

ΕΚΔΟΣΕΙΣ ΚΛΕΙΔΑΡΙΘΜΟΣ

# ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ

## ΑΡΧΕΣ ΚΑΙ ΠΡΑΚΤΙΚΕΣ

3η αμερικανική έκδοση



William Stallings • Lawrie Brown



# Κεφάλαιο 5

Ασφάλεια βάσεων δεδομένων  
και νέφους



# Βάσεις δεδομένων

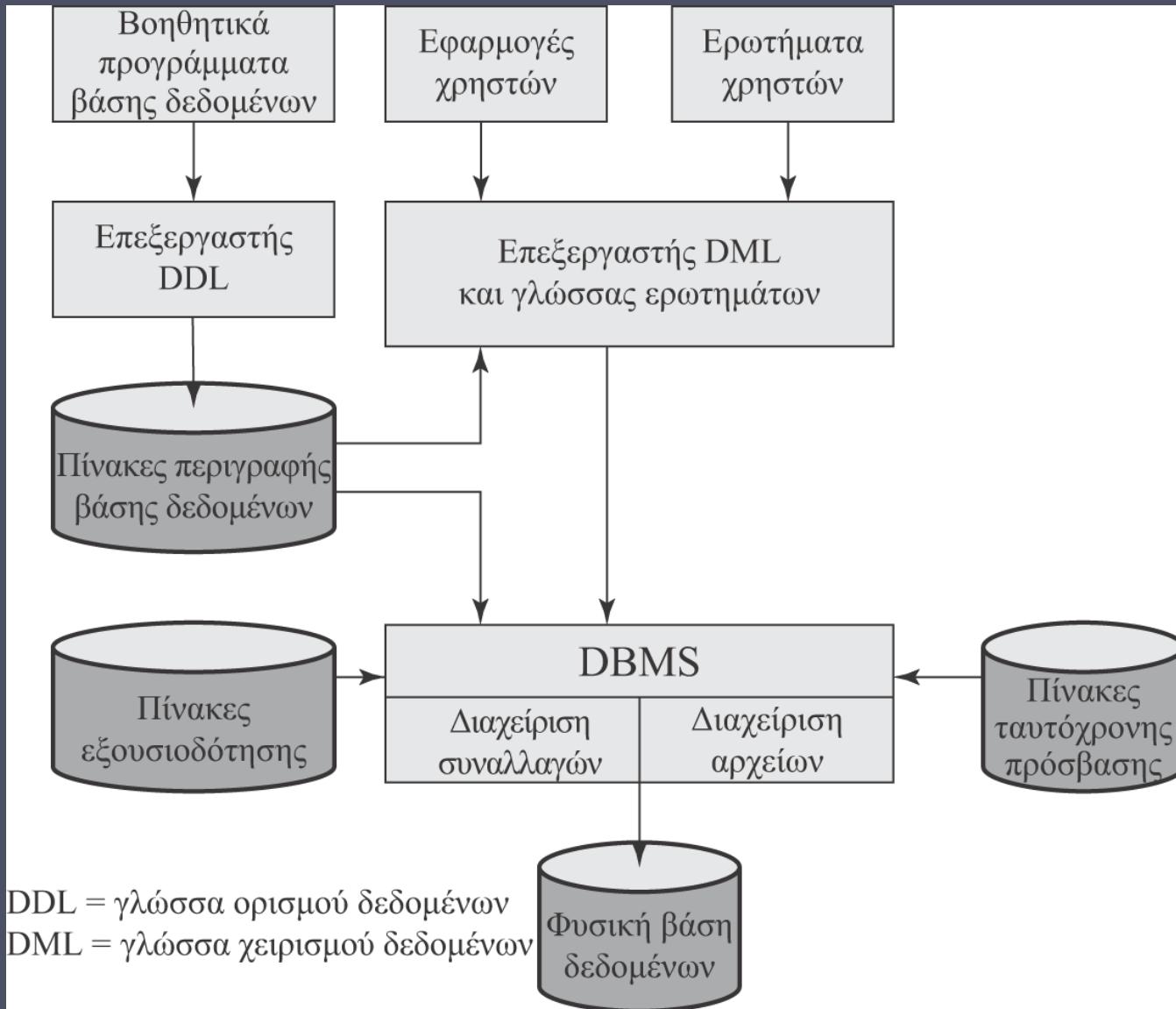
- Δομημένη συλλογή αποθηκευμένων δεδομένων για χρήση από μία ή περισσότερες εφαρμογές
- Περιέχει τις σχέσεις μεταξύ μεμονωμένων στοιχείων δεδομένων και ομάδων στοιχείων δεδομένων
- Ενδέχεται να περιέχει δεδομένων που πρέπει να διασφαλιστούν

Γλώσσα ερωτημάτων

- Παρέχει ομοιόμορφη διασύνδεση με τη βάση δεδομένων

Σύστημα διαχείρισης βάσεων δεδομένων (DBMS)

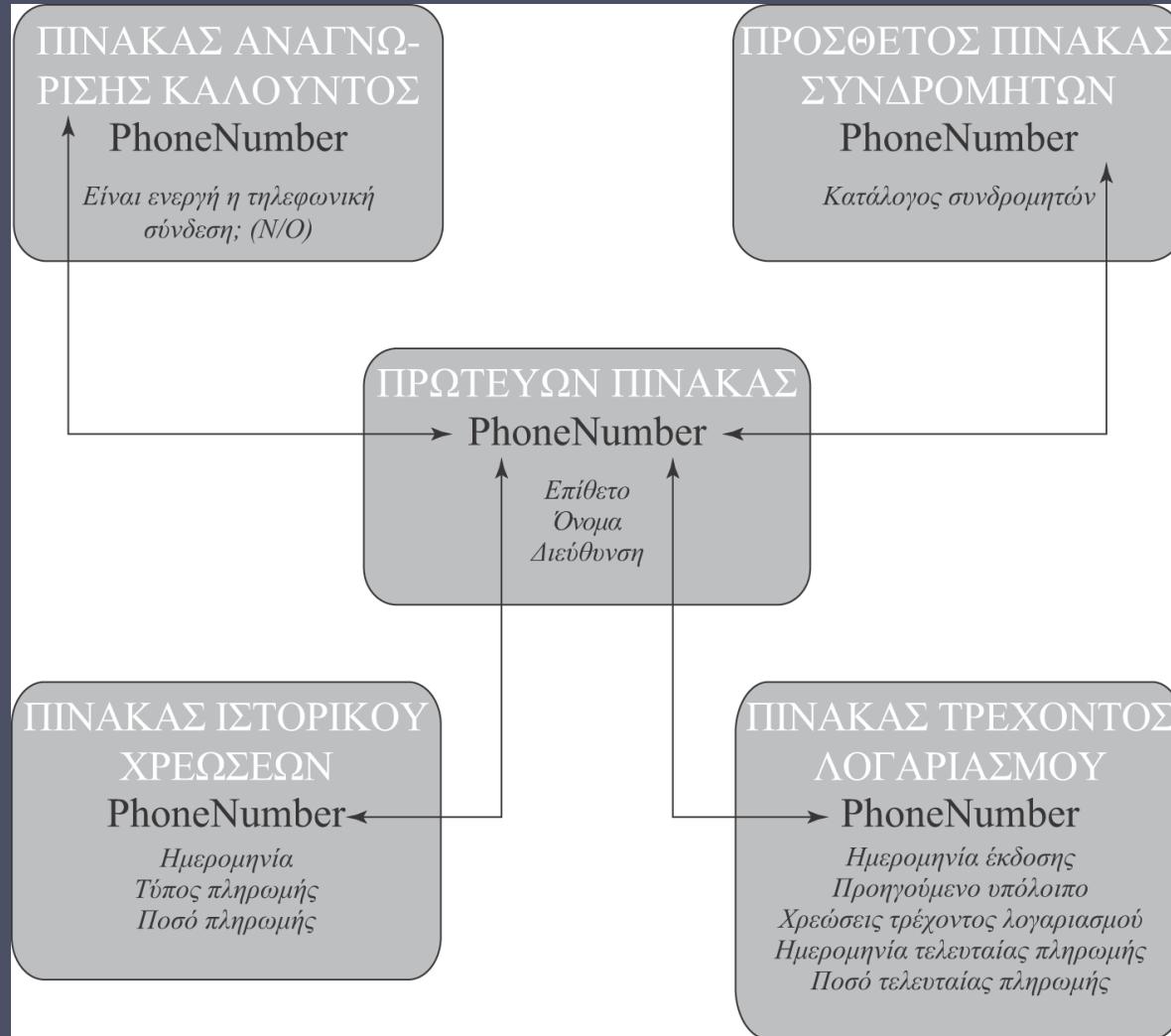
- Πακέτο προγραμμάτων για τη δημιουργία και συντήρηση της βάσης δεδομένων
- Προσφέρει σε χρήστες και εφαρμογές πρόσθιτες δυνατότητες υποβολής ειδικών ερωτημάτων



Εικόνα 5.1 Αρχιτεκτονική DBMS

# Σχεσιακές βάσεις δεδομένων

- Πίνακας δεδομένων, ο οποίος αποτελείται από γραμμές και στήλες
  - Κάθε στήλη περιλαμβάνει έναν συγκεκριμένο τύπο δεδομένων
  - κάθε γραμμή περιέχει μια συγκεκριμένη τιμή για κάθε στήλη
  - Ιδανικά, έχει μια στήλη στην οποία κάθε τιμή είναι μοναδική, και άρα μπορεί να χρησιμοποιηθεί ως αναγνωριστικό για τη συγκεκριμένη γραμμή
- Επιτρέπει τη δημιουργία πολλών πινάκων που συνδέονται μεταξύ τους με ένα μοναδικό αναγνωριστικό το οποίο υπάρχει σε όλους τους πίνακες
- Χρήστες και εφαρμογές κάνουν χρήση μιας σχεσιακής γλώσσας ερωτημάτων για να προστελάσουν τη βάση δεδομένων
  - Επιτρέπει στον χρήστη να υποβάλλει αίτηση για στοιχεία δεδομένων τα οποία πληρούν ένα ορισμένο σύνολο κριτηρίων



Εικόνα 5.2 Παράδειγμα μοντέλου σχεσιακής βάσης δεδομένων. Μια σχεσιακή βάση δεδομένων χρησιμοποιεί πολλούς πίνακες που συσχετίζονται μεταξύ τους μέσω ενός καθορισμένου κλειδιού· σε αυτή την περίπτωση, το κλειδί είναι το πεδίο **PhoneNumber** (αριθμός τηλεφώνου)

# Στοιχεία σχεσιακής βάσης δεδομένων



- Σχέση/πίνακας/αρχείο
- Πλειάδα/γραμμή/εγγραφή
- Ιδιότητα/στήλη/πεδίο

## Πρωτεύον κλειδί (primary key)

- Προσδιορίζει μια γραμμή με μοναδικό τρόπο
- Αποτελείται από ένα ή περισσότερα ονόματα στηλών

## Ξένο κλειδί (foreign key)

- Συνδέει έναν πίνακα με ιδιότητες κάποιου άλλου

## Όψη (view)/εικονικός πίνακας

- Το αποτέλεσμα ενός ερωτήματος που επιστρέφει επιλεγμένες γραμμές και στήλες από έναν ή περισσότερους πίνακες

# Πίνακας 5.1

## Βασική ορολογία

### για σχεσιακές βάσεις δεδομένων

Επίσημη ονομασία	Κοινή ονομασία	Εναλλακτική ονομασία
Σχέση	Πίνακας	Αρχείο
Πλειάδα	Γραμμή	Εγγραφή
Ιδιότητα	Στήλη	Πεδίο

		Ιδιότητες										
		$A_1$	$\dots$			$A_j$	$\dots$			$A_M$		
Εγγραφές	1	$x_{11}$	$\dots$			$x_{1j}$	$\dots$			$x_{1M}$		
	$\vdots$	$\vdots$				$\vdots$				$\vdots$		
	$\vdots$	$\vdots$				$\vdots$				$\vdots$		
	$\vdots$	$\vdots$				$\vdots$				$\vdots$		
	$i$	$x_{i1}$	$\dots$			$x_{ij}$	$\dots$			$x_{iM}$		
	$\vdots$	$\vdots$				$\vdots$				$\vdots$		
	$\vdots$	$\vdots$				$\vdots$				$\vdots$		
	$\vdots$	$\vdots$				$\vdots$				$\vdots$		
	$N$	$x_{N1}$	$\dots$			$x_{Nj}$	$\dots$			$x_{NM}$		

Εικόνα 5.3 Αφηρημένο μοντέλο σχεσιακής βάσης δεδομένων

Πίνακας Department			Πίνακας Employee				
Did	Dname	Dacctno	Ename	Did	SalaryCode	Eid	Ephone
4	human resources (ανθρώπινων πόρων)	528221	Robin	15	23	2345	6127092485
8	education (κατάρτισης)	202035	Neil	13	12	5088	6127092246
9	accounts (λογιστήριο)	709257	Jasmine	4	26	7712	6127099348
13	public relations (δημοσίων σχέσεων)	755827	Cody	15	22	9664	6127093148
15	services (εξυπηρέτησης πελατών)	223945	Holly	8	23	3054	6127092729

Πρωτεύον κλειδί

Ξένο κλειδί

Πρωτεύον κλειδί

(α) Δύο πίνακες μιας σχεσιακής βάσεων δεδομένων

Dname	Ename	Eid	Ephone
human resources	Jasmine	7712	6127099348
education	Holly	3054	6127092729
education	Robin	2976	6127091945
accounts	Smith	4490	6127099380
public relations	Neil	5088	6127092246
services	Robin	2345	6127092485
services	Cody	9664	6127093148

(β) Μια όψη που έχει εξαχθεί από τη βάση δεδομένων

Εικόνα 5.4 Παράδειγμα σχεσιακής βάσης δεδομένων

# Δομημένη γλώσσα ερωτημάτων (SQL)

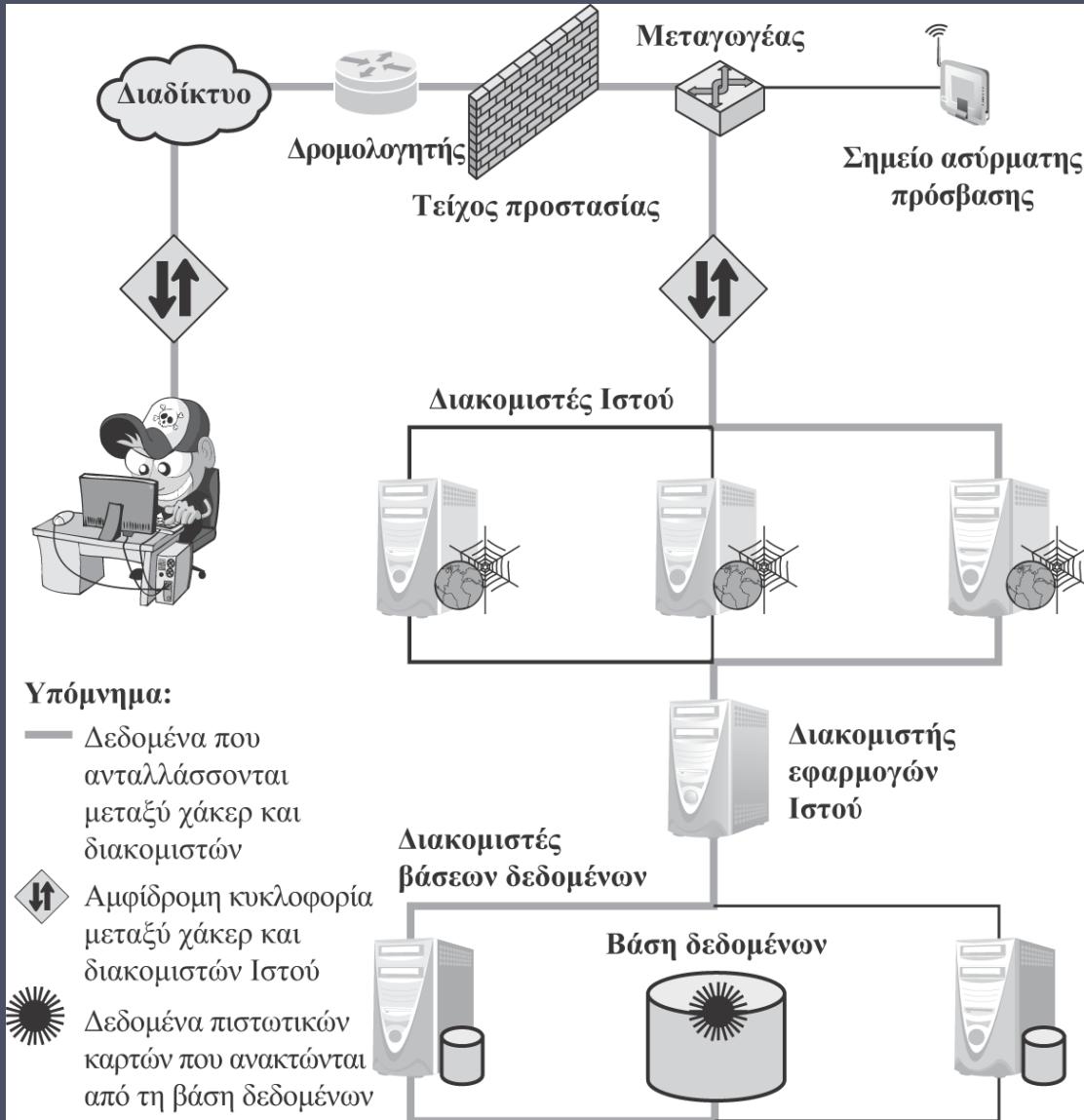
- Προτυποποιημένη γλώσσα η οποία μπορεί να χρησιμοποιηθεί για τον ορισμό ενός σχήματος (schema), τον χειρισμό δεδομένων και την υποβολή ερωτημάτων σε μια σχεσιακή βάση δεδομένων
- Αρκετές παρόμοιες εκδόσεις του προτύπου ANSI/ISO
- Όλες ακολουθούν την ίδια βασική σύνταξη και σημασιολογία

## Πιθανές χρήσεις εντολών SQL

- Δημιουργία πινάκων
- Εισαγωγή και διαγραφή δεδομένων σε πίνακες
- Δημιουργία όψεων
- Ανάκτηση δεδομένων με εντολές ερωτημάτων

# Επιθέσεις εισαγωγής εντολών SQL (SQLi)

- Μία από τις πιο διαδεδομένες και επικίνδυνες δικτυακές απειλές για την ασφάλεια
- Σχεδιασμένες να εκμεταλλεύονται τη φύση των ιστοσελίδων που περιέχουν εφαρμογές
- Στέλνουν κακόβουλες εντολές SQL στον διακομιστή της βάσης δεδομένων
- Συνηθέστερος στόχος: μαζική εξαγωγή δεδομένων
- Ανάλογα με το περιβάλλον, μπορεί να χρησιμοποιηθεί επίσης για τα εξής:
  - Τροποποίηση ή διαγραφή δεδομένων
  - Εκτέλεση αυθαίρετων εντολών του λειτουργικού συστήματος
  - Πραγματοποίηση επιθέσεων άρνησης εξυπηρέτησης (denial-of-service, DoS)

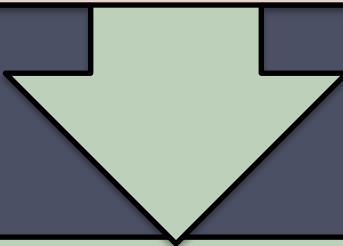


Εικόνα 5.5 Τυπική επίθεση εισαγωγής εντολών SQL

# Τεχνική εισαγωγής εντολών

Συνήθως η επίθεση SQLi τερματίζει πρόωρα μια ακολουθία χαρακτήρων και προσαρτά μια νέα εντολή

Επειδή στην εντολή που εισάγεται μπορούν να προσαρτηθούν πρόσθετες ακολουθίες πριν από την εκτέλεσή της, ο επιτιθέμενος τερματίζει την εισαχθείσα ακολουθία με ένα σύμβολο σχολίου '--'



Το κείμενο που ακολουθεί μετά το συγκεκριμένο σύμβολο αγνοείται κατά τον χρόνο εκτέλεσης

# Τρόποι επιθέσεων SQLi

## Δεδομένα εισόδου του χρήστη (user input)

- Οι επιτιθέμενοι εισάγουν εντολές SQL παρέχοντας κατάλληλα «κατασκευασμένα» δεδομένα που υποτίθεται ότι εισάγουν οι χρήστες

## Μεταβλητές διακομιστή (server variables)

- Οι επιτιθέμενοι μπορούν να πλαστογραφήσουν τις τιμές που τοποθετούνται μέσα σε κεφαλίδες HTTP και κεφαλίδες δικτύου και να εκμεταλλευθούν τη συγκεκριμένη ευπάθεια εισάγοντας δεδομένα απευθείας μέσα στις κεφαλίδες

## Εισαγωγή εντολών δευτέρου βαθμού (second-order injection)

- Ένας κακόβουλος χρήστης θα μπορούσε να στηριχθεί σε δεδομένα που υπάρχουν ήδη στο σύστημα ή τη βάση δεδομένων για να ξεκινήσει μια επίθεση εισαγωγής εντολών SQL, έτσι ώστε όταν πραγματοποιηθεί η επίθεση, τα δεδομένα εισόδου που τροποποιούν το ερώτημα και προκαλούν την επίθεση να μην προέρχονται από τον χρήστη, αλλά από το εσωτερικό του ίδιου του συστήματος

## «Μπισκότα» (cookies)

- Ένας επιτιθέμενος μπορεί να τροποποιήσει μπισκότα με τέτοιον τρόπο ώστε, όταν ο διακομιστής εφαρμογών δημιουργήσει ένα ερώτημα SQL με βάση το περιεχόμενο του μπισκότου, να τροποποιηθούν η δομή και η λειτουργία του ερωτήματος

## Φυσικά δεδομένα εισόδου του χρήστη

- Παροχή δεδομένων εισόδου του χρήστη τα οποία ξεκινούν μια επίθεση έξω από το σύμπαν των αιτήσεων Ιστού

# Ενδοζωνική επίθεση

- Χρησιμοποιεί το ίδιο κανάλι επικοινωνίας για την εισαγωγή κώδικα SQL και την ανάκτηση αποτελεσμάτων
- Τα ανακτηθέντα αποτελέσματα εμφανίζονται απευθείας στην ιστοσελίδα της εφαρμογής
- Στις ενδοζωνικές επιθέσεις περιλαμβάνονται τα εξής:

## Ταυτολογία

Εισάγει κώδικα σε μία ή περισσότερες εντολές συνθήκης έτσι ώστε να επιστρέφουν πάντα τιμή true

## Σχόλιο τέλους γραμμής

Μετά από την εισαγωγή κώδικα σε ένα συγκεκριμένο πεδίο, ο έγκυρος κώδικας που ακολουθεί εξουδετερώνεται μέσω της χρήσης σχολίων τέλους γραμμής

## Εμβόλιμα ερωτήματα

Ο επιτιθέμενος προσθέτει επιπλέον ερωτήματα στο επιδιωκόμενο ερώτημα, προσαρτώντας την επίθεση σε μια έγκυρη αίτηση

# Επίθεση συμπερασμού

- Δεν πραγματοποιείται μεταφορά δεδομένων, αλλά ο επιτιθέμενος είναι σε θέση να ανακατασκευάσει τις πληροφορίες στέλνοντας συγκεκριμένες αιτήσεις και παρατηρώντας την επακόλουθη συμπεριφορά του διακομιστή της βάσης δεδομένων ή του ιστότοπου
- Στις επιθέσεις συμπερασμού περιλαμβάνονται τα εξής:
  - • Μη αποδεκτά/λογικά εσφαλμένα ερωτήματα
    - Η επίθεση επιτρέπει στον επιτιθέμενο να συγκεντρώσει σημαντικές πληροφορίες για τον τύπο και τη δομή της βάσης δεδομένων οπισθοφυλακής μιας εφαρμογής Ιστού
    - Θεωρείται προπαρασκευαστικό βήμα συλλογής πληροφοριών για άλλες επιθέσεις
  - Η τυφλή εισαγωγή εντολών SQL
    - Επιτρέπει στους επιτιθέμενους να συμπεράνουν τα δεδομένα που υπάρχουν σε ένα σύστημα βάσης δεδομένων ακόμα και όταν το σύστημα είναι επαρκώς ασφαλές ώστε να μην επιστρέφει πληροφορίες σφαλμάτων στον επιτιθέμενο

# Εξωζωνική επίθεση

- Ανακτώνται δεδομένα με χρήση διαφορετικού καναλιού
- Μια τέτοια προσέγγιση μπορεί να υιοθετηθεί όταν υπάρχουν μεν περιορισμοί στην ανάκτηση πληροφοριών, αλλά η συνδεσιμότητα του διακομιστή της βάσης δεδομένων με τον έξω κόσμο δεν ελέγχεται διεξοδικά



# Αντίμετρα για επιθέσεις SQLi

- Τρεις τύποι:

- Πρακτικές μη αυτόματης αμυντικής συγγραφής κώδικα
- Παραμετροποιημένη εισαγωγή ερωτημάτων
- SQL DOM

Αμυντική συγγραφή κώδικα

## Ανίχνευση

- Βασισμένη σε υπογραφές
- Βασισμένη σε ανωμαλίες
- Ανάλυση κώδικα

- Έλεγχος ερωτημάτων κατά τον χρόνο εκτέλεση για να διαπιστωθεί αν αυτά συμφωνούν με κάποιο μοντέλο προβλεπόμενων ερωτημάτων

Αποτροπή κατά τον χρόνο εκτέλεσης

# Έλεγχος πρόσβασης σε βάσεις δεδομένων

Το σύστημα ελέγχου πρόσβασης  
στη βάση δεδομένων  
προσδιορίζει:

Αν ο χρήστης επιτρέπεται να έχει πρόσβαση  
σε ολόκληρη τη βάση δεδομένων  
ή μέρος αυτής

Τα δικαιώματα πρόσβασης του χρήστη  
(δημιουργία, εισαγωγή, διαγραφή,  
ενημέρωση, ανάγνωση και εγγραφή)

Μπορεί να υποστηρίζει  
διάφορες πολιτικές διαχείρισης

Κεντρική διαχείριση

- Ένας μικρός αριθμός προνομιακών χρηστών μπορούν να χορηγούν και να ανακαλούν δικαιώματα πρόσβασης

Διαχείριση βασισμένη στην κυριότητα

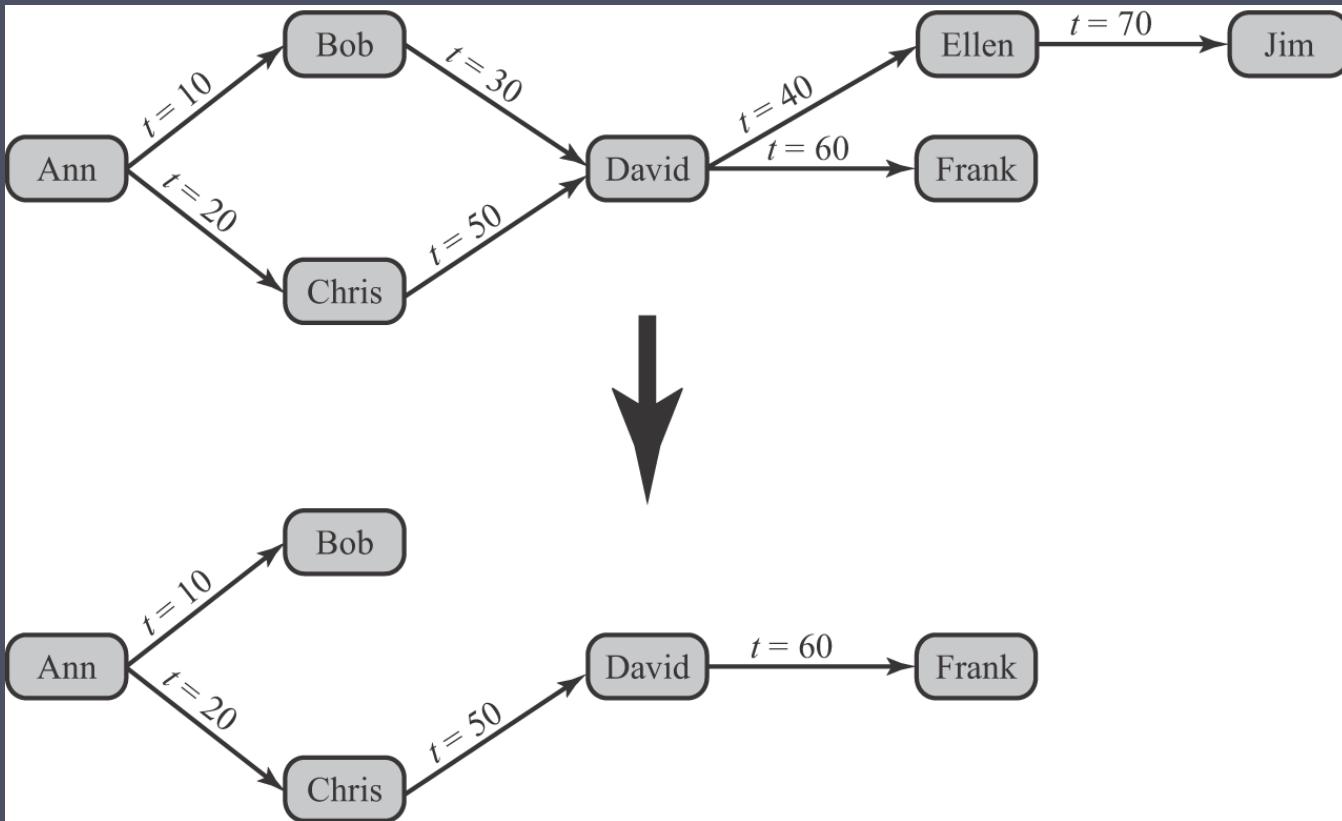
- Ο κάτοχος (δημιουργός) ενός πίνακα μπορεί να χορηγεί και να ανακαλεί δικαιώματα πρόσβασης στον πίνακα

Αποκεντρωμένη διαχείριση

- Ο κάτοχος του πίνακα μπορεί να χορηγεί και να ανακαλεί δικαιώματα εξουσιοδότησης σε/από άλλους χρήστες, επιτρέποντάς τους να χορηγούν και να ανακαλούν δικαιώματα πρόσβασης στον πίνακα

# Ορισμός πρόσβασης βασισμένος σε SQL

- Δύο εντολές για τη διαχείριση δικαιωμάτων πρόσβασης:
  - grant (χορήγηση)
    - Χρησιμοποιείται για τη χορήγηση ενός ή περισσοτέρων δικαιωμάτων πρόσβασης ή για την ανάθεση ενός ρόλου σε έναν χρήστη
  - revoke (ανάκληση)
    - Ανακαλεί τα δικαιώματα πρόσβασης
- Τυπικά δικαιώματα πρόσβασης:
  - Επιλογή (select)
  - Εισαγωγή (insert)
  - Ενημέρωση (update)
  - Διαγραφή (delete)
  - Αναφορές (references)



Εικόνα 5.6 Ο Bob ανακαλεί το προνόμιο του David

# Έλεγχος πρόσβασης βασισμένος σε ρόλους (RBAC)

- Ο βασισμένος σε ρόλους έλεγχος πρόσβασης παρέχει έναν τρόπο ελάφρυνσης του διαχειριστικού φόρτου και ενίσχυσης της ασφάλειας
- Το υποσύστημα RBAC μιας βάσης δεδομένων πρέπει να παρέχει τις εξής δυνατότητες:
  - Δημιουργία και διαγραφή ρόλων
  - Ορισμός αδειών (δικαιωμάτων πρόσβασης) για έναν ρόλο
  - Ανάθεση και αφαίρεση ρόλων σε/από χρήστες
- Κατηγορίες χρηστών μιας βάσης δεδομένων:

## Κάτοχος εφαρμογής

- Τελικός χρήστης που είναι κάτοχος αντικειμένων της βάσης δεδομένων στα πλαίσια μιας εφαρμογής

## Τελικός χρήστης

- Τελικός χρήστης που εκτελεί διάφορες ενέργειες σε αντικείμενα της βάσης δεδομένων μέσω συγκεκριμένης εφαρμογής, αλλά δεν είναι κάτοχος κάποιου αντικειμένου

## Διαχειριστής

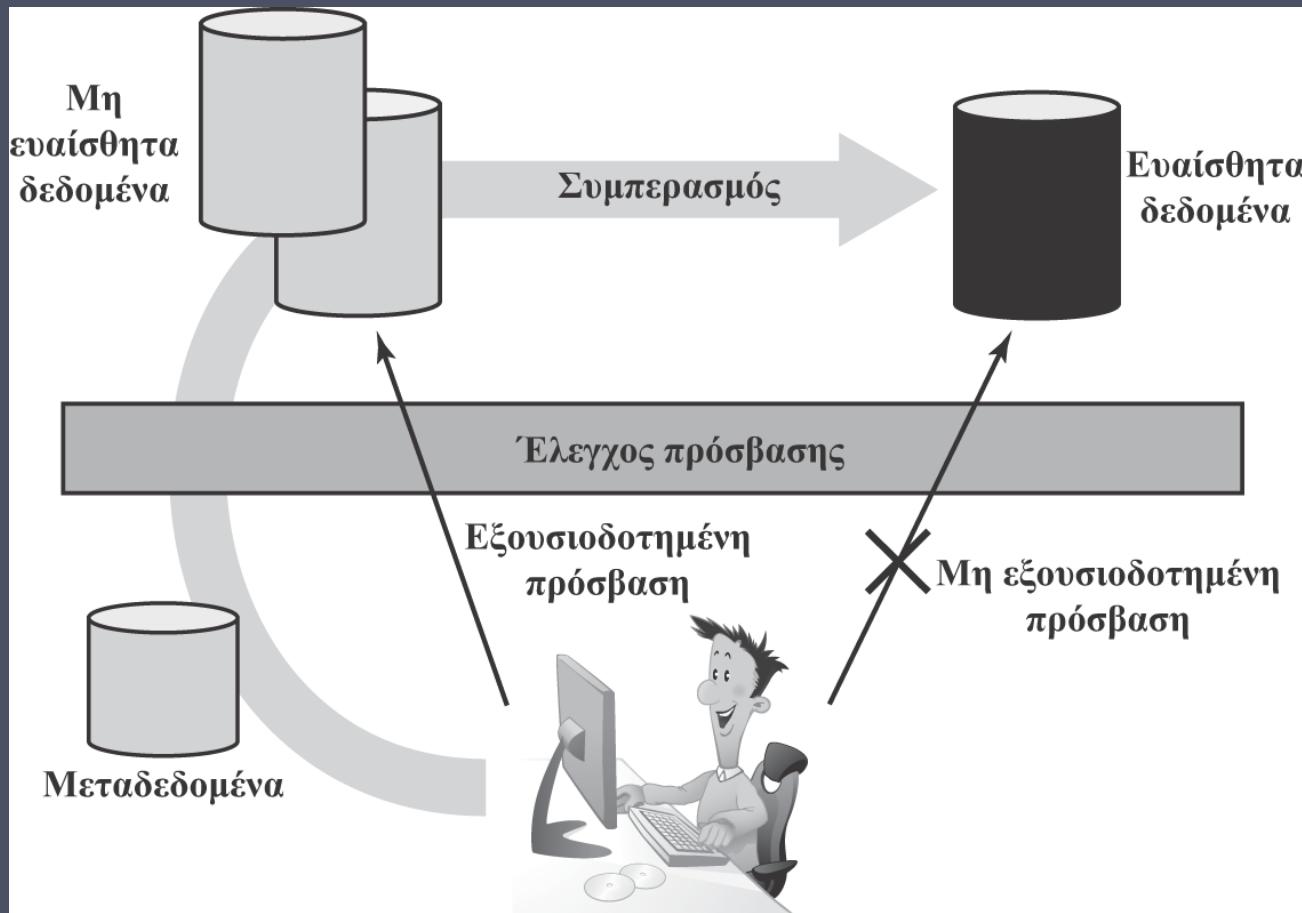
- Χρήστης ο οποίος έχει την ευθύνη διαχείρισης ενός μέρους ή ολόκληρης της βάσης δεδομένων

# Πίνακας

## 5.2

### Σταθεροί ρόλοι στον Microsoft SQL Server

Ρόλος	Άδειες (δικαιώματα πρόσβασης)
<b>Σταθεροί ρόλοι διακομιστή</b>	
sysadmin	Μπορεί να εκτελεί όλες τις δραστηριότητες του SQL Server και έχει τον πλήρη έλεγχο όλων των λειτουργιών μιας βάσης δεδομένων
serveradmin	Μπορεί να ορίζει επιλογές διευθέτησης που ισχύουν σε όλο τον διακομιστή, καθώς και να τερματίζει τον διακομιστή
setupadmin	Μπορεί να διαχειρίζεται συνδεδεμένους διακομιστές και διαδικασίες εκκίνησης
securityadmin	Μπορεί να διαχειρίζεται συνδέσεις (logins) και άδειες CREATE DATABASE, καθώς και να διαβάζει αρχεία καταγραφής σφαλμάτων και να αλλάζει κωδικούς πρόσβασης
processadmin	Μπορεί να διαχειρίζεται διεργασίες που εκτελούνται στον SQL Server
Dbcreator	Μπορεί να δημιουργεί, να τροποποιεί και να καταργεί βάσεις δεδομένων
diskadmin	Μπορεί να διαχειρίζεται αρχεία δίσκων
bulkadmin	Μπορεί να εκτελεί εντολές BULK INSERT
<b>Σταθεροί ρόλοι βάσης δεδομένων</b>	
db_owner	Διαθέτει όλες τις άδειες της βάσης δεδομένων
db_accessadmin	Μπορεί να προσθέτει ή να καταργεί αναγνωριστικά χρηστών
db_datareader	Μπορεί να επιλέγει όλα τα δεδομένα από οποιονδήποτε πίνακα της βάσης δεδομένων
db_datawriter	Μπορεί να τροποποιεί οποιαδήποτε δεδομένα σε οποιονδήποτε πίνακα της βάσης δεδομένων
db_ddladmin	Μπορεί να ορίζει όλες τις εντολές της γλώσσας ορισμού δεδομένων (DDL)
db_securityadmin	Μπορεί να διαχειρίζεται όλες τις άδειες, τις κυριότητες αντικειμένων, τους ρόλους, και τα μέλη των ρόλων
db_backupoperator	Μπορεί να ορίζει εντολές DBCC, CHECKPOINT και BACKUP
db_denydatareader	Μπορεί να απορρίπτει αιτήσεις επιλογής δεδομένων από τη βάση
db_denydatawriter	Μπορεί να απορρίπτει αιτήσεις τροποποίησης δεδομένων στη βάση



Εικόνα 5.7 Έμμεση προσπέλαση πληροφοριών μέσω καναλιού συμπερασμού

Item (προϊόν)	Availability (διαθεσιμότητα)	Cost (κόστος, σε \$)	Department (τμήμα)
Shelf support	in-store/online	7,99	hardware
Lid support	online only	5,49	hardware
Decorative chain	in-store/online	104,99	hardware
Cake pan	online only	12,99	housewares
Shower/tub cleaner	in-store/online	11,99	housewares
Rolling pin	in-store/online	10,99	housewares

(α) Πίνακας Inventory

Availability	Cost (\$)	Item	Department
in-store/online	7,99	Shelf support	hardware
online only	5,49	Lid support	hardware
in-store/online	104,99	Decorative chain	hardware

(β) Δύο όψεις

Item	Availability	Cost (\$)	Department
Shelf support	in-store/online	7,99	hardware
Lid support	online only	5,49	hardware
Decorative chain	in-store/online	104,99	hardware

(γ) Πίνακας που προκύπτει από τον συνδυασμό απαντήσεων σε ερωτήματα

## Εικόνα 5.8 Παράδειγμα συμπερασμού

# Ανίχνευση συμπερασμού



- Σε οποιαδήποτε από τις παραπάνω προσεγγίσεις απαιτείται κάποιου είδους αλγόριθμος ανίχνευσης του συμπερασμού
- Αρκετή πρόοδος έχει σημειωθεί στις περιπτώσεις των βάσεων δεδομένων με πολυεπίπεδη ασφάλεια και των στατιστικών βάσεων δεδομένων, με την έννοια ότι έχουν αναπτυχθεί συγκεκριμένες τεχνικές ανίχνευσης του συμπερασμού

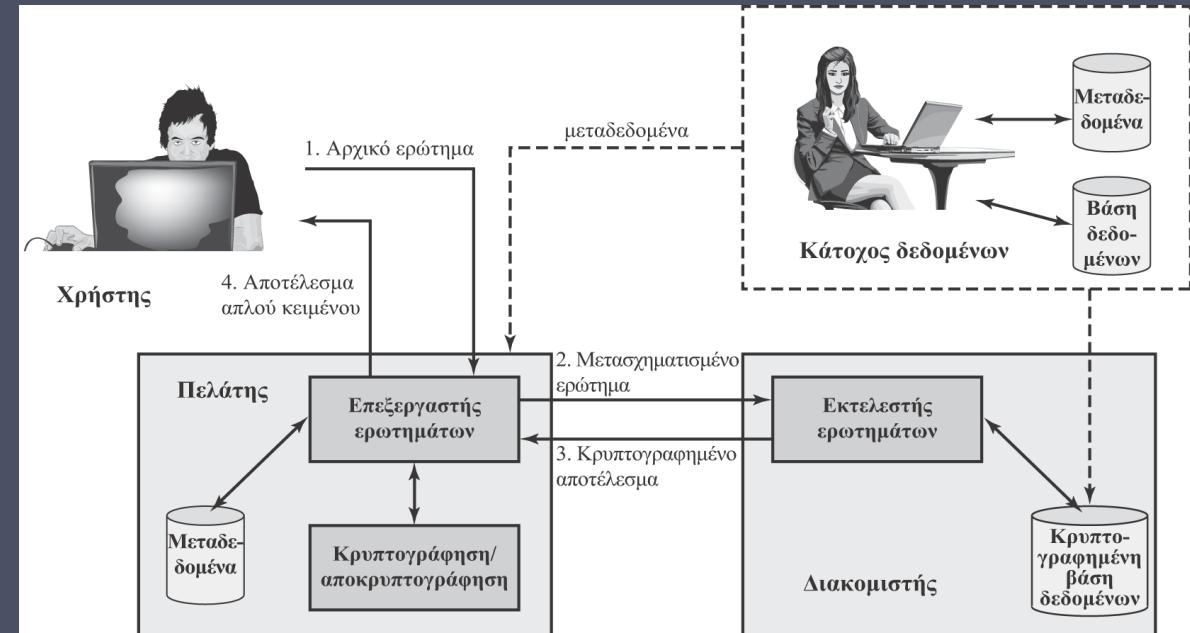
# Κρυπτογράφηση βάσεων δεδομένων

- Συνήθως η βάση δεδομένων αποτελεί τον πιο πολύτιμο πληροφοριακό πόρο για οποιονδήποτε οργανισμό
  - Προστατεύεται από πολλά επίπεδα ασφαλείας
    - Τείχη προστασίας (firewalls), μηχανισμοί πιστοποίησης ταυτότητας, συστήματα γενικού ελέγχου πρόσβασης, συστήματα ελέγχου πρόσβασης σε βάσεις δεδομένων, κρυπτογράφηση βάσεων δεδομένων
    - Η κρυπτογράφηση αποτελεί την έσχατη γραμμή άμυνας για την ασφάλεια των βάσεων δεδομένων
  - Μπορεί να εφαρμοστεί σε ολόκληρη τη βάση δεδομένων ή σε επίπεδο εγγραφών, ιδιοτήτων, ή μεμονωμένων πεδίων
- Μειονεκτήματα της κρυπτογράφησης:
  - Διαχείριση κλειδιών
    - Οι εξουσιοδοτημένοι χρήστες πρέπει να έχουν πρόσβαση στο κλειδί αποκρυπτογράφησης των δεδομένων τα οποία μπορούν να προσπελάσουν
  - Έλλειψη ευελιξίας
    - Όταν ένα μέρος ή το σύνολο μιας βάσης δεδομένων είναι κρυπτογραφημένο, καθίσταται πιο δύσκολη η εκτέλεση αναζητήσεων στις εγγραφές

**Κάτοχος δεδομένων –**  
οργανισμός που παράγει  
δεδομένα τα οποία θα  
διατεθούν με ελεγχόμενο  
τρόπο

**Χρήστης –** ανθρώπινη  
οντότητα που υποβάλλει  
ερωτήματα στο σύστημα

**Πελάτης –** εμπροσθοφυλακή  
που μετασχηματίζει  
τα ερωτήματα των χρηστών  
σε ερωτήματα τα οποία  
μπορούν να εκτελεστούν  
στα κρυπτογραφημένα  
δεδομένα που βρίσκονται  
αποθηκευμένα στον  
διακομιστή



Εικόνα 5.9 Σχήμα κρυπτογράφησης βάσεων δεδομένων

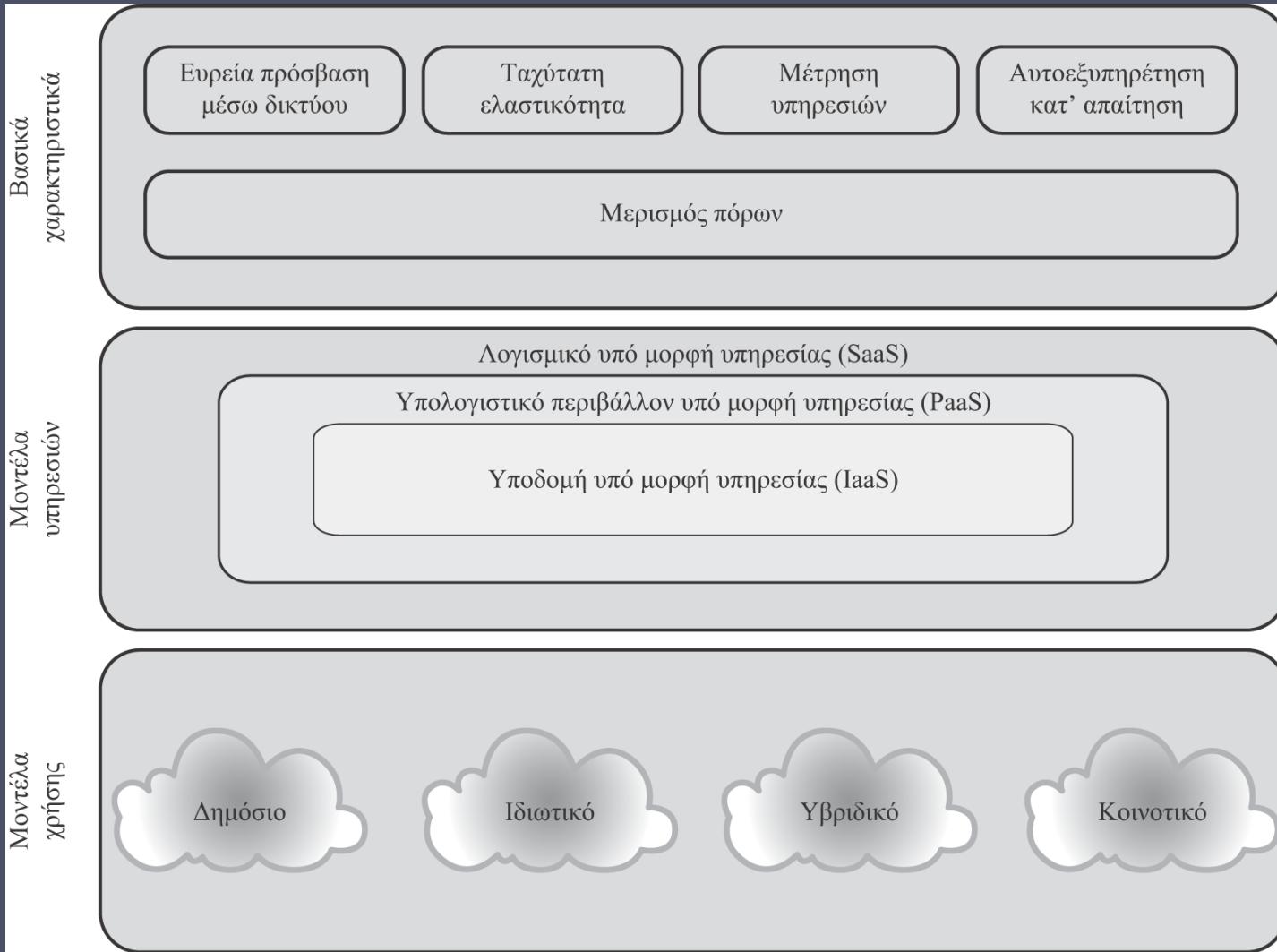
**Διακομιστής –** οργανισμός  
που λαμβάνει τα  
κρυπτογραφημένα  
δεδομένα από τον κάτοχο  
τους και τα διαθέτει για  
διανομή σε πελάτες



# Ασφάλεια νέφους

Το έγγραφο SP 800-145 ορίζει την υπολογιστική νέφους ως εξής:

«Ένα μοντέλο που καθιστά εφικτή την πρακτική, κατ' απαίτηση, παγκόσμια πρόσβαση μέσω δικτύου σε μια κοινόχρηστη δεξαμενή διευθετήσιμων υπολογιστικών πόρων (π.χ. δίκτυα, διακομιστές, μονάδες αποθηκευτικού χώρου, εφαρμογές και υπηρεσίες) οι οποίοι μπορούν να δεσμεύονται και να αποδεσμεύονται ταχύτατα με ελάχιστο φόρτο διαχείρισης ή αλληλεπίδραση με τον πάροχο υπηρεσιών. Αυτό το μοντέλο νέφους προάγει τη διαθεσιμότητα και αποτελείται από πέντε βασικά χαρακτηριστικά, τρία μοντέλα υπηρεσίας, και τέσσερα μοντέλα χρήσης.»



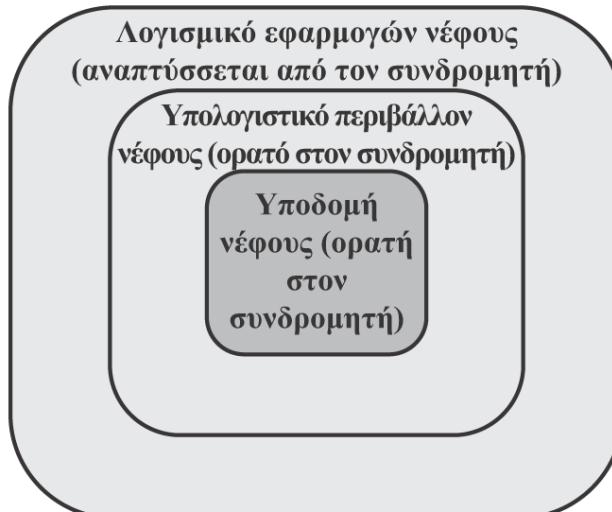
Εικόνα 5.11 Στοιχεία της υπολογιστικής νέφους



(α) SaaS



(β) PaaS



(γ) IaaS

Εικόνα 5.12 Μοντέλα υπηρεσίας νέφους

# Μοντέλα χρήσης του NIST

## Δημόσιο νέφος

- Η υποδομή νέφους είναι διαθέσιμη στο ευρύ κοινό ή σε έναν μεγάλο κλάδο και ανήκει σε κάποιον οργανισμό ο οποίος παρέχει υπηρεσίες νέφους επί πληρωμή
- Ο πάροχος νέφους είναι υπεύθυνος για την υποδομή νέφους και για τον έλεγχο των δεδομένων και των λειτουργιών εντός του νέφους

## Ιδιωτικό νέφος

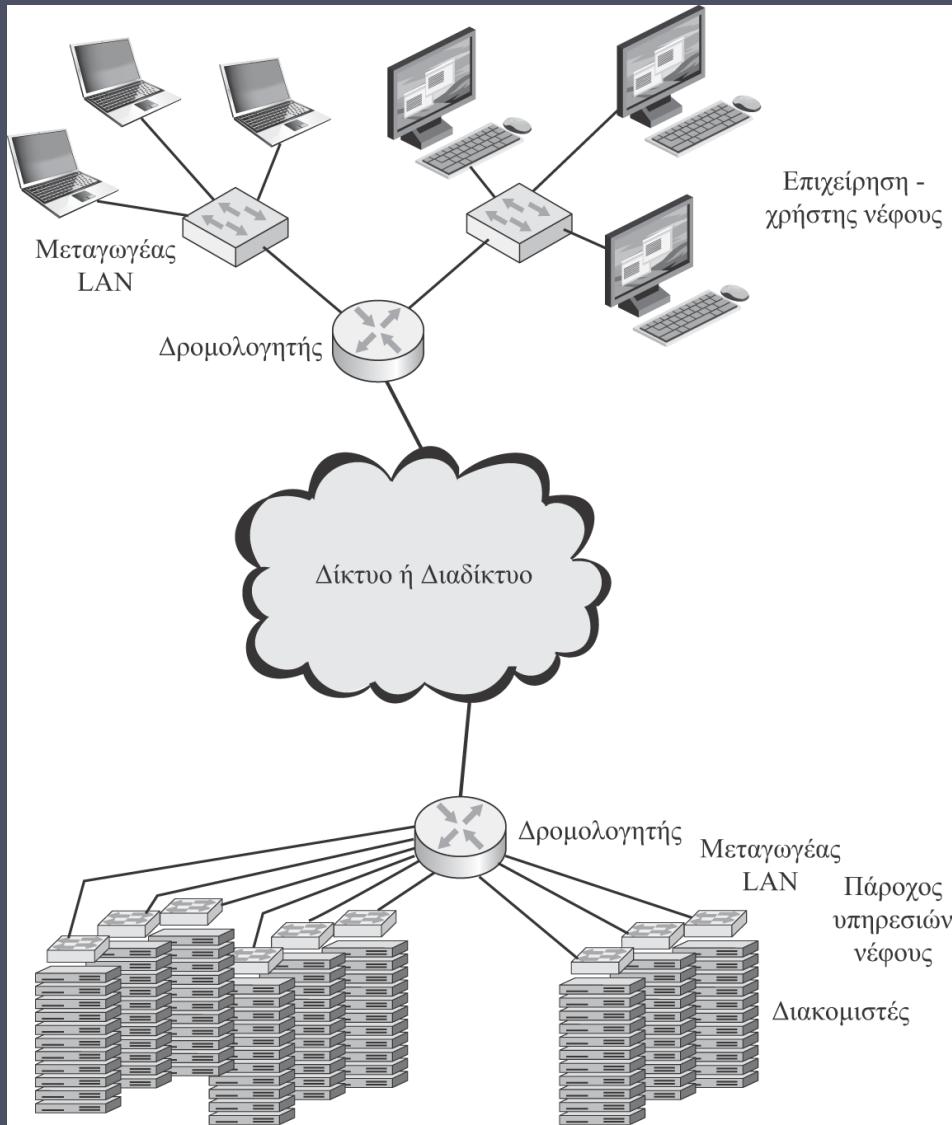
- Η ευθύνη λειτουργίας της υποδομής νέφους ανήκει αποκλειστικά σε έναν οργανισμό
- Η διαχείριση της υποδομής μπορεί να γίνεται από τον ίδιο τον οργανισμό ή από κάποιον τρίτο, και η υποδομή μπορεί να βρίσκεται εντός ή εκτός των εγκαταστάσεων του οργανισμού
- Ο πάροχος νέφους είναι υπεύθυνος για την υποδομή, όχι για τον έλεγχο

## Κοινοτικό νέφος

- Η υποδομή νέφους χρησιμοποιείται από κοινού από πολλούς οργανισμούς και υποστηρίζει μια συγκεκριμένη κοινότητα με κοινά ενδιαφέροντα
- Η διαχείριση της υποδομής μπορεί να γίνεται από τους οργανισμούς ή από κάποιον τρίτο, και η υποδομή μπορεί να βρίσκεται εντός ή εκτός των εγκαταστάσεων των οργανισμών

## Υβριδικό νέφος

- Η υποδομή νέφους αποτελεί σύνθεση δύο ή περισσότερων νεφών που εξακολουθούν να αποτελούν μοναδικές οντότητες, αλλά ενώνονται μεταξύ τους με χρήση προτυποποιημένης ή αποκλειστικής τεχνολογίας που καθιστά εφικτή τη φορητότητα δεδομένων και εφαρμογών



Εικόνα 5.13 Γενικό πλαίσιο υπολογιστικής νέφους

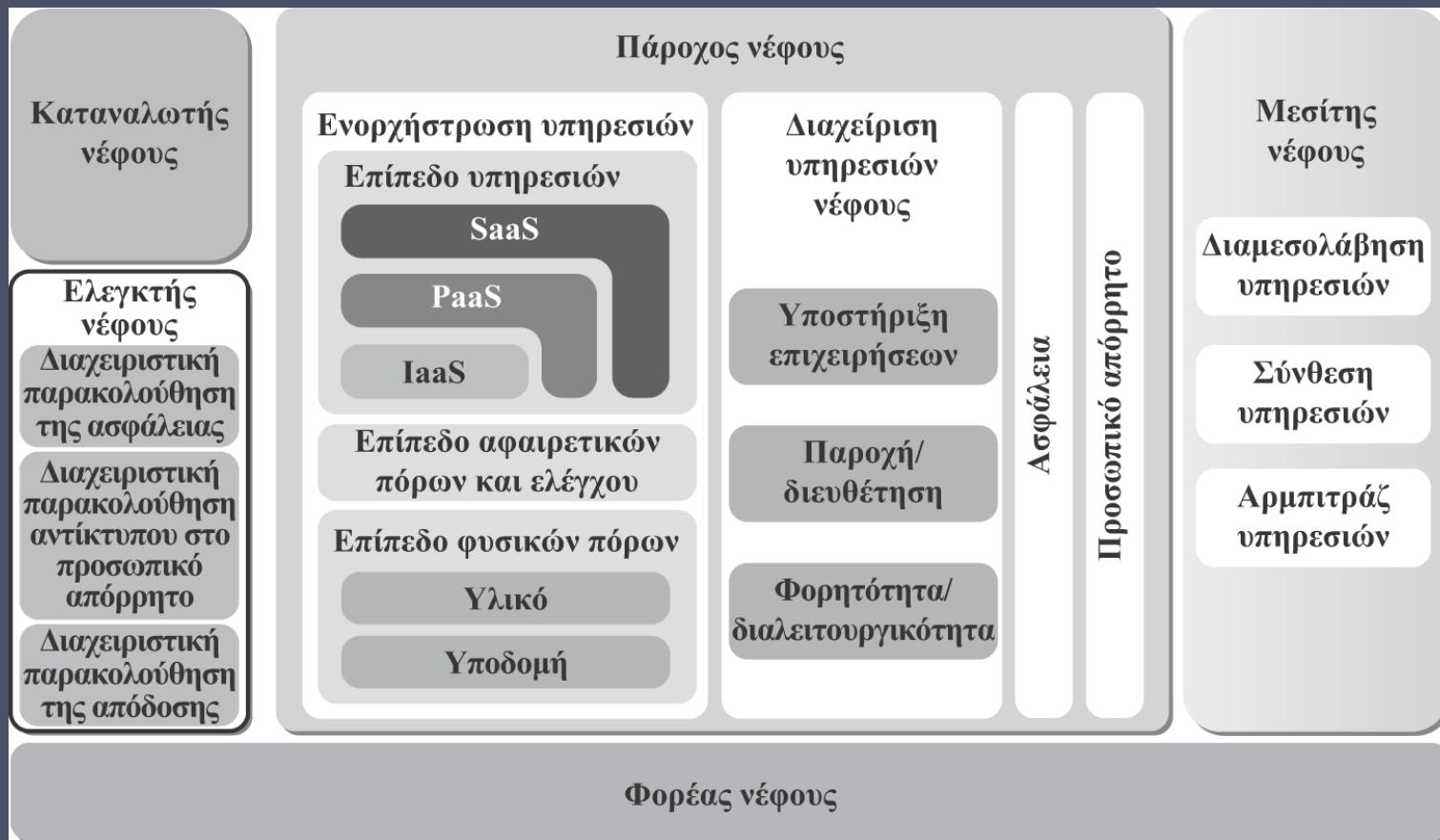
# Αρχιτεκτονική αναφοράς της υπολογιστικής νέφους

Στο έγγραφο SP 500-292 του NIST, η αρχιτεκτονική αναφοράς ορίζεται ως εξής:

«Η αρχιτεκτονική αναφοράς του NIST για την υπολογιστική νέφους εστιάζει στις απαιτήσεις του «τι» παρέχουν οι υπηρεσίες νέφους, και όχι στο «πώς μπορεί» να σχεδιαστεί και να υλοποιηθεί μια λύση. Η αρχιτεκτονική αναφοράς έχει ως στόχο να διευκολύνει την κατανόηση των λειτουργικών πολυπλοκοτήτων της υπολογιστικής νέφους. Δεν αναπαριστά την αρχιτεκτονική συστήματος ενός συγκεκριμένου συστήματος υπολογιστικής νέφους· αντίθετα, αποτελεί εργαλείο για την περιγραφή, ανάλυση, και ανάπτυξη μιας αρχιτεκτονικής εξειδικευμένης για συστήματα με χρήση ενός κοινού πλαισίου αναφοράς.»

# Αντικειμενικοί στόχοι

- Το NIST ανέπτυξε την αρχιτεκτονική αναφοράς λαμβάνοντας υπόψη τους εξής αντικειμενικούς στόχους:
  - Την κατανόηση και αποσαφήνιση των διαφόρων υπηρεσιών νέφους στα πλαίσια ενός συνολικού εννοιολογικού μοντέλου της υπολογιστικής νέφους
  - Την παροχή μιας τεχνικής αναφοράς η οποία βοηθά τους καταναλωτές να κατανοήσουν, αναλύσουν, κατηγοριοποιήσουν και συγκρίνουν διάφορες υπηρεσίες νέφους
  - Τη διευκόλυνση της ανάλυσης υποψήφιων προτύπων για την ασφάλεια, τη διαλειτουργικότητα και τη φορητότητα, καθώς και υλοποιήσεων αναφοράς



Εικόνα 5.14 Αρχιτεκτονική αναφοράς του NIST για την υπολογιστική nέφους

# Κίνδυνοι της ασφάλειας νέφους

Σύμφωνα με τον Συνασπισμό Ασφάλειας Νέφους, οι κορυφαίες απειλές ασφαλείας που σχετίζονται αποκλειστικά με το νέφος είναι οι εξής:

Κατάχρηση  
και ειδεχθής χρήση  
της υπολογιστικής  
νέφους

Μη ασφαλείς  
διασυνδέσεις  
και API

Κακόβουλοι  
χρήστες εκ των έσω

Ζητήματα  
κοινόχρηστης  
τεχνολογίας

Απώλεια ή διαρροή  
δεδομένων

«Πειρατεία»  
λογαριασμών  
ή υπηρεσιών

Άγνωστο  
προφίλ κινδύνου

# Πίνακας 5.4 Κατευθυντήριες γραμμές και συστάσεις του NIST για την ασφάλεια νέφους και ζητήματα προσωπικού απορρήτου

## Διαχείριση

Πρέπει να επεκτείνετε τις πρακτικές του οργανισμού σας οι οποίες αφορούν τις πολιτικές, τις διαδικασίες και τα πρότυπα που χρησιμοποιούνται για την ανάπτυξη εφαρμογών και την παροχή υπηρεσιών στο νέφος, καθώς και τον σχεδιασμό, την υλοποίηση, την πραγματοποίηση δοκιμών, τη χρήση και την παρακολούθηση των χρησιμοποιούμενων ή δεσμευόμενων υπηρεσιών.

Πρέπει να θέσετε σε εφαρμογή μηχανισμούς και εργαλεία διαχειριστικής παρακολούθησης ώστε να εξασφαλίσετε ότι οι πρακτικές του οργανισμού σας θα ακολουθούνται καθ' όλη τη διάρκεια του κύκλου ζωής των συστημάτων.

## Συμμόρφωση

Πρέπει να κατανοήσετε τους διάφορους τύπους νόμων και κανονισμών που επιβάλλουν στον οργανισμό σας υποχρεώσεις σχετικές με την ασφάλεια και το προσωπικό απόρρητο, οι οποίες θα μπορούσαν δυνητικά να επηρέασουν πρωτοβουλίες που αφορούν την υπολογιστική νέφους, ειδικά εκείνες που αφορούν τη γεωγραφική τοποθεσία και τον χώρο φύλαξης των δεδομένων, τους ελέγχους προσωπικού απορρήτου και ασφάλειας, τη διαχείριση εγγραφών, και τις απαιτήσεις ηλεκτρονικής ανακάλυψης (electronic discovery).

Πρέπει να ελέγχετε και να αξιολογήσετε τα όσα προσφέρει ο πάροχος νέφους σε σχέση με τις απαιτήσεις του οργανισμού σας που πρέπει να ικανοποιηθούν, και να βεβαιωθείτε ότι οι όροι της σύμβασης ικανοποιούν επαρκώς τις απαιτήσεις. Πρέπει επίσης να βεβαιωθείτε ότι οι δυνατότητες και διεργασίες ηλεκτρονικής ανακάλυψης του παρόχου δεν θέτουν σε κίνδυνο το προσωπικό απόρρητο ή την ασφάλεια δεδομένων και εφαρμογών.

## Εμπιστοσύνη

Πρέπει να βεβαιωθείτε ότι οι συμφωνίες παροχής υπηρεσιών προβλέπουν επαρκή μέσα τα οποία εξασφαλίζουν τη διαφάνεια των μηχανισμών ελέγχου και των διαδικασιών που χρησιμοποιεί ο πάροχος νέφους αναφορικά με την ασφάλεια και το προσωπικό απόρρητο, καθώς και η απόδοσή τους ως προς τον χρόνο.

Πρέπει να κατοχυρώσετε σαφή, αποκλειστικά δικαιώματα κυριότητας των δεδομένων.

Πρέπει να θεσπίσετε ένα πρόγραμμα διαχείρισης κινδύνων το οποίο θα είναι επαρκώς ευέλικτο ώστε να προσαρμόζεται στο συνεχώς εξελισσόμενο και μεταβαλλόμενο τοπίο των κινδύνων για όλο τον κύκλο ζωής του συστήματος.

Πρέπει να παρακολουθείτε σε μόνιμη βάση την κατάσταση της ασφάλειας του πληροφοριακού συστήματος ώστε να είστε σε θέση να υποστηρίξετε τη διαρκή λήγη αποφάσεων διαχείρισης κινδύνων.

## Αρχιτεκτονική

Πρέπει να κατανοήσετε τις υποκείμενες τεχνολογίες που χρησιμοποιεί ο πάροχος προκειμένου να παρέχει υπηρεσίες νέφους, συμπεριλαμβανομένων και των επιπτώσεων που επιφέρουν οι εμπλεκόμενοι τεχνικοί μηχανισμοί ελέγχου στην ασφάλεια του συστήματος και το προσωπικό απόρρητο, για όλη τη διάρκεια του κύκλου ζωής του συστήματος και για όλα τα επιμέρους υποσυστήματά του.

## Διαχείριση ταυτοτήτων και πρόσβασης

Πρέπει να βεβαιωθείτε ότι έχουν ληφθεί επαρκή μέτρα περιφρούρησης για τη διασφάλιση της πιστοποίησης ταυτότητας, της εξουσιοδότησης και άλλων λειτουργιών διαχείρισης ταυτοτήτων και πρόσβασης, τα οποία είναι κατάλληλα για τον οργανισμό σας.

## Απομόνωση λογισμικού

Πρέπει να κατανοήσετε την εικονικοποίηση και άλλες τεχνικές λογικής απομόνωσης τις οποίες χρησιμοποιεί ο πάροχος νέφους στην αρχιτεκτονική πολυμίσθωσης λογισμικού του, καθώς και να εκτιμήσετε τους κινδύνους που εγείρουν αυτές για τον οργανισμό σας.

## Προστασία δεδομένων

Πρέπει να αξιολογήσετε την καταλληλότητα των λύσεων διαχείρισης δεδομένων του παρόχου νέφους για τα σχετικά δεδομένα του οργανισμού σας, καθώς και τη δυνατότητα 1) ελέγχου της πρόσβασης στα δεδομένα, 2) προστασίας των δεδομένων ενόσω βρίσκονται σε ακινησία, κίνηση και χρήση, και 3) «απολύμανσης» των δεδομένων.

Πρέπει να λάβετε υπόψη τον κίνδυνο να συνδύουστον τα δεδομένα του οργανισμού σας με εκείνα άλλων οργανισμών οι οποίοι διαθέτουν προφίλ απειλών υψηλής επικινδυνότητας ή δεδομένα που έχουν συλλογικά μεγάλη συγκεντρωτική αξία.

Πρέπει να κατανοήσετε πλήρως και να σταθμίσετε τους κινδύνουν που εγείρει η διαχείριση κρυπτογραφικών κλειδιών με τις δυνατότητες που υπάρχουν στο περιβάλλον του νέφους, καθώς και τις σχετικές διαδικασίες που έχει θεσπίσει ο πάροχος νέφους.

## Διαθεσιμότητα

Πρέπει να κατανοήσετε τις ρήτρες και διαδικασίες που προβλέπονται από τη σύμβαση για τη διαθεσιμότητα, τη λήψη αντιγράφων ασφαλείας, την ανάκτηση των δεδομένων, και την ανάκαμψη από καταστροφές, και να βεβαιωθείτε ότι ικανοποιούν τις απαιτήσεις του οργανισμού σας για επιχειρησιακή συνέχεια και εκπόνηση σχεδίων έκτατης ανάγκης.

Πρέπει να βεβαιωθείτε ότι οι κρίσιμες λειτουργίες θα συνεχίσουν να παρέχονται απρόσκοπτα κατά τη διάρκεια μιας σχετικά σύντομης ή παρατεταμένης διακοπής ή μιας σοβαρής καταστροφής, καθώς και ότι θα αποκατασταθούν τελικά όλες οι λειτουργίες εγκαίρως και με οργανωμένο τρόπο.

## Αντιμετώπιση περιστατικών

Πρέπει να κατανοήσετε τις ρήτρες και διαδικασίες που προβλέπονται από τη σύμβαση για την αντιμετώπιση περιστατικών, και να βεβαιωθείτε ότι ικανοποιούν τις απαιτήσεις του οργανισμού σας.

Πρέπει να βεβαιωθείτε ότι ο πάροχος νέφους έχει θεσπίσει μια διαφανή διαδικασία αντιμετώπισης και διαθέτει επαρκείς μηχανισμούς για τη γνωστοποίηση των σχετικών πληροφοριών κατά τη διάρκεια ενός περιστατικού ή μετά από αυτό.

Πρέπει να βεβαιωθείτε ότι ο οργανισμός σας μπορεί να αντιμετωπίζει περιστατικά σε συνεργασία με τον πάροχο νέφους και κατά τρόπο σύμφωνο με τους αντίστοιχους ρόλους και τις ανάλογες αρμοδιότητες που προβλέπονται στο υπολογιστικό περιβάλλον.

# Προστασία δεδομένων στο νέφος

Η απειλή της παραβίασης  
δεδομένων αυξάνεται στο νέφος

Κίνδυνοι και  
προκλήσεις  
μοναδικές  
για το νέφος

Αρχιτεκτονικά ή  
λειτουργικά  
χαρακτηριστικά  
του  
περιβάλλοντος  
του νέφους

## Μοντέλο πολλών στιγμιοτύπων

Παρέχει ένα μοναδικό  
DBMS που εκτελείται  
σε ένα στιγμιότυπο  
εικονικού μηχανήματος  
για κάθε συνδρομητή

Δίνει στον συνδρομητή  
τον πλήρη έλεγχο  
διαχειριστικών  
εργασιών που  
αφορούν την ασφάλεια

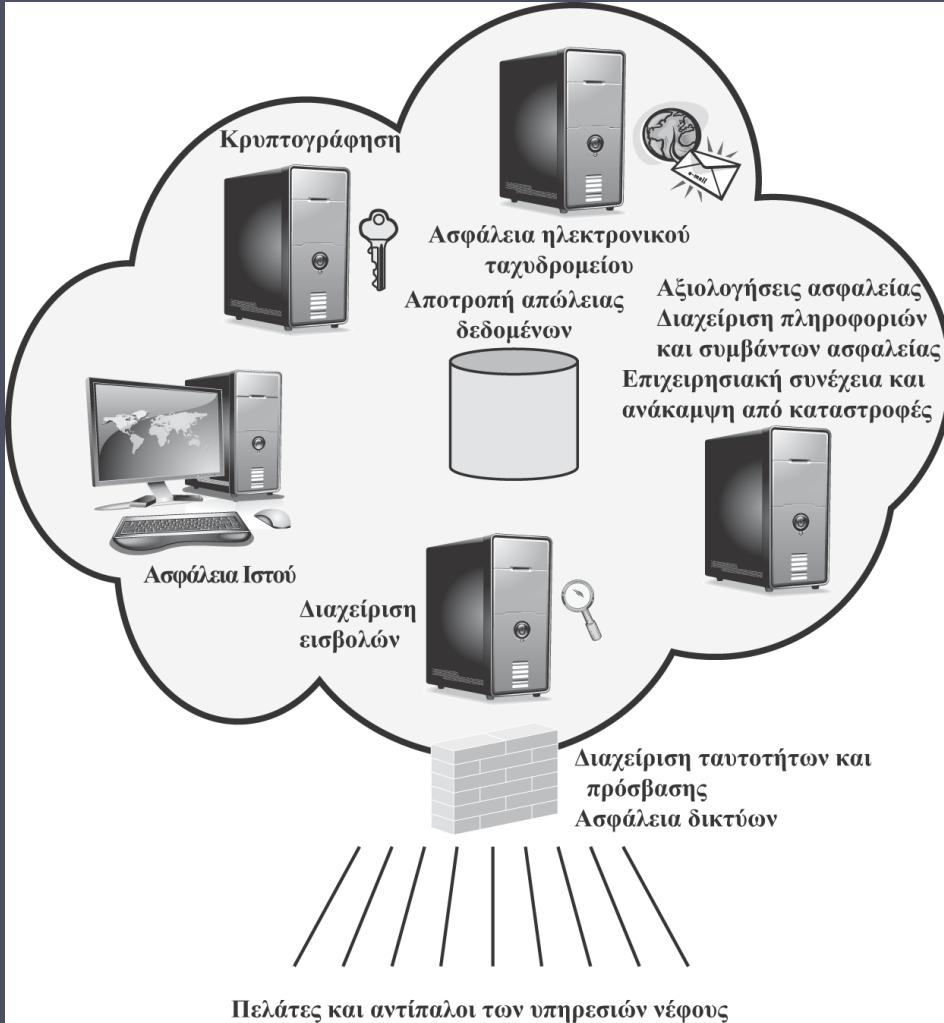
## Μοντέλο πολυμίσθωσης

Παρέχει προκαθορισμένο περιβάλλον  
για τον συνδρομητή, το οποίο  
χρησιμοποιείται από κοινού με άλλους  
συνδρομητές, συνήθως μέσω  
της ενσωμάτωσης στα δεδομένα  
ετικετών που περιέχουν ένα  
αναγνωριστικό συνδρομητή

Δίνει την εντύπωση αποκλειστικής  
χρήσης του στιγμιοτύπου, αλλά η  
δημιουργία και διατήρηση ενός σωστού  
και ασφαλούς περιβάλλοντος βάσεων  
δεδομένων εξαρτάται αποκλειστικά  
από τον πάροχο νέφους

# Ασφάλεια νέφους υπό μορφή υπηρεσίας

- SecaaS
- Αποτελεί τμήμα του λογισμικού υπό μορφή υπηρεσίας (SaaS) που προσφέρεται από έναν πάροχο νέφους
- Ορίζεται από τον Συνασπισμό Ασφάλειας Νέφους ως «η παροχή εφαρμογών και υπηρεσιών ασφαλείας μέσω του νέφους, είτε προς υποδομές και λογισμικό που βασίζονται στο νέφος είτε από το ίδιο το νέφος προς συστήματα που βρίσκονται στις εγκαταστάσεις του πελάτη».



Εικόνα 5.15 Στοιχεία της ασφάλειας νέφους υπό μορφή υπηρεσίας

# Σύνοψη

- Η ανάγκη για την ασφάλεια βάσεων δεδομένων
- Συστήματα διαχείρισης βάσεων δεδομένων
- Σχεσιακές βάσεις δεδομένων
  - Στοιχεία ενός συστήματος σχεσιακής βάσης δεδομένων
  - Δομημένη γλώσσα ερωτημάτων
- Επιθέσεις εισαγωγής εντολών SQL
  - Μια τυπική επίθεση SQLi
  - Η τεχνική εισαγωγής εντολών
  - Τρόποι και τύποι επιθέσεων SQLi
  - Αντίμετρα για επιθέσεις SQLi
- Συμπερασμός
- Έλεγχος πρόσβασης σε βάσεις δεδομένων
  - Ορισμός πρόσβασης βασισμένος σε SQL
  - Στοιβαγμένες εξουσιοδοτήσεις
  - Έλεγχος πρόσβασης βασισμένος σε ρόλους
- Κρυπτογράφηση βάσεων δεδομένων
- Υπολογιστική νέφους
  - Στοιχεία της υπολογιστικής νέφους
  - Αρχιτεκτονική αναφοράς της υπολογιστικής νέφους
- Κίνδυνοι της ασφάλειας νέφους και αντίμετρα
- Προστασία δεδομένων στο νέφος
- Ασφάλεια νέφους υπό μορφή υπηρεσίας

