ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

UNIVERSITY OF PIRAEUS

Ιδιωτικότητα στη Νεφοϋπολογιστική

Μαυρίδης Δ. Κλαυδιανός Γ. Ραυτόπουλος Χ. Αλεστάς Β. Κατσιάνος Ε. Φούγιας Β. Γεωργίου Μ.

SCROLL DOWN

Εισαγωγή στη Νεφοϋπολογιστική

01

« Ως υπολογιστικό νέφος ορίζεται το μοντέλο το οποίο επιτρέπει τη συνεχή δικτυακή πρόσβαση σε ένα μεγάλο εύρος διαμοιραζόμενων και έτοιμων προς ρύθμιση υπολογιστικών πηγών (πχ δικτυακές συσκευές, servers, αποθηκευτικά μέσα) οι οποίες μπορούν να διατεθούν άμεσα και με ελάχιστο χρόνο διαχείρισης (ανθρωποώρα) ή διεπαφής με τον πάροχο»

NIST (National Institute of Standards and Technology)

Ο «παλιός» στην ασφάλεια

Σύντομη ιστορία του νέφους

Ιστορική αναδρομή

Το 1997 ο καθηγητής Ramnath Chelappa σε έρευνα του, όρισε το υπολογιστικό νέφος ως ένα υπολογιστικό παράδειγμα του οποίου τα όρια θα ορίζονται οικονομικούς όρους και όχι από τεχνικούς περιορισμούς. Για την εποχή, ο ορισμός αυτός θεωρούταν ριζοσπαστικός

1960 -1970

1960’s

Το 1960, το ARPANET με υπεύθυνο έρευνας τον J.C. Licklider βοήθησε σημαντικά στην εφεύρεση του παγκόσμιου ιστού ο οποίος με τη σειρά του έθεσε τους θεμέλιες λίθους για την δημιουργία παροχών ψηφιακών υπηρεσιών, ανάμεσα τους και το cloud. Πάραυτα, η έννοια «Υπολογιστικό νέφος – cloud computing» δεν αναφέρθηκε πριν το 1997

1970’s

1990’s

Το 1999 η εταιρεία salesforce, διέθεσε στην αγορά ένα λογισμικό CRM (Software As a Service) το οποίο διασφάλιζε το πελατολόγιο. Η επένδυση της εταιρείας αντιμετώπισε προβλήματα καθώς μετά το 2001 η μείωση των τιμών στο Hardware οδήγησε πολλούς οργανισμούς να επενδύσουν σε δικές τους εγκαταστάσεις

Σύντομη ιστορία του νέφους

Ιστορική αναδρομή

2000's

Το 2002 η Amazon έθεσε σε παραγωγή την πρώτη υπηρεσία νέφους η οποία παρείχε και αποθηκευτικές λύσεις

Το 2006 η Amazon έθεσε σε παραγωγή την υπηρεσία νέφους με όνομα Elastic Compute Cloud EC2 όπου διέθετε στους χρήστες εικονικές μηχανές.

2010's

Το 2008 η Google εισέρχεται στο χώρο του υπολογιστικού νέφους διαθέτοντας υπηρεσίες για προγραμματιστές.

Το 2009 ακολουθεί η Microsoft, δίνοντας στη δημοσιότητα το Azure

2010's

Το 2010 η Apple ενημερώνει τους χρήστες της για για μια νέα υπηρεσία συγχρονισμού αρχείου το iCloud

Το 2011 η IBM δημιουργεί την λύση για επιχειρήσεις με την επωνυμία SmartCloud

Το 2012 γίνεται διαθέσιμο στο ευρύ κοινό για πρώτη φορά με δωρεάν πρόσβαση το DropBox το οποίο και μέσα στα πρώτα χρόνια καταφέρνει να συλλέξει 100 εκατομμύρια χρήστες

2013

Η κρίσιμη στιγμή στην πορεία της ιστορίας φτάνει το 2013, με την διαρροή δεδομένων από τον Edward Snowden σχετικά με τακτικές της NSA για πρόσβαση σε διασυνδεδεμένα υπολογιστικά συστήματα, όπου και ξεκινούν να εγείρονται ερωτήματα περί ασφάλειας πληροφοριών και ρίσκου για τα δεδομένα στο νέφος.

“ Τι στο καλό έχει συμβεί με το cloud !“

Δυστυχώς, οι εταιρείες συχνά δεν έχουν προχωρήσει σε ανάλυση ρίσκου και του κινδύνου που εγκυμονούν οι εφαρμογές νέφους, καταλήγοντας να μεταφέρουν προβληματικά συστήματα τα οποία βρίσκονται εσωτερικά, σε ένα περιβάλλον προσβάσιμο σε όλο τον κόσμο.

Ελαστικότητα:

Οι υπηρεσίες μπορούν να κλιμακωθούν επάνω ή κάτω ανάλογα με τις ανάγκες, προσφέροντας πόρους "κατά παραγγελία ".

Αυτόματη Διαχείριση:

Η αναβάθμιση λογισμικού, η ασφάλεια δικτύου και άλλες διαχειριστικές λειτουργίες γίνονται αυτόματα από τον πάροχο

Μοντέλα Υπηρεσιών:

Περιλαμβάνει την υποδομή ως υπηρεσία (IaaS), την πλατφόρμα ως υπηρεσία (PaaS) και το λογισμικό ως υπηρεσία (SaaS).

Αρχιτεκτονική (Υπηρεσίες) του Νέφους

1

IaaS

Ο πελάτης έχει πλήρη πρόσβαση σε δικτυακές παραμετροποιήσεις όσο και σε επίπεδο λειτουργικού συστήματος. Ο πάροχος και πάλι ευθύνεται για την διαρκή ενημέρωση του πυρήνα του λογισμικού και του hypervisor όπως και για το υλισμικό του τεχνικού εξοπλισμού

2

SaaS

ενοικίαση μονάχα του λογισμικού δίχως να απαιτείται η διαδικασία εγκατάστασης κάποιου επιπλέον λογισμικού από την πλευρά του πελάτη. Δίνει την ευχέρεια στο χρήση να έχει πλήρη πρόσβαση μέσω φιλομετριτή από όπου και αν βρίσκεται

3

PaaS

Ο πάροχος είναι υπεύθυνος για τις ενημερώσεις και έλεγχο του λειτουργικού.
Το μοντέλο αυτό είναι το πιο κοινό
το χρησιμοποιούν εκατοντάδες επιχειρήσεις για να μεταπωλήσουν τις υπηρεσίες τους. Οι επιχειρήσεις που χρησιμοποιούν το μοντέλο αυτό αναπτύσσοντας δικές του υπηρεσίες θα πρέπει να λαμβάνουν υπόψιν τους τις ανάγκες δεδομένων τις οποίες ο πάροχος τους απαιτεί ώστε μαζί με τις δικές τους να ενημερώνουν πλήρως τον τελικό χρήστη

Μοντέλα του Νέφους

1

Δημόσιο Νέφος (Public Cloud):

Οι υποδομές και οι υπηρεσίες παρέχονται από τρίτους παρόχους και διατίθενται στο κοινό μέσω του διαδικτύου.

Παράδειγμα: Amazon Web Services (AWS) Microsoft Azure, Google Cloud Platform.

2

Ιδιωτικό Νέφος (Private Cloud):

Οι υποδομές και οι υπηρεσίες χρησιμοποιούνται αποκλειστικά από έναν οργανισμό.

Μπορεί να βρίσκεται εντός των εγκαταστάσεων του οργανισμού ή να φιλοξενείται από τρίτο πάροχο.

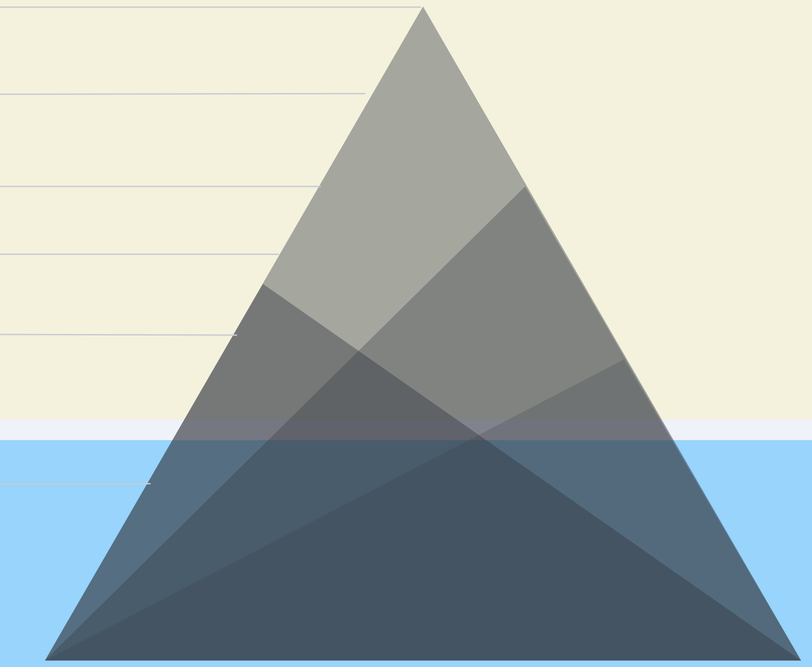
3

Υβριδικό Νέφος (Hybrid Cloud):

Συνδυασμός δημόσιων και ιδιωτικών νέφων, επιτρέποντας τη μεταφορά δεδομένων και εφαρμογών μεταξύ τους.

Παρέχει τη δυνατότητα χρήσης των πλεονεκτημάτων και των δύο μοντέλων.

Μεγάλο κόστος κτήσης ή νέφος ;!



Τι πραγματικά διαχειριζόμαστε

IaaS – Managed by us

On premises

Pay for licenses, maintenance, electricity, FTEs, Real Estate

Networking Hardware

Τι διαχειρίζεται ο πάροχος

Provider pay for the cost of facility

Γιατί όλοι ξεκινούν από το νέφος; Γιατί 30% Συνολικό κέρδος από το Κόστος κτήσης

Αφορά άσκηση κτήσης IaaS έναντι data center.

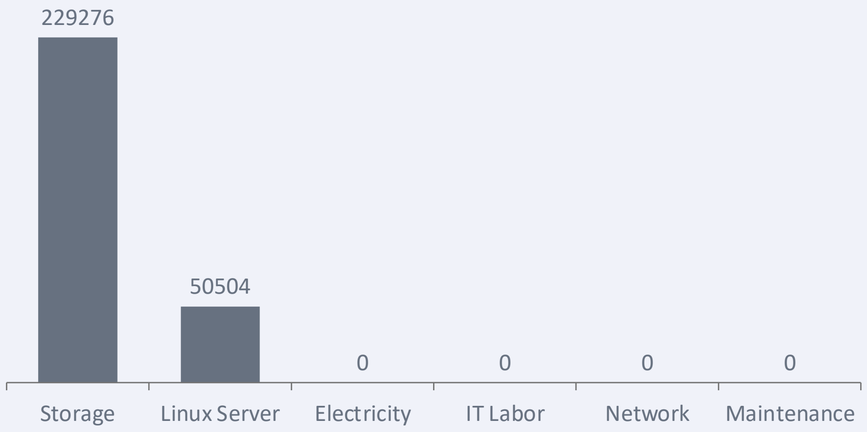
***Οι τιμές αφορούν πραγματική άσκηση – Q3 2022**

CLOUD MIGRATION

Operational efficiencies and lower TCO

0% Upfront Charges

279,780$ Per Month

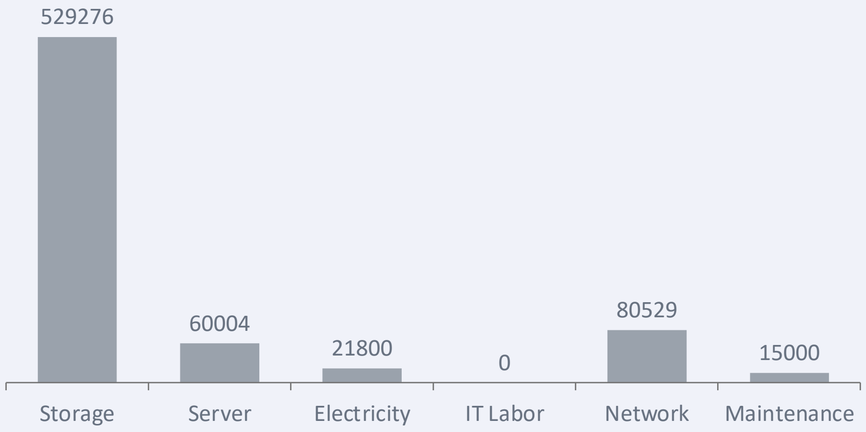


ON-PREMISES

Estimates using Amazon and our current data for expanding our current Data Center.

80% Upfront Charges

706,600$ Per Month

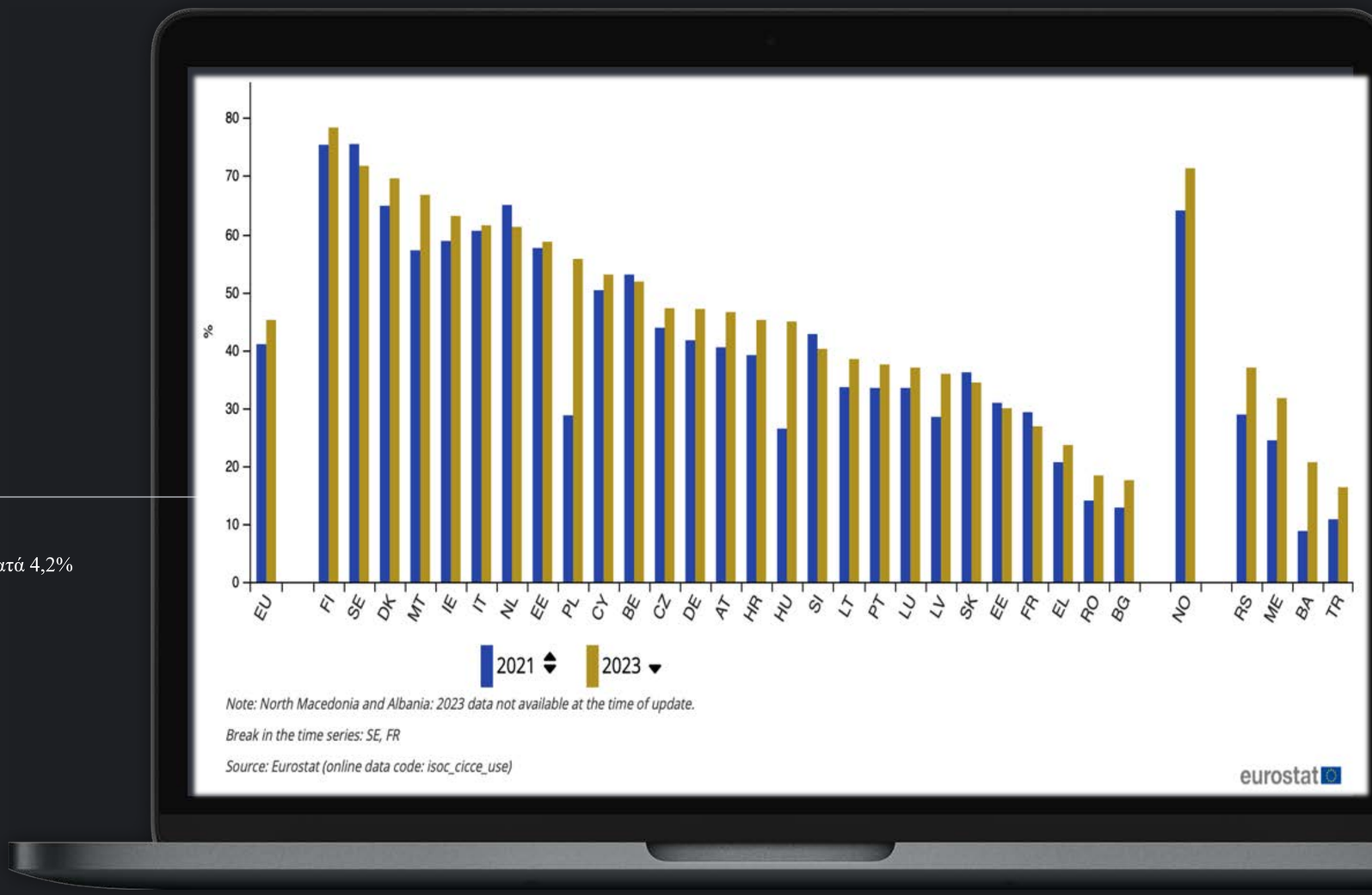


https://calculator.aws/#/estimate?id=3892b7b044c39fc4e42190459729c375a9259436

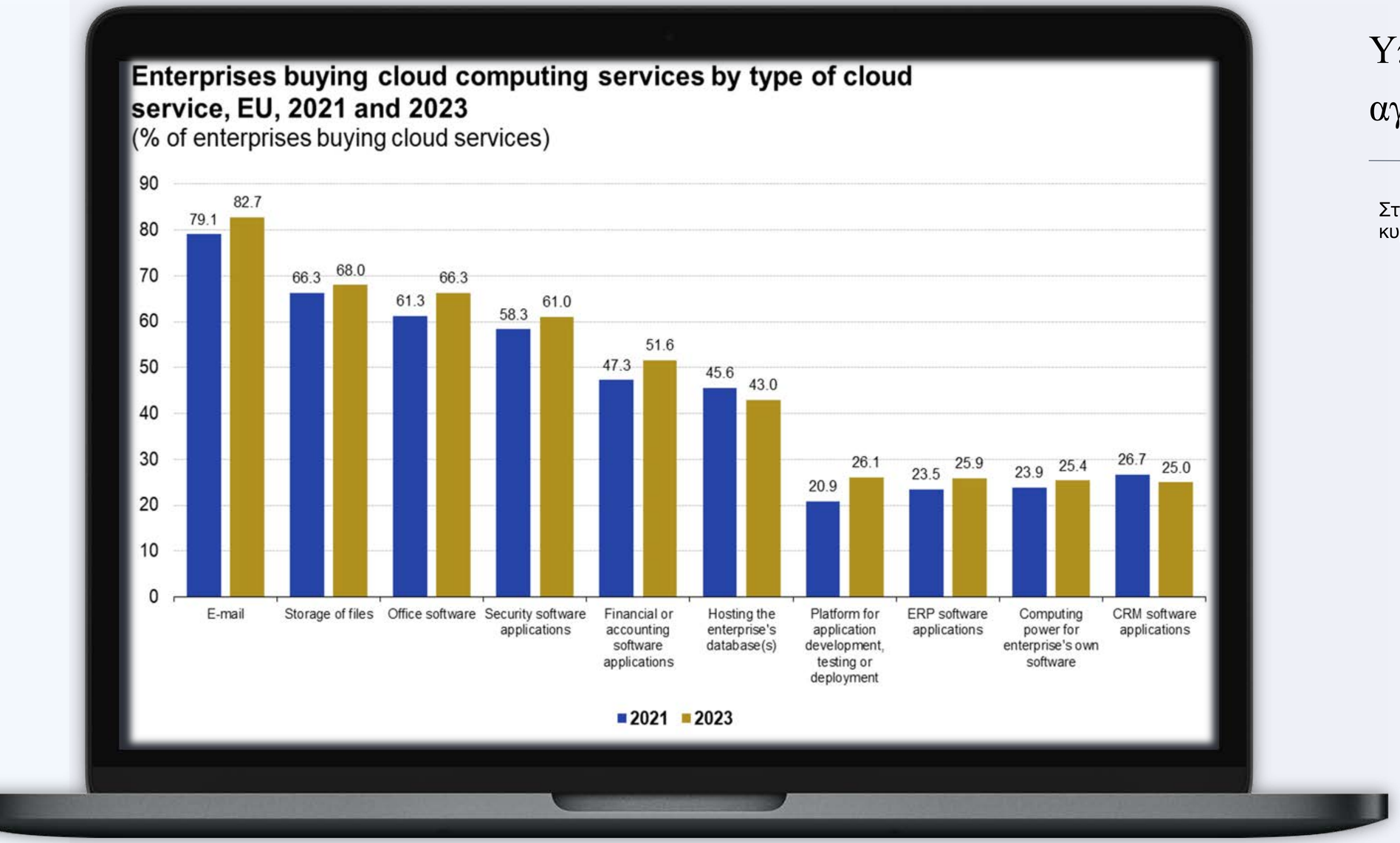
Χρήση του υπολογιστικού νέφους στην Ευρωπαϊκή Ένωση

4,2%

το 2023 παρατηρήθηκε αύξηση κατά 4,2% στη χρήση υπηρεσιών cloud



οι επιχειρήσεις στην Ευρωπαϊκή Ένωση φαίνεται να προτιμούν τις υπηρεσίες cloud – Νέφους αντί της επένδυσης σε δικές τους υποδομές.



Υπηρεσίες νέφους που αγοράζονται στην ΕΕ.

Στην Τρίτη θέση οι υπηρεσίες κυβερνοασφάλειας

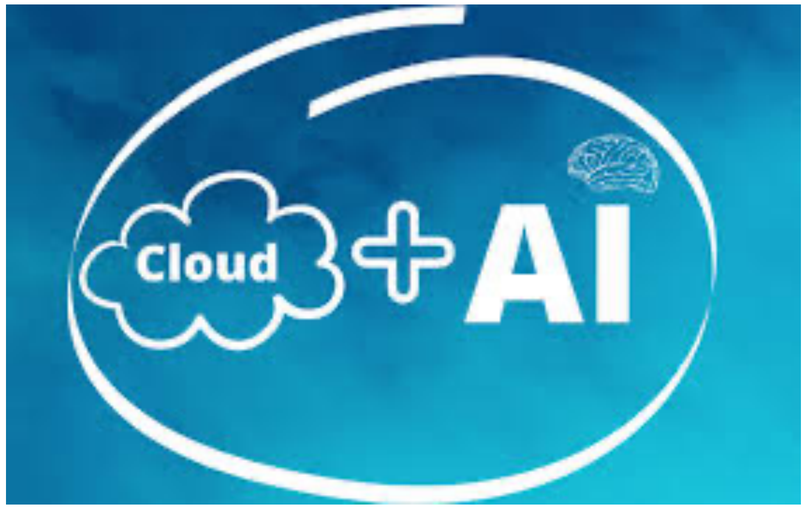
Τεχνητή Νοημοσύνη στη Νεφοϋπολογιστική

02

Εισαγωγή στην Τεχνητή Νοημοσύνη στο Cloud Computing

Η Τεχνητή Νοημοσύνη στο cloud computing αναφέρεται στην ενσωμάτωση των δυνατοτήτων της σε υποδομές βασισμένες στο cloud, προκειμένου να βελτιωθεί η απόδοση, η ασφάλεια και η διαχειριστική αποτελεσματικότητα των υπηρεσιών cloud.

- **Καινοτομία και Τεχνολογική Εξέλιξη:** Συμβάλλει στην ανάπτυξη νέων τεχνολογιών όπως το Internet of Things (IoT), τα software defined δίκτυα (SDN) και πρωτοπόρες τεχνολογίες όπως το 6G και το Open RAN, που ωθούν την εποχή της καινοτομίας.
- **Αποδοτικότητα και Λειτουργικότητα:** Η Τεχνητή Νοημοσύνη ενισχύει τις δυνατότητες ανάλυσης και διαχείρισης δεδομένων στα cloud συστήματα, βελτιώνοντας σημαντικά το scalability και την αξιοπιστία των υπηρεσιών.
- **Έξυπνες Λειτουργίες:** Η AI επιτρέπει στα μηχανήματα και τα συστήματα να λειτουργούν με προηγμένες γνωστικές δυνατότητες, προσφέροντας λύσεις που προσαρμόζονται δυναμικά στις ανάγκες των χρηστών.



Μία Αμφίδρομη Σχέση

Η αλληλεπίδραση του AI με το cloud οδηγεί σε μια αμφίδρομη σχέση όπου κάθε τεχνολογία ενισχύει την άλλη, ανοίγοντας νέες δυνατότητες για καινοτομία και βελτίωση στον τομέα της πληροφορικής και τηλεπικοινωνιών.

Το Cloud μας επιτρέπει να χρησιμοποιούμε το AI πιο αποδοτικά

Το AI επιτρέπει βελτιώσεις σε εφαρμογές που παρέχονται από cloud υποδομές

Βασικές εφαρμογές του AI στο Cloud

1. **Εκπαίδευση και Βελτιστοποίηση Μοντέλων AI:** Η εκπαίδευση και βελτιστοποίηση μοντέλων AI σε cloud περιβάλλοντα επιτρέπει την ταχεία επεξεργασία και ανάλυση μεγάλων δεδομένων, βελτιώνοντας την ακρίβεια και την αποδοτικότητα των αλγορίθμων.

2. **Cognitive Computing:** Το Cognitive Computing χρησιμοποιεί την AI για να μιμείται τις ανθρώπινες νοητικές διεργασίες, παρέχοντας προηγμένες λύσεις σε τομείς όπως η υγεία και οι χρηματοοικονομικές υπηρεσίες.

3. **Βελτιστοποίηση Πόρων:** Το AI βοηθά στη βελτιστοποίηση των υπολογιστικών πόρων σε cloud περιβάλλοντα, επιτρέποντας αποδοτικότερη διαχείριση και μείωση του κόστους λειτουργίας.

4. **AI as a Service:** Οι υπηρεσίες AI as a Service προσφέρουν πρόσβαση σε προηγμένα εργαλεία AI μέσω του cloud, επιτρέποντας στις επιχειρήσεις να εκμεταλλευτούν την τεχνολογία χωρίς σημαντικές επενδύσεις σε υποδομές.

5. **Business Intelligence:** Το AI ενισχύει τα εργαλεία Business Intelligence, παρέχοντας αναλύσεις και προβλέψεις που βοηθούν τις επιχειρήσεις να λαμβάνουν καλύτερες και στρατηγικά τεκμηριωμένες αποφάσεις.

6. **Internet of Things:** Οι αρχιτεκτονικές cloud ενισχύουν τις λύσεις IoT, διευκολύνοντας την αποθήκευση και ανάλυση δεδομένων από συνδεδεμένες συσκευές, επιτρέποντας τη δημιουργία πιο έξυπνων και αποδοτικών συστημάτων.

Πλεονεκτήματα του AI στο Cloud

1

Εξοικονόμηση Κόστους

Η χρήση του cloud μειώνει σημαντικά τα έξοδα που συνδέονται με την ανάπτυξη μοντέλων μηχανικής μάθησης, τα οποία παραδοσιακά απαιτούσαν εκτεταμένες υλικές υποδομές.

2

Αυξημένη Παραγωγικότητα

Το AI απλοποιεί τη ρύθμιση και τη διαχείριση των cloud περιβαλλόντων, μειώνοντας το διοικητικό βάρος και επιτρέποντας στο προσωπικό IT να επικεντρωθεί στην καινοτομία.

3

Αυτοματοποίηση

Η ενσωμάτωση του AI στις cloud υποδομές βοηθά στην αυτοματοποίηση των καθημερινών διαδικασιών, βελτιώνοντας την επιχειρησιακή απόδοση και αξιοπιστία των συστημάτων.

4

Ανάλυση και Διαχείριση Δεδομένων

Τα εργαλεία AI επεξεργάζονται και αναλύουν δεδομένα σε πραγματικό χρόνο, παρέχοντας πολύτιμες πληροφορίες και βελτιώνοντας τις υπηρεσίες σε διάφορες εφαρμογές όπως η υποστήριξη πελατών, το μάρκετινγκ και η διαχείριση της αλυσίδας εφοδιασμού..

5

Επεκτασιμότητα

Τα cloud περιβάλλοντα επιτρέπουν την εύκολη κλιμάκωση των πόρων AI ανάλογα με τις απαιτήσεις, διευκολύνοντας τη διαχείριση των πόρων.

Ζητήματα Ιδιωτικότητας με τη Χρήση του AI στο Cloud Computing

Παρά τα πολυάριθμα οφέλη του AI στο cloud computing, εισάγονται επίσης σημαντικοί κίνδυνοι για την Ιδιωτικότητα που πρέπει να διαχειριστούν προσεκτικά.

- **Έκθεση Ευαίσθητων Δεδομένων:** Η διαχείριση δεδομένων που περιλαμβάνουν προσωπικές πληροφορίες αυξάνει τους κινδύνους παραβίασης ιδιωτικότητας
- **Κίνδυνοι Ασφάλειας και Εμπιστευτικότητας:** Το AI μπορεί ακούσια να παρακάμψει μέτρα ασφαλείας κατά την προσπάθεια βελτιστοποίησης της απόδοσης.
- **Προβλήματα με τη Συμμόρφωση σε Κανονισμούς Ιδιωτικότητας:** Το AI μπορεί να βοηθήσει στη συμμόρφωση με κανονιστικές απαιτήσεις αυτοματοποιώντας τις διαδικασίες διαχείρισης και προστασίας δεδομένων

Σημασία της Ιδιωτικότητας στη Νεφοϋπολογιστική

03

Κατηγορίες δεδομένων

Η προστασία των προσωπικών δεδομένων αφορά τη διαφύλαξη ευαίσθητων πληροφοριών που σχετίζονται με άτομα, θεσμούς και οργανισμούς κατά τη διάρκεια ολόκληρου του κύκλου ζωής τους.

Η αποτελεσματική διαχείριση της ιδιωτικότητας των δεδομένων απαιτεί να κατηγοριοποιούνται τα συλλεγμένα δεδομένα σε τέσσερις διακριτές ομάδες:

- **Αναγνωριστικά (Identifiers):** Άμεσα και μοναδικά αναγνωριστικά όπως ονόματα και αριθμοί ασφαλείας κοινωνικής ασφάλισης που μπορούν να εντοπίσουν ατομικές ταυτότητες.
- **Πάρα-αναγνωριστικά (Quasi-identifiers):** Έμμεσα αναγνωριστικά όπως ηλικία, φύλο ή ταχυδρομικός κωδικός, τα οποία μπορούν να αναγνωρίσουν πιθανώς άτομα όταν συνδυάζονται με άλλα δεδομένα.
- **Ευαίσθητα χαρακτηριστικά (Sensitive attributes):** Ιδιωτικά δεδομένα όπως καταστάσεις υγείας ή οικονομικές πληροφορίες που είναι κρίσιμα για την ατομική ιδιωτικότητα.
- **Μη ευαίσθητα χαρακτηριστικά (Insensitive attributes):** Γενικά δεδομένα που δεν απειλούν την αναγνώριση ατόμων, όπως στατιστικά σύνολα ή ανωνυμοποιημένα δεδομένα.

Ιδιωτικότητα δεδομένων

1

Πρόσβαση στα δεδομένα:

Στο πλαίσιο του cloud computing, η εξασφάλιση της πρόσβασης των ατόμων στα δεδομένα τους και η τήρηση αιτημάτων όπως η διαγραφή δεδομένων παρουσιάζει προκλήσεις.

2

Ταυτοποίησης χρηστών:

Οι πάροχοι cloud πρέπει να διασφαλίσουν την αποτελεσματική ταυτοποίηση των χρηστών για να αποτρέψουν την πρόσβαση στα δεδομένα από μη εξουσιοδοτημένα άτομα.

3

Μηχανισμοί ασφαλείας:

Η χρήση μηχανισμών ασφαλείας για την προστασία και την αποφυγή διαρροής δεδομένων αποτελεί μεγάλη πρόκληση για τους cloud παρόχους.

Συμμόρφωση με τους κανόνες ιδιωτικότητας

Η συμμόρφωση με τους κανόνες ιδιωτικότητας στο cloud είναι η τήρηση των νόμων, κανονισμών και προτύπων που διέπουν τη συλλογή, αποθήκευση και διαχείριση προσωπικών δεδομένων σε περιβάλλοντα υπολογιστικού νέφους.

- **Εγκαταστάσεις υποδομών cloud:** Σε πολλές περιπτώσεις οι υποδομές ενός παρόχου cloud εκτείνονται σε πολλαπλές δικαιοδοσίες, δυσκολεύοντας τις προσπάθειες συμμόρφωσης με τους κανόνες ιδιωτικότητας.
- **Μεταφορά δεδομένων:** Η τοποθεσία και οι πρακτικές αποθήκευσης δεδομένων στο cloud δημιουργούν ανησυχίες για την ιδιωτικότητα, ειδικά όταν τα δεδομένα μπορεί να μεταφερθούν σε διάφορες χώρες ή να αναμιγνύονται με πληροφορίες από άλλους οργανισμούς.
- **Διαφορετικοί κανονισμοί:** Για παράδειγμα, ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) στην Ευρωπαϊκή Ένωση επιβάλλει αυστηρές απαιτήσεις για την επεξεργασία και μεταφορά προσωπικών δεδομένων, δημιουργώντας προκλήσεις για παγκόσμιους οργανισμούς που χρησιμοποιούν υπηρεσίες cloud.

Διαχείριση δεδομένων

1

Πλήρης καταστροφή δεδομένων:

Η διασφάλιση της πλήρους καταστροφής των δεδομένων αποτελεί θέμα ζωτικής σημασίας, ιδίως σε περιπτώσεις που εμπλέκονται ευαίσθητα δεδομένα.

2

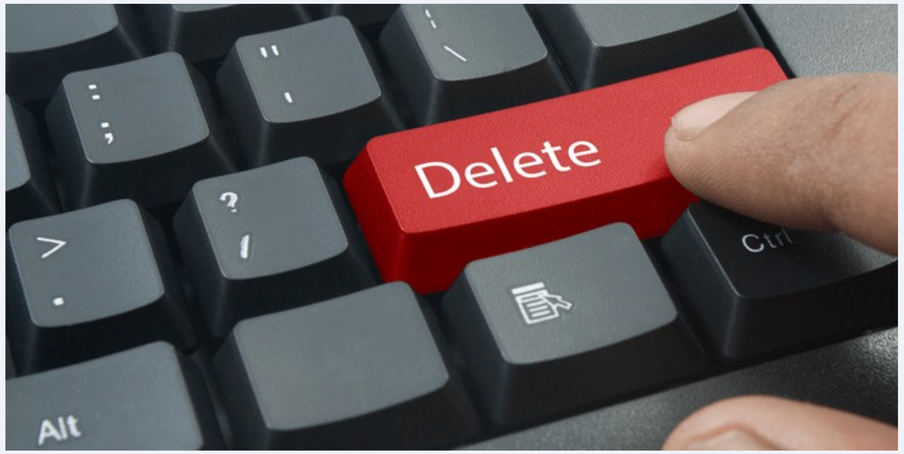
Μεταφορά Δεδομένων:

Η μετάβαση της κατοχής και του ελέγχου δεδομένων μεταξύ οργανισμών και CSP απαιτεί σαφείς συμβατικές συμφωνίες και μηχανισμούς επικοινωνίας.

3

Διατήρηση δεδομένων:

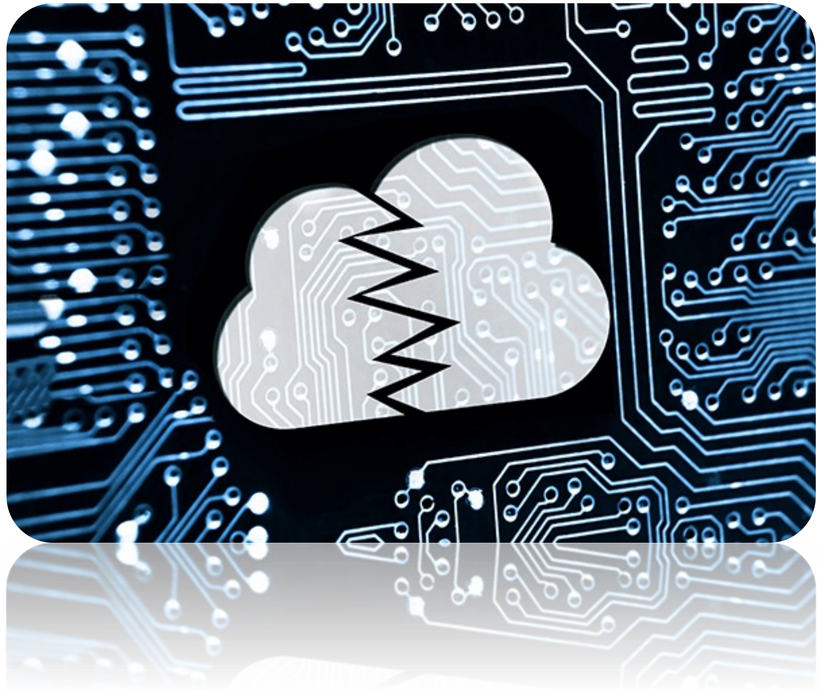
Οι οργανισμοί πρέπει να διευκρινίσουν τις πολιτικές διατήρησης δεδομένων, να διασφαλίσουν τη συμμόρφωση με τις νομικές απαιτήσεις και να αντιμετωπίσουν εξαιρέσεις.



Παραβιάσεις ιδιωτικότητας

Παραβίαση ιδιωτικότητας στο cloud προκύπτει σε περιπτώσεις όπου ευαίσθητες ή προσωπικές πληροφορίες ενός χρήστη εκτίθενται, αποκτώνται ή χρησιμοποιούνται χωρίς εξουσιοδότηση.

- **Ανίχνευση και διαχείρηση παραβιάσεων:** Χρήση κατάλληλων μηχανισμών ελέγχου πρόσβασης και ασφάλειας από τους παρόχους για να αποτρέψουν μη εξουσιοδοτημένα άτομα να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα.
- **Ανάθεση ευθυνών:** Οι συμβάσεις με τους CSP πρέπει να καθορίζουν την ευθύνη για τις παραβιάσεις και να θεσπίζουν διαδικασίες για την επιβολή των συμβατικών υποχρεώσεων σε περίπτωση παραβίασης.
- **Αντιμετώπιση παραβιάσεων:** Εφαρμογή σχεδίων αντίδρασης σε περίπτωση παραβίασης. Εφαρμογή τακτικών αξιολογήσεων ασφάλειας για την μείωση των επιπτώσεων των παραβιάσεων ιδιωτικότητας και την προστασία των δεδομένων που αποθηκεύονται στο cloud.



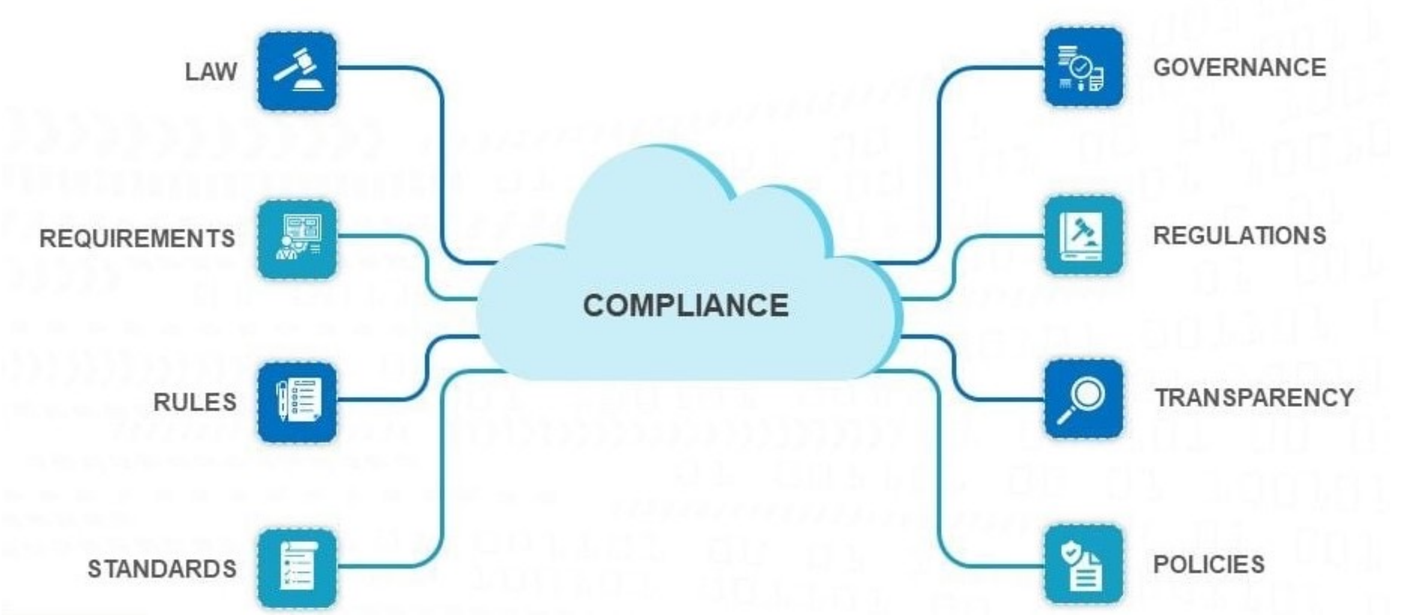
Προτυποποίηση και Συμμόρφωση

04

Προτυποποίηση και Συμμόρφωση

Διασφαλίζει ότι η χρήση Cloud Υπηρεσιών ευθυγραμμίζεται με πρότυπα και πλαίσια

- ρυθμιστικά
- νομικά
- κανονιστικά



Προτυποποίηση και Συμμόρφωση

- Ενισχυμένη προστασία δεδομένων
- Υιοθέτηση Βέλτιστων Πρακτικών
- Εμπιστοσύνη Χρηστών
- Διαχείριση Ρίσκων και περιστατικών ιδιωτικότητας και ασφάλειας
- Ανταγωνισμός

- Νομικές κυρώσεις και πρόστιμα
- Παραβιάσεις δεδομένων και περιστατικά ασφαλείας
- Ζημία στην Φήμη
- Δυσπιστία από το κοινό
- Απώλεια Επιχειρηματικών Ευκαιριών

Προτυποποίηση και Συμμόρφωση

Με την άνοδο των υπηρεσιών cloud, προέκυψε και η επιτακτική ανάγκη συμμόρφωσης με τον εν λόγω πλαίσιο. Αυτά τα πρότυπα, σχεδιάζονται από

- ✓ κυβερνητικούς φορείς
- ✓ ιδιωτικούς φορείς
- ✓ Εντός Οργανισμών και Εταιρειών

Διασφαλίζουν ότι τα δεδομένα που αποθηκεύονται και διαχειρίζονται στο νέφος προστατεύονται και χρησιμοποιούνται
Υπεύθυνα.

General Data Protection Regulation (GDPR)

Health Insurance Portability and Accountability Act (HIPAA)

Payment Card Industry Data Security Standard (PCI DSS)

National Institute of Standards and Technology (NIST)

ISO/IEC 27001, 27002, 27017 και 27018

Cloud Controls Matrix (CCM)

Νομικό και Κανονιστικό Πλαίσιο

Νομικό και Κανονιστικό Πλαίσιο

- **Τεκμηρίωση Νομικής Βάσης Επεξεργασίας**: Για την επεξεργασία δεδομένων, απαιτείται η τήρηση μιας Νομικής βάσης κατά την οποία θα υλοποιείται η επεξεργασία των δεδομένων.
- **Διαδικασίες άσκησης δικαιωμάτων φυσικών προσώπων**: Πρέπει να υπάρχουν διαδικασίες και μηχανισμοί άσκησης των δικαιωμάτων των φυσικών προσώπων οποιαδήποτε στιγμή το αιτηθούν.
- **Λογοδοσία και επαρκής τεκμηρίωση**: Απαιτείται αυστηρή τεκμηρίωση για την εφαρμογή του κανονισμού συμπεριλαμβανομένων DPIAs (Data Protection Impact Assessments), Αρχείο Επεξεργασίας Δεδομένων και Ανάθεση DPO (Data Protection Officer)
- **Επικοινωνία Παραβιάσεων Ιδιωτικότητας**: Απαιτείται η άμεση ενημέρωση των Αρμόδιων Αρχών και των φυσικών προσώπων, σε περίπτωση παραβίασης (ή εν δυνάμει Παραβίασης) προσωπικών δεδομένων
- **Εφαρμογή τεχνικών μέτρων:** Υλοποίηση τεχνικών μέτρων και λύσεων για την προστασία των δεδομένων κατά την τήρηση, αποστολή και επεξεργασία δεδομένων.

Νομικό και Κανονιστικό Πλαίσιο

Health Insurance Portability and Accountability Act (HIPAA)

- **Κρυπτογράφηση δεδομένων**: Το HIPAA απαιτεί ότι κάθε PHI που είναι αποθηκευμένο στο cloud πρέπει να είναι κρυπτογραφημένο τόσο κατά τη μεταφορά όσο και σε κατάσταση ηρεμίας.
- **Έλεγχοι πρόσβασης**: Πρέπει να υπάρχουν ισχυροί μηχανισμοί ελέγχου πρόσβασης για να διασφαλίζεται ότι μόνο εξουσιοδοτημένα άτομα μπορούν να έχουν πρόσβαση στο PHI.
- **Συμφωνία Επιχειρηματικού Συνεργάτη** (BAA): Οι πάροχοι υπηρεσιών Cloud πρέπει να υπογράψουν BAA με την καλυπτόμενη οντότητα. Αυτή η συμφωνία ορίζει ότι ο πάροχος θα προστατεύει κατάλληλα την PHI και θα συμμορφώνεται με τις απαιτήσεις HIPAA.
- **Δημιουργία αντιγράφων ασφαλείας και ανάκτηση δεδομένων**: Πρέπει να υπάρχουν ασφαλείς διαδικασίες δημιουργίας αντιγράφων ασφαλείας και ανάκτησης για το PHI που είναι αποθηκευμένες στο cloud για την αποφυγή απώλειας δεδομένων σε περίπτωση καταστροφής ή καταστροφής δεδομένων.
- **Διαχείριση και αξιολόγηση κινδύνου**: Πρέπει να διενεργούνται τακτικές αξιολογήσεις κινδύνου για τον εντοπισμό πιθανών τρωτών σημείων στο περιβάλλον cloud. Πρέπει να ληφθούν μέτρα για τον μετριασμό των εντοπισμένων κινδύνων για την PHI.

Λοιπά Κανονιστικά Πλαίσια

GLBA (Gramm-Leach-Bliley Act)

CCPA (California Consumer Protection Act)

COPPA (Children's Online Privacy Protection Act)

DORA (Digital Operational Resilience Act)

POPI (Protection of Personal Information)

Cybersecurity Law of the People's Republic of China

Προτυποποίηση του νέφους

ISO/IEC 27001, 27002, 27017 και 27018

- **ISO 27017:2015 - Ασφάλεια Πληροφοριών στο Cloud**: Παρέχει πλαίσιο ασφαλείας για οργανισμούς που χρησιμοποιούν υπηρεσίες νέφους. Εντείνει την προσοχή στην ανάλυση και τον διαχωρισμό των ευθυνών στις Cloud Υπηρεσίες

- **ISO 27018:2019 - Προστασία Προσωπικών Δεδομένων στο Cloud**: Περιγράφει αρχές για τη διασφάλιση των προσωπικών δεδομένων σε δημόσια cloud περιβάλλοντα, παρέχοντας μέτρα ελέγχου και κατευθυντήριες γραμμές για την ασφάλεια των δεδομένων.

Προτυποποίηση του νέφους

ISO/IEC 27001, 27002, 27017 και 27018

- **ISO 27018:2019 - Προστασία Προσωπικών Δεδομένων στο Cloud**: Συγκεκριμένα, αναλύει τις απαιτήσεις για:
  - Εφαρμογή μέσων κρυπτογράφησης των δεδομένων
  - Ασφαλή πρόσβαση και διαγραφή δεδομένων
  - Ανάλυση σκοπών επεξεργασίας
  - Κανάλια επικοινωνίας για άσκηση δικαιωμάτων ως προς τα δεδομένα
  - Διαχείριση Προσβάσεων

Προτυποποίηση του νέφους

National Institute of Standards and Technology (NIST)

Όμοια με το ISO, παρουσιάζει κατευθυντήριες γραμμές για την υλοποίηση μέτρων που αφορούν την ασφάλεια πληροφοριών και ανά περίπτωση εμβαθύνει περισσότερο σε ζητήματα προστασίας της Ιδιωτικότητας. Πιο συγκεκριμένα:

- **NIST 800-122** - «Οδηγίες για την προστασία της εμπιστευτικότητας των προσωπικών δεδομένων
- **NIST Special Publication 800-53** - "Έλεγχοι ασφάλειας και προστασίας της ιδιωτικής ζωής για ομοσπονδιακά συστήματα και οργανισμούς πληροφοριών

Προτυποποίηση του νέφους

National Institute of Standards and Technology (NIST) - **NIST Special Publication 800-144**

NIST Special Publication 800-144 - «Κατευθυντήριες γραμμές για την ασφάλεια και την ιδιωτικότητα στο δημόσιο υπολογιστικό νέφος»

- **Οδηγίες Χειρισμού Δεδομένων**: Συνιστά προσεκτική εξέταση των απαιτήσεων χειρισμού δεδομένων πριν από την υιοθέτηση λύσεων νέφους.
- **Αξιολόγηση Τρίτων**: Η δημοσίευση υπογραμμίζει τη σημασία της αξιολόγησης των συστημάτων και των υπηρεσιών τρίτων σε περιβάλλοντα νέφους.
- **Ευθύνη και Μοντέλα Ανάπτυξης**: Συνιστά τον διαχωρισμό των ευθυνών και την κατανόηση του Μοντέλου κοινής ευθύνης (Shared Responsibility Model)
- **Αξιολόγηση Κινδύνου και Συμμόρφωση**: Η δημοσίευση ενθαρρύνει τους οργανισμούς να διενεργούν λεπτομερείς αξιολογήσεις κινδύνου πριν από την υιοθέτηση λύσεων νέφους.
- **Συνεχής Παρακολούθηση και Αξιολόγηση**: Το NIST 800-144 υπογραμμίζει τη συνεχή παρακολούθηση και αξιολόγηση των υπηρεσιών νέφου.

Προτυποποίηση του νέφους

Cloud Security Alliance - Cloud Control Matrix (CCM)

- Συμβάλλει στην αξιολόγηση κινδύνων που σχετίζονται με τα υπολογιστικά νέφη και στην λήψη αντιμέτρων
- Παρέχει πλήρη χαρτογράφηση με τα μέτρα λοιπών προτύπων ασφάλειας (Βλ. ISO, NIST κλπ.)
- Περιλαμβάνει εκτεταμένες απαιτήσεις όσον αφορά στην διαχείριση κρυπτογραφικών κλειδιών, της εφοδιαστικής αλυσίδας και την διαχείριση
- Ενσωματώνει απαιτήσεις του GDPR όπως η DPIA και το αρχείο δραστηριοτήτων

Προτυποποίηση του νέφους

Payment Card Industry Data Security Standard (PCI DSS)

- **Διαχείριση Δικτύου**: Εφαρμογή ισχυρών μέτρων ελέγχου πρόσβασης και χρήση Firewalls για την προστασία των δεδομένων κατόχου κάρτας σε περιβάλλοντα cloud.
- **Παρακολούθηση και καταγραφή**: Τήρηση καταγραφών και παρακολούθηση όλων των προσβάσεων σε πόρους δικτύου και δεδομένα κατόχων κάρτας. ,
- **Τήρηση και διαγραφή δεδομένων:** Καταγραφή πολιτικών και διαδικασιών για την τήρηση και την ασφαλή διαγραφή δεδομένων με το πέρας του διαστήματος τήρησής τους.
- **Κρυπτογράφηση Δεδομένων:** Υλοποίηση μεθόδων κρυπτογράφησης και απόκρυψης δεδομένων καρτών για την αντιμετώπιση των συνέπειών από πιθανή διαρροή τους

Λοιπά Πρότυπα

CIS Benchmarks

CIS Benchmarks

FedRAMP

FedRAMP (Federal Risk and Authorization Management Program)

AICPA Service Organization Control Reports
AICPA
SOC 2
Formerly SAS 70 Reports

COPPA (Children's Online Privacy Protection Act)

Καλές Πρακτικές και Προτάσεις

05

Διαχείριση Δεδομένων

Πριν τη σύναψη συμφωνίας με πάροχο υπηρεσιών νεφοϋπολογιστικής για την μετάβαση των ηλεκτρονικών δεδομένων στο cloud, πρέπει να εξεταστούν τα ακόλουθα ζητήματα:

- **Ασφάλεια Δεδομένων:** Διάκριση και επιπλέον ασφάλεια για ευαίσθητα και ρυθμιζόμενα πληροφοριακά στοιχεία.
- **Τοποθεσία Δεδομένων:** Γνώση των servers, της τοποθεσίας χρηστών και μεταφοράς δεδομένων, καθώς και των σχετικών νομικών δικαιοδοσιών.
- **Επιτήρηση Δεδομένων:** Πολιτικές ανίχνευσης παραβιάσεων, αναφοράς και ελέγχου ασφαλείας. Συμμόρφωση με νόμους ιδιωτικότητας και άμεση ειδοποίηση σε περιπτώσεις παραβίασης.
- **Έλεγχος Δεδομένων:** Κατανόηση της πρόσβασης στα δεδομένα, των υπαλλήλων του παρόχου και ενδεχόμενη χρήση τρίτων με πρόσβαση.

Κατανόηση των Κινδύνων

Τα δεδομένα είναι κρίσιμα για άτομα και επιχειρήσεις. Η ασφάλεια δεδομένων και η ιδιωτικότητα είναι πιο σημαντικές με την ανάπτυξη του cloud computing. Οι κύριοι κίνδυνοι περιλαμβάνουν:

- **Παραβίαση Δεδομένων**: Οικονομική ζημία, αρνητικές επιπτώσεις στη φήμη και νομικές συνέπειες από μη εξουσιοδοτημένη πρόσβαση.
- **Απώλεια Δεδομένων**: Σφάλματα ή διακοπές στις υπηρεσίες cloud μπορεί να οδηγήσουν σε σοβαρό αντίκτυπο στις λειτουργίες.
- **Παραβάσεις Συμμόρφωσης**: Μη τήρηση κανονισμών όπως GDPR και HIPAA μπορεί να οδηγήσει σε πρόστιμα και νομικές συνέπειες.
- **Εσωτερικές Απειλές**: Κίνδυνοι από εσωτερικούς παράγοντες με πρόσβαση σε ευαίσθητες πληροφορίες.

Οδηγίες για Ασφάλεια και Ιδιωτικότητα Δεδομένων στο Cloud

1. **Κρυπτογράφηση.**
2. **Έλεγχος Πρόσβασης.**
3. **Συνεχής Έλεγχος και Παρακολούθηση.**
4. **Ταξινόμηση Δεδομένων.**
5. **Ασφαλής Διαμόρφωση.**
6. **Δημιουργία αντιγράφων ασφαλείας και ανάκτηση από καταστροφές.**
7. **Σχέδιο Ανταπόκρισης σε Περιστατικά.**
8. **Εκπαίδευση και Ευαισθητοποίηση των Εργαζομένων.**
9. **Συνεχής Βελτίωση.**

Στρατηγικές Εκπαίδευσης και Ενημέρωσης

Αξιολόγηση των τρεχουσών αναγκών και στόχων:

- **Κύριοι Κίνδυνοι και Απειλές**: Ποιοι είναι οι βασικοί κίνδυνοι στο περιβάλλον του cloud;
- **Απαιτήσεις Συμμόρφωσης**: Ποιες είναι οι ρυθμιστικές απαιτήσεις που πρέπει να πληρούνται;
- **Κενά Δεξιοτήτων**: Ποια είναι τα κενά γνώσεων στην ομάδα;

Επιλογή Μεθόδων Εκμάθησης:

- **Διαδικτυακά Μαθήματα και Πιστοποιήσεις**: Πηγές όπως το Cloud Security Alliance (CSA), AWS, Microsoft Learn και Google Cloud Training.
- **Άλλες Πηγές:** Βιβλία, ιστολόγια, podcast, διαδικτυακά σεμινάρια, εργαστήρια και μέντορες.

Εφαρμογή της Εκμάθησης:

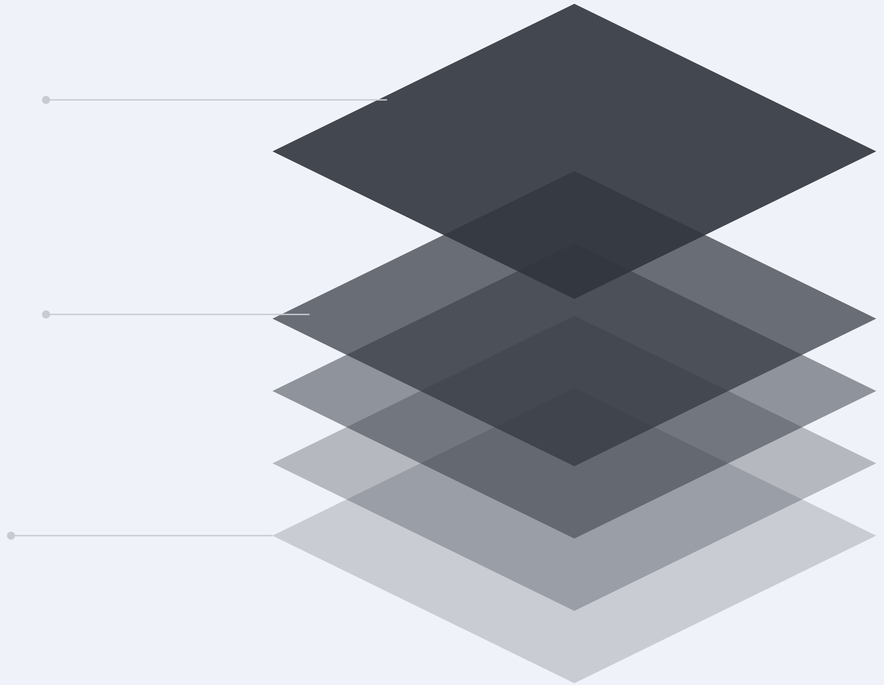
- **Πραγματικά Σενάρια και Projects:** Χρήση εργαλείων και πλατφορμών όπως το Cloud Playground και τα Cloud Security Labs.
- **Πρακτικές Ασκήσεις:** Συμμετοχή σε Cloud Security Challenges.

Τεχνολογικές Λύσεις για την Ιδιωτικότητα στη Νεφοϋπολογιστική

Ανωνυμοποίηση και Ψευδωνυμοποίηση

Τεχνικές Ελαχιστοποίησης Δεδομένων

Κρυπτογράφηση Δεδομένων



Κρυπτογράφηση Δεδομένων

Βασικές Έννοιες της Κρυπτογράφησης

- Κρυπτογράφηση Συμμετρικού Κλειδιού
- Κρυπτογράφηση Ασύμμετρου Κλειδιού

Σημασία στη Νεφοϋπολογιστική

- Εμπιστευτικότητα
- Έλεγχος

Πρακτική Εφαρμογή της Κρυπτογράφησης

- Προστασία δεδομένων σε διακομιστές νέφους και κατά τη μεταφορά
- Διατήρηση απόδοσης και ρευστότητας διαδικασιών

Τεχνικές Ελαχιστοποίησης Δεδομένων

Ελαχιστοποίηση δεδομένων

- Περιορισμός Συλλογής Δεδομένων
- Αποθήκευση Δεδομένων για Περιορισμένο Χρόνο
- Διαγραφή Αναγνωριστικών Στοιχείων

Οφέλη Ελαχιστοποίησης Δεδομένων

- Βελτίωση της Ιδιωτικότητας
- Μείωση του Κόστους
- Συμμόρφωση με τη Νομοθεσία (GDPR)

Πρακτική Εφαρμογή της Ελαχιστοποίησης

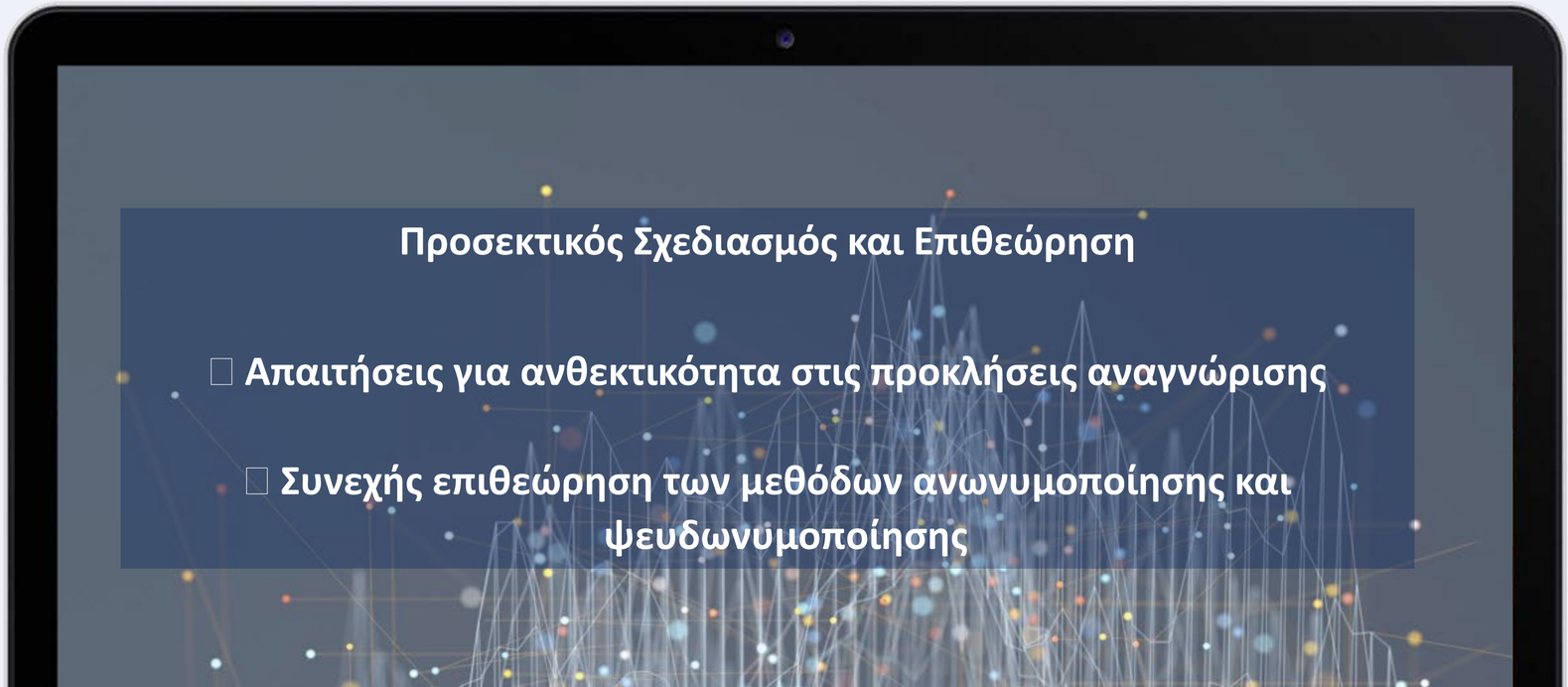
- Επανεξέταση πρακτικών συλλογής και αποθήκευσης δεδομένων
- Εκπαίδευση εργαζομένων
- Τεχνολογικές λύσεις αυτοματοποιημένης διαγραφής ή ανωνυμοποίησης

Ανωνυμοποίηση και Ψευδωνυμοποίηση

Ανωνυμοποίηση: Αφαίρεση ταυτοποιητικών στοιχείων
Ψευδωνυμοποίηση: Αντικατάσταση προσωπικών δεδομένων με ψευδώνυμο

Εφαρμογές και Οφέλη

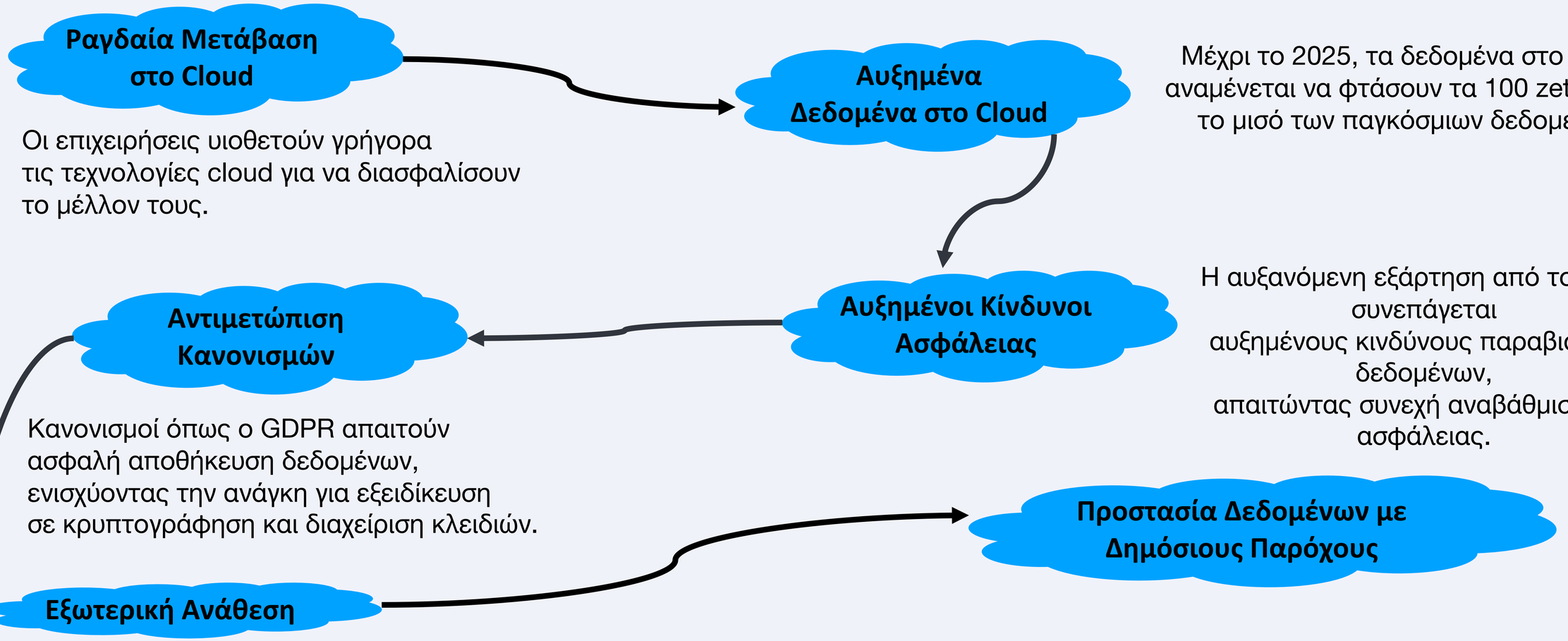
- Βελτίωση της Ιδιωτικότητας και της Ασφάλειας
- Συμμόρφωση με Νομοθεσίες
- Ευελιξία στη Χρήση Δεδομένων



Μελλοντικές προκλήσεις & προοπτικές

06

Μετάβαση στη Νεφοϋπολογιστική



Οι επιχειρήσεις υιοθετούν γρήγορα τις τεχνολογίες cloud για να διασφαλίσουν το μέλλον τους.

Μέχρι το 2025, τα δεδομένα στο cloud αναμένεται να φτάσουν τα 100 zettabyte, το μισό των παγκόσμιων δεδομένων.

Η αυξανόμενη εξάρτηση από το cloud συνεπάγεται αυξημένους κινδύνους παραβιάσεων δεδομένων, απαιτώντας συνεχή αναβάθμιση της ασφάλειας.

Κανονισμοί όπως ο GDPR απαιτούν ασφαλή αποθήκευση δεδομένων, ενισχύοντας την ανάγκη για εξειδίκευση σε κρυπτογράφηση και διαχείριση κλειδιών.

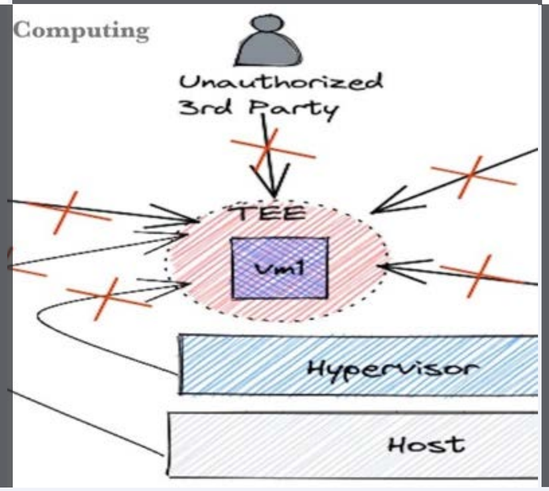
Πολλές επιχειρήσεις αναθέτουν την ανάπτυξη cloud εφαρμογών σε εξειδικευμένους τρίτους για αποτελεσματική και ασφαλή διαχείριση.

Επιλογή παρόχων όπως το Microsoft Azure, που προσφέρουν εργαλεία συμμόρφωσης και ασφάλειας, για την περαιτέρω προστασία των δεδομένων.

Αναδυόμενες Τεχνολογίες - Μελλοντικές Κατευθύνσεις

1. Ομομορφική Κρυπτογράφηση (Homomorphic Encryption)

2. Confidential Computing



3. Αρχιτεκτονικές Μηδενικής Εμπιστοσύνης (Zero-Trust Architecture)

4. Ανάπτυξη Προτύπων Προστασίας της Ιδιωτικής Ζωής για Αναδυόμενες Τεχνολογίες

Αναδυόμενες Τεχνολογίες - Μελλοντικές Κατευθύνσεις

Διαχείριση Απορρήτου με Τεχνητή Νοημοσύνη

Διεπιστημονικές Προσεγγίσεις

Blockchain & RegTech

Μετρικές Ιδιωτικότητας για Υπηρεσίες Cloud

Βέλτιστες πρακτικές Απορρήτου Δεδομένων

1 Data Loss Prevention (DLP)

2 Cloud Access Security Brokers (CASB)

3 Privacy by Design

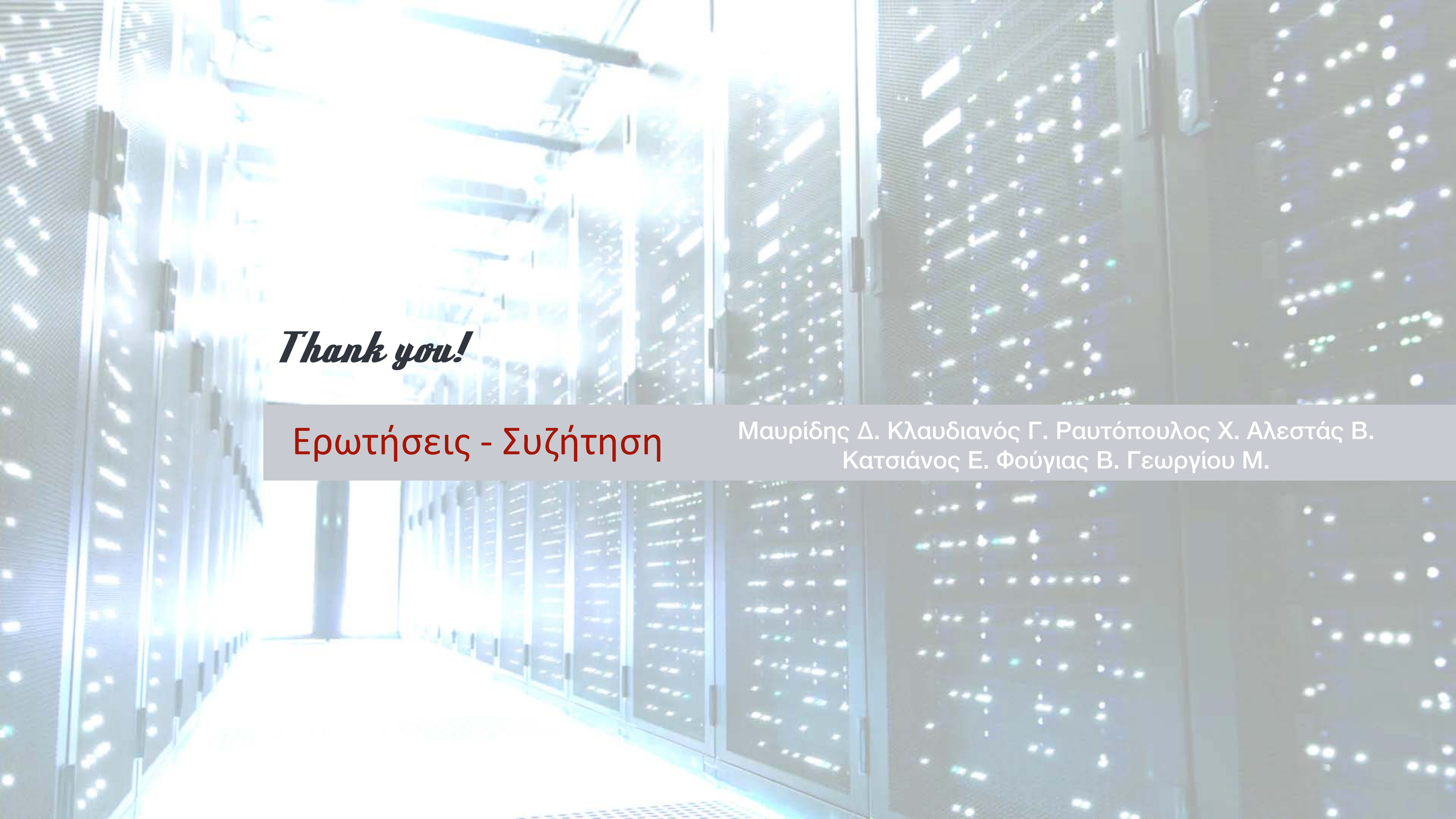
4 Τακτικοί έλεγχοι και αξιολογήσεις

5 Εκπαίδευση χρηστών

6 Συνεπής Διακυβέρνηση

Συμπεράσματα

- **Κίνδυνοι Ασφάλειας: Τα προβλήματα ασφαλείας στο cloud μπορούν να εκθέσουν προσωπικά δεδομένα, θέτοντας σε κίνδυνο την Ιδιωτικότητα των χρηστών.**
- **Προτεραιότητα στην Ιδιωτικότητα: Απαραίτητη η εστίαση στην Ιδιωτικότητα σε όλες τις πλατφόρμες και υποδομές για την αύξηση της εμπιστοσύνης των χρηστών.**
- **Καινοτόμες Λύσεις: Προσαρμοστικές τεχνικές και καινοτόμες λύσεις απαιτούνται για την αντιμετώπιση νέων απειλών και την ισορροπία μεταξύ ακεραιότητας, εμπιστευτικότητας και Ιδιωτικότητα.**



Thank you!

Ερωτήσεις - Συζήτηση

Μαυρίδης Δ. Κλαυδιανός Γ. Ραυτόπουλος Χ. Αλεστάς Β.
Κατσιάνος Ε. Φούγιας Β. Γεωργίου Μ.