δικτύου που παρακολουθεί και ελέγχει την εισερχόμενη και εξερχόμενη κίνηση του δικτύου ακολουθώντας κάποιους προκαθορισμένους

κανόνες ασφάλειας. Ένα firewall τυπικά εγκαθιδρύει ένα φράγμα μεταξύ ενός έμπιστου, ασφαλούς δικτύου και ενός εξωτερικού δικτύου, όπως είναι το Διαδίκτυο, το οποίο υποθέτουμε ότι δεν είναι ασφαλές και έμπιστο. Τα firewall συνήθως κατηγοριοποιούνται σαν firewall δικτύου ή τοπικά firewall. Τα firewall δικτύου είναι λογισμικό που εκτελείται σε υλικό γενικής χρήσης ή μπορούν να εκτελούνται σε συγκεκριμένο υλικό, με εξειδικευμένο λογισμικό που φιλτράρουν την κίνηση μεταξύ δύο ή και παραπάνω δικτύων. Τα τοπικά firewall προσφέρουν ένα επίπεδο λογισμικού που ελέγχει την κίνηση δικτύου της συγκεκριμένης μηχανής. Οι εφαρμογές firewall μπορούν επίσης να προσφέρουν και άλλες δυνατότητες στο εσωτερικό δίκτυο που προστατεύουν, όπως DHCP ή VPN διακομιστή για το δίκτυο.

3.10.1 Τύποι

Τα firewall διαφέρουν ανά τύπο ανάλογα από που προέρχεται η επικοινωνία, από που ανακόπτουν την κίνηση του δικτύου και το τύπο της επικοινωνίας που παρακολουθούν.

3.10.1.1 Επίπεδο δικτύου ή φίλτρα πακέτων

Τα firewall επιπέδου δικτύου, λέγονται επίσης και φίλτρα πακέτων, λειτουργούν σε ένα χαμηλό επίπεδο της στοίβας πρωτοκόλλων TCP/IP, δεν επιτρέπουν πακέτα να περάσουν μέσω του firewall εκτός αν ταιριάζουν με τους κανόνες που έχουν ρυθμιστεί. Ο διαχειριστής του firewall επιτρέπεται να καθορίσει τους κανόνες ή αλλιώς ισχύουν οι προεπιλεγμένες ρυθμίσεις. Ο όρος φίλτρο πακέτων προέρχεται από τα λειτουργικά συστήματα BSD.

Τα firewall επιπέδου δικτύου γενικά χωρίζονται σε δύο υποκατηγορίες: με κατάσταση και χωρίς κατάσταση. Τα firewall με κατάσταση διατηρούν πληροφορίες από τις ενεργές συνεδρίες, και τις χρησιμοποιούν για να αυξήσουν την ταχύτητα επεξεργασίας πακέτων. Κάθε υφιστάμενη σύνδεση δικτύου μπορεί να περιγραφτεί με διάφορες ιδιότητες, την IP διεύθυνση του αποστολέα και του προορισμού, θύρες UDP ή TCP, και την τωρινή κατάσταση του χρόνου ζωής της σύνδεσης (μαζί με την έναρξη της συνεδρίας, handshake, δεδομένα μεταφοράς). Εάν ένα πακέτο

δεν ταιριάζει με μια υπάρχουσα σύνδεση, τότε θα αξιολογηθεί σύμφωνα με τους κανόνες που αφορούν νέες συνδέσεις. Εάν ένα πακέτο ταιριάζει με μια υπάρχουσα σύνδεση, συγκρίνοντας το με το πίνακα κατάστασης του firewall, τότε θα του επιτραπεί η είσοδος χωρίς περαιτέρω επεξεργασία.

Τα firewall χωρίς κατάσταση απαιτούν λιγότερη μνήμη και μπορούν να είναι γρηγορότερα για απλά φίλτρα που απαιτούν λιγότερο χρόνο για να φιλτράρουν παρά να ψάξουν μια συνεδρία. Μπορεί και να είναι απαραίτητα για να φιλτράρουν πρωτόκολλα δικτύου χωρίς κατάσταση, που δεν γνωρίζουν την έννοια της συνεδρίας. Ωστόσο, δεν μπορούν να κάνουν παραπάνω πολύπλοκες αποφάσεις βασισμένες σε ποιο στάδιο επικοινωνίας βρίσκονται οι υπολογιστές.

Νεότερα firewall μπορούν να φιλτράρουν κίνηση βασισμένα σε ιδιότητες πακέτων όπως διεύθυνση IP αποστολέα, θύρα αποστολέα, διεύθυνση IP προορισμού ή θύρα, υπηρεσία προορισμού π.χ. WWW ή FTP. Μπορούν να φιλτράρουν με βάση πρωτόκολλα, TTL αξίες και άλλες ιδιότητες.

Τα πιο δημοφιλή φίλτρα πακέτων σε διάφορες εκδόσεις του Unix είναι τα IPFilter, ipfw (FreeBSD/Mac OS X), NPF (NetBSD), PF (OpenBSD, BSDs), iptables/ipchains (Linux).

3.10.1.2 Επίπεδο εφαρμογής

Τα firewall επιπέδου εφαρμογής δουλεύουν στο επίπεδο εφαρμογής της στοίβας TCP/IP (δηλ. όλη η κίνηση των προγραμμάτων περιηγητών ή όλη η κίνηση telnet ή ftp) και μπορούν να αναχαιτίσουν όλα τα πακέτα που ταξιδεύουν από ή προς μια εφαρμογή. Μπλοκάρουν τα άλλα πακέτα (συνήθως χωρίς να το ξέρει ο αποστολέας).

Στην επιθεώρηση όλων των πακέτων για ακατάλληλο περιεχόμενο, τα firewall μπορούν να περιορίσουν ή να αποτρέψουν εντελώς την εξάπλωση Trojans και computer worms. Το επιπλέον κριτήριο επιθεώρησης μπορεί να προσθέσει παραπάνω καθυστέρηση στην αποστολή των πακέτων στον προορισμό τους.

Τα firewall εφαρμογής λειτουργούν καθορίζοντας αν μια διαδικασία πρέπει να δεχτεί οποιαδήποτε σύνδεση. Τα firewall εφαρμογής πετυχαίνουν την λειτουργία τους συνδέοντας σε

socket calls για να φιλτράρουν τις συνδέσεις μεταξύ του επιπέδου εφαρμογής και των κατώτερων επιπέδων του μοντέλου OSI. Τα firewall εφαρμογής που συνδέονται σε socket calls λέγονται επίσης φίλτρα socket. Τα firewall εφαρμογής δουλεύουν σαν ένα φίλτρο πακέτων αλλά τα φίλτρα εφαρμογής εφαρμόζουν κανόνες φιλτραρίσματος ανάλογα την διαδικασία, αντίθετα με τα φίλτρα πακέτων που φιλτράρουν ανάλογα την θύρα. Είναι σπάνιο να βρεις firewall εφαρμογής να μην είναι συνδυασμένα ή να χρησιμοποιούνται μαζί με φίλτρα πακέτων.

Επίσης τα firewall εφαρμογής φιλτράρουν περαιτέρω συνδέσεις εξετάζοντας την διαδικασία ID των πακέτων δεδομένων χρησιμοποιώντας ένα σύνολο κανόνων για την τοπική διαδικασία που συμμετέχει στην μετάδοση δεδομένων. Το μέγεθος του φιλτραρίσματος που εμφανίζεται ορίζεται από τους παρεχόμενους κανόνες. Δεδομένου της ποικιλίας του λογισμικού που υπάρχει, τα firewall εφαρμογής έχουν μόνο πολύπλοκους κανόνες για τις κανονικές υπηρεσίες, όπως υπηρεσίες διαμοιρασμού. Αυτοί οι κανόνες ανά διαδικασία έχουν μειωμένη αποτελεσματικότητα στο φιλτράρισμα κάθε πιθανής σχέσης που μπορεί να προκύψει με άλλες διαδικασίες. Επίσης αυτοί οι κανόνες ανά διαδικασίες δεν μπορούν να αμυνθούν απέναντι σε τροποποιημένες διαδικασίες, όπως διαφθορά μνήμης. Εξαιτίας αυτών των περιορισμών, τα firewall εφαρμογής αρχίζουν να αντικαθίστανται από μια νέα γενιά firewall εφαρμογής που βασίζονται στον υποχρεωτικό έλεγχο πρόσβασης (mandatory access control - MAC), επίσης λέγεται και sandbox, για την προστασία ευάλωτων υπηρεσιών.

3.10.1.3 Proxies

Ένας διακομιστής proxy (που εκτελείται σε συγκεκριμένο υλικό ή ως λογισμικό σε ένα μηχάνημα γενικού σκοπού) μπορεί να λειτουργήσει ως firewall ανταποκρίνοντας σε εισερχόμενα πακέτα (αιτήσεις σύνδεσης για παράδειγμα) σαν μια εφαρμογή, ενώ μπλοκάρει άλλα πακέτα. Ένας διακομιστής proxy είμαι μια διέξοδος από ένα δίκτυο σε ένα άλλο για μια συγκεκριμένη εφαρμογή δικτύου, με την έννοια ότι λειτουργεί στην θέση του χρήστη του δικτύου.

Οι proxy κάνουν την αλλοίωση ενός εσωτερικού συστήματος από το εξωτερικό δίκτυο δυσκολότερη και η κακή χρήση ενός εσωτερικού συστήματος δεν θα προκαλέσει ρήξη ασφάλειας απ’ έξω από το firewall (όσο ο proxy εφαρμογής παραμένει άθικτος και σωστά

ρυθμισμένος). Αντιστρόφως, εισβολείς ενδέχεται να πάρουν υπό τον έλεγχο τους ένα δημόσια διαθέσιμο σύστημα και να το χρησιμοποιήσουν σαν proxy για τους δικούς τους σκοπούς, ο proxy τότε μεταμφιέζεται σαν αυτό το σύστημα σε άλλες εσωτερικές μηχανές. Ενώ η χρήση θέσεων εσωτερικών διευθύνσεων ενισχύει την ασφάλεια, crackers ενδέχεται να χρησιμοποιήσουν μεθόδους όπως IP spoofing για να προσπαθήσουν να περάσουν πακέτα σε ένα δίκτυο στόχο.

3.10.1.4 Μετάφραση διευθύνσεων δικτύου

Τα firewall συνήθως έχουν δυνατότητα μετάφρασης διευθύνσεων δικτύου (network address translation - NAT), και οι υπολογιστές που είναι προστατευμένοι πίσω από ένα firewall, έχουν διευθύνσεις που ανήκουν στην ιδιωτική περιοχή διευθύνσεων. Τα firewall έχουν συχνά την δυνατότητα να κρύβουν την αληθινή διεύθυνση των προστατευόμενων υπολογιστών. Αρχικά, η λειτουργία NAT αναπτύχθηκε για να αντιμετωπίσει τον περιορισμένο αριθμό IPv4 διευθύνσεων που μπορούσαν να χρησιμοποιηθούν ή ήταν ανατεθειμένες σε εταιρίες ή άτομα, καθώς και να μειώσει το ποσό και το κόστος της απόκτησης αρκετών δημόσιων διευθύνσεων για κάθε υπολογιστή σε μια οργάνωση. Αν και το NAT μόνο του δεν θεωρείται χαρακτηριστικό ασφάλειας, η απόκρυψη των διευθύνσεων των προστατευόμενων συσκευών έχει γίνει μια συνήθης άμυνα κατά της αναγνώρισης δικτύου. (Firewall (computing) 2016)

3.11 Πιστοποίηση χρήστη

Η πιστοποίηση είναι ένα απαραίτητο συστατικό ενός τυπικού μοντέλου ασφάλειας. Είναι η διαδικασία της επιβεβαίωσης της ταυτότητας ενός χρήστη (ή σε μερικές περιπτώσεις, μιας μηχανής) που προσπαθεί να συνδεθεί ή να έχει πρόσβαση σε πόρους. Υπάρχουν πολλοί διαφορετικοί μηχανισμοί πιστοποίησης, αλλά όλοι τους εξυπηρετούν τον ίδιο σκοπό.

3.11.1 Πιστοποίηση και εξουσιοδότηση

Είναι εύκολο να μπερδέψει κάποιος την πιστοποίηση με ένα άλλο συστατικό ασφάλειας: την εξουσιοδότηση. Ενώ η πιστοποίηση επαληθεύει την ταυτότητα του χρήστη, η εξουσιοδότηση επαληθεύει αν ο χρήστης έχει τα σωστά δικαιώματα πρόσβασης στους πόρους που θέλει. Όπως βλέπετε τα δύο αυτά συστατικά δουλεύουν μαζί. Πρώτα εμφανίζεται η πιστοποίηση και μετά η εξουσιοδότηση.

Για παράδειγμα, όταν ένα χρήστης που ανήκει σε ένα Windows domain συνδεθεί σε ένα δίκτυο, η ταυτότητα του θα επαληθευτεί μέσω ενός τύπου πιστοποίησης. Τότε χορηγείτε στον χρήστη ένα access token, το οποίο περιέχει πληροφορίες για τις ομάδες ασφάλειας στις οποίες ανήκει ο χρήστης. Όταν ο χρήστης προσπαθεί να χρησιμοποιήσει ένα δικτυακό πόρο (π.χ. να ανοίξει ένα αρχείο, να εκτυπώσει σε ένα εκτυπωτή), η λίστα ελέγχου πρόσβασης (access control list - ACL) που σχετίζεται με το συγκεκριμένο πόρο ελέγχεται με το access token. Εάν η λίστα δείχνει ότι τα μέλη της ομάδας των διευθυντών έχουν τα δικαιώματα για πρόσβαση στον πόρο και το access token του χρήστη δείχνει ότι είναι μέλος της ομάδας των διευθυντών, τότε σε αυτόν το χρήστη θα παραχωρηθεί πρόσβαση (εκτός αν ο λογαριασμός του χρήστη, ή η ομάδα στην οποία ανήκει ο χρήστης, έχει απαγορευτεί ρητά η πρόσβαση στον πόρο).

3.11.2 Πιστοποίηση σύνδεσης

Τα περισσότερα λειτουργικά συστήματα δικτύου απαιτούν από ένα χρήστη να πιστοποιηθεί για να συνδεθεί στο δίκτυο. Αυτό μπορεί να γίνει πατώντας έναν κωδικό, εισάγοντας μια έξυπνη κάρτα και πατώντας το PIN, με τη χρήση δακτυλικού αποτυπώματος, δείγματος φωνής ή σάρωση του ματιού, ή χρησιμοποιώντας κάποιο άλλο τρόπο για να αποδείξει στο σύστημα ότι είναι αυτός που υποστηρίζει ότι είναι.

3.11.3 Πιστοποίηση πρόσβασης δικτύου

Η πιστοποίηση πρόσβασης δικτύου επαληθεύει την ταυτότητα του χρήστη σε κάθε υπηρεσία δικτύου που ο χρήστης προσπαθεί να εισέλθει. Διαφέρει από άλλες, επειδή αυτή η διαδικασία πιστοποίησης είναι, στις περισσότερες περιπτώσεις, μη ορατή στο χρήστη εφόσον έχει συνδεθεί. Αλλιώς, ο χρήστης θα έπρεπε να ξανά εισάγει τον κωδικό του ή να παρέχει άλλα διαπιστευτήρια κάθε φορά που θα ήθελε να χρησιμοποιήσει μια υπηρεσία δικτύου ή πόρο άλλου δικτύου.

3.11.4 Πιστοποίηση IPSec

Η ασφάλεια IP (IP security) παρέχει στους χρήστες τα μέσα για κρυπτογράφηση και υπογραφή μηνυμάτων που στέλνονται δια μέσου του δικτύου για να εξασφαλίσουν την εμπιστευτικότητα, ακεραιότητα και αυθεντικότητα τους. Οι μεταδόσεις IPSec μπορούν να χρησιμοποιήσουν μια ποικιλία μεθόδων πιστοποίησης, συμπεριλαμβανομένου του πρωτοκόλλου Kerberos, πιστοποιητικά δημόσιου κλειδιού που έχουν εκδοθεί από μια έμπιστη αρχή έκδοσης πιστοποιητικών, ή ένα απλό μυστικό κλειδί (μια σειρά από χαρακτήρες γνωστή στον αποστολέα και παραλήπτη).

Μια σημαντική παρατήρηση είναι ότι και οι δύο υπολογιστές, του αποστολέα και του παραλήπτη, πρέπει να είναι ρυθμισμένοι να χρησιμοποιούν μία κοινή μέθοδο πιστοποίησης, αλλιώς δεν θα μπορούν να πραγματοποιήσουν ασφαλείς επικοινωνίες.

3.11.5 Απομακρυσμένη πιστοποίηση

Υπάρχουν πολλές μέθοδοι πιστοποίησης που μπορούν να χρησιμοποιηθούν για να επιβεβαιώσουν την ταυτότητα των χρηστών που συνδέονται στο δίκτυο μέσω μιας απομακρυσμένης σύνδεσης όπως είναι dial up ή VPN. Αυτές είναι:

- Το Password Authentication Protocol (PAP)

- Το Shiva PAP (SPAP)
- Το Challenge Handshake Authentication Protocol (CHAP)
- Το Microsoft CHAP (MS-CHAP)
- Το Extensible Authentication Protocol (EAP)

Είναι ιδιαίτερα σημαντικό, οι απομακρυσμένοι χρήστες να πιστοποιούνται καταλλήλως, επειδή αποτελούν μεγαλύτερο κίνδυνο για την ασφάλεια από τους τοπικούς χρήστες.

3.11.6 Single Sign-On (SSO)

Το Single Sign-On είναι ένα χαρακτηριστικό που επιτρέπει σε ένα χρήστη να χρησιμοποιεί ένα κωδικό (ή έξυπνη κάρτα) για να πιστοποιείται σε πολλαπλούς διακομιστές σε ένα δίκτυο χωρίς να ξανά εισάγει διαπιστευτήρια. Αυτή είναι μια εμφανής ευκολία για χρήστες, που δεν χρειάζεται να θυμούνται πολλαπλούς κωδικούς ή να χρησιμοποιούν την διαδικασία πιστοποίησης ξανά και ξανά για να εισέλθουν σε διαφορετικούς πόρους.

3.11.7 Τύποι πιστοποίησης

Υπάρχουν αρκετά φυσικά μέσα με τα οποία μπορείς να προσφέρεις τα διαπιστευτήρια πιστοποίησης στο σύστημα. Το συνηθέστερο, αλλά όχι το ασφαλέστερο, είναι η πιστοποίηση με χρήση κωδικού. Το ανταγωνιστικό εταιρικό περιβάλλον του σήμερα, απαιτεί επιλογές που προσφέρουν περισσότερη προστασία, όταν οι δικτυακοί πόροι συμπεριλαμβάνουν εξαιρετικά ευαίσθητα δεδομένα. Έξυπνες κάρτες και η βιομετρική πιστοποίηση προσφέρουν αυτή την επιπλέον προστασία.

3.11.7.1 Πιστοποίηση με χρήση κωδικού

Οι περισσότεροι είμαστε οικείοι με την πιστοποίηση κωδικού. Για να συνδεθείς σε έναν υπολογιστή ή δίκτυο, εισάγεις ένα όνομα λογαριασμού χρήστη και τον κωδικό που έχει ανατεθεί σε αυτό το λογαριασμό. Αυτός ο κωδικός ελέγχεται σε μια βάση δεδομένων που περιέχει όλους τους εξουσιοδοτημένους χρήστες και τους κωδικούς τους. Σε ένα δίκτυο με Windows, για παράδειγμα, αυτή η πληροφορία περιέχεται στο Active Directory.

Για την διατήρηση της ασφάλειας του δικτύου, οι κωδικοί πρέπει να είναι ισχυροί. Δηλαδή πρέπει να περιέχουν ένα συνδυασμό από γράμματα, αριθμούς και σύμβολα, δεν πρέπει να είναι λέξεις που μπορούν να βρεθούν στο λεξικό και πρέπει να είναι σχετικά μεγάλοι (οκτώ χαρακτήρες ή περισσότεροι). Εν συντομία δεν πρέπει να είναι εύκολοι για κάποιον να τους μαντέψει.

Η πιστοποίηση με χρήση κωδικού είναι ευάλωτη σε ένα cracker, με πρόγραμμα που χρησιμοποιεί επιθέσεις ωμής βίας (δοκιμάζοντας κάθε πιθανό συνδυασμό μέχρι να βρεθεί ο σωστός) ή κάποιον που χρησιμοποιεί ένα sniffer πρωτοκόλλων, ένα πρόγραμμα που διαβάζει πακέτα αν οι κωδικοί δεν είναι κρυπτογραφημένοι, όταν αποστέλλονται μέσω ενός δικτύου.

3.11.7.2 Πιστοποίηση με έξυπνη κάρτα

Οι έξυπνες κάρτες είναι συσκευές σε μέγεθος πιστωτικής κάρτας που περιέχουν ένα μικρό τσιπ, το οποίο χρησιμοποιείται για την αποθήκευση δημόσιων, ιδιωτικών κλειδιών και άλλων προσωπικών αρχείων για την αναγνώριση ενός προσώπου και την πιστοποίηση του στο σύστημα. Η σύνδεση στο δίκτυο με μια έξυπνη κάρτα απαιτεί την φυσική τοποθέτηση της κάρτας σε ένα σαρωτή και την εισαγωγή του PIN, με τον ίδιο τρόπο που χρησιμοποιούμε μια κάρτα σε ένα ATM.

Οι έξυπνες κάρτες χρησιμοποιούν κρυπτογραφημένη πιστοποίηση και προσφέρουν μεγαλύτερη ασφάλεια από ένα κωδικό επειδή για να αποκτήσει πρόσβαση, ο χρήστης πρέπει να έχει στην κατοχή του την κάρτα και να γνωρίζει το PIN.

3.11.7.3 Βιομετρική πιστοποίηση

Μια πιο ασφαλής μορφή πιστοποίησης από τις έξυπνες κάρτες, η βιομετρική πιστοποίηση περιλαμβάνει την χρήση βιολογικών στατιστικών που δείχνουν ότι η πιθανότητα δύο ανθρώπων να έχουν πανομοιότυπα βιολογικά χαρακτηριστικά όπως είναι τα δακτυλικά αποτυπώματα είναι απειροελάχιστα μικρή, έτσι αυτά τα βιολογικά γνωρίσματα μπορούν να χρησιμοποιηθούν για την θετική αναγνώριση ενός προσώπου.

Επιπλέον τα πρότυπα δακτυλικά αποτυπώματα, φωνής και αμφιβληστροειδούς είναι σχεδόν μοναδικά σε κάθε άνθρωπο και μπορούν να χρησιμοποιηθούν για σκοπούς πιστοποίησης. Αυτή η μέθοδος απόδειξης της ταυτότητας είναι πολύ δύσκολη να παραβιαστεί, αν και απαιτεί ακριβό εξοπλισμό για την εισαγωγή δακτυλικών αποτυπωμάτων, δείγματος φωνής ή για την σάρωση του ματιού. Άλλο ένα πλεονέκτημα απέναντι στις έξυπνες κάρτες είναι ότι ο χρήστης δεν χρειάζεται να θυμάται να κουβαλάει μια συσκευή, τα βιολογικά του διαπιστευτήρια είναι πάντα μαζί του.

3.11.8 Πως δουλεύει η πιστοποίηση;

Στην θεωρία, η πιστοποίηση είναι σχετικά απλή: ο χρήστης παρέχει μια μορφή διαπιστευτηρίων, ένα κωδικό, μια έξυπνη κάρτα, ένα δακτυλικό αποτύπωμα, ένα ψηφιακό πιστοποιητικό, το οποίο αναγνωρίζει τον χρήστη ως το πρόσωπο το οποίο είναι εξουσιοδοτημένο να εισέλθει στο σύστημα. Υπάρχουν, ωστόσο, πολλές μέθοδοι και πρωτόκολλα που μπορούν να χρησιμοποιηθούν για να επιτευχθεί αυτό. Ανεξάρτητα της μεθόδου, η βασική διαδικασία πιστοποίησης παραμένει η ίδια.

3.11.9 Η διαδικασία πιστοποίησης

Στις περισσότερες περιπτώσεις, ο χρήστης πρέπει να έχει ένα έγκυρο λογαριασμό ρυθμισμένο από το διαχειριστή δικτύου που καθορίζει τα δικαιώματα του χρήστη. Τα διαπιστευτήρια του χρήστη πρέπει να σχετίζονται με τον λογαριασμό του, πρέπει να ανατεθεί κωδικός, να εκδοθεί

πιστοποιητικό έξυπνης κάρτας ή να προστεθεί μια βιομετρική σάρωση στη βάση δεδομένων, όπου θα συγκρίνονται οι μελλοντικές αναγνώσεις.

Όταν ο χρήστης θέλει να συνδεθεί, προσφέρει τα διαπιστευτήρια του και το σύστημα ελέγχει την βάση δεδομένων για την αρχική εγγραφή και κάνει την σύγκριση. Αν τα διαπιστευτήρια που έχει προσφέρει ο χρήστης ταιριάζουν με αυτά της βάσης δεδομένων, τότε του επιτρέπεται η είσοδος.

3.11.10 Πλεονεκτήματα πιστοποίησης πολλών επιπέδων

Σε ένα περιβάλλον υψηλής ασφάλειας, η πιστοποίηση πολλών επιπέδων προσφέρει επιπλέον προστασία. Με άλλα λόγια, μπορείς να απαιτήσεις από τον χρήστη να προσφέρει παραπάνω από ένα τύπο διαπιστευτηρίων, όπως ένα δακτυλικό αποτύπωμα και ένα κωδικό εισόδου. Αυτό μειώνει ακόμη περισσότερο τις πιθανότητες ενός μη εξουσιοδοτημένου ατόμου να παρακάμψει την ασφάλεια του συστήματος.

3.11.11 Μέθοδοι και πρωτόκολλα πιστοποίησης

Υπάρχει ένας μεγάλος αριθμός μεθόδων και πρωτοκόλλων πιστοποίησης που μπορούν να χρησιμοποιηθούν, ανάλογα την εφαρμογή και τις απαιτήσεις ασφάλειας. Στις επόμενες ενότητες θα παρουσιαστούν οι πιο συνηθισμένες μέθοδοι πιστοποίησης.

3.11.11.1 Kerberos

Ο Kerberos αναπτύχθηκε στο MIT για να προσφέρει ασφαλή πιστοποίηση για UNIX δίκτυα. Έχει γίνει πρότυπο στο Διαδίκτυο και υποστηρίζεται από το τελευταίο δικτυακό λειτουργικό σύστημα της Microsoft. Ο Kerberos χρησιμοποιεί προσωρινά πιστοποιητικά που ονομάζονται tickets, τα οποία περιέχουν τα διαπιστευτήρια που αναγνωρίζουν τον χρήστη στους διακομιστές

του δικτύου. Στην τωρινή έκδοση 5, τα δεδομένα που βρίσκονται στα tickets είναι κρυπτογραφημένα συμπεριλαμβανομένου του κωδικού του χρήστη.

Ένα κέντρο διανομής κλειδιών (Key Distribution Center - KDC) είναι μια υπηρεσία που τρέχει σε ένα διακομιστή δικτύου, το οποίο εκδίδει tickets που ονομάζονται Ticket Granting Ticket (TGT) στους πελάτες που πιστοποιούνται στην υπηρεσία χορήγησης ticket (Ticket Granting Service - TGS). Ο πελάτης χρησιμοποιεί το TGT για να έχει πρόσβαση στο TGS (το οποίο μπορεί να τρέχει στον ίδιο υπολογιστή με το KDC). Το TGS εκδίδει ένα ticket υπηρεσίας ή συνεδρίας, το οποίο χρησιμοποιείται για την πρόσβαση σε μια υπηρεσία δικτύου ή σε κάποιο πόρο.

Το όνομα Kerberos προέρχεται από το τρικέφαλο σκυλί της Ελληνικής μυθολογίας που φυλούσε τις πύλες του Άδη. Παρόμοια ο Kerberos στέκεται φρουρός στο δίκτυο και διασφαλίζει ότι μόνο εκείνοι που είναι εξουσιοδοτημένοι μπορούν να εισέλθουν.

3.11.11.2 Secure Sockets Layer (SSL)

Το πρωτόκολλο SSL είναι άλλο ένα πρότυπο του Διαδικτύου, που χρησιμοποιείται συχνά για να προσφέρει ασφαλή πρόσβαση σε ιστοσελίδες χρησιμοποιώντας ένα συνδυασμό τεχνολογιών δημόσιου κλειδιού και μυστικού κλειδιού. Η κρυπτογράφηση μυστικού κλειδιού (επίσης καλείται και συμμετρική κρυπτογράφηση) είναι γρηγορότερη, αλλά η ασύμμετρη κρυπτογράφηση δημόσιου κλειδιού προσφέρει καλύτερη πιστοποίηση, έτσι το SSL είναι σχεδιασμένο να επωφελείται από τα πλεονεκτήματα και των δύο. Υποστηρίζεται από όλους τους μεγάλους περιηγητές Διαδικτύου και από το περισσότερο λογισμικό διακομιστή όπως είναι ο Apache.

Το SSL λειτουργεί στο επίπεδο εφαρμογής του μοντέλου OSI. Αυτό σημαίνει ότι εφαρμογές πρέπει να γραφτούν για να το χρησιμοποιήσουν, σε σχέση με άλλα πρωτόκολλα ασφάλειας (όπως το IPSec) που λειτουργεί στα κατώτερα επίπεδα. Το πρωτόκολλο TLS βασίζεται στο SSL.

Η πιστοποίηση SSL βασίζεται σε ψηφιακά πιστοποιητικά που επιτρέπουν στους διαδικτυακούς διακομιστές και πελάτες να επαληθεύουν τις ταυτότητες τους πριν ιδρύσουν μια σύνδεση. (Αυτό

ονομάζεται αμοιβαία πιστοποίηση). Έτσι, δύο τύποι πιστοποιητικών χρησιμοποιούνται: πιστοποιητικά πελάτη και πιστοποιητικά διακομιστή.

3.11.11.3 PAP

Το PAP χρησιμοποιείται για την πιστοποίηση ενός χρήστη πάνω από ένα απομακρυσμένο σημείο πρόσβασης. Ένα σημαντικό χαρακτηριστικό του PAP είναι ότι στέλνει τους κωδικούς χρήστη μέσω του δικτύου στο διακομιστή πιστοποίησης σε απλό κείμενο. Αυτό αυξάνει σημαντικά το ρίσκο, επειδή κάποιος μη εξουσιοδοτημένος χρήστης μπορεί να διαβάσει τα πακέτα δεδομένων χρησιμοποιώντας έναν αναλυτή πρωτοκόλλων και να αποκτήσει το κωδικό.

Το πλεονέκτημα του PAP είναι η συμβατότητα του με τους πολλούς τύπους διακομιστών που τρέχουν διαφορετικά λειτουργικά συστήματα. Το PAP πρέπει να χρησιμοποιείται μόνο όταν υπάρχουν προβλήματα συμβατότητας.

3.11.11.4 SPAP

Το SPAP είναι μια βελτίωση του PAP σε θέματα ασφάλειας, επειδή χρησιμοποιεί μια μέθοδο κρυπτογράφησης (χρησιμοποιείται από τους απομακρυσμένους διακομιστές πρόσβασης Shiva, όπου προέρχεται και το όνομα).

Ο πελάτης στέλνει το όνομα χρήστη μαζί με το κρυπτογραφημένο κωδικό και ο απομακρυσμένος διακομιστής αποκρυπτογραφεί τον κωδικό. Αν το όνομα χρήστη και ο κωδικός ταιριάζουν με την πληροφορία που βρίσκεται στη βάση δεδομένων του διακομιστή, ο απομακρυσμένος διακομιστής στέλνει ένα μήνυμα Acknowledgment (ACK) και επιτρέπει την σύνδεση. Αλλιώς στέλνεται ένα μήνυμα Negative Acknowledgment (NAK) και η σύνδεση απορρίπτεται.

3.11.11.5 CHAP και MS-CHAP

Το CHAP είναι άλλο ένα πρωτόκολλο πιστοποίησης που χρησιμοποιείται για απομακρυσμένη ασφάλεια πρόσβασης. Είναι ένα πρότυπο Διαδικτύου που χρησιμοποιεί την MD5, μια μέθοδο κρυπτογράφησης μιας κατεύθυνσης, η οποία εκτελεί μια διαδικασία hash στον κωδικό και μεταδίδει το αποτέλεσμα του hash, αντί για τον κωδικό στο δίκτυο.

Το πρωτόκολλο είναι πιο ασφαλές από το PAP/SPAP, επειδή ο κωδικός δεν στέλνεται στο δίκτυο και έτσι δεν μπορεί να βρεθεί.

Ο αλγόριθμος hash διασφαλίζει ότι η διαδικασία δεν μπορεί να αντιστραφεί για να αποκτήσουν τον αρχικό κωδικό από το αποτέλεσμα του hash. Το CHAP όμως είναι ευάλωτο στην προσωποποίηση απομακρυσμένου διακομιστή.

Το MS-CHAP είναι η έκδοση CHAP της Microsoft. Το MS-CHAP 2 χρησιμοποιεί πιστοποίηση δύο κατευθύνσεων έτσι ώστε η ταυτότητα του διακομιστή και του πελάτη να επαληθευτεί. Αυτή προστατεύει απέναντι στην προσωποποίηση διακομιστή. Το MS-CHAP επίσης αυξάνει την ασφάλεια χρησιμοποιώντας ξεχωριστά κλειδιά κρυπτογράφησης για μεταδιδόμενα και λαμβανόμενα δεδομένα.

3.11.11.6 EAP

Το EAP είναι μια μορφή πιστοποίησης μιας σύνδεσης με Point-to-Point Protocol (PPP) που επιτρέπει στους υπολογιστές να διαπραγματευτούν μια ακριβής μορφή πιστοποίησης (που ονομάζεται τύπος EAP).

Ένα βασικό χαρακτηριστικό του EAP είναι η επεκτασιμότητα, όπως υποδηλώνει και το όνομα του. Επιπλέον λογισμικό μπορεί να προστεθεί στον πελάτη και στον διακομιστή για να υποστηρίζουν νέους τύπους EAP.

Το EAP μπορεί να χρησιμοποιηθεί με TLS (EAP-TLS) για να προσφέρει αμοιβαία πιστοποίηση μέσω της ανταλλαγής πιστοποιητικών μεταξύ του χρήστη και της μηχανής.

3.11.12 Υπηρεσίες πιστοποιητικών

Τα ψηφιακά πιστοποιητικά αποτελούνται από δεδομένα που χρησιμοποιούνται για πιστοποίηση και ασφάλεια των διαβιβάσεων, ειδικά σε μη ασφαλή δίκτυα (για παράδειγμα το Διαδίκτυο). Τα πιστοποιητικά συνδέουν ένα δημόσιο κλειδί σε ένα χρήστη ή κάποια άλλη οντότητα (έναν υπολογιστή ή υπηρεσία) που κατέχει το αντίστοιχο ιδιωτικό κλειδί.

Τα πιστοποιητικά εκδίδονται από τις αρχές πιστοποιητικών, οι οποίες είναι αξιόπιστες οντότητες που εγγυούνται την ταυτότητα του χρήστη ή του υπολογιστή. Η αρχή υπογράφει ψηφιακά τα πιστοποιητικά που εκδίδει, χρησιμοποιώντας το ιδιωτικό της κλειδί. Τα πιστοποιητικά είναι έγκυρα για μια συγκεκριμένη χρονική περίοδο, όταν το πιστοποιητικό λήγει, πρέπει να εκδοθεί ένα καινούριο. Η αρχή μπορεί επίσης να ανακαλέσει πιστοποιητικά. (Understanding and selecting authentication methods 2016)

Βιβλιογραφία

Cloud computing security, 2016. Διαθέσιμο από: <https://en.wikipedia.org/wiki/Cloud_computing_security>. [10 Αυγούστου 2016]

The dirty dozen: 12 cloud security threats, 2016. Διαθέσιμο από: <http://www.infoworld.com/article/3041078/security/the-dirty-dozen-12-cloud-security-threats.html>. [6 Σεπτεμβρίου 2016]

HTTPS, 2016. Διαθέσιμο από: <https://en.wikipedia.org/wiki/HTTPS>. [10 Αυγούστου 2016]

Encryption, 2016. Διαθέσιμο από: <https://en.wikipedia.org/wiki/Encryption>. [10 Αυγούστου 2016]

Secure Shell, 2016. Διαθέσιμο από: <https://en.wikipedia.org/wiki/Secure_Shell>. [10 Αυγούστου 2016]

Firewall (computing), 2016. Διαθέσιμο από: <https://en.wikipedia.org/wiki/Firewall_(computing)>. [10 Αυγούστου 2016]

Understanding and selecting authentication methods, 2016. Διαθέσιμο από: <http://www.techrepublic.com/article/understanding-and-selecting-authentication-methods>. [10 Αυγούστου 2016]

4. Υπόθεση εργασίας

4.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα αναλύσουμε την καθημερινή ζωή ενός απλού χρήστη που χρησιμοποιεί εφαρμογές cloud στο χώρο που εργάζεται και στην καθημερινή του ζωή.

4.2 Καθημερινές εφαρμογές cloud

4.2.1 Κοινωνικά δίκτυα

Οι πιο δημοφιλείς εφαρμογές που χρησιμοποιούνται είναι οι εφαρμογές κοινωνικής δικτύωσης (Facebook, Twitter, LinkedIn και πολλές άλλες), που ελέγχονται και ενημερώνονται από τον χρήστη πολλές φορές μέσα στην ημέρα. Έχουν πρόσβαση σε αυτές μέσω υπολογιστών (φορητών και μη) και μέσω φορητών συσκευών (smartphones και tablets). Ο σκοπός αυτών των εφαρμογών είναι να βρεις ανθρώπους που γνωρίζεις, να γνωρίσεις καινούριους ανθρώπους και να μοιραστείς πληροφορίες μαζί τους.

Ενώ ο κύριος σκοπός των κοινωνικών δικτύων είναι η διασύνδεση των ανθρώπων, μπορούν και οι εταιρίες να τα χρησιμοποιήσουν. Δημιουργώντας μια σελίδα για την εταιρία π.χ. στο Facebook, μια εταιρία μπορεί να αλληλοεπιδρά με τους πελάτες της και εκείνοι με την σειρά τους να την προωθούν. Γενικά έχουν αναπτυχθεί πολλές τακτικές για marketing στα κοινωνικά δίκτυα, με ειδικούς δημόσιων σχέσεων να εξειδικεύονται στο marketing κοινωνικών δικτύων.

4.2.2 Ηλεκτρονικό ταχυδρομείο

Από τις δημοφιλέστερες εφαρμογές cloud, οι εφαρμογές ηλεκτρονικού ταχυδρομείου χρησιμοποιούνται καθημερινά από εκατομμύρια ανθρώπους για επικοινωνία στην καθημερινότητα τους αλλά και στο χώρο εργασίας τους. Με πολλές εταιρίες να προσφέρουν δωρεάν υπηρεσίες ηλεκτρονικού ταχυδρομείου, καθώς και την φιλοξενία και συντήρηση των διακομιστών (Google, Microsoft, Yahoo και άλλες), ο χρήστης ασχολείται μόνο με την διαχείριση του λογαριασμού του, το οποίο είναι διαθέσιμο παντού.

4.2.3 Ιατρική ασφάλιση

Στην Αμερική, το Υπουργείο Υγείας χρησιμοποιεί ένα σύστημα cloud computing για την καταχώρηση και διαχείριση ηλεκτρονικών δελτίων υγείας. Η Microsoft με την υπηρεσία Microsoft HealthVault, προσφέρει στο κοινό τον τρόπο δημιουργίας προσωπικών δελτίων υγείας. Έτσι ο καθημερινός χρήστης μπορεί να δημιουργήσει, αποθηκεύσει και να έχει πρόσβαση στο ηλεκτρονικό του δελτίο υγείας από τη σελίδα της εφαρμογής.

Η Google στο παρελθόν είχε δημιουργήσει την αντίστοιχη εφαρμογή Google Health, αλλά η λειτουργία της πλέον έχει σταματήσει.

4.2.3 Κυβέρνηση

Τον Οκτώβριο του 2009 η Αμερικάνικη κυβέρνηση ξεκίνησε την λειτουργία της σελίδας Apps.gov, μιας ιστοσελίδας που προσφέρει υπηρεσίες cloud computing για ομοσπονδιακές υπηρεσίες.

4.2.4 Video games

Το cloud gaming ή αλλιώς gaming on demand είναι ένας τύπος online gaming. Υπάρχουν δύο τύποι cloud gaming: χρησιμοποιώντας βίντεο streaming και χρησιμοποιώντας streaming αρχείων. Στον πρώτο τύπο, το παιχνίδι γίνεται streaming σε μια συσκευή πελάτη, όμως το παιχνίδι είναι αποθηκευμένο και εκτελείται από μια απομακρυσμένη συσκευή ή διακομιστή. Στον δεύτερο τύπο το παιχνίδι πάλι γίνεται streaming σε μια συσκευή πελάτη, αλλά αυτή τη φορά το παιχνίδι αποθηκεύεται και εκτελείται από την συσκευή πελάτη.

Μερικές από τις πιο δημοφιλείς εφαρμογές είναι οι: GeForce Now, Steam In-Home Streaming, Remote Play και PlayStation Now. (GeForce Now 2016) (PlayStation Now 2016)

4.2.5 Blog

Πολλοί άνθρωποι θέλουν να μοιράζονται τις σκέψεις και τις απόψεις τους, οι πιο πολλοί το κάνουν στα κοινωνικά δίκτυα. Για εκείνους όμως που θέλουν ένα δικό τους χώρο, μακριά από διαφημίσεις και αντιπερισπασμούς υπάρχουν τα blog. Χρησιμοποιούνται από απλούς χρήστες και εταιρίες είτε για απλά κείμενα είτε για ενημερώσεις πελατών.

Οι πιο δημοφιλείς πλατφόρμες για blogging είναι οι: WordPress.com, WordPress.org, Tumblr, Blogger και Medium.

4.2.6 Αποθηκευτικός χώρος

Τη σημερινή εποχή σχεδόν όλοι έχουν κινητά με πολύ καλές κάμερες, που τραβάνε αμέτρητες φωτογραφίες και βίντεο. Πολλοί προτιμούν τη cloud αποθήκευση, επειδή προσφέρει περισσότερα πλεονεκτήματα από την απλή αποθήκευση. Για παράδειγμα, οι χρήστες μπορούν να έχουν πρόσβαση στα δεδομένα τους από οποιαδήποτε συσκευή, με πολλές εφαρμογές να προσφέρουν δωρεάν αποθηκευτικό χώρο.

Μερικές από τις πιο δημοφιλείς εφαρμογές είναι: Dropbox, Microsoft OneDrive, Google Drive, Mega, Box και iCloud. (Dropbox (service) 2016) (iCloud 2016)

4.2.7 Εκπαίδευση

Η χρήση του cloud στο χώρο της εκπαίδευσης έχει βοηθήσει πολύ στην οργάνωση και ενημέρωση μαθητών, δασκάλων και γονιών. Στην Εσθονία, το 90% των δημόσιων σχολείων είναι συνδεδεμένα στο σύστημα eKool, ένα σύστημα όπου βρίσκονται τα ωρολόγια προγράμματα, βαθμοί, ασκήσεις, απουσίες και άλλα. Επίσης μια περιοχή στην Ινδία έχει αναπτύξει ένα αντίστοιχο πρόγραμμα, το Fedena με παρόμοιες λειτουργίες. (eKool 2016) (Fedena 2016)

4.2.8 Συγχρονισμός

Οι εφαρμογές συγχρονισμού επιτρέπουν στους χρήστες να συγχρονίζουν σελιδοδείκτες, επαφές, συμβάντα ημερολογίου, εργασίες και σημειώσεις σε υπολογιστές και φορητές συσκευές. Οι περισσότερες εφαρμογές χρησιμοποιούν κρυπτογράφηση SSL για το συγχρονισμό των αρχείων, η Mozilla όμως για την εφαρμογή της Firefox Sync, κρυπτογραφεί τα δεδομένα στους διακομιστές της με τέτοιο τρόπο, που ούτε η ίδια δεν μπορεί να έχει πρόσβαση.

Δύο από τις δημοφιλέστερες εφαρμογές συγχρονισμού είναι οι: Firefox Sync και fruux. (Firefox Sync 2016) (fruux 2016)

4.3 Εφαρμογές cloud στο χώρο εργασίας

4.3.1 Σουίτα γραφείου

Από τις πιο κοινές εφαρμογές στο χώρο εργασίας, οι σουίτες γραφείου περιέχουν όλα τα απαραίτητα προγράμματα για την επεξεργασία εγγράφων (επεξεργαστή κειμένου, υπολογιστικών φύλλων, παρουσίασης, βάσης δεδομένων, ημερολόγιο, ηλεκτρονικό ταχυδρομείο κ.ά.). Είναι πιο δημοφιλής από τις κοινές σουίτες γραφείου, επειδή μπορεί να παρέχει πρόσβαση σε οποιαδήποτε συσκευή συνδεδεμένη στο Διαδίκτυο, ανεξαρτήτου λειτουργικού συστήματος και λόγω του χαμηλού κόστους του.

Μερικές από τις πιο δημοφιλείς σουίτες είναι οι: Google Docs, Sheets and Slides, Office 365, iWork. (Office 365 2016) (iWork 2016)

4.3.2 Marketing

Για όσους εργάζονται σε εταιρίες μάρκετινγκ, τους είναι απαραίτητα εργαλεία όπως είναι το Adobe Marketing Cloud, Monitis και MailChimp. Το Adobe Marketing Cloud είναι μια σουίτα που περιέχει εφαρμογές για ανάλυση και παρακολούθηση στατιστικών μιας ιστοσελίδας, δημιουργία διαφημιστικών εκστρατειών, marketing μηχανών αναζήτησης και εφαρμογή διαχείρισης κοινωνικών δικτύων. Το Monitis είναι μια παρόμοια εφαρμογή, αλλά περιέχει μόνο εφαρμογή ανάλυσης και παρακολούθησης στατιστικών. Το MailChimp είναι μια τελείως διαφορετική εφαρμογή, αφού προσφέρει στους χρήστες του μαζική αποστολή email σε χιλιάδες χρήστες. (Adobe Marketing Cloud 2016) (Monitis 2016) (MailChimp 2016)

4.3.3 Video

Για χρήστες που εργάζονται στο χώρο εργασίας τους με βίντεο υπάρχει η πλατφόρμα Aframe. Η εφαρμογή προσφέρει ευκολίες στην επεξεργασία βίντεο μεγάλων αναλύσεων και πολλών τύπων, συγκεντρώνοντας τα κεντρικά κομμάτια στο cloud. Έτσι είναι ευκολότερη η συνεργασία μεταξύ ομάδων, αυξάνεται η παραγωγικότητα και μειώνεται το κόστος. (Aframe 2016)

4.3.4 Τηλεφωνία

Πολλές μικρές και μεσαίες εταιρίες προτιμούν για την επικοινωνία τους να χρησιμοποιούν τηλεφωνία στο cloud. Οι λόγοι είναι μικρότερο κόστος, μεγαλύτερη ασφάλεια και η συντήρηση γίνεται από τους παρόχους. Μια τέτοια εταιρία είναι η CallFire που χρεώνει τους πελάτες της ανάλογα με την χρήση της υπηρεσίας. Επίσης εκτός από τηλεφωνικές κλήσεις, προσφέρει και αποστολή γραπτών μηνυμάτων. (CallFire 2016)

4.3.5 Είσοδος σε υπηρεσίες cloud

Πάρα πολύ χρήστες χρησιμοποιούν τις υπηρεσίες για σύνδεση στις υπηρεσίες cloud, μερικοί μπορεί να μην τις γνωρίζουν, αλλά είναι πολύ σημαντικές. Προσφέρουν εργαλεία για την είσοδο σε όλες τις υπηρεσίες με ένα τρόπο (μπορεί να είναι όνομα χρήστη/κωδικός, έξυπνη κάρτα, κ.ά.). Για επιπλέον ασφάλεια υποστηρίζουν πιστοποίηση πολλών επιπέδων και εντοπισμό ανωμαλιών. Επίσης υποστηρίζουν πρόσβαση μέσω Facebook Connect, Active Directory, LDAP και Google Apps.

Οι πιο δημοφιλείς υπηρεσίες είναι οι: Auth0, OneLogin, Gigya και Bitium. (OneLogin 2016) (Gigya 2016) (Bitium 2016)

4.3.6 Πληρωμές

Πολλές εταιρίες επιλέγουν να πραγματοποιούν τις συναλλαγές τους μέσω cloud. Ο λόγος είναι επειδή προσφέρουν πολλά πλεονεκτήματα σε σχέση με άλλους τρόπους πληρωμής. Τους επιτρέπει να χρησιμοποιούν τοπικές μεθόδους πληρωμής σε παγκόσμιες αγορές. Επίσης προσφέρει προστασία απέναντι σε απάτες, αυτόματο υπολογισμό και περισυλλογή φόρου και αναλυτική αναφορά των μεθόδων πληρωμής.

Μια από τις πιο δημοφιλείς εταιρίες online συναλλαγών είναι η Emergent Payments. (Emergent Payments 2016)

Βιβλιογραφία

GeForce Now, 2016. Διαθέσιμο από:
<https://en.wikipedia.org/wiki/GeForce_Now>. [1 Νοεμβρίου 2016]

PlayStation Now, 2016. Διαθέσιμο από:
<https://en.wikipedia.org/wiki/PlayStation_Now>. [1 Νοεμβρίου 2016]

Dropbox (service), 2016. Διαθέσιμο από:
<https://en.wikipedia.org/wiki/Dropbox_(service)>. [1 Νοεμβρίου 2016]

iCloud, 2016. Διαθέσιμο από:
<https://en.wikipedia.org/wiki/iCloud>. [1 Νοεμβρίου 2016]

eKool, 2016. Διαθέσιμο από:
<https://en.wikipedia.org/wiki/EKool>. [1 Νοεμβρίου 2016]

Fedena, 2016. Διαθέσιμο από:
<https://en.wikipedia.org/wiki/Fedena>. [1 Νοεμβρίου 2016]

Firefox Sync, 2016. Διαθέσιμο από:
<https://en.wikipedia.org/wiki/Firefox_Sync>. [1 Νοεμβρίου 2016]

fruux, 2016. Διαθέσιμο από:
<https://en.wikipedia.org/wiki/Fruux>. [1 Νοεμβρίου 2016]

Office 365, 2016. Διαθέσιμο από:
<https://en.wikipedia.org/wiki/Office_365>. [1 Νοεμβρίου 2016]

iWork, 2016. Διαθέσιμο από:
<https://en.wikipedia.org/wiki/iWork>. [1 Νοεμβρίου 2016]

Adobe Marketing Cloud, 2016. Διαθέσιμο από:
<https://en.wikipedia.org/wiki/Adobe_Marketing_Cloud>. [1 Νοεμβρίου 2016]

Monitis, 2016. Διαθέσιμο από:
<https://en.wikipedia.org/wiki/Monitis>. [1 Νοεμβρίου 2016]

MailChimp, 2016. Διαθέσιμο από:
<https://en.wikipedia.org/wiki/MailChimp>. [1 Νοεμβρίου 2016]

Aframe, 2016. Διαθέσιμο από:
<https://en.wikipedia.org/wiki/Aframe>. [1 Νοεμβρίου 2016]

CallFire, 2016. Διαθέσιμο από:
<https://en.wikipedia.org/wiki/CallFire>. [1 Νοεμβρίου 2016]

Gigya, 2016. Διαθέσιμο από:
<https://en.wikipedia.org/wiki/Gigya>. [1 Νοεμβρίου 2016]

OneLogin, 2016. Διαθέσιμο από:
<https://en.wikipedia.org/wiki/OneLogin>. [1 Νοεμβρίου 2016]

Bitium, 2016. Διαθέσιμο από:
<https://en.wikipedia.org/wiki/Bitium>. [1 Νοεμβρίου 2016]

Emergent Payments, 2016. Διαθέσιμο από:
<https://en.wikipedia.org/wiki/Emergent_Payments>. [1 Νοεμβρίου 2016]

5. Νομοθεσία σχετική με cloud computing

5.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα αναλύσουμε την νομοθεσία που σχετίζεται με το cloud computing και θα εξηγήσουμε τι είναι τα service-level agreement (συμφωνία σε επίπεδο υπηρεσιών).

5.2 Service-level agreement (SLA)

Το service-level agreement (συμφωνία σε επίπεδο υπηρεσιών) ορίζεται ως μια επίσημη δέσμευση μεταξύ του παρόχου της υπηρεσίας και του πελάτη. Ιδιαίτερες πτυχές της υπηρεσίας, π.χ. ποιότητα, διαθεσιμότητα, ευθύνες, είναι συμφωνημένα μεταξύ του παρόχου της υπηρεσίας και του πελάτη. Το πιο κοινό συστατικό του SLA είναι η σωστή παροχή των υπηρεσιών, όπως αυτές περιγράφονται στο συμβόλαιο. Για παράδειγμα παροχείς internet και τηλεπικοινωνιακές εταιρίες συμπεριλαμβάνουν SLAs στους όρους των συμβολαίων τους. Πολύ συχνά περιλαμβάνουν τους όρους MTBF (mean time between failures – μέσος όρος μεταξύ βλαβών) και MTTR (mean time to recovery – μέσος όρος για αποκατάσταση), ποια πλευρά είναι υπεύθυνη για αναφορά σφαλμάτων ή για πληρωμή αμοιβών, επίσης ευθύνη για τις ροές δεδομένων, throughput, jitter κ.ά..

5.2.1 Κατηγορίες SLA

SLA βασισμένο σε πελάτη: Μια συμφωνία με μια ομάδα πελατών, που καλύπτει όλες τις υπηρεσίες που χρησιμοποιεί. Για παράδειγμα, ένα SLA μεταξύ ενός προμηθευτή (πάροχος υπηρεσιών IT) και το οικονομικό τμήμα μιας μεγάλης οργάνωσης για τις υπηρεσίες οικονομικών, πληρωμής μισθών, αγορών κ.ά..

SLA βασισμένο σε υπηρεσία: Μια συμφωνία για όλους τους πελάτες που χρησιμοποιούν τις υπηρεσίες που προσφέρει ο πάροχος υπηρεσιών. Για παράδειγμα, ένας πάροχος υπηρεσιών κινητής τηλεφωνίας προσφέρει σε όλους τους πελάτες του μια υπηρεσία ρουτίνας και προσφέρει σίγουρη συντήρηση σαν μέρος μιας προσφοράς μαζί με την κανονική χρέωση.

SLA πολλών επιπέδων: Αυτό το SLA είναι χωρισμένο σε διαφορετικά επίπεδα, με το καθένα να εξυπηρετεί διαφορετικούς πελάτες για τις ίδιες υπηρεσίες, στο ίδιο SLA.

SLA επιπέδου εταιρίας: Καλύπτει όλα τα θέματα του service level management (SLM), κατάλληλα για κάθε πελάτη στην οργάνωση.

SLA επιπέδου πελάτη: Καλύπτει όλα τα θέματα του SLM σχετικά με μια συγκεκριμένη ομάδα πελατών, ανεξάρτητα των υπηρεσιών που χρησιμοποιούν.

SLA επιπέδου υπηρεσίας: Καλύπτει όλα τα θέματα του SLM σχετικά με τις συγκεκριμένες υπηρεσίες, μιας ομάδας πελατών.

5.2.2 Συστατικά SLA

Ένα καλά ορισμένο και τυπικό SLA θα περιέχει τα παρακάτω συστατικά:

Τύπος της παρεχόμενης υπηρεσίας: Καθορίζει τον τύπο της υπηρεσίας καθώς και άλλες λεπτομέρειες τύπου υπηρεσίας. Στην περίπτωση ενός IP δικτύου, ο τύπος της υπηρεσίας θα περιγράφει λειτουργίες όπως είναι η λειτουργία και συντήρηση του υλικού δικτύωσης, το εύρος ζώνης της σύνδεσης κ.ά..

Το επιθυμητό επίπεδο επίδοσης της υπηρεσίας, ειδικά η αξιοπιστία και αποκριτικότητα της: Μια αξιόπιστη υπηρεσία θα υποφέρει από λιγότερες διακοπές σε ένα συγκεκριμένο χρονικό διάστημα και είναι διαθέσιμη σχεδόν οποιαδήποτε στιγμή. Μια υπηρεσία με καλή αποκριτικότητα θα εκτελεί την επιθυμητή δράση του πελάτη αμέσως, όταν την ζητήσει.

Χρονικό πλαίσιο απάντησης και αποκατάστασης θεμάτων: Το χρονικό πλαίσιο απάντησης είναι η χρονική περίοδος στην οποία ο πάροχος της υπηρεσίας θα ξεκινήσει την έρευνα του θέματος.

Το χρονικό πλαίσιο αποκατάστασης θεμάτων είναι η χρονική περίοδος στην οποία το τρέχων θέμα θα επιλυθεί.

Διαδικασία παρακολούθησης και αναφορά επιπέδου υπηρεσίας: Αυτό το συστατικό περιγράφει πως παρακολουθούνται και πως εποπτεύονται τα επίπεδα απόδοσης. Αυτή η διαδικασία περιλαμβάνει την συλλογή στατιστικών διαφορετικών τύπων, πόσο συχνά θα συλλέγονται αυτά τα συστατικά και πως θα έχουν πρόσβαση σε αυτά οι πελάτες.

Επιπτώσεις για τον πάροχο υπηρεσίας αν δεν πληροί την δέσμευση: Αν ο πάροχος δεν είναι ικανός να πληροί τις απαιτήσεις που έχουν οριστεί στο SLA, τότε θα υποστεί τις συνέπειες. Αυτές οι συνέπειες μπορεί να συμπεριλαμβάνουν το δικαίωμα του πελάτη να ζητήσει τη λήξη του συμβολαίου του ή να ζητήσει αποζημίωση για ζημίες που προκλήθηκαν από την αποτυχία της υπηρεσίας.

5.2.3 SLA στο cloud computing

Το όφελος του cloud computing είναι οι κοινόχρηστοι πόροι, το οποίο υποστηρίζεται από τη φύση ενός περιβάλλοντος κοινής υποδομής. Έτσι, τα SLAs εκτείνονται σε όλο το cloud και προσφέρονται από τους παρόχους υπηρεσιών, σαν μια σύμβαση βασισμένη σε υπηρεσίες αντί ως σύμβαση βασισμένη σε πελάτη. Η καταμέτρηση, παρακολούθηση και αναφορά της επίδοσης του cloud βασίζεται στις εμπειρίες του χρήστη ή στην ικανότητα τους να καταναλώνουν πόρους. Το μειονέκτημα του cloud computing σε σχέση με τα SLAs είναι η δυσκολία εντοπισμού της κύριας αιτίας των διακοπών της υπηρεσίας, λόγω της πολύπλοκης φύσης του περιβάλλοντος.

Όσο οι εφαρμογές μετακινούνται από ειδικό υλικό στο cloud, πρέπει να πετύχουν τα ίδια ή πιο απαιτητικά επίπεδα της υπηρεσίας από τις κλασσικές εγκαταστάσεις. Τα SLAs για τις υπηρεσίες cloud επικεντρώνονται στα χαρακτηριστικά του data center και πιο πρόσφατα περιλαμβάνουν χαρακτηριστικά του δικτύου για να υποστηρίζουν SLAs απ’ άκρη σε άκρη.

Κάθε στρατηγική διαχείρισης SLA εξετάζει δύο διαφορετικές φάσεις: διαπραγμάτευση του συμβολαίου και παρακολούθηση της ολοκλήρωσης του σε πραγματικό χρόνο. Έτσι, η διαχείριση SLA περικλείει τον ορισμό του SLA συμβολαίου: το βασικό σχήμα με τις παραμέτρους QoS,

διαπραγμάτευση του SLA, παρακολούθηση του SLA, ανίχνευση παραβίασης του SLA και επιβολή του SLA σύμφωνα με τις καθορισμένες πολιτικές.

Το κύριο σημείο είναι να χτιστεί ένα καινούριο επίπεδο πάνω από το πλέγμα cloud και την αρχιτεκτονική υπηρεσιών, ικανό να δημιουργήσει ένα μηχανισμό διαπραγματεύσεων μεταξύ παρόχων και καταναλωτών των υπηρεσιών. Ένα παράδειγμα είναι το χρηματοδοτούμενο από την Ευρωπαϊκή Ένωση ερευνητικό πρόγραμμα Framework 7, το οποίο ερευνά πτυχές SLA πολλών επιπέδων και πολλών παρόχων εντός μιας υποδομής υπηρεσιών και cloud computing, ενώ ένα άλλο πρόγραμμα χρηματοδοτούμενο από την Ευρωπαϊκή Ένωση, το VISION Cloud, έχει προσφέρει αποτελέσματα σε SLAs περιεχομένου. (Service-level agreement 2017)

5.3 Νομοθετικό πλαίσιο του cloud computing

5.3.1 Εισαγωγή

Στον τομέα των τηλεπικοινωνιών, σύμφωνα με τη νομοθεσία θεωρούνται απόρρητα: το περιεχόμενο της επικοινωνίας (το οποίο μπορεί να είναι φωνή, εικόνα, βίντεο ή δεδομένα), η ταυτότητα του λήπτη και αποστολέα και η τοποθεσία της τερματικής συσκευής. Η προστασία του απορρήτου σε οποιαδήποτε μορφή επικοινωνίας αποτελεί συνταγματικό δικαίωμα και ο νόμος ορίζει σε ποιες συνθήκες μπορεί να αρθεί, π.χ. σε περιπτώσεις εθνικής ασφάλειας ή σοβαρών εγκλημάτων.

Η παραβίαση του απορρήτου είναι ποινικό αδίκημα. Στην νομοθεσία οι ποινές που προβλέπονται είναι αυστηρές, έως 10 χρόνια κάθειρξη έναντι φυσικών προσώπων. Ειδικά για τους παρόχους τηλεπικοινωνιακών υπηρεσιών οι ποινές είναι περισσότερες, από σύσταση και χρηματικό πρόστιμο μέχρι ανάκληση του δικαιώματος παροχής υπηρεσιών, από την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών και άλλων δημόσιων αρχών.

Επίσης η νομοθεσία περί της προστασίας απορρήτου ισχύει και στον εργασιακό χώρο, αν οι εργαζόμενοι χρησιμοποιούν το εσωτερικό δίκτυο της εταιρίας. Η άρση του νόμου γίνεται μόνο για συγκεκριμένες περιπτώσεις.

5.3.2 Το πλαίσιο προστασίας δεδομένων στην Ευρωπαϊκή Ένωση

Το νομικό πλαίσιο για την προστασία των δεδομένων είναι η οδηγία 95/46/ΕΚ, η οποία ισχύει σε κάθε περίπτωση στην οποία γίνεται επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τη χρήση υπηρεσιών cloud. Η οδηγία 2002/58/ΕΚ ισχύει σε περιπτώσεις επεξεργασίας δεδομένων προσωπικού χαρακτήρα που έχουν σχέση με παροχή υπηρεσιών επικοινωνιών σε δημόσια δίκτυα επικοινωνιών και εφαρμόζεται όταν οι υπηρεσίες παρέχονται μέσω cloud.

5.3.3 Εφαρμοστέο δίκαιο

Τα κριτήρια με βάση τα οποία καθορίζεται πιο δίκαιο ισχύει σε κάθε περίπτωση βρίσκονται στο άρθρο 4 της οδηγίας 95/46/ΕΚ. Ένα κριτήριο για την εφαρμογή του νόμου της Ευρωπαϊκής Ένωσης είναι η τοποθεσία του υπεύθυνου επεξεργασίας και οι δραστηριότητες του, ενώ κανέναν ρόλο δεν παίζει το μοντέλο παροχής υπηρεσιών cloud. Με βάση αυτό το κριτήριο, ισχύει το δίκαιο της χώρας στην οποία βρίσκεται ο υπεύθυνος της επεξεργασίας και όχι το δίκαιο της χώρας στην οποία βρίσκεται ο πάροχος υπηρεσιών cloud.

Εάν ο υπεύθυνος της επεξεργασίας βρίσκεται σε περισσότερες από μια χώρες και επεξεργάζεται δεδομένα στο πλαίσιο των δραστηριοτήτων της κάθε χώρας, τότε ισχύει το δίκαιο της χώρας στη οποία γίνεται η επεξεργασία.

Υπάρχει και η περίπτωση όπου ο υπεύθυνος της επεξεργασίας βρίσκεται εκτός της Ευρωπαϊκής Ένωσης, αλλά χρησιμοποιεί υπηρεσίες κάποιου παρόχου που βρίσκεται στην Ευρωπαϊκή Ένωση. Τότε για τον πελάτη αυτών των υπηρεσιών ισχύει το δίκαιο που ισχύει για το πάροχο των υπηρεσιών cloud.

5.3.4 Καθήκοντα και ευθύνες των διαφόρων παραγόντων

Στην παροχή υπηρεσιών cloud εμπλέκονται πολλοί και διάφοροι φορείς. Ο ορισμός του κάθε φορέα είναι πολύ σημαντικός για τον προσδιορισμό των υποχρεώσεων του, που προκύπτουν από την νομοθεσία προστασίας δεδομένων.

5.3.4.1 Πελάτης υπηρεσιών cloud

Ο πελάτης υπηρεσιών cloud καθορίζει τον σκοπό της επεξεργασίας και αν θα αναθέσει την επεξεργασία και την εκχώρηση των αποτελεσμάτων σε τρίτο οργανισμό. Ο πελάτης τότε είναι ο υπεύθυνος της επεξεργασίας δεδομένων και σύμφωνα με την οδηγία, ως υπεύθυνος της επεξεργασίας ορίζεται «το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή , η υπηρεσία ή οποιοσδήποτε άλλος φορέας που μόνος ή από κοινού με άλλους καθορίζει τους στόχους και τον τρόπο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα». Ο πελάτης ως υπεύθυνος της επεξεργασίας πρέπει να συμμορφώνεται με τη νομοθεσία προστασίας δεδομένων. Επίσης ο πελάτης μπορεί να αναθέσει στον πάροχο υπηρεσιών την ευθύνη επιλογής μεθόδων που θα χρησιμοποιήσει για να επιτύχει τους σκοπούς του υπεύθυνου της επεξεργασίας.

Σε πολλές περιπτώσεις είναι πιθανό οι πελάτες να μην μπορούν να διαπραγματευτούν τους συμβατικούς όρους χρήσης των υπηρεσιών cloud, καθώς πολλές υπηρεσίες παρέχονται μέσω τυποποιημένων συμβάσεων. Ο πελάτης όμως είναι εκείνος που αποφασίζει αν τελικά θα εκχωρήσει τα δεδομένα του σε υπηρεσίες cloud. Για τον λόγο αυτό ο υπεύθυνος της επεξεργασίας πρέπει να επιλέγει παρόχους που εγγυώνται τη συμμόρφωση προς τη νομοθεσία περί προστασίας δεδομένων.

5.3.4.2 Πάροχος υπηρεσιών cloud

Ο πάροχος υπηρεσιών cloud είναι η οντότητα που παρέχει τις υπηρεσίες σε διάφορες μορφές. Όταν ο πάροχος παρέχει τα μέσα και την πλατφόρμα για την επεξεργασία του πελάτη, τότε

θεωρείται ο εκτελών την επεξεργασία ή σύμφωνα με την οδηγία «το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή οποιοσδήποτε άλλος φορέας που επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας».

Οι πάροχοι υπηρεσιών ως υπεύθυνοι εκτέλεσης της επεξεργασίας πρέπει να διασφαλίζουν το απόρρητο. Επίσης πρέπει να λαμβάνουν υπόψη τον τύπο του συστήματος (δημόσιο, ιδιωτικό, κοινοτικό ή υβριδικό / IaaS, SaaS ή PaaS) και το είδος της υπηρεσίας για τα οποία έχει συνάψει σύμβαση ο πελάτης. Επίσης οι υπεύθυνοι εκτέλεσης οφείλουν να λαμβάνουν μέτρα ασφαλείας που προβλέπονται από την νομοθεσία της Ευρωπαϊκής Ένωσης, όπως εφαρμόζονται στις δικαιοδοσίες του υπεύθυνου της επεξεργασίας. Οι υπεύθυνοι εκτέλεσης πρέπει να συμμορφώνουν τον υπεύθυνο επεξεργασίας ως προς τα δικαιώματα των προσώπων στα οποία αναφέρονται τα δεδομένα.

5.3.4.3 Υπεργολάβοι

Στην παροχή υπηρεσιών είναι πολύ πιθανή η συμμετοχή τρίτων οργανισμών για την εκτέλεση της επεξεργασίας, οι οποίοι προσλαμβάνονται ως υπεργολάβοι. Επειδή οι υπεργολάβοι έχουν πρόσβαση στα δεδομένα του πελάτη, οι υπεύθυνοι εκτέλεσης είναι υποχρεωμένοι να ενημερώσουν τον πελάτη και να αναφέρουν αναλυτικά τις εργασίες που έχουν αναθέσει στους υπεργολάβους.

Όλες οι υποχρεώσεις που ισχύουν για τους υπεργολάβους, οι οποίες αναγράφονται στη σύμβαση μεταξύ παρόχου και υπεργολάβου πρέπει να είναι σύμφωνες με εκείνες που αναγράφονται στη σύμβαση παρόχου και πελάτη.

Ένα μοντέλο για το σαφή καθορισμό των καθηκόντων των υπεύθυνων εκτέλεσης είναι η ανάθεση της επεξεργασίας μόνο αν ο υπεύθυνος της επεξεργασίας έχει υπογράψει γραπτή συμφωνία, η οποία επιβάλλει στον υπεργολάβο τα ίδια καθήκοντα με τον πάροχο. Σε περίπτωση που ο υπεργολάβος δεν εκπληρώσει τα καθήκοντα του, τότε υπεύθυνος για την ολοκλήρωση είναι ο πάροχος. Ένα τέτοιο μοντέλο θα μπορούσε να χρησιμοποιείται σε όλες τις συμβάσεις μεταξύ πελάτη και παρόχου, αν ο πάροχος σκοπεύει να χρησιμοποιήσει υπεργολάβους.

5.3.5 Απαιτήσεις περί προστασίας των δεδομένων στο πλαίσιο της σχέσης πελάτη – παρόχου

5.3.5.1 Συμμόρφωση προς τις βασικές αρχές

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να συμμορφώνεται με τις βασικές αρχές της νομοθεσίας προστασίας των δεδομένων της Ευρωπαϊκής Ένωσης. Συγκεκριμένα πρέπει να διασφαλίζεται η διαφάνεια του προσώπου στο οποίο αναφέρονται τα δεδομένα, πρέπει να τηρείται η αρχή του προσδιορισμού και του περιορισμού του σκοπού και να διαγράφονται τα δεδομένα προσωπικού χαρακτήρα όταν εξυπηρετήσουν το σκοπό τους. Πρέπει επιπλέον να εφαρμόζονται κατάλληλα μέτρα ασφάλειας των δεδομένων.

5.3.5.2 Διαφάνεια

Η διαφάνεια είναι καθοριστικής σημασίας για την θεμιτή και νόμιμη επεξεργασία δεδομένων προσωπικού χαρακτήρα. Ο πελάτης είναι υποχρεωμένος να παρέχει στο πρόσωπο από το οποίο συλλέγονται τα δεδομένα πληροφορίες για το σκοπό της επεξεργασίας. Προτείνεται επίσης να παρέχεται από τον πελάτη επιπλέον πληροφορίες, όπως είναι οι αποδέκτες των δεδομένων.

Η διαφάνεια πρέπει να διασφαλίζεται και μεταξύ πελάτη, παρόχου και υπεργολάβων (αν υπάρχουν). Ο πελάτης μπορεί να ελέγχει την νομιμότητα της επεξεργασίας των δεδομένων, μόνο αν ο πάροχος τον ενημερώνει για όλα τα ζητήματα. Επίσης ο πελάτης πρέπει να ελέγχει προσεκτικά τους όρους της σύμβασης του παρόχου και να τους αξιολογεί από τη σκοπιά της προστασίας δεδομένων.

Διαφάνεια σημαίνει ο πελάτης πρέπει να είναι ενήμερος για όλους τους υπεργολάβους που βοηθούν στην παροχή των υπηρεσιών, καθώς και για τις τοποθεσίες των data centers όπου βρίσκονται τα δεδομένα του.

Εάν η υπηρεσία απαιτεί την εγκατάσταση λογισμικού στα συστήματα του πελάτη όπως π.χ. plug-ins στον φυλλομετρητή, τότε ο πάροχος πρέπει να ενημερώσει τον πελάτη και να τον πληροφορήσει για τις επιπτώσεις που θα έχει στην ασφάλεια των δεδομένων.

5.3.5.3 Προσδιορισμός και περιορισμός του σκοπού

Σύμφωνα με την αρχή του προσδιορισμού και του περιορισμού του σκοπού, τα δεδομένα προσωπικού χαρακτήρα πρέπει να συλλέγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς και η επεξεργασία τους μετά την ολοκλήρωση του σκοπού να συμβιβάζεται με αυτούς. Ο πελάτης πρέπει να προσδιορίζει το σκοπό ή σκοπούς της επεξεργασίας πριν τη συλλογή δεδομένων και να ενημερώσει το πρόσωπο στο οποίο γίνεται η συλλογή. Ο πελάτης δεν πρέπει να επεξεργάζεται δεδομένα για διαφορετικούς σκοπούς από τον αρχικό.

Επιπλέον πρέπει να διασφαλίζεται ότι τα δεδομένα δεν χρησιμοποιούνται παράνομα από τον πάροχο ή από τους υπεργολάβους του. Επειδή στις περισσότερες περιπτώσεις χρησιμοποιούνται πολλοί υπεργολάβοι, ο κίνδυνος για παράνομη επεξεργασία δεδομένων είναι υψηλός. Για την ελαχιστοποίηση του κινδύνου, προτείνεται να περιλαμβάνονται μέτρα μετριασμού και καταγραφή των διαδικασιών επεξεργασίας δεδομένων από τους υπαλλήλους του παρόχου ή των υπεργολάβων. Επίσης η σύμβαση πρέπει να περιέχει κυρώσεις σε περίπτωση παραβίασης της νομοθεσίας περί προστασίας των δεδομένων.

5.3.5.4 Διαγραφή δεδομένων

Τα δεδομένα προσωπικού χαρακτήρα πρέπει να διατηρούνται σε μορφή που επιτρέπει την αναγνώριση της ταυτότητας των προσώπων στα οποία αναφέρονται, μέχρι την ολοκλήρωση της επεξεργασίας τους. Τα δεδομένα που δεν είναι πλέον απαραίτητα, πρέπει να διαγράφονται ή να καθίστανται ανώνυμα. Εάν τα δεδομένα δεν μπορούν να διαγραφούν λόγω νομικών κανόνων (π.χ. φορολογικές ρυθμίσεις) προτείνεται να είναι αδύνατη η πρόσβαση σε αυτά. Είναι ευθύνη του πελάτη να διασφαλίζει ότι τα δεδομένα διαγράφονται μόλις εκπληρώσουν το σκοπό τους.

Η αρχή της διαγραφής δεδομένων ισχύει για όλα τα δεδομένα ανεξαρτήτου αποθηκευτικού μέσου(π.χ. σκληρός δίσκος, εφεδρικές ταινίες). Επειδή τα δεδομένα μπορεί να είναι αποθηκευμένα σε πολλαπλά αντίγραφα, πρέπει να διαγράφονται από παντού, οι τωρινές και προηγούμενες εκδόσεις τους καθώς και τα προσωρινά αρχεία ή τμήματα αρχείων.

Για την ασφαλή διαγραφή των δεδομένων πρέπει να καταστρέφονται ή να απομαγνητίζονται τα μαγνητικά μέσα αποθήκευσης ή να χρησιμοποιηθεί η μέθοδος της επεγγραφής (overwriting). Στην επεγγραφή χρησιμοποιούνται ειδικά λογισμικά όπου επεγγράφουν δεδομένα πάρα πολλές φορές.

Ο πελάτης πρέπει να βεβαιώνεται ότι ο πάροχος διασφαλίζει την ασφαλή διαγραφή των δεδομένων, όπως αναφέραμε στην προηγούμενη παράγραφο, τοποθετώντας μια σχετική διάταξη στην σύμβαση μεταξύ πελάτη και παρόχου. Το ίδιο ισχύει και για τις συμβάσεις παρόχου και υπεργολάβων.

5.3.5.5 Συμβατικές εγγυήσεις μεταξύ πελάτη και παρόχου υπηρεσιών

Όταν ο πελάτης αποφασίζει να συνάψει σύμβαση παροχής υπηρεσιών cloud οφείλει να επιλέγει πάροχο που να μπορεί να λάβει τα απαραίτητα μέτρα ασφάλειας και οργάνωσης. Σύμφωνα με τον νόμο πρέπει να υπογραφεί σύμβαση που να θεσπίζει τη σχέση μεταξύ τους σε έγγραφη ή άλλη μορφή. Έτσι η σύμβαση πρέπει κατ' ελάχιστον να προβλέπει ότι ο πάροχος εκτελεί την επεξεργασία σύμφωνα με τις οδηγίες του πελάτη και με γνώμονα την προστασία των δεδομένων προσωπικού χαρακτήρα.

Για να διασφαλίζεται η ασφάλεια δικαίου, η σύμβαση πρέπει να προβλέπει τα ακόλουθα θέματα:

1. Αναλυτικές οδηγίες για τον πάροχο από τον πελάτη, με έμφαση στις συμφωνίες επιπέδου εξυπηρέτησης και στις συναφείς κυρώσεις.

2. Προσδιορισμός των μέτρων ασφαλείας, τα οποία πρέπει να λάβει ο πάροχος.

3. Το αντικείμενο και το χρονοδιάγραμμα της υπηρεσίας που θα προσφέρει ο πάροχος, το μέγεθος, τον τρόπο και τον σκοπό της επεξεργασίας των δεδομένων καθώς και τις κατηγορίες δεδομένων που θα υποστούν επεξεργασία.

4. Προσδιορισμός μεθόδων επιστροφής των δεδομένων ή καταστροφής τους μόλις ολοκληρωθεί η υπηρεσία. Ακόμη πρέπει να υπάρχει μέριμνα για την ασφαλή διαγραφή των δεδομένων προσωπικού χαρακτήρα.

5. Συμπερίληψη ρήτρας εμπιστευτικότητας που θα είναι δεσμευτική για τον πάροχο και τους υπαλλήλους του. Η πρόσβαση στα δεδομένα πρέπει να γίνεται μόνο σε όσους έχουν την απαραίτητη άδεια.

6. Υποχρέωση του παρόχου να επιτρέπει στον πελάτη την πρόσβαση στα δεδομένα σε άτομα στα οποία αναφέρονται τα δεδομένα για έλεγχο, διόρθωση και διαγραφή.

7. Στην σύμβαση πρέπει να αναφέρεται ότι πάροχος δεν μπορεί να αποθηκεύει τα δεδομένα σε τρίτους, παρά μόνο σε υπεργολάβους. Ο πάροχος πρέπει να έχει την έγκριση του πελάτη για την πρόσληψη υπεργολάβων και να μπορεί να αλλάζει ή να τερματίζει την συνεργασία τους. Η σύμβαση μεταξύ παρόχου και υπεργολάβου πρέπει να είναι αντίστοιχη με αυτή του παρόχου πελάτη. Επίσης πρέπει να διασφαλίζεται ότι ο πάροχος και οι υπεργολάβοι εκτελούν μόνο τις οδηγίες του πελάτη.

8. Σαφής καθορισμός των ευθυνών του παρόχου για ενημέρωση του πελάτη σε περίπτωση παραβίασης δεδομένων.

9. Υποχρέωση του παρόχου να παρέχει λίστα τοποθεσιών στις οποίες γίνεται επεξεργασία των δεδομένων του πελάτη.

10. Το δικαίωμα του πελάτη να παρακολουθεί τις διαδικασίες επεξεργασίας του παρόχου και την υποχρέωση του παρόχου να συνεργάζεται.

11. Προτείνεται να υπάρχει στην σύμβαση η ενημέρωση του πελάτη σε τυχόν αλλαγές στις υπηρεσίες που παρέχονται, όπως π.χ. η εκτέλεση πρόσθετων λειτουργιών.

12. Προτείνεται να υπάρχει στην σύμβαση καταγραφή και έλεγχος των διαδικασιών επεξεργασίας δεδομένων προσωπικού χαρακτήρα που εκτελούνται από τον πάροχο ή τους υπεργολάβους.

13. Ενημέρωση του πελάτη σε περίπτωση που χρειαστεί να γίνει κοινοποίηση των δεδομένων προσωπικού χαρακτήρα του από αρχή επιβολής του νόμου, όπως π.χ. μια αστυνομική έρευνα.

14. Υποχρέωση του παρόχου να παρέχει διαβεβαιώσεις ότι οι μέθοδοι οργάνωσης και επεξεργασίας που χρησιμοποιούνται από εκείνον και τους υπεργολάβους τηρούν την εθνική και διεθνή νομοθεσία.

Σε περίπτωση παραβίασης από τον πελάτη, κάθε πρόσωπο το οποίο υπέστη ζημιά ως αποτέλεσμα επεξεργασίας των δεδομένων του δικαιούται αποζημίωση. Στην περίπτωση που ο πάροχος ή οι υπεργολάβοι χρησιμοποιήσουν τα δεδομένα για άλλους σκοπούς ή τα κοινοποιήσουν σε τρίτους, τότε είναι και εκείνοι υπεύθυνοι και φέρουν ευθύνη για τις παραβιάσεις.

Είναι σημαντικό να τονιστεί ότι πολλοί πάροχοι παρέχουν τυποποιημένες συμβάσεις και υπηρεσίες στους πελάτες. Αυτή η ανισότητα, ενός μικρού πελάτη και ενός μεγάλου παρόχου δεν πρέπει να σταθεί εμπόδιο και ο πελάτης δεν πρέπει να δεχτεί όρους που δεν είναι σύμφωνοι με την νομοθεσία για την προστασία των δεδομένων.

5.3.6 Μέτρα προστασίας και ασφάλειας των δεδομένων

Οι πελάτες είναι υπεύθυνοι για την σωστή επιλογή παρόχων υπηρεσιών που εφαρμόζουν τα απαραίτητα μέτρα ασφάλειας για την επαρκή προστασία των δεδομένων προσωπικού χαρακτήρα και είναι υπεύθυνοι.

Εκτός από τους βασικούς στόχους ασφάλειας των δεδομένων, δηλαδή την διαθεσιμότητα, το απόρρητο και την ακεραιότητα, πρέπει να εφαρμόζονται και συμπληρωματικοί στόχοι, όπως είναι η διαφάνεια, η απομόνωση, η δυνατότητα παρέμβασης, η λογοδοσία και η φορητότητα.

5.3.6.1 Διαθεσιμότητα

Ως εξασφάλιση διαθεσιμότητας ορίζεται η διασφάλιση έγκαιρης και αξιόπιστης πρόσβασης σε δεδομένα προσωπικού χαρακτήρα.

Μερικά προβλήματα διαθεσιμότητας είναι η τυχαία απώλεια σύνδεσης δικτύου μεταξύ πελάτη και παρόχου, λόγω κακόβουλων επιθέσεων, όπως π.χ. επιθέσεις άρνησης υπηρεσίας (DoS), οι τυχαίες αστοχίες υλικού στο δίκτυο και στο σύστημα επεξεργασίας του παρόχου ή στο σύστημα αποθήκευσης, οι διακοπές ρεύματος και λοιπά προβλήματα υποδομής.

Οι πελάτες προτείνεται να ελέγχουν αν ο πάροχος λαμβάνει τα απαραίτητα μέτρα για την αντιμετώπιση κινδύνων, όπως π.χ. εφεδρικούς διαδικτυακούς συνδέσμους δικτύου, μηχανισμούς πολλαπλής αποθήκευσης και εφεδρική αποθήκευση δεδομένων.

5.3.6.2 Ακεραιότητα

Ως ακεραιότητα ορίζεται η ιδιότητα των δεδομένων να διατηρούν τη γνησιότητα τους και να μην υφίστανται κακόβουλη ή τυχαία τροποποίηση κατά την επεξεργασία, αποθήκευση ή διαβίβαση. Τυχόν αλλαγές μπορούν να εντοπιστούν με κρυπτογραφικούς μηχανισμούς ελέγχου γνησιότητας, όπως κωδικοί ή υπογραφές ελέγχου γνησιότητας μηνύματος.

5.3.6.3 Απόρρητο

Στις υπηρεσίες cloud, η κρυπτογράφηση είναι πολύ σημαντική για την προστασία του απορρήτου των δεδομένων προσωπικού χαρακτήρα εφόσον εφαρμόζεται σωστά. Η κρυπτογράφηση προτείνεται να είναι ενεργή συνέχεια, είτε τα δεδομένα είναι αδρανή ή βρίσκονται σε κίνηση. Επίσης πρέπει να τονιστεί ότι τα κλειδιά κρυπτογράφησης πρέπει να κρατούνται σε ασφαλές μέρος, αφού από αυτά εξαρτάται η ασφάλεια των δεδομένων.

Η επικοινωνία του παρόχου και του πελάτη, καθώς και μεταξύ των data centers προτείνεται να είναι πάντα κρυπτογραφημένη. Ακόμη η διαχείριση της πλατφόρμας cloud να γίνεται μόνο μέσω ασφαλής σύνδεσης.

Πρόσθετα τεχνικά μέτρα για την διασφάλιση του απορρήτου είναι οι μέθοδοι πιστοποίησης, που προτείνεται να χρησιμοποιούνται από τους υπαλλήλους του παρόχου και των υπεργολάβων.

5.3.6.4 Απομόνωση των δεδομένων

Στις υποδομές cloud οι πόροι (αποθηκευτικός χώρος, μνήμη και δίκτυα) μοιράζονται από πολλούς πελάτες, με αποτέλεσμα να υπάρχει κίνδυνος κοινοποίησης των δεδομένων τους. Η απομόνωση στοχεύει στην προστασία των δεδομένων από την χρησιμοποίηση τους για άλλους σκοπούς, στην προστασία του απορρήτου και της ακεραιότητας των δεδομένων.

Για να επιτευχθεί η απομόνωση των δεδομένων απαιτείται η απόδοση δικαιωμάτων στους αρμόδιους για την επεξεργασία, τα οποία πρέπει να εξετάζονται τακτικά. Προτείνεται οι αρμόδιοι να κατέχουν τα ελάχιστα δικαιώματα που χρειάζονται για να έχουν πρόσβαση μόνο στα δεδομένα που χρειάζονται. Επίσης η απομόνωση των δεδομένων εξαρτάται και από τεχνικά μέτρα όπως η σωστή διαχείριση των εικονικών μηχανών για τον σωστό επιμερισμό των πόρων του συστήματος.

5.3.6.5 Δυνατότητα παρέμβασης

Ο νόμος παρέχει στο πρόσωπο στο οποίο αναφέρονται τα δεδομένα, δικαιώματα πρόσβασης, διόρθωσης, διαγραφής και κλειδώματος. Ο πελάτης πρέπει να ελέγχει αν ο πάροχος παρέχει αυτά τα δικαιώματα, ακόμη και σε δεδομένα που επεξεργάζονται από υπεργολάβους. Η σύμβαση μεταξύ πελάτη και παρόχου πρέπει να βοηθάει το πελάτη να κάνει χρήση αυτών των δικαιωμάτων, όπως και να ισχύει το ίδιο και τους υπεργολάβους.

5.3.6.6 Φορητότητα

Οι περισσότεροι πάροχοι χρησιμοποιούν δικούς τους τύπους δεδομένων και διεπαφών που δυσκολεύουν την διαλειτουργικότητα και φορητότητα μεταξύ άλλων παρόχων. Εάν ο πελάτης αποφασίσει να αλλάξει πάροχο, αυτή η έλλειψη διαλειτουργικότητας μπορεί να κάνει την μεταφορά δεδομένων πολύ δύσκολη έως αδύνατη. Το ίδιο ισχύει και για τις υπηρεσίες που έχει αναπτύξει στις πλατφόρμες και υποδομές του παρόχου. Έτσι ο πελάτης προτείνεται να ελέγχει αν ο πάροχος μπορεί να εγγυηθεί την φορητότητα των δεδομένων του, πριν κάνει χρήση κάποιας υπηρεσίας του παρόχου.

5.3.6.7 Λογοδοσία

Στις τεχνολογίες πληροφορίας, ως λογοδοσία ορίζεται η ικανότητα ενός οργανισμού να αποδεικνύει τι έκανε και με ποιον τρόπο, σε κάποια στιγμή στο παρελθόν. Στον τομέα προστασίας των δεδομένων επεκτείνεται και περιγράφει τα μέτρα για την σωστή εφαρμογή των αρχών προστασίας των δεδομένων.

Η λογοδοσία στις τεχνολογίες πληροφορίας είναι σημαντική για την έρευνα παραβιάσεων δεδομένων προσωπικού χαρακτήρα, σε περίπτωση που όλοι έχουν μερίδιο ευθύνης. Η ικανότητα της πλατφόρμας να παρακολουθεί και να καταγράφει τις διαδικασίες επεξεργασίας είναι υψίστης σημασίας.

Ακόμη προτείνεται οι πάροχοι να παρέχουν έγγραφα που να αποδεικνύουν ότι λαμβάνουν αποτελεσματικά μέτρα για την επίτευξη των στόχων των βασικών αρχών της προστασίας των δεδομένων. Παραδείγματα τέτοιων μέτρων είναι οι διαδικασίες αναγνώρισης των μηχανισμών επεξεργασίας δεδομένων, οι διαδικασίες απάντησης σε αιτήματα πρόσβασης, η κατανομή πόρων, ο καθορισμός υπευθύνων προστασίας.

5.3.7 Διεθνής διαβίβαση δεδομένων

Σύμφωνα με τα άρθρα 25 και 26 της οδηγίας 95/46/ΕΚ, τα δεδομένα προσωπικού χαρακτήρα μπορούν να κυκλοφορήσουν σε χώρες εκτός της Ευρωπαϊκής Ένωσης, μόνο εάν οι χώρες ή ο αποδέκτης παρέχουν επαρκές επίπεδο προστασίας των δεδομένων. Αλλιώς ο πελάτης και ο πάροχος πρέπει να λάβουν ειδικά μέτρα. Ωστόσο, βασικό χαρακτηριστικό του cloud είναι η έλλειψη σταθερής τοποθεσίας των δεδομένων. Έτσι ο πελάτης δεν γνωρίζει που βρίσκονται, που αποθηκεύονται ή που διαβιβάζονται τα δεδομένα του. Αυτό κάνει τα παραδοσιακά νομικά μέσα ανίσχυρα σε τρίτες χώρες εκτός Ευρωπαϊκής Ένωσης, όπου διαβιβάζονται τα δεδομένα.

5.3.7.1 Χώρες που τηρούν τις αρχές ασφαλούς λιμένα και χώρες που παρέχουν αρκετή προστασία

Οι διαπιστώσεις επαρκούς προστασίας των δεδομένων, συμπεριλαμβανομένων των αρχών ασφαλούς λιμένα έχουν περιορισμένο γεωγραφικό πεδίο εφαρμογής και έτσι δεν καλύπτουν όλες τις διαδικασίες διαβίβασης εντός του cloud. Σύμφωνα με τους νόμους της Ευρωπαϊκής Ένωσης η διαβίβαση δεδομένων σε οργανισμούς των ΗΠΑ επιτρέπεται, μόνο εάν παρέχουν επαρκές επίπεδο προστασίας στα διαβιβασθέντα δεδομένα.

Δεν αρκεί όμως μόνο η συμμόρφωση προς τις αρχές ασφαλούς λιμένα, εάν δεν τηρούνται οι βασικές αρχές προστασίας των δεδομένων. Το άρθρο 17 της οδηγίας της Ευρωπαϊκής Ένωσης επιβάλλει στον πελάτη την σύναψη σύμβασης με τον πάροχο. Η εν λόγω σύμβαση δεν απαιτεί προηγούμενη έγκριση από τις ευρωπαϊκές αρμόδιες αρχές προστασίας δεδομένων και περιγράφει αναλυτικά την επεξεργασία και τα μέτρα προστασίας που λαμβάνονται για την ασφαλή

διατήρηση των δεδομένων. Οι διάφοροι εθνικοί νόμοι και αρμόδιες αρχές προστασίας δεδομένων προβλέπουν πρόσθετες απαιτήσεις.

Επίσης οι επιχειρήσεις που εξάγουν δεδομένα δεν πρέπει να βασίζονται μόνο στην πιστοποίηση ασφαλούς λιμένα του παρόχου, αλλά πρέπει να ζητούν αποδείξεις για αυτές. Αυτό έχει ιδιαίτερη σημασία για τις πληροφορίες που παρέχονται στα πρόσωπα τα οποία θίγονται από την επεξεργασία δεδομένων.

Ο πελάτης πρέπει να ελέγχει εάν οι τυποποιημένες συμβάσεις του παρόχου ακολουθούν τις εθνικές απαιτήσεις που διέπουν τις συμβάσεις επεξεργασίας δεδομένων. Η εθνική νομοθεσία μπορεί να απαιτεί αναλυτική περιγραφή των εργασιών επεξεργασίας στη σύμβαση, η οποία περιλαμβάνει μεταξύ άλλων, τις τοποθεσίες των υπεργολάβων καθώς και δεδομένα που σχετίζονται με την ανιχνευσιμότητα των δεδομένων. Συνήθως οι πάροχοι δεν παρέχουν στον πελάτη αυτές τις πληροφορίες. Ο πάροχος πρέπει να τις παρέχει αν απαιτούνται από την εθνική νομοθεσία. Αλλιώς ο πελάτης μπορεί να χρησιμοποιήσει τυποποιημένες συμβατικές ρήτρες ή δεσμευτικούς εταιρικούς κανόνες.

5.3.7.2 Τυποποιημένες συμβατικές ρήτρες

Οι τυποποιημένες συμβατικές ρήτρες που έχει θεσπίσει η Ευρωπαϊκή Επιτροπή για την οριοθέτηση της διεθνούς διαβίβασης δεδομένων μεταξύ του πελάτη και του παρόχου βασίζονται σε διμερή προσέγγιση. Οι ρήτρες μπορούν να χρησιμοποιηθούν για την παροχή επαρκών εγγυήσεων για τη διεθνή διαβίβαση δεδομένων στο cloud.

Εκτός από τις τυποποιημένες συμβατικές ρήτρες, οι πάροχοι θα μπορούσαν να προτείνουν διατάξεις βάσει των εμπειριών τους, εάν αυτές δεν παραβαίνουν τις τυποποιημένες συμβατικές ρήτρες της Ευρωπαϊκής Επιτροπής ή τα δικαιώματα και τις ελευθερίες των προσώπων στα οποία αναφέρονται τα δεδομένα. Έτσι οι επιχειρήσεις δεν μπορούν να τροποποιούν τις ρήτρες γιατί θα πάψουν να θεωρούνται τυποποιημένες.

Όταν ο πάροχος είναι εγκατεστημένος στην Ευρωπαϊκή Ένωση, τότε η κατάσταση περιπλέκεται γιατί οι τυποποιημένες συμβατικές ρήτρες ισχύουν μόνο σε περίπτωση διαβίβασης δεδομένων από πελάτη στην Ευρωπαϊκή Ένωση σε πάροχο εκτός Ευρωπαϊκής Ένωσης.

Ακόμη η σχέση μεταξύ παρόχου και υπεργολάβων πρέπει να διέπετε από γραπτή συμφωνία η οποία θα επιβάλλει στους υπεργολάβους τις ίδιες υποχρεώσεις που βαρύνουν τον πάροχο, οι οποίες προέρχονται από τυποποιημένες ρήτρες.

5.3.7.3 Δεσμευτικοί εταιρικοί κανόνες

Οι δεσμευτικοί εταιρικοί κανόνες συνιστούν κώδικα δεοντολογίας για επιχειρήσεις που διαβιβάζουν δεδομένα εντός του ομίλου τους. Αυτοί οι κανόνες μπορούν να χρησιμοποιηθούν για τη διαβίβαση δεδομένων χωρίς να απαιτείται η υπογραφή συμβάσεων μεταξύ παρόχου και υπεργολάβων ανά πελάτη.

Η ύπαρξη δεσμευτικών εταιρικών κανόνων θα επιτρέπει στον πελάτη να εμπιστεύεται τα δεδομένα προσωπικού χαρακτήρα του στον πάροχο, παρέχοντας του διαβεβαίωση ότι τα δεδομένα που διαβιβάζονται στο επιχειρηματικό πεδίο του παρόχου είναι επαρκώς προστατευμένα. (Ομάδα Εργασίας του Άρθρου 29 για την Προστασία των Δεδομένων)

Βιβλιογραφία

Service-level agreement, 2017. Διαθέσιμο από: <https://en.wikipedia.org/wiki/Service-level_agreement>. [4 Φεβρουαρίου 2017]

Ομάδα Εργασίας του Άρθρου 29 για την Προστασία των Δεδομένων 2012, Γνώμη 05/2012 σχετικά με τη νεφοϋπολογιστική. Διαθέσιμο από: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_el.pdf >. [4 Φεβρουαρίου 2017]