Τμήμα Μηχανικών Πληροφορικής & Τηλεπικοινωνιών
Πολυτεχνική Σχολή Κοζάνης
Πανεπιστήμιο Δυτικής Μακεδονίας

http://arch.icte.uowm.gr

Συστήματα Παρ. & Κατ. Επεξεργασίας
Επιβλέπων καθηγητής : Δρ. Δασυγένης Μηνάς

Κοντόπουλος Ιάσων 410
Ματσαρίδης Παναγιώτης 420
Εξάμηνο: 6ο
Ημερομηνία: 17/07/2013

Περιεχόμενα (1/2)

- Ορισμός Υπολογιστικού Νέφους
- Ιστορική Αναδρομή
- Πλεονεκτήματα/Μειονεκτήματα Υπολογιστικού Νέφους
- Γενικά Χαρακτηριστικά Υπολογιστικού Νέφους
- Τεχνικά Χαρακτηριστικά Υπολογιστικού Νέφους
- Μοντέλα ανάπτυξης Υπολογιστικού Νέφους
- Μοντέλα υπηρεσιών Υπολογιστικού Νέφους
- Βασικά Θέματα Ασφαλείας Υπολογιστικού Νέφους

Περιεχόμενα (2/2)

- Θέματα Ασφαλείας στα μοντέλα υπηρεσιών
- Ασφάλεια Δεδομένων
- Τεχνολογίες για την ασφάλεια δεδομένων
- Πώς Χρησιμοποιείται το υπολογιστικό νέφος
- Επίλογος
- Βιβλιογραφία

Το Υπολογιστικό Νέφος

Το υπολογιστικό νέφος είναι ένα νέο πεδίο πληροφορικής, που παρέχει νέες προοπτικές σε τεχνολογίες δικτύωσης και θέτει ζητήματα στην αρχιτεκτονική, το σχεδιασμό, και την υλοποίηση των υπαρχόντων δικτύων και κέντρων δεδομένων.

Ορισμός

Ορισμός του NIST (1/2)

Το υπολογιστικό νέφος σύμφωνα με το US National Institute for Standards and Technology είναι:

« Ένα μοντέλο που δίνει τη δυνατότητα της συνεχούς, εύκολης και υψηλών απαιτήσεων πρόσβασης σε μια κοινόχρηστη συλλογή ρυθμιζόμενων υπολογιστικών πόρων, οι οποίοι τροφοδοτούνται και απελευθερώνονται με ελάχιστη προσπάθεια διαχείρισης και αλληλεπίδρασης παροχής υπηρεσιών».

Χρησιμοποιώντας απλούς όρους, θα μπορούσαμε να πούμε ότι τεχνολογία υπολογιστικού νέφους αποτελεί οποιοδήποτε λογισμικό χρησιμοποιεί ο χρήστης, το οποίο όμως δεν τρέχει στον υπολογιστή του, αλλά τρέχει στο διαδίκτυο.

Ορισμός του NIST (2/2)

Το υπολογιστικό νέφος δίνει τη δυνατότητα στους χρήστες του, οι οποίοι μπορεί να είναι είτε εξατομικευμένοι χρήστες διαδικτύου, είτε ολόκληρες επιχειρήσεις ή οργανισμοί, να αποθηκεύουν, να επεξεργάζονται και να διαχειρίζονται τα δεδομένα τους τα οποία, βρίσκονται σε ένα «νέφος» απόμακρων δικτύων στο οποίο, έχουν πολύ εύκολη πρόσβαση.

Η εικόνα(1) που ακολουθεί είναι ένα οπτικό μοντέλο του ορισμού του υπολογιστικού νέφους, που στηρίζεται στον ορισμό που δόθηκε παραπάνω από το National Institute for Standards and Technology (NIST).

Οπτικό μοντέλο του ΥΝ

Βασικά Χαρακτηριστικά	Ευρεία συνδεσιμότητα – Μεγάλη Ελαστικότητα- Ελεγχόμενες Υπηρεσίες- Self Service Ανάλογα με τη Ζήτηση- Δεξαμενή Πληροφοριών
Μοντέλα Υπηρεσιών	SaaS - PaaS - IaaS
Μοντέλα Ανάπτυξης	Δημόσιο Σύννεφο * Ιδιωτικό Σύννεφο * Υβριδικό Σύννεφο * Κοινοτικό Σύννεφο

1. Απεικόνιση ορισμού του υπολογιστικού νέφους.

Ιστορική Αναδρομή

Η Ιδέα του John McCarthy

Το “cloud computing” θεωρείται η φυσική συνέχεια της ευρείας αποδοχής τεχνολογιών όπως το virtualization, η αρχιτεκτονική SOA (Service-Oriented Architecture) και του “utility computing”.

Σε αυτές τις τεχνολογίες, αφαιρούνται τα εσωτερικά χαρακτηριστικά των συστημάτων από τους τελικούς χρήστες καθώς και η ανάγκη οι τελευταίοι να έχουν πόρους και τεχνογνωσία για την υποστήριξή τους.

Η κεντρική ιδέα πίσω από το “cloud computing” απαντάται πίσω στη δεκαετία του 1960, όταν ο John McCarthy είχε δηλώσει πως “ίσως, κάποια μέρα, τα υπολογιστικά συστήματα να είναι οργανωμένα και να διατίθενται ως δημόσια αγαθά”.

Προέλευση του όρου

Ο όρος cloud, δανεισμένος από τα τηλεφωνικά δίκτυα, μέχρι τις αρχές της δεκαετίας του 1990 υπονοούσε κυκλώματα από το ένα άκρο στο άλλο, ενώ αργότερα εικονικά ιδιωτικά δίκτυα (VPNs) όπου μέρος των δικτύων παρεχόταν σε συγκεκριμένους χρήστες.

Μετά την έκρηξη του web, η Amazon ήταν αυτή που έπαιξε καθοριστικό ρόλο στην εξέλιξη του cloud computing. Όπως και στις περισσότερες μεγάλες εταιρίες, οι υπολογιστικοί πόροι ήταν άφθονοι, με μέση χρήση κάτω του 10%, απλώς μόνο και μόνο για να μπορούν να αντεπεξέλθουν σε ξαφνικές εκρήξεις του φόρτου εργασίας και της ζήτησης.

Το έναυσμα

Το έναυσμα για την υλοποίηση του cloud τους ήταν αυτή ακριβώς η χαμηλή χρήση των υπολογιστών τους και η πίστη πως η ενοικίαση των μη χρησιμοποιούμενων πόρων θα μπορούσε να είναι κερδοφόρος.

Έτσι, το 2006 παρουσίασαν τα Amazon Web Services (AWS) στη βάση του computing utility.

Στις αρχές του 2008, το eucalyptus έγινε το πρώτο σύστημα ανοιχτού λογισμικού που προσέφερε μια πλατφόρμα συμβατή με αυτή της Amazon.

Την ίδια εποχή, εμφανίστηκε και το OpenNebula βελτιωμένο από ένα έργο της ευρωπαϊκής ένωσης, το RESERVOIR, και αποτελούσε το πρώτο σύστημα ανοιχτού κώδικα που προσέφερε τη δυνατότητα για private και hybrid clouds.

Ιστορική αναδρομή

2005
Eze Builds First Hedge Fund Hosted Platform

2006-2007
18 Hedge Funds Run on Hosted Platform

2008
Eze Hedge Fund Hotel Open: 200+ Users on Hosted Platform

January 2009
Eze Private Cloud Launched; Platform Available to All

Sept 2010
30+ Apps Running in Eze Private Cloud Platform

March & June 2011
Eze Private Cloud Expands to London & San Francisco

Dec 2011
130 Clients Operate in Eze Private Cloud

February 2012
Eze Ranked #20 on Global Managed Service Provider List

March 2012
Eze Private Cloud Reaches 1 Petabyte of Data

Σήμερα

Από εκεί και πέρα, η εξέλιξη είναι ραγδαία, με πάρα πολλές εταιρίες να προσφέρουν υπηρεσίες cloud computing σε διάφορα επίπεδα.

Πλεονεκτήματα/Μειονεκτήματα Υπολογιστικού Νέφους

Πλεονεκτήματα (1/2)

Αποδοτικό κόστος υπηρεσίας: Το cloud computing είναι ίσως η πιο οικονομικά αποδοτική μέθοδος για τη χρήση, τη συντήρηση και αναβάθμιση.

Σχεδόν Απεριόριστη αποθήκευση: Η αποθήκευση πληροφοριών στο σύννεφο δίνει σχεδόν απεριόριστη ικανότητα αποθήκευσης. Ως εκ τούτου, δεν χρειάζεται πλέον να ανησυχείτε για τυχόν εξάντληση του διαθέσιμου χώρου αποθήκευσης ή την αύξηση της διαθεσιμότητας του χώρου αποθήκευσης σας.

Δημιουργία αντιγράφων ασφαλείας και ανάκτησης: Δεδομένου ότι όλα τα δεδομένα σας είναι αποθηκευμένα στο σύννεφο το backup και το restore είναι σχετικά πολύ πιο εύκολο από ότι σε μια φυσική συσκευή.

Πλεονεκτήματα (2/2)

Εύκολη πρόσβαση σε πληροφορίες: Μόλις εγγραφείτε στο σύννεφο, μπορείτε να αποκτήσετε πρόσβαση στις πληροφορίες από οπουδήποτε, όπου υπάρχει μια σύνδεση στο Internet. Αυτή η βολική λειτουργία σας επιτρέπει να προχωρήσετε πέρα από γεωγραφικά ζητήματα τοποθεσίας.

Γρήγορη Ανάπτυξη: Τελευταίο, και σημαντικότερο, το cloud computing δίνει το πλεονέκτημα της γρήγορης εγκατάστασης. Μόλις επιλέξετε αυτή τη μέθοδο λειτουργίας, ολόκληρο το σύστημά σας μπορεί να είναι πλήρως λειτουργικό σε λίγα λεπτά. Φυσικά, το ποσό του χρόνου θα εξαρτηθεί από το ακριβές είδος της τεχνολογίας που χρειάζεστε για την επιχείρησή σας.

Μειονεκτήματα (1/2)

Ασφάλεια και μυστικότητα: Τα δύο αυτά χαρακτηριστικά μπορούν να θεωρηθούν ως μειονεκτήματα για τον λόγο ότι όταν οι χρήστες δίνουν τα στοιχεία τους σε έναν τρίτο υπάρχει η πιθανότητα να μην είναι άνετοι και αυτή η ανησυχία είναι ακόμη μεγαλύτερη για τις επιχειρήσεις διότι μερικές φορές επιθυμούν να κρατήσουν τις πληροφορίες τους στα υπολογιστικά νέφη.

Απώλεια ελέγχου: Μπορεί να υπάρξουν προβλήματα απώλειας ελέγχου, με τους φορείς παροχής υπηρεσιών στα επίπεδα συντήρησης και συχνότητας.

Μειονεκτήματα (2/2)

Υψηλό κόστος: Όπως είδαμε πριν, αποφέρει μεγάλη εξοικονόμηση κόστους λόγω του ότι δεν χρειάζεται τόσος εξοπλισμός, συγχρόνως όμως επειδή είναι καινούρια τεχνολογία την καθιστά ακριβότερη. Πρέπει να αγοράσει κάποιος το λογισμικό που θα τρέφει το "σύννεφο", και ίσως να υπάρξουν προβλήματα με την εγκατάσταση της στις μηχανές.

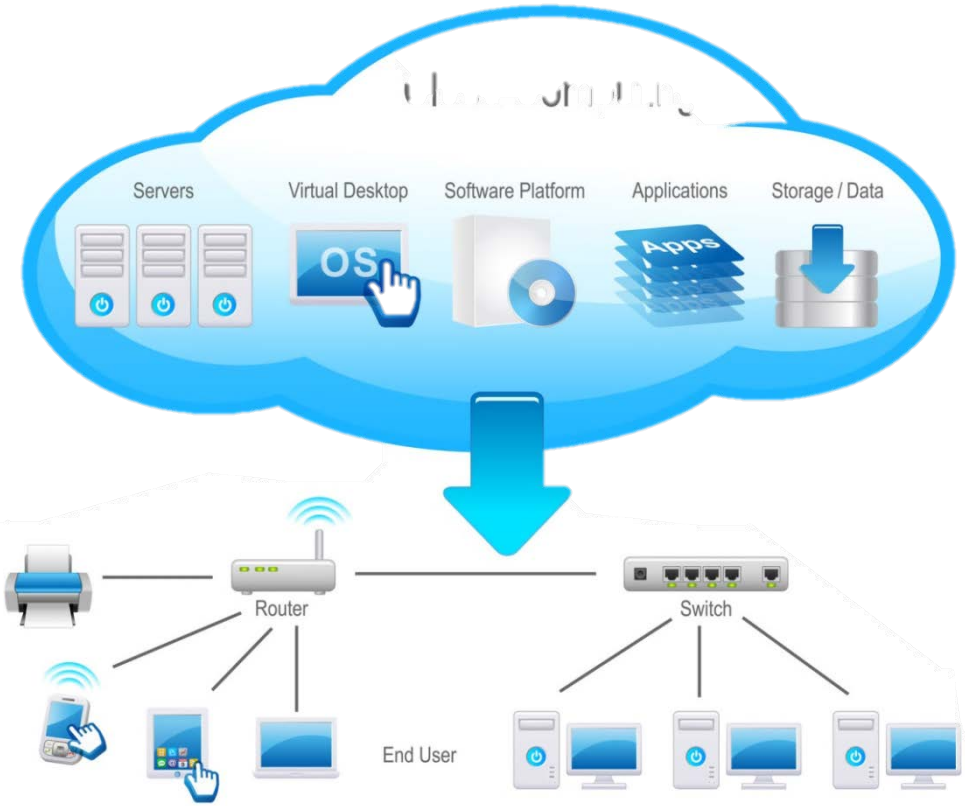
Ευελιξία: Η ευελιξία επίσης είναι ένα προσωρινό πρόβλημα όμως, επειδή η τεχνολογία του cloud computing είναι ακόμα καινούρια και στα αρχικά στάδια δεν έχει τελειοποιηθεί και ίσως να μην δίνει την ευελιξία που χρειάζονται οι χρήστες. Αυτό έχει ως επιβάρυνση σε αυτούς προσωρινά, να αναβαθμίσουν τον υπολογιστή συννέφων με απώλεια μερικών στοιχείων.

Χαρακτηριστικά του ΥΝ

Αυτοεξυπηρέτηση

Οι χρήστες μπορούν να αυτοεξυπηρετηθούν την εκάστοτε στιγμή ανάλογα με το τι επιθυμούν.

Κάθε καταναλωτής μπορεί να ζητήσει αυτόματα μια υπηρεσία με βάση τις ανάγκες του, χωρίς να μεσολαβήσει κάποια ανθρώπινη αλληλεπίδραση με το φορέα παροχής υπηρεσιών.



Κόστος χρησιμοποίησης

Η συγκέντρωση των πόρων (επεξεργαστές, μνήμη, κ.λπ.) που χρησιμοποιούνται, μοιράζονται μεταξύ πολλών χρηστών και δίνεται χρόνος εκτέλεσης εργασιών για τον κάθε χρήστη, την εκάστοτε στιγμή που ζητάτε.

Γεγονός που μειώνει το κόστος χρησιμοποίησης τους για τους χρήστες του νέφους και τους συμφέρει να κάνουν κοινή χρήση, δεδομένου ότι ο χρόνος χρησιμοποίησης που δίνεται σε κάθε χρήστη βασίζεται σε έναν προγραμματιστικό αλγόριθμο.

Μέτρηση υπηρεσιών

Επιπρόσθετα, χαρακτηριστικό είναι και η μέτρηση των προσφερόμενων υπηρεσιών ώστε η ποιότητα τους να είναι σε πολύ ικανοποιητικό επίπεδο.

Υπάρχουν ειδικοί μηχανισμοί οι οποίοι, προσμετρούν την χρησιμότητα, καθώς και την υγεία των υπηρεσιών με στόχο την διαφάνεια μεταξύ καταναλωτών και παρόχων, την επίτευξη βελτιστοποίησης των πόρων, καθώς και τη δημιουργία ενός συστήματος υπολογιστικού νέφους κλειστού κύκλου, το οποίο είναι πλήρως αυτοματοποιημένο.

Έλεγχος

Τελευταίο χαρακτηριστικό που απορρέει από τον ορισμό του υπολογιστικού νέφους είναι η δυνατότητα ελέγχου.

Για να υπάρχει σωστή εφαρμογή κανονισμών, στις υπηρεσίες που προσφέρονται είναι απαραίτητο να παρέχουν αρχεία καταγραφής που εξασφαλίζουν την ιχνηλασιμότητα των πολιτικών που εφαρμόζονται από τους παρόχους του νέφους.

Τεχνικά χαρακτηριστικά (1/3)

Αποϋλοποίηση: Η διάρθρωση, ο τόπος εγκατάστασης και η συντήρηση αυτών των υπηρεσιών πληροφορικής τους πρέπει να είναι όσο το δυνατόν πιο αόρατες για τους χρήστες, είτε πρόκειται για ιδιώτες είτε για επιχειρήσεις.

Ευκολία πρόσβασης: Εφόσον διαθέτουν σύνδεση στο Διαδίκτυο, οι χρήστες έχουν πρόσβαση στα δεδομένα και στις εφαρμογές τους από οποιονδήποτε τόπο και από οποιαδήποτε συσκευή, είτε πρόκειται για προσωπικό υπολογιστή, επιπαλάμιο (ταμπλέτα) ή έξυπνο τηλέφωνο (smartphone).

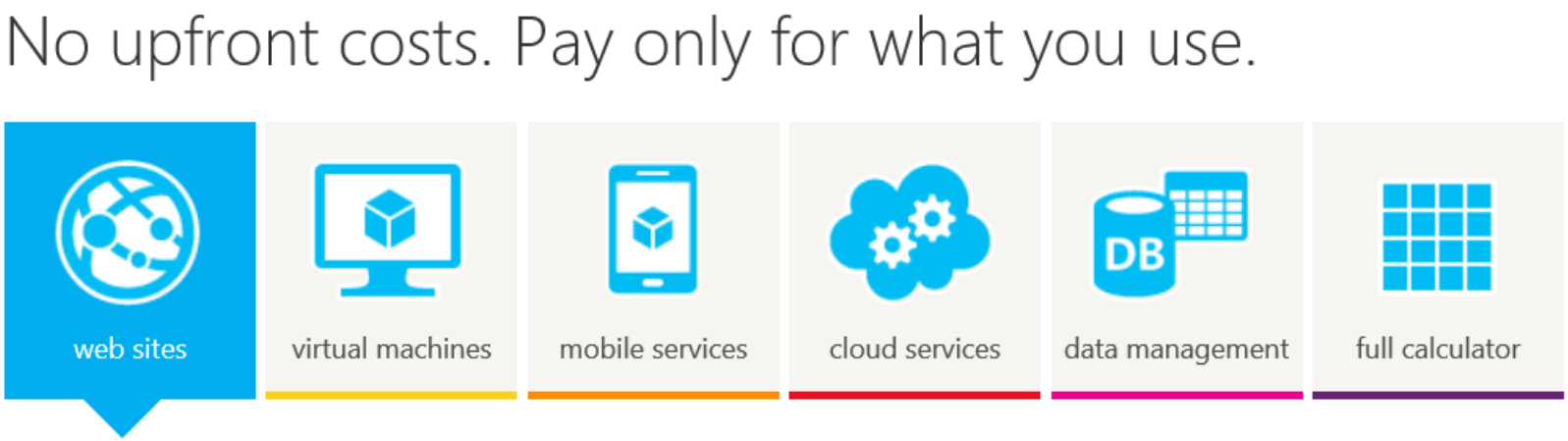
Τεχνικά χαρακτηριστικά (2/3)

Κλιμακωσιμότητα: Ο προμηθευτής προσαρμόζει σε πραγματικό χρόνο την υπολογιστική ισχύ στις ανάγκες του εκάστοτε χρήστη. Αυτό σημαίνει ότι ο χρήστης θα μπορεί να καλύπτει τις ανάγκες του ακόμη και σε περίοδο αιχμής, χωρίς να πρέπει να επενδύσει σε εξοπλισμό πληροφορικής που θα χρησιμοποιεί ελάχιστα ανάμεσα σε δύο περιόδους αιχμής.

Κοινή χρήση: Η κλιμακωσιμότητα είναι εφικτή επειδή ο πάροχος θέτει τα εργαλεία πληροφορικής στη διάθεση πολλών χρηστών ταυτόχρονα. Η πρακτική αυτή επιτρέπει τη μέγιστη και καλύτερη δυνατή αξιοποίηση τεράστιων πάρκων εξυπηρετητών με πολλές χιλιάδες ηλεκτρονικούς υπολογιστές.

Τεχνικά χαρακτηριστικά (3/3)

Τιμολόγηση ανάλογη με τη χρήση: Ο χρήστης καταβάλλει μόνον το ποσό που αντιστοιχεί στις υπηρεσίες που χρησιμοποίησε πραγματικά, ανάλογα με τις ανάγκες του σε υπολογιστική ισχύ. Οι συμβάσεις ΥΝ είναι συχνά ακόμη εξατομικευμένες, αλλά τείνουν ολοένα και περισσότερο προς την τυποποίηση.



Μοντέλα Ανάπτυξης ΥΝ

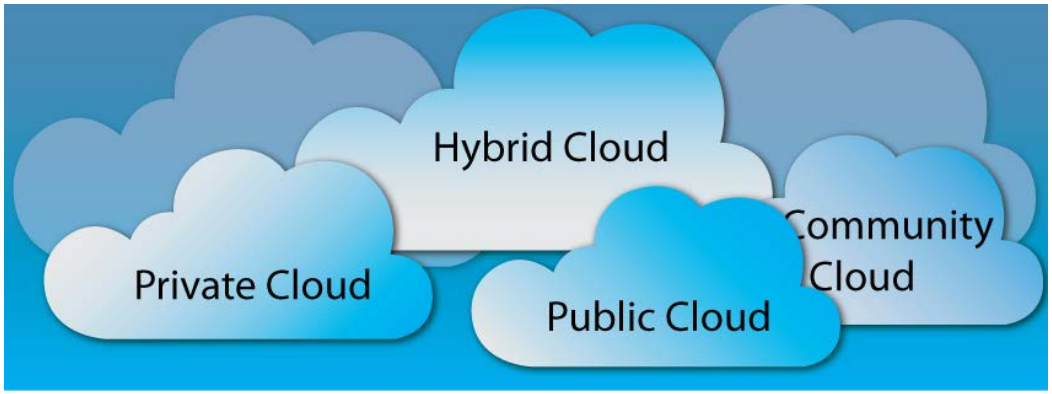
Τέσσερις τύποι ΥΝ

Υπάρχουν τέσσερις διαφορετικοί τύποι του υπολογιστικού νέφους.

Ο κάθε τύπος, περιγράφει το περιβάλλον ανάπτυξης, στο οποίο οι εφαρμογές και οι υπηρεσίες του νέφους μπορούν να εγκατασταθούν, έτσι ώστε να είναι διαθέσιμες στους χρήστες.

Το περιβάλλον αυτό αναφέρεται στην φυσική τοποθεσία του υπολογιστικού νέφους, στις εγκαταστάσεις των υποδομών και κατ' επέκταση σε οτιδήποτε μπορεί να επηρεάσει τους μηχανισμούς πρόσβασης των εφαρμογών, για τον εκάστοτε τύπο υπολογιστικού νέφους.

Οι τύποι είναι το δημόσιο νέφος, το ιδιωτικό νέφος, το υβριδικό νέφος και το κοινοτικό νέφος.



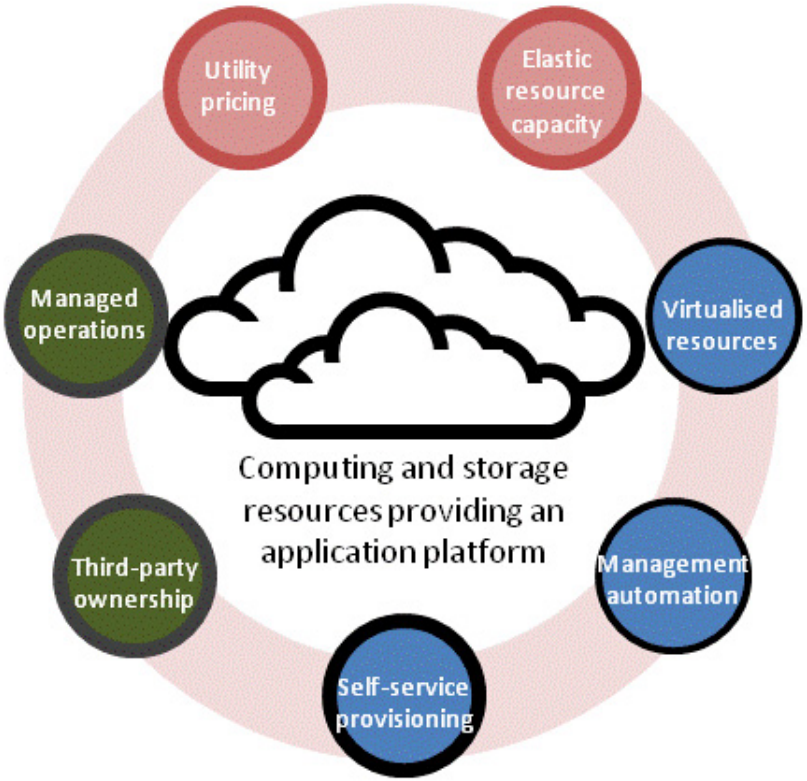
Δημόσιο νέφος (public cloud) (1/3)

Το Δημόσιο ή κοινό νέφος είναι και ο πιο γνωστός τύπος του υπολογιστικού νέφους και αναφέρεται σε ένα μοντέλο, στο οποίο οι εγκαταστάσεις υποδομής του και οι προσφερόμενες υπηρεσίες, παρέχονται από τους παρόχους του, σύμφωνα με τον διακανονισμό που έχει γίνει μεταξύ παρόχου – πελάτη.

Το μοντέλο βασίζεται σε παγκόσμια δίκτυα κέντρων πληροφοριών, προσφέροντας υπηρεσίες με πληρωμή ανά χρήση, δηλαδή οι βιομηχανίες ή τα πρόσωπα που χρησιμοποιούν τις υπηρεσίες του νέφους, χρεώνονται για όσο τις χρησιμοποιούν.

Δημόσιο νέφος (public cloud) (2/3)

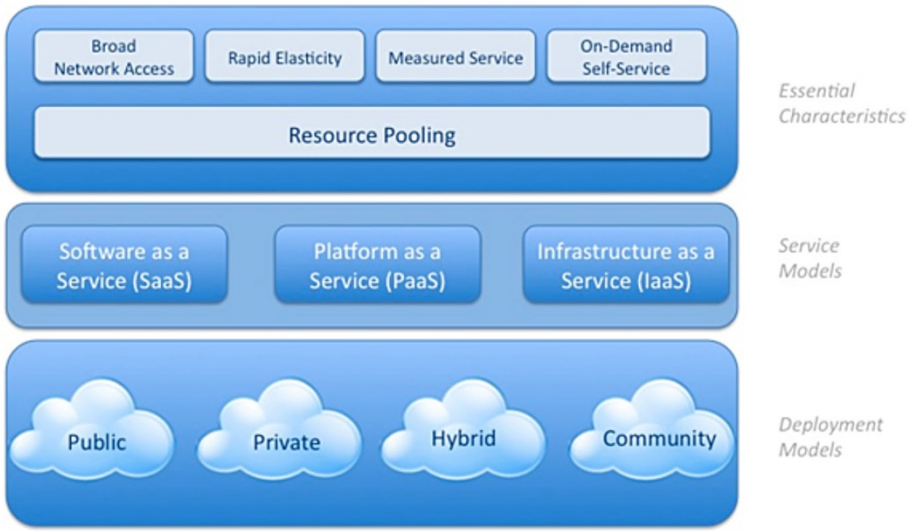
Αυτόματα, αυτό το γεγονός τον καθιστά, ως την λιγότερο ακριβή επιλογή φιλοξενίας εφαρμογών εφόσον υπάρχει μεγάλη ζήτηση από τους χρήστες, δεδομένης βέβαια της αγοραστικής τους δύναμης, την εκάστοτε χρονική στιγμή.



Δημόσιο νέφος (public cloud) (3/3)

Από τη φύση του το δημόσιο υπολογιστικό νέφος, χαρακτηρίζεται από μειωμένα κόστη εργασίας. Σε πολλές περιπτώσεις υπάρχουν και εντελώς δωρεάν προσφερόμενες υπηρεσίες, προκειμένου να προσελκύσουν νέους πελάτες.

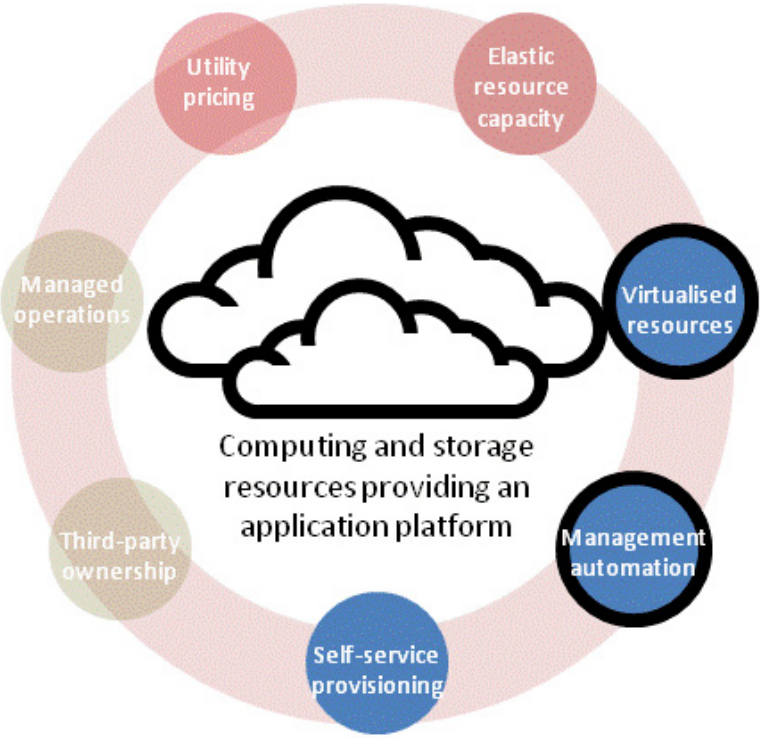
Το βασικό μειονέκτημα του μοντέλου, είναι η έλλειψη εμπιστοσύνης μεταξύ παρόχων και καταναλωτών, που πηγάζει κυρίως από θέματα ασφάλειας, τα οποία θα μελετηθούν εκτενέστερα παρακάτω.



Ιδιωτικό νέφος (Private cloud) (1/3)

Το ιδιωτικό νέφος είναι ένα κέντρο δεδομένων, που ανήκει σε έναν πάροχο υπηρεσιών ο οποίος είναι υπεύθυνος για την υποδομή και τη λειτουργία της πλατφόρμας του υπολογιστικού νέφους.

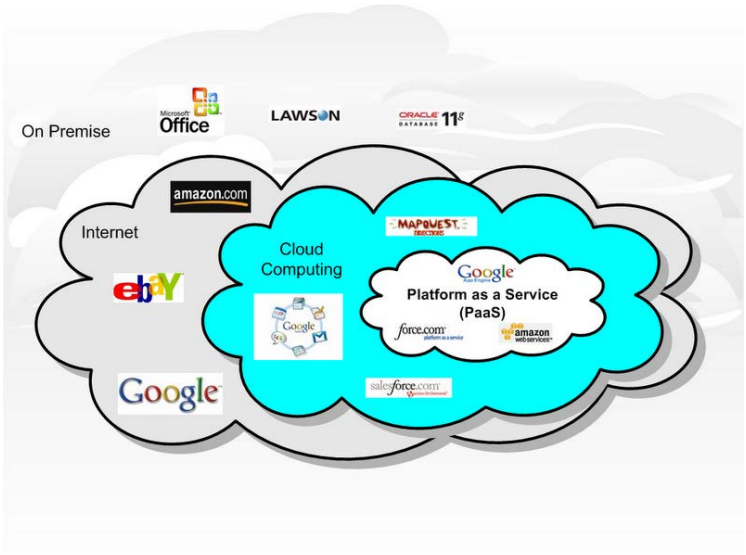
Έτσι, το μοντέλο αυτό προσφέρει στους χρήστες μεγαλύτερη ευελιξία και εμπνέει περισσότερη εμπιστοσύνη, μεταξύ παρόχου και πελάτη συγκριτικά με το δημόσιο που προαναφέρθηκε.



Ιδιωτικό νέφος (Private cloud) (2/3)

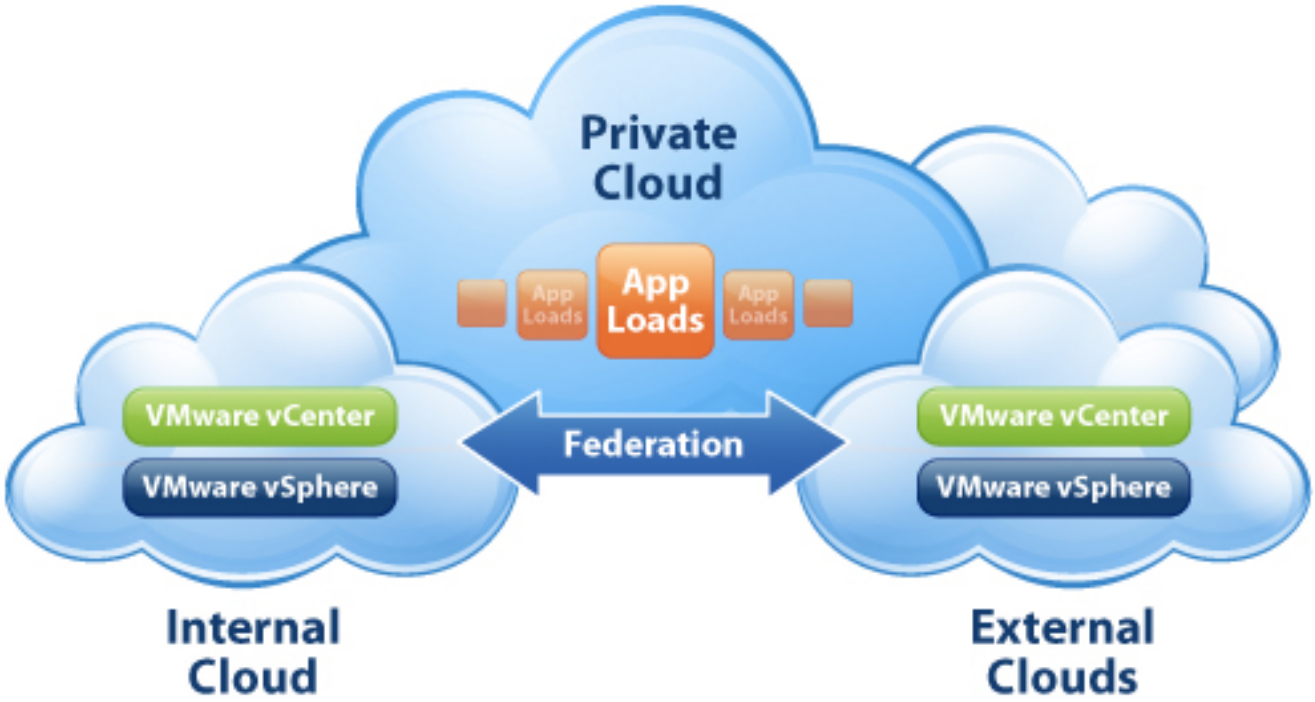
Αυτό συμβαίνει διότι, οι επιχειρήσεις μπορούν να εφαρμόσουν τις πολιτικές εκείνες που οι ίδιες επιλέγουν, σε θέματα που αφορούν την ασφάλεια και την προστασίας της ιδιωτικότητας των δεδομένων τους και τους μηχανισμούς πρόσβασης τους.

Η επιλογή αυτού του τύπου υπολογιστικού νέφους, είναι πιο δαπανηρή από άποψη απαιτούμενων πόρων αλλά και ανθρώπινου δυναμικού που απαιτείται, για τη διαχείριση των πόρων συγκριτικά με το δημόσιο νέφος.



Ιδιωτικό νέφος (Private cloud) (3/3)

Το ιδιωτικό νέφος, προτιμάται κυρίως από μεγάλες επιχειρήσεις ή αρχές οι οποίες επιλέγουν να χτίσουν τα δικά τους ιδιωτικά υπολογιστικά νέφη ,που βέβαια στηρίζονται στο υπάρχων υλικό υπολογιστών που διαθέτουν.



Υβριδικό νέφος (Hybrid cloud) (1/2)

Το υβριδικό μοντέλο του υπολογιστικού νέφους βρίσκεται, ανάμεσα στο δημόσιο και ιδιωτικό νέφος.

Συγκριτικά με το ιδιωτικό, είναι λιγότερο δαπανηρό και εξαλείφει την ανάγκη για ένα μοντέλο εμπιστοσύνης.

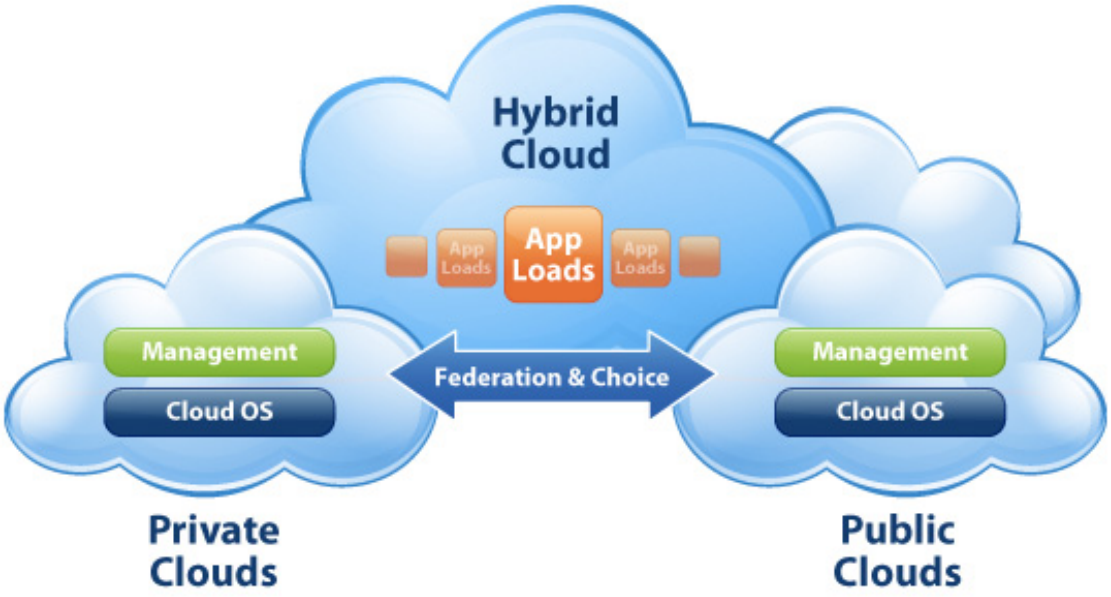
Κάποιο μέρος των δεδομένων αποθηκεύεται στο ιδιωτικό νέφος και κάποιο άλλο στο δημόσιο.

Έτσι, επιλέγονται τα σημαντικά και άκρως απόρρητα δεδομένα, για αποθήκευση στο ιδιωτικό μέρος του υπολογιστικού νέφους και αυτό είναι που συμβάλλει στην εμπιστοσύνη των χρηστών.

Από την άλλη, τα προσωπικά δεδομένα που είναι λιγότερο σημαντικά, αποθηκεύονται στο δημόσιο μέρος του υπολογιστικού νέφους, που αποτελεί πολύ πιο οικονομική λύση.

Υβριδικό νέφος (Hybrid cloud) (2/2)

Η παράλληλη χρήση των δυο αυτών μοντέλων, απαιτεί δια-λειτουργικότητα και δυνατότητα μεταφοράς, τόσο δεδομένων, όσο και ολόκληρων εφαρμογών μεταξύ των μοντέλων, έτσι ώστε να επιτρέπεται η άμεση επικοινωνία τους.

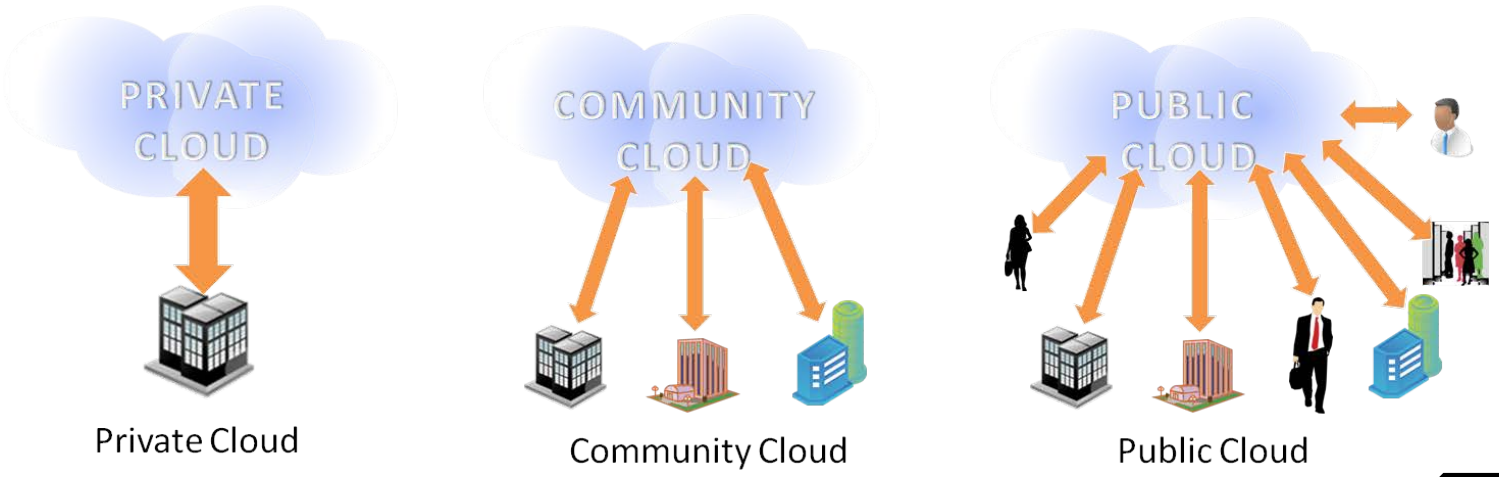


Κοινοτικό νέφος (Community cloud) (1/3)

Σε αυτόν τον τύπο, συναντούμε πολλές ομοιότητες με τα εξωτερικά δίκτυα (extranets).

Έχει δυνατότητες ανάλογες με τη ζήτηση των χρηστών.

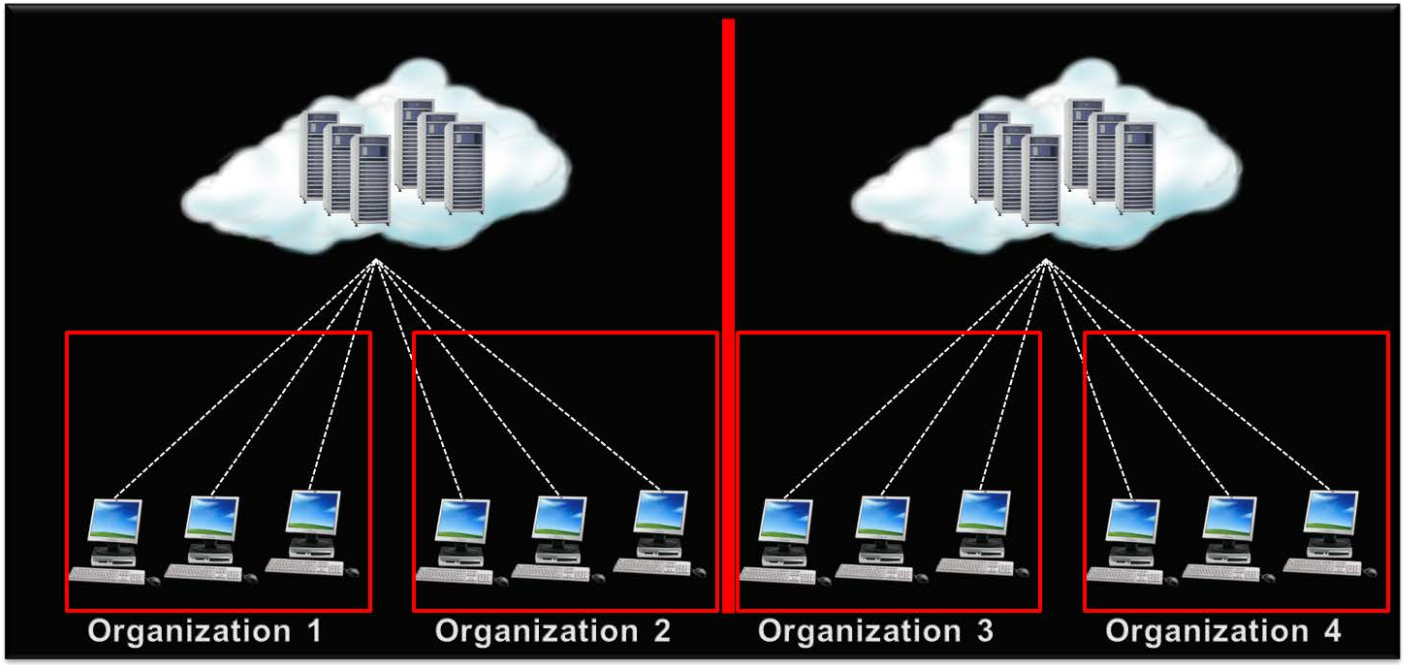
Πολλές επιχειρήσεις που έχουν κοινούς στόχους και παρόμοιους σκοπούς λειτουργίας, μπορούν να απαρτίσουν μια κοινότητα και να χτίσουν ένα κέντρο δεδομένων στο υπολογιστικό νέφος, το οποίο φυσικά μοιράζονται και να έχουν πρόσβαση σε αυτό, όλα τα μέλη της κοινότητας.



Κοινοτικό νέφος (Community cloud) (2/3)

Αυτό το μοντέλο, στοχεύει στη μείωση των ελλείψεων των μεμονωμένων τεχνολογιών υποδομής, και στη μείωση του κόστους διοίκησης.

Μπορούν να δημιουργηθούν πολλές κοινότητες διαφορετικής φύσεως σε ένα κοινοτικό σύννεφο.



Κοινοτικό νέφος (Community cloud) (3/3)

Το κοινοτικό νέφος, στηρίζεται κυρίως στις σχέσεις εμπιστοσύνης μεταξύ των μελών του γεγονός που καθιστά το συγκεκριμένο μοντέλο περισσότερο έμπιστο, συγκριτικά με το δημόσιο υπολογιστικό νέφος και λιγότερο ακριβό από το ιδιωτικό υπολογιστικό νέφος.

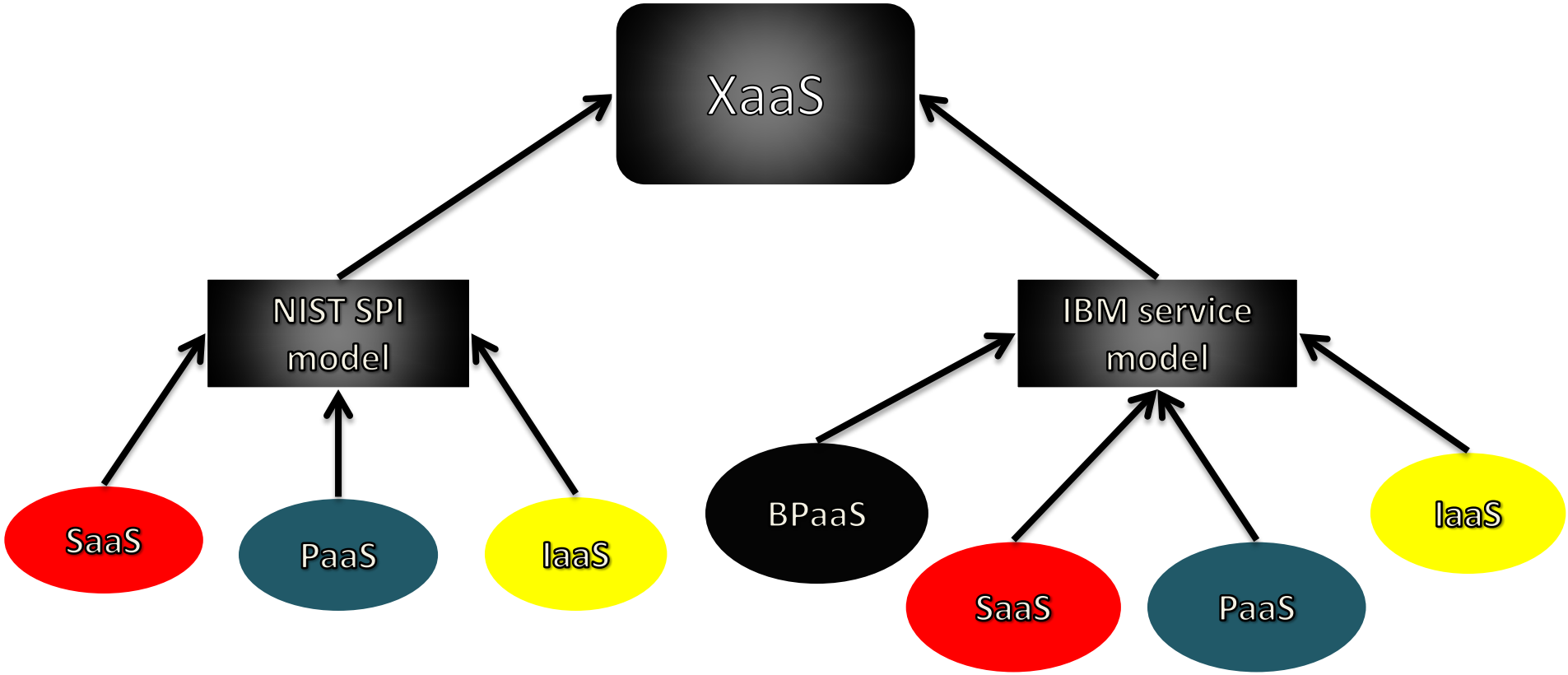
Ακόμα, το κοινοτικό νέφος, παρέχει στους χρήστες του μεγάλη δυνατότητα ελέγχου των κοινών πόρων υποδομής που χρησιμοποιούνται.

Η βασικότερη δυσκολία είναι η συμμόρφωση όλων των χρηστών με τους κανονισμούς. Συνήθως είναι δύσκολο να

επιτευχθεί συμφωνία απόψεων, στον τρόπο με τον οποίο διατίθενται και χρησιμοποιούνται οι παρεχόμενες υπηρεσίες.

Μοντέλα Υπηρεσιών ΥΝ

Δύο Βασικά Μοντέλα Υπηρεσιών



Ονομασία μοντέλων (1/2)

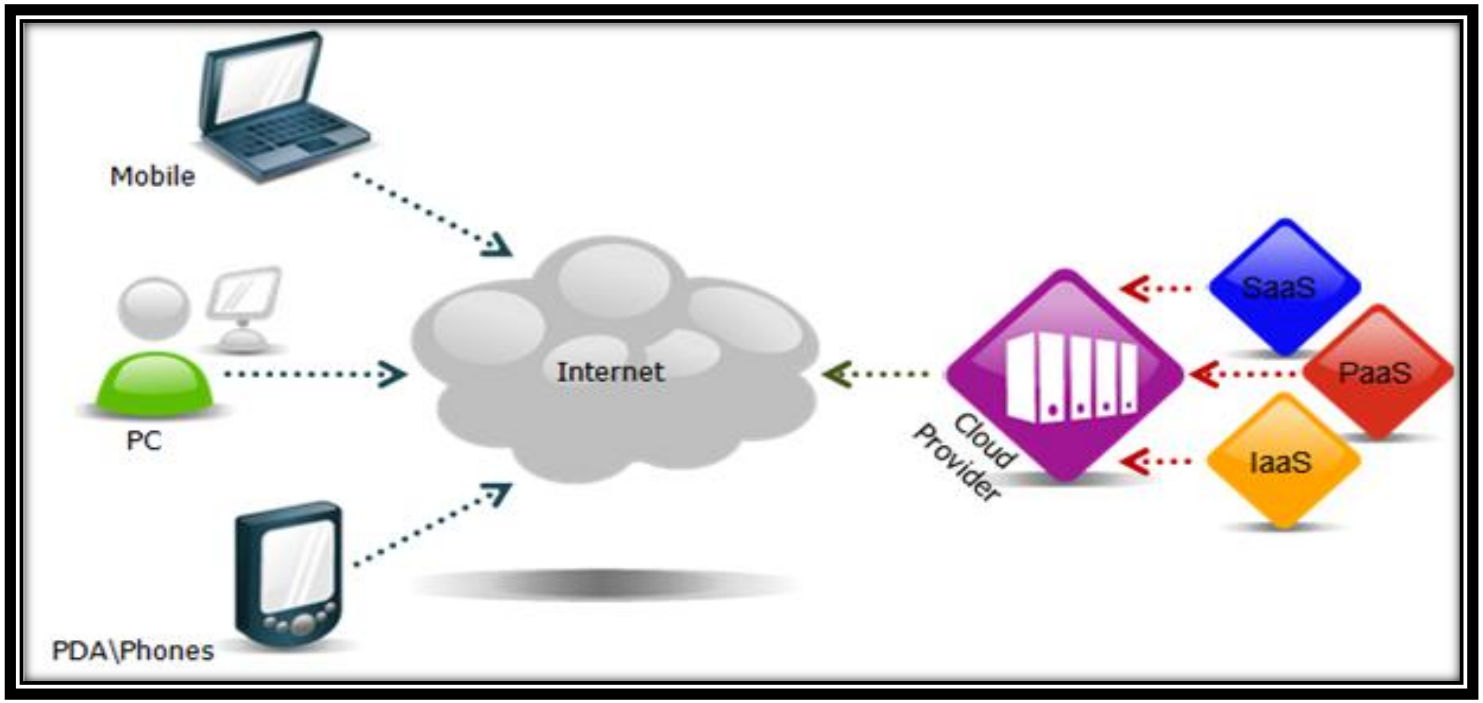
Τα μοντέλα, πολλές φορές, συναντώνται στη βιβλιογραφία ως ιεραρχική απεικόνιση των προσφερόμενων υπηρεσιών του σύννεφου, ως μοντέλα παροχής υπηρεσιών του υπολογιστικού νέφους ή ως υπηρεσίες πολύ-επίπεδης αρχιτεκτονικής του νέφους, σε αναλογία με το δίκτυο πολύ-επίπεδης αρχιτεκτονικής.

Τα μοντέλα υπηρεσιών, προσπαθούν να κατατάξουν οτιδήποτε οι πάροχοι προσφέρουν σαν υπηρεσία και αυτό στη βιβλιογραφία συμβολίζεται ως **X**aaS.

Ονομασία μοντέλων (2/2)

Το X μπορεί να είναι οποιαδήποτε αυθαίρετη υπηρεσία, όπως για παράδειγμα οι υποδομές, το λογισμικό, η αποθήκευση κ.α.

Τα υπόλοιπα γράμματα του συμβολισμού(X**aaS**), προκύπτουν από την αγγλική έκφραση “**as a service**”.



Ορισμός των μοντέλων

Ένα μοντέλο προσφερόμενων υπηρεσιών υπολογιστικού νέφους αντιπροσωπεύει μια πολύ-επίπεδη, υψηλού επιπέδου άντληση, από τις κύριες κατηγορίες των υπηρεσιών που υπάρχουν στο μοντέλο και περιγράφει πως αυτά τα πολλά επίπεδα συνδέονται μεταξύ τους.

Τα επίπεδα διαφέρουν ως προς τη διαχείριση του πεδίου εφαρμογής που καθορίζει ο πάροχος. Έτσι ένας χρήστης ο οποίος βρίσκεται στα ανώτερα επίπεδα δεν μπορεί να παρακάμψει τις διασυνδέσεις που βρίσκονται στο ακριβώς από κάτω επίπεδο, έτσι ώστε να έχει άμεση πρόσβαση στους πόρους.

Τα διαφορετικά επίπεδα, βοηθούν τους παρόχους να έχουν μεγαλύτερη ευελιξία στην διαχείριση των πόρων, καθώς και μεγαλύτερη δυνατότητα ελέγχου και ασφάλειας.

Δύο μεγάλες κατηγορίες

Οι δύο μεγάλες κατηγορίες μοντέλων υπηρεσιών είναι το NIST SPI model και το IBM service model.

Το πρώτο είναι ένα μοντέλο τριών επιπέδων υπηρεσιών, ενώ το δεύτερο τεσσάρων επιπέδων υπηρεσιών.

Οι διαφορές τους έχουν να κάνουν με τον χρόνο που προτάθηκαν.

Οι διαφορές μεταξύ των μοντέλων δεν αλληλοσυγκρούονται μεταξύ τους, αλλά λειτουργούν συμπληρωματικά.

IBM®

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

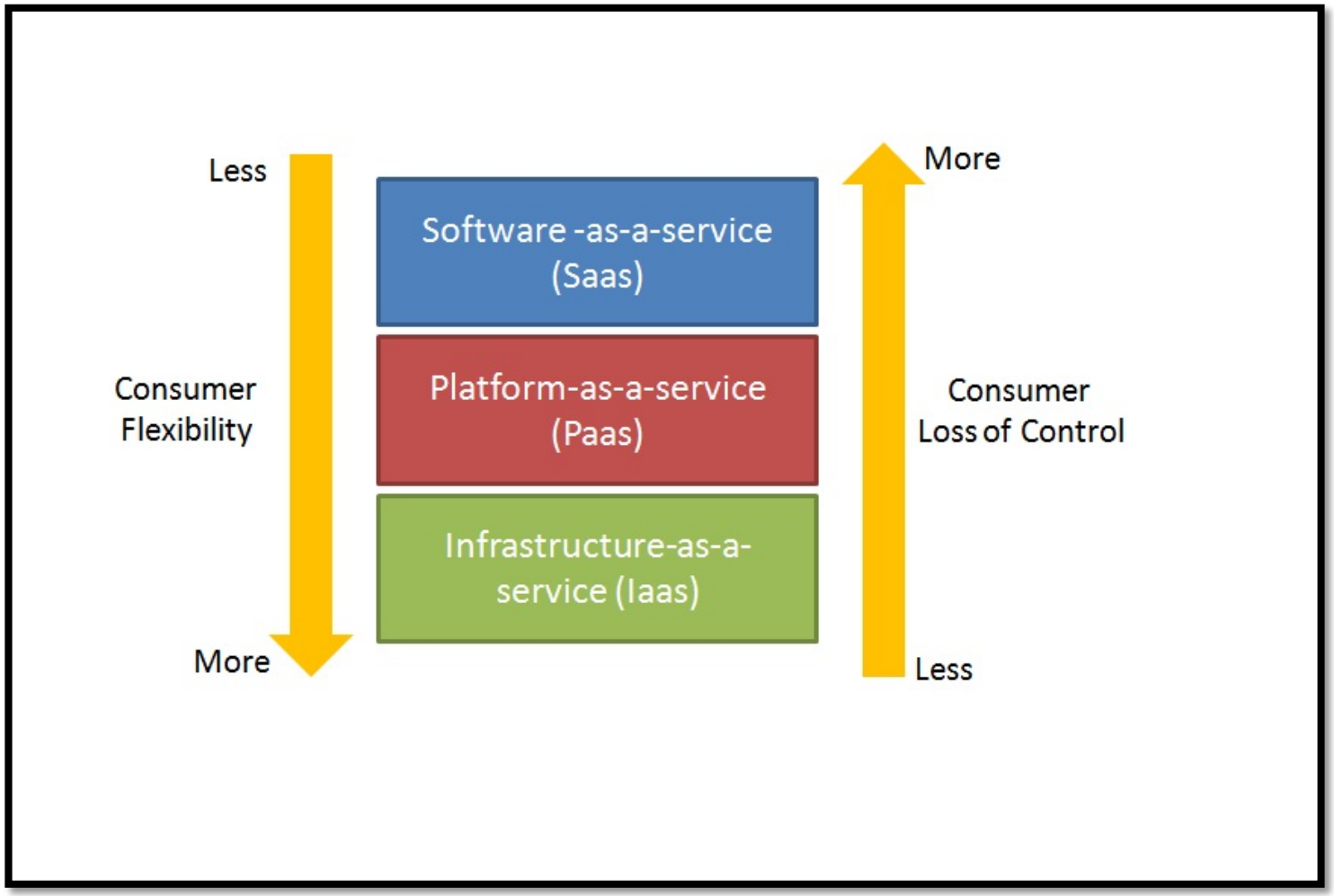
Μοντέλο SPI

Πήρε το όνομα του από τα αρχικά των λέξεων Service, Platform και Infrastructure.

Κύρια λειτουργία του είναι, η ταξινόμηση των προσφερόμενων υπηρεσιών του παρόχου σε τρείς κατηγορίες (επίπεδα) οι οποίες είναι οι εξής:

- Software as a Service/Υπηρεσίες Λογισμικού (SaaS)
- Platform as a Service/Υπηρεσίες Πλατφόρμας (PaaS)
- Infrastructure as a Service/Υποδομή ως υπηρεσία (IaaS)

Τρία επίπεδα του SPI



SPI: SaaS (1/2)

Υπηρεσίες Λογισμικού (SaaS): Ο πελάτης και τελικός χρήστης έχει πρόσβαση και μπορεί να χρησιμοποιεί κάποια εφαρμογή παροχής λογισμικού, η οποία φιλοξενείται, αναπτύσσεται και διαχειρίζεται, από τον πάροχο.

Μια υπηρεσία λογισμικού ισοδυναμεί, με εφαρμογές που κανονικά θα έπρεπε να εγκατασταθούν και να τρέξουν στην επιφάνεια εργασίας του χρήστη.

Οι χρήστες έχουν περιορισμένο έλεγχο της SaaS υπηρεσίας. Περιορίζονται ως προς το πώς μπορούν να χρησιμοποιήσουν και να αλληλεπιδράσουν με την εφαρμογή.

Η πρόσβαση στην εφαρμογή, γίνεται συνήθως μέσω κάποιου προγράμματος, όπως ο Web browser (φυλλομετρητής).

SPI: SaaS (2/2)

Οι SaaS υπηρεσίες είναι ικανές να προσφέρουν, ένα πλήρες λογισμικό απομακρυσμένου περιβάλλοντος στους πελάτες.

Οι περισσότερες υπηρεσίες είναι συγκεκριμένες εφαρμογές και όχι γενικές υπηρεσίες λογισμικού.

Παραδείγματα SaaS υπηρεσιών, είναι οι υπηρεσίες περιεχομένου, υπηρεσίες ηλεκτρονικού ταχυδρομείου, καθώς και επιχειρηματικές εφαρμογές, όπως για παράδειγμα οι εφαρμογές διαχείρισης σχέσεων με τους πελάτες.

SPI: PaaS (1/3)

Υπηρεσίες Πλατφόρμας (PaaS): Ο χρήστης της υπηρεσίας, ο οποίος συνήθως είναι ένας SaaS πάροχος, ή ένας προγραμματιστής του σύννεφου, ή ο διαχειριστής έχει τη δυνατότητα να καθορίσει, να αναπτύξει, να διαχειριστεί και να παρακολουθήσει τις εφαρμογές του νέφους.

Αυτό σημαίνει ότι οι χρήστες, δημιουργούν εφαρμογές μέσα στο νέφος επωφελούμενοι τη δυνατότητα του, να παρέχει αυτόματα πρόσθετους πόρους υπολογιστικούς, αλλά και πόρους αποθήκευσης, όταν χρειάζονται.

SPI: PaaS (2/3)

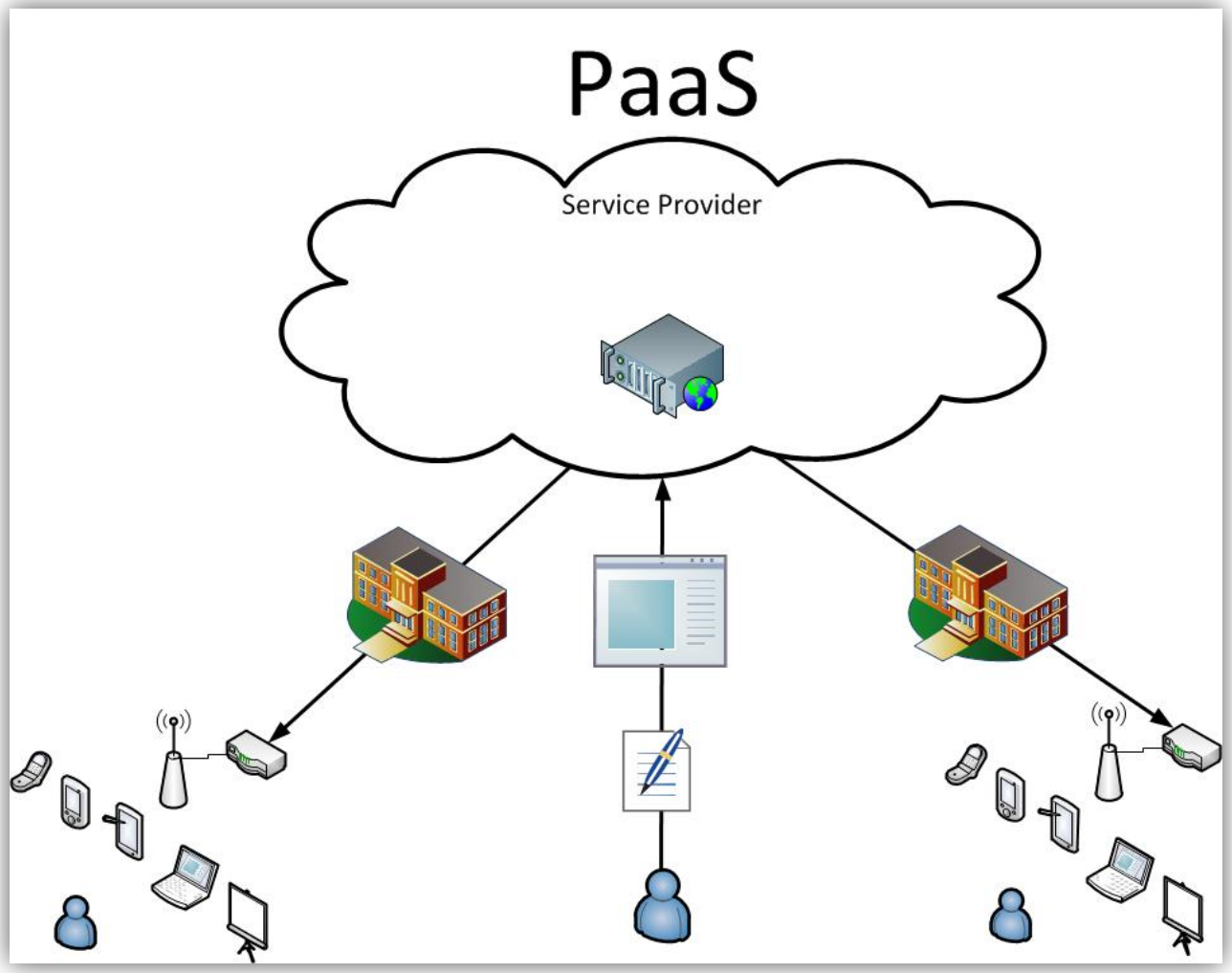
Από την άλλη μεριά δεν επιτρέπεται ο έλεγχος της υποδομής του νέφους από τον χρήστη.

Τα λειτουργικά συστήματα και τα πλαίσια εφαρμογών, είναι κομμάτι του PaaS επιπέδου.

Ενδεικτικά, παραδείγματα PaaS υπηρεσιών είναι τα εξής: Google app Engine, Microsoft Windows Azure, Mozilla, Bespin κ.α.

mozilla LABS
Bespin

SPI: PaaS (3/3)



SPI: IaaS (1/2)

Υποδομή ως υπηρεσία (IaaS): Επιτρέπει στους χρήστες των υπηρεσιών, που συνήθως είναι PaaS πάροχοι, να εκμισθώνουν δυνατότητες βάση της ζήτησης.

Στόχος είναι να καταργηθεί η ανάγκη των πελατών να έχουν δικά τους κέντρα δεδομένων.

Έτσι, οι IaaS πάροχοι εκμισθώνουν στους πελάτες αποθηκευτικό διαδικτυακό χώρο, στους διακομιστές τους και σε διαδικτυακές συνδέσεις.

Κατ' επέκταση, οι πελάτες έχουν πρόσβαση σε βασικούς υπολογιστικούς πόρους που μπορούν να χρησιμοποιηθούν, για να αναπτυχθούν και να λειτουργήσουν πλατφόρμες, όπως πλατφόρμες λειτουργικών συστημάτων, αλλά και εφαρμογές που αναπτύχθηκαν στις πλατφόρμες αυτές.

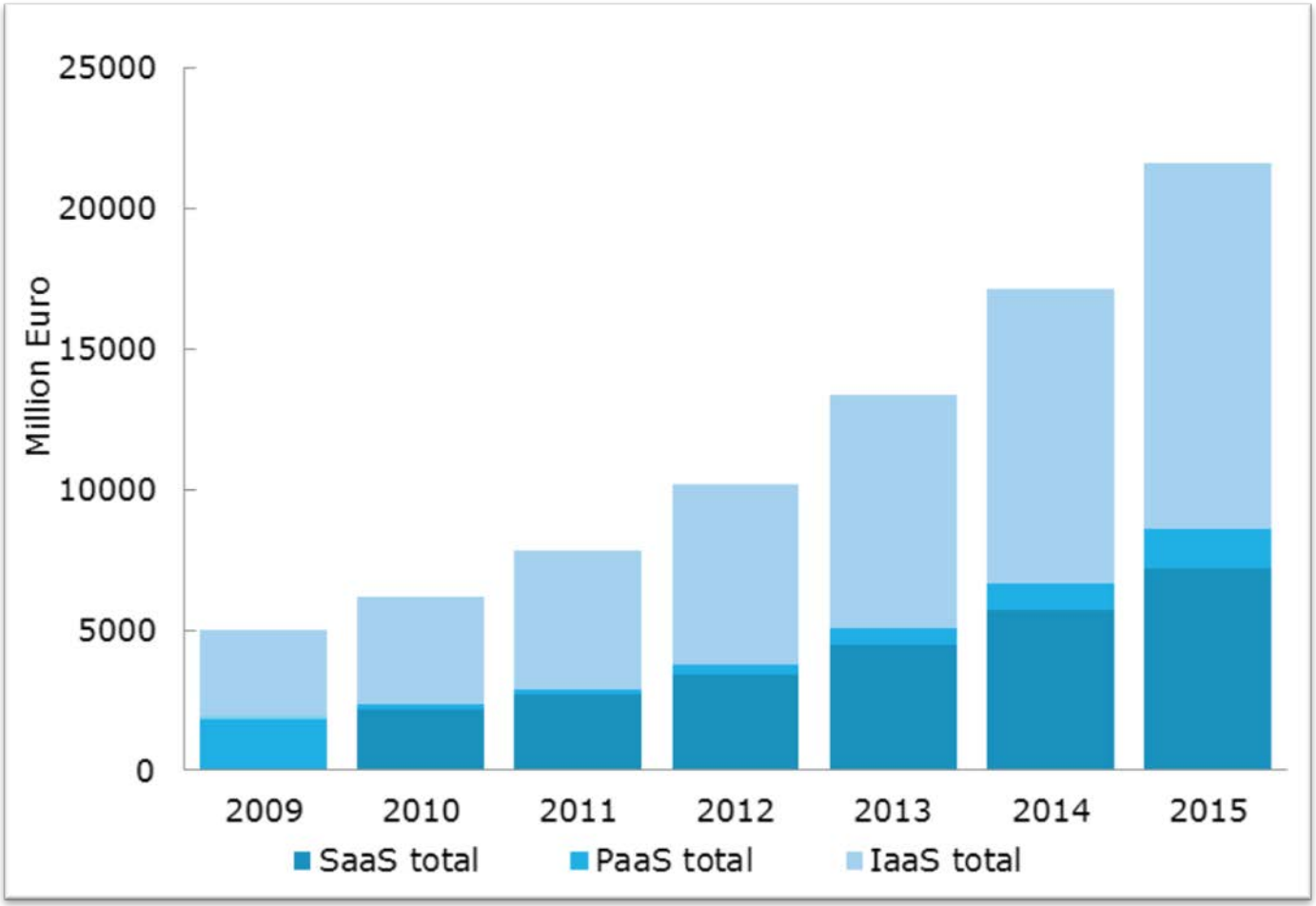
SPI: IaaS (2/2)

Και σε αυτήν την περίπτωση, η πρόσβαση στους πόρους από τους χρήστες δεν είναι άμεση, (οι IaaS πάροχοι έχουν στην κατοχή τους και διατηρούν το υλικό) αλλά τους δίνεται η δυνατότητα να επιλέξουν και να ρυθμίσουν τους πόρους που απαιτούνται, βάση των αναγκών τους, αφού μπορούν να τους εκμισθώσουν από τους παρόχους.

Παράδειγμα IaaS υπηρεσιών είναι οι υπηρεσίες διαδικτύου της Amazon.

amazon.com®
and you're done.™

Αξία των μοντέλων έως το 2015



Γραφική απεικόνιση της εκτιμώμενης αξίας, των μοντέλων υπηρεσιών του υπολογιστικού νέφους στην Ευρώπη, μετρημένη σε εκατομμύρια ευρώ, από το 2009 έως το 2015.

Μοντέλο IBM

Σύμφωνα με την αναφορά της αρχιτεκτονικής του IBM υπολογιστικού νέφους, ένα μοντέλο IBM αποτελείται από τέσσερα επίπεδα υπηρεσιών.

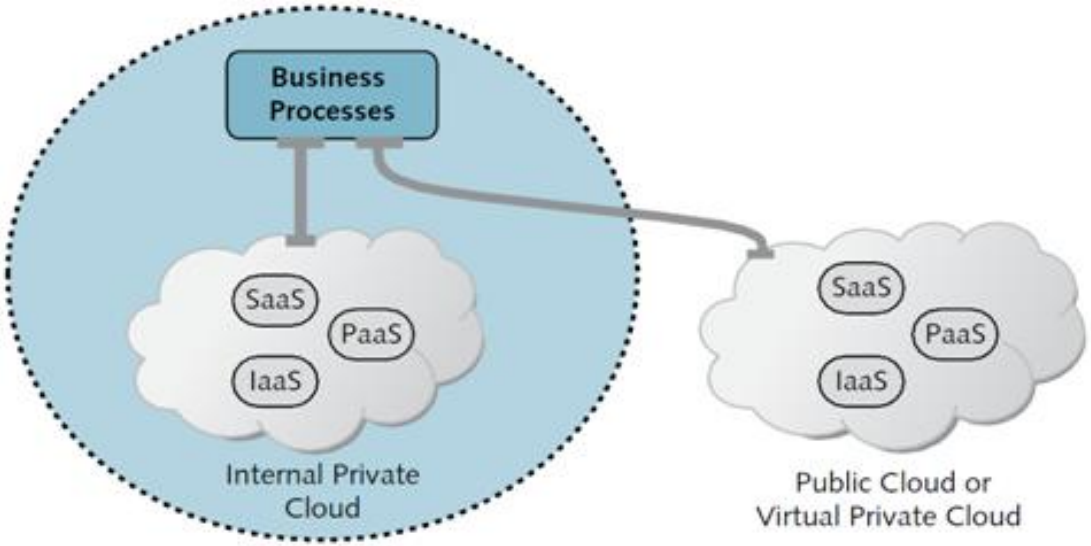
Ξεκινώντας την αναφορά, από πάνω προς τα κάτω, τα επίπεδα αυτά είναι:

- Business Process as a Service
- Software as a Service
- Platform as a Service
- Infrastructure as a Service

Το επιπλέον επίπεδο

Τα τελευταία τρία επίπεδα είναι ακριβώς τα ίδια με το προηγούμενο μοντέλο που αναλύθηκε, το SPI.

Η μοναδική διαφορά των δυο μοντέλων, βρίσκεται στο επιπλέον επίπεδο που διαθέτει το IBM, το Business Process as a Service/Υπηρεσία Επιχειρηματικής Διαδικασίας (BPaaS).



IBM: BPaaS (1/2)

Υπηρεσία Επιχειρηματικής Διαδικασίας (BPaaS): Επιτρέπει στον πελάτη, ο οποίος μπορεί να είναι ένας απλός χρήστης ή ένας διευθυντής επιχειρηματικών διαδικασιών, να σχεδιάζει, να διαχειρίζεται και να ενσωματώνει συνεργατικές δραστηριότητες, που στηρίζονται στις SaaS υπηρεσίες και βρίσκονται ένα επίπεδο παρακάτω, έτσι ώστε να επιτευχθεί ένας επιχειρηματικός στόχος.

Το συγκεκριμένο μοντέλο ταξινομεί οποιαδήποτε υπηρεσία επιχειρηματικής διαδικασίας, ως BPaaS υπηρεσία, εάν πρόκειται αυστηρά για επιχειρηματική διαδικασία η οποία επιτελείται, μέσα από το υπολογιστικό νέφος και βασίζεται στα κύρια χαρακτηριστικά του, όπως αυτά ορίστηκαν από τον NIST ορισμό.

IBM: BPaaS (2/2)

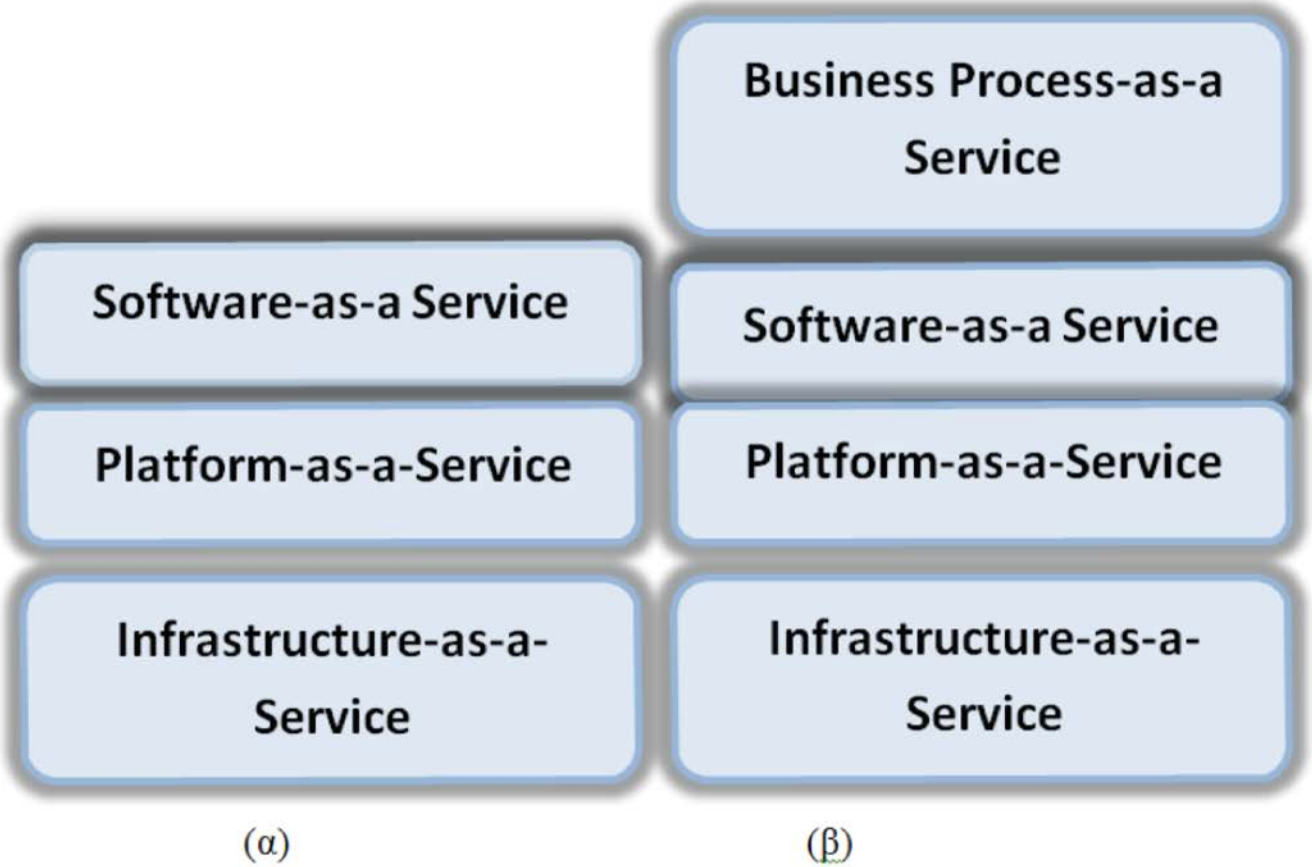
Ο BPaaS πάροχος προσφέρει εργαλεία για πρόσβαση και αξιοποίηση των πόρων στο BPaaS επίπεδο.

Οι χρήστες, δεν είναι αναγκαίο να έχουν πρόσβαση στα υποκείμενα επίπεδα.

Ο πάροχος είναι υπεύθυνος για τις επιχειρηματικές λειτουργίες.

Μερικά παραδείγματα BPaaS υπηρεσιών, είναι οι διαδικασίες διαχείρισης των επιδομάτων των εργαζομένων, ή οι διαδικασίες δοκιμής λογισμικού, συμπεριλαμβανομένων και των ελέγχων του προσωπικού, που παρέχονται μέσω των υπηρεσιών του υπολογιστικού νέφους.

Επίπεδα SPI και IBM μοντέλων



Εικόνα 3: (α) SPI μοντέλο vs (β) IBM μοντέλο

Δύο ακόμα μοντέλα

Όπως αναφέρθηκε και νωρίτερα, υπάρχουν πολλά διαφορετικά μοντέλα υπολογιστικών νεφών στην αγορά.

Αυτό συμβαίνει γιατί, ο κάθε πάροχος χρησιμοποιεί και διαφορετικό μοντέλο, στοχεύοντας στην προώθηση των υπηρεσιών που προσφέρει.

Στην πραγματικότητα οι διαφορές μεταξύ των μοντέλων, είναι πολύ μικρές και ουσιαστικά τα μοντέλα συμπληρώνουν το ένα, το άλλο.

Άλλα δύο μοντέλα που αναφέρονται στη βιβλιογραφία είναι το *Hardware as a Service (HaaS)* και το *Database as a Service (DaaS)*.

HaaS (1/2)

Στο ***HaaS*** μοντέλο ο πάροχος επιτρέπει στους πελάτες του να ενοικιάζουν hardware.

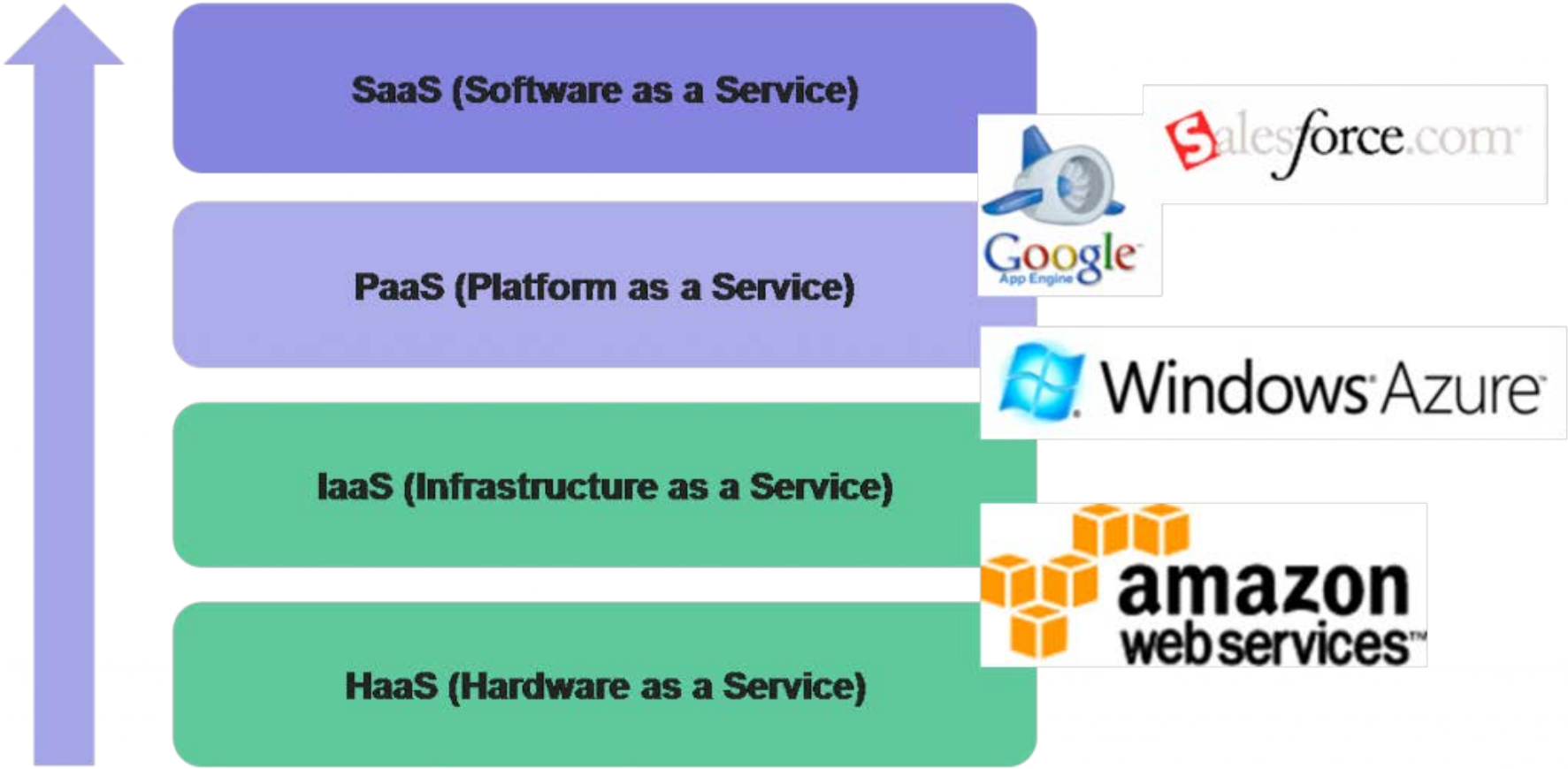
Με άλλα λόγια, πρόκειται για την ενοικίαση υλικού, που επιτρέπει στους χρήστες τη δημιουργία data-centers χωρίς να πρέπει να αγοράσουν το υλικό που απαιτείται.

Συνοπτικά το HaaS επιτρέπει να νοικιαστούν ο χώρος σε έναν διακομιστή, ο εξοπλισμός δικτύου, η μνήμη, η χρήση της CPU και ο χώρος αποθήκευσης.

Ο εξοπλισμός αυτός μπορεί να χρησιμοποιείται ταυτόχρονα από πολλαπλούς χρήστες και οι πόροι χρεώνονται ανάλογα με την χρήση τους.

HaaS (2/2)

Στις περισσότερες βιβλιογραφίες το HaaS μοντέλο τοποθετείται κάτω από το IaaS.



DaaS

Η κεντρική ιδέα του *DaaS* μοντέλου είναι να αποφευχθεί το μεγάλο κόστος για την λειτουργία μιας ιδιωτικής βάσης δεδομένων.

Δεν υπάρχει η ανάγκη για κάποιο πλεονασματικό σύστημα στο οποίο να αποθηκεύεται η βάση δεδομένων και να απαιτεί συντήρηση, καθώς επίσης δεν χρειάζεται να αγοραστεί το υλικό, το λογισμικό και το κόστος συντήρησης του υλικού για την βάση δεδομένων.

Η βάση δεδομένων παραμένει λειτουργική και αποτελεσματική παρόλο που δεν υπάρχει τοπικά.

Η βάση δεδομένων μπορεί να συνεργαστεί και με άλλες υπηρεσίες ώστε να αποκτήσει μεγαλύτερη αξία.

Θέματα Ασφαλείας

Βασικά Θέματα Ασφαλείας ΥΝ

Το υπολογιστικό νέφος είναι μια πρόσφατη τεχνολογική εξέλιξη, παρόλα αυτά όμως, επειδή η διάδοση του είναι μεγάλη και είναι ευρέως χρησιμοποιούμενο υπάρχουν πολλές κριτικές από τους χρήστες του βασισμένες στις εμπειρίες τους, σχετικές με τα επίπεδα ασφάλειας.

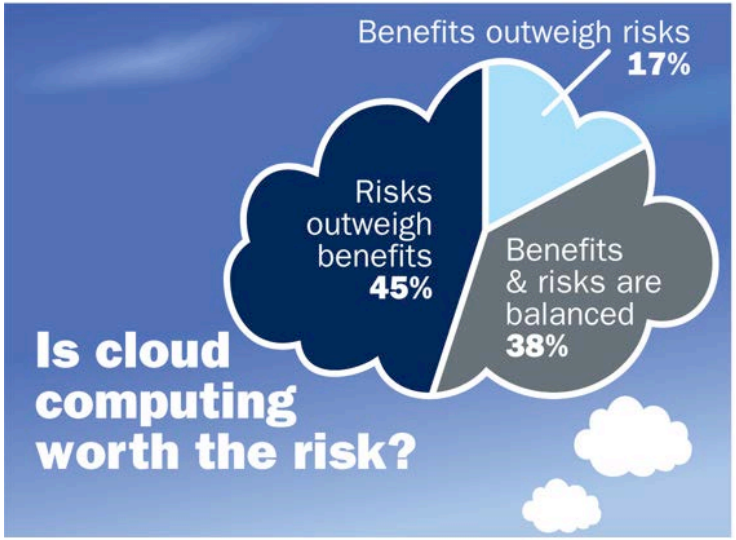
Παράλληλα, υπάρχουν πολλοί ερευνητές που μελετούν κατά καιρούς τα κενά που υπάρχουν στην ασφάλεια των σύννεφων.

Τα κενά αυτά, συνήθως αναφέρονται στις απειλές, στους κινδύνους και στην εμπιστοσύνη.

Ασφάλεια μοντέλων υπηρεσιών (1/3)

Στο περιβάλλον του νέφους, τα μοντέλα έχουν διαφορετικές απαιτήσεις σε θέματα ασφαλείας.

Το IaaS είναι το μοντέλο που αποτελεί θεμέλιο, διότι σε αυτό βασίζονται όλες οι προσφερόμενες υπηρεσίες, με το PaaS μοντέλο να χτίζεται πάνω του και με τη σειρά του το SaaS, να χτίζεται πάνω στο PaaS.



Ασφάλεια μοντέλων υπηρεσιών (2/3)

Με τον ίδιο τρόπο λοιπόν, που μεταφέρονται οι δυνατότητες από το ένα μοντέλο στο άλλο, έτσι μεταφέρονται και οι κίνδυνοι και τα διάφορα ζητήματα που προκύπτουν σε θέματα ασφαλείας.

Έτσι, εάν ο πάροχος φροντίσει για την αρχιτεκτονική ασφαλείας από τα χαμηλότερα επίπεδα, τότε και οι χρήστες γίνονται περισσότερο υπεύθυνοι σε ότι έχει να κάνει με τη διαχείριση και την εφαρμογή των δυνατοτήτων ασφαλείας.

Ασφάλεια μοντέλων υπηρεσιών (3/3)

Οι επιχειρήσεις που χρησιμοποιούν το υπολογιστικό νέφος ως υπηρεσία υποδομής, εξετάζουν αυστηρά τα θέματα ασφάλειας και εμπιστοσύνης των εφαρμογών που χρησιμοποιούν, τα οποία είναι ζωτικής σημασίας για την εύρυθμη λειτουργία τους.

Ωστόσο όμως η ασφάλεια των προσωπικών δεδομένων μέσα στο νέφος δεν μπορεί να εγγυηθεί, καθώς παρέχονται διαφορετικές υπηρεσίες (SaaS, PaaS, IaaS) οι οποίες ακολουθούν και διαφορετικές πολιτικές ασφαλείας.

Ασφάλεια στο SaaS

Ο πελάτης βασίζεται στον πάροχο για την κάλυψη των κατάλληλων μέτρων ασφαλείας.

Ο πάροχος πρέπει να φροντίσει να μην μπορούν οι χρήστες να δουν, ο ένας τα προσωπικά δεδομένα και αρχεία του άλλου.

Οι πελάτες δεν μπορούν να είναι απόλυτα σίγουροι ότι ο πάροχος λαμβάνει τα κατάλληλα μέτρα, για να το πετύχει αυτό και παράλληλα δεν μπορούν να είναι σίγουροι ότι οι εφαρμογές τους θα είναι διαθέσιμες όταν εκείνοι τις χρειάζονται.

Τρωτά σημεία

Τα δεδομένα των επιχειρήσεων αποθηκεύονται στο κέντρο δεδομένων του παρόχου, μαζί με δεδομένα άλλων επιχειρήσεων και αυτό το γεγονός καθιστά ευκολότερη την παραβίαση τους.

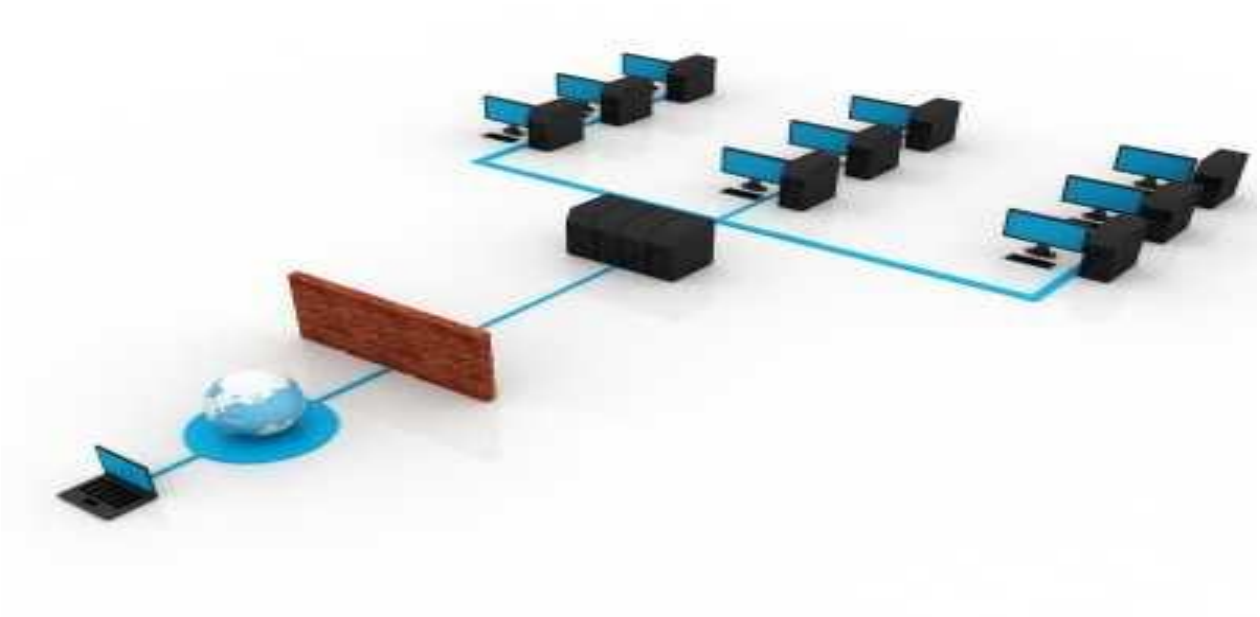
Επιπρόσθετα, εάν ο πάροχος χρησιμοποιεί υπηρεσίες δημόσιου νέφους, τότε τα δεδομένα των επιχειρήσεων αποθηκεύονται με δεδομένα SaaS εφαρμογών που δεν σχετίζονται καθόλου με τις επιχειρήσεις.

Ο πάροχος του υπολογιστικού νέφους μπορεί να αποθηκεύει τα προσωπικά δεδομένα και αρχεία των πελατών του, σε διάφορες τοποθεσίες σε πολλές χώρες προκειμένου να διατηρεί υψηλή διαθεσιμότητα.

Υποχρεώσεις

Κατά συνέπεια, υπάρχει μια μεγάλη δυσφορία σχετικά με το πώς τα δεδομένα αυτά φυλάσσονται.

Υπάρχουν έντονες ανησυχίες, σχετικά με τις παραβιάσεις των δεδομένων, στα τρωτά σημεία των εφαρμογών που μπορούν να οδηγήσουν σε οικονομικές και νομικές υποχρεώσεις.



Σημεία κλειδιά (1/2)

Τα σημεία κλειδιά του SaaS μοντέλου που πρέπει να αντιμετωπίζονται με ιδιαίτερη προσοχή και υπευθυνότητα από τους παρόχους του υπολογιστικού νέφους, είναι τα εξής:

- Ασφάλεια Δεδομένων
- Ασφάλεια Δικτύων
- Δεδομένα Τοποθεσίας
- Ακεραιότητα Δεδομένων
- Διαχωρισμός Δεδομένων
- Πρόσβαση Δεδομένων
- Έλεγχος Ταυτότητας και Εξουσιοδότησης

Σημεία κλειδιά (2/2)

Τα σημεία κλειδιά του SaaS μοντέλου που πρέπει να αντιμετωπίζονται με ιδιαίτερη προσοχή και υπευθυνότητα από τους παρόχους του υπολογιστικού νέφους, είναι τα εξής:

- Εμπιστευτικότητα των Δεδομένων
- Ασφάλεια Εφαρμογών Διαδικτύου
- Παραβίαση Δεδομένων
- Ευπάθεια Εικονικοποίησης
- Διαθεσιμότητα Εφαρμογών και Δεδομένων
- Δημιουργία Εγγράφων Ασφαλείας

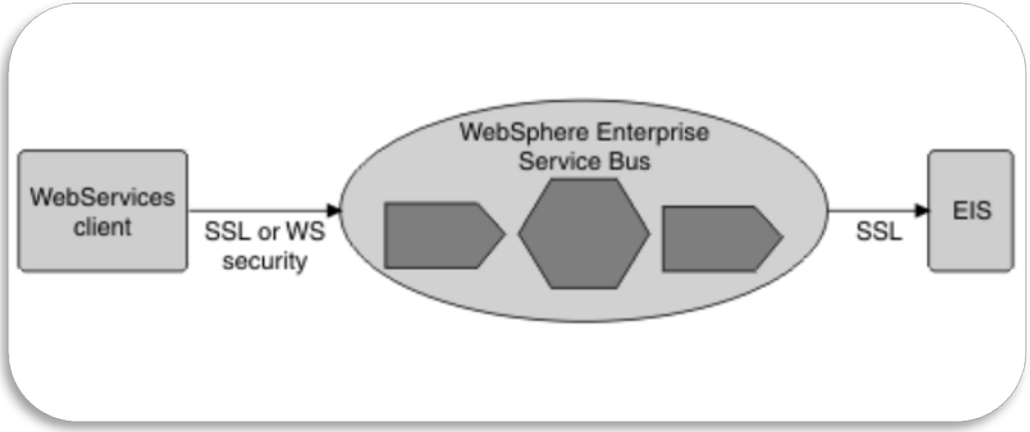
Ασφάλεια στο PaaS

Το PaaS μοντέλο βρίσκεται ένα επίπεδο πάνω από το IaaS και έτσι προσφέρει στους προγραμματιστές ένα προγραμματιστικό περιβάλλον το οποίο μπορεί να αξιοποιηθεί για την δημιουργία εφαρμογών χωρίς να έχουν καμία ιδέα για το τι συμβαίνει στο παρακάτω επίπεδο υπηρεσιών.

Προσφέρει υπηρεσίες διαχείρισης λογισμικού, πλήρους κύκλου ανάπτυξης, από το σχεδιασμό μέχρι τη δημιουργία εφαρμογών ελέγχου συντήρησης.

Η σκοτεινή πλευρά του PaaS μοντέλου, είναι ότι όλα αυτά τα πλεονεκτήματα μπορούν να φανούν χρήσιμα και σε έναν χάκερ που μπορεί να χρησιμοποιήσει το μοντέλο για την ανάπτυξη κακόβουλου λογισμικού, ικανού να περάσει ακόμα και στις εφαρμογές του IaaS επιπέδου.

Enterprise Service Bus



Στο συγκεκριμένο μοντέλο, υπάρχουν αρκετά πολύπλοκες εφαρμογές όπως οι Enterprise Service Bus (ESB), στις οποίες πρέπει να παρέχεται υψηλό επίπεδο ασφαλείας, αξιοποιώντας πρωτόκολλα, όπως το πρωτόκολλο της ασφάλειας των υπηρεσιών διαδικτύου(Web Service Security protocol,WS).

Προσφέρει υπηρεσίες διαχείρισης λογισμικού, πλήρους κύκλου ανάπτυξης, από το σχεδιασμό μέχρι τη δημιουργία εφαρμογών ελέγχου συντήρησης.

Μετρήσεις

Η δυνατότητα να τμηματοποιηθούν οι υπηρεσίες ESB δεν είναι διαθέσιμη στο περιβάλλον του PaaS μοντέλου.

Για αυτό οι πάροχοι πρέπει να είναι σε θέση, με τη χρήση μετρικών, ανά πάσα στιγμή να εκτιμήσουν την αποτελεσματικότητα των προγραμμάτων ασφαλείας των εφαρμογών.

Ανάμεσα στις άμεσες εφαρμογές που προσφέρονται, είναι διαθέσιμες και συγκεκριμένες μετρήσεις που βαθμολογούν τα επίπεδα κάλυψης επιπέδου ασφαλείας που υπάρχουν.

Οι μετρήσεις αυτές, μπορούν να δείξουν την ποιότητα της κωδικοποίησης των εφαρμογών.

Κακόβουλοι φορείς

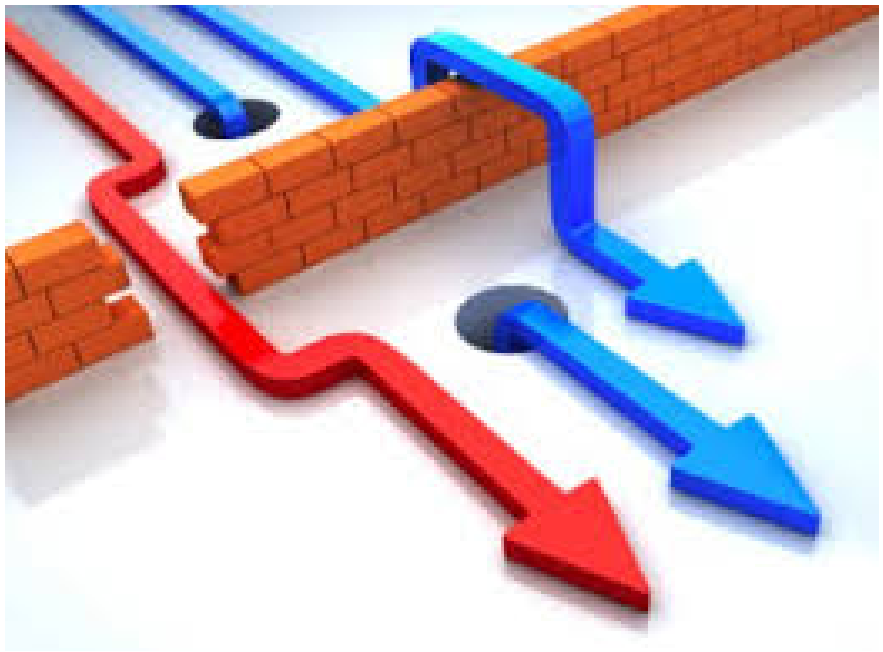
Ιδιαίτερη προσοχή θα πρέπει να δοθεί, στον τρόπο που αντιδρούν οι κακόβουλοι φορείς των αρχιτεκτονικών εφαρμογών του νέφους, στην προσπάθεια τους να εμποδίσουν τον έλεγχο των εφαρμογών.

Οι χάκερς είναι ικανοί να επιτεθούν, σε ορατό κώδικα και σε κώδικα που εκτελείται στο περιβάλλον του χρήστη.

Είναι πιθανό να επιτεθούν ακόμα και στην ίδια την υποδομή του μοντέλου.

Machine to Machine Service Oriented Architecture

Δυστυχώς, τα τρωτά σημεία του υπολογιστικού νέφους δεν περιορίζονται μόνο στις εφαρμογές διαδικτύου, αλλά και στις αδυναμίες των εφαρμογών των υπηρεσιών που προσανατολίζονται στην αρχιτεκτονική (machine to machine Service Oriented Architecture), οι οποίες αναπτύσσονται ολοένα και περισσότερο στο νέφος.



Ασφάλεια στο IaaS

Στο IaaS μοντέλο, ο προγραμματιστής έχει καλύτερο έλεγχο σε σχέση με το προηγούμενο μοντέλο σε θέματα ασφαλείας, με την προϋπόθεση ότι δεν υπάρχει κάποια τρύπα ασφαλείας στην διαχείριση της εικονικοποίησης.

Αν και στη θεωρία οι εικονικές πλατφόρμες είναι σε θέση να αντιμετωπίσουν τα ζητήματα ασφαλείας, που μπορεί ενδεχομένως να προκύψουν, στην πράξη δημιουργούνται πολλά προβλήματα.

Σημαντικό σημείο που χρίζει ιδιαίτερης προσοχής, είναι η αξιοπιστία των δεδομένων που είναι αποθηκευμένα στις υποδομές του παρόχου, στο μοντέλο αυτό.

Απόλυτος έλεγχος δεδομένων

Λόγω της εικονικοποίησης των πάντων, στην κοινωνία της πληροφορίας, η διατήρηση του απόλυτου ελέγχου των δεδομένων κάποιου σε σχέση με την τοποθεσία στην οποία βρίσκεται, είναι ένα θέμα εξαιρετικά ενδιαφέρον.

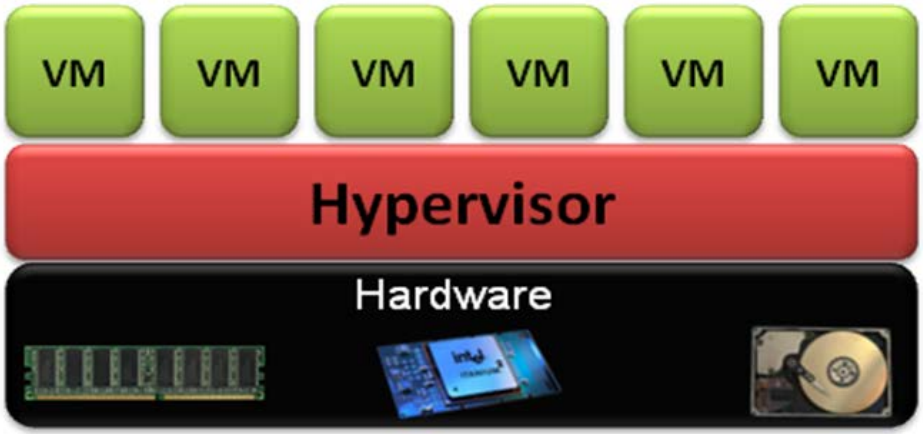
Για να επιτευχθεί η μέγιστη ασφάλεια και εμπιστοσύνη σε ένα υπολογιστικό νέφος, πρέπει να εφαρμοστούν πολλές πρακτικές διασφάλισης ικανοποιητικού επιπέδου ασφαλείας.

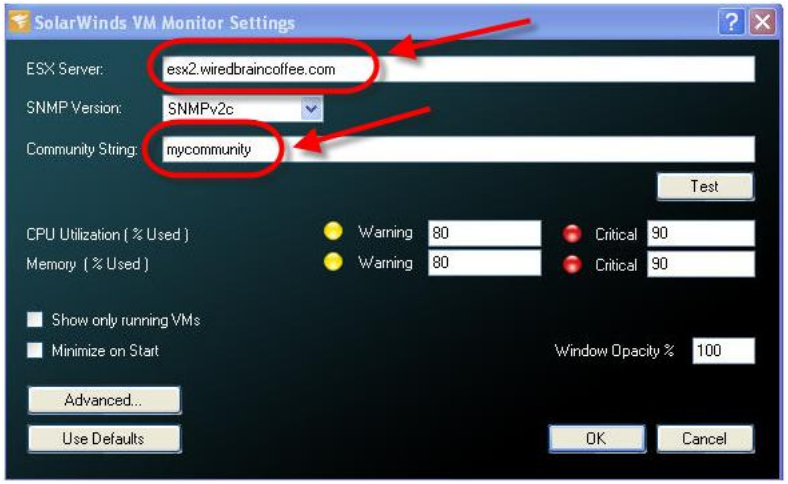
Οι ευθύνες ασφαλείας, τόσο του παρόχου, όσο και του πελάτη, διαφέρουν μεταξύ των διαφορετικών μοντέλων υπηρεσιών νέφους.

Hypervisor ή VM monitor

Ο hypervisor ή αλλιώς VM monitor είναι ένα κομμάτι λογισμικού της εικονικοποίησης, που επιτρέπει πολλαπλά λειτουργικά συστήματα να τρέχουν σε έναν υπολογιστή ξενιστή και παρόλο που έτσι παρέχεται ένα χρήσιμο μέσο για τη δημιουργία πόρων, που μπορούν να διαμοιραστούν, η συγκεκριμένη τεχνολογία αυξάνει τις πιθανότητες επίθεσης.

Ο πελάτης με τη σειρά του, είναι υπεύθυνος για το κομμάτι της ασφάλειας που ελέγχει οτιδήποτε σχετίζεται με το σύστημα τεχνολογίας πληροφορίας.





Ο Ρόλος των μοντέλων ανάπτυξης

Το IaaS μοντέλο παρουσιάζει διάφορα ζητήματα ασφαλείας, ο βαθμός των οποίων εξαρτάται, από τα μοντέλα ανάπτυξης μέσω των οποίων διατίθεται. Το δημόσιο νέφος φαίνεται να παρουσιάζει μεγαλύτερα προβλήματα ασφαλείας, συγκριτικά με το ιδιωτικό.

Η φυσική ασφάλεια των υποδομών και η διαχείριση των καταστροφών είναι ύψιστης σημασίας σε περίπτωση που προκύψει κάποια ζημία στην υποδομή, είτε αυτή η ζημιά είναι τυχαία, είτε είναι εσκεμμένη.

Να σημειωθεί ότι, με τον όρο υποδομή, δεν αναφερόμαστε μόνον στο υλικό στο οποίο τα δεδομένα αποθηκεύονται ή επεξεργάζονται, αλλά και στην διαδρομή που διανύουν όταν διαβιβάζονται.

Κακόβουλη δρομολόγηση

Σε ένα τυπικό περιβάλλον νέφους, τα δεδομένα μεταδίδονται από την πηγή τους στον τελικό προορισμό, μέσω εξωτερικών συσκευών υποδομής άπειρων σε αριθμό.

Και φυσικά, υπάρχει μεγάλη πιθανότητα τα δεδομένα να δρομολογούνται μέσω της υποδομής κάποιου εισβολέα, σε περίπτωση που εντοπίσει κάποιο τρωτό σημείο ασφαλείας και παραβιάσει το νέφος.

Αν και η αρχιτεκτονική του νέφους, αποτελεί μια αυτοσχέδια τεχνολογία, οι βασικές τεχνολογίες παραμένουν οι ίδιες. Εφόσον το νέφος είναι χτισμένο ουσιαστικά πάνω στο διαδίκτυο, επόμενο είναι όλα τα προβλήματα που σχετίζονται με την ασφάλεια στο διαδίκτυο, να αφορούν άμεσα και το την ασφάλεια του νέφους.

Βασικό πρόβλημα

Η βάση της τεχνολογίας του νέφους, θέτει τόσο τον καταναλωτή, όσο και τον πάροχο σε φυσική απόσταση και ουσιαστικά η πρόσβαση τους στους πόρους, είναι εικονική και πραγματοποιείται μέσω διαδικτύου. Έτσι, ακόμα και τεράστια μέτρα ασφαλείας να τεθούν σε εφαρμογή στο σύννεφο, τα δεδομένα εξακολουθούν να μεταφέρονται, μέσω της συνήθους υποκείμενης τεχνολογίας διαδικτύου.

Όμως στο νέφος, οι κίνδυνοι είναι σημαντικά υψηλοί, γιατί τα τρωτά σημεία του διαδικτύου είναι πολλά και σε συνδυασμό με την αξία των πόρων και την επικινδυνότητα που προκύπτει, εφόσον μεταδίδονται σαν σύνολο, οι κίνδυνοι αυξάνονται ολοένα και περισσότερο.

Συνδυασμός πολιτικών και πρωτοκόλλων

Τα συστήματα υπολογιστικού νέφους, εξακολουθούν να χρησιμοποιούν πρωτόκολλα και μέτρα ασφαλείας που χρησιμοποιούνται στο διαδίκτυο, αλλά οι απαιτήσεις τους στην πραγματικότητα βρίσκονται σε πολύ υψηλότερο επίπεδο.

Η κρυπτογράφηση και η χρήση ασφαλών πρωτοκόλλων, μπορούν να εξυπηρετήσουν τις ανάγκες σε κάποιο βαθμό όμως δεν αποτελούν λύση.

Αυτό που χρειάζεται το νέφος για να είναι απόλυτα ασφαλές, είναι ένα σύνολο πολιτικών και πρωτοκόλλων που θα συμβάλλουν στην ασφαλή μετάδοση των δεδομένων στο εσωτερικό του.

Εξωτερικός παράγοντας

Επιπρόσθετα, θα πρέπει να ληφθούν υπόψη και να αντιμετωπιστούν και οι εισβολές που γίνονται στα δεδομένα από εξωτερικούς, μη χρήστες του νέφους μέσω του διαδικτύου.

Όλα αυτά τα μέτρα, θα πρέπει να τεθούν σε εφαρμογή έτσι ώστε να γίνει το περιβάλλον του ασφαλές, ιδιωτικό και απομονωμένο, αποτρέποντας τους εγκληματίες του κυβερνοχώρου να επιτεθούν στο υπολογιστικό νέφος.

Ασφάλεια δεδομένων

Μία από τις βασικές υπηρεσίες που παρέχονται από το cloud computing είναι η αποθήκευση δεδομένων (data storage).

Έτσι δημιουργούνται νέες προκλήσεις στην ασφάλεια και αξιοπιστία αποθήκευσης δεδομένων και πρόσβασης σε υπηρεσίες απομακρυσμένων cloud παρόχων.

Η ασφάλεια της αποθήκευσης των δεδομένων ήταν μία από τις απαραίτητες εργασίες που έπρεπε να δρομολογηθούν πριν γίνει αποδεκτό το cloud computing

Κατανεμημένη αποθήκευση

Κατά τις τελευταίες δεκαετίες, η αποθήκευση δεδομένων έχει αναγνωριστεί ως ένα από τις πιο κύριες ανησυχίες της τεχνολογίας πληροφοριών.

Τα οφέλη των δικτυακών εφαρμογών οδήγησαν στη μετάβαση από την server-attached αποθήκευση στην κατανεμημένη αποθήκευση (distributed storage).

Με βάση το γεγονός ότι η ασφάλεια των δεδομένων είναι το θεμέλιο της ασφάλειας των πληροφοριών, έχει γίνει ένας μεγάλος αριθμός προσπαθειών στον τομέα της ασφάλειας κατανεμημένης αποθήκευσης.

Ωστόσο, οι έρευνες στην ασφάλεια του cloud computing βρίσκονται ακόμα σε αρχικό στάδιο.

Η άποψη των ερευνητών

Μερικοί ερευνητές πιστεύουν ότι η ασφάλεια στο cloud computing δεν είναι πολύ διαφορετική από τις υπάρχουσες πρακτικές ασφάλειας και ότι οι πτυχές της ασφάλειας του cloud computing μπορεί να διαχειριστούν σωστά, χρησιμοποιώντας τις υπάρχουσες τεχνικές, όπως ψηφιακές υπογραφές, κρυπτογράφηση, τείχη προστασίας, και απομόνωση των εικονικών περιβαλλόντων.

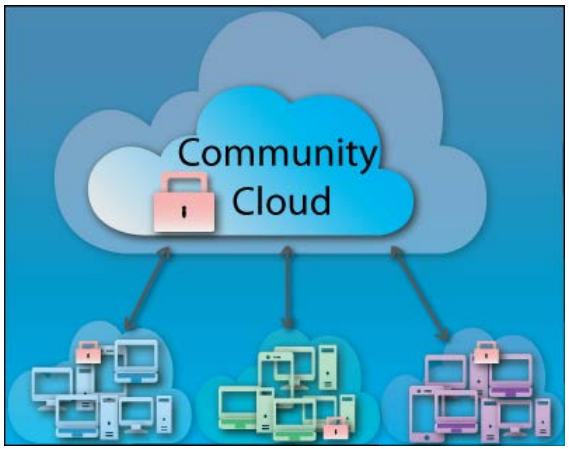
Ένα άλλο ζήτημα είναι ότι οι ειδικές απαιτήσεις ασφάλειας του cloud computing δεν έχουν οριστεί επ' ακριβώς εντός της κοινότητας. Πολλοί σύμβουλοι και πάροχοι υπηρεσιών ασφάλειας έχουν παρουσιάσει προειδοποιήσεις σχετικά με τις απειλές για την ασφάλεια του μοντέλου cloud computing.

Ανησυχίες των χρηστών

Από τη μεριά των χρηστών διατυπώνονται δύο ανησυχίες.

Η μία ανησυχία είναι ότι οι χρήστες δεν θέλουν να αποκαλύψουν τα στοιχεία τους στον πάροχο cloud υπηρεσιών.

Μια άλλη ανησυχία είναι ότι οι χρήστες δεν είναι σίγουροι για την ακεραιότητα των δεδομένων που λαμβάνουν από το σύννεφο και ως εκ τούτου απαιτείται κάτι περισσότερο από τους συμβατικούς μηχανισμούς ασφαλείας για την ασφάλεια των δεδομένων.



Τεχνολογίες για την ασφάλεια δεδομένων

Εξωτερική ανάθεση καθηκόντων

Λόγω των ραγδαίων εξελίξεων στην τεχνολογία του δικτύου, το κόστος της μετάδοσης ενός μεγάλου αριθμού δεδομένων σε μεγάλες αποστάσεις έχει μειωθεί σημαντικά κατά την τελευταία δεκαετία.

Επιπλέον, το συνολικό κόστος της διαχείρισης των δεδομένων είναι πέντε έως δέκα φορές υψηλότερο από ό, τι το αρχικό κόστος κτήσης των δεδομένων.

Ως αποτέλεσμα, υπάρχει ένα αυξανόμενο ενδιαφέρον για την εξωτερική ανάθεση καθηκόντων διαχείρισης των βάσεων δεδομένων σε τρίτα μέρη, που μπορούν να παρέχουν αυτές τις εργασίες σε ένα πολύ χαμηλότερο κόστος.

Προσωπικά δεδομένα

Η γενική ανησυχία για την ασφάλεια στη βάση δεδομένων εξωτερικής ανάθεσης καθηκόντων είναι η προστασία των προσωπικών δεδομένων.

Για την προστασία των προσωπικών δεδομένων έχει προταθεί μια μέθοδος για να εκτελεί ερωτήματα SQL πάνω σε κρυπτογραφημένες βάσεις δεδομένων.

Η στρατηγική αυτής της μεθόδου είναι η επεξεργασία ενός ερωτήματος όσο το δυνατόν περισσότερο από τους φορείς παροχής υπηρεσιών, χωρίς να χρειάζεται να αποκρυπτογραφηθούν τα δεδομένα.

Η αποκρυπτογράφηση και το υπόλοιπο της επεξεργασίας του ερωτήματος εκτελούνται στον πελάτη.

Κρυπτογράφηση

Έχει προταθεί επίσης μία σειρά συστημάτων κρυπτογράφησης για τις αριθμητικές τιμές που επιτρέπει σε κάθε λειτουργία να εφαρμόζεται άμεσα στα κρυπτογραφημένα δεδομένα.

Σε γενικές γραμμές, οι υπάρχουσες μέθοδοι επιτρέπουν την άμεση εκτέλεση των κρυπτογραφημένων ερωτημάτων σχετικά με τα κρυπτογραφημένα σύνολα δεδομένων και επιτρέπουν στους χρήστες να ζητήσουν διάφορα στοιχεία ταυτότητας ανάμεσα σε διάφορα κρυπτογραφημένα δεδομένα.

Ακεραιότητα δεδομένων

Ενώ το διαφανές σύννεφο παρέχει ευέλικτη χρησιμότητα των network-based πόρων, ο φόβος της απώλειας του ελέγχου των δεδομένων είναι μία από τις μεγαλύτερες ανησυχίες που εμποδίζουν τους τελικούς χρήστες από τη μετάβαση στην υπηρεσία της cloud αποθήκευσης.

Στην πραγματικότητα είναι ένας πιθανός κίνδυνος ότι οι πάροχοι των υποδομών αποθήκευσης γίνονται ιδιοτελείς, αναξιόπιστοι, ή ακόμη και κακόβουλοι.

Ύπαρξη πρωτοκόλλων

Στην πραγματικότητα, πριν ο όρος «cloud computing» να εμφανιστεί ως όρος πληροφορικής, υπήρχαν διάφορα πρωτόκολλα απομακρυσμένης αποθήκευσης και ελέγχου δεδομένων.

Απαραίτητες προϋποθέσεις (1/3)

Στην πράξη, ένα πρωτόκολλο απομακρυσμένου ελέγχου δεδομένων πρέπει να πληροί τις ακόλουθες πέντε προϋποθέσεις:

1. Δεν θα πρέπει να είναι ένα προαπαιτούμενο ότι ο επαληθευτής (verifier) πρέπει να διαθέτει ένα πλήρες αντίγραφο των δεδομένων που πρέπει να ελεγχθούν. Και πρακτικά δεν έχει νόημα για έναν επαληθευτή να κρατήσει ένα αντίγραφο του περιεχομένου που επαληθεύεται.

Απαραίτητες προϋποθέσεις (2/3)

Στην πράξη, ένα πρωτόκολλο απομακρυσμένου ελέγχου δεδομένων πρέπει να πληροί τις ακόλουθες πέντε προϋποθέσεις:

2. Το πρωτόκολλο θα πρέπει να είναι πολύ ισχυρό, λαμβάνοντας υπόψη έναν αναξιόπιστο επαληθευτή. Ένας κακόβουλος επαληθευτής έχει κίνητρα να κρύψει την παραβίαση της ακεραιότητας των δεδομένων και έτσι το πρωτόκολλο θα πρέπει να είναι αρκετά ισχυρό ώστε να οδηγήσει σε αποτυχία έναν κακόβουλο επαληθευτή.
3. Ο αριθμός των πληροφοριών που ανταλλάσσονται κατά τη διάρκεια της λειτουργίας επαλήθευσης δεν πρέπει να οδηγήσει σε επικοινωνία υψηλού κόστους.

Απαραίτητες προϋποθέσεις (3/3)

Στην πράξη, ένα πρωτόκολλο απομακρυσμένου ελέγχου δεδομένων πρέπει να πληροί τις ακόλουθες πέντε προϋποθέσεις:

4. Το πρωτόκολλο θα πρέπει να είναι υπολογιστικά αποδοτικό.
5. Θα πρέπει να είναι δυνατό να εκτελείται η επαλήθευση σε έναν απεριόριστο αριθμό φορών.

Σημειώνεται ότι ένας επαληθευτής μπορεί να είναι ο κάτοχος των δεδομένων ή ένα έμπιστο τρίτο μέρος, ένας πάροχος υπηρεσιών αποθήκευσης ή ο διαχειριστής του συστήματος.

Ασφάλεια web-based εφαρμογών

Σε περιβάλλοντα cloud computing, οι πόροι παρέχονται ως υπηρεσία μέσω του διαδικτύου με έναν δυναμικό, εικονικό, και κλιμακούμενο τρόπο.

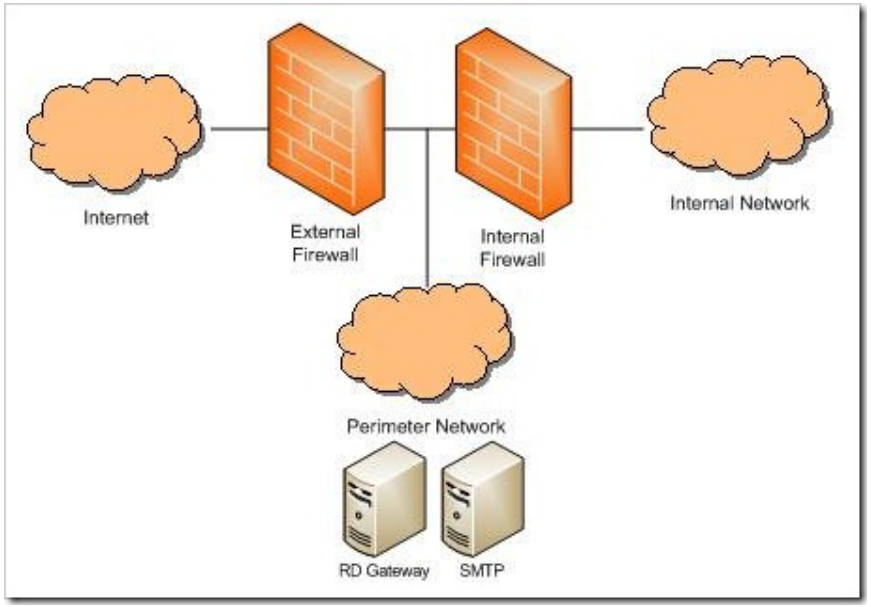
Μέσω των cloud υπηρεσιών, οι χρήστες μπορούν να έχουν on-line πρόσβαση σε επιχειρηματικές εφαρμογές από μια ιστοσελίδα περιήγησης, ενώ το λογισμικό και τα δεδομένα αποθηκεύονται στους διακομιστές.

Ως εκ τούτου, στην εποχή του cloud computing, η web ασφάλεια παίζει έναν πολύ σημαντικό ρόλο.

Πρώτη πύλη

Ο διακομιστής της ιστοσελίδας είναι η πρώτη πύλη που προστατεύει τους τεράστιους cloud πόρους.

Από τη στιγμή που το σύννεφο μπορεί να λειτουργεί συνεχώς για να επεξεργάζεται καθημερινά on-line συναλλαγές εκατομμυρίων, η επίδραση της ευπάθειας ασφαλείας στο διαδίκτυο θα πρέπει να ενισχύεται σε ολόκληρο το σύννεφο.

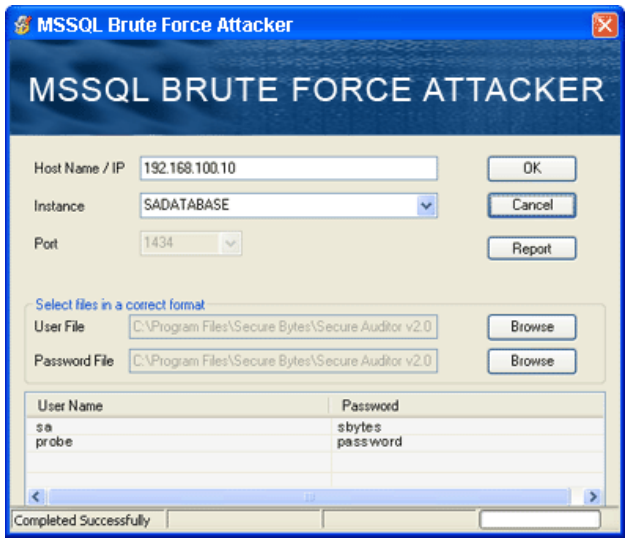


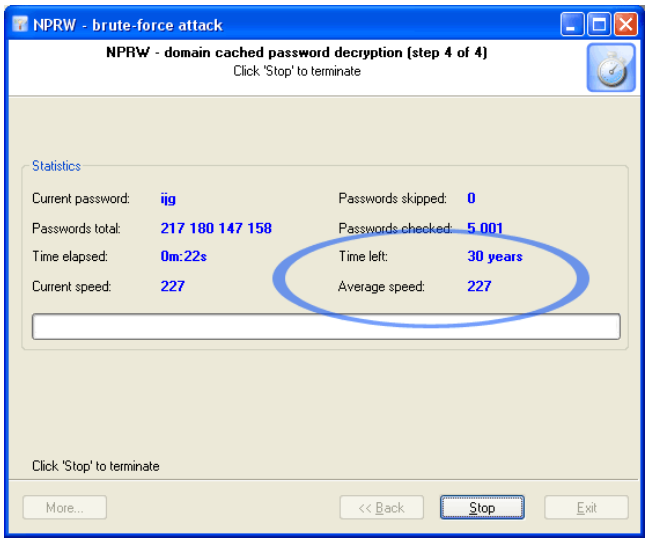
«Κατηγορία της επίθεσης»

Οι τεχνικές διαδικτυακών επιθέσεων αναφέρονται συχνά ως «κατηγορία της επίθεσης».

Όταν εντοπίζεται οποιαδήποτε ευπάθεια στην διαδικτυακή ασφάλεια, ο εισβολέας θα χρησιμοποιήσει αυτές τις τεχνικές για να εκμεταλλευτεί αυτή την ευπάθεια ασφάλειας.

Τα είδη της επίθεσης μπορεί να κατηγοριοποιούνται σε επιθέσεις Πιστοποίησης (Authentication) και Εξουσιοδότησης (Authorization).





Πιστοποίηση (Authentication) (1/2)

Η πιστοποίηση είναι η διαδικασία της επαλήθευσης ενός ισχυρισμού ότι ένα αντικείμενο ενεργεί για λογαριασμό μιας συγκεκριμένης αρχής.

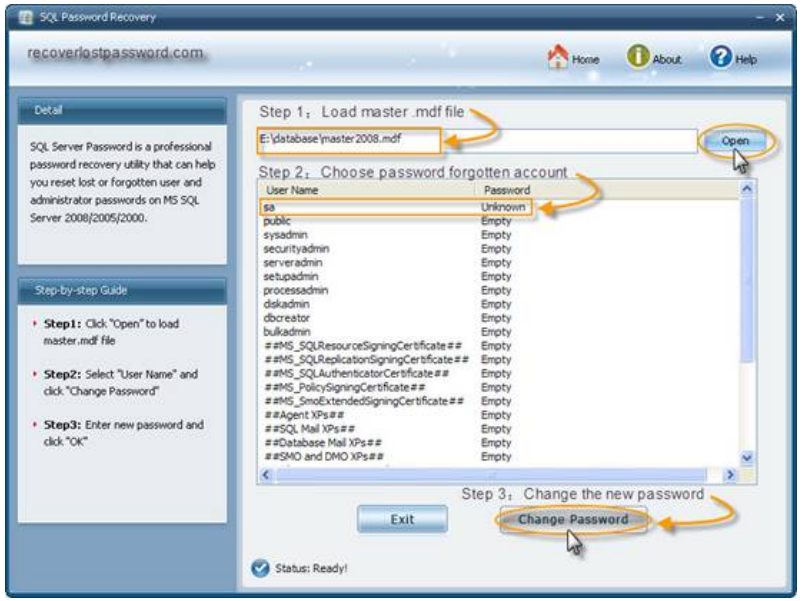
Οι επιθέσεις πιστοποίησης στοχεύουν στην μέθοδο των ιστοσελίδων για την επικύρωση της ταυτότητας ενός χρήστη, υπηρεσιών ή εφαρμογών.

Οι τεχνικές επιθέσεων που χρησιμοποιούνται για της επιθέσεις πιστοποίησης είναι οι Brute Force Attack, Insufficient Authentication και Weak Password Recovery Validation.

Πιστοποίηση (Authentication) (2/2)

Για την πιστοποίηση του χρήστη και την αποφυγή επιθέσεων, πολλές τοποθεσίες Web παρέχουν μια υπηρεσία ανάκτησης κωδικού πρόσβασης.

Αυτή η υπηρεσία ανακτά αυτόματα το όνομα χρήστη ή τον κωδικό πρόσβασης του χρήστη, αν αυτός μπορεί να απαντήσει σε μερικές ερωτήσεις που ορίζεται ως μέρος της διαδικασίας εγγραφής του χρήστη.



Εξουσιοδότηση (Authorization) (1/2)

Η εξουσιοδότηση χρησιμοποιείται για να επαληθεύσει αν ένα επικυρωμένο αντικείμενο μπορεί να εκτελέσει μια συγκεκριμένη λειτουργία και πρέπει να προηγείται της έγκρισης.

Για παράδειγμα, ορισμένοι μόνο χρήστες μπορούν να έχουν πρόσβαση σε συγκεκριμένο περιεχόμενο ή συγκεκριμένη λειτουργικότητα.

Οι επιθέσεις εξουσιοδότησης χρησιμοποιούν διάφορες τεχνικές για να αποκτήσουν πρόσβαση σε προστατευόμενες περιοχές πέρα από τα προνόμιά τους.

Εξουσιοδότηση (Authorization) (2/2)

Όταν ένας χρήστης είναι εξουσιοδοτημένος σε μια τοποθεσία, δεν σημαίνει απαραίτητα ότι θα πρέπει να έχει πρόσβαση σε κάποιο συγκεκριμένο περιεχόμενο που έχει χορηγηθεί αυθαίρετα.

Σε πολλές ιστοσελίδες, μετά από μια επιτυχή ταυτοποίηση του χρήστη με την ιστοσελίδα για πρώτη φορά, η ιστοσελίδα δημιουργεί μια συνεδρία και δημιουργεί ένα μοναδικό “Session ID" για τον προσδιορισμό αυτής της συνεδρίας.

Αυτό το Session ID επισυνάπτεται στις μετέπειτα αιτήσεις στην τοποθεσία ως "απόδειξη" της εξουσιοδοτημένης συνεδρίας.

Χρήση του Υπολογιστικού Νέφους

Πώς Χρησιμοποιείται το ΥΝ

Σε αυτήν την παράγραφο, θα δοθούν μερικά παραδείγματα περιπτώσεων, στις οποίες χρησιμοποιείται το υπολογιστικό νέφος, προκειμένου να γίνουν σαφέστερα τα όσα περιγράφηκαν παραπάνω. Τα παραδείγματα που θα ακολουθήσουν, βασίζονται στον ορισμό αλλά και στα χαρακτηριστικά του υπολογιστικού νέφους που προαναφέρθηκαν και αναφέρονται σε υπηρεσίες του νέφους, που προσφέρονται σε φυσικά πρόσωπα, σε επιχειρήσεις ή οργανισμούς και σε δημόσιες αρχές.

Διακρίνονται τρείς κατηγορίες υπηρεσιών: *Υπηρεσίες Καταναλωτών, Υπηρεσίες Επιχειρήσεων και Υπηρεσίες Δημόσιων Αρχών*

Ο ~*okeanos* ανήκει στην κατηγορία «Υπηρεσίες Καταναλωτών».

Είναι μια καινούργια, ελληνική, IaaS υπηρεσία.

Δίνει τη δυνατότητα στους χρήστες να χτίσουν το δικό τους προσωπικό υπολογιστή ο οποίος θα έχει συνεχή πρόσβαση στη διαδίκτυο, χωρίς να ανησυχούν για προβλήματα λογισμικού και υλικού και αποτυχίες συνδέσεων.

Ο χρήστης έχει τη δυνατότητα να διαχειριστεί τα εικονικά μηχανήματά του, να τα καταστρέψει, και να συνδεθεί σε αυτά μέσα από τον αγαπημένο του φυλλομετριτή.

Επίσης μέσω του *pithos+* ο okeanos διαθέτει αποθηκευτικό χώρο τον οποίο ο χρήστης μπορεί να διαμοιράζεται με φίλους και στον οποίο μπορεί να έχει πρόσβαση από οπουδήποτε και σε οποιαδήποτε χρονική στιγμή. https://okeanos.grnet.gr/home/

Amazon Cloud Drive

Το *Amazon Cloud Drive* ανήκει στην κατηγορία «Υπηρεσίες Καταναλωτών» και αποτελεί μια IaaS υπηρεσία.

Είναι ο προσωπικός σκληρός δίσκος του χρήστη μέσα στο νέφος.

Μπορεί να αποθηκεύσει τη μουσική, τα βίντεο, τις φωτογραφίες και τα έγγραφα του σε ασφαλείς υποδομές του Amazon.

Το μόνο που χρειάζεται είναι ένας φυλλομετρητής, προκειμένου να μπορεί να ανεβάσει, να κατεβάσει και να έχει πρόσβαση στα αρχεία του από οποιονδήποτε υπολογιστή.

Έτσι, τα αρχεία του χρήστη δεν μπορούν να χαθούν σε περίπτωση βλάβης του σκληρού δίσκου του υπολογιστή του, αλλά ούτε και σε περίπτωση κλοπής του.

http://www.amazon.com/gp/feature.html?ie=UTF8&docId=1000828861

Apple iCloud

Το *Apple iCloud* ανήκει στην κατηγορία «Υπηρεσίες Καταναλωτών» και αποτελεί μια SaaS υπηρεσία.

Έχει τη δυνατότητα να αποθηκεύει φωτογραφίες, βίντεο, έγγραφα και πολλά άλλα και να τα στέλνει ασύρματα σε όλες τις συσκευές του χρήστη.

Αυτόματα και εύκολα το iCloud μπορεί να αποθηκεύσει με ασφάλεια αρχεία, έτσι ώστε να είναι πάντα διαθέσιμα στο iPhone, το iPad, το iPod Touch, το MAC ή το PC.

Έτσι, η πρόσβαση τους γίνεται από οποιαδήποτε συσκευή χρησιμοποιεί ο χρήστης. Δεν απαιτείται συγχρονισμός και διαχείριση γιατί το iCloud τα κρατά όλα ενημερωμένα από μόνο του.

http://www.apple.com/icloud/

Dropbox

Το *Dropbox* ανήκει στην κατηγορία «Υπηρεσίες Καταναλωτών» και αποτελεί μια SaaS υπηρεσία.

Είναι μια δωρεάν υπηρεσία που επιτρέπει στο χρήστη να έχει πρόσβαση σε όλα του τα αρχεία, από οπουδήποτε.

Αυτό σημαίνει ότι, οποιοδήποτε αρχείο αποθηκευτεί στο Dropbox, αυτόματα αποθηκεύεται στον υπολογιστή ή στο κινητό που χρησιμοποιεί.

Επίσης, δίνει τη δυνατότητα πολύ εύκολα να μοιραστεί τα αρχεία του, με όποιον επιλέξει.

Έτσι, δεν μπορούν να χαθούν σε περίπτωση βλάβης του υπολογιστή και είναι πάντα ασφαλή.

https://www.dropbox.com/

Google Apps

Το *Google Apps* ανήκει στην κατηγορία «Υπηρεσίες Καταναλωτών» και αποτελεί μια SaaS υπηρεσία.

Δίνει τη δυνατότητα στους χρήστες, να δημιουργήσουν διευθύνσεις ηλεκτρονικού ταχυδρομείου, να οργανώσουν το πρόγραμμα τους και να μοιραστούν εκδηλώσεις με φίλους, να αποθηκεύσουν έγγραφα και να έχουν πρόσβαση σε αυτά οποιαδήποτε στιγμή, να δημιουργήσουν έγγραφα τα οποία μπορούν να μοιραστούν με συνεργάτες και να τα δουλεύουν όλοι μαζί, σε πραγματικό χρόνο και να δημιουργήσουν παρουσιάσεις και βίντεο τα οποία αποθηκεύονται και δεν χρειάζεται καν να πατήσουν αποθήκευση.

http://www.google.com/enterprise/apps/business/

SkyDrive

Το *Windows Live SkyDrive* (προηγουμένως γνωστό ως *Windows Live Folders*) ανήκει στην κατηγορία «Υπηρεσίες Καταναλωτών» και αποτελεί μια SaaS υπηρεσία.

Είναι μέρος της οικογένειας προγραμμάτων και υπηρεσιών του Windows Live της Microsoft.

Το SkyDrive επιτρέπει στους χρήστες να αποθηκεύουν αρχεία στο διαδίκτυο και να αποκτούν πρόσβαση σε αυτά από οποιονδήποτε υπολογιστή.

Η υπηρεσία SkyDrive χρησιμοποιεί το Windows Live ID περιορίζοντας την πρόσβαση στα ιδιωτικά αρχεία ενός χρήστη, τον διαμοιρασμό τους με επαφές ή τη δημοσιοποίησή τους.

Δεν χρειάζεται Windows Live ID για να προβληθούν τα κοινόχρηστα αρχεία. https://login.live.com/

Amazon S3

Το *AmazonS3* ανήκει στην κατηγορία «Υπηρεσίες Επιχειρήσεων» και αποτελεί μια PaaS υπηρεσία.

Είναι χώρος αποθήκευσης στο διαδίκτυο και εξυπηρετεί πολύ τους προγραμματιστές. Παρέχει ένα απλό διαδικτυακό περιβάλλον, για υπηρεσίες που χρησιμοποιούνται για την αποθήκευση και την ανάκτηση δεδομένων, οποιαδήποτε στιγμή, από οπουδήποτε στο διαδίκτυο.

Δίνει σε κάθε προγραμματιστή πρόσβαση στην ίδια εξαιρετικά επεκτάσιμη, αξιόπιστη, γρήγορη και φθηνή υποδομή που χρησιμοποιεί και η Amazon, για να τρέχει το δικό της παγκόσμιο δίκτυο ιστοσελίδων.

Στόχος της υπηρεσίας είναι, να μεγιστοποιηθούν τα οφέλη της και να περάσουν τα οφέλη αυτά στους προγραμματιστές. http://aws.amazon.com/s3/

Box

Η *Box* ανήκει στην κατηγορία «Υπηρεσίες Επιχειρήσεων» και αποτελεί μια PaaS υπηρεσία.

Επιτρέπει στους πελάτες της να αποθηκεύσουν μεγάλο όγκο δεδομένων on-line και έτσι, μπορούν να έχουν πρόσβαση σε αυτά και να τα διαχειρίζονται από οπουδήποτε.

Δίνει τη δυνατότητα ανατροφοδότησης σε ένα σημείο, είτε η ανατροφοδότηση αυτή είναι ένα γρήγορο σχόλιο, είτε είναι μια ολόκληρη συζήτηση.

Ο πελάτης, μπορεί να έχει μια λεπτομερή, πραγματικού χρόνου εικόνα, σχετικά με το τι αλλαγές υπάρχουν στα δεδομένα του.

https://www.box.com/

Υπηρεσίες Δημοσίων Αρχών (1/2)

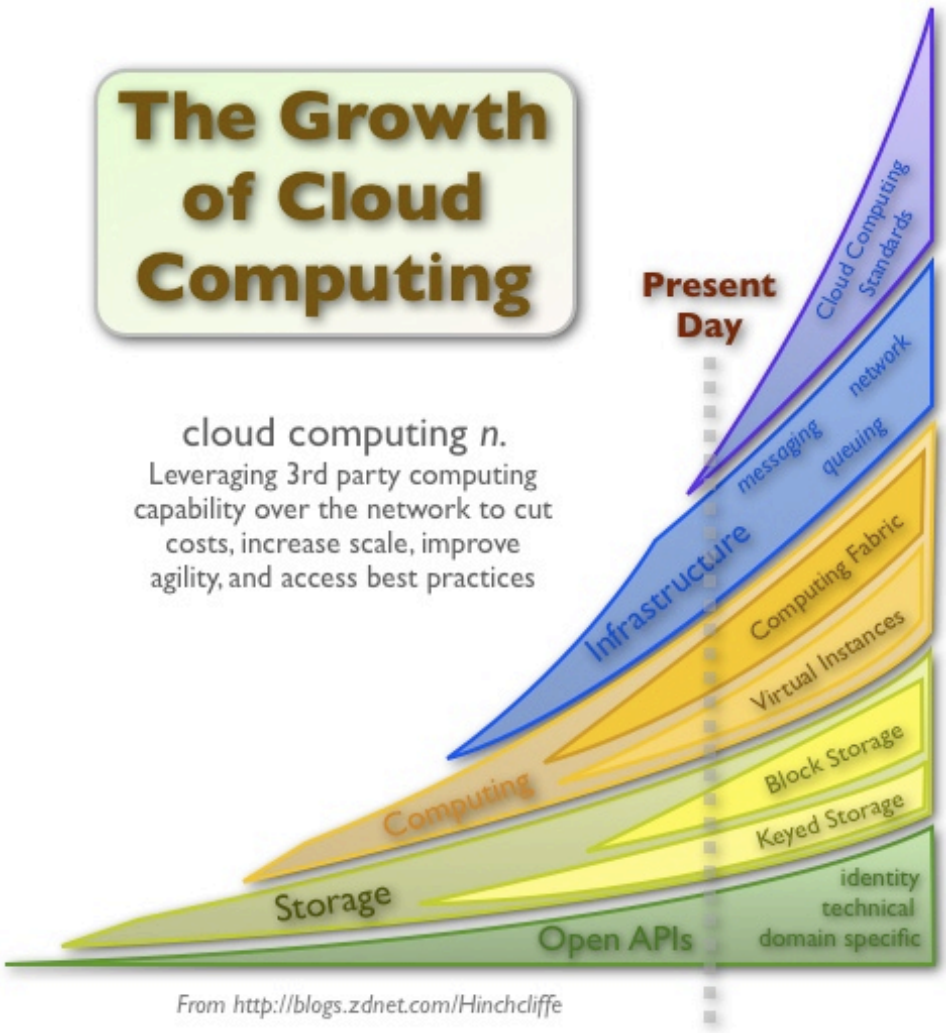
Η υιοθέτηση υπηρεσιών υπολογιστικού νέφους από τις δημόσιες αρχές στοχεύει στην υψηλή παραγωγικότητα και στη χρήση εργαλείων διαχείρισης έργου, που χρησιμοποιούνται ευρέως και από τις επιχειρήσεις. Ο λόγος που οι δημόσιες αρχές στράφηκαν στις υπηρεσίες νεφών, είναι η εξοικονόμηση κόστους αλλά και η καλύτερη ποιότητα προσφερόμενων υπηρεσιών στους πολίτες.

Υπηρεσίες Δημοσίων Αρχών (2/2)

Έτσι, αυτές οι υπηρεσίες αυξάνονται σταδιακά όλο και περισσότερο στους κλάδους μεταφορών, υγείας και εκπαίδευσης. Βέβαια, δεν είναι ακόμα ευρέως διαδεδομένη η χρήση των υπηρεσιών αυτών σε αυτούς τους κλάδους. Έτσι, πολλά κράτη και χώρες της Ευρωπαϊκής Ένωσης, βρίσκονται ακόμα σε επίπεδο έρευνας και ανάπτυξης του υπολογιστικού νέφους και όχι σε επίπεδα υιοθέτησης.

Επίλογος

Ραγδαία ανάπτυξη



Γίνεται αντιληπτό ότι το υπολογιστικό νέφος αποτελεί ένα τεχνολογικό επίτευγμα το οποίο είναι ευρέως διαδεδομένο και φαίνεται ότι θα *μονοπωλήσει* το ενδιαφέρον τα επόμενα χρόνια στον τομέα της πληροφορικής.

Το νέο κύμα στην πληροφορική

Το cloud computing θεωρείται από πολλούς ως το επόμενο κύμα της τεχνολογίας των πληροφοριών για ιδιώτες, εταιρείες και κυβερνήσεις.

Η αφθονία των δυνατοτήτων της τεχνολογίας πληροφοριών με χαμηλό κόστος προσφέρει πολλές δελεαστικές ευκαιρίες.

Εκτός από τη μείωση των λειτουργικών δαπανών, οι τεχνολογίες cloud έχουν γίνει η βάση για ριζική επιχειρηματική καινοτομία και νέα επιχειρηματικά μοντέλα, καθώς και για σημαντικές βελτιώσεις στην αποτελεσματικότητα οποιουδήποτε χρησιμοποιεί την τεχνολογία πληροφοριών - το οποίο, αυτές τις μέρες, σημαίνει το μεγαλύτερο μέρος του κόσμου.

Βιβλιογραφία

Alleweldt, F. / Kara, S., ‘’Cloud Computing’’, 2012.

Almond, C., «A Practical Guide to Cloud Computing Security», 2009.

Briscoe, G. / Marinos, A., in: DEST’09, Third IEEE International. Conference on Digital Ecosystems and Technologies, IEEE, 2009.

Choudhary, V., Software as a service: implications for investment in software development. In: International conference on system sciences.

http://en.wikipedia.org/wiki/Cloud_computing.

Introduction to cloud computer architecture, White paper, 1st Edition.

Cloud computer for dummies, Judith Hurwitz, Robin Bloor, Marcia.

Cloud Computing Principles, Nick Antonopoulos, Lee Gillam, Springer.

Cloud Computing and Software Services Theory and Techniques.

Τέλος