Cloud Computing και Ζητήματα Προστασίας Προσωπικών Δεδομένων

Λ. Μήτρου, Αναπληρώτρια Καθηγήτρια
Πανεπιστήμιο Αιγαίου

Περί τίνος πρόκειται …

Κατά NIST πρόκειται για ένα μοντέλο που ενεργοποιεί

- **ευχερή, σύμφωνα με τη ζήτηση, διαδικτυακή πρόσβαση**
- **σε ένα διαμοιραζόμενο χώρο από κατάλληλα διαμορφωμένους υπολογιστικούς πόρους, οι οποίοι μπορούν να κλιμακώνονται, δηλαδή να δεσμεύονται και να απελευθερώνονται,**
- **προκειμένου να συμβάλλουν στην ομαλή λειτουργία του συστήματος**
- **απαιτώντας ελάχιστη διαχειριστική προσπάθεια ή την παρέμβαση του παρόχου του υπολογιστικού νέφους**

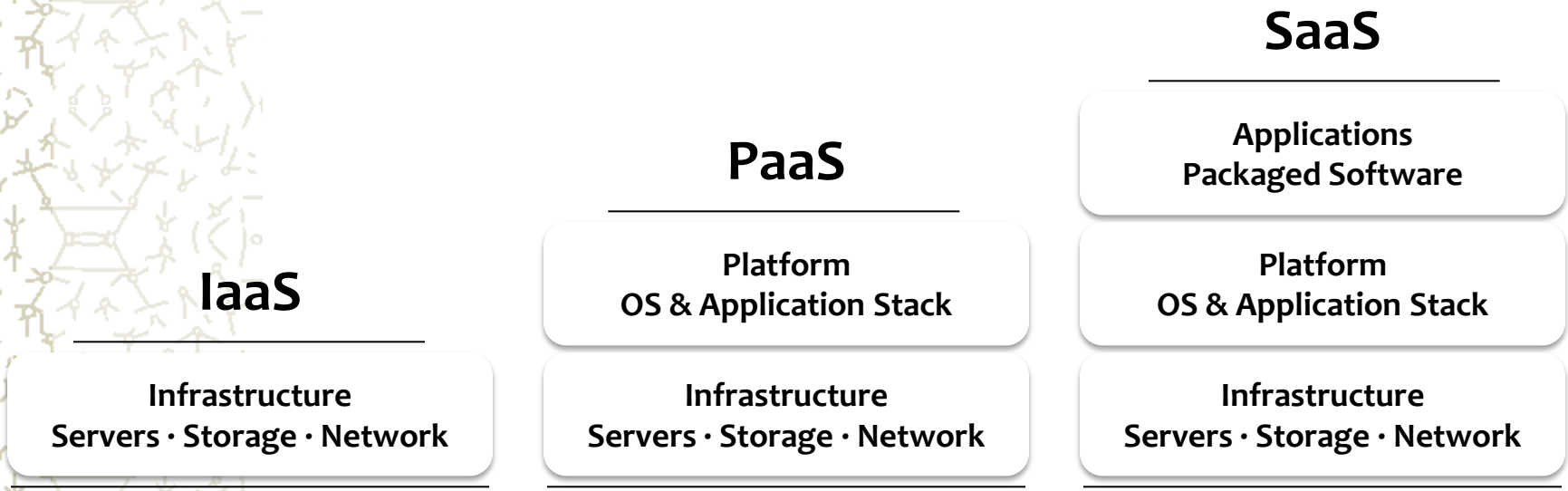
(NIST)

δηλαδή....

- *Ένα μοντέλο που καθιστά εφικτή την άνετη, ανεξάρτητη από τόπο (δηλ. από παντού) και σύμφωνα με τη ζήτηση δικτυακή πρόσβαση σε ένα κοινό σύνολο παραμετροποιήσιμων υπολογιστικών πόρων (π.χ. δίκτυα, διακομιστές, αποθηκευτικά μέσα, εφαρμογές και υπηρεσίες)*
- *Αποθήκευση, επεξεργασία και χρήση δεδομένων σε απομακρυσμένους υπολογιστές που είναι προσβάσιμοι μέσω του διαδικτύου.*

3 μοντέλα παροχής υπηρεσιών

- **Infrastructure as a Service – IaaS :** χώρο στον εξυπηρετητή / στο κέντρο δεδομένων ή εξοπλισμό δικτύου)
- **Platform as a Service – PaaS:** παροχή εργαλείων από την Υποδομή ως υπηρεσία (IaaS) για την κατασκευή και τη φιλοξενία εξατομικευμένων εφαρμογών)
- **Software as a Service – SaaS:** μοντέλο παροχής λογισμικού



4 μοντέλα ανάπτυξης

- Δημόσιο νέφος (Public Cloud)
  - Ευρύ κοινό
- Ιδιωτικό νέφος (Private Cloud)
  - Ένας οργανισμός/ περισσότεροι πελάτες
- Κοινοτικό νέφος (Community Cloud)
  - Κοινότητα πελατών
- Υβριδικό νέφος (Hybrid Cloud)

Κίνδυνοι για την ιδιωτικότητα

- Η τεχνολογία του υπολογιστικού νέφους επαναπροσδιορίζει πώς, πού και από ποιον (μπορούν να) συλλέγονται, διαβιβάζονται και χρησιμοποιούνται τα δεδομένα
- (Εξ ορισμού;) συσσώρευση μεγάλου όγκου προσωπικών δεδομένων
- …ζήτημα όταν συνοδεύεται από την εμπορευματοποίηση προσωπικών δεδομένων

Απώλεια ελέγχου;

- των δεδομένων – πρόσβαση / ανάκτηση με τη σύμπραξη του παρόχου
- των πρακτικών διαχείρισης / επεξεργασίας των δεδομένων εκ μέρους του παρόχου
- του «τόπου» τήρησης ….

- Διατήρηση / Ανάκτηση ελέγχου – κρίσιμο ζήτημα

Το ζήτημα του «τόπου»

- Πολλαπλές θέσεις κέντρων δεδομένων: εγγενές χαρακτηριστικό του υπολογιστικού νέφους
- ….κι εγγενές ζήτημα
  - κέντρα δεδομένων εγκατεστημένα και κατανεμημένα σε πολλαπλές δικαιοδοσίες
    - Νομιμοτητα-διαδικασία διασυνοριακών ροών δεδομένων
    - Εφαρμοστέο δίκαιο;

Οι ιδιαιτερότητες του νέφους

- Διαφορές σε σχέση με την «κλασική» εξωτερική ανάθεση (outsourcing): επίπεδα ευελιξίας/ βαθμός εξατομίκευσης συμβατικών όρων – τυποποιημένες συμβατικές ρήτρες – πολλαπλοί (κι άγνωστοι;) τόποι
- Ανάθεση ευθύνης στον πάροχο υπολογιστικού νέφους για διαθεσιμότητα, ακεραιότητα, απόρρητο, διαφάνεια - απομόνωση -μη συνδεσιμότητα και δυνατότητα παρέμβασης

Πολλαπλοί παράγοντες – αδιευκρίνιστοι ρόλοι;

- Πολλαπλοί και διαφορετικοί ρόλοι στην αλυσίδα του υπολογιστικού νέφους: πάροχοι υπηρεσιών και πλατφορμών, προμηθευτές λογισμικού και εξοπλισμού, πάροχοι υπηρεσιών τηλεπικοινωνιών, διαμεσολαβητές και χρήστες
- Αναγκαιότητα προσδιορισμού και αποσαφήνισης, μέσω κανονιστικού πλαισίου ή/και συμβατικής ρύθμισης, του ρόλου κάθε παράγοντα, προκειμένου να θεσπιστούν οι υποχρεώσεις, οι αρμοδιότητες, η λογοδοσία και η ευθύνη

Το ζήτημα της εμπιστοσύνης

- Αλυσίδα εμπιστοσύνης…
- Οι πάροχοι υπηρεσιών νέφους πρέπει
  - να δημιουργούν εμπιστοσύνη και
  - να βοηθούν τους πελάτες να διασφαλίζουν αλλά και
  - να βεβαιώνονται ότι συμμορφώνονται με την ισχύουσα νομοθεσία
- Ικανότητα συμμόρφωσης : αποφασιστική παράμετρος κατά την επιλογή παρόχου υπηρεσιών νέφους

Οι απαιτήσεις της εμπιστοσύνης

- Πεποίθηση ότι άνθρωποι, δεδομένα, οντότητες, πληροφορίες και διεργασίες θα συμπεριφερθούν ή/και αντίστοιχα θα λειτουργήσουν σύμφωνα με τις νομικές απαιτήσεις/ συμφωνίες
- Ασφάλεια των δεδομένων και η συμμόρφωση με τους κανόνες και τις αρχές προστασίας των δεδομένων
- Προαπαιτούμενα: Ύπαρξη σαφήνειας και ασφάλειας δικαίου ως προς το ισχύον δίκαιο, την κατανομή ρόλων και αρμοδιοτήτων, τα μέτρα ασφάλειας και το καθεστώς των διασυνοριακών διαβιβάσεων δεδομένων

Ποιος είναι ο Υπεύθυνος επεξεργασίας;

- Ο προσδιορισμός σκοπού/μέσων επεξεργασίας και η λήψη μέτρων ασφαλείας βαρύνουν τον υπεύθυνο επεξεργασίας, ο οποίος λογοδοτεί και (ενδέχεται να) ευθύνεται για τη (μη) συμμόρφωση
- Δυσεφάρμοστες έννοιες στις υπηρεσίες υπολογιστικού νέφους καθώς οι αρμοδιότητες και οι ρόλοι κατανέμονται, επιμερίζονται και μετατοπίζονται και τα δεδομένα προσωπικού χαρακτήρα μετακινούνται, αναδιοργανώνονται και επαναχρησιμοποιούνται συνεχώς

Και ποιος ο εκτελών;

- Οι πάροχοι υπηρεσιών νέφους μπορεί να μην γνωρίζουν καθόλου τη λειτουργία των προγραμμάτων που διαχειρίζονται ή το περιεχόμενο των δεδομένων που επεξεργάζονται οι πελάτες τους
- Πάροχοι υπηρεσιών νέφους (υλισμικού, πλατφόρμας ή λογισμικού) ως εκτελούντες την επεξεργασία
- …ακόμη και αν καθορίζουν υπό μία έννοια «τρόπο/ μέσα επεξεργασίας», όπως π.χ. το υλικό, χωρίς ωστόσο να καταλήγουν να θεωρούνται «υπεύθυνοι επεξεργασίας»
- Υπεύθυνοι μόνο εφόσον επεξεργάζονται δεδομένα για ίδιους σκοπούς

Νομικές απαιτήσεις

- Αρχή προσδιορισμού / περιορισμού σκοπού: Απαγόρευση χρήσης δεδομένων για άλλους (ίδιους) σκοπούς
  - Διαφήμιση/ κέρδος με βάση δεδομένα πελατών
- Οργάνωση της πρόσβασης με τρόπο ώστε να προστατεύεται η εμπιστευτικότητα (λογικός διαχωρισμός δεδομένων διάφορων πελατών)
- Διαγραφή – «επιστροφή» δεδομένων

Δυνατότητα παρέμβασης και διαφάνεια

- Διασφάλιση της δυνατότητας παρέμβασης,όπως π.χ. η δυνατότητα άσκησης των δικαιωμάτων πρόσβασης, διόρθωσης, διαγραφής, δέσμευσης και αντίταξης
- Διαφάνεια έναντι του πελάτη αναφορικά με μέτρα ασφάλειας/συμβάντα παραβίασης/ συνέπειες επεξεργασίας / Εμπλοκή «υπεργολάβων»/ τόπο τήρησης δεδομένων

Το ζήτημα των «υπεργολάβων»

- Η αλυσιδωτή επεξεργασία/ αποθήκευση μπορεί να περιλαμβάνει πολλαπλούς/ περισσότερους υπεργολάβους
- Πολυδιάσπαση επεξεργασίας/ ευθύνης
- Υποχρέωση ενημέρωσης (κι έγκρισης) του πελάτη υπηρεσιών νέφους για τους υπεργολάβους εκτελούντες την επεξεργασία

Το ζήτημα του «τόπου»

- Διαβίβαση και αποθήκευση δεδομένων σε εξυπηρετητές/κέντρα δεδομένων που συχνά
  - βρίσκονται εκτός της επικράτειας του πελάτη υπηρεσιών νέφους,
  - χωρίς αυτός να γνωρίζει τον ακριβή τόπο των παρεχόμενων πόρων
- Η έλλειψη ενός/ σταθερού τόπου ως εγγενές χαρακτηριστικό του υπολογιστικού νέφους
- Ενημέρωση του πελάτη…

Διασυνοριακά νέφη

- Ικανοποιητικό επίπεδο προστασίας/ safe harbour principles
- Παρεκκλίσεις (συναίνεση, σύμβαση κ.α.)
- Επαρκείς εγγυήσεις
  - Πρότυπες συμβατικές ρήτρες (Standard Contractual Clauses)
    - (EU Model clauses - 2010/87/EU)
  - Δεσμευτικοί εταιρικοί κανόνες (Binding Corporate Rules)
  - 2012 - Πλαίσιο για την έγκριση δεσμευτικών εταιρικών κανόνων
  - Εφόσον υπάρχει εναρμόνιση με πρότυπες ρήτρες 2010/87/EU δεν απαιτείται άδεια ΑΠΔΠΧ

Ποιο δίκαιο εφαρμόζεται;

- Η δικαιοδοσία δεν εξαρτάται ούτε από τον τόπο στον οποίο βρίσκονται υλικά τα δεδομένα ούτε από την ιθαγένεια ή τον τόπο κατοικίας των προσώπων, στα οποία αναφέρονται τα δεδομένα
- Κριτήρια
  - Εγκατάσταση σε χώρα ΕΕ
  - Χρήση εξοπλισμού σε ΕΕ
  - Αποφασιστικής σημασίας ο τόπος εγκατάστασης των κέντρων δεδομένων

Νέφος κι επιβολή του νόμου/1

- Ζητήματα αναφορικά με την πρόσβαση αρχών επιβολής του νόμου (διωκτικές, ανακριτικές αρχές) σε δεδομένα αποθηκευμένα σε περιβάλλοντα υπολογιστικού νέφους
- Ζητήματα ως προς τις ψηφιακές αποδείξεις: κεντρική αποθήκευση, διαμοιρασμένη χρήση, υψηλή μεταβλητότητα, δυσδιάκριτα όρια προσωπικής – εταιρικής χρήσης

Νέφος κι επιβολή του νόμου/2

- Ανησυχίες σε σχέση με την προστασία και την επιβολή των κανόνων προστασίας των δεδομένων ιδίως εκτός της δικαιοδοσίας της ΕΕ
- Υποχρέωση ανταπόκρισης στα αιτήματα πρόσβασης
- Ενημέρωση του πελάτη υπηρεσιών νέφους;

Ειδικά νομικά «εμπόδια»

- Ειδικές απαιτήσεις ως προς την επεξεργασία / ασφάλεια δεδομένων
  - Π.χ. ευαίσθητα δεδομένα
  - Ζητήματα εθνικής ασφάλειας
  - Εκ του νόμου απαιτήσεις ως προς τον τόπο τήρησης/ απαιτήσεις ασφάλειας
  - Απαιτήσεις αλλά και «δυσκαμψία» δημόσιου τομέα

Συμπερασματικές σκέψεις

- Η προσαρμογή του κανονιστικού πλαισίου και η σαφήνεια των κανόνων είναι καθοριστικής σημασίας ώστε να καθοριστούν επακριβώς οι απαιτήσεις, οι υποχρεώσεις και τα δικαιώματα παρόχων και πελατών υπηρεσιών νέφους σε σχέση με την αποθήκευση και την επεξεργασία δεδομένων
- Οι συμβάσεις υπολογιστικού νέφους με σύννομες και θεμιτές ρήτρες και η βεβαιότητα ως προς τη συμμόρφωση του παρόχου υπηρεσιών νέφους με τις νομικές απαιτήσεις προστασίας /ασφάλειας μπορούν να διευκολύνουν την οικοδόμηση της αναγκαίας εμπιστοσύνης

,

Σας ευχαριστώ

για την προσοχή

και την υπομονή σας