ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ (Πάτρα)

Πτυχιακή Εργασία:

« Τεχνολογίες Υπολογιστικού Νέφους και Θέματα Ασφάλειας»

Βαρμπετιάν Αγκόπ

Κόντης Κωνσταντίνος

Παπανικολάου Αλέξανδρος

Επιβλέπων Καθηγητής:

Δρ. Γιωτόπουλος Κωνσταντίνος

Πάτρα 2015

ΠΡΟΛΟΓΟΣ

Η παρούσα πτυχιακή εργασία πραγματοποιήθηκε στο Ανώτατο Τεχνολογικό Ίδρυμα Δυτικής Ελλάδος, στο Τμήμα Διοίκησης Επιχειρήσεων (Πάτρα). Στόχος αυτής της εργασίας είναι η ανάλυση τεχνολογιών και υπηρεσιών υπολογιστικού νέφους και θέματα ασφάλειας που προκύπτουν σε αυτά καθώς και τεχνικές λύσεις για την επίλυση αυτών.

ΠΕΡΙΛΗΨΗ

Στις μέρες μας παρατηρείται ταχεία ανάπτυξη υπηρεσιών και εφαρμογών που αφορούν στο υπολογιστικό νέφος. Τα πάντα, πλέον κινούνται μέσω cloud. Ο αριθμός των εταιρειών που χρησιμοποιούν αποκλειστικά και κατά κόρον τις υπηρεσίες που εφαρμόζονται σε αυτό, ολοένα και αυξάνεται. Από την άλλη σκοπιά, ένας απλός χρήστης του διαδικτύου χρησιμοποιεί τις ευκολίες που προσφέρουν οι υπηρεσίες και οι εφαρμογές αυτές, χρησιμοποιώντας το Smartphone, το tablet ή τον υπολογιστή του. Το cloud computing υπάρχει παντού στην καθημερινότητα, ανεξάρτητα αν οι χρήστες του γνωρίζουν ότι το χρησιμοποιούν ή όχι.

Υπάρχει, βέβαια για τους πιο προσεκτικούς, η αμφιβολία της ασφάλειας που μπορεί να εξασφαλίσει ένας χρήστης του cloud computing. Στην εργασία αυτή θα παρατεθεί μια αναλυτική μελέτη του κλάδου της επιστήμης της Πληροφορικής που αφορά στο Cloud Computing (Συστήματα Υπολογιστικού Νέφους) καθώς και κατά πόσο, σε ποιο ποσοστό αλλά και με τι μέτρα ασφάλειας μπορεί κανείς να περιηγείται άφοβα στις ευκολίες των εφαρμογών και υπηρεσιών του υπολογιστικού νέφους.

Αρχικά, θα γίνει μια ανάλυση του ορισμού και της ιστορίας του υπολογιστικού νέφους (cloud computing). Εν συνεχεία, θα γίνει αναφορά σε εισαγωγικές έννοιες της ασφάλειας συστημάτων αλλά και στη σημαντικότητα της ασφάλειας του χρήστη. Συνεχίζοντας, θα αναλυθούν τα πιο συχνά ζητήματα ασφάλειας που προκύπτουν κατά την χρήση υπηρεσιών υπολογιστικού νέφους, επιθέσεις και τεχνολογίες που χρησιμοποιούνται για την αντιμετώπισή τους.

Τέλος, θα παρατεθούν κάποιες από τις πιο αποτελεσματικές εφαρμογές μέτρων προστασίας σε τέτοια συστήματα.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ ΣΤΟ CLOUD COMPUTING

1.1 Εισαγωγή

Τα Συστήματα υπολογιστικού Νέφους (Cloud Computing) αποτελούν μια καινούρια προσέγγιση στην επιστήμη των κατανεμημένων συστημάτων. Πρόκειται για χρήση υπολογιστικής ισχύος που χωροταξικά βρίσκεται σε ένα «σύννεφο» απόμακρων δικτύων. Αυτή η πρακτική είναι γνώριμη σε οποιονδήποτε χρησιμοποιεί διαδικτυακές υπηρεσίες για τη διαχείριση και αποθήκευση δεδομένων. Παρόλο τον μικρό χρόνο της ευρείας τους χρήσης, ο αριθμός των χρηστών τους αυξάνεται σημαντικά. Το γεγονός ότι οι λειτουργίες τους έχουν βασιστεί σε παλαιότερες τεχνολογίες, δοκιμασμένες και γνωστές, προσδίδει κύρος και ασφάλεια στον χρήστη για την αξιοπιστία τους.

Το σημαντικότερο πλεονέκτημα του Cloud Computing (θα αναφερόμαστε σε αυτό με αυτόν τον όρο) είναι πως οι υπηρεσίες που παρέχονται μέσω αυτού χαρακτηρίζονται από ταχύτητα, μικρή ανάγκη για υπολογιστική ισχύ και αποθηκευτική δυνατότητα από τον χρήστη του συστήματος, καθώς οι ανάγκες αυτές καλύπτονται από τις εφαρμογές του.

Το Cloud Computing, έχει ως βασική του προϋπόθεση την χρήση του διαδικτύου. Θα μπορούσε κανείς να το αντιστοιχίσει με το Internet Computing. Η πιο συνήθης απεικόνιση του διαδικτύου είναι με ένα σύννεφο (cloud). Οι χρήστες, λοιπόν, του Cloud Computing μπορούν να χρησιμοποιήσουν πόρους βάσεων δεδομένων μέσω διαδικτύου από οποιαδήποτε συσκευή ή μέρος, για οποιοδήποτε χρονικό περιθώριο χωρίς να ανησυχούν για τη συντήρηση και τη διαχείριση των πραγματικών πόρων που τίθενται σε εφαρμογή. Οι βάσεις δεδομένων στο Cloud Computing είναι δυναμικές και εξελικτικές, ώστε να είναι εφικτά τα παραπάνω. Με απλά λόγια, αποτελείται από μεγάλα κέντρα δεδομένων, δελεαστικές παροχές στους χρήστες του, όπως οι απαιτήσεις που αναφέρονται παραπάνω, αλλά και η οικονομική ευελιξία. Ο χρήστης του Cloud υποχρεούται να πληρώνει ανάλογα με τη χρήση και την εφαρμογή. Είναι γενικά αποδεκτό ότι τόσο χρήστες όσο και προγραμματιστές έχουν έτσι τη δυνατότητα να κάνουν περισσότερα με λιγότερα: έχουν πρόσβαση σε

μεγαλύτερη υπολογιστική ισχύ χωρίς να χρειάζεται να επενδύσουν μεγάλα ποσά σε εξοπλισμό.

Το Cloud Computing πολλές φορές, λανθασμένα, ταυτίζεται με το Grid Computing. Το πρώτο, σε αντίθεση με το δεύτερο, έχει χαρακτήρα autonomic computing. Πρόκειται για μια αυτόνομη και ανεξάρτητη πλατφόρμα από πλευράς υπολογισμού. Το πιο απλό παράδειγμα εφαρμογών του Cloud Computing είναι τα Google Apps, τα οποία προσφέρουν πρόσβαση σε άπειρες εφαρμογές, και μόνο με τη χρήση ενός φυλλομετρητή μπορεί κανείς να επεκταθεί σε χιλιάδες υπολογιστές μέσω διαδικτύου.

Το Cloud Computing πιστεύεται επίσης ότι μπορεί να συμβάλλει στην μείωση της εκπομπής διοξειδίου του άνθρακα. Υπηρεσίες πληροφορικής για ιδιώτες και οργανισμούς φιλοξενούνται στο Διαδίκτυο και έτσι δεν υπάρχει ανάγκη για τοπικούς server στο χώρο τους. Οι υπολογιστές βρίσκονται σε κέντρα δεδομένων σχεδιασμένα για βέλτιστη ενεργειακή αποδοτικότητα (για παράδειγμα, όσο το δυνατόν πιο κοντά σε σταθμούς παραγωγής ενέργειας). Επιπλέον, επιχειρήσεις και οργανισμοί αποφεύγουν την επένδυση και τη χρήση επιπλέον εξοπλισμού για να καλύψουν εποχιακές ανάγκες.

1.2 Ιστορική Αναδρομή

Η κεντρική ιδέα ενός συστήματος της νοοτροπίας του Cloud Computing χρονολογείται πίσω στο 1950. Κεντρικοί υπολογιστές μεγάλου όγκου και κλίμακας φαίνονται να αποτελούν το μέλλον της επιστήμης της Πληροφορικής, γίνονται ολοένα και πιο διαδεδομένοι, είτε σε εταιρίες είτε σε πανεπιστήμια είτε σε οργανισμούς. Η πρόσβαση ήταν επιτυχής μέσω client/terminal υπολογιστές, γνωστούς ως “dump terminals”, καθώς χρησιμοποιούνταν για επικοινωνία χωρίς όμως να μπορούν να παρέχουν εσωτερική επεξεργαστική δυνατότητα.

Στην προσπάθεια να γίνει πιο αποτελεσματική χρήση υπολογιστών, μια καινούργια τεχνική εξελίχθηκε, κατά την οποία επιτρεπόταν η χρήση της CPU αλλά και του φυσικού μέσου από πολλά τερματικά και χρήστες αντίστοιχα. Κάτι τέτοιο εξάλειφε την περίοδο αχρηστίας του υπολογιστή επομένως γινόταν πιο αποτελεσματική η

επένδυση σε αυτόν. Διαμοιράζοντας την CPU σε έναν κεντρικό υπολογιστή, άνθισε το time-sharing στη βιομηχανία της πληροφορικής.

Κατά τη δεκαετία του ’70, το time-sharing έγινε γνωστό ως RJE (Remote Job Entry). Η ονοματολογία συσχετιζόταν κυρίως με μεγάλους παράγοντες της πληροφορικής, όπως IBM και DEC. Από αυτό η IBM εμπνεύστηκε το VM Operating System ώστε να μπορεί να παρέχει time-sharing υπηρεσίες.

Το 1990, οι εταιρίες τηλεπικοινωνιών, οι οποίες μέχρι πρότινος παρείχαν αποκλειστικά point-to-point κυκλώματα δεδομένων, ξεκινούν να προσφέρουν υπηρεσίες μέσω VPNs, με σχετικά χαμηλότερη ποιότητα στην υπηρεσία αλλά με ιδιαίτερα ανταγωνιστικό κόστος. Η προσαρμογή της κίνησης του δικτύου, για την καλύτερη χρήση των servers, έδωσε την δυνατότητα της αποτελεσματικής χρήσης του συνολικού bandwidth. Τότε, ξεκινά να χρησιμοποιείται το «σύννεφο» σαν σύμβολο του δικτύου, για να μπορεί να οριοθετηθεί το σημείο που ο πάροχος παύει να είναι υπεύθυνος και αυτός ο ρόλος περνά στον χρήστη. Το cloud computing επεκτείνει και άλλο τα όρια του και καλύπτει servers και δίκτυο(υποδομή και σύστημα).

Όσο οι υπολογιστές γίνονται ολοένα μέρος της καθημερινότητας, επιστήμονες ψάχνουν τρόπους επέκτασης της υπολογιστικής ισχύς ώστε να δύναται η κάλυψη όλο και περισσότερων χρηστών σε time-sharing υπηρεσίες. Αλγόριθμοι γράφονται, πρωτόκολλα εγκαθιδρύονται, λαμβάνει χώρα η βελτιστοποίηση των υποδομών, των πλατφορμών, και των εφαρμογών που θέτουν σε προτεραιότητα τη CPU με αποτέλεσμα να αυξηθεί κατακόρυφα η αποδοτικότητα για τους τελικούς χρήστες.

Από το 2000 το Cloud Computing είναι πραγματικότητα. Μπαίνει στην αγορά και κερδίζει αμέσως το ενδιαφέρον πολλών εταιριών. Στις αρχές του 2008 η OpenNebula, χρηματοδοτούμενη από το πρόγραμμα RSERVOIR European Commission, έγινε το πρώτο open-source λογισμικό που χρησιμοποιήθηκε για ναν ανάπτυξη ιδιωτικών και υβριδικών clouds. Την ίδια χρονιά, έγιναν προσπάθειες παροχής εγγυημένης ποιότητας υπηρεσιών σε cloud υποδομές, υπό το πλαίσιο του χρηματοδοτούμενου προγράμματος IRMOS (by European Commission). Η απόρροια των παραπάνω ήταν η εγκαθίδρυση του cloud computing σε πραγματικό χρόνο.

Στα μέσα του 2008, η Gartner χρησιμοποίησε το cloud computing για να διαμορφώσει τη σχέση μεταξύ των καταναλωτών των υπηρεσιών πληροφορικής, όσων χρησιμοποιούν υπηρεσίες πληροφορικής και όσους τις πωλούν. Παρατήρησε, λοιπόν, ότι οι οργανώσεις αλλάζουν από την εταιρεία που ανήκει το υλικό και το λογισμικό σε μοντέλα υπηρεσιών μιας χρήσης, επομένως η προβλεπόμενη μετάβαση στην πληροφορική θα οδηγούσε σε δραματική αύξηση των προϊόντων πληροφορικής σε κάποιες περιοχές αλλά σε σημαντική μείωση προϊόντων σε άλλες περιοχές. Στο τέλος του 2008, το Microsoft Azure ήρθε στο φως.

Τον Ιούλιο του 2010, ξεκινά μια συνεργασία Rackspace Hosting και NASA για τη δημιουργία ενός open-source cloud λογισμικού, γνωστό ως OpenStack. Στόχος ήταν να βοηθηθούν οργανισμοί που προσέφεραν υπηρεσίες cloud computing που έτρεχαν συγκεκριμένο υλικό. Ο πρώτος κώδικας ήρθε από την πλατφόρμα Nebula της NASA και από την πλατφόρμα Rackspace Cloud File.

Τον Μάρτιο του 2011, η IBM εξέδωσε το IBM SmartCloud για να υποστηρίξει το Smarter Planet. Ανάμεσα σε πολλά συστατικά των θεμελίων του Smarter Computing, το cloud computing καταλαμβάνει μια σημαντική θέση.

Τον Ιούνιο του 2012, η Oracle ανακοίνωσε το Oracle Cloud. Παρόλο που το Oracle Cloud βρίσκεται εν εξελίξει, θεωρείται το πρώτο που θα παρέχει σε χρήστες τη δυνατότητα να έχουν πρόσβαση σε μια ολοκληρωμένη σειρά τεχνολογιών πληροφορικής, συμπεριλαμβανομένων επιπέδων του SaaS(Applications-Εφαρμογές), IaaS(Infrastructure-Υποδομή) και PaaS(Platform-Πλατφόρμα).

1.3 Ορισμός

Για να μπορεί να υπάρξει ένας ξεκάθαρος ορισμός του Cloud Computing, αναλύθηκαν μια σειρά από επιμέρους ορισμούς με τα εξής βασικά χαρακτηριστικά να αναφέρονται σε όλους:

- Scalability
- Virtualization
- Pay-per-use μοντέλο

- User Friendliness
- Internet Centric
- Variety of resources
- Automatic Adaption
- Resource Optimization
- Service SLAs (Service-level Agreement)
- Infrastructure SLAs

Από τη σύνθεση των χαρακτηριστικών και των ορισμών που επικρατούσαν μέχρι πρότινος, προκύπτει ο εξής ορισμός:

"Clouds are a large pool of **easily usable** and **accessible virtualized** resources (such as hardware, development platforms and/or services). These **resources** can be **dynamically reconfigured** to **adjust to a variable load** (scale), allowing also for an **optimum resource utilization**. This pool of resources is typically exploited by a **pay-per-use model** in which guarantees are offered by the **Infrastructure Provider** by means of customized **SLAs**."

Τα Συστήματα Υπολογιστικού Νέφους είναι μια μεγάλη ομάδα εύχρηστων και εικονικά προσβάσιμων πόρων (όπως υλικό, πλατφόρμες και υπηρεσίες). Αυτοί οι πόροι μπορούν να αναδιαμορφωθούν δυναμικά ώστε να προσαρμόζονται σε μεταβλητό περιβάλλον επιτρέποντας έτσι την βέλτιστη χρήση των πόρων. Αυτή την ομάδα πόρων, την εκμεταλλεύεται τυπικά από το μοντέλο pay-per-use του οποίου οι εγγυήσεις καθορίζονται από τον Πάροχο Υποδομής μέσω των προσαρμοσμένων SLAs.

Πέραν του καθορισμού του ορισμού, έγινε και μια προσπάθεια σύγκρισης του Grid Computing και του Cloud Computing η οποία βασίζεται σε ένα σύνολο χαρακτηριστικών αναφορικά με τις δικτυακές υπηρεσίες και τα κατανεμημένα συστήματα.

Κοινά Χαρακτηριστικά Cloud και Grid Computing:

Resource Heterogeneity	Υποστηρίζουν την συνάθροιση ετερογενών πόρων
User Access	Πρόσβαση χρηστών στους πόρους με

διαφανή τρόπο

Κοινά Χαρακτηριστικά με διαφορετική προσέγγιση :

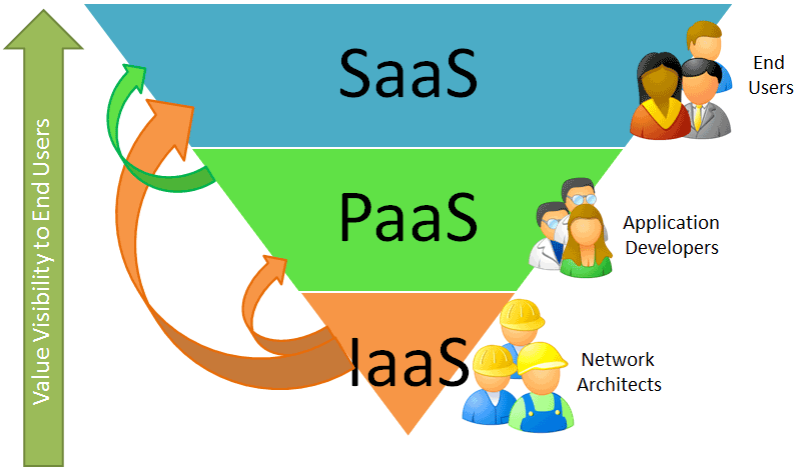
	GRID	CLOUD
Virtualization	Καλύπτει την ετερογένεια των πόρων μέσω του Virtualization δεδομένων και πόρων	Επεκτείνει την διαδικασία και στο υλικό
Security	Αυθεντικοποίηση μέσω πιστοποιητικών	Κάθε χρήστης έχει μοναδικά πρόσβαση σε κάθε εικονικό περιβάλλον (isolation-απομόνωση)
Scalability	Μέσω αύξηση του αριθμού των κόμβων	Αναπροσαρμογή των πόρων με αυτοματοποιημένο τρόπο
Self Management	Πιο εύκολη όταν υπάρχει ενιαία διαχείριση του συστήματος.	Αυτοματοποιούμενη διαδικασία, προβλέπονται δυσκολίες σε περίπτωση απουσίας ενιαίας διαχείρισης
Qos Guarantees	Περιορισμένες εγγυήσεις συχνά μόνο αυτή της υπηρεσίας βέλτιστης προσπάθειας. Οι εφαρμογές αναγκάζονται να καλύψουν αυτόν τον τομέα	Περιορισμένες, οι εφαρμογές κληρονομούν από την πλατφόρμα τις εγγυήσεις.

Διαφορές Cloud και Grid Computing:

	GRID	CLOUD
Resource Sharing	Υποστηρίζει κοινή χρήση των πόρων	Δεν υποστηρίζεται λόγο της απομόνωσης μέσου της Virtualization
High Level Services	Πληθώρα υπηρεσιών όπως υπηρεσίες μεταφοράς δεδομένων και εύρεση μέσο μεταδεδομένων	Έλλειψη που πιθανόν να οφείλεται στο χαμηλό επίπεδο ωριμότητας
Architecture	Προσανατολισμένη στις υπηρεσίες	Αρχιτεκτονικές που επιλέγονται από τον χρήστη
Software Dependencies	Εξάρτηση από την περιοχή εφαρμογής	Ανεξαρτησία από την περιοχή εφαρμογής
Platform Awareness	Απαραίτητη η γνώση του λογισμικού-πελάτη σχετικά με grid λειτουργίες	Ο SP δεν προαπαιτεί γνώση
Software Workflow	Οι εφαρμογές απαιτούν μια προκαθορισμένη ροή εργασιών που να συντονίζει τις υπηρεσίες	Η ροή εργασιών δεν παίζει σημαντικό ρόλο για τις εφαρμογές
Usability	Μικρότερος βαθμός ευχρηστίας	Μεγαλύτερη ευχρηστία μέσω της απόκρυψης λεπτομερειών
Standardization	Υπάρχουν πρότυπα μέσω των οποίων επιτυγχάνεται η διαλειτουργικότητα	Ανάγκη για πρότυπα στην αποθήκευση, ποιότητα υπηρεσιών και καθορισμού των διεπαφών
Payment Model	Ανελαστικό, τιμολόγηση βάση ενός σταθερού	Ευέλικτο, τιμολόγηση βάση της χρήσης της

	ποσού ανά υπηρεσία	υπηρεσίας.

1.4 Παροχή υπηρεσιών Cloud Computing



Εικόνα 1.1. Μοντέλα παροχής υπηρεσιών Cloud Computing
Πηγή http://www.finoit.com/blog/cloud-computing-service-models/

Στο υποκεφάλαιο αυτό, αναφέρονται τα δημοφιλέστερα μοντέλα παροχής υπηρεσιών Cloud Computing, με άξονα την υπηρεσία που χρήζει ανάπτυξης. Τα τρία αυτά μοντέλα αποτελούν το SPI μοντέλο, το οποίο πήρε την ονομασία του από τις λέξεις Service, Platform και Infrastructure. Τα επιμέρους μοντέλα (επίπεδα) προσφερόμενων υπηρεσιών παρόχου σε Cloud Computing Systems είναι:

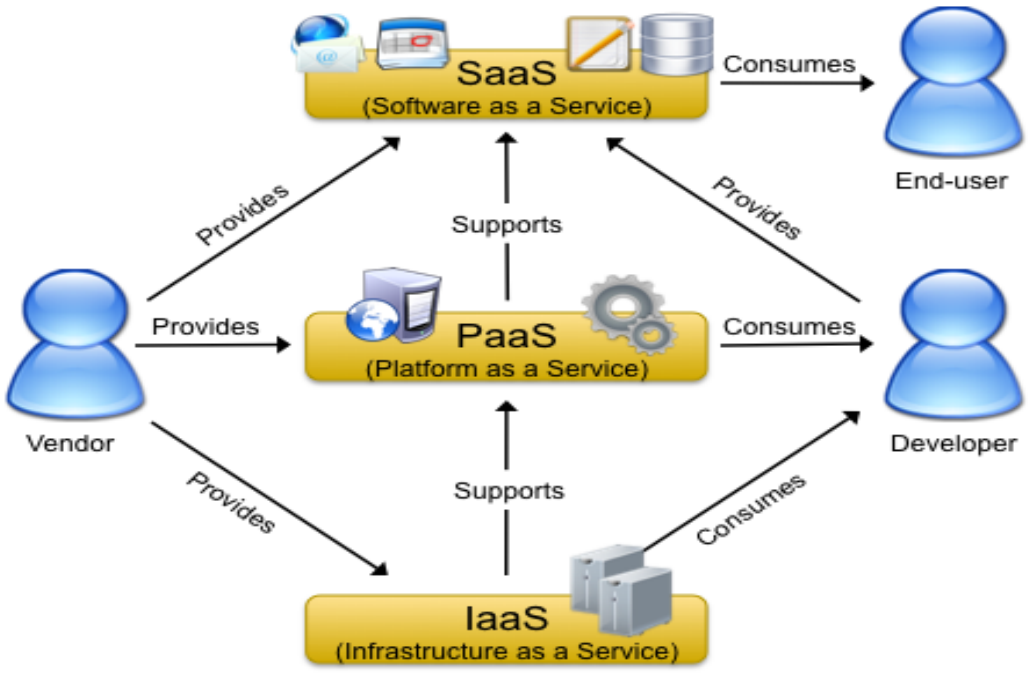
- Λογισμικό ως υπηρεσία (Software as a Service-**SaaS**): Πρόκειται για τον πιο διαδεδομένο μοντέλο παροχής υπηρεσιών Cloud Computing. Δίνεται η δυνατότητα στον χρήστη να χρησιμοποιεί τις εγκατεστημένες σε υποδομή cloud εφαρμογές του παρόχου, χωρίς όμως να έχει την δυνατότητα να ελέγχει, να διαχειρίζεται ή να αναπτύσσει την εν λόγω

υποδομή. Ο απλός χρήστης δεν μπορεί να αντιγράφει ή να διανέμει το λογισμικό αυτό. Η φιλοξενία και η διαχείριση των εφαρμογών ανατίθενται σε τρίτο παράγοντα (third party, τον προμηθευτή του λογισμικού και πάροχο υπηρεσιών). Μια απλή εφαρμογή SaaS μπορεί να εκτελεστεί σε οποιαδήποτε υπάρχουσα υποδομή πρόσβασης στο Internet (browser). Δεν απαιτείται περεταίρω υλικό. Εφαρμογές όπως GoogleApps, Office 365, απέκτησαν φανατικούς χρήστες λόγω της ελαστικότητας που τους δόθηκε από την τεχνολογία αυτή, γνωστή ως CRM(Customer relationship management).

- Πλατφόρμα ως υπηρεσία (Platform as a Service-**PaaS**): Δίνεται η δυνατότητα στον χρήστη να χρησιμοποιήσει υποδομή Cloud Computing για να αναπτύξει εφαρμογές (οι οποίες έχουν υλοποιηθεί με τη χρήση γλωσσών προγραμματισμού ή εργαλείων που υποστηρίζονται από τον πάροχο) που έχει υλοποιήσει ή αποκτήσει. Με άλλα λόγια, η υπηρεσία αφορά ένα ολοκληρωμένο περιβάλλον εφαρμογών και όχι μια μεμονωμένη εφαρμογή. Ο χρήστης έχει τον έλεγχο των εφαρμογών που έχουν αναπτυχθεί, στις οποίες είναι εξουσιοδοτημένος, και όχι τη διαχείριση ολόκληρης της υποδομής. Στην ουσία είναι μια παραλλαγή της SaaS κατά την οποία το περιβάλλον ανάπτυξης για τον χρήστη ως μια υπηρεσία. Με αυτή τη μέθοδο, προγραμματιστές μπορούν να υλοποιούν και αναπτύσσουν web εφαρμογές, χωρίς να απαιτείται επιπλέον υλικό στον υπολογιστή τους.
- Υποδομή ως υπηρεσία (Infrastructure as a Service-**IaaS**): Με αυτό το μοντέλο δίνεται η δυνατότητα στον χρήστη να χρησιμοποιεί συγκεκριμένη επεξεργαστική ισχύ, δίκτυα, αποθηκευτικούς χώρους καθώς και άλλους υπολογιστικούς πόρους. Όπως και παραπάνω, ο χρήστης δεν έχει δυνατότητα ελέγχου και διαχείρισης της υποδομής αλλά έλεγχο των

λειτουργικών συστημάτων και των υπολογιστικών πόρων που χρησιμοποιεί. Τα περιβάλλοντα είναι απομακρυσμένα virtual machines. Το IaaS είναι πρακτική τεχνολογία σε εφαρμογές επικοινωνιών και μεταφοράς πληροφοριών, σε client-server επικοινωνίες αλλά και σε εργασιακά περιβάλλοντα. Από τους πιο δημοφιλείς παρόχους τέτοιων υπηρεσιών είναι Amazon, Orange, Rackspace.

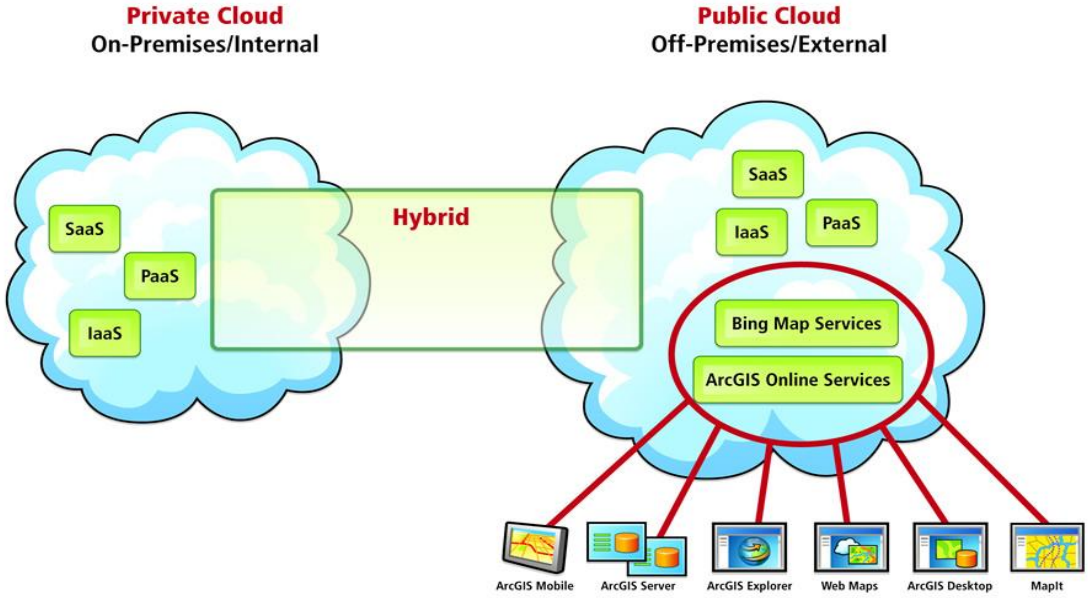
Κάποια χαρακτηριστικά που μπορεί κανείς να συναντήσει στο μοντέλο αυτό είναι **κλιμάκωση**(κλιμάκωση στους υπολογιστικούς πόρους σε υψηλές ταχύτητες), **"pay as you go"** (η δυνατότητα να πληρώνει ο χρήστης στον πάροχο τις υποδομές που χρησιμοποίησε μόνο) και **"best-of-breed"** (η χρήση των τελευταίων τεχνολογιών είναι επιλογή).



Εικόνα 1.2. Σχέση εξαρτώμενων μελών στα cloud συστήματα.

1.5 Μοντέλα ανάπτυξης και Αρχιτεκτονικής Cloud Computing Systems

Υπάρχουν τρεις μεγάλες κατηγορίες Cloud ανάλογα με την ανάπτυξης ενός συστήματος Cloud Computing. Αυτές είναι τα **Δημόσια (ή Εξωτερικά, Public Clouds)**, τα **Ιδιωτικά (ή Εσωτερικά, Private Clouds)**, **Κοινότητας (Community Clouds)** και τα **Υβριδικά (Hybrid Clouds)**.



Εικόνα 1.3. Μοντέλα Ανάπτυξης συστημάτων Cloud Computing

Πηγή https://imclone7.wordpress.com/2015/03/10/advantages-and-dis-advantages-on-cloud-computing/

1.5.1 Δημόσια Εξωτερικά Νέφη (Public Clouds)

Η δομή του Δημοσίου Νέφους είναι διαθέσιμη σε όλο το κοινό. Πρόκειται για τον πιο γνωστό τύπο υπολογιστικών νεφών. Η υποδομή και οι υπηρεσίες που προσφέρουν εξαρτώνται από τον πάροχο. Παρέχουν υπηρεσίες σε πληθώρα πελατών υπό μια κοινή υποδομή. Η διαχείριση της λειτουργίας της ασφάλειας γίνεται μέσω τρίτων πωλητών, που είναι υπεύθυνοι για τις υπηρεσίες (την προσφορά τους) στο νέφος.

Το συγκεκριμένο μοντέλο στηρίζεται σε παγκόσμια δίκτυα κέντρων πληροφοριών, προσφέροντας υπηρεσίες με πληρωμή ανά χρήση. Αυτό αποτελεί και ένα από τα

βασικά του πλεονεκτήματα- την πιο οικονομική επιλογή χρήσης εφαρμογών cloud. Σε πολλές περιπτώσεις, η παροχή των δημόσιων νεφών γίνεται και εντελώς δωρεάν. Υπάρχουν, σαφώς, και μειονεκτήματα στη χρήση του συγκεκριμένου μοντέλου. Το σημαντικότερο αυτών είναι η έλλειψη εμπιστοσύνης στη σχέση παρόχου και καταναλωτή, λόγω θεμάτων ασφάλειας που λαμβάνουν χώρα σε συστήματα νεφών.

1.5.2 Ιδιωτικά Εσωτερικά Νέφη (Private Clouds)

Η δομή του Ιδιωτικού Νέφους είναι διαθέσιμη σε έναν οργανισμό. Η εφαρμογή τους αφορά στα ιδιωτικά δίκτυα. Πρόκειται για το κέντρο δεδομένων που ανήκει σε συγκεκριμένο πάροχο υπηρεσιών, υπεύθυνο για την υποδομή και τη λειτουργία της πλατφόρμας του νέφους. Οι υπηρεσίες (virtualization και αυτοματοποίησης) αποτελούν οφέλη του συστήματος παρέχοντας ασφάλεια στα δεδομένα και εμπιστοσύνη(εν αντιθέσει με τα δημόσια, όπως αναφέρθηκε παραπάνω), δίνοντας την δυνατότητα στους πελάτες-οργανισμούς που θα τα χρησιμοποιήσουν να εφαρμόσουν πολιτικές ασφάλειας και προστασίας της ιδιωτικότητας των δεδομένων τους.

Οι πελάτες των ιδιωτικών νεφών θα πρέπει να αγοράσουν, να χτίσουν και να διαχειριστούν το σύστημα. Είναι αρμόδιοι της ορθής λειτουργίας του νέφους τους. Απαιτείται άτομο ή ομάδα ατόμων να ασχολείται με τη διαχείριση του νέφους και με την ανάπτυξή του καθώς και με τους μηχανισμούς πρόσβασης σε αυτό από τους χρήστες. Τέλος η απόλυτη συμμόρφωση των χρηστών στις πολιτικές και στους μηχανισμούς ασφάλειας που εφαρμόζονται.

Τα ιδιωτικά νέφη είναι πιο δαπανηρά από τα δημόσια, όσων αφορά τους πόρους αι το ανθρώπινο δυναμικό που απαιτείται για την συντήρησή τους. Είναι, όμως, προτιμότερα σε μεγάλες επιχειρήσεις και οργανισμούς, που θα χρησιμοποιήσουν έτσι και αλλιώς τους πόρους που ήδη έχουν.

1.5.3 Νέφη Κοινότητας (Community Clouds)

Η δομή του Νέφους Κοινότητας είναι διαθέσιμη για αρκετούς οργανισμούς και υποστηρίζει μια συγκεκριμένη κοινότητα με κοινές ανάγκες και απαιτήσεις. Στο συγκεκριμένο μοντέλο υπάρχει η δυνατότητα προσαρμογής ανάλογα με τις ανάγκες

και τη ζήτηση των χρηστών. Για παράδειγμα, επιχειρήσεις με κοινούς στόχους υπό συνεργασία, αποτελώντας μια κοινότητα, δομούν ένα κέντρο δεδομένων στο υπολογιστικό νέφος, το οποίο και διαμοιράζονται.

Βασικός στόχος αυτού του μοντέλου είναι η μείωση των ελλείψεων υποδομής του κάθε πελάτη και άμεση μείωση κόστους πόρων και διοίκησης. Είναι πιθανή η ύπαρξη πολλών κοινοτήτων στο ίδιο community cloud.

Βασική απαίτηση για την επιτυχία του μοντέλου είναι η ύπαρξη εμπιστοσύνης μεταξύ των μελών της κοινότητας.

Σε συνεργαζόμενες επιχειρήσεις και οργανισμού το community cloud είναι αρκετά διαδεδομένο, δεδομένου ότι το κόστος διαμοιράζεται συγκριτικά με το Private cloud.

1.5.4 Υβριδικά Νέφη (Hybrid Clouds)

Αποτελείται από ένα συνδυασμό όλων ή κάποιων από τα παραπάνω. Η εφαρμογή του μοντέλου είναι πιο οικονομική συγκριτικά με το ιδιωτικό νέφος. Μέρος των δεδομένων αποθηκεύονται στο δημόσιο και κάποια στο ιδιωτικό νέφος. Τα δεδομένα που χρήζουν προστασίας (απόρρητα και σημαντικά) αποθηκεύονται στο τμήμα που αφορά στο ιδιωτικό νέφος και τα δεδομένα που χρήζουν χαμηλότερης ασφάλειας στο δημόσιο.

Έτσι, παρέχεται μια πιο οικονομική λύση χρήσης μοντέλου ανάπτυξης υπολογιστικών νεφών, η οποία ταυτόχρονα παρέχει μεγάλο επίπεδο ασφάλειας δεδομένων, λόγω της εμπιστοσύνης στο ιδιωτικό νέφος.

1.6 Επιλογή Cloud Computing Systems

Υπάρχουν πολλοί λόγοι, πέραν των δελεαστικών χαρακτηριστικών των συστημάτων Cloud Computing, που θα παρότρυναν κάποιον απλό χρήστη του διαδικτύου έως και έναν ολόκληρο όμιλο εταιριών να τα προτιμήσουν έναντι των συμβατικών δικτύων.

Καταρχάς, πρέπει να αναφερθεί πως οι επιχειρήσεις και οι οργανισμοί στις μέρες μας, ανεξαρτήτως βεληνεκούς, έχουν στραφεί προς το Cloud Computing.

Τα βασικά πλεονεκτήματα έναντι των τεχνολογιών που χρησιμοποιούνται μέχρι και σήμερα είναι:

- Χαμηλές επενδύσεις σε πρωταρχικό στάδιο καθώς και επιλογή πληρωμής των εφαρμογών ανάλογα με τη χρήση των νεφών. Εν αντιθέσει, σε κάποια άλλη περίπτωση απαιτούνται υψηλές επενδύσεις για νέα κτήρια και υλικό.
- Λόγω της αρχιτεκτονικής του cloud προσφέρεται αξιοπιστία στον πελάτη, χωρίς περεταίρω έξοδα. Σε άλλες τεχνολογίες, το να γίνει η υποδομή αξιόπιστη συνεπάγεται υψηλό κόστος.
- Αρθρωτή αρχιτεκτονική περιβάλλοντος τεχνολογίας πληροφορικής, κλιμακούμενη πολυπλοκότητα ανάλογα τη χρήση. Σε άλλα συστήματα, η πολυπλοκότητα είναι υψηλή όσον αφορά το περιβάλλον τεχνολογίας πληροφορικής.
- Είναι τα μοναδικά συστήματα που δεν απαιτούν την ύπαρξη οποιασδήποτε υποδομής.

1.7 Σύνοψη κεφαλαίου

Σε αυτό το κεφάλαιο έγινε ανάλυση και επεξήγηση του Cloud Computing, του ορισμού, των χαρακτηριστικών και των υπηρεσιών που μπορεί να παρέχει. Συνοψίζοντας, λοιπόν, το cloud computing, εν αντιθέσει με άλλα μοντέλα συστημάτων, στηρίζεται στη λογική της χρήσης ενός πόρου από πολλούς χρήστες.

Η υιοθέτηση του Cloud Computing από επιχειρήσεις, επαγγελματικούς αλλά και κρατικούς φορείς γίνεται με ραγδαίους ρυθμούς τα τελευταία χρόνια. Τα χαρακτηριστικά του αποτελούν και τα πλεονεκτήματα του και σε επαγγελματικό και σε προσωπικό επίπεδο. Τα μοντέλα παροχής υπηρεσιών προσφέρουν την ευελιξία που χρειάζονται οι χρήστες ώστε να επιλέξουν την τεχνολογία και να την υιοθετήσουν σε πολλές πτυχές της καθημερινότητάς τους,

Το σημαντικότερο μειονέκτημα όμως της εφαρμογής του Cloud Computing είναι η έλλειψη ασφάλειας σε πολλά επίπεδα[13].

ΚΕΦΑΛΑΙΟ 2: ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΑΣΦΑΛΕΙΑ

2.1. Ιστορική Αναδρομή

Η πρώτη επιστημονική μελέτη για την ασφάλεια ενός συστήματος, έλαβε χώρα στις Ηνωμένες Πολιτείες Αμερικής από την ομάδα Εργασίας του Συμβουλίου Αμυντικής Επιστήμης του υπουργείου Άμυνας το 1970. Κατά τη δεκαετία αυτή, γινόταν χρήση τερματικών για την σύνδεση απομακρυσμένων υπολογιστών με βασική προϋπόθεση όμως την φυσική παρουσία χρήστη ή Administrator στον κεντρικό υπολογιστή του συστήματος. Η μελέτη στηρίχτηκε στο μοντέλο αυτό και στο δεδομένο του ότι μέχρι τότε, η ασφάλεια επιτυγχανόταν με φυσική απομόνωση , έλεγχο πρόσβασης και προστασία του κεντρικού υπολογιστή. Τα αποτελέσματα της εν λόγω μελέτης, έφεραν στην επιφάνεια ποικίλες και καινοτόμες ιδέες, οι οποίες και χρησιμοποιούνται σαν τεχνολογίες και στην εποχή μας, όπως η αρχή της ισορροπίας μεταξύ της ευχρηστίας ενός συστήματος και της προστασίας των πληροφοριών. Η έρευνα αποτέλεσε πυλώνα στις μετέπειτα μελέτες και έρευνες και αποτελεί παράδειγμα καινοτομιών μέχρι και σήμερα.

Το 1967, τέθηκε σε λειτουργία ο πρώτος υπολογιστής με λειτουργικά σύστημα Multics. Οι δύο του δημιουργοί ήταν ο Ken Thomson Dennis Ritchie, οι οποίοι εφάρμοσαν μέτρα ασφάλειας στο σχεδιασμό λειτουργικών, όπως κωδικοί πρόσβασης για χρήστες και άλλα πολλά, και συντέλεσαν σημαντικά στην ανάπτυξη του Unix, παρόλο που η πρώτη έκδοση του λειτουργικού δεν ακολουθούσε πολιτικές με κωδικούς, αλλά εφαρμόστηκε πια το 1973. Η μη τήρηση της σωστής πολιτικής χρήστης των κωδικών των χρηστών, αποτελεί μεγάλο πρόβλημα μέχρι και σήμερα και έχει αποτελέσει αντικείμενο έρευνας αλλά και επιθέσεων. Οι κωδικοί, ως μηχανισμός αυθεντικοποίησης, είναι η πιο ευρέως χρησιμοποιούμενη τακτική. Παρόλα αυτά, άλλοι μηχανισμοί αυθεντικοποίησης μπορούν να χρησιμοποιηθούν πια, όπως οι έξυπνες κάρτες, τα ψηφιακά πιστοποιητικά και άλλες τεχνολογίες.

Στο κεφάλαιο αυτό αναλύονται βασικοί όροι και έννοιες που αφορούν στην ασφάλεια δικτύων και πληροφοριακών συστημάτων. Πόσο σημαντικό είναι να παρέχεται

ασφάλεια σε συστήματα, σε ποιες κατηγορίες ανάγεται αυτή, διαφορές εννοιών αλλά και κίνδυνοι που καραδοκούν με απώτερο σκοπό την καταπάτησή της.

2.2. Τι είναι ασφάλεια

Η ασφάλεια πληροφοριακών συστημάτων εντάσσεται στην επιστήμη της πληροφορικής και είναι ο κλάδος που ασχολείται με την προστασία των υπολογιστών, των δικτύων που τους συνδέουν και των δεδομένων που μεταφέρονται ή διατηρούνται στα συστήματα αυτά. Στόχος είναι η αποφυγή μη εξουσιοδοτημένης πρόσβασης ή (και) χρήσης της πληροφορίας που συντελούν τα δεδομένα αυτά. Η ασφάλεια στηρίζεται σε βασικές ιδέες (αρχές). Η παραβίασή της έχει επιχειρηθεί πάμπολλες φορές και με ποικίλους τρόπους και αποτελεί αστείρευτο θέμα μελέτης.

2.3. Για την Ιστορία

Η ασφάλεια ενός συστήματος μελετήθηκε πρώτη φορά στις αρχές της δεκαετίας του ’70 από την ομάδα Εργασίας του Συμβουλίου Αμυντικής Επιστήμης του υπουργείου Άμυνας των ΗΠΑ, όπως μαρτυρά σχετική δημοσίευση εκείνης της περιόδου. Η μελέτη αυτή εξέταζε την χρήση υπολογιστών εξ αποστάσεως μέσω τερματικών εφόσον μέχρι εκείνη την περίοδο η πρόσβαση σε σύστημα έθετε ως βασική προϋπόθεση την φυσική παρουσία του χρήστη ή διαχειριστή του *κεντρικού υπολογιστή*. Η ασφάλεια, με τα δεδομένα έως τότε, διασφαλιζόταν με την φυσική απομόνωση, προστασία του κεντρικού υπολογιστή αλλά και τον έλεγχο πρόσβασης σε αυτόν. Η μελέτη αυτής της ομάδας απέφερε ως αποτέλεσμα πολλές καινοτόμες για την εποχή ιδέες, όπως για παράδειγμα η αναγνώριση από τους ερευνητές της αρχής της ισορροπίας μεταξύ της ευκολίας εργασίας του χρήστη και της προστασίας των πληροφοριών, όπου είχαν μεγάλη απήχηση και αποτελούν τα θεμέλια ερευνών σε θέματα ασφάλειας ακόμα και σήμερα.

Παρόλο που ο πρώτος υπολογιστής με το λειτουργικό σύστημα Multics εγκαταστάθηκε το 1967 με κωδικό πρόσβασης για χρήστες και με άλλα μέτρα ασφάλειας στο σχεδιασμό του, και δύο από τους δημιουργούς του, ο *Ken Thompson* και ο *Dennis Ritchie*, έπαιξαν κρίσιμο ρόλο στην ανάπτυξη του Unix, η πρώτη

έκδοση του Unix δεν διέθετε κωδικούς. Η λειτουργία αυτή προστέθηκε αργότερα, το 1973. Σήμερα η χρήση αδύναμων κωδικών πρόσβασης παραμένει μία από τις κυριότερες δυσκολίες που αντιμετωπίζει ο επαγγελματίας στον τομέα. Χρησιμοποιούνται και άλλες μέθοδοι αυθεντικοποίησης, για παράδειγμα οι έξυπνες κάρτες, αλλά μόνο σε συγκεκριμένους τομείς.

2.4. Βασικές Αρχές Ασφάλειας

Η ασφάλεια στηρίζεται στις τρεις βασικές αρχές που αναλύονται παρακάτω:

1) Ακεραιότητα

   Η ακεραιότητα είναι συνυφασμένη με την διατήρηση της πληροφορίας σε κάποια δεδομένη κατάσταση κατά την οποία δεν είναι θεμιτή η τροποποίηση, η διαγραφή και η προσθήκη αυτής από μη εξουσιοδοτημένες οντότητες. Επιπροσθέτως, πρέπει να αποτρέπεται η χρήση και η πρόσβαση σε υπολογιστές ή/και σε συστήματα από τέτοια άτομα.

2) Διαθεσιμότητα

Αφορά στην εξασφάλιση της διαθεσιμότητας των υπολογιστών, των δικτύων, των πόρων και των δεδομένων του συστήματος, όταν απαιτείται η χρήση τους από τους εξουσιοδοτημένους σε αυτά χρήστες.

3) Εμπιστευτικότητα

Δηλώνει πως τα δεδομένα του συστήματος και οι ευαίσθητες πληροφορίες των χρηστών παραμένουν μυστικά σε μη εξουσιοδοτημένους χρήστες.

Χρησιμοποιώντας, λοιπόν, τις τρεις βασικές αρχές της ασφάλειας, μπορούμε να την ορίσουμε ως «τον αριθμό των διαδικασιών, τεχνολογικές και διοικητικές, οι οποίες εφαρμόζονται σε συστήματα υπολογιστών με σκοπό να διασφαλιστεί η ακεραιότητα, η διαθεσιμότητα και η εμπιστευτικότητα της πληροφορίας και των δεδομένων που χειρίζεται το προστατευόμενο σύστημα.

2.5. Βασική ορολογία

Στην ανάλυση της ασφάλειας ενός συστήματος χρησιμοποιείται συγκεκριμένη ορολογία ώστε να υπάρχει καθολική κατανόηση των προβλημάτων και των συστατικών του συστήματος που τίθεται προς προστασία. Οι πιο συχνοί όροι ενός προστατευόμενου συστήματος είναι:

- Το αγαθό (asset) : πρόκειται για τον πόρο που χρήζει ασφάλειας
- Ιδιοκτήτης ή χρήστης (user/ owner) : το φυσικό ή το νομικό πρόσωπο το οποίο διαθέτει ή χρησιμοποιεί νομίμως το αγαθό
- Ιδιότητα (attribute) : το συγκεκριμένο χαρακτηριστικό του αγαθού που πρέπει να προστατευθεί
- Ζημιά (harm) : οι περιορισμοί της αξίας ενός αγαθού, όπως ορίζονται κατά τον ορισμό του αγαθού
- Κίνδυνος (danger) : Το ενδεχόμενο ύπαρξης της ζημιάς
- Στόχος της Ασφάλειας (Infosec goal) : πρόκειται για τον αντικειμενικό σκοπό του ιδιοκτήτη ή χρήστη του προστατευόμενου συστήματος και καθορίζει ποια είναι η επιθυμητή ισορροπία των όρων Κόστος και Ζημιά που πιθανόν να υποστεί το αγαθό σε περίπτωση Κινδύνου.
- Μέσο προστασίας (safeguard) : το σύνολο των ενεργειών που μπορεί να πράξει ο χρήστης ή ιδιοκτήτης του Αγαθού, με σκοπό να περιοριστεί ο Κίνδυνος να υποστεί αυτό Ζημιά.
- Κόστος (cost): επιβάρυνση, οικονομικής φύσεως ή γενικά, που πιθανόν να προκύψει από τη χρήση ενός μέσου προστασίας
- Εξασφάλιση (assurance): η βεβαιότητα ότι οι στόχοι της ασφάλειας έχουν επιτευχθεί με την χρήση των μέσων προστασίας που υιοθετήθηκαν.
- Απειλή (threat): Η οντότητα που μπορεί να προκαλέσει Ζημιά ή παραβίαση σε τμήμα ή και στο σύνολο του συστήματος ή του δικτύου

- Επίθεση (attack): η υλοποίηση μιας Απειλής από εισβολέα, εκμεταλλευόμενος κάποια αδυναμία
- Αντίμετρα (countermeasures) : μηχανισμοί και διαδικασίες που διατίθενται για την εξαφάνιση ή περιορισμό των επιπτώσεων μιας Απειλής

2.6. Συχνές Επιθέσεις

Για να λαμβάνει χώρα η υγιής λειτουργία ενός συστήματος θα πρέπει να υπάρχει ένα σημαντικό επίπεδο ασφάλειας αυτού, δεδομένου του ότι υπάρχουν πολλών τύπων επιθέσεις που δύναται να το πλήξουν. Οι επιθέσεις, ανάλογα με τον στόχο τους, μπορούν να προκαλέσουν προβλήματα σε διάφορα τμήματα του συστήματος. Οι κακόβουλοι (ή εισβολείς) είναι οι χρήστες (εξουσιοδοτημένοι και μη) που επιχειρούν την επίθεση στο σύστημα. Μερικές από τις πιο συχνές επιθέσεις είναι:

- Εισαγωγή, μετατροπή ή ακόμα και καταστροφή δεδομένων και λογισμικού από μη εξουσιοδοτημένους χρήστες
- Αλλοίωση ή μείωση της αξιοπιστίας των δεδομένων του συστήματος (λόγω πιθανής παρέμβασης χωρίς εξουσιοδότηση)
- Παρεμπόδιση της ομαλής λειτουργίας του συστήματος στην ολότητά του με ποικίλους τρόπους
- Εισβολή και αφαίρεση πληροφορίας και δεδομένων από το σύστημα χωρίς εξουσιοδότηση
- Παραβίαση πνευματικών δικαιωμάτων

2.6.1. Τύποι επιθέσεων

Η πραγματοποίηση οποιασδήποτε επίθεσης πλέον είναι πολύ εύκολο να συμβεί. Στο διαδίκτυο υπάρχουν ελεύθερα tutorials που υποδεικνύουν τους τρόπους. Οι βασικότεροι τύποι επιθέσεων σε ένα σύστημα ή δίκτυο είναι:

1. Μη εξουσιοδοτημένη χρήση (masquerade) : ο επιτιθέμενος επιχειρεί πρόσβαση σε πόρους προστατευμένου συστήματος για τους οποίους δεν έχει λάβει σχετική άδεια. _

2. Μη ενεργός (παθητική) παρακολούθηση (passive tapping): παρακολούθηση των δεδομένων που ανταλλάσσουν οι χρήστες του συστήματος
3. Ενεργός παρακολούθηση (active tapping) : παρακολούθηση και τροποποίηση των δεδομένων που ανταλλάσσουν ι χρήστες του συστήματος
4. Αποποίηση (repudiation) : Αποποίηση συμμετοχής ενός πόρου ή οντότητας ενός συστήματος (πχ ένας server) στην επικοινωνία
5. Άρνηση παροχής υπηρεσιών (denial of service) : παρεμπόδιση της απόδοσης του συστήματος και των υπηρεσιών που παρέχει (και ως συνέπεια και της ομαλής λειτουργίας του)
6. Επανεκπομπή μηνυμάτων (replay) : Καταγραφή έγκυρων μηνυμάτων έτσι ώστε να μπορούν να σταλούν επαναλαμβανόμενα ώστε να αποκτήσει ο εισβολέας πρόσβαση
7. Ανάλυση επικοινωνίας (traffic analysis) : με σκοπό την έμμεση εξαγωγή συμπερασμάτων για τον στόχο του συστήματος, υποκλέπτεται πληροφορία που αφορά στην διακίνηση δεδομένων μεταξύ των οντοτήτων
8. Κακόβουλο λογισμικό (malware) : λογισμικό που εγκαθίσταται στους πόρους του συστήματος και παρεμποδίζει τη σωστή του λειτουργία (viruses, worms, Trojans, horses)

2.6.2. Τεχνικές επιθέσεων και κίνδυνοι

Οι τεχνικές επιθέσεων είναι το αλφάβητο του επιτιθέμενου. Ανάλογα στο τι αποσκοπεί, χρησιμοποιεί άλλη τεχνική, ώστε να εξασφαλίσει την μεγαλύτερη πιθανότητα επιτυχίας της επίθεσης. Οι βασικότεροι κίνδυνοι βάσει τεχνικών επιθέσεων είναι:

- Επίθεση από ωτακουστές (eavesdropping): τα δεδομένα που μεταδίδονται εντός του συστήματος παρακολουθούνται από

τον εισβολέα «ωτακουστή», ο οποίος στοχεύει στην ανίχνευση των δύο άκρων μιας επικοινωνίας

- Επίθεση αντίστροφης πορείας (trace back attack) : γνωρίζοντας τον παραλήπτη, ο επιτιθέμενος, ιχνηλατεί το μονοπάτι της επικοινωνίας και εντοπίζει τον αποστολέα (ή το αντίστροφο-γνωρίζοντας τον αποστολέα εντοπίζεται ο παραλήπτης)
- Επίθεση κωδικοποίησης Μηνυμάτων (message coding attack): ο επιτιθέμενος ιχνηλατεί μηνύματα στην περίπτωση, πάντα, που η κωδικοποίησή τους δεν έχει υποστεί κάποια τροποποίηση κατά την μετάδοση
- Επίθεση Χρονοσήμανσης (Timing attack): γίνεται μετάδοση των πακέτων και ο εντοπισμός του αποστολέα με κριτήριο τους συσχετιζόμενους χρόνους εκπομπής
- Επίθεση από εχθρικούς συνεργάτες (malicious collaborators): αυτοί είναι οι εξουσιοδοτημένοι χρήστες του συστήματος που στοχεύουν στον περαιτέρω έλεγχο της μεταφοράς της πληροφορίας που γίνεται στο δίκτυο ή στην διαστρέβλωσή της

2.7. Μηχανισμοί Ασφάλειας

Η ανάπτυξη πολλών τεχνολογιών τα τελευταία χρόνια και κυρίως η καθολική τους αποδοχή από εταιρίες και ιδιώτες, συντέλεσαν στο αυξανόμενο μένος των κακόβουλων να ανακαλύψουν καινούργιους τρόπους επιθέσεων αλλά και των επιστημόνων στην ανακάλυψη νέων μηχανισμών προστασίας αλλά και ενίσχυση των ήδη επιτυχώς δοκιμασμένων. Η διατήρηση μηχανισμών ασφάλειας, βέβαια, δεν αποτελεί πανάκεια, παρόλα αυτά υπάρχουν καθορισμένοι μηχανισμοί που εφαρμόζονται κατά κόρον στα συστήματα και στα δίκτυα. Τέτοιοι είναι:

- Η Κρυπτογραφία: αποτελεί μεγάλο αντικείμενο μελέτης και ξέχωρο κομμάτι της επιστήμης της Πληροφορικής. Προσφέρει εμπιστευτικότητα των δεδομένων , με άλλα λόγια ότι τα

δεδομένα δεν θα είναι αναγνώσιμα σε μη εξουσιοδοτημένες οντότητες

- Μηχανισμοί Ελέγχου πρόσβασης: παρέχουν αυθεντικοποίηση των χρηστών του συστήματος. Εξασφαλίζεται η εγκυρότητα των μηνυμάτων λόγω της ταυτότητας της οντότητας. Αν δεν εγκρίνει ο μηχανισμός την οντότητα ως εξουσιοδοτημένη, δεν επιτρέπεται η προσπέλαση τους στους πόρους του συστήματος.
- Ψηφιακές Υπογραφές: μηχανισμός αυθεντικοποίησης επίσης. Γίνεται ταυτοποίηση των συμμετεχόντων στην επικοινωνία. Έχουν το ίδιο νόημα με τις πραγματικές μας ταυτότητες, αλλά με ψηφιακό τρόπο
- Μηχανισμοί Ανταλλαγής Αυθεντικοποίησης: αμοιβαία επιβεβαίωση της ταυτότητας των οντοτήτων που επικοινωνούν.
- Μηχανισμοί Ακεραιότητας Δεδομένων: εξασφαλίζουν ότι τα δεδομένα που διακινούνται στο σύστημα δεν είναι αλλοιωμένα. Μηχανισμός ακεραιότητας.
- Μηχανισμοί Επιπρόσθετης Κίνησης: εξυπηρετούν την αποφυγή επιθέσεων τύπου Ανάλυσης Επικοινωνίας. Χωρίζονται σε ισχυρούς και ασθενείς, ανάλογα με τη χρήση ή μη αντίστοιχα, της Κρυπτογραφίας.

2.8. Συνοπτικά

Συνοψίζοντας, η ασφάλεια είναι ένα πολύ σημαντικό κομμάτι στην δημιουργία και τη σωστή πορεία ενός συστήματος αλλά και σαν Κλάδος επιστήμης επίσης. Καθημερινά προκύπτουν καινούριες επιθέσεις και καινούργια μέτρα προστασίας. Στο Cloud Computing, παίζει καθοριστικό ρόλο καθώς αποτελεί ένα από τα «αγκάθια» του. Πρέπει να κατανοεί κανείς πως ποτέ δεν έχεις την τέλεια ασφάλεια. Πάντα υπάρχουν πόρτες που είναι πρόκληση για έναν κακόβουλο χρήστη.

Στο κεφάλαιο, έγινε μια μικρή ανάλυση βασικών χαρακτηριστικών και όρων που αφορούν στην ασφάλεια, ώστε να γίνονται απόλυτα κατανοητοί στην πορεία της εργασίας[1].

ΚΕΦΑΛΑΙΟ 3: ΑΣΦΑΛΕΙΑ ΚΑΙ CLOUD

3.1. Γενικά

Είναι γεγονός ότι το μεγαλύτερο μέρος των επιχειρήσεων χρησιμοποιούν το Cloud Computing προκειμένου να αποκτήσουν χώρο για την αποθήκευση πληροφορίας και το πραγματοποιούν πρωτίστως μέσω της μεθόδου χρονικής μίσθωσης με στόχο να μειώσουν το οικονομικό τους κόστος. Ένα σημαντικό όμως θέμα με το οποίο οφείλουν οι επιχειρήσεις να ασχοληθούν είναι το υψίστης σημασίας για αυτές ζήτημα της ασφάλειας της οικονομικά ευμενέστερης προαναφερθείσας μεθόδου αποθήκευσης.

Σε ό, τι αφορά τη χρήση του Cloud Computing θα πρέπει να σημειωθεί ότι η ασφάλεια είναι η πιο συχνή αμφιβολία. Παρόλα αυτά δεν είναι αρκετά τεκμηριωμένη, καθώς οι πάροχοι εγγυώνται ότι πραγματοποιούν τις απαραίτητες αναλύσεις για την ασφάλεια των υποδομών. Υποστηρίζουν επιπρόσθετα την ύπαρξη ευρέως δοκιμασμένων τεχνικών λύσεων που μπορούν να χρησιμοποιηθούν. Κάποια τέτοια ενδεικτικά παραδείγματα είναι η ασφάλεια των καναλιών επικοινωνίας, η κρυπτογράφηση των αποθηκευμένων δεδομένων αποτελούν όπου γνωστές τεχνικές μπορεί να χρησιμοποιηθούν σε αυτούς τους τομείς. Επιπλέον, έρευνες που έχουν πραγματοποιηθεί σχετικά με παραβιάσεις της ασφάλειας δείχνουν ότι σημαντικός αριθμός των παραβάσεων συμβαίνουν στο εσωτερικό του οργανισμού. Αυτό σημαίνει ότι το υπολογιστικό νέφος θα μπορούσε να κάνει την πληροφοριακή υποδομή της επιχείρησης πιο ασφαλή αν δεχτούμε αυτή την πλευρά.

What are your main concerns in your approach to Cloud Computing?

Answer Options	Answer Options	Not Important	Medium Importance	Very Important	Showstopper	Rating Average	Response Count
Privacy		0	7	28	31	3,36	66
Availability of services and/or data		3	9	28	26	3,17	66
Integrity of services and/or data		0	9	28	27	3,28	64
Confidentiality of corporate data		1	3	17	43	3,59	64
Repudiation		1	24	25	7	2,67	57
Loss of control of services and/or data		2	14	29	17	2,98	62
Lack of liability of providers in case of security incidents		1	15	25	19	3,03	60
Inconsistency between trans national laws and regulations		8	25	15	12	2,52	60
Unclear scheme in the pay per use approach		10	26	14	9	2,37	59
Uncontrolled variable cost		4	21	26	7	2,62	58
Cost and difficulty of migration to the cloud (legacy software etc...)		7	31	14	6	2,33	58
Intra-clouds (vendor lock-in) migration		5	21	20	10	2,63	56
Other (please specify)							3

Σχήμα 3.1: Αποτελέσματα μελέτης σχετικά με τα κυριότερα προβλήματα στην υιοθέτηση του Cloud Computing.

Πηγή

https://www.google.gr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCQQFjABahUKEwicnp_BoPTHAhXGiywKHbk9CgQ&url=https%3A%2F%2Fwww.enisa.europa.eu%2Fact%2Frm%2Ffiles%2Fdeliverables%2Fcloud-computing-sme survey%2Fat_download%2FfullReport&usg=AFQjCNHtFZH-slik

Στην πραγματικότητα είναι γεγονός πως στο διαδίκτυο υπάρχουν ήδη πολλές αποδείξεις για τη λήψη μέτρων από τους πιο φημισμένους παρόχους υπηρεσιών Cloud (π.χ. google datacenter, Amazon datacenter, salesforce κ.α.) όσο αφορά την φυσική και περιβαλλοντική ασφάλεια.. Λαμβάνοντας υπόψη τις έρευνες που έχουν γίνει αλλά και από άλλες δηλώσεις των εταιριών, φαίνονται οι προθέσεις τουλάχιστον των εν λόγω οργανισμών για την θωράκιση των υποδομών ενάντια σε φυσικές και περιβαλλοντικές απειλές. Παρόλα αυτά, όλα τα παραπάνω δεν αρκούν για να διαβεβαιώσουν τους υποψήφιους πελάτες σχετικά με την εξασφάλιση των δεδομένων τους απέναντι σε διάφορες απειλές που πιθανόν να δεχτεί το εν λόγω σύστημα.

Σε ό, τι αφορά τα μέτρα ασφαλείας και τις δεσμεύσεις που λαμβάνονται από τους παρόχους υπηρεσιών Cloud, αυτές μπορούν να αναζητηθούν μόνο μέσα στις αντίστοιχες συμβάσεις η ανασκόπηση των οποίων μπορεί να μας οδηγήσει στην εξαγωγή ορισμένων συμπερασμάτων. Αρχικά, ανεξάρτητα από το αν η υπηρεσία δίνεται επί πληρωμή ή δωρεάν ζητείται η δέσμευση του πελάτη σε συγκεκριμένους όρους χωρίς αυτό να εξαρτάται επιπλέον από το πιο μοντέλο υπηρεσίας Cloud παρέχεται (SaaS, PaaS, IaaS).

- Πάροχος και τον πελάτης δεσμεύονται από τους όρους των συμβάσεων αυτών (agreements) σε διαφορετικό βαθμό τον.

- Υπάρχουν όροι που σχετίζονται με την έννοια της ασφάλειας (εμπιστευτικότητα, ακεραιότητα και σε κάποιες περιπτώσεις διαθεσιμότητα).

- Δεν αναγράφεται σε καμία από τις συμφωνίες αυτές τι μέτρα λαμβάνονται αλλά ότι ο πάροχος δεσμεύεται να λάβει μέτρα. Οι όροι ασφάλειας δηλαδή είναι περιγραφικοί και όχι συγκεκριμένοι.

- Γίνεται επίσης χρήση του όρου reasonable και σχετίζεται με την έκταση των μέτρων. Συνεπώς, δεν καθορίζεται κάποιο ελάχιστο κοινά αποδεκτό επίπεδο ασφαλείας.

Συνεπώς δεν είναι ανυπόστατες οι ανησυχίες των υποψηφίων πελατών σχετικά με το επίπεδο ασφαλείας των υπηρεσιών Cloud και θα πρέπει να λαμβάνονται σοβαρά υπόψη όλα τα μέτρα προστασίας που μπορούν να εφαρμοστούν προκειμένου να διασφαλιστεί.

Η δομή του συστήματος στο Cloud Computing και η κατανόηση του αποτελεί το βασικότερο βήμα για την κατανόηση του ζητήματος της ασφάλειας. Είναι γεγονός πως η έλλειψη ελέγχου πάνω στη δομή του Cloud Computing από την πλευρά του χρήστη ή των επιχειρήσεων, καθώς υπάρχει άγνοια για το που αποθηκεύονται τα δεδομένα τους και για τι είδους μηχανισμοί λαμβάνουν χώρα για να τα

προστατέψουν, έχει ως αποτέλεσμα την πληθώρα των ζητημάτων που αφορούν την ασφάλεια στο νέφος.

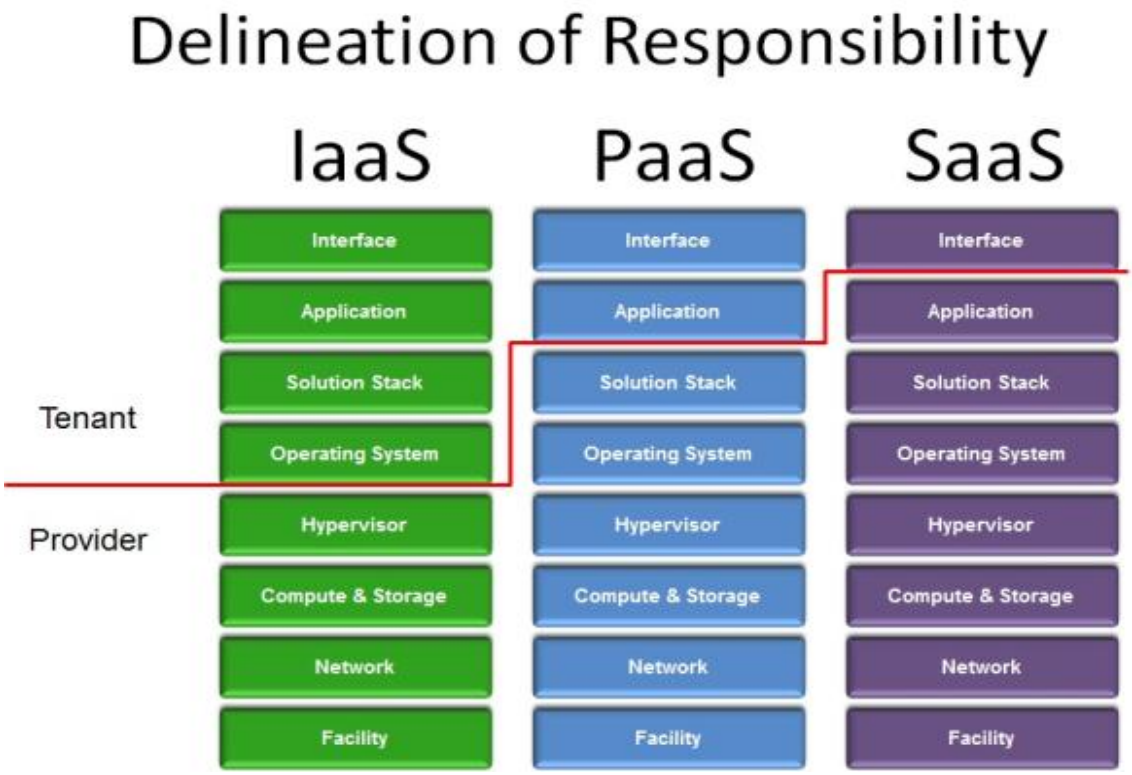
Από τα σημαντικότερα ζητήματα ασφάλειας αποτελούν τα προβλήματα των υπηρεσιών δικτύου και των προγραμμάτων περιήγησης αφού το Cloud Computing και οι χρήστες του χρησιμοποιούν εκτενέστατα τα προαναφερθέντα, προκειμένου να έχουν πρόσβαση στις υπηρεσίες δικτύου αφορούν το XML πλαίσιο της υπογραφής, όπου η XML υπογραφή χρησιμοποιείται για πιστοποίηση.

Συγκεκριμένα σε ό, τι αφορά την ασφάλεια των προγραμμάτων περιήγησης θα πρέπει να αναφέρουμε ότι οι υπολογισμοί στο Cloud Computing γίνονται σε απομακρυσμένους servers και ότι ο περιφερειακός υπολογιστής (client) χρησιμοποιείται μόνο για να κάνει τις μεταβιβάσεις των πληροφοριών (I/O) και να πιστοποιεί τις εντολές στο Νέφος. Επομένως τα τυπικά προγράμματα περιήγησης είχαν την ανάγκη να στείλουν I/O. Έτσι χρησιμοποιήθηκαν διαδικτυακές πλατφόρμες με διάφορα ονόματα όπως: εφαρμογές δικτύου, «web 2.0» ή SaaS. Παρόλο που η αμφιβολία της ασφάλειας από τη χρήση των προγραμμάτων περιήγησης εξακολούθησε να υπάρχει.

Προκειμένου να πιστοποιήσουμε και να κρυπτογραφήσουμε δεδομένα χρησιμοποιείται ευρύτατα το TLS (Transport Layer Security – Ασφάλεια Μεταφοράς σε Επίπεδα) μιας και η κωδικοποίηση μπορεί να επιτευχθεί μόνο μέσω του TLS και οι υπογραφές μπορούν να χρησιμοποιηθούν μόνο μέσω της «χειραψίας» TLS. Δηλαδή η υπογραφή XML ή κωδικοποίηση XML δε μπορούν να χρησιμοποιηθούν απευθείας από το πρόγραμμα περιήγησης.

Αξίζει να σημειωθεί πως οι έλεγχοι ασφαλείας στο Cloud Computing είναι όμοιοι με αυτούς σε ένα περιβάλλον πληροφοριακού συστήματος. Επειδή όμως το Υπολογιστικό Νέφος χρησιμοποιεί διαφορετικά μοντέλα υπηρεσίας, λειτουργικά μοντέλα και τεχνολογίες δημιουργεί και διαφορετικό κίνδυνο για έναν οργανισμό. Είναι επομένως υψίστης σημασίας η επίτευξη της κατανόησης των σχέσεων και της εξάρτησης μεταξύ των μοντέλων Νέφους. Επίσης, όπως φαίνεται στο παρακάτω

σχήμα ανάλογα με το μοντέλο (SaaS, IaaS, PaaS) που θα χρησιμοποιηθεί από τον πελάτη, έχει ο ίδιος αλλά και ο πάροχος των Cloud υπηρεσιών διαφορετικό «μερίδιο» ευθύνης ή καλύτερα είναι διαφορετικοί οι τομείς στους οποίους υπεισέρχεται κανείς προκειμένου να διασφαλίσει την ασφάλεια των δεδομένων-πληροφοριών.



Σχήμα 3.2: Σχεδιαγραμματική απεικόνιση ευθύνης για τα μοντέλα SaaS, IaaSS, PaaS
Πηγή http://blog.cloudpassage.com/2011/06/06/whos-responsible-for-security-in-a-cloud/

3.2. Τομέας Διακυβέρνησης και Επιχειρησιακός Τομέας

Ο επιχειρησιακός τομέας και ο τομέας Διακυβέρνησης αποτελούν επίσης δύο σημαντικούς τομείς οι οποίοι πρέπει να συμπεριληφθούν στους παράγοντες που έχουν να κάνουν με την ασφάλεια του Cloud Computing.

Ο τομέας Διακυβέρνησης ο οποίος είναι ευρύς και αντιμετωπίζει στρατηγικά ζητήματα εντός του περιβάλλοντος Νέφους περιλαμβάνει:

- Διακυβέρνηση και διαχείριση επιχειρηματικού ρίσκου

Είναι γεγονός ότι η χρήση του Υπολογιστικού Νέφους προκαλεί επιχειρηματικό ρίσκο. Η ικανότητα της επιχείρησης να διοικείται και να μετρά το συγκεκριμένο ρίσκο αποτελεί κύρια ασχολία της διακυβέρνησης και διαχείρισης επιχειρηματικού ρίσκου. Επίσης, τα κυριότερα ζητήματα που αντιμετωπίζονται είναι η ευθύνη της προστασίας ευαίσθητών δεδομένων, η ικανότητα των χρηστών να εκτιμήσουν επαρκώς το ρίσκο του παρόχου υπηρεσιών καθώς και η εκτίμηση νομικών προτεραιοτήτων για παραβιάσεις της συμφωνίας.

- Νομική και ηλεκτρονική κάλυψη

Τα νομικά ζητήματα που δημιουργούνται με τη μετάβαση μιας επιχείρησης στη χρήση υπηρεσιών Cloud και τα οποία πρέπει να αντιμετωπιστούν αφορούν το συγκεκριμένα τομέα. Τέτοια νομικά ζητήματα είναι οι απαιτήσεις απορρήτου, οι παραβιάσεις ασφαλείας, οι κανονιστικές απαιτήσεις, η τήρηση της εθνικής και διεθνούς νομοθεσίας κ.α.

- Συμβατότητα και λογιστικός έλεγχος

Προκειμένου να μεταβεί επιτυχώς μια επιχείρηση σε υπηρεσίες Cloud, απαραίτητη προϋπόθεση αποτελεί η διατήρηση και παροχή συμβατότητας.

- Διαχείριση κύκλου ζωής των πληροφοριών

Τα δεδομένα που παραμένουν στο Cloud διαχειρίζονται από το συγκεκριμένο τομέα. Πιο εξειδικευμένα ασχολείται με τους ελέγχους αποζημίωσης, την ευθύνη για το απόρρητο των πληροφοριών καθώς επίσης για τη διαθεσιμότητα και την ακεραιότητά τους.

- Φορητότητα και διαλειτουργικότητα

Ο τομέας αυτός ασχολείται με τη μεταφορά δεδομένων μεταξύ παρόχων αλλά και με την επιστροφή τους στις επιχειρήσεις. Γεγονός αποτελούν οι ανοιχτές δομές στις οποίες βασίζονται οι περισσότεροι πάροχοι υπηρεσιών Νέφους και οι οποίες επιτρέπουν τις προαναφερθείσες μεταφορές δεδομένων.

Ο επιχειρησιακός τομέας ο οποίος ασχολείται με πιο βραχυπρόθεσμα ζητήματα ασφαλείας και ζητήματα εφαρμογής των ποικιλιών αρχιτεκτονικής περιλαμβάνει:

- Παραδοσιακή ασφάλεια, επιχειρησιακή συνοχή και ανάκτηση πληροφοριών

Αφορά τον τρόπο με τον οποίο το Cloud Computing επηρεάζει τις λειτουργικές διαδικασίες που χρησιμοποιούνται ήδη στην εφαρμογή της ασφάλειας. Επιπλέον, καθώς μια επιχείρηση προσδοκά καλύτερη διαχείριση ρίσκου ο τομέας αυτός εστιάζει και στα ρίσκα που λαμβάνονται από τις υπηρεσίες Cloud ως συνάρτηση αυτής της προσδοκίας.

- Λειτουργίες του κέντρου πληροφοριών

Αξιολογεί το κέντρο πληροφοριών του παρόχου υπηρεσιών Νέφους καθώς και την αρχιτεκτονική του ως παράγοντες με σκοπό τη μακροχρόνια αποδοτικότητα και σταθερότητα του.

- Αντιμετώπιση περιστατικών, ειδοποίησης και αποκατάσταση

Αφορά στην εξασφάλιση της σωστής αντιμετώπισης ενός απρόβλεπτου περιστατικού εστιάζοντας στις εφαρμογές που πρέπει να εγκατασταθούν τόσο στον πάροχο όσο και στο χρήστη.

- Ασφάλεια εφαρμογών

Ο τομέας αυτός ασχολείται με το αν μια επιχείρηση θα μεταβεί σε Cloud υπηρεσίες και υιοθετώντας ποιο από τα SaaS, PaaS, IaaS μοντέλο. Έτσι πρέπει να εστιάσει στην ασφάλιση του λογισμικού εφαρμογών που τρέχουν ή αναπτύσσονται εντός του Cloud περιβάλλοντος.

- Κωδικοποίηση και διαχείριση κλειδιών

Ασχολείται με τη σωστή χρήση κωδικοποίησης καθώς επίσης και με την επεκτασιμότητα στη διαχείριση κλειδιών στα πλαίσια λειτουργίας της επιχείρησης. Αποφασίζει επιπροσθέτως αν είναι αναγκαία η χρήση κωδικοποίησης και διαχείρισης κλειδιών προκειμένου να προστατευθούν τα δεδομένα και να υπάρχει διασφάλιση στην πρόσβαση στους πόρους.

- Διαχείριση ταυτότητας και πρόσβασης

Διαχειρίζεται τις ταυτότητες και τις υπηρεσίες καταλόγου με σκοπό τον έλεγχο πρόσβασης καθώς επίσης εκτιμά την επιχείρηση ως προς την ετοιμότητά της στο να διαχειριστεί την πρόσβαση βάσει των ταυτοτήτων και τις αρχές του Cloud.

- Δημιουργία εικονικών πόρων

Αφορά τη χρήση εικονικών πόρων στο Cloud Computing και τα ζητήματα που συσχετίζονται με τη δημιουργία εικονικού software ή hardware. Ασχολείται επίσης με τους κινδύνους που έχουν να κάνουν με την πολλαπλή μίσθωση, με την απομόνωση των εικονικών μηχανημάτων, με τη συστέγαση των τελευταίων, με τα τρωτά σημεία του κεντρικού ελέγχου των εικονικών μηχανημάτων κλπ[12].

3.3. Οφέλη ασφαλείας από το Cloud Computing

Ο Ευρωπαϊκός Οργανισμός Δικτύου και Ασφάλειας Πληροφοριών (ENISA – European Network and Information Security Agency έχοντας ερευνήσει το όφελος των επιχειρήσεων που χρησιμοποιούν το Cloud Computing, προτείνει τρόπους ώστε να βελτιωθεί ο παράγοντας της ασφάλειας της επιχείρησης. Παρακάτω θα αναφερθούν πρωτίστως τα σημαντικότερα οφέλη από την προαναφερθείσα χρήση:

- <u>Οφέλη οικονομικής κλίμακας</u>

Υιοθετώντας μέτρα ασφαλείας τα οποία εφαρμόζονται σε μεγάλη κλίμακα είναι βέβαιο ότι πετυχαίνουμε οικονομία. Επομένως κάνοντας χρήση του Cloud Computing οι επιχειρήσεις προστατεύονται καλύτερα διοχετεύοντας το ίδιο ποσό χρημάτων. Η ισχυρή πιστοποίηση, η αποτελεσματική πρόσβαση βάσει του ρόλου του καθενός στην επιχείρηση, τα φίλτρα των διακινούμενων πληροφοριών, η πρόσβαση και οι προεπιλεγμένες, κεντρικά υποβοηθούμενες λύσεις διαχείρισης ταυτότητας αναγνώρισης είναι κάποια από τα μέτρα άμυνας που περιλαμβάνει ο όρος προστασία και τα οποία συντελούν στη βελτίωση των επιδράσεων των συνεργατών. Τα πλεονεκτήματα από μια τέτοια βελτίωση μπορούν να συμπτυχθούν στα παρακάτω:

- Πολλαπλές τοποθεσίες. Η διατήρηση οικονομικών πόρων από τους παρόχους υπηρεσιών Cloud προκειμένου να αναπαράγουν το περιεχόμενο ενισχύει την ανεξαρτησία αλλά και την αποφυγή μιας αναπάντεχης αποτυχίας.

- Δίκτυα Αιχμής. Το γεγονός ότι το Cloud Computing παρέχει στις επιχειρήσεις δυνατότητες αποθήκευσης, επεξεργασίας και παράδοσης πληροφοριών τελευταίας τεχνολογίας το καθιστά ιδιαίτερα αξιόπιστο και παρέχει βελτιωμένη ποιότητα και λιγότερα προβλήματα δικτύου.

- Ταχύτερη ανταπόκριση σε οποιαδήποτε μορφής περιστατικό. Οι πάροχοι Cloud υπηρεσιών ανταποκρίνονται ταχύτερα και πιο αποτελεσματικά λόγω γρήγορης αναγνώρισης μιας εφαρμογής κακόβουλου λογισμικού χάρις στα συστήματα που χρησιμοποιούν.

- Διαχείριση απειλών. Οι πάροχοι υπηρεσιών Cloud είναι σε θέση να διαθέσουν πόρους καθώς και να αναπτύξουν στρατηγικές διαχείρισης αυτών δίνοντας έτσι τη δυνατότητα σε μικρές επιχείρησης που δεν έχουν την ίδια δυνατότητα να αντιμετωπίσουν συγκεκριμένα ζητήματα ασφαλείας.

- <u>Η ασφάλεια μέσω διαφοροποίησης της αγοράς</u>

Για τις περισσότερες επιχειρήσεις η ασφάλεια είναι το πιο σημαντικό ζήτημα που λαμβάνεται υπόψη κατά τη μετάβαση των λειτουργιών τους σε Νέφος. Οι επιλογές τους γίνονται βάση της εμπιστευτικότητας, τα γενικά οφέλη από το Cloud Computing, τα ρίσκα και τις συστάσεις για την ακεραιότητα και την αυθεντικότητα ασφάλειας των πληροφοριών, όπως επίσης και την ασφάλεια των υπηρεσιών που προσφέρει ο πάροχος. Αυτό οδηγεί τους παρόχους των υπηρεσιών Νέφους να βελτιώσουν την ασφάλεια που προσφέρουν μέσα από τον ανταγωνισμό της αγοράς.

- <u>Τυποποιημένα περιβάλλοντα διαχείρισης υπηρεσιών ασφαλείας</u>

Για τη διαχείριση των υπηρεσιών ασφαλείας προσφέρονται από τους μεγάλους παρόχους cloud υπηρεσιών ανοιχτά τυποποιημένα περιβάλλοντα με στόχο οι χρήστες να μπορούν να επιλέξουν έναν πάροχο αλλά και να τον αλλάξουν πιο εύκολα και πολύ πιο οικονομικά. Έχουν τη δυνατότητα επομένως να έχουν στη διάθεση τους πόρους που προσφέρονται από έναν πάροχο και τον πόρο παροχής ασφάλειας να τον αντλούν από άλλο πάροχο επιλέγοντας ανά πάσα στιγμή από μια ανοιχτή αγορά. Συνεπώς οι χρήστες δύνανται να αυξήσουν τον τελευταίο πόρο όπως επιθυμούν χωρίς να επηρεάζονται οι υπόλοιποι πόροι του συστήματος του και πάντα ανάλογα με την εκάστοτε ζήτηση.

- Γρήγορη επέκταση των πόρων

Όλοι οι πόροι που οι υπηρεσίες Νέφους υποστηρίζουν δύνανται να επεκταθούν γρήγορα και ευέλικτα ακολουθώντας τη ζήτηση. Τέτοιοι πόροι είναι η αποθήκευση, η διάρκεια χρήσης επεξεργασίας δεδομένων, η μνήμη, οι υπηρεσίες δικτύου και η χρήση εικονικών μηχανημάτων. Προκειμένου να αυξήσουν τα μέτρα ασφάλειας και να ελαχιστοποιήσουν ορισμένες επιθέσεις κατά της διαθεσιμότητας πόρων που φιλοξενούνται στο Νέφος, οι πάροχοι είναι δυνατό να διαθέσουν επίσης πόρους και να έχουν δυνατότητες αναδιανομής τους όπως είναι το φιλτράρισμα των πληροφοριών για λόγους ασφαλείας. Συνεπώς, οι επιχειρήσεις έχουν ένα ακόμη όφελος από την ικανότητα των πόρων που έχουν να κάνουν με την άμυνα να επεκτείνονται ευέλικτα και δυναμικά καθώς επίσης είναι γεγονός πως τα μικρά «κομμάτια» στα οποία μπορούν να διαιρεθούν οι πόροι καθιστούν την απόκριση των επιχειρήσεων σε απότομες κορυφώσεις ζήτησης, αμεσότερη και πιο οικονομική.

- Έλεγχος και συλλογή στοιχείων

Το μοντέλο IaaS δίνει τη δυνατότητα κλωνοποίησης όποτε αυτό είναι επιθυμητό των virtual μηχανών. Η δυνατότητα αυτή παρέχει πολλαπλά οφέλη. Καταρχάς, σε περίπτωση παραβίασης της ασφάλειας οι χρήστες μπορούν να επεξεργαστούν το περιστατικών εκτός δικτύου (offline) κατασκευάζοντας μια εικόνα της παραπάνω μηχανής. Επίσης, σε περίπτωση ανάγκης επιπρόσθετου αποθηκευτικού χώρου μπορεί η ανάλυση να γίνει παράλληλα δημιουργώντας πολλούς κλώνους. Και οι δύο

παραπάνω περιπτώσεις δείχνουν τη δυνατότητα μείωσης του χρόνου που απαιτείται για ανάλυση και επεξεργασία βελτιώνοντας συνεχώς όλη τη διαδικασία.

- Καλύτερη διαχείριση κινδύνου

Οι πάροχοι Cloud υπηρεσιών προχωρούν σε περισσότερους εσωτερικούς ελέγχους αλλά και σε διαδικασίες αξιολόγησης ρίσκου τόσο λόγω της ανάγκης διατήρησης της φήμης τους σε υψηλά επίπεδα όσο και λόγω της διαχείρισης σεναρίων κινδύνου σε μια Συμφωνία Επίπεδου Υπηρεσιών με αποτέλεσμα την κινητοποίηση τους και τον εντοπισμό κινδύνων που διαφορετικά δε θα είχαν ανιχνευτεί.

- Συγκέντρωση πόρων

Αν θεωρήσουμε δεδομένα και ικανοποιητικά τα μέτρα ασφάλειας που υπάρχουν και επομένως να παραβλέψουμε τη μειωμένη ασφάλεια που περικλείει η συγκέντρωση πόρων, θα μπορούσαμε να επικεντρωθούμε στα πλεονεκτήματα που παρουσιάζει αυτή η συγκέντρωση όπως είναι οι οικονομικότερες διαδικασίες συντήρησης, η οικονομικότερη παραμετροποίηση και εφαρμογή ολοκληρωμένης πολιτικής ασφάλειας και ελέγχου.

- Αποτελεσματικότερες αναβαθμίσεις και προεπιλογές.

Είναι γεγονός πως στο Cloud Computing το λογισμικό που χρησιμοποιείται καθώς και οι εικόνες από τις virtual μηχανές έχουν τη δυνατότητα να αναβαθμιστούν, με τις πιο πρόσφατες εκδόσεις και ρυθμίσεις ασφάλειας και πολλές φορές οι αναβαθμίσεις αυτές πραγματοποιούνται πάνω στην πλατφόρμα συμβάλλοντας στη βελτίωση της ασφάλειας.

3.4. Τα τεχνικά οφέλη του Cloud Computing στις μικρομεσαίες επιχειρήσεις

Στη συνέχεια θα αναφερθούμε στα τεχνικά οφέλη που υφίστανται σχετικά με την ασφάλεια των επιχειρήσεων με βραχυχρόνιες ή μακροχρόνιες επιπτώσεις στη λειτουργία των επιχειρήσεων. Οι μικρομεσαίες επιχειρήσεις ωφελούνται ιδιαιτέρως από τους παρόχους Cloud υπηρεσιών καθώς καλύπτουν αδυναμίες λόγω περιορισμών ή ανύπαρκτων πόρων και προϋπολογισμών. Τα τεχνικά αυτά χαρακτηριστικά είναι :

- Κεντρική διαχείριση δεδομένων

Η κεντρική διαχείριση δεδομένων που προσφέρει το Cloud Computing έχει δύο πολύ σημαντικά πλεονεκτήματα. Αρχικά είναι η μειωμένη διαρροή πληροφοριών η οποία αποτελεί και το δημοφιλέστερο όφελος που παρέχει το Υπολογιστικό Νέφος στις επιχειρήσεις. Παίρνοντας ως δεδομένο το γεγονός ότι οι περισσότερες επιχειρήσεις διακινδυνεύουν την ασφάλεια των δεδομένων τους αποθηκεύοντας τα σε φορητούς υπολογιστές και δίσκους, είναι σίγουρα ασφαλέστερο να μεταφέρουν τα δεδομένα τους σε προσωρινές συσκευές αποθήκευσης. Επιπλέον, η ασφάλεια των δεδομένων σε μικρές επιχειρήσεις διασφαλίζεται από το Cloud Computing αφού παρέχει επιπλέον τη δυνατότητα χρήσης τεχνικών κρυπτογράφησης που δε θα χρησιμοποιούσαν διαφορετικά. Στη συνέχεια, το δεύτερο σημαντικό πλεονέκτημα έχει να κάνει με τον έλεγχο των δεδομένων καθώς είναι γεγονός ότι είναι πιο εύκολο να ελέγχονται και να παρακολουθούνται τα δεδομένα όταν είναι συγκεντρωμένα. Θα πρέπει να σημειώσουμε εδώ ότι θα ήταν εύλογη να διατυπωθεί και η άποψη ότι η συγκέντρωση αυτή είναι και αρκετά ριψοκίνδυνη σε περίπτωση κλοπής και ολικής απώλειας των δεδομένων. Παρόλα αυτά εκτιμάται ότι η κεντρική διαχείριση είναι προτιμότερη καθώς είναι λιγότερο δαπανηρή χρονικά η εύρεση τρόπου ασφάλειας για ένα κεντρικό σύστημα παρά για τα επιμέρους μέρη μιας επιχείρησης.

- Αντιμετώπιση περιστατικών παραβίασης ασφαλείας

Ένας σημαντικός τρόπος αντιμετώπισης περιστατικών παραβίασης ασφαλείας ο οποίος έχει ως αποτέλεσμα τη δραστική μείωση του χρόνου απόκτησης στοιχείων για τη συγκεκριμένη παραβίαση είναι ο ξεχωριστής διακομιστής Νέφους που χρησιμοποιεί το μοντέλο IaaS. Ο διακομιστής βρίσκεται σε κατάσταση offline και έχει την αρμοδιότητα της αντιμετώπισης των περιστατικών «διάρρηξης» όποτε αυτό κριθεί απαραίτητο. Συγκεκριμένα, τίθεται σε λειτουργία online από το περιβάλλον του παρόχου κατά το συμβάν της παραβίασης χωρίς την ανάγκη μεσολάβησης κάποιου τρίτου. Με τον τρόπο αυτό σε περίπτωση που κάποιος διακομιστής βρίσκεται σε κίνδυνο, αντιγράφεται και διατίθεται στο διακομιστή που έχει την ευθύνη εντοπισμού της παραβίασης ενώ ο ίδιος παραμένει διαθέσιμος στο χρήστη. Συνεπώς μειώνονται οι «νεκροί χρόνοι» αφού το αντίγραφο του hardware χρησιμοποιείται έτσι ώστε να παραμένει το σύστημα της επιχείρησης online, κάτι

ιδιαιτέρως ωφέλιμο για τις επιχειρήσεις. Το Cloud Computing παρέχοντας στο χρήστη το hardware που χρειάζεται για τον εντοπισμό κάποιας διαρροής μειώνει τον αντίστοιχο χρόνο. Σε αυτό συμβάλλει επίσης και το γεγονός ότι το σύνολο του hardware βρίσκεται σε ηλεκτρονική μορφή καθιστώντας σαφώς γρηγορότερο τον έλεγχο και τον εντοπισμού του προβλήματος.

Άλλο ένα όφελος του Cloud Computing είναι η δυνατότητα εξάλειψης του χρόνου προσπέλασης των αρχείων που προστατεύονται κάνοντας χρήση κρυπτογραφημένων κλειδιών ή εντολών εντοπισμού πληροφορίας. Οι διάφοροι πάροχοι έχουν αναπτύξει διάφορους τρόπους επίτευξης αυτού. Το S3 της Amazon.com παράγει MD5 hash αυτόματα κατά την αποθήκευση αρχείων ή αντικειμένων και συνεπώς δεν αποτελεί ανάγκη η παραγωγή επιπλέον κλειδιών κρυπτογράφησης. Επιπλέον λόγω της μεγάλης ισχύος επεξεργασίας δεδομένων του Νέφους μειώνεται ο χρόνος προσπέλασης των παραπάνω αρχείων. Στην περίπτωση τώρα που είναι αναγκαίο να διερευνηθεί αν ένα ξένο αρχείο αποτελεί κακόβουλο λογισμικό, οι Cloud υπηρεσίες προσφέρουν τη δυνατότητα δοκιμής διαφορετικών κωδικών σε πολύ μικρό χρονικό διάστημα προκειμένου να το ανοίξει πολύ γρήγορα.

- Έλεγχος αξιοπιστίας κωδικού (cracking)

Ένα ακόμη από τα οφέλη χρήσης υπηρεσιών Cloud είναι και η μείωση του χρόνου ελέγχου της αξιοπιστίας ενός κωδικού. Αυτό συμβαίνει γιατί οι πάροχοι υπηρεσιών Cloud κάνουν αυτοβούλως ελέγχους της ισχύος ενός κωδικού την ίδια στιγμή που για μια επιχείρηση η παραπάνω διαδικασία είναι ιδιαιτέρως χρονοβόρα. Επίσης στο Cloud Computing οι διαδικασίες cracking μεταβιβάζονται σε άλλες μηχανές την ίδια ώρα που μια επιχείρηση χρησιμοποιεί cracking λογισμικά τα οποία διανέμονται σε πολλές μηχανές για μείωση του φόρτου εργασίας.

- Καταγραφή αρχείων

Οι υπολογιστικές υπηρεσίες που παρέχει το Cloud Computing στις επιχειρήσεις μπορεί να αξιοποιηθεί από αυτές με σκοπό την αναζήτηση αρχείων γρήγορα και αποτελεσματικά μιας και το Νέφος παρέχει τη δυνατότητα απεριόριστης αποθήκευσης αρχείων. Όπως καταλαβαίνουμε η συμβολή αυτής της δυνατότητας στην αποτελεσματική λειτουργία της επιχείρησης είναι μεγάλη. Παρόλο λοιπόν που

τα περισσότερα σύγχρονα λειτουργικά συστήματα προσφέρουν εκτεταμένα συστήματα καταγραφής στη μορφή της ελεγκτικής ιχνηλάτησης C2 σχεδόν ποτέ δεν χρησιμοποιούνται. Αυτός συμβαίνει γιατί οι επιχειρήσεις επιθυμούν να αποφύγουν την υψηλή κατανάλωση ισχύος επεξεργασίας. Το Cloud Computing προσφέρει επί πληρωμής τη δυνατότητα χρήσης υπηρεσίας η οποία δεν υποβαθμίζει την αποθηκευτική δυνατότητα ή την ισχύ επεξεργασίας του συστήματος της επιχείρησης.

- Βελτίωση της κατάστασης των λογισμικών ασφαλείας (επιδόσεις)

Η συνεχής καταγραφή των χρεώσιμων διαδικασιών στο Cloud έχει ως αποτέλεσμα τη στροφή της προσοχής των παρόχων στις διαδικασίες οι οποίες δεν αποδίδουν τόσο έτσι ώστε να τις βελτιώσουν και με απώτερο στόχο πιο αποδοτικά software ασφαλείας.

- Δομές Ασφαλείας

Σε περίπτωση που μια επιχείρηση επιθυμεί να δοκιμάσει κάποια αλλαγή στις δομές ασφάλειας μπορεί να το κάνει πολύ εύκολο χρησιμοποιώντας το Cloud. Δημιουργώντας ένα αντίγραφο του παραγωγικού περιβάλλοντος τους δίνεται η δυνατότητα να κάνουν αλλαγές και να ελέγξουν τις επιδράσεις οικονομικά και γρήγορα, κάτι που θα ήταν πολύ δύσκολο να συμβεί δουλεύοντας στο παραγωγικό τους περιβάλλον αυτό καθεαυτό.

- Δοκιμές ασφαλείας

Στο μοντέλο SasS δεδομένου ότι οι επιχειρήσεις χρησιμοποιούν τις ίδιες εφαρμογές ως υπηρεσίες, ο πάροχος ζητά μερικώς το συνολικό κόστος ελέγχου της ασφάλειας μειώνοντας το κόστος των επιχειρήσεων. . Έτσι, μπορούμε να πούμε ότι το Υπολογιστικό Νέφος παρέχει δοκιμές ασφάλειας σε χαμηλό κόστος.

3.5 Η παροχή δεδομένων και η ασφάλεια τους

Είναι γεγονός ότι οι χρήστες θα πρέπει να λαμβάνουν υπόψη και το ρίσκο για την ασφάλεια, όχι μόνο των δεδομένων που συλλέγει ο πάροχος και για το πώς το CSP

τα προστατεύει, αλλά και για τα μεταδεδομένα που έχει ο πάροχος σχετικά με αυτά τα δεδομένα. Συγκεκριμένα, θα πρέπει να γνωρίζουν τι είδους ασφάλειας εφαρμόζεται σε αυτά και το είδος της πρόσβασης τους.

Επίσης θα πρέπει να συλλέγεται και να προστατεύεται από τον προμηθευτή ένα πολύ μεγάλο ποσό που αφορά την ασφάλεια των δεδομένων και των μεταδεδομένων που συνεχώς αυξάνουν σε όγκο.

Αν θελήσουμε να δώσουμε ένα παράδειγμα, μπορούμε να πούμε ότι σε επίπεδο δικτύου η συλλογή πληροφοριών, προκειμένου να ελεγχθεί και να προστατευθεί το firewall, το σύστημα αποτροπής εισβολών και η ροή δεδομένων του δρομολογητή, είναι υποχρέωση του εκάστοτε παρόχου. Στη συνέχεια, σε επίπεδο φορέα υποδοχής αλλά και σε επίπεδο εφαρμογής του μοντέλου SaaS θα πρέπει να συλλέγονται αρχεία καταγραφής του συστήματος, της εφαρμογής των δεδομένων καθώς επίσης θα πρέπει να συμπεριλαμβάνεται η ταυτότητα και τα στοιχεία άδειας.

Όλα τα παραπάνω σε περίπτωση ύπαρξης κάποιου νομικού ζητήματος, θα πρέπει να είναι στη διάθεση των παρόχων αλλά και των χρηστών

- Αποθήκευση

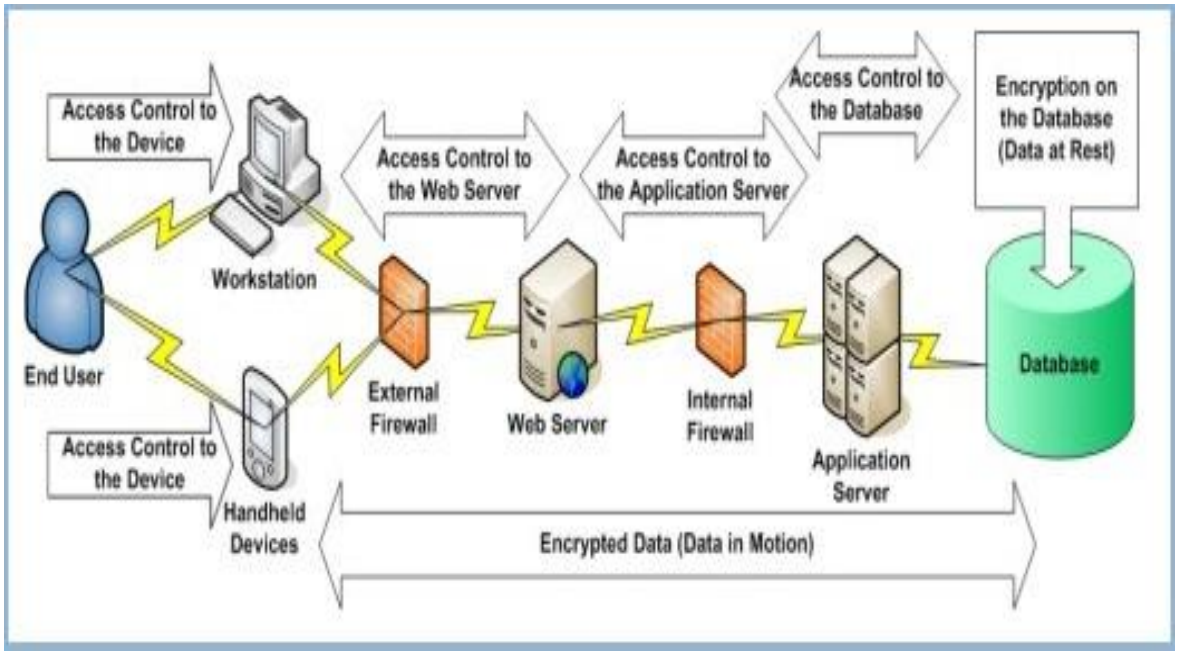
Σχετικά με την αποθήκευση δεδομένων στο Υπολογιστικό Νέφος και την ασφάλεια τους μας ενδιαφέρει η διαδικασία που γίνεται στο μοντέλο IaaS και η οποία περιλαμβάνει την ακεραιότητα, την εμπιστευτικότητα και τη διαθεσιμότητα τους.

- ✓ <u>Εμπιστευτικότητα</u>

Κάνοντας λόγο για την εμπιστευτικότητα και την προστασία των δεδομένων που αποθηκεύονται σε ένα Public Cloud, κυρίως μας απασχολεί ο έλεγχος πρόσβασης αλλά και ο τρόπος με τον οποίο τα δεδομένα αυτά προστατεύονται. Σε ό, τι αφορά τον έλεγχο πρόσβασης οι χρήστες θα πρέπει να επικεντρωθούν τόσο στην επαλήθευση ταυτότητας όσο και στην αδειοδότηση. Είναι σύνηθες ως επίπεδο ασφάλειας να παρέχεται μόνο η άδεια διαχειριστή και η άδεια χρήσης χωρίς να δίνεται η δυνατότητα ενδιάμεσων επιπέδων.

Μια εύλογη επόμενη ερώτηση είναι για τον τρόπο με τον οποίο τα δεδομένα που είναι στο Υπολογιστικό Νέφος προστατεύονται. Η χρήση κρυπτογράφησης για την προστασία των δεδομένων που είναι αποθηκευμένα στο σύννεφο κρίνεται φυσικά απαραίτητη.

Στην ανησυχία για το αν στην πραγματικότητα τα δεδομένα που είναι αποθηκευμένα στο Cloud είναι και κρυπτογραφημένα, έρχεται να προστεθεί και το ποιος αλγόριθμος κρυπτογράφησης χρησιμοποιείται και το αν αυτός είναι αποτελεσματικός. Επίσης, το κλειδί κρυπτογράφησης, είναι αρκετά ισχυρό ώστε να μας εξασφαλίσει την επιθυμητή ασφάλεια; Παραδείγματος χάριν, το S3 δεν κρυπτογραφεί τα δεδομένα των πελατών αλλά οι ίδιοι οι πελάτες είναι σε θέση να κρυπτογραφήσουν τα δεδομένα τους.



Σχήμα 3.3: Σχεδιάγραμμα βασικών τμημάτων της κρυπτογράφησης των δεδομένων

Πηγη http://www.cdc.gov/cancer/npcr/tools/security/encryption2.htm

Πιο λεπτομερώς, εφόσον διασφαλίσουμε ότι τα δεδομένα κρυπτογραφούνται η αμέσως επόμενη ανησυχία είναι, ο αλγόριθμος κρυπτογράφηση που χρησιμοποιείται. Παρόλο που πολλοί αλγόριθμοι παρέχουν επαρκή ασφάλεια μόνο οι αλγόριθμοι που έχουν δημοσίως ελεγχθεί από ένα επίσημο πρότυπο (π.χ., NIST) ή τουλάχιστον ανεπίσημα από την κρυπτογραφική κοινότητα θα πρέπει να χρησιμοποιούνται. Οποιοσδήποτε «ιδιόκτητος» αλγόριθμος δε θα πρέπει να χρησιμοποιείται. Θα πρέπει να τονίσουμε ότι εμείς σε ό, τι αφορά το είδος του αλγόριθμου, μιλάμε για συμμετρική αλγοριθμική κρυπτογράφηση. Η Συμμετρική

κρυπτογράφηση περιλαμβάνει τη χρήση ενός ενιαίου μυστικού κλειδιού τόσο για την κρυπτογράφηση όσο και την αποκρυπτογράφηση των δεδομένων και έχει την ταχύτητα και την υπολογιστική απόδοση για να χειριστεί μεγάλο όγκο δεδομένων. Συνεπώς, σε αυτή την περίπτωση δε θα ήταν ιδιαίτερα αποδοτική η χρήση μη συμμετρικού αλγορίθμου για την κρυπτογράφηση.

Στη συνέχεια θα πρέπει να εξετάσουμε το μήκος του κλειδιού που χρησιμοποιείται. Στη συμμετρική κρυπτογράφηση το μήκος του κλειδιού (δηλαδή μεγάλος αριθμός των bits του κλειδιού) παίζει σημαντικό ρόλο. Όσο πιο μεγάλο είναι τόσο ισχυρότερη είναι η κρυπτογράφηση παρόλο που είναι γεγονός ότι τα κλειδιά με μεγάλα μήκη παρέχουν μεγαλύτερη προστασία μεν αλλά μπορεί να καταπονήσουν τις δυνατότητες των επεξεργαστών των ηλεκτρονικών υπολογιστών.

Ένα σημαντικό θέμα εμπιστευτικότητας για την κρυπτογράφηση είναι η διαχείριση των προαναφερθέντων κλειδών. Το ερώτημα που υπάρχει είναι για το πώς γίνεται η διαχείριση των κλειδιών κρυπτογράφησης που χρησιμοποιούνται και ειδικά από ποιον. Αν ο χρήστης σκοπεύει να διαχειριστεί μόνος του τα κλειδιά, δηλαδή αν έχει την εμπειρία και τις τεχνικές γνώσεις να το κάνει τότε είναι εντάξει. Διαφορετικά θα πρέπει να λάβουμε υπόψη το γεγονός ότι δε συνιστάται να αναθέσει στον πάροχο να διαχειριστεί τα κλειδιά του- τουλάχιστον όχι στον ίδιο πάροχο, ο οποίος χειρίζεται τα δεδομένα του. Αυτό σημαίνει πρόσθετους πόρους και ικανότητες.

- ✓ Ακεραιότητα

Η επιχείρηση θα πρέπει επίσης να ανησυχεί για την ακεραιότητα των δεδομένων της εκτός από την προστασία του απορρήτου των δεδομένων της. Ένα εύλογο ερώτημα θα ήταν το αν η εμπιστευτικότητα συνεπάγεται και την ακεραιότητα. Τα δεδομένα μπορούν να κρυπτογραφούνται για λόγους εμπιστευτικότητας και παρόλα αυτά να μην μπορεί η επιχείρηση να έχει έχουμε έναν τρόπο να επαληθεύσει την ακεραιότητα των δεδομένων. Η διαδικασία της κρυπτογράφησης από μόνη της είναι αρκετή ως προς την εμπιστευτικότητα, αλλά η ακεραιότητα απαιτεί επίσης επιπλέον διεργασίες που πρέπει να ληφθούν υπόψη και να υλοποιηθούν.

Η χρήση ενός συμμετρικού αλγορίθμου και η συμπερίληψη μιας συνάρτησης hash ώστε να περιλαμβάνουν μια μονόδρομη συνάρτηση κατακερματισμού αποτελεί τον απλούστερο τρόπο για να χρησιμοποιήσουμε κρυπτογραφημένα δεδομένα. Το γεγονός αυτό είναι ιδιαίτερης σημασίας για την ακεραιότητα των δεδομένων του πελάτη, αλλά θα χρησιμεύσει επίσης για να παρέχουν πληροφορίες σχετικά με το πόσο εξελιγμένο πρόγραμμα ασφάλειας χρησιμοποίει ο πάροχος. Παρόλα αυτά θα πρέπει να σημειωθεί ότι δεν γίνεται κρυπτογράφηση των δεδομένων των πελατών, ειδικά για τις PaaS και SaaS υπηρεσίες.

Στη συνέχεια θα πρέπει να δώσουμε προσοχή σε μια άλλη πτυχή της ακεραιότητας των δεδομένων η οποία είναι σημαντική ιδιαίτερα αν η επιχείρηση κάνει χρήση αποθήκευσης στην υπηρεσία IaaS. Το ερώτημα που γεννάται είναι το πώς ο χρήστης, ο οποίος έχει κάποια gigabytes (ή περισσότερα) δεδομένων του στο σύννεφο για αποθήκευση, μπορεί να είναι σε θέση να ελέγξει την ακεραιότητα των δεδομένων που είναι αποθηκευμένα εκεί. Επίσης εφόσον υπάρχει κάποιος τρόπος θα υπάρχει και κόστος που συνδέεται με τη μεταφορά και τη μετακίνηση των δεδομένων από και προς το Νέφος.

Η επαλήθευση της ακεραιότητας των δεδομένων του, χωρίς να χρειάζεται να κατεβάσει και να ανεβάσει τα δεδομένα κάθε φορά από το Cloud, είναι αυτό που θέλει πραγματικά ο χρήστης. Η διαδικασία αυτή είναι ακόμη πιο δύσκολη καθώς ο χρήστης δεν είναι σε θέση να γνωρίζει που ακριβώς είναι αποθηκευμένα τα δεδομένα του, τα οποία μάλιστα αλλάζουν χώρο αποθήκευσης δυναμικά.

- ✓ <u>Διαθεσιμότητα</u>

Υποθέτοντας ότι τα στοιχεία μιας επιχείρησης έχουν διατηρήσει την εμπιστευτικότητα και την ακεραιότητά τους, θα πρέπει επίσης να ανησυχεί για την διαθεσιμότητα των δεδομένων της. Υπάρχουν επί του παρόντος τρεις μεγάλες απειλές σε όσον αφορά αυτό.

Η πρώτη απειλή αφορά τη διαθεσιμότητα του δικτύου σχετικά με τις επιθέσεις. Ένας χρήστης μπορεί να είναι τυχερός με το να λάβει “three 9s” του uptime χρήσης. Μια σειρά από μεγάλες διακοπές παροχής έχουν συμβεί. Για παράδειγμα, το Amazon 3 υπέστη 2,5 ώρες διακοπής το Φεβρουάριο του 2008 και μια οκτάωρη διακοπή τον

Ιούλιο του 2008. Αυτές οι διακοπές του Amazon άρχισαν να γίνονται όλο και πιο εμφανείς με την αύξηση του αριθμού των πελατών.

Εκτός από τις διακοπές της υπηρεσίας, σε ορισμένες περιπτώσεις, τα δεδομένα που αποθηκεύονται στο σύννεφο έχουν πράγματι χαθεί. Οι χρήστες της υπηρεσίας αυτή πρέπει να εξετάσουν κατά πόσον οι πάροχοι αποθήκευσης σε τεχνολογία cloud θα κατέχουν και μελλοντικά την επιχείρηση.

Τέλος, αξίζει να σημειωθεί ότι πολλοί πάροχοι αποθήκευσης στην τεχνολογία cloud δεν δημιουργούν αντίγραφα ασφαλείας των δεδομένων των πελατών τους, ή το κάνουν μόνο ως πρόσθετη υπηρεσία με επιπλέον κόστος. Η διαθεσιμότητα είναι φαινομενικά κάτι απλό αλλά κρίσιμο ερώτημα για το αν οι πελάτες θα πρέπει να ζητούν την αποθήκευση των δεδομένων τους ή όχι από τους παρόχους[16],[17].

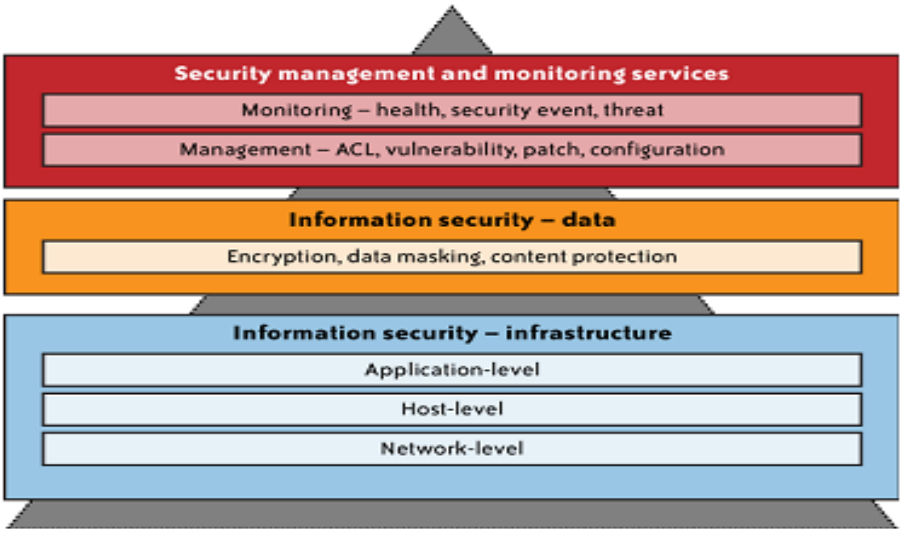
ΚΕΦΑΛΑΙΟ 4: ΤΕΧΝΟΛΟΓΙΕΣ ΑΣΦΑΛΕΙΑΣ ΣΕ CLOUD

4.1. Γενικά

Εφόσον αποφασίσουμε να υιοθετήσουμε δημόσιες Cloud υπηρεσίες, γνωρίζουμε ότι ένα μεγάλο τμήμα του δικτύου μας, τα συστήματα, οι εφαρμογές και τα δεδομένα θα βρίσκονται κάτω από τον έλεγχο του παρόχου. Η παράδοση των Cloud μοντέλων υπηρεσιών θα δημιουργήσει νησιά (Clouds) εικονικών περιμέτρων καθώς και ένα πρότυπο ασφαλείας με τις αρμοδιότητες να μοιράζονται μεταξύ του πελάτη και του παρόχου των Cloud υπηρεσιών (CSP). Συνεπώς θα υπάρξει ένα μοντέλο κοινής ευθύνης το οποίο θα φέρει νέες προκλήσεις στη διαχείριση της ασφάλειας στο IT προσωπικού ενός οργανισμού. Έχοντας αυτό υπόψη, ένας υπεύθυνος ασφάλειας πληροφοριών θα πρέπει να απαντήσει στο ερώτημα που είναι αν έχει επαρκή διαφάνεια από τις υπηρεσίες Cloud για τη διαχείριση της διακυβέρνησης (κοινές ευθύνες) και της εφαρμογής των διαδικασιών διαχείρισης της ασφάλειας (πρόληψη και ανίχνευση ελέγχου). Με τον τρόπο αυτό θα γνωρίζει αν διασφαλίζεται η επιχείρηση και ειδικά αν τα δεδομένα της είναι κατάλληλα προστατευμένα στο Cloud.

Συνεπώς θα πρέπει να απαντηθούν κατ' ουσία δύο ερωτήσεις: η πρώτη είναι το τι ελέγχους ασφαλείας πρέπει να έχει ο πελάτης πέρα και πάνω από τους ελέγχους που συνυπάρχουν στη πλατφόρμα του Cloud, και η δεύτερη είναι το πώς πρέπει τα εργαλεία και οι διαδικασίες διαχείρισης ασφάλειας μιας επιχείρησης να προσαρμοστούν για τη διαχείριση της ασφάλειας στο Cloud. Δίνοντας βάση την ευαισθησία των δεδομένων και των service - level και οι δύο απαντήσεις θα πρέπει να αξιολογούνται συνεχώς.

Από την πλευρά του πελάτη Cloud, θα πρέπει να ξεκινήσουμε με το να κατανοήσουμε το όριο εμπιστοσύνης των υπηρεσιών μας στο Cloud. Είναι αναγκαίο να καταλάβουμε όλα τα στρώματα που έχουμε στη κατοχή μας, που αγγίζουμε, ή τη διασύνδεσή μας με το δίκτυο υπηρεσιών του Cloud– το δίκτυο, host, εφαρμογές, βάση δεδομένων, αποθήκευση και web υπηρεσίες οι οποίες περιέχουν και υπηρεσίες γνησιότητας.



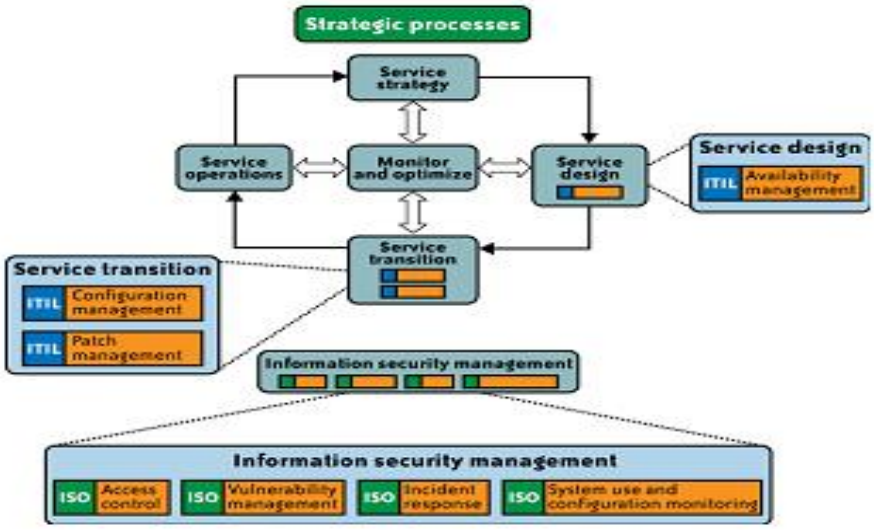
Σχήμα 4.1: Σχεδιάγραμμα βασικών στρωμάτων σε ένα δίκτυο Cloud

Πηγή http://www.teilar.gr/dbData/ProfAnn/profann-1c85fbaa.pdf

Το περιεχόμενο της διαχείρισης του συστήματος πληροφορικής και η παρακολούθηση των ευθυνών που εμπίπτουν πάνω μας είναι υψίστης σημασίας να κατανοηθούν πλήρως. Στα παραπάνω συμπεριλαμβάνονται η πρόσβαση, η αλλαγή, η

διαμόρφωση, τα patches και η διαχείριση ευπάθειας. Όπως έχουμε πει και σε προηγούμενο κεφάλαιο παρόλο που μπορεί να μεταφέρει μερικές από τις επιχειρησιακές ευθύνες στο πάροχο, το επίπεδο ευθυνών ποικίλει και εξαρτάται από μια ποικιλία παραγόντων, συμπεριλαμβανομένης της υπηρεσίας Service delivery model (SPI), service-level συμφωνία παρόχου (SLA), και του provider -specific ικανότητες να υποστηρίξουν την επέκταση των εσωτερικών διαδικασιών διαχείρισης της ασφάλειας και των εργαλείων μας.

Η ITIL, παλαιότερα γνωστό ως Βιβλιοθήκη Υποδομής Πληροφορικής, είναι ένα σύνολο πρακτικών διαχείρισης υπηρεσιών πληροφορικής (IT Service Management ITSM) που εστιάζει στην ευθυγράμμιση υπηρεσιών πληροφορικής με τις ανάγκες της επιχείρησης. Στη σημερινή της μορφή (γνωστή ως ITIL), η ITIL δημοσιεύεται ως μια σειρά από πέντε τόμους, καθένας από τους οποίους καλύπτει ένα διαφορετικό στάδιο κύκλου ζωής του ITSM. Αν και η ITIL υποστηρίζει το ISO / IEC 20000, το Διεθνές Πρότυπο Διαχείρισης Υπηρεσιών στη διαχείρισης IT υπηρεσιών, υπάρχουν ορισμένες διαφορές μεταξύ του πρότυπου ISO 20000 και του πλαισίου ITIL.
Από τον Ιούλιο του 2013, η ITIL ανήκει στην AXELOS Ltd, μια κοινοπραξία μεταξύ της HM Cabinet Office και Capita Plc. Η AXELOS πιστοποιεί τους οργανισμούς να χρησιμοποιήσουν την πνευματική ιδιοκτησία της ITIL, παρέχει διαπίστευση για πιστοποιημένα Ινστιτούτα εξετάσεων και διαχειρίζεται ενημερώσεις για το πλαίσιο.

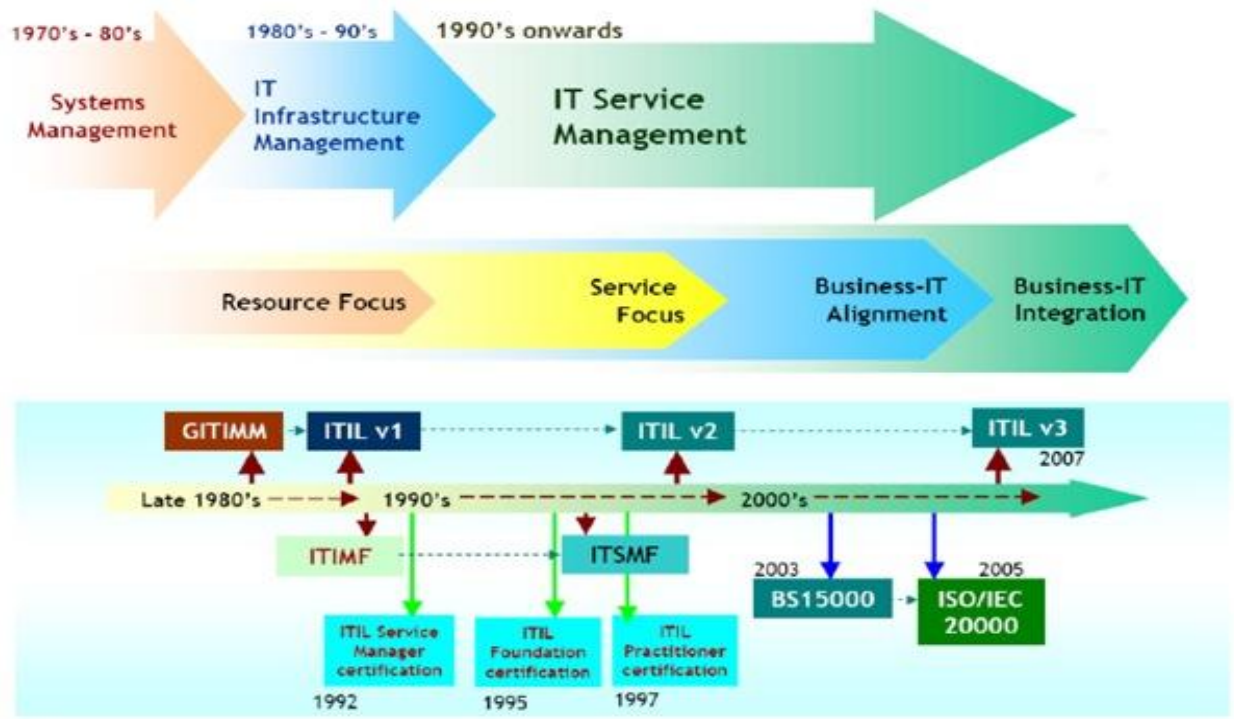


Σχήμα 4.2: Ο κύκλος ζωής ενός ITIL μιας επιχείρησης.

Πηγή http://www.teilar.gr/dbData/ProfAnn/profann-1c85fbaa.pdf

4.2. Πρότυπα Διαχείρισης Ασφάλειας

Όπως αναφέραμε και προηγουμένως τα πρότυπα που έχουν σχέση με τις πρακτικές διαχείρισης της ασφάλειας στο Cloud computing είναι το ITIL και το ISO/IEC27001 και 27002.



Σχήμα 4.3: Εξέλιξη προτύπων ασφάλειας και ISO

Τα πρότυπα ITIL και ISO/IEC27001 και 27002 είναι τα σχετικά με τη διαχείριση ασφάλειας και τις πρακτικές της. Παρακάτω θα αναφερθούμε στα συγκεκριμένα πρότυπα και τις κατευθυντήριες γραμμές που προτείνουν όπως επίσης και στους ελέγχους πρόσβασης στα μοντέλα SaaS, IaaS, PaaS.

4.2.1. ITIL

Η Information Technology Infrastructure Library (ITIL), η οποία έχει εφαρμογή στα IT περιβάλλοντα, όπως επίσης στο περιβάλλον λειτουργίας του Cloud, είναι ένα

σύνολο βέλτιστων πρακτικών και κατευθυντήριων γραμμών που καθορίζουν μια ολοκληρωμένη διαδικασία προσέγγισης για τη διαχείριση πληροφοριών των υπηρεσιών τεχνολογίας. Έχοντας ως στόχο την εξασφάλιση μέτρων ασφαλείας που θα είναι αποτελεσματικά στο θέμα των πληροφοριών και θα λαμβάνονται σε τακτικό και επιχειρησιακό επίπεδο, η ITIL θεωρεί την ασφάλεια των πληροφοριών ως μια διαδικασία η οποία πρέπει να ελέγχεται, να σχεδιάζεται, να εφαρμόζεται, να αξιολογείται και να διατηρείται επομένως τη θεωρεί μια επαναληπτική διαδικασία.

Οι κατηγορίες που χωρίζει η ITIL την ασφάλεια των πληροφοριών είναι οι Πολιτικές, οι Διεργασίες, οι Διαδικασίες και οι Οδηγίες Εργασίας.

4.2.2. ISO 27001/27002

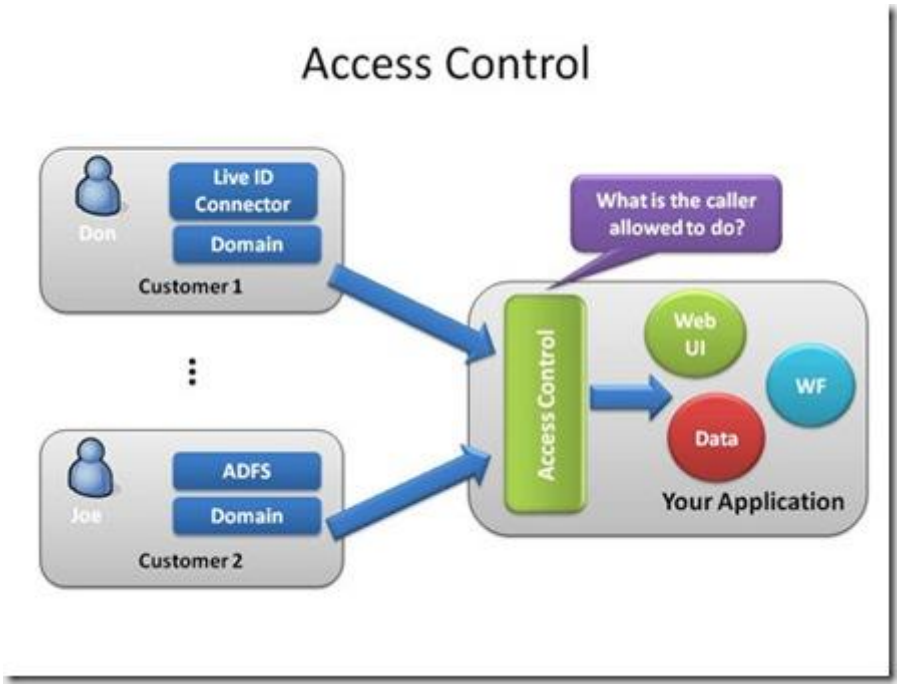
Το ISO / IEC 27002 είναι ένα συμβουλευτικό πρότυπο που προορίζεται να ερμηνευτεί και να εφαρμοστεί σε όλους τους τύπους και τα μεγέθη οργανισμών σύμφωνα με τους ιδιαίτερους κινδύνους ασφάλειας των πληροφοριών που αντιμετωπίζουν. Στην πράξη, αυτή η ευελιξία δίνει στους χρήστες τη μεγάλη ευχέρεια να υιοθετήσουν τα στοιχεία ελέγχου της ασφάλειας των πληροφοριών που έχουν νόημα για αυτούς, αλλά το καθιστά ακατάλληλο για την σχετικά απλή δοκιμή της συμμόρφωσης.

Το ISO / IEC 27001: 2005 (Τεχνολογία της πληροφορίας - Τεχνικές Ασφάλειας - Συστήματα διαχείρισης της ασφάλειας των πληροφοριών - Απαιτήσεις) είναι ένα ευρέως αναγνωρισμένο πρότυπο πιστοποίησης. Το ISO / IEC 27001 καθορίζει μια σειρά από σταθερές απαιτήσεις για την κατάρτιση, την εφαρμογή, τη διατήρηση και τη βελτίωση ενός ISMS. Μια νέα έκδοση του προτύπου είναι στο σχέδιο ISO / IEC 27001: 2013.

4.2.3. Access Control

Ο έλεγχος πρόσβασης αποτελεί ένα σημαντικό κομμάτι στο θέμα της ασφάλειας. Η διαχείρισή του έχει μια ευρύτερη έννοια με πολλές συνιστώσες όπως το τι απαιτείται για την πρόσβαση των χρηστών και των διαχειριστών του συστήματος στο δίκτυο, στους πόρους και τις εφαρμογές του συστήματος. Καταρχάς, θα πρέπει να γίνει

εκχώρηση δικαιωμάτων σε χρήστες δηλαδή να διευκρινιστεί το ποιός θα έχει άδεια πρόσβασης και σε ποιους πόρους του συστήματος. Στη συνέχεια, είναι αναγκαία η εκχώρηση δικαιωμάτων με βάση τα καθήκοντα και τις ευθύνες του χρήστη δηλαδή να διευκρινιστεί ο λόγος για τον οποίο ένας χρήστης θα έχει πρόσβαση σε κάποιον πόρο του συστήματος. Επιπλέον, απαραίτητη κρίνεται η μέθοδος με την οποία ελέγχουμε την ταυτότητα και την ισχύ της πριν χορηγηθεί πρόσβαση στους πόρους. Τέλος, θα πρέπει να γίνει έλεγχος που επαληθεύει τα δικαιώματα των χρηστών και τις αναθέσεις καθώς επίσης και η αντίστοιχη υποβολή εκθέσεων.



Σχήμα 4.4: Απλοποιημένη απεικόνιση του ελέγχου πρόσβασης

Πηγή http://www.techbubbles.com/microsoft/net-access-control-service/

Όλα τα προαναφερθέντα θα πρέπει να ληφθούν υπόψη από τα πρότυπα πρόσβασης και τις πολιτικές οργανισμών. Επίσης, κρίνεται απαραίτητο οι ρόλοι του χρήστη και οι ευθύνες του, όπως επίσης οι τελικοί χρήστες και οι προνομιακοί διαχειριστές του συστήματος. να ευθυγραμμιστούν με όλα τα προαναφερθέντα.

4.2.4. Έλεγχος Πρόσβασης στο Cloud

Είναι γεγονός πως το σύνολο των παραδοσιακών ελέγχων πρόσβασης σε ένα δίκτυο επικεντρώνεται στην προστασία των πόρων από μη εξουσιοδοτημένη πρόσβαση με βάση τα χαρακτηριστικά του κεντρικού υπολογιστή, ο οποίος τις περισσότερες περιπτώσεις είναι ανεπαρκής, και μπορεί να προκαλέσει λανθασμένους υπολογισμούς.

Από την άλλη μεριά, σε μοντέλο Υπολογιστικού Νέφους, οι χρήστες από οποιοδήποτε σημείο πρόσβασης στο internet θα μπορούν να έχουν πρόσβαση στις υπηρεσίες Νέφους. Συνεπώς, ο ρόλος του ελέγχου πρόσβασης θα μειώνεται. Σε αυτή την περίπτωση του Νέφους, λοιπόν εφαρμόζονται πολιτικές firewall προκειμένου να ελεγχθεί η πρόσβαση στο διαδίκτυο. Επιβάλλεται η ύπαρξη ενός host-based ελέγχου πρόσβασης στην είσοδο και στην έξοδο του Cloud και λογική ομαδοποίηση των instances μέσα στο Cloud. Στη συγκεκριμένη περίπτωση χρησιμοποιείται τυποποιημένο πρωτόκολλο μετάδοσης ελέγχου, Protocol/Internet(TCP/IP) παραμέτρους, που συμπεριλαμβάνει την πηγή IP, τη θύρα πηγής, τη διεύθυνση προορισμού IP και το destination port.

Ένα άλλο ζήτημα που θα πρέπει να λαμβάνεται υπόψη είναι ότι μέσα στο Cloud ο έλεγχος πρόσβασης των χρηστών είναι πιθανό να είναι συνδεδεμένη με τους πόρους του Cloud. Είναι πολύ χρήσιμο λοιπόν ένας λεπτομερής έλεγχος πρόσβασης, με λογιστικούς υπολογισμούς του χρήστη και συμμόρφωση ως προς τα δεδομένα προστασίας. Τέλος, σημαντικό ρόλο στην προστασία του απορρήτου και στην ακεραιότητα των πληροφοριών στο Νέφος διαδραματίζουν οι έλεγχοι διαχείρισης της πρόσβασης των χρηστών καθώς και των single-sign-on(SSO), τα προνόμια διαχείρισης και η καταγραφή των πόρων του.

4.2.5. Έλεγχος Πρόσβασης στο SaaS

Στο μοντέλο SaaS η εκάστοτε εφαρμογή αποτελεί υπηρεσία στον τελικό χρήστη η οποία παρέχεται μέσω ενός web browser. Συνεπώς οι έλεγχοι πρόσβασης των χρηστών αντικαθιστούν τους ελέγχους που βασίζονται στο δίκτυο. Ένα παράδειγμα τέτοιων ελέγχων είναι η χρήση ταυτότητας one-time password. Το CSP στο

συγκεκριμένο μοντέλο είναι αυτό που έχει την ευθύνη και διαχειρίζεται όλους τους τομείς του δικτύου την εφαρμογή και την υποδομή του διακομιστή. Σύμφωνα με τα παραπάνω πρέπει να υπάρξει η επικέντρωση του ενδιαφέροντος στον έλεγχο πρόσβασης των χρηστών προκειμένου οι πληροφορίες που φιλοξενούνται από τις SaaS να προστατεύονται.

Η Slaesforce.com, μια υπηρεσία του μοντέλου SaaS έχει στρέψει το ενδιαφέρον της από τον έλεγχο πρόσβασης στο διαδίκτυο στον έλεγχο πρόσβασης των χρηστών δίνοντας τη δυνατότητα να προστεθούν παράμετροι της πολιτικής ελέγχου των χρηστών στην πρόσβαση με βάση το δίκτυο.

Παρόλα αυτα όσον αφορά τον έλεγχο πρόσβασης των χρηστών, οι πάροχοι διαφοροποιούνται σε ό, τι έχει να κάνει με τις δυνατότητες και την υποστήριξη που παρέχουν. Προς το παρόν, μόνο λίγοι CSPs και αυτοί είναι εταιρίες όπως η, Google, η Microsoft και η Salesforce.com δείχνουν ενδιαφέρον στο τι απαιτεί η IAM βιομηχανία παρόλο που οι δυνατότητες της βρίσκονται σε εμβρυικό ακόμη στάδιο. Και σε αυτό το ενδιαφέρον προστίθεται η υποστήριξη για το SAML πρότυπο, αλλά και άλλα παρεμφερή, το οποίο διευκολύνει τη χρήση τεχνικών γνησιότητας από την SSO. Οι χρήστες ωστόσο δε θα πρέπει να σταματήσουν να απαιτούν από τα CSP την παροχή IAM χαρακτηριστικών, SAML υποστήριξης, user provisioning χρησιμοποιώντας SPML, και ενός ανοικτού API για την υποστήριξη διαφόρων χρηστών και την πρόσβαση σε διαδικασίες αυτοματισμών. Τέλος, η πρόσβαση των χρηστών στη διαχείριση θα πρέπει να υποστηριχτεί ιδιαιτέρως από τους οργανισμούς οι οποίοι είναι απαραίτητο να αξιοποιήσουν για το σκοπό αυτό τις μέχρι τώρα εφαρμοζόμενες μεθόδους τους, τις πρακτικές διαχείρισης ταυτότητας, τις διαδικασίες και την αρχιτεκτονική τους

4.2.6. Έλεγχος Πρόσβασης στο PaaS

Στο μοντέλο PaaS ο πελάτης έχει την ευθύνη του ελέγχου της πρόσβασης στις εφαρμογές που αναπτύχθηκαν στην πλατφόρμα αυτή. Από την άλλη η CSP ευθύνεται για τους servers, την υποδομή της πλατφόρμας εφαρμογών και διαχειρίζεται τον έλεγχο πρόσβασης στο δίκτυο. Ο έλεγχος πρόσβασης στις εφαρμογές για τον οποίο

είναι υπεύθυνος ο πελάτης ουσιαστικά αποτελεί τη διαχείριση πρόσβασης στους τελικούς χρήστες. Εκτός των άλλων η διαχείριση αυτή προσπαθεί να προβλέψει και να εξακριβώσει τη γνησιότητα των χρηστών.

Οι δυνατότητες που προσφέρονται από τους παρόχους σε ό, τι αφορά την υποστήριξη για τον έλεγχο πρόσβασης των χρηστών δεν έχει κάποια συνέπεια. Μεγάλοι πάροχοι PaaS προσφέρουν πολύ μικρή υποστήριξη για τον έλεγχο πρόσβασης των χρηστών. Εξαίρεση σε αυτό αποτελούν οι Force.com και Microsoft Azure. Η Google παραδείγματος χάριν υποστηρίζει μια υβριδική έκδοση του πρωτοκόλλου OpenID και Oauth που συνδυάζει την έγκριση και την γνησιότητα της ροής σε λιγότερα βήματα έτσι ώστε να δίνεται ιδιαίτερο βάρος στη χρηστικότητα με στόχο την ενίσχυσή της. Επίσης φέρνοντας ως παράδειγμα την Security Assertion Markup Language (SAML) είναι δυνατή και η ανάθεση την γνησιότητα του IdP μας εάν υπάρχει υποστήριξη των ομοσπονδιακών προτύπων από την CSP.

4.2.7. Έλεγχος Πρόσβασης στο IaaS

Στο μοντέλο IaaS η διαχείριση του ελέγχου πρόσβασης στους πόρους του cloud είναι απόλυτη ευθύνη των πελατών. Αυτό σημαίνει ότι οι πελάτες είναι υπεύθυνοι τόσο για την πρόσβαση στους εικονικούς servers, στα εικονικά δίκτυα και στην εικονική αποθήκευση όσο και για τις εφαρμογές που φιλοξενούνται σε μια πλατφόρμα IaaS. Συγκεκριμένα είναι οι πελάτες θα πρέπει να σχεδιάζουν και να διαχειρίζονται την παραπάνω πρόσβαση.

Υπάρχουν δύο κατηγορίες διαχείρισης ελέγχου πρόσβασης που έχουν να κάνουν νε το μοντέλο χορήγησης IaaS: η CSP infrastructure access control και η Customer virtual infrastructure access control. Η πρώτη κατηγορία είναι έχει να κάνει με τη διαχείριση του ελέγχου πρόσβασης στις εφαρμογές του κεντρικού υπολογιστή, του δικτύου και της διαχείρισης των εφαρμογών που ανήκουν και διοικούνται από την CSP ενώ η δεύτερη έχει να κάνει με τη διαχείριση ελέγχου πρόσβασης στον εικονικό (virtual) server, στην εικονική αποθήκευση, στα εικονικά δίκτυα και στις εφαρμογές που φιλοξενούνται από τους εικονικούς servers[6].

4.3. Security ως cloud υπηρεσία

Στο κεφάλαιο αυτό θα ασχοληθούμε με την security-as-a-service δηλαδή την ασφάλεια που παρέχεται μέσω του cloud. Σε αντίθεση με τα είδη της ασφάλειας που έχουμε συναντήσει μέχρι τώρα, δηλαδή την παροχή ασφάλειας από τους παρόχους Cloud υπηρεσιών αλλά και την παροχή ασφάλειας από τους πελάτες που κάνουν χρήση του Νέφους, η security-as-a-service παρέχεται ως υπηρεσία του Cloud.

Στο μοντέλο SaaS υπάρχουν δύο τύποι παρόχου. Ο πρώτος περιλαμβάνει εγκατεστημένες πληροφορίες ασφάλειας των παρόχων οι οποίοι αλλάζουν τις μεθόδους παράδοσής τους για να συμπεριλάβουν τις υπηρεσίες που παραδίδονται μέσω του Cloud. Ο δεύτερος τύπος περιλαμβάνει τις start-up πληροφορίες των εταιρειών ασφάλειας που εμφανίζονται επίσης σε αυτό το τομέα ως καθαρές, παίζοντας με τα CSPs. Αυτό σημαίνει ότι οι συγκεκριμένες εταιρείες δεν παρέχουν την παραδοσιακή ασφάλεια των πληροφοριών client/server στο δίκτυο, στους hosts και από ή προς τις εφαρμογές αλλά παρέχουν ασφάλεια μόνο ως υπηρεσία cloud.

Οι εταιρίες που παρέχουν προγράμματα antimalware είναι αυτές, που εκτός των καθιερωμένων εταιριών ασφάλειας της πληροφορίας, αλλάζουν τα επιχειρηματικά τους μοντέλα με σκοπό να συμπεριληφθεί και το μοντέλο SaaS. Παρόλα αυτά θα πρέπει να αναφέρουμε ότι και άλλες εταιρίες οι οποίες παρέχουν ασφάλεια πληροφοριών δραστηριοποιούνται στην παροχή SaaS και ιδιαιτέρως σχετικά με το φιλτράρισμα ηλεκτρονικού ταχυδρομείου (Email Filtering) το οποίο θα αναλύσουμε στη συνέχεια.

4.3.1. Email Filtering

Σε ό, τι αφορά την προστασία του ηλεκτρονικού ταχυδρομείου, το μοντέλο SaaS αναλαμβάνει τον καθαρισμό των phishing emails, του spam, και του κακόβουλου software που τυχόν περιλαμβάνεται σε ένα email όταν αυτό φτάνει στο εισερχόμενο ρεύμα ενός οργανισμού. Αφού το καθαρίσει, το παραδίδει στη συνέχεια «καθαρό» και ασφαλές στον οργανισμό και έτσι έχει εξασφαλίσει ότι το μήνυμα ηλεκτρονικού ταχυδρομείου είναι αποτελεσματικό.

Λόγω του ότι το antimalware τρέχει μέσα στο Cloud και όχι κατευθείαν στο endpoint οι συσκευές των πελατών έχουν καλύτερη απόδοση. Επίσης, εξαιτίας της χρήσης πολλών κινητήρων δίνεται η δυνατότητα μιας πιο ολοκληρωμένης ασφάλειας για τους πελάτες καθώς επίσης μια βελτιωμένη antimalware διαχείριση. Η συγκεκριμένη διαχείριση παρουσιάζει πλεονεκτήματα στις endpoint λύσεις καθώς έχει OS επεξεργαστή. Έτσι μπορεί να διαχειρίζεται κεντρικά μέσω του Cloud αντί να εργάζεται με πολλαπλά συστήματα διαχείρισης, κατά πάσα πιθανότητα από πολλαπλούς antimalware πωλητές.

Το όφελος από αυτή την cleansing-in-the-cloud υπηρεσία είναι πολλαπλό. Καταρχάς, το μειωμένο εύρος ζώνης που χρησιμοποιεί το ηλεκτρονικό ταχυδρομείο, στη συνέχεια ο μειωμένος φόρτος των email servers των οργανισμών και τέλος η βελτιωμένη αποτελεσματικότητα των antimalware προσπαθειών των οργανισμών.

Πολλοί οργανισμοί επιθυμούν να διασφαλίσουν ότι δε θα στέλνουν ακουσίως μολυσμένα emails. Γι αυτό το λόγο κάποιο πάροχοι SaaS που αφορούν email χρησιμοποιούνται και φια τα εξερχόμενα emails παρόλο που οι περισσότεροι επικεντρώνονται στα εισερχόμενα. Με αυτό τον τρόπο επιτυγχάνεται μια αρκετά καλή πρόληψη των προβλημάτων που δημιουργούνται από την ακούσια αποστολή malware emails.

Επιπλέον, μπορεί να επιτύχει την ενίσχυση των οργανωτικών πολιτικών γύρω από την κρυπτογράφηση του ηλεκτρονικού ταχυδρομείου της οποίας η εκτέλεση γίνεται γενικά στο server-to-server επίπεδο έτσι ώστε οι μοναδικές ενέργειες του κάθε χρήστη και το κλειδί διαχείρισης να μην είναι υποχρεωτικά. Αυτό μπορεί να επιτευχθεί στο στρώμα μεταφορών με τη χρήση είτε Secure Sockets Layer(SSL) ή Transport Layer Security(TLS) στο δίκτυο επικοινωνιών.

Είναι επίσης χρήσιμο να αναφερθεί η συλλογική νοημοσύνη η οποία αποκτάται από την προβολή του συνόλου των malware απειλών για όλες τις παραμέτρους σε μια επιχείρηση. Αυτές οι παράμετροι αφορούν κάθε είδος (π.χ., server, desktop, laptop, ή κινητή συσκευή), θέση, λειτουργικό σύστημα ή αρχιτεκτονική του επεξεργαστή.

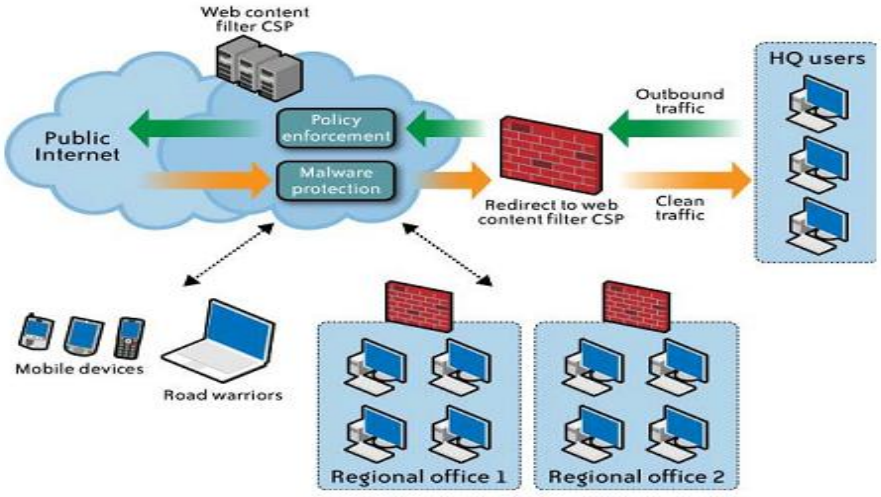
Τέλος, αξίζει να σημειωθεί ότι το SaaS περιλαμβάνει επίσης email backup και αρχειοθέτηση για το ηλεκτρονικό ταχυδρομείο. Ο κεντρικός χώρος αποθήκευσης τον οποίο χρησιμοποιεί η υπηρεσία για την αποθήκευση και εύρεση των μηνυμάτων ενός οργανισμού, επιτρέπει σε έναν οργανισμό να αναζητά τα μηνύματα ηλεκτρονικού ταχυδρομείου με βάση μια σειρά παραμέτρων, συμπεριλαμβανομένου του εύρους, της ημερομηνίας, του αποδέκτη, του αποστολέα, του θέματος καθώς και του περιεχομένου. Οι δυνατότητες αυτές είναι ιδιαίτερα χρήσιμες για σκοπούς e-discovery, οι οποίοι χωρίς αυτές μπορούν να είναι εξαιρετικά δαπανηροί.

4.3.2. Φιλτράρισμα WEB περιεχομένου

Αν τα τελικά σημεία (endpoints) ανήκουν σε μια οργάνωση προσπαθούμε να ανακτήσουμε την ιστοσελίδα της κυκλοφορίας, έτσι η κυκλοφορία εκτρέπεται σε έναν πάροχο SaaS ο οποίος σαρώνει για απειλές malware. Με τον τρόπο αυτό διασφαλίζει την πληροφορία ως προς την καθαρότητά της ότι οι χρήστες θα παραλάβουν μόνο καθαρή κυκλοφορία.

Η ενίσχυση των πολιτικών των οργανισμών μπορεί επίσης να πραγματοποιηθεί με το να επιτρέπουν, μπλοκάρουν ή κάνουν throttle την κυκλοφορία. Η χρήση του εύρους ζώνης για την εν λόγω κίνηση μειώνεται. Εξαιτίας της αύξησης στον αριθμό των δικτυακών τόπων που είναι προσβάσιμοι σήμερα, αναπτύχθηκαν στις εγκαταστάσεις των οργανισμών λύσεις φιλτραρίσματος URL προκειμένου να έχουν καλύτερο αποτέλεσμα.

Το φιλτράρισμα URL συμπληρώνεται με την εξέταση των Hypertext Transfer Protocol (HTTP) πληροφοριών, τις ενσωματωμένες συνδέσεις καθώς επίσης και το περιεχόμενο της σελίδας προκειμένου το περιεχόμενο της ιστοσελίδας να κατανοηθεί καλύτερα. Τέλος, η ακρίβεια του φιλτραρίσματος ενισχύεται λόγω του ότι οι υπηρεσίες χρησιμοποιούν ένα συλλογικό βαθμολογικό σύστημα.



Σχήμα 4.5 Απεικόνιση συστήματος

Πηγη http://digilib.lib.unipi.gr/dspace/bitstream/unipi/5295/1/Sofikitis.pdf

4.3.3. Διαχείριση ευπάθειας (vulnerability management)

Ο σχεδιασμός της διαχείρισης ευπάθειας είναι μια ολοκληρωμένη προσέγγιση για την ανάπτυξη ενός συστήματος πρακτικών και διαδικασιών που αποσκοπούν στον εντοπισμό, την ανάλυση και την αντιμετώπιση ελαττωμάτων στο υλικό ή το λογισμικό που θα μπορούσαν να αποτελέσουν φορείς μιας επίθεσης. Ένα θέμα ευπάθειας, επίσης γνωστό ως μια τρύπα ασφάλειας (a Security hole), είναι ένα αδύναμο σημείο του συστήματος που ένας εισβολέας θα μπορούσε να εκμεταλλευτεί για να αποκτήσει πρόσβαση σε πόρους του συστήματος για την κλοπή δεδομένων ή για άλλους δόλιους σκοπούς. Τα βασικά στοιχεία της διαχείρισης ευπάθειας περιλαμβάνουν την ανίχνευση, αξιολόγηση και αποκατάσταση αυτών των τρωτών σημείων. Μέθοδοι ανίχνευσης, όπως σάρωση ευπάθειας;, δοκιμές διείσδυσης και το Google hacking, μπορούν να βοηθήσουν στην εξεύρεση πιθανών φορέων επίθεσης.

4.3.4. Identity Management - As - a - Service

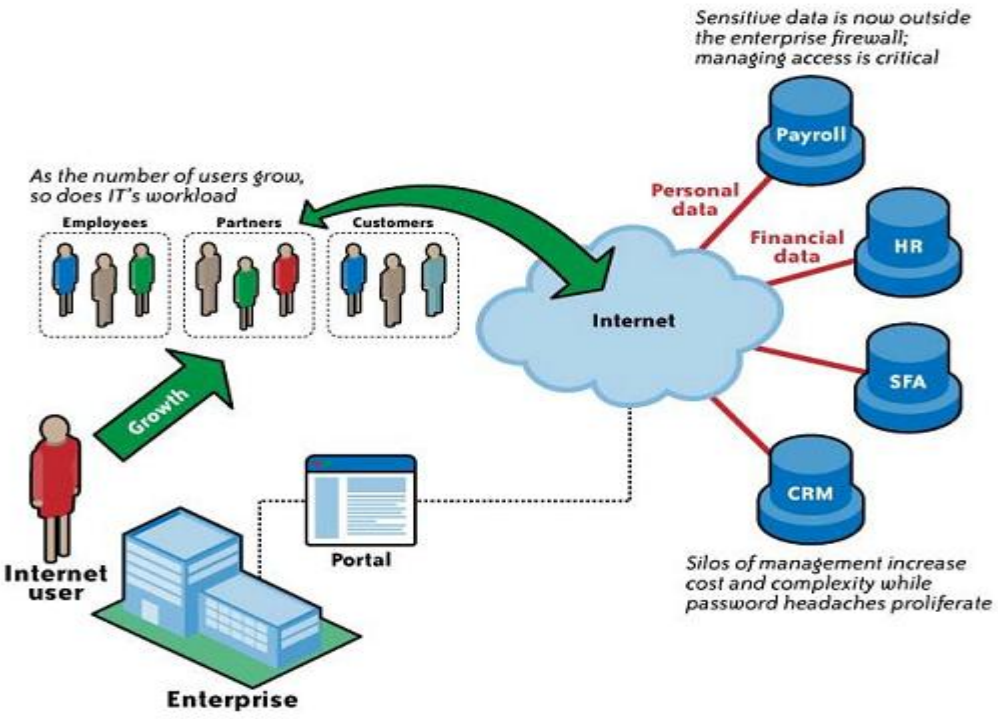
Η Identity-as-Service ("IDaaS") είναι μια Cloud-based υπηρεσία που παρέχει μια σειρά από λειτουργίες διαχείρισης ταυτότητας και πρόσβασης σε συστήματα

προορισμού στις εγκαταστάσεις των πελατών ή / και στο σύννεφο και η οποία περιλαμβάνει:

- Διαχείριση διοίκησης και ταυτοτήτων (IGA) - αυτό περιλαμβάνει την ικανότητα να προβλέψει ταυτότητες οι οποίες υπάρχουν στην υπηρεσία με στόχο κάποια εφαρμογή.

- Πρόσβαση - αυτό περιλαμβάνει την ταυτοποίηση του χρήστη, single sign-on (SSO), και την εκτέλεση της άδειας.

- Ευφυΐα - αυτό περιλαμβάνει καταγραφή συμβάντων και την παροχή πληροφόρησης που μπορεί να απαντήσει σε ερωτήματα όπως «ποιος έχει πρόσβαση τι και πότε;"



Σχήμα 4.6: IDaaS και δυνατότητες

Πηγή http://mrbool.com/saas-security-as-a-service-in-cloud-computing/29995

4.4. Chinese Wall Security Access Control in Cloud computing

Το cloud computing μετατοπίζει τη θέση της υπολογιστικής υποδομής του δικτύου και την αντιμετωπίζει ως υπηρεσία. Αυτό επιτρέπει να ενισχυθεί η συνεργασία, η ευκινησία και η διαθεσιμότητα και επιτρέπει στις εταιρείες να διαχειριστεί τους πόρους της, σύμφωνα με τις απαιτήσεις της. Παρέχει λοιπόν στους χρήστες τη δυνατότητα επέκτασης πόρων σύμφωνα με το μοντέλο pay-as-you με σχετικά χαμηλό κόστος. Δεδομένου ότι ένας πάροχος υπηρεσιών μπορεί να έχει πρόσβαση σε πολλαπλές εικονικές μηχανές cloud όπου είναι αποθηκευμένα τα δεδομένα διαφόρων πελατών, μια μη ασφαλής ροή πληροφοριών που μπορεί να συμβεί αποτελεί ένα από τα μειονεκτήματα της λύσης cloud. Η πολιτική Chinese Wall Security Access Policy (CWSAP) εφαρμόζει περιορισμούς στην πρόσβαση στις πληροφορίες μεταξύ υποκειμένων και αντικειμένων που θα μπορούσαν να δημιουργήσουν μια σύγκρουση συμφερόντων

Ένα υποκείμενο σε ένα σύννεφο που εφαρμόζει CWSA είναι ένας χρήστης που έχει πρόσβαση στις υπηρεσίες ή τα δεδομένα που φιλοξενούνται στο σύννεφο. Ένα αντικείμενο είναι η υπηρεσία του σύννεφου που εγγυάται την πρόσβαση στη ροή των πληροφοριών. Κάθε αντικείμενο που ανήκει στην ίδια ομάδα ασφαλείας ανήκει στην ίδια κατηγορία Σύγκρουσης ενδιαφέροντος Conflict Of Interest (COI). Κάθε αντικείμενο που ανήκει σε διαφορετικές κατηγορίες COI ανήκει σε διαφορετικές ομάδες ασφαλείας. Μια λειτουργία πρόσβασης περιλαμβάνει την ικανότητα να διαβάζει και να γράφει δεδομένα χρησιμοποιώντας τις υπηρεσίες που φιλοξενείται στο νέφος από ένα υποκείμενο. Οι σχέσεις υποκειμένου προς αντικείμενο μπορεί να είναι «πολλοί για πολλούς», «ένας προς ένα» ή «ένας προς πολλούς».

Η ετερογένεια των υπηρεσιών που προσφέρονται από το σύννεφο απαιτούν ένα μηχανισμό ελέγχου πρόσβασης που να αποτρέπει τη μη εξουσιοδοτημένη χρήση των πόρων και των υπηρεσιών cloud. Η Chinese Wall Security Access Policy που προτάθηκε από τους Newer and Nash εξασφαλίζει ότι καμία πληροφορία δεν μπορεί να ρέει μεταξύ υποκειμένου και αντικειμένων η οποία θα μπορούσε να δημιουργήσει

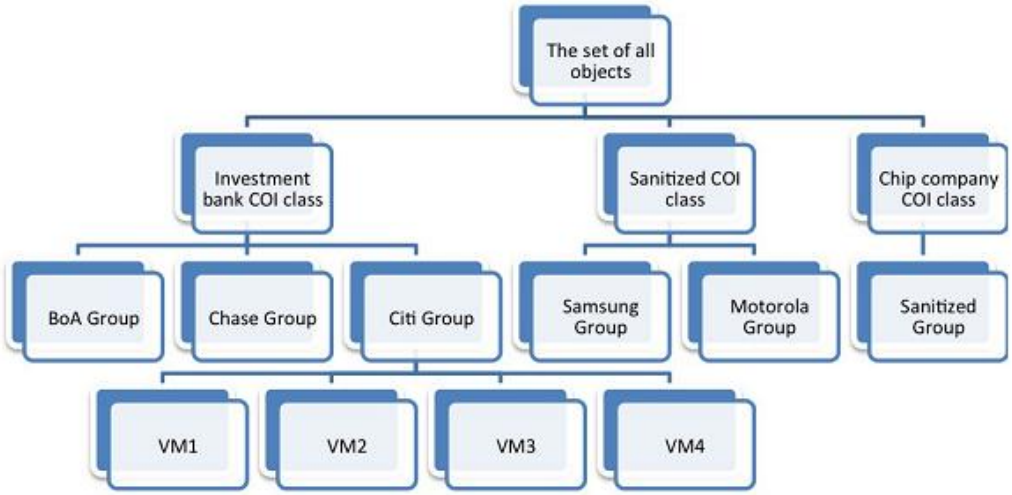
μια σύγκρουση συμφερόντων (COI). Μια cloud μηχανή αποθήκευσης αποθηκεύει και επεξεργάζεται ευαίσθητες πληροφορίες. Πολιτικές για τον καθορισμό της πρόσβαση στις εικονικές μηχανές στο σύννεφο πρέπει να υπάρχουν για την αποφυγή διαρροής πληροφοριών. Η εφαρμογή της CWSAP σε μοντέλο IaaS για παράδειγμα αποτρέπει αυτήν την διαρροή πληροφοριών.

Ας θεωρήσουμε έναν πελάτη ο οποίος ελέγχει τις εικονικές μηχανές όπου υπάρχουν ευαίσθητες πληροφορίες. Μια εταιρεία συμβούλων που συνεργάζεται με τους πελάτες, θα πρέπει να έχει πρόσβαση σε αυτές τις εικονικές μηχανές όπου υπάρχουν αυτά τα ευαίσθητα δεδομένα. Κάθε εικονική μηχανή που ο σύμβουλος θα έχει πρόσβαση συνδέεται με το όνομα του συνόλου δεδομένων της εταιρείας και την κατηγορία COI στην οποία ανήκουν τα αντικείμενα. Το υποκείμενο είναι ο σύμβουλος του συστήματος που προσπαθεί να αποκτήσει πρόσβαση στο αντικείμενο. Αν η απόφαση δεν απαιτεί παραβίαση της CWSAP τότε παρέχεται πρόσβαση στη VM. Εάν η απόφαση απαιτεί παραβίαση των κανόνων της CWSAP τότε δεν παρέχεται πρόσβαση. Εδώ το αντικείμενο είναι μια εικονική μηχανή που κατέχει τα οικονομικά έγγραφα που περιέχουν ευαίσθητες πληροφορίες σχετικά με την κάθε εταιρεία.

Το αντικείμενο έχει τις ακόλουθες ιδιότητες:

• Κάθε αντικείμενο έχει μία σχέση τύπου «πολλοί προς ένα» στο σύννεφο μεταξύ των ομάδων ασφαλείας που έχουν πρόσβαση στο αντικείμενο.

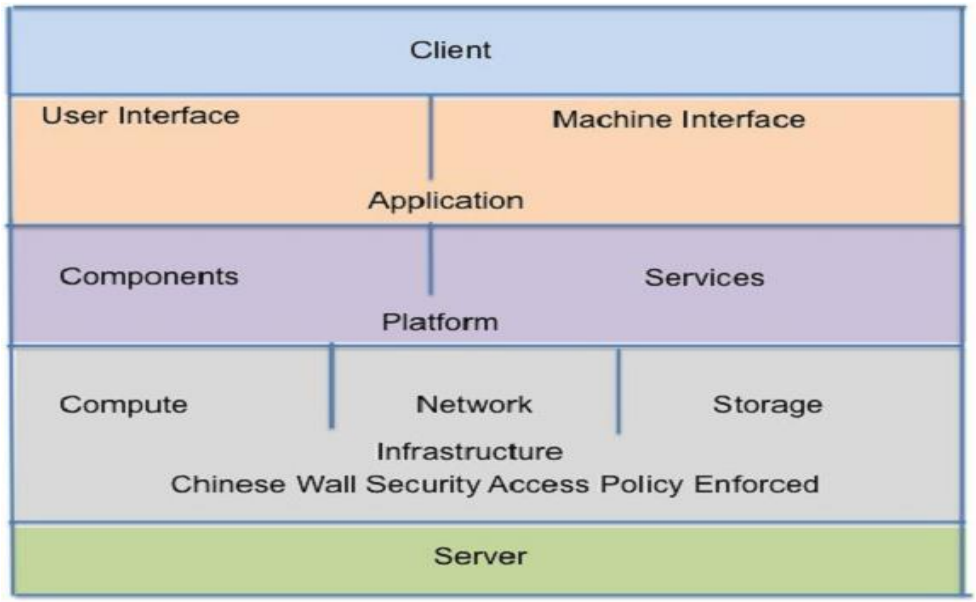
• Κάθε ομάδα ασφαλείας σε ένα σύννεφο έχει σχέση «πολλοί προς ένα» μεταξύ της ομάδας ασφαλείας και της κατηγορίας Σύγκρουση συμφερόντων (COI).



Σχήμα 4.7: Η σύνθεση των αντικειμένων σε περιβάλλον cloud.

Πηγή http://www.teilar.gr/dbData/ProfAnn/profann-1c85fbaa.pdf

Το υποκείμενο είναι ένας σύμβουλος που προσπαθεί να έχει πρόσβαση σε εικονικές μηχανές (ή αντικείμενα). Κάθε υποκείμενο έχει πρόσβαση σε όλα τα αντικείμενα στην ίδια ομάδα ασφαλείας. Ένα υποκείμενο έχει επίσης πρόσβαση σε αντικείμενα που ανήκουν σε διαφορετικές κατηγορίες COI. Κάθε αντικείμενο στην κοινή ομάδα ασφαλείας είναι προσβάσιμο σε όλους τους χρήστες. Αυτά τα αντικείμενα είναι προσιτά σε όλες τις ομάδες ασφαλείας. Τα αντικείμενα που ανήκουν στην ομάδα αυτή συνήθως παρέχουν υπηρεσίες κοινής ωφέλειας. Τα αντικείμενα επίσης που ανήκουν στη ομάδα αυτή δεν θα αποθηκεύουν πληροφορίες που αφορούν τους πελάτες.



Σχήμα 4.8: Υπολογισμός στοίβας σε cloud περιβάλλον.

Πηγή http://www.teilar.gr/dbData/ProfAnn/profann-1c85fbaa.pdf

Μια τροποποίηση της Chinese Wall Security Access Policy (CWSAP) προτάθηκε από τους Atluri, Chun, και Mazzoleni. Η λύση αυτή προσφέρει ένα αποκεντρωμένο περιβάλλον ροής εργασίας. Εάν περιέχονται ευαίσθητες πληροφορίες μέσα στο αντικείμενο τότε παράγεται μια διχοτόμηση περιορισμού από τον αλγόριθμο. Οι κανόνες για την πρόσβαση στη διαδικασία ανάγνωσης και γραφής επιβάλλονται από αυτή την περιοριστική στεγανοποίηση.

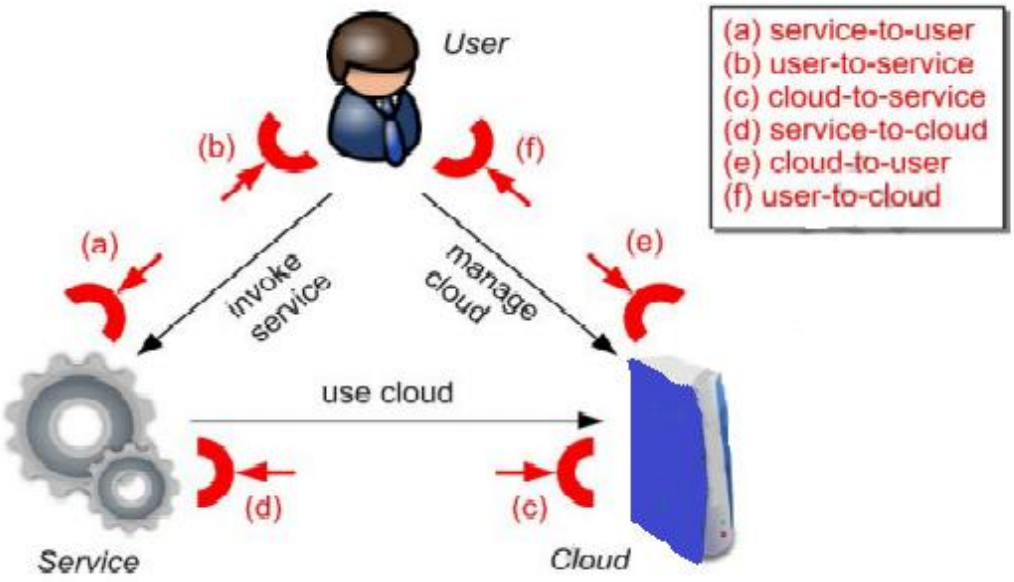
Αυτή η λύση δεν μπορεί να κλιμακωθεί για να υποστηρίξει ένα σύννεφο καθώς αυτή η προσέγγιση είναι εξαρτάται από την εφαρμογή και δεν μπορεί να εφαρμοστεί ως μια λύση στο επίπεδο υποδομής. Μια άλλη λύση που εφαρμόζει Chinese Wall Security Access Policy (CWSAP) σε κατανεμημένο περιβάλλον αποδίδεται στο Minsky και επιλύει τους περιορισμούς της συγκεντρωτικής επιβολής πολιτικών πρόσβασης και προσφέρει μια επεκτάσιμη λύση στο εγγενώς αποκεντρωμένο μηχανισμό LGI (Lawgoverned Interaction)

Το κόστος από την εφαρμογή αυτής της λύσης θα περιόριζε τα οφέλη της λειτουργίας σε cloud περιβάλλον από. Μια άλλη λύση που προσφέρεται από τον Ruoyu Wu εφαρμόζει την Chinese Wall Security Access Policy (CWSAP) σε κατανεμημένο περιβάλλον για τον έλεγχο της ροής πληροφοριών. Η προσέγγιση αυτή επιβάλλει, επίσης, την εφαρμογή πολιτικών σε επίπεδο υποδομή. Η λύση αυτή όμως δεν αντιμετωπίζει καταστάσεις όταν οι ιδιοκτήτες απελευθερώνονται από τα καθήκοντά τους επί των αντικείμενων. Αυτή η προσέγγιση επιλύει επίσης ζητήματα COI για τους παρόχους υπηρεσιών και εμποδίζει τη διαρροή πληροφοριών[5],[2].

ΚΕΦΑΛΑΙΟ 5: ΕΠΙΘΕΣΕΙΣ ΣΕ CLOUD

5.1. Ταξινόμηση επιθέσεων στο υπολογιστικό νέφος

Ένα σενάριο για το cloud computing μπορεί να αναπαρασταθεί χρησιμοποιώντας τρεις διαφορετικές κατηγορίες συμμετεχόντων: τους χρήστες των υπηρεσιών, τις περιπτώσεις υπηρεσιών (ή απλά υπηρεσίες), και τον πάροχο του Νέφους. Κάθε αλληλεπίδραση σε ένα σενάριο του cloud computing μπορεί να απευθύνεται σε δύο οντότητες από αυτές τις κατηγορίες συμμετεχόντων (π.χ. ένας χρήστης ζητά μια υπηρεσία ή μια υπηρεσία ζητά περισσότερη επεξεργαστική ισχύ από το σύστημα υποδομής).



Εικόνα 5.1: Το τρίγωνο του Υπολογιστικού Νέφους

Πηγή http://digilib.lib.unipi.gr/dspace/bitstream/unipi/6241/1/Aslanis%20-%20Vasileiou.pdf

Κατά τον ίδιο τρόπο, κάθε απόπειρα επίθεσης στο σενάριο αυτό του Cloud Computing μπορεί να αναλυθεί σε ένα σύνολο αλληλεπιδράσεων μέσα σε αυτό το μοντέλο των 3 κλάσεων - κατηγοριών. Για παράδειγμα, μεταξύ ενός χρήστη και μιας υπηρεσίας κάποιος έχει το ίδιο σετ των «διανυσμάτων» - φορέων της επίθεσης που υπάρχουν έξω από το σενάριο του υπολογιστικού νέφους (π.χ. επίθεση με δηλητηρίαση SQL κώδικα, επιθέσεις πλημμύρας, ...).

Ως εκ τούτου, το να μιλάμε για την ασφάλεια του Cloud Computing σημαίνει ουσιαστικά να μιλάμε για τις επιθέσεις με τον πάροχο των Cloud υπηρεσιών ανάμεσα στη λίστα των συμμετεχόντων. Αυτό βέβαια δεν σημαίνει ότι ο πάροχος του νέφους πρέπει να είναι κακόβουλος από μόνος του, αλλά μπορεί επίσης να παίξει έναν ενδιάμεσο ρόλο κατά τη διάρκεια μιας συνδυασμένης επίθεσης.

Για να είμαστε πιο ακριβείς, ο κάθε ένας από τους τρείς ρόλους των συμμετεχόντων παρέχει ένα συγκεκριμένο είδος διεπαφής με την κατηγορία κάθε άλλου συμμετέχοντα. Για παράδειγμα, το Cloud System παρέχει κάθε περίπτωση υπηρεσίας

με μια συγκεκριμένη διεπαφή (API ανάλογα τον τύπο του μοντέλου παροχής υπηρεσιών, IaaS, PaaS, ή SaaS) την οποία η υπηρεσία μπορεί να χρησιμοποιήσει. Κατά τον ίδιο τρόπο, μια υπηρεσία παρέχει τις υπηρεσίες της σε ένα χρήστη με μια ειδική διεπαφή (π.χ. ιστοσελίδα, σύνδεση SSH, υπηρεσία Web, ...). Έτσι, με 3 συμμετέχοντες, υπάρχουν 6 τέτοιες διασυνδέσεις που πρέπει να εξεταστούν.

5.2. Επιφάνειες επιθέσεων

Α) Επίθεση μίας υπηρεσίας προς ένα χρήστη

- επιθέσεις υπερχείλισης - buffer overflow attack

Σε γενικές γραμμές, επίθεση υπερχείλισης συμβαίνει κάθε φορά που το πρόγραμμα γράφει περισσότερες πληροφορίες στο buffer από το χώρο που έχει διατεθεί από τη μνήμη. Αυτό επιτρέπει σε έναν εισβολέα να αντικαταστήσει τα δεδομένα που ελέγχουν την πορεία εκτέλεσης του προγράμματος και να παραβιάσουν τον έλεγχο του προγράμματος προκειμένου να εκτελεστεί ο κώδικας του εισβολέα αντί του κώδικα που πρέπει να εκτελεστεί για τη σωστή λειτουργία των διαδικασιών.
Μια επίθεση υπερχείλισης συμβαίνει όταν περισσότερα δεδομένα εγγράφονται σε ένα buffer από όσα μπορεί να χωρέσει. Η περίσσεια δεδομένων γράφεται στη adjacent memory, αντικαθιστώντας τα περιεχόμενα της εν λόγω θέσης και προκαλώντας απρόβλεπτα αποτελέσματα σε ένα πρόγραμμα. Υπερχειλίσεις μνήμης συμβαίνουν όταν υπάρχει ακατάλληλη επιβεβαίωση και θεωρείται σφάλμα ή αδυναμία στο λογισμικό.

Οι attackers μπορούν να εκμεταλλευτούν το σφάλμα από μια υπερχείλιση του buffer και να εισάγουν κώδικα που είναι ειδικά σχεδιασμένος για να προκαλέσει buffer overflow με το αρχικό μέρος ενός συνόλου δεδομένων, και στη συνέχεια, γράφοντας το υπόλοιπο των δεδομένων στη γειτονική διεύθυνση μνήμης του buffer που έχει υπερχειλίσει. Τα δεδομένα που έχουν υπερχειλίσει μπορεί να περιέχουν εκτελέσιμο κώδικα που επιτρέπει στους attackers να τρέξουν μεγαλύτερα και πιο εξελιγμένα προγράμματα ή να χορηγούν στους εαυτούς τους πρόσβαση στο σύστημα

Οι επιθέσεις υπερχείλισης είναι ένα από τα χειρότερα σφάλματα που μπορούν να αξιοποιηθούν από έναν εισβολέα κυρίως επειδή είναι πολύ δύσκολο να τις εντοπίσουμε και να τις διορθώσουμε, ειδικά αν το λογισμικό αποτελείται από εκατομμύρια γραμμές κώδικα. Επιπλέον οι διορθώσεις για αυτά τα σφάλματα είναι αρκετά πολύπλοκες και επιρρεπείς σε λάθη. Αυτός είναι ο λόγος για τον οποίο είναι πραγματικά σχεδόν αδύνατο να αφαιρεθεί αυτό το είδος του σφάλματος εντελώς. Αν και όλοι οι προγραμματιστές γνωρίζουν τα πολύ σοβαρά προβλήματα από την επίθεση υπερχείλισης στα προγράμματά τους, εξακολουθούν να υπάρχουν πολλά σφάλματα που σχετίζονται με τις απειλές αυτού του είδους της επίθεσης τόσο σε νέο και όσο και σε παλιό λογισμικό, ανεξάρτητα από τον αριθμό των ενημερώσεων κώδικα που έχουν ήδη διενεργηθεί.

- επίθεση με δηλητηρίαση SQL κώδικα – sql injection

Μια επίθεση με δηλητηρίαση SQL είναι μια επίθεση υπολογιστή στον οποίο κακόβουλος κώδικας είναι ενσωματωμένος σε μια κακώς σχεδιασμένη εφαρμογή και στη συνέχεια περνάει στη βάση δεδομένων. Τα κακόβουλα δεδομένα στη συνέχεια παράγουν αποτελέσματα επερωτήσεων ή ενέργειες που δεν πρέπει ποτέ να έχουν εκτελεστεί. Παρακάτω παρουσιάζεται ένα παράδειγμα επίθεσης με δηλητηρίαση SQL κώδικα σε εφαρμογή προκειμένου να καταλάβουμε τον τρόπο με τον οποίο λειτουργεί:

Μια εφαρμογή που τρέχει λειτουργίες μιας τράπεζας περιέχει μενού που μπορεί να χρησιμοποιηθεί για να ψάξει τα στοιχεία των πελατών που χρησιμοποιούν σημεία δεδομένων, όπως ο αριθμός κοινωνικής ασφάλισης του πελάτη. Στο background η εφαρμογή καλεί ένα SQL query που εκτελείται στη βάση δεδομένων περνώντας τις εισερχόμενες τιμές αναζήτησης ως εξής:

SELECT client_name, telephone, address, date_of_birth WHERE social_sec_no=23425

Σε αυτό το δείγμα script, ο χρήστης εισάγει την τιμή 23425 στο παράθυρο μενού της εφαρμογής, ζητώντας από το χρήστη να πληκτρολογήσει τον αριθμό Κοινωνικής

Ασφάλισης. Στη συνέχεια, χρησιμοποιώντας την τιμή που δόθηκε από το χρήστη, ένα ερώτημα SQL εκτελείται στη βάση δεδομένων. Ένας χρήστης με γνώσεις SQL μπορεί να καταλάβει την εφαρμογή και, αντί να εισάγει μια μοναδική τιμή όταν ερωτηθεί για τον αριθμό Κοινωνικής Ασφάλισης, να εισάγει τη συμβολοσειρά "23.425 ή 1 = 1," η οποία περνάει στη βάση δεδομένων ως εξής:

SELECT client_name, telephone, address, date_of_birth WHERE social_sec_no=23425 or 1=1

Το clause WHERE είναι σημαντικό, διότι εισάγει την ευπάθεια. Σε μια βάση δεδομένων, η συνθήκη 1 = 1 είναι πάντα αληθής και επειδή το ερώτημα έχει οριστεί να επιστρέψει πελάτη Κοινωνικής Ασφάλισης με αριθμό (23425) ή όπου 1 = 1, το ερώτημα θα επιστρέψει όλες τις γραμμές του πίνακα που όμως δεν ήταν η αρχική πρόθεση.

Η παραπάνω επίθεση με δηλητηρίαση SQL κώδικα αποτελεί ένα απλό παράδειγμα, αλλά δείχνει τον τρόπο με τον οποίο μπορεί να εκμεταλλευτεί κανείς ένα τρωτό σημείο προκειμένου να ξεγελάσει μια εφαρμογή, στη συγκεκριμένη περίπτωση ώστε να τρέξει ένα ερώτημα βάσης δεδομένων ή μια εντολή.

Οι επιθέσεις με δηλητηρίαση SQL κώδικα μπορούν να μετριαστούν με τη διασφάλιση της ορθού σχεδιασμού της εφαρμογής, ιδιαίτερα στις ενότητες που απαιτούν είσοδο από το χρήστη για την εκτέλεση ερωτημάτων βάσης δεδομένων ή εντολών. Στο παραπάνω παράδειγμα, η εφαρμογή θα μπορούσε να αλλάξει έτσι ώστε να δέχεται μία μόνο αριθμητική τιμή.

- κλιμάκωση προνομίων

Μια επίθεση κλιμάκωσης προνομίων είναι ένας τύπος διείσδυσης δικτύου που εκμεταλλεύεται σφάλματα προγραμματισμού ή σχεδιασμού με σκοπό τη χορήγησης στον εισβολέα αυξημένης πρόσβασης στο δίκτυο και τα σχετικά δεδομένα και εφαρμογές. Αρχικά τα περισσότερα συστήματα δεν παρέχουν σε ένα μη εξουσιοδοτημένο χρήστη πλήρη πρόσβαση στο σύστημα. Υπό τις συνθήκες αυτές

απαιτείται κλιμάκωση προνομίων. Υπάρχουν δύο είδη κλιμακώσεων προνομίων: η κάθετη και η οριζόντια:

Στην κάθετη κλιμάκωση προνομίων ο εισβολέας απαιτεί να χορηγήσει στον εαυτό του υψηλότερα δικαιώματα. Αυτό συνήθως επιτυγχάνεται με την εκτέλεση εργασιών επιπέδου πυρήνα που επιτρέπουν στον εισβολέα να εκτελέσει μη εξουσιοδοτημένο κώδικα.

Στην οριζόντια κλιμάκωση προνομίων ο εισβολέας απαιτεί να χρησιμοποιούν το ίδιο επίπεδο προνομίων που του έχει ήδη χορηγηθεί, αλλά να αναλάβει την ταυτότητα ενός άλλου χρήστη με παρόμοια προνόμια. Για παράδειγμα, κάποιος που αποκτά πρόσβαση στον τραπεζικό λογαριασμό ενός άλλου ατόμου αποτελεί παράδειγμα οριζόντιας κλιμάκωσης προνομίων.

Β) Επίθεση χρήστη προς μία υπηρεσία

- επιθέσεις μέσω σελιδοδεικτών για τύπου HTML υπηρεσίες

Αφορά επιθέσεις μέσω δέσμης ενεργειών από άλλη τοποθεσία με σκοπό τη προσθήκη κώδικα δέσμης ενεργειών από μια τοποθεσία Web σε άλλη

- παραπλάνηση SSL Πιστοποιητικού

Τα SSL πιστοποιητικά χρησιμοποιούνται για να διασφαλίσουν ασφαλείς κρυπτογραφημένες συνδέσεις στο Internet συνδέοντας την ταυτότητα ενός οργανισμού, για παράδειγμα μια τράπεζα, με το κατάλληλο domain name, με το όνομα του διακομιστή, ή το όνομα του κεντρικού υπολογιστή. Η παραπλάνηση αφορά την προσπάθεια των χρηστών μίας ιστοσελίδας προκειμένου να ανασχετήσει τα δεδομένα που έχει στείλει ο χρήστης στο διακομιστή μέσω της χρήσης προβληματικού πιστοποιητικού ασφαλείας στη τοποθεσία Web.

- επιθέσεις στη κρυφή μνήμη των προγραμμάτων περιήγησης

Ο στόχος του εισβολέα είναι να αντικαταστήσει ένα κομμάτι του JavaScript στην κρυφή μνήμη του προγράμματος περιήγησης του θύματος με ένα κομμάτι με κακόβουλο περιεχόμενο. Ειδικότερα, ο εισβολέας προσπαθεί να μεγιστοποιήσει το χρόνο μέχρις ότου το θύμα επικυρώσει το κακόβουλο κομμάτι της κρυφής μνήμης και να αποφεύγει τις αποτυχίες Ο χρήστης μπορεί λοιπόν να δώσει τη συγκατάθεση του για την εγκατάσταση πρόσθετων προγραμμάτων στην εφαρμογή περιήγησης. Ένα τέτοιο κακόβουλο πρόγραμμα προσθέτει κρυφά αρχεία στη μνήμη της εφαρμογής περιήγησης με σκοπό την ανάσχεση δεδομένων του χρήστη.

- επιθέσεις (Phishing) πελατών ηλεκτρονικού ταχυδρομείου

Το phishing είναι μια μέθοδος απάτης μέσω e-mail στο οποίο ο δράστης στέλνει φαινομενικά νόμιμα email σε μια προσπάθεια να συγκεντρώσει προσωπικές και οικονομικές πληροφορίες από τους αποδέκτες. Συνήθως, τα μηνύματα φαίνεται να προέρχονται από γνωστούς και αξιόπιστους δικτυακούς τόπους. Web sites που συχνά πλαστογραφούνται από phishers είναι μεταξύ άλλων η PayPal, eBay, το MSN, Yahoo, BestBuy, και η America Online. Μια αποστολή phishing είναι μια κερδοσκοπική επιχείρηση: ο phisher βάζει το δέλεαρ ελπίζοντας να ξεγελάσει τουλάχιστον μερικά από τα υποψήφια θύματα. Οι pphishers χρησιμοποιούν πολλών ειδών τεχνάσματα social engineering και e-mail spoofing για να προσπαθήσουν να ξεγελάσουν τα θύματά τους. Ο σκοπός τους είναι η εξαπάτηση και η λήψη ευαίσθητων προσωπικών δεδομένων από τους χρήστες.

Γ) Επίθεση μίας υπηρεσίας προς την υποδομή του Υπολογιστικού Νέφους

- επιθέσεις εξάντλησης πόρων με συνεχή αιτήματα προς τον πάροχο για περισσότερους πόρους μέχρι να επιτευχθεί άρνηση της υπηρεσίας (Denial-of-Service)

Οι επιθέσεις άρνησης υπηρεσίας είναι μια παλιά διακοπή των online υπηρεσιών, αλλά εξακολουθούν να αποτελούν απειλή, ακόμη και σήμερα. Η επίθεση από εκατοντάδες χιλιάδες ή εκατομμύρια ταυτόχρονα αυτόματα αιτήματα για μια υπηρεσία, πρέπει να

ανιχνευθούν και να ελεγχθούν πριν δεσμευτούν λειτουργίες. Όμως, οι εισβολείς έχουν αναπτύξει αυτοσχέδιους και όλο και περισσότερο εξελιγμένους τρόπους να διεξάγουν την επίθεση, γεγονός που καθιστά δυσκολότερη την ανίχνευση των κομματιών της εισερχόμενης κυκλοφορίας τα οποία είναι κακόβουλα και το διαχωρισμό τους από τους νόμιμους χρήστες.

Για τους πελάτες των cloud υπηρεσιών, «το να βιώσουν μια επίθεση denial-of-service είναι σαν να πιάστηκαν σε ώρα αιχμής σε αδιέξοδο κυκλοφορίας: δεν υπάρχει κανένας τρόπος για να φτάσουν στον προορισμό τους, και τίποτα που μπορούν να κάνουν γι 'αυτό, εκτός από το να καθίσουν και να περιμένουν" σύμφωνα με τις σχετικές εκθέσεις . Όταν μια άρνηση των υπηρεσιών επιτίθεται σε μια υπηρεσία του πελάτη στο σύννεφο, αυτό μπορεί να επηρεάσει την υπηρεσία, χωρίς όμως να την κλείσει. Σε αυτή την περίπτωση ο πελάτης θα χρεωθεί από την υπηρεσία του νέφους του για όλους τους πόρους που καταναλώνονται κατά τη διάρκεια της επίθεσης. Επίμονες επιθέσεις με αποτέλεσμα την άρνησης της υπηρεσίας μπορούν επομένως να αποβούν και πολύ ακριβές για τον πελάτη που θα τις υποστεί.

- επιθέσεις στο υποσύστημα-επόπτη του Υπολογιστικού Νέφους

Το κύριο συστατικό του εικονικού συστήματος είναι ο επόπτης (hypervisor) και είναι υπεύθυνος για την επιβολή απομόνωσης μεταξύ των εικονικών μηχανών και της διαχείριση των πόρων του υλικού. Ο hypervisor είναι το λογισμικό που επιτρέπει πολλαπλά εικονικές μηχανές επισκεπτών να τρέχουν ταυτόχρονα στον ίδιο διακομιστή. Η ασφάλεια του εικονικού περιβάλλοντος είναι σε μεγάλο βαθμό εξαρτώμενη από την ατομική ασφάλεια του κάθε συστατικού, από τον hypervisor και το host λειτουργικό σύστημα μέχρι τα λειτουργικά συστήματα των επισκεπτών, τις εφαρμογές και την αποθήκευση. Ο hypervisor είναι ο κύριος υπεύθυνος ελέγχου για την πρόσβαση εικονικών μηχανών στους φυσικούς πόρους του διακομιστή.

Κάθε συμβιβασμός του hypervisor παραβιάζει την ασφάλεια των εικονικών μηχανών, διότι όλες οι λειτουργίες των εικονικών μηχανών γίνονται εντοπισημες. Παραβίαση της ασφάλειας στο μηχάνημα υποδοχής μπορεί να οδηγήσει σε μεγάλο συμβιβασμό

του συνόλου των υποδομών. Ο εισβολέας μπορεί να εκμεταλλευτεί την ευπάθεια στην εικονική μηχανή. Ο hypervisor είναι το μοναδικό σημείο αποτυχίας. Έτσι, ο hypervisor πρέπει επίσης να παρακολουθεί προσεκτικά για σημεία συμβιβασμού. Η ασφάλεια του hypervisor μπορεί να γίνει στόχος παραβίασης από διάφορες κακόβουλες επιθέσεις.

Δ) Επίθεση της υποδομής του Υπολογιστικού Νέφους προς μία υπηρεσία

- περιορισμό της διαθεσιμότητας (πχ εκτέλεση εντολών τερματισμού της υπηρεσίας)

Ο attacker είναι ικανός να κάνει παρεμβάσεις στις διαχειριστικές εντολές. Είτε είναι εσωτερικός χρήστης ή κακόβουλο πρόγραμμα ο εισβολέας για να έχει φτάσει στο σημείο να μπορεί να το κάνει αυτό σημαίνει ότι έχει αποκτήσει πρόσβαση στη διεπαφή διαχείρισης των υπηρεσιών ή των εφαρμογών των χρηστών.

- παραβίαση της ιδιωτικότητας των δεδομένων που διαχειρίζεται η υπηρεσία

Σε αυτού του είδους την επίθεση ο εισβολέας ο οποίος είναι εσωτερικός χρήστης και ο οποίος έχει διαχειριστικό ρόλο μπορεί να υποκλέψει απόρρητα δεδομένα των χρηστών. Τα δεδομένα αυτά μπορούν να χρησιμοποιηθούν ποικιλοτρόπως όπως για παράδειγμα για σκοπούς marketing. Όπως είναι αυτονόητο τα αποτελέσματα από την κακόβουλη παρεμβολή προς υποκλοπή δεδομένων είναι πολύ άσχημα και έχουν τεράστιες συνέπειες. Το ίδιο ισχύει και για την εκτέλεση παρένθετων λειτουργιών μίας υπηρεσίας.

Ε) Επίθεση της υποδομής του Υπολογιστικού Νέφους προς ένα χρήστη

Το είδος αυτής της επίθεσης αφορά κατά κύριο λόγο το interface που παρέχει το Υπολογιστικό Νέφος στους χρήστες προκειμένου αυτοί να μπορούν να διαχειριστούν τις υπηρεσίες τους. Ο Cloud controller είναι αυτό το interface που επιτρέπει τη προσθήκη νέων υπηρεσιών, αύξηση του ορίου δημιουργίας νέων αντιγράφων

των υπηρεσιών, διαγραφή αντιγράφων. Παρόλα αυτά θα πρέπει να σημειώσουμε ότι αυτός ο τύπος επίθεσης, λόγω του ότι παρεμβαίνει πάντα μια υπηρεσία, δεν είναι εύκολο να διακριθεί.

ΣΤ) Επίθεση ενός χρήστη προς την υποδομή του ΥΝ

Η συγκεκριμένη κατηγορία επιθέσεων μπορεί να συμπεριλαμβάνει απόπειρες τύπου phishing ώστε να προκαλέσουν ένα χρήστη να προχωρήσει σε χρήση υπηρεσιών του παρόχου. Σε γενικές γραμμές, περιλαμβάνει κάθε είδους επίθεση που έχει ως στόχο την εξαπάτηση ενός χρήστη και προέρχεται από το cloud system.

5.3. Επιθέσεις σε πρωτόκολλα

Οι σχεδιαστές web υπηρεσιών προσφέρουν τεράστια ευελιξία, όταν πρόκειται για τη χρησιμοποίηση στοιχείων ακεραιότητας. Συνήθως, προκειμένου να διασφαλιστεί η ακεραιότητα του μηνύματος, ορισμένα προκαθορισμένα μέρη του μηνύματος SOAP υπογράφονται.

Ας υποθέσουμε ότι ένας πελάτης μιας υπηρεσίας web στέλνει ένα υπογεγραμμένο μήνυμα στην υπηρεσία web υποδοχής. Ιδανικά οποιαδήποτε κακόβουλη τροποποίηση των δεδομένων που έχουν υπογραφεί ανιχνεύεται από την υπηρεσία web υποδοχής, εκτός εάν ο εισβολέας είναι σε θέση να σπάσει τον αλγόριθμο υπογραφής από μόνος του. Ωστόσο, κατά την εκτέλεση μιας XML Signature Wrapping επίθεσης ένας εισβολέας είναι σε θέση να αλλάξει το περιεχόμενο του υπογεγραμμένου μέρους, χωρίς να ακυρώσει την υπογραφή. Η επίθεση αυτή είναι επίσης γνωστή ως επίθεση XML Rewriting.

Υποθέτοντας ότι τα δύο μέρη συμφώνησαν εκ των προτέρων σχετικά με το ποια μέρη του μηνύματος SOAP θα υπογραφούν, χωρίς να μας ενδιαφέρει ο τρόπος με τον οποίο πραγματοποιήθηκε αυτή η συμφωνία θα προχωρήσουμε στην ανάλυση αυτών των ειδών των επιθέσεων.

5.3.1. Κατηγορίες επιθέσεων

Υπάρχουν διάφορες επιθέσεις XML Signature Wrapping. Λόγω της πολυπλοκότητας τους, θα αναφέρουμε επιγραμματικά τους διαφορετικούς αυτούς τύπους οι οποίοι είναι:

* XML Signature Wrapping – Απλό Πλαίσιο, το οποίο είναι και το πιο εύκολο να εκτελέσει επίθεση XML Signature Wrapping. Αυτή ήταν και η πρώτη επίθεση XML Signature Wrapping η οποία ανακαλύφθηκε το 2005. Τα υπογεγραμμένα δεδομένα περιέχονται μέσα στο κύριο σώμα του SOAP μηνύματος.

* XML Signature Wrapping - Προαιρετικό στοιχείο. Αποτελεί μια πιο εξελιγμένη επίθεση. Τα υπογεγραμμένα δεδομένα περιέχονται μέσα στην επικεφαλίδα του SOAP μηνύματος.

* XML Signature Wrapping - Προαιρετικό στοιχείο στην επικεφαλίδα Ασφάλειας. Αποτελεί μια πιο εξελιγμένη επίθεση. Τα υπογεγραμμένα δεδομένα περιέχονται μέσα στην επικεφαλίδα Ασφάλειας.

* XML Signature Wrapping - με εισαγωγή χώρου ονομάτων. Αυτή αποτελεί την πιο σύνθετη από όλες τις επιθέσεις Signature Wrapping. Η επίθεση πραγματοποιείται με τη χρησιμοποίηση μιας τεχνικής εισαγωγής ονομάτων XML.

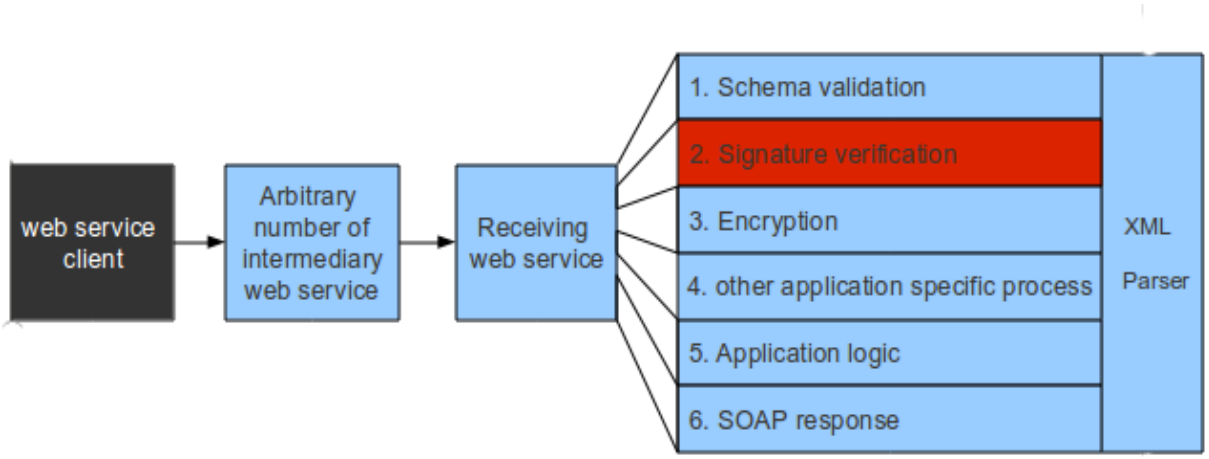
5.3.2. Προαπαιτούμενα για επίθεση

Προκειμένου αυτή η επίθεση να λειτουργήσει ο εισβολέας πρέπει να έχει γνώσεις σχετικά με τα εξής πράγματα:

1. Ο εισβολέας γνωρίζει το καταληκτικό σημείο της διαδικτυακής υπηρεσίας. αλλιώς δεν είναι σε θέση να φθάσει στην υπηρεσία web.

2. Ο εισβολέας γνωρίζει ότι η διαδικτυακή υπηρεσία επεξεργάζεται την κεφαλίδα ασφάλειας και το στοιχείο «υπογραφή». Εάν η υπηρεσία Web δεν «περιμένει» ένα μέρος το οποίο έχει υπογραφεί, απορρίπτει απλά την υπογραφή και η επίθεση δεν λειτουργεί.

3. Ο εισβολέας μπορεί να φτάσει στο καταληκτικό σημείο από τη θέση του. Απαιτείται η πρόσβαση στη διαδικτυακή υπηρεσία στην οποία επιτίθεται. Αν η διαδικτυακή υπηρεσία είναι διαθέσιμη μόνο για τους χρήστες μέσα σε ένα συγκεκριμένο δίκτυο μιας εταιρείας, η επίθεση αυτή είναι περιορισμένη.



- **Κόκκινο = συνιστώσα της web υπηρεσίας που δέχτηκε επίθεση**
- **Μαύρο = τοποθεσία του εισβολέα**
- **Μπλε = συνιστώσα της web υπηρεσίας που δεν εμπλέκεται άμεσα στην επίθεση**

Εικόνα 5.2: Γραφική αναπαράσταση επίθεσης

Πηγή http://www.ws-attacks.org/index.php/XML_Entity_Expansion

5.4. Επιθέσεις στην Ακεραιότητα και Δέσμευση Δεδομένων Υπηρεσιών του Υπολογιστικού Νέφους

- **Επίθεση Ενσωμάτωσης Κακόβουλης Υπηρεσίας σε Εικονική Μηχανή (Cloud Malware Injection)**

Σε μια επίθεση ενσωμάτωσης κακόβουλης υπηρεσίας, ένας αντίπαλος προσπαθεί να εισάγει μια κακόβουλη υπηρεσία ή κώδικα, ο οποίος εμφανίζεται ως μία από τις έγκυρες υπηρεσίες που εκτελείται στο σύννεφο. Αν ο εισβολέας επιτύχει το σκοπό του, τότε η υπηρεσία cloud θα υποφέρει από υποκλοπές.

Αυτό μπορεί να επιτευχθεί μέσω ανεπαίσθητων τροποποιήσεων των δεδομένων προκειμένου να μεταβληθεί η λειτουργία, ή προκαλώντας αδιέξοδα, που αναγκάζουν ένα νόμιμο χρήστη να περιμένει μέχρι την ολοκλήρωση μιας εργασίας που δεν δημιουργήθηκε από τον ίδιο. Εδώ ο εισβολέας παίρνει το προβάδισμα, με την εφαρμογή κακόβουλης υπηρεσίας του κατά τέτοιο τρόπο ώστε να τρέξει σε IaaS ή SaaS των cloud διακομιστών, για παράδειγμα με διαγραφή χρήστη και θέτοντας δικαιώματα administrator. Αυτό το είδος της επίθεσης είναι επίσης γνωστή ως μια επίθεση spoofing μετά-δεδομένων.

Όταν μια υπηρεσία ενός νόμιμου χρήστη είναι έτοιμη να τρέξει στον cloud διακομιστή, τότε η αντίστοιχη υπηρεσία αποδέχεται το την υπηρεσία του νόμιμου χρήστη για τον υπολογισμό της στο σύννεφο. Ο μόνος έλεγχος που γίνεται είναι να καθοριστεί αν η περίπτωση ταιριάζει σε μια νόμιμη υφιστάμενη υπηρεσία. Ωστόσο, η ακεραιότητα της δεν ελέγχεται. Με το να τη διαπεράσουν και να προχωρήσουν στην αναπαραγωγή της, αντιμετωπίζοντάς τη σαν να είναι μία έγκυρη υπηρεσία, η δραστηριότητα του κακόβουλου λογισμικού έχει καταφέρει να επιτύχει το σκοπό του μέσα στο σύννεφο.

- **Επίθεση πλαστογράφησης μεταδεδομένων**

Ένας πελάτης μιας web υπηρεσίας ανακτά όλες τις πληροφορίες που χρειάζονται σχετικά με την επίκληση μιας υπηρεσίας web (δηλαδή τη μορφή μηνύματος, τη θέση δικτύου, τις απαιτήσεις ασφάλειας κ.λπ.), από τα μεταδεδομένα που παρέχονται από τον εξυπηρετητή αυτής της υπηρεσία web. Επί του παρόντος, αυτά τα μεταδεδομένα συνήθως διανέμονται με τη χρήση των πρωτοκόλλων επικοινωνίας, όπως το HTTP ή το mail. Αυτές οι συνθήκες προσφέρουν νέες δυνατότητες επίθεσης με στόχο την πλαστογράφηση αυτών των μεταδεδομένων.

Οι πιο σημαντικές επιθέσεις σε αυτή την κατηγορία είναι η πλαστογράφηση WSDL (Web Services Description Language) και η πλαστογράφηση της Πολιτικής Ασφάλειας. Υποθετικά η πιο πολλά υποσχόμενη για την WSDL πλαστογράφηση είναι η τροποποίηση των παραμέτρων του δικτύου και οι αναφορές σε θέματα

πολιτικής ασφάλειας. Ένα τροποποιημένο τελικό σημείο καθιστά ικανό τον εισβολέα στο να δημιουργήσει εύκολα μια επίθεση man-in-the-middle για υποκλοπές ή τροποποιήσεις των δεδομένων. Αν επιπλέον μια πλαστογραφημένη πολιτική ασφάλειας με πολύ χαμηλές ή χωρίς καμιά ασφάλεια απαιτήσεις χρησιμοποιείται, τέτοιες επιθέσεις είναι δυνατόν να πραγματοποιηθούν και να επιτύχουν παρά τη χρήση των WS-Security.

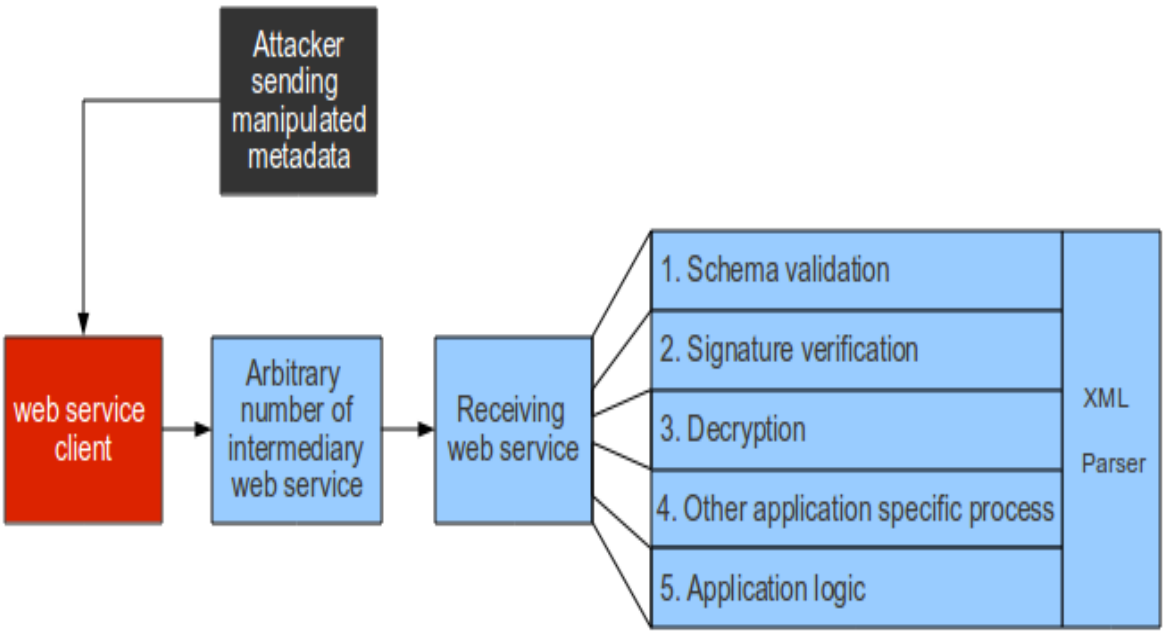
.Για την αποφυγή πλαστογράφησης Μεταδεδομένων, όλα τα έγγραφα για τα μεταδεδομένα πρέπει να ελέγχονται προσεκτικά για την αυθεντικότητα. Ωστόσο, οι μηχανισμοί για τη διασφάλιση των εγγράφων των μεταδεδομένων δεν έχει τυποποιηθεί-σε αντίθεση με τις μεθόδους για την εξασφάλιση των μηνυμάτων SOAP. Επιπλέον, μια προηγμένη δημιουργία σχέσεων εμπιστοσύνης είναι απαραίτητη, το οποίο δεν είναι πάντα εφικτή.

Θέλοντας να αναλύσουμε λίγο περισσότερο την επίθεση αυτή θα μπορούσαμε να πούμε ότι η επίθεση αυτή εκτελείται στον web service client. Η διαδικτυακή υπηρεσία που προορίζεται να αποτελέσει αντικείμενο επίθεσης δεν χρειάζεται καν να είναι ευάλωτη σε οποιαδήποτε επίθεση. Εμείς απλά υποθέτουμε ότι ένας εισβολέας είναι σε θέση να πλαστογραφήσει τα έγγραφα των μεταδεδομένων της web υπηρεσίας που ο πελάτης θέλει να επικαλεσθεί. Για έναν εισβολέα τρία σενάρια είναι πιθανά, προκειμένου να επιτύχει το στόχο του:

1. Εναλλαγή του αρχικού αρχείου στον διακομιστή της web υπηρεσίας που έχει δεχτεί επίθεση με το πλαστογραφημένο αρχείο.

2. Σενάρια MITM (Man-in-the-Middle) , όπου ένας εισβολέας μεταβάλλει το έγγραφο στην κυκλοφορία, ενώ ο πελάτης ανακτά το έγγραφο μεταδεδομένων από το διακομιστή των web services.

3. Ο εισβολέας εναλλάσσει το αρχείο στον τοπικό υπολογιστή του πελάτη της υπηρεσία web. Απαιτείται τοπική πρόσβαση στο μηχάνημα του πελάτη.
Σε αυτό το σενάριο η web υπηρεσία υποδοχής και η λειτουργία που εκτελείται στην υπηρεσία web γίνονται όπως αυτά καθορίζονται από τον εισβολέα στο πλαστογραφημένο έγγραφο.



- **Κόκκινο = συνιστώσα της web υπηρεσιας που δέχτηκε επίθεση**
- **Μαύρο = τοποθεσία του εισβολέα**
- **Μπλε = συνιστώσα της web υπηρεσιας που δεν εμπλέκεται άμεσα στην επίθεση**

Εικόνα 5.3: Γραφική αναπαράσταση της επίθεσης

Πηγή http://www.ws-attacks.org/index.php/XML_Entity_Expansion

- **Επίθεση πλημμύρας**

Ορισμός της Distributed Denial of Service Attack (DDoS):

DDoS στα αγγλικά σημαίνει "Distributed Denial of Service." Μια επίθεση DDoS είναι μια κακόβουλη προσπάθεια να γίνει ένας διακομιστή ή ένας πόρος δικτύου μη διαθέσιμος για τους χρήστες, συνήθως με προσωρινή διακοπή ή αναστολή των υπηρεσιών μιας μηχανής που είναι συνδεδεμένη στο Διαδίκτυο.

Σε αντίθεση με μια επίθεση Denial of Service (DoS), στην οποία ένας υπολογιστής και μία σύνδεση στο internet χρησιμοποιούνται για να υπερχειλίσει ένας στοχευμένος πόρος με πακέτα, η επίθεση DDoS χρησιμοποιεί πολλούς υπολογιστές και πολλές

συνδέσεις στο Διαδίκτυο, οι οποίοι συχνά διανέμονται σε παγκόσμιο επίπεδο και είναι αυτό που συχνά αναφέρεται ως ένα botnet (δηλαδή ένα δίκτυο ιδιωτικών υπολογιστών οι οποίοι έχουν μολυνθεί με κακόβουλο λογισμικό και ελέγχονται ως ομάδα εν αγνοία των ιδιοκτητών τους, π.χ., για την αποστολή spam μηνυμάτων).

Οι DDoS επιθέσεις μπορούν να χωριστούν σε τρεις κατηγορίες:

- Επιθέσεις με βάση τον όγκο

Περιλαμβάνει πλημμύρες UDP, πλημμύρες ICMP και άλλες πλημμύρες πλαστογραφημένων πακέτων. Ο στόχος της επίθεσης είναι να κορεστεί το εύρος ζώνης του χώρου στον οποίο επιτέθηκαν, και το μέγεθος μετριέται σε bits ανά δευτερόλεπτο (bps).

- Επιθέσεις πρωτοκόλλου

Περιλαμβάνει πλημμύρες SYN, αποσπασματικές επιθέσεις πακέτων, Ping of Death, Smurf DDoS και πολλά άλλα. Αυτό το είδος της επίθεσης καταναλώνει πραγματικούς πόρους του διακομιστή, ή του ενδιάμεσου εξοπλισμού επικοινωνίας, όπως firewalls και εξισορροπητές φορτίου, και μετριέται σε πακέτα ανά δευτερόλεπτο.

- Επιθέσεις σε επίπεδο εφαρμογής

Περιλαμβάνει Slowloris, Zero-day επιθέσεις DDoS, επιθέσεις DDoS που στοχεύουν στα τρωτά σημεία των Apache, Windows ή OpenBSD και άλλων. Αποτελούμενες από φαινομενικά νόμιμα και αθώα αιτήματα, ο στόχος αυτών των επιθέσεων είναι να συντρίψει τον web server, και το μέγεθος μετριέται σε αιτήσεις ανά δευτερόλεπτο.

Μερικοί συγκεκριμένοι και ιδιαίτερα δημοφιλείς και επικίνδυνοι τύποι των επιθέσεων DDoS περιλαμβάνουν:

- UDP Flood

Αυτή η επίθεση DDoS αξιοποιεί την πρωτοκόλλου User Datagram Protocol (UDP), ένα sessionless πρωτόκολλο δικτύωσης. Αυτό το είδος της επίθεσης πλημμυρίζει τυχαίες θύρες σε έναν απομακρυσμένο υπολογιστή με πολλά πακέτα UDP, προκαλώντας τον host να ελέγχει κατ' επανάληψη για την εφαρμογή αν «ακούει» στην θύρα, και (όταν καμία εφαρμογή δεν έχει βρεθεί) να απαντήσει με ένα πακέτο ICMP απρόσιτου προορισμού. Η διαδικασία αυτή ζημιώνει τους πόρους του host, και μπορεί τελικά να οδηγήσει σε αδυναμία πρόσβασης.

- Πλημμύρες ICMP (Ping)

Παρόμοια με τις αρχές που ακολουθεί η επίθεση πλημμύρας UDP, μια πλημμύρα ICMP κατακλύζει τον πόρο προορισμού με ICMP Echo Request (ping) πακέτα, αποστέλλοντας γενικά πακέτα όσο το δυνατόν γρηγορότερα, χωρίς να περιμένει για τις απαντήσεις. Αυτό το είδος της επίθεσης μπορεί να καταναλώσει τόσο το εισερχόμενο όσο και το εξερχόμενο εύρος ζώνης, δεδομένου ότι οι διακομιστές του θύματος συχνά θα προσπαθήσει να απαντήσει με ICMP Echo πακέτα, με αποτέλεσμα μια σημαντική συνολική επιβράδυνση του συστήματος.

- Πλημμύρα SYN

Μια DDoS επίθεση SYN πλημμύρας εκμεταλλεύεται μια γνωστή αδυναμία στην ακολουθία της TCP σύνδεσης (την " three-way handshake»), όπου ένα αίτημα SYN για να ξεκινήσει μια σύνδεση TCP με έναν host πρέπει να απαντηθεί με μια απάντηση SYN-ACK από αυτόν τον κεντρικό υπολογιστή και στη συνέχεια να επιβεβαιωθεί από μια απάντηση ACK από τον αιτούντα. Σε ένα σενάριο πλημμύρας SYN, ο αιτών στέλνει πολλαπλά αιτήματα SYN, αλλά είτε δεν αποκρίνεται στην απάντηση SYN -ACK του host, ή στέλνει τα αιτήματα SYN από μια πλαστογραφημένη διεύθυνση IP. Είτε έτσι είτε αλλιώς, το σύστημα υποδοχής εξακολουθεί να περιμένει για την αναγνώριση για κάθε ένα από τα αιτήματα, δεσμεύοντας πόρους έως ότου να μην μπορούν

να γίνουν νέες συνδέσεις, και τελικά οδηγείται το σύστημα σε άρνηση υπηρεσίας.

- Ping of Death

Μια επίθεση Ping of Death ("POD") περιλαμβάνει τον εισβολέα ο οποίος κάνει αποστολή πολλαπλών ακατάλληλων ή κακόβουλων pings σε έναν υπολογιστή. Το μέγιστο μήκος ενός IP πακέτου (συμπεριλαμβανομένης της επικεφαλίδας) είναι 65.535 bytes. Ωστόσο, το στρώμα σύνδεσης δεδομένων Data Link Layer θέτει συνήθως όρια στο μέγιστο μέγεθος του πλαισίου - για παράδειγμα 1.500 bytes μέσω ενός δικτύου Ethernet. Σε αυτήν την περίπτωση, ένα μεγάλο πακέτο IP είναι χωρισμένο σε πολλαπλά πακέτα IP (γνωστό ως θραύσματα - fragments), και ο παραλήπτης υποδοχής ξαναενώνει τα IP θραύσματα στο πλήρες πακέτο. Σε σενάριο Ping of Death, μετά από τις κακόβουλες πράξεις χειραγώγησης του περιεχομένου των fragments, ο παραλήπτης καταλήγει με ένα πακέτο IP που είναι μεγαλύτερο από 65.535 bytes. Αυτό μπορεί να υπερχειλίσει τους buffer μνήμης που διατίθενται για το πακέτο, προκαλώντας άρνηση υπηρεσίας για τα νόμιμα πακέτα.

- Slowloris

Slowloris είναι μια εξαιρετικά στοχευμένη επίθεση, που επιτρέπει σε ένα web server να καταστρέψει έναν άλλο διακομιστή, χωρίς να επηρεάζει άλλες υπηρεσίες ή θύρες του δικτύου προορισμού. Η επίθεση Slowloris το καταφέρνει αυτό κρατώντας ανοικτές όσες πιο πολλές συνδέσεις προς το web server-στόχο για όσο το δυνατόν περισσότερο. Το πετυχαίνει αυτό με τη δημιουργία συνδέσεων στο διακομιστή προορισμού, αλλά μη αποστέλλοντας ολοκληρωμένο αιτήματος. Η επίθεση Slowloris στέλνει συνεχώς περισσότερες κεφαλίδες HTTP, αλλά ποτέ δεν ολοκληρώνει ένα αίτημα. Ο server - στόχος κρατά κάθε μία από αυτές τις ψεύτικες συνδέσεις ανοιχτή. Αυτό τελικά οδηγεί σε υπερχείλιση και οδηγεί σε άρνηση υπηρεσίας στις επιπλέον συνδέσεις που θα γίνουν από νόμιμους πελάτες.

- NTP Ενίσχυση (NTP Amplification)

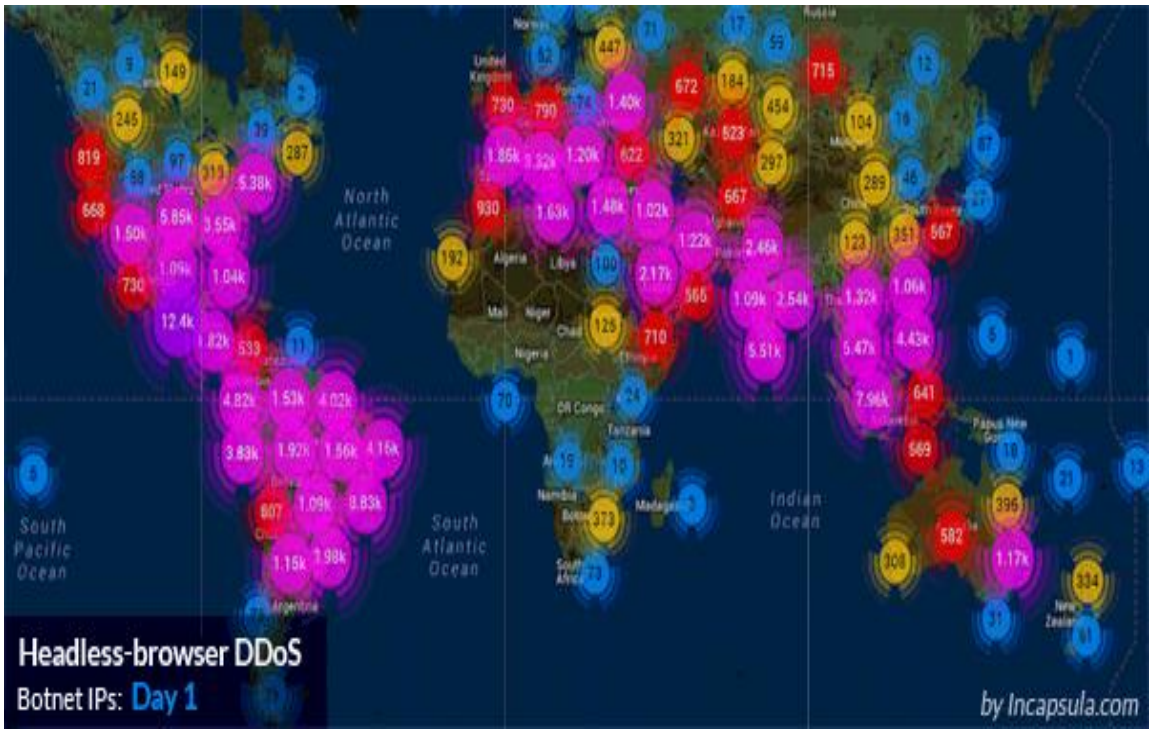
Στις επιθέσεις NTP Amplification ο δράστης εκμεταλλεύεται δημόσια προσβάσιμους Πρωτόκολλο Δικτυακού Χρόνου (NTP) εξυπηρετητές για να κατακλύσει τον server - -στόχο με User Datagram Protocol (UDP) κυκλοφορία. Σε μια επίθεση NTP Amplification, η αναλογία ερώτημα προς απάντηση είναι οπουδήποτε μεταξύ 1:20 και 1: 200 ή περισσότερο. Αυτό σημαίνει ότι κάθε εισβολέας που αποκτά μια λίστα με ανοικτούς διακομιστές NTP (π.χ., χρησιμοποιώντας το εργαλείο όπως Metasploit ή δεδομένων από την ανοικτή NTP έργο) μπορεί εύκολα να δημιουργήσει μια καταστροφική υψηλού εύρους ζώνης και υψηλού όγκου DDoS επίθεση.

- Πλημμύρα HTTP

Στο DDoS επίθεση HTTP πλημμύρας ο εισβολέας εκμεταλλεύεται φαινομενικά νόμιμα αιτήματα HTTP GET ή POST για να επιτεθεί σε ένα web server ή μία εφαρμογή. Οι επιθέσεις πλημμύρας HTTP δεν χρησιμοποιούν ακατάλληλα πακέτα, τεχνικές πλαστογράφησης ή αντανάκλασης, και απαιτούν λιγότερο εύρος ζώνης από άλλες επιθέσεις για να κατεδαφίσουν το site-στόχο ή τον server-στόχο. Η επίθεση είναι πιο αποτελεσματική όταν αναγκάζει τον server ή την εφαρμογή να διαθέσουν τους μέγιστους δυνατούς πόρους στην απάντηση για κάθε ένα αίτημα.

- DDoS επιθέσεις Zero-day

Οι επιθέσεις «Zero-day" είναι απλά άγνωστες ή νέες επιθέσεις, που εκμεταλλεύονται τα τρωτά σημεία για τα οποία δεν έχει ακόμα κυκλοφορήσει κανένα patch. Ο όρος είναι γνωστός μεταξύ των μελών της κοινότητας των hacker, όπου η πρακτική των συναλλαγών Zero-day τρωτών σημείων έχει γίνει μια δημοφιλής δραστηριότητα.



Εικόνα 5.4: Μία μαζική HTTP flood: 690,000,000 DDoS αιτήματα από 180,000 botnets IPs (Incapsula.com)

Πηγή https://www.incapsula.com/blog/headless-browser-ddos.html

Πηγές των DDoS επιθέσεων

Οι DDoS επιθέσεις γίνονται γρήγορα τα πιο διαδεδομένα είδη επιθέσεων, έχοντας παρουσιάσει τεράστια αύξηση τα τελευταία χρόνια τόσο σε αριθμό όσο και σε όγκο, σύμφωνα με συνεχείς έρευνες της αγοράς. Η τάση που επικρατεί είναι προς τη μικρότερη διάρκεια επίθεσης, αλλά μεγαλύτερο σε όγκο πακέτο ανά δευτερόλεπτο επίθεση, και ο συνολικός αριθμός των επιθέσεων που αναφέρονται έχει επίσης αυξηθεί σημαντικά.

Μιλώντας για πιο παλιά έτη αλλά θέλοντας να δείξουμε το ρυθμό με τον οποίο αυξάνονται αυτές οι επιθέσεις έχει αναφερθεί ότι κατά τη διάρκεια του 2011, μια έρευνα διαπίστωσε 45% περισσότερες επιθέσεις DDoS σε σύγκριση με την παράλληλη περίοδο του 2010, και πάνω από το διπλάσιο του αριθμού των επιθέσεων που παρατηρούνται κατά τη διάρκεια του αμέσως προηγούμενου τριμήνου του 2011.

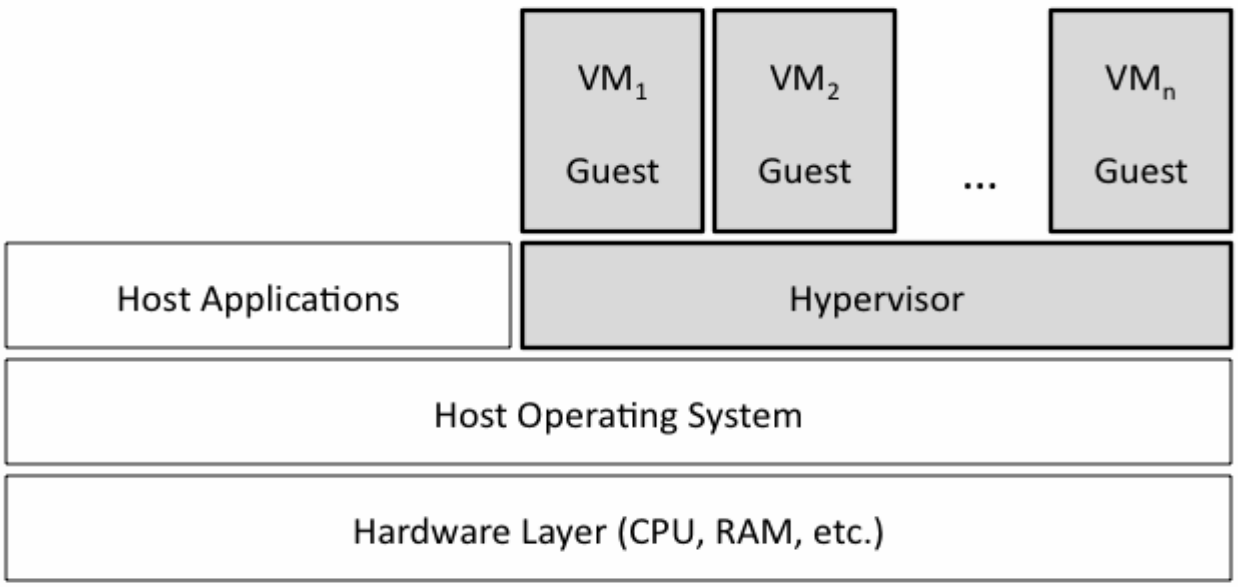
Το μέσο εύρος ζώνης επιθέσεων που παρατηρήθηκε κατά τη διάρκεια αυτής της περιόδου ήταν 5.2Gbps, το οποίο είναι 148% υψηλότερο από το προηγούμενο τρίμηνο.

Μια άλλη έρευνα για τις επιθέσεις DDoS διαπίστωσε ότι περισσότερο από το 40% των συμμετεχόντων στην έρευνα είχαν την εμπειρία επιθέσεων που ξεπέρασε σε εύρος ζώνης το 1Gbps το 2013, και το 13% των συμμετεχόντων είχαν γίνει στόχος τουλάχιστον μίας επίθεση που ξεπέρασε τα 10Gbps.

Από μια άλλη προοπτική, πρόσφατη έρευνα διαπίστωσε ότι DDoS επιθέσεις με ιδεολογικά κίνητρα βρίσκονται σε άνοδο. Η έρευνα αναφέρεται επίσης σε οικονομικούς λόγους (π.χ., ανταγωνιστικά feuds) ως μια άλλη κοινή αιτία για τέτοιου είδους επιθέσεις.

5.5. Επιθέσεις σε Εικονικές Μηχανές

Οι εικονικές μηχανές (VM) αντικαθιστούν ταχύτατα τις υποδομές φυσικών μηχανών λόγω των ικανοτήτων τους να μιμηθούν τα περιβάλλοντα hardware, να μοιραστούν τους πόρους hardware, και να χρησιμοποιήσουν μια ποικιλία λειτουργικών συστημάτων (OS). Οι εικονικές μηχανές παρέχουν ένα καλύτερο μοντέλο ασφάλειας από ό, τι τα παραδοσιακά συστήματα, παρέχοντας ένα επιπλέον επίπεδο αφαίρεσης υλικού και απομόνωση, αποτελεσματική εξωτερική παρακολούθηση και καταγραφή, και on-demand πρόσβαση.



Εικόνα 5.5: Αρχιτεκτονική εικονικής μηχανής

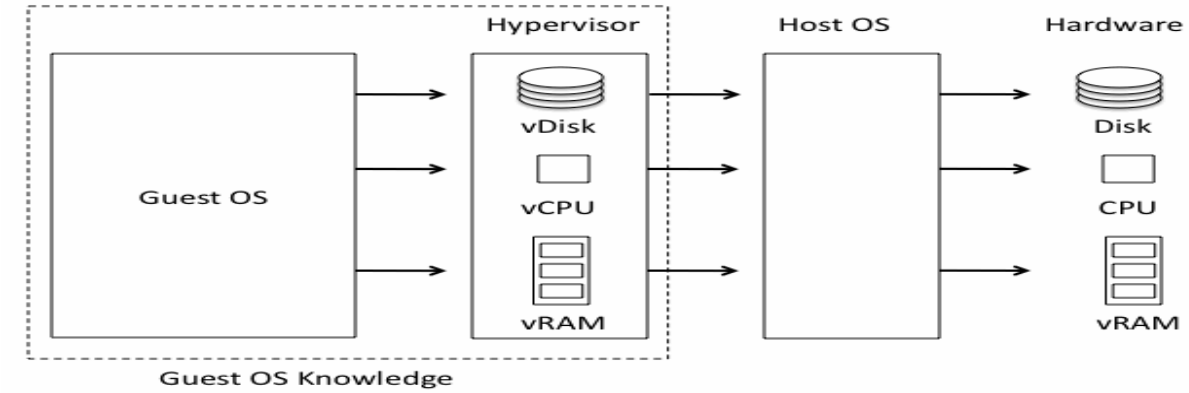
Πηγή http://www.cse.wustl.edu/~jain/cse571-09/ftp/vmsec/index.html

Ωστόσο, αυτό το νέο μοντέλο απαιτεί την προσαρμογή των υφιστάμενων μεθόδων ασφάλειας, οι οποίες δεν μπορούν προς το παρόν να συμβαδίσουν με την ευκολία της δημιουργίας νέων VMs με μια ποικιλία χαρακτηριστικών configurations και διάρκειας ζωής. Οι εισβολείς έχουν παραβιάσει επιτυχώς τις υποδομές των VM, γεγονός που τους επιτρέπει να έχουν πρόσβαση σε άλλα VMs στο ίδιο σύστημα, ακόμα και στον host. Ευτυχώς, αυτές οι ανησυχίες για την ασφάλεια αντιμετωπίζονται και οι χρήστες μπορούν να αποτρέψουν τις περισσότερες εισβολές με την εφαρμογή των παραδοσιακών μέτρων ασφαλείας σε κάθε εικονική μηχανή.
Δεν υπάρχει τίποτα σχετικά με το virtual Computing που είναι εγγενώς μη ασφαλές. Αυτό που θα μπορούσαμε να πούμε είναι απλά ότι αποτελεί ένα νέο φορέα επίθεσης στην ασφάλεια. Το επίπεδο της εικονικής μηχανής είναι πιο ασφαλές από οποιοδήποτε άλλο λειτουργικό σύστημα, λόγω της απλότητάς του και του αυστηρού έλεγχου της πρόσβασης. Το να τεθεί σε κίνδυνο ο hypervisor θα μπορούσε να δώσει στους εισβολείς την πρόσβαση σε όλες τις εικονικές μηχανές που ελέγχονται από αυτόν ακόμα και να τους δοθεί πρόσβαση στον host, γεγονός που καθιστά το hypervisor ένα συναρπαστικό στόχο. Η μη εξουσιοδοτημένη επικοινωνία μεταξύ των

επισκεπτών αποτελεί παραβίαση της αρχής της απομόνωσης, αλλά μπορεί ενδεχομένως να πραγματοποιηθεί μέσω της κοινής μνήμης.

Όπως και οι φυσικές μηχανές, οι εικονικές μηχανές είναι ευάλωτες στην υποκλοπή και στις επιθέσεις άρνησης παροχής υπηρεσίας. Τα περιεχόμενα του εικονικού δίσκου για κάθε εικονική μηχανή συνήθως αποθηκεύονται ως ένα αρχείο, το οποίο μπορεί να εκτελεστεί από hypervisors σε άλλα μηχανήματα, επιτρέποντας στους εισβολείς να αντιγράψουν τον εικονικό δίσκο και να αποκτήσουν απεριόριστη πρόσβαση στα ψηφιακά περιεχόμενα της εικονικής μηχανής.

Καθώς οι εικονικές μηχανές διαμοιράζονται πόρους από την φυσική μηχανή, οι υποδομές των εικονικών μηχανών ήταν ιδιαίτερα ευάλωτες σε επιθέσεις άρνησης υπηρεσίας, οι οποίες θα μπορούσαν να οδηγήσουν τους πόρους σε λιμοκτονία από όλες τις VMs στην φυσική μηχανή. Ευτυχώς, αυτό το πρόβλημα μπορεί εύκολα να λυθεί από τον περιορισμό της κατανάλωσης των πόρων για κάθε VM. Πιο καινούρια προϊόντα που έχουν βγει στην αγορά λύνουν πολλά από τα προβλήματα αυτά, ωστόσο, παραμένουν ανησυχίες που οι hypervisors θα πρέπει να συνεχίσουν να τα βλέπουν από τη σκοπιά της ανάπτυξης.



Εικόνα 5.6: Αφαίρεση φυσικών πόρων

Πηγή http://www.cse.wustl.edu/~jain/cse571-09/ftp/vmsec/index.html

5.5.1. Κινητικότητα

Οι εικονικές μηχανές δεν είναι εγγενώς φυσικές, πράγμα που σημαίνει ότι η κλοπή τους μπορεί να λάβει χώρα χωρίς φυσική κλοπή της μηχανής του host. Τα

περιεχόμενα του εικονικού δίσκου για κάθε εικονική μηχανή αποθηκεύονται ως αρχείο από τους περισσότερους hypervisors, το οποίο επιτρέπει στις VMs να αντιγραφούν και να εκτελεστούν από άλλες φυσικές μηχανές. Ενώ αυτό αποτελεί ένα χαρακτηριστικό ευκολίας, μπορεί εξίσου να αποτελέσει μια απειλή για την ασφάλεια.

Οι εισβολείς μπορούν να αντιγράψουν την εικονική μηχανή μέσω του δικτύου ή σε ένα φορητό μέσο αποθήκευσης και να έχουν πρόσβαση σε αυτά τα δεδομένα από τη δική τους μηχανή χωρίς να έχουν κλέψει με φυσικό τρόπο το σκληρό δίσκο. Μόλις οι εισβολείς αποκτήσουν άμεση πρόσβαση στον εικονικό δίσκο, έχουν απεριόριστο χρόνο για να νικήσουν όλους τους μηχανισμούς ασφαλείας, όπως είναι για παράδειγμα οι κωδικοί πρόσβασης, χρησιμοποιώντας offline επιθέσεις. Δεδομένου ότι ο εισβολέας θα έχει πρόσβαση σε ένα αντίγραφο του VM και όχι στο πρωτότυπο, η εικονική μηχανή δεν θα δείξει κανένα αρχείο εισβολής.

Ο δεύτερος κίνδυνος των εικονικών δίσκων είναι ότι ο εισβολέας θα μπορούσε να φθείρει ή να τροποποιήσετε εξωτερικά το αρχείο, ενώ η εικονική μηχανή δεν είναι συνδεδεμένη. Αυτό σημαίνει ότι η ακεραιότητα μιας offline εικονικής μηχανής μπορεί να τεθεί σε κίνδυνο εάν ο host δεν είναι καλά προστατευμένος. Αυτό δεν είναι συνήθως ένα ζήτημα όταν κάνουμε χρήση φυσικών εξυπηρετητών, διότι η μηχανή πρέπει να λειτουργεί ώστε να είναι προσβάσιμη από το δίκτυο. Σύγχρονοι αλγόριθμοι κρυπτογράφησης και ακεραιότητας μπορούν να εφαρμοστούν από το hypervisor υποδοχής έτσι ώστε να διασφαλίζεται η πρόσβαση και η ακεραιότητα.

5.5.2. Εισβολή Hypervisor

Ο hypervisor παρέχει την άντληση και την διανομή των πόρων μεταξύ του host και των επισκεπτών. Ο απώτερος στόχος των εισβολέων είναι να θέσουν σε κίνδυνο τον hypervisor προκειμένου να αποκτήσουν τη δυνατότητα να εκτελέσουν αυθαίρετο κώδικα στον κεντρικό υπολογιστή με τα προνόμια της διαδικασία του hypervisor.

Ο hypervisor είναι ένα πρόγραμμα, που τρέχει στον κεντρικό υπολογιστή, οπότε αν τεθεί σε κίνδυνο, όλες οι εικονικές μηχανές που ελέγχει αλλά και ο ίδιος ο host γίνονται προσβάσιμα από τον εισβολέα. Ο hypervisor μετατρέπει τις οδηγίες για το

λειτουργικό σύστημα των επισκεπτών σε οδηγίες για το λειτουργικό σύστημα του host. Ωστόσο, εάν ο πελάτης είναι σε κίνδυνο, τότε οι οδηγίες που αποστέλλονται στον hypervisor μπορεί να είναι ανορθολογικές.

Ερευνητές έτρεξαν δύο εργαλεία, το crashme και το iofuzz, τα οποία παράγουν τυχαίες I/O θύρες δραστηριότητας μέσα στις εικονικές μηχανές, μέχρι ο hypervisor ή η εικονική μηχανή να κρασάρει. Οι λεπτομέρειες αυτών των επιθέσεων δεν περιλαμβάνονται στην παρούσα εργασία καθώς όλα τα ελαττώματα που ανιχνεύτηκαν έχουν ήδη διορθωθεί.

Θα πρέπει να αναφέρουμε ωστόσο ότι ήταν σε θέση να θέσουν σε κίνδυνο τον hypervisor και να αποκτήσουν πρόσβαση στο host χρησιμοποιώντας οποιοδήποτε major hypervisor στη που είναι διαθέσιμος στο κοινό. Ωστόσο, οι hypervisors είναι γενικά πιο ασφαλείς από τα λειτουργικά συστήματα, δεδομένου ότι ο hypervisor είναι ένα σχετικά μικρό και απλό πρόγραμμα, το οποίο βοηθά να περιοριστούν τρωτά σημεία χαμηλού επιπέδου που μπορεί να υπάρχουν σε πολλά προγράμματα. Τελικά, εάν το φιλοξενούμενο λειτουργικό σύστημα δεν είναι ασφαλές, σφάλματα ασφαλείας έχουν τη δυνατότητα να διαφύγουν διαμέσου του επιπέδου του hypervisor.

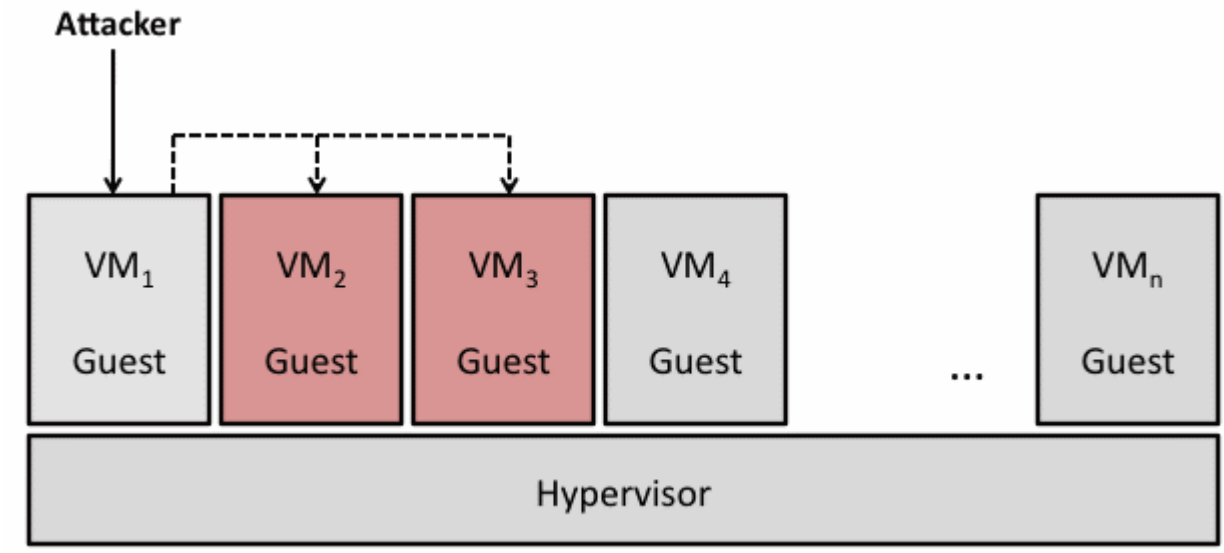
5.5.3. Τροποποίηση Hypervisor

Δεν έχει σημασία πόσο ασφαλής είναι ο πρωτότυπος hypervisor είναι εάν είναι δυνατόν να τροποποιηθεί εξωτερικά προκειμένου να χρησιμοποιήσει το λογισμικό του εισβολέα. Μια επίθεση τέτοιου τύπου είναι γνωστή ως Virtual Machine Based Root Kits (VMBR). Σε αυτήν την επίθεση, οι κλήσεις του συστήματος του hypervisor προς το λειτουργικό σύστημα του host έχουν υποστεί αλλαγές προκειμένου να τρέξει κακόβουλο κώδικα αντί του κανονικού. Ευτυχώς, υπάρχουν διάφορες μέθοδοι για την πρόληψη της τροποποίησης του hypervisor. Ο host μπορεί να χρησιμοποιήσει μια αξιόπιστη μονάδα πλατφόρμας (Trusted Platform Module -TPM) για να δημιουργήσει μια αξιόπιστη σχέση με τον hypervisor. Εναλλακτικά, ο πελάτης μπορεί να επαληθεύσει την ακεραιότητα του hypervisor κατά την εκκίνησή του. Μια τρίτη λύση είναι να χρησιμοποιηθεί ένας ενσωματωμένος hypervisor. Ένας ενσωματωμένος

hypervisor τρέχει χωρίς ένα λειτουργικό σύστημα του host και εγγενώς δεν μπορεί να τροποποιηθεί.

5.5.4. Επικοινωνία

Η επικοινωνία της εικονικής μηχανής αναφέρεται σε όλες εκείνες τις επιθέσεις στις οποίες οι εισβολείς χρησιμοποιούν μια εικονική μηχανή για να αποκτήσουν πρόσβαση ή έλεγχο άλλων εικονικών μηχανών στον ίδιο hypervisor. Αυτές οι επιθέσεις μπορούν να συμβούν χωρίς να τεθεί σε κίνδυνο το επίπεδο του hypervisor. Μια κακόβουλη εικονική μηχανή μπορεί ενδεχομένως να έχει πρόσβαση σε άλλες εικονικές μηχανές διαμέσου κοινής μνήμης, συνδέσεων δικτύου, και άλλων κοινόχρηστων πόρων. Για παράδειγμα, αν μια κακόβουλη εικονική μηχανή έχει καθορίσει πού βρίσκεται η μνήμη μιας άλλης εικονικής μηχανής, τότε θα μπορούσε να διαβάσει ή να γράψει σε αυτή τη θέση και να παρέμβει σε άλλες λειτουργίες. Το παρακάτω σχήμα δείχνει μια επίθεση από την εικονική μηχανή VM1 στις εικονικές μηχανές VM2 και VM3. Ο εισβολέας μπορεί να είναι εξουσιοδοτημένος να έχει πρόσβαση στην VM1 αλλά μπορεί και όχι. Σε αυτό ωστόσο το παράδειγμα έχει προσπελάσει δύο μη εξουσιοδοτημένη εικονικές μηχανές



Εικόνα 5.7: Επίθεση VM επικοινωνίας στις VM2 και VM3

Πηγή http://www.cse.wustl.edu/~jain/cse571-09/ftp/vmsec/index.html

Μερικές φορές είναι επιθυμητό για δύο εικονικές μηχανές να είναι σε θέση να επικοινωνήσουν. Αυτό έχει πολλές εφαρμογές, όπως για παράδειγμα προκειμένου να πραγματοποιηθεί ειδική παρακολούθηση μιας εικονικής μηχανής ή για την εφαρμογή μιας τεχνολογίας δικτύου που απαιτεί πολλούς ομότιμους «συνομιλητές». Αντί να παρέχει πλήρη απομόνωση, ο security hypervisor sHype της IBM για παράδειγμα είναι διατεθειμένος να έχει μια ασφαλή αρχιτεκτονική για την αντιμετώπιση της επικοινωνίας μεταξύ των εικονικών μηχανών σε μια υποδομή VM. Ο sHype επιτρέπει στους διαχειριστές του συστήματος να καθορίσουν τις πολιτικές για την επικοινωνία μεταξύ κάθε εικονικής μηχανής και να διασφαλίσει ότι μόνο οι εξουσιοδοτημένα εικονικές μηχανές μπορούν να έχουν πρόσβαση στην μεταξύ τους επικοινωνία

5.5.5. Άρνηση Υπηρεσίας (DoS)

Οι επιθέσεις DoS είναι μια απειλή για όλους τους διακομιστές, όμως ένας λανθασμένα ρυθμισμένος hypervisor μπορεί να επιτρέψει σε μία μοναδική εικονική μηχανή να καταναλώνει όλους τους πόρους, αφήνοντας με τον τρόπο αυτό κάθε άλλη εικονική μηχανή που τρέχει στην ίδια φυσική μηχανή χωρίς κανέναν πόρο. Οι επιθέσεις DoS μπορούν να καταστήσουν το δίκτυο του host ανίκανο να λειτουργήσει δεδομένου ότι κρίσιμες διεργασίες δεν έχουν τους πόρους του υλικού για την εκτέλεση τους εν ευθέτω χρόνω. Ευτυχώς, η λύση είναι απλή. Οι hypervisors εμποδίζουν οποιαδήποτε εικονική μηχανή από το να αποκτήσουν το 100% της χρήσης οποιωνδήποτε πόρων, συμπεριλαμβανομένων των CPU, RAM, του εύρους ζώνης δικτύου, και της μνήμης γραφικών.

Επιπλέον, ο hypervisor μπορεί να διαμορφωθεί έτσι ώστε όταν ανιχνεύει την υπερβολική κατανάλωση πόρων, να μπορεί να αξιολογήσει κατά πόσον λαμβάνει χώρα μια επίθεση και να κάνει αυτόματη επανεκκίνηση της εικονικής μηχανής. Οι εικονικές μηχανές μπορούν συνήθως να αρχικοποιηθούν πολύ πιο γρήγορα από ό, τι φυσικές μηχανές, επειδή η ακολουθία εκκίνησης τους δεν χρειάζεται να προετοιμαστεί και να ελέγξει το υλικό. Έτσι η επανεκκίνηση μιας εικονικής μηχανής έχει μικρότερη επίδραση από ό, τι η επανεκκίνηση μια φυσικής μηχανής[4].

ΚΕΦΑΛΑΙΟ 6:
ΣΗΜΑΝΤΙΚΟΤΗΤΑ ΠΡΟΣΤΑΣΙΑΣ ΣΤΟ CLOUD

Στο κεφάλαιο αυτό, θα γίνει αναφορά στην διαφορά ασφάλειας και ιδιωτικότητας, το πόσο σημαντική είναι η δεύτερη αλλά και σε θέματα εμπιστοσύνης που καλούμαστε να προσέξουμε στο Cloud Computing. Τέλος θα προταθούν τρόποι προστασίας και μηχανισμοί που εξυπηρετούν σε αυτή.

6.1. Ιδιωτικότητα

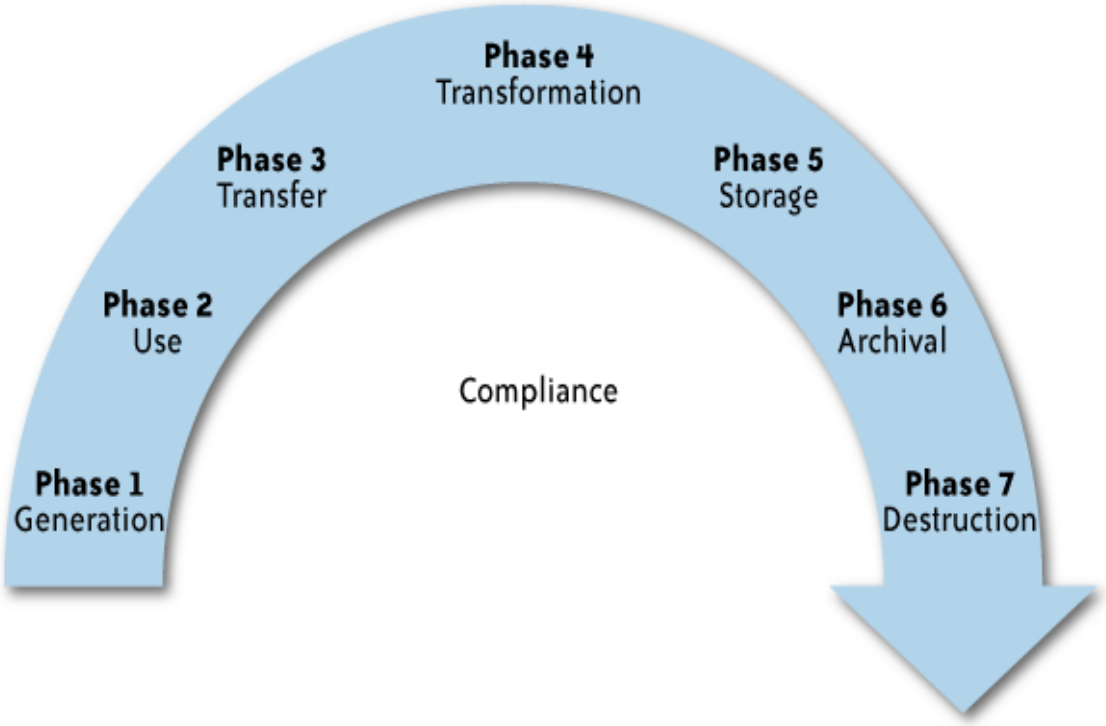
Η ιδιωτικότητα έχει οριστεί με πολλούς και διαφορετικούς τρόπους. Η πιο διαδεδομένος είναι «το δικαίωμα του να είσαι μόνος- the right to be left alone». Αφορά προσωπικά και ευαίσθητα δεδομένα και έχει κατοχυρωθεί ως ανθρώπινο δικαίωμα. Σε κάθε χώρα ή κουλτούρα διαφέρουν οι νόμοι, παρόλα αυτά υπάρχουν συγκεκριμένοι κανόνες που ισχύουν σε ολόκληρη την υφήλιο.

Δεν πρέπει κανείς όμως να μπερδεύει την ασφάλεια με την ιδιωτικότητα. Ο Tim Mather έχει δηλώσει χαρακτηριστικά «μπορείς να έχεις ασφάλεια χωρίς ιδιωτικότητα, όμως όχι ιδιωτικότητα χωρίς ασφάλεια». Υπάρχει καταπάτηση της ιδιωτικότητας όταν τα προσωπικά δεδομένα που διακινούνται στο Cloud γίνονται γνωστά σε μη εξουσιοδοτημένες οντότητες, και μπορούν να ταυτιστούν με φυσικό πρόσωπο. Επομένως, όταν τηρούνται οι πολιτικές και οι μηχανισμοί ασφάλειας, θα προστατεύεται και η ιδιωτικότητα κατά συνέπεια.

6.2. Κύκλος Ζωής Δεδομένων

Οι προσωπικές πληροφορίες θα πρέπει να οργανώνονται σε τμήματα δεδομένων από τη στιγμή που δημιουργούνται έως τη στιγμή της καταστροφής τους. Για την προστασία των προσωπικών δεδομένων στα συστήματα υπολογιστικού νέφους, έχει δημιουργηθεί το παρακάτω μοντέλο οργάνωσης και οι πολιτικές που πρέπει να τηρούνται σε αυτό, ανάλογα με τη φάση του κύκλου ζωής στην οποία ανήκει η κάθε προσωπική πληροφορία τη δεδομένη στιγμή.

Σε κάθε περίπτωση, πρέπει να λαμβάνεται υπόψη πως ο κάτοχος της πληροφορίας (είτε είναι φυσικό είτε νομικό πρόσωπο) θα πρέπει να έχει πλήρη γνώση αλλά και έλεγχο της διάδοσης της πληροφορίας. Η ιδιωτικότητα του αφορά την συλλογή, χρήση, διατήρηση και καταστροφή των προσωπικών του δεδομένων, κάτι που θα πρέπει και ο ίδιος να παρακολουθεί.



Σχήμα 6.1. Σχηματικά ο Κύκλος Ζωής Δεδομένων

Πηγή http://imageck.com/1260047247-detailed-class-diagram-visio.html

Τα στοιχεία που απαρτίζουν την κάθε από αυτές τις φάσεις είναι τα εξής:

- Δημιουργία (Generation)
  - Ιδιοκτησία, δηλαδή ποιος οργανισμός είναι ο νομικός κάτοχος της πληροφορίας, και κατά πόσο ο οργανισμός έχει διατηρήσει την ιδιοκτησία όσο χρησιμοποιεί το Cloud
  - Ταξινόμηση. Πως ταξινομείται η πληροφορία στο cloud, έλεγχος των περιορισμών στη χρήση και κατά πόσο η πληροφορία πρέπει να ταξινομηθεί με συγκεκριμένο τρόπο.

- Χρήση (Use)
    - Εσωτερική και εξωτερική, δηλαδή κατά πόσο η πληροφορία συλλέγεται μόνο από τον οργανισμό που του ανήκει ή αν συλλέγεται και από άλλους οργανισμούς (για παράδειγμα ένα δημόσιο νέφος- public cloud)
    - Τρίτη οντότητα. Κατά πόσο η πληροφορία διαδίδεται σε τρίτες οντότητες
    - Καταλληλότητα, δηλαδή αν συνάδει ο σκοπός της συλλογής της πληροφορίας με τον σκοπό της χρήσης της. Επίσης, κατά πόσο η χρήση στο cloud είναι κατάλληλη σύμφωνα με τους περιορισμούς στους οποίους έχει γίνει η ανάλυση της πληροφορίας.
    - Ανακάλυψη/ κλήτευση. Αν ακολουθούνται κατά γράμμα οι νόμοι που υπάρχουν για την χρήση πληροφορίας σε cloud συστήματα.
- Μετάδοση (Transfer)
    - Δημόσια και ιδιωτικά δίκτυα. Όταν η πληροφορία διαδίδεται σε δημόσιο cloud πρέπει να προστατεύεται ανάλογα.
    - Απαιτήσεις Κρυπτογραφίας. Υπάρχουν νόμοι που επιβάλλουν όλα τα δεδομένα που μεταδίδονται σε δημόσιο cloud να είναι κρυπτογραφημένα.
    - Έλεγχοι Πρόσβασης και κατά πόσο τηρούνται
- Μεταμόρφωση (Transformation)
    - Καταγωγή. Αν διατηρούνται όλοι οι περιορισμοί και η ασφάλεια των δεδομένων ή αν διαφοροποιούνται κατά την φάση της μεταμόρφωσης
    - Συνάθροιση, δηλαδή αν τα δεδομένα συναθροίζονται κατά την μεταμόρφωση σε βαθμό τέτοιο που δεν θα μπορούν να ταυτιστούν πια με φυσικό πρόσωπο
    - Ακεραιότητα και κατά πόσο διατηρείται στο cloud

- Αποθήκευση (Storage)
    - Έλεγχος Πρόσβασης. Τηρούνται οι απαιτούμενοι έλεγχοι πρόσβασης της πληροφορίας κατά την αποθήκευσή της στο cloud με τρόπο τέτοιο που να μπορεί να έχει πρόσβαση μόνο όποιος έχει σε αυτή την δικαιοδοσία;
    - Δομημένη και μη. Αν η αποθήκευση της πληροφορίας γίνεται με δομημένο ή όχι τρόπο, για να χρησιμοποιηθούν στο μέλλον.
    - Ακεραιότητα, διαθεσιμότητα, εμπιστευτικότητα στο cloud
    - Κρυπτογραφία. Τα δεδομένα προσωπικών πληροφοριών πρέπει να αποθηκεύονται στο cloud κρυπτογραφημένα, βάσει κάποιων νόμων.
- Αρχειοθέτηση (Archival)
    - Νομικό πλαίσιο. Νομικά, υπάρχουν συγκεκριμένες απαιτήσεις που καθορίζουν το όριο ζωής της πληροφορίας που αποθηκεύεται και αρχειοθετείται.
    - Παράπλευρη αποθήκευση, αν δηλαδή επιτρέπει το σύστημα να αποθηκεύεται και να αρχειοθετείται η πληροφορία μακροπρόθεσμα
- Καταστροφή (Destruction)
    - Ασφάλεια. Αν γίνεται η καταστροφή της πληροφορίας, όταν την λαμβάνει ο οργανισμός, με τρόπο τέτοιο ώστε να διασφαλίζεται πως κανένα από τα τμήματα δεδομένων της πληροφορίας δεν παραμένει στο cloud
    - Ολοκλήρωση, να γίνεται η καταστροφή της πληροφορίας να γίνεται εξ ολοκλήρου όταν λήξει το χρονικό περιθώριο της ζωής της.

Η επίδραση διαφέρει ανάλογα το μοντέλο Cloud computing που χρησιμοποιείται, την φάση κύκλου ζωής των προσωπικών πληροφοριών που διακινούνται αλλά και τη φύση του οργανισμού[3].

6.3. Βασικοί παράγοντες Ιδιωτικότητας στο Cloud

Οι νομικοί σύμβουλοι για την ιδιωτικότητα εξέφρασαν τις ανησυχίες τους για το cloud computing. Γίνεται μια μίξη ασφάλειας και ιδιωτικότητας και των βασικών αρχών. Επιπλέον παράγοντες που πρέπει να λαμβάνονται υπόψη αναφέρονται παρακάτω.

Πρόσβαση: τα τμήματα δεδομένων (τα σημεία που αποθηκεύονται τα δεδομένα) θα πρέπει να είναι ορισμένα έτσι ώστε να γίνεται ξεκάθαρο τι προσωπικά δεδομένα αποθηκεύονται, πόσο και ποιος έχει τη δικαιοδοσία να τα επεξεργαστεί και έως πότε. Στο cloud computing, μεγάλο ενδιαφέρον έχει η δυνατότητα πρόσβασης του οργανισμού- ιδιοκτήτη των προσωπικών πληροφοριών- σε όλα τα προσωπικά δεδομένα και το πώς θα συμμορφωθεί αυτός με τους κανόνες. Για παράδειγμα, αν σε κάποιο τμήμα δεδομένων θεωρηθεί πως πρέπει ένας οργανισμός να σβήσει όλα του τα δεδομένα, πρέπει να διασφαλίζεται πως ο αρμόδιος της διαδικασίας έχει πλήρη πρόσβαση σε αυτά, και πως θα διαγραφούν εξολοκλήρου από το Cloud.

Συμμόρφωση στους νόμους: ποιες οι νομικές απαιτήσεις για το cloud. Ποιοι οι νόμοι, οι αρχές, οι κανόνες, οι περιορισμοί, τα standards που πρέπει να τηρούνται στην διακυβέρνηση της πληροφορίας στο cloud αλλά και ποιος είναι υπεύθυνος για την διατήρηση των παραπάνω στο σύστημα. Πόσο μπορεί να επηρεαστεί η κίνηση στο cloud βάσει της ισχύουσας νομικής προστασίας της ιδιωτικότητας, αλλά και πόσο μπορεί να διαφέρει αυτό ανάλογα με την κάθε χώρα γεωγραφική θέση.

Αποθήκευση: που αποθηκεύονται τα δεδομένα στο cloud. Αν δίνεται η δυνατότητα μεταφοράς τους σε κάποιο άλλο data center ή σε κάποια άλλη χώρα, αν αναμειγνύονται με περαιτέρω πληροφορίες άλλων οργανισμών που χρησιμοποιούν το κέντρο διανομής του cloud συστήματος. Όταν τα δεδομένα αποθηκεύονται στο cloud, πρέπει, ανάλογα με τους ισχύοντες νόμους (γεωγραφικά και καθολικά), να υπάρχει πλήρη γνώση και συμμόρφωση για να μην γίνεται κάποια καταπάτηση της αποθηκευμένης πληροφορίας και των νόμων που την προστατεύουν.

Διατήρηση: ποιος ο χρονικός περιορισμός διατήρησης της πληροφορίας στο cloud, ποια πολιτική τον αποσαφηνίζει αλλά και ποιος είναι ο κάτοχος της πληροφορίας (το κέντρο ή ο οργανισμός). Τέλος, ποιος είναι υπεύθυνος της διατήρησης της πολιτικής

αυτής στο cloud καθώς και ανάλυση της πολιτικές στις επιμέρους απαιτήσεις ανάλογα με το σύστημα.

Καταστροφή: με ποιόν τρόπο επιτυγχάνει ο πάροχος του cloud την καταστροφή των δεδομένων όταν λήξει η περίοδος διατήρησής τους και πως ο κάθε οργανισμός είναι ασφαλής ότι τα δεδομένα έχουν καταστραφεί εντελώς και εξονυχιστικά, δηλαδή δεν έχουν απομείνει αντίγραφα σε συστήματα που αργότερα θα χρησιμοποιηθούν από άλλους οργανισμούς.

Έλεγχος και παρακολούθηση: πως ελέγχουν οι οργανισμοί τα κέντρα παρόχων ώστε να εξασφαλιστεί πως δεν γίνεται με κάποιον τρόπο υποκλοπή προσωπικών δεδομένων κατά το στάδιο της παρακολούθησης της κίνησης πληροφορίας στο cloud.

6.4. Ευθύνη προστασίας την Ιδιωτικότητας

Υπάρχουν συγκρουόμενες απόψεις για το ποιος είναι υπεύθυνος για την ασφάλεια και την ιδιωτικότητα σε συστήματα Cloud Computing. Κάποιες υποχρεώσεις ανατίθενται στους παρόχους. Παρόλο που μπορεί να υπάρχει αλληλομετάθεση της ευθύνης κατά τις συμφωνίες που γίνονται, δεν είναι πιθανή η μεταφορά της τελικής ευθύνης της προστασίας. Στο τέλος, το βάρος της ασφάλειας και της ιδιωτικότητας της πληροφορίας αφορά τον οργανισμό που σύλλεξε την πληροφορία αρχικά. Ακόμα και στην περίπτωση που ο εν λόγο οργανισμός δεν μπορεί να παράσχει το απαιτούμενο υπόβαθρο για τη διασφάλιση των παραπάνω, υποχρεούται να ελέγχει το κέντρο πληροφορίας και τους παρόχους που είναι υπεύθυνοι εν τέλει για την προστασία.

Η ιστορία έχει δείξει πως οι παραβιάσεις των δεδομένων μπορούν να αποφέρουν καταιγιστικές επιδράσεις. Όταν ο οργανισμός χάνει τον έλεγχο των προσωπικών πληροφοριών του χρήστη, τότε ο χρήστης είναι υπεύθυνος για τις παράπλευρες απώλειες που μπορεί να επιφέρει η απώλεια της πληροφορίας, είναι έμμεσα είτε άμεσα. Η υποκλοπή ιδιωτικότητας μπορεί να είναι ένα βασικό αποτέλεσμα αυτού. Στην περίπτωση που ένας χρήστης έχει γίνει θύμα στο cloud, μπορεί να κατηγορήσει τον ευθηνόν της συμφωνίας χρήσης της υπηρεσίας αλλά και τον πάροχο της υπηρεσίας. Η τυφλή εμπιστοσύνη σε κάποια τρίτη οντότητα, όσον αφορά την

προστασία προσωπικών δεδομένων, θεωρείται ανεύθυνη στάση και σίγουρα κρύβει επικινδυνότητα.

Η υπεύθυνη εποπτεία των δεδομένων απαιτεί εξαιρετική γνώση της λειτουργίας του συστήματος και του τεχνολογικού υπόβαθρου καθώς και των νομικών αρχών προστασίας αλλά και νομικών υποχρεώσεων. Μόνο οργανισμοί πολλαπλής λειτουργικότητας είναι ασφαλές να διατηρούν τους μηχανισμούς ασφάλειας και ιδιωτικότητας.

Συνοψίζοντας, το μοντέλο ευθύνης υποβάλλει:

- ✓ Οι οργανισμοί μπορούν να αναθέσουν την προστασία της πληροφορίας αλλά όχι την ευθύνη αυτής
- ✓ Κατά την διάρκεια και τη φάση του κύκλου ζωής των δεδομένων, η αξιολόγηση της επικινδυνότητας και της παράπλευρης αποθήκευσης την πληροφορίας αποτελούν κρίσιμα σημεία
- ✓ Η πολύ καλή γνώση ων νομικών υποχρεώσεων και της συμφωνίας αλλά και της ανάθεσης καθηκόντων. Υπάρχουν, βέβαια, πολλοί νέοι κίνδυνοι, καθώς οι κακόβουλοι χρήστες δεν σταματούν ποτέ να ψάχνουν καινούργιους τρόπους επίθεσης. Για όλους αυτούς τους λόγους, η καθολική ασφάλεια του συστήματος, της πληροφορίας και της ιδιωτικότητας σε Cloud Computing συστήματα, αποτελεί μεγάλη πρόκληση για τους επιστήμονες[14].

6.5. Αλλαγές στην Διαχείριση Κινδύνου και στη Συμμόρφωση των σχέσεων στο Cloud

6.5.1. Αρχή Οριοθέτησης Συλλογής

Η αρχή αυτή προσδιορίζει πως η συλλογή των προσωπικών δεδομένων πρέπει να οριοθετείται στο ελάχιστο ποσοστό δεδομένων που απαιτούνται για να επιτευχθεί ο στόχος της συλλογής. Η συλλογή των δεδομένων θα πρέπει να γίνεται με νόμιμα και

ασφαλή μέσα και με περιληπτική γνώση του περιεχομένου των δεδομένων, όπου αυτή επιτρέπεται.

Όσον αφορά την ιδιωτικότητα, η έλλειψη ιδιαίτερων χαρακτηριστικών των δεδομένων που συλλέγονται από τους παρόχους δημιουργεί κάποια μπερδέματα. Για παράδειγμα, ένας πάροχος Cloud υπηρεσιών είχε δηλώσει «οι πελάτες έρχονται αναμένοντας τα σωστά πράγματα για την ασφάλεια αλλά τα λάθος για την ιδιωτικότητα. Αναμένουν τους καλύτερους μηχανισμούς χωρίς όμως να ξέρουν ποιοι είναι αυτοί». Υπάρχουν ολοκληρωμένες προτάσεις ασφάλειας και standards (όπως τα ISO 27000, Οδηγίες NIST κ.ά.) και οργανισμοί που ξέρουν να τα εφαρμόσουν πολύ σωστά. Παρόλα αυτά, δεν υπάρχει κάποιο διεθνές standard που να αφορά την προστασία της ιδιωτικότητας και που να έχει εφαρμοστεί καθολικά. Αυτό το ρόλο τον παίζουν οι σχετικοί νόμοι, οι οδηγίες και οι ορισμοί της ιδιωτικότητας αλλά και των απαιτήσεων της προστασίας της. Οι περισσότεροι οργανισμοί ακολουθούν μια πορεία σε αυτόν τον τομέα, που τους έχουν υποδείξει και θεωρούν το πιο σωστό πράγμα για το θέμα. Βέβαια, η πορεία αυτή μπορεί να μην συμβαδίζει πάντα με το νομικό πλαίσιο της εκάστοτε χώρας ή εποχής με αποτέλεσμα να υπάρχει απόκλιση στην εφαρμογή των μέτρων διασφάλισης ιδιωτικότητας που χρησιμοποιούνται και στις αρχικές προσδοκίες των πελατών.

Βασική προϋπόθεση είναι να ορίζονται στην αρχή της συμφωνίας με τον οργανισμό τα SLAs (service level-agreements) πριν να γίνει οποιαδήποτε παροχή ή διαμοιρασμός πληροφορίας, καθώς θα είναι δύσκολο να διαπραγματευτεί κανείς για την ασφάλεια της πληροφορίας αυτής από τη στιγμή που βγαίνει στο cloud. Αρχικά, στην αποστολή αίτησης πρότασης (RFP-request for proposal) με έναν SLA target, μπορεί ο χρήστης να αποκλείσει παρόχους που δεν καλύπτουν τις εκφρασμένες του ανάγκες. Τα πολύ καλά καθορισμένα από άποψη ασφάλειας και ιδιωτικότητας SLAs θα πρέπει να είναι μέρος του SOW (statement of Work). Θα πρέπει να διασφαλίζεται ότι το SLA που χρησιμοποιείται καλύπτεται από κάποιες νομικές δικλείδες, ώστε να αποφεύγονται ποινές που μπορεί να υπάρξουν. Ο πελάτης δεν θα πρέπει να παραχωρήσει όλο το σχεδιασμό της χρήσης της υπηρεσίας και των διαπραγματεύσεων στον πάροχο.

Επιπρόσθετα, οι οργανισμοί αντιμετωπίζουν το ρίσκο να διωχθούν ποινικά, καθώς ο διαφορετικός τύπος δεδομένων που συλλέγουν για κάποιες οντότητες, στην πορεία συγχωνεύονται και αποτελούν δελεαστικό αποτέλεσμα.

6.5.2. Χρήση της Αρχής

Η αρχή προσδιορίζει ότι τα προσωπικά δεδομένα δεν θα πρέπει να αποκαλύπτονται ή να είναι διαθέσιμα ώστε να μην χρησιμοποιηθούν για σκοπούς διαφορετικούς από αυτούς της δημιουργίας τους ή ποινικά αποδοκιμασμένους.

Το cloud computing παρέχει μια πληθώρα πληροφοριών, είτε χρηστών είτε εταιριών, σε ένα σημείο. Κατά την μετάδοση των πληροφοριών στο cloud, η σωστή και αυστηρή διακυβέρνηση των δεδομένων απαιτείται για την διασφάλιση της διατήρησης του σκοπού δημιουργίας της πληροφορίας που απαρτίζεται από τα δεδομένα αυτά, καθώς και της χρήσης, του διαμοιρασμού και της συλλογής των δεδομένων. Αυτό είναι πολύ σημαντικό, ειδικά στη περίπτωση που ο οργανισμός χρησιμοποιεί μια κεντρική βάση δεδομένων, καθώς σε μελλοντική χρήση θα είναι δυνατό να χρησιμοποιηθούν τα δεδομένα και να συνδυαστούν για σκοπούς που δεν θα επιτρέπονταν εξ αρχής.

Η δυνατότητα να συνδυαστούν δεδομένα από διαφορετικές πηγές αυξάνει τον κίνδυνο της μη επιτρεπόμενης χρήσης της πληροφορίας κατά την διακυβέρνηση. Κυβερνητικές οργανώσεις ασφάλειας, αιτούνται από τα κέντρα των παρόχων να ενημερώνουν στην περίπτωση που παρατηρήσουν τυχόν τέτοιες συμπεριφορές, ειδικά για συγκεκριμένες κατηγορίες δεδομένων χρηστών.

6.5.3. Αρχή Ασφάλειας

Η ασφάλεια αποτελεί μια σημαντική απαίτηση για να μπορεί να υπάρξει ιδιωτικότητα. Αυτή η αρχή καθορίζει όταν τα προσωπικά δεδομένα θα πρέπει να προστατεύονται από λογικές δικλείδες ασφάλειας απέναντι σε κινδύνους όπως απώλεια ή μη εξουσιοδοτημένη χρήση, καταστροφή, χρήση, διαμόρφωση ή αποκάλυψη της πληροφορίας.

6.5.4. Αρχή Διατήρησης και Καταστροφής

Η αρχή εξασφαλίζει ότι τα προσωπικά δεδομένα δεν κρατούνται περαιτέρω από το χρονικό διάστημα που απαιτείται για να έρθει εις πέρας η εργασία για την οποία συλλέχθηκαν αρχικά, ή παραπάνω από το χρονικό περιθώριο που ορίζεται από τους νόμους. Όταν έρθει, λοιπόν, το πλήρωμα αυτού του χρόνου, τα δεδομένα θα πρέπει να καταστρέφονται.

Το πόσο μπορούν να κρατηθούν τα δεδομένα στο cloud πριν καταστραφούν, αποτελεί ένα κομμάτι έρευνας και συνεχής πρόκλησης για τις εταιρείες. Η συνεχής αύξηση των δεδομένων έχει οδηγήσει σε δημιουργία ορισμών, κανόνων, πολιτικών, και διαδικασίες για την διατήρηση και την καταστροφή των δεδομένων. Οι περισσότερες πολιτικές καθοδηγούνται ή υποβάλλονται από την νομοθεσία και υπηρεσίες (κυβερνητικές και μη) που αφορούν σε αυτό το κομμάτι.

Η διαδικασία της διαγραφής των δεδομένων μερικές φορές ορίζεται αρκετά λυτά. Αυτό που πρέπει κανείς να σκέφτεται είναι κατά πόσο τα αντίγραφα των δεδομένων, τα backup αρχεία ή τα στοιχεία αρχειοθέτησης διαγράφονται πραγματικά χωρίς να αφήνουν κανένα ίχνος. Κατά τη διαγραφή ενός αρχείου, στην ουσία μαρκάρονται τα blocks του δίσκου ως μη χρησιμοποιημένα. Μέχρι, λοιπόν τη στιγμή να γραφτεί κάτι καινούριο πάνω σε αυτά τα blocks, στην ουσία δεν διαγράφεται τίποτα και τα δεδομένα μπορούν να ανακτηθούν. Στην ουσία, στο χώρο του δίσκου που φαίνεται διαθέσιμος εξακολουθούν να υπάρχουν τα δεδομένα και τα blocks θα πρέπει να γραφτούν πολλές φορές άλλα δεδομένα ως την ολοκληρωτική διαγραφή των πρώτων σε σημείο που να είναι αδύνατη και η ανάκτηση της με οποιοδήποτε τρόπο.

Σε πολλές περιπτώσεις, ο δίσκος χρησιμοποιείται ξανά και ξανά προς την εξυπηρέτηση της αποθήκευσης επιπλέον δεδομένων. Βέβαια, η διαγραφή των δεδομένων δεν αποτελεί τόσο μεγάλο θέμα για τους κύκλους ασφάλειας. Παρόλα αυτά, πρέπει με οποιονδήποτε τρόπο να διασφαλίζεται από τους υπεύθυνους ασφάλειας ότι τα δεδομένα δεν θα μπορούν ποτέ να ανακτηθούν.

Η κρυπτογράφηση παίζει σπουδαίο ρόλο στο στάδιο της καταστροφής των δεδομένων. Τα κρυπτογραφημένα δεδομένα μπορούν να καταστραφούν πολύ πιο εύκολα, μόνο καταστρέφοντας το κλειδί της κρυπτογράφησης. Τα δεδομένα δεν

μπορούν να αποκρυπτογραφηθούν με αποτέλεσμα να είναι αδύνατον να ανακτηθεί η πληροφορία.

Πρόβλημα προκύπτει όταν υπάρχει έλλειψη από καλά προσδιορισμένες πολιτικές που αφορούν την καταστροφή δεδομένων σε cloud computing συστήματα. Εικονικές μηχανές αποθήκευσης διατίθενται προς χρήση σε άλλους χρήστες (χωρίς να έχουν διαγραφεί τα δεδομένα), και έπειτα σε άλλους και σε άλλους χρήστες. Οι προσωπικές πληροφορίες που βρίσκονται σε αυτές τις μηχανές μπορούν να είναι ορατές στους επόμενους χρήστες, με αποτέλεσμα να παραβιάζονται τα προσωπικά δεδομένα, η ιδιωτικότητα, οι νόμοι και οι περιορισμοί που τέθηκαν από τον αρχικό χρήστη της εικονικής αυτής μηχανής. Οι servers και οι δίσκοι που χρησιμοποιούνται μπορούν να ρυθμιστούν έτσι ώστε να οριοθετείται αν τα δεδομένα θα είναι διαθέσιμα και μέχρι πότε.

Υπάρχει πληθώρα από επιβεβαιωμένες μεθόδους που υλοποιούν την καταστροφή δεδομένων, την πολλαπλή καταγραφή άλλων (τυχαίων και χωρίς νόημα συνήθως) δεδομένων στα blocks του δίσκου και καταστροφής του κρυπτογραφικού κλειδιού σε περίπτωση κρυπτογραφημένων δεδομένων.

6.5.5. Αρχή Μετάδοσης

Η αρχή της μετάδοσης επιβάλλει πως τα δεδομένα δεν πρέπει να μεταφέρονται σε χώρες που δεν παρέχουν ίσιου επιπέδου νομοθεσίες για την προστασία της ιδιωτικότητας όσο το επίπεδο που προσφέρει ο οργανισμός που συλλέγει την πληροφορία. Σε ένα περιβάλλον cloud computing η υποδομή διαμοιράζεται μεταξύ πολλών οργανισμών και επομένως υπάρχουν πολλές απειλές που σχετίζονται με το γεγονός ότι δεδομένα αποθηκεύονται και επεξεργάζονται από απόσταση, ο αριθμός των κοινόχρηστων πλατφορμών έχει αυξητική πρόοδο και, επομένως, η ανάγκη για προστασία των δεδομένων στο cloud αυξάνεται συνεχώς. Το δυναμικό περιβάλλον του cloud, δηλαδή η δυνατότητα αλληλεπίδρασης υπηρεσιών με δυναμικό τρόπο ανάμεσα στους χρήστες, μπορεί να προσφέρει ένα από τα μεγαλύτερα προτερήματα της τεχνολογίας αλλά συνάμα και ένα από τα μειονεκτήματα στην παροχή ασφάλειας. Ο στόχος την ολοκληρωμένων υπηρεσιών που παρέχονται από πολλούς παρόχους είναι να βελτιστοποιήσουν την δυνατότητα μεταφοράς δεδομένων μέσω τρίτων

οντοτήτων, σε αυτή τη μετάδοση πρέπει να αποκαλυφθεί το περιεχόμενο των δεδομένων πριν τη συλλογή αυτών. Σε πολλές περιπτώσεις υπάρχει η υποχρέωση της ρητής συγκατάθεσης του υποκειμένου των δεδομένων, για την μετάδοση τους. Τυπικά, ο οργανισμός πρέπει να συμφωνήσει με τους default όρους υπηρεσιών των server του παρόχου, χωρίς να δίνεται κάποιο διέξοδο διαπραγμάτευσης. Οι όροι αυτοί κυρίως είναι υπέρ του παρόχου και πάντα υπάρχει η πιθανότητα ο οργανισμός να μην μπορεί να έχει πλήρη γνώση της συμφωνίας που κάνει, καθώς δεν μπορεί να έχει γνώση όλων των διαδικασιών που εμπλέκονται στην υπηρεσία.

Η μετάδοση της πληροφορίας στο cloud αποτελεί πρόκληση στο cloud γιατί τα δεδομένα θα μπορούσαν να βρίσκονται οπουδήποτε στον κόσμο (ως φυσική θέση). Συνήθως, ούτε οι ίδιες οι εταιρίες που χρησιμοποιούν συστήματα Cloud computing δεν ξέρουν που βρίσκονται τα δεδομένα τους ανά πάσα στιγμή, ούτε καν την χώρα. Αντί τα δεδομένα να αποθηκεύονται στους Servers της εταιρίας, αποθηκεύονται σε οποιοδήποτε μέρος της υφηλίου. Αυτό το δόγμα του cloud computing έρχεται σε αντίθεση με πολλούς από τους νομικούς περιορισμούς, όπως για παράδειγμα το Ευρωπαϊκό νομικό πλαίσιο για την προστασία των επικοινωνιών, οπότε, για να πληρούνται αυτοί οι περιορισμοί και νόμοι ίσως απαιτούνται περαιτέρω έλεγχοι και καταγραφές των μεταφερόμενων δεδομένων, που φυσικά διαφέρουν ανά περίπτωση.

6.5.6. Αρχή Ευθύνης

Βάσει αυτής της αρχής ο οργανισμός είναι υπεύθυνος για τα προσωπικά δεδομένα που βρίσκονται υπό τον έλεγχο του και πρέπει να ορίζει την οντότητα ή τις οντότητες που ευθύνονται για την συμμόρφωση του οργανισμού με τις αρχές και τους κανόνες. Η ευθύνη κατά το cloud μπορεί να επιτευχθεί μέσω πολιτικών ασφάλειας για τα δεδομένα και τους μηχανισμούς που επιβεβαιώνουν ότι οι πολιτικές αυτές ακολουθούνται από όποιον εμπλέκεται με τη χρήση, αποθήκευση, επεξεργασία ή διαμοιρασμό δεδομένων.

Ο δρόμος για την πρόοδο είναι οι οργανισμοί να επενδύσουν στην ευθύνη της πληροφορίας και στους μηχανισμούς που είναι υπεύθυνοι για την λήψη αποφάσεων που αφορούν προστασία πληροφοριών. Ειδικότερα, οι οργανισμοί που φέρουν

ευθύνη πρέπει να διασφαλίζουν πως οι περιορισμοί για την ιδιωτικότητα τηρούνται από όλα τα συμβαλλόμενα στο cloud μέλη[9].

6.6. Μοντέλα Εμπιστοσύνης

Για να έχει έννοια ο ορισμός της Προστασίας σε συστήματα Cloud Computing θα πρέπει να τηρούνται κάποιες απαιτήσεις εμπιστοσύνης. Οι επιστήμονες, έχουν αναπτύξει τα μοντέλα εμπιστοσύνης που αναλύονται παρακάτω, ώστε να είναι πιο εύκολος ο προσδιορισμός του τι προστασία χρειάζεται ο κάθε χρήστης cloud ανάλογα με το επίπεδο εμπιστοσύνης που ανήκει .

6.6.1. Μοντέλο Εμπιστοσύνης Khan & Malluhi

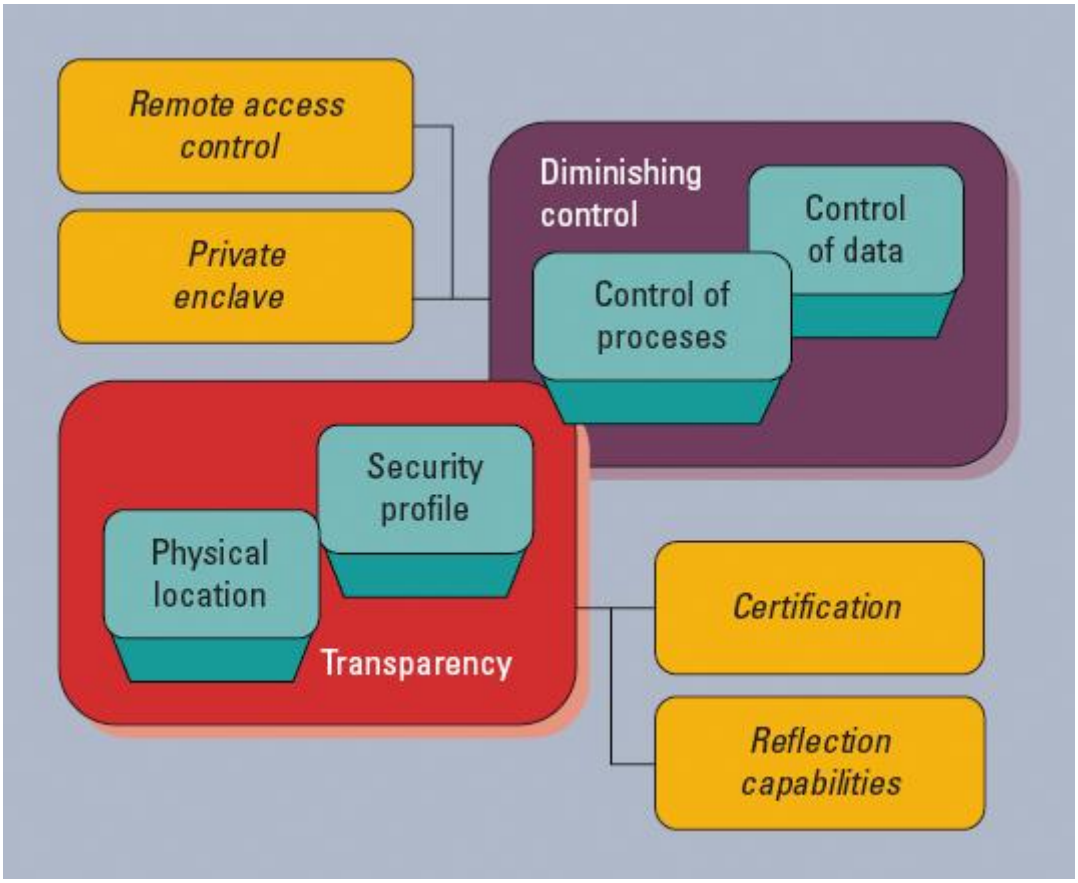
Λόγω της έλλειψης διαφάνειας, μη ξεκάθαρες διασφαλίσεις για την προστασία και την ασφάλεια του υπολογιστικού νέφους αλλά και της απώλειας ελέγχου, οι χρήστες αδυνατούν να εμπιστευτούν απόλυτα τις σύγχρονες πλατφόρμες του cloud. Το πρώτο μοντέλο εμπιστοσύνης, που πρότειναν σε σχετική μελέτη τους οι Khan και Malluhi έχει ως εξής:

- Ο πάροχος ενημερώνει τον πελάτη κάθε φορά που μια οντότητα έχει πρόσβαση σε αρχεία που είναι στην δικαιοδοσία του
- Το κέντρο δεδομένων του παρόχου, και όποιο άλλο κέντρο δεδομένων εμπλέκεται στην επικοινωνία, δεν αποθηκεύουν δεδομένα που αφορούν τον πελάτη, ούτε σε αντίγραφα ασφαλείας έως ότου να λάβουν εξουσιοδότηση από τον ιδιοκτήτη
- Ο πάροχος θα πρέπει να καταστρέψει αρχεία και δεδομένα από όλα τα κέντρα δεδομένων που διαχειρίζεται, όταν ο σκοπός της πληροφορίας που απαρτίζουν τα δεδομένα έχει έρθει εις πέρας

Το μοντέλο αυτό, εξασφαλίζει ότι υπάρχει έλεγχος των διεργασιών και των εφαρμογών που ευθύνονται για την επεξεργασία των προσωπικών δεδομένων των χρηστών. Ο εκάστοτε χρήστης οφείλει να γνωρίζει (να απαιτεί την γνώση) την τοποθεσία του server που αποθηκεύονται τα δεδομένα του και ποιες οντότητες

εμπλέκονται στην επεξεργασία τους. Ο πάροχος οφείλει να κάνει γνωστό στον χρήστη όλα τα χαρακτηριστικά και τα μέτρα ασφάλειας που ορίζονται από το επίπεδο της ασφάλειας που παρέχει η υπηρεσία που εμπλέκεται.

Υπάρχουν συγκεκριμένες τεχνολογίες που απαιτούνται για την επίτευξη του μοντέλου εμπιστοσύνης αυτού. Φλέγοντα θέματα είναι η κρυπτογράφηση και η διασφάλιση της ιδιωτικότητας των δεδομένων όπως επίσης και ξ εφαρμογή τεχνολογιών όπως είναι οι ψηφιακές υπογραφές και οι μηχανισμοί ελέγχου πρόσβασης που συμβάλλουν στην διατήρηση της ακεραιότητας των δεδομένων. Πλέον, δύναται η επεξεργασία κρυπτογραφημένων δεδομένων από τους παρόχους cloud υπηρεσιών χωρίς να απαιτείται η αποκρυπτογράφηση των δεδομένων αυτών ή μόνο με μερική αποκρυπτογράφηση.



Σχήμα 6.3. Απεικόνιση μοντέλου εμπιστοσύνης Khan & Malluhi

Πηγή http://www.computer.org/csdl/mags/it/2010/05/mit2010050020-abs.html

6.6.2. Μοντέλο Εμπιστοσύνης Sato, Kanai & Tanimoto

Πρόκειται για μια πλατφόρμα που παρέχει εγγύηση ότι η διοίκηση και η λειτουργία σε έναν προβλεπόμενο κύκλο εμπιστοσύνης τηρούνται, κάτι που ελέγχεται από τον οργανισμό. Η εμπιστοσύνη εξασφαλίζεται με την εφαρμογή συστημάτων (Trust Platform Models). Σε περίπτωση που κάτι απαιτεί μεγάλης κλίμακας ασφάλεια από τον οργανισμό τοποθετείται στον κύκλο εμπιστοσύνης. Επιβάλλεται, φυσικά, ο κύκλος εμπιστοσύνης του συστήματος να παραμένει εντός του οργανισμού.

Το επίπεδο συμβατικής εμπιστοσύνης προσδιορίζει ότι η εμπιστοσύνη εξασφαλίζεται από το συμβόλαιο του παρόχου και του οργανισμού. Το συμβόλαιο εμπιστοσύνης περιλαμβάνει τους εξής τύπου εγγράφου:

- Δήλωση Πολιτικής - Πρακτικής Υπηρεσιών: δηλώνει ποιο επίπεδο ασφάλειας των υπηρεσιών που εγγυάται ο πάροχος

- Δήλωση Πολιτικής -Πρακτικής Αναγνωριστικών Ταυτοποίησης: δηλώνει το επίπεδο ποιότητας και ασφάλειας αναγνωριστικών των παρόχων άρα και τον βαθμό εμπιστοσύνης από την οπτική του παρόχου της cloud computing υπηρεσίας προς τους χρήστες της.

- Σύμβαση: ορίζει ποιος οργανισμός μπορεί να χρησιμοποιεί τις υπηρεσίες κάποιου παρόχου cloud και επιβεβαιώνει ότι ο οργανισμός έχει πλήρη γνώση και ευθύνη όσων αναφέρονται στα δύο παραπάνω έγγραφα.

Τα επίπεδα αυτά εμπιστοσύνης αφορούν χαρακτηριστικά που καταμετρούνται για την ασφάλεια. Κατά συνέπεια, ανάλογα με τις ανάγκες του οργανισμού και το κόστος, τα μέτρα μπορούν να γίνουν πιο αυστηρά ή πιο χαλαρά.

6.6.3. Μοντέλο Εμπιστοσύνης Hwang, Kulkareni & Hu

Στο μοντέλο αυτό εμπιστοσύνης βασικό είναι η προστασία των δημόσιων συστημάτων νεφών. Δημιουργεί μια ιεραρχία δικτύων επικάλυψης που συνδυάζονται μεταξύ τους μέσω κατανεμημένων πινάκων (hash). Με αυτόν τον τρόπο

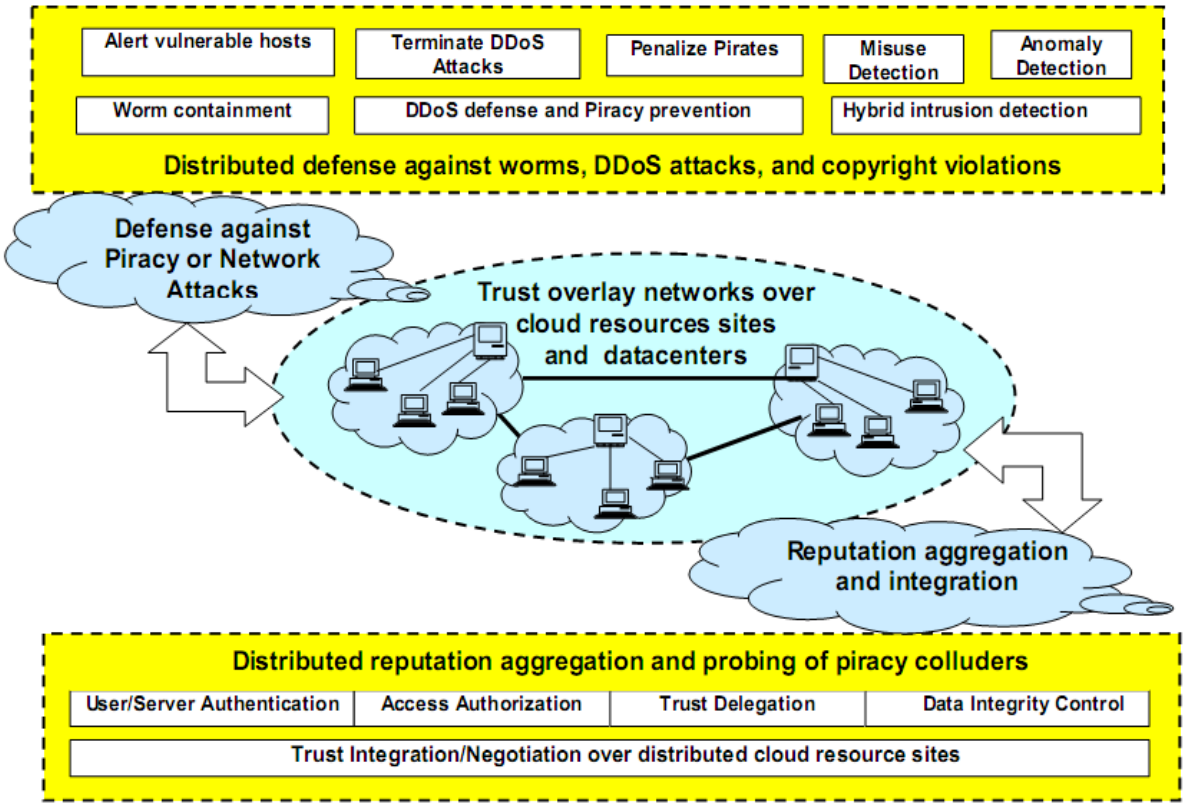
διαμορφώνονται συστήματα ελέγχου του βαθμού αξιοπιστίας και της εμπιστοσύνης των συστημάτων.

Στο παρακάτω σχήμα αναλύεται το επίπεδο εμπιστοσύνης κατά το οποίο:

- Στο κάτω επίπεδο συγκεντρώνονται τα στοιχεία για το επίπεδο αξιοπιστίας και διαθέσιμων κόμβων στο παρεχόμενο cloud και διαδίδει στοιχεία για πιθανή χρήση παράνομων προγραμμάτων λογισμικού

- Στο πιο υψηλό επίπεδο ενεργοποιούνται μηχανισμοί για την προστασία από ιούς, γίνεται έλεγχος για εντοπισμό προσπάθειας εισβολής στο σύστημα (IDS τύπου), αλλοίωση δεδομένων προσωπικού τύπου ή καταπάτησης πνευματικών δικαιωμάτων και ιδιωτικότητας

- Τέλος, προστατεύεται η ιεραρχία πόρων του cloud μέσω end-to-end συστημάτων ελέγχου αξιοπιστίας (για παράδειγμα ελέγχονται ιστότοποι, βάσεις δεδομένων, αρχεία).



Σχήμα 6.4. Απεικόνιση μοντέλου εμπιστοσύνης Hwang, Kulkareni & Hu

Τα δεδομένα που αφορούν σε χρήστες αντιγράφονται σε κατανεμημένα κέντρα δεδομένων και πιο συγκεκριμένα σε δίκτυα αποθήκευσης δεδομένων. Επομένως, οι χρήστες μπορούν να χρησιμοποιήσουν τα δεδομένα τους από οποιοδήποτε αφού η επιλογή του κέντρου δεδομένων που εξυπηρετούν ένα αίτημα ακολουθεί χωροταξικά κριτήρια. Ο κάθε χρήστης έχει στη διάθεσή του τα απαραίτητα κλειδιά ανάλογα με την υπηρεσία που έχει επιλέξει.

6.6.4. Μοντέλο Εμπιστοσύνης Wenjuan Li & Lingdi Ping

Όταν έχουμε μεγάλης κλίμακας αρχιτεκτονικές Cloud Computing όπου διαφορετικοί πάροχοι αλληλεπιδρούν στοχεύοντας στην παροχή ενιαίων υπηρεσιών σε τελικούς χρήστες, προτείνεται αυτό το μοντέλο εμπιστοσύνης. Βάση αυτού, οι χρήστες μπορούν να διατηρήσουν έναν πίνακα εμπιστοσύνης (customer trust table) σημειώνοντας το επίπεδο εμπιστοσύνης των υπηρεσιών που τους προσφέρει ο κάθε πάροχος. Αυτή η πληροφορία λαμβάνεται μέσω ενός μηχανισμού και γίνεται

υπόδειξη συστάσεων για τις υπηρεσίες που προσφέρονται από έναν πάροχο συγκριτικά με κάποιον άλλον από τους συνεργαζόμενους στο σύστημα. Οι συστάσεις αυτές καταγράφονται σε ένα πίνακα της παρακάτω μορφής:

Domain name	Service type	Trust value/trust degree	Generation time

Domain name	Cooperation type	Trust value/trust degree	Generation time

Ο πρώτος πίνακας αφορά στην καταμέτρηση του βαθμού εμπιστοσύνης του κάθε παρόχου, ενώ ο δεύτερος στη καταμέτρηση του βαθμού εμπιστοσύνης συνεργάτη αντίστοιχα.

Από την σκοπιά των παρόχων, διατηρούνται πίνακες εμπιστοσύνης (domain trust table). Οι πάροχοι λειτουργούν κατανεμημένα αν και είναι υπεύθυνοι για ένα συνεργατικό επίπεδο παροχής υπηρεσιών με την χρήση των παρεχόμενων κατανεμημένων πόρων. Ο πίνακας που διατηρούν τους εξυπηρετεί στην ανίχνευση της αξιοπιστίας των υποψήφιων συνεργατών ώστε να διαμορφώσουν την πιο αξιόπιστη πρόταση για τον τελικό χρήστη. Η αλληλεπίδραση μεταξύ των συνεργατών ώστε να διαμορφωθεί το επίπεδο της καθολικής εμπιστοσύνης πραγματοποιείται μέσω παραγόντων (agents).

Με αυτό το μοντέλο, επιτρέπεται στους πελάτες να λαμβάνουν αποφάσεις για τον πάροχο που θέλουν να επιλέξουν, με συνιστώσα τις πληροφορίες που τους παρέχονται για την εμπιστοσύνη. Από την πλευρά του παρόχου, επιλέγεται ο κάθε συνεργάτης αξιολογώντας τον βαθμό εμπιστοσύνης ανά τύπο υπηρεσίας που καταγράφονται στους πίνακές τους. Σε κάθε περίπτωση ορίζεται ένα όριο υπό το οποίο τίθεται η συνεργασία με κάθε υφιστάμενο πάροχο και χρήστη ώστε να αποφασιστεί αν η κάθε συνεργασία διακόπτεται είτε διαιωνίζεται. Η ενημέρωση του κάθε πίνακα γίνεται μετά από κάθε συναλλαγή.

6.7. Συνοπτικά

Στο κεφάλαιο αυτό αναλύθηκε η έννοια της ιδιωτικότητας, η διαφοροποίηση της από την ασφάλεια και η σημαντικότητά της σε συστήματα υπολογιστικού νέφους.

Είναι πια σαφές ότι η πληροφορία μπορεί να έχει πολλά στάδια κύκλου ζωής, κατά τα οποία οι εκτίθεται σε κινδύνους και συνάμα εξυπηρετεί σκοπούς προστασίας. Η προστασία της ιδιωτικότητας αποτελεί φλέγον ζήτημα στα συστήματα Cloud Computing στις μέρες μας, κάτι που φαίνεται με τον ολοένα αυξανόμενο αριθμό κανόνων και νόμων στο θέμα. Η ύπαρξη των Αρχών που αφορούν στην ροή των δεδομένων που απαρτίζουν πληροφορίες (ειδικά αν αυτές είναι πληροφορίες προσωπικού χαρακτήρα) αποτελεί σημαντικό κομμάτι στην προστασία των χρηστών συστημάτων υπολογιστικού νέφους.

Επιπλέον, η προστασία σε Cloud μπορεί να απαιτηθεί μέσω εγγράφων και συμβολαίων που ορίζονται από διάφορα μοντέλα εμπιστοσύνης που έχουν αναλυθεί από επιστήμονες τα τελευταία χρόνια. Τα μοντέλα αυτά εμπιστοσύνης εξυπηρετούν κυρίως στην προστασία των τελικών χρηστών ενός συστήματος αλλά και στην υποχρέωση που έχουν οι πάροχοι απέναντι τους τελικούς χρηστές αλλά και στους συνεργαζόμενους παρόχους εντός ενός μεγάλου καθολικού Cloud.

Η προστασία ενός τελικού χρήστη μιας υπηρεσίας υπολογιστικού νέφους ξεκινά και τελειώνει στην συμφωνία με τον πάροχο, στην αμοιβαία εμπιστοσύνη μεταξύ των δύο άκρων αλλά κυρίως στην δέσμευση των παρόχων και των συνεργατών τους ότι τηρούνται οι μηχανισμοί της ασφάλειας και προστασίας της ιδιωτικότητας σε όλα τα στάδια της επικοινωνίας. Αν τηρούνται οι μηχανισμοί αυτοί και υπάρχει σεβασμός και από τα δύο άκρα στο άλλο μπορούμε να μιλάμε για διατήρηση της προστασίας[21],[22].

ΚΕΦΑΛΑΙΟ 7: ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΥΠΑΡΧΟΝΤΑ SECURITY MEASURES

7.1. Εισαγωγή

Στο παρόν κεφάλαιο θα συνοψίσουμε όλους τους τρόπους προστασίας που θα πρέπει να αναλάβει ένας πελάτης υπηρεσιών Cloud ώστε να ελαχιστοποιήσει τους κινδύνους και τις επιθέσεις που προέρχονται από τη χρήση του Νέφους. Είναι σίγουρο πως από την πρώτη εμφάνιση του Cloud Computing μέχρι σήμερα έχουν γίνει σημαντικά βήματα προς αυτή την κατεύθυνση. Οι πάροχοι υπηρεσιών Cloud (Cloud service providers CSPs) έχουν γίνει όλο και πιο ενεργοί στην εφαρμογή επιθετικών μέτρων για την αντιμετώπιση των θεμάτων που τέθηκαν σε προηγούμενα κεφάλαια, καθώς και άλλες σχετικές ανησυχίες για την ασφάλεια..

7.2. Μέτρα ασφάλειας

Παρακάτω παρουσιάζονται μερικές από τις πρωτοβουλίες που οι πάροχοι έχουν αναλάβει για την ενίσχυση της ασφάλειας στο σύννεφο:

Συστήματα ανίχνευσης εισβολών (Intrusion Detection Systems IDSs): Παραδοσιακά, διάφοροι τύποι συστημάτων IDS έχουν υλοποιηθεί και χρησιμοποιηθεί με επιτυχία σε δίκτυα υψηλής έντασης για την παρακολούθηση και καταγραφή δραστηριοτήτων, προκειμένου να εντοπιστούν πιθανές εισβολές κακόβουλες δραστηριότητες ή παραβιάσεις της πολιτικής. Ορισμένα από αυτά τα συστήματα προβαίνουν σε συγκεκριμένες ενέργειες για να καταπνίξουν απόπειρες εισβολής, αλλά ακριβώς για όλα αυτά είναι αποτελεσματικές στον εντοπισμό και την αναφορά πιθανών συμβάντων. Στο παράδειγμα όμως για το cloud, το διακύβευμα είναι μεγαλύτερο όπως επίσης και οι προκλήσεις.

Απόπειρες εισβολής είναι δυνητικά πιο εύστοχες (για παράδειγμα, ο εισβολέας μπορεί να είναι ο ανταγωνιστής ενός πελάτη cloud υπηρεσιών) και η πολυπλοκότητα του νέφους μπορεί να επιμηκύνει τα όρια ενός παραδοσιακού συστήματος IDS.

Ευτυχώς, multi-threaded κατανεμημένα μοντέλα ανίχνευσης εισβολής όπως έχει αναφερθεί έχει αποδειχθεί ότι λειτουργούν πολύ αποτελεσματικά στο σύννεφο.

Η ανάπτυξη αισθητήρων των συστημάτων IDS σε ξεχωριστά επίπεδα νέφους (επίπεδο εφαρμογής, επίπεδο συστήματος, και επίπεδο πλατφόρμας) διαχειριζόμενα από μια multi-threaded ουρά και διατυπωμένα στο πλαίσιο ενός συντονισμένου μηχανισμού επικοινωνίας σε μια ενιαία πλατφόρμα μπορεί να μετριάσει σημαντικά τις πολυπλοκότητες που υπάρχουν στο περιβάλλον Cloud.

Συστήματα Ασφάλειας Πληροφοριών και Διαχείρισης Συμβάντων (Security Information and Event Management Systems SIEM): Τα παραδοσιακά συστήματα SIEM κατευθύνουν την αντιμετώπιση των βασικών αναγκών ασφάλειας σε πολλά επίπεδα: παρακολούθησης, ειδοποίησης, δημιουργίας εκθέσεων, ανάλυσης των τάσεων, και τήρησης της ασφάλειας. Αυτό που κάνουν αυτά τα συστήματα είναι να συλλέγουν συνεχώς δεδομένα του συστήματος και να δημιουργούν αναφορές, οι οποίες στη συνέχεια συσχετίζονται και αναλύονται. Επίσης ανταποκρίνεται αυτόματα για την επίλυση των συμβάντων ασφαλείας.

Η μεγάλη ανακάλυψη των τελευταίων ετών υπήρξε η δυνατότητα να αναπτυχθούν συστήματα SIEM σε περιβάλλοντα Cloud. Αυτό κατέστη δυνατό σε μεγάλο βαθμό μέσω της τεχνολογικής προόδου στην ταχύτητα (ταχύτεροι ρυθμοί συλλογής) και τον όγκο (ικανότητα χειρισμού εκατομμυρίων πηγών αποθήκευσης καθημερινά). Χάρη σε αυτές τις εξελίξεις, πολλοί πάροχοι Cloud υπηρεσιών είναι πλέον σε θέση να προσφέρουν τη δημιουργία και διαχείριση της έκθεσης των δεδομένων ως κοινές υπηρεσίες μέσα στο σύννεφο.

Firewalls: Οι προκλήσεις για την ασφάλεια που τίθενται από το νέφος κάνουν τα firewalls περισσότερο αναγκαία από ποτέ. Αλλά συνήθως, τα firewalls για τις Web εφαρμογές (WAF) έχουν «δεθεί» σε συσκευές hardware, προκαλώντας ένα σοβαρό δίλημμα για τους παρόχους υπηρεσιών Cloud. Ασφάλεια και αποδοτικότητα βρίσκεται το ένα ενάντια στο άλλο όταν οι πάροχοι αναγκάζονται να υποστηρίξουν ένα μεγάλο φάσμα εξειδικευμένων μηχανημάτων WAF (μία ανά πελάτη), όταν αυτό που προσπαθούν να επιτύχουν, αντίθετα, είναι ένα πλήρως εικονοποιημένο περιβάλλον. Ευτυχώς, το πρόβλημα αυτό λύνεται με την έναρξη των κατανεμημένων firewalls για εφαρμογές, τα οποία είναι σε θέση να εξυπηρετήσουν όλο το φάσμα των

παραδοσιακών και εικονικών τεχνολογιών που χρησιμοποιούνται από τους παρόχους cloud υπηρεσιών για να λειτουργήσουν τα σύννεφα τους. Σε μια σχετική ανάπτυξη, οι πάροχοι κάνουν επίσης φιλελεύθερη χρήση των πληρεξουσίων σε επίπεδο εφαρμογής που υλοποιούνται μέσα σε μια περίμετρο του τείχους προστασίας για να κατανοήσουν και να ερμηνεύσουν τη διάδοση δεδομένων στο πρωτόκολλο εντολής της συγκεκριμένης εφαρμογής. Αυτά τα πληρεξούσια βασίζεται σε μοντέλα αποκεντρωμένου έλεγχου της ροής πληροφοριών (DIFC), τα οποία διαθέτουν μια αποκεντρωμένη δημιουργία και διαχείριση των τάξεων ασφάλειας κατά το χρόνο εκτέλεσης - μια κρίσιμη δυναμική όταν εργαζόμαστε σε περιβάλλοντα Cloud.

Πρότυπα Ασφαλείας Βιομηχανίας: Ίσως η πιο σημαντική εξέλιξη όσον αφορά την ασφάλεια στο cloud computing τα τελευταία χρόνια είναι η διάδοση των προτύπων της βιομηχανίας και των απαιτήσεων πιστοποίησης που σχετίζονται με την ασφάλεια των πληροφοριών. Αυτές περιλαμβάνουν:

Πιστοποίηση ISO / IEC 27001, το οποίο καθορίζει τους κανόνες που ένα σύστημα διαχείρισης θα πρέπει να πληροί προκειμένου να διασφαλιστεί ότι ένα μετρήσιμο και επαρκές επίπεδο ασφάλειας και διαχείρισης κινδύνων των δεδομένων εφαρμόζεται. Το ISO / IEC 27001 είναι ένα πρότυπο σύστημα διαχείρισης ασφάλειας πληροφοριών (ISMS) το οποίο δημοσιεύθηκε τον Οκτώβριο του 2005 από το Διεθνή Οργανισμό Τυποποίησης (ISO) και τη Διεθνή Ηλεκτροτεχνική Επιτροπή (IEC). Αν και δεν είναι επικεντρωμένο στην cloud τεχνολογία, αυτό το πρότυπο έχει καθιερωθεί ως βάση στη cloud βιομηχανία και σημείο αναφοράς ως προς τη συμμόρφωση ασφάλειας από τους παρόχους. Για να γίνει η πιστοποίηση, οι προμηθευτές υποχρεούνται να ικανοποιήσουν μια διαδικασία ελέγχου τριών σταδίων που αναλαμβάνονται από ανεξάρτητους ελεγκτές και ελέγχονται σε τακτά χρονικά διαστήματα στη συνέχεια.

Εγγραφή στην CSA STAR (Cloud Security Alliance’ s Security, Trust, & Assurance registry): Το 2011, το Συμβούλιο Ασφαλείας Cloud (CSA) ξεκίνησε μια νέα πρωτοβουλία για την προώθηση της διαφάνειας των πρακτικών ασφάλειας ανάμεσα στους παρόχους Cloud υπηρεσιών. Η STAR είναι ένα δωρεάν και προσβάσιμο για το κοινό μητρώο που τεκμηριώνει τους ειδικούς ελέγχους ασφαλείας που παρέχονται από διάφορους παρόχους. Το μητρώο είναι ανοιχτό σε όλους τους παρόχους Cloud, οι οποίοι μπορούν να υποβάλλουν τις εκθέσεις αυτοαξιολόγησης που να τεκμηριώνουν

τη συμμόρφωση με τις βέλτιστες πρακτικές της CSA. Το μητρώο STAR είναι εύκολα προσβάσιμο και με δυνατότητα αναζήτησης, καθιστώντας το μια μεγάλη πηγή για τους πελάτες cloud υπηρεσιών να επανεξετάσει τις πρακτικές ασφάλειας διαφορετικών παρόχων. Με διάφορους τρόπους, είναι ένα μεγάλο βήμα προς τη διαφάνεια της βιομηχανίας και όσον αφορά τα κίνητρα για τους παρόχους θα μπορούσαμε να πούμε ότι με αυτό τον τρόπο ασκούν ιδιαίτερη επιμέλεια και πληρότητα στα μέτρα ασφαλείας σύννεφο τους.

Το **Cloud Control Matrix (Cloud Control Matrix CCM)** είναι ένα βασικό σύνολο ελέγχων ασφαλείας που δημιουργήθηκε από το CSA. Οργανωμένη σε κατηγορίες, η μήτρα αυτή αποτελείται από ένα μεγάλο κατάλογο ελέγχων ασφαλείας που αντιστοιχίζονται με μία ποικιλία από καλά αναγνωρισμένα πρότυπα ασφάλειας της βιομηχανίας. Η CCM είναι ακόμη ένα πολύτιμο εργαλείο που μπορεί να βοηθήσει τους υποψήφιους πελάτες στην αξιολόγηση των κινδύνων ασφάλειας που σχετίζονται με έναν πάροχο Cloud Computing.

Η ευρέως διαδεδομένη αντίληψη ότι μια υποδομή site-specific είναι εγγενώς πιο ασφαλής από μια υποδομή που διαχειρίζεται από έναν φορέα παροχής υπηρεσιών στο σύννεφο μπορεί πλέον να χαρακτηριστεί με ασφάλεια ως μια παρανόηση. Παρόλο που η ασφάλεια στο σύννεφο θέτει πάντα μεγάλες προκλήσεις, αυτές οι προκλήσεις ασφάλειας έχουν αντιμετωπιστεί σε μεγάλο βαθμό[20].

7.3. Βήματα διαβεβαίωσης της ασφάλειας στο Cloud Computing

Προς την κατεύθυνση της δημιουργίας μιας ολοκληρωμένης αντίληψης των χρηστών υπηρεσιών cloud προχώρησε και το συμβούλιο Cloud Standards Customer Council (CSCC) δημιουργώντας ένας οδηγό 10 βημάτων προκειμένου οι χρήστες να μην παραβλέψουν την πλειοψηφία των παραμέτρων ασφάλειας που θα πρέπει να λάβουν. Τα βήματα αυτά είναι τα παρακάτω:

7.3.1. Επιβεβαίωση της ύπαρξης αποτελεσματικών διαδικασιών διακυβέρνησης, κινδύνου και συμμόρφωσης

Το πιο ευρέως αναγνωρισμένο διεθνές πρότυπο για την τήρηση της ασφάλειας των πληροφοριών είναι το πρότυπο ISO / IEC 270014 οποίο περιλαμβάνει διάφορες παραλλαγές και καλά ανεπτυγμένο καθεστώς πιστοποίησης. Το ISO αναπτύσσει συνεχώς νέα πρότυπα, ISO / IEC 270175 «Ασφάλεια στο Cloud Computing" και το πρότυπο ISO / IEC 270186 "Ιδιωτικότητα στο Cloud Computing", τα οποία θα ασχοληθούν με συγκεκριμένα ζητήματα ασφάλειας και ιδιωτικότητας του Cloud κατά το πρότυπο ISO / IEC 27001. Επίσης, υπάρχουν και άλλοι οργανισμοί που προσφέρουν τέτοιου είδους πλαίσια και πιστοποιήσεις όπως είναι οι American Institute of Certified Public Accountants (AICPA), Information Systems Audit and Control Association (ISACA), Cloud Security Alliance (CSA) και άλλες.

7.3.2. Έλεγχος λειτουργικών και επιχειρησιακών διαδικασιών

Η συμμόρφωση Ασφαλείας όπως αναφέρθηκε και στην προηγούμενη ενότητα τείνει να είναι ένα σημαντικό στοιχείο κάθε πλαισίου συμμόρφωσης. Υπάρχουν τρεις σημαντικές περιοχές όπου η εξέταση των μεθόδων ασφαλείας για το Cloud Computing παρουσιάζουν ιδιαίτερο ενδιαφέρον για τους αλλά και τους καταναλωτές cloud υπηρεσιών:

1. Η κατανόηση του εσωτερικού περιβάλλοντος ελέγχου του παρόχου, συμπεριλαμβανομένων των κινδύνων, των ελέγχων και άλλων θεμάτων διακυβέρνησης.

2. Πρόσβαση στο μονοπάτι ελέγχου της εταιρείας, συμπεριλαμβανομένου της ροής εργασίας και άδειας, όταν η διαδρομή ελέγχου καλύπτει τις υπηρεσίες Cloud.

3. Διασφάλιση των εγκαταστάσεων για τη διαχείριση και τον έλεγχο των υπηρεσιών Cloud που διατίθενται στους καταναλωτές από τους παρόχους και τον τρόπο με τον οποίο τέτοιες εγκαταστάσεις είναι εξασφαλισμένες.

Εκτός από τους ελέγχους που εφαρμόζονται στις Cloud υπηρεσίες, υπάρχει επίσης ανάγκη για τους παρόχους να μπορούν οι καταναλωτές να διαχειρίζονται και παρακολουθούν στενά τη χρήση του Cloud που φιλοξενεί τις εφαρμογές και τις υπηρεσίες τους. Οι παροχές αυτές μπορούν να περιλαμβάνουν: καταλόγους υπηρεσίας, συνδρομητικές υπηρεσίες, διαδικασίες πληρωμής, δεδομένα μέτρησης της χρήσης, των παροχών για τη ρύθμιση των υπηρεσιών, συμπεριλαμβανομένων της προσθαφαίρεσης χρηστών και τη διαμόρφωση των αδειών.

7.3.3. Διαχείριση ανθρώπων, ρόλων και ταυτοτήτων

Στον παρακάτω πίνακα επισημαίνονται τα βασικά σημεία που ένας πάροχος θα πρέπει να υποστηρίζει, προκειμένου ο καταναλωτής να διαχειρίζεται αποτελεσματικά τους ανθρώπους, τους ρόλους και ταυτότητες στο σύννεφο:

Provider Supports	Consumer Considerations and Questions
Federated Identity Management (FIM), External Identity Providers (EIP)	• Enterprises that are cloud consumers, in many cases, already have an existing database of users, most likely stored in an enterprise directory, and they wish to leverage this user database without recreating user identities. • Question to cloud provider: Can I integrate my current user store (internal database or directory of users) without recreating all my users within your cloud environment?
Identity Provisioning and Delegation	• Consumer organizations need to administer their own users; the cloud provider should support delegated administration. • Question to cloud provider: What provisioning tools do you provide for on-boarding and off-boarding users? • Question to cloud provider: Does your platform offer delegated administration for my organization to administer users?

Single Sign-On (SSO), Single Sign-Off	• Consumer organizations may wish to federate identity across applications to provide single-sign-on (SSO) along with single sign-off to assure user sessions get terminated properly. For example, an organization using separate SaaS applications for CRM and ERP would like single-sign-on and sign-off across these applications (e.g. using standards such as SAML[12], WS-Federation[13] and OAuth[14]). • Question to cloud provider: Do you offer single-sign-on for access across multiple applications you offer or trusted federated single-sign-on across applications with other vendors?
Identity and Access Audit	• Consumers need auditing and logging reports relating to service usage for their own assurance as well as compliance with regulations. • Question to cloud provider: What auditing logs, reports, alerts and notifications do you provide in order to monitor user access both for my needs and for the needs of my auditor?
Robust Authentication	• For access to high value assets hosted in the cloud, cloud consumers may require that their provider support strong, multi-factor, mutual and/or even biometric authentication. • Question to cloud provider: If required, does your platform support strong, multi-factor or mutual authentication?
Role, Entitlement and Policy Management	• Cloud consumers need to be able to describe and enforce their security policies, user roles, groups and entitlements to their business and operational applications and assets, with due consideration for any industry, regional or corporate requirements. • Question to cloud provider: Does your platform offer fine-grained access control so that my users can have different roles that do not create conflicts or violate compliance guidelines?

Πίνακας 7.1: Υποστήριξη του παρόχου για το προσωπικό, τους ρόλους, και τις ταυτότητες

7.3.4. Εξασφάλιση της ορθής προστασίας των δεδομένων και των πληροφοριών

Οι γενικές προσεγγίσεις για την ασφάλεια των δεδομένων περιγράφονται σε προδιαγραφές, όπως το πρότυπο ISO 27002 – και ειδικότερα στο πιο εξειδικευμένο για την τεχνολογία cloud πρότυπο ISO 27017. Οι έλεγχοι ασφαλείας, όπως περιγράφονται στο πρότυπο ISO 27002 τονίζουν τα γενικά χαρακτηριστικά που πρέπει να αντιμετωπιστούν, και στα οποία στη συνέχεια μπορούν να εφαρμοστούν συγκεκριμένες τεχνικές και τεχνολογίες.

Ο παρακάτω πίνακας παρουσιάζει τα βασικά βήματα που οι καταναλωτές θα πρέπει να λάβει υπόψη για να διασφαλίσουν ότι τα δεδομένα που συμμετέχουν στις δραστηριότητες του Cloud Computing είναι ασφαλή.

Controls	Description
Create a data asset catalog	• A key aspect of data security is the creation of a data asset catalog, identifying all data assets, classifying those data assets in terms of criticality to the business (which can involve financial and legal considerations, including compliance requirements), specifying ownership and responsibility for the data and describing the location(s) and acceptable use of the assets. • Relationships between data assets also need to be cataloged. • An associated aspect is the description of responsible parties and roles, which in the case of cloud computing must span the cloud service consumer organization and the cloud service provider organization.
Consider all forms of data	• Organizations are increasing the amount of unstructured data held on IT systems, which can include items such as images of scanned documents and pictures of various kinds. • Unstructured data can be sensitive and require specific treatment - for example redaction or masking of personal information such as signatures, addresses, license plates. • For structured data, in a multi-tenancy cloud environment, data held in databases needs consideration. Database segmentation can be offered in a couple of varieties: shared or isolated data schema.

	○ In a shared data schema, each customer's data is intermixed within the same database. This means that customer A's data may reside in row 1 while customer B's data resides in row 2. ○ In an isolated architecture, the consumers' data is segregated into its own database instance. While this may provide additional isolation, it also impacts the providers' economies of scale and could, potentially, increase the cost to the consumer. ○ In either scenario, database encryption should be employed to protect all data at rest.
Consider privacy requirements	• Data privacy often involves laws and regulations relating to the acquisition, storage and use of personally identifiable information (PII). • Typically, privacy implies limitations on the use and accessibility of PII, with associated requirements to tag the data appropriately, store it securely and to permit access only by appropriately authorized users. • This requires appropriate controls to be in place, particularly when the data is stored within a cloud provider's infrastructure. The ISO 27018 standard (in preparation) addresses the controls required for PII. These controls may restrict the geographical location in which the data is stored, for example, which runs counter to one aspect of cloud computing which is that cloud computing resources can be distributed in multiple locations.

Apply confidentiality, integrity and availability	• The key security principles of *confidentiality, integrity and availability* are applied to the handling of the data, through the application of a set of policies and procedures, which should reflect the classification of the data. • Sensitive data should be encrypted, both when it is stored on some medium and also when the data is in transit across a network - for example, between storage and processing, or between the provider's system and a consumer user's system. o An extra consideration when using cloud computing concerns the handling of encryption keys - where are the keys stored and how are they made available to application code that needs to decrypt the data for processing? It is not advisable to store the keys alongside the encrypted data, for example. • Integrity of data can be validated using techniques such as message digests or secure hash algorithms, allied to data duplication, redundancy and backups. • Availability can be addressed through backups and/or redundant storage and resilient systems, and techniques related to the handling of denial-of-service attacks. There is also a need for a failover strategy, either by using a service provider who offers this as part of their service offering, or if the provider does not offer resiliency as a feature of their services the consumer may consider self provision of failover by having equivalent services on standby with another provider.
Apply identity and access management	• Identity and access management is a vital aspect of securing data (refer to "Step 3: Manage people, roles and identities" on page 13) with appropriate authorization being required before any user is permitted to access sensitive data in any way. • Related to this is the requirement for logging and security event management (e.g. the reporting of any security breaches) relating to the activities taking place in the cloud service provider environment. • Following from this is the need for a clear set of procedures relating to data forensics in the event of a security incident. Note that the logs and reporting mechanisms are also in need of appropriate security treatment, to prevent a wrongdoer from being able to cover their tracks.

Πίνακας 7.2: Έλεγχοι για την ασφάλεια των δεδομένων στο Cloud Computing

7.3.5. Επιβολή πολιτική προστασίας προσωπικών δεδομένων

Η προστασία της ιδιωτικής ζωής συνήθως συνεπάγεται περιορισμούς σχετικά με τη χρήση και την προσβασιμότητα της χρήσης προσωπικών πληροφοριών (Personally Identifiable Information PII). Θα πρέπει να υπάρχουν πάντα σχετικές απαιτήσεις ώστε τα στοιχεία να σημειώνονται σωστά, να αποθηκεύονται με ασφάλεια και να επιτρέπεται η πρόσβαση μόνο από κατάλληλα εξουσιοδοτημένους χρήστες. Αυτό απαιτεί κατάλληλους ελέγχους ιδίως στην περίπτωση που τα δεδομένα είναι αποθηκευμένα μέσα στην υποδομή ενός παρόχου νέφους. Το πρότυπο ISO 27018 αντιμετωπίζει τους ελέγχους που απαιτούνται για την PII.

7.3.6. Αξιολόγηση των διατάξεων ασφαλείας για τις εφαρμογές Cloud

Οι οργανισμοί θα πρέπει να προστατεύσουν ενεργά τις κρίσιμες εφαρμογές τους από τις εξωτερικές και εσωτερικές απειλές καθ 'όλη τη διάρκεια του κύκλου ζωής τους, από το σχεδιασμό έως την εφαρμογή στην παραγωγή. Σαφώς καθορισμένες πολιτικές και διαδικασίες ασφάλειας είναι ζωτικής σημασίας να εφαρμοστούν. Η ανάγκη για ασφάλεια των εφαρμογών θέτει συγκεκριμένες προκλήσεις στον πάροχο και αλλά και στον καταναλωτή. Οι οργανισμοί πρέπει να αντιμετωπίζουν με την ίδια επιμέλεια την ασφάλεια εφαρμογών όπως κάνουν για τη φυσική ασφάλεια και την ασφάλεια των υποδομών.

Προκειμένου να προστατευθεί η εφαρμογή από τα διάφορα είδη των παραβάσεων, είναι σημαντικό να κατανοήσουμε τους λόγους πολιτικής ασφάλειας των εφαρμογών με βάση τα διαφορετικά μοντέλα ανάπτυξης νέφους (SaaS, IaaS, PaaS).

7.3.7. Επιβεβαίωση ότι τα δίκτυα Cloud και οι συνδέσεις είναι ασφαλείς

Ένας πάροχος υπηρεσιών Cloud πρέπει να επιτρέπει τη νόμιμη κίνηση του δικτύου και την να αποφεύγει την κακόβουλη κίνηση δικτύου. Ωστόσο, σε αντίθεση με πολλούς άλλους οργανισμούς, ένας πάροχος υπηρεσιών Cloud δεν είναι δυνατόν να γνωρίζει σε ποιο δίκτυο κυκλοφορίας προγραμματίζουν οι καταναλωτές να στέλνουν και να λαμβάνουν. Παρ 'όλα αυτά, οι καταναλωτές θα πρέπει να αναμένουν ορισμένες εξωτερικά μέτρα ασφαλείας στην περίμετρο του δικτύου από τους παρόχους τους.

Provider Responsibility	Description / Guidance
Traffic screening	• Certain traffic is almost never legitimate – for example, traffic to known malware ports. The provider should block this traffic on behalf of the consumers. • Traffic screening is generally performed by firewall devices or software. Some firewall considerations: o Does the provider publish a standard perimeter block list that aligns with the terms of service for the offering? Consumers should request a copy of the block list; a reasonable block list can provide a consumer with both assurance of a thoughtful network protection plan as well as some functional guidelines on what is allowed. There may be some cause for concern if the block list is not in line with the terms of service. o Does the provider's firewall block all IPv6 access, or protect against both IPv4 and IPv6 attacks? More and more devices are IPv6 capable, and some providers forget to limit IPv6 access – which can allow an attacker an easy way around the IPv4 firewall. o Is the traffic screening able to withstand and adapt to attacks such as Distributed Denial-of-Service attacks? DDOS attacks are more and more commonly used for extortion purposes by organized crime, and the ability of a cloud service provider and its Internet service provider to assist in blocking the unwanted traffic can be crucial to withstanding an attack.
Intrusion detection/prevention	• Some traffic may look legitimate, but deeper inspection indicates that it is carrying malicious payload such as spam, viruses, or known attacks. The provider should block or at least notify consumers about this traffic. • Intrusion detection and/or prevention systems (IDS/IPS) may be software or devices. Whereas a firewall usually only makes decisions based on source/destination, ports, and existing connections, an IDS/IPS looks at both overall traffic patterns as well as the actual contents of the messages. Many firewalls now include IDS/IPS capabilities. • Although technically not IDS/IPS devices, application-level proxies (such as e-mail gateways/relays) will often perform similar functions for certain types of network traffic and are considered here as well.

	• An IDS will typically only flag potential problems for human review; an IPS will take action to block the offending traffic automatically. Some IDS/IPS considerations: o IDS/IPS content matching can detect or block known malware attacks, virus signatures, and spam signatures, but are also subject to false positives. Does the cloud provider have a documented exception process for allowing legitimate traffic that has content similar to malware attacks or spam? o Similarly, IDS/IPS traffic pattern analysis can often detect or block attacks such as a denial-of-service attack or a network scan. However, in some cases this is perfectly legitimate traffic (such as using cloud infrastructure for load testing or security testing). Does the cloud provider have a documented exception process for allowing legitimate traffic that the IDS/IPS flags as an attack pattern?
Logging and notification	• For assurance purposes and troubleshooting, it's important that consumers have some visibility into the network health. • Incident reporting and incident handling procedures must be clear and the consumer should look for visibility into the handling process. Note that if any PII is stored in the cloud computing environment, there may be legal requirements associated with any incident. • Some network logging information is of a sensitive nature and may reveal information about other clients, so a cloud provider may not allow direct access to this information. However, it is recommended that consumers ask certain questions about logging and notification policies: o What is the network logging and retention policy? In the event of a successful attack, the consumer may want to perform forensic analysis, and the network logs can be very helpful. o What are the notification policies? As a cloud consumer, you should be notified in timely manner if your machines are attacked or compromised and are attacking someone else. o Are historical statistics available on the number of attacks detected and blocked? These statistics can help a consumer understand how effective the provider's detection and blocking capabilities actually are.

Πίνακας 7.3: Απαιτήσεις εξωτερικού δικτύου

Provider Responsibility	Description / Guidance
Protect clients from one another	Cloud providers are responsible for separating their clients in multi-tenant situations. Most cloud service providers will use one or more of the following technologies for this purpose: 1. Dedicated virtual LANs, or VLANs, are a technology that makes a collection of ports on a physical Ethernet switch appear to be a separate switch. In theory, network traffic on one VLAN cannot be seen on a different VLAN any more than network traffic on one physical Ethernet switch can be seen on a different, non-connected Ethernet switch. VLAN separation technology is often a primary control for cloud providers and is generally very effective. However, there are documented "VLAN hopping" attacks that allow unauthorized traffic between VLANs, such as "double-tagging" and "switch spoofing". Many cloud providers offer dedicated VLANs for consumers that no other consumers should be able to access. It is recommended that consumers verify that the provider's VLAN controls address the known VLAN hopping attacks. 2. Virtual Private Networks (VPNs, and also sometimes referred to simply as "tunnels") can be used to connect a consumer's dedicated cloud VLAN back to the consumer's network; this configuration is commonly known as a "site-to-site" VPN. VPNs can also be used to allow roaming users anywhere on the Internet to securely access the consumer's VLAN; this configuration is commonly called "client-to-site". In both cases, there are multiple technologies (such as SSL and IPSec) with different security implementations (such as certificate/credential based or endpoint authentication). It is recommended that consumers decide whether VPNs are required, and if so ensure that the cloud provider supports the required operating mode (client-to-site or site-to-site) and security implementation. 3. Per-instance software firewalls are one of the "last lines of defense" and allow consumers to regulate what traffic comes into their instances by configuring the software firewall on the instance itself. If using a cloud provider's images, consumers should ensure that the images contain proper software firewall capabilities and that the rules are simple to deploy and modify. Per-instance software firewalls are particularly important when sharing a VLAN with other consumers. 4. "Private VLAN" (PVLAN) is a term that has two meanings. One meaning is a VLAN that is dedicated to a particular consumer, which is defined simply as "Dedicated VLAN" above. The second more technical use of the term is a VLAN that prohibits all traffic between hosts on the private VLAN by default. With Private VLAN technology, consumer A and consumer B could be on the same VLAN, but still be unable to communicate with one another – they may only be allowed to talk to the router that allows internet access.

	Private VLAN technology is effective as long as the router, which is permitted to talk to all stations on the network, is not configured to relay traffic originating in the VLAN back in to the VLAN, thereby bypassing the switch's controls. Private VLAN technology provides good isolation but can lead to functional problems, as cloud instances often need to talk to other cloud instances in addition to systems out on the Internet. For this reason, per-instance firewalls are more commonly used for instance separation on the same VLAN. If PVLAN technology is needed, it is recommended that the consumer test to ensure that the router is properly configured and that traffic between cloud instances on the same VLAN is blocked.
	5. Hypervisor based filters, such as *ebtables* on Linux, are functionally similar to private VLANs in that they can prohibit or allow communications at the "virtual switch" level. However, these can also be used to prevent attacks such as IP and MAC address spoofing. If dedicated VLANs are not used, it is recommended that the consumer ask what protections are in place to prevent another consumer's instance from masquerading as one of your instances.
Protect the provider's network	• Separate the provider's network from all clients. If the provider's network is breached, it could lead to almost undetectable data loss. • The client separation strategies above are worthless if the provider's control network is not properly protected. An attacker who gains access to the provider's control network may be able to perform attacks on other consumers from the control network. • Consumers should ask what security controls are in place for the cloud infrastructure itself. While many cloud providers will not give out in-depth details of their security measures due to valid security concerns, there should be a stated security policy and some assurance (e.g. via audit and certification) that it is followed.
Monitor for intrusion attempts	• Activity auditing and logging are an important part of preventive security measures as well as incident response and forensics. Audit information and logs should be subject to appropriate security controls to prevent unauthorized access, destruction or tampering. • Cloud consumers should ask what types of internal network security incidents have been reported and if there are any published statistics or metrics. • Consumers should also ask for the provider's processes for alerting consumers about both successful and unsuccessful internal network attacks.

7.3.8. Αξιολόγηση ελέγχων ασφαλείας στις υλικές υποδομές και εγκαταστάσεις

Μία σημαντική παράμετρος για την ασφάλεια της λειτουργίας του συστήματος αφορά την ασφάλεια των φυσικών υποδομών και εγκαταστάσεων. Στην περίπτωση

του Cloud Computing, ισχύουν εξίσου οι ίδιες παράμετροι, αλλά στην περίπτωση αυτή η ασφάλεια των υποδομών και των εγκαταστάσεων θα πρέπει ελέγχονται από τον πάροχο υπηρεσιών Cloud. Είναι όμως στην ευθύνη του καταναλωτή να πάρει διαβεβαίωση από τον πάροχο ότι εφαρμόζονται οι κατάλληλοι έλεγχοι ασφαλείας. Διαβεβαίωση μπορεί να παρέχεται μέσω του ελέγχου και της αξιολόγησης των εκθέσεων, που αποδεικνύουν τη συμμόρφωση με πρότυπα ασφάλειας, όπως το ISO 27002. Μια σύντομη περιγραφή των ελέγχων ασφαλείας που πρέπει να παρέχει ο πάροχος περιλαμβάνει:

• Η υλική υποδομή και τις εγκαταστάσεις θα πρέπει να βρίσκονται σε ασφαλείς περιοχές.
• Προστασία έναντι εξωτερικών και περιβαλλοντικών απειλών.
• Έλεγχος του προσωπικού να εργάζεται σε ασφαλείς περιοχές.
• Έλεγχοι ασφαλείας εξοπλισμού.
• Έλεγχος της ασφάλειας των καλωδιώσεων.
• Η σωστή συντήρηση του εξοπλισμού.
• Έλεγχος της απομάκρυνσης περιουσιακών στοιχείων.
• Ασφαλής διάθεση ή επαναχρησιμοποίηση του εξοπλισμού.
• Ασφάλεια του ανθρώπινου δυναμικού.
• Δημιουργία αντιγράφων ασφαλείας, σχέδια πλεονασμού και συνέχισης.

Για περισσότερες λεπτομέρειες σχετικά με τους ελέγχους και τις εκτιμήσεις που ισχύουν για κάθε κάθε ένα από αυτά τα στοιχεία, θα πρέπει να ανατρέξει κανείς στο πρότυπο ISO 27002.

7.3.9. Διαχείριση όρων ασφαλείας στο σύννεφο SLA

Δεδομένου ότι το Cloud Computing περιλαμβάνει συνήθως δύο οργανώσεις – την υπηρεσία του καταναλωτή και την υπηρεσία του παρόχου, οι ευθύνες για την ασφάλεια του κάθε μέρους πρέπει να καταστούν σαφείς. Αυτό γίνεται συνήθως μέσω μιας συμφωνίας επιπέδου υπηρεσιών (SLA) που εφαρμόζεται στις υπηρεσίες που παρέχονται, καθώς και με τους όρους της σύμβασης μεταξύ του καταναλωτή και του

παρόχου. Το SLA πρέπει να προσδιορίσει τις αρμοδιότητές της ασφάλειας και θα πρέπει να περιλαμβάνει θέματα όπως την αναφορά της παραβίασης της ασφάλειας.

7.3.10. Κατανόηση των απαιτήσεων ασφάλειας της διαδικασίας εξόδου

Από την άποψη της ασφάλειας, είναι σημαντικό μόλις ο καταναλωτής έχει ολοκληρώσει τη διαδικασία τερματισμού κανένα από τα δεδομένα των καταναλωτών δε θα πρέπει να παραμείνει στον πάροχο. Ο πάροχος πρέπει να διασφαλίζει ότι τυχόν αντίγραφα των δεδομένων «καθαρίζονται» από το περιβάλλον του παρόχου, οπουδήποτε και αν αυτά έχουν αποθηκευτεί (δηλαδή συμπεριλαμβάνοντας τις θέσεις των αντίγραφων ασφαλείας, καθώς και την online αποθήκευση δεδομένων).

Δεν υπάρχει καμία αμφιβολία ότι η ασφάλεια εξακολουθεί να είναι από τις κορυφαίες ανησυχίες η οποία προβληματίζει τους οι πιθανούς χρήστες Cloud τεχνολογιών. Αλλά θα πρέπει να αναγνωριστεί ότι έχουν γίνει τεράστια άλματα στον τομέα αυτό τα τελευταία χρόνια. Γίνεται επομένως ολοένα και πιο σαφές ότι οι απειλές για την ασφάλεια στο περιβάλλον Cloud είναι σήμερα μικρότερες, και σε πολλές περιπτώσεις λιγότερο διαδεδομένες από αυτές που αντιμετωπίζουν τα on-site συστήματα[7],[15].

ΠΑΡΑΡΤΗΜΑ 1
Το Ευρωπαϊκό πλαίσιο για το Υπολογιστικό νέφος

Ηλίας Καστρίτης, 4.10.2013

Περιεχόμενα

• Η Στρατηγική της Ευρώπης για το Ευρωπαϊκό νέφος

• Αναμενόμενα οφέλη

• Βασικές δράσεις που έχουν αναληφθεί

• Πρόοδος εργασιών

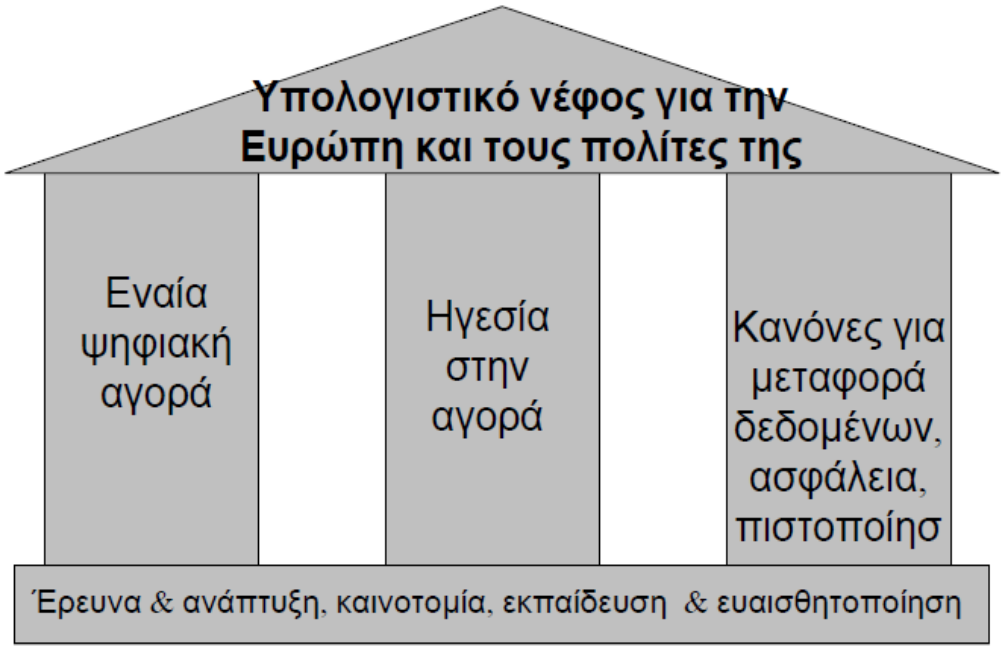
• Δημόσια Υπολογιστικά νέφη στην Ελλάδα που συγχρηματοδοτούνται από το Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης (ΕΠ Ψηφιακή Σύγκλιση)

• Προκλήσεις

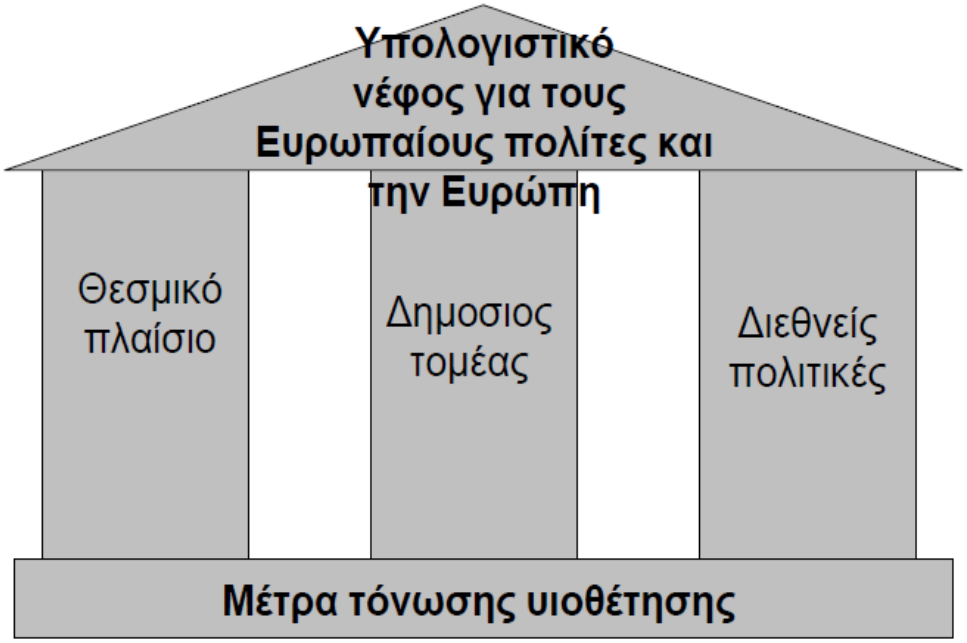
Ευρωπαϊκή στρατηγική για το Υπολογιστικό νέφος

Στο έγγραφο της ΕΕ για την «αξιοποίηση των δυνατοτήτων του υπολογιστικού νέφους» ένα χρόνο πριν, η Ευρωπαϊκή Ένωση δεσμεύτηκε πολιτικά στην ενεργοποίηση και στη διευκόλυνση ταχύτερης υιοθέτησης του υπολογιστικού νέφους σε όλους τους τομείς της οικονομίας, με αποτέλεσμα τη μείωση του κόστους των ΤΠΕ, και - εφόσον συνδυαστεί με νέες ψηφιακές επιχειρηματικές πρακτικές,– με δυνατότητα ώθησης στην παραγωγικότητα, στην οικονομική μεγέθυνση και στην απασχόληση.

Στόχοι



Στρατηγική



Εκτιμήσεις – Οφέλη

Μέχρι το 2014 τα έσοδα από το υπολογιστικό νέφος μπορούν να αγγίξουν τα 148,8 δισεκατομμύρια.

Το 60% του φόρτου εργασίας του συνόλου των διακομιστών θα έχει εικονοποιηθεί.

Επιπλέον άμεσες δαπάνες 45 δισ. ευρώ για το υπολογιστικό νέφος στην ΕΕ το 2020,

Συνολική αθροιστική επίπτωση στο ΑΕΠ ύψους 957 δισεκατομμυρίων ευρώ και

8,3 εκατ. θέσεις εργασίας, μέχρι το 2020

Μελέτη αναφέρει ότι το δημόσιο υπολογιστικό νέφος θα δημιουργήσει το 2020 ΑΕΠ ύψους 250 δισεκατομμύρια ευρώ με πολιτικές ευνοϊκές για το υπολογιστικό νέφος, έναντι 88 δισεκατομύρια. Στο σενάριο «χωρίς καμία παρέμβαση», με επιπλέον σωρευτικό αντίκτυπο από το 2015 ως το 2020 ύψους 600 δισεκατομμύρια. ευρώ. Ή δημιουργία 2,5 εκατ. επιπλέων θέσεων απασχόλησης.

Βασικές Δράσεις για την εκπλήρωση της δέσμευσης

Αντιμετώπιση του κυκεώνα των προτύπων

-Ανεξάρτητη εμπιστευμένη πιστοποίηση των υπηρεσιών νέφους σε σχέση με τα πρότυπα που πληρούν, με έγκριση από αρχές για τη συμμόρφωση με νομικές υποχρεώσεις ώστε να μη στερείται τη διαλειτουργικότητα, τη φορητότητα των δεδομένων και την αντιστρεψιμότητα.

-Το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων (ETSI), έχει συστήσει ομάδα για το υπολογιστικό νέφος προκειμένου να εξετάσει τις ανάγκες τυποποίησης και τη συμμόρφωση με τα πρότυπα διαλειτουργικότητας με ένα λεπτομερή χάρτη προτύπων για την ασφάλεια, διαλειτουργικότητας, μεταφερσιμότητα και αντιστρεψιμότητα και σχήματα ασφάλειας από την ENISA.

Ασφαλείς και δίκαιοι συμβατικοί όροι και προϋποθέσεις

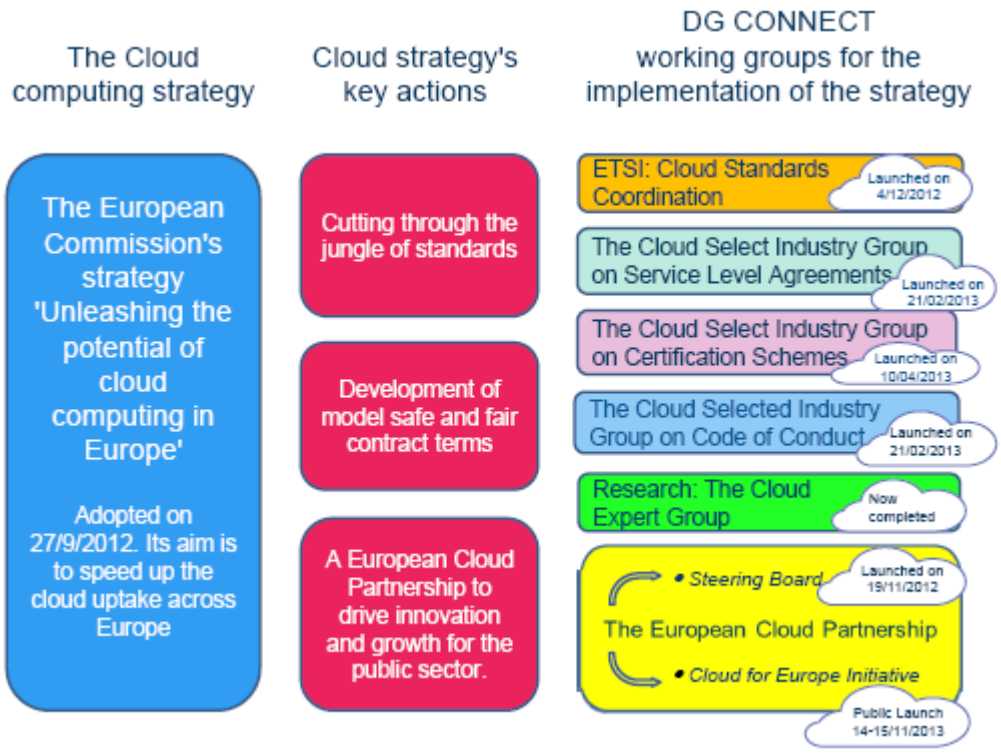
- Εκπόνηση πρότυπων όρων όσον αφορά τις συμφωνίες για το επίπεδο υπηρεσιών υπολογιστικού νέφους για συμβάσεις μεταξύ των παρόχων και των χρηστών υπολογιστικού νέφους

- η παροχή συμβατικών όρων βέλτιστης πρακτικής για την παροχή υπηρεσιών υπολογιστικού νέφους για τις πτυχές που σχετίζονται με την προμήθεια «ψηφιακού περιεχομένου»
- Προσδιορισμός δίκαιων συμβατικών όρων και προϋποθέσεων για τους καταναλωτές και τις μικρές επιχειρήσεις, και για τα συναφή με το νέφος θέματα πέραν του κοινού ευρωπαϊκού δικαίου των πωλήσεων.
- συμφωνία σε έναν κώδικα δεοντολογίας για παρόχους υπολογιστικού νέφους με σκοπό την υποστήριξη ομοιόμορφης εφαρμογής των κανόνων προστασίας των δεδομένων προκειμένου να εξασφαλιστεί η ασφάλεια δικαίου και η συνοχή μεταξύ του κώδικα δεοντολογίας και της ενωσιακής νομοθεσίας.

Συγκρότηση ευρωπαϊκής σύμπραξης για το υπολογιστικό νέφος για την προώθηση καινοτομίας και οικονομικής μεγέθυνσης στον δημόσιο τομέα.

Η σύμπραξη θα

- συγκεντρώσει τεχνογνωσία του κλάδου και των χρηστών του δημόσιου τομέα εργαζόμενη στην κατεύθυνση θέσπισης κοινών απαιτήσεων σύναψη συμβάσεων υπολογιστικό νέφος με ανοιχτό και πλήρως διαφανή τρόπο ώστε να διασφαλίσει ότι η εμπορική προσφορά στην Ευρώπη είναι προσαρμοσμένη στις ευρωπαϊκές ανάγκες.
- συμβάλει στην αποφυγή κατακερματισμού και στη διασφάλιση διαλειτουργικής, ασφαλούς και πράσινης δημόσιας χρήσης του υπολογιστικού νέφους, σε πλήρη ευθυγράμμιση με τους ευρωπαϊκούς κανόνες, π.χ. στα πεδία της προστασίας των δεδομένων και της ασφάλειας.
- προσδιορίσει τις απαιτήσεις υπολογιστικού νέφους του δημόσιου τομέα και θα εκπονήσει προδιαγραφές για συμβάσεις προμήθειας
- προμηθευτεί εφαρμογές αναφοράς που να τεκμηριώνουν τη συμμόρφωση και την απόδοση.



Δημόσια Υπολογιστικά νέφη που συγχρηματοδοτούνται από το Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης

(ΕΠ Ψηφιακή Σύγκλιση)

Για την αποφυγή αύξησης του κόστους κτήσης υποδομών (300 εκ. € στο ΕΠ «ΚτΠ» για υποδομές, υπεγράφη Μνημόνιο Συνεργασίας μεταξύ των κύριων φορέων της διοίκησης (2010)

Σήμερα

• Ωκεανός – ΕΔΕΤ 18, 8 εκατ €, IaaS – PaaS, σε λειτουργία

• Κεντρικές Υπολογιστικές Υποδομές (G-Cloud) «Δημιουργία και θέση σε λειτουργία πλήρους κόμβου φιλοξενίας προηγμένου υπολογιστικού εξοπλισμού υψηλής πυκνότητας» - ΚτΠ ΑΕ, 16,3 εκατ €, IaaS – PaaS σε τεχνική αξιολόγηση

• Κόμβος G-Cloud της ΓΓΠΣ, 5,5 εκατ. € IaaS – PaaS- SaaS, τεχνική αξιολόγηση Εγκατάσταση κέντρου δεδομένων και υπηρεσιών με υποστήριξη φιλικής προς το

περιβάλλον κατανάλωση ενέργειας, ΕΔΕΤ 8,6 εκατ. € IaaS disaster recovery ΥπΕΠΘ, σε διαβούλευση

• Ολοκληρωμένο Σύστημα Διαχείρισης Δικαστικών Υποθέσεων για την Πολιτική και την Ποινική Δικαιοσύνη, Υπουργείο Δικαιοσύνης, 9,9 εκατ. € IaaS για τα Ποινικά Δικαστήρια, σε διαβούλευση

• Πλατφόρμα Παροχής Υπηρεσιών Κατάθεσης, Διαχείρισης και Διάθεσης Ανοικτών Δημοσίων Δεδομένων Τεκμηρίωσης και Ψηφιακού Περιεχομένου, ΕΚΤ, 4,5 ακατ. €, IaaS (ΕΠΣΕΤ ΙΙ), SaaS (Αποθετηρίου σε δημοτικές βιβλιοθήκες και ΝΠΙΔ με ψηφιοποιημένα αρχεία, σε υλοποίηση

• Προηγμένες Κεντρικές Υπηρεσίες Ψηφιακών Βιβλιοθηκών Ανοικτής Πρόσβασης, ΣΕΑΒ – ΕΜΠ, 4,5 εκατ. €, IaaS – SaaS στις ακαδημαικές βιβλιοθήκες, σε διαβούλευση

• Ψηφιακές Υπηρεσίες μιας στάσης του ΥΕΚΑ 5 εκατ. €, IaaS στην Κοινωνική Ασφάλιση, σε προκήρυξη

Συνολικά μια επένδυση 73,3, εκατ €

Προκλήσεις

• **Διαλειτουργικότητα**

-Κίνδυνοι καταστάσεων δέσμιων πελατών.

-Μεταφερσιμότητα δεδομένων, ασφάλεια

• **Προστασία δεδομένων και ασφάλεια**

-Πού βρίσκονται τα δεδομένα μου; Ποιοί νόμοι κατισχύουν; Ποιός έχει πρόσβαση σε αυτά (PRISM)

• **Διακυβέρνηση και έλεγχος**

-Έλεγχος όρων διαθεσιμότητας, SLA, χρήση εφαρμογών legacy

• **Ασφάλεια, διαθεσιμότητα και αξιοπιστία**

-δεδομένα, χρόνοι εκτός λειτουργίας

• Συνέχεια στο Μνημόνιο Συνεργασίας για την ανάπτυξη και λειτουργία Κεντρικών Υπολογιστικών Υποδομών (G-Data Centers / G-Cloud) – Καλή διακυβέρνηση – δομές – επίλυση οριζοντίων θεμάτων – ανοικτό δίκτυο συνεργασίας
• Πειστική πρόταση συνεργασίας, ολοκληρωμένο SLA, απόδειξη μείωσης TCO, διαδικασίες μεταφοράς, επιχειρησιακή συνέχεια,
• Οριζόντια φιλοξενία Πληροφοριακών Συστημάτων φορέων – πλάνο μετάβασης
• Γρήγορη υλοποίηση των έργων με τήρηση των όρων αποδοχής χρηματοδότησης και των προδιαγραφών ποιότητας
• Ασφάλεια δεδομένων
- («λαμβάνουν όλα τα δυνατά μέτρα για τη διασφάλιση της ακεραιότητας των αποθηκευμένων δεδομένων από βλάβες ή κακόβουλες ενέργειες, καθώς και για τη διαφύλαξη της ιδιωτικότητας και των προσωπικών δεδομένων των πολιτών τηρουμένης της ισχύουσας νομοθεσίας (Ν. 2472/1997, 3471/2006), των Κανονιστικών Πράξεων και των οδηγιών της Αρχής Προστασίας Προσωπικών Δεδομένων

Υπηρεσία Ανάπτυξης Πληροφορικής

Να ληφθεί μέριμνα για υποχρεωτική ένταξη και υποστήριξη των πληροφοριακών απαιτήσεων των φορέων, μέσα από τις υπό ανάπτυξη υποδομές του DC, στο πλαίσιο απαραίτητων θεσμικών ρυθμίσεων κατά αντιστοιχία με το Σύζευξις Ειδικότερα, θα πρέπει να υποχρεούνται οι φορείς οι οποίοι υλοποιούν νέα «μεγάλα» έργα, κυρίως μέσω των επιχειρησιακών προγραμμάτων, να καλύπτουν τις συγκεκριμένες ανάγκες τους μέσα από τις υποδομές του παρόντος έργου στο πλαίσιο συγκεκριμένου back-to-back SLA μεταξύ Κυρίου του έργου-Φορέα λειτουργίας και της ΚτΠ Α.Ε και των Φορέων (η Προγραμματική Συμφωνία μεταξύ ΚτΠ ΑΕ και Φορέων δεν αποτελεί σε καμία περίπτωση πλαίσιο διασφάλισης της ποιότητας των υπηρεσιών προς τους φορείς). Επίσης, να υπάρξει πρόβλεψη για την ομαλή μετάπτωση των συστημάτων στις υποδομές του παρόντος έργου στο
πλαίσιο συγκεκριμένου χρονοδιαγράμματος, μεθοδολογίας κλπ, που θα συμφωνηθεί από κοινού με το ΥΔιΜΗΔ και δεν θα διαταράσσει την ομαλή λειτουργία των Υπηρεσιακών Μονάδων και θα διασφαλίζει συγχρόνως την ποιότητα των

παρεχόμενων υπηρεσιών προς τους πολίτες, τις επιχειρήσεις ή τρίτους φορείς του Δημοσίου Τομέα[19].

ΠΑΡΑΡΤΗΜΑ 2
Πάροχοι Cloud Computing

Οι πάροχοι του υπολογιστικού νέφους ανταγωνίζονται μεταξύ τους προσφέροντας ολοένα και πιο δελεαστικές υπηρεσίες. Κάποιοι από τους πιο διαδεδομένους παρόχους θα αναλυθούν παρακάτω.

Το lunacloud είναι ένας Ευρωπαϊκός πάροχος Cloud Computing υπηρεσιών που αντιμετωπίζει με μεγάλη προσοχή στην αξιοπιστία, στην ευελιξία και στο χαμηλό κόστος για την παροχή υπηρεσιών. Οι υποδομές που υποστηρίζουν είναι IaaS, και δίνουν τη δυνατότητα εφαρμογής οποιουδήποτε λειτουργικού συστήματος, εφαρμογών και αποθήκευσης δεδομένων.

Δημιουργήθηκε και βγήκε στην αγορά το 2011 από τους Charles Nasser και Antonio Miguel Ferreira, οι οποίοι είχαν πολυετή εμπειρία σε εμπορικά τεχνολογικά δημιουργήματα και εταιρίες με εκατομμύρια πελάτες ανά τον κόσμο.

Η εταιρία προτείνει ότι είναι η καλύτερη επιλογή καθώς προσφέρει αξιόπιστες υπηρεσίες cloud αλλά και όλα τα βασικά χαρακτηριστικά του cloud και την δυνατότητα στον πελάτη να διευρύνει τις προτεινόμενες υπηρεσίες καθώς έχει φιλικό προς τον χρήστη περιβάλλον.

Η εταιρία Distil Networks προσφέρει ολοκληρωμένες λύσεις σε παροχή υπηρεσιών over the Internet αλλά και γενικά σε θέματα δικτύου. Δεν θα μπορούσε από το να παρέχει ολοκληρωμένες προτάσεις παροχής cloud υπηρεσιών. Ο συγκεκριμένος πάροχος υποστηρίζει οποιαδήποτε δομή cloud computing και αν επιθυμεί πελάτης του, είτε αυτό είναι public, private ή hybrid cloud. Οι υπηρεσίες είναι είτε PaaS είτε SaaS.

Η εταιρία ιδρύθηκε το 2011 και εξ αρχής προσέφερε υπηρεσίες υπολογιστικού νέφους καθώς και ολοκληρωμένες προτάσεις ασφάλειας σε αυτό. Οι τρεις ιδρυτές της εταιρίας είναι ο Rami Essaid, Engin Akyol και Andrew Stein οι οποίοι στόχευσαν εξ αρχής στην διασφάλιση της ασφάλειας των υπηρεσιών που προσφέρουν. Το βασικό προτέρημα αυτού του παρόχου είναι ότι διακόπτουν τα bot attacks στα συστήματα νεφών.

Η εταιρία προσφέρει συστήματα νεφών όλων των τύπων- Hybrid Cloud, Private Cloud και Public Cloud- και υπηρεσίες IaaS. Προφέρουν έναν συνδυασμό από δυνατή υπολογιστική ισχύ και υπηρεσίες cloud που να μπορούν να χρησιμοποιήσουν αποτελεσματικά αυτή την ισχύ. Η ομάδα που ασχολείται με τις υπηρεσίες έχει δώσει

έμφαση σε εργαλεία που εξασφαλίζουν ασφάλεια στο Cloud, τουλάχιστον μέχρι έναν μεγάλο βαθμό.

Η Cloud Sigma αποτελείται από μία μεγάλη ομάδα επιστημόνων, πιστών στις νέες τεχνολογίες και τις καινοτομίες στο Cloud Computing και σε tools που βελτιστοποιούν την ασφάλεια σε αυτό.

Η Engine Yard προσφέρει Public Cloud συστήματα και αποκλειστικά PaaS υπηρεσίες. Η χρήση των υπηρεσιών της εταιρίας από τους πελάτες παρακολουθείτε στενά από το προσωπικό, ώστε νε ελέγχονται και παράμετροι που διασφαλίζουν την ασφάλεια και την ιδιωτικότητα από πλευράς του τελικού χρήστη αλλά και την συνεργασία που τυχόν υπάρχει στο δίκτυο με άλλους παρόχους.

Οι ιδρυτές της εταιρίας είναι οι Beau Vrolyk, Alan Cyron, Paul Melmon και Carl Meadows. Ο καθένας έχει διαφορετικές σπουδές και διαφορετικές προσεγγίσεις στις τεχνολογίες που ολοένα εμφανίζονται στο προσκήνιο. Έτσι, οι ομάδες που διευθύνουν, έχουν αναλάβει διαφορετικά προγράμματα με αποτέλεσμα να προσεγγίζουν οποιαδήποτε θέματα μπορούν να προκύψουν σε ένα δημόσιο δίκτυο ώστε να έχουν τον καλύτερο έλεγχο και αποτελέσματα στα θέματα που πιθανόν να προκύψουν σε ένα τέτοιο, συνεργατικό δίκτυο.

Προσφέρονται υπηρεσίες IaaS και Paas, και αποκλειστικά δημόσιο νέφος (public cloud). Πρόκειται για την ολοκληρωμένη πρόταση της Microsoft για τη χρήση υπηρεσιών υπολογιστικού νέφους, και συγκεκριμένα για ένα δημόσιο δίκτυο κατά το οποίο υπάρχουν συνεργασίες με άλλους παρόχους.

Προσφέρει ευελιξία στον χρήστη, υποστήριξη των υπηρεσιών που επιλέγει, δυνατότητα free developing υπό την χρήση, οικονομική κλιμάκωση ανάλογα με τις υπηρεσίες που χρησιμοποιούνται και παρέχουν ασφάλεια στα δεδομένα, η οποία κατοχυρώνονται από αναγνωρισμένη πιστοποίηση της Ευρωπαϊκής Ένωσης, για τη διατήρηση των νομικών πλαισίων της Ε.Ε. Σαφώς, πιστοποιήσεις για την ασφάλεια και την ιδιωτικότητα που προσφέρεται από το Azure έχουν και διεθνές υπόβαθρο, όπως το ISO 27018.

Προσφέρονται συστήματα νεφών Hybrid Cloud, Private Cloud και Public Cloud και υπηρεσίες PaaS. Θεωρείται αξιόπιστο και έχει μεγάλη απήχηση σε εταιρίες. Θεωρείται πως παρέχει βελτιστοποιημένο λογισμικό σε χαμηλό κόστος, γρήγορη απόδοση και με χαμηλό ρίσκο ασφάλειας.

Η Amazon παρέχει συστήματα νεφών Hybrid Cloud, Private Cloud και Public Cloud και υπηρεσίες IaaS. Είναι ο πιο διαδεδομένος πάροχος υπολογιστικών νεφών. Η εταιρία είναι γνωστή στου κύκλους της πληροφορικής για διάφορες υπηρεσίες που παρέχει και κυρίως για την αξιοπιστία της. Οι μηχανισμοί ασφάλειας και ελέγχου των πελατών και των συνεργατών της είναι καινοτόμες και πολύ αποδοτικές. Έχει εξασφαλίσει διεθνείς πιστοποιήσεις για την συμμόρφωση στο νομικό πλαίσιο που αφορά του είδους τις υπηρεσίες που προσφέρει.
Διαθέτει τη μεγαλύτερη λίστα πελατών, η οποία αποτελείται κατά βάση από μεγάλου βεληνεκούς εταιρίες.

Προσφέρονται όλοι οι τύποι Cloud Computing – Hybrid, private, public- και IaaS υπηρεσίες. Πρόκειται για πολυεθνική εταιρία με έμφαση στην παροχή υπηρεσιών και μηχανισμών σε εταιρίες ανά τον κόσμο, με τις οποίες δημιουργεί ισχυρές και ιδιαίτερα συμφέρουσες συνεργασίες. Οι Cisco, Amazon και Microsoft είναι τρείς από τους σταθερούς συνεργάτες της, δίνοντας έτσι τη δυνατότητα στην εταιρία να προσφέρει δελεαστικά πακέτα υπηρεσιών συνδυασμένα με υπέρτατες πολιτικές ασφάλειας και συνεργασίας αλλά και υπολογιστικής ισχύος.
Μεγάλη προσοχή έχει δοθεί στα θέμα ασφάλειας και κατοχύρωσης της ιδιωτικότητας στο cloud περιβάλλον που προσφέρεται. Είναι από τις λίγες εταιρίες που δεν προσφέρουν πακέτο με τις πολιτικές ασφάλειας που πρέπει αν τηρούνται, αλλά υπόσχεται πραγματοποίηση risk analysis διαδικασιών ανάλογα με τον πελάτη-συνεργάτη και τις υπηρεσίες που έχει επιλέξει να χρησιμοποιήσει[11].

ΠΑΡΑΡΤΗΜΑ 3
Τι ζητούν οι ελληνικές επιχειρήσεις για να χρησιμοποιήσουν συστήματα νεφών

Η Microsoft επιχείρησε να αποδείξει πόσο πρακτικό είναι το cloud computing στους συνεργάτες της και να τους πείσει να το χρησιμοποιήσουν. Βασικά της επιχειρήματα ήταν η εξοικονόμηση χρόνου και χρήματος αλλά και αύξηση της παραγωγικότητας, καθώς τα πάντα θα μπορούσαν να επικοινωνούν υπό ένα ενιαίο σύστημα. Σε έρευνα που διεξήγαγε, κατέγραψε τις απαιτήσεις των εταιριών ώστε να υιοθετήσουν το cloud computing.

Η έρευνα διεξήχθη σε 21 ευρωπαϊκές χώρες, μεταξύ αυτών και η Ελλάδα. Υπεύθυνη εταιρία για την έρευνα ήταν η Vanson Bourne. Η έρευνα αυτή ξεκίνησε το Νοέμβριο του 2011, κομβική χρονική περίοδος για την οικονομική κρίση στη χώρα μας.

Από την έρευνα προκύπτει, λίγο πολύ, ότι οι ελληνικές επιχειρήσεις δεν τολμούν να χρησιμοποιήσουν το διαδίκτυο για εφαρμογές που θεωρούνται κρίσιμες για την εταιρία, καθώς επίσης και πως δεν εμπιστεύονται να αποθηκεύουν τα δεδομένα τους σε άγνωστα κέντρα δεδομένων ανά τον κόσμο, αλλά στην έδρα τους. Βέβαια, δεν έχουν συνειδητοποιήσει το σημαντικότερο- χρησιμοποιούν ήδη το cloud στην καθημερινότητα τους χωρίς να το συνειδητοποιούν.

Αν μεγάλες εταιρίες χρησιμοποιούσαν υπηρεσίες cloud, θα παραδειγματίζονταν και άλλες επιχειρήσεις, τουλάχιστον στην Ελλάδα, και θα πείθονταν απέναντι στη χρήση τους. Η πλειοψηφία των εταιριών που έχουν ενταχθεί στην πραγματικότητα του υπολογιστικού νέφους, δηλώνουν πως έχουν εξοικονομήσει πραγματικά χρόνο και χρήμα. Επίσης, οι CEO των εταιριών αυτών, δηλώνουν πως η παραγωγικότητα στην εταιρία έχει αυξηθεί σημαντικά.

Ο βασικότερος λόγος για τον οποίο διστάζουν οι ελληνικές επιχειρήσεις διστάζουν είναι η ασφάλεια των δεδομένων τους και η άγνοιά τους για το τι εστί cloud computing και το πώς θα μπορούσαν να διαχειριστούν τις υπηρεσίες τους.

Βασικά αποτελέσματα της έρευνας:

Οι ιδιοκτήτες μικρών και μεσαίων επιχειρήσεων πιστεύουν ότι ο ρόλος τους στην πορεία της οικονομίας είναι σημαντικός. Το 83% των ερωτηθέντων, «συμφωνεί» ή «συμφωνεί απόλυτα» ότι οι μικρές και μεσαίες επιχειρήσεις αποτελούν τη ραχοκοκαλιά της ελληνικής οικονομίας.

Η πλειονότητα των ιδιοκτητών μικρών και μεσαίων επιχειρήσεων συμφωνούν στο ότι η επιχείρησή τους μπορεί να κάνει τη διαφορά στη γενική εικόνα της οικονομίας μας (65% «συμφωνούν», 7% «διαφωνούν»)

Πάνω από τους μισούς (54%), δηλώνουν ότι «επιχειρήσεις σαν τη δική μου επωμίζονται την ευθύνη να προσφέρουν δουλειές και να παρέχουν καινοτομία**,** ώστε να ξαναγυρίσουν οι παλιές καλές μέρες»

Σχεδόν οι μισοί από τους ερωτηθέντες (42%) προχωρούν ακόμα παραπέρα και δηλώνουν ότι υπάρχουν οι κατάλληλες συνθήκες εξισορρόπησης της οικονομίας, εστιάζοντας σε μικρές, ευέλικτες και καινοτόμες επιχειρήσεις και υπαλλήλους

Η τεχνολογία θεωρείται κρίσιμος παράγοντας σε αυτή την εξισορρόπηση. Το 52% συμφωνεί ότι η πληροφορική θα παίξει σημαντικό ρόλο στην έξοδο της επιχείρησής τους από την τωρινή οικονομική κρίση

Το 43% μάλιστα, πιστεύει ότι η χρήση της πληροφορικής και των υπολογιστών θα αποτελέσει τον καθοριστικό παράγοντα για το αν η επιχείρησή τους απλά θα επιβιώσει ή θα αναπτυχθεί σημαντικά

Υπάρχουν όμως κρίσιμες ανησυχίες για θέματα ασφάλειας και προστασίας προσωπικών δεδομένων καθώς και κάποια έλλειψη εμπιστοσύνης προς τον κλάδο της Πληροφορικής, τα οποία πρέπει να ξεπεραστούν.

Οι μικρομεσαίες Επιχειρήσεις αποζητούν τη βοήθεια της κυβέρνησης στην προσπάθεια τους για ανάπτυξη

Στην Ελλάδα, οι ιδιοκτήτες μικρομεσαίων επιχειρήσεων είναι λιγότερο αισιόδοξοι για τη μελλοντική τους πορεία τους επόμενους 12 – 18 μήνες, σε σχέση με τους Ευρωπαίους ομολόγους τους. Σε σχέση με το 28% του Ευρωπαϊκού μέσου όρου, μόλις το 8% των ερωτηθέντων από την Ελλάδα προβλέπουν ότι θα πετύχουν

καλύτερα αποτελέσματα σε σχέση με το 2010-2011. Μόνο το 7% δηλώνουν ότι σκοπεύουν να κάνουν προσλήψεις, σε σύγκριση με τον Ευρωπαϊκό μέσο όρο που είναι 24%

Παρόλα αυτά, όταν ερωτώνται για την γενική πορεία της Οικονομίας, σχεδόν οι μισοί (38%) συμφωνούν πως αν και οι επόμενοι 12-18 μήνες θα είναι δύσκολοι, η χώρα στο τέλος θα ωφεληθεί.

Η Ελληνική κυβέρνηση θα πρέπει να γνωρίζει ότι οι ερωτηθέντες επεσήμαναν την ύπαρξη σημαντικών εμποδίων για την εγχώρια ανάπτυξη. Η πλειοψηφία (76%) ανέφερε την οικονομική αβεβαιότητα ως την κυριότερη ανησυχία τους, αλλά και η χαμηλή ζήτηση (33%) όπως και η δυσχέρεια οικονομικής ρευστότητας (47%), αποτελούν πολύ σημαντικά εμπόδια, σύμφωνα με την έρευνα.

Οι μικρομεσαίες επιχειρήσεις δίνουν ξεκάθαρο μήνυμα στους φορείς που χαράζουν τις πολιτικές της αγοράς, για συγκεκριμένες αλλαγές που θεωρούν ότι μπορούν να συμβάλουν στην ανάπτυξη. Οι τρεις κυριότερες προτάσεις που προτείνουν οι ιδιοκτήτες των μικρομεσαίων επιχειρήσεων είναι: χαμηλότερη φορολογία (85%), μειωμένο κόστος για πρόσληψη νέου ταλαντούχου ανθρώπινου δυναμικού (60%), και μεγαλύτερη προστασία από το κράτος (45%).

Τι είναι το cloud computing στις υπηρεσίες;

Με δεδομένο ότι το 52% των ερωτηθέντων απαντά ότι η πληροφορική και οι υπολογιστές θα αποτελέσουν καθοριστικό παράγοντα για το αν η επιχείρησή τους απλά θα επιβιώσει ή θα αναπτυχθεί σημαντικά, η Microsoft πιστεύει ότι είναι ζωτικής σημασίας να ενημερώσει/εκπαιδεύσει τις μικρομεσαίες επιχειρήσεις για τα οφέλη των τεχνολογιών εκείνων που προωθούν την παραγωγικότητα και μειώνουν τα κόστη μέσω της χρήσης του cloud computing.

Για να υιοθετήσουν οι Μικρομεσαίες Επιχειρήσεις το Cloud Computing, η αγορά της Πληροφορικής πρέπει να φροντίσει να επικοινωνήσουν τα οφέλη του και να εξαλειφθούν οι όποιες ανησυχίες /αμφιβολίες γύρω από αυτό.

Το Cloud Computing υπόσχεται τεράστια οφέλη για τις επιχειρήσεις. Οι εταιρίες πληροφορικής όμως, δεν κάνουν αρκετά για να εξηγήσουν τους λόγους που έχουν οι

μικρομεσαίες επιχειρήσεις να μεταβούν στο Cloud και για να τους δώσουν τις εγγυήσεις ότι αποτελεί μια ασφαλή και σίγουρη εναλλακτική.

Προς το παρόν, η βιομηχανία της πληροφορικής δεν κάνει αρκετά για να αποδείξει τα απτά οφέλη του Cloud: σχεδόν 4 στους 10 ερωτηθέντες (38%) πιστεύουν ότι η πληροφορική σαν τομέας δεν κάνει καλή δουλειά στο να εξηγήσει πώς το Cloud Computing μπορεί να ωφελήσει την επιχείρηση τους.

Επιπλέον, η έρευνα δείχνει ότι θα άξιζε να ακούσουν οι μικρομεσαίες επιχειρήσεις τι λένε κάποιες εταιρίες που έχουν ήδη κάνει τη μετάβαση στο Cloud, διότι όσες το έχουν κάνει αναφέρουν πολύ απτά και συγκεκριμένα οφέλη. 52% από αυτές λένε ότι η επιχείρηση τους έγινε πιο ευέλικτη, 52% ότι εξοικονομούν χρήματα και 33% λένε ότι έχουν γίνει πιο παραγωγικές.

Σημαντικός αριθμός μικρομεσαίων επιχειρήσεων πιστεύουν ότι το Cloud θα μεταμορφώσει κυριολεκτικά το επιχειρηματικό περιβάλλον. Οι μισοί περίπου ιδιοκτήτες (45%) «συμφωνούν» ή «συμφωνούν απόλυτα» ότι το Cloud Computing θα γίνεται «όλο και πιο σημαντικό για μια εταιρία σαν τη δική μου». Το ένα τρίτο όλων (31%) πιστεύει ότι θα αποτελέσει κοινή πρακτική για τις μικρομεσαίες επιχειρήσεις.

Οι μικρομεσαίες επιχειρήσεις είναι ξεκάθαρες ως προς το ποιος είναι υπεύθυνος να εξασφαλίσει ότι τόσο οι επιχειρήσεις όσο και οι ιδιώτες μπορούν να υιοθετήσουν τις υπηρεσίες του Cloud εύκολα και με ασφάλεια, σε επίπεδο πρόσβασης, διαφάνειας, προστασίας δεδομένων και ασφάλειας. Το 60% λέει ότι αυτή η ευθύνη ανήκει στη βιομηχανία της πληροφορικής.

Όμως ακόμα κι έτσι, υπάρχουν ανησυχίες σε επίπεδο ασφάλειας: το 25% των ερωτηθέντων αμφισβητούν το κατά πόσο οι υπηρεσίες Cloud έχουν αποδείξει την αξία τους και τις θεωρούν επίφοβες, ενώ το 23% συμφωνεί απόλυτα στο ότι «τα δεδομένα στο Cloud δεν είναι ασφαλή». Επιπλέον, το 83% δηλώνουν ότι θέλουν να γνωρίζουν που είναι αποθηκευμένα τα δεδομένα τους. Διαβάστε την απάντηση της Microsoft, σχετικά με το Κέντρο Αξιοπιστίας.

Ποια είναι η πρόταση της Microsoft για το Cloud

Η Microsoft βασίστηκε στην επιτυχία του MS Office στο desktop και διέθεσε, λίγους μόλις μήνες πριν το 2011, μια ολοκληρωμένη πρόταση που αξιοποιεί την οικειότητα

των χρηστών με τις εφαρμογές παραγωγικότητας, αλλά και την ύπαρξη πρόσβασης στο Διαδίκτυο για ολοένα μεγαλύτερο ποσοστό επιχειρήσεων. Το MS Office στο desktop μπορεί πλέον να συνοδεύεται από τις διαδικτυακές εκδόσεις του, που εκτελούνται από τον browser (άρα, από οποιαδήποτε συσκευή έχει browser που πληροί τις ελάχιστες απαιτήσεις).

Εκτός όμως από αυτές, η εταιρεία προσθέτει σειρά εργαλείων που αξιοποιούν τη δικτύωση. Έτσι, εκτός από τις Office Web Apps, δηλαδή το Word, το Excel, το PowerPoint και το OneNote σε προστατευμένο χώρο φιλοξενίας για την εκάστοτε επιχείρηση και τους συνεργάτες της, διαθέτει προηγμένες υπηρεσίες επικοινωνίας και συνεργασίας της επιχείρησης όχι μόνο με τα μέλη της αλλά και με τους συνεργάτες ή τους πελάτες της μέσω Διαδικτύου.

Αυτό είναι με πολύ λίγα λόγια το Cloud Computing που προσφέρει η Microsoft. Πρόσφατα, έδωσε μια ηχηρή απάντηση και στις ανησυχίες των επιχειρήσεων για την προστασία των δεδομένων τους, με την υπογραφή πρότυπων ρητρών σε Ευρώπη και Η.Π.Α., δεσμευόμενη απέναντι στις Αρχές ότι το Office 365 πληροί τα αυστηρά κριτήρια προστασίας δεδομένων, αλλά και της επεξεργασίας τους.

Επιπλέον, εγγυάται διαθεσιμότητα κατά 99,9%, αποδίδοντας ιδιαίτερη έμφαση στην παράμετρο αυτή που αντικατοπτρίζεται και με την επιλογή της επωνυμίας της υπηρεσίας (διαθεσιμότητα 365 ημέρες το χρόνο)[18].

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] https://cloudsecurityalliance.org

[2] "Risk Landscape of Cloud Computing", Vasant Raval, 2010

[3] "Προστασία της ιδιωτικότητας και τεχνολογίες πληροφορικής και επικοινωνιών", Γκρίτζαλης, Λαμπρινουδάκης, Κάτσικας, Μήτρου, 2010

[4] "Security Threats in Cloud Computing Environments", Kangchan Lee, 2012

[5] "Gartner: Seven cloud-computing security risks", Jon Brodkin, 2008

[6] http://www.cloud-standards.org

[7] "Cloud Computing: Μια πρακτική προσέγγιση", Anthony T. Velte, Toby J. Velte, Robert P. Elsenpeter, μετάφραση: Μαίρη Γκλαβά

[8] http://cloudforum.boussiasconferences.gr

[9] "Cloud Computing Explained: Implementation Handbook for Enterprises", John Rhoton, (2010)

[10] http://www.boussiasconferences.gr/default.asp?pid=86&confID=201&la=1

[11] http://cloud-computing.softwareinsider.com/

[12] "Cloud Computing και ασφάλεια", Professional ITSecurity magazine, Ιανουάριος 2010

[13] https://en.wikipedia.org/wiki/Cloud_computing

[14] https://www.privacyrights.org/ar/cloud-computing.htm

[15] "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing", Robert Gellman, 2009

[16] "Cloud Computing Security", Ankur Mishra, Ruchita Mathur, Shishir Jain, Jitendra Singh Rathore

[17] "The NIST Definition of Cloud Computing", Peter Mell Timothy Grance, 2011

[18] http://reviews.in.gr/science-tech/MicrosoftOffice365/article/?aid=1231142710

[19] "Το Ευρωπαϊκό πλαίσιο για το Υπολογιστικό νέφος", υπό τη διεύθυνση: http://www.google.gr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCAQFjAAahUKEwi1zLyO85HGAhUJhywKHXf_AC0&url=http%3A%2F%2Fwww.pde.

gov.gr%2Fgr%2Fenimerosi%2Fitem%2Fdownload%2F5006.html&ei=wt9-VbXjJImOsgH3_oPoAg&usg=AFQjCNFaD76rsatu3WZugdYqFOlYJLlJHg&bvm=bv.95515949,d.bGg

[20] "An Applied Evaluation and Assessment of Cloud Computing Platforms", Hogberg, 2012

[21] "A Cloud Trust Model in a Security Aware Cloud", Sato, H., Kanai, A. ; Tanimoto, S., 2010

[22] "Establishing Trust in Cloud Computing", Khan, Malluki, 2010