Безопасность «облачных» технологий

Выполнила:
Мангыр Диана
Проверил:
Тренькаев В.Н.

Сервисы облачного хранения данных

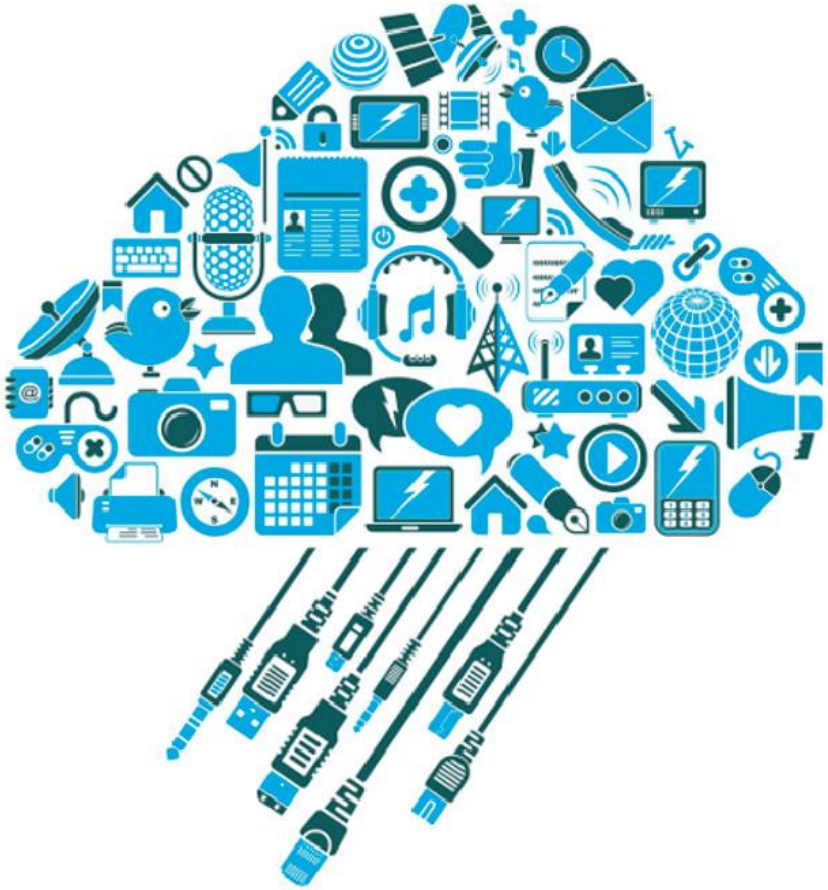
Облачное хранилище и его многогранное использование

Blockchain


BLOCKCHAIN
VERIFIED
ADDRESS
WALLET
ICO
NETWORK
TRUST
TRANSACTION
CRYPTOCURRENCY
MINING
%
SMART CONTRACTS

Internet of Things

Виртуализация данных



Гибридные облачные решения

При переходе в облако важно, чтобы предприятия понимали:

- хотя облачные провайдеры и несут ответственность за защиту облака, только предприятия могут обеспечить безопасность при использовании облака.
- Для этого требуется выработать новый подход к безопасности. Попытка просто взять и применить привычный локальный стек безопасности обречена на провал.

Защита на уровне платформы

- Классические антивирусные технологии были нацелены в первую очередь на защиту рабочих мест, ПК
- Основной целью хакеров теперь являются гибридные ЦОД, а не отдельные ПК и почтовые рассылки
- Существенно выросла база сигнатур и ее размер влияет на производительность ПК
- Ресурс физических серверов ограничен и делится между ВМ.

Русский международный банк раскрыл в своей отчетности, что 21 января 2016 г. на него была совершена хакерская атака, в результате которой с корсчета банка в ЦБ было похищено 508 млн руб

- 29 февраля 2016 г. хакеры вывели с корсчета Металлинвестбанка в ЦБ 667 млн руб.
- Международная группировка хакеров Carbanak похитила со счетов клиентов 100 банков и других финансовых институтов в 30 странах мира $300-900 млн.
- В США хакеры украли данные о пластиковых картах почти 70 миллионов клиентов у американской розничной сети Target, и банкам пришлось потратить $200 млн на их перевыпуск

- Многие вирусы и злоумышленники стараются блокировать работу агента защиты в ВМ
- Базы сигнатур и антивирусный агент потребляют большой объем ресурсов ВМ и сети , приводя к понижению производительности хоста и скорости обмена
- При инфицировании одной или нескольких ВМ на хосте или одновременном сканировании повышается кол-во обращений к дискам, что приводит к антивирусному шторму и деградации производительности хоста.

Рекомендации ЦБ РФ по «Обеспечению информационной безопасности при использовании технологии виртуализации».

- Глава 9 «Рекомендации по обеспечению ИБ виртуальных машин» : 9.6. «Рекомендуемым решением является использование средств защиты от воздействия вредоносного кода на уровне гипервизора без установки агентского ПО на виртуальные машины.»

Новые подходы к защите

- Многоуровневая защита:, межсетевой экран, антивирус, система обнаружения вторжений в едином решении

- Аутентификация - облачные сервисы двухфакторной аутентификации SafeNet.
- Шифрование данных

- Простота управления и интеграция в средства управления инфраструктурой
- Защита базируется на сервере, а не АРМ пользователя

- СЗИ максимально интегрировано в ОС, что позволяет использовать все ее возможности, ускорить работу приложения, уменьшить потребляемый ресурс, повысить эффективность вложений в новые технологии. Современные технологии СЗИ позволяют экономить до 30% ресурсов сервера и работают до 70 раз быстрее классических.
- Безагентный способ защиты, не зависящий от действий пользователя и его гостевой ОС.

Повышение безопасности виртуальной среды при помощи безагентных СЗИ

- Защищают от новых угроз в виртуальной среде, таких как атаки внутри виртуальной среды
- Уменьшают влияние персонала или пользователей на безопасность.
- Понижают трудоемкость обеспечения безопасности: нет необходимости проверять и обновлять сигнатуры на каждой ВМ. Эти процедуры автоматически выполняются на хосте.
- Улучшается гибкость и масштабирование в динамичной виртуальной среде (создание, удаление ВМ , миграция)
- Предотвращаются «антивирусные штормы», проблемы с сетью и падение производительности хоста
- Инкрементальная технология сканирования 5nine позволяет экономить ресурсы сервера, что позволяет выделить больше ресурсов для клиентских ВМ и приложений

Спасибо за внимание!