

ОБЛАЧНЫЕ ТЕХНОЛОГИИ

Рассмотрены основные проблемы облачных технологий связанные с конфиденциальностью информации размещенной в хранилище. Предложены несколько рекомендаций по защите персональных данных.

С появлением таких мощных и надежных «облачных» технологий (cloud technologies), появились такие сервисы: программное обеспечение как услуга (англ. Software as a Service, SaaS), платформа как услуга (англ. Platform as a Service, PaaS), инфраструктура как услуга (англ. Infrastructure as a Service, IaaS) [2]. Предполагалось, что они займут лидирующее место на рынке в 2011 году. Однако недавно проведенное исследование компанией PEER 1 показало, что из 88% респондентов, которые не используют эти технологии, 39% высказали мнение, что не применяли облачные технологии, потому что не владели достаточной информацией о них.

Суть данной технологии заключается в том, что облачные вычисления дают возможность хранить файлы и программное обеспечение удаленно, а не на жестком диске или сервере. Многие из нас уже пользуются этими технологиями и даже не подозревают об этом, будь то по работе или в личных целях. Примерами служат веб-почта, такая как Gmail и Hotmail, средства связи, такие как Skype, видеосайты, такие как YouTube и Vimeo и т.д.

Благодаря тому, что облачные вычисления включают программное обеспечение как услугу (SaaS), хранение файлов, синхронизацию файлов данных и файлов резервного копирования, многие предприятия могут иметь свои собственные частные «Облака», которые включают в себя конкретные услуги и доступ к ним возможен только для ограниченного числа людей.

Одна из причин, по которой многие предприятия применяют облачные вычисления – затруднение изменения и уничтожения их данных. Однако существуют некоторые потенциальные недостатки облачных вычислений, которые стоит иметь в виду. Обратная сторона в том, что многие обеспокоены вопросами безопасности, связанными с хранением своих данных в Сети.

Недавний инцидент, произошедший с «облачным» хранилищем Dropbox, заставляет все больше задумываться о конфиденциальности информации [1]. Данные (изображения, документы) 15-ти млн. пользователей можно было просмотреть любому желающему.

Некоторые эксперты утверждают, что облачные вычисления более безопасны, чем традиционные методы, но предприятия по-прежнему беспокоятся, что злоумышленники, могут обойти защиту системы и получить доступ к конфиденциальным данным. Исследование, проведенное IDC (International Data Corporation — компания занимающаяся аналитикой) в 2011 году, показало, что безопасность была главной темой для беспокойства. Тем не менее, стоит взвешивать риски и помнить, что традиционные серверы также могут быть взломаны, а жесткие диски могут выйти из строя.

Еще одной проблемой для пользователей и компаний, становится потеря подключения к Internet. Риски, связанные с этим, в нашей стране являются актуальными, поскольку исправление неполадок в работоспособности системы занимает обычно от 3 до 5 дней и это, как правило, вызывает огромные простои на предприятиях и потерю финансовых средств. Предприятиям, которые реализованы с помощью облачных вычислений, необходимо предпринять меры, чтобы снизить риск каких либо сбоев в работе Internet и понизить скорость передачи информации.

Нужно учитывать, что облачная технология не может быть идеальна для всех сфер бизнеса. Это может быть выгодно только тем компаниям, для которых важным элементом является хранение больших объемов данных и их обработка лицензионным программным обеспечением удаленно. Прежде чем приступить к использованию «cloud technologies», необходимо взвесить все плюсы и минусы, попробовать использовать некоторые приложения, чтобы иметь наглядное представление, как они работают и нужно ли это предприятию, а потом постепенно внедрять и расширять их использование.

Как обеспечить защиту данных, размещенных в интернет-хранилище? На сегодня это является самой актуальной задачей и вот несколько простых мер безопасности.

Личная информация.

При использовании веб-сервисов указывайте только самые необходимые сведения. Поля, необязательные для заполнения оставляете пустыми.

Банковские карты.

Для совершения платежей в Сети пользуйтесь prepaid-картами или виртуальной картой Visa (такую услугу предлагает платежная система QIWI). Если даже злоумышленники завладеют данными, то даже в самом худшем случае они смогут воспользоваться только prepaid-картой номиналом, который должен быть самым минимальным.

Шифрование.

Используйте для своих фотографий и данных, помещенных в «облачное» хранилище, программу шифрования – например, FreewareBoxCryptor. Эта утилита работает в фоновом режиме и шифрует данные перед их отправкой в «облако». Для других сервисов применять утилиту TrueCrypt [1].

Главной проблемой этой технологии на сегодня является безопасность и от этого никуда не деться. Пока что, это новшество и все недостатки проявляются в огромных количествах. Всем хочется показать насколько «cloud technologies» уязвимы и небезопасны, но всему нужно время, чтобы устояться.

За данными технологиями будущее, поскольку будет возможность использовать все ресурсы, не боясь за целостность, доступность и конфиденциальность своих данных.

Перечень литературы:

1. Компьютерный журнал «CHIP» №10 октябрь 2011;
2. <http://kanobu.ru/blog/id177990> (Облачные вычисления).