

Риски для информационной безопасности облачных сред и виртуальной инфраструктуры

 Нуйкин Андрей

 05.2021

Все сервисы внутри периметра

Польный контроль доступа

Понятные средства защиты

Контроль и мониторинг ресурсов

Где расположен сервис?

Как защищать ресурсы?

Где мой периметр?

Кто имеет доступ?

По данным опроса PWC компании в РФ идут в облака медленно, но верно.

Основными преимуществами называются:

- Масштабируемость по мере необходимости (74%)
- Оптимизация затрат (67%)
- Доступ к недоступным локально технологиям (48%)



Безопасности здесь нет.

Основными факторами для перехода в облако являются следующие:

- Наличие надежных каналов связи, современных средств защиты от DDoS-атак (41%)
- Наличие дата-центров в России (38%)
- Низкая цена, понятное и гибкое ценообразование (34%)



И здесь безопасности нет.

Безопасность особо не интересует.

При этом 58% считают облака небезопасными

Примеры рисков:

- НСД к данным со стороны третьих лиц

Провайдер может иметь доступ к данным, бэкдоры для спецслужб, и т.д.

- НСД при управлении сервисом (разграничение доступа, контроль доступа и т.д.

Как организован доступ к консоли из Интернет, кто имеет доступ и т.д.

- Утечки данных

Причинами могут быть риски выше

- Риск потери доступа к данным по разным причинам (например, санкции)

Если облако не в РФ могут закрыть доступ. Причем как зарубежные «партнеры», так и российские.

- Недостаточные меры защиты со стороны провайдера
Сделал ли провайдер все для защиты или экономил
- Неправильная настройка облачных сервисов
При слабом процессе управления доступом и полномочиями возможна ситуация при которой настройки делаются без учета требований ИБ
- Нарушение изолирования между клиентами облачного провайдера
Насколько качественно провайдер разграничивает доступы к средам клиентов
- Несоответствие требованиям законодательства
Насколько провайдер соответствует требованиям законодательства (например, ФЗ №152)

- **Динамичность виртуальных машин**

В облаке легко создать новые виртуальные машины. И ИБ не всегда успевает за этим.

- **Уязвимости виртуальной среды**

Серверы облачных вычислений и локальные серверы используют одни и те же операционные системы и приложения. Система обнаружения и предотвращения вторжений должна быть способна обнаруживать вредоносную активность на уровне виртуальных машин, вне зависимости от их расположения в облачной среде.

- **Периметр сети размывается**

При использовании облачных вычислений периметр сети размывается или исчезает. Это приводит к тому, что защита менее защищенной части сети определяет общий уровень защищенности.

- **Процессы разграничения и контроля доступа**

Доступ через Интернет к управлению вычислительной мощностью одна из ключевых характеристик облачных вычислений. В большинстве традиционных ЦОД доступ инженеров к серверам контролируется на физическом уровне, в облачных средах они работают через Интернет. Разграничение контроля доступа и обеспечение прозрачности изменений на системном уровне является одним из главных критериев защиты.

- **Настройки корпоративных средств защиты**

Настройки должны быть приближены к корпоративным, но из-за динамичности среды не всегда соблюдается.

Спасибо за внимание



+7(495) 363-19-60



Andrey.nuykin@evraz.com



www.evraz.com

