OUCH! | Сентябрь 2014

Ежемесячник по информационной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

- **Обзор**
- **Выбор «облачного» провайдера**
- **Безопасность ваших данных**

Правила безопасной работы с «облаком»

Обзор

«Облако» - очень мощная технология, которую активно используют как корпорации, так и отдельные люди. Сам термин «облако» может трактоваться разными людьми по-разному, но, как правило, под ним подразумевается использование Интернет провайдера для хранения и управления данными. Преимущество «облачных технологий не только в легком доступе с различных устройств и синхронизации данных из любой точки мира, но и в возможности делиться информацией с кем угодно. Сервис называется «облачным», так как точно неизвестно физическое место хранения данных. Примерами «облачных» сервисов могут быть создание документов на Google Docs, обмен файлами на Dropbox или внедрение вашего собственного сервера на Amazon Cloud, или хранение музыки на Apple iCloud. Все эти сервисы повышают продуктивность, но их использование добавляет ряд новых, уникальных рисков. В этом выпуске мы поговорим о безопасности при работе с «облаком».

Об авторе

Джеймс и Келли Тарала (**@isaudit** / **@kellitarala**) - одни из ведущих консультантов компании Enclave Security. Они читают ряд курсов SANS, а именно: SANS Audit 566: Implementing and Auditing the Twenty Critical Security Controls and MGT 415: A Practical Introduction to Risk Assessments.

Выбор «облачного» провайдера

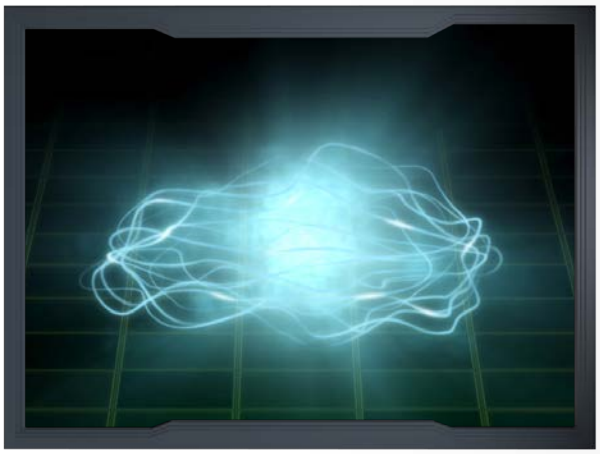
Нельзя однозначно сказать, что «облако» это добро или зло, это лишь инструмент для работы дома и в офисе. Однако следует помнить, что при работе с данным сервисом вы вручаете ваши данные незнакомым людям и ожидаете получить безопасный и бесперебойный доступ к своей информации. Следовательно, вы хотите быть уверенны в своем выборе. При использовании рабочего компьютера или официальных данных стоит обсудить возможность «облачных» технологий и выбор провайдера с руководством. Если использование «облачных» сервисов допустимо, уточните, какие именно сервисы разрешены и какова политика их использования. Если вы хотите использовать «облачные» технологии в личных целях, следует обратить внимание на следующее:

1. **Поддержка**. Насколько легко получить ответы на вопросы? Есть ли телефон или электронный адрес службы поддержки? Есть ли другие варианты поддержки, например, форумы или Раздел Часто Задаваемых Вопросов (FAQ) на сайте.

© The SANS Institute 2014

Правила безопасной работы с «облаком»

2. **Простота**. Насколько просто пользоваться услугой? Чем сложнее пользоваться сервисом, тем выше вероятность ошибок, ведущих к потере данных или их нежелательному распространению. Используйте «облачные» услуги Поставщика, которые вам легко понять, сконфигурировать и использовать.
3. **Безопасность**. Как ваши данные будут передаваться на «облако», используется ли шифрование при обмене данными? Хранятся ли данные в зашифрованном виде, и кто может их расшифровать?
4. **Условия предоставления услуг**. Найдите время для прочтения Правил предоставления услуг (иногда их очень легко понять). Уточните, кто именно имеет доступ к вашим данным, и каковы ваши законные права.



С помощью «облака» информация становится доступней, а работа продуктивней, но следует внимательно следить за тем, как вы эту информацию храните и как ей делитесь.

Безопасность ваших данных

Если вы решили воспользоваться «облачным» сервисом, то в первую очередь следует убедиться, что вы делаете это правильно. Безопасность, прежде всего, зависит от способа доступа к данным и способа обмена данными. Вот некоторые шаги, которые следует предпринять:

1. **Аутентификация**. Используйте сильную, уникальную парольную фразу для доступа к «облачному» аккаунту. Если ваш провайдер предлагает двухступенчатую аутентификацию, настоятельно рекомендуем ей воспользоваться.
2. **Общие файлы/папки**. При использовании «облачного» сервиса делиться информацией очень легко, иногда даже слишком легко. В худшем случае вы можете случайно открыть доступ к вашим файлам и папкам абсолютно всем в Интернете. Лучший способ защиты – разрешить доступ к данным по умолчанию только вам. Разрешайте доступ к папкам или файлам только некоторым людям (или группе людей) по мере надобности. Если доступ им больше не нужен, удалите их. Как правило, Провайдер предоставляет возможность отслеживать тех, кто имеет доступ к папкам и файлам.
3. **Доступ к файлам/папкам с помощью ссылки**. Практически все провайдеры «облачных» услуг предоставляют возможность создавать ссылку, ведущую к файлам или папкам. Эта функция позволяет делиться файлами с теми, кому вы её пошлете. Однако, данный способ не очень безопасный, так как абсолютно любой, кто получит ссылку, получит и доступ к вашим файлам. Даже если вы посылаете

© The SANS Institute 2014

Правила безопасной работы с «облаком»

ссылку одному человеку, нет гарантий, что он не разошлет её другим или она не попадет в поисковые системы. Если вы решите обмениваться данными этим способом, то отключите ссылку после того, как она уже не нужна или защитите её паролем, по возможности.

4. **Настройки**. Изучите, как следует, настройки, установленные Провайдером. Например, если вы поделитесь папкой с кем-то, может ли он, в свою очередь, поделиться информацией без вашего ведома?
5. **Антивирус**. Убедитесь, что на вашем компьютере и всех компьютерах, используемых для обмена данными, установлена последняя версия антивируса. Если файл, которым вы обмениваетесь, заражен, то он заразит и все компьютеры, с которых он будет использован.
6. **Резервное копирование**. Даже если ваш провайдер «облачных» услуг предоставляет услугу резервного копирования, все равно следует перидически делать собственное резервное копирование. Это защитит ваши данные в случае выхода Провайдера из бизнеса, в случае зависания системы или других причин отсутствия доступа к ним, также облегчит и ускорит восстановление данных: с локальной копии это сделать проще, чем с «облака». Кроме того, следует уточнить, как часто Провайдер создает резервные копии, позволяют ли они восстановить предыдущие версии файлов и как долго хранятся резервные копии?

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 http://www.securingthehuman.org.

Ресурсы

Пароли:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201305_ru.pdf
Менеджер паролей:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201310_ru.pdf
Резервное копирование и восстановление:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201309_ru.pdf
Security Terms:	http://www.securingthehuman.org/resources/security-terms

OUCH! выпускается Институтом SANS в рамках программы «Securing The Human». Распространение журнала регулируется Creative Commons BY-NC-ND 4.0 license. Вы можете использовать и распространять журнал при условии, что ничего не будете менять. Для перевода или получения более подробной информации, пожалуйста, обращайтесь: ouch@securingthehuman.org

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

© The SANS Institute 2014