OUCH! Август 2021

SANS SECURITY AWARENESS

OUCH!

Ежемесячный информационный бюллетень по безопасности

Безопасное использование облака

Обзор

Возможно, вы слышали о концепции под названием «облако». Это означает использование поставщика услуг в Интернете для хранения ваших данных и управления ими. Примеры включают создание документов в Google Docs, доступ к электронной почте в Microsoft O365, совместное использование файлов через Dropbox или сохранение ваших изображений в Apple iCloud. В то время как вы получаете доступ и синхронизируете свои данные с нескольких устройств в любой точке мира и делитесь своей информацией с кем угодно, вы часто не знаете и не можете контролировать, где физически хранятся ваши данные.

Выбор облачного провайдера

Облачные сервисы не являются ни добром, ни злом. Это инструменты для достижения цели. Однако, когда вы пользуетесь этими услугами, вы, по сути, передаете свои личные данные незнакомцам, ожидая, что они сохранят их в безопасности и при этом будут доступны. Таким образом, вы хотите быть уверены, что выбираете поставщика услуг с хорошей репутацией. Для получения информации, связанной с работой, обратитесь к своему руководителю, чтобы узнать, разрешено ли вам использовать облачные службы и какие из них разрешены. Если вы планируете использовать облачные сервисы в личных целях, примите во внимание следующее:

1. **Доверие:** можете ли вы доверять облачному провайдеру? Это хорошо известная публичная компания, которой уже пользуются миллионы людей, или это небольшая, неизвестная компания, базирующаяся в стране, о которой вы никогда не слышали?
2. **Служба поддержки**: насколько легко получить помощь или получить ответ на свой вопрос? Есть ли номер телефона, по которому можно позвонить, или адрес электронной почты, по которому можно связаться? Есть ли другие варианты поддержки, такие как общественные форумы или часто задаваемые вопросы на их веб-сайте?
3. **Простота**: насколько легко пользоваться сервисом? Чем сложнее сервис, тем больше вероятность того, что вы сделаете ошибки и случайно раскроете или потеряете информацию. Воспользуйтесь услугами облачного провайдера, которого легко понять, настроить и использовать.
4. **Безопасность**: как ваши данные попадут с вашего компьютера в облачный сервис? Защищено ли соединение шифрованием? Как хранятся ваши данные? Зашифрован ли он, и если да, то кто может расшифровать ваши данные? При переносе данных помните, что безопасность - это общая ответственность между вами и поставщиком.

5. **Совместимость:** поддерживает ли поставщик услуги всех устройств и операционных систем, которые вы используете или планируете использовать?
6. **Условия использования**: найдите минутку, чтобы ознакомиться с условиями обслуживания (их часто на удивление легко читать). По законам какой страны работает поставщик услуг? Обратите особое внимание на права, которые вы уступаете своему поставщику услуг.

Защита ваших данных

Следующий шаг - убедиться, что вы правильно используете свои облачные сервисы. То, как вы получаете доступ и делитесь своими данными, часто может иметь гораздо большее влияние на безопасность ваших данных, чем что-либо еще. Вот некоторые ключевые шаги, которые вы можете предпринять:

1. **Аутентификация**: используйте надежный уникальный пароль для защиты своей облачной учетной записи. Если ваш облачный провайдер предлагает двухэтапную проверку, мы настоятельно рекомендуем вам включить ее.
2. **Совместное использование файлов / папок**: облачные провайдеры делают обмен данными очень простым - иногда даже слишком простым. Очень легко случайно поделиться своей информацией публично. Защитите себя, разрешив доступ к определенным файлам или папкам только определенным людям (или группам людей). Когда кому-то больше не нужен доступ, удалите его. Ваш облачный провайдер должен предоставить простой способ отслеживать, кто имеет доступ к вашим файлам и папкам.
3. **Настройки**: узнайте о настройках безопасности, предлагаемых вашим облачным провайдером. Например, если вы делитесь изображениями, файлами или папкой с кем-то еще, могут ли они поделиться вашими данными с другими без вашего ведома?
4. **Возобновлять**: не забудьте продлить подписку, иначе вы можете потерять доступ к своим данным.

Приглашенный редактор

Тамейка Рид (@womeninlinux), основательница организации Women in Linux. Она возглавляет инициативы с акцентом на поиск карьеры в сфере инфраструктуры, кибербезопасности, DevSecOps и лидерства. Она проводит еженедельные встречи на разные темы, от инфраструктуры до блокчейна. Выступала на OSCon, LISA, Seagl и HashiConf EU.

Ресурсы

Социальный инжиниринг:https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Создание простых паролей: https://www.sans.org/newsletters/ouch/making-passwords-simple/
Менеджеры паролей: https://www.sans.org/newsletters/ouch/password-managers/
Сила обновления: https://www.sans.org/newsletters/ouch/the-power-of-updating/

Роман Полаков