РИСКИ ИСПОЛЬЗОВАНИЯ ОБЛАЧНЫХ ХРАНИЛИЩ

Институт информационных технологий БГУИР,
г. Минск, Республика Беларусь

Крень Н.С., Бакунович Д.С.

Савенко А.Г.- магистр технических наук, ассистент

Облачные хранилища получили большое распространение в последние годы. С развитием технологий стремительно увеличивается объём хранимой и обрабатываемой информации, а также требования к скорости обмена данными. В связи с этим сервисы облачных хранилищ стали популярны и востребованы пользователями.

Существуют различные вариации облачных хранилищ, отличающиеся структурой и функционалом, со своими достоинствами и недостатками. В этом месте встает вопрос о рисках использования такого типа систем.

Данную проблему мы можем разделить на три категории:

1. Сохранность данных;
2. Доступность данных;
3. Конфиденциальность данных.

Сохранность данных напрямую зависит от конфигурации и качества обслуживания сервера.

Применение RAID-технологий, настройка автоматического резервного копирования, своевременное техническое обслуживание сервера и другие подобные меры приводят к обеспечению максимально высокого показателя сохранности, что положительно отражается на безопасности облачных хранилищ.

Однако, в случае несоблюдения данных мер, вероятность потери информации куда выше, чем при хранении данных на локальном диске или переносном носителе.

Рассмотрим категорию доступности данных. Мы не всегда можем получить ту информацию, которая находится на сервере. К примеру, если у нас отсутствует подключение к серверу, либо он неправильно настроен мы не сможем подключиться для получения данных. На доступность данных влияют: настройки сервера, доступ к интернету, аварии на линиях, DDOS-атаки и так далее. Мы не можем повлиять на большую часть этих проблем, если сервер не обслуживается самостоятельно и не находится в локальной сети. Обычно, именно так и происходит: арендуется удалённый облачный сервер, так как настраивать и содержать собственный менее выгодно и безопасно - на крупных сервисах закрыта большая часть уязвимостей.

Минимизировать проблемы доступа в данном случае можно путём использования нескольких различных интернет-подключений. Чтобы иметь возможность получать данные из любой точки мира, рекомендуется использовать спутниковое подключение. Однако, полностью избежать проблем с доступом на данный момент невозможно в связи с возможными авариями и хакерскими атаками.

Последняя и наиболее важная категория - конфиденциальность. При использовании локального сервера, особенно без доступа в интернет, вероятность утечки данных минимальна. В данном случае, она зависит от уязвимостей системы и добросовестности людей, имеющих доступ к серверу.

Первая проблема, с которой можно столкнуться - перехват данных при отправке на сервер, либо загрузке с сервера. Это достижимо при использовании так называемых снифферов - программ для перехвата сетевого трафика. Избежать данной проблемы можно путём использования зашифрованных соединений (например, FTPS, SFTP) либо шифруя данные локально, до начала передачи.

Вторая проблема - утечка данных прямо с сервера. Её возникновение возможно по различным причинам, таким как: уязвимости системы, неправильная конфигурация сервера, не добросовестный администратор и так далее.

Большинство серверов хранят данные в зашифрованном виде, что позволяет обезопасить хранящуюся информацию. В противном случае следует шифровать важные данные на локальном устройстве перед загрузкой на сервер. Шифровать публичные данные просто не имеет смысла.

В качестве третьей проблемы можно выделить авторизацию. Завладев данным для авторизации, злоумышленник может получить доступ ко всей вашей информации, хранящейся на сервере. Чтобы этого избежать, рекомендуется настроить двухфакторную аутентификацию и установить защиту от перебора пароля. Со стороны пользователя требуется хранить в секрете данные аутентификации и сопутствующие личные данные.

Подводя итог, можно сказать, что при корректном использовании и настройке облачного сервера, хранение данных достаточно безопасно. Однако, остаётся открытым вопрос доступа к информации, так как под воздействием различных, часто не зависящих от пользователя факторов, соединение с сервером может быть прервано.