О.Пардаев (ТУИТ Каршинский филиал,ассистент)

Таким образом, эффективное решение по обеспечению информационной безопасности облачной инфраструктуры должно включать:

- Закрытый доступ к данным

Необходимо обеспечить надежное управление ключами шифрования.

- Политики доступа

Только авторизированные пользователи должны иметь доступ к конфиденциальной информации.

- Интеллектуальная система

Система должна собирать информацию для анализа поведения пользователей и оповещать в случае обнаружения подозрительной активности. Обеспечение информационной безопасности в облаке это не тривиальная задача, однако, при соответствующем подходе Вы получаете идеальный баланс всех преимуществ облачной модели и высокого уровня защиты, безопасности и доступности ваших данных и информационных систем. Лучший вариант: когда каждый из клиентов использует индивидуальную виртуальную машину (VirtualMachine – VM) и виртуальную сеть. Разделение между VM и, следовательно, между пользователями, обеспечивает гипервизор. Виртуальные сети, в свою очередь, развертываются с применением стандартных технологий, таких как VLAN (VirtualLocalAreaNetwork), VPLS (VirtualPrivateLANService) и VPN (VirtualPrivateNetwork). Некоторые провайдеры помещают данные всех клиентов в единую программную среду и за счет изменений в ее коде пытаются изолировать данные заказчиков друг от друга. Такой подход опрометчив и ненадежен. Во-первых, злоумышленник может найти брешь в нестандартном коде, который позволит ему получить доступ к данным, которые он не должен видеть. Во-вторых, ошибка в коде может привести к тому, что один клиент случайно «увидит» данные другого. За последнее время встречались и те, и другие случаи. Поэтому для разграничения пользовательских данных применение разных виртуальных машин и виртуальных сетей является более разумным шагом.

В зависимости от юрисдикции, законы, правила и какие-то особые положения могут различаться. Например, они могут запрещать экспорт данных, требовать использования строго определенных мер защиты, наличия совместимости с определенными стандартами и наличия возможности аудита. В конечном счете, они могут требовать, чтобы в случае необходимости доступ к информации смогли иметь государственные

ведомства и судебные инстанции. Небрежное отношение провайдера к этим моментам может привести его клиентов к существенным расходам, обусловленными правовыми последствиями.

Провайдер обязан следовать жестким правилам и придерживаться единой стратегии в правовой и регулятивной сферах. Это касается безопасности пользовательских данных, их экспорта, соответствия стандартам, аудита, сохранности и удаления данных, а также раскрытия информации (последнее особенно актуально, когда на одном физическом сервере может храниться информация нескольких клиентов). Чтобы это выяснить, клиентам настоятельно рекомендуется обратиться за помощью к специалистам, которые изучат данный вопрос досконально. Поэтому провайдер услуг обязан придерживаться конкретных правил поведения в случае возникновения непредвиденных обстоятельств. Эти правила должны быть задокументированы. Провайдеры обязательно должны заниматься выявлением инцидентов и минимизировать их последствия, информируя пользователей о текущей ситуации. В идеале им следует регулярно снабжать клиентов информацией с максимальной детализацией по проблеме. Кроме того, клиенты сами должны оценивать вероятность возникновения проблем, связанных с безопасностью, и предпринимать необходимые меры. Несмотря на то, что сегодня мы имеем значительно более широкий набор инструментов для обеспечения безопасности, чем прежде, работа далеко не окончена. Самозащищенные данные (self-protecteddata) – это зашифрованные данные, в которые интегрирован механизм обеспечения безопасности. Такой механизм включает в себя набор правил, которым может или не может удовлетворять среда, в которой находятся самозащищенные данные. При попытке доступа к этим данным, механизм проверяет среду на безопасность и раскрывает их, только если среда является безопасной.

Доверенный монитор (trustedmonitor) – это программное обеспечение, устанавливаемое на сервер провайдера облачных вычислений. Оно позволяет наблюдать за действиями провайдера и передавать результаты пользователю, который может убедиться в том, что компания действует в соответствии с принятым регламентом.

Список использованной литературы:

1. Основы информационной безопасности. Учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. -М.:, 2006. - 544 с

2 . Вихорев С.В., Кобцев Р.Ю. Как определить источники угроз? // Открытые системы №7-8/2002г. http://www.elvis.ru/files/howto.pdf.

3. ГОСТ РИСО/МЭК 17799-2005.

4. ISO/IEC 17799:2000 (BS 7799-1:2000).