Ежемесячник по информационной безопасности для всех

OUCH!

В ЭТОМ ВЫПУСКЕ…

Безопасность при использовании «облака»

Обзор

Для каждого человека термин «облако» имеет своё значение, но для большинства - это предоставитель интернет услуг по хранению и поддержке ваших компьютерных систем и/или данных. Преимущества «облака» заключаются в том, что вы можете получить доступ и синхронизировать ваши данные с любого устройства и из любой точки мира, а также обменяться информацией с кем угодно. Такую услугу называют «облаком» потому, что зачастую вы не знаете, где физически хранятся данные. Можно привести следующие примеры облачных технологий: создание документа на Google Docs, обмен файлами через Dropbox, создание сервера на Amazon Cloud, хранение информации клиентов в Salesforce или архивирование музыки или фотографий на Apple iCloud. Все эти сервисы очень упрощают жизнь, но и таят в себе много опасностей. В этом выпуске мы поговорим о том, как можно безопасно использовать возможности Облака.

Об авторе

Дэйв Шэклефорд (@daveshackleford) - профессиональный консультант, владелец компании Voodoo Security. Дэйв является автором многих тренингов Института SANS, включая такие курсы как SANS Security 579: Виртуализация и Безопасность Облачных Технологий и Security 524: Основы Безопасности Облачных Технологий.

Выбор провайдера облачных технологий

Облачные технологии не являются богом или дьяволом, а всего лишь предлагают решения для рабочих и личных целей. Пользуясь данной технологией, следует помнить, что вы передаёте свою персональную информацию другим на хранение и ожидаете, что её будут хранить доступно и безопасно одновременно. Поэтому следует подходить к выбору провайдера «облака» очень серьёзно. Если вы собираетесь использовать Облачные решения на рабочих компьютерах, проверьте, разрешено ли использовать облачные технологии в вашей компании. Ваш руководитель или отдел ИТ могут проконсультировать вас. Если использование Облака разрешено, следует определиться, какими именно услугами вы будете пользоваться и внимательно прочитать Правила пользования. Если вам нужен провайдер для личного использования, следующие критерии помогут вам сделать правильный выбор:

1. **Поддержка**. Насколько легко получить помощь или ответ на вопрос? Есть ли контактный адрес электронной почты, форумы, на которых можно задавать вопросы или рубрика «Вопросы-ответы» на сайте компании?
2. **Простота**. Насколько легко пользоваться услугами? Чем больше комплекс услуг, тем больше шансов ошибиться

Безопасность при использовании «облака»

и случайно удалить вашу информацию или сделать её общедоступной. Выбирайте провайдера, услуги которого легко понять, конфигурировать и использовать.

3. **Безопасность**. Собирают ли данные о вас? Если да, то какие именно? Как попадают ваши данные с компьютера на облако, как они там хранятся: шифруются или нет, если да, то кто может их расшифровать?
4. **Условия предоставления услуг**. Обязательно найдите время и прочитайте Условия Предоставления Услуг (часто они очень просты). Подтвердите, кто имеет право доступа к вашим данным и какие вы имеете юридические права, а также какие правила безопасности должны соблюдать вы, а какие провайдер услуг.

облачные технологии позволяют сделать вашу информацию более доступной, а работу – более эффективной, но только при соблюдении правил безопасного доступа и обмена.

Безопасность ваших данных

После выбора провайдера следует убедиться, что вы используете облачный сервис правильно. Ведь то, как вы получаете доступ и обмениваетесь данными, оказывает большое влияние на безопасность ваших данных. Вот некоторые ключевые моменты, на которые следует обратить внимание:

1. **Аутентификация**: Используйте сильную и уникальную парольную фразу для доступа к облачному аккаунту. Если ваш провайдер поддерживает двухступенчатую аутентификацию, обязательно воспользуйтесь этим. Это один из самых важных шагов по защите вашего аккаунта.
2. **Обмен файлами/папками**: Облачный сервис позволяет очень легко обмениваться данными, даже слишком легко. В худшем случае, вы можете быть уверены, что обмениваетесь информацией с определённым кругом людей, а на самом деле вы случайно открыли доступ к файлам всему Интернету. Лучший способ защитить себя – закрыть обмен файлами по умолчанию. И потом открыть доступ к некоторым папкам только некоторым людям (или группе людей), которым эта информация действительно необходима. Если файлы больше им не нужны, заблокируйте их доступ. У вашего провайдера облачных услуг должно быть удобное меню, с помощью которого вы моете конфигурировать доступ к файлам и папкам.
3. **Обмен файлами/папками с помощью ссылки**: одной из возможностей некоторых провайдеров облачных услуг является возможность отправлять ссылку, ведущую к вашим файлам и папкам. Проще говоря, для

Безопасность при использовании «облака»

того, чтобы разрешить доступ к файлам, достаточно отправить ссылку. Но в этом случае безопасность очень низкая, так как любой человек, получив ссылку, получит доступ к вашим файлам. Вы можете отправить ссылку только одному человеку, а он перешлёт её другим или опубликует в поисковой системе. Поэтому обмениваясь данными с помощью ссылки, обязательно запретите повторную отправку ссылки; по возможности, установите срок действия, и защитите ссылку паролем.

4. **Настройки**: ознакомьтесь с настройками безопасности, предоставляемыми вашим провайдером. Например, если вы разрешили кому-то доступ к вашей папке, может ли он передать доступ кому-либо ещё без вашего ведома? Есть ли возможность посмотреть, кто смотрел вашу информацию, и когда? Можете ли вы предоставить доступ «только для чтения», вместо опции «читать и писать», которая позволяет другим людям редактировать файл?
5. **Антивирус**: убедитесь, что используете последнюю версию антивирусной программы не только на вашем компьютере, но и на других, с которыми вы обмениваетесь данными. Если ваш файл будет инфицирован, то другие компьютеры, получившие этот файл, получат этот вирус.

Узнайте Больше

Подпишитесь на OUCH! – ежемесячный журнал по информационной безопасности, получите доступ к архивам OUCH! и узнайте больше о решениях SANS в вопросах информационной безопасности на нашем сайте securingthehuman.sans.org/ouch/archives.

Ресурсы

Двухступенчатая верификация:	https://securingthehuman.sans.org/ouch/2015#september2015
Парольные фразы:	https://securingthehuman.sans.org/ouch/2015#april2015
Менеджеры паролей:	https://securingthehuman.sans.org/ouch/2015#october2015
Что такое вредоносные программы:	https://securingthehuman.sans.org/ouch/2016#march2016
Институт SANS – Курс SEC524: Cloud Security Fundamentals:	https://sans.org/sec524

Редакция: Билл Уайман, Уолт Скривенс, Фил Хоффман, Боб Рудис, Шерил Конли
Русский перевод: Александр Котков, Ирина Коткова

