ΕΛΛΗΝΙΚΟ ΑΝΟΙΚΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ & ΤΕΧΝΟΛΟΓΙΑΣ

ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ
ΜΕΤΑΠΤΥΧΙΑΚΗ ΕΞΕΙΔΙΚΕΥΣΗ
ΣΤΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΈΛΕΓΧΟΣ ΜΗΧΑΝΙΣΜΩΝ ΑΣΦΑΛΕΙΑΣ ΣΤΟ CLOUD

ΧΑΤΖΟΠΟΥΛΟΥ ΑΡΓΥΡΩ
Α.Μ.: 65753

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΕΥΣΤΑΘΙΟΣ ΧΑΤΖΗΕΥΘΥΜΙΑΔΗΣ

ΠΑΤΡΑ
ΙΟΥΛΙΟΣ, 2012

ΕΛΛΗΝΙΚΟ ΑΝΟΙΚΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ & ΤΕΧΝΟΛΟΓΙΑΣ

ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ
ΜΕΤΑΠΤΥΧΙΑΚΗ ΕΞΕΙΔΙΚΕΥΣΗ
ΣΤΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΈΛΕΓΧΟΣ ΜΗΧΑΝΙΣΜΩΝ ΑΣΦΑΛΕΙΑΣ ΣΤΟ CLOUD

ΧΑΤΖΟΠΟΥΛΟΥ ΑΡΓΥΡΩ
Α.Μ.: 65753

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ	ΜΕΛΟΣ 2	ΜΕΛΟΣ 3
ΕΥΣΤΑΘΙΟΣ ΧΑΤΖΗΕΥΘΥΜΙΑΔΗΣ	ΚΩΝ/ΝΟΣ ΧΩΡΙΑΝΟΠΟΥΛΟΣ	ΓΡΗΓΟΡΙΟΣ ΜΠΕΛΗΓΙΑΝΝΗΣ

Περίληψη

Η υπολογιστική νέφους ή αλλιώς το cloud computing αποτελεί μία αναπτυσσόμενη τεχνολογία που χρησιμοποιείται από όλο και περισσότερους οργανισμούς. Από έρευνες που έχουν διενεργηθεί παγκοσμίως, οι συμμετέχοντες αναγνώρισαν τα πολύ μεγάλα οφέλη και πλεονεκτήματα της χρήσης υπηρεσιών cloud computing αλλά ταυτόχρονα επέδειξαν και έναν βασικό ανασταλτικό παράγοντα, την ασφάλεια. Η συντριπτική πλειοψηφία των συμμετεχόντων διατηρεί επιφυλάξεις σε σχέση με την ασφάλεια στην χρήση υπηρεσιών cloud computing με έμφαση άλλοτε στην εμπιστευτικότητα, την εχεμύθεια, την διαθεσιμότητα και την ακεραιότητα των πληροφοριών του.

Οι επιφυλάξεις αυτές στηρίζονται στο γεγονός ότι η υλοποίηση των υπηρεσιών αυτών είναι ως έχει (as is) χωρίς να υπάρχει από την πλευρά του πελάτη ουσιαστικός έλεγχος επί του επιπέδου ασφαλείας της παρεχόμενης υπηρεσίας.

Το αντικείμενο της εργασίας αυτής είναι η δημιουργία ενός αντικειμενικού τρόπου αποτίμησης της ασφάλειας των υπηρεσιών cloud computing. Ο τρόπος αυτός συνίσταται στην μέτρηση της επίδοσης των μηχανισμών ασφαλείας των υπηρεσιών cloud computing με χρήση εργαλείων. Τα εργαλεία αυτά είναι εξειδικευμένα και οι μετρήσεις τους δίνουν την ύπαρξη ή όχι συγκεκριμένων αδυναμιών που με την σειρά τους συνδέονται με συγκεκριμένες ομάδες κινδύνων.

Λέξεις – Κλειδία:
Υπολογιστική νέφους, ασφάλεια υπηρεσιών cloud computing, μέτρηση ασφάλειας, μέτρηση μηχανισμών ασφαλείας

Abstract

Cloud computing is a fast growing technology that is nowadays used by an increasing amount of organizations. Surveys, that have been conducted internationally, point out the advantages of the use of cloud computing services as well as a major inhibitor: security. The majority of the participants, say that they have reservations towards using cloud computing services due to privacy, availability, confidentiality and in general security concerns.

These concerns are based on the fact (due to the service model of cloud computing) that the cloud computing services are offered as is without the client having any actual knowledge or control of the security controls taken by the cloud provider.

In this master thesis a methodology for the evaluation of the security controls enforced by the cloud provider is described. According to the methodology, specific tools are used in order to evaluate the compliance to criteria. These criteria have a direct mapping to vulnerabilities (that can be lead to security risks) of the cloud computing services.

Key-words:

Cloud computing, Cloud computing services security, evaluation of security controls in cloud computing

Ευχαριστίες

Από την αρχική σύλληψη της ιδέας αυτής της εργασίας ως την υλοποίηση και την ολοκλήρωσή της συνεισέφεραν πολλοί άνθρωποι που θα ήταν άδικο να προσπαθήσω να τους απαριθμήσω και ονοματίσω.

Σε όλους όσους με ενέπνευσαν, βοήθησαν, υποστήριξαν, καθοδήγησαν, υπέμειναν, συμβούλεψαν ή απλά υπήρξαν εκεί για εμένα όλο αυτό το διάστημα και όχι μόνο, απευθύνω τις θερμότερές μου ευχαριστίες.

ΠΕΡΙΕΧΟΜΕΝΑ

Εισαγωγή στο Cloud Computing

Ιστορικά στοιχεία

Η έννοια του cloud computing δεν είναι καινούργια. Στην βιβλιογραφία εμφανίζονται διαφορετικές απόψεις σχετικά με την προέλευσή της. Εδώ, αποφασίστηκε να παρουσιαστεί κάποια που εμφανίζεται ως η επικρατέστερη (χωρίς βέβαια να σημαίνει ότι είναι σίγουρα ορθή).

Σύμφωνα με την θεωρία αυτή, το cloud computing σαν έννοια ξεκίνησε την δεκαετία του 60 και αποτελεί μια μετεξέλιξη μέσω μια σειράς από στάδια τα οποία περιλαμβάνουν το grid & utility computing, το application service provision (ASP) και το Software as a Service (SaaS).

Συγκεκριμένα, σύμφωνα με την θεωρία αυτή, η έννοια του cloud computing γεννήθηκε από τους προβληματισμούς του J.C.R. Licklider στα πλαίσια της επικοινωνίας με τα μέλη της ομάδας Members and Affiliates of the Intergalactic Computer Network, του ADVANCED RESEARCH PROJECTS AGENCY, στην Washington στις 23 Απριλίου του 1963. Ο προβληματισμός που οδήγησε στην διατύπωση μιας δομής cloud computing ξεκίνησε από το γεγονός ότι υπάρχουν πολλές διαφορετικές γλώσσες προγραμματισμού και ότι από την στιγμή που αυτές δεν μπορούν να μειωθούν ή να συγχωνευτούν σε μια, θα πρέπει να δοθεί στον χρήστη η δυνατότητα να έχει πρόσβαση σε πολλά συστήματα και επιλέγει ποια να χρησιμοποιήσει. (…It seems to me to be interesting and important, nevertheless, to develop a capability for integrated network operation….) [1]

Από την δεκαετία του ΄60 μέχρι σήμερα, η έννοια του cloud computing έχει περάσει από διάφορα στάδια για να φτάσει στην πιο σύγχρονη μετεξέλιξή του με το Web 2.0. Η ουσία και τα οφέλη του cloud computing άρχισαν να γίνονται πιο χειροπιαστά από την στιγμή που η πρόσβαση μέσω του διαδικτύου έγινε εφικτή σε μεγαλύτερη κλίμακα. Η πρώτη εταιρία η οποία προσέφερε εφαρμογές μέσω του διαδικτύου θεωρείται ότι είναι η εταιρία Saleforce (www.saleforce.com) το 1999, ενώ ακολούθησαν οι Amazon με τα Amazon Web Services το 2002 και το Elastic Compute cloud (EC2) το 2006. Η χρήση

υπηρεσιών cloud απογειώθηκε από το 2009 με την προσφορά στο ευρύ κοινό των υπηρεσιών της Google (από το Gmail ως τα Google Apps).

Τι είναι το cloud computing

Το Cloud computing είναι ένα μοντέλο για την εύκολη, βολική και on-demand πρόσβασης σε μια σειρά από παραμετροποιήσιμους διαμοιραζόμενους πόρους (π.χ δίκτυα,servers, αποθηκευτικοί χώροι, εφαρμογές και υπηρεσίες) που μπορούν να διατεθούν γρήγορα και να λειτουργήσουν με ελάχιστη διαχειριστική προσπάθεια ή παρέμβαση του παρόχου της υπηρεσίας. [2]

Το μοντέλο αυτό, σύμφωνα με τον παραπάνω ορισμό, προάγει την διαθεσιμότητα και αποτελείται από 5 βασικά χαρακτηριστικά, τρία μοντέλα υπηρεσιών και 4 μεθόδους υλοποίησης.

Βασικά Χαρακτηριστικά:

On-demand self-service:

Ο τελικός χρήστης αποκτά πρόσβαση στους υπολογιστικούς πόρους (είτε πρόκειται για αποθηκευτικό χώρο, ή υπολογιστική ισχύ, ή λοιπές υπηρεσίες), όταν το χρειάζεται (on-demand) χωρίς την ανάγκη παρέμβασης από τον πάροχο της υπηρεσίας (self-service).

Broad network access:

Οι απαιτήσεις για την πρόσβαση στις υπηρεσίες cloud είναι συγκεκριμένες και ελάχιστες. Στην ουσία, απαιτείται απλά πρόσβαση στο internet μέσω οποιουδήποτε μέσου (π.χ. κινητών τηλεφώνων, φορητών υπολογιστών, PDAs κ.α.)

Resource pooling:

Οι τεχνολογίες και αρχιτεκτονικές που χρησιμοποιούνται από τους παρόχους υπηρεσιών cloud, βασίζονται στην χρήση πολλαπλών συστοιχιών πόρων.

Rapid elasticity:

Οι πόροι που χρησιμοποιούνται διαμοιράζονται στις περισσότερες των περιπτώσεων ιδεατά (virtually) και δυναμικά, επιτρέποντας έτσι την εκχώρηση και άλλων πόρων σε περίπτωση που χρειαστεί. Η μετάβαση αυτή (scale out/in) μπορεί να γίνει αυτόματα και γρήγορα αν χρειαστεί.

Measured Service:

Μέσω των συστημάτων του παρόχου, μπορεί να γίνεται παρακολούθηση της χρήσης των πόρων ανά σύστημα και ανά πελάτη.

Ποιοι είναι οι διάφοροι τύποι cloud services (SaaS, PaaS, IaaS)

Cloud Software as a Service (SaaS).

Στα πλαίσια της παροχής αυτού του είδους της υπηρεσίας Cloud, ο πελάτης έχει την δυνατότητα να χρησιμοποιεί εφαρμογές που ανήκουν στον πάροχο και τρέχουν στην υποδομή του παρόχου. Ο πελάτης χρησιμοποιεί μια σύνδεση στο διαδίκτυο και τον εξοπλισμό της επιλογής του (φορητός υπολογιστής, PDA, netbook, desktop, mobile phone….) προκειμένου να πετύχει αποκτήσει πρόσβαση στη /στις εφαρμογή/ές. Ο πελάτης δεν έχει δυνατότητα να επηρεάζει ή να ελέγχει το υλικό ή το λογισμικό μέσω του οποίου γίνεται διαθέσιμη η εφαρμογή. [3]

Cloud Platform as a Service (PaaS).

Στα πλαίσια της παροχής αυτού του είδους της υπηρεσίας Cloud, ο πελάτης έχει την δυνατότητα να δημιουργεί και να λειτουργεί εφαρμογές που έχουν δημιουργηθεί ή αποκτηθεί χρησιμοποιώντας γλώσσες ή εργαλεία προγραμματισμού που παρέχονται από τον πάροχο. Ο πελάτης δεν έχει δυνατότητα να διαχειρίζεται ή να ελέγχει το υλικό μέσω του οποίου γίνεται διαθέσιμη η υπηρεσία αλλά έχει την δυνατότητα ελέγχου, διαχείρισης και αλλαγών πάνω στις εφαρμογές που τρέχει και πιθανώς ανά περίπτωση στην διαμόρφωση του περιβάλλοντος φιλοξενίας των εφαρμογών.

Cloud Infrastructure as a Service (IaaS).

Στα πλαίσια της παροχής αυτού του είδους της υπηρεσίας Cloud, ο πελάτης έχει διαθέσιμη υπολογιστική δυνατότητα, χωρητικότητα, δίκτυα και άλλες υπολογιστικές ικανότητες έτσι ώστε ο πελάτης να μπορεί να λειτουργήσει εφαρμογές οι οποίες μπορεί να είναι και λειτουργικά συστήματα και εφαρμογές. Ο πελάτης δεν έχει δυνατότητα να διαχειρίζεται ή να ελέγχει το υλικό μέσω του οποίου γίνεται διαθέσιμη η υπηρεσία αλλά έχει την δυνατότητα ελέγχου, διαχείρισης και αλλαγών πάνω στο λειτουργικό σύστημα, τον αποθηκευτικό χώρο, τις εφαρμογές, και πιθανώς ανά περίπτωση στην περιορισμένη δυνατότητα στην επιλογή συστατικών διαδικτύωσης (π.χ. firewalls κ.α.)

Ποια είναι τα διαφορετικά μοντέλα υλοποίησης cloud services

Private Cloud

Πρόκειται για υποδομή cloud η οποία λειτουργεί και εξυπηρετεί μόνο για έναν μόνο οργανισμός. Μπορεί να διαχειρίζεται και να παρακολουθείται η λειτουργία του από κάποιο άλλο τρίτο μέρος και μπορεί να φιλοξενείται και σε κάποιο μέρος εκτός των εγκαταστάσεων του εν λόγω οργανισμού.

Community cloud

Πρόκειται για υποδομή cloud η οποία διαμοιράζεται μεταξύ διαφόρων οργανισμών και υποστηρίζει μια συγκεκριμένη κοινότητα η οποία έχει κοινό ενδιαφέρον (αντικείμενο π.χ. σκοπό, απαιτήσεις ασφαλείας, πολιτική, ανάγκες συμμόρφωσης κ.α.). Μπορεί να διαχειρίζεται και να παρακολουθείται η λειτουργία του από τους οργανισμούς ή από κάποιο άλλο τρίτο μέρος και μπορεί να φιλοξενείται και σε κάποιο μέρος εκτός των εγκαταστάσεων των οργανισμών.

Public cloud

Πρόκειται για υποδομή cloud η οποία είναι διαθέσιμη στο ευρύ κοινό ή σε ένα μεγάλο κομμάτι της αγοράς. Ανήκει σε έναν οργανισμό ο οποίος πουλάει υπηρεσίες cloud.

Hybrid cloud

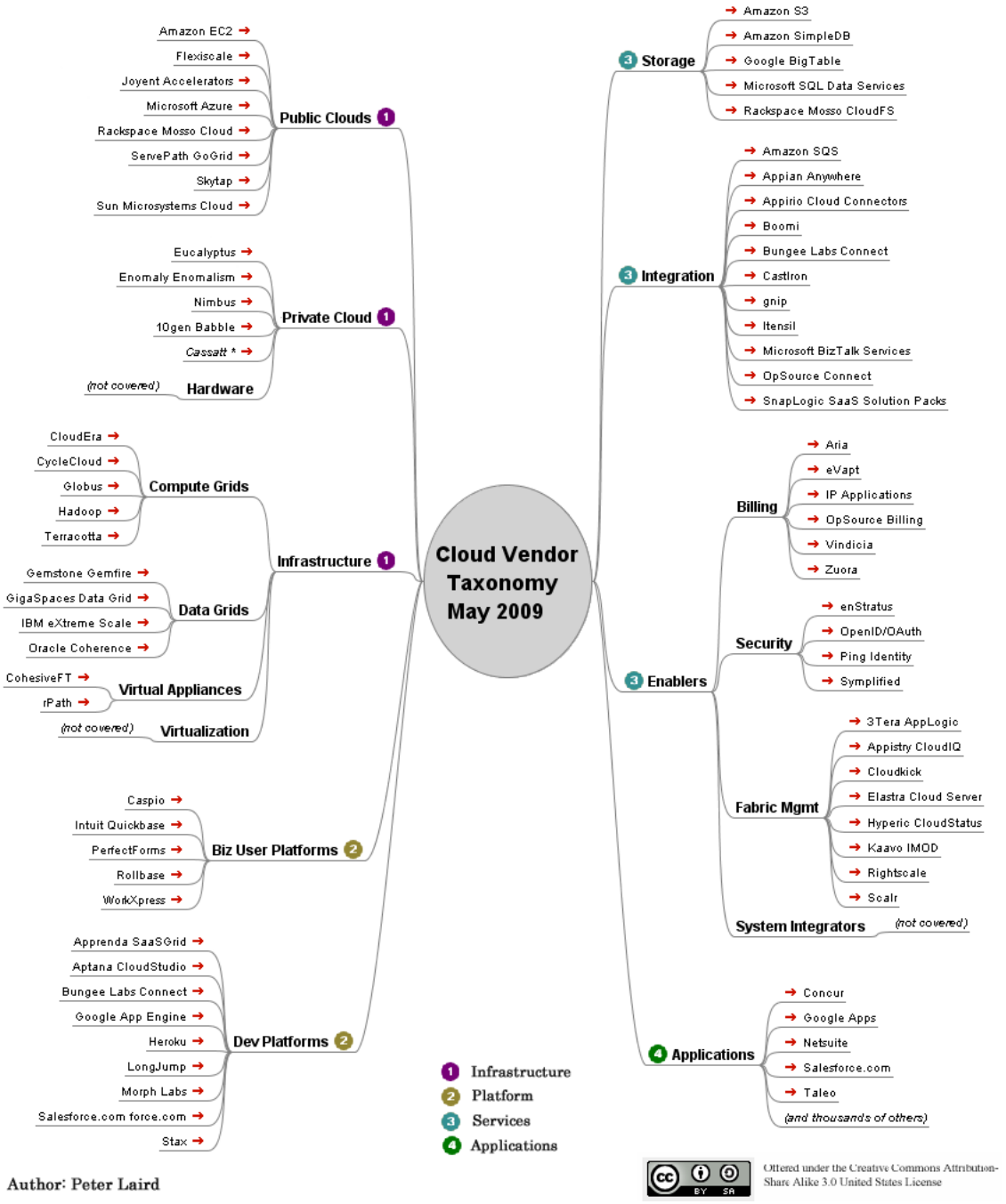
Πρόκειται για υποδομή cloud η οποία έχει προκύψει από τον συνδυασμό δυο ή περισσοτέρων cloud (private,community, or public) τα οποία παραμένουν ως διακριτές οντότητες , οι οποίες όμως είναι μεταξύ τους συνδεδεμένες μέσω τεχνολογιών που επιτρέπουν φορητότητα στα δεδομένα και τις εφαρμογές.

Δημοφιλή παραδείγματα ανά τύπο και μοντέλο

Στους παρόχους υπηρεσιών cloud computing ανήκουν και οι ακόλουθες εταιρίες και υπηρεσίες:

Nimbus	GoGrid	Cloudera
Amazon	Cloud9Analytics	Cloudscale
Force.com	Skytap	Arjuan
NetSuite	3Tera	3LeafSystems
Cloudshare	Appiro	Cohesiveft
Flexiscale	Appistry	Citrix
Wolf Frameworks	Rackspace	enStratus
RightScale	ReliaCloud	Cloud Leverage
Cirrhus9	Kaavo	Elastichosts
Monitis	Appnexus	Elastra
Joyent	BlueWolf	GigaSpaces
Enomaly	VMware	Citrix
HP	Intalio	Magic Software
IBM	EMC	UtilityStatus
10 Gen	Boomi	Symetriq
Akamai	AT&T	Google
Hadoop	CloudSwitch	
Synage	CloudWorks	

Το παρακάτω σχήμα δείχνει μερικά παραδείγματα υπηρεσιών cloud που προσφέρονται ανά τύπο:



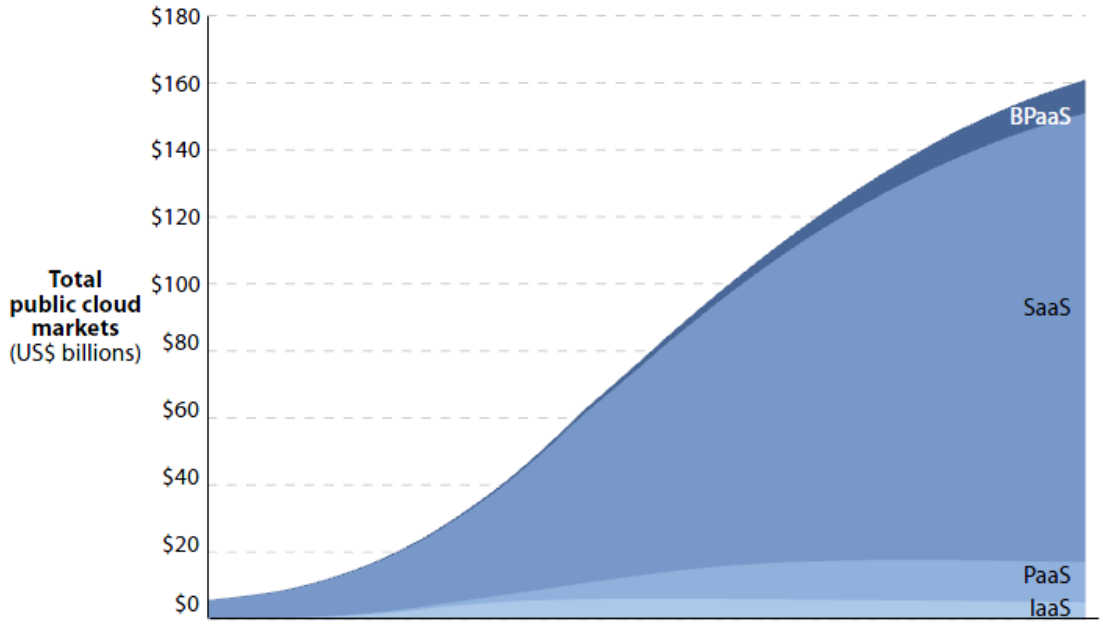
Σχήμα 1: Cloud Vendor Taxonomy

Ποια είναι τα trends σχετικά με το cloud computing

Η έννοια και η πρακτική του cloud computing έχει αναγνωριστεί από την αγορά. Συγκεκριμένα, μελέτες και έρευνες έχουν μετρήσει την κατάσταση στην οποία βρίσκεται η υιοθέτηση του cloud computing καθώς επίσης και ποια είναι τα επιμέρους στάδια στην πορεία εξέλιξης του [4]. [5]

Figure 3 Forecast: Global Public Cloud Market Size, 2011 To 2020

The spreadsheet detailing this forecast is available online.



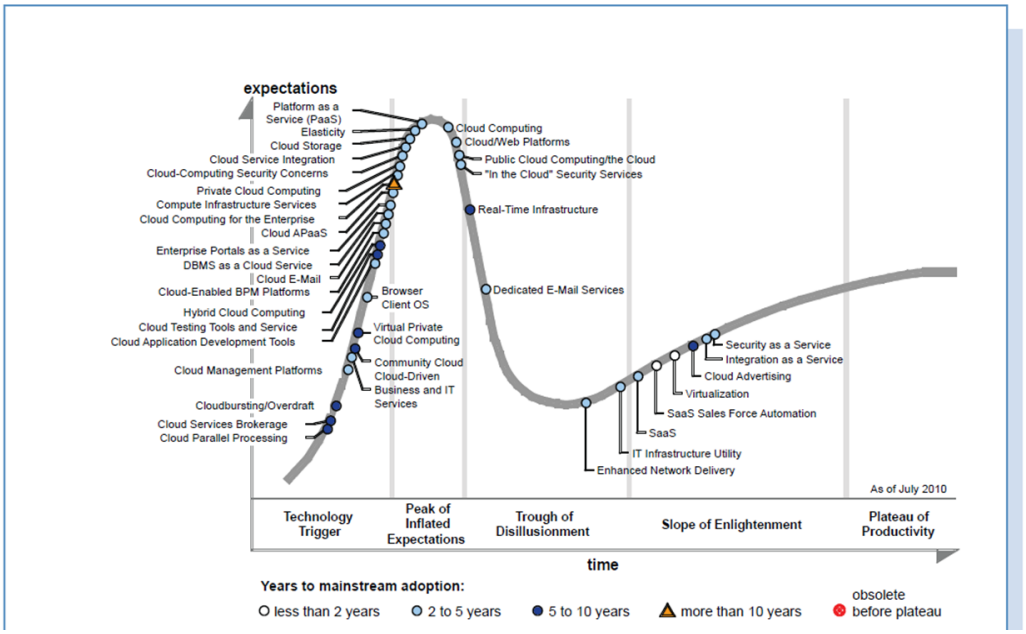
	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
BPaaS ($)	0.15	0.23	0.35	0.53	0.80	1.26	1.95	2.93	4.28	6.00	7.66	9.08	10.02
SaaS ($)	5.56	8.09	13.40	21.21	33.09	47.22	63.19	78.43	92.75	105.49	116.39	125.52	132.57
PaaS ($)	0.05	0.12	0.31	0.82	2.08	4.38	7.39	9.80	11.26	11.94	12.15	12.10	11.91
IaaS ($)	0.06	0.24	1.02	2.94	4.99	5.75	5.89	5.82	5.65	5.45	5.23	5.01	4.78

58161 Source: Forrester Research, Inc.

Σχήμα 2: Forrester Research

Καθώς επίσης και ,

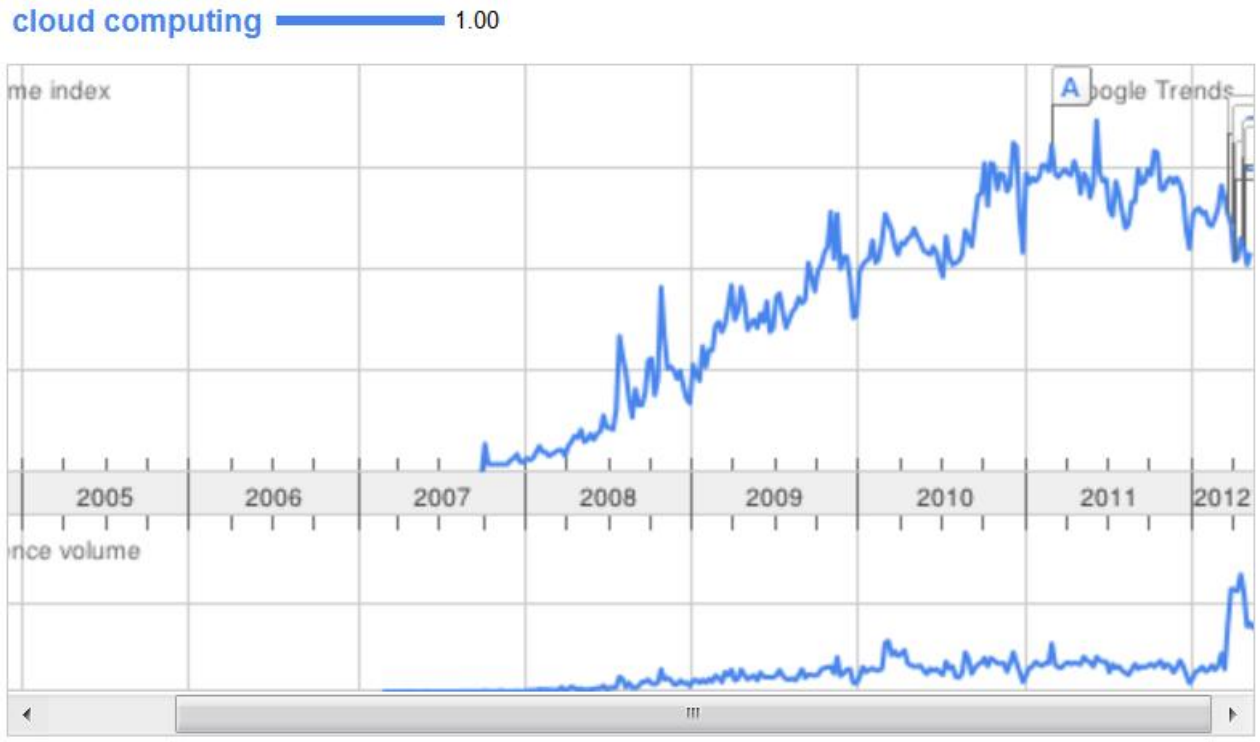
Figure 1. Hype Cycle for Cloud Computing, 2010



Σχήμα 3: Hype Cycle for Cloud Computing

[5]

Μετρήσεις στο διαδίκτυο (google trends) δείχνουν το συνεχιζόμενο ενδιαφέρον του ευρύ κοινού για την έννοια του CloudComputing.

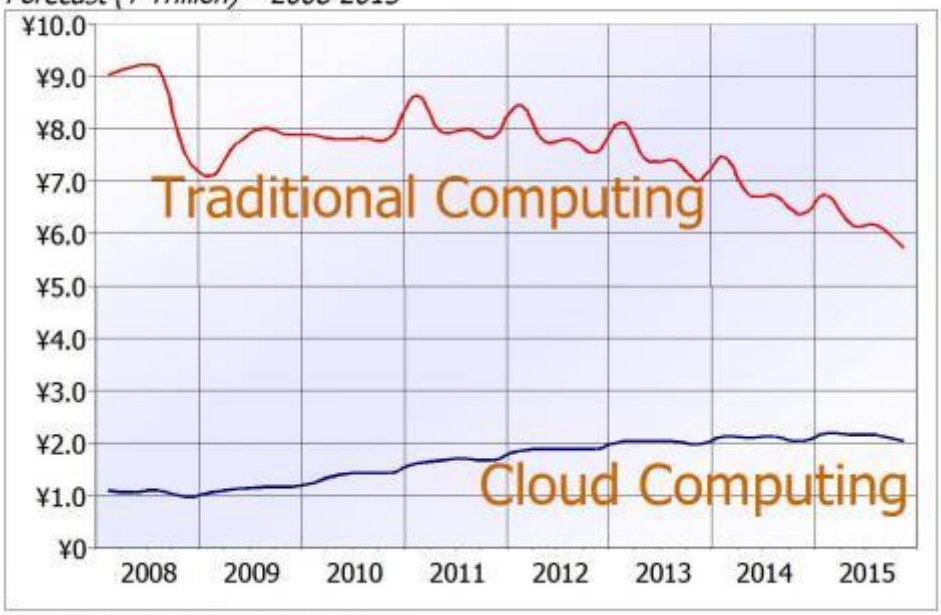


[6]

Σχήμα 4: Cloud Computing μέσω των Google trends

Καθώς επίσης και την πορεία του cloud computing σε σύγκριση με το παραδοσιακό computing (έρευνα για τα έτη 2008-2015 για την Ιαπωνία. Το μετρήσιμο μέγεθος είναι επένδυση σε χρήματα)

Figure 2 – Japan Traditional And Cloud Computing Quarterly Spending Forecast (¥ Trillion) – 2008-2015



Source: ITCandor, February 2011 [7]

Σχήμα 5: Πρόβλεψη για τις επενδύσεις σε cloud computing στην Ιαπωνία

Χαρακτηριστικά της υιοθέτησης του cloud computing

Πλεονεκτήματα και προστιθέμενη αξία του Cloud computing

Με βάση αυτά που περιγράφηκαν παραπάνω για τα βασικά πλεονεκτήματα του cloud computing, ο βαθμός υιοθέτησης είναι περιορισμένος ή μάλλον δεν είναι αντίστοιχος του πλήθους και της έκτασης των πλεονεκτημάτων.

What are the reasons behind your possible engagement in the Cloud Computing area?		
Answer Options	**Response Percent**	**Response Count**
Remove economic/expertise barriers impeding to modernize business processes by the introduction of Information Technology	30,6%	22
Avoiding capital expenditure in hardware, software, IT support, Information Security by outsourcing infrastructure/platforms/services	68,1%	49
Flexibility and scalability of IT resources	63,9%	46
Increasing computing capacity and business performance	36,1%	26
Diversification of IT systems	11,1%	8
Local and global optimisation of IT infrastructure through automated management of virtual machines	25,0%	18
Business Continuity and Disaster recovery capabilities	52,8%	38
Assessing the feasibility and profitability of new services (i.e. by developing business cases into the Cloud)	29,2%	21
Adding redundancy to increase availability and resilience	27,8%	20
Controlling marginal profit and marginal costs	15,3%	11
Other (please specify)	13,9%	10

Σχήμα 6: Αποτελέσματα έρευνας σχετικά με τους λόγους υιοθέτησης του cloud computing

Η έλλειψη αυτή έχει παρατηρηθεί και καταγραφεί μέσω μια σειράς από μελέτες – έρευνες. Μέσω των ερευνών αυτών έχει γίνει μια προσπάθεια αποσαφήνισης και απεικόνισης των εμποδίων στην υιοθέτηση του cloud computing.

Σύμφωνα με την έρευνα που δημοσιεύτηκε από την KPMG το 2011, [8] τα κύρια πλεονεκτήματα του cloud computing είναι η μείωση δαπανών, η βελτιωμένη ευελιξία και η καλύτερη scalability. Σύμφωνα με αυτούς που έχουν ήδη προχωρήσει στην υιοθέτηση

του cloud computing, θεωρούν ότι τους έχει φέρει μεγαλύτερη συγκέντρωση στους επιχειρησιακούς στόχους και μειωμένη πολυπλοκότητα στο IT. Συγκεκριμένα, οργανισμοί με περισσότερους από 5.000 χρήστες υπολογιστών δηλώνουν την ευελιξία ως έναν από τους σημαντικούς λόγους γιατί κάποιος θα πρέπει να μεταβεί στο «cloud». Ενώ, εξίσου ενθαρρυντικά και ιδιαίτερα θετικά ήταν και τα υπόλοιπα αποτελέσματα της έρευνας.

Σύμφωνα με την έρευνα: «Οι προσδοκίες είναι υψηλές και σήμερα κάθε μεγάλη εταιρία πληροφορικής προσφέρει υπηρεσίες στον χώρο του Cloud. Σύμφωνα με τον Γενικό Διευθυντή της Microsoft, Steve Ballmer, «το cloud computing είναι το επόμενο βήμα, η επόμενη φάση, είναι η επόμενη μετάβαση». Η εμπορική του βιωσιμότητα θα εξαρτηθεί από την θέληση και την διάθεση των πελατών να χρησιμοποιήσουν τις προσφερόμενες υπηρεσίες. Σύμφωνα με την έρευνα το 45% των συμμετεχόντων εταιριών χρησιμοποιούν ήδη υπηρεσίες cloud computing και 13% πρόκειται να τις υιοθετήσουν στους επόμενους 12 μήνες. Μόνο μια μικρή μειονότητα – 8%- δεν έχουν κάποια πρόθεση να υιοθετήσουν υπηρεσίες cloud computing.

Ποια είναι τα μεγαλύτερα προβλήματα του Cloud Computing.

Η πλειοψηφία των ερευνών καταλήγουν ότι ένα από τα μεγαλύτερα θέματα με το cloud computing είναι η ασφάλεια.

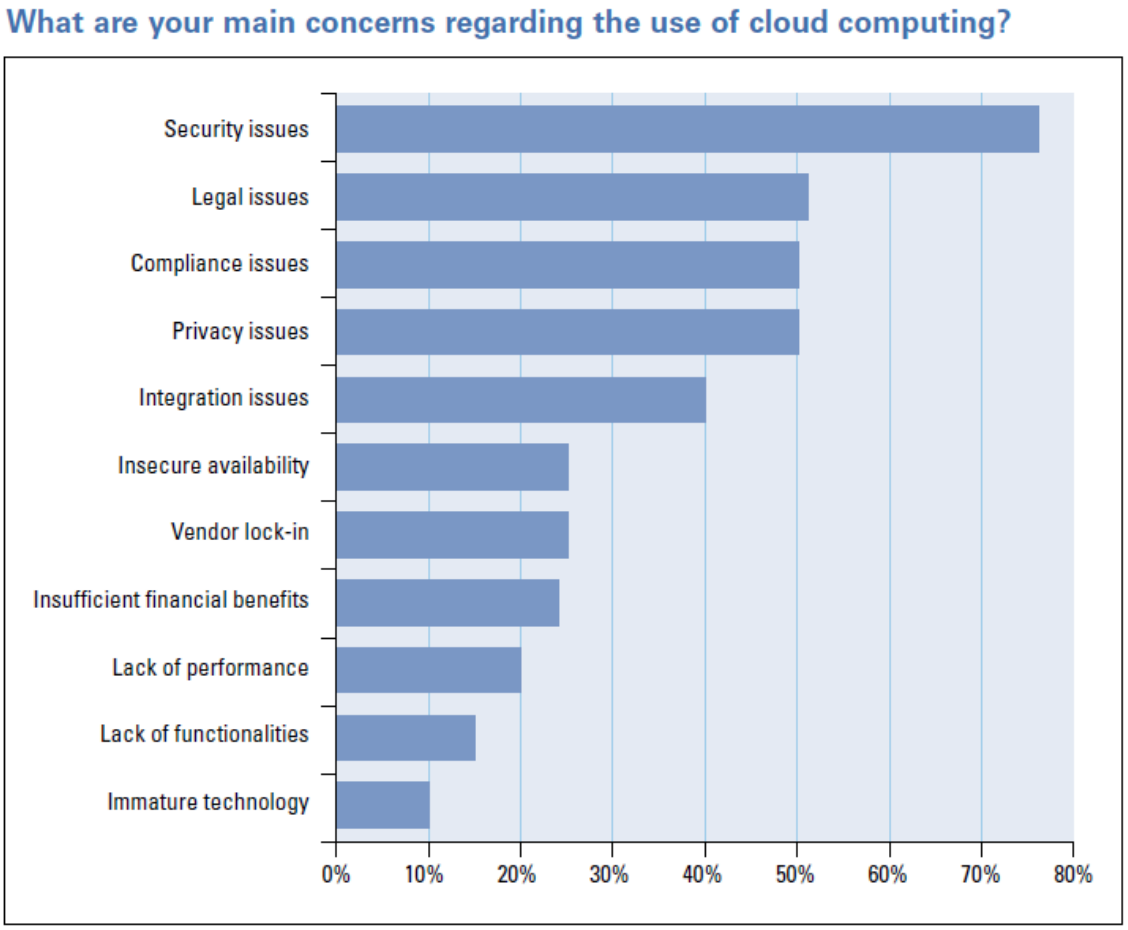
What are your main concerns in your approach to Cloud Computing?

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

Σχήμα 7: Αποτελέσματα μελέτης σχετικά με τα κυριότερα προβλήματα στην υιοθέτηση του cloud computing

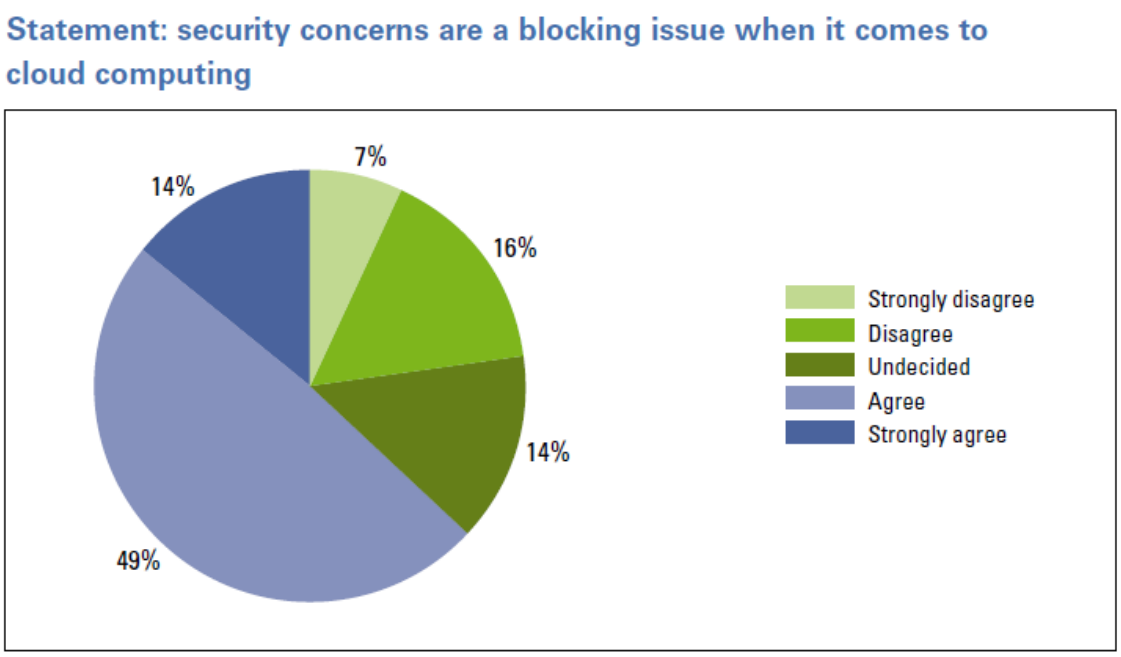
Από το έγγραφο The survey "An SME perspective on cloud computing, Νοέμβριος 2009, European Network and Information Security Agency (ENISA). [9]

Σύμφωνα με την έρευνα της KPMG, η ασφάλεια αποτελεί το κύριο εμπόδιο που συναντά κάποιος στην πορεία υλοποίησης μιας λύσης cloud computing, ενώ ακολουθούν η συμμόρφωση, η ιδιωτικότητα, και τα νομικά θέματα. Οι οργανισμοί ανησυχούν για την ασφάλεια και την ιδιωτικότητα, ειδικά (σύμφωνα πάλι με την έρευνα της KPMG) γιατί η αγορά προσφέρει οριακές διαβεβαιώσεις. Η ευθυγράμμιση των εσωτερικών απαιτήσεων ασφαλείας με τις δυνατότητες που προσφέρει η υποδομή, η υπηρεσία και η υλοποίηση του συγκεκριμένου μοντέλου cloud αποδεικνύεται δύσκολη στην εφαρμογή.



Σχήμα 8: Αποτελέσματα μελέτης σχετικά με τα μεγαλύτερα προβλήματα στην χρήση του cloud computing.

Ειδικά για τα θέματα ασφάλειας, 63% των συμμετεχόντων συμφωνούν ότι θέματα που σχετίζονται με την ασφάλεια αποτελούν εμπόδια στην μεγαλύτερη χρήση του cloud. Σύμφωνα με την έρευνα, εξάγεται το συμπέρασμα ότι δεν ανησυχούν κυρίως για την έλλειψη μέτρων ασφαλείας όσο για την έλλειψη διαφάνειας από την μεριά των παρόχων.



Σχήμα 9: Αποτελέσματα μελέτης σχετικά με τα μεγαλύτερα προβλήματα στην χρήση του cloud computing.

Είναι τα security concerns των υποψήφιων πελατών δικαιολογημένα;

Τι συμβαίνει στην πραγματικότητα;

Στο διαδίκτυο υπάρχουν ήδη πολλές αποδείξεις για τα μέτρα που λαμβάνουν οι πιο γνωστοί πάροχοι υπηρεσιών cloud όσο αφορά την φυσική και περιβαλλοντική ασφάλεια. (βλ. youtube: google datacenter, amazon datacenter, salesforce κ.α.). Από τις ξεναγήσεις αυτές και από άλλες δηλώσεις των εταιριών, φαίνονται οι προθέσεις τουλάχιστον των εν λόγω οργανισμών για την θωράκιση των υποδομών ενάντια σε φυσικές και περιβαλλοντικές απειλές. Όμως, από μόνα τους αυτά τα μέτρα και αυτές οι δηλώσεις δεν επαρκούν για να προσφέρουν τις διαβεβαιώσεις στους υποψήφιους πελάτες σχετικά με την εξασφάλιση των δεδομένων τους απέναντι σε διάφορες απειλές.

Όσο αφορά τις δεσμεύσεις και τα μέτρα ασφαλείας που λαμβάνονται από τους παρόχους υπηρεσιών cloud, αυτές μπορούν να αναζητηθούν μόνο μέσα στις αντίστοιχες συμβάσεις. Τμήματα των συμβάσεων αυτών περιέχονται στο Παράρτημα Α.

Μια ανασκόπηση των συμβάσεων αυτών, οδηγεί στα ακόλουθα συμπεράσματα:

- Ανεξάρτητα από το αν η υπηρεσία δίνεται επί πληρωμή ή δωρεάν και ανεξάρτητα από το πιο μοντέλο υπηρεσίας cloud παρέχεται (SaaS, PaaS, IaaS) ζητείται η δέσμευση του πελάτη σε συγκεκριμένους όρους
- Οι όροι των συμβάσεων αυτών (agreements) δεσμεύουν σε διαφορετικό βαθμό τον πάροχο και τον πελάτη.
- Σε κάθε περίπτωση υπάρχουν όροι που σχετίζονται με την έννοια της ασφάλειας (εμπιστευτικότητα, ακεραιότητα και σε κάποιες περιπτώσεις διαθεσιμότητα).
- Οι όροι ασφάλειας είναι περιγραφικοί και όχι συγκεκριμένοι. Δεν αναγράφεται σε καμία από τις συμφωνίες αυτές τι μέτρα λαμβάνονται αλλά ότι ο πάροχος δεσμεύεται να λάβει μέτρα.
- Ο όρος reasonable όσο αφορά την έκταση των μέτρων χρησιμοποιείται. Συνεπώς, δεν καθορίζεται κάποιο ελάχιστο κοινά αποδεκτό επίπεδο ασφαλείας.

Όλα τα παραπάνω οδηγούν στο συμπέρασμα ότι, υπάρχει βάση στις ανησυχίες των υποψηφίων πελατών σχετικά με το επίπεδο ασφαλείας των υπηρεσιών cloud.

Ανάλυση και αποτίμηση κινδύνου

Μεθοδολογίες για την ανάλυση και αποτίμηση κινδύνων που σχετίζονται με την ασφάλεια των πληροφοριών και τα συστήματα πληροφορικής υπάρχουν πολλές. Μάλιστα, ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια (ENISA, European Network and Information Security Agency) μέσω μιας ομάδας που συγκρότησε το 2005, δημοσίευσε μια λίστα με τις επικρατέστερες μεθοδολογίες αποτίμησης / διαχείρισης κινδύνου (Risk Assessment / Risk Management Methodologies, http://rm-inv.enisa.europa.eu/rm_ra_methods.html).

Παρόλο που η έννοια του cloud computing υπάρχει και χρησιμοποιείται στην αγορά τα τελευταία τρία χρόνια, έχει γίνει περιορισμένη έρευνα πάνω σε μεθοδολογίες ανάλυσης και αποτίμησης κινδύνου που να είναι ειδικά προσαρμοσμένες στις

ιδιαιτερότητες του Cloud computing. Συγκεκριμένα, οι Prasad Saripalli & Ben Walters προτείνουν ένα ποσοτικό πλαίσιο για την αποτίμηση των κινδύνων στο cloud computing το 2010 [10], ενώ ο ENISA [11], η CSA [12] και η Gardner [13], έχουν κάνει έρευνες για τους κινδύνου στο Cloud Computing και έχουν εκδώσει τα αποτελέσματα των ερευνών αυτών χωρίς όμως να δημοσιεύσουν την ακριβή μεθοδολογία την οποία ακολούθησαν. Επίσης, αξίζει να σημειωθεί ότι τα τελευταία χρόνια έχουν δημοσιευτεί πολλές εργασίες και άρθρα που πραγματεύονται τις απειλές και τα μέτρα ασφάλειας στο cloud computing χωρίς όμως (κατά την γνώμη μου) να έχουν την συστηματικότητα και την πληρότητα των αναφερόμενων παραπάνω. Ενδεικτικά παραδείγματα είναι: [14], [15], [16], [17], [18] και [19].

Η περίπτωση που ερευνάται στην συγκεκριμένη εργασία έχει την ιδιαιτερότητα ότι δεν ερευνά κάποιο συγκεκριμένο σύστημα το οποίο να μπορεί να αναλυθεί ως προς τους κινδύνους με ακρίβεια και άρα δεν μπορεί να εφαρμοστεί η μεθοδολογία των Prasad Saripalli & Ben Walters [10]. (Η μεθοδολογία είναι ποσοτική και βασίζεται στην γνώση με σχετική ακρίβεια πιθανοτήτων υλοποίησης συγκεκριμένων κινδύνων).

Συνεπώς, οι κίνδυνοι που αναγνωρίζονται στα πλαίσια της συγκεκριμένης εργασίας ως πιθανοί ειδικά για τις υπηρεσίες cloud είναι ο συνδυασμός των κινδύνων που αναφέρονται στις τρεις παραπάνω μελέτες.

Ένα μέρος των κινδύνων (απειλών) που έχουν αναγνωριστεί περιέχονται στον παρακάτω πίνακα, κατανεμημένοι ανάλογα με το μοντέλο της υπηρεσίας Cloud.

Πίνακας 1: Παραδείγματα Απειλών ανά μοντέλο υπηρεσίας Cloud.

SaaS	PaaS	IaaS
Insecure Interfaces and APIs	*Abuse and Nefarious Use of Cloud Computing*	*Abuse and Nefarious Use of Cloud Computing*
Malicious Insiders	*Insecure Interfaces and APIs*	*Insecure Interfaces and APIs*
Data Loss or Leakage	*Malicious Insiders*	*Malicious Insiders*
Account or Service Hijacking	*Shared Technology Issues*	*Data Loss or Leakage*
Unknown Risk Profile	*Data Loss or Leakage*	*Account or Service Hijacking*

Τι μπορεί να γίνει προκειμένου να ποσοτικοποιηθεί η ασφάλεια στις υπηρεσίες Cloud?

Το αντικείμενο της εργασίας αυτής είναι να προτείνει έναν τρόπο με τον οποίο ένας υποψήφιος πελάτης να μπορεί να μετρήσει με αντικειμενικό τρόπο το επίπεδο ασφαλείας των προσφερόμενων υπηρεσιών.

Αυτό από μόνο του οδηγεί σε έναν περιορισμό των απειλών σε εκείνες μόνο οι αδυναμίες και ο βαθμός έκθεσης ενός οργανισμού σε συγκεκριμένες απειλές μπορεί να μετρηθεί από απόσταση και αυτοματοποιημένα.

Αυτό σημαίνει ότι κίνδυνοι που αναφέρονται σε απειλές και αδυναμίες που σχετίζονται με θέματα φυσικής ασφάλειας, προστασίας και διαχείρισης από την πλευρά του προσωπικού του παρόχου δεν μπορούν να μετρηθούν.

Κατηγορίες Κινδύνων

Παρακάτω ακολουθούν οι κατηγορίες κινδύνων που παραμένουν χρησιμοποιώντας το παραπάνω φίλτρο. Για να μπορεί να διαβαστεί ο παρακάτω πίνακας θα πρέπει να λάβουμε υπόψη μας τον τρόπο υπολογίσιμου του κινδύνου. Ο κίνδυνος (Risk) προκύπτει από το γινόμενο της Πιθανότητας να εκδηλωθεί μια απειλή (Probability) με την επίπτωση (Impact) στα δεδομένα και στην λειτουργία που θα προκύψει αν η απειλή πραγματοποιηθεί. Τα αποτελέσματα του γινομένου αυτού για κάθε διαφορετικό ζευγάρι τιμών αποτυπώνονται στον παρακάτω πίνακα. Ο πίνακας αντιστοιχεί σε μια από τις προτεινόμενες μεθοδολογίες αποτίμησης κινδύνου όπως αυτή περιγράφεται στο πρότυπο ISO 27005:2011. [20]

Πίνακας 2 Πίνακας συσχέτισης μεγεθών αποτίμησης κινδύνου

	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

Επίσης, ο προκύπτων κίνδυνος μετράται σε μια κλίμακα 0 ως 8,στοιχείο που μπορεί στην συνέχεια να μας βοηθήσει στην δημιουργία κριτηρίων αποδοχής. Η κλίμακα κινδύνου σε αυτή την περίπτωση είναι απλή και αποτελείται από την ακόλουθη αντιστοιχία:

Πίνακας 3: Πίνακας αντιστοιχίας περιγραφής επιπέδου κινδύνου και κλίμακας μεθοδολογίας κινδύνου

Low risk: 0-2	Medium Risk: 3-5	High Risk: 6-8

Στην μελέτη / ανάλυση αυτή κάθε κίνδυνος (risk) φέρει έναν μοναδικό αριθμό και έναν τίτλο π.χ. R.4 LOSS OF BUSINESS REPUTATION DUE TO CO-TENANT ACTIVITIES. Για κάθε κίνδυνο έχει προσδιοριστεί η Πιθανότητα να υλοποιηθεί ο κίνδυνος (Probability) π.χ. σε συνέχεια του προηγούμενου παραδείγματος Probability: Low, και η επίπτωση impact στην υπηρεσία και τα δεδομένα του πελάτη π.χ. σε συνέχεια του προηγούμενου παραδείγματος Impact: High. Βάση του πίνακα που φαίνεται παραπάνω, ο συνδυασμός Probability: Low και Impact: High, δίνουν Επίπεδο κινδύνου 4, δηλαδή Medium. Για να μπορέσει να υλοποιηθεί αυτή η απειλή και να υπάρχει και η αντίστοιχη επίπτωση, θα πρέπει να υπάρχουν συγκεκριμένες αδυναμίες τις οποίες μπορεί να εκμεταλλευτεί μια απειλή. Π.χ. σε συνέχεια του προηγούμενου παραδείγματος οι Αδυναμίες είναι V6. Lack of resource isolation, V7. Lack of reputational isolation και V5. HYPERVISOR VULNERABILITIES. Τέλος στο πεδίο Details, περιέχονται κάποιες επιπλέον διευκρινιστικές πληροφορίες προκειμένου να μπορεί να γίνει περισσότερο κατανοητός ο κίνδυνος.

R.4 Απώλεια της Φήμης του οργανισμού λόγω των ενεργειών των συν-ενοικιαστών

(LOSS OF BUSINESS REPUTATION DUE TO CO-TENANT ACTIVITIES)

Probability: Low

Impact: High

Risk: 4

Αδυναμίες:

V5. Αδυναμίες του hypervisor (Hypervisor Vulnerabilities)

V6. Έλλειψη απομόνωσης πόρων (Lack of resource isolation)

V7. Έλλειψη απομόνωσης φήμης Lack of reputational isolation

Λεπτομέρειες:

Στην περίπτωση που υπάρχει διαμοιρασμός πόρων ανάμεσα σε διαφορετικούς χρήστες (ή οργανισμούς), σημαίνει ότι κακόβουλες ενέργειες που υλοποιούνται από τον ένα χρήστη (ένοικο) μπορεί να επηρεάσουν και την λειτουργία και φήμη του άλλου χρήστη (ένοικου). Για παράδειγμα, η αποστολή spam e-mails, η διενέργεια port scans ή η δημοσίευση και διοχέτευση κακόβουλου λογισμικού από μια υποδομή cloud μπορεί να οδηγήσει σε π.χ. αποκλεισμό των IP που χρησιμοποιούν οι χρήστες (ένοικοι) (του επιτιθέμενου μαζί με τους υπόλοιπους «αθώους» μια και συνήθως μοιράζονται το ίδιο IP range), ή σε κατανάλωση των πόρων από τον κακόβουλο χρήστη με αποτέλεσμα την μειωμένη διαθεσιμότητα για τους υπόλοιπους χρήστες κ.α.

R.8 Εξάντληση πόρων

(RESOURCE EXHAUSTION (UNDER OR OVER PROVISIONING))

Probability:

A. Ανικανότητα να διαθέσει επιπλέον χωρητικότητα προς τον πελάτη: MEDIUM

B. Ανικανότητα να διαθέσει την τρέχουσα και συμφωνηθείσα χωρητικότητα προς τον πελάτη: LOW

C. Ανικανότητα να διαθέσει επιπλέον χωρητικότητα προς τον πελάτη: LOW/MEDIUM (π.χ. σε συγκεκριμένες χρονικές εποχές Χριστούγεννα κ.α.)

Impact: High

Risk: 4

Αδυναμίες

V15. Μη Ακριβής μοντελοποίηση της χρήσης των πόρων (Inaccurate modeling of resource usage)

V27. Ανεπαρκής διαδικασία προμήθειας και επένδυσης σε υποδομή(Inadequate resource provisioning and investments in infrastructure)

V28. Απουσία πολιτικής σχετικά με ανώτατα όρια στους πόρους (No policies for resource capping)

V47. Απουσία πλεονασμού προμηθευτή (Lack of supplier redundancy)

Λεπτομέρειες

Οι υπηρεσίες cloud είναι υπηρεσίες που δουλεύουν χρησιμοποιώντας ένα μοντέλο on-demand. Ο χρήστης χρησιμοποιεί την υπηρεσία όταν την χρειάζεται. Υπάρχει η συμφωνία για το επίπεδο και τους πόρους που ενοικιάζει ο χρήστης αλλά μπορεί ανάλογα με τις ανάγκες του να ζητήσει παραπάνω, εκμεταλλευόμενος ένα από τα βασικά χαρακτηριστικά των υπηρεσιών cloud - Rapid elasticity. Ο διαμοιρασμός και καταμερισμός των πόρων του παρόχου γίνεται με την χρήση στατιστικών προβλέψεων. Αυτό εμπεριέχει τον κίνδυνο ότι αν οι προβλέψεις αυτές έχουν γίνει με λάθος τρόπο λόγω κακής χρήσης των αλγορίθμων/ μοντέλων ή λόγω κακής ποιότητας δεδομένων, μπορεί ο οργανισμός να μην έχει λάβει τα απαραίτητα μέτρα (επενδύσεις) ή να μην έχει ορθά καταμερίσει τους πόρους. Αυτό με την σειρά του μπορεί να οδηγήσει σε μη διαθεσιμότητα της υπηρεσίας (Denial of Service / Service Unavailability).

R.9 Αστοχία στην απομόνωση των πόρων (Isolation Failure)

Probability:

A. Private Cloud: LOW

B. Public Cloud: MEDIUM

Impact: Very High

Risk: 6

Αδυναμίες

V5. Αδυναμίες του hypervisor (Hypervisor Vulnerabilities)

V6. Έλλειψη απομόνωσης πόρων (Lack of resource isolation)

V7. Έλλειψη απομόνωσης φήμης Lack of reputational isolation

V17. Πιθανότητα ότι θα γίνει έλεγχος από το εσωτερικό του cloud (Possibility that internal (cloud) network probing will occur)

V18.Πιθανότητα ότι θα διενεργηθούν έλεγχοι συνύπαρξης (Possibility that co-residence checks will be performed)

Λεπτομέρειες

Ο κίνδυνος αυτό περιλαμβάνει την αστοχία των μηχανισμών που χρησιμοποιεί ο πάροχος για τον διαμοιρασμό των πόρων μεταξύ των ενοίκων (π.χ. μνήμη, χωρητικότητα κ.α.). Ενδεικτικά αναφέρεται ως παράδειγμα μια επίθεση SQL injection από έναν πελάτη / ένοικο σε κάποιον άλλο, με τον οποίο μοιράζονται τους ίδιους πίνακες σε μια βάση δεδομένων.

R.11 Διακύβευση του interface για την διαχείριση της υπηρεσίας (Management interface compromise (manipulation, availability of infrastructure))

Probability: MEDIUM

Impact: Very High

Risk: 6

Αδυναμίες

V1. Αδυναμίες AAA (AAA Vulnerabilities)

V4. Δυνατότητα απομακρυσμένης πρόσβασης στο interface διαχείρισης (Remote access to management interface)

V38. Κακή διαμόρφωση (Misconfiguration)

V39. Αδυναμίες του συστήματος ή του λειτουργικού συστήματος (System or OS vulnerabilities)

V48. Αδυναμίες των εφαρμογών ή κακή διαχείριση των ενημερώσεων (patch) (Application vulnerabilities or poor patch management)

Λεπτομέρειες

Επειδή η πρόσβαση των υπηρεσιών γίνεται μέσω του διαδικτύου, για να μπορεί ο πελάτης να έχει πρόσβαση και να διαχειρίζεται (στον βαθμό που επιτρέπεται από το είδος της υπηρεσίας που του παρέχεται) την υπηρεσία του διατίθεται ένα interface. Μέσα από αυτό ο εξουσιοδοτημένος χρήστης διαχείρισης της εταιρίας μπορεί να εκτελέσει ενέργειες υψηλότερου επιπέδου από αυτό των τυπικών χρηστών. Και επειδή το interface

αυτό είναι δημόσια προσπελάσιμο και έχει αυτά τα υψηλότερα δικαιώματα και λειτουργίες, αποτελεί και έναν μεγαλύτερο κίνδυνο.

R.12 Υποκλοπή των δεδομένων κατά την μεταφορά

(Intercepting data in transit)

Probability: MEDIUM

Impact: High

Risk: 5

Αδυναμίες

V1. Αδυναμίες AAA (AAA Vulnerabilities)

V8.Αδυναμίες της κρυπτογράφησης της επικοινωνίας (Communication encryption Vulnerabilities)

V9. Απουσία ύπαρξης ή αδύναμη κρυπτογράφηση στα δεδομένα που μεταφέρονται ή αποθηκεύονται (Lack of or weak encryption of archives and data in transit)

V17. Πιθανότητα ότι θα γίνει έλεγχος από το εσωτερικό του cloud (Possibility that internal (cloud) network probing will occur)

V18.Πιθανότητα ότι θα διενεργηθούν έλεγχοι συνύπαρξης (Possibility that co-residence checks will be performed)

V31. Απουσία όρων ή απουσία διαφάνειας στους όρους χρήσης (Lack of completeness and transparency in terms of use)

Λεπτομέρειες

Σε αντίθεση με τις τυπικές υποδομές, στο Cloud computing εξ ορισμού υπάρχουν περισσότερα δεδομένα που μεταφέρονται. Για παράδειγμα, δεδομένα πρέπει να μεταφερθούν προκειμένου να συγχρονιστούν δεδομένα ανάμεσα σε διάφορα φυσικά και ιδεατά μηχανήματα, ανάμεσα στον διαχειριστή και ανάμεσα στους χρήστες. Επίσης, έχει παρατηρηθεί ότι σε αντίθεση με τις τυπικές υλοποιήσει που η απομακρυσμένη πρόσβαση υλοποιήσει μέσω κάποιου είδους secure vpn σύνδεσης, στο περιβάλλον cloud ο ένοικος αρκείται στην χρήση των παρεχόμενων μηχανισμών από την μεριά του παρόχου για την πρόσβαση στην υπηρεσία. Σε κάποιες περιπτώσεις δεν υπάρχει γνώση από την μεριά του ενοίκου για το αν χρησιμοποιείται κάποιος μηχανισμός για την προστασία των δεδομένων κατά την μεταφορά.

Sniffing, spoofing, επιθέσεις man-in–the-middle, side channel attacks είναι πιθανές μεθοδολογίες που μπορεί να εξαπολύσει κάποιος προκειμένου να υποκλέψει τα δεδομένα κατά την μεταφορά τους.

R.13 Διαρροή δεδομένων κατά το ανέβασμα και το κατέβασμά τους στο cloud (Data leakage on up/download, intra-cloud)

Probability: MEDIUM

Impact: High

Risk: 5

Αδυναμίες

V1. Αδυναμίες AAA (AAA Vulnerabilities)

V8.Αδυναμίες της κρυπτογράφησης της επικοινωνίας (Communication encryption Vulnerabilities)

V10. Αδυναμία επεξεργασίας των δεδομένων σε κρυπτογραφημένη μορφή (Impossibility of processing data in encrypted form)

V17. Πιθανότητα ότι θα γίνει έλεγχος από το εσωτερικό του cloud (Possibility that internal (cloud) network probing will occur)

V18.Πιθανότητα ότι θα διενεργηθούν έλεγχοι συνύπαρξης (Possibility that co-residence checks will be performed)

V48. Αδυναμίες των εφαρμογών ή κακή διαχείριση των ενημερώσεων (patch) (Application vulnerabilities or poor patch management)

R.15 Κατανεμημένη απώλεια υπηρεσίας - DDoS (Distributed Denial of Service DDoS)

Probability: Πελάτης: MEDIUM / Πάροχος: LOW

Impact: Πελάτης: HIGH / Πάροχος: VERY HIGH

Risk: 5

Αδυναμίες

V38. Κακή διαμόρφωση (Misconfiguration)

V39. Αδυναμίες του συστήματος ή του λειτουργικού συστήματος (System or OS vulnerabilities)

V53. Μη επαρκείς ή με κακή διαμόρφωση πόροι που ελέγχουν (φιλτράρουν) την πρόσβαση (Inadequate or misconfigured filtering resources)

R.15 Διεξαγωγή κακόβουλων ελέγχων

(Undertaking Malicious probes or scans)

Probability: MEDIUM

Impact: MEDIUM

Risk: 4

Αδυναμίες

V17. Πιθανότητα ότι θα γίνει έλεγχος από το εσωτερικό του cloud (Possibility that internal (cloud) network probing will occur)

V18.Πιθανότητα ότι θα διενεργηθούν έλεγχοι συνύπαρξης (Possibility that co-residence checks will be performed)

R.19 Διακύβευση της μηχανής παροχής υπηρεσίας

(Compromise service engine)

Probability: LOW

Impact: VERY HIGH

Risk: 5

Αδυναμίες

V5. Αδυναμίες του hypervisor (Hypervisor Vulnerabilities)

V6. Έλλειψη απομόνωσης πόρων (Lack of resource isolation)

Λεπτομέρειες

Προκειμένου να μπορεί να παρασχεθεί η κάθε υπηρεσία cloud στηρίζεται σε μια εξειδικευμένη πλατφόρμα που ονομάζεται service engine. Το service engine επικάθεται στους φυσικούς υλικούς πόρους και διαχειρίζεται τους πόρους του πελάτη σε διάφορα επίπεδα. Για παράδειγμα, στην περίπτωση IaaS cloud, το service engine είναι ο hypervisor. Σε κάποιες περιπτώσεις το service engine αναπτύσσεται και υποστηρίζεται από τις αντίστοιχες εταιρίες και σε κάποιες περιπτώσεις και από την κοινότητα ανοικτού κώδικα. Ανά περίπτωση οι πλατφόρμες αυτές μπορεί να παραμετροποιηθούν ξεχωριστά και ειδικά για χωριστό πάροχο υπηρεσιών cloud. Προφανώς, όπως οποιαδήποτε

εφαρμογή έτσι και το service engine μπορεί να έχει αδυναμίες και να είναι επιρρεπές σε επιθέσεις ή μη αναμενόμενες αστοχίες. Ένας επιτιθέμενος μπορεί να παρεισφρήσει μέσα σε ένα π.χ. ιδεατό μηχάνημα (virual machine) και να διακυβεύσει το σύνολο της λειτουργίας του service engine και συνεπώς και του παρόχου. Ενώ επίσης αν κάποιος παρεισφρήσει στο service engine μπορεί να έχει πρόσβαση σε όλες τις πιθανές πληροφορίες που είναι αποθηκευμένες μέσα σε αυτόν και να μπορεί στην συνέχεια να τις επεξεργαστεί, να παρακολουθήσει την χρήση τους ή να επέμβει σε μεγαλύτερο επίπεδο και να επηρεάσει τον τρόπο που είναι διαμοιρασμένοι οι πόροι κα.

R.25 Παραβιάσεις του δικτύου

(Network Breaks)

Probability: LOW

Impact: VERY HIGH

Risk: 5

Αδυναμίες

V6. Έλλειψη απομόνωσης πόρων (Lack of resource isolation)

V38. Κακή διαμόρφωση (Misconfiguration)

V39. Αδυναμίες του συστήματος ή του λειτουργικού συστήματος (System or OS vulnerabilities)

V41. Σχέδιο συνέχισης επιχειρησιακής λειτουργίας και Σχέδιο ανάκαμψης από καταστροφή τα οποία είναι ελλειπή ή δεν έχουν δοκιμαστεί ή απουσιάζουν εντελώς (Lack of, or a poor and untested, business continuity and disaster recovery plan)

Λεπτομέρειες

Πρόκειται για έναν κίνδυνο που αν υλοποιηθεί μπορεί να επηρεάσει το σύνολο των πελατών του παρόχου.

R.26 Διαχείριση Δικτύου

(Network Management)

Probability: MEDIUM

Impact: VERY HIGH

Risk: 6

Αδυναμίες

V6. Έλλειψη απομόνωσης πόρων (Lack of resource isolation)

V38. Κακή διαμόρφωση (Misconfiguration)

V39. Αδυναμίες του συστήματος ή του λειτουργικού συστήματος (System or OS vulnerabilities)

V41. Σχέδιο συνέχισης επιχειρησιακής λειτουργίας και Σχέδιο ανάκαμψης από καταστροφή τα οποία είναι ελλειπή ή δεν έχουν δοκιμαστεί ή απουσιάζουν εντελώς (Lack of, or a poor and untested, business continuity and disaster recovery plan)

R.27 Αλλαγή στην κίνηση δικτύου

(Modifying Network Traffic)

Probability: LOW

Impact: HIGH

Risk: 4

Αδυναμίες

V2.Αδυναμίες στην διαχείριση δικαιωμάτων χρηστών (User provisioning vulnerabilities)

V3. Αδυναμίες στην απομάκρυνση δικαιωμάτων χρηστών (User de-provisioning vulnerabilities)

V8.Αδυναμίες της κρυπτογράφησης της επικοινωνίας (Communication encryption Vulnerabilities)

V16.Αδυναμία ελέγχου της διεργασίας αποτίμησης αδυναμιών (No control on vulnerability assessment process)

R.28 Κλιμάκωση δικαιωμάτων

(PRIVILEGE ESCALATION**)**

Probability: LOW

Impact: HIGH

Risk: 4

Αδυναμίες

V1. Αδυναμίες AAA (AAA Vulnerabilities)

V2.Αδυναμίες στην διαχείριση δικαιωμάτων χρηστών (User provisioning vulnerabilities)

V3. Αδυναμίες στην απομάκρυνση δικαιωμάτων χρηστών (User de-provisioning vulnerabilities)

V5. Αδυναμίες του hypervisor (Hypervisor Vulnerabilities)

V34. Μη ξεκάθαρα ορισμένοι ρόλοι και υπευθυνότητες (Unclear roles and responsibilities)

V35. Κακή εφαρμογή των ρόλων (Poor enforcement of role definitions)

V36. Δεν εφαρμόζεται η αρχή Need-to-know (Need-to-know principle not applied)

V38. Κακή διαμόρφωση (Misconfiguration)

Λεπτομέρειες

Όταν υπάρχει διαμοιρασμός πόρων υπάρχει πάντα η πιθανότητα οι κακόβουλες δραστηριότητες ενός χρήση (ενοίκου) να έχουν κάποια (κακή) επίπτωση και στην φήμη του άλλου χρήστη (ενοίκου). Για παράδειγμα αποστολή spam e-mails από την δημόσια IP του παρόχου, την οποία την ίδια ή πιο πιθανά στο ίδιο range να χρησιμοποιούν και οι υπόλοιποι ένοικοι. Αυτό θα είχε ως αποτέλεσμα οι συγκεκριμένες IP να σημανθούν ως spammers και να μπουν στην αντίστοιχη black list παρεμποδίζοντας έτσι την σωστή λειτουργία των άλλων ενοίκων. Το ίδιο ισχύει και με άλλες ενέργειες όπως π.χ. port scanning κ.α.

Αδυναμίες

Δεδομένου ότι οι απειλές υπάρχουν αλλά εκδηλώνονται μόνο όταν μπορούν να εκμεταλλευτούν (exploit) κάποια αδυναμία, αρκεί κάποιος να μπορεί να αναγνωρίσει τον βαθμό ύπαρξης των σχετικών αδυναμιών. Ήδη στην βιβλιογραφία υπάρχουν αρκετές πηγές για αδυναμίες στο Cloud computing. Ενδεικτικά αναφέρονται οι: [21] και [22].

Οι αδυναμίες που σχετίζονται με τους παραπάνω κινδύνους και απειλές περιέχονται στον ακόλουθο πίνακα.

Πίνακας 4 Ονομαστικός πίνακας Αδυναμιών

Αναγνωριστικό	**Περιγραφή**
V1	Αδυναμίες AAA (AAA Vulnerabilities)
V2	Αδυναμίες στην διαχείριση δικαιωμάτων χρηστών (User provisioning vulnerabilities)
V3	Αδυναμίες στην απομάκρυνση δικαιωμάτων χρηστών (User de-provisioning vulnerabilities)
V4	Δυνατότητα απομακρυσμένης πρόσβασης στο interface διαχείρισης (Remote access to management interface)
V5	Αδυναμίες του hypervisor (Hypervisor Vulnerabilities)
V6	Έλλειψη απομόνωσης πόρων (Lack of resource isolation)
V7	Έλλειψη απομόνωσης φήμης (Lack of reputational isolation)
V8	Αδυναμίες της κρυπτογράφησης της επικοινωνίας (Communication encryption Vulnerabilities)
V9	Απουσία ύπαρξης ή αδύναμη κρυπτογράφηση στα δεδομένα που μεταφέρονται ή αποθηκεύονται (Lack of or weak encryption of archives and data in transit)
V10	Αδυναμία επεξεργασίας των δεδομένων σε κρυπτογραφημένη μορφή (Impossibility of processing data in encrypted form)
V15	Μη Ακριβής μοντελοποίηση της χρήσης των πόρων (Inaccurate modelling of resource usage)
V16	Αδυναμία ελέγχου της διεργασίας αποτίμησης αδυναμιών (No control on vulnerability assessment process)
V17	Πιθανότητα ότι θα γίνει έλεγχος από το εσωτερικό του cloud (Possibility that internal (cloud) network probing will occur)
V18	Πιθανότητα ότι θα διενεργηθούν έλεγχοι συνύπαρξης (Possibility that co-residence checks will be performed)
V27	Ανεπαρκής διαδικασία προμήθειας και επένδυσης σε υποδομή(Inadequate resource provisioning and investments in infrastructure)
V28	Απουσία πολιτικής σχετικά με ανώτατα όρια στους πόρους (No policies for resource capping)
V31	Απουσία όρων ή απουσία διαφάνειας στους όρους χρήσης (Lack of completeness and transparency in terms of use)
V34	Μη ξεκάθαρα ορισμένοι ρόλοι και υπευθυνότητες (Unclear roles and responsibilities)
V35	Κακή εφαρμογή των ρόλων (Poor enforcement of role definitions)
V36	Δεν εφαρμόζεται η αρχή Need-to-know (Need-to-know principle not applied)
V38	Κακή διαμόρφωση (Misconfiguration)
V39	Αδυναμίες του συστήματος ή του λειτουργικού συστήματος (System or OS vulnerabilities)

V41	Σχέδιο συνέχισης επιχειρησιακής λειτουργίας και Σχέδιο ανάκαμψης από καταστροφή τα οποία είναι ελλειπή ή δεν έχουν δοκιμαστεί ή απουσιάζουν εντελώς (Lack of, or a poor and untested, business continuity and disaster recovery plan)
V47	Απουσία πλεονασμού προμηθευτή (Lack of supplier redundancy)
V48	Αδυναμίες των εφαρμογών ή κακή διαχείριση των ενημερώσεων (patch) (Application vulnerabilities or poor patch management)
V53	Μη επαρκείς ή με κακή διαμόρφωση πόροι που ελέγχουν (φιλτράρουν) την πρόσβαση (Inadequate or misconfigured filtering resources)

Ενώ στον ακόλουθο πίνακα φαίνεται η σύνδεση ανάμεσα στις απειλές και στο επίπεδο του παραγόμενου κινδύνου. Δηλαδή:

Αδυναμίες σχετικά με τον τρόπο αυθεντικοποίησης, αναγνώρισης και ελέγχου της πρόσβασης ενός χρήστη στο σύστημα, σχετίζεται με τους κινδύνους R12, R13, R28 και σε κάθε περίπτωση το αποτέλεσμα εκδήλωσης αυτών των κινδύνων είναι Medium.

Πίνακας 5 Αποτύπωση της σύνδεση ανάμεσα στις απειλές, στο επίπεδο του παραγόμενου κινδύνου και στην συχνότητα εμφάνισης της κάθε αδυναμίας στον αντίστοιχο κίνδυνο

Number	Description	R4	R8	R9	R11	R12	R13	R15	R18	R19	R25	R26	R27	R28	Count	Max
V1	AAA vulnerabilities				H	M	M							M	4	H
V2	User provisioning vulnerabilities												M	M	2	M
V3	User de-provisioning vulnerabilities												M	M	2	M
V4	Remote access to management interface				H										1	H
V5	Hypervisor vulnerabilities	M		H						M				M	4	H
V6	Lack of resource isolation	M		H						M	M	H			5	H
V7	Lack of reputational isolation	M		H											2	H
V8	Communication encryption vulnerabilities					M	M						M		3	M
V9	Lack of or weak encryption of archives and data in transit					M									1	M
V10	Impossibility of processing data in encrypted form						M								1	M
V15	Inaccurate modelling of resource usage		M												1	M
V16	No control on vulnerability assessment process Affected assets												M		1	M
V17	Possibility that internal (cloud) network probing will occur			H		M	M		M						4	H
V18	Possibility that co-residence checks will be performed			H		M	M		M						4	H
V27	Inadequate resource provisioning and investments in infrastructure		M												1	M
V28	No policies for resource capping		M												1	M
V31	Lack of completeness and transparency in terms of use Affected assets					M									1	M
V34	Unclear roles and responsibilities													M	1	M
V35	Poor enforcement of role definitions													M	1	M
V36	Need-to-know principle not applied													M	1	M
V38	Misconfiguration				H			M			M	H		M	5	H
V39	System or OS vulnerabilities				H			M			M	H			4	H
V41	Lack of, or a poor and untested, business continuity and disaster recovery plan Affected assets										M	H			2	H
V47	Lack of supplier redundancy Affected assets		M												1	M
V48	Application vulnerabilities or poor patch management Affected assets				H		M								2	H
V53	Inadequate or misconfigured filtering resources Affected assets							M							1	M

Στην ενότητα που ακολουθεί αναλύονται οι αδυναμίες και ορίζεται ένα baseline με βάση διάφορες πηγές βιβλιογραφίας. Ενδεικτικά αναφέρονται οι: [23], [24], [25], [26], [27], [28], [29], [30] και [3]

Ανάλυση των αδυναμιών (Vulnerabilities)

V1 Αδυναμίες AAA

(Authentication, Authorization, Accounting)

Ο όρος Authentication αναφέρεται στην διεργασίας με την οποία η ταυτότητα μιας οντότητας ταυτοποιείται, συνήθως παρέχοντας τεκμήρια ότι έχει στην διάθεσή του συγκεκριμένα στοιχεία (όπως είναι αναγνωριστικό και μυστικός κωδικός, στοιχεία που εξάγονται από μια γεννήτρια αριθμών, κ.α.).

Η διαδικασία του authorization προσδιορίζει αν μια συγκεκριμένη οντότητα είναι εξουσιοδοτημένη να εκτελεί μια συγκεκριμένη δραστηριότητα. Πιο συγκεκριμένα, με τον όρο Authorization περιγράφεται η διαδικασία μέσω της οποίας καθορίζονται τα δικαιώματα χρήσης στους πόρους. Συνήθως η εξουσιοδότηση αποτελεί συνέχεια της διαδικασίας (ή κληρονομείται) της διαδικασίας του Authentication, όταν κάποιος εισέρχεται σε μια υπηρεσία cloud computing. Η εξουσιοδότηση μπορεί να οριστεί μέσα από μια σειρά από περιορισμούς που μπορεί να αφορούν τον χρόνο σύνδεσης (ώρα και ημέρα), ή περιορισμούς τόπου ή τρόπου σύνδεσης κ.α..

Ενώ τέλος, με τον όρο Accounting περιγράφεται η παρακολούθηση και ο έλεγχος της κατανάλωσης πόρων από την πλευρά των χρηστών αλλά και η συμπεριφορά της διαδικασίας authentication και authorization. Τα αποτελέσματα της διαδικασίας accounting επιτρέπουν την επαλήθευση την ορθότητα της εφαρμογής των διαδικασιών του συστήματος (περιλαμβανομένων και των authentication και authorization διαδικασιών). Οι συνήθεις πληροφορίες που συλλέγονται από την λειτουργία μιας διαδικασίας accounting είναι η ταυτότητα του χρήστη ή της οντότητας που προσπελαύνει τον πόρο, το είδος της υπηρεσίας που παρέχεται, ο χρόνος της έναρξης και λήξης της παροχής της υπηρεσίας, η συμμόρφωση ή όχι κάποιου κανόνα κ.α.

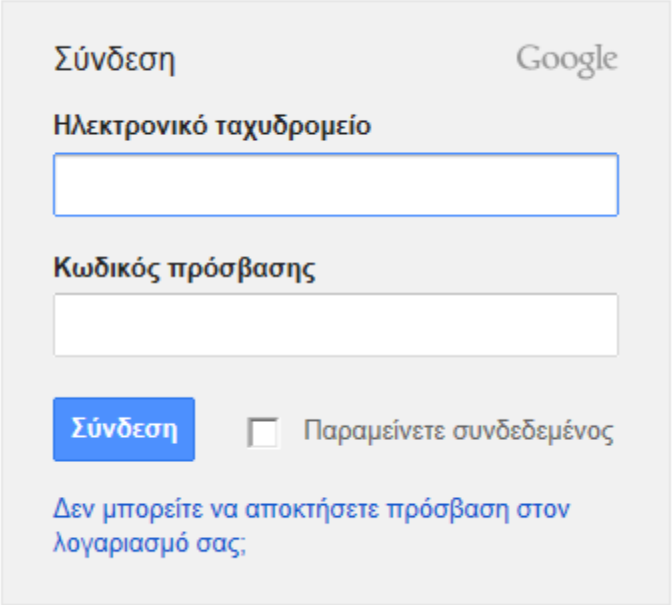
Ένα πολύ απλό (χαμηλής ασφάλειας) σύστημα που ελέγχει την αυθεντικοποίηση, εξουσιοδότηση και έλεγχο των χρηστών στις υπηρεσίες μπορεί να διευκολύνει την μη εξουσιοδοτημένη πρόσβαση στους πόρους, την πρόσβαση σε πόρους που έχουν μεγαλύτερο επίπεδο ασφαλείας από αυτό που επιθυμεί ο οργανισμός για τον αντίστοιχο χρήστη ενώ μπορεί να οδηγήσει σε αδυναμία από την πλευρά του ιδιοκτήτη των πόρων να ελέγξει (ιχνηλατήσει / παρακολουθήσει) την κακή χρήση των πόρων και την εκδήλωση περιστατικών ασφαλείας.

Αυτή τη στιγμή, το μεγαλύτερο μέρος των υπηρεσιών cloud computing παρέχουν έναν συνδυασμό user name και password ως τρόπο αυθεντικοποίησης για την είσοδο.

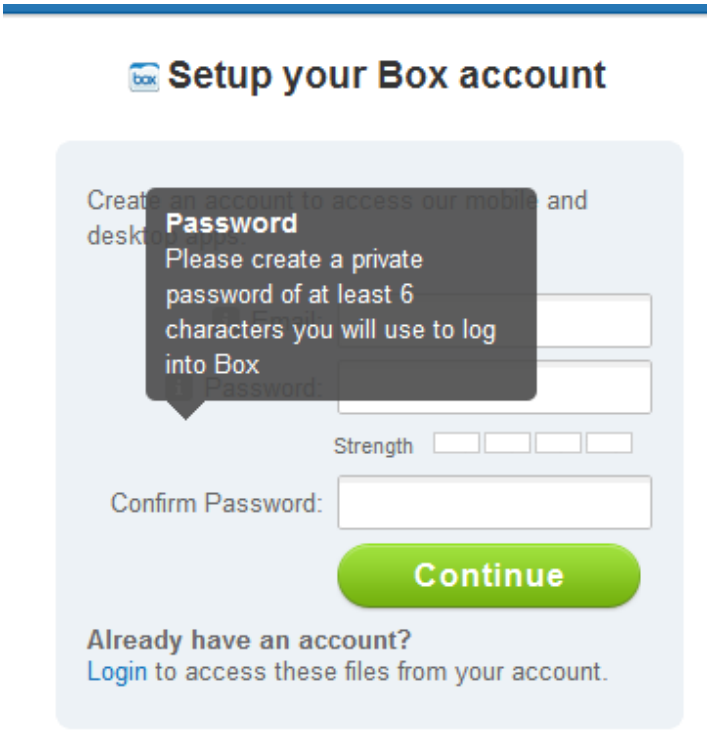
Αυτό σημαίνει ότι για να αποκτήσει κάποιος πρόσβαση στην υπηρεσία απλά χρησιμοποιείς ένα συνδυασμό user name και password.

Παραδείγματα τρόπου εισόδου σε υπηρεσίες cloud computing:

Gmail



Google Box (on line storage):



Το κάθε σύστημα αυθεντικοποίησης εισόδου μπορεί να έχει μόνο ένα user name και password αλλά υπάρχουν διάφοροι μηχανισμοί και μέτρα ασφάλειας που μπορεί να εισάγει ο πάροχος προκειμένου να παρέχει το επιθυμητό επίπεδο ασφαλείας.

Τέτοια χαρακτηριστικά είναι:

Το πλήθος των χαρακτήρων που απαρτίζουν κατ'ελάχιστον τον κωδικό password

Το είδος των χαρακτήρων που απαρτίζουν κατ'ελάχιστον τον κωδικό password

Την συχνότητα με την οποία επιβάλλεται η αλλαγή κωδικού password

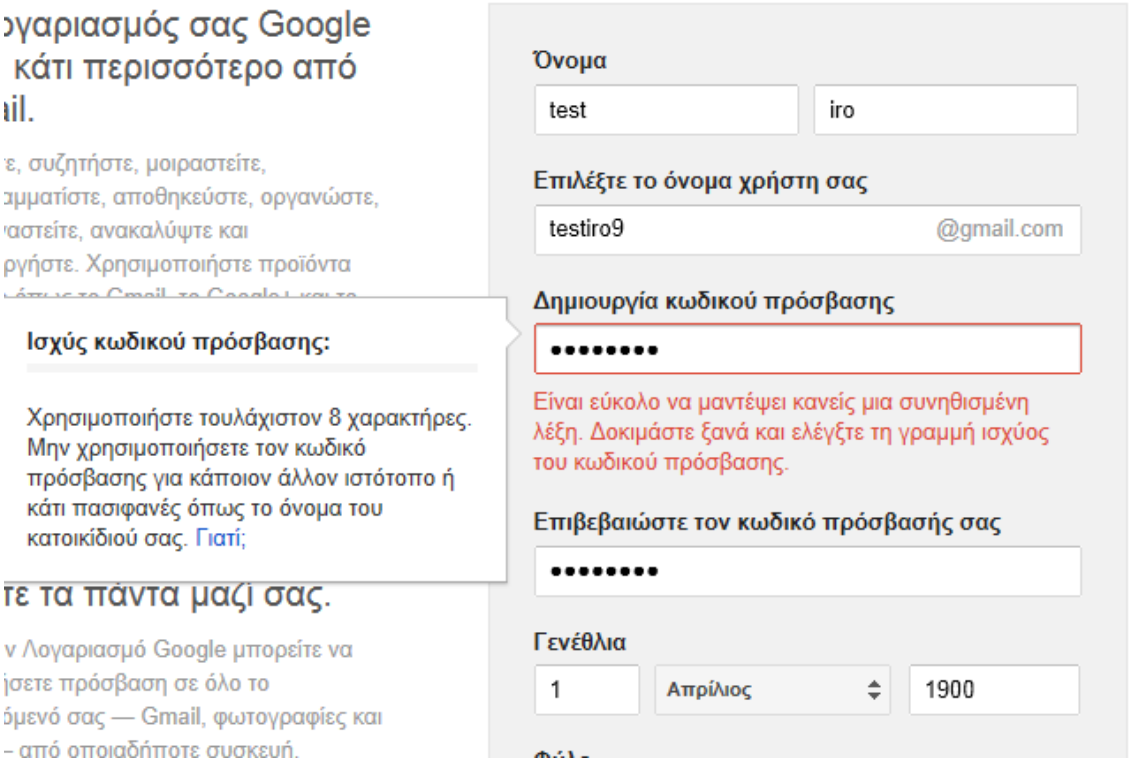
Το πλήθος ιστορικού που διατηρείται (password history 1 σημαίνει ότι κάποιος δεν μπορεί όταν αλλάξει το password του να βάλει αυτό που είχε πριν)

Το πλήθος των αποτυχημένων προσπαθειών εισαγωγής password μέχρι να κλειδώσει ο λογαριασμός

Το χρονικό διάστημα κλειδώματος και ο τρόπος ξεκλειδώματος.

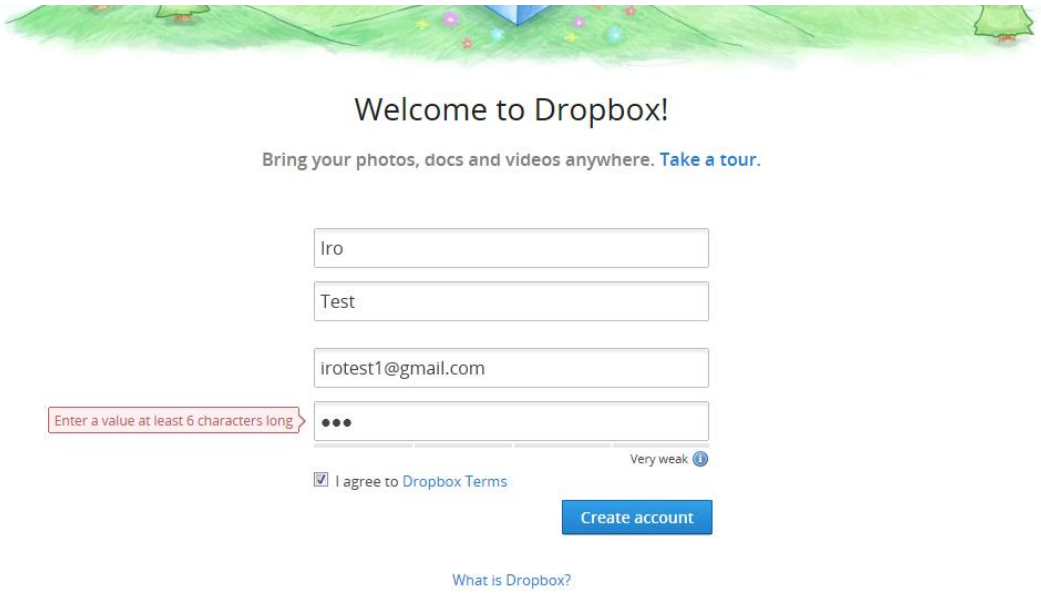
Ακολουθούν κάποια παραδείγματα από τα μέτρα ασφαλείας που έχουν εισαχθεί σε κάποιες υπηρεσίες cloud computing:

Google mail:



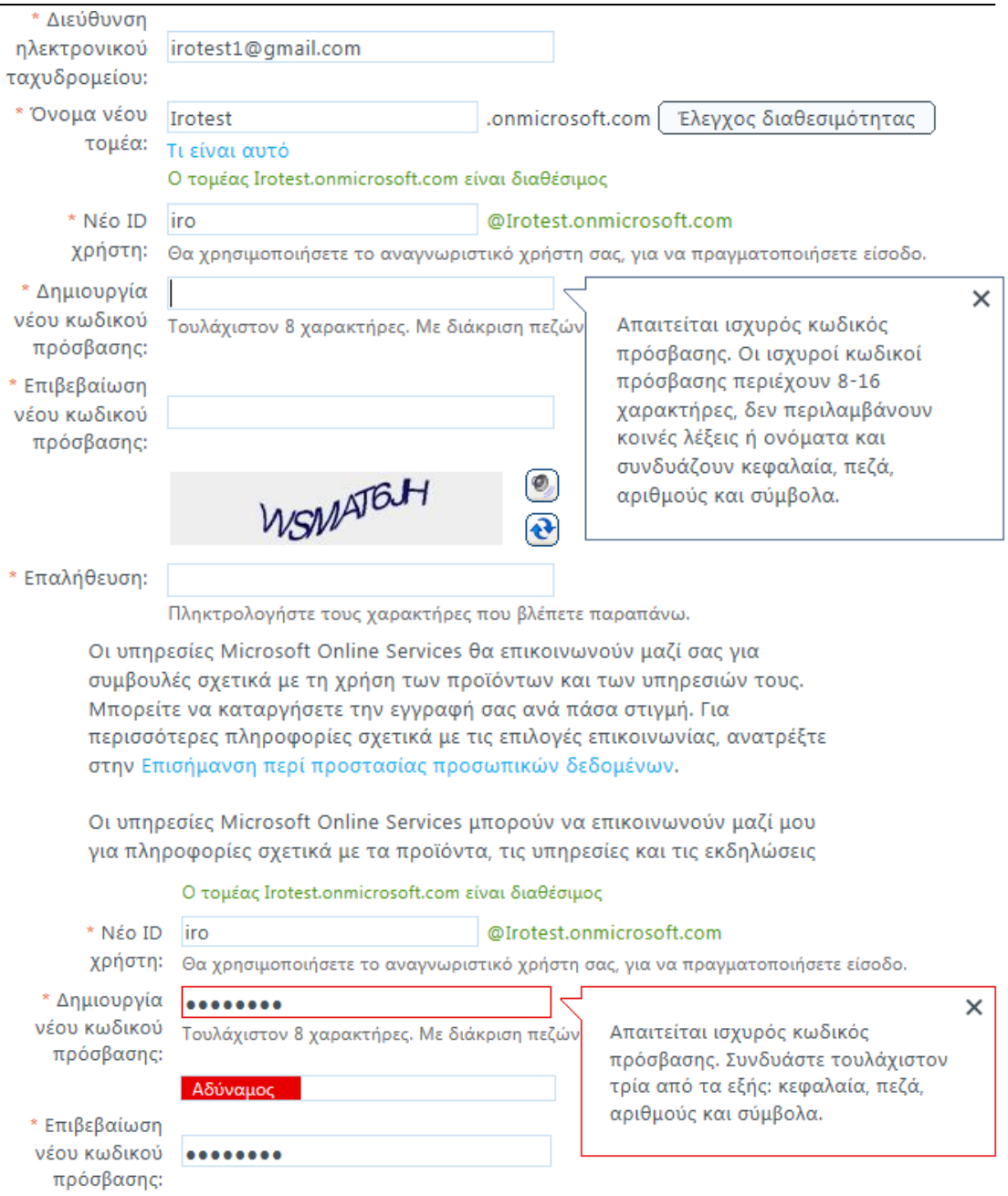
(Restriction in password creation: τουλάχιστον 8 χαρακτήρες και complexity)

Dropbox (storage)



Το μόνο restriction είναι να είναι το password έξι οποιοιδήποτε χαρακτήρες (complecity δεν είναι υποχρεωτικό).

Microsoft Online Services (Office 365)



Όπως γίνεται αντιληπτό βλέποντας τα παραπάνω παραδείγματα, κάθε πάροχος και για κάθε υπηρεσία μπορεί να εφαρμόζει διαφορετική πολιτική για το authentication.

Είναι κρίσιμο σε αυτό το στοιχείο να τεθεί ένα baseline, μια βέλτιστη κοινά αποδεκτή πρακτική σχετικά με τα user names και passwords.

Κατά καιρούς, με την εξέλιξη της τεχνολογίας και από την μεριά της ασφάλειας αλλά και από την άλλη πλευρά, η βέλτιστη πρακτική αλλάζει. Αυτή τη στιγμή σύμφωνα

με στοιχεία της βιβλιογραφίας, οι παρακάτω ρυθμίσεις είναι γενικά αποδεκτές ως baseline:

Το πλήθος των χαρακτήρων που απαρτίζουν κατ'ελάχιστον τον κωδικό password: 7

Το είδος των χαρακτήρων που απαρτίζουν κατ'ελάχιστον τον κωδικό password: Συνδυασμός από τουλάχιστον ένα πεζό γράμμα, ένα κεφαλαίο γράμμα και ένα νούμερο.

Πλήθος συμβόλων: Τουλάχιστον 1

Κάθε μια από αυτές τις επιλογές από μόνες τους οδηγεί σε ένα πλήθος δυνατών συνδυασμών. Ο προτεινόμενος συνδυασμός χαρακτήρων στο password, δίνει την δυνατότητα επιλογής ανάμεσα σε 6.48 10^{13} διαφορετικούς κωδικούς, κάνοντας την εργασία «σπασίματος» του κωδικού πολύ πιο δύσκολη από ότι αν ο κωδικός απαρτιζόταν από 7 χαρακτήρες (μόνο αριθμοί – 10^7).

Πίνακας 6 Πλήθος διαφορετικών συνδυασμών ανά πλήθος και είδος ψηφίων

Character set	**5**	**6**	**7**	**8**	**9**	**10**
0-9	1.00e05	1.00e06	1.00e07	1.00e08	1.00e09	1.00e10
a-z	1.19e07	3.09e08	8.03e09	2.09e11	5.43e12	1.41e14
a-z,0-9	6.05e07	2.18e09	7.84e10	2.82e12	1.02e14	3.66e15
a-z,0-9,3 punct	9.02e07	3.52e09	1.37e11	5.35e12	2.09e14	8.14e15
a-z,A-Z	3.80e08	1.98e10	1.03e12	5.35e13	2.78e15	1.45e17
a-z,A-Z,0-9	9.16e08	5.68e10	3.52e12	2.18e14	1.35e16	8.39e17
a-z,A-Z,0-9,32 punct	7.34e09	6.90e11	6.48e13	6.10e15	5.73e17	5.39e19

Την συχνότητα με την οποία επιβάλλεται η αλλαγή κωδικού password: όχι μεγαλύτερη των 90 ημερών

Το πλήθος ιστορικού που διατηρείται: 10

Το πλήθος των αποτυχημένων προσπαθειών εισαγωγής password μέχρι να κλειδώσει ο λογαριασμός: 10 αποτυχημένες προσπάθειες εισόδου σε 5 λεπτά.

Το χρονικό διάστημα κλειδώματος: 10 λεπτά

ο τρόπος ξεκλειδώματος: Σε περίπτωση που δεν υπάρχει διαθέσιμο άτομο για να κάνει χειροκίνητα την διαδικασία ξεκλειδώματος των λογαριασμών, θα πρέπει να υπάρχει ένας αυτόματος τρόπος. Με τον τρόπο αυτό μειώνεται η ανάγκη για ύπαρξη ατόμων και λογαριασμών με υψηλά δικαιώματα και δίνει και ένα μεγαλύτερο επίπεδο ευελιξίας για τον χρήστη. Η διαδικασία ξεκλειδώματος θα πρέπει να έχει ένα

ικανοποιητικό επίπεδο ασφαλείας. Περισσότερα στοιχεία αναφέρονται στην επόμενη ενότητα.

Επίσης τα Passwords δεν πρέπει:

Να περιέχουν το όνομα του χρήστη ή το login ID.

Να περιέχουν κανονική λέξη η οποία μπορεί να περιέχεται μέσα σε ένα λεξικό.

Να έχουν περισσότερα από 2 ίδια γράμματα (π.χ. abbbcdd).

Σχεδόν όλα από τα παραπάνω μπορούν να ελεγχθούν από την πολιτική του οργανισμού και της υπηρεσίας χωρίς να γίνει log in ή χρησιμοποιώντας μια πρόσβαση trial.

Πίνακας 7: Παραδείγματα αξιολόγησης

Cloud Services Examples	min ammount of characters	complexity	punctuation mark possible
Dropbox	6	no	yes
Microsoft 365	8	yes	yes
Google apps	8	yes	yes
googlebox	6	no	yes

‘Η εναλλακτικά, ο έλεγχος μπορεί να γίνει απευθείας σε προγράμματα όπως το passwordmeter (www.passwordmeter.com), το οποίο δίνει ένα συνολικό scoring για το πόσο ασφαλές και άρα λιγότερο εύκολο να σπάσει είναι το κάθε password.

Παρακάτω ακολουθούν κάποια παραδείγματα:

Test Your Password		Minimum Requirements
Password:		• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☑	
Score:	0%	
Complexity:	Too Short	

Additions		Type	Rate	Count	Bonus
✗	Number of Characters	Flat	+(n*4)	0	0
✗	Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
✗	Lowercase Letters	Cond/Incr	+((len-n)*2)	0	0
✗	Numbers	Cond	+(n*4)	0	0
✗	Symbols	Flat	+(n*6)	0	0
✗	Middle Numbers or Symbols	Flat	+(n*2)	0	0
✗	Requirements	Flat	+(n*2)	0	0
Deductions					
✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
✓	Repeat Characters (Case Insensitive)	Comp	-	0	0
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
✓	Consecutive Lowercase Letters	Flat	-(n*2)	0	0
✓	Consecutive Numbers	Flat	-(n*2)	0	0
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0
✓	Sequential Numbers (3+)	Flat	-(n*3)	0	0
✓	Sequential Symbols (3+)	Flat	-(n*3)	0	0

Legend

Exceptional: Exceeds minimum standards. Additional bonuses are applied.
Sufficient: Meets minimum standards. Additional bonuses are applied.
Warning: Advisory against employing bad practices. Overall score is reduced.
Failure: Does not meet the minimum standards. Overall score is reduced.

Test Your Password		Minimum Requirements
Password:	123123	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	7%	
Complexity:	Very Weak	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	6	+ 24
Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
Lowercase Letters	Cond/Incr	+((len-n)*2)	0	0
Numbers	Cond	+(n*4)	6	0
Symbols	Flat	+(n*6)	0	0
Middle Numbers or Symbols	Flat	+(n*2)	4	+ 8
Requirements	Flat	+(n*2)	1	0
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	6	- 6
Repeat Characters (Case Insensitive)	Comp	-	6	- 6
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	0	0
Consecutive Numbers	Flat	-(n*2)	5	- 10
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	1	- 3
Sequential Symbols (3+)	Flat	-(n*3)	0	0

Legend

Exceptional: Exceeds minimum standards. Additional bonuses are applied.
Sufficient: Meets minimum standards. Additional bonuses are applied.
Warning: Advisory against employing bad practices. Overall score is reduced.
Failure: Does not meet the minimum standards. Overall score is reduced.

Test Your Password		Minimum Requirements
Password:	Hello!12	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	72%	
Complexity:	Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	8	+ 32
Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 14
Lowercase Letters	Cond/Incr	+((len-n)*2)	4	+ 8
Numbers	Cond	+(n*4)	2	+ 8
Symbols	Flat	+(n*6)	1	+ 6
Middle Numbers or Symbols	Flat	+(n*2)	2	+ 4
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	2	- 2
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	3	- 6
Consecutive Numbers	Flat	-(n*2)	1	- 2
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	0	0
Sequential Symbols (3+)	Flat	-(n*3)	0	0

Legend

Exceptional: Exceeds minimum standards. Additional bonuses are applied.
Sufficient: Meets minimum standards. Additional bonuses are applied.
Warning: Advisory against employing bad practices. Overall score is reduced.
Failure: Does not meet the minimum standards. Overall score is reduced.

Για την προδιαγραφή:

Το πλήθος των αποτυχημένων προσπαθειών εισαγωγής password μέχρι να κλειδώσει ο λογαριασμός: 10 αποτυχημένες προσπάθειες εισόδου σε 5 λεπτά.

Ο έλεγχος μπορεί να γίνει μόνο με κάποιο εργαλείο το οποίο να διενεργήσει ένα brute force attack. Ο σκοπός χρήσης του εργαλείου είναι ελέγξει όχι μόνο την δύναμη του

password αλλά και την ύπαρξη ή όχι πολιτικής για προστασία απέναντι σε brute force attack (lockout after 10 failed login attempts in 5 minutes and the corresponding lockout duration).

Μερικά από αυτά τα εργαλεία είναι:

Aircrack

Cain and Abel

John the Ripper

THC Hydra

ophcrack

Medusa

fgdump

L0phtCrack

SolarWinds

RainbowCrack

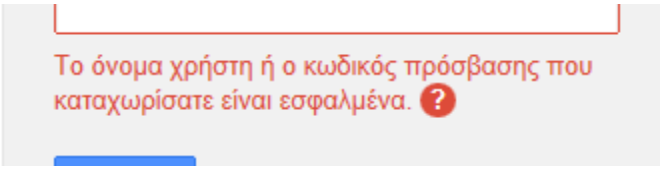
Wfuzz

Brutus

Δεν υπάρχει η δυνατότητα να γίνει έλεγχος του Authentication εκτός από μια περίπτωση. Η περίπτωση αυτή είναι όταν έχει γίνει ένας χρήστης lockout ή έχει ξεχάσει το username ή το password του.

Στις περιπτώσεις αυτές, η βέλτιστη πρακτική είναι να δημιουργείται ένα μήνυμα λάθους το οποίο όμως να μην περιέχει κάποιο αναγνωριστικό και να μην δίνει πληροφορίες σχετικά με το ποιο στοιχείο είναι λάθος.

Π.χ.



Επίσης, είναι σημαντικό σε περίπτωση που κάποιος χρήστης έχει αποκλειστεί (lockout) να εξασφαλίζεται ότι οι χρήστες που ζητάνε επαναφορά κωδικού πρόσβασης, να γίνεται θετική επιβεβαίωση της ταυτότητάς τους.

Σε αυτές τις περιπτώσεις η βέλτιστη πρακτική είναι:

Να χρησιμοποιούνται όπου είναι δυνατό One-time-password tokens ή smart cards ή βιομετρικά στοιχεία του χρήστη. Όπου αυτό δεν είναι δυνατό θα πρέπει να χρησιμοποιείται ο μηχανισμός των security questions.

Σε αυτές τις περιπτώσεις θα πρέπει:

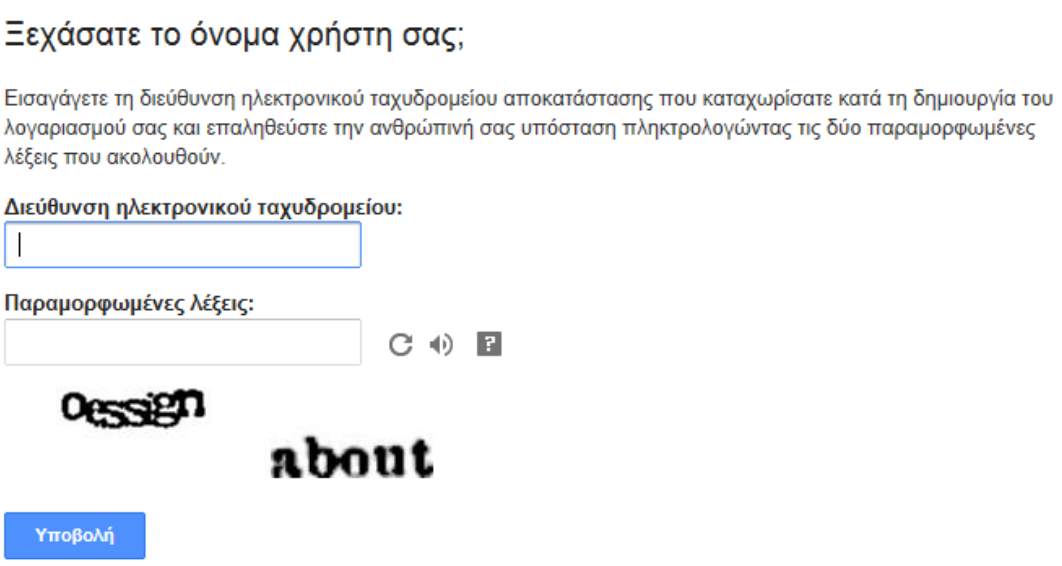
Να ζητούνται απαντήσεις σε όσο περισσότερες ερωτήσεις γίνεται

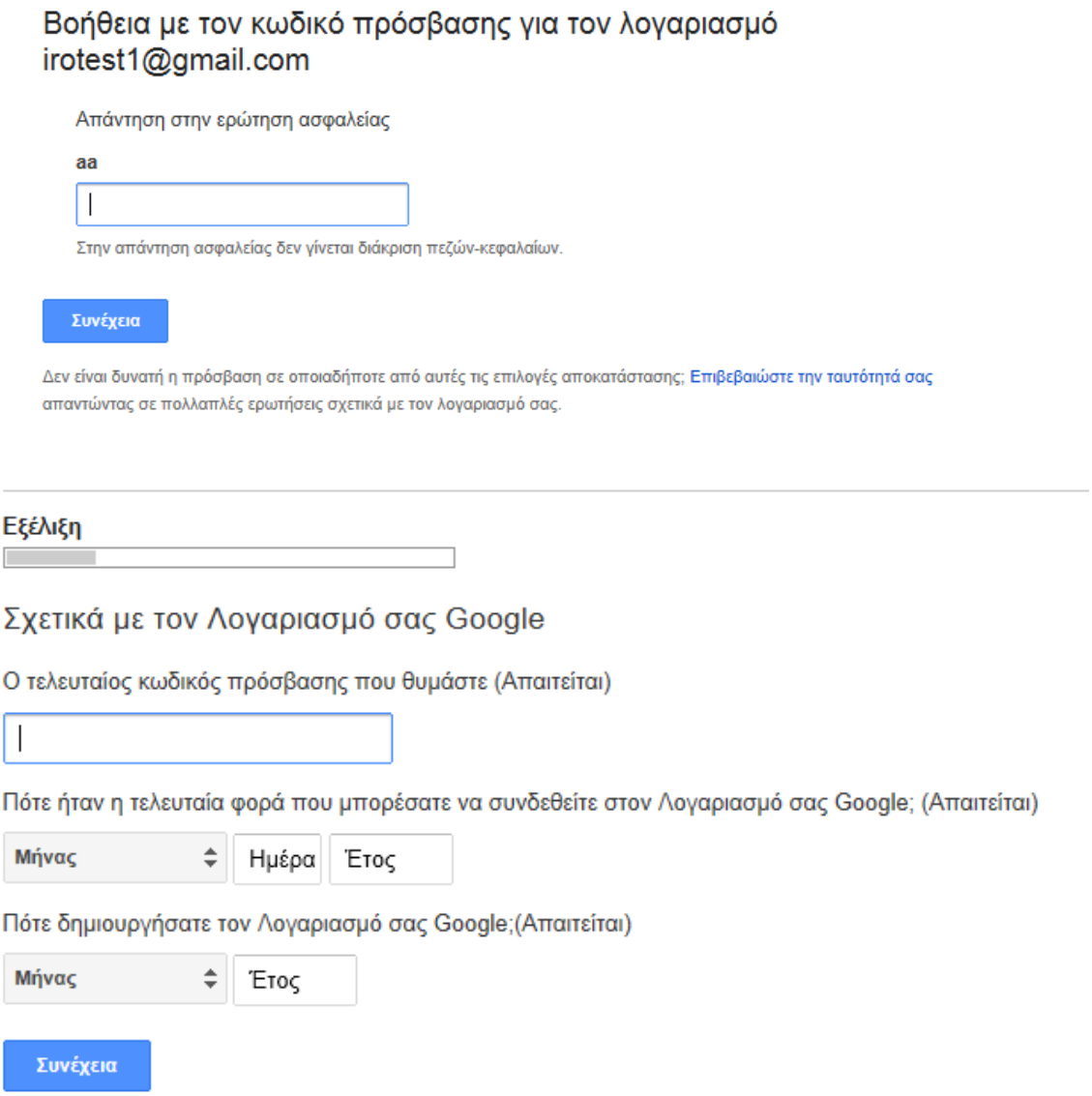
As many questions as possible should be used.

Η δυσκολία απάντησης της κάθε ερώτησης θα πρέπει να προσδιοριστεί. Η συνολική δυσκολία του να μαντέψει κάποιος τις απαντήσεις στις ερωτήσεις ασφαλείας που αυθεντικοποιούν τον χρήστη θα πρέπει να είναι περίπου η ίδια με την δυσκολία να μαντέψει κάποιος το password του χρήστη.

Οι χρήστες θα πρέπει να καλούνται να δώσουν απαντήσεις τόσο σε προσωπικά επιλεγμένες ερωτήσεις όσο και σε τυπικές. Η διαδικασία του lockout θα πρέπει να εφαρμόζεται με τον ίδιο τρόπο όπως και στην περίπτωση του password.

Π.χ.





Όσο αφορά τις υπόλοιπες παραμέτρους του authentication και accounting δεν μπορεί να υπάρξει κάποιος τρόπος αυτοματοποιημένου ή ημι-αυτοματοποιημένου ελέγχου των σχετιζόμενων αδυναμιών.

V2 Αδυναμίες στην διαχείριση δικαιωμάτων χρηστών (User provisioning vulnerabilities)

Σε ένα οργανωμένο σύστημα, σε κάθε χρήστη αποδίδονται δικαιώματα βάση της πολιτικής ελέγχου πρόσβασης του οργανισμού. Όταν στην διαδικασία απόδοσης των δικαιωμάτων αλλά και στην χρήση τους υπάρχουν αδυναμίες, τότε μπορεί υλοποιηθούν

κίνδυνοι. Τέτοιες αδυναμίες μπορεί να είναι: κακή διαδικασία απόδοσης δικαιωμάτων, καθυστερημένος συγχρονισμός ανάμεσα στα συστήματα που διατηρούν στοιχεία σε σχέση με την πρόσβαση και τα δικαιώματα, ύπαρξη πολλαπλών αντίγραφων των στοιχείων της ταυτότητας, τα στοιχεία ταυτοποίησης να είναι επιρρεπή στην υποκλοπή ή αναπαραγωγή (relay) (π.χ. όταν χρειάζεται να γίνεται συχνά ανταλλαγή των στοιχείων ταυτοποίησης με μεγάλη συχνότητα και χωρίς κάποια άλλα προστασία – π.χ. in clear text form.)

Το μόνο κομμάτι που μπορεί να ελεγχθεί σε αυτό το σημείο είναι αν υπάρχει κάποια επικοινωνία και ανταλλαγή κωδικών και ταυτοτήτων χρηστών μεταξύ των συστημάτων. Σε περίπτωση που αυτή υπάρχει τότε θα πρέπει να γίνεται (best practice) σε μορφή hash ή σε κρυπτογραφημένη μορφή.

Για να γίνει ο έλεγχος της ύπαρξης και της μορφής μιας τέτοιας επικοινωνίας μπορεί να χρησιμοποιηθεί οποιοδήποτε εργαλείο το οποίο εκτελεί traffic sniffing.

Σε αυτή την κατηγορία ανήκουν οι ακόλουθες εφαρμογές:

Ettercap

Ntop

SolarWinds

Ngrep

EtherApe

Splunk

NetWitness NextGen

Argus

P0f

V3 Αδυναμίες στην απομάκρυνση δικαιωμάτων χρηστών (User de-provisioning vulnerabilities)

Αντίστοιχα προς την διαδικασία με την οποία αποδίδονται σε κάθε χρήστη δικαιώματα βάση της πολιτικής ελέγχου πρόσβασης του οργανισμού, εξίσου σημαντικό είναι να υπάρχει μια διαδικασία για την απομάκρυνση των δικαιωμάτων των χρηστών. Η διαδικασίας αυτή θα πρέπει να περιλαμβάνει εκείνες τις ρυθμίσεις και τις προβλέψεις ώστε για τους χρήστες οι οποίοι μετακινούνται από μια θέση σε μια άλλη (και άρα

μεταβάλλονται τα δικαιώματα τους) ή σταματάνε να είναι χρήστες του οργανισμού, να μεταβάλλονται ή να αφαιρούνται / καταργούνται δικαιώματα και λογαριασμοί.

Για τον έλεγχο της συγκεκριμένης κατηγορίας αδυναμιών, δεν υπάρχει κάποιος αυτόματος τρόπος ελέγχου.

V4 Απομακρυσμένη πρόσβαση στο interface διαχείρισης (Remote access to management interface)

Επειδή η πρόσβαση των υπηρεσιών γίνεται μέσω του διαδικτύου, για να μπορεί ο πελάτης να έχει πρόσβαση και να διαχειρίζεται (στον βαθμό που επιτρέπεται από το είδος της υπηρεσίας που του παρέχεται) την υπηρεσία του, διατίθεται ένα interface. Μέσα από αυτό ο εξουσιοδοτημένος χρήστης διαχείρισης της εταιρίας μπορεί να εκτελέσει ενέργειες υψηλότερου επιπέδου από αυτό των τυπικών χρηστών. Και επειδή το interface αυτό είναι δημόσια προσπελάσιμο και έχει αυτά τα υψηλότερα δικαιώματα και λειτουργίες, αποτελεί και έναν μεγαλύτερο κίνδυνο. Αν το interface αυτό ή γενικά η εφαρμογή αυτή έχει αδυναμίες, τότε μπορεί να παρεισφρήσει κάποιος κακόβουλος στο σύστημα και να υπάρχει διαρροή δεδομένων, απώλεια υπηρεσίας κ.α.

Για να μπορεί να αξιολογηθεί η ύπαρξη αδυναμιών αυτής της κατηγορίας μπορεί να εκτελεστεί κάποιο εργαλείο αξιολόγησης αδυναμιών προσαρμοσμένο σε web εφαρμογές, με στόχο την υπηρεσία/ εφαρμογή του interface διαχείρισης.

Κάποιες από αυτές τις εφαρμογές είναι:

Penetrator Vulnerability Scanning Appliance by SecPoint

Nessus

QualysGuard

i-Security Vulnerability Management System (VMS™)

FoundScan Engine

STAT Scanner

Retina Network Security Scanner

Acunetix Web Vulnerability Scanner

V5 Αδυναμίες του hypervisor (Hypervisor Vulnerabilities)

Ο hypervisor είναι ο μηχανισμός εκείνος που ελέγχει τους φυσικούς πόρους και τα ιδεατά συστήματα που τρέχουν πάνω σε αυτούς τους πόρους. Η κρισιμότητα της λειτουργίας του hypervisor, σημαίνει ότι οι πιθανές του αδυναμίες μπορούν εύκολα να οδηγήσουν στην κατάρρευση του συστήματος ή διατάραξη του επιπέδου ασφαλείας των συστημάτων.

Σύμφωνα με τα παραπάνω αν κάποιος παρεισφρήσει στον hypervisor μπορεί να του δοθεί η δυνατότητα να παρεισφρήσει σε κάθε VM που φιλοξενείται στον hypervisor. Παραδείγματα στην βιβλιογραφία τέτοιου είδους επιθέσεων υπάρχουν πολλά. Π.χ. στο άρθρο των King et al [31] φαίνεται ένας τρόπος με τον οποίο ένας κακόβουλος εξωτερικός παράγοντας μπορεί να εξαπολύσει μια επίθεση μέσω ενός virtual machine-based Rootkit. Από τότε για κάθε σύστημα hupervisor ανακαλύπτονται συνεχώς νέες αδυναμίες, και στις περισσότερες φορές η εταιρία ιδιοκτήτης εκδίδει το αντίστοιχο patch για να καλύψει την αντίστοιχη αδυναμία (π.χ. [32], [33] ενώ μια λίστα για το 2012 φαίνεται στο [34]).

Εκμεταλλευόμενος κάποιος επιτιθέμενος μια αδυναμία του συστήματος που φιλοξενεί το χρήστη ή / και μια αδυναμία του hypervisor, μπορεί να αποκτήσει τον έλεγχο του hypervisor. Το είδος των επιθέσεων αυτών ονομάζεται ‘guest to host escape’ και ένα σχετικό παράδειγμα είναι το ‘Cloudburst’ [35]. Ένα άλλο σενάριο είναι το ‘VM hopping’ στο οποίο ο επιτιθέμενος παρεισφρέει σε ένα VM με κάποιο τρόπο και μετά εκμεταλλευόμενος μια αδυναμία του hypervisor αποκτά τον έλεγχο των άλλων VMs στον ίδιο Hypervisor (βλ. *Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments* [22]).

Για να αξιολογηθεί το επίπεδο κινδύνου στο οποίο θα βρεθεί κάποιος που θα κάνει host τις υπηρεσίες του στο cloud θα πρέπει να μπορεί να εξάγει για μια κρίση σχετικά με τις αδυναμίες του hypervisor (ποιες είναι και πόσες από αυτές δεν έχουν αντιμετωπιστεί ακόμα), ο οποίος χρησιμοποιείται για δοθεί η υπηρεσία. Για να γίνει αυτός ο έλεγχος θα πρέπει να μπορεί ο χρήστης να έχει την δυνατότητα να μπει σε τέτοιο επίπεδο εσωτερικά ώστε να μπορεί να τρέξει κάποια εφαρμογή η οποία να βρίσκει τις αδυναμίες του hypervisor.

Τέτοιες εφαρμογές είναι:

vCenter Protect Essentials

Cloud Penetrator™ Web Vulnerability Scanner

Penetrator Vulnerability Scanning Appliance by SecPoint

Nessus

QualysGuard

i-Security Vulnerability Management System (VMS™)

FoundScan Engine

STAT Scanner

Retina Network Security Scanner

Acunetix Web Vulnerability Scanner

V6 Έλλειψη απομόνωσης πόρων (Lack of resource isolation)

Ένα χαρακτηριστικό του cloud computing είναι ο διαμοιρασμός των φυσικών πόρων. Αυτό σημαίνει ότι η χρήση ενός πόρου από έναν πελάτη μπορεί να επηρεάσει την χρήση του ίδιου πόρου από άλλο πελάτη.

Στην περίπτωση του SaaS είναι πολύ εύκολο αυτός ο διαμοιρασμός να γίνει αντιληπτός, δεδομένου ότι όλοι οι πελάτες χρησιμοποιούν την ίδια υπηρεσία και άρα όλοι οι πόροι που δεσμεύονται από την υπηρεσία είναι διαμοιρασμένοι σε όλους τους χρήστες. Στην περίπτωση των IaaS και PaaS η κατάσταση δεν είναι πολύ διαφορετική. Μπορεί οι πόροι να μην είναι μοιράζονται την ίδια εφαρμογή, αλλά συνήθως οι υπηρεσίες αυτές είναι δομημένες σε αρχιτεκτονικές οι οποίες μοιράζονται τους φυσικούς πόρους π.χ. μέσω virtualization.

Η εκμετάλλευση αδυναμιών του hypervisor μπορεί να οδηγήσει σε μη εξουσιοδοτημένη πρόσβαση στους διαμοιρασμένους πόρους. Για παράδειγμα τα virtual machines του Πελάτη1 και του Πελάτη2 μπορεί να έχουν αποθηκευμένες τις περιοχές του storage τους (δίσκους) στο ίδιο διαμοιρασμένο LUN (Logical Unit Number). Σε αυτή την περίπτωση και ανάλογα με τον τρόπο υλοποίησης και μέτρα που έχουν ληφθεί, μπορεί ο Πελάτης2 να κάνει map το virtual hard drive του Πελάτη1 και να μπορεί να δει έτσι τα δεδομένα του Πελάτη1.

Η διαχείριση των hypervisors συνήθως γίνεται μέσω συστημάτων που έχουν στις περισσότερες περιπτώσεις προσαρμοστεί από τον πάροχο. Πιθανές αδυναμίες στο σύστημα πρόσβασης και παρακολούθησης του hypervisor μπορεί να οδηγήσει σε μη εξουσιοδοτημένη πρόσβαση σε δεδομένα. Επίσης, αν ένας κακόβουλος επιτιθέμενος μπορέσει και παρεισφρήσει σε αυτό το επίπεδο, τότε θα μπορεί να αλλάξει και να επηρεάσει τους πόρους που υποστηρίζουν την παροχή της υπηρεσίας, οδηγώντας σε denial of service (π.χ. σταματώντας την λειτουργία των virtual machines), διαρροή δεδομένων (π.χ. έχοντας πρόσβαση στα virtual machines και στα δεδομένα τους) κ.α.

Τέλος, κάποιος θα μπορούσε να φορτώσει την χρήση του συστήματός του, και ανάλογα με τα μέτρα που έχει λάβει ο πάροχος, θα μπορούσε να οδηγήσει στην εξάντληση των πόρων και στην οδήγηση της υπηρεσίας σε denial of service για τους υπόλοιπους πελάτες.

Η αδυναμία αυτή μπορεί να μετρηθεί εμμέσως μετρώντας τις αδυναμίες του hypervisor και του λοιπού λογισμικού αλλά και κάνοντας ένα stress testing για να επιβεβαιωθεί η λήψη μέτρων για την αποτελεσματική διαχείριση των διαμοιραζόμενων πόρων.

Τα εργαλεία που μπορούν να κάνουν αυτή την αναγνώριση είναι:

Τέτοιες εφαρμογές είναι:

vCenter Protect Essentials

Cloud Penetrator™ Web Vulnerability Scanner

Penetrator Vulnerability Scanning Appliance by SecPoint

Nessus

QualysGuard

i-Security Vulnerability Management System (VMS™)

FoundScan Engine

STAT Scanner

Retina Network Security Scanner

Acunetix Web Vulnerability Scanner

Και

IBM Rational Performance Tester

Apache JMeter .

Load Test

Load Impact

LoadRunner

loadUI

OpenSTA

HTTP Test Tool

SLAMD

Telerik Test Studio

Visual Studio

V7 Έλλειψη απομόνωσης φήμης (Lack of reputational isolation)

Μια ακόμα αδυναμία στις υπηρεσίες cloud computing είναι ότι ενέργειες ενός πελάτη μπορεί να επηρεάσουν και την φήμη των υπόλοιπων συστεγαζόμενων πελατών (π.χ. λόγω IP blocking κ.α.)

Για τον έλεγχο της συγκεκριμένης κατηγορίας αδυναμιών, δεν υπάρχει κάποιος αυτόματος τρόπος ελέγχου.

V8 Αδυναμίες της κρυπτογράφησης της επικοινωνίας (Communication encryption Vulnerabilities)

Οι υπηρεσίες cloud computing παρέχονται μέσω της επικοινωνίας του χρήστη από κάποιο απομακρυσμένο σημείο με το σημείο στο οποίο φιλοξενείται ο εξοπλισμός (υλικό και λογισμικό) διαμέσου του διαδικτύου. Αυτό σημαίνει ότι διακινείται μια μεγάλη ποσότητα πληροφορίας μέσα από ένα μη ασφαλές δίκτυο (untrust), αυξάνοντας την πιθανότητα να υποκλαπούν τα δεδομένα εν κινήσει μέσω π.χ. Man in the Middle attacks κ.α. Για να μπορεί κάποιος να θωρακιστεί απέναντι σε αυτού του είδους τις αδυναμίες θα πρέπει η πληροφορία που διακινείται μέσω του διαδικτύου να μην μπορεί να δώσει πληροφορίες σε κάποιο κακόβουλο, που μπορεί να οδηγήσουν στην αποκάλυψη πληροφοριών ή στην παρείσφρηση στα συστήματα.

Για να γίνει ο έλεγχος της ύπαρξης και της μορφής μιας τέτοιας επικοινωνίας μπορεί να χρησιμοποιηθεί οποιοδήποτε εργαλείο το οποίο εκτελεί traffic sniffing.

Σε αυτή την κατηγορία ανήκουν οι ακόλουθες εφαρμογές:

Ettercap

Ntop

SolarWinds

Ngrep

EtherApe

Splunk

NetWitness NextGen

Argus

P0f

V9 Απουσία ύπαρξης ή αδύναμη κρυπτογράφηση στα δεδομένα που μεταφέρονται ή αποθηκεύονται (Lack of or weak encryption of archives and data in transit)

Σε συνέχεια προς την προηγούμενη αδυναμία, αν τα δεδομένα εν κινήσει ή και τα δεδομένα που αποθηκεύονται σε βάσεις και αρχεία ή σε εικόνες μηχανημάτων κ.α. δεν είναι κρυπτογραφημένα, τότε αποτελούν αδυναμία για το σύστημα.

Όπως και προηγούμενα, για να γίνει ο έλεγχος της ύπαρξης και της μορφής μιας τέτοιας επικοινωνίας μπορεί να χρησιμοποιηθεί οποιοδήποτε εργαλείο το οποίο εκτελεί traffic sniffing.

Σε αυτή την κατηγορία ανήκουν οι ακόλουθες εφαρμογές:

Ettercap

Ntop

SolarWinds

Ngrep

EtherApe

Splunk

NetWitness NextGen

Argus

P0f

V10 Αδυναμία επεξεργασίας των δεδομένων σε κρυπτογραφημένη μορφή (Impossibility of processing data in encrypted form)

Η εφαρμογή της κρυπτογραφίας σε δεδομένα που είναι αποθηκευμένα (in rest) είναι κάτι σχετικό απλό. Εκεί που υπάρχει δυσκολία είναι να εφαρμοστεί κρυπτογράφηση στα δεδομένα κατά τη διάρκεια της επεξεργασίας. Σε περίπτωση που κάποιος θέλει να την υλοποιήσει το κόστος σε υπολογιστική ισχύ θα αυξανόταν κατά 1 τρισεκατομμύριο φορές. σύμφωνα με τον Bruce Schneier [36].

Για την συγκεκριμένη αδυναμία, παρόλο που το επιθυμητό θα ήταν να είναι κρυπτογραφημένη η πληροφορία κατά την επεξεργασία, το εφικτό αυτή την στιγμή είναι να μην είναι.

Για τον έλεγχο της συγκεκριμένης κατηγορίας αδυναμιών, δεν υπάρχει κάποιος αυτόματος τρόπος ελέγχου.

V15 Μη Ακριβής μοντελοποίηση της χρήσης των πόρων (Inaccurate modeling of resource usage) Inaccurate modeling of resource usage

Οι υπηρεσίες cloud computing βασίζονται στον διαμοιρασμό πόρων μέσω της εφαρμογής στατιστικών μοντέλων. Αυτό σημαίνει ότι είναι ιδιαίτερα επιρρεπείς σε κινδύνους που σχετίζονται με την χρήση και την διαθεσιμότητα των πόρων.

Κάποιες από τις αδυναμίες που μπορεί να υπάρξουν σε αυτό το σημείο είναι:

- Εφαρμογή ενός μοντέλου χρήσης πόρων το οποίο δεν μπορεί να αποδώσει την κατάλληλη ακρίβεια. Αυτό μπορεί με την σειρά του να οδηγήσει σε λάθος αρχικό καταμερισμό των πόρων και πιθανώς την υπερενοικίαση πόρων (overbooking). Π.χ. **Devera, Martin** [Online] http://luxik.cdi.cz/~devik/qos/htb/old/htbtheory.htm
- Αδυναμία πρόβλεψης, μέσω της εφαρμογής του αντίστοιχου μοντέλου, τον καταμερισμό των πόρων σε περίπτωση εξαιρετικού γεγονότος (π.χ. χρήση πόρων από μεγαλύτερο ποσοστό χρηστών από ότι είναι αναμενόμενο σε περίπτωση έκτακτου συμβάντος). Χαρακτηριστικό παράδειγμα, αν και από

άλλου είδους υπηρεσίας αποτελεί η εξάντληση των πόρων στον σεισμό της Αθήνα στο 1997. Σε αυτή την περίπτωση λόγω του σεισμού και της αδυναμίας λειτουργίας του σταθερού δικτύου, τα δίκτυα της κινητής τηλεφωνίας δεν μπόρεσαν να ανταποκριθούν.

- Και γενικά αδυναμίες στην ορθή εκτέλεση των αλγορίθμων ή αδυναμίες των αλγορίθμων.

Ανεξάρτητα του λόγου που οδηγεί σε ένα denial of Service εξαιτίας εξάντλησης πόρων, το αποτέλεσμα είναι το ίδιο (η εξάντληση πόρων). Για να ελεγχθούν τα μέτρα που έχει πάρει ο πάροχος έναντι τέτοιων απειλών και η συμπεριφορά του συστήματος μπορούν να χρησιμοποιηθούν εφαρμογές που κάνουν load, stress and performance testing.

Τα εργαλεία που ανήκουν σε αυτή την κατηγορία είναι:

WAPT

IBM Rational Performance Tester

Apache JMeter .

Load Test

Load Impact

LoadRunner

loadUI

OpenSTA

HTTP Test Tool

SLAMD

Telerik Test Studio

Visual Studio

V16 Αδυναμία ελέγχου της διεργασίας αποτίμησης αδυναμιών (No control on vulnerability assessment process)

Η διενέργεια port scan και vulnerability testing, ειδικά από το εξωτερικό του δικτύου αλλά και πλέον (αφού οι πελάτες είναι περισσότεροι από ένας και φιλοξενούνται στον πάροχο) από το εσωτερικό μπορεί να είναι μια κακόβουλη ενέργεια. Δεν υπάρχουν μέτρα

που μπορεί ο πάροχος να πάρει έναντι της διενέργειας τέτοιων ενεργειών αλλά μπορεί να έχει πάρει μέτρα για την μείωση της επίπτωσης τέτοιων ενεργειών. Π.χ. θα μπορούσε αν αντιληφθεί στο firewall ότι γίνεται ένα port scan μέσω του αντίστοιχου IDS (Intrusion Detection System), να κάνει drop το traffic και να εισάγει την διεύθυνση του επιτιθέμενου στο black list.

Για να γίνει ο έλεγχος της ύπαρξης και της μορφής μιας τέτοιας επικοινωνίας μπορεί να τρέξει κάποιο port scan tool προκειμένου να αξιολογηθεί η ανταπόκριση των συστημάτων του παρόχου. Το best practice σε αυτή την περίπτωση είναι όταν γίνεται κάποιο port scan να γίνεται αναγνώριση της κίνηση, την αποστολή κάποιου είδους alert στα αρμόδια άτομα και την διατήρηση logs.

Εργαλεία για την διενέργεια port scanning είναι:

Ettercap

Ntop

SolarWinds

Ngrep

EtherApe

Splunk

NetWitness NextGen

Argus

P0f

V17 Πιθανότητα ότι θα γίνει έλεγχος από το εσωτερικό του cloud (Possibility that internal (cloud) network probing will occur)

Η διενέργεια port scan και vulnerability testing, ειδικά από το εξωτερικό του δικτύου αλλά και πλέον (αφού οι πελάτες είναι περισσότεροι από ένας και φιλοξενούνται στον πάροχο) από το εσωτερικό μπορεί να είναι μια κακόβουλη ενέργεια.

Μέσω της πολιτικής του firewall ή του antivirus ή γενικά τέτοιου είδους εφαρμογών μπορεί να απαγορευτεί η εκτέλεση τέτοιων δραστηριοτήτων στο εσωτερικό για κάθε είδος παρεχόμενης υπηρεσίας cloud computing (SaaS, PaaS, IaaS).

Για να ελεγχθεί η ύπαρξη της συγκεκριμένης αδυναμίας μπορεί να διενεργηθεί ένα port scan μέσω συγκεκριμένης εφαρμογής εσωτερικά. Αν μπορούν να υλοποιηθούν οι παραπάνω κινήσεις εσωτερικά, τότε είναι ενεργό. Για την διενέργεια αυτού του ελέγχου πρέπει κάποιος να έχει τη δυνατότητα (έστω και με test account) να μπει εσωτερικά.

Τέτοια προγράμματα είναι:

Angry IP Scanner

Superscan

NetScanTools

Unicornscan

Wapiti

V18 Πιθανότητα ότι θα διενεργηθούν έλεγχοι συνύπαρξης (Possibility that co-residence checks will be performed)

Από την στιγμή που οι πόροι είναι διαμοιρασμένοι, δίνεται η δυνατότητα εξαπόλυσης επιθέσεων Side-channel. Ακόμα και όταν η κίνηση είναι σε κρυπτογραφημένη μορφή, κάποια βασικά χαρακτηριστικά των εφαρμογών web, όπως low entropy input, stateful communications, και σημαντικές διαφοροποιήσεις στην κίνηση, μπορεί να οδηγήσουν στην πραγματοποίηση side-channel επιθέσεις που οποίες μπορεί να οδηγήσουν στην διαρροή των δεδομένων και διακύβευση της εμπιστευτικότητας των δεδομένων. Μια σχετική μελέτη είναι των Shuo Chen, Rui Wang, XiaoFeng Wang και Kehuan Zhang [37]. Σύμφωνα με την ίδια μελέτη υπάρχει δυνατότητα αντιμετωπιστούν τέτοιου είδους αδυναμίες. Η διαδικασία αναλύεται στα εξής βήματα: αναγνώριση των αδυναμιών και στην συνέχεια εισαγωγή μέτρων / πολιτικών αντιμετώπισης. Η διαδικασία αυτή απαιτεί ανάλυση της εφαρμογής, της πορείας κίνησης της πληροφορίας και προτύπων κίνησης δικτύου (network traffic patterns.

Αυτή τη στιγμή δεν υπάρχει κάποιο αποδεκτό μέτρο για την μέτρηση και την ποσοτικοποίηση της ευπάθειας ενός συστήματος υπηρεσίας Cloud σε side channel attacks.

V27 Ανεπαρκής διαδικασία προμήθειας και επένδυσης σε υποδομή (Inadequate resource provisioning and investments in infrastructure)

Ένα από τα βασικά πλεονεκτήματα των υπηρεσιών cloud computing είναι ότι ο πελάτης δεν χρειάζεται να κάνει κάποια επένδυση σε υποδομή. Αυτό το κομμάτι έχει ήδη καλυφθεί από αυτόν που παρέχει την υπηρεσία. Τυπικά, πριν κάποιος περάσει στην υλοποίηση μιας υπηρεσίας cloud computing θα πρέπει να έχει κάνει κάποια ανάλυση μέσω της οποίας να έχει καταλήξει στους πόρους που χρειάζεται να εξασφαλίσει για συγκεκριμένο χρονικό διάστημα. Οι μελέτες αυτές θα πρέπει να επαναλαμβάνονται ανά κάποια διαστήματα προκειμένου να εξασφαλίζεται ότι οι πόροι που χρειάζονται, θα υπάρχουν διαθέσιμοι. Αν σε οποιοδήποτε από τα παραπάνω σημεία έχει γίνει κάποιο λάθος ή υπάρχει κάποια αδυναμία, τότε το σύστημα μπορεί να οδηγηθεί σε denial of Service λόγω εξάντλησης πόρων.

Για να ελεγχθούν τα μέτρα που έχει πάρει ο πάροχος έναντι τέτοιων απειλών και η συμπεριφορά του συστήματος μπορούν να χρησιμοποιηθούν εφαρμογές που κάνουν load, stress and performance testing.

Τα εργαλεία που ανήκουν σε αυτή την κατηγορία είναι:

WAPT

IBM Rational Performance Tester

Apache JMeter .

Load Test

Load Impact

LoadRunner

loadUI

OpenSTA

HTTP Test Tool

SLAMD

Telerik Test Studio

Visual Studio

V28 Απουσία πολιτικής σχετικά με ανώτατα όρια στους πόρους (No policies for resource capping)

Όπως αναφέρθηκε και στην αρχή, ένα από τα πλεονεκτήματα των υπηρεσιών cloud computing είναι η ελαστικότητα των πόρων. Ένα πελάτης κάνει μια συμφωνία για συγκεκριμένη χωρητικότητα και πόρους αλλά αυτό μπορεί να αλλάξει ανάλογα με τις απαιτήσεις του χρήστη. Είναι σημαντικό όμως να υπάρχει κάποια πολιτική για ένα ανώτατο όριο ποσότητας πόρων που μπορεί να χρησιμοποιήσει ένας πελάτης. Αν δεν υπάρχει αυτό το όριο, τότε μπορεί ένας χρήστης/ πελάτης να οδηγήσει το σύστημα σε resource exhaustion.

Για να ελεγχθεί αν ο πάροχος έχει λάβει σχετικά μέτρα και έχει εφαρμόσει πολιτικές μπορούν να χρησιμοποιηθούν εφαρμογές που κάνουν load, stress and performance testing.

Τα εργαλεία που ανήκουν σε αυτή την κατηγορία είναι:

WAPT

IBM Rational Performance Tester

Apache JMeter .

Load Test

Load Impact

LoadRunner

loadUI

OpenSTA

HTTP Test Tool

SLAMD

Telerik Test Studio

Visual Studio

V31 Απουσία όρων ή απουσία διαφάνειας στους όρους χρήσης (Lack of completeness and transparency in terms of use)

Οι αδυναμίες αυτής της κατηγορίας αφορούν τους όρους χρήσης, τις υποχρεώσεις των πελατών και του παρόχου. Είναι σημαντικό να είναι ξεκάθαροι οι όροι και υπάρχουν προβλέψεις για το επίπεδο εξυπηρέτησης και την ασφάλεια (SLA και Security).

Για τον έλεγχο της συγκεκριμένης κατηγορίας αδυναμιών, δεν υπάρχει κάποιος αυτόματος τρόπος ελέγχου.

V34 Μη ξεκάθαρα ορισμένοι ρόλοι και υπευθυνότητες (Unclear roles and responsibilities)

Οι αδυναμίες αυτού του είδους σχετίζονται με μη ικανοποιητικό διαχωρισμό και ορισμό ρόλων και αρμοδιοτήτων στο εσωτερικό του παρόχου. Αυτές οι αδυναμίες μπορεί να οδηγήσουν στην έκθεση του οργανισμού σε απειλές.

Για τον έλεγχο της συγκεκριμένης κατηγορίας αδυναμιών, δεν υπάρχει κάποιος αυτόματος τρόπος ελέγχου.

V35 Κακή εφαρμογή των ρόλων (Poor enforcement of role definitions)

Αντίστοιχα, αν υπάρχουν διαχωρισμένοι και ορθά ορισμένοι ρόλοι και αρμοδιότητες, και πάλι το σύστημα του παρόχου είναι εκτεθειμένο σε κινδύνους όταν οι ρόλοι αυτοί εφαρμόζονται λανθασμένα ή πλημμελώς,

Για τον έλεγχο της συγκεκριμένης κατηγορίας αδυναμιών, δεν υπάρχει κάποιος αυτόματος τρόπος ελέγχου.

V36 Δεν εφαρμόζεται η αρχή Need-to-know (Need-to-know principle not applied)

Μια βασική αρχή που έχει καθιερωθεί ως best practice για τον καλύτερο έλεγχο της πρόσβασης στην πληροφορία είναι η αρχή Need-to-know. Αυτό σημαίνει ότι αν κάποιος δεν χρειάζεται συγκεκριμένη πρόσβαση για να εκτελέσει αποτελεσματικά τα καθήκοντά του, τότε δεν χρειάζεται να την έχει. Αυτό μπορεί να αφορά τόσο προνόμια φυσικής πρόσβασης όσο και λογικής πρόσβασης.

Για τον έλεγχο της συγκεκριμένης κατηγορίας αδυναμιών, δεν υπάρχει κάποιος αυτόματος τρόπος ελέγχου.

V38 Κακή διαμόρφωση (Misconfiguration)

Πολύ μικρό ποσοστό εγκαταστάσεων σήμερα (και ειδικά στις επαγγελματικής χρήσης εγκαταστάσεις) δεν λαμβάνουν μέτρα και δεν έχουν εγκαταστήσει μηχανισμούς για την προστασία από απειλές. Τέτοια μέτρα είναι π.χ. η εισαγωγή firewalls, antivirus κ.α. Η αποτελεσματικότητα ενός μηχανισμού δεν κρίνεται όμως απλά από την ύπαρξη τους. Θα πρέπει να αποδειχθεί ότι έχουν παραμετροποιηθεί με τέτοιο τρόπο ώστε να προσφέρουν στον πάροχο το επιθυμητό επίπεδο ασφαλείας.

Για να γίνει η αξιολόγηση αυτή θα πρέπει να διεξαχθεί ένας συνδυασμός των vulnerability scan, port scan και security assessment tools.

Παραδείγματα τέτοιων εργαλείων είναι:

AppScan

Netsparker

HP WebInspect

Wikto

Samurai Web Testing Framework

Firebug

ratproxy

Websecurify

Grendel-Scan

DirBuster

Wfuzz

Wapiti

Nikto

V39 Αδυναμίες του συστήματος ή του λειτουργικού συστήματος (System or OS vulnerabilities)

Για να αξιολογηθεί το επίπεδο κινδύνου στο οποίο θα βρεθεί κάποιος που θα κάνει host τις υπηρεσίες του στο cloud θα πρέπει να μπορεί να εξάγει για μια κρίση σχετικά με τις αδυναμίες του συστήματος ή του λειτουργικού συστήματος που δίνεται η υπηρεσία. Για να γίνει αυτός ο έλεγχος θα πρέπει να μπορεί ο χρήστης να έχει την δυνατότητα να

μπει σε τέτοιο επίπεδο εσωτερικά ώστε να μπορεί να τρέξει κάποια εφαρμογή η οποία να βρίσκει τις αδυναμίες.

Τέτοιες εφαρμογές είναι:

Nessus - Scans for Αδυναμίες.

SARA – Scanner to scan for Αδυναμίες.

vCenter Protect Essentials

Cloud Penetrator™ Web Vulnerability Scanner

Penetrator Vulnerability Scanning Appliance by SecPoint

i-Security Vulnerability Management System (VMS™)

FoundScan Engine

STAT Scanner

Retina Network Security Scanner

Nessus

OpenVAS

Core Impact

Nexpose

GFI LanGuard

QualysGuard

MBSA

Retina

Secunia PSI

Nipper

SAINT

V41 Σχέδιο συνέχισης επιχειρησιακής λειτουργίας και Σχέδιο ανάκαμψης από καταστροφή τα οποία είναι ελλειπή ή δεν έχουν δοκιμαστεί ή απουσιάζουν εντελώς (Lack of, or a poor and untested, business continuity and disaster recovery plan)

Το σχέδιο επιχειρησιακής συνέχειας περιέχει αποτελεί μια συλλογή των ρυθμίσεων και των προβλέψεων που έχει κάνει ο οργανισμός, προκειμένου να συνεχίσει τις επιχειρησιακές λειτουργίες του σε προκαθορισμένο επίπεδο και σε συμφωνημένο χρονικό διάστημα. Είναι σημαντικό ο πελάτης / ένοικος να γνωρίζει τις προβλέψεις και

τα μέτρα που έχει πάρει ο πάροχος, επειδή επηρεάζεται άμεσα. Π.χ. ο πάροχος μπορεί να έχει ως σχέδιο επιχειρησιακής συνέχειας σε περίπτωση συνεχόμενης διακοπής τηλεπικοινωνιών, την χρήση μιας γραμμής διαφορετικού πάροχου για ενημέρωση των πελατών ότι δεν μπορεί να εργαστεί μέχρι να ανακάμψει ο τηλεπικοινωνιακός πάροχος. Η εταιρία πελάτης θα πρέπει να μπορεί να αξιολογήσει ποιο είναι το σχέδιο και αν είναι αυτό συμβατό με την πολιτική και τους στόχους της για επιχειρησιακή λειτουργία.

Για τον έλεγχο της συγκεκριμένης κατηγορίας αδυναμιών, δεν υπάρχει κάποιος αυτόματος τρόπος ελέγχου.

V47 Απουσία πλεονασμού προμηθευτή (Lack of supplier redundancy)

Ο κάθε πάροχος χρησιμοποιεί προμηθευτές σε κάποιο βαθμό για να μπορεί να δώσει τις υπηρεσίες του στο επιθυμητό επίπεδο. Π.χ. Εταιρίες πληροφορικής, τηλεπικοινωνιών, εξοπλισμού, συντήρησης, υποστήριξης, φύλαξης, φιλοξενίας κ.α. Σε περίπτωση που κάποιος από τους προμηθευτές του σταματήσει να μπορεί να τους παρέχει το προϊόν ή την υπηρεσία η βέλτιστη πρακτική είναι να έχουν εναλλακτική διαθέσιμη ώστε να μην επηρεαστεί η λειτουργία τους από το πρόβλημα του προμηθευτή.

Για τον έλεγχο της συγκεκριμένης κατηγορίας αδυναμιών, δεν υπάρχει κάποιος αυτόματος τρόπος ελέγχου.

V48 Αδυναμίες των εφαρμογών ή κακή διαχείριση των ενημερώσεων (patch) (Application vulnerabilities or poor patch management)

Αντίστοιχα με τις αδυναμίες του hypervisor και του λειτουργικού συστήματος, και οι εφαρμογές αυτές καθ' αυτές μπορεί να έχουν αδυναμίες. Η ύπαρξη αυτών των αδυναμιών μπορεί να οδηγήσει στην διαρροή των πληροφοριών, στην παρείσφρηση στα συστήματα κ.α.

Για να γίνει η αξιολόγηση αυτή θα πρέπει να διεξαχθεί ένα vulnerability scan για τις συγκεκριμένες εφαρμογές. Προϋπόθεση για την διεξαγωγή του ελέγχου αυτού είναι η δυνατότητα πρόσβασης στο εσωτερικό.

Παραδείγματα τέτοιων εργαλείων είναι:

Nessus

OpenVAS

Core Impact

Nexpose

GFI LanGuard

QualysGuard

MBSA

Retina

Secunia PSI

Nipper

SAINT

V53 Μη επαρκείς ή με κακή διαμόρφωση πόροι που ελέγχουν (φιλτράρουν) την πρόσβαση (Inadequate or misconfigured filtering resources)

Σε ένα οργανωμένο σύστημα, σε κάθε χρήστη αποδίδονται δικαιώματα βάση της πολιτικής ελέγχου πρόσβασης του οργανισμού. Η απόδοση δικαιωμάτων είναι άμεσα συνδεδεμένη με τα μέτρα και τους μηχανισμούς που έχει ο οργανισμός προκειμένου να ελέγχονται οι πόροι. Συστήματα τα οποία δεν λειτουργούν σωστά ή δεν υπάρχουν, μπορεί να οδηγήσουν σε διακύβευση της ασφάλειας του συστήματος.

Για τον έλεγχο της συγκεκριμένης κατηγορίας αδυναμιών, δεν υπάρχει κάποιος αυτόματος τρόπος ελέγχου.

Μοντέλο Αξιολόγησης

Το μοντέλο αξιολόγησης περιλαμβάνει μια σειρά από κριτήρια τα οποία πρέπει να αξιολογηθούν βάση του προτεινόμενου τρόπου και τα αποτελέσματα συλλέγονται μέσα σε ένα αρχείο Excel.

Στον πίνακα που ακολουθεί αποτυπώνονται:

Οι αδυναμίες που αναλύθηκαν παραπάνω και εκτιμήθηκε ότι υπάρχει έστω και ένα εργαλείο μέσου του οποίου να μπορεί να γίνει η αξιολόγηση της ύπαρξης της αδυναμίας. Σε κάποιες περιπτώσεις π.χ. αδυναμία V1. τα στοιχεία ελέγχου μπορεί να είναι περισσότερα από 1. Σε αυτή την περίπτωση αναγράφεται κάθε κριτήριο σε διαφορετική σειρά.

Ο τρόπος αξιολόγησης π.χ. η αξιολόγηση του password σε σχέση με το πλήθος χαρακτήρων που έχει ή η μέτρηση των αδυναμιών κ.α.

Το baseline, βάση του οποίου συγκρίνεται το αποτέλεσμα της κάθε αξιολόγησης.

Στην συνέχεια και μετά την ολοκλήρωση των διαδικασιών αξιολόγησης, τα αποτελέσματα θα εισαχθούν στο αρχείο, μαζί με τα αποτελέσματα της σύγκρισης των τιμών αυτών με τις τιμές του Baseline.

Πίνακας 8: Κριτήρια και μέθοδοι αξιολόγησης

Corresponding V.	ΑΠΑΙΤΗΣΕΙΣ	Method of Assesment	Baseline
V1	Passwords must be at least seven (7) characters long.	If the a minimum acceptable password is known the characters can be counted. If the password is not known, a new registration should be undertaken to evaluate the rules that apply	7
V1	Passwords must contain at least one lowercase letter, at least one uppercase letter and at least one digit. (this is usually named - in Windows systems as complexity)	If the a minimum acceptable password is known the characters can be counted. If the password is not known, a new registration should be undertaken to evaluate the rules that apply	Complexity enabled
V1	If technically possible, passwords must contain at least one punctuation mark, so long as there are many (10 or more) available punctuation marks.	If the a minimum acceptable password is known the characters can be counted. If the password is not known, a new registration should be undertaken to evaluate the rules that apply	Special Characters required
V1	The password should not contain a dictionary word, in any language that users can reasonably be expected to know.	If the a minimum acceptable password is known the characters can be counted. If the password is not known, a new registration should be undertaken to evaluate the rules that apply	dictionary word not possible
V1	The password should not contain more than two paired letters (e.g. abbcdde is valid, but abbbcdd is not).	If the a minimum acceptable password is known the characters can be counted. If the password is not known, a new registration should be undertaken to evaluate the rules that apply	More than 2 Paired letters not allowed
V1	Account Lockout: all accounts should be set to "lock out" a user after a maximum of 5 incorrect password or failed login attempts	A password cracking software has to be launched. A brute force attack, should lead to the lock out of the account	lockout after max. 5 attempts
V1	Lockout Threshold: the minimum "lock out" time should be set to five (5) minutes	A password cracking software has to be launched. A brute force attack, should lead to the lock out of the account. The time of acoount lock out can be measured in minutes.	lockout time more than 5 mins
V1	Password History: systems should be configured to require a password that is different from the last ten (10) passwords	With a valid account, the user has to change the passwords and try to restore a previous one. The number of passwords remembered has to be more than 10.	At least 10 passwords remembered
V1	When authentication fails, no information regarding the point of failure should be displayed	A log in should be attempted first with a user name that does not exist and then to a valid account but with a wrong password	No display whether user name or password failed

V1	After lockout, users who request a password reset should be reliably authenticated	After a valid account has been locked, the procedure for reseting the password should be followed	Authentication Procedure for resenting password after lockout available - It should contain at least one security question should be asked
V2	If copies of identity data are made, and credentials are transferred securely between systems.	A sniffing software will be used in order to capture the traffic between the source and the destination. The traffic will have to be analyzed and the parts containing the credentials should be identified.	The credentials (in hash form) in transit are encrypted
V4	No major vulnerabilities of the management Interface should exist	A web vulnerability scanner should perform a vulnerability scan on the management interface.	0 major/ high vulnerabilities found from all vulnerability scanners. Less than 20 middle severity vulenarbilities as a sum.
V5, V39, V48	No major vulnerabilities of the Hypervisor should exist	A selection of 3 vulnerability scanners should perform a vulnerability scan on the hypervisor.	0 major/ high vulenrabilities found from all vulnerability scanners. Less than 20 middle severity vulenarbilities as a sum.
V6	No major vulnerabilities of the Hypervisor should exist	A selection of 3 vulnerability scanners should perform a vulnerability scan on the hypervisor	0 major/ high vulenrabilities found from all vulnerability scanners. Less than 20 middle severity vulenarbilities as a sum.
V6	The modeling of resource usage has to be effective and the system should be able to provide even if the request is increased rapidly.	A stress / load testing software will be used to test the parameters of the SLA regarding resources.	The service was able to be provided at a 150% of all the resources prescribed in the SLA
V8, V9	If the communication between the systems in facilitated through encryption , then it should be an encryption that can be not be cracked easily	A sniffing software will be used in order to capture the traffic between the source and the destination. The traffic will have to be analyzed and the parts containing the credentials should be identified. The encrypted information should be processed through a password cracking system to evaluate the time needed to access the information.	2 hours of processing without cracking the encryption

V15, V27, V28	The modelling of resource usage has to be effective and the system should be able to provide even if the request is increased rapidly.	A stress / load testing software will be used to test the parameters of the SLA regarding resources.	The service was able to be provided at a 150% of all the resourses prescribed in the SLA
V16	Restrictions on port scanning and vulnerability testing should be enforced	Port scanning software and vulnerability assessment software can be run in order to assess the existence of the capability to execute them and the response of the system to their actions	In case of a port scan beeing carried out, the system should be able to alert the responsible person(s) and keep logs
V17	Cloud customers should not be able to conduct tests (e.g. Port scans, vas ech)	Port scanning software and vulnerability assessment software can be run in order to assess the existence of the capability to execute them	They are not allowed to be run from an internal IP
V38	Misconfiguration. The systems and components have to be configured appropriately to their use. No inadequate application of security baseline and hardening procedures should exists.	Συνδυασμός των vulnerability scan, port scan και security assessment	0 major/ high vulnerabilities found from all vulnerability scanners. Less than 20 middle severity vulenarbilities as a sum.
V38	Misconfiguration. The systems and components have to be configured appropriately to their use. No inadequate application of security baseline and hardening procedures should exists.	Συνδυασμός των vulnerability scan, port scan και security assessment	The results of the port scan should not reveal any ports that are open except the necessary (this is double checked with the type of the service)
V38	Misconfiguration. The systems and components have to be configured appropriately to their use. No inadequate application of security baseline and hardening procedures should exists.	Συνδυασμός των vulnerability scan, port scan και security assessment	0 major/ high security holes found from the security scanner.

Στην συνέχεια τα αποτελέσματα με την μορφή ποσοστού συμμόρφωσης αποτυπώνονται στον παρακάτω πίνακα.

Πίνακας 9: Αποτύπωση στοιχείων Συμμόρφωσης

Corresponding V.	Sum of Baseline	Score of Actual	Percentage of Compliance to baseline	**Rating Scale According to ISO 15504**
V1	10	0	0%	**Not achieved**
V2	1	0	0%	**Not achieved**
V4	1	0	0%	**Not achieved**
V5	1	0	0%	**Not achieved**
V6	2	0	0%	**Not achieved**
V8, V9	1	0	0%	**Not achieved**
V15, V27, V28	1	0	0%	**Not achieved**
V16	1	0	0%	**Not achieved**
V17	1	0	0%	**Not achieved**
V38	3	0	0%	**Not achieved**
V39	1	0	0%	**Not achieved**
V48	1	0	0%	**Not achieved**

Για την εξαγωγή της αξιολόγησης των αποτελεσμάτων χρησιμοποιείται μια τετραβάθμια κλίμακα, η οποία αποτυπώνεται στο πρότυπο ISO 15504 [38].

Not achieved (0 - 15%)

Partially achieved (>15% - 50%)

Largely achieved (>50%- 85%)

Fully achieved (>85% - 100%).

Δεδομένου ότι όλες οι αδυναμίες δεν επηρεάζουν στο ίδιο ποσοστό και με την ίδια βαρύτητα την ασφάλεια, στο επόμενο βήμα γίνεται ένας συσχετισμός ανάμεσα στο πλήθος επηρεαζόμενων κινδύνων (frequency), και την μέγιστη επίπτωση (max of Impact) όπως αυτά αποτυπώνονται στον πίνακα 5 και προέκυψαν από την ανάλυση κινδύνου. Ο τελικός υπολογισμός του επιπέδου ασφαλείας επιτυγχάνεται από τον πολλαπλασιασμό της τιμής του frequency με το impact ανά αδυναμία (με την μορφή ποσοστού που συμμετέχει στο σύνολο) και πολλαπλασιασμού του με την τιμή που είχε προκύψει από το προηγούμενο στάδιο της αποτίμησης.

Στο τέλος, στο τελευταίο κελί της στήλης **Assessment Result taking in account the frequency/impact factor** θα περιέχεται το τελικό αποτέλεσμα αξιολόγησης.

Vulnerability ID	Frequency	Max. of Impact	Value of max of Impact (L-1, M-2, H-3)	The result of frequency and Impact	Assessment Value	Assesment Result taking in account the frequency/impact factor	
V1	4	M	2	8	0%	0,00	
V2	2	M	2	4	0%	0,00	
V4	1	H	3	3	0%	0,00	
V5	4	H	3	12	0%	0,00	
V6	5	H	3	15	0%	0,00	
V8	3	M	2	6	0%	0,00	
V9	1	M	2	2	0%	0,00	
V15	1	M	2	2	0%	0,00	
V16	1	M	2	2	0%	0,00	
V17	4	H	3	12	0%	0,00	
V27	1	M	2	2	0%	0,00	
V28	1	M	2	2	0%	0,00	
V38	5	H	3	15	0%	0,00	
V39	4	H	3	12	0%	0,00	
V48	2	M	2	4	0%	0,00	
SUM	33			85	0%	0,00	
					Not achieved	0,00%	Not achieved
	in comparison to all vas			in comparison to all vas	Average of Assesment Value	in comparison to the maximum achievable of the result of frequency and Impact	

Συμπεράσματα

Σε ένα πολύ μεγάλο ποσοστό υπάρχει πλέον συμφωνία ότι οι υπηρεσίες Cloud είναι το επόμενο βήμα, που θα κάνει ακόμα πιο προσιτή την χρήση συστημάτων και υπολογιστικών δυνατοτήτων. Η χρήση υπηρεσιών cloud computing απαλλάσσει μια επιχείρηση από κόστη απόκτησης, εγκατάστασης, διαχείρισης και διατήρησης εξοπλισμού (υλικού και λογισμικού) με το έξτρα bonus της δυνατότητας πρόσβασης από οπουδήποτε (με την προϋπόθεση ύπαρξης σύνδεσης στο internet) οποιαδήποτε στιγμή.

Ένας από τους πιο βασικούς ανασταλτικούς παράγοντες προς την χρήση των υπηρεσιών Cloud, είναι η ασφάλεια. Προς το παρόν, οι υπηρεσίες δίνονται με την μορφή one size fits all και χωρίς εξειδίκευση στις ανάγκες ασφαλείας του πελάτη, υπό το πρόσχημα ότι πρέπει να είναι τόσο «ευέλικτες» προκειμένου να μπορούν να εξυπηρετήσουν όλους τους πελάτες τους.

Μέσα από την εργασία αυτή, έγινε μια επεξεργασία ενός συνόλου αδυναμιών των υπηρεσιών cloud και ορίστηκε ανά περίπτωση ένα baseline πάνω από το οποίο ή υπηρεσία θα ήταν επιθυμητό να βρίσκεται σε σχέση με την ασφάλεια. Οι αδυναμίες αυτές, έχουν επιλεχτεί διότι μπορούν να μετρηθούν αυτόματα ή ημι-αυτόματα πριν την τελική επιλογή ενός παρόχου υπηρεσιών cloud.

Για την αξιολόγηση της επίτευξης του baseline αυτού, προτείνονται ανά αδυναμία μια σειρά από χαρακτηριστικά και μια μεθοδολογία ανά χαρακτηριστικό για την μέτρησή τους. Η αποτύπωση της αξιολόγησης των κριτηρίων αυτών ως προς το baseline μπορεί να γίνει μέσω του αρχείου Excel που συνοδεύει την μεθοδολογία. Η αποτίμηση γίνεται με βάση τα κριτήρια και τελικά εξάγεται σε μια κλίμακα (ISO 15504) βαθμού επίτευξης. Ο βαθμός αυτός μπορεί να οδηγήσει στην διευκόλυνση της επιλογής παρόχου υπηρεσίας cloud ή στον έλεγχο μιας παρούσας υπηρεσίας ως προς το baseline.

Ενδιαφέρον, για μελλοντική μελέτη θα ήταν το θέμα της δημιουργίας μιας πλήρους αυτοματοποιημένης λύσης για την αποτίμηση της ασφάλειας μιας υπηρεσίας cloud αλλά και την συσχέτιση της βαθμολογίας αυτής με τα αντίστοιχα συμβόλαια (SLAs) καθώς επίσης και της δημιουργίας μιας μεθοδολογίας και εργαλείου για συστηματικό και συνεχές έλεγχο της ασφάλειας των υπηρεσιών cloud.

Βιβλιογραφία

[1] J. C. R. Licklider, «MEMORANDUM FOR: Members and Affiliates of the Intergalactic Computer Network,» σε *ADVANCED RESEARCH PROJECTS AGENCY*, Washington 25, D.C., 1969.

[2] T. G. Peter Mell, "DRAFT "NIST Cloud Computing Definition", NIST SP 800-145," National Institute of Standards and Technology, Gaithersburg, USA, 2011.

[3] N. I. o. S. a. Technology, «Special Publication 800-146, DRAFT Cloud Computing Synopsis and Recommendations,» National Institute of Standards and Technology, Gaithersburg, MD, 2011.

[4] Hinchliffe, «http://blogs.zdnet.com/Hinchliffe,» Hinchliffe, 1 1 2010. [Ηλεκτρονικό]. Available: http://blogs.zdnet.com/Hinchliffe. [Πρόσβαση 7 7 2012].

[5] H. K. w. P. M. A. B. M. L. Stefan Ried, «Sizing The Cloud – A BT Futures Report, Understanding And Quantifying The Future Of Cloud Computing,» FORRESTER, Cambridge, Mass., 2011.

[6] I. Gartner, «Hype Cycle for Cloud Computing,» Gartner, Inc, Stamford, CT, USA, 2010.

[7] Google, «Google trends,» Google Inc., 1 5 2012. [Ηλεκτρονικό]. Available: www.google.com/trends. [Πρόσβαση 1 5 2012].

[8] ITCandor, «Cloud computing,» ITCandor, 2011.

[9] K. I. Advisory, «From Hype to Future, KPMG's 2010 Cloud Computing Survey,» KPMG IT Advisory, Amstelveen, The Netherlands, 2010.

[10] E. N. a. I. S. A. (ENISA), «An SME perspective on cloud computing,» ENISA, Heraclion, Crete, Greece, 2009.

[11] B. W. Prasad Saripalli, «QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security,» σε *2010 IEEE 3rd International Conference on Cloud Computing*, 2010.

[12] ENISA, «Cloud Computing, benefits, risks and recommendations for information security,» ENISA, Herklion, Crete, Greece, 2009.

[13] C. S. Alliance, «Top Threats to Cloud Computing V1.0,» Cloud Security Alliance, USA, 2010.

[14] M. N. Jay Heiser, «Assessing the Security Risks of Cloud Computing,» Gardner, The Netherlands, 2008.

[15] A. MATHEW, «SECURITY AND PRIVACY ISSUES OF CLOUD COMPUTING; SOLUTIONS AND SECURE FRAMEWORK,» *International Journal of Multidisciplinary Research,* pp. 182-193, Vol.2 Issue 4, 1 04 2012.

[16] D. L. Dimitrios Zissis, «Addressing cloud computing security issues,» *Future Generation Computer Systems,* pp. 583-592, 22 12 2010.

[17] C. B. W. C. M. W. a. G. A. G. Shirlei A. de Chaves, «Customer Security Concerns in Cloud Computing,» ICN 2011 : The Tenth International Conference on Networks, Florianópolis – SC - Brazil, 2011.

[18] I. S. &. M. D.-G. S. &. S. A. I. a. E. U. Commission of the European Communities, *THE FUTURE OF CLOUD COMPUTING. OPPORTUNITIES FOR EUROPEAN CLOUD COMPUTING BEYOND 2010,* European Commission, Information Society and Media, 2010.

[19] NIST , *Special Publication 800-39, Managing Enterprise Risk A Framework for Addressing Cyber Threats to Organizations, Individuals, and the Nation,* NIST , 2007.

[20] Federal Cloud Computing Initiative, *Proposed Security Assessment & Authorization for U.S. Government Cloud Computing,* Federal Cloud Computing Initiative, 2010.

[21] I. t. S. S. 2. I. S. t. Joint Technical Committee ISO/IEC JTC 1, *Information technology — Security techniques — Information security risk management,* Geneva: International Organization for Standardization (ISO), 2011.

[22] R. B. Ajay Jangra, «A SURVEY ON VARIOUS POSSIBLE VULNERABILITIES AND ATTACKS IN CLOUD COMPUTING ENVIRONMENT,» *International Journal of Computing and Business Research,* p. Volume 3 Issue 1, 1 01 2012.

[23] T. Ormandy, *An Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments,* Google Inc., 2007.

[24] M. S. Karen Scarfone, *Guide to Enterprise Password Management (Draft),* Gaithersburg, MD: National Institute of Standards and Technology, 2009.

[25] T. G. Wayne Jansen, *Guidelines on Security and Privacy in Public Cloud Computing,* Gaithersburg, MD: National Institute of Standards and Technology, 2011.

[26] DMTF Informational, *Use Cases and Interactions for Managing Clouds,* Distributed Management Task Force, Inc., 2010.

[27] L. B. M. I. J. M. S. C. Fred Whiteside, *Challenging Security Requirements for US Government Cloud Computing Adoption (Draft,* Gaithersburg, MD: National Institute of Standards and Technology, May 2012.

[28] R. B. S. C. M. H. F. L. V. K. J. M. J. M. K. M. A. S. J. T. F. W. a. D. L. Lee Badger, *US Government Cloud Computing Technology Roadmap Volume II - Useful Information for Cloud Adopters,* Gaithersburg, MD: NIST Cloud Computing Program, 2011.

[29] C. H. a. A. F. Gary Stoneburner, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A,* Gaithersburg, MD: National Institute of Standards and Technology,

2004.

[30] M. S. A. C. A. O. Karen Scarfone, *Technical Guide to Information Security Testing and Assessment,* Gaithersburg, MD: National Institute of Standards and Technology, 2008.

[31] T. G. Wayne Jansen, *Guidelines on Security and Privacy Cloud Computing,* Gaithersburg, MD: National Institute of Standards and Technology, 2011.

[32] P. M. C. Y.-M. W. C. V. H. J. W. J. R. L. Samuel T King, «SubVirt: implementing malware with virtual machines,» Michigan, 21-24 May 2006.

[33] VMware Inc, «VMware Inc,» VMware Inc, 16 10 2009. [Ηλεκτρονικό]. Available: http://lists.vmware.com/pipermail/security-announce/2009/000067.html. [Πρόσβαση 7 7 2012].

[34] VMware Inc, «VMware Inc,» VMware Inc, 20 8 2009. [Ηλεκτρονικό]. Available: http://lists.vmware.com/pipermail/security-announce/2009/000062.html. [Πρόσβαση 7 7 2012].

[35] VMware Inc., «VMware Inc.,» VMware Inc., 10 6 2012. [Ηλεκτρονικό]. Available: http://lists.vmware.com/pipermail/security-announce/2012/subject.html#start. [Πρόσβαση 7 7 2012].

[36] K. Kortchinsky, *CLOUDBURST A VMware Guest to Host Escape Story,* Las Vegas: Immunity, Black Hat 2009, 2009.

[37] B. Schneier, «www.schneier.com,» Schneier, Bruce, 1 7 2009. [Ηλεκτρονικό]. Available: http://www.schneier.com/blog/archives/2009/07/homomorphic_enc.html. [Πρόσβαση 7 7 2012].

[38] R. W. X. W. K. Z. Shuo Chen, «Side-Channel Leaks in Web Applications: a Reality Today, a Challenge Tomorrow,» Microsoft Research, Redmond, WA, USA, 2010.

[39] *Information technology -- Process assessment -- Part 3: Guidance on performing an assessment,* International Organization for Standardization (ISO), 2004.

[40] L. B. M. I. J. M. S. C. Fred Whiteside, «Challenging Security Requirements for US Government Cloud Computing Adoption (Draft),» Cloud Computing Program Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, May 2012.

Παράρτημα Α

GOOGLE – generic

Google Terms of Service

Last modified: March 1, 2012

Welcome to Google!

Thanks for using our products and services ("Services"). The Services are provided by Google Inc. ("Google"), located at 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States.

….

Your Google Account

You may need a Google Account in order to use some of our Services. You may create your own Google Account, or your Google Account may be assigned to you by an administrator, such as your employer or educational institution. If you are using a Google Account assigned to you by an administrator, different or additional terms may apply and your administrator may be able to access or disable your account.

If you learn of any unauthorized use of your password or account, follow these instructions.

Privacy and Copyright Protection

Google's privacy policies explain how we treat your personal data and protect your privacy when you use our Services. By using our Services, you agree that Google can use such data in accordance with our privacy policies.

We respond to notices of alleged copyright infringement and terminate accounts of repeat infringers according to the process set out in the U.S. Digital Millennium Copyright Act.

We provide information to help copyright holders manage their intellectual property online. If you think somebody is violating your copyrights and want to notify us, you can find information about submitting notices and Google's policy about responding to notices in our Help Center.

Your Content in our Services

Some of our Services allow you to submit content. You retain ownership of any intellectual property rights that you hold in that content. In short, what belongs to you stays yours.

When you upload or otherwise submit content to our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content. The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones. This license continues even if you stop using our Services (for example, for a business listing you have added to Google Maps). Some Services may offer you ways to access and remove content that has been provided to that Service. Also, in some of our Services, there are terms or settings that narrow the scope of our use of the content submitted in those Services. Make sure you have the necessary rights to grant us this license for any content that you submit to our Services.

You can find more information about how Google uses and stores content in the privacy policy or additional terms for particular Services. If you submit feedback or suggestions about our Services, we may use your feedback or suggestions without obligation to you.

About Software in our Services

When a Service requires or includes downloadable software, this software may update automatically on your device once a new version or feature is available. Some Services may let you adjust your automatic update settings.

…

We believe that you own your data and preserving your access to such data is important. If we discontinue a Service, where reasonably possible, we will give you reasonable advance notice and a chance to get information out of that Service.

…

Other than as expressly set out in these terms or additional terms, neither Google nor its suppliers or distributors make any specific promises about the Services. For example, we don't make any commitments about the content within the Services, the specific functions of the Services, or their reliability, availability, or ability to meet your needs. We provide the Services "as is".

Some jurisdictions provide for certain warranties, like the implied warranty of merchantability, fitness for a particular purpose and non-infringement. To the extent permitted by law, we exclude all warranties.

Liability for our Services

When permitted by law Google, and Google's suppliers and distributors, will not be responsible for lost profits, revenues, or data, financial losses or indirect, special, consequential, exemplary, or punitive damages.

To the extent permitted by law, the total liability of Google, and its suppliers and distributors, for any claims under these terms, including for any implied warranties, is limited to the amount you paid us to use the Services (or, if we choose, to supplying you the Services again).

In all cases, Google, and its suppliers and distributors, will not be liable for any loss or damage that is not reasonably foreseeable

…

The courts in some countries will not apply California law to some types of disputes. If you reside in one of those countries, then where California law is excluded from applying, your country's laws will apply to such disputes related to these terms. Otherwise, you agree that the laws of California, U.S.A., excluding California's choice of law rules, will apply to any disputes arising out of or relating to these terms or the Services. Similarly, if the courts in your country will not permit you to consent to the jurisdiction and venue of the courts in Santa Clara County, California, U.S.A., then your local jurisdiction and venue will apply to such disputes related to these terms. Otherwise, all claims arising out of or relating to these terms or the services will be litigated exclusively in the federal or state courts of Santa Clara County, California, USA, and you and Google consent to personal jurisdiction in those courts.

For information about how to contact Google, please visit our contact page.

Salesforce

Master Subscription Agreement

This master subscription agreement (“agreement”) governs your acquisition and use of our services.

If you register for a free trial for our services, this agreement will also govern that free trial.

By accepting this agreement, either by clicking a box indicating your acceptance or by executing an order form that references this agreement, you agree to the terms of this agreement. If you are entering into this agreement on behalf of a company or other legal entity, you represent that you have the authority to bind such entity and its affiliates to these terms and conditions, in which case the terms "you" or "your" shall refer to such entity and its affiliates. If you do not have such authority, or if you do not agree with these terms and conditions, you must not accept this agreement and may not use the services.

…

4. USE OF THE SERVICES

4.1. Our Responsibilities. We shall: (i) provide Our basic support for the Purchased Services to You at no additional charge, and/or upgraded support if purchased separately, (ii) use commercially reasonable efforts to make the Purchased Services available 24 hours a day, 7 days a week, except for: (a) planned downtime (of which We shall give at least 8 hours notice via the Purchased Services and which We shall schedule to the extent practicable during the weekend hours from 6:00 p.m. Friday to 3:00 a.m. Monday Pacific Time), or (b) any unavailability caused by circumstances beyond Our reasonable control, including without limitation, acts of God, acts of government, floods, fires, earthquakes, civil unrest, acts of terror, strikes or other labor problems (other than those involving Our employees), Internet service provider failures or delays, or denial of service attacks, and (iii) provide the Purchased Services only in accordance with applicable laws and government regulations.

4.2. Our Protection of Your Data. We shall maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Your Data. We shall not (a) modify Your Data, (b) disclose Your Data except as compelled by law in accordance with Section 8.3 (Compelled Disclosure) or as expressly permitted in writing by You, or (c) access Your Data except to provide the Services and prevent or address service or technical problems, or at Your request in connection with customer support matters.

4.3. Your Responsibilities. You shall (i) be responsible for Users' compliance with this Agreement, (ii) be responsible for the accuracy, quality and legality of Your Data and of the means by which You acquired Your Data, (iii) use commercially reasonable efforts to prevent unauthorized access to or use of the Services, and notify Us promptly of any such unauthorized access or use, and (iv) use the Services only in accordance with the User Guide and applicable laws and government regulations. You shall not (a) make the Services available to anyone other than Users, (b) sell, resell, rent or lease the Services, (c) use the Services to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy rights, (d) use the Services to store or transmit Malicious Code, (e) interfere with or disrupt the integrity or performance of the Services or third-party data contained therein, or (f) attempt to gain unauthorized access to the Services or their related systems or networks.

4.3. Usage Limitations. Services may be subject to other limitations, such as, for example, limits on disk storage space, on the number of calls You are permitted to make against Our application programming interface, and, for Services that enable You to provide public websites, on the number of page views by visitors to those websites. Any such limitations are specified in the User Guide. The Services provide real-time information to enable You to monitor Your compliance with such limitations.

…

8. CONFIDENTIALITY

8.1. Definition of Confidential Information. As used herein, "Confidential Information" means all confidential information disclosed by a party ("Disclosing Party") to the other party ("Receiving Party"), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of

the information and the circumstances of disclosure. Your Confidential Information shall include Your Data; Our Confidential Information shall include the Services; and Confidential Information of each party shall include the terms and conditions of this Agreement and all Order Forms, as well as business and marketing plans, technology and technical information, product plans and designs, and business processes disclosed by such party. However, Confidential Information (other than Your Data) shall not include any information that (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party, (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party, (iii) is received from a third party without breach of any obligation owed to the Disclosing Party, or (iv) was independently developed by the Receiving Party.

8.2. Protection of Confidential Information. The Receiving Party shall use the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind (but in no event less than reasonable care) (i) not to use any Confidential Information of the Disclosing Party for any purpose outside the scope of this Agreement, and (ii) except as otherwise authorized by the Disclosing Party in writing, to limit access to Confidential Information of the Disclosing Party to those of its and its Affiliates' employees, contractors and agents who need such access for purposes consistent with this Agreement and who have signed confidentiality agreements with the Receiving Party containing protections no less stringent than those herein. Neither party shall disclose the terms of this Agreement or any Order Form to any third party other than its Affiliates and their legal counsel and accountants without the other party's prior written consent.

8.3. Compelled Disclosure. The Receiving Party may disclose Confidential Information of the Disclosing Party if it is compelled by law to do so, provided the Receiving Party gives the Disclosing Party prior notice of such compelled disclosure (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure. If the Receiving Party is compelled by law to disclose the Disclosing Party's Confidential Information as part of a civil proceeding to which the Disclosing Party is a party, and the Disclosing Party is not

contesting the disclosure, the Disclosing Party will reimburse the Receiving Party for its reasonable cost of compiling and providing secure access to such Confidential Information.

Back to Top

9. WARRANTIES AND DISCLAIMERS

9.1. Our Warranties. We warrant that (i) We have validly entered into this Agreement and have the legal power to do so, (ii) the Services shall perform materially in accordance with the User Guide, (iii) subject to Section 5.3 (Integration with Non-Salesforce.com Services), the functionality of the Services will not be materially decreased during a subscription term, and (iv) We will not transmit Malicious Code to You, provided it is not a breach of this subpart (iv) if You or a User uploads a file containing Malicious Code into the Services and later downloads that file containing Malicious Code. For any breach of a warranty above, Your exclusive remedy shall be as provided in Section 12.3 (Termination for Cause) and Section 12.4 (Refund or Payment upon Termination) below.

9.2. Your Warranties. You warrant that You have validly entered into this Agreement and have the legal power to do so.

9.3. Disclaimer. EXCEPT AS EXPRESSLY PROVIDED HEREIN, NEITHER PARTY MAKES ANY WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND EACH PARTY SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.

9.4. Non-GA Services. From time to time We may invite You to try, at no charge, Our products or services that are not generally available to Our customers ("Non-GA Services"). You may accept or decline any such trial in Your sole discretion. Any Non-GA Services will be clearly designated as beta, pilot, limited release, developer preview, non-production or by a description of similar import. Non-GA Services are provided for evaluation purposes and not for production use, are not supported, may contain bugs or errors, and may be subject to additional terms. NON-GA SERVICES ARE NOT CONSIDERED "SERVICES" HEREUNDER AND ARE PROVIDED "AS IS" WITH

NO EXPRESS OR IMPLIED WARRANTY. We may discontinue Non-GA Services at any time in Our sole discretion and may never make them generally available.

Back to Top

10. MUTUAL INDEMNIFICATION

10.1. Indemnification by Us. We shall defend You against any claim, demand, suit, or proceeding made or brought against You by a third party alleging that the use of the Services as permitted hereunder infringes or misappropriates the intellectual property rights of a third party (a "Claim Against You"), and shall indemnify You for any damages, attorney fees and costs finally awarded against You as a result of, and for amounts paid by You under a court-approved settlement of, a Claim Against You; provided that You (a) promptly give Us written notice of the Claim Against You; (b) give Us sole control of the defense and settlement of the Claim Against You (provided that We may not settle any Claim Against You unless the settlement unconditionally releases You of all liability); and (c) provide to Us all reasonable assistance, at Our expense. In the event of a Claim Against You, or if We reasonably believe the Services may infringe or misappropriate, We may in Our discretion and at no cost to You (i) modify the Services so that they no longer infringe or misappropriate, without breaching Our warranties under “Our Warranties” above, (ii) obtain a license for Your continued use of the Services in accordance with this Agreement, or (iii) terminate Your User subscriptions for such Services upon 30 days’ written notice and refund to You any prepaid fees covering the remainder of the term of such User subscriptions after the effective date of termination.

10.2. Indemnification by You. You shall defend Us against any claim, demand, suit or proceeding made or brought against Us by a third party alleging that Your Data, or Your use of the Services in breach of this Agreement, infringes or misappropriates the intellectual property rights of a third party or violates applicable law (a "Claim Against Us"), and shall indemnify Us for any damages, attorney fees and costs finally awarded against Us as a result of, or for any amounts paid by Us under a court-approved settlement of, a Claim Against Us; provided that We (a) promptly give You written notice of the Claim Against Us; (b) give You sole control of the defense and settlement of the Claim Against Us (provided that You may not settle any Claim Against Us unless the

settlement unconditionally releases Us of all liability); and (c) provide to You all reasonable assistance, at Your expense.

10.3. Exclusive Remedy. This Section 10 (Mutual Indemnification) states the indemnifying party's sole liability to, and the indemnified party's exclusive remedy against, the other party for any type of claim described in this Section.

…

12.5. Return of Your Data. Upon request by You made within 30 days after the effective date of termination of a Purchased Services subscription, We will make available to You for download a file of Your Data in comma separated value (.csv) format along with attachments in their native format. After such 30-day period, We shall have no obligation to maintain or provide any of Your Data and shall thereafter, unless legally prohibited, delete all of Your Data in Our systems or otherwise in Our possession or under Our control.

12.6. Surviving Provisions. Section 6 (Fees and Payment for Purchased Services), 7 (Proprietary Rights), 8 (Confidentiality), 9.3 (Disclaimer), 10 (Mutual Indemnification), 11 (Limitation of Liability), 12.4 (Refund or Payment upon Termination), 12.5 (Return of Your Data), 13 (Who You Are Contracting With, Notices, Governing Law and Jurisdiction) and 14 (General Provisions) shall survive any termination or expiration of this Agreement.

Salesforce – II

Statements

At salesforce.com, there is no higher priority than the privacy and security of our customers' data. We believe that protecting the privacy of our customers' data is integral to our mission of earning and maintaining the trust of each of our customers. We seek to lead the industry as a trusted repository for customer data through a world-class privacy program and provide a secure infrastructure and flexible tools that help enable our customers to comply with global privacy and data protection regulations.

Salesforce.com understands that the confidentiality, integrity, and availability of our customers' information are vital to their business operations and our own success. We use a multi-layered approach to protect that key information, constantly monitoring and improving our application, systems, and processes to meet the growing demands and challenges of security.

Secure data centers

Our service is collocated in dedicated spaces at top-tier data centers. These facilities provide carrier-level support, including:

Access control and physical security

24-hour manned security, including foot patrols and perimeter inspections

Biometric scanning for access

Dedicated concrete-walled Data Center rooms

Computing equipment in access-controlled steel cages

Video surveillance throughout facility and perimeter

Building engineered for local seismic, storm, and flood risks

Tracking of asset removal

Environmental controls

Humidity and temperature control

Redundant (N+1) cooling system

Power

Underground utility power feed

Redundant (N+1) CPS/UPS systems

Redundant power distribution units (PDUs)

Redundant (N+1) diesel generators with on-site diesel fuel storage

Network

Concrete vaults for fiber entry

Redundant internal networks

Network neutral; connects to all major carriers and located near major Internet hubs

High bandwidth capacity

Fire detection and suppression

VESDA (very early smoke detection apparatus)

Dual-alarmed, dual-interlock, multi-zone, pre-action dry pipe water-based fire suppression

Secure transmission and sessions

Connection to the Salesforce environment is via SSL 3.0/TLS 1.0, using global step-up certificates from Verisign, ensuring that our users have a secure connection from their browsers to our service

Individual user sessions are identified and re-verified with each transaction, using a unique token created at login

Network protection

Perimeter firewalls and edge routers block unused protocols

Internal firewalls segregate traffic between the application and database tiers

Intrusion detection sensors throughout the internal network report events to a security event management system for logging, alerts, and reports

A third-party service provider continuously scans the network externally and alerts changes in baseline configuration

Disaster Recovery

The Salesforce service performs real-time replication to disk at each data center, and near real-time data replication between the production data center and the disaster recovery center

Data are transmitted across encrypted links.

Disaster recovery tests verify our projected recovery times and the integrity of the customer data

Backups

All data are backed up to tape at each data center, on a rotating schedule of incremental and full backups

The backups are cloned over secure links to a secure tape archive

Tapes are not transported offsite and are securely destroyed when retired

Internal and Third-party testing and assessments

Salesforce.com tests all code for security vulnerabilities before release, and regularly scans our network and systems for vulnerabilities. Third-party assessments are also conducted regularly:

Application vulnerability threat assessments

Network vulnerability threat assessments

Selected penetration testing and code review

Security control framework review and testing

Security Monitoring

Our Information Security department monitors notification from various sources and alerts from internal systems to identify and manage threats.

RightNow Technologies

Mater Cloud Services Agreement with Customer

This Master Agreement ("Agreement") is between RightNow Technologies, Inc. ("RightNow"), a Delaware corporation, and Customer. It should be read together with each Order Form. Parts of this Agreement may not apply to a particular Customer.

…

1.2. Customer must have a high speed Internet connection, and hardware and software that is compatible with the Subscription Services, as set out in the Documentation. None of these things are RightNow's responsibility.

1.3. RightNow regularly upgrades and updates the Subscription Services. This means that the Subscription Services are continually evolving. Some of these changes will occur automatically, while others may require Customer to schedule and implement the changes. The changes may also mean that Customer needs to upgrade its equipment in order to make efficient use of the Subscription Services. RightNow will provide Customer with advance notification in this case.

1.4. RightNow recognizes that Customer may have legitimate business reasons for not upgrading to a new version of the Subscription Services as soon as the version becomes available. However, RightNow will not support old versions indefinitely. RightNow has policy that sets out what happens when old versions reach end-of-life (to view the current policy, click on this link). When an old version used by Customer is at end-of-life, RightNow may remove Customer's access to that version and upgrade Customer to a new version.

…

3. Customer Data.

3.1. Customer must provide all data for use in the Subscription Services, and RightNow is not obliged to modify or add to the Customer Data. Customer is solely responsible for the content and accuracy of the Customer Data.

3.2. The Customer Data belongs to Customer, and RightNow makes no claim to any right of ownership in it.

3.3. RightNow must keep the Customer Data confidential in accordance with Section 13of this Agreement.

3.4. RightNow must use the Customer Data strictly as necessary to carry out its obligations under this Agreement, and for no other purpose. However, RightNow:

3.4.1. may observe and report back to Customer on Customer's usage of the Subscription Services, and make recommendations for improved usage of the Subscription Services;

3.4.2. may identify trends and publish reports on its findings provided the reports include data aggregated from more than one customer site and do not identify Customer; and,

3.4.3. must ensure that the data center containing the Customer Data meets the following physical and electronic security requirements: (i) single point of entry; (ii) main access monitored with additional access for emergency purposes only; (iii) surveillance cameras in facility; (iv) access validation with identity check; (v) access only to persons on RightNow approved access list; (vi) log-in validation; (vii) creation of accounts only as verified by RightNow or sub-contracted hosting provider; (viii) access to servers via encrypted means; and, (ix) servers running behind secure firewall.

3.5. RightNow must comply with the principles of the EU Data Protection Directive 95/46 and the Telecoms Data Protection Directive as amended ("the Directives") and any successor legislation, in relation to any "personal data" received by or originating from Customer and Customer clients, to the extent that the Directives apply to "data processors".

3.6. RightNow must take reasonable technical and organizational measures to keep personal data secure and to protect it against accidental loss or unlawful destruction, alteration, disclosure or access; and, must deal with the information only in accordance with Customer's instructions, provided they are reasonable and lawful.

3.7. RightNow must back up Customer Data once in each 24-hour period.

4. Subscription Services Warranties. RightNow warrants that: (i) the Subscription Services will function substantially as described in the Documentation; and (ii) RightNow owns or otherwise has the right to provide the Subscription Services to Customer under this Agreement.

….

13. Confidentiality.

13.1. The Subscription Services, Software, Documentation and Work Product contain valuable trade secrets that are the sole property of RightNow, and Customer agrees to use reasonable care to prevent other parties from learning of these trade secrets. Customer must take reasonable care to prevent unauthorized access to or duplication of the Subscription Services, Software, Documentation, and Work Product.

13.2. The Customer Data may include valuable trade secrets that are the sole property of Customer. RightNow must take reasonable care to prevent other parties from learning of these trade secrets.

13.3. Sections 13.1 and 13.2 do not apply to any information that (i) is now, or subsequently becomes, through no act or failure to act on the part of receiving party (the "Receiver"), generally known or available; (ii) is known by the Receiver at the time of receiving such information, as evidenced by the Receiver's records; (iii) is subsequently provided to the Receiver by a third party, as a matter of right and without restriction on disclosure; or (iv) is required to be disclosed by law, provided that the party to whom the information belongs is given prior written notice of any such proposed disclosure.

14. Indemnification by RightNow. RightNow must indemnify and hold harmless Customer, its affiliates, directors and employees from any damages finally awarded against Customer (including, without limitation, reasonable costs and legal fees incurred by Customer) arising out of any third party suit, claim or other legal action alleging that the use of the Subscription Services, Documentation or Work Product by Customer infringes any copyright, trade secret or United States patent, ("Legal Action"). RightNow must also assume the defense of the Legal Action.

14.1. However, RightNow shall have no indemnification obligations for any Legal Action arising out of: (i) a combination of the Subscription Services, Software or Work Product with software or products not supplied, or approved in writing by RightNow; (ii) any repair, adjustment, modification or alteration to the Subscription Services by Customer or any third party, unless approved in writing by RightNow; or (iii) any refusal by Customer to install and use a non-infringing version of the Subscription Services, or

Work Product offered by RightNow under Section 4.2(ii). Section 4.2(ii) and this Section 14 state the entire liability of RightNow with respect to any intellectual property infringement by the Subscription Services, Software or Work Product.

AWS Customer Agreement

Last updated March 15, 2012

(current AWS customers: See What's Changed)

This AWS Customer Agreement (this "Agreement") contains the terms and conditions that govern your access to and use of the Service Offerings (as defined below) and is an agreement between Amazon Web Services LLC ("AWS," "we," "us," or "our") and you or the entity you represent ("you"). This Agreement takes effect when you click an "I Accept" button or check box presented with these terms or, if earlier, when you use any of the Service Offerings (the "Effective Date"). You represent to us that you are lawfully able to enter into contracts (e.g., you are not a minor). If you are entering into this Agreement for an entity, such as the company you work for, you represent to us that you have legal authority to bind that entity. Please see Section 14 for definitions of certain capitalized terms used in this Agreement.

…

1.2 Your Account. To access the Services, you must create an AWS account associated with a valid e-mail address. Unless explicitly permitted by the Service Terms, you may only create one account per email address. You are responsible for all activities that occur under your account, regardless of whether the activities are undertaken by you, your employees or a third party (including your contractors or agents) and, except to the extent caused by our breach of this Agreement, we and our affiliates are not responsible for unauthorized access to your account. You will contact us immediately if you believe an unauthorized third party may be using your account or if your account information is lost or stolen. You may terminate your account and this Agreement at any time in accordance with Section 7.

….

3. Security and Data Privacy.

3.1 AWS Security. Without limiting Section 10 or your obligations under Section 4.2, we will implement reasonable and appropriate measures designed to help you secure Your Content against accidental or unlawful loss, access or disclosure.

3.2 Data Privacy. We participate in the safe harbor programs described in the Privacy Policy. You may specify the AWS regions in which Your Content will be stored and accessible by End Users. We will not move Your Content from your selected AWS regions without notifying you, unless required to comply with the law or requests of governmental entities. You consent to our collection, use and disclosure of information associated with the Service Offerings in accordance with our Privacy Policy, and to the processing of Your Content in, and the transfer of Your Content into, the AWS regions you select.

…

4.2 Other Security and Backup. You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain appropriate security, protection and backup of Your Content, which may include the use of encryption technology to protect Your Content from unauthorized access and routine archiving Your Content. AWS log-in credentials and private keys generated by the Services are for your internal use only and you may not sell, transfer or sublicense them to any other entity or person, except that you may disclose your private key to your agents and subcontractors performing work on your behalf.

…

13.1 Confidentiality and Publicity. You may use AWS Confidential information only in connection with your use of the Service Offerings as permitted under this Agreement. You will not disclose AWS Confidential Information during the Term or at any time during the 5 year period following the end of the Term. You will take all reasonable measures to avoid disclosure, dissemination or unauthorized use of AWS Confidential Information, including, at a minimum, those measures you take to protect your own

confidential information of a similar nature. You will not issue any press release or make any other public communication with respect to this Agreement or your use of the Service Offerings. You will not misrepresent or embellish the relationship between us and you (including by expressing or implying that we support, sponsor, endorse, or contribute to you or your business endeavors), or express or imply any relationship or affiliation between us and you or any other person or entity except as expressly permitted by this Agreement.

13.2 Force Majeure. We and our affiliates will not be liable for any delay or failure to perform any obligation under this Agreement where the delay or failure results from any cause beyond our reasonable control, including acts of God, labor disputes or other industrial disturbances, systemic electrical, telecommunications, or other utility failures, earthquake, storms or other elements of nature, blockages, embargoes, riots, acts or orders of government, acts of terrorism, or war.

Amazon.com Privacy Notice

Last updated: April 6, 2012. To see what has changed, click here.

Amazon.com knows that you care how information about you is used and shared, and we appreciate your trust that we will do so carefully and sensibly. This notice describes our privacy policy. By visiting Amazon.com, you are accepting the practices described in this Privacy Notice.

What About Cookies?

Cookies are unique identifiers that we transfer to your device to enable our systems to recognize your device and to provide features such as 1-Click purchasing, Recommended for You, personalized advertisements on other Web sites (e.g., Amazon Associates with content served by Amazon.com and Web sites using Checkout by Amazon payment service), and storage of items in your Shopping Cart between visits.

…

How Secure Is Information About Me?

We work to protect the security of your information during transmission by using Secure Sockets Layer (SSL) software, which encrypts information you input.

We reveal only the last four digits of your credit card numbers when confirming an order. Of course, we transmit the entire credit card number to the appropriate credit card company during order processing.

It is important for you to protect against unauthorized access to your password and to your computer. Be sure to sign off when finished using a shared computer. Click here for more information on how to sign off.

…

Information You Give Us

You provide most such information when you search, buy, post, participate in a contest or questionnaire, or communicate with customer service. For example, you provide information when you search for a product; place an order through Amazon.com

or one of our third-party sellers; provide information in Your Account (and you might have more than one if you have used more than one e-mail address when shopping with us) or Your Profile; communicate with us by phone, e-mail, or otherwise; complete a questionnaire or a contest entry form; use our services such as Amazon Instant Video; compile Wish Lists or other gift registries; participate in Discussion Boards or other community features; provide and rate Reviews; specify a Special Occasion Reminder; and employ Product Availability Alerts, such as Available to Order Notifications. As a result of those actions, you might supply us with such information as your name, address, and phone numbers; credit card information; people to whom purchases have been shipped, including addresses and phone number; people (with addresses and phone numbers) listed in 1-Click settings; e-mail addresses of your friends and other people; content of reviews and e-mails to us; personal description and photograph in Your Profile; and financial information, including Social Security and driver's license numbers.

Automatic Information

Examples of the information we collect and analyze include the Internet protocol (IP) address used to connect your computer to the Internet; login; e-mail address; password; computer and connection information such as browser type, version, and time zone setting, browser plug-in types and versions, operating system, and platform; purchase history, which we sometimes aggregate with similar information from other customers to create features like Top Sellers; the full Uniform Resource Locator (URL) clickstream to, through, and from our Web site, including date and time; cookie number; products you viewed or searched for; and the phone number you used to call our 800 number. We may also use browser data such as cookies, Flash cookies (also known as Flash Local Shared Objects), or similar data on certain parts of our Web site for fraud prevention and other purposes. During some visits we may use software tools such as JavaScript to measure and collect session information, including page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page. We may also collect technical information to help us identify your device for fraud prevention and diagnostic purposes.

….

AWS Customer Agreement

Last updated March 15, 2012
(current AWS customers: See What's Changed)

This AWS Customer Agreement (this "Agreement") contains the terms and conditions that govern your access to and use of the Service Offerings (as defined below) and is an agreement between Amazon Web Services LLC ("AWS," "we," "us," or "our") and you or the entity you represent ("you"). This Agreement takes effect when you click an "I Accept" button or check box presented with these terms or, if earlier, when you use any of the Service Offerings (the "Effective Date"). You represent to us that you are lawfully able to enter into contracts (e.g., you are not a minor). If you are entering into this Agreement for an entity, such as the company you work for, you represent to us that you have legal authority to bind that entity. Please see Section 14 for definitions of certain capitalized terms used in this Agreement.

…

1.2 Your Account. To access the Services, you must create an AWS account associated with a valid e-mail address. Unless explicitly permitted by the Service Terms, you may only create one account per email address. You are responsible for all activities that occur under your account, regardless of whether the activities are undertaken by you, your employees or a third party (including your contractors or agents) and, except to the extent caused by our breach of this Agreement, we and our affiliates are not responsible for unauthorized access to your account. You will contact us immediately if you believe an unauthorized third party may be using your account or if your account information is lost or stolen. You may terminate your account and this Agreement at any time in accordance with Section 7.

…

3. Security and Data Privacy.

3.1 AWS Security. Without limiting Section 10 or your obligations under Section 4.2, we will implement reasonable and appropriate measures designed to help you secure Your Content against accidental or unlawful loss, access or disclosure.

3.2 Data Privacy. We participate in the safe harbor programs described in the Privacy Policy. You may specify the AWS regions in which Your Content will be stored and accessible by End Users. We will not move Your Content from your selected AWS regions without notifying you, unless required to comply with the law or requests of governmental entities. You consent to our collection, use and disclosure of information associated with the Service Offerings in accordance with our Privacy Policy, and to the processing of Your Content in, and the transfer of Your Content into, the AWS regions you select.

…

4.2 Other Security and Backup. You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain appropriate security, protection and backup of Your Content, which may include the use of encryption technology to protect Your Content from unauthorized access and routine archiving Your Content. AWS log-in credentials and private keys generated by the Services are for your internal use only and you may not sell, transfer or sublicense them to any other entity or person, except that you may disclose your private key to your agents and subcontractors performing work on your behalf.

…

11. Limitations of Liability.

WE AND OUR AFFILIATES OR LICENSORS WILL NOT BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, OR DATA), EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHER, NEITHER WE NOR ANY OF OUR

AFFILIATES OR LICENSORS WILL BE RESPONSIBLE FOR ANY COMPENSATION, REIMBURSEMENT, OR DAMAGES ARISING IN CONNECTION WITH: (A) YOUR INABILITY TO USE THE SERVICES, INCLUDING AS A RESULT OF ANY (I) TERMINATION OR SUSPENSION OF THIS AGREEMENT OR YOUR USE OF OR ACCESS TO THE SERVICE OFFERINGS, (II) OUR DISCONTINUATION OF ANY OR ALL OF THE SERVICE OFFERINGS, OR, (III) WITHOUT LIMITING ANY OBLIGATIONS UNDER THE SLAS, ANY UNANTICIPATED OR UNSCHEDULED DOWNTIME OF ALL OR A PORTION OF THE SERVICES FOR ANY REASON, INCLUDING AS A RESULT OF POWER OUTAGES, SYSTEM FAILURES OR OTHER INTERRUPTIONS; (B) THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; (c) ANY INVESTMENTS, EXPENDITURES, OR COMMITMENTS BY YOU IN CONNECTION WITH THIS AGREEMENT OR YOUR USE OF OR ACCESS TO THE SERVICE OFFERINGS; OR (D) ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ANY OF YOUR CONTENT OR OTHER DATA. IN ANY CASE, OUR AND OUR AFFILIATES' AND LICENSORS' AGGREGATE LIABILITY UNDER THIS AGREEMENT WILL BE LIMITED TO THE AMOUNT YOU ACTUALLY PAY US UNDER THIS AGREEMENT FOR THE SERVICE THAT GAVE RISE TO THE CLAIM DURING THE 12 MONTHS PRECEDING THE CLAIM.

…

13. Miscellaneous.

13.1 Confidentiality and Publicity. You may use AWS Confidential information only in connection with your use of the Service Offerings as permitted under this Agreement. You will not disclose AWS Confidential Information during the Term or at any time during the 5 year period following the end of the Term. You will take all reasonable measures to avoid disclosure, dissemination or unauthorized use of AWS Confidential

Information, including, at a minimum, those measures you take to protect your own confidential information of a similar nature. You will not issue any press release or make any other public communication with respect to this Agreement or your use of the Service Offerings. You will not misrepresent or embellish the relationship between us and you (including by expressing or implying that we support, sponsor, endorse, or contribute to you or your business endeavors), or express or imply any relationship or affiliation between us and you or any other person or entity except as expressly permitted by this Agreement.

….

AWS Service Terms

Last updated: May 8, 2012

The following Service Terms apply only to the specific Services to which the Service Terms relate. In the event of a conflict between the terms of these Service Terms and the terms of the AWS Customer Agreement or other agreement with us governing your use of our Services (the "Agreement"), the terms and conditions of these Service Terms apply, but only to the extent of such conflict. Capitalized terms used herein but not defined herein shall have the meanings set forth in the Agreement.

…

We may disclose your company name, the IBM Software your company has used, and your company's total usage fees for the IBM Software (collectively, "Usage Data"). IBM is required to keep Usage Data confidential and IBM cannot use Usage Data for marketing or lead generation.

…

13.6. You should back-up Data prior to delivery to us. Your Data should not include live or production data or any other data that you are not prepared to lose. For avoidance of doubt, Your Content includes Data.

13.7. You represent that you have all necessary rights to (a) provide the Media and Data to us for upload into Amazon S3 or Amazon EBS and (b) authorize our transfer of any Data specified by you to the Media. You represent that import or export of the Media or Data to or from us does not require a license under the laws or regulations of any country.

13.8. We may reproduce Data as necessary to transfer it between Media and Amazon S3 or Amazon EBS.

….

14. Amazon Virtual Private Cloud (Amazon VPC)

14.1. You may only use Amazon VPC to connect your computing resources to certain AWS computing resources via a Virtual Private Network (VPN) connection.

14.2. Use of Amazon VPC requires the use of other Services. You are responsible for all applicable fees associated with your use of other Services in connection with Amazon VPC. When you transfer data between AWS computing resources running inside Amazon VPC and AWS computing resources running outside Amazon VPC, you will be charged VPN data transfer rates in addition to any applicable Internet data transfer changes. VPN connection charges accrue during any time your VPN connection is in the "available" state.

14.3. You are solely responsible for the configuration, operation, performance and security of all equipment and computing resources you use with Amazon VPC, including any gateways or other devices you use to connect to Amazon VPC.

15. AWS Multi-Factor Authentication (AWS MFA)

15.1. You may only use AWS MFA in connection with accessing your AWS account.

15.2. Your use of AWS MFA requires the use of other Services. You are responsible for all applicable fees associated with your use of other Services in connection with AWS MFA.

15.3. You are solely responsible for the procurement and for the configuration, operation, performance and security of any hardware or non-AWS software that you use in connection with AWS MFA, including any compatible authentication devices.

16. Amazon Relational Database Service (Amazon RDS)

16.1. You may only use Amazon RDS to store, query, retrieve and serve data and other content owned, licensed or lawfully obtained by you. You acknowledge that neither we nor our licensors are responsible in any manner, and you are solely responsible, for the proper configuration of database security groups and other security settings associated with Amazon RDS.

16.2. You may store snapshots of Your Amazon RDS Content for later use in Amazon RDS but snapshots cannot be downloaded outside the Services.

16.3. We may terminate your Amazon RDS database instance if you attempt to access or tamper with any software we pre-load on the database instance, including the operating system software running on the database instance.

16.4. You are responsible for configuring your backup retention period to give yourself enough time to recover data from your backups in the event of a hardware or file system failure.

16.5. Reserved DB Instance Pricing. You may designate Amazon RDS database instances as subject to the reserved pricing and payment terms ("Reserved DB Instance Pricing") set forth on the Amazon RDS detail page on the AWS Site (each designated instance, a "Reserved DB Instance"). You may designate database instances as Reserved DB Instance by calling to the Purchasing API or selecting the Reserved DB Instance option in the AWS console. When you designate a database instance as a Reserved DB Instance, you must designate a region, instance type and quantity for the applicable Reserved DB Instances. The Reserved DB Instances may only be used in the designated region. We may change Reserved DB Instance Pricing at any time but price changes will not apply to previously designated Reserved DB Instances. We may terminate the Reserved DB Instance Pricing program at any time. Reserved DB Instances are nontransferable and all amounts paid in connection with the Reserved DB Instances are nonrefundable, except that if we terminate the Agreement other than for cause, terminate an individual Reserved DB Instance type, or terminate the Reserved DB Instance Pricing

program, we will refund you a pro rata portion of any up-front fee paid in connection with any previously designated Reserved DB Instances. Upon expiration or termination of the term of a Reserved DB Instance, the Reserved DB Instance Pricing will expire and standard on-demand usage prices will apply to the database instance. In addition to being subject to Reserved DB Instance Pricing, Reserved DB Instances are subject to all data transfer and other fees applicable under the Agreement.

…

27.4 You may only use Amazon VPC to connect your computing resources to the AWS GovCloud (US) region.

27.5 AWS Services may not be used to process or store classified data. If you or your end users introduce classified data into the AWS Network, you will be responsible for all sanitization costs incurred by AWS.

28. Amazon DynamoDB

28.1 You will be charged for the throughput capacity (reads and writes) you provision in your Amazon DynamoDB tables even if you do not fully utilize the provisioned capacity.

28.2 The actual reads and writes performance of your Amazon DynamoDB tables may vary and may be less than the throughput capacity that you provision.

29. AWS Storage Gateway

29.1 You may only use the AWS Storage Gateway on computer equipment owned or controlled by you for your internal business purposes, solely to access Your Content used in connection with the Services. Your use of the AWS Storage Gateway is governed by the AWS Storage Gateway License, located here: AWS Storage Gateway License Agreement

30. AWS Marketplace

30.1 The AWS Marketplace is a venue operated by AWS that allows Content to be offered, sold, and bought. Content may sold by AWS or a third party, and the party offering or selling the Content may specify separate terms and conditions and privacy policies for the use of the Content. If the Content is offered or sold by a third party, that party will be the seller of record for the Content. AWS is not a party to the terms with respect to Content offered or sold by third parties. Any Content of third parties offered through the AWS Marketplace constitutes "Third Party Content" under the Agreement. While AWS may help facilitate the resolution of disputes between you and third parties, AWS is not responsible for Third Party Content and has no control over and does not guarantee the quality, safety or legality of items advertised, the truth or accuracy of Third Party Content or listings, or the ability of sellers to offer the Content.

…

Δηλώνω ρητά ότι, σύμφωνα με το άρθρο 8 του Ν. 1599/1988 και τα άρθρα 2,4,6 παρ. 3 του Ν. 1256/1982, η παρούσα εργασία αποτελεί αποκλειστικά προϊόν προσωπικής εργασίας και δεν προσβάλλει κάθε μορφής πνευματικά δικαιώματα τρίτων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον