Облачни Технологии и Архитектури

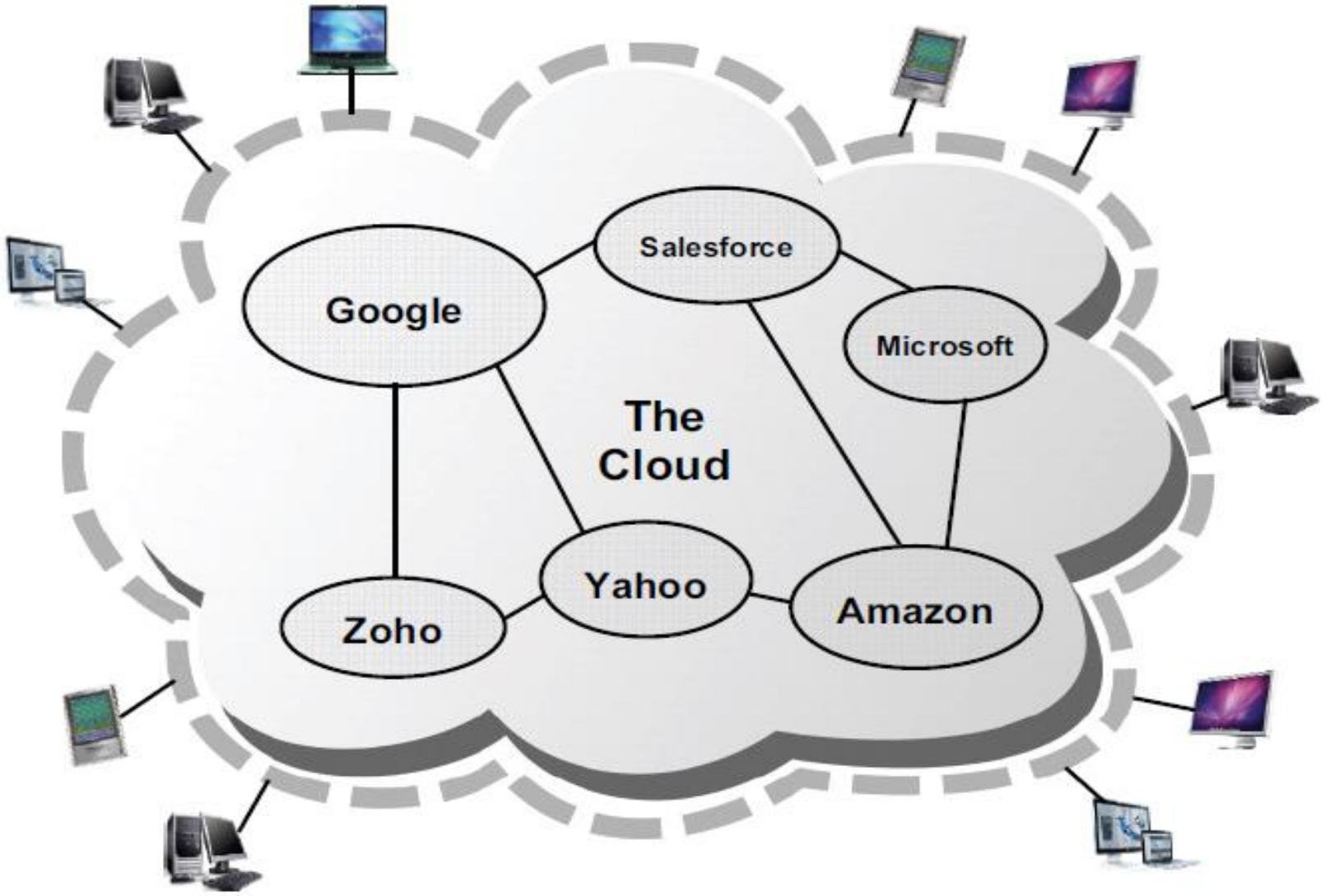
Сигурност в Облака

Гл.ас. д-р Галя Новакова
Софийски Университет
ФМИ

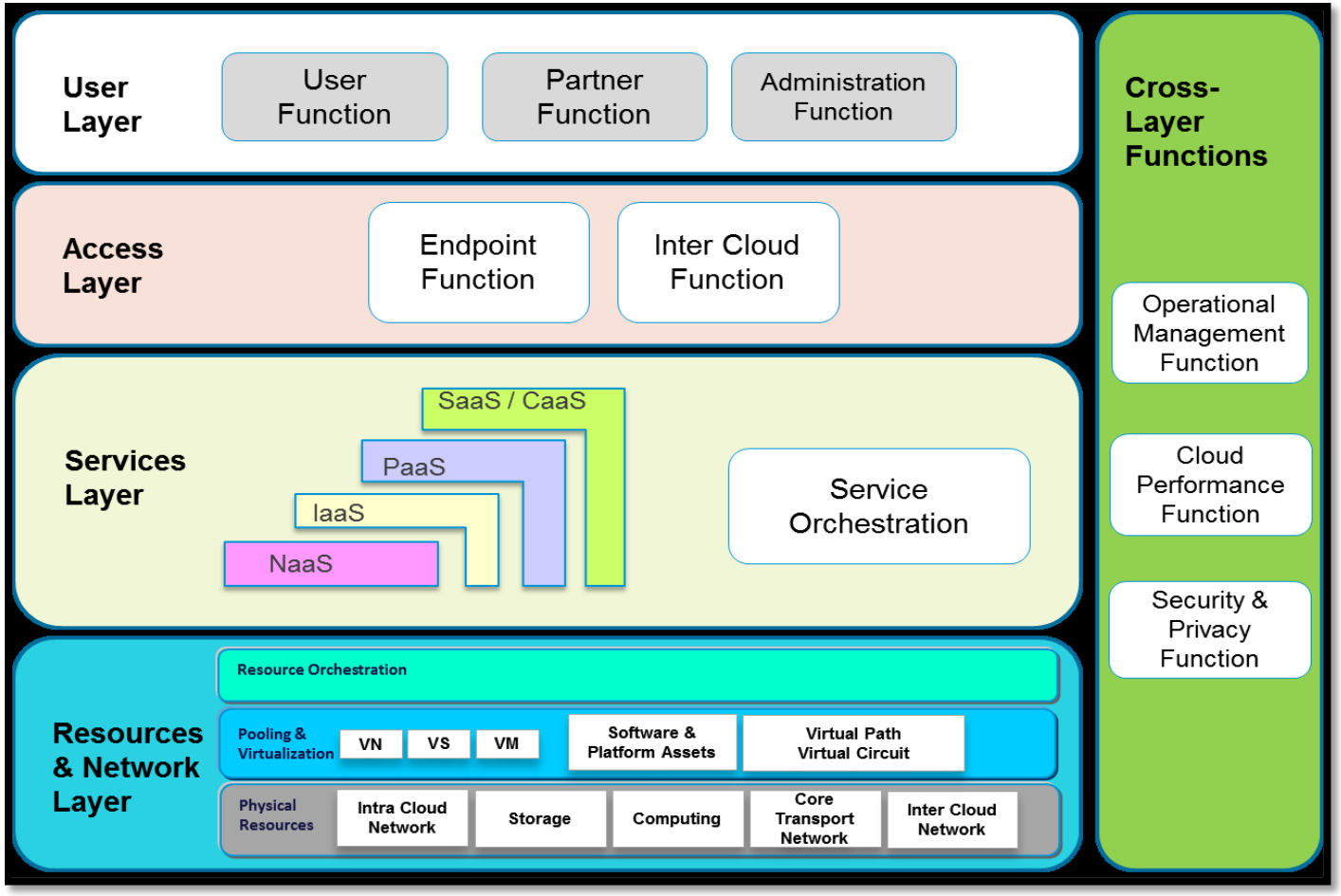
Съдържание

- Сигурността в Облака
- Облачни услуги и сигурността на данните

Логическа диаграма на Облака



Логическа диаграма на Облака



Рискове, които идентифицира потребителя

- Загуба на управление (Loss of Governance)
- Загуба на доверие (Loss of Trust)
- Несигурен достъп до облачните услуги (Unsecure Cloud Service User Access)
- Липса на информираност (Lack of Information/Asset Management)
- Загуба и изтичане на данни (Data loss and leakage)

Рискове, които идентифицира доставчикът

- Protection Inconsistency
- Evolutional Risks
- Business Discontinuity
- License Risks
- Bad Integration
- Unsecure Administration API
- Shared Environment
- Hypervisor Isolation Failure
- Data Unreliability
- Abuse Right of Cloud Service Provider

Контролите се разделят на следните категории

- Възспиращи (Deterrent)
- Превантивни (Preventive)
- Откриващи (Detective)
- Коригиращи (Corrective)

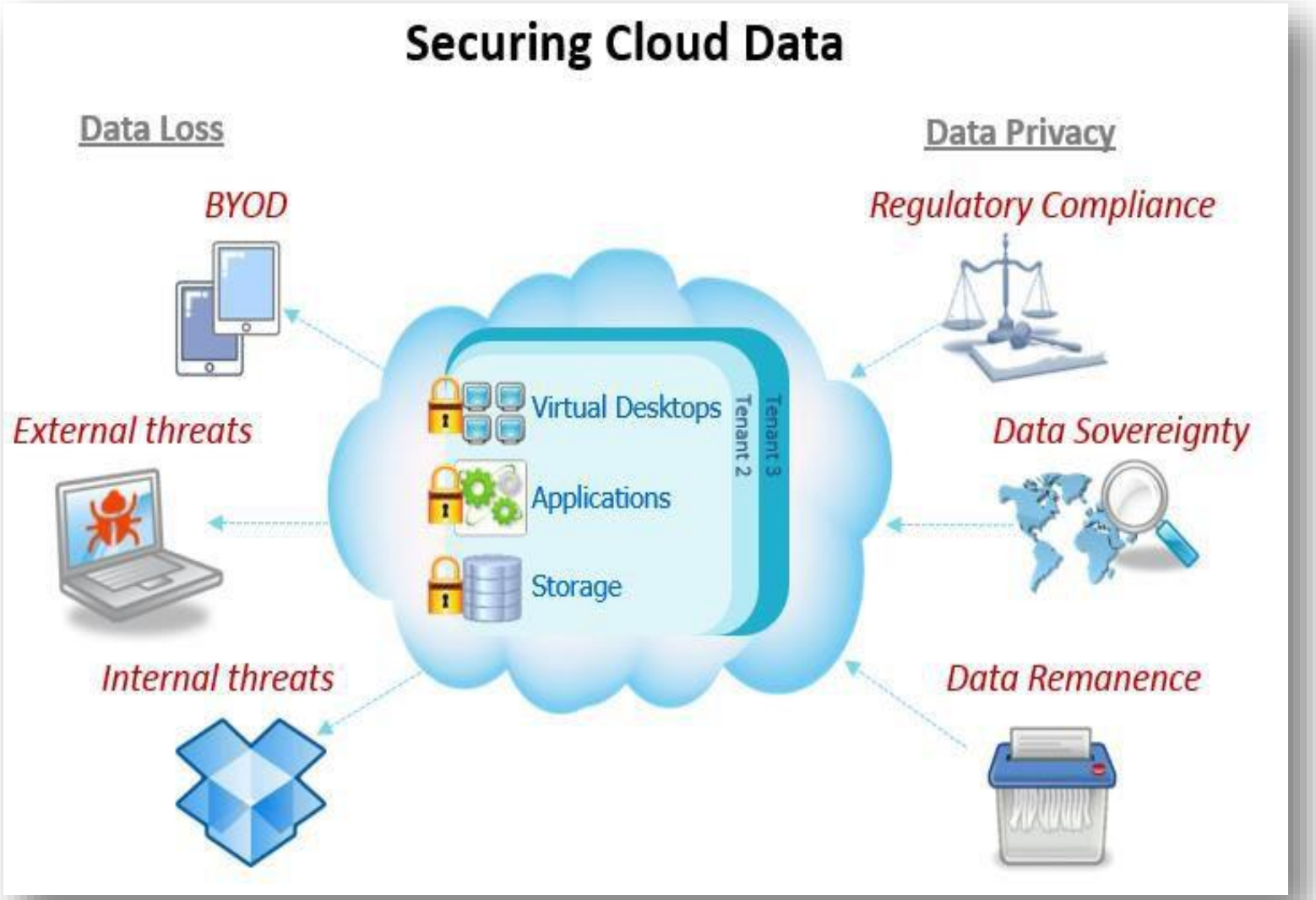
Сигурност и поверителност

- Управление на идентичността (Identity management)
- Сигурност на хардуера (Physical security)
- Поверителност (Privacy)
- Загуба на управление (Loss of Governance)
- Hyper jacking

Защита на данните

- Конфиденциалност (Confidentiality)
- Контролиране на достъпа (Access controllability)
- Достъпност (Availability)
- Интегритет (Integrity)

Защита на данните



Примери от практиката

- Microsoft - Наличието на проблем позволил на неоторизирани потребители да достъпят информация за контактите на служител в техния offline указател.
- Dropbox – откраднати данни на 68 милиона потребители, включително емайли и пароли, представляващи почти 5 GB данни.
- National Electoral Institute of Mexico - 93 милиона записи от регистации на гласоподаватели са компроментирани. Повечето от записите били изгубени. Данните били съхранявани на небезопасна, нелегална облачна сървър на Amazon извън Мексико.

Примери от практиката

- LinkedIn - 6 милиона потребители били откраднати и публикувани в руски форум. 167 милиона емайл адреси и пароли от LinkedIn били обявени за продан в dark web.
- Apple iCloud
- Yahoo - 1 милиард акаунта са компроментирани. Откраднатите данни включват имена, имейли, дати на раждане и въпрос и отговор на таен въпрос.

Инструменти за обезопасяване на виртуални машини

- Защитна стена (firewall)
- IPS (Intrusion prevention solution): Инструменти за проверка на целостта на данните
- Антивирусна защита

Сигурността като услуга

Основни характеристики на сигурността като услуга

- Гарантираност
- Постоянност
- Надеждност на доставчика
- Поверителност
- Интегритет
- Наличност

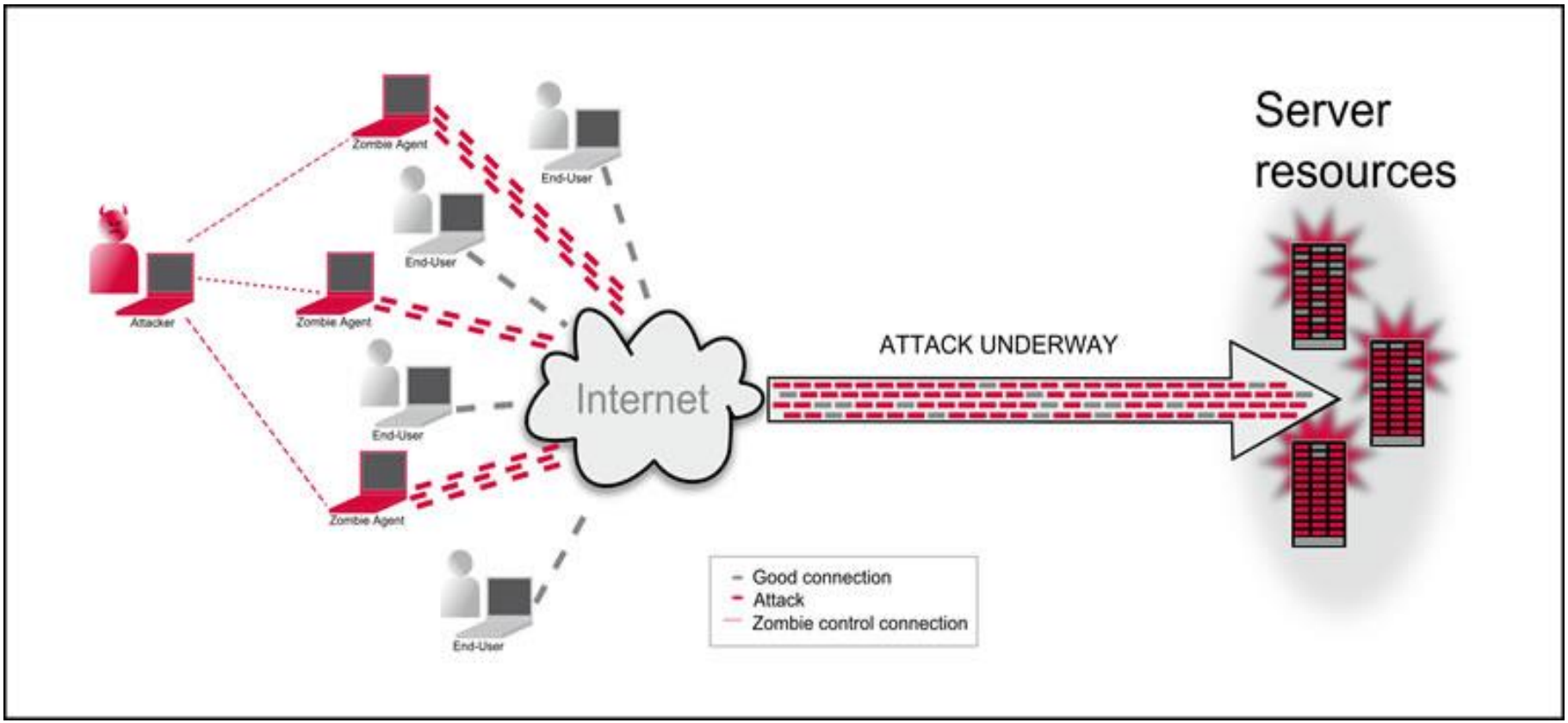
Видове атаки в Облака

- Denial of Service (DoS) attacks
- Side Channel attacks
- Authentication attacks
- Man-in-the-middle cryptographic attacks
- Inside-job

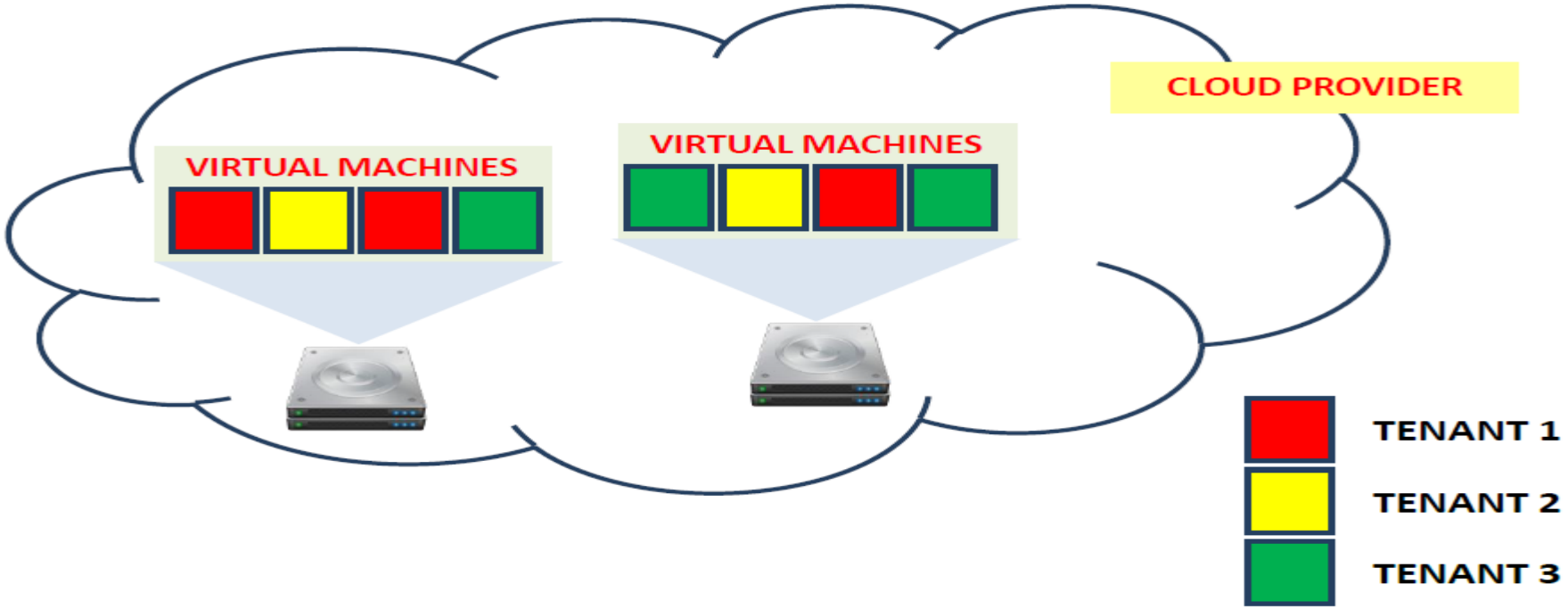
Видове атаки в Облака

- Denial of Service (DoS) attacks
- Side Channel attacks
- Authentication attacks
- Man-in-the-middle cryptographic attacks
- Inside-job

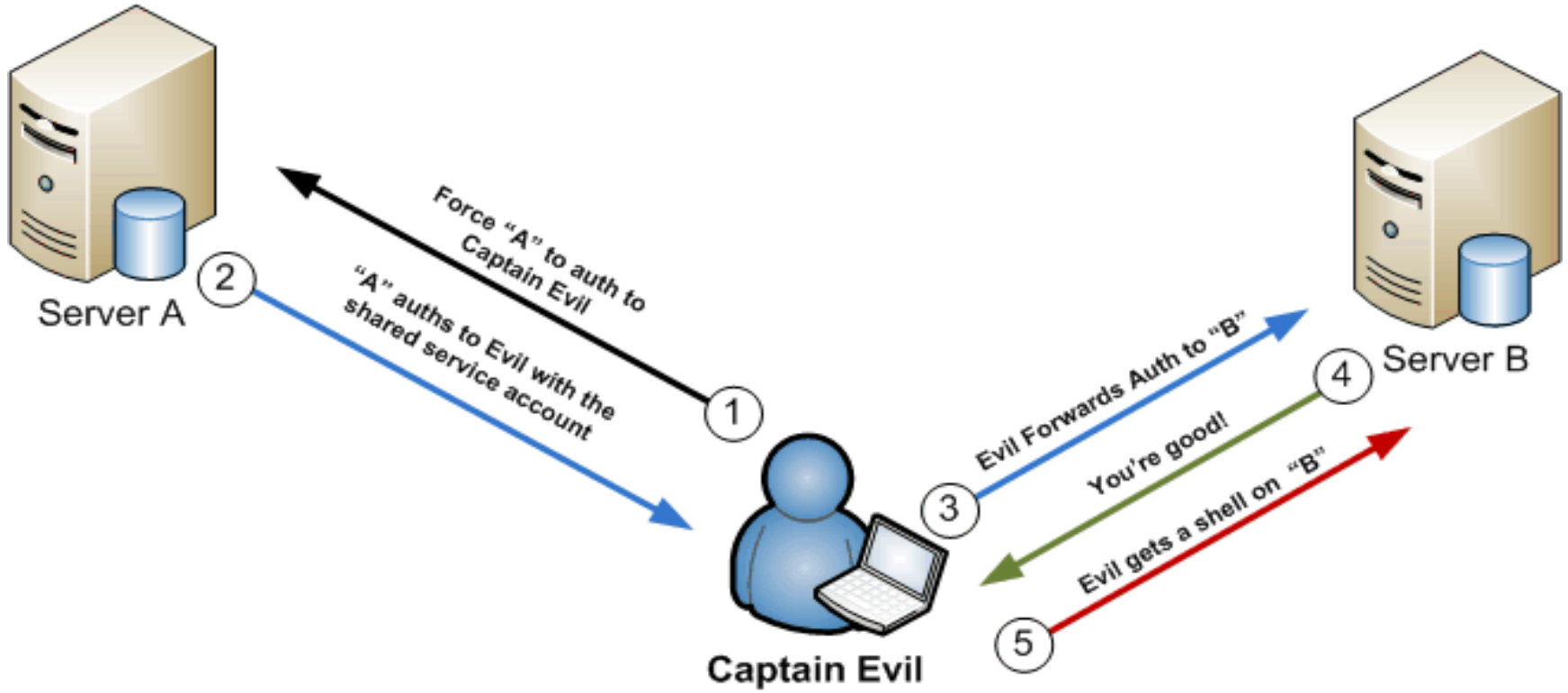
Denial of Service (DOS) attacks



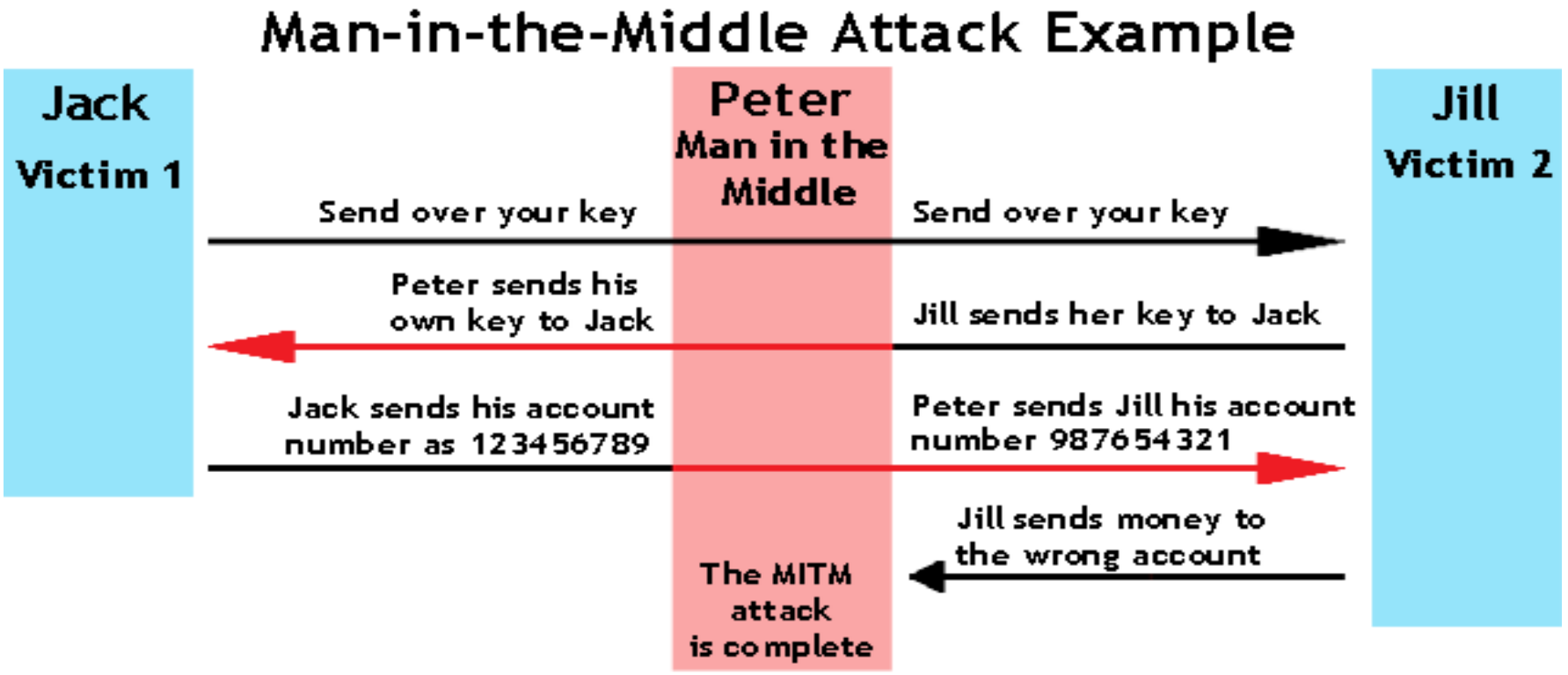
Side Channel Attacks



Authentication Attacks



Man-in-the-Middle Cryptographic Attacks



In-side-job

If cloud computing is so great, whyisn't everyone using it?

Clouds are still subject to traditional data confidentiality, integrity, availability, and privacy issues, plus some additional attacks

Опорни услуги на сигурността

- Идентификация (присвояване на име) – еднозначна идентификация на обектите и субектите на информационно взаимодействие.
- Управление на криптографски ключове – съвкупност от методи и процедури, осъществяващи определение и управление на криптографски ключове, използвани от оторизирани обекти.
- Администриране на сигурността – управление и разпространение на информация, необходима за реализиране на различните услуги за сигурност.
- Защитеност на системата – съвкупност от свойства на системата, които осигуряват доверие в техническата ѝ реализация.

Услуги за откриване и възстановяване

- Одит на сигурността – откриване на събития, оказващи влияние на сигурността на системата.
- Откриване на произшествия – услугата е насочена както към откриване на опити за нарушаване на сигурността, така и към регистриране на легитимната активност на потребителите.
- Контрол на целостта- своевременно откриване на нарушения на цялостта на програмната, апаратната и информационна част на ИТ системата.
- Възстановяване на сигурността – изпълнява функция на реакция на системата при нарушаване на сигурността.

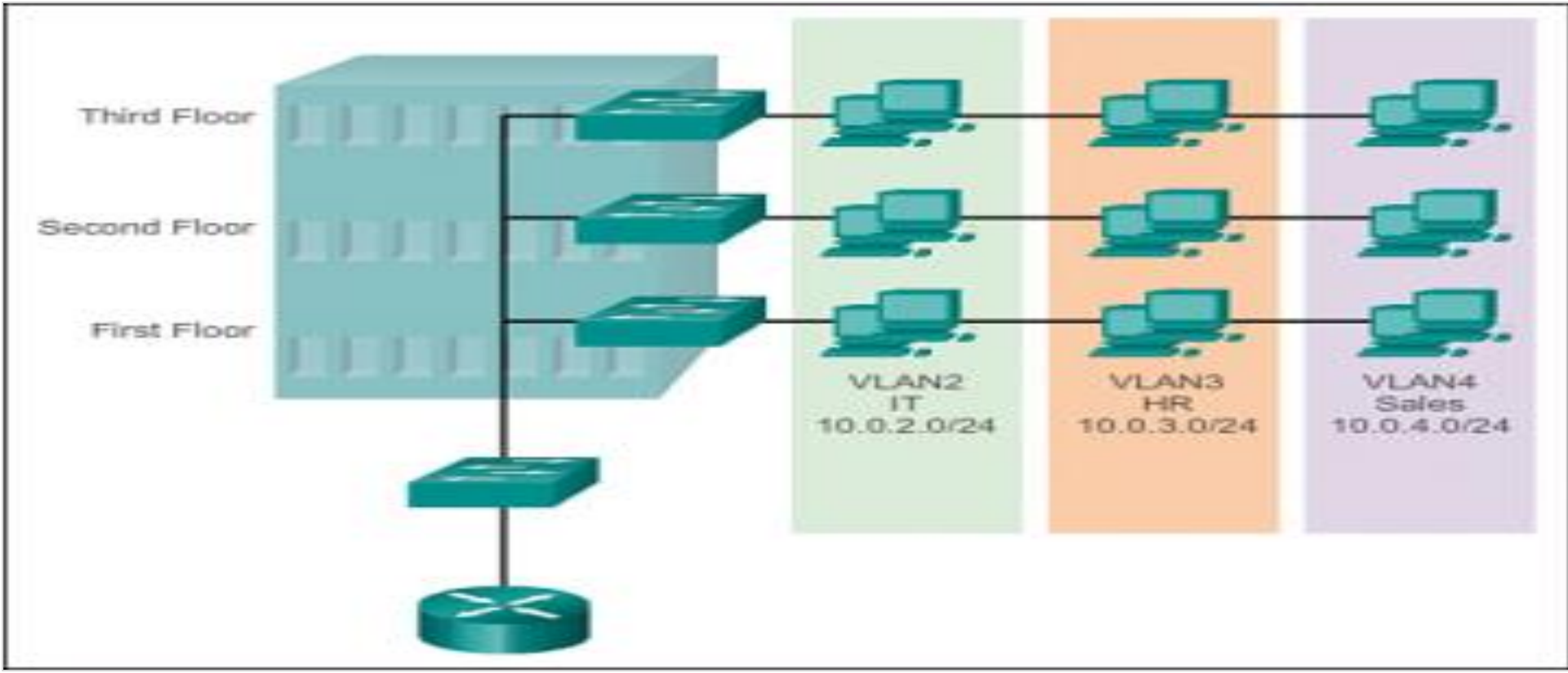
Облачни услуги и сигурността

- Неправомерно използване на облачни услуги
- Незащитени API
- Действия на сътрудниците на компанията, доставяща услугите
- Уязвимости на споделяната среда
- Загуба или кражба на данни
- Кражба на акаунти
- Неизвестни и неидентифицирани рискове

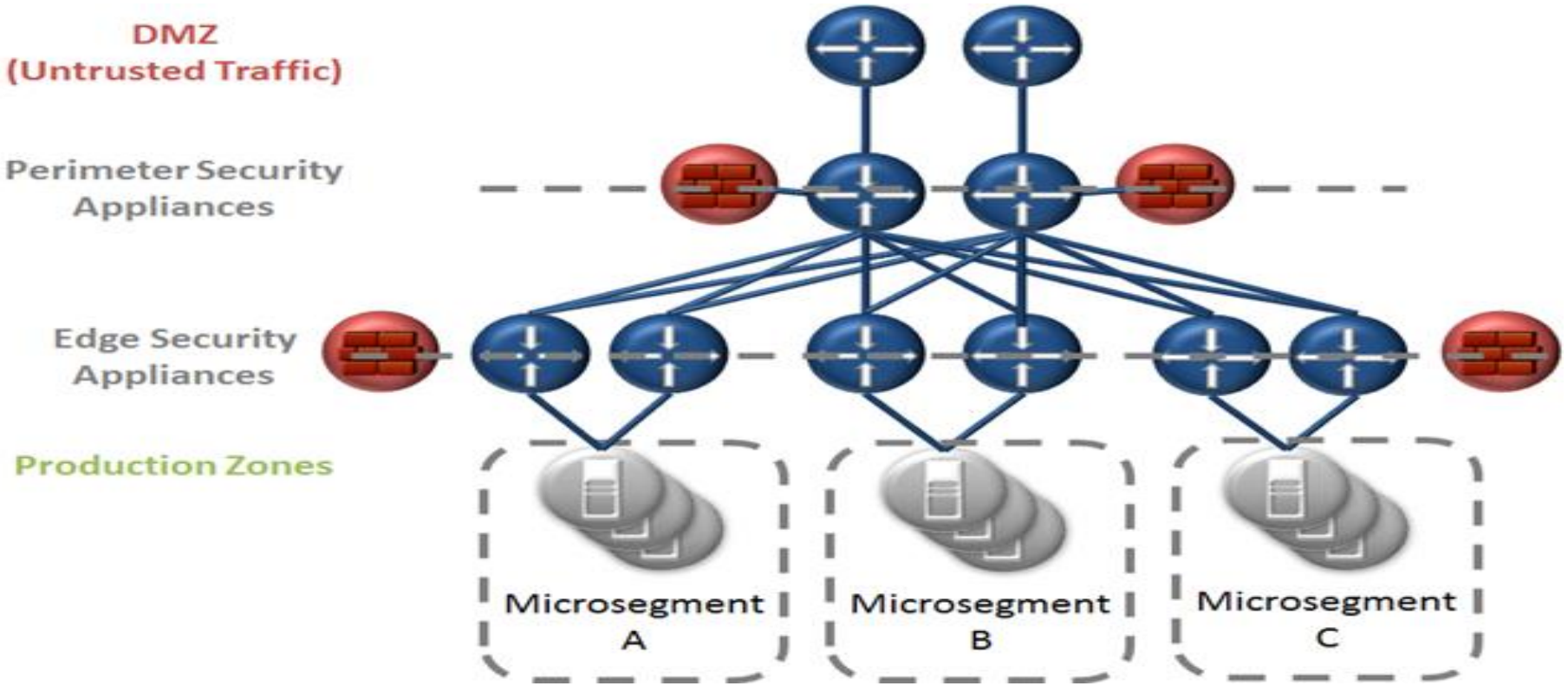
VLAN Сегментация

- VLAN позволява на администратора да сегментира мрежи, основани на фактори като функционалност, проектов отбор или приложение, без да се интересува от физическото местоположение на потребителя или устройството

VLAN Сегментация



Микро Сегментация



Пробиви на сигурността в Облака

- Epsilon - Този провайдър на облачни услуги беше жертва на хакерска атака към края на март 2012 г.
- Dropbox - базиран на облачната Amazon S3 услуга за съхранение, Dropbox беше успешно атакуван през юли 2012 г.
- iCloud - iCloud акаунтът на журналиста на Wired Matt Honan беше хакнат след като с помощта на социално инженерство е била взета паролата му от персонала по поддръжката на Apple.

Пробиви на сигурността в Облака

- CloudFlare - посредством многослоева crack атака, провайдърът на облачни услуги за сигурност CloudFlare беше атакуван през май 2012 г.
- Playstation Network - След като данните на над 100 милиона клиенти бяха компрометирани, Sony беше поставен между чука и наковалнята през април 2011 г.

Заключение

- Защитата и безопасността в Cloud computing е комплексна задача, изискваща много усилия и компетентност в Облачните технологии.
- Основната цел е сигурността на данните, която включва тяхната достъпност, достоверност и поверителност.
- Защитата на данните обаче не се ограничава само до тяхната сигурност, а включва и прозрачност, изолация, възможност за интервенция и преносимост.
- Всичко това е в подкрепа на правото на лицата на защита на техните данни.

Cloud Computing and Technologies

Q & A