Методы защиты информационных данных в облаках

Г. А. Шангытбаева
Казахский национальный технический университет имени К.И.Сатпаева,
г. Алматы, Республика Казахстан
gul_janet@mail.ru

Введение

Желание владельцев данных обезопасить свои информационные активы восходит к самым началам вхождения вычислительной техники в нашу жизнь. Подготовив колоду перфокарт с работающим кодом, программист тут же делал ее копию. И если при очередном прогоне ридер замял пару карт - не беда, есть резервная колода. Все ценные магнитные ленты имели дубликат, особо ценные - несколько дубликатов. Поскольку магнитный слой на ленте имел обыкновение со временем осыпаться, данные приходилось время от времени перезаписывать на новые ленты. Резервное копирование было обязательным, поскольку несовершенство технологий не давало расслабиться.

В мире облачных вычислений все еще сложнее, так как здесь «сторонняя организация» занимается поддержкой и управлением вашей инфраструктурой. Сама природа взаимоотношений предусматривает доступ поставщика этих услуг к вашим данным.

Если вы собираете и храните в облаке данные, которые подчиняются определенным нормативным актам, например закону об ответственности и переносе данных о страховании здоровья граждан (HIPAA) или закону Грэма-Лича-Блайли (GLBA), необходимо удостовериться, что поставщик облачных услуг надежно защищает ваши данные. Как и информация собранная внутри вашей организации, собранные в облаке данные должны использоваться только для тех целей, ради которых они были первоначально собраны. Если пользователь точно указал и разрешил только одну цель использования данных, нужно обеспечить выполнение этого требования.

Любая компания, действующая полностью или частично в Интернете, или частные лица, ведущие блоги в социальных сетях, хранят данные на одном или нескольких серверах, которые могут находиться где угодно. Размещаете ли вы личную информацию в Facebook или поддерживаете бизнес-связи в LinkedIn — все эти данные должны где-то храниться. Так как компании движутся ко все более тесному активному использованию услуг облачных сервис-поставщиков, в свете безопасности данных, правовых и нормативных запросов к ним, место расположения данных будет становиться все более значимым.

Глобальным компаниям необходимо обеспечить, чтобы любая служба, развернутая в облаке, использовалась в соответствии с законом и правовыми нормами, применимыми к сотрудникам, иностранным дочерним компаниям и сторонним организациям. Законы США могут заметно отличаться в разных штатах, так что если службой пользуются ваши сотрудники, но в другом регионе страны, следует обеспечивать выполнение законов, действующих на территории, где эти сотрудники находятся.

Для соблюдения всех этих законов и нормативов необходимо знать расположение основных данных и резервных копий. Часто, бывает необходимо определить место хранения резервных копий. Например, у Amazon.com Inc. есть большие центры данных в США и Ирландии, и при использовании их для хранения резервных копий данных некоторых типов данных могут возникать серьезные правовые проблемы.

Вы должны убедиться, что все поставщики облачных услуг, с которыми вы работаете и которые находятся вне вашей юрисдикции, обладают адекватными средствами безопасности. Сюда входит местоположение основных и резервных копий данных, а также любых промежуточных хранилищ, если данные переносятся из-под одной юрисдикции в другую.

Помещая ваши данные на сервер третьей стороны, облачного или любого другого поставщика, вы фактически передаете ваши данные этой третьей стороне. Поэтому вы должны быть уверены в существовании у третьей стороны надлежащих средств безопасности соответствующих вашим потребностям и отвечающим всем предъявляемым к ним законодательным и правовым нормативам. Процессы управления и процедуры поставщика также не должны противоречить никаким региональным законам в месте установки сервера. Если вы заключили соглашение с компанией в Соединенных Штатах, которая потеряла данные на сервере в ЕС, скорее всего вы будете вынуждены подчиняться законам ЕС, если захотите внести данные или получить их из системы.

В зависимости от типа поставщика облака, с которым вы заключили договор, может потребоваться выяснить, будет ли поставщик или другие лица работать с вашими данными. Воспользоваться вашими данными могут без вашего ведома или в результате ошибки конфигурации на стороне поставщика. При достаточно высокой конфиденциальности данных может потребоваться, чтобы договор запрещал или ограничивал использование этих данных поставщиком облачных услуг.

Данные, которые вы храните в облаке, могут быть конфиденциальными и содержать личную информацию, для которой необходимо обеспечить безопасность. Скорее всего у поставщика облачных услуг будет доступ к этим данным для поддержки и управления вашими серверами. Вам необходимо убедиться, при работе с данными не будет места злоупотреблениям любого рода. С юридической точки зрения договор может защищать вас от последствий подобных действий поставщика облачных услуг, но это не избавляет вас от необходимости убедиться, что поставщик сможет обнаружить несанкционированный доступ к вашим данным.

Находясь в облаке, ваши данные могут подвергнуться компрометации или взлому. В таком случае вас об этом уведомят через систему поставщика или другим способом. Хочется надеяться, что об этом вам сообщит не покупатель, у которого украли личные данные.

Сложные угрозы сегодняшнего дня не могут быть остановлены точечными продуктами обеспечения сетевой безопасности. Компаниям требуется глобальная визуализация, глубокий анализ и хирургическая защита для предотвращения этих угроз.

Для дальнейшего развития распределенных сетевых приложений и концентрации вычислительных ресурсов все более важной становится проблема обеспечения информационной безопасности. Использование облачных вычислений влечет за собой не только значительные экономические преимущества, такие как снижение затрат, оптимизация структуры инвестиций, повышение защищенности данных и перенос ответственности за обеспечение безопасности на поставщика услуг, но и значительные риски с точки зрения обеспечения информационной безопасности.
Рассмотренные виды услуг облачных вычислений и основных рисков, возникающих при их использовании, среди которых можно выделить организационные (такие как зависимость от поставщика услуг, невозможность соблюдения новых требований, ограничение контроля над используемыми службами) и технические (такие как нарушение изоляции данных, эксплуатация уязвимостей системы облачных вычислений, истощение ресурсов и отказ в обслуживании, несовместимость используемых разработок), лежат в основе рекомендаций для перехода на облачные технологии.

Вывод

Фундаментальный и многосторонний анализ рисков для информационной безопасности является неотъемлемой предпосылкой разработки и сопровождения успешных и эффективных мер по защите информации в условиях облачных вычислений.

Несмотря на все достоинства облачных вычислений, на сегодняшний день потребителям необходимо взвешенно подходить к их внедрению, органично сочетать традиционные (локальные) и облачные инфраструктуры в организации вычислительного процесса.

Ссылки

1. Демидов М. Облачные вычисления витают в облаках [Электронный ресурс]. – Режим доступа: http://softlab.pp.ua/article/333-oblachnye-vychisleniya-vitayut-v-oblakax.html (дата обращения: 27.11.2013).
2. http://okitgo.ru/gis/oblachnye-vychisleniya.html
3. http://www.it.ua/news.php