LSI SIN (10)02

Πηγή: Marko Hölbl

Cloud Computing- Θέματα Ασφαλείας και Προστασίας Δεδομένων

Η **CEPIS** (Council of European Professional Informatics Societies) είναι ένας μη κερδοσκοπικός οργανισμός που οι δράσεις του στοχεύουν στην προώθηση υψηλών κριτηρίων για τους επαγγελματίες της Πληροφορικής αναγνωρίζοντας τον κρίσιμο ρόλο που διαδραματίζουν στην κοινωνική και οικονομική πρόοδο. Η **CEPIS,** η οποία αντιπροσωπεύει 36 ενώσεις Επαγγελματιών Πληροφορικής και Τηλεπικοινωνιών από 33 Ευρωπαϊκές χώρες συμφώνησε στην παρακάτω έκθεση.

1.Ιστορικό

Το cloud computing δεν είναι και τόσο νέα έννοια ή καινοτομία στην Πληροφορική, αφού στην πραγματικότητα είναι μια πιο προχωρημένη έκδοση των Υπηρεσιών Επεξεργασίας Δεδομένων (Data Processing Service Bureaus) τις οποίες συναντήσαμε πριν 40 χρόνια. Ωστόσο, οι δημοφιλέστερες εταιρείες Πληροφορικής παρέχουν, ή θα παρεχουν υπηρεσίες Cloud σε μια μεγάλη γκάμα πελατών από μεμονωμένους πελάτες έως εταιρείες οποιουδήποτε μεγέθους. Οι μεγαλύτεροι και δημοφιλέστεροι πάροχοι νεφοϋπολογιστικής (Cloud Computing) περιλαμβάνουν τους Amazon με το EC2 [5], την Microsoft με το Azure [6] και την Google με τις εφαρμογές της (Gmail, Google Docs, Google Calendar) [7]. Το μοντέλο του Νέφους (Cloud) μπορεί να αναλυθεί με απλούς όρους ως η παροχή συγκεκριμένων υπηρεσίων πληροφορικής οι οποίες φιλοξενούνται στο Διαδίκτυο (Internet), από τις οποίες οι πιο γνωστές είναι η χρήση μιας Πλατφόρμας, μιας Υποδομής ή ενός Λογισμικού ως Υπηρεσία – πιο συγκεκριμένα οι υπηρεσίες: Platform as a Service (Paas), Infrastructure as a Service (Iaas) και Software as a Service (Saas).

Το Cloud Computing συχνά διαφημίζεται/ διατίθεται στην αγορά ως μια φθηνή και αποτελεσματική λύση η οποία θα αντικαταστήσει το μοντέλο του υπολογιστή διακομιστή-εξυπηρετητή (client/server). Η αλλαγή του μοντέλου

προς το νέφος (Cloud) επιφέρει την απώλεια του ελέγχου των δεδομένων και την ανάδειξη νέων προβλημάτων ασφάλειας και προστασίας των δεδομένων. Για αυτόν το λόγο οι επιχειρήσεις που θέλουν να εφαρμόσουν λύσεις Cloud Computing πρέπει να είναι πλήρως ενήμερες σχετικά με τους κινδύνους της. Το πρώτο μεγάλο θέμα σε σχέση με την προστασία και την ασφάλεια δεδομένων προέκυψε στα τέλη του 1960, όταν μια Σουηδική εταιρεία ανέθεσε την επεξεργασία των δεδομένων της σε ένα γραφείο παροχής υπηρεσιών στην Γερμανία ενώ η νομοθεσία προστασίας δεδομένων στις δύο αυτές χώρες ήταν διαφορετική.

Με το Cloud Computing να κερδίζει δημοτικότητα με ταχύτατους ρυθμούς, ο εντοπισμός των κινδύνων που προκύπτουν είναι πολύ σημαντικός. Επιπρόσθετα, τα θέματα ασφάλειας και προστασίας δεδομένων είναι μείζονος σημασίας και πρέπει να διευθετηθούν πριν η νεφοϋπολογιστική καταλάβει ένα μεγάλο μερίδιο της αγοράς. Πολλοί οργανισμοί Πληροφορικής καθώς και αρκετά ερευνητικά κέντρα είναι ενήμεροι αυτών των κινδύνων, έχοντας γράψει αρκετές προτάσεις για την διευθέτηση του προβλήματος [1], [2], [3], [4].

2.Ανησυχίες

Φαίνεται να μην υπάρχει κάποιο πεδίο στην Πληροφορική το οποίο να μην επηρεάζεται από το Cloud Computing. Τα δύο πιο σημαντικά προβλήματα που αφορούν τα θέματα προστασίας και ασφάλειας της νεφοϋπολογιστικής είναι:

1) Η απώλεια του ελέγχου στα δεδομένα και
2) Η εξάρτηση από τον πάροχο των υπηρεσιών Cloud Computing

Τα παραπάνω προβλήματα μπορούν να οδηγήσουν σε μια σειρά από νομικά προβλήματα καθώς και ζητήματα ασφαλείας που σχετίζονται με την υποδομή (infrastructure), την διαχείριση ταυτότητας (identity management), τον έλεγχο πρόσβασης, τη διαχείριση ρίσκου (risk management), την κανονιστική και νομοθετική συμμόρφωση στο νόμο (regulatory and legislative compliance, τον έλεγχο πρόσβασης και την καταγραφή (auditing and logging), τον έλεγχο ακεραιότητας (integrity control) όπως επίσης και τους κινδύνους που εξαρτώνται από τον συγκεκριμένο πάροχο υπηρεσειών νεφοϋπολογιστικής (Cloud).

Μερικά προβλήματα που σχετίζονται με την απώλεια ελέγχου των δεδομένων είναι:

1) Οι περισσότεροι πελάτες γνωρίζουν τους κινδύνους που σχετίζονται με την παραχώριση του ελέγχου και αποθήκευσης των δεδομενων τους σ’ έναν πάροχο υπηρεσιών νεφοϋολογιστικής (Cloud Computing Provider).Τα

δεδομένα μπορούν κάλλιστα να υποκλαπούν από τον Cloud Computing Provider όπως επίσης και από άλλες ανταγωνιστικές εταιρείες οι οποίες έχουν τον ίδιο πάροχο. Υπάρχει μια έλλειψη διαφάνειας (προς τον πελάτη) όσο αφορά τον τρόπο, τον χρόνο και τον τόπο διαχείρισης των δεδομένων. Αυτό αντιτίθεται στην απαίτηση προστασίας δεδομένων που συνιστά οι πελάτες να γνωρίζουν τι συμβαίνει με τα δεδομένα τους.

2)Τεχνικά, πολλοί πάροχοι υπηρεσιών νεφοϋολογιστικής είναι τεχνικά ικανοί μπορούν να κάνουν εξόρυξη δεδομένων (data mining) και να επεξεργαστούν και να αναλύσουν τα δεδομένα. Είναι μια πολύ λεπτή λειτουργία και ακόμα περισσότερο όταν οι χρήστες αποθηκεύουν και διαχειρίζονται τα δεδομένα αυτά μέσω υπηρεσιών νεφοϋπολογιστικής. Αυτό γίνεται πιο κατανοητό με τις εφαρμογές των μέσων κοινωνικής δικτύωσης (social media) όπου οι χρήστες ενθαρύνονται να δημοσιεύσουν στοιχεία της ιδιωτικής τους ζωής, όπως για παράδειγμα προσωπικές φωτογραφίες[1].

3) Οι φορητές συσκευές (mobile devices) και ειδικότερα ο περιορισμένος αποθηκευτικός χώρος και οι δυνατότητες που έχουν, οδηγούν στην ανάγκη χρησιμοποίησης υπηρεσιών που στηρίζονται στην νεφοϋπολογιστική και όχι στο λογισμικό (software) των Η/Υ. Ακόμη και όταν πρέπει να μεταφερθούν δεδομένα από μια φορητή συσκευή σε μια άλλη τοπική συσκευή, συχνά χρησιμοποιούνται εφαρμογές cloud όταν η συσκευή έχει τέτοιες δυνατότητες και υπηρεσίες..Ως εκ τούτου οι χρήστες βάζουν τον εαυτό τους σε κίνδυνο χωρίς να το συνειδητοποιήσουν αφού πιστεύουν ότι η μεταφορά των δεδομένων γίνεται τοπικά.

4) Από τη στιγμή που το Cloud είναι μια υπηρεσία, είναι προσβάσιμη εξ' αποστάσεως. Η σύνδεση μεταξύ του παρόχου υπηρεσειών νεφοϋολογιστικής και του πελάτη δεν προστατεύεται πάντα επαρκώς. Προκύπτουν κίνδυνοι ασφάλειας οι οποία απειλούν την μεταφορά των δεδομένων και μπορεί να περιέχουν υποκλοπές, πλαστογράφηση του DNS (DNS spoofing), καθώς και επιθέσεις Denial-of-Service.

5) Η στροφή προς τη νεφοϋπολογιστική (cloud computing) καθιστά τη χρήση των παραδοσιακών προσεγγίσεων διαχείρισης κινδύνων δύσκολη έως και αδύνατη. Ανεξάρτητα από το γεγονός ότι ο έλεγχος των δεδομένων μεταφέρεται στον πάροχο των υπηρεσιών νεφοϋολογιστικής, η διαχείριση των κινδύνων όπως επίσης και τα θέματα συμμόρφωσης καταμερίζονται μεταξύ του πελάτη, του πάροχου υπηρεσιών Διαδικτύου (ISP) και του πάροχου υπηρεσιών νεφοϋολογιστικής . Επιπρόσθετα, η συμμόρφωση με το νόμο είναι ένας πολύ σημαντικός παράγοντας μεταξύ του πελάτη και του παρόχου υπηρεσιών νεφοϋολογιστικής την ώρα που οι περισσότερες

[1] Περισσότερες πληροφορίες σε θέματα σχετικά με τις εφαρμογές των social media μπορείτε να βρείτε στο CEPIS statement για τα Social Networks-Problems of Security and Data Privacy[8].

ρυθμιστικές και νομοθετικές συμφωνίες είναι συνήθως προβληματικές. Τα data centres των υπηρεσιών cloud μπορούν να εξαπλωθούν γεωγραφικά. Επομένως η νομοθετική δικλείδα δεν έχει ακόμα αποσαφηνιστεί.

6) Αφού όλος ο τεχνικός έλεγχος ανατίθεται στον πάροχο υπηρεσιών νεφοϋολογιστική , οι πελάτες συχνά θέλουν να γίνεται εξωτερικός έλεγχος του παρόχου αυτού. Επομένως, οι πληροφορίες που σχετίζονται με τον έλεγχο πρόσβασης και την καταγραφή θα πρέπει να αποθηκευτούν και να προστατευτούν με απώτερο σκοπό να επαληθευτούν. Η κατάλληλη καταγραφή μπορεί να παρέχει την δυνατότητα για επιστημονική εξερεύνηση σε περίπτωση κάποιου απρόοπτου.

7) Υπάρχουν ανησυχίες που σχετίζονται με τη διαγραφή των δεδομένων καθώξείναι δύσκολο να διαγράψεις όλα τα ηλεκτρονικά αντίγραφα μιας πληροφορίας/ενός δεδομένου αφού δε μπορείς να τα βρεις όλα. Είναι αδύνατον να εγγυηθείς την πλήρη διαγραφή όλων των δεδομένων. Ώς αποτέλεσμα, είναι πολύ δύσκολο να επιβάλλεις την υποχρεωτική διαγραφή των δεδομένων. Ωστόσο, η υποχρεωτική διαγραφή δεδομένων πρέπει να συμπεριληφθεί στον προκείμενο κανονισμό των υπηρεσιών νεφοϋπολογιστικής, αλλά ακόμα δεν μπορούμε να στηριχθούμε σε αυτόν: αν υπήρξε ποτέ εποχή με "Εγγυημένη συνολική διαγραφή δεδομένων", έχει πια περάσει. Αυτη η παράμετρος θα πρέπει να λαμβάνεται υπόψη πολύ σοβαρά, όταν τα δεδομένα συλλέγονται και αποθηκεύονται.

8. Η προστασία δεδομένων και η νομοθεσία περι ιδιωτικότητας δεν είναι παρόμοιες στις περισσότερες χώρες του κόσμου ενώ η νεφοϋπολογιστική είναι η παγκόσμια υπηρεσία του μέλλοντος. Συνεπώς προβλήματα και κίνδυνοι οι οποίοι επηρεάζουν τους κανόνες προστασίας των δεδομένων πρέπει να ληφθούν σοβαρά υπόψη όταν οι πλατφόρμες των υπηρεσιών νεφοϋπολογιστικής βρίσκονται σε διακομιστές (servers) εκτός των Ευρωπαϊκών χωρών.

9. Η νεφοϋπολογιστική εξαρτάται από την έμπιστη και ασφαλή χρήση του τηλεπικοινωνιακού δικτύου το οποίο διασφαλίζει και εγγυάται την διεκπεραίωση των τερματικών χρηστών από τις παρεχόμενες υπηρεσίες του cloud από τον πάροχο των υπηρεσιών cloud. Οι τηλεπικοινωνιακοί πάροχοι συχνά διαφέρουν από τους παρόχους υπηρεσιών cloud.

Τυπικά ζητήματα σχετικά με την εξάρτηση στον πάροχο υπηρεσιών νεφοϋπολογιστικής συμπεριλαμβάνουν:

1) Μια μεγάλη ανησυχία σχετικά με τον βαθμό εξάρτησης ενός συγκεκριμένου παρόχου υπηρεσιών νεφοϋπολογιστικής είναι η διαθεσιμότητα. Αν ο πάροχος οδεύει προς την «χρεωκοπία» και σταματήσει να παρέχει υπηρεσίες, ο πελάτης, μπορεί να αντιμετωπίσει προβλήματα

πρόσβασης στα δεδομένα του και ως εκ τούτου και στην συνέχεια του κύκλου εργασιών της επιχείρησης.

2) Μερικές διαδεδομένες εφαρμογές νεφοϋπολογιστικών υπηρεσιών (όπως το Google Docs) δεν συμπεριλαμβάνουν κάποιο συμφωνητικό, ή σύμβαση ανάμεσα στον πελάτη και τον πάροχο. Ως αποτέλεσμα ο πελάτης δεν έχει κανένα αποδεικτικό στην περίπτωση πιθανού προβλήματος.

3) Οι υπηρεσίες νεφοϋπολογιστικής είναι υπηρεσίες παρόμοιες με άλλες παραδοσιακές υπηρεσίες και εφαρμογές (π.χ τηλεπικοινωνίες,τραπεζικές συναλλαγές ηλεκτρικό ρεύμα, νερό κ.λ.π). Και οι παραδοσιακές αλλά και οι υπηρεσίες νεφοϋπολογιστικής είναι υπηρεσίες οι οποίες παρέχονται από μεγάλους πάροχους και «φιλοξενούν» μικρούς πελάτες. Επομένως οι πελάτες εξαρτώνται συχνά από του παρόχους επειδή είναι δύσκολο να αλλάξουν πάροχο εάν η αλλαγή αυτή είναι εφικτή. Ως συνέπεια οι παραδοσιακές υπηρεσίες ρυθμίζονται συχνά αναφορικά με την έκταση των λειτουργιών όπως η τιμολόγηση, η αξιοπιστία του πάροχου κ.λ.π

Το Cloud ενισχύει την τάση ότι η ασφάλεια στην Πληροφορική δεν είναι ένα καθαρά τεχνικό ζήτημα αλλά ένα ζήτημα μεταξύ ατόμων και οργανισμών και για αυτό τον λόγο περιλαμβάνει πολλές ανθρώπινες και οργανωτικές προοπτικές όπως τη διαχείριση, τα συμφωνητικά και τη νομική προστασία.

3.Προτάσεις/Συστάσεις

Συγκεκριμένα, θα πρέπει να εξεταστούν τα παρακάτω σημεία:

1) Η διαχείριση του ρίσκου και οι νομικές δικλείδες πρέπει να αποσαφηνιστούν ξεκάθαρα μεταξύ του παρόχου και του πελάτη με τρόπο διαφανή και σε σχέση με την αποθήκευση και την πρόσβαση των δεδομένων (πχ. η φυσική θέση αποθήκευσης των δεδομένων). Με αυτό τον τρόπο μπορούν να αναπτυχθούν σχέσεις εμπιστοσύνης μεταξύ των δύο πλευρών.

2) Η παρεχόμενη υπηρεσία πρέπει να είναι συμβατή με την κανονιστική ρύθμιση και την νομοθεσία που ο πελάτης χρειάζεται να ακολουθήσει ενώ επίσης και ο πελάτης πρέπει να έχει την δυνατότητα να συμμορφώνεται με αυτήν.

3. Τα προβλήματα και οι κίνδυνοι τα οποία επηρεάζουν την ασφάλεια των δεδομένων στην Ευρώπη θα πρέπει να λαμβάνονται υπόψιν κατάλληλα όταν ο πάροχος των υπηρεσιών νεφοϋπολογιστικής βρίσκεται εκτός Ευρώπης.

4. Η επικοινωνία μεταξύ του πελάτη και του πάροχου πρέπει να προστατεύεται κατάλληλα και να διασφαλίζει την εμπιστοσύνη, την ακεραιότητα, τον πιστοποιημένο έλεγχο και να ελαχιστοποιεί το ρίσκο των επιθέσων denial-of-service. Ένας σαφής προσδιορισμός των μέτρων που πρέπει να ληφθούν για την ασφάλεια της επικοινωνίας είναι απαραίτητο να

υιοθετείται από τον πάροχο και να βασίζεται σε ανοιχτά και διαφανή πρότυπα (standards) και τεχνολογίες.

5) Οι πάροχοι θα πρέπει να είναι υποχρεωμένοι να διασφαλίζουν την εμπιστευτικότητα των δεδομένων.

6) Η υποχρεωτική διαγραφή των δεδομένων πρέπει να συμπεριληφθεί στην επικείμενη νομοθετική ρύθμιση σχετικά με τις υπηρεσίες νεφοϋπολογιστικής αλλά δεν πρέπει να βασιζόμαστε σ' αυτήν σε μεγάλο βαθμό.

7) Το γεγονός ότι δεν υπάρχει κάποια εγγυημένη διαγραφή δεδομένων πρέπει να ληφθεί σοβαρά υπόψη στην περίπτωση που τα δεδομένα συλλέγονται και αποθηκεύονται.

8) Με σκοπό τη διασφάλιση της διαθεσιμότητας των δεδομένων, οι πελάτες πρέπει να κρατούν τοπικά αντίγραφα ασφαλείας.

9) Πρέπει να ενθαρρυνθεί η ανάπτυξη και η καλύτερη προώθηση του λογισμικού που επιτρέπει την τοπική μεταφορά δεδομένων μεταξύ συσκευών.

10) Το τηλεπικοινωνιακό δίκτυο το οποίο υποστηρίζει τις υπηρεσίες νεφοϋπολογιστικής πρέπει να προστατεύεται ενάντια σε ιούς και σε επιθέσεις DoS (Denial of Service).

11) Πρέπει να παρέχεται κατάλληλη καταγραφή και έλεγχος πρόσβασης των δεδομένων. Ένας εξωτερικός έλεγχος μπορεί να είναι ευεργετικός για την φήμη των παρόχων νεφοϋπολογιστικής όπως επίσης και για την ενδυνάμωση της εμπιστοσύνης με τον πελάτη.

12) Οι απλοί χρήστες πρέπει να εκπαιδεύονται με βάση το νέο μοντέλο. Η εκπαίδευση πρέπει να τους προετοιμάζει να παίρνουν πιο αρμόδιες αποφάσεις στο τρόπο που χρησιμοποιούν τις υπηρεσίες νεφοϋπολογιστικής καθώς και τις πληροφορίες που πρέπει να μεταφερθούν στο Νέφος και κάτω από συγκεκριμένες συνθήκες.

13) Οι επαγγελματίες πρέπει να αναπτύσσουν τις δεξιότητες τους στη διαχείριση νέων ειδών κινδύνων.

14) Με τη λογική ότι κάποιος κανονισμός θα χρειαστεί στο μέλλον, π.χ η εξισορρόπηση της δύναμης μεταξύ πελατών και παρόχων υπηρεσιών νεφοϋπολογιστικής,θα ήταν συνετό να αναλογιστούμε τις αδυναμίες και τα θέματα πριν η νεφοϋπολογιστική γίνει μια κρίσιμη υπηρεσία ή υποδομή. Χρειάζεται να εξεταστεί ποιες από τις διαστάσεις των συγκρούσεων και των ρυθμιστικών προοπτικών είναι σχετικές (για παράδειγμα η εγγύηση και η αξιοπιστία σε συνδυασμό με την εμπιστεύτικότητα και την ακεραιότητα των δεδομένων). Πιο συγκεκριμένα όταν ο πάροχος υπηρεσιών νεφοϋπολογιστικής αποτελεί τμήμα μιας σημαντικής υποδομής πληροφοριών

κρίνονται απαραίτητοι μερικοί κανονισμοί ή περιορισμοί σχετικά με την πιθανή εξαγορά του από κάποιον τρίτο ή ανταγωνιστή.

15) Η έρευνα σε βασικές αρχές στην Πληροφορική, στην ασφάλεια, στην ιδιωτικότητα και στις συνέπειες σχετικά με τη νεφοϋπολογιστική πρέπει να ενθαρύννεται. Επίσης ζητήματα σχετικά με το πιθανό αποτέλεσμα των υπηρεσιών νεφοϋπολογιστικής στην επαλήθευση των πιστοποιητικών των εφαρμογών καθώς και την καταλληλότητα τους πρέπει να διευρενηθούν περαιτέρω.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] J. Brodkin, Gartner: Seven cloud-computing security risks, available at: www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853.

[2] Cloud Computing Security Considerations, A Microsoft Perspective, Microsoft Whitepaper, 2010, available at: www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=3269a73d-9a74-4cbf-aa6c-11fbafdb8257.

[3] Cloud Computing: Benefits, Risks and Recommendations for Information Security, ENISA Report, 2009, available at: www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.

[4] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, Cloud Security Alliance (CSA) Report, 2009, available at: www.cloudsecurityalliance.org/csaguide.pdf.

[5] Amazon Elastic Compute Cloud (Amazon EC2), http://aws.amazon.com/ec2/.

[6] Windows Azure platform, www.microsoft.com/windowsazure/.

[7] Google Apps, www.google.com/apps/

[8] CEPIS Statement, Social Networks – Problems of Security and Data Privacy, 2008, www.cepis.org/index.jsp?p=942&n=963#Social%20Networks