АНАЛИЗ ПРОБЛЕМ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ ГИБРИДНОЙ ОБЛАЧНОЙ АРХИТЕКТУРЫ

Ермошкин Григорий Николаевич
Финансовый университет при Правительстве РФ, Москва, аспирант
ermoshkin_nn@mail.ru

Аннотация. В статье будет проведен анализ гибридных систем и освещены их проблемы и достоинства, предпринята попытка разрешить часть вопросов в данной сфере.

Ключевые слова: информационная безопасность, гибридная облачная архитектура, оценка рисков.

Введение

Все больше организаций выбирают облачные системы. И беря в учет преимущества этих систем это вполне понятно. Однако любая такая система имеет ряд врожденных недостатков, способных перевесить все достоинства.

Основными рисками можно считать потерю контроля, недостаток безопасности, доступности данных, а так же вероятные финансовые потери которые это может повлечь.

Использование частного облака способно решить большинство проблем, но его развертывание и обслуживание дорого стоит. Публичное облако намного экономичней в короткой перспективе, но влечет за собой высокие риски. Гибридное облако потенциально способно разрешить данное противоречие. Но, к сожалению, здесь следует отметить недостаток изученности данных систем и отсутствие достаточной информации для построения системы способной сбалансировать преимущества и риски.

В данной статье предпринята попытка разрешить часть вопросов в данной сфере. Будет проведен анализ гибридных систем и освещены проблемы и достоинства.

Гибридная архитектура содержит две основных части: частную и публичную. Каждая из них имеет достоинства и недостатки. Достоинства и недостатки гибридных систем можно представить в двух измерениях: наследственные и уникальные. Наследственные преимущества и риски происходят напрямую из частного и публичного сегментов. Уникальные происходят из особенностей комбинации этих двух частей. Большинство наследственных преимуществ связанны с частным облаком; в то же время основные риски проистекают от публичного облака.

Основным преимуществом гибридного облака является возможность сбалансировать наследственные достоинства и риски, относительная простота и скорость развертывания.

Важнейшие риски это безопасность, разрозненный контроль и настройка, доступность и законодательные аспекты.

Правильная стратегия применения гибридной модели направлена на максимизацию преимуществ и минимизацию рисков, эффективное поддержание и улучшение баланса на протяжении жизненного цикла – в соответствии с состоянием организации.

Провайдеры публичных облачных вычислений указывают на достоинства, такие как скорость и простота развертывания. Однако забывают упомянуть риски связанные с использованием этой модели. Проблемы безопасности, потеря контроля, недостаток производительности, доступность и законодательные аспекты. Хотя, гибридная модель подразумевает баланс между рисками и преимуществами, организация должна быть осторожна в принятии этой модели, тщательно оценив свое положение.

Понимание основных особенностей модели позволяет принять правильное решение и эффективно управлять рисками.

Облачная модель предоставляет услуги информационных технологий по требованию через сеть. Частное облако представляет модель, в которой сетевая инфраструктура и услуги являются собственностью организации и распространяются внутри. Это наиболее удачный вариант, но требующий наибольших начальных вложений. Публичное облако является точной противоположностью. В данной модели услуги и поддерживающая их инфраструктура находятся во владении внешнего провайдера. Доступ к сервисам осуществляется через интернет. Но, при всех недостатках эта модель достаточно экономична – в короткой перспективе (например, как временное решение перед переходом к частному облаку).

В гибридном облаке часть сервисов находится внутри организации, в то время как другая часть располагается у внешнего провайдера. Внутренние

сервисы доступны через внутреннюю сеть организации, внешние - через внешнюю сеть, например интернет. Пользователь обычно взаимодействует с внешними сервисами через web интерфейс.

1. Преимущества использования гибридных облаков

Большинство преимуществ являются наследованными от частного облака. Однако публичные облака также имеют ряд достоинств.

Список преимуществ гибридных систем:

- Сбалансированность: данная модель имеет потенциальную возможность достигнуть баланса между риском и достоинствами. Менеджеры должны принимать положительные особенности и минимизировать недостатки.
- Подобие: Принятие облачной модели подобно аутсорсингу. Это одинаково верно и для частного, и для публичного облаков, т.о., менеджеры способны использовать существующий опыт для быстрого перехода.
- Скорость: Облачная архитектура и сервисы могут быть развернуты относительно быстро. Публичное облако специально создано для быстрого развертывания. Существует ряд готовых решений частных облаков.
- Простота: Облачные сервисы могут быть развернуты без особых затрат. Принятие нового готового к использованию облачного решения просто. Это, однако, не касается переноса сервисов.
- Снижение расходов.
- Масштабируемость: ресурсы могут, масштабированы в зависимости от потребностей.
- Оплата: пользователь платит лишь за ресурсы, которые потребляет.

2. Риски использования гибридных облаков

Следует учитывать следующие риски гибридных облачных систем:

- Неверный баланс: неправильное соотношение частей способно повлечь различные риски.
- Потеря контроля: поддержание контроля данных и сервисов крайне важно. Полный контроль возможен лишь в частном сегменте.
- Ограниченная настройка: потеря контроля означает ограниченность или невозможность настройки.
- Безопасность: Открытость публичного облака ведет к серьезным проблемам безопасности. Ценные данные могут быть скомпромитированны.

- Доступность: сетевая природа сервисов приводит к риску потери доступа, что может привести к остановке работы организации.
- Законность: т.к. публичное облако физически может находиться в любой точке мира, то данные могут оказаться в регионе без законодательной защиты.

Заключение

Результаты проведенного в работе анализа могут быть использованы при разработке модели оценки рисков распределенных систем облачной архитектуры, которую можно будет использовать в ходе аудита информационной безопасности для повышения эффективности процедур менеджмента риска облачных систем.

Список источников

1. "Risk Management in Cloud Computing" By Sri Prakash, Technology Risk Management Consultant, E-Com Canada Inc. Fri, April 15, 2011.

2. "The future of IT outsourcing and cloud computing" PwC study, November, 2011.

3. http://csrc.nist.gov/groups/SNS/cloud-computing/

4. Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, Joint Task Force Transformation Initiative, NIST Special Publication 800-37, Revision 1, <URL:http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-l.pdf>.

5. Steve Elky. An Introduction to Information System Risk Management -SANS Institute, 2007.