Πανεπιστήμιο Πειραιά
Τμήμα Ψηφιακών Συστημάτων
ΠΜΣ - Κατεύθυνση: ¨Ψηφιακές Επικοινωνίες & Δίκτυα¨

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ζητήματα Ασφάλειας στο Υπολογιστικό Νέφος

Νικόλαος Α. Τζανετάκος

Επιβλέπων Καθηγητής : Λαμπρινουδάκης Κωνσταντίνος

Αθήνα

Ιούνιος 2011

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ζητήματα Ασφάλειας στο Υπολογιστικό Νέφος

Νικόλαος Α. Τζανετάκος
Α.Μ: ΜΕ/09097

Επιβλέπων Καθηγητής : Λαμπρινουδάκης Κωνσταντίνος

Τριμελής Εξεταστική Επιτροπή: Λαμπρινουδάκης Κωνσταντίνος

Ξενάκης Χρήστος

Κάτσικας Σωκράτης

Περιεχόμενα

ΠΡΟΛΟΓΟΣ

Η παρούσα εργασία εκπονήθηκε στα πλαίσια της υποχρεωτικής διπλωματικής εργασίας κατά τη διάρκεια του Δ' εξαμήνου των σπουδών μου στο ΠΜΣ του Πανεπιστημίου Πειραιώς, στο Τμήμα Ψηφιακών Συστημάτων, κατά το Ακαδημαϊκό Έτος 2010 – 2011, υπό την επίβλεψη του καθηγητή κ. Λαμπρινουδάκη Κωνσταντίνου.

Σκοπός αυτής της διπλωματικής εργασίας με τίτλο «Ζητήματα Ασφάλειας στο Υπολογιστικό Νέφος», είναι να παρουσιαστούν τα σημαντικότερα θέματα στο Υπολογιστικό Νέφος που αφορούν στην Ασφάλεια, καθώς και να εξεταστούν μερικοί τρόποι αντιμετώπισής τους όπου είναι αυτό εφικτό.

Η διπλωματική εργασία αυτή αποτελείται από επτά επιμέρους κεφάλαια.

Αναλυτικότερα:

Το πρώτο κεφάλαιο είναι εισαγωγικό και αναφέρεται γενικά στην έννοια του Υπολογιστικού Νέφους, στα βασικά χαρακτηριστικά και τις ιδιότητές του, τη δομή του, τα είδη των υπηρεσιών που εξυπηρετεί, τα επιχειρησιακά του οφέλη, καθώς και μερικά θέματα που απασχολούν τους επαγγελματίες που έχουν σκοπό να αγοράσουν υπηρεσίες Νέφους.

Το δεύτερο κεφάλαιο, επικεντρώνεται στους παρόχους υπηρεσιών Υπολογιστικού Νέφους και στις επιχειρήσεις που δραστηριοποιούνται στο χώρο αυτό, παρουσιάζοντας τους δέκα ισχυρότερους παρόχους νέφους. Επιπλέον, γίνεται εκτενέστερη αναφορά σε ένα από αυτούς, τη Microsoft, δίνοντας λεπτομέρειες για τη δομή και τις υπηρεσίες του Νέφους που προσφέρει. Το δεύτερο κεφάλαιο ολοκληρώνεται με θέματα που αφορούν στη δραστηριοποίηση μικρομεσαίων, καθώς και πιο συγκεκριμένα, Ελληνικών επιχειρήσεων στο Υπολογιστικό Νέφος.

Στο τρίτο κεφάλαιο, γίνεται εκτενής αναφορά στην Ασφάλεια στο Υπολογιστικό Νέφος. Παρουσιάζονται οι κυριότερες απειλές για την ασφάλεια της τεχνολογίας Νέφους, τα βασικότερα προβλήματα και οι κίνδυνοι που ελλοχεύουν. Εξετάζονται συγκεκριμένες αρχές προστασίας, διατήρησης και καταστροφής των προσωπικών δεδομένων και των πληροφοριών σε συνδυασμό με ζητήματα προστασίας της ιδιωτικότητας.

Το τέταρτο κεφάλαιο, αναλύει λεπτομερώς τις κυριότερες κρίσιμες απειλές της Ασφάλειας του Υπολογιστικού Νέφους, προτείνοντας παράλληλα μέτρα για την αντιμετώπισή τους.

Στο πέμπτο κεφάλαιο, παρουσιάζονται τα πλεονεκτήματα της Ασφάλειας στο Νέφος, καθώς και μερικές συμβουλές και πρακτικές για την, όσο το δυνατό, διασφάλιση των διακινούμενων πληροφοριών και δεδομένων, σε συνδυασμό με τη Διακυβέρνηση στο Νέφος.

Το έκτο κεφάλαιο, αφορά στις προβλέψεις των ειδικών σχετικά με τα θέματα Ασφάλειας στο Υπολογιστικό Νέφος και στις μελλοντικές τους εκτιμήσεις γενικότερα για την τεχνολογία αυτή.

Τέλος, το έβδομο και τελευταίο κεφάλαιο είναι ο επίλογος της διπλωματικής εργασίας στον οποίο δίνονται κάποια συμπεράσματα και προσωπικές εκτιμήσεις για το Υπολογιστικό Νέφος, την Ασφάλεια που απαιτείται για την ανάπτυξή του και την περαιτέρω εξάπλωσή του στο χώρο της Πληροφορικής παγκοσμίως.

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω τον πατέρα μου Τζανετάκο Αντώνιο καθώς και τη μητέρα μου Ευαγγελία, για την ηθική και ψυχολογική συμπαράσταση που μου προσέφεραν κατά τη διεκπεραίωση της διπλωματικής μου μελέτης.

Επιπλέον, θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή της διπλωματικής μου μελέτης, τον κ. Λαμπρινουδάκη Κωνσταντίνο.

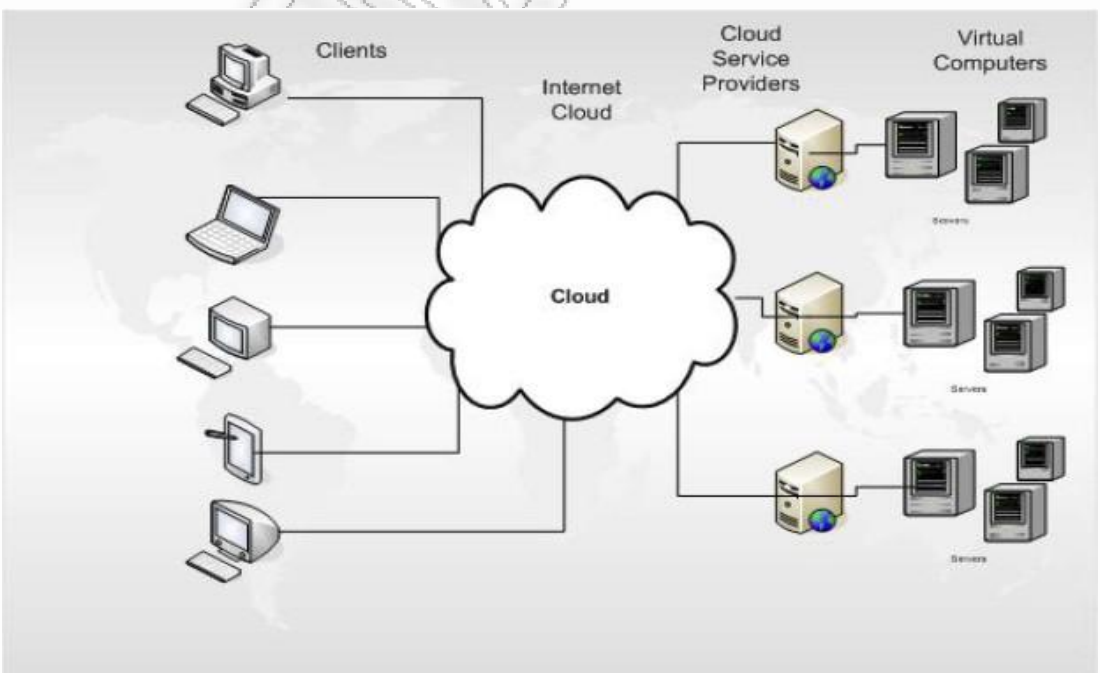
ΚΕΦΑΛΑΙΟ 1 : ΕΙΣΑΓΩΓΗ – Η ΕΝΝΟΙΑ ΤΟΥ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ

1.1Ορισμός Υπολογιστικού Νέφους

Σχεδόν όλη η βιομηχανία του IT αυτή την εποχή μιλάει για το Υπολογιστικό νέφος και ειδικότερα για το τι είναι το σύννεφο, πως μπορεί να χρησιμοποιηθεί και ποια προβλήματα και προκλήσεις θα φέρει στο τραπέζι. Ας πάρουμε τα πράγματα από την αρχή για να έχουμε μια πιο ξεκάθαρη εικόνα του σύννεφου.

Σήμερα αν κάνουμε την ερώτηση σε διαφορετικούς ανθρώπους «Τι είναι Υπολογιστικό Νέφος» θα διαπιστώσουμε ότι δεν υπάρχει μια απλή απάντηση. Οι απόψεις για τα είδη του διαφοροποιούνται, τόσο σε επίπεδο IaaS, PaaS ή SaaS όσο και στο διαχωρισμό Private, Community ή Public νέφους. Επίσης δεν είναι λίγοι αυτοί που θα το ταυτίσουν με το Virtualization.

Θα ξεκινήσουμε λοιπόν από τον όρο «Νέφος», ο οποίος πιθανότατα προκύπτει από τα γνωστά σκίτσα που έχει κατά καιρούς ζωγραφίσει καθένας από εμάς προσπαθώντας να αναπαραστήσει στο χαρτί το διαδίκτυο. Με το σκίτσο του νέφους συνήθως προσπαθούμε να περιγράψουμε ένα απομακρυσμένο σύνολο αξιόπιστων υπηρεσιών στον οποίο και στηριζόμαστε, χωρίς όμως να μας ενδιαφέρει το πώς λειτουργεί αυτό στα ενδότερα του. Όπως ακριβώς συμβαίνει και με το ηλεκτρικό ρεύμα όπου ο καταναλωτής ασχολείται μόνο με που βρίσκεται μια πρίζα και όχι με το πώς παράγεται ή μεταφέρεται η ηλεκτρική ενέργεια. Εννοιολογικά αυτό το γνωρίζουμε και ως utility ή grid computing.



Το Υπολογιστικό Νέφος λοιπόν, είναι ένα μοντέλο που επιτρέπει ευέλικτη, on-demand δικτυακή πρόσβαση σε ένα κοινόχρηστο σύνολο παραμετροποιήσιμων υπολογιστικών πόρων (π.χ. δίκτυα, servers, αποθηκευτικοί χώροι, εφαρμογές και υπηρεσίες), το οποίο μπορεί να τροφοδοτηθεί γρήγορα και να διατεθεί με ελάχιστη προσπάθεια διαχείρισης ή αλληλεπίδραση με τον πάροχο της υπηρεσίας, προωθώντας τη διαθεσιμότητα.

Το Υπολογιστικό νέφος κληρονομεί τα χαρακτηριστικά του utility computing και επιπλέον παρέχει ένα δυναμικό και ελαστικό περιβάλλον διάθεσης υπηρεσιών το οποίο μπορεί να είναι ανθεκτικό σε ραγδαίες και γιγαντιαίας κλίμακας μεταβολές των συνθηκών του. Αυτό επιτυγχάνεται με τα εγγενή χαρακτηριστικά του, που είναι η αυτόματη ανάκαμψη, η αυτό-επιτήρηση, η αυτό-διαχείριση, η αυτόματη επαναδιαμόρφωση, η δυνατότητα καθορισμού SLAs, και οι υψηλές δυνατότητες (αυτό)κλιμάκωσης.

Παρατηρώντας τα παραπάνω μπορούμε εύκολα να διαπιστώσουμε ότι πρόκειται για κάτι πολύ μεγαλύτερο και πιο πλούσιο από το utility computing και την τεχνολογία του virtualization, το οποίο σε συνδυασμό με τεράστιες οικονομίες κλίμακας που προσφέρει, θα αποτελέσει τη νέα εποχή του computing.

Η Gartner έχει ορίσει το υπολογιστικό νέφος σαν ένα στυλ computing, στο οποίο δυνατότητες πληροφορικής υποδομής κλιμακούμενες σε τεράστιο βαθμό παρέχονται σε μια μορφή υπηρεσίας σε πολλαπλούς εξωτερικούς πελάτες. Πέρα από τον ορισμό της Gartner όμως θα πρέπει να σημειώσουμε ότι τα διάφορα νέφη διαθέτουν και ένα self-service interface το οποίο παρέχει στους πελάτες τη δυνατότητα να αγοράσουν resources σε δεδομένη χρονική στιγμή και να σταματήσουν να τις χρησιμοποιούν όταν πλέον δεν θα είναι απαραίτητες.

Το νέφος δεν είναι στην πραγματικότητα μια τεχνολογία από μόνο του. Κατά βάση αποτελεί μια προσέγγιση στην δημιουργία υπηρεσιών IT, οι οποίες μπορούν να εκμεταλλευτούν στο έπακρο την αυξανόμενη δύναμη του hardware αλλά και των τεχνολογιών virtualization, που συνδυάζουν πολλούς servers σε μεγάλα pools resources αλλά και διαιρούν ενιαίους servers σε πολλαπλά εικονικά συστήματα, τα οποία μπορούν να ξεκινούν και να σταματούν ανά πάσα στιγμή.

1.2 Είδη υπηρεσιών Υπολογιστικού νέφους

Το Υπολογιστικό νέφος μπορεί να διαχωριστεί σε **δυο κατηγορίες**: ως προς το **είδος της υπηρεσίας** που προσφέρεται και ως προς το **deployment μοντέλο**.

Ξεκινώντας από τα είδη των υπηρεσιών, τα διαθέσιμα μοντέλα του Υπολογιστικού Νέφους είναι τα Software-as-as-a-Service, Platform-as-a-Service και Infrastructure-as-a-Service. Το κάθε ένα από αυτά, εξυπηρετεί διαφορετικές ανάγκες και προσφέρει διαφορετικές υπηρεσίες.

1.2.1 Διαθέσιμα μοντέλα υπηρεσιών Υπολογιστικού Νέφους

Το **Software-as-a-Service** βασίζεται στη λογική της υπενοικίασης λογισμικού από έναν πάροχο υπηρεσιών, αντί της αγοράς της άδειας χρήσης. Το λογισμικό λειτουργεί σε ένα κεντρικοποιημένο δίκτυο servers προκειμένου να διατίθεται ως υπηρεσία από το web ή το διαδίκτυο. Επίσης καλείται και ως «software on demand» και αποτελεί τον πλέον γνωστό τύπο Υπολογιστικού Νέφους λόγω της μεγάλης ευελιξίας, ποιότητας υπηρεσιών, υψηλής σταθερότητας και της ελάχιστης δυνατής συντήρησης που απαιτεί. Ο Πάροχος της υπηρεσίας φιλοξενεί και την εφαρμογή αλλά και τα δεδομένα έτσι οι χρήστες μπορούν να τη χρησιμοποιήσουν από οπουδήποτε. Το SaaS μοντέλο είναι πολύ αποτελεσματικό στη μείωση του κόστους αφού παρέχεται στην επιχείρηση ως μηνιαίο λειτουργικό κόστος το οποίο συνήθως είναι κατά πολύ οικονομικότερο από την αγορά των αντίστοιχων αδειών χρήσης και υποδομής. Στο SaaS μοντέλο δεν απαιτείται καμία συντήρηση ή αναβάθμιση, αφού ο τελικός αποδέκτης δε χρειάζεται να μεριμνήσει για τη διαθεσιμότητα, την κλιμάκωση, τη χωρητικότητα και το SLA της υποδομής, της πλατφόρμας και της υπηρεσίας. Η Microsoft παρέχει τις παρακάτω SaaS υπηρεσίες:, Exchange Online (ηλεκτρονικό ταχυδρομείο), SharePoint Online (Σύστημα διαχείρισης κειμένων και περιεχομένου) CRM Online, Office Live Meeting(ηλεκτρονικός χώρος συναντήσεων), Office Communications Online (Instant Messaging), Hotmail, Live Messenger, LiveID.

Ως συνέχεια του SaaS το **Platform-as-a-Service** παρέχει μια πλατφόρμα εφαρμογών νέφους για εταιρείες ή ιδιώτες που κατασκευάζουν λογισμικό είτε για ιδία χρήση είτε για τρίτους. Το μοντέλο αυτό παρέχει τις κατάλληλες υπηρεσίες προκειμένου κάποιος να μπορέσει να αναπτύξει, να δοκιμάσει, να διαθέσει και να συντηρήσει εφαρμογές και υπηρεσίες μέσα ένα ενιαίο περιβάλλον πλατφόρμας το οποίο είναι εγγενώς υψηλά διαθέσιμο, ελαστικό και ευέλικτο, με δυνατότητες πλήρους αυτό-διαχείρισης, αυτό-συντήρησης και αυτό-κλιμάκωσης της υποδομής, του λειτουργικού συστήματος και της πλατφόρμας εφαρμογών. Δηλαδή με το PaaS δεν χρειάζεται να ασχολούμαστε με τη συντήρηση του λειτουργικού συστήματος και της πλατφόρμας, όμως από την άλλη πλευρά δεν θα έχουμε και δυνατότητα λεπτομερούς ελέγχου αυτών. Το PaaS βασίζεται στο μοντέλο «Pay-per-use» με τέτοιο τρόπο έτσι ώστε να επιτυγχάνεται η πλήρης αξιοποίηση των υπολογιστικών πόρων που χρησιμοποιούνται σε σχέση με το κόστος χρήσης. Αν συνδυαστεί με το χαρακτηριστικό της αυτό-κλιμάκωσης μπορούμε να πετύχουμε τη διάθεση υπηρεσιών που να μπορούν να ανταποκρίνονται σε οποιαδήποτε ραγδαία ή αναμενόμενη μεταβολή χωρητικότητας (ισχύς, μνήμη, αποθηκευτικό χώρο, δίκτυο) που θα απαιτηθεί ανά πάσα χρονική στιγμή χωρίς να έχουμε δεσμευτεί εκ των προτέρων είτε με αγορά υποδομής, λογισμικού πλατφόρμας, δικτυακή γραμμή υψηλής χωρητικότητας κλπ. είτε με ένα συμβόλαιο παροχής υπηρεσιών φιλοξενίας υποδομής και πλατφόρμας συγκεκριμένης χωρητικότητας και χρονικής διάρκειας. Η Microsoft παρέχει τις παρακάτω PaaS υπηρεσίες: Windows Azure, SQL Azure, Windows Azure AppFabric.

Το τρίτο και τελευταίο μοντέλο είναι το **Infrastructure-as-a-Service** το οποίο είναι η παροχή υπολογιστικών και δικτυακών υποδομών ως μια πλήρως outsourced υπηρεσία. Η εταιρεία ή ο ιδιώτης μπορεί να υπενοικιάσει υποδομή (όχι όμως και πλατφόρμα όπως στο PaaS) ανάλογα με τις απαιτήσεις εκείνης της χρονικής στιγμής με λογική, όπως και στο PaaS, «Pay as you go» αντί να προβεί στην αγορά

εξοπλισμού (υπολογιστικού, δικτυακού, κλπ) ή στη σύναψη συμβολαίου παροχής υπηρεσιών φιλοξενίας υποδομής για συγκεκριμένο χρονικό διάστημα. Σημαντικό πλεονέκτημα του IaaS είναι επίσης η δυνατότητα μεταφοράς εικονικών μηχανών από το ιδιόκτητο περιβάλλον της εταιρείας ή του ιδιώτη στο νέφος, με συνοπτικές διαδικασίες. Σε αυτό το μοντέλο το γεγονός του ότι «αποκτώ πρόσβαση στο λειτουργικό σύστημα» (αφού παίρνω το Hardware ως υπηρεσία) μεταφράζεται στο «πως μπορώ να έχω από τη μια έλεγχο του λειτουργικού συστήματος και ό,τι εγκαθιστώ σε αυτό, αλλά από την άλλη να είμαι υπεύθυνος και για τη διαχείριση και συντήρηση αυτών». Η Microsoft παρέχει IaaS υπηρεσίες μέσω του Windows Azure.

1.2.2 Deployment Μοντέλα στο Υπολογιστικό Νέφος

Το deployment μοντέλο των υπηρεσιών Υπολογιστικού Νέφους διαχωρίζεται σε Public Νέφος, Community, Private και Hybrid.

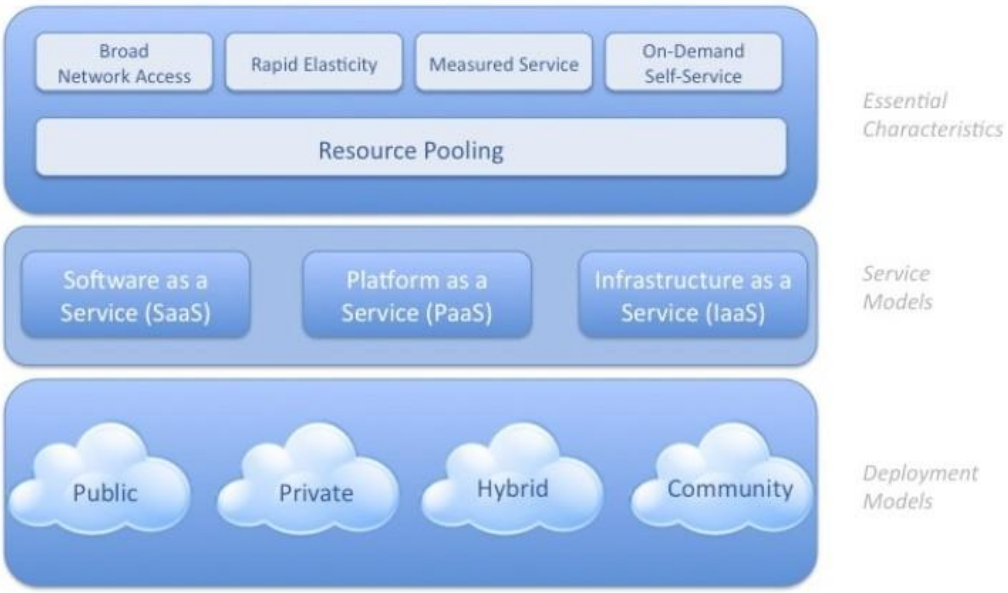
Το **Public Νέφος** αποτελεί ένα σύνολο από υπολογιστικούς πόρους οι οποίοι διατίθενται πάνω από το διαδίκτυο. Προσφέρονται από έναν πάροχο συνήθως με μοντέλο «pay as you go». Το Public Υπολογιστικό Νέφος έχει τα ακόλουθα πλεονεκτήματα: Η χρέωση της υπηρεσίας είναι για όσο χρησιμοποιηθεί, μεγάλη ευελιξία λόγω της άμεσης διάθεσης υπηρεσιών, υπάρχει άμεση κλιμάκωση σε μεγαλύτερη ή μικρότερη χωρητικότητα σε μόλις μερικά λεπτά και όλες οι υπηρεσίες προσφέρονται με βελτιωμένη και συνεχή διαθεσιμότητα, ελαστικότητα, ασφάλεια και διαχειρισιμότητα. Η Microsoft προσφέρει τις υπηρεσίες BPOS-S & Windows Azure Platform ενώ σύντομα και το CRM Online.

Στο **Community Νέφος,** η υποδομή μοιράζεται μεταξύ πολλών οργανισμών και υποστηρίζει μια συγκεκριμένη κοινότητα που έχει κοινές ανησυχίες (π.χ. αποστολή, απαιτήσεις ασφαλείας, πολιτική και θέματα συμμόρφωσης). Η διαχείρισή της μπορεί να γίνεται από τον ίδιο τον οργανισμό ή από τρίτους και μπορεί να βρίσκεται εντός ή εκτός των εγκαταστάσεων του οργανισμού.

Το **Private Νέφος** αποτελεί ένα σύνολο από υπολογιστικούς πόρους που προσφέρονται ως ένα προτυποποιημένο σύνολο υπηρεσιών οι οποίες καθορίζονται, σχεδιάζονται και ελέγχονται από ένα συγκεκριμένο οργανισμό. Η επιλογή ανάπτυξης ενός Private νέφους συνήθως καθοδηγείται από την ανάγκη για τη διατήρηση του πλήρους ελέγχου ενός παραγωγικού περιβάλλοντος εξ' αιτίας ιδιαίτερων απαιτήσεων των εφαρμογών από πλευράς απόδοσης, ωριμότητας ή νομικού πλαισίου λειτουργίας. Σημαντικό χαρακτηριστικό του είναι πολύ υψηλό κόστος απόκτησης και λειτουργίας του. Το Private νέφος συχνά συγχέεται με το Virtualization, το όποιο όμως αποτελεί μόνο ένα μικρό μέρος αυτού, αφού ακόμα και ως private θα πρέπει να έχει τα χαρακτηριστικά αυτόματης ανάκαμψης, αυτό-επιτήρησης, αυτό-διαχείρισης, αυτόματης επαναδιαμόρφωσης, δυνατότητας καθορισμού SLAs, και δυνατότητες (αυτό)κλιμάκωσης. Η Microsoft μέσω του Dynamic Datacenter Toolkit προσφέρει τη δυνατότητα ανάπτυξης Private νεφών.

Στο **Hybrid Νέφος**, η υποδομή είναι μια σύνθεση από δύο ή περισσότερα υπλογιστικά νέφη (private, community or public) τα οποία παραμένουν μοναδικές οντότητες, αλλά συνδέονται μεταξύ τους με τυποποιημένη ή αποκλειστική τεχνολογία που επιτρέπει τη φορητότητα δεδομένων και εφαρμογών (π.χ. εξισορρόπηση φόρτου εργασίας μεταξύ των clouds).

Μια νέα κατηγορία νέφους που έκανε την εμφάνιση της είναι το **Private Cloud Appliance** το οποίο αποτελεί ένα αποκλειστικό περιβάλλον που μπορεί να μεταφερθεί (συνήθως σε μορφή container) το οποίο παρέχεται και κατασκευάζεται από ένα κατασκευαστή ο οποίος έχει τον αρχιτεκτονικό έλεγχό του, την ευθύνη διαχείρισης και συντήρησης των φυσικών υποδομών, ενώ η λογική διαχείρισή του παραμένει στον τελικό καταναλωτή. Έτσι συνδυάζονται τα πλεονεκτήματα χρήσης προκαθορισμένης λειτουργικής αρχιτεκτονικής, μειώνοντας το ρίσκο διάθεσης υπηρεσιών μέσω της εσωτερικής ασφάλειας και ελέγχου. Παράδειγμα αυτής της κατηγορίας είναι το Windows Azure Appliance - http://www.microsoft.com/windowsazure/appliance/



1.3 Χαρακτηριστικά του Υπολογιστικού Νέφους

Τα **χαρακτηριστικά του Υπολογιστικού Νέφους** που προσφέρονται από τους παρόχους είναι:

- ***Scalability*:** Ανακατανομή δεδομένων καθώς εισάγεται νέο υλικό.
- ***Virtualization*:** Δυνατότητα εικονικών μηχανών.
- ***Pay as you Go / Pay as you Grow*:** Πληρωμή ανάλογα με τη ζήτηση πόρων και μέσων και την ανάπτυξη των αναγκών του πελάτη.
- ***Multitenancy*:** Δυνατότητα υποστήριξης διαφορετικών εφαρμογών.
- ***Elasticity*:** Δυνατότητα λήψης επιπλέον πόρων στις διάφορες εφαρμογές που υποστηρίζονται και πλήρη κάλυψη των αναγκών που προκύπτουν.
- ***Load and Tenant Balancing*:** Δυνατότητα μεταφοράς φορτίου ανάμεσα στους εξυπηρετητές για την αποφυγή υπερφόρτωσης.
- ***Availability*:** Συνέχιση λειτουργίας συστήματος ακόμα και σε περίπτωση υψηλών ποσοστών αποτυχίας εξυπηρετητών χωρίς την "πτώση" των υπηρεσιών που παρέχονται.
- ***Security*:** Μεγάλη ασφάλεια για την αδιάλειπτη λειτουργία των εφαρμογών χωρίς κανένα πρόβλημα.
- ***Operability*:** Δυνατότητα εύκολης διαχείρισης των συστημάτων νέφους.
- ***Metering*:** Δυνατότητα παρακολούθησης της χρήσης των πόρων που προσφέρονται καθώς και λήψη ειδοποιήσεων όταν κάποιος πόρος φτάσει σε οριακό σημείο και πρέπει να αυξηθεί.
- ***Global*:** Δυνατότητα χρήσης των υπηρεσιών νέφους από παντού.
- ***Simple APIs*:** Διευκόλυνση ανάπτυξης των εφαρμογών που χρησιμοποιούνται για υπηρεσίες νέφους.

Πως γίνεται η χρέωση;

Οι vendors που παρέχουν λύσεις SaaS εδώ και πολύ καιρό φωνάζουν ότι πουλάνε software με τη λογική του pay as you go, βάσει των αναγκών του πελάτη, χωρίς να τον κλειδώνει με μακρόχρονες συμφωνίες licensing για χρήση software on premise. Οι εταιρείες που παρέχουν infrastructure νέφους κάνουν ακριβώς το ίδιο. Για παράδειγμα το Amazon χρεώνει για ώρες χρήσης των δυνατοτήτων ενός virtualized server. Αντίστοιχα μοντέλα υπάρχουν και στις υπηρεσίες storage όπου η χρέωση μπορεί να γίνεται για αποθήκευση για GB ανά μήνα, με επιπλέον χρεώσεις για κάθε upload και download.

Ποιες εφαρμογές είναι φιλικές προς το νέφος;

Μιλώντας με τεχνικούς όρους, οποιαδήποτε εφαρμογή μπορεί να τρέξει στο νέφος, αλλά αυτό δεν σημαίνει ότι κάτι τέτοιο θα έχει νόημα, αφού για παράδειγμα δε θα είχε νόημα να βρίσκεται στο νέφος κάποια εφαρμογή, η οποία θα αφορά ένα συγκεκριμένο desktop. Πέρα από αυτό όμως υπάρχουν μια σειρά από νομικά θέματα και ζητήματα compliance, τα οποία δεν επιτρέπουν στις επιχειρήσεις να στείλουν συγκεκριμένα δεδομένα στο νέφος, ειδικά όσα αφορούν σε ευαίσθητα προσωπικά δεδομένα πελατών. Σύμφωνα με έρευνα της IDC οι βασικές χρήσεις του νέφους είναι το IT management, το collaboration, οι προσωπικές και επιχειρηματικές εφαρμογές, η ανάπτυξη εφαρμογών και το deployment αλλά και η παροχή πόρων server και storage.

Πόσο εύκολα αλλάζει κανείς νέφος;

Η απάντηση είναι ότι η αλλαγή μπορεί να πραγματοποιηθεί αλλά μάλλον δεν είναι καθόλου εύκολη σαν διαδικασία. Για το λόγο αυτό έχουν προκύψει μια σειρά από υπηρεσίες, οι οποίες αναλαμβάνουν τη μετακίνηση από το ένα νέφος στο άλλο ή από την εταιρική υποδομή στο νέφος. Αλλά η τάση που υποδεικνύεται από την αγορά, είναι ότι οι vendors, που έχουν εμπλακεί στο νέφος θα πρέπει να υιοθετήσουν τεχνολογίες, οι οποίες στηρίζονται σε στάνταρ, ώστε να διασφαλιστεί η απροβλημάτιστη μεταφορά ανάμεσα στις λύσεις των κατασκευαστών. Μάλιστα πριν από λίγο καιρό παρουσιάστηκε το Open Cloud Manifesto (www.opencloudmanifesto.org), που υποστηρίζει τη διαδραστικότητα των δεδομένων ανάμεσα στα διάφορα υπολογιστικά νέφη. Την ίδια στιγμή το Open Cloud Consortium προωθεί ανοικτά frameworks, τα οποία επιτρέπουν στα νέφη που λειτουργούν από διαφορετικές εταιρείες να λειτουργούν με απόλυτη διαφάνεια. Ο στόχος είναι να μπορούν οι εφαρμογές να μεταφερθούν από το ένα νέφος στο άλλο χωρίς να χρειάζεται να ξαναγραφτούν.

Θέματα licensing

Τόσο οι vendors αλλά και οι πελάτες έχουν προβληματιστεί σε μεγάλο βαθμό για τον τρόπο με τον οποίο οι πολιτικές licensing θα πρέπει να εφαρμοστούν στο νέφος. Οι vendors πακέτων software απαιτούν εξαρχής πληρωμής του 100% των χαρακτηριστικών μιας εφαρμογής, ακόμα και αν ο χρήστης χρησιμοποιεί το 50% αυτών ή ακόμη λιγότερες. Αυτό το μοντέλο δεν εκμεταλλεύεται την ευελιξία των υπηρεσιών νέφους.

Εταιρείες όπως η Oracle και η IBM έχουν εκδώσει σχετικούς πίνακες, στους οποίους εξηγούν με ποιο τρόπο το software τους αδειοδοτείται για το Amazon νέφος, αλλά οι περισσότεροι αναλυτές δείχνουν ότι απαιτούνται να γίνουν αρκετά βήματα ακόμα όσον αφορά στο licensing του software στο νέφος. Πρόσφατα και η Microsoft προχώρησε σε ανακοινώσεις σχετικά με την δική της τιμολογιακή πολιτική αλλά και τη δική της πρόταση για το νέφος. Το δεδομένο είναι ότι σε κάθε περίπτωση έχουμε μια μεγάλη αλλαγή σε επίπεδο business model, κάτι που καθιστά σαφές ότι θα

υπάρξουν καθυστερήσεις στις αναπροσαρμογές των τιμολογιακών πολιτικών των παραδοσιακών παικτών.

Τι γίνεται με το SLA;

Το τυπικό SLA που παρέχουν οι vendors νέφους είναι τουλάχιστον 99%, αλλά σε κάθε περίπτωση διαφέρει ο τρόπος με τον οποίο αυτό υπολογίζεται και υλοποιείται. Η Amazon αναφέρει ότι οι προσπάθειές της έχουν σαν στόχο να διασφαλίσει uptime της τάξης του 99,95%. Αλλά το uptime υπολογίζεται σε ετήσια βάση, έτσι αν αυτό το ποσοστό δεν τηρηθεί για μια βδομάδα ας πούμε δεν υπάρχει κάποια ποινή. Σε κάθε περίπτωση απαιτείται ιδιαίτερη προσοχή στα ψιλά γράμματα των συμβολαίων.

Τι γίνεται με την ασφάλεια των δεδομένων;

Το ζήτημα της ασφάλειας δεδομένων στο νέφος δεν είναι μια απλή περίπτωση, Υπάρχουν περιπτώσεις εταιρειών, οι οποίες έχασαν τα δεδομένα των πελατών τους και δεν μπόρεσαν να τα ανακτήσουν. Επιπλέον υπάρχει η περίπτωση ευαίσθητα δεδομένα να πέσουν σε λάθος χέρια. Πριν λοιπόν μια εταιρεία μπει στη διαδικασία να υπογράψει με κάποιο vendor νέφους θα πρέπει να απαιτήσει ιδιαίτερα έντονα πληροφορίες σχετικά με τις πρακτικές ασφάλειας που χρησιμοποιεί ο vendor και να διασφαλίσει την ικανότητα κρυπτογράφησης δεδομένων τόσο στη διάρκεια της μεταφοράς τους όσο και όσο βρίσκονται αποθηκευμένα στο νέφος.

Τι γίνεται με την απόδοση των εφαρμογών;

Πριν μια εταιρεία προχωρήσει στην επιλογή ενός vendor νέφους θα πρέπει να διαβάσει ιδιαίτερα προσεκτικά τι εγγυάται και τι όχι το SLA που παρέχει ο vendor αλλά επίσης θα πρέπει να εξετάσει και όποια δεδομένα υπάρχουν διαθέσιμα συνολικά. Για παράδειγμα το Amazon διαθέτει ένα Service Health Dashboard, που δείχνει τα ιστορικά δεδομένα αλλά και το τι συμβαίνει τη συγκεκριμένη στιγμή με το uptime των διαφόρων υπηρεσιών του.

Σε κάθε περίπτωση για τις εφαρμογές, που βρίσκονται στο νέφος θα πρέπει να περιμένουμε μια καθυστέρηση σε σχέση με το αν η ίδια εφαρμογή βρισκόταν στο τοπικό data center. Αλλά υπάρχει ήδη μια γενιά κατασκευαστών, οι οποίοι δημιουργούν υπηρεσίες για τη διασφάλιση της καλής κλιμάκωσης των υπηρεσιών αλλά και της καλής τους απόδοσης.

1.4 Κλιμάκωση – Απλότητα – Ασφάλεια

Ένα βασικό πλεονέκτημα της τεχνολογίας Cloud Computing, αποτελεί η δυνατότητα γρήγορης κλιμάκωσης. Αρχικά ο πελάτης μπορεί να πληρώνει μια χαμηλή – εισαγωγική συνδρομή, καθώς η εταιρία του θα αυξάνει την πελατειακή της βάση και της υπολογιστικές της ανάγκες, έχει την δυνατότητα για άμεση επέκταση της πληροφοριακής του υποδομής απλά μεταπηδώντας σε ένα «μεγαλύτερο» και φυσικά ακριβότερο πακέτο υπηρεσιών.

Στη συνέχεια εφόσον οι ανάγκες μειωθούν, προσαρμοζόμαστε στο κατάλληλο πακέτο υπηρεσιών που προσφέρονται με μικρότερο κόστος. Με τα κλασσικά πρότυπα ανάπτυξης πληροφοριακών υποδομών μια απότομη αύξηση της ζήτησης για υπολογιστικούς πόρους θα έπρεπε να περιμένει την έγκριση της σχετικής δαπάνης, την επιλογή και την αγορά εξοπλισμού, την παραμετροποίηση του λογισμικού κ.τ.λ., χρονικά αυτά μεταφράζεται σε αρκετές ημέρες αναμονής. Παράλληλα, το γεγονός ότι ο οργανισμός δεν αγοράζει την υποδομή αλλά μονό της υπηρεσία, αποκτά την δυνατότητα να μην νοιάζεται για την παραμετροποίηση, την συμβατότητα και αλλά θέματα λογισμικού και υλικού που αυξάνουν την πολυπλοκότητα της επένδυσης.

Ένα άλλο χαρακτηριστικό της αγοράς Νέφους είναι η δραστηριοποίηση εταιριών με μεγάλη εμπειρία στην παροχή υψηλού επιπέδου υπηρεσιών πληροφορικής (Google, Microsoft, Amazon). Η ύπαρξη αυτών των γιγάντων της πληροφορικής αποτελεί εχέγγυο για την βιωσιμότητα και την ομαλή εξέλιξη του μοντέλου Cloud Computing.

1.5 Λάθη και μύθοι για το Υπολογιστικό Νέφος

1.5.1 Λάθη που γίνονται στο νέφος

Υπάρχουν πολλές εταιρείες, οι οποίες κάνουν τα πρώτα τους βήματα στο κομμάτι του Υπολογιστικού Νέφους και προσπαθούν να επεκτείνουν την αρχιτεκτονική SOA στο νέφος. Σε αρκετές περιπτώσεις αυτές οι εταιρείες πραγματοποιούν κάποια ιδιαίτερα σημαντικά λάθη, τα οποία αν είχαν προσεχθεί θα είχαν αποφευχθεί εξ αρχής.

Λάθος Νο 1: Αντιμετώπιση του νέφους σαν αλλαγή πλατφόρμας και όχι αρχιτεκτονικής

Υπάρχουν πολλοί, οι οποίοι αντιλαμβάνονται το νέφος σαν μια απλή αλλαγή από το on-premise στο off-premise, αλλά υπάρχει ένας αριθμός από “κινούμενα μέρη” που επηρεάζονται, ανάμεσα στα οποία ξεχωρίζουν η ολοκλήρωση, η ασφάλεια, η διαχείριση υπηρεσιών κ.α.. Έτσι θα πρέπει να αντιμετωπίσουμε ολιστικά την αλλαγή πλατφόρμας σαν αλλαγή αρχιτεκτονικής. Αν χαθεί αυτό η διαδικασία θα μοιάζει με ταγκό – δυο βήματα μπροστά και ένα πίσω.

Συμβουλή: Αντιμετώπιση του νέφους σαν αρχιτεκτονική και όχι σαν μια αλλαγή τακτικής. Υπολογισμός του κόστους της αλλαγής αρχιτεκτονικής και όχι της πλατφόρμας.

Λάθος Νο 2: Αγνοήστε την απόδοση

Η χρήση τεχνολογίας, όπως αυτή που συναντάμε στο Υπολογιστικό Νέφος, συνήθως έχει επίπτωση στην απόδοση του συστήματος, καθώς οι διαδικασίες, οι υπηρεσίες και τα δεδομένα δεν βρίσκονται στον ίδιο φυσικό χώρο. Το σύνηθες λάθος είναι ότι τα προβλήματα απόδοσης γίνονται αντιληπτά όταν είναι πλέον πολύ αργά.

Συμβουλή: Δημιουργία ενός μοντέλου απόδοσης και υποβολή τεστ απόδοσης πριν την υιοθέτηση του Υπολογιστικού Νέφους σε επίπεδο παραγωγής.

Λάθος Νο 3: Η ερώτηση είναι γιατί και όχι πότε

Το hype που έχει δημιουργηθεί γύρω από το Υπολογιστικό Νέφος έχει πραγματικά ξεφύγει από κάθε σχεδόν όριο. Αυτό έχει σαν αποτέλεσμα πολλοί να θεωρούν τη μετάβαση στο νέφος όχι απλά σαν μια επιπλέον επιλογή, αλλά σαν κάτι που είναι απαραίτητο. Παρά το γεγονός ότι το Υπολογιστικό Νέφος παρέχει αρκετές ευκαιρίες για να αυξηθεί η αποτελεσματικότητα, δεν πρέπει όλες οι εφαρμογές, οι υπηρεσίες και τα δεδομένα να βρίσκονται στο νέφος. Θα πρέπει όλα αυτά να εξεταστούν σε μεγάλη λεπτομέρεια και να υπάρξει πλήρης κατανόηση των βασικών απαιτήσεων των συγκεκριμένων components πριν μεταφερθούν στο νέφος. Θα γίνει σαφές ότι σε πολλές περιπτώσεις, το Υπολογιστικό Νέφος δεν αποτελεί την κατάλληλη λύση.

Συμβουλή: Καθορισμός της αρχιτεκτονικής της εταιρείας σαν ένα σύνολο από components, κατανόηση του κάθε component και αποτίμηση της αξίας μετάβασής του στο νέφος. Αντικειμενικές αποφάσεις και όχι επιρροή από το hype.

1.5.2 7 Μύθοι για το Υπολογιστικό Νέφος

Το Hype που δημιουργούν οι vendors αλλά και πολλές φορές η υπερβολική αυτοπεποίθηση που δείχνουν τα τμήματα IT οδηγούν σε απογοητεύσεις. Αν μια εταιρεία εξετάζει το ενδεχόμενο να μεταβεί σε μια στρατηγική που περιλαμβάνει το νέφος δεν θα πρέπει να πιστέψει τα ακόλουθα:

Μύθος Νο 1: Υπάρχει ένα μόνο νέφος

Όπως έχουμε ήδη αναφέρει υπάρχουν τουλάχιστον τρεις τύποι Υπολογιστικού Νέφους – κάθε ένας με τα δικά του πλεονεκτήματα και μειονεκτήματα. Πιο συγκεκριμένα:

- Infrastructure as a Service
- Platform as a Service
- Software as Service

Η επιλογή θα πρέπει να γίνει βάσει του τύπου της εφαρμογής, που τρέχει η εταιρεία και στον τύπο των δεδομένων που χρησιμοποιεί.

Μύθος Νο 2: Μπορείτε να δουλέψετε αμέσως στο νέφος

Αν ο ενδιαφερόμενος είναι ένας μεμονωμένος developer με αρκετό χρόνο για χάσιμο, η ρύθμιση ενός virtual server από το μηδέν μπορεί να μην αποτελεί πρόβλημα. Αλλά στην περίπτωση μιας επιχείρησης, η διαδικασία εγκατάστασης και ρύθμισης του λειτουργικού συστήματος, πολλαπλών λειτουργικών και συνδέσεων με βάσεις δεδομένων, μπορεί να αποτελέσει σημαντικό εμπόδιο στην εισροή εσόδων. Αν μάλιστα η επιχείρηση είναι αρκετά μεγάλη, ώστε να διαθέτει τυποποιημένες διαδικασίες ασφάλειας, συγκεκριμένους τύπους δεδομένων το ζήτημα θα τραβήξει σε μάκρος.

Επιπλέον σε λίγες περιπτώσεις, έχει παρατηρηθεί οι παροχές IaaS να μην μπορούν να καλύψουν τις ανάγκες κλιμάκωσης συγκεκριμένων επιχειρησιακών εφαρμογών με μοντέλο on demand. Η Amazon πρόσφατα ανακοίνωσε την έναρξη public beta νέων χαρακτηριστικών για το νέφος της, ανάμεσα στα οποία ξεχωρίζει το auto-scaling, η παρακολούθηση και το load balancing.

Μύθος Νο 3: Το νέφος μειώνει το φόρτο εργασίας

Μακροπρόθεσμα αυτό μπορεί να είναι αλήθεια. Αλλά η εκκίνηση δεν είναι απλή αφού θα πρέπει η επιχείρηση να επιλέξει ποιο μοντέλο Υπολογιστικού Νέφους είναι το κατάλληλο προς χρήση, ποιες εφαρμογές ταιριάζουν καλύτερα σε αυτό, αλλά και να υπάρξει διασφάλιση των κατάλληλων επιπέδων ασφάλειας, compliance και uptime.

Μύθος Νο 4: Ομαλή ενοποίηση του datacenter με το public νέφος

Υπάρχουν κάποιοι ευαγγελιστές του νέφους, οι οποίοι ισχυρίζονται ότι μια εταιρεία μπορεί να εκμεταλλευτεί τα καλύτερα στοιχεία και από τους δυο κόσμους. Με άλλα λόγια τον έλεγχο που μπορεί να έχει μια επιχείρηση, στο δικό της datacenter με ταυτόχρονα τα χαμηλά έξοδα αλλά και την ευελιξία που παρέχει το νέφος. Αλλά κάτι τέτοιο δεν είναι καθόλου εύκολο στην πραγματικότητα, ειδικότερα για εφαρμογές multi-tier, οι οποίες εξαρτώνται σε μεγάλο βαθμό από τις εσωτερικές βάσεις δεδομένων. Αλλά ισχύει και το αντίστροφο, δηλαδή:

Μύθος Νο 5: Δεν θα μπορέσετε ποτέ να ενοποιήσετε το private και το public νέφος

Οι vendors προσπαθούν με ιδιαίτερη θέρμη να φτάσουν σε αυτό το αποτέλεσμα. Μέχρι όμως να φτάσουμε σε αυτό το αποτέλεσμα χρειάζεται να κοιτάξουμε ορισμένες άλλες προϋποθέσεις, όπως την τυποποίηση των διαμορφώσεων, τη μοντελοποίηση δεδομένων και την αυτοματοποιημένη εφαρμογή πολιτικών τόσο στο public όσο και στο private νέφος.

Μύθος Νο 6: Οι πάροχοι υπηρεσιών νέφους μπορούν να εγγυηθούν για την ασφάλεια

Ακόμα και στην περίπτωση που ένας πάροχος νέφους διαθέτει οποιαδήποτε πιστοποίηση νέφους μπορείτε να σκεφτείτε, δεν αποτελεί εχέγγυο, ότι οι servers σας, οι εφαρμογές σας αλλά και τα δεδομένα σας είναι ασφαλή. Αν για οποιοδήποτε λόγο, ο τρόπος με τον οποίο έχει σεταριστεί μια εφαρμογή δεν είναι σωστός, η εταιρεία δεν πρόκειται να ωφεληθεί από την ασφάλεια της πλατφόρμας του παρόχου του υπολογιστικού νέφους.

Μύθος Νο 7: Το Υπολογιστικό Νέφος είναι τεχνολογία

Η τεχνολογία καθιστά το Υπολογιστικό Νέφος εφικτό, αλλά για να μπορέσει μια επιχείρηση να απολαύσει τις μειώσεις στις δαπάνες και την ευελιξίας, απαιτείται η ύπαρξη των κατάλληλων διαδικασιών, διαφορετικά τα αποτελέσματα αναμένεται να είναι αποκαρδιωτικά.

1.6 Επιχειρησιακά Οφέλη του Υπολογιστικού Νέφους

Αν και τα οικονομικά οφέλη μοιάζουν να είναι ελκυστικά, σημαντικότερα ίσως είναι τα οφέλη που προκύπτουν από την εξομάλυνση των επιχειρησιακών διαδικασιών και την αύξηση της παραγωγικότητας μέσω της καινοτομίας.

Μερικά από τα επιχειρησιακά οφέλη λοιπόν του Υπολογιστικού Νέφους είναι τα παρακάτω:

Περιορισμός του Κόστους : Η δυνατότητα άμεσης αναβάθμισης των υπηρεσιών επιτρέπει την αποδέσμευση κεφαλαίων από ετεροχρονισμένες επενδύσεις σε έργα υποδομής με αποτέλεσμα το Συνολικό Κόστος Κτήσης (Total Cost of Ownership) των αντίστοιχων πληροφοριακών συστημάτων να κυμαίνεται σε χαμηλά επίπεδα.

Αμεσότητα : Η πρόσβαση με υψηλές ταχύτητες, η επέκταση του αποθηκευτικού χώρου και η ευρυζωνικότητα, επιτυγχάνονται με υψηλά επίπεδα διαθεσιμότητας μέσα από εναλλακτικά δίκτυα, προσφέροντας έτσι δυνατότητες εξορθολογισμού της ισχύος και αποφεύγοντας επομένως καθυστερήσεις στην επικοινωνία ή υπερφορτώσεις.

Αναβαθμισιμότητα : Η απεριόριστη προσφορά πόρων και υποδομής καλύπτει κάθε εμφανιζόμενη ζήτηση για νέες υπηρεσίες, σε πολύ σύντομο χρονικό διάστημα.

Αποτελεσματικότητα στη Διαχείριση Πόρων : Οι ανθρώπινοι πόροι που απασχολούνται στην παραγωγή μπορούν να διαχειριστούν αποτελεσματικότερα και να απασχοληθούν σε αποδοτικότερες εργασίες, όπως αυτές της Έρευνας και Ανάπτυξης.

Ανθεκτικότητα : Οι πάροχοι υπηρεσιών «νέφους» υλοποιούν παράλληλα συστήματα για τη διαχείριση σεναρίων καταστροφής αλλά και τον εξορθολογισμό της απαιτούμενης ισχύος.

1.6.1 Οι καταναλωτές είναι και επαγγελματίες

Οι επαγγελματίες αγκαλιάζουν τις ιδέες που φέρνει το Υπολογιστικό Νέφος χωρίς κάποιο αντίστοιχο προηγούμενο. Βλέπουν απευθείας αξία στην εταιρεία τους από τις προσφερόμενες εφαρμογές και υπηρεσίες. Καθώς η τεχνολογία γίνεται ολοένα και πιο εύκολη σε θέματα ανάπτυξης, μοιάζει ότι δεν υπάρχει όριο στο τι μπορεί να δοθεί από το νέφος, με μια τελείως μάλιστα νέα εμπειρία που δεν αφήνει κανένα αδιάφορο.

Όταν ο business χρήστης λαμβάνει μια εξαιρετικής ποιότητας υπηρεσίας σαν καταναλωτής είναι σχεδόν αδύνατο να μη την φέρει μαζί του στο χώρο εργασίας. Με υπηρεσίες όπως είναι το online backup, το project management, το CRM, τα εργαλεία collaboration και κοινωνικής δικτύωσης να γίνονται διαθέσιμα μέσω ενός browser, θα μπορούσε να θεωρηθεί έκπληξη το γεγονός ότι δεν προχωρούν όλοι οι χρήστες σε χρήση των συγκεκριμένων υπηρεσιών παρατώντας αυτές που παρέχει το τμήμα IT.

Δεν έχει περάσει πάρα πολύ μεγάλο χρονικό διάστημα από τη στιγμή που μια κεντρική κυβερνητική υπηρεσία στη Βρετανία ανακάλυψε στο δίκτυό της πάνω από 2.500 εφαρμογές, τις οποίες δεν υποστήριζε. Από αυτές οι 500 είχαν πλέον αναχθεί σε mission critical για αυτούς που τις χρησιμοποιούσαν. Μέσω του νέφους είναι σχεδόν αδύνατο να ανακαλυφθούν ποιες εφαρμογές και υπηρεσίες χρησιμοποιούνται από κάθε χρήστη.

1.7 Προβληματισμοί για υιοθέτηση τεχνολογίας νέφους

Μπορεί σε πρώτη φάση, η χρήση των υπηρεσιών αυτών να δίνει την εντύπωση ότι αφαιρεί κάποιο βάρος από το τμήμα IT. Υπάρχουν κυριολεκτικά χιλιάδες start-ups, που παρέχουν λύσεις σε επιχειρηματικά ζητήματα, με μικρό κόστος ή ακόμη και δωρεάν. Τα τμήματα IT θα πρέπει να αντιμετωπίσουν το Υπολογιστικό Νέφος σαν ένα σύμμαχο, καθώς θα τους κάνει να φανούν σαφώς πιο αποτελεσματικοί στις εταιρείες τους. Όμως οι υπηρεσίες που χρησιμοποιούνται εν αγνοία τους μοιάζει να έχουν το ανάποδο αποτέλεσμα.

Δεν είναι κρυφό ότι υπάρχει μια πολύ μεγάλη συζήτηση για το διαχωρισμό του IT και του business. Δυστυχώς οι υπηρεσίες και εφαρμογές νέφους που χρησιμοποιούνται εν αγνοία τους, κάνουν το κενό ανάμεσα στο IT και το business ακόμη μεγαλύτερο. Από την πλευρά τους οι business χρήστες βλέπουν τις αντιρρήσεις που έχει το IT σαν έλλειψη ευελιξίας και ανταπόκρισης. Το τμήμα IT από την άλλη βλέπει όλους τους κινδύνους που υπάρχουν από τη χρήση των συγκεκριμένων εφαρμογών που σχετίζονται με τις λειτουργίες, το compliance και την ολοκλήρωση με τις υπόλοιπες εφαρμογές, καταδεικνύοντας την αφέλεια των χρηστών.

Τα εταιρικά συστήματα έχουν σημαντικό κόστος για να δημιουργηθούν. Είναι ζωτικής σημασίας και πρέπει να υποστηρίξουν όλη την επιχείρηση και αυτοί είναι λίγοι από τους λόγους, για τους οποίους η εταιρεία δεν μπορεί να αποχωριστεί εν ριπή οφθαλμού τα εν λόγω συστήματα. Άλλωστε δεν πρέπει να μας διαφεύγει το γεγονός ότι ελάχιστες υπηρεσίες από αυτές που έχουν προκύψει από το νέφος είναι πραγματικά έτοιμες για χρήση σε εταιρικό περιβάλλον. Το βασικό στοιχείο είναι ότι υπάρχει ένα σύνολο από ερωτήσεις, που θα πρέπει να απαντηθούν πριν μια επιχείρηση αρχίσει να χρησιμοποιεί εφαρμογές, οι οποίες βρίσκονται στο νέφος. Πολλές από αυτές, οι επιχειρήσεις τις έχουν κάνει στους κατασκευαστές εφαρμογών που χρησιμοποιούνται on-premise. Υπάρχουν και άλλες ερωτήσεις, οι οποίες όμως θα πρέπει να απαντηθούν και αφορούν στο νέφος. Αλλά ένα βασικό σημείο που θα πρέπει να προσεχθεί από όλους, είναι ότι οι χρήστες οι οποίοι αρχίζουν να παίρνουν αποφάσεις για το ποιες εφαρμογές νέφους θα πρέπει να χρησιμοποιήσουν, δεν ξέρουν ποιες ερωτήσεις θα πρέπει να κάνουν.

Τι πρέπει να γίνει;

Δεν μπορείτε να αγνοήσετε το Υπολογιστικό Νέφος. Για όσο οι χρήστες διαθέτουν ένα browser και μια σύνδεση στο Internet τόσο το πρόβλημα παραμένει. Όπως μπορεί να καταλάβει κανείς δεν μπορεί να κόψει απλά την πρόσβαση στο Internet και να λύσει το πρόβλημα. Κάτι τέτοιο θα είχε ακριβώς τα ανάποδα αποτελέσματα. Οι χρήστες θα προσπαθήσουν με κάθε τρόπο να προσπεράσουν το IT. Πόσο δύσκολο είναι να συνδέσει κάποιος ένα 3G modem στον υπολογιστή του και να αποκτήσει πρόσβαση πιστεύετε; Υπάρχει ένα νέο αρκτικόλεξο που περιγράφει τη λύση στο πρόβλημα. Υποδεχτείτε το PASTA (Policy, Amnesty, Support (υποστήριξη επί το ελληνικότερο), Technology Evaluation (Αποτίμηση τεχνολογίας), Adoption (Υιοθέτηση)) και πιο συγκεκριμένα:

Policy: Ποια είναι η εταιρική πολιτική για το Υπολογιστικό Νέφος; Θυμηθείτε ότι η απάντηση δεν είναι μια απλή απάντηση, η οποία γίνεται αποδεκτή, καθώς θα κάνει πιο δημιουργικούς τους εργαζόμενους που θέλουν να έχουν πρόσβαση στις υπηρεσίες που χρησιμοποιούν. Οι πολιτικές που θα υλοποιηθούν θα πρέπει να είναι ρεαλιστικές.

Αμνηστία: Θα πρέπει να ανακαλύψετε ποιοι είναι οι χρήστες, οι οποίοι χρησιμοποιούν αυτές τις υπηρεσίες, κάτι που θα είναι πολύ δύσκολο αν πιστεύουν ότι κάτι τέτοιο θα τους στοιχίσει την καριέρα τους. Η περίοδος αμνηστίας δεν θα πρέπει να ξεπερνά το μήνα, καθώς θα πρέπει να κάνει κατανοητό το επείγον του θέματος και θα πρέπει να γίνει όσο το δυνατόν πιο ευρέως γνωστή. Μετά το πέρας της δε θα πρέπει να υπάρχουν δικαιολογίες για τη συνέχιση της χρήσης υπηρεσιών που δεν είναι εγκεκριμένες.

Υποστήριξη: Οι τελικοί χρήστες θα πρέπει να πιστέψουν ότι αν είναι ειλικρινείς με τις πληροφορίες που θα δώσουν για τις υπηρεσίες που χρησιμοποιούν θα έχουν την απαραίτητη βοήθεια και υποστήριξη για να συνεχίσουν να χρησιμοποιούν τις ίδιες τεχνολογίες. Αυτό είναι ένα ιδιαίτερα δύσκολο σημείο, αλλά θα πρέπει να τηρηθεί ανεξάρτητα από το πόσο αναξιόπιστη θεωρείται η συγκεκριμένη εφαρμογή.

Αποτίμηση τεχνολογίας: Πρόκειται για μια πλήρη αποτίμηση, τόσο σε τεχνικό όσο και εμπορικό μοντέλο για τις εφαρμογές νέφους που χρησιμοποιούνται. Αυτό όπως αντιλαμβάνεται κανείς δεν είναι μια συνηθισμένη διαδικασία, αν αναλογιστεί κανείς το μεγάλο αριθμό των εφαρμογών που χρησιμοποιούνται και το χρόνο που απαιτείται για να ανακαλυφθούν.

Υιοθέτηση: Τώρα θα πρέπει να μπείτε στη διαδικασία να δημιουργήσετε την αρχιτεκτονική νέφους της επιχείρησή σας. Αυτό μπορεί να έχει σαν αποτέλεσμα να πρέπει να υιοθετήσετε πολλές από τις εφαρμογές, που χρησιμοποιούν οι χρήστες σας, αλλά και να μεταφέρετε πάλι κάποιους χρήστες πίσω στο εταιρικό στάνταρ. Στη συνέχεια θα πρέπει να δουλέψετε για να επιβάλλετε την υιοθέτηση της εφαρμογής που έχετε επιλέξει, αλλά αυτό δεν είναι κάτι καινούργιο.

Οι τρεις πρώτες φάσεις είναι και οι πιο σημαντικές για να μπορέσετε να μπείτε πραγματικά σε μια διαδικασία ελέγχου και εκτίμησης των πραγματικών κινδύνων που φέρνουν οι εν λόγω εφαρμογές στην επιχείρηση. Οι δυο επιπλέον φάσεις θα χρειαστούν κάποιο επιπλέον χρόνο.

Το Υπολογιστικό Νέφος είναι εδώ για να μείνει. Οι εταιρικοί χρήστες χρησιμοποιούν τους browsers που διαθέτουν για να αποκτήσουν πρόσβαση σε εφαρμογές νέφους, αλλά δεν γνωρίζουν για τυχόν κινδύνους. Ο ρόλος του CIO είναι αυτός που θα μπορέσει να ξεχωρίσει τις καλύτερες εφαρμογές από κάθε περίπτωση και θα τις ενσωματώσει στην εταιρική κουλτούρα και υποδομή.

1.7.1 Αγοράζοντας υπηρεσίες νέφους

Η αγορά υπηρεσιών Υπολογιστικού Νέφους δεν είναι τόσο απλή σαν τη διαδικασία servers και storage. Προτού μια εταιρεία μπει στη διαδικασία να εμπλακεί με κάποιο πάροχο νέφους, οι άνθρωποι του IT θα πρέπει να δουν ποιες πηγές έχουν διαθέσιμες, τι αγοράζουν και πως αυτό λειτουργεί σε μια public διαμοιρασμένη υποδομή. Μερικά σημεία που πρέπει να προσεχθούν είναι τα ακόλουθα:

1. Είναι οι εφαρμογές σας έτοιμες;

Δεν είναι λίγες οι περιπτώσεις, που μια εφαρμογή πρέπει να περάσει από αλλαγή αρχιτεκτονικής για να μπορεί να χρησιμοποιηθεί στο νέφος. Η αλλαγή αυτή είναι επιβεβλημένη καθώς η ήδη υπάρχουσα λύση, μπορεί να αποτελεί ανασταλτικό παράγοντα για τη μετάβαση στο νέφος.

2. Που βρίσκονται τα δεδομένα?

Ένας vendor νέφους δεν πρόκειται να μοιραστεί τις λεπτομέρειες για το δίκτυό του, αλλά θα πρέπει σε κάποιο βαθμό να δίνει ικανοποιητικές απαντήσεις στον πελάτη του. Για παράδειγμα το Νέφος της Amazon παρέχει τη δυνατότητα αποθήκευσης των δεδομένων μεταξύ Η.Π.Α. και Ευρώπης και στη συνέχεια μπορεί ο ενδιαφερόμενος να επιλέξει και ζώνη διαθεσιμότητας. Αν μια εταιρεία γνωρίζει που βρίσκονται τα δεδομένα της σε επίπεδο IP νέφους, τότε μπορεί να έχει μια καλή εικόνα για την πρόσβαση στους πόρους του νέφους και πως αυτή θα επηρεαστεί από την επιλογή παρόχου σύνδεσης.

3. Πως προστατεύονται τα δεδομένα;

Η συνεργασία με έναν πάροχο νέφους , ο οποίος επιτρέπει τη γεωγραφική τοποθέτηση των δεδομένων, μπορεί να βοηθήσει και σε ζητήματα ασφάλειας και ακόμη περισσότερο σε θέματα compliance. Δεν είναι λίγες οι εταιρείες που πλέον ρωτούν πρώτα για compliance και στη συνέχεια για ασφάλεια. Ειδικότερα όσον αφορά στην ασφάλεια θα πρέπει να σημειώσουμε ότι απαιτείται να υπάρχει η δυνατότητα κρυπτογράφησης των δεδομένων τόσο κατά τη διάρκεια της μεταφοράς όσο και στη φάση της αποθήκευσής τους με τη χρήση ασφαλών πρωτοκόλλων όπως το Secure-HTTP. Επιπλέον καλό είναι να γνωρίζει η εταιρεία που ενδιαφέρεται για υπηρεσίες νέφους, ποιος έχει φυσική πρόσβαση στα συστήματα που φιλοξενούν τα δεδομένα της, ενώ θα πρέπει να έχει καθοριστεί με ιδιαίτερη ακρίβεια ποιοι έχουν δικαίωμα να πραγματοποιήσουν αλλαγές σε αυτά. Καλό θα ήταν σε όλο το πακέτο να υπάρχει και μια διαδικασία disaster recovery για να αποφευχθεί οποιοδήποτε σημαντικό πρόβλημα.

4. Τι γίνεται με την υποστήριξη;

Πολλά τμήματα IT μπορεί να μην έχουν τον απαραίτητο χρόνο ή και την τεχνογνωσία για να αντεπεξέλθουν στη μετάβαση στο νέφος και μπορεί να χρειαστούν τη βοήθεια του support του vendor. Χαρακτηριστικό παράδειγμα είναι οι αλλαγές που απαιτούνται σε μια εφαρμογή, που περνά από το on-premise στο νέφος.

5. Τι γίνεται αν θέλω να φύγω;

Δεν αρκεί να γνωρίζουμε όλες τις λεπτομέρειες για τη μετάβαση στο νέφος, αλλά θα πρέπει να γνωρίζουμε τι θα συμβεί αν κάποια στιγμή αποφασίσουμε να μεταβούμε σε κάποιο άλλο πάροχο ή αν θελήσουμε να υιοθετήσουμε κάποιο hybrid μοντέλο. Καλό είναι λοιπόν να έχουμε σχεδιάσει και μια στρατηγική εξόδου από το νέφος.

ΚΕΦΑΛΑΙΟ 2 : ΠΑΡΟΧΟΙ ΚΑΙ ΕΠΙΧΕΙΡΗΣΕΙΣ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ

2.1 Δέκα πάροχοι νέφους που ξεχωρίζουν

Υπάρχουν πάρα πολλοί vendors, οι οποίοι παρέχουν υπηρεσίες Υπολογιστικού Νέφους. Επιλέξαμε και παρουσιάζουμε 10 εταιρείες που ξεχωρίζουν.

Amazon

Τι προσφέρει: Ανάμεσα στις υπηρεσίες του ξεχωρίζουν, οι Amazon Web Services περιλαμβανομένου του Elastic Compute Cloud, αλλά και η υπηρεσία Simple Storage για on-demand storage.

Σε ποιον απευθύνεται: Κυρίως σε επιχειρήσεις – ανεξαρτήτως μεγέθους – αλλά και μεμονωμένους χρήστες.

AT&T

Τι προσφέρει: Την υπηρεσία Synaptic Hosting, για φιλοξενία εφαρμογών που προσφέρει πρόσβαση pay as you go σε virtual servers και storage ολοκληρωμένη με ασφάλεια και δικτυακές λειτουργίες.

Σε ποιον απευθύνεται: Κυρίως σε εταιρείες, που χρειάζονται ιδιαίτερα ισχυρή παρουσία στο Internet χωρίς να θέλουν να επενδύσουν στην αντίστοιχη υποδομή.

Enomaly

Τι προσφέρει: Η Elastic Computing Platform της Enomaly είναι software που ολοκληρώνει τα data centers των επιχειρήσεων με εμπορικές προσφορές Υπολογιστικού Νέφους, δίνοντας τη δυνατότητα στους IT Pros να διαχειρίζονται τόσο τα εσωτερικά όσο και εξωτερικά resources από μια ενιαία κονσόλα διευκολύνοντας τη μετάβαση virtual συστημάτων από το ένα data center στο άλλο.

Σε ποιον απευθύνεται: Όπως αντιλαμβάνεται κανείς η εν λόγω υπηρεσία αφορά κυρίως μεγάλες επιχειρήσεις και ανάμεσα στους πελάτες της εταιρείας φιγουράρουν ονόματα όπως η Deutsche Bank, η France Telecom και η κυβέρνηση του Καναδά.

Google

Τι προσφέρει: Ξεκινάμε από τα Google Apps, ένα σύνολο online εργαλείων παραγωγικότητας που περιλαμβάνουν e-mail, calendar, επεξεργαστή κειμένου και ένα απλό εργαλείο δημιουργίας σελίδων web. Προχωράμε στην υπηρεσία Postini (που έχει προκύψει από την εξαγορά της ομώνυμης εταιρείας), ένα σύνολο από υπηρεσίες ασφαλείας για e-mail και web. Τέλος δεν θα πρέπει να ξεχάσουμε να αναφέρουμε την Google App Engine μια προσφορά Platform as a Service που επιτρέπει στους developers να δημιουργήσουν εφαρμογές, οι οποίες φιλοξενούνται στις υποδομές του Google.

Σε ποιον απευθύνεται: Κυρίως σε μικρές εταιρείες αλλά και σε μεγαλύτερους οργανισμούς, ενώ στο εξωτερικό έχει αρκετά μεγάλη επιτυχία και σε εκπαιδευτικό επίπεδο.

GoGrid

Τι προσφέρει: Η πλατφόρμα GoGrid platform προσφέρει web-based storage και τη δυνατότητα γρήγορης εγκατάστασης Windows ή Linux virtual servers στο νέφος με προεγκατεστημένο software, που περιλαμβάνει Apache, PHP, Microsoft SQL και MySQL.

Σε ποιον απευθύνεται: Κυρίως σε start-ups και εταιρείες που θέλουν να λειτουργήσουν σε περιβάλλον Web 2.0 και SaaS.

Microsoft

Τι προσφέρει: Η βασική προσφορά της εταιρείας έχει την ονομασία Azure και πρόκειται για μια πλατφόρμα Windows as a Service, που περιλαμβάνει και πολλές υπηρεσίες ειδικά σχεδιασμένες για developers (SQL, Sharepoint, CRM κ.α.), που μπορούν να χρησιμοποιηθούν για το κτίσιμο και την αναβάθμιση των web-hosted εφαρμογών.

Σε ποιον απευθύνεται: Κατά βάση σε εταιρείες, που θέλουν να δημιουργήσουν εφαρμογές που θα προσφέρουν στη συνέχεια μέσω του νέφους.

NetSuite

Τι προσφέρει: Μια σουίτα business software, που περιλαμβάνει e-commerce, CRM, λογιστικά και ERP εργαλεία.

Σε ποιον απευθύνεται: Κατά βάση σε επιχειρήσεις ανεξαρτήτου μεγέθους.

Rackspace

Τι προσφέρει: Το νέφος της εταιρείας, που είναι γνωστό με την ονομασία Mosso αποτελείται από τρεις βασικές υπηρεσίες: sites νέφους, μια πλατφόρμα για τη δημιουργία Web Sites, Files νέφους, μια υπηρεσία αποθήκευσης, και Servers νέφους μια υπηρεσία που παρέχει πρόσβαση σε virtualized server instances.

Σε ποιον απευθύνεται: Κατά βάση σε web developers αλλά και παρόχους Software as a Service, όπως η Zapproved που παρέχει ένα online εργαλείο παραγωγικότητας.

RightScale

Τι προσφέρει: Μια πλατφόρμα Software as a Service, που επιτρέπει στους πελάτες να διαχειρίζονται τις διεργασίες IT που έχουν κάνει outsource σε vendors νέφους. Η λύση της RightScale παρέχει στους πελάτες τη δυνατότητα να δημιουργήσουν και να κλωνοποιήσουν virtual servers για το νέφος, παρέχει load balancing ανάλογα με το φόρτο εργασίας της δεδομένης στιγμής, αυτοματοποιεί τις διαδικασίες backup και προσφέρει παρακολούθηση και αναφορά λαθών.

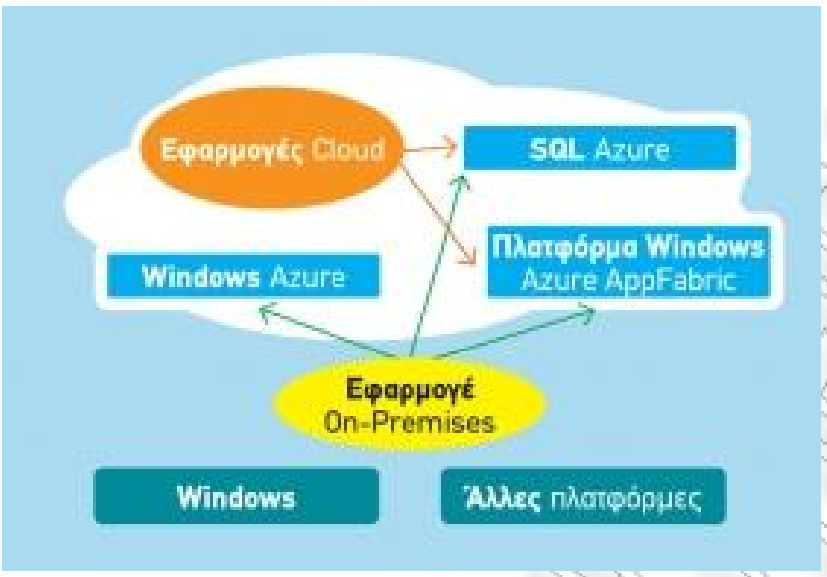
Σε ποιον απευθύνεται: Την εν λόγω υπηρεσία χρησιμοποιούν μεγάλες εταιρείες, οι οποίες χρειάζεται να διαχειριστούν μεγάλο αριθμό από servers βασιζόμενων σε τεχνολογία νέφους.

Salesforce.com

Τι προσφέρει: Η ναυαρχίδα της εταιρείας είναι ένα σύνολο από εργαλεία CRM, συμπεριλαμβανομένων salesforce automation, analytics, marketing αλλά και εργαλεία social networking. Μια δεύτερη μεγάλη υπηρεσία της εταρείας είναι η Force.com μια πλατφόρμα για τη δημιουργία εφαρμογών web και φιλοξενία στην υποδομή της εταιρείας.

Σε ποιον απευθύνεται: Την υπηρεσία χρησιμοποιούν πάνω από 55.000 πελάτες σε διάφορους χώρους της βιομηχανίας όπως οικονομικές υπηρεσίες, επικοινωνίες, retail και πολλά άλλα.

2.2 Παράδειγμα παρόχου : Η Microsoft στα σύννεφα



Η πλατφόρμα της Microsoft με την ονομασία Azure, είναι ένα σύνολο τεχνολογιών νέφους, κάθε μια από τις οποίες παρέχει ένα συγκεκριμένο σετ υπηρεσιών στους developers εφαρμογών.

Τα βασικά components της πλατφόρμας Azure είναι τα ακόλουθα:

- **Windows Azure:** παρέχει ένα windows-based περιβάλλον πάνω στο οποίο τρέχουν οι εφαρμογές και αποθηκεύονται τα δεδομένα
- **SQL Azure:** Παρέχει υπηρεσίες δεδομένων στο νέφος που στηρίζονται στον SQL Server
- **Windows Azure AppFabric:** Παρέχει υπηρεσίες νέφους για τη σύνδεση εφαρμογών που τρέχουν στο νέφος και on premise.

Κάθε κομμάτι της πλατφόρμας Azure έχει ένα συγκεκριμένο ρόλο. Πιο συγκεκριμένα:

2.2.1 Windows Azure

Σε υψηλό επίπεδο το Azure είναι ιδιαίτερα απλό να γίνει αντιληπτό. Είναι μια πλατφόρμα πάνω στην οποία τρέχουν εφαρμογές και αποθηκεύουν τα δεδομένα στο νέφος. Το Windows Azure τρέχει στα datacenters της Microsoft και η πρόσβαση γίνεται μέσω του Internet. Η υπηρεσία του Windows Azure στηρίζεται όπως είναι εύκολο να καταλάβει κανείς στα Windows. Οι developers μπορούν να δημιουργήσουν τις εφαρμογές τους χρησιμοποιώντας το .Net Framework, unmanaged κώδικα ή άλλες προσεγγίσεις. Αυτές οι εφαρμογές μπορούν να γραφτούν σε μια σειρά από γλώσσες όπως C#, Visual Basic, C++ και Java χρησιμοποιώντας το Visual

Studio ή οποιαδήποτε άλλη εφαρμογή. Επίσης μπορεί κάποιος να δημιουργήσει εφαρμογές web, χρησιμοποιώντας τεχνολογίας όπως είναι οι ASP.NET, Windows Communication Foundation (WCF) και PHP, εφαρμογές που τρέχουν σαν ανεξάρτητες διαδικασίες στο background ή και συνδυασμό τους.

Τόσο οι εφαρμογές Windows Azure όσο και οι εφαρμογές που τρέχουν on premise, μπορούν να έχουν πρόσβαση στον αποθηκευτικό χώρο του Azure και μάλιστα με τον ίδιο τρόπο χρησιμοποιώντας την προσέγγιση RESTFul. Αυτή η υπηρεσία επιτρέπει την αποθήκευση μεγάλων δυαδικών αντικειμένων (binary large objects - blobs) για την επικοινωνία ανάμεσα στα components των εφαρμογών Windows Azure ενώ παρέχει μια φόρμα πινάκων με μια απλή γλώσσα query. Για τις εφαρμογές που χρειάζονται την παραδοσιακή relational αποθήκευση το Windows Azure παρέχει το SQL Azure Database, για το οποίο θα μιλήσουμε στη συνέχεια. Μια εφαρμογή, η οποία χρησιμοποιεί την πλατφόρμα Azure είναι δυνατό να χρησιμοποιήσει οποιοδήποτε συνδυασμό αποθήκευσης. Το τρέξιμο εφαρμογών κα η αποθήκευση δεδομένων στο νέφος έχει ξεκάθαρα πλεονεκτήματα. Μια επιχείρηση - σε ακραία περίπτωση - δεν χρειάζεται να αγοράζει, εγκαθιστά και να λειτουργεί τα δικά της συστήματα αλλά να συνεργάζεται μια εταιρεία παροχής υπηρεσιών νέφους για αυτό το ρόλο. Επιπλέον οι πελάτες πληρώνουν μόνο για την υπολογιστική ισχύ και τον αποθηκευτικό χώρο που χρησιμοποιούν και δεν διατηρούν ένα μεγάλο αριθμό servers για τις στιγμές που έχουν μεγάλο φόρτο. Και αν οι εφαρμογές έχουν γραφτεί σωστά, μπορούν να κλιμακωθούν ιδιαίτερα εύκολα και να εκμεταλλευτούν την τεράστια ισχύ που παρέχουν τα datacenters. Για να επιτευχθούν αυτά τα αποτελέσματα απαιτείται αποτελεσματική διαχείριση. Στην περίπτωση του Windows Azure κάθε εφαρμογή διαθέτει ένα αρχείο διαμόρφωσης. Αλλάζοντας αυτό το αρχείο είτε χειροκίνητα είτε προγραμματιστικά, ο developer μπορεί να ελέγξει διάφορα στοιχεία της συμπεριφοράς της εφαρμογές, όπως για παράδειγμα τον αριθμό των instances της εφαρμογής που τρέχουν. Το Windows Azure fabric στη συνέχεια παρακολουθεί την εφαρμογή και φροντίζει να διατηρήσει την επιθυμητή κατάσταση.

Για να μπορέσουν οι πελάτες να δημιουργήσουν, ρυθμίσουν αλλά και να παρακολουθούν τις εφαρμογές, το Windows Azure παρέχει ένα portal το οποίο είναι προσβάσιμο μέσω browser.

2.2.2 SQL Azure

Ένας από τους πιο ενδιαφέροντες τρόπους αξιοποίησης των servers που έχουμε πρόσβαση μέσω Internet είναι η διαχείριση δεδομένων. Ο στόχος του SQL Azure είναι να καλύψει αυτή την ανάγκη, προσφέροντας υπηρεσίες στο νέφος για την αποθήκευση πληροφοριών αλλά και για να μπορεί κάποιος να δουλέψει με αυτές τις πληροφορίες. Η Microsoft έχει ανακοινώσει ότι ο SQL Azure θα παρέχει τελικά ένα μεγάλο αριθμό χαρακτηριστικών σχετιζόμενων με τα δεδομένα, ανάμεσα στα άλλα συγχρονισμό δεδομένων, reporting, data analytics και άλλα. Το πρώτο όμως component που εμφανίστηκε είναι το SQL Azure Database.

Στην ουσία μιλάμε για ένα DBMS που έχει τη βάση του στο νέφος. Αυτή η τεχνολογία επιτρέπει τόσο στις on-premise όσο και στις εφαρμογές νέφους να αποθηκεύουν δεδομένα (relational αλλά και άλλων τύπων) στο datacenter της Microsoft. Όπως συμβαίνει και με άλλες τεχνολογίες νέφους, η επιχείρηση πληρώνει για ότι ακριβώς χρησιμοποιεί, ανεβάζοντας ή κατεβάζοντας τη χρήση και κατ' επέκταση το κόστος καθώς οι ανάγκες της επιχείρησης αλλάζουν.

Η χρήση μιας βάσης δεδομένων στο νέφος επιτρέπει τη μετατροπή του CAPEX (σκληροί δίσκοι και DBMS) σε OPEX. Επιπλέον θα πρέπει να σημειώσουμε ότι το SQL Azure στηρίζεται στον SQL Server. Η εταιρεία με στόχο να κάνει ακόμη πιο ενδιαφέρον το offering της προσφέρει ένα περιβάλλον SQL Server στο νέφος ολοκληρωμένο με δείκτες, stored procedures, views και άλλα. Η πρόσβαση σε αυτά τα δεδομένα μπορεί να γίνει με τη χρήση του ADO.NET είτε με άλλα interfaces πρόσβασης δεδομένων. Στην πραγματικότητα, εφαρμογές, οι οποίες σήμερα έχουν πρόσβαση σε ένα τοπικό SQL Server θα μπορούν να λειτουργήσουν με ελάχιστες αλλαγές στο SQL Azure Database. Οι πελάτες θα μπορούν να χρησιμοποιήσουν εφαρμογές που έχουν on premise όπως για παράδειγμα τις υπηρεσίες SQL Server Reporting για να δουλέψουν με δεδομένα που θα στηρίζονται στο νέφος. Τη στιγμή που οι εφαρμογές μπορούν να χρησιμοποιήσουν το SQL Azure Database με τον ίδιο τρόπο που χρησιμοποιούν ένα τοπικό DBMS, οι απαιτήσεις σε θέματα διαχείρισης μειώνονται σημαντικά. Επιπλέον υπάρχει το πλεονέκτημα ότι οι πελάτες πλέον δεν χρειάζεται να ασχολούνται με την παρακολούθηση της χρήσης του δίσκου ή τα log files, αλλά μπορούν να επικεντρωθούν σε αυτό όπου είναι πραγματικά χρήσιμο και είναι τα δεδομένα. Η Microsoft διαχειρίζεται όλες τις λειτουργικές λεπτομέρειες. Και όπως συμβαίνει με άλλα components της πλατφόρμας Azure, η διαχείριση είναι συγκεκριμένη μέσω της χρήσης ενός web portal.

2.2.3 Windows Azure AppFabric

Το τρέξιμο εφαρμογών και η αποθήκευση δεδομένων στο νέφος αποτελούν δυο από τα πιο σημαντικά στοιχεία του Υπολογιστικού Νέφους, αλλά σε καμιά περίπτωση δεν μπορούν να θεωρηθούν ότι αποτελούν το σύνολο του νέου μοντέλου. Για να δέσει καλύτερα το γλυκό, μπορεί να προστεθεί και η παροχή υπηρεσιών infrastructure, που θα βασίζονται στο νέφος. Αυτό το κενό έρχεται να καλύψει η πλατφόρμα Windows Azure AppFabric. Οι λειτουργίες που παρέχει το AppFabric δίνει απάντηση στις συνηθέστερες ανάγκες που υπάρχουν σε θέματα υποδομών για τη διασύνδεση distributed εφαρμογών. Τα components της πλατφόρμας AppFabric είναι τα ακόλουθα:

Service Bus: Η έκδοση των υπηρεσιών μιας εφαρμογής στο Internet είναι μια διαδικασία πιο δύσκολη από ότι φαίνεται. Ο στόχος του Service Bus είναι να κάνει αυτή τη διαδικασία πιο απλή, επιτρέποντας σε μια εφαρμογή να δώσει τα endpoints, στα οποία μπορούν να έχουν πρόσβαση άλλες εφαρμογές είτε είναι on premise είτε στο νέφος. Κάθε τέτοιο endpoint διαθέτει ένα UNI, το οποίο επιτρέπει στους clients να βρίσκουν και να χρησιμοποιούν την υπηρεσία. Το service bus αναλαμβάνει το

ρόλο του network address translation αλλά και της πρόσβασης μέσω firewall χωρίς το άνοιγμα νέων ports.

Access Control: Η εν λόγω υπηρεσία παρέχει ένα RESTful client για τη δική της πιστοποίηση αλλά και για να παρέχει τις απαραίτητες πληροφορίες ταυτότητας στον εκάστοτε server που θα το ζητήσει. Ο server μπορεί να χρησιμοποιήσει αυτές τις πληροφορίες για να αποφασίσει ποια εφαρμογή επιτρέπεται να έχει πρόσβαση και ποια όχι.

2.3 Το νέφος είναι και για τις μικρομεσαίες επιχειρήσεις

Οι μικρομεσαίες επιχειρήσεις έχουν σε αρκετές περιπτώσεις τη δυνατότητα να εμπλακούν εμμέσως με το Υπολογιστικό Νέφος λόγω της σχέσης τους με application service providers ή εταιρείες που παρέχουν hosted υπηρεσίες. Αλλά ποια είναι τα οφέλη για μια μικρομεσαία επιχείρηση να μπει στη διαδικασία μετάβασης κάποιων components στο νέφος; Ας δούμε τα πιο σημαντικά.

- Η πρόσβαση σε υπολογιστική ισχύ δεν σχετίζεται με συγκεκριμένη τοποθεσία, συσκευή ή κομμάτι hardware. Μέσω του Υπολογιστικού Νέφους, η τοποθεσία των υπολογιστικών resources αποκτά σχετική έννοια και δεν απαιτείται η ύπαρξη πολλών μηχανημάτων στο χώρο της εταιρείας. Το νέφος λειτουργεί σαν υπολογιστής της εταιρείας.
- Είναι πιο απλό: Δουλεύοντας στο νέφος είναι σαν να δουλεύουμε σε μια τεράστια πλατφόρμα, η οποία λειτουργεί συνεχώς. Μια εταιρεία μπορεί να αποθηκεύσει και να επεξεργαστεί τις πληροφορίες μέσω του Internet, κάτι που παρέχει στις επιχειρήσεις επιπρόσθετη ελευθερία καθώς αφήνει τη συντήρηση, την υποστήριξη και την επέκταση στους vendors της εφαρμογής που χρησιμοποιεί. Αυτός ο επιπλέον χρόνος μπορεί να χρησιμοποιηθεί για πιο στρατηγικές διαδικασίες. Η εργασία στο νέφος είναι πιο αποτελεσματική, εξοικονομεί χρόνο και χρήμα για τις μικρομεσαίες επιχειρήσεις, που παραδοσιακά δεν διαθέτουν πολλά IT resources.

Παρόλα αυτά, όπως είναι εύκολο να αντιληφθεί κανείς δεν είναι όλα ρόδινα και πρέπει να δοθεί σημασία σε κάποιες λεπτομέρειες, με σημαντικότερες τις ακόλουθες:

Συνδέσεις always on: Το Υπολογιστικό Νέφος παρέχει ταχύτητα ακόμα και σε περίπλοκες διαδικασίες, αλλά η αποτελεσματικότατα αυτή μπορεί να χαθεί χωρίς την ύπαρξη της κατάλληλης σύνδεσης. Η αξιοπιστία της σύνδεσης είναι κρίσιμη για την επιτυχία του business όταν χρησιμοποιούνται οι δυνατότητες του νέφους. Για την

καλύτερη διασφάλιση της σύνδεσης σίγουρα είναι προτιμητέο να χρησιμοποιηθούν πολλαπλές συνδέσεις Internet.

Ζητήματα ασφάλειας: Αν όλα γίνουν με το σωστό τρόπο, το Υπολογιστικό Νέφος δεν παρουσιάζει επιπλέον κινδύνους ασφάλειας συγκρινόμενο με το παραδοσιακό computing. Ακόμη και έτσι όμως τα ευαίσθητα δεδομένα θα πρέπει να κρυπτογραφούνται όταν αποθηκεύονται στο νέφος ενώ θα πρέπει να υπάρχει μέριμνα και για τα λειτουργικά συστήματα, τα οποία θα πρέπει να έχουν σχεδιαστεί γύρω από έναν ιδιαίτερα ασφαλή πυρήνα. Σαν βέλτιστη πρακτική θα πρέπει να προσέχουμε οποτεδήποτε δεδομένα περνούν μέσα από το δίκτυο να έχουν εφαρμοστεί όλες οι δικλείδες ασφαλείας.

Κατανόηση των hosted και managed υπηρεσιών: Οι μικρομεσαίες εταιρείες, που δεν διαθέτουν την κατάλληλη εμπειρία για να εγκαταστήσουν εσωτερικά το απαραίτητο hardware και να το συντηρήσουν, αλλά αυτό δεν πρέπει να αποτελεί εμπόδιο. Οι εταιρείες παροχής hosted και managed υπηρεσιών αποτελούν μια βιώσιμη, ανταγωνιστική και κλιμακούμενη εναλλακτική για επιχειρήσεις όλων των μεγεθών, που καθίσταται ιδιαίτερα ελκυστική για τις μικρές επιχειρήσεις με περιορισμένες οικονομικές δυνατότητες. Παρόλα αυτά, η εργασία με αυτούς τους παρόχους υπηρεσιών απαιτεί μια κατανόηση των τεχνολογιών και των συστημάτων που παρέχουν, οπότε ένα υπόβαθρο σε θέματα IT είναι απαραίτητο.

2.4 Η ελληνική επιχείρηση στο νέφος

Θα ξεκινήσουμε με μία αντίφαση. Η ανεξάρτητη εταιρεία συμβούλων McKinsey εκτιμά ότι οι δαπάνες για εξοπλισμό και υπηρεσίες που σχετίζονται με την αποθήκευση και το datacenter υπερβαίνουν σήμερα τα 350 δις δολάρια ετησίως σε παγκόσμιο επίπεδο, ενώ περίπου το 20% αυτής της αγοράς θα αφορά στο virtualization και το private νέφος τα επόμενα χρόνια - μέχρι το 2015. Δυστυχώς όμως, τουλάχιστον το 70% του προϋπολογισμού χρησιμοποιείται για τη συντήρηση της υπάρχουσας υποδομής, αφήνοντας λιγότερο από 30% για νέες επενδύσεις.

Την ίδια στιγμή, σύμφωνα με πρόσφατη έρευνα της Forrester, το 86% των ερωτηθεισών επιχειρήσεων δεν έχει κανένα πλάνο για hosted λύση αποθήκευσης δεδομένων, ενώ μόλις ένα 10% έχει ήδη μια τέτοια λύση ή εξετάζει σοβαρά το ενδεχόμενο να αποκτήσει μία στο μέλλον. Τα αποτελέσματα αυτά δεν είναι εντελώς αντιφατικά. Το γεγονός ότι μόλις 30% του προϋπολογισμού μπορεί να διατεθεί σε νέες επενδύσεις στο IT, αίρει από μόνο του ένα σημαντικό ζήτημα: Μήπως θα μπορούσε η επιχείρηση να εξετάσει την εναλλακτική του storage στο νέφος;

Η αλήθεια είναι πως η λύση του storage στο νέφος έχει αρκετά πλεονεκτήματα, τα οποία μάλιστα είναι εύκολο να γίνουν αντιληπτά από τους ανθρώπους που

παίρνουν τις τελικές αποφάσεις, ακόμα και αν δεν έχουν καθόλου τεχνικές γνώσεις (όπως άλλωστε συμβαίνει στις περισσότερες μικρές επιχειρήσεις).

Το πρώτο επιχείρημα είναι η Ασφάλεια. Αν έχει γίνει σωστή επιλογή Παρόχου, τότε ο πελάτης δεν χρειάζεται να ανησυχεί καθόλου για την ασφάλεια των δεδομένων του. Αντίθετα, θα κερδίσει μερικά επιπλέον επίπεδα ασφάλειας, που σχετίζονται με φυσικές καταστροφές, δολιοφθορές, ζημιές και άλλα απρόοπτα μέσα στον φυσικό χώρο της επιχείρησης.

Το δεύτερο επιχείρημα είναι το χαμηλό Κόστος Κτήσης (TCO). Στη λύση του storage στο νέφος, δεν υπάρχουν έξοδα που σχετίζονται με τη συντήρηση και την αναβάθμιση του εξοπλισμού, ενώ τα κόστη διαχείρισης μειώνονται σημαντικά – και άμεσα. Αυτό συνεπάγεται λιγότερο χρόνο απασχόλησης σε χρονοβόρες διαχειριστικές ενέργειες για τους ανθρώπους του IT, άρα περισσότερο χρόνο για να διαθέσουν σε πιο ουσιαστικά θέματα.

Το τρίτο επιχείρημα είναι η ανεξάντλητη Χωρητικότητα. Στο storage στο νέφος δεν υπάρχουν περιορισμοί στον διαθέσιμο χώρο. Η υπάρχουσα λύση μπορεί να επεκταθεί όσο χρειάζεται η επιχείρηση, χωρίς επιπλοκές ούτε δυσλειτουργίες, αλλά και χωρίς να δαπανηθεί πολύτιμος χρόνος σε έρευνα αγοράς, αναζήτηση προμηθευτή, σχεδιασμό της κατάλληλης λύσης, εγκατάσταση και παραμετροποίηση, τεχνική υποστήριξη κ.λπ.

Μία αντίρρηση από τη μεριά του πελάτη ενδέχεται να αφορά στη διατήρηση του ελέγχου πάνω στον εξοπλισμό και τα δεδομένα. Αυτή η αντίρρηση μπορεί να αντιμετωπιστεί με το επιχείρημα της δοκιμής. Η λύση του storage στο νέφος έχει το πλεονέκτημα της «μη-αγοράς». Η επιχείρηση μπορεί να δοκιμάσει τη λύση για κάποιο χρονικό διάστημα και, αν θεωρεί ότι δεν ταιριάζει στη φιλοσοφία ή τις ανάγκες της, να προβεί κατόπιν στην αγορά εξοπλισμού.

Το μεγαλύτερο επιχείρημα βέβαια έχει να κάνει με την ίδια την επιχείρηση και τους διαθέσιμους πόρους της. Οι εταιρείες που έχουν χαμηλά κεφάλαια να διαθέσουν στην πληροφορική υποδομή τους, αλλά και έλλειψη εξειδικευμένων ανθρώπων που θα την υποστηρίζουν, είναι εκείνες που θα δουν τα μεγαλύτερα οφέλη από το storage στο νέφος. Οποιαδήποτε Μικρή Επιχείρηση, που ενδεχομένως δεν έχει απεριόριστους πόρους, αλλά αντιλαμβάνεται τη σημασία της ασφαλούς αποθήκευσης της πληροφορίας, μπορεί να επωφεληθεί από τις λύσεις storage στο νέφος.

Στην Ελλάδα αυτή η αγορά μόλις ξεκινά να κινείται, με πολλή δυναμική και μεγάλες προοπτικές. Θα μπορούσαμε να πούμε, με σχετική ασφάλεια, ότι θα αναπτυχθεί μάλλον γρήγορα. Όχι τόσο βασιζόμενοι στις προβλέψεις των σχετικών ερευνών, αλλά βασιζόμενοι περισσότερο στην ψυχολογία της ελληνικής αγοράς - και στην επιτακτική ανάγκη των επιχειρήσεων, ειδικά αυτήν τη δύσκολη χρονική περίοδο, να λαμβάνουν καλές υπηρεσίες με τη μικρότερη δυνατή επένδυση κεφαλαίου.

ΚΕΦΑΛΑΙΟ 3 : ΑΣΦΑΛΕΙΑ ΣΤΟ ΥΠΟΛΟΓΙΣΤΙΚΟ ΝΕΦΟΣ

3.1 Ασφάλεια : το αμφιλεγόμενο ζήτημα στο Υπολογιστικό Νέφος

Το Υπολογιστικό Νέφος είναι το θέμα που το τελευταίο διάστημα σχεδόν μονοπωλεί κάθε συζήτηση των επαγγελματιών του IT. Προσφέρει τη δυνατότητα στις επιχειρήσεις να αποσυνδέσουν τις ανάγκες τους σε υποδομές πληροφορικής, από την υλοποίηση και συντήρηση των υποδομών αυτών. Επιπροσθέτως, παρέχει τους αναγκαίους πόρους με τη μορφή υπηρεσίας και ο πελάτης/ επιχείρηση κάνει χρήση των παροχών αυτών βάσει των αναγκών του. Ο πελάτης δε χρειάζεται να επενδύσει σε υποδομές αλλά ούτε και να επωμιστεί το κόστος συντήρησής τους. Αντιθέτως, συνδέεται στην υποδομή του παρόχου και κάνει χρήση υπηρεσιών, εφαρμογών και αρχιτεκτονικών χωρίς να χρειάζεται να ανησυχεί για το που και πως οι υποδομές αυτές υπάρχουν.

Ένας διαφορετικός τρόπος περιγραφής των υποδομών και των υπηρεσιών Υπολογιστικού Νέφους είναι ο παραλληλισμός τους με μια δημόσια παρεχόμενη υπηρεσία. Ακριβώς όπως οι επιχειρήσεις πληρώνουν για την ηλεκτρική ενέργεια, το φυσικό αέριο και το νερό που χρησιμοποιούν, τους δίνεται πλέον η δυνατότητα να πληρώνουν για υπηρεσίες πληροφορικής με βάση τη χρήση που κάνουν.

Για παράδειγμα, το Υπολογιστικό Νέφος συγκρίνεται συχνά με την εξάπλωση του ηλεκτρισμού. Τα νοικοκυριά, οι επιχειρήσεις και οι πόλεις δεν ήθελαν να παράγουν ή να βασίζονται στις δικές τους πηγές ενέργειας. Ξεκίνησαν λοιπόν να συνδέονται με μεγαλύτερα δίκτυα ηλεκτρικής ενέργειας, τα οποία υποστηρίζονταν και ελέγχονταν από τις δημόσιες (ή μη) εταιρείες ηλεκτρικής ενέργειας, επιτυγχάνοντας με αυτό τον τρόπο εξοικονόμηση χρόνου και κόστους, καθώς και μεγαλύτερη πρόσβαση αλλά και περισσότερο αξιόπιστη διαθεσιμότητα ηλεκτρικής ενέργειας.

Το Υπολογιστικό Νέφος αντιπροσωπεύει μία σημαντική ευκαιρία τόσο για τους παρόχους υπηρεσιών, όσο και για τις εταιρείες. Με το να βασιστούν στο Υπολογιστικό Νέφος, οι εταιρείες μπορούν να επιτύχουν μειώσεις κόστους, ευελιξία και περισσότερες επιλογές όσον αφορά στους υπολογιστικούς πόρους.
Η τάση παρουσιάζεται ολοένα αυξανόμενη: οι οργανισμοί στρέφονται στο Υπολογιστικό Νέφος για να βελτιώσουν τη λειτουργική τους αποδοτικότητα και να ενισχύσουν την κερδοφορία τους.

Οι προοπτικές για τη βελτίωση της αποδοτικότητας και ευελιξίας καθώς και την εξοικονόμηση κόστους που ανοίγονται με την υιοθέτηση της τεχνολογίας

Υπολογιστικού Νέφους σε επιχειρήσεις και οργανισμούς είναι πολλές και σημαντικές. Τι γίνεται όμως με το θέμα της ασφάλειας; Συνήθως, πολύ νωρίς σε κάθε συζήτηση σχετικά με τα προβεβλημένα μοντέλα νέφους, το ενδιαφέρον στρέφεται στο ζήτημα της ασφάλειας. Από εδώ λοιπόν ξεκινούν και τα ερωτηματικά αλλά και η εισαγωγή των κινδύνων ασφαλείας πληροφοριών που αφορούν στις υπηρεσίες μέσω των υποδομών Υπολογιστικού Νέφους.

Οι απόψεις γύρω από το θέμα είναι αρκετές και πολλές είναι και αντιφατικές μεταξύ τους- όπως άλλωστε και σε κάθε τεχνολογία- αλλά τελικά αυτό που μετράει είναι από ποια πλευρά βλέπουμε τα πράγματα. Ο Prof. Whitfield Diffie του Royal Holloway University of London και πρωτοπόρος σε θέματα κρυπτογραφίας, δίνει ένα πολύ εύστοχο παράδειγμα, λέγοντας: «Όλοι κατά γενική ομολογία εμπιστευόμαστε το Gmail ή την τηλεφωνική μας εταιρεία για να στείλουμε εμπιστευτικές πληροφορίες. Θεωρούμε πως υπάρχει η απαραίτητη ασφάλεια για να μεταδώσουμε μια εμπιστευτική πληροφορία τηλεφωνικά και εμπιστευόμαστε τον πάροχό μας. Υπάρχει όμως και μία μερίδα ανθρώπων που δε μιλάνε στο τηλέφωνο αν δεν πάρουν περισσότερα μέτρα ασφαλείας, πέρα από αυτά που παρέχονται από τις εταιρείες τηλεφωνίας ».

Σύμφωνα τον Milind Goverak, αναλυτή της Gartner, το Υπολογιστικό Νέφος εκτοξεύτηκε το 2010 στη δεύτερη θέση της λίστας του ετήσιου CIO survey της Gartner για τις κυρίαρχες τεχνολογικές επενδύσεις, από τη 16η θέση που ήταν το 2009. «Και όπως οτιδήποτε καινούργιο, η βασικότερη ανησυχία είναι η ασφάλεια», υποστηρίζει ο ίδιος. Στην πραγματικότητα, η μεγάλη πλειοψηφία των εταιρειών που εξετάζουν λύσεις Υπολογιστικού Νέφους, όπως λέει, θα προτιμούσαν να δημιουργήσουν ένα virtualized data center σε δικό τους premise -αυτό που κάποιοι ονομάζουν private νέφος-, καθώς δεν νιώθουν άνετα με τα ζητήματα ασφάλειας που προκύπτουν από το Υπολογιστικό Νέφος αλλά και την ικανότητα του κλάδου να τα αντιμετωπίσει.

«Είμαστε στα αρχικά στάδια ενός συναρπαστικού ταξιδιού σε ένα καινούργιο πληροφορικό μοντέλο, που παρά τα διαδεδομένα πλεονεκτήματά του, από την άποψη της ασφάλειας και των κινδύνων, είναι δύσκολο να το διαχειριστούμε», επισημαίνει ο Jay Heiser, επίσης αναλυτής της Gartner. «Τα στοιχεία αυτά που καθιστούν εύκολο και ελκυστικό το Υπολογιστικό Νέφος -όπως η άμεση plug-and-play παραγωγικότητα- είναι ταυτόχρονα τα στοιχεία που καθιστούν δύσκολη, αν όχι αδύνατη, την αποτίμηση των συσχετιζόμενων κινδύνων. Οι υπάρχουσες πιστοποιήσεις, όπως το SAS 70 και το ISO 27001 και 27002, δεν επαρκούν», υποστηρίζει ο Heiser, «δημιουργώντας απογοήτευση τόσο σε παρόχους όσο και στις εταιρείες».

Για αυτό το λόγο, η διασφάλιση των περιβαλλόντων Υπολογιστικού Νέφους θα αποτελέσει τη βασική εστίαση των επενδύσεων των παρόχων τα επόμενα χρόνια, λέει ο Jonathan Penn, αναλυτής της Forrester Research. Βραχυπρόθεσμα, οι χρήστες θα κληθούν να «κάνουν όλη τη δουλειά, αλλά μακροπρόθεσμα οι πάροχοι υπηρεσιών

νέφους θα αξιοποιήσουν την ευκαιρία να διαφοροποιηθούν από τον ανταγωνισμό ενσωματώνοντας οι ίδιοι την ασφάλεια».

Από την άλλη, οι πάροχοι τεχνολογιών και υπηρεσιών ασφάλειας που είχαν συνηθίσει να πωλούν απευθείας στις εταιρείες θα ανακαλύψουν ότι χρειάζονται τους παρόχους νέφους ως το μέσο για να φτάσουν στην αγορά, λέει ο Penn, και καθώς η αγορά θα ωριμάζει, οι εταιρείες θα αξιώνουν αυτά τα πράγματα ενσωματωμένα στην υπηρεσία που αγοράζουν. «Αυτό θα αποτελέσει μία μάλλον δραστική αλλαγή και αναταραχή», προσθέτει.

3.2 Οι κυριότερες απειλές για την τεχνολογία Υπολογιστικού Νέφους

Στη συνέχεια λοιπόν θα εστιάσουμε αναλυτικότερα στις ανησυχίες και στους κινδύνους που συνοδεύουν την τεχνολογία και τις υπηρεσίες Υπολογιστικού Νέφους, θα παρουσιάσουμε τα πλεονεκτήματα που προκύπτουν και θα δούμε τι ρίσκα παίρνουμε υιοθετώντας αυτή την τεχνολογία. Τέλος, θα κάνουμε μια αναφορά σε γεγονότα τα οποία έχουν λάβει χώρα, ώστε να κατανοήσουμε την αιτία κάποιων προβλημάτων ασφαλείας.

3.2.1 Ανησυχίες και προβληματισμοί

Όπως σε κάθε νέα τεχνολογική τάση, έτσι και στην περίπτωση του Υπολογιστικού Νέφους, οι επιχειρήσεις που σκοπεύουν να υιοθετήσουν τέτοιου είδους υπηρεσίες χρειάζεται να ενισχύσουν και να προσαρμόσουν ανάλογα τις διαδικασίες που αφορούν στην ασφάλεια των πληροφοριών τους, προκειμένου να

ανταποκριθούν στις νέες ανάγκες. Χρειάζεται δηλαδή οι διαδικασίες ασφάλειας πληροφοριών να αναφέρονται και να λαμβάνουν υπόψη τους τη χρήση της υποδομής Υπολογιστικού Νέφους και όχι να αναφέρονται σε γενικούς κανόνες.

Δεδομένου του δυναμικού επιχειρηματικού περιβάλλοντος που διαμορφώνεται, ολοένα και περισσότερες εταιρείες θα κάνουν χρήση υπηρεσιών μέσω του Υπολογιστικού Νέφους, προκειμένου να αναθέσουν σε τρίτους Οργανισμούς μέρος των λειτουργικών τους δραστηριοτήτων. Η διαμόρφωση μιας τέτοιας σχέσης με τον εκάστοτε πάροχο των υπηρεσιών Υπολογιστικού Νέφους δεν αφορά μόνο στη χρήση των υπηρεσιών και της τεχνολογικής υποδομής. Έχει σχέση και επηρεάζεται από το επιχειρηματικό μοντέλο λειτουργίας του παρόχου, από την οργάνωσή του και από την κουλτούρα του. Πράγματα δηλαδή, τα οποία επηρεάζουν άμεσα την ασφάλεια των δεδομένων της επιχείρησης που αποφασίζει να εναποθέσει τη διαχείρισή τους σε υποδομή την οποία διαχειρίζεται ο πάροχος.

Πολλοί από τους κινδύνους που αφορούν στο Υπολογιστικό Νέφος δεν είναι καινούριοι και τους συναντάμε σήμερα στην καθημερινή λειτουργία των επιχειρήσεων. Ως εκ τούτου, η εξασφάλιση της διαθεσιμότητας και της προστασίας των επιχειρησιακών πληροφοριών απαιτούν καλά προγραμματισμένες δραστηριότητες διαχείρισης κινδύνων.

Οι ανησυχίες για την ασφάλεια υψώνουν ένα σημαντικό εμπόδιο. Σε μια εποχή που οι συνέπειες και τα πιθανά κόστη από λάθη αυξάνονται με γεωμετρική πρόοδο για τις εταιρείες που διαχειρίζονται εμπιστευτικά και ιδιωτικά δεδομένα, οι εταιρείες και ειδικά τα τμήματα Πληροφορικής πρέπει να αναπτύξουν καλύτερους τρόπους για την αξιολόγηση των πρακτικών ασφάλειας και μυστικότητας στις υπηρεσίες Υπολογιστικού Νέφους. Σε αντιδιαστολή με το παραδοσιακό outsourcing, που εξακολουθεί να βασίζεται κυρίως σε αυτόνομο computing, το νέφος διαχωρίζει τα δεδομένα από την υποδομή και «κρύβει» χαμηλού επιπέδου λειτουργικές λεπτομέρειες, όπως το πού βρίσκονται τα δεδομένα σας και πώς γίνονται replicated.

Το multitenancy, παρόλο που σπανίως χρησιμοποιείται στο παραδοσιακό IT outsourcing, είναι σχεδόν δεδομένο στις υπηρεσίες Υπολογιστικού Νέφους. Αυτές οι διαφορές δίνουν ώθηση σε μία σειρά μοναδικών θεμάτων ασφάλειας και ιδιωτικότητας που επηρεάζουν τις πρακτικές διαχείρισης κινδύνου της εταιρείας, αλλά επίσης προκαλούν μία καινούργια θεώρηση νομικών ζητημάτων σε περιοχές όπως η συμμόρφωση, το auditing κ.ά.

Μέσα από μία σειρά συνεντεύξεων και συζητήσεων τόσο με παρόχους όσο και με χρήστες Πληροφορικής σχετικά με τα ζητήματα ασφάλειας γύρω από τις υπηρεσίες Υπολογιστικού Νέφους, οι ειδικοί κατέληξαν σε τρεις βασικές περιοχές τις οποίες πρέπει να λάβουν υπόψη τους οι εταιρείες:

1. Ασφάλεια και μυστικότητα (privacy). Ανησυχίες όπως η προστασία των δεδομένων, η λειτουργική ακεραιότητα, η διαχείριση τρωτότητας, το business

continuity (BC), το disaster recovery (DR) και το identity management (IAM) είναι τα πρώτα στη λίστα των ζητημάτων ασφάλειας του Υπολογιστικού Νέφους. Η μυστικότητα είναι άλλη μία βασική ανησυχία - τα δεδομένα που μια υπηρεσία συγκεντρώνει σχετικά με το χρήστη δίνουν στον πάροχο σημαντικές πληροφορίες marketing, ενώ μπορεί επίσης να οδηγήσει και σε κακή χρήση ή παραβίαση της ιδιωτικότητας. Ένας τρόπος που οι εταιρείες μπορούν να αξιολογήσουν τις πρακτικές ασφάλειας και μυστικότητας του παρόχου νέφους υπηρεσιών είναι μέσω του auditing, το οποίο μπορεί να βοηθήσει στην απόκτηση κάποιας ορατότητας στις εσωτερικές λειτουργίες του παρόχου.

Ωστόσο, το auditing αντιτάσσεται στο βασικό χαρακτηριστικό του Υπολογιστικού Νέφους, που είναι η παράβλεψη των λειτουργικών λεπτομερειών και η παροχή εύκολων στη χρήση interfaces και APIs. Ένας πάροχος υπηρεσιών νέφους μπορεί να μην επιτρέψει εσωτερικούς ελέγχους (internal audits), αλλά θα πρέπει να προσφέρει provisions για κάποια μορφή εξωτερικών ελέγχων για την υποδομή τους και το δίκτυό τους.

2. Συμμόρφωση. Οι εταιρείες που πρέπει να ανταποκριθούν σε απαιτήσεις συμμόρφωσης θα πρέπει να κατανοήσουν πού και πώς η χρήση υπηρεσιών Υπολογιστικού Νέφους μπορεί να επηρεάσει τους στόχους συμμόρφωσής τους. Η μυστικότητα των δεδομένων και η επιχειρησιακή συνέχεια είναι δύο μεγάλα κομμάτια της συμμόρφωσης. Ένας μεγάλος αριθμός νόμων και κανονιστικών πλαισίων εγείρουν συγκεκριμένες απαιτήσεις ως προς τη διαχείριση δεδομένων και τον σχεδιασμό business continuity.

Για παράδειγμα, ρυθμιστικά πλαίσια της Ευρωπαϊκής Ενωσης (και της Ιαπωνίας) ορίζουν ότι η αποθήκευση και διαχείριση προσωπικών δεδομένων -το email είναι μια μορφή προσωπικών δεδομένων αναγνωρισμένη από την ΕΕ- πρέπει να γίνεται σε data centers που βρίσκονται στην Ευρωπαϊκή Ένωση (ή στην Ιαπωνία, αντίστοιχα).

3. Νομικά και συμβατικά ζητήματα. Η ευθύνη και η πνευματική ιδιοκτησία είναι δύο μόνο από τα νομικά ζητήματα που πρέπει να λάβει υπόψη μια εταιρεία. Η ευθύνη δεν είναι πάντα ξεκάθαρη όταν πρόκειται για υπηρεσίες νέφους. Το ίδιο ισχύει και για την πνευματική ιδιοκτησία. Για κάποιες υπηρεσίες, το ζήτημα της πνευματικής ιδιοκτησίας είναι ξεκάθαρο - ο πάροχος υπηρεσιών νέφους είναι ο ιδιοκτήτης της υποδομής και των εφαρμογών, ενώ η εταιρεία-χρήστης είναι ιδιοκτήτης των δεδομένων και των υπολογιστικών αποτελεσμάτων.

Σε άλλες περιπτώσεις, όμως, ο διαχωρισμός δεν είναι τόσο ξεκάθαρος. Μερικές φορές, όπως για παράδειγμα στο software components-as-a-service, είναι δύσκολο να περιγραφεί ποιος κατέχει τι και ποια δικαιώματα έχει ο πελάτης πάνω στον πάροχο. Είναι λοιπόν απαραίτητο να ρυθμιστεί η ευθύνη και τα ζητήματα πνευματικής ιδιοκτησίας πριν ξεκινήσει η υπηρεσία. Άλλα συμβατικά ζητήματα περιλαμβάνουν την end-of-service υποστήριξη - όταν τελειώσει η σχέση παρόχου-πελάτη, τα δεδομένα του πελάτη και οι εφαρμογές πρέπει να «πακεταριστούν» και να

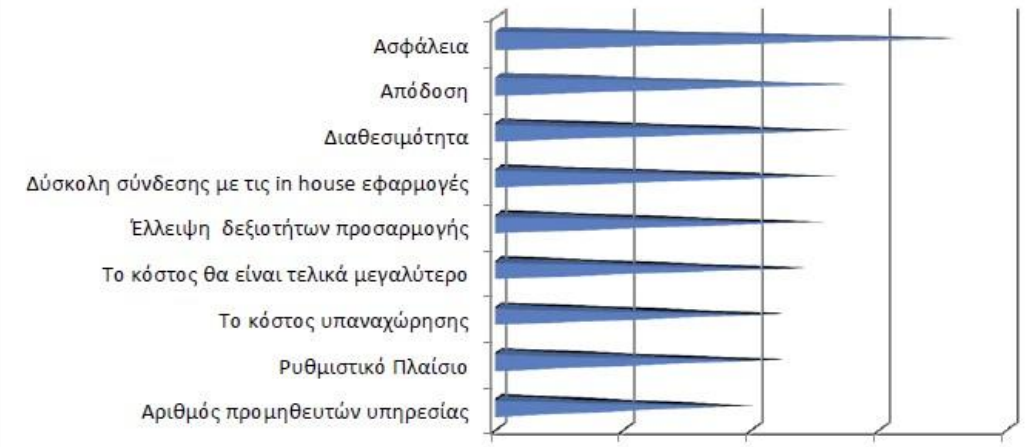
παραδοθούν στον πελάτη, και όποια εναπομείναντα αντίγραφα των δεδομένων του πελάτη πρέπει να διαγραφούν από τις υποδομές του παρόχου.

Ταυτόχρονα, οργανισμοί όπως το Cloud Security Alliance (CSA) εργάζονται προκειμένου να θέσουν ένα πλαίσιο γύρω από τα ζητήματα ασφάλειας και τους τρόπους για την αντιμετώπισή τους. Μέσα στο 2010, το CSA κυκλοφόρησε μία περίληψη των στρατηγικών και τακτικών σημείων αυτών ασφάλειας, καθώς και συστάσεις για την αντιμετώπισή τους. Ο οργανισμός χώρισε τις περιοχές αυτές σε δύο ευρείες κατηγορίες: διακυβέρνηση (governance) και λειτουργίες (operations).

Οι περιοχές που τοποθετούνται κάτω από την κατηγορία διακυβέρνηση περιλαμβάνουν:
• Διακυβέρνηση και ERM
• Συμμόρφωση και έλεγχοι
• Νομικό και ηλεκτρονικό discovery
• Information lifecycle management
• Μεταφερσιμότητα και διαλειτουργικότητα.

Οι περιοχές που τοποθετούνται κάτω από την κατηγορία operations περιλαμβάνουν:
• Παραδοσιακή ασφάλεια, business continuity και disaster recovery
• Data center operations
• Ασφάλεια εφαρμογών
• Incident response, notification & remediation
• Κρυπτογράφηση και key management
• Identity & access management
• Virtualization.

Σε έρευνα που διεξήγαγε η IDC, με δείγμα 244 στελέχη IT αναφορικά με τις υπηρεσίες Νέφους, σημαντικότερα θέματα για προβληματισμό για τις IT εταιρείες:



Ειδικότερα είναι απαραίτητο, να εξασφαλίσουμε ότι ο πάροχός μας, θα προσφέρει όλα τα απαραίτητα εχέγγυα και θα εφαρμόζει εκείνες τις πολιτικές ασφαλείας που θα διασφαλίζουν τα δεδομένα έτσι ώστε να παραμείνουν συμβατά με τις εφτά βασικές ιδιότητες που πρέπει να έχουν οι πληροφορίες για να είναι ασφαλείς:

1. Ακεραιότητα (Information Integrity)
2. Ιδιωτικότητα (Privacy)
3. Εμπιστευτικότητα(Confidentiality)
4. Διαθεσιμότητα (Availability)
5. Γνησιότητα (Authenticity)
6. Χρησιμότητα (Utility)
7. Έλεγχος και κατοχή της πληροφορίας (Possession or Control)

3.3 Προσωπικά δεδομένα και ιδιωτικότητα στο Υπολογιστικό Νέφος

Πολλοί χρήστες συχνά θεωρούν ότι η διασφάλιση της ιδιωτικότητας είναι υποσύνολο των υπηρεσιών ασφαλείας πληροφοριακών συστημάτων. Η παραπάνω θεώρηση δεν είναι απολύτως ακριβής, διότι ενώ οι δυο έννοιες (ιδιωτικότητα και ασφάλεια της πληροφορίας) είναι στενά συνδεδεμένες, η ιδιωτικότητα αποτελεί ένα ξεχωριστό τομέα που χρήζει ιδιαίτερης μεταχείρισης. Στο κεφάλαιο αυτό θα εξετάσουμε την έννοια της ιδιωτικότητας, μέσα στο περιβάλλον που διαμορφώνεται από τις τεχνολογίες Υπολογιστικού Νέφους.

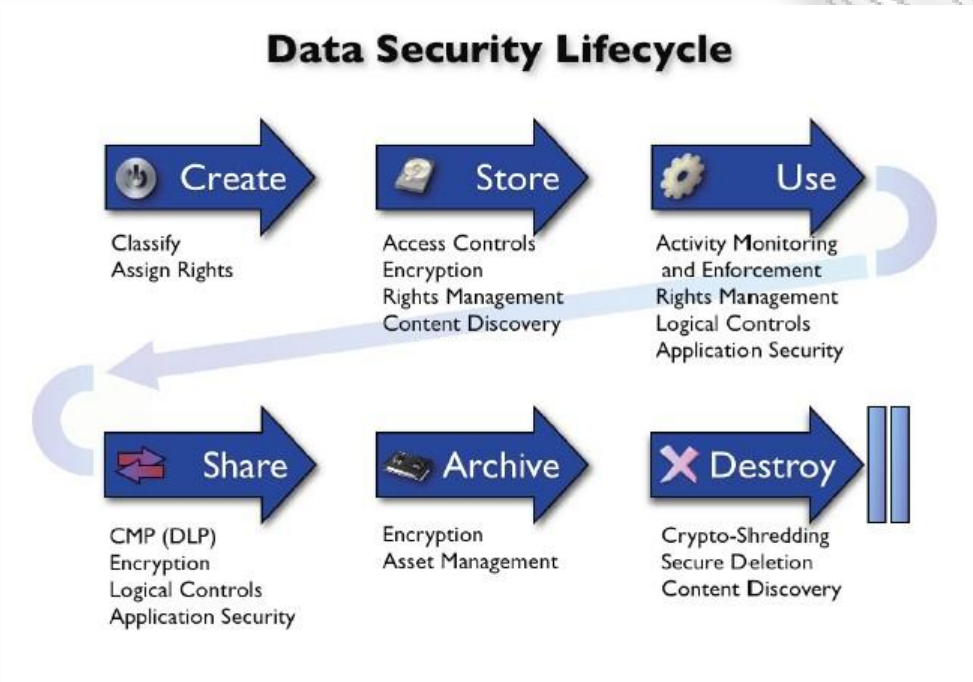
3.3.1 Προστασία της ιδιωτικότητας

Η προστασία των προσωπικών δεδομένων αναφέρεται στα δικαιώματα ή στις υποχρεώσεις που σχετίζονται με τη συλλογή, την επεξεργασία, την κοινοποίηση, την αποθήκευση και την καταστροφή των προσωπικών δεδομένων. Ουσιαστικά, όταν μιλάμε για την διασφάλιση του απορρήτου των επικοινωνιών και την προστασία προσωπικών δεδομένων στο νέφος εννοούμε την υπευθυνότητα των παρόχων απέναντι στους αρχικούς ιδιοκτήτες των δεδομένων που συνήθως είναι και οι τελικοί χρήστες, καθώς και το βαθμό διαφάνειας που χαρακτηρίζει την πολιτική των παρόχων αυτών σε σχέση με τη διαχείριση των δεδομένων.

Τα παραπάνω συμπυκνώνονται στον ορισμό που έχει δοθεί από το American Institute of Certified Public Accountants (AICPA) και το Canadian Institute of Charted Accountants (CICA) κάτω από το πρότυπο Generally Accepted Privacy Principles (GAPP) και αναφέρει ως προστασία δεδομένων προσωπικού χαρακτήρα: «τα δικαιώματα και υποχρεώσεις φυσικών προσώπων και οργανισμών σε σχέση με τη συλλογή, χρήση, κατακράτηση και δημοσιοποίηση των προσωπικών πληροφοριών».

3.3.2 Ο Κύκλος Ζωής των Δεδομένων

Για να κατανοήσουμε καλυτέρα τις απαιτούμενες πολιτικές είναι χρήσιμο να κάνουμε μια γρήγορη ανασκόπηση του κύκλου ζωής των δεδομένων. Ο κύκλος ζωής των δεδομένων αναφέρεται στην διαδρομή που ακολουθεί η πληροφορία από τη στιγμή που γίνεται αρχικά διαθέσιμη έως την τελική της καταστροφή.



Ειδικά χαρακτηρίστηκα του Data Security Lifecycle

Φάση 1 : Δημιουργία της πληροφορίας

• Ιδιοκτησία: ποιος από τον οργανισμό είναι ο κάτοχος των προσωπικών δεδομένων και πώς η ιδιοκτησία διατηρείται εάν ο οργανισμός χρησιμοποιεί τεχνολογίες Υπολογιστικού Νέφους.

• Ταξινόμηση: πώς και πότε ένα προσωπικό δεδομένο ταξινομείται; Υπάρχουν περιορισμοί σχετικά με τη χρήση και επεξεργασία συγκεκριμένων κατηγοριών δεδομένων σε περιβάλλον Νέφους;

• Διακυβέρνηση: υπάρχει μια δομή στην εταιρική διακυβέρνηση που να διασφαλίζει τη διαχείριση και προστασία των προσωπικών δεδομένων σύμφωνα με τις πρότυπες πολιτικές του οργανισμού; Και αν ναι, η δομή αυτή μπορεί να εξασφαλίσει τη ροή ελέγχου για τα δεδομένα που μεταναστεύουν στο νέφος;

Φάση 2 : Αποθήκευση

• Έλεγχος πρόσβασης: Υπάρχουν δομές έλεγχου πρόσβασης για τα δεδομένα προσωπικού χαρακτήρα, που να διασφαλίζουν ότι όταν πλέον αυτά αποθηκεύονται

στο νέφος, μόνο τα άτομα έχουν δικαιοδοσία και μόνο αυτά, θα μπορούν να έχουν πρόσβαση σε αυτά

• Δομημένη έναντι αδόμητης: Με ποια μεθοδολογία αποθηκεύονται τα δεδομένα και πως μπορεί ο οργανισμός να έχει μελλοντικά πρόσβαση και να τα διαχειριστεί;

• Ακεραιότητα/διαθεσιμότητα/εμπιστευτικότητα: Με ποιούς μηχανισμούς εξασφαλίζεται η ακεραιότητα των δεδομένων, με ποιους η διαθεσιμότητά τους και πώς επιτυγχάνεται η διατήρηση της εμπιστευτικότητά τους όταν αυτά αποθηκεύονται σε περιβάλλον νέφους;

• Κρυπτογράφηση: πολλές νομοθετικές και κανονιστικές διατάξεις σε διάφορες χώρες προβλέπουν ότι ορισμένοι τύποι προσωπικών δεδομένων πρέπει να αποθηκεύονται σε κρυπτογραφημένη μορφή. Δημιουργείται λοιπόν το ερώτημα, αν και σε ποιο βαθμό, ο πάροχος των υπηρεσιών Νέφους είναι σε θέση να προσφέρει υπηρεσίες σύμφωνα με τις παραπάνω νομικές απαιτήσεις.

Φάση 3 : Χρήση

• Εσωτερική και εξωτερική χρήση: Τα προσωπικά δεδομένα χρησιμοποιούνται μόνο στο πλαίσιο του φορέα που αρχικά τα συλλέγει ή χρησιμοποιούνται και εκτός του οργανισμού (π.χ. υπηρεσίες ΤΕΙΡΕΣΙΑΣ Α.Ε);

• Τρίτα μέρη: είναι οι πληροφορίες που οργανισμός «μοιράζεται» από κοινού με τρίτους (π.χ. τους υπεργολάβους ενός προγράμματος πληροφορικής);

• Καταλληλότητα: η χρήση των πληροφοριών συνάδει με τον σκοπό για τον οποίο έχουν συλλεχθεί; Είναι ορθή η χρήση των δεδομένων όταν αυτά βρίσκονται σε περιβάλλον Νέφους και είναι σύμφωνη με τις νομικές (κατ ελάχιστον) δεσμεύσεις που έχει αναλάβει ο οργανισμός απέναντι στα υποκείμενα των δεδομένων;

• Αποκάλυψη/Συμμόρφωση : Γίνεται η διαχείριση των πληροφοριών που βρίσκονται στο νέφος με τέτοιο τρόπο ώστε να είναι εφικτή η συμμόρφωση του οργανισμού σε νομικές απαιτήσεις σε περίπτωση δικαστικής διερεύνησης ή προστατευτικών μέτρων ;

Φάση 4 : Μεταφορά

• Δημόσια ή Ιδιωτικά δίκτυα: όταν οι πληροφορίες μεταφέρονται σε ένα περιβάλλον νέφους και αυτό είναι δημόσιο, προστατεύονται καταλλήλως;

• Απαιτήσεις κρυπτογράφησης: Τα προσωπικά δεδομένα κρυπτογραφούνται; Τι ισχύει αναφορικά με την κρυπτογράφηση για όσα δεδομένα ταξιδεύουν στο νέφος;

• Έλεγχος πρόσβασης: Υπάρχουν επαρκείς μηχανισμοί ελέγχου πρόσβασης σε δεδομένα προσωπικού χαρακτήρα;

• Συγκέντρωση-συσχέτιση: Τα δεδομένα όταν μεταφερθούν σε πλατφόρμα νέφους συνεχίζουν να σχετίζονται με ένα αναγνωρίσιμο άτομο (και αρά διατηρούν το χαρακτήρα του προσωπικού δεδομένου);

• Ακεραιότητα: η ακεραιότητα των προσωπικών δεδομένων διατηρείται όταν αυτά πλέον υπάρχουν στο νέφος;

Φάση 5 : Αρχειοθέτηση

• Νομικές Δεσμεύσεις: Τα προσωπικά δεδομένα υπόκεινται σε ρυθμίσεις που υπαγορεύουν για πόσο χρόνο θα πρέπει να αποθηκευτούν και να αρχειοθετηθούν. Είναι λοιπόν ζωτικής σημασίας η πλήρης συμμόρφωση του παρόχου στις απαιτήσεις αυτές.

• Τεχνικοί προβληματισμοί: Το αποθηκευτικό μέσο που χρησιμοποιείται για την αρχειοθέτηση των πληροφοριών θα είναι προσπελάσιμο και στο μέλλον (π.χ. οι δισκέτες 5,2’ δεν μπορούν πλέον να διαβαστούν γιατί οι σχετικές συσκευές ανάγνωσης έχουν αποσυρθεί). Ποιος ελέγχει τα μέσα μαζικής αποθήκευσης και ποιά είναι η ικανότητα για την ανάκτηση των δεδομένων από τον πάροχο Νέφους;

• Κατακράτηση: για πόσο καιρό τα δεδομένα θα διατηρούνται από τον πάροχο; Η περίοδος διατήρησης είναι συνεπής με την πολιτική του οργανισμού-πελάτη;

Φάση 6 : Καταστροφή της πληροφορίας

• Ασφαλής και αποτελεσματική καταστροφή: Η πολιτική αποδόμησης και καταστροφής της πληροφορίας γίνεται με τον ενδεδειγμένο τρόπο ώστε να είναι αδύνατη η μη εξουσιοδοτημένη επανάκτηση της ; Οι πληροφορίες καταστρέφονται ολοσχερώς και με τρόπο που να κάνει αδύνατη την ανάκτηση τους από τον οποιοδήποτε;

3.3.3 Ζητήματα προστασίας των προσωπικών δεδομένων

Στη συνέχεια θα αναλύσουμε βασικά ζητήματα που τέθηκαν παραπάνω. Γενικά κάθε οργανισμός πρέπει να εκτελεί συχνά ασκήσεις διασφάλισης της ιδιωτικότητας Privacy Impact Assessment (PIA), προκειμένου να εντοπίζει εγκαίρως τυχόν αδυναμίες στο σχεδιασμό του και να προχωρά στις ανάλογες προσαρμογές. Από πολλούς ειδικούς, εγείρονται διάφορα ερωτήματα σχετικά με την προστασία των προσωπικών δεδομένων, όταν αυτά εκτίθενται σε περιβάλλοντα νέφους. Οι προβληματισμοί αυτοί πηγάζουν από το συνδυασμό θεμάτων ασφάλειας των πληροφοριακών συστημάτων και ιδιωτικότητας.

Συμμόρφωση

Ποιές είναι οι απαιτήσεις συμμόρφωσης αναφορικά με το ιδιωτικό απόρρητο σε περιβάλλον νέφους; Ποια είναι η ισχύουσα νομοθεσία, οι κανονισμοί, τα πρότυπα και οι συμβατικές δεσμεύσεις που ρυθμίζουν τον κύκλο ζωής των πληροφοριών αυτών; Ποιος είναι υπεύθυνος για την τήρηση και την εφαρμογή των νομικών και άλλων δεσμεύσεων; Πώς η υφιστάμενη δομή που εξασφαλίζει την τήρηση του απορρήτου επηρεάζεται από τη μετάβαση σε περιβάλλον Νέφους; Πώς ενσωματώνεται στην πολιτική των εταιρειών το γεγονός ότι οι υποδομές νέφους είναι αντικείμενα πολλών, και κάποιες φορές αντικρουόμενων, εθνικών και υπερεθνικών ρυθμίσεων, δεδομένης μάλιστα και της γεωγραφικής διασποράς τους σε διαφορετικές χώρες;

Για παράδειγμα, ποιο δικαστήριο είναι αρμόδιο και ποια νομοθεσία θα πρέπει να εφαρμοστεί στην περίπτωση που τα δεδομένα χρησιμοποιούνται στην Ελλάδα αλλά αποθηκεύονται στις ΗΠΑ;

Πρόσβαση

Το υποκείμενο των δεδομένων έχει δικαίωμα να γνωρίζει ποιες προσωπικές πληροφορίες κατακρατηθήκαν και, σε ορισμένες περιπτώσεις, μπορεί να ζητήσει την διακοπή της παραπέρα επεξεργασίας τους (Νόμος 3471/2006 & Ν.2472/97 για την Ελληνική Δημοκρατία) . Οι σχετικές ρυθμίσεις παίζουν σημαντικό ρόλο στο σχεδιασμό των εκστρατειών Marketing και άλλων εμπορικών δραστηριοτήτων ενώ κατά κανόνα οι κανονισμοί ενσωματώνονται αναγκαστικά στην πολιτική προστασίας προσωπικών δεδομένων του κάθε οργανισμού (π.χ. τράπεζες). Όμως σε ένα πολύπλοκο σύστημα όπως το περιβάλλον Νέφους, δημιουργείται ανησυχία σχετικά με την ικανότητα του οργανισμού για την παροχή όλων των απαραίτητων πληροφοριών στο υποκείμενο της πληροφορίας και εν τέλει, η συμμόρφωση του οργανισμού με της νομικές του δεσμεύσεις. Εάν ο ενδιαφερόμενος εξασκήσει το δικαίωμα να ζητήσει από τον Οργανισμό να καταστρέψει τα προσωπικά του στοιχεία, πως μπορεί αυτός να εξασφαλίσει ότι όλες οι πληροφορίες του υποκειμένου έχουν διαγραφεί και στο νέφος;

Σε ποιον ανήκουν τα δεδομένα

Υπάρχουν σημαντικά ερωτήματα που οι κυβερνήσεις πρέπει να επεξεργαστούν με πρώτο και σημαντικότερο το ερώτημα «ποιός είναι ο νόμιμος ιδιοκτήτης των δεδομένων». Επίσης θα πρέπει να δοθούν απαντήσεις σχετικά με το σύνολο των εγγυήσεων που θα παρέχεται και που θα προστατεύει την ιδιωτικότητα των χρηστών, θα παρέχει τα εχέγγυα για την αντιμετώπιση παράνομων συμπεριφορών (τρομοκρατικές ενέργειες, ξέπλυμα μαύρου χρήματος κτλ) .

Ένα μεγάλο πρόβλημα είναι ότι άτομα που χρησιμοποιούν υπηρεσίες νέφους, δεν αντιλαμβάνονται τις επιπλοκές που επιφέρει στο προσωπικό απόρρητο η μεταφορά προσωπικών δεδομένων, σε κοινόχρηστες υποδομές, ενώ παράλληλα δεν είναι

κατάλληλα εκπαιδευμένοι να αντιμετωπίζουν τις προσκλήσεις ασφάλειας που συνεπάγεται η κατοχή ενός λογαριασμού e-mail, LinkedIn, MySpace ή Facebook.

Η τρέχουσα νομοθεσία στις ΗΠΑ τείνει στην παραδοχή ότι τα ιδιωτικά δεδομένα που είναι αποθηκευμένα στο νέφος δεν μπορούν να απολαμβάνουν το ίδιο επίπεδο προστασίας προσωπικών δεδομένων με τα δεδομένα που είναι αποθηκευμένα σε προσωπικό υπολογιστή, αλλά αντίθετα θα πρέπει να είναι εύκολα και γρήγορα προσβάσιμα από τις αρχές ασφαλείας των ΗΠΑ.

Υπάρχουν επίσης ερωτηματικά για το κατά πόσον οι κυβερνητικές υπηρεσίες, είναι αποδεκτό να αποθηκεύουν τα δεδομένα τους σε περιβάλλον νέφους. Ακόμη και αν ξεπεραστούν τα ηθικά διλλήματα που δημιουργούνται από την έκθεση ευαίσθητων πληροφοριών που οι πολίτες εμπιστεύτηκαν αποκλειστικά στη δημόσια εξουσία του τόπου τους σε περιβάλλοντα νέφους, θα πρέπει να θεσπιστούν κατάλληλες δικλείδες ασφαλείας που θα διασφαλίζουν την αποκλειστική ιδιοκτησία των δεδομένων από τους εξουσιοδοτημένους φορείς κρατικής εξουσίας.

Αποθήκευση

Πού αποθηκεύονται τα δεδομένα στο νέφος; Ποια πληροφορία μεταβιβάζεται στα διάφορα datacenters και σε ποιες χώρες; Υπάρχει μίξη των πληροφοριών από άλλες οργανώσεις που χρησιμοποιούν το ίδιο CSP (Cloud Service Provider);

Η νομοθεσία για τη διασφάλιση του απορρήτου των επικοινωνιών [Ν.3674 (ΦΕΚ **136/10-07-2008)**, **Ν.3471 (ΦΕΚ 133/Α/28-06-2006), Ν.3431 (ΦΕΚ 13/Α/3-2-2006), Ν.3115 (ΦΕΚ 47/Α/27-02-2003)** για την Ελλάδα**]** στις διάφορες χώρες, θέτει περιορισμούς στη δυνατότητα των οργανισμών να μεταφέρουν ορισμένους τύπων προσωπικών δεδομένων σε άλλες χώρες. Στην περίπτωση που τα δεδομένα αποθηκεύονται στο νέφος, ενδέχεται να υπάρξει διαβίβαση τους σε διαφορετικές κρατικές οντότητες, χωρίς αυτό να γίνεται εν γνώση του οργανισμού πελάτη, με αποτέλεσμα την πιθανή παραβίαση του τοπικού δικαίου (π.χ. προσωπικά δεδομένα Ελλήνων, αποθηκεύονται για λογαριασμό Ελληνικού Οργανισμού, στις ΗΠΑ).

Διατήρηση

Για πόσο χρονικό διάστημα αποθηκεύονται πριν διαγράφουν οριστικά και αποτελεσματικά, τα προσωπικά δεδομένα που μεταφέρονται; Ποια πολιτική διατήρησης διέπει τα δεδομένα; Ποιος είναι ο ουσιαστικός κάτοχος των δεδομένων, είναι δηλαδή ο οργανισμός-πελάτης ή ο CSP; Ποιος ελέγχει την πολιτική διατήρησης των πληροφοριών, και πώς γίνεται ο χειρισμός λεπτών περιπτώσεων (π.χ. δεδομένα που αφορούν ύποπτους για τρομοκρατικές ενέργειες) και ποιες εγγυήσεις παρέχονται για τη διασφάλιση των ατομικών δικαιωμάτων.

Καταστροφή

Με ποια μέθοδο ο CSP οδηγεί τα προσωπικά δεδομένα στην καταστροφή , μετά το πέρας της περιόδου υποχρεωτικής διατήρησης; Πώς ο οργανισμός διασφαλίζει ότι

τα προσωπικά δεδομένα καταστρέφονται από τους CSPs στο σωστό χρονικό σημείο και δεν είναι διαθέσιμα σε άλλους, μη εξουσιοδοτημένους χρήστες του Νέφους; Πώς διασφαλίζεται ότι το CSP δεν διατηρεί πρόσθετα αντίγραφα; Να σημειωθεί ότι για την επίτευξης της μέγιστης διαθεσιμότητας πολλοί CSP παρέχουν την υπηρεσία replication, η οποία συνιστάται στην αυτόματη αναπαραγωγή/ αποθήκευση της πληροφορίας σε πολλαπλά συστήματα ή και τοποθεσίες.

Το replication μετατρέπεται σε πρόκληση, όταν ο οργανισμός προσπαθεί να καταστρέψει τα δεδομένα. Δημιουργείται λοιπόν το ζήτημα αν μπορούμε να καταστρέψουμε αποτελεσματικά το σύνολο των δεδομένων όταν αυτά μεταναστεύσουν στο νέφος; Ο CSP πραγματικά καταστρέφει τα δεδομένα ή απλά τα κάνει απροσπέλαστα για τον πελάτη του;

Έλεγχος και παρακολούθηση

Πώς μπορεί οι οργανισμοί να παρακολουθούν τους CSP και να παρέχουν τις απαραίτητες εγγυήσεις προς τα ενδιαφερόμενα μέρη ότι πληρούνται οι απαιτήσεις για την προστασία του ιδιωτικού απορρήτου, όταν τα προσωπικά τους δεδομένα βρίσκονται σε μια άλλη φυσική τοποθεσία;

Παραβίαση της ιδιωτικής ζωής

Πώς μπορούμε να γνωρίζουμε ότι σημειώθηκε παραβίαση των δεδομένων, πώς μπορεί να διασφαλιστεί ότι ο πάροχος προχωρά σε έγκαιρη ενημέρωση όταν παρουσιάζεται μια παραβίαση και ποιός είναι υπεύθυνος για τη διαχείριση της κοινοποίησης της παραβίασης ; Ποιος είναι ο φορέας (ο οργανισμός-πελάτης ή ο πάροχος) που επιβαρύνεται με τα κόστη της αποζημίωσης των πελατών αλλά και της λογοδοσίας απέναντι στις αρχές

Ποιος έχει την ευθύνη για την προστασία του απορρήτου;

Υπάρχουν αντικρουόμενες απόψεις σχετικά με το ποιος φορέας είναι υπεύθυνος για την ασφάλεια και το ιδιωτικό απόρρητο. Ορισμένοι νομικοί και κάποιες επιστημονικές εργασίες αποδίδουν την ευθύνη στους παρόχους των υποδομών Νέφους, αλλά παρόλο που νομικά είναι δυνατή η μεταβίβαση της αστικής ευθύνης μέσω συμβατικών συμφωνιών (π.χ. μίσθωσης έργου), είναι αδύνατη η μεταφορά της απαίτησης για λογοδοσία. Σε τελική ανάλυση, στα μάτια του κοινού και του φυσικού δικαστή, το βάρος για την ασφάλεια των δεδομένων και της ιδιωτικής ζωής εμπίπτει στις υποχρεώσεις της οργάνωσης που συλλέγει αρχικά τα δεδομένα. Αυτό ισχύει ακόμη και αν ο χρήστης ή η εταιρεία δεν έχει την υποδομή να εξασφαλίσει την τήρηση των συμβατικών υποχρεώσεων του παρόχου.

Τα ιστορικά στοιχεία δείχνουν ότι παραβιάσεις στην ιδιωτικότητα των προσωπικών δεδομένων έχουν ένα συνεχές αποτέλεσμα . Όταν ένας οργανισμός χάνει τον έλεγχο των προσωπικών δεδομένων των χρηστών, οι χρήστες υφίστανται (άμεσα ή έμμεσα) ζημίες, σε μεταγενέστερο χρόνο, ως αποτέλεσμα της απώλειας. Η κλοπή

των στοιχείων ταυτότητας και η χρήση τους σε μη εξουσιοδοτημένες ενέργειες είναι μόνο ένα παράδειγμα για το τι μπορεί να συμβεί σε περίπτωση διάρρηξης της ιδιωτικότητας.

Αν κάτι τέτοιο συμβεί σε περιβάλλον Νέφους, τότε οι ευθύνες θα αναζητηθούν σε αυτόν που πήρε την απόφαση για την επιλογή του παρόχου και την μεταφορά των δεδομένων στο νέφος. Είναι ευθύνη του οργανισμού να λαμβάνει όλες τις απαραίτητες ενέργειες για τη διασφάλιση των δεδομένων των χρηστών, καθώς κανείς δεν θα επιδεχθεί τη δικαιολογία ότι κάποιος άλλος (ο πάροχος) «έφταιγε».

Ο υπεύθυνος για την επιτήρηση της κατάστασης των δεδομένων απαιτείται να έχει κατάλληλο υπόβαθρο, που να του επιτρέπει την σε βάθος κατανόηση της τεχνολογίας που χρησιμοποιείται ως υποδομή για την ανάπτυξη και παροχή υπηρεσιών Νέφους αλλά και να αντιλαμβάνεται τις νομικές δεσμεύσεις που αναλαμβάνει ο οργανισμός. Στην πραγματικότητα η αποτελεσματική διαχείριση των προσωπικών δεδομένων απαιτεί την ύπαρξη μια ομάδας νομικών και τεχνικών, με ειδίκευση στις ιδιαιτερότητες των δομών Υπολογιστικού Νέφους.

Το **μοντέλο λογοδοσίας** έχει τα ακόλουθα χαρακτηρίστηκα:

1. Οι οντότητες που συλλέγουν αρχικά τα δεδομένα, μπορούν να μεταφέρουν την αστική (αποζημιώσεις) και σε κάποιες περιπτώσεις την ποινική ευθύνη σε τρίτους (π.χ. CSP), αλλά τελικά είναι αυτές που φέρουν το βάρος της λογοδοσίας απέναντι στον πελάτη – υποκείμενο των δεδομένων.
2. Η αξιολόγηση των κινδύνων (Risk Assessment) και η ορθή διαχείριση του (Risk Management) πρέπει να επιτελείται με συνέπεια σε ολόκληρο τον κύκλο ζωής των δεδομένων.
3. Η κατανόηση των νομικών δεσμεύσεων και των συμβατικών υποχρεώσεων παίζει κρίσιμο ρόλο για την προστασία του υποκειμένου των δεδομένων αλλά και την προστασία του ίδιου του οργανισμού από παραβιάσεις της νομοθεσίας και τις συνέπειες αυτών.

Οι αλλαγές στη διαχείρισης κινδύνων που αφορούν την ιδιωτικότητα σε συνάρτηση με περιβάλλοντα Υπολογιστικού Νέφους.

Παρότι αρκετοί οργανισμοί, σε συμμόρφωση προς εθνικές νομοθεσίες και υπερεθνικούς κανόνες δικαίου, έχουν θέσει σε λειτουργία συστήματα διαχείρισης κινδύνου αναφορικά με τη διαρροή προσωπικών δεδομένων, το νέο περιβάλλον που διαμορφώνει η αρχιτεκτονική του Υπολογιστικού Νέφους οδηγεί στην ανάγκη ανασχεδιασμού των διαδικασιών και των πολιτικών που ακολουθούνταν μέχρι σήμερα.

3.4 Αρχή της ελάχιστης συλλογής δεδομένων

Η αρχή αυτή καθορίζει ότι η συλλογή των δεδομένων προσωπικού χαρακτήρα πρέπει να περιορίζεται στο ελάχιστο δυνατό επίπεδο που απαιτείται για το σκοπό για τον οποίο συλλέγονται. Τέτοια δεδομένα θα πρέπει να συλλέγονται με θεμιτά και σύννομα μέσα και μάλιστα για την πλειονότητα των περιπτώσεων για την Ελλάδα, με τη γνώση ή συγκατάθεση του υποκειμένου των δεδομένων.

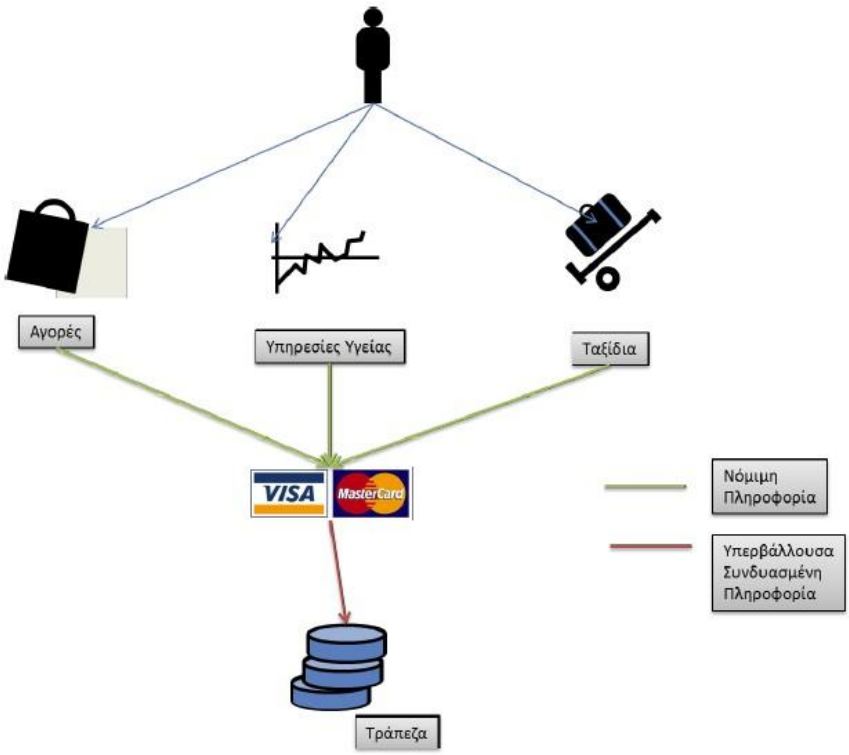
Ένα πρόβλημα που συχνά έρχεται στην επιφάνεια, έχει να κάνει με τη διαφορετική κατανόηση που εμφανίζουν τα εμπλεκόμενα μέρη σχετικά με τις πρέπουσες διαδικασίες και τις επαρκείς πρακτικές που εφαρμόζονται για τη διασφάλιση του προσωπικού απορρήτου. Είναι συχνό το φαινόμενο να υπάρχουν διαφορετικές προσδοκίες από τους πελάτες και διαφορετικές παροχές από τους παρόχους, χωρίς αυτό να γίνεται άμεσα αντιληπτό, καθώς τα μέρη προσβλέπουν σε «αυτονόητες» συνθήκες και δράσεις που τελικά μόνο αυτονόητες δεν είναι.

Το πρόβλημα έγκειται στο ότι δεν υπάρχει κάποιο κοινά αποδεκτό πρότυπο, αντίθετα υφίσταται ένα πλήθος αντιφατικών νομοθετημάτων, κανόνων και απόψεων σχετικά με το τι είναι προσωπικό απόρρητο και ποιες είναι προϋποθέσεις για την αποτελεσματική του προστασία από τους οργανισμούς που διαχειρίζονται δεδομένα προσωπικού χαρακτήρα. Πολλές εταιρείες θέλουν να υλοποιήσουν τη στρατηγική που εκείνες αντιλαμβάνονται ως ορθή. Ωστόσο, μπορεί να υπάρχει διαφοροποίηση ανάμεσα στη δίκη τους αντίληψη και αυτή του νομοθέτη. Ως αποτέλεσμα, ενδέχεται να υπάρχουν διαφορετικές προσδοκίες όσον αφορά ποια στοιχεία θεωρεί ως προσωπικά δεδομένα ο νομοθέτης και ποια ο πάροχος υπηρεσιών Νέφους.

Είναι σημαντικό ότι οι συμβάσεις επιπέδου υπηρεσιών (SLA) πρέπει να έχουν οριστικοποιηθεί πριν οποιαδήποτε δεδομένο τοποθετηθεί στο νέφος, επειδή είναι πολύ δύσκολο να διαπραγματευθεί κάνεις στη συνέχεια ειδικούς όρους και απαιτήσεις. Εφόσον υπάρχει μια προαποφασισμένη πολιτική που αποτυπώνεται στην πρόσκληση/διακήρυξη που απευθύνει ο οργανισμός στους CSP για την υποβολή πρότασης και περιγράφονται με σαφήνεια οι απαιτήσεις του SLA, δίνεται η δυνατότητα να αποκλειστούν τυχόν CSPs που δεν πληρούν τα κριτήρια του οργανισμού και άρα δεν είναι συμβατοί με τις απαιτήσεις για την προστασία της ιδιωτικότητας.

Είναι υποχρέωση του οργανισμού να δώσει μια σαφώς καθορισμένη πολιτική ενεργειών και μια λίστα απαιτήσεων αναφορικά με την ασφάλεια και τη διασφάλιση του απορρήτου, ενώ θα πρέπει να υπάρχουν ρήτρες αποζημίωσης με σαφώς καθορισμένες συνθήκες ενεργοποίησης και ύψος αποζημιώσεων που να καλύπτουν την όποια ζημία προκύψει για τον οργανισμό. Ειδικά για θέματα προσωπικού απόρρητου δεν πρέπει να παρέχεται καμιά δυνατότητα στο CSP να υπαναχωρήσει από τις αρχικές του δεσμεύσεις.

Μια δεύτερη πηγή προβληματισμού είναι το γεγονός ότι, ενώ κατά την διάρκεια της λειτουργίας πληροφοριακών συστημάτων που τροφοδοτούνται από διαφορετικές πήγες, εισέρχονται πληροφορίες που ενώ μεμονωμένα δεν παραβιάζουν τους κανόνες προστασίας δεδομένων προσωπικού χαρακτήρα, εντούτοις όταν συνδυαστούν οδηγούν σε μια συγκέντρωση που υπερβαίνει τις ανοχές του νομοθέτη.



Συνδυασμός πληροφοριών από διαφορετικές πηγές οδηγεί σε υπερβάλλουσα πληροφορία

3.5 Αρχή της περιορισμένης πρόσβασης

Η αρχή αυτή καθορίζει ότι τα δεδομένα προσωπικού χαρακτήρα πρέπει να μην γνωστοποιούνται, να γίνονται διαθέσιμα και να χρησιμοποιούνται μόνο για τους σκοπούς αυτούς που υπάρχει ρητή, με τη συγκατάθεση του υποκειμένου των δεδομένων, ή ανάλογη εξουσιοδότηση από αρχή δικαίου. Καθώς προσωπικά δεδομένα από διάφορες πηγές, ρέουν σε περιβάλλοντα Νέφους και κοινωνικά δίκτυα, γίνεται επιτακτική η ανάγκη για άσκηση αποτελεσματικής διαχείρισης των δεδομένων. Είναι εξαιρετικά σημαντικό να διασφαλίσουμε ότι τα συναχθέντα δεδομένα χρησιμοποιούνται αποκλειστικά και μόνο για τον αρχικό σκοπό της συλλογής τους και συνεχίζουν να υφίστανται τους απαραιτήτους περιορισμούς επεξεργασία τους.

Η σημασία των περιορισμών αυτών, γίνεται αντιληπτή όταν οι οργανισμοί που συλλέγουν τα δεδομένα αποφασίσουν να δημιουργήσουν ένα κεντρικό σημείο συγκέντρωσης των επιμέρους πληροφοριών. Ας φανταστούμε ένα δημόσιο υπάλληλο που πληρώνεται από την ενιαία αρχή πληρωμών. Ο υποθετικός υπάλληλος χρησιμοποιεί την κάρτα αγορών του υπουργείου οικονομικών, ενώ παράλληλα πάσχει από σοβαρή ασθένεια που του επιβάλει τη λήψη συγκεκριμένων φαρμάκων.

Όταν όλα τα παραπάνω δεδομένα συγκεντρωθούν στο ΚΕΠΥΟ τότε θα είναι δυνατή η μερική ανασύσταση του Ιατρικού φακέλου του υπαλλήλου με ένα πλήθος στοιχείων, που σαφώς υπερβαίνουν τα ανεκτά από το νόμο όρια και την επικρατούσα ηθική.

Είναι ορθό λοιπόν οι αρχικοί περιορισμοί να ενσωματώνονται στα σχετικά δεδομένα, ενώ θα πρέπει να υπάρχει ισχυρή νομική προστασία που να αποτρέπει αποτελεσματικά τον συνδυασμό δεδομένων χωρίς σαφή εξουσιοδότηση. Αντίστοιχα οι μηχανικοί της πληροφορικής πρέπει να σχεδιάζουν και να εφαρμόζουν διαδικασίες που θα αποτρέπουν και θα προλαμβάνουν τέτοιους συνδυασμούς είτε γίνονται εκούσια είτε ακούσια.

3.6 Αρχή της ασφαλείας

Η ασφάλεια των δεδομένων από μη εξουσιοδοτημένη πρόσβαση, παίζει πρωταγωνιστικό ρολό στην προστασία της ιδιωτικής ζωής. Η συγκεκριμένη αρχή καθορίζει τα προσωπικά δεδομένα που θα πρέπει να περιβάλλονται από επαρκείς εγγυήσεις κατά κινδύνων όπως η απώλεια τους, η μη εξουσιοδοτημένη προσπέλαση τους, η τροποποίηση ή η δημοσιοποίηση τους.

3.7 Αρχή της Διατήρησης και καταστροφής

Η αρχή αυτή καθορίζει ότι τα δεδομένα προσωπικού χαρακτήρα δε θα πρέπει να διατηρούνται για περισσότερο διάστημα από αυτό που είναι απολύτως αναγκαίο για την επίτευξη του στόχου για το οποίο έχουν συλλεχτεί, ή από τον χρόνο που απαιτείται από νομοθετικές ή κανονιστικές διατάξεις. Τα δεδομένα θα πρέπει να καταστρέφονται με ασφαλή τρόπο στο τέλος της περιόδου υποχρεωτικής διατήρησης. Η απάντηση στο ερώτημα αναφορικά με τον εύλογο χρόνο που θα πρέπει να διατηρούνται τα δεδομένα και πότε αυτά θα πρέπει να καταστρέφονται, εξακολουθεί να είναι μια πρόκληση για τις περισσότερες εταιρείες. Ο μεγάλος όγκος πληροφοριών που συσσωρεύονται σήμερα στα διάφορα Datacenters, οδήγησε στην ανάγκη για τον καθορισμό πολιτικών και διαδικασιών αναφορικά με τη διατήρηση των δεδομένων και την καταστροφή.

Σε χώρες με ανεπτυγμένη την κουλτούρα της πληροφορικής, οι παραπάνω πολιτικές έχουν θεσμοθετηθεί και επιβάλλονται από τη νομοθεσία και ειδικούς κανονισμούς, όπως η πράξη για τη Φορητότητα και τη Λογοδοσία Δεδομένων Κοινωνικής Ασφάλειας του 1996 (HIPAA), η πράξη Sarbanes-Oxley (SOX) στις ΗΠΑ αλλά και η νομοθεσία για την επί εξάμηνο και διετία διατήρηση των δεδομένων επικοινωνίας για την αντιμετώπιση της τρομοκρατίας (οδηγία 2006/2).

Σε κάποιες περιπτώσεις υπάρχει μια επικίνδυνη ασάφεια σχετικά με τον ορισμό της αποτελεσματικής διαγραφής των δεδομένων. Για παράδειγμα όταν τα αρχικά

δεδομένα διαγράφονται συμβαίνει το ίδιο με τα αντίγραφα ασφαλείας (Backup) και τελικά έχει γίνει οριστική διαγραφή των δεδομένων ή μήπως η μέθοδος καταστροφής που επιλέχθηκε επιτρέπει την επανάκτηση τους; Η απλή διαγραφή ενός αρχείου απλά σηματοδοτεί ότι μια διεύθυνση στο αποθηκευτικό μέσο είναι πλέον διαθέσιμη για την αποθήκευση νέων δεδομένων, όμως μέχρι τα νέα δεδομένα να εγγράφουν, τα παλιά ουσιαστικά βρίσκονται ακόμη εκεί και μπορούν να ανακτηθούν.

Το πρόβλημα απαιτεί ιδιαίτερο χειρισμό όταν τα μέσα αποθήκευσης δεν βρίσκονται στον έλεγχο των οργανισμών αλλά μισθώνονται ή περνούν στη δικαιοδοσία τρίτων για ανακύκλωση ή καταστροφή. Στην περίπτωση αυτή, ο οργανισμός πρέπει να εφαρμόζει διαδικασίες οριστικής διαγραφής και πιστοποίησης ότι τα αποθηκευτικά μέσα δεν περιέχουν ανακτήσιμες πληροφορίες.

3.8 Καταστροφή και Κρυπτογράφηση δεδομένων

Η Κρυπτογράφηση είναι σημαντικό εργαλείο για την επίτευξη αποτελεσματικής καταστροφής. Αυτό ισχύει διότι αρκεί η καταστροφή ενός ισχυρού κλειδιού κρυπτογράφησης για να περιπέσουν τα δεδομένα σε κατάσταση αχρηστίας ακόμη και όταν οργανώσεις χάσουν τη δυνατότητα διαχείρισης του φυσικού μέσου (π.χ. κλοπή σκληρών δίσκων ή υπολογιστών).

Η σπουδαιότητα της κρυπτογράφησης γίνεται αντιληπτή όταν τα δεδομένα διατηρούνται στους παρόχους καθώς επιτρέπει στον οργανισμό να διαχειρίζεται αποτελεσματικά την καταστροφή των δεδομένων χωρίς τη συνδρομή του παρόχου. Όπως έχουμε ήδη συζητήσει στο Υπολογιστικό Νέφος οι πόροι αποθήκευσης αποτελούν εικονικές συσκευές, με αποτέλεσμα ένας οργανισμός να μοιράζεται το ίδιο φυσικό μέσο με άλλους πελάτες ενός παρόχου.

Οι εικονικοί αυτοί πόροι μπορούν να αναδιανεμηθούν σε νέους χρήστες χωρίς να διαγραφούν προηγουμένως τα δεδομένα που υπήρχαν εκεί. Προσωπικές πληροφορίες που αποθηκεύονται σε αυτή τη συσκευή μπορεί τώρα να είναι διαθέσιμες στο νέο τους χρήστη, παραβιάζοντας πιθανώς τα ατομικά δικαιώματα, νόμους και κανονισμούς για την προστασία του απορρήτου των επικοινωνιών και των προσωπικών δεδομένων.

3.9 Κίνδυνοι και προβλήματα ασφάλειας στο Υπολογιστικό Νέφος

Μερικά συγκεκριμένα παραδείγματα των κινδύνων που αφορούν στη χρήση των υπηρεσιών Υπολογιστικού Νέφους είναι τα ακόλουθα:

- Προσεκτική επιλογή του παρόχου της υπηρεσίας Υπολογιστικού Νέφους. Η φήμη, το ιστορικό και η βιωσιμότητα αποτελούν παράγοντες που πρέπει να

εξετάζονται. Η βιωσιμότητα αποτελεί ιδιαίτερα σημαντικό παράγοντα, διότι εξασφαλίζει ότι οι προσφερόμενες υπηρεσίες θα είναι διαθέσιμες και ως εκ τούτου τα δεδομένα μπορούν να υφίστανται και να εξασφαλίζεται η παρακολούθηση της διαχείρισής τους.

- Ο πάροχος της υπηρεσίας αναλαμβάνει την ευθύνη για τη διαχείριση των πληροφοριών, οι οποίες αποτελούν κρίσιμο μέρος της επιχείρησης-πελάτη. Η αδυναμία εκπλήρωσης των συμβατικών υποχρεώσεων του παρόχου μπορεί να έχει επιπτώσεις όχι μόνο στην εμπιστευτικότητα αλλά και στη διαθεσιμότητα των πληροφοριών, καθώς επηρεάζουν σημαντικά τις επιχειρηματικές δραστηριότητες.

- Η παροχή υπηρεσίας στου «σύννεφου» χρησιμοποιεί την υποδομή του παρόχου. Ουσιαστικά δηλαδή, ο χρήστης παραχωρεί κομμάτι του ελέγχου στον πάροχο. Την ίδια στιγμή, η συμφωνία σε επίπεδο υπηρεσιών μεταξύ πελάτη-παρόχου (Service Level Agreement ή SLA) δε διασαφηνίζει αυτό το θέμα, αφήνοντας ερωτηματικά και κενά σε επίπεδα ασφάλειας. Τι θα μπορούσε αλήθεια να συμβεί αν χανόταν ο έλεγχος από τον πάροχο;

- Αυτή τη στιγμή τα εργαλεία που προσφέρονται, οι διαδικασίες, το πρότυπο τυποποιημένης μορφής και υπηρεσίες που μπορούν να παρέχουν ασφάλεια δεδομένων, φορητότητα και μετάβαση σε άλλον πάροχο, δεν μπορούν να θεωρηθούν ότι έχουν φτάσει σε ένα υψηλό επίπεδο. Με λίγα λόγια, αν θέλουμε να αλλάξουμε πάροχο υπηρεσιών Υπολογιστικού Νέφους έχουμε δύο προβλήματα. Το ένα είναι ότι υπάρχει δυσκολία στη μεταφορά αρχείων και υπηρεσιών, ενώ ακόμα πιο δύσκολα γίνονται τα πράγματα αν θα θέλαμε να γυρίσουμε στην κλασσική λύση με server και clients εντός της επιχείρησης. Εάν η φορητότητα των δεδομένων δεν είναι εφικτή, δε γίνεται να γυρίσουμε πίσω στον παλιό κλασσικό server. Σε αυτό το σημείο μάλιστα, τίθεται και θέμα εξάρτησης από τον πάροχο.

- Η δυναμική φύση λειτουργίας της τεχνολογίας Υπολογιστικού Νέφους μπορεί να οδηγήσει σε σύγχυση ως προς τον πραγματικό τόπο αποθήκευσης και επεξεργασίας των πληροφοριών. Σε περιπτώσεις που απαιτείται η ανάκτηση των πληροφοριών, αυτό μπορεί να δημιουργήσει καθυστερήσεις.

- Η κοινή διαχείριση αρχείων και πόρων που προσφέρει το Υπολογιστικό Νέφος, έχει ένα μειονέκτημα σε σχέση με τη multi-tenant αρχιτεκτονική. Για να εξηγήσουμε τον όρο multi-tenant, με απλά λόγια ας υποθέσουμε ότι το δίκτυο είναι σαν μια πολυκατοικία. Όλοι μπορούν να έχουν κοινή χρήση του ανελκυστήρα και μόνο ο διαχειριστής έχει πρόσβαση στο μηχανοστάσιο. Το πρόβλημα στη συγκεκριμένη περίπτωση είναι πώς διασφαλίζεται το δίκτυο

από τους ενοίκους, συνολικά και ατομικά. Για παράδειγμα, το διαμέρισμα Α του 2ου ορόφου με το Β συγκοινωνούν με κοινή ας υποθέσουμε εσωτερική πόρτα. Έρχεται ο κλέφτης να μπει στο Α, αλλά η πόρτα ασφαλείας του διαμερίσματος είναι αδιαπέραστη και θωρακισμένη. Πάει λοιπόν στο Β, στο οποίο η πόρτα είναι κλασσική μη ασφαλείας και ξεκλείδωτη. Με την ταυτότητα και μόνο ανοίγει, μπαίνει εύκολα και το χειρότερο είναι ότι αποκτά πρόσβαση και στο διαμέρισμα Α. Θεωρητικά περιγράψαμε πώς θα μπορούσε να επιτευχθεί μια επίθεση τύπου guest-hopping. Ας φανταστούμε ανάλογα εικονικές μηχανές (διαμερίσματα) και τον επόπτη τους (hypervisor ή virtual machine monitor). Στην πραγματικότητα βέβαια, ο βαθμός δυσκολίας μια τέτοιας επίθεσης είναι μεγάλος σε σχέση με τις κλασσικές επιθέσεις στο παραδοσιακό λειτουργικό. Δεν παύουν ωστόσο να αποτελούν μια σημαντική απειλή.

- Η πρόσβαση τρίτων σε κρίσιμες πληροφορίες δημιουργεί τον κίνδυνο μη εξουσιοδοτημένης αποκάλυψης εμπιστευτικών πληροφοριών. Αυτό μπορεί να αποτελέσει σημαντική απειλή για τη διασφάλιση της προστασίας της πνευματικής ιδιοκτησίας και των διάφορων επιχειρηματικών σχεδίων.

- Η κανονιστική συμμόρφωση σε διαφορετικές γεωγραφικές περιοχές αποτελεί ακόμα μία σημαντική πρόκληση. Προς το παρόν υπάρχει λιγοστό νομικό προηγούμενο σχετικά με την ανάληψη ευθυνών αναφορικά με υπηρεσίες Υπολογιστικού Νέφους. Επομένως, είναι σημαντικό να ληφθούν οι κατάλληλες νομικές συμβουλές, έτσι ώστε η σύμβαση με τον πάροχο να διευκρινίζει τους τομείς στους οποίους ο πάροχος είναι υπεύθυνος και υπόλογος για τις περιπτώσεις που αφορούν στην ασφάλεια των πληροφοριών και προκύπτουν από πιθανά προβλήματα.

- Λόγω της δυναμικής φύσης του Υπολογιστικού Νέφους, τα δεδομένα ίσως να μη μπορούν να είναι άμεσα διαθέσιμα σε περίπτωση καταστροφής, λόγω του ότι δεν μπορούμε να ξέρουμε που πραγματικά βρίσκονται. Οι διαδικασίες επιχειρηματικής συνέχειας και τα σχέδια ανάκαμψης από καταστροφή πρέπει να είναι καλά τεκμηριωμένα και να ελέγχονται. Ο πάροχος των υπηρεσιών Υπολογιστικού Νέφους χρειάζεται να κατανοήσει το ρόλο του και να λάβει όλα τα σχετικά μέτρα προστασίας που αφορούν στην ύπαρξη αντιγράφων ασφαλείας, την αντιμετώπιση περιστατικών ασφαλείας και την ανάκτηση των υπηρεσιών μετά από καταστροφή.

- Το Υπολογιστικό Νέφος προσφέρει πρόσβαση μέσω παγκόσμιου ιστού και κοινόχρηστων δικτύων. Είναι ευνόητο πως υπάρχει αυξημένο ρίσκο στην ασφάλεια, ειδικά όταν συνδυάζεται και με απομακρυσμένη σύνδεση.

- Πόσο σίγουροι είμαστε ότι τα δεδομένα μας είναι ασφαλή; Πόσο κατοχυρωμένοι είμαστε ότι δε θα χαθεί ένα σημαντικό αρχείο; Είναι γνωστό ότι τα αρχεία μας στο «σύννεφο» ταξιδεύουν μεταξύ δικτύων ανά τον κόσμο. Η ερώτηση είναι, ποιος τα ελέγχει; Και αν κάποιος ελέγχει που θα πάνε, τα διαχειρίζεται με σωστό και νόμιμο τρόπο; Γενικά είναι απαραίτητο να γνωρίζουμε την πολιτική του παρόχου. Κάποιοι παρέχουν μάλιστα και πιστοποιητικά. Στο θέμα των αρχείων, ένας κίνδυνος εμφανίζεται κατά τη διαγραφή τους. Στην πραγματικότητα, αν θέλαμε να σβήσουμε τα πάντα από το δίσκο υπάρχουν άπειρες τεχνικές. Από ένα απλό delete έως και πιο σύνθετες, που κάνουν δυσκολότερη έως αδύνατη την ανάκτηση των δεδομένων. Στο «σύννεφο» όμως, δε θα μπορούσαμε να κάνουμε κάτι τέτοιο. Μην ξεχνάμε ότι μοιραζόμαστε το δίσκο και με άλλους πελάτες και ότι στην πραγματικότητα το σβήσιμο δε γίνεται πάντα σε πραγματικό χρόνο.

- Ας υποθέσουμε ότι το «σύννεφο» είναι σωστά διασφαλισμένο εξωτερικά. Τι θα γινόταν όμως στην περίπτωση που το κακό ξεκινάει μέσα από την υποδομή; Εμείς πώς διασφαλιζόμαστε;

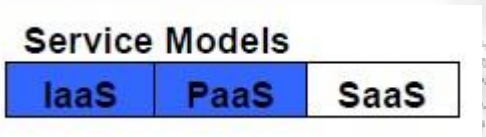
- Επειδή η ασφάλεια δεν είναι μόνο το τεχνικό επίπεδο και ο κώδικας ενός υπολογιστή, ένας κίνδυνος που αφορά στις επιχειρήσεις είναι ο ακόλουθος: μια επένδυση που χρειάζεται απόλυτη συμμόρφωση με συγκεκριμένους όρους για την εκπόνησή της, ίσως να μην είναι καλή ιδέα να εμπλακεί με το «σύννεφο». Ειδικά στην περίπτωση που ο πάροχος δε δίνει αποδεικτικό ότι η υπηρεσία θα δουλεύει σύμφωνα με τις απαιτήσεις. Μεγάλη προσοχή λοιπόν χρειάζεται σε θέματα που αφορούν σε κανονιστικά πλαίσια και πρότυπα λειτουργίας.

ΚΕΦΑΛΑΙΟ 4 : ΑΝΑΛΥΣΗ ΑΠΕΙΛΩΝ ΚΑΙ ΜΕΤΡΑ ΑΝΤΙΜΕΤΩΠΙΣΗΣ

Στις παραγράφους που ακολουθούν, προσδιορίζονται αναλυτικότερα οι κυριότερες από τις απειλές που αφορούν στις υποδομές Υπολογιστικού Νέφους καθώς και μερικά από τα προτεινόμενα μέτρα προστασίας (από την Cloud Security Alliance). Τα μέτρα αυτά αφορούν τόσο στη μεριά του παρόχου υπηρεσιών όσο και στη μεριά της επιχείρησης-χρήστη.

4.1 Ανάλυση των κυριότερων απειλών για το Υπολογιστικό Νέφος

1) Κακόβουλη και έκνομη χρήση του υπολογιστικού νέφους



Οι πάροχοι του Infrastructure as a Service (IaaS) προσφέρουν στους πελάτες τους την ψευδαίσθηση της απεριόριστης υπολογιστικής, δικτυακής και αποθηκευτικής χωρητικότητας, σε συνδυασμό με την προβολή μιας πολύ εύκολης διαδικασίας εγγραφής κατά την οποία κάθε απλός κάτοχος μιας πιστωτικής κάρτας δύναται άμεσα να εγγραφεί και να ξεκινήσει να χρησιμοποιεί της υπηρεσίες του υπολογιστικού νέφους. Επιπλέον, κάποιοι πάροχοι προσφέρουν ακόμη και δωρεάν δοκιμαστικές περιόδους περιορισμένης πρόσβασης στις υπηρεσίες. Εκμεταλλευόμενοι λοιπόν τη σχετική ανωνυμία αυτών των διαδικασιών εγγραφής και των μοντέλων χρήσης των υπηρεσιών, οι spammers, οι προγραμματιστές κακόβουλων προγραμμάτων καθώς και πολλοί άλλοι ηλεκτρονικοί εγκληματίες, έχουν τη δυνατότητα να διεξάγουν τις δραστηριότητές τους με ασυδοσία. Οι εγκληματίες συνεχίζουν να χρησιμοποιούν τις νέες τεχνολογίες προκειμένου να αυξήσουν την επέκτασή τους, να αποφύγουν τον εντοπισμό και να βελτιώσουν την αποτελεσματικότητα των δραστηριοτήτων τους. Οι πάροχοι υπηρεσιών υπολογιστικού νέφους, είναι επομένως ενεργά στο στόχαστρο, εν μέρει εξαιτίας του σχετικά αδύναμου συστήματος καταχώρισης στις υπηρεσίες που διευκολύνει την ανωνυμία, ενώ και η δυνατότητα ανίχνευσης της απάτης των παρόχων είναι περιορισμένη.

Οι πάροχοι που υπέφεραν παραδοσιακά από τέτοιου είδους επιθέσεις είναι αυτοί των Platform as a Service (PaaS). Ωστόσο, πρόσφατες έρευνες δείχνουν ότι πλέον οι

hackers έχουν αρχίσει να στοχεύουν και σε IaaS. Επιπροσθέτως, μερικές από τις περιοχές ενδιαφέροντος που ενδέχεται να δεχτούν τέτοιου είδους επιθέσεις μελλοντικά είναι το σπάσιμο κωδικών και κλειδιών, η κατανεμημένη άρνηση παροχής υπηρεσιών (DDOS), οι επιθέσεις από διαφορετικά σημεία δυναμικά, η φιλοξενία κακόβουλων δεδομένων, ο έλεγχος και η καθοδήγηση botnets καθώς και η δημιουργία πινάκων rainbow.

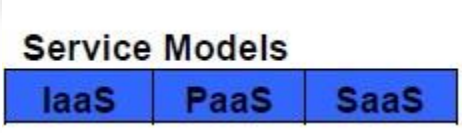
Παραδείγματα:

Προσφορές IaaS, έχουν φιλοξενήσει το Zeus botnet, το «δούρειο ίππο» InfoStealer πέρα από αρχεία για το Microsoft Office και το Adobe PDF. Τα botnets λοιπόν χρησιμοποίησαν τους IaaS εξυπηρετητές προκειμένου να πάρουν υπό την κυριαρχία τους και να ελέγξουν διάφορες λειτουργίες του συστήματος. Επιπλέον, λόγω του spam ολόκληρα blocks διευθύνσεων του IaaS δικτύου έχουν μπει δημοσίως στη μαύρη λίστα.

Αντιμετώπιση:

- Αυστηρότερες διαδικασίες που αφορούν στην αρχική εγγραφή και την επικύρωση της ταυτότητας των χρηστών των υποδομών Υπολογιστικού Νέφους
- Ενισχυμένες διαδικασίες και καλύτερος συντονισμός αναφορικά με λειτουργίες ελέγχου απάτης
- Αυξημένες διαδικασίες παρακολούθησης και ελέγχου με σκοπό την αποκάλυψη περιπτώσεων μη εξουσιοδοτημένης χρήσης των υποδομών Υπολογιστικού Νέφους αναφορικά με τα δεδομένα της επιχείρησής μας
- Παρακολούθηση των «μαύρων λιστών» που αφορούν στα κακόβουλα δίκτυα και έχουν δοθεί δημοσίως

2) Επισφαλείς διεπαφές προγραμματισμού εφαρμογών (APIs)



Οι πάροχοι υπηρεσιών για το υπολογιστικό νέφος, προσφέρουν μια σειρά από διεπαφές γραφικού περιβάλλοντος με το χρήστη, μέσω των οποίων οι πελάτες

διαχειρίζονται και αλληλεπιδρούν με τις υπηρεσίες του νέφους. Η τροφοδότηση, η διαχείριση, η ενορχήστρωση καθώς και η παρακολούθηση εκτελούνται χρησιμοποιώντας αυτές τις διασυνδέσεις. Επομένως, η ασφάλεια και η διαθεσιμότητα γενικώς των υπηρεσιών νέφους, είναι άμεσα εξαρτώμενες από την ασφάλεια σε αυτές τις βασικές διεπαφές. Καθώς στην όλη υπόθεση εμπλέκονται σοβαρά ζητήματα αυθεντικοποίησης, ελέγχου πρόσβασης, κρυπτογράφησης και παρακολούθησης των διεργασιών, οι διεπαφές πρέπει να σχεδιάζονται έτσι ώστε να προστατεύουν το σύστημα τόσο από τυχαίες όσο και από κακόβουλες προσπάθειες καταστρατήγησης. Επίσης, πολλοί οργανισμοί συχνά βασίζονται σε αυτές τις διεπαφές ώστε να προσφέρουν στους πελάτες υπηρεσίες προστιθέμενης αξίας. Το γεγονός αυτό αυξάνει το ρίσκο καθώς ενδέχεται οι οργανισμοί να παραδώσουν κάποια πολύ σημαντικά στοιχεία τους σε τρίτους με σκοπό την προσφορά των υπηρεσιών τους.

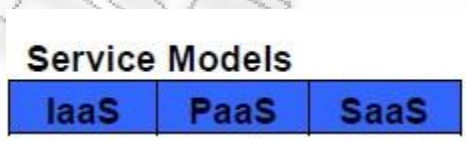
Παραδείγματα:

Ανώνυμη πρόσβαση, επαναχρησιμοποίηση κωδικών πρόσβασης, αυθεντικοποίηση κειμένου ή μετάδοση περιεχομένου, άκαμπτος έλεγχος πρόσβασης, περιορισμένη παρακολούθηση, άγνωστη υπηρεσία ή εξαρτήσεις μεταξύ των API.

Αντιμετώπιση:

- Ανάλυση του μοντέλου ασφάλειας της διασύνδεσης χρήστη του παρόχου
- Αυστηρή αυθεντικοποίηση και έλεγχος πρόσβασης σε συνδυασμό με κρυπτογραφημένη μετάδοση δεδομένων μέσω των APIs
- Πλήρης κατανόηση της λειτουργίας αλλά και των αλληλεξαρτήσεων που αφορούν στη χρήση των APIs

3) Κακόβουλοι χρήστες από την πλευρά του παρόχου



Η απειλή «εκ των έσω» είναι ένα πολύ γνωστό πρόβλημα για τους οργανισμούς. Η απειλή του «ανθρώπινου παράγοντα» ενισχύεται για τους πελάτες υπηρεσιών υπολογιστικού νέφους λόγω του ότι υπόκεινται σε ένα κοινό σύστημα διαχείρισης σε

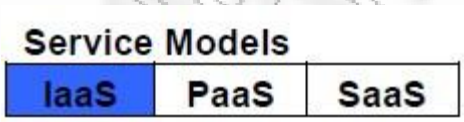
συνδυασμό με μια γενικότερη έλλειψη διαφάνειας στις διαδικασίες και τις διεργασίες του παρόχου. Για παράδειγμα, ένας πάροχος ενδέχεται να μην αποκαλύπτει πώς οι εργαζόμενοί του έχουν πρόσβαση σε φυσικά και εικονικά δεδομένα, πώς εποπτεύει αυτούς τους εργαζόμενους ή πώς η ανάλυση και η επεξεργασία των δεδομένων συμμορφώνονται στην πολιτική της εταιρείας.

Το πρόβλημα ενισχύεται όταν συχνά υπάρχει πολύ μικρή έως και καθόλου διαφάνεια στα κριτήρια πρόσληψης των εργαζομένων του οργανισμού. Αυτού του είδους η κατάσταση, προφανώς δημιουργεί μια ελκυστική ευκαιρία για κακόβουλη επίθεση ξεκινώντας από έναν απλό hacker μέχρι και οργανωμένους κυβερνο-εγκληματίες διεθνώς. Η πρόσβαση τέτοιων προσώπων σε εμπιστευτικά και ζωτικής σημασίας δεδομένα ή ακόμη και στον έλεγχο ολόκληρων υπηρεσιών του υπολογιστικού νέφους, μπορεί να γίνει με πολύ μικρό ρίσκο ανίχνευσης, άνετα και «αθόρυβα».

Αντιμετώπιση:

- Καθορισμός απαιτήσεων για το ανθρώπινο δυναμικό ως μέρος νόμιμων συμβολαίων
- Διαφάνεια και πληροφόρηση για την ασφάλεια και τις πρακτικές διαχείρισης.
- Προσδιορισμός διαδικασιών ενημέρωσης των πελατών από τον πάροχο σε περίπτωση παραβίασης της ασφάλειας της υποδομής Υπολογιστικού Νέφους.

4) Ζητήματα τεχνολογίας κοινής χρήσης



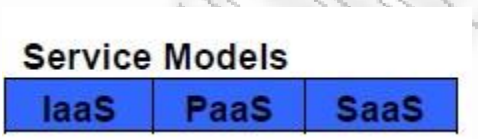
Οι πάροχοι του IaaS προσφέρουν τις υπηρεσίες τους με ένα κλιμακούμενο τρόπο μέσω της κοινής χρήσης της υποδομής. Συχνά όμως τα στοιχεία που συνθέτουν αυτή την υποδομή, όπως είναι η CPU και η GPU, δεν έχουν εξαρχής σχεδιαστεί ώστε να προσφέρουν ισχυρή ανεξαρτησία στις ιδιότητές τους όταν χρησιμοποιούνται σε μια πολυεπίπεδη αρχιτεκτονική. Προκειμένου να καλυφθεί αυτό το κενό, χρησιμοποιείται ένας εικονικός τρόπος πρόσβασης μεταξύ των δευτερευόντων λειτουργικών συστημάτων και των διαθέσιμων φυσικών πόρων. Ωστόσο, ακόμη και αυτή η δίοδος έχει τα ελαττώματά της διότι είναι δυνατό τα δευτερεύοντα λειτουργικά συστήματα

να αποκτούν έλεγχο ή επιρροή σε μη επιτρεπτά επίπεδα του συστήματος. Για το λόγο αυτό, προτείνεται μια αμυντική στρατηγική ασφάλειας εις βάθος που θα αφορά σε υπολογιστική, αποθηκευτική και δικτυακή επίβλεψη και επιβολή αυστηρών μέτρων ασφάλειας. Επιπλέον, ενδείκνυται ένας αυστηρός διαχωρισμός του χώρου φιλοξενίας σε τμήματα έτσι ώστε κάθε πελάτης του υπολογιστικού νέφους να μη συγκρούεται με άλλους πελάτες του ίδιου παρόχου όταν προσπαθούν να προσπελάσουν παρόμοιες εφαρμογές. Θα πρέπει δηλαδή ένας πελάτης να μην έχει δικαίωμα πρόσβασης σε κανενός άλλου τα δεδομένα, τη δικτυακή κίνηση κτλ.

Αντιμετώπιση:

- Εφαρμογή ισχυρών πρακτικών εγκατάστασης και παραμετροποίησης της τεχνολογικής υποδομής
- Επίβλεψη του περιβάλλοντος για μη εξουσιοδοτημένες αλλαγές ή δραστηριότητες
- Επιβολή ισχυρής αυθεντικοποίησης και ελέγχου πρόσβασης για τον έλεγχο και τις εφαρμογές των διαχειριστών
- Επαρκείς διαδικασίες ανάλογα με το επίπεδο της υπηρεσίας για την αντιμετώπιση της ευπάθειας και των κενών ασφαλείας
- Εφαρμογή σαρώσεων ευπάθειας και ελέγχου ρυθμίσεων των υποδομών Υπολογιστικού Νέφους

5) Απώλεια ή διαρροή δεδομένων



Υπάρχουν πολλοί τρόποι για την απώλεια/έκθεση των δεδομένων. Η διαγραφή και η αλλαγή των εγγραφών χωρίς να υπάρχει εφεδρικό αντίγραφο είναι δύο προφανή παραδείγματα. Ακόμη, η διακοπή της σύνδεσης μιας εγγραφής από ένα ευρύ ευρετήριο ενδέχεται να οδηγήσει σε επισφαλή δεδομένα. Επίσης, η απώλεια ενός κλειδιού κωδικοποίησης μπορεί να προκαλέσει την καταστροφή, ενώ θα πρέπει να προλαμβάνεται η πρόσβαση μη εξουσιοδοτημένων οντοτήτων σε ευαίσθητα δεδομένα. Η απειλή της απώλειας/έκθεσης των δεδομένων αυξάνεται στο υπολογιστικό νέφος εξαιτίας του μεγάλου αριθμού των προκλήσεων και του ρίσκου σε κάθε συναναστροφή με το νέφος λόγω των ιδιαιτεροτήτων της αρχιτεκτονικής του.

Η απώλεια ή η διαρροή δεδομένων ενδέχεται να έχει καταστροφικό αντίκτυπο σε μια επιχείρηση. Πέρα από τη ζημιά στη φήμη και το όνομα μια εταιρείας, μπορεί να προκληθεί ανεπανόρθωτο πλήγμα στην εμπιστοσύνη των συνεργατών, των πελατών ακόμη και των ίδιων των υπαλλήλων. Επιπροσθέτως, η απώλεια ζωτικής σημασίας δεδομένων, ενδέχεται να έχει ιδιαίτερα αρνητικές ανταγωνιστικές και οικονομικές συνέπειες. Στη χειρότερη περίπτωση, ανάλογα με τα στοιχεία που διαρρέουν, μπορεί να υπάρξουν ακόμη και νομικά προβλήματα.

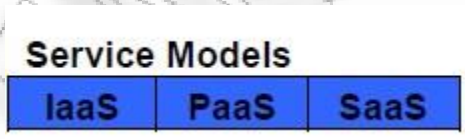
Παραδείγματα:

Ανεπαρκής αυθεντικοποίηση, εξουσιοδότηση και έλεγχος, ανακόλουθη χρήση κρυπτογράφησης και κλειδιών λογισμικού, αποτυχίες εφαρμογών, αξιοπιστία του κέντρου δεδομένων, επαναφορά από καταστροφή, δικαιοδοσία και πολιτικά ζητήματα.

Αντιμετώπιση:

- Υιοθέτηση αυστηρού ελέγχου πρόσβασης στα APIs
- Κρυπτογράφηση και προστασία της ακεραιότητας των μεταφερόμενων δεδομένων
- Προστασία δεδομένων τόσο στη διαδικασία του σχεδιασμού όσο και της εκτέλεσης
- Εφαρμογή αυστηρής πολιτικής δημιουργίας κλειδιών κρυπτογράφησης, αποθήκευσης, διαχείρισης και καταστροφής
- Καθορισμός της στρατηγικής δημιουργίας αντιγράφων ασφαλείας και της συντήρησης των δεδομένων από τον πάροχο

6) Πειρατεία Λογαριασμού ή Υπηρεσίας



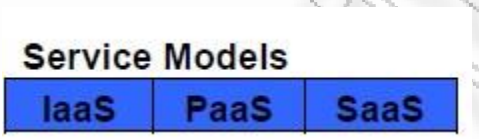
Η πειρατεία λογαριασμού ή υπηρεσίας δεν είναι κάτι νέο στο χώρο της τεχνολογίας. Επιθέσεις όπως είναι το phising, η απάτη και η εξερεύνηση των ευπαθειών του λογισμικού ακόμη είναι επιτυχείς. Το πρόβλημα τέτοιων επιθέσεων ενισχύεται με τη συχνή επαναχρησιμοποίηση κωδικών και κλειδιών. Τα υπολογιστικά

νέφη και η λύσεις που προτείνουν φέρνουν νέες απειλές στο προσκήνιο. Εάν ένας επιτιθέμενος αποκτήσει πρόσβαση στους κωδικούς ενός χρήστη και επομένως υποκλέψει την ψηφιακή του ταυτότητα, θα μπορεί να εποπτεύει τις δραστηριότητες, τις συναλλαγές του, να τροποποιεί δεδομένα, να επιστρέφει ψευδείς πληροφορίες αλλά και να ανακατευθύνει τους πελάτες σε παράνομα sites. Έχοντας ως βάση για τις επιθέσεις του το λογαριασμό ενός πελάτη και τις υπηρεσίες που χρησιμοποιεί, ο επιτιθέμενος μπορεί να εκμεταλλευτεί τη δύναμη της φήμης του πελάτη για να εξαπολύσει διαδοχικές επιθέσεις σε ανυποψίαστους χρήστες.

Αντιμετώπιση:

- Απαγόρευση διαμοιρασμού των στοιχείων λογαριασμών μεταξύ χρηστών και υπηρεσιών
- Υιοθέτηση ισχυρών τεχνικών διπλής αυθεντικοποίησης όπου είναι δυνατό
- Εγκατάσταση επίβλεψης για την εξεύρεση μη εξουσιοδοτημένων δραστηριοτήτων
- Κατανόηση της πολιτικής ασφάλειας κάθε παρόχου υπηρεσιών υπολογιστικού νέφους

7) Άγνωστο προφίλ κινδύνου



Όταν μια εταιρεία εγγράφεται σε μια υπηρεσία του υπολογιστικού νέφους, τα χαρακτηριστικά και οι λειτουργίες της υπηρεσίας είναι σίγουρα καλά διαφημισμένες αλλά τι συμβαίνει με τις λεπτομέρειες των εσωτερικών διαδικασιών ασφάλειας; Τι συμβαίνει με την παραμετροποίηση, τα κενά ασφαλείας και την αντιμετώπισή τους; Πώς αποθηκεύονται τα δεδομένα και οι σχετικές εγγραφές της εταιρείας και ποιος έχει πρόσβαση σε αυτά; Τι πληροφορίες θα διαρρεύσουν σε περίπτωση προβλήματος ασφάλειας; Πολύ συχνά τέτοιες ερωτήσεις δεν απαντώνται ξεκάθαρα από τους παρόχους ή παραβλέπονται με αποτέλεσμα οι πελάτες να αφήνονται με ένα άγνωστο προφίλ κινδύνου το οποίο φυσικά μπορεί να περιέχει σοβαρές απειλές.

Αντιμετώπιση:

- Μερική ή πλήρης κοινοποίηση λεπτομερειών της υποδομής (π.χ. τείχη προστασίας, τρόποι αντιμετώπισης κενών ασφαλείας κτλ.)
- Επίβλεψη και ειδοποίηση για απαραίτητα ζητήματα ασφαλείας

4.2 Το ρίσκο της επιλογής παρόχου

Το θέμα της ασφάλειας στην τεχνολογία Υπολογιστικού Νέφους δε θα πρέπει να μας απασχολεί μόνο σε επίπεδο απειλών δικτύου και κενών ασφαλείας. Οι παρεχόμενες υπηρεσίες μιας εταιρείας πρέπει να αξιολογηθούν πριν την επιλογή παρόχου, ώστε να γίνει σαφές ποια είναι η καλύτερη επιλογή προκειμένου η εταιρεία να χρησιμοποιεί σωστά το «σύννεφο».

Για παράδειγμα, ας δούμε την περίπτωση κλειδώματος (lock-in) στα τρία μοντέλα SaaS, PaaS και IaaS. Στο SaaS οι πληροφορίες των πελατών αποθηκεύονται σε μία βάση δεδομένων. Οι περισσότεροι πάροχοι προσφέρουν μια διαδικασία μέσω API για την εξαγωγή δεδομένων. Στην περίπτωση που ο πάροχος δεν προσφέρει αυτή τη διαδικασία, δεν μπορούμε να αλλάξουμε πάροχο, διότι δεν μπορούμε να ανακτήσουμε τα αρχεία σε μια μορφή που να μπορούν να αναγνωριστούν από το νέο. Από πάροχο σε πάροχο μπορεί να υπάρχει διαφορά στο σκελετό και τη δομή της βάσης δεδομένων. Ο νέος πάροχος ενδέχεται να προσφέρει βοήθεια για τη μεταφορά (με κάποιο κόστος) ώστε να συγκροτηθεί η βάση στο καινούριο περιβάλλον. Αντίστοιχα, θα ήταν καλό να έχουμε γνώση αν ο πάροχος που επιλέγουμε προσφέρει διαδικασία μεταφοράς των αρχείων μας στον παλιό κλασσικό server μας. Σε επίπεδο εφαρμογών για μια επιχείρηση ισχύει το ίδιο. Σε περίπτωση αλλαγής παρόχου, η εφαρμογή θα πρέπει να ξαναγραφεί ουσιαστικά ακολουθώντας το νέο API.

Στο PaaS το κλείδωμα προκύπτει και στο API και στο υλικό που δίνει πρόσβαση σε ένα πολύ γρήγορο αποθηκευτικό σύστημα. Αν λοιπόν γίνει αλλαγή παρόχου, τόσο η εφαρμογή όσο και το πρόγραμμα που ελέγχει την πρόσβαση στο αποθηκευτικό σύστημα πρέπει να ξαναγραφούν. Είναι φανερό ότι αυτό θα επιφέρει μεγαλύτερο κόστος. Ακόμα και στην περίπτωση που το API είναι το ίδιο, ο κώδικας για το αποθηκευτικό μοντέλο ενδέχεται να διαφέρει. Πρέπει να γνωρίζουμε ότι οι εφαρμογές του νέφους είναι γραμμένες ξανά για να λειτουργούν στο νέφος. Για παράδειγμα μια εφαρμογή Java μπορεί να έχει ξαναγραφεί και να της έχουν αφαιρεθεί λειτουργίες που θα μπορούσαν να προδώσουν την ασφάλεια του «σύννεφου». Το PaaS μοντέλο μπορεί να προκαλέσει κλείδωμα στον πελάτη και σε αυτή την περίπτωση το βάρος εξαγωγής των αρχείων πέφτει αποκλειστικά στον ίδιο.

Στο IaaS τώρα, το κλείδωμα προκύπτει σε επίπεδο υποδομών και κατανάλωσης πόρων. Για παράδειγμα ένας πελάτης που χρησιμοποιεί αποθηκευτικό χώρο, δε θα έχει πρόβλημα αν χρησιμοποιήσει μη συμβατή μορφή (format) εικονικών μηχανών. Τα προγράμματα και οι πληροφορίες εικονικών μηχανών μπορούν να μετακινούνται στο ίδιο «σύννεφο» προσφέροντας φορητότητα. Η αλλαγή παρόχου όμως θα είναι πρόβλημα μέχρι να υιοθετηθούν από όλους κάποια κοινά πρότυπα όπως το OVF.

Αντίστοιχα προβλήματα εντοπίζονται στην περίπτωση που για κάποιους λόγους χαθεί ο έλεγχος της διαχείρισης. Όπως προαναφέραμε, ένα κομμάτι του ελέγχου ασφαλείας μεταφέρεται στον πάροχο υπηρεσιών Υπολογιστικού Νέφους.

Προκειμένου να διασφαλιστεί η θέση, η πολιτική και τα συμφωνητικά της εταιρείας, είναι απαραίτητο να μελετηθεί το συμφωνητικό του παρόχου ώστε να μη συγκρούεται με την εταιρεία. Αν για παράδειγμα θέλετε να κάνετε penetration testing και ο πάροχος το απαγορεύει, τότε υπάρχει πρόβλημα. Είναι επίσης καλό να θυμόμαστε πως οι όροι του παρόχου ενδέχεται να αλλάξουν ανά πάσα στιγμή. Αυτό μπορεί να επηρεάσει μια από τις εφαρμογές σας, με αποτέλεσμα τη δυσλειτουργία ή ακόμη χειρότερα τη διακοπή της. Κάποιες φορές οι πάροχοι αναθέτουν σε τρίτους διάφορες ειδικευμένες εργασίες. Ας πάρουμε τον τομέα ασφαλείας. Σκεφτείτε λοιπόν ότι ο πάροχος που διαλέξατε έχει αναθέσει την υπηρεσία διαχείρισης ταυτότητας σε τρίτους. Σε περίπτωση διακοπής της υπηρεσίας λόγω διακοπής της σύνδεσης ή μιας αδυναμίας στο δικό τους σύστημα, τα δεδομένα εύκολα μπορούν να διαρρεύσουν.

Επομένως μια σωστή έρευνα επιλογής παρόχου θα πρέπει να εξετάζει αν ένας πάροχος δε λέει ποιον πυρήνα από υπηρεσίες χρησιμοποιεί καθώς σε αυτή την περίπτωση συνήθως αναθέτει σε τρίτους διάφορα καθήκοντα. Εάν δεν υπάρχει διαφάνεια στο συμβόλαιο για αυτό το θέμα, ο πελάτης δεν μπορεί να εκτιμήσει ορθά τι κίνδυνο ενδέχεται να αντιμετωπίσει. Ωστόσο, ρεαλιστικά, οι πάροχοι δεν μπορούν να παρέχουν λίστες με όλους τους συνεργάτες διότι αυτοί αλλάζουν συχνά.

Τέλος, πρέπει πάντα να έχουμε στο μυαλό μας ότι υπάρχουν και απειλές και ατέλειες που δεν καθορίζονται από το «σύννεφο» αλλά έχουν άμεση σχέση με αυτό και μπορούν να προκαλέσουν προβλήματα ασφάλειας. Λάθος παραμετροποίηση του συστήματος θα αποφέρει κενό ασφάλειας. Ευπάθεια του συστήματος ή του λειτουργικού επηρεάζει άμεσα την ασφάλεια του «σύννεφου» και οι πόροι του συστήματος επιβάλλεται να απομονωθούν σωστά. Αν δε γίνει αυτό, είναι πιθανό κάποιος να υφαρπάξει την πληροφορία που θέλει.

ΚΕΦΑΛΑΙΟ 5 : ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΝΕΦΟΣ ΚΑΙ ΓΕΝΙΚΕΣ ΠΡΑΚΤΙΚΕΣ ΔΙΑΣΦΑΛΙΣΗΣ ΠΛΗΡΟΦΟΡΙΩΝ

Οι παραπάνω κίνδυνοι θεωρούνται οι πιο σημαντικοί και πάνω σε αυτούς θα χτίσουμε και την άλλη πλευρά του νομίσματος. Ας δούμε τώρα τι είδους διασφάλιση προσφέρει το «σύννεφο» και ποια είναι τα πλεονεκτήματα στην ασφάλειά του.

5.1 Πλεονεκτήματα Ασφαλείας στο Υπολογιστικό Νέφος

Το «σύννεφο» σαν τεχνολογία έχει μεγάλες προοπτικές να αναδείξει την ασφάλειά του σε όλους τους τομείς. Καταρχήν έχει το πλεονέκτημα ότι τα μέτρα ασφαλείας κοστίζουν λιγότερο, καθώς φτιάχνονται για δίκτυα μεγάλης κλίμακας. Είναι σαφές ότι τα ίδια μέτρα θα καλύπτουν και τα μικρότερα δίκτυα που υπάρχουν μέσα στο «σύννεφο». Άρα ο χρήστης υπηρεσιών Υπολογιστικού Νέφους, σίγουρα θα έχει πολύ καλά εγκατεστημένη ασφάλεια με φίλτρα, αναβαθμίσεις και διασφαλίσεις στο «σύννεφο» αλλά και σε τοπικό επίπεδο. Οι περισσότεροι πάροχοι κάνουν αναπαραγωγή δεδομένων σε πολλές περιοχές, ώστε να διασφαλίσουν ότι τα δεδομένα θα είναι πάντα διαθέσιμα. Με αυτόν τον τρόπο, μπορούμε να είμαστε σχεδόν σίγουροι ότι δε θα χάσουμε κάποιο αρχείο. Οι αποθηκευτικοί χώροι καθώς και η ταχύτητα λήψης των δεδομένων, παρέχουν βέλτιστη απόδοση στο τοπικό σύστημα. Οι καθυστερήσεις σχεδόν δεν υπάρχουν και ακόμα και σε περίπτωση βλάβης τοπικού δικτύου θα είναι τοπικές, σε συγκεκριμένα υποδίκτυα παρά σε όλη την επιχείρηση ή τον οργανισμό. Πολύ σημαντικό κομμάτι της ασφάλειας είναι ότι οι πάροχοι Υπολογιστικού Νέφους έχουν την πολυτέλεια να προσλάβουν ειδικευμένο προσωπικό με συγκεκριμένα καθήκοντα στον τομέα ασφάλειας. Οι μικρότερες εταιρείες συνήθως έχουν μικρό αριθμό ατόμων που ασχολούνται με όλα τα προβλήματα.

Είναι ευνόητο λοιπόν ότι ένας μεγάλος πάροχος υπηρεσιών Υπολογιστικού Νέφους μπορεί να προσφέρει καλύτερες, πιο εξελιγμένες και πιο φθηνές υπηρεσίες ασφάλειας στους πελάτες του. Το ίδιο συμβαίνει και με τους πόρους δικτύου. Ο πάροχος μπορεί να φιλτράρει ή να διαμορφώσει την κίνηση στο δίκτυο. Μπορεί επίσης να προσφέρει κωδικοποίηση με σκοπό να αυξήσει την αποδοτικότητα μέτρων που λαμβάνει ώστε να αποφεύγει απειλές. Στο «σύννεφο», οι εικονικές μηχανές που χρησιμοποιούνται από τους πελάτες είναι από πριν ελεγμένες και διασφαλισμένες με τις τελευταίες ενημερώσεις για ιούς, απειλές ή κενά ασφαλείας. Ένα πρόσθετο χαρακτηριστικό είναι ότι κάθε εικόνα (image) που χρησιμοποιείται σε μια εικονική

μηχανή επανελέγχεται συχνά, με στόχο να βεβαιωθούμε ότι, για παράδειγμα, οι κανόνες του firewall δεν έχουν αλλάξει.

5.2 Γενικές πρακτικές για τη διασφάλιση πληροφοριών στο Νέφος

Το Υπολογιστικό Νέφος έχει μια σειρά από εγγενείς περιορισμούς και αδυναμίες που μπορούν να επηρεάσουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων που εμπιστευόμαστε στους παρόχους. Ωστόσο είναι εφικτό να έχουμε ένα ασφαλές και αξιόπιστο υπολογιστικό περιβάλλον νέφους. Αν και είναι μια αναδυόμενη περιοχή, μερικές καλές πρακτικές για τη διασφάλιση της προστασίας των πληροφοριών μας είναι οι ακόλουθες:

Η μη αποθήκευση κρίσιμων ή προσωπικών δεδομένων σε υποδομές Υπολογιστικού Νέφους. Οι κρίσιμες πληροφορίες μπορεί να αποθηκεύονται στα συστήματα τα οποία διαχειρίζεται η επιχείρηση. Ακόμα και αν χρειάζεται τα κρίσιμα επιχειρησιακά δεδομένα να επεξεργάζονται από εφαρμογές οι οποίες παρέχονται μέσω του Υπολογιστικού Νέφους, χρειάζεται η ανάλογη αρχιτεκτονική ασφάλειας η οποία θα ελαχιστοποιεί τη χρήση αυτών των κρίσιμων δεδομένων από το νέφος.

- Όταν γίνεται χρήση βάσεων δεδομένων οι οποίες βρίσκονται σε υποδομή Υπολογιστικού Νέφους, τότε τα δεδομένα τα οποία αποθηκεύονται στη βάση αυτή πρέπει να είναι κρυπτογραφημένα.
- Αποφυγή της επικοινωνίας μεταξύ βάσεων δεδομένων που βρίσκονται σε υποδομή Υπολογιστικού Νέφους και το εσωτερικό της επιχείρησης. Η διεργασία αυτή απαιτεί το άνοιγμα συγκεκριμένων δικτυακών θυρών και τη χρήση λογαριασμών χρηστών σε επίπεδο βάσεων δεδομένων, τα προνόμια πρόσβασης των οποίων γνωρίζει και πάροχος της υποδομής Υπολογιστικού Νέφους.
- Εφαρμογές οι οποίες έχουν διαμορφωθεί μετά από πολλή και εξειδικευμένη παραμετροποίηση καθώς και εφαρμογές με αυξημένες και συχνές απαιτήσεις επεξεργασίας δεδομένων, καλό είναι να μη λειτουργούν σε περιβάλλοντα Υπολογιστικού Νέφους.
- Αυξημένη προστασία της επικοινωνίας που αφορά στις υπηρεσίες διαχείρισης της υποδομής Υπολογιστικού Νέφους.
- Χρησιμοποίηση παρόχου που εξασφαλίζει περισσότερα από ένα σημεία παρουσίας
- Έλεγχος και καταγραφή ενεργειών όλων των διεργασιών διαχείρισης, καθώς και των σημείων διασύνδεσης της υποδομής μας με την υποδομή Υπολογιστικού Νέφους.

Για να απαντήσουμε λοιπόν και στους υπόλοιπους προβληματισμούς, είναι πολύ σημαντικό να προσέχουμε τι ανοίγουμε. Ένα κακόβουλο μήνυμα ηλεκτρονικού ταχυδρομείου ή ένας σύνδεσμος αρκούν για να κλέψουν άμεσα πληροφορίες.

Πρέπει να γνωρίζουμε πάντα τι προσφέρει ο πάροχος και κάνουμε backup ή την αντίστοιχη υπηρεσία που προσφέρει ο πάροχος αυτόματα. Η κωδικοποίηση στα δίκτυα προσφέρει μεγαλύτερη ασφάλεια. Μία αδυναμία του «σύννεφου» και των εικονικών μηχανών είναι ότι δεν υπάρχει καλή κωδικοποίηση, γεγονός που ενδέχεται να κάνει την πρόσβαση πιο εύκολη σε περίπτωση επίθεσης. Η ιδέα πίσω από το «σύννεφο» είναι να αποθηκεύεται όσο το δυνατό λιγότερη πληροφορία στο τερματικό του χρήστη. Στο «σύννεφο» υπάρχουν ειδικοί που ασχολούνται με την ασφάλεια, όμως πίσω από το εταιρικό laptop είναι μόνο ένας απλός χρήστης. Η εντύπωση που υπάρχει είναι ότι σε αυτή την περίπτωση ίσως το laptop να μη χρειάζεται να έχει ασφάλεια. Το «σύννεφο» όμως στο οποίο βρίσκεται συνδεδεμένο, πρέπει να είναι πλήρως ασφαλισμένο.

Επιπροσθέτως πρέπει να εξασφαλίζουμε τη γνώση για τα πιστοποιητικά και για το πώς γίνεται μια ασφαλής συναλλαγή στο διαδίκτυο. Οι πάροχοι υπηρεσιών Υπολογιστικού Νέφους πρέπει να είναι ενήμεροι για τις ευπάθειες του συστήματος και όχι να μαθαίνουν αφού πρώτα έχει γίνει το κακό. Ένα αρχείο ιστορικού (log) είναι πάντα χρήσιμο και θα πρέπει να φυλάσσεται για οποιαδήποτε περίπτωση. Δε θα πρέπει να το υποτιμάμε καθώς μπορούμε να διαπιστώσουμε πολλά πράγματα σχετικά με τη χρήση του δικτύου μας, τους χρήστες ή μια επίθεση που προσπαθεί να λάβει χώρα.

5.3 Διακυβέρνηση και Διασφάλιση στο Υπολογιστικό Νέφος

Οι κλασσικές ενέργειες που περιλαμβάνει η Διακυβέρνηση, όπως ο καθορισμός στόχων, η ανάπτυξη πολιτικής, η ανάθεση αρμοδιοτήτων και η διαχείριση του κινδύνου, διαδραματίζουν και στο Υπολογιστικό Νέφος πρωτεύοντα ρόλο. Συχνά επιβάλλονται προσαρμογές στις εταιρικές διαδικασίες αλλά και στην καθημερινή διαχείριση των συστημάτων. Αναμφίβολα, το γεγονός ότι οι μονάδες μιας εταιρείας μπορούν να παρακάμψουν εντελώς τη Διοίκηση της Πληροφορικής και να αποκτήσουν πρόσβαση σε νέες υπηρεσίες από το «σύννεφο», αποτελεί μια νέα πρόκληση στη Διακυβέρνηση. Με στόχο να παρασχεθεί στους άμεσους και έμμεσους χρήστες του «σύννεφου» ένα υψηλό επίπεδο διασφάλισης της ποιότητας της παρεχόμενης πληροφορίας, πρέπει να επιτυγχάνονται τα ακόλουθα:

1) Διαφάνεια στην προστασία των πληροφοριών μέσω ασφαλιστικών δικλείδων κατά της μη εξουσιοδοτημένης πρόσβασης, αλλαγής και καταστροφής δεδομένων,

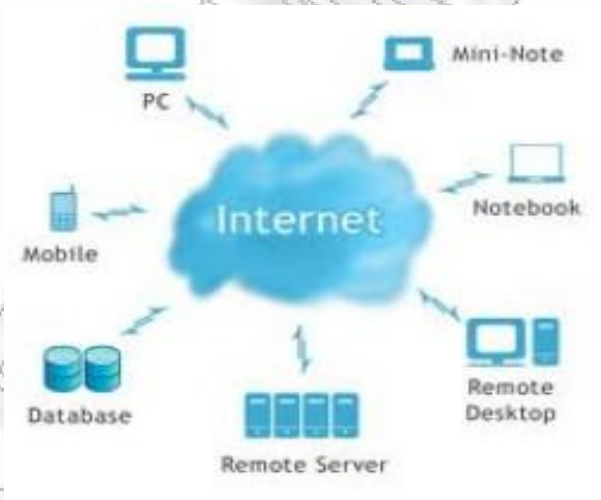
αλλά και μέσω του διαχωρισμού αρμοδιοτήτων και της πρόβλεψης πλάνου αντιμετώπισης επιθέσεων και ανάκαμψης από καταστροφή.

2) Ιδιωτικότητα με την πρόληψη, ανίχνευση και την ταχύτατη αντίδραση σε πιθανές επιθέσεις κατά της ασφάλειας, με ταυτόχρονη πρόβλεψη για δοκιμασμένα αντίστοιχα κανάλια επικοινωνίας.

3) Συμμόρφωση με το θεσμικό πλαίσιο και πρόβλεψη για την έγκαιρη παροχή προβλεπόμενων στοιχείων στις εποπτεύουσες αρχές από τον οργανισμό αλλά κυρίως από τρίτους παρόχους.

4) Η Διασυνοριακή ροή πληροφοριών θέτει θέματα όπως η ισχύουσα νομοθεσία για το απόρρητο των πληροφοριών και η αρμοδιότητα δικαστηρίων για την επίλυση διαφορών.

5) Πιστοποίηση από ανεξάρτητους ελεγκτές που θα διενεργείται στο πρόγραμμα διαπίστευσης των τρίτων παρόχων, καθώς δεν υπάρχουν ακόμα διαδεδομένα πρότυπα εξειδικευμένα για το Υπολογιστικό Νέφος.



ΚΕΦΑΛΑΙΟ 6 : ΑΣΦΑΛΕΙΑ ΝΕΦΟΥΣ ΣΤΟ ΜΕΛΛΟΝ - ΕΚΤΙΜΗΣΕΙΣ ΚΑΙ ΠΡΟΒΛΕΨΕΙΣ

6.1 Οι προβλέψεις των ειδικών για τα ζητήματα ασφαλείας στο Υπολογιστικό Νέφος

Ποια αναμένουν οι Chief Security Officers και οι υπόλοιποι IT Security experts να είναι τα πρώτα ζητήματα ασφάλειας στο Υπολογιστικό Νέφος για τη χρονιά που διανύουμε; Το csoonline.com αναφέρει τα παρακάτω πέντε ζητήματα που χρήζουν προσοχής τους επόμενους μήνες, σταχυολογώντας τις απόψεις έμπειρων στελεχών της αγοράς:

1. Τα smartphones και η ανταλλαγή δεδομένων. Ολοένα και περισσότεροι χρήστες θα έχουν πρόσβαση σε μεγάλους όγκους δεδομένων μέσα από συσκευές της επιλογής τους, λέει ο Randy Barr, Chief Security Officer στην Qualys Inc. και μέλος του Νέφους Security Alliance.

«Και αυτό συνοδεύεται από πολλά μη αντιμετωπιζόμενα ζητήματα ασφάλειας», υποστηρίζει ο ίδιος. «Αναμένουμε νέες λύσεις για την κάλυψη των αναγκών των κινητών συσκευών, αλλά είναι πιθανό να βιώσουμε μεγάλες παραβιάσεις που θα αναδεικνύουν το ζήτημα του mobile security, πριν δούμε μια λύση». Ανάμεσα στα πιθανά σενάρια, πάντα σύμφωνα με τον Barr, είναι το μη ασφαλές cloud-based back-up και τα άκρως εμπιστευτικά δεδομένα στις κινητές συσκευές.

«Υπάρχουν κάποιες ενδιαφέρουσες αλληλεξαρτήσεις όταν χρησιμοποιούνται πολλαπλές υπηρεσίες νέφους σε κινητές συσκευές, με συχνά διαφορετικά μοντέλα ασφάλειας», επισημαίνει. Και συνεχίζει «Ένας «hacked» πάροχος νέφους μπορεί, άθελά του, να παράσχει μαζική πρόσβαση σε εμπιστευτικά δεδομένα κινητών συσκευών, όταν οι mobile χρήστες χρησιμοποιούν cloud-based υποστήριξη στις συσκευές τους».

Επιπλέον, η κλοπή ή η απώλεια των συσκευών ενέχει τον κίνδυνο κακόβουλης πρόσβασης σε υπηρεσίες και δεδομένα νέφους. «Οι mobile εφαρμογές συχνά παρέχουν απευθείας και αυτοματοποιημένη πρόσβαση σε υπηρεσίες νέφους και δεδομένα».

2. Ανάγκη για καλύτερο έλεγχο πρόσβασης και διαχείριση ταυτότητας. «Το νέφος από τη φύση του είναι άκρως virtualized και federated, και για αυτό οι εταιρείες χρειάζονται μία προσέγγιση που θα καθιερώνει τον έλεγχο και τη διαχείριση των ταυτοτήτων (identity management) για όλο το νέφος, καθώς και για τα σύννεφα των άλλων», υποστηρίζει ο Alan Boehme, Senior Vice President για την IT

στρατηγική και αρχιτεκτονική στην ING. «Υπάρχουν φυσικά λύσεις και υπηρεσίες τρίτων εταιρειών που ανταποκρίνονται σε αυτά τα ζητήματα, αλλά αυτά μπορεί να μην είναι αρκετά για μεγάλες εταιρείες που διαθέτουν ένα μίγμα από legacy και από components νέφους».

3. Συνεχείς ανησυχίες για θέματα συμμόρφωσης. «Πιστεύω ότι η συμμόρφωση, θα εξακολουθήσει να αποτελεί ζήτημα ασφάλειας», υποστηρίζει ο Andy Ellis, CSO, Akamai.

4. Ο κίνδυνος των πολλαπλών «ενοίκων» του σύννεφου. Με δεδομένο ότι οι περισσότερες υπηρεσίες νέφους αξιοποιούν σημαντικά τεχνολογίες virtualization, οι κίνδυνοι που σχετίζονται με τη φιλοξενία δεδομένων πολλών οργανισμών σε μία φυσική hypervisor πλατφόρμα υπάρχει, και θα εξακολουθήσουν να υπάρχουν μέχρι να θεσπιστούν μέτρα κατάτμησης, σύμφωνα με τον Dave Shacklefold, Επικεφαλής Security, Risk & Compliance στην Sword & Shield Enterprise Security.

5. Ανάδυση προτύπων και πιστοποιήσεων. Καθώς η ασφάλεια θα αποτελέσει κρίσιμο παράγοντα στην επιλογή υπηρεσιών νέφους, τα πρότυπα και οι πιστοποιήσεις θα καταστούν εξαιρετικά σημαντικά στοιχεία τα οποία θα βοηθήσουν να εκτιμήσουν πόσο ασφαλή είναι τα δεδομένα τους. Προφανώς και οι εταιρείες που αξιοποιούν υπηρεσίες νέφους θα εξακολουθήσουν να αξιοποιούν τις υπάρχουσες διαδικασίες για την αξιολόγηση της ασφάλειας που προσφέρουν οι πάροχοι υπηρεσιών νέφους, αλλά θα επιζητούν και κάποια από τα πλέον δημοφιλή πρότυπα και best practices.

6.2 Τοπίο στην ομίχλη

Αυτή την περίοδο υπάρχει μια έντονη διχογνωμία από τους ειδικούς για το τι είναι ασφαλές και τι όχι, σε σχέση με το Υπολογιστικό Νέφος. Ο μεταδιδακτορικός ερευνητής Eran Tromer, με βάση το MIT στο εργαστήριο Computer Science and Artificial Intelligence Lab, ισχυρίστηκε πρόσφατα ότι θα παρουσιάσει στοιχεία που δείχνουν ότι η Amazon παρουσιάζει ευπάθεια σε επιθέσεις. Η Amazon από την πλευρά της, αρνείται ότι τα ευρήματά του ανταποκρίνονται στην πράξη. Ο αναλυτής πληροφορικής John Pescatore από τους Financial Times, σημειώνει «…το Υπολογιστικό Νέφος σήμερα είναι όπως ήταν τα windows το 1999. Το μόνο κακό είναι πως είναι εκτεθειμένο στο διαδίκτυο και ξέρουμε ότι μπορεί κάτι κακό να συμβεί»». Στο Black Hat USA στο Λας Βέγκας παρουσιάστηκαν μέθοδοι επίθεσης στο νέφος, ενώ τελικά η μεγαλύτερη ερώτηση του άρθρου είναι η εξής: «Μήπως το «σύννεφο» βάζει εμάς και τις πληροφορίες μας σε κίνδυνο; Μπορώ να προστατευτώ»;

Η ιστορία έχει δείξει πως το «σύννεφο» μπορεί σε κάποιες περιπτώσεις να μην είναι απόλυτα ασφαλές. Η Salesforce.com με SaaS κατακρίθηκε, καθώς στις 06/01/2009 άφησε 900,000 συνδρομητές χωρίς υπηρεσίες. Το κλείδωμα προκλήθηκε από ένα κομμάτι του δικτύου που δε δούλεψε λόγω κακής διαχείρισης της μνήμης. Όπως λοιπόν επισημαίνει και η Google, η αντιγραφή δεδομένων σε διαφορετικά σημεία είναι το κλειδί της επιτυχίας, ώστε να είναι πάντα διαθέσιμες οι πληροφορίες και τα δεδομένα τους. Αυτός είναι και ένας λόγος για τον οποίο οι βιομηχανίες δεν προχωρούν εύκολα στο νέφος, καθώς υπάρχουν κανόνες που πρέπει να τηρούνται και να συμφωνούν με τα στάνταρ και την πολιτική κάθε εταιρείας.

Η Amazon με το Elastic Compute Cloud (EC2) δίνει τη δυνατότητα να χτίσουμε μια εικόνα συστήματος (AMI) που περιέχει τις εφαρμογές, τις βιβλιοθήκες και αρχεία του συστήματος. Μπορούμε λοιπόν να διαλέξουμε ένα έτοιμο σύστημα ή να χτίσουμε το δικό μας γρήγορα και εύκολα. Αν και σας φαίνεται πολύ απλό και σίγουρο, υπάρχει μια μικρή λεπτομέρεια που μας ξεφεύγει. Οι πρώτες 47 εικόνες χτίστηκαν από την Amazon. Οι υπόλοιπες όμως χτίστηκαν από χρήστες. Μπορούμε να είμαστε σίγουροι πως οι εικόνες αυτές χτίστηκαν σωστά και με ασφάλεια; Το βασικό αρχείο περιγράμματος (templates) είναι βασισμένο σε αρχείο που φτιάχτηκε από απλούς χρήστες.

Το Google Docs παρέχει πραγματικά αρκετές δικλείδες ασφαλείας και όμως ο λογαριασμός μας είναι τόσο ασφαλής, όσο η ασφάλεια που παρέχει ο κωδικός. Ένα σκάνδαλο ξέσπασε με το όνομα Twittergate, όταν ένας hacker απέκτησε πρόσβαση μέσω του Twitter στους λογαριασμούς χρηστών και έκλεψε ευαίσθητα εταιρικά στοιχεία. Αντί λοιπόν τα αρχεία αυτά να μένουν στην εταιρεία πίσω από ένα τοίχος προστασίας υπήρχαν σε μια υπηρεσία, που για να σπάσει ήταν αρκετό και μόνο να βρεθεί ο σωστός κωδικός. Τα ευαίσθητα αρχεία επομένως, ίσως είναι καλό να φυλάσσονται τοπικά και κλειδωμένα σε ασφαλείς χώρους. Εννοείται πως οι

υπολογιστές με τα δεδομένα δεν πρέπει να έχουν καμία σύνδεση με τον έξω κόσμο μέσω εσωτερικού δικτύου ή διαδικτύου.

ΚΕΦΑΛΑΙΟ 7 : ΕΠΙΛΟΓΟΣ

Όπως διαπιστώσαμε, το Υπολογιστικό Νέφος αποτελεί μια νέα τεχνολογία με πολλές υποσχέσεις αλλά και με ειδικούς να έχουν ισχυρές επιφυλάξεις. Τόσο οι κίνδυνοι όσο και τα πλεονεκτήματα που προσφέρει το Υπολογιστικό Νέφος είναι σημαντικά. Αποτελεί εξέλιξη των σημερινών δικτύων και υπόσχεται πολύ σοβαρές αλλαγές που θα μας λύσουν τα χέρια. Ένα από τα δόγματα του Υπολογιστικού Νέφους είναι η μείωση του κόστους λειτουργίας και συντήρησης υλικού και λογισμικού, με αποτέλεσμα η επιχείρηση- πελάτης να μπορεί να επικεντρωθεί στις κύριες επιχειρηματικές του δραστηριότητες. Αυτό έχει σαφή οικονομικά και επιχειρησιακά οφέλη, τα οποία πρέπει να σταθμίζονται προσεκτικά έναντι των κινδύνων ασφάλειας πληροφοριών που εμπεριέχει η χρήση τεχνολογικών υποδομών Υπολογιστικού Νέφους που περιγράψαμε.

Κάποιοι ίσως να μην το εμπιστεύονται και ίσως να έχουν και δίκιο, αν το καλοσκεφτούμε όμως έχει πάρα πολλά θετικά. Στην πραγματικότητα, δεν είναι χειρότερο από τη σημερινή κλασσική δικτυακή τεχνολογία. Το αντίθετο μάλλον συμβαίνει. Η μόνη διαφορά με την παρούσα προσέγγιση δικτύων και ασφαλείας είναι ότι θα προσφέρει νέες προκλήσεις και προβλήματα που θα πρέπει να επιλυθούν. Με την εξάπλωση της τεχνολογίας του «σύννεφου», θα επιβιώσουν οι πάροχοι που έχουν προσέξει τον πελάτη και τον έχουν διασφαλίσει όσο το δυνατόν καλύτερα. Αυτή τη στιγμή ίσως το «σύννεφο» να μη θεωρείται ακόμα απόλυτα ασφαλές. Όσο όμως περνάει ο χρόνος, είναι πιθανό να αρθούν όλες οι επιφυλάξεις και τελικά το Υπολογιστικό Νέφος να αποδειχθεί η πλέον ασφαλής πλατφόρμα λειτουργίας των πληροφοριακών υποδομών μιας επιχείρησης ή οργανισμού.

Παρόλο που το Υπολογιστικό Νέφος μπορεί να προσδώσει πολλαπλά οφέλη, οι εταιρείες δεν πρέπει να βιαστούν να «ανέβουν στο βαγόνι» του νέφους χωρίς επιτακτικούς επιχειρηματικούς λόγους και χωρίς σαφή κατανόηση των ζητημάτων ασφάλειας, μυστικότητας και συμμόρφωσης, καθώς και των νομικών συνεπειών. Το Υπολογιστικό Νέφος είναι ένας καινούριος κόσμος τόσο για την πληροφορική όσο και την νομική επιστήμη. Αυτό έχει ως επακόλουθο να έρχονται στην επιφάνεια διαρκώς νέες προκλήσεις , που απαιτούν συντονισμένη δράση ανθρώπων με διαφορετικά γνωστικά αντικείμενα, για την αποτελεσματική διαχείριση τους.

Μία αποτελεσματική στρατηγική που θα καλύπτει όλα αυτά τα ζητήματα θα βοηθήσει τις εταιρείες να κατακτήσουν τον απόλυτο στόχο: να κάνουν τις υπηρεσίες νέφους να λειτουργούν όπως το δικό τους τμήμα IT security και να βρουν τρόπους να διασφαλίσουν και να μεγιστοποιήσουν τις επενδύσεις τους στο σύννεφο.

Η ασφάλεια και το νομικό τοπίο όσον αφορά το Υπολογιστικό Νέφος είναι ακόμα γεμάτο με αστοχίες και αβεβαιότητες. Σε μακροπρόθεσμο ορίζοντα, ωστόσο, είναι σίγουρο ότι οι πάροχοι υπηρεσιών νέφους θα εξακολουθούν να βρίσκουν οικονομίες κλίμακας, όχι μόνο για τις βασικές τους υπηρεσίες αλλά και για τη διαχείριση της ασφάλειας.

Προκειμένου να αξιοποιήσουν πλήρως τη δύναμη του Υπολογιστικού Νέφους, οι εταιρείες πρέπει να επιτύχουν εγγυήσεις για τη διαχείριση της ασφάλειας, της μυστικότητας και των ζητημάτων συμμόρφωσης. Για το σκοπό αυτό χρειαζόμαστε, μία αγορά με ανοιχτά standards, σαφέστερες ρυθμίσεις και community-driven διαλειτουργικότητα.

Μία προσέγγιση βάσει προτύπων θα καταστήσει ευκολότερη την υποστήριξη ευελιξίας από την πλευρά των παρόχων, καθώς και την παροχή διευρυμένων υπηρεσιών νέφους, ενώ θα είναι πιο εύκολο για τις εταιρείες να αξιολογήσουν τους παρόχους και να εμπιστευτούν τις υποσχέσεις τους για ασφάλεια και μυστικότητα.

Στο μέλλον οι μεγάλες εταιρίες θα διατηρήσουν in house λειτουργίες σημαντικού χαρακτήρα, καθώς η ιδιωτικότητα, η εμπιστευτικότητα και η απόλυτη ιδιοκτησία παίζουν σημαντικό ρολό. Όμως, αναμένουμε ότι εν τέλει οι τεχνολογίες και το θεσμικό πλαίσιο του νέφους θα ωριμάσουν και θα αναπτυχθούν, προσφέροντας νέες ευκαιρίες και προκλήσεις στην παγκόσμια κοινότητα.

Σε εποχές οικονομική στενότητας φαίνεται ότι η επιλογή χρήσης τεχνολογιών Υπολογιστικού Νέφους μπορεί να εξοικονομήσει αρκετά χρήματα στον κρατικό προϋπολογισμό. Αλλά και πάλι πρέπει να γίνεται προσεκτική εκτίμηση κόστους/οφέλους και η σχετική άσκηση έρευνας αναφορικά με την διαχείριση κίνδυνων.

ΑΝΑΦΟΡΕΣ

1.https://cloudsecurityalliance.org/

2.Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1",December 2009

3.Cloud Security Alliance, "Guidance for Identity & Access Management V2.1", April 2010

4.www.securitymanager.gr/it_security

5.ISACA white paper "Cloud Computing Business Benefits With Security, Governance and Assurance Perspectives", October 2009

6. IT Security Professional magazine No 14, "Cloud computing και ασφάλεια", January 2010

7. IT Security Professional magazine No 16, "Διαχείριση κινδύνων ασφάλειας στο cloud computing", May 2010

8.Vasant Raval, "Risk Landscape of Cloud Computing", 2010

9. Tommie W. Singleton, "IT Audits of Cloud and SaaS", 2010

10.http://www.acm.org/

11.http://blogs.msdn.com/b/gkanel/archive/2010/10/29/cloud-computing.aspx

12.http://www.interworks.gr/cloudcomputing.el.aspx

13.http://www.itcentral.gr/index.php?option=com_k2&view=item&id=84%3Acloud-computing&Itemid=65

14.http://www.itcentral.gr/index.php?option=com_k2&view=item&id=123:cloud-services-out-of-control&Itemid=65

15.http://www.itcentral.gr/index.php?option=com_k2&view=item&id=89:buying-cloud-services&Itemid=65

16.http://www.itcentral.gr/index.php?option=com_k2&view=item&id=88:10-remarkable-cloud-vendors&Itemid=65

17.http://www.itcentral.gr/index.php?option=com_k2&view=item&id=101:microsoft-azure&Itemid=54

18.http://www.scribd.com/doc/56407083/My-Final-Thesis-draft

19.http://www.netweek.gr/default.asp?pid=9&la=1&arId=21320&pg=2&ss=

20.http://www.facultyresourcecenter.com/curriculum/facetmain.aspx