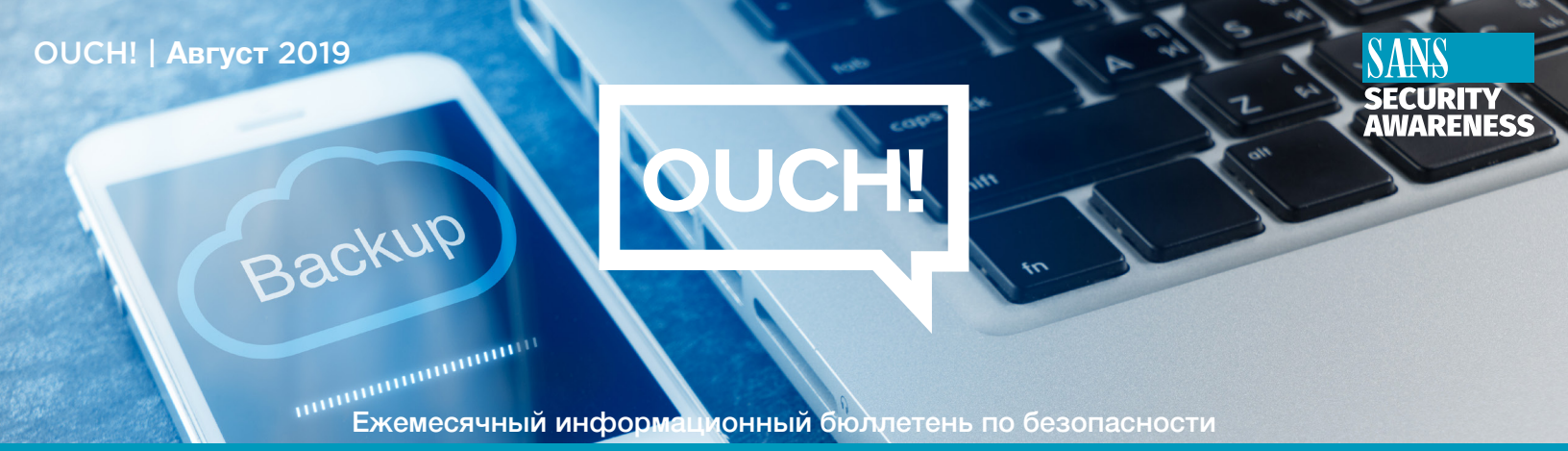

Ежемесячный информационный бюллетень по безопасности

Резервные копии

Обзор

Если вы используете компьютер или мобильное устройство достаточно долго, рано или поздно что-то пойдет не так. Вы можете случайно удалить неправильные файлы, вызвать аппаратный сбой или потерять устройство. Хуже того, вредоносные программы, такие как вымогатели, могут стирать ваши файлы или держать их в плену. В такие времена резервные копии часто являются единственным способом восстановления цифровой жизни.

Что это?

Резервные копии - это копии вашей информации, хранящиеся где-то, кроме вашего компьютера или мобильного устройства. Когда вы потеряете ценные данные, вы можете восстановить их из резервных копий. Первым шагом является определение того, что вы хотите сохранить в резервной копии, (1) конкретные данные, которые важны для вас; или (2) всё, включая всю операционную систему. Многие решения для резервного копирования по умолчанию настроены на использование первого подхода, они выполняют резервное копирование наиболее часто используемых папок. Если вы не уверены что делать и хотите предостеречься, сделайте резервную копию всего.

Во-вторых, решите, как часто делать резервные копии. Встроенные программы резервного копирования, такие как Apple Time Machine или Windows Backup and Restore, позволяют автоматически создавать расписание «установите и забудьте». К общим параметрам относятся почасовая, ежедневная, еженедельная и т. д. Другие решения предлагают «непрерывную защиту», при которой новые или измененные файлы резервируются сразу при каждом сохранении документа. Как минимум, мы рекомендуем автоматическое ежедневное резервное копирование критических файлов.

Наконец, решите, как вы собираетесь делать резервные копии. Есть два способа: локальное или облачное хранилище. Локальное резервное копирование зависит от управляемых вами устройств, таких как внешние USB-накопители или сетевые устройства, доступные по Wi-Fi. Преимущество локальных заключается в том, что они позволяют быстро создавать резервные копии и восстанавливать большие объемы данных. Недостатком является то, что если вы заражаетесь вредоносными программами, такими как Ransomware, заражение может распространиться на ваши резервные копии. Кроме того, в случае аварии, например пожара или кражи, вы можете потерять не только компьютер, но и резервные копии. Если вы используете внешние устройства для резервного копирования, храните копию за пределами сайта в безопасном месте и убедитесь, что ваши резервные копии помечены правильно.

Облачные решения - это онлайн-сервисы, которые хранят ваши файлы в Интернете. Как правило, вы устанавливаете приложение на свой компьютер, затем приложение автоматически создает резервные копии ваших файлов по

расписанию или по мере их изменения. Преимуществом облачных решений является их простота, резервные копии часто выполняются автоматически, и вы можете получить доступ к своим файлам из любого места. Кроме того, поскольку ваши данные находятся в облаке, домашние бедствия, такие как пожар или кража, не повлияют на вашу резервную копию. Наконец, облачные резервные копии могут помочь вам восстановиться от вредоносных программ, таких как Ransomware. Недостатками является то, что ваша способность выполнять резервное копирование и восстановление зависит от объема резервных копий данных и скорости вашей сети. Не уверены, хотите ли вы использовать локальное или облачное хранилище для резервного копирования? Обезопасьте себя и используйте оба.

С мобильными устройствами большая часть ваших данных уже хранится в облаке. Однако конфигурации вашего мобильного приложения, последние фотографии и системные настройки могут не совпадать. Благодаря резервному копированию вашего мобильного устройства вы не только сохраняете эту информацию, но и легче переносите свои данные при обновлении на новое устройство.

Ключевые моменты

- **Резервное копирование ваших данных - это только полдела, вы должны быть уверены, что сможете восстановить его. Периодически проверяйте, что ваши резервные копии работают, извлекая и открывая файл.**
- **Если вы перестраиваете систему из резервной копии, перед повторным использованием убедитесь, что вы повторно применили последние обновления для системы безопасности.**
- **Если вы используете облачное решение, выберите то, которое вам легко использовать, и изучите варианты безопасности. Например, поддерживают ли они двухэтапную аутентификацию для защиты вашей учетной записи в Интернете.**

Резервные копии - это простой и недорогой способ защитить вашу цифровую жизнь.

Приглашенный

Мэтт Бромил *специалист по кибербезопасности и реагирующий на инциденты. Имеет опыт работы с организациями любого масштаба. Он также является инструктором SANS, преподает расширенные классы реагирования на инциденты на хосте и в сети и классы поиска угроз, FOR508 и FOR572. Вы можете связаться с ним в Twitter* @mbromileyDFIR.

Ресурсы

Упрощение паролей:	https://www.sans.org/u/TqR
Остановить вредоносное ПО:	https://www.sans.org/u/TqW
Соблюдение кибербезопасности дома:	https://www.sans.org/u/Tr1