OUCH! Сентябрь 2022

Ежемесячный информационный бюллетень по безопасности

Есть ли у вас резервные

Обзор

Если вы используете компьютер или мобильное устройство достаточно долго, рано или поздно что-то пойдет не так. Вы можете случайно удалить неправильные файлы, произойдет аппаратный сбой или потерять устройство. Хуже того, вредоносные программы могут заразить и стереть или зашифровать ваши файлы. В такие моменты резервные копии часто являются единственным способом восстановить свою цифровую жизнь.

Резервные копии — это копии вашей информации, хранящиеся не на вашем компьютере или мобильном устройстве. Когда вы потеряете или не сможете получить доступ к ценным данным на своем устройстве, вы можете восстановить свои данные из резервных копий. Многие файлы, которые мы создаем сегодня, уже автоматически сохраняются и резервируются в облаке, например документы Microsoft Word, хранящиеся в Microsoft OneDrive, Dropbox или Google Drive, или личные фотографии, хранящиеся в Apple iCloud. Но могут быть созданные вами файлы, которые не сохраняются автоматически в облаке или, возможно, вам нужны дополнительные резервные копии для личного использования.

Что, Когда и Как

Первый шаг — решить, что вы хотите создать резервную копию: (1) конкретные данные, которые важны для вас; или (2) все, включая всю вашу операционную систему. Многие решения для резервного копирования по умолчанию настроены на использование первого подхода и резервное копирование только наиболее часто используемых папок. Если вы не знаете, на что делать резервную копию, или хотите быть особенно осторожным, подумайте о резервном копировании всего.

Во-вторых, решите, как часто выполнять резервное копирование данных. Встроенные программы резервного копирования, такие как Apple Time Machine или Windows Backup and Restore, позволяют создать автоматический график «установил и забыл». Общие параметры планирования включают ежечасно, ежедневно и еженедельно. Другие решения могут предлагать «непрерывную защиту», при которой файлы немедленно резервируются по мере их редактирования или сохранения. Как минимум, мы рекомендуем автоматические ежедневные резервные копии важных файлов.
Наконец, решите, как вы собираетесь выполнять резервное копирование. Есть два способа: локальное или облачное резервное копирование. Локальные резервные копии зависят от устройств, которыми вы физически управляете, таких как внешние USB-накопители или устройства, доступные по сети. Преимущество локальных резервных копий заключается в том, что они позволяют быстро создавать резервные копии и восстанавливать большие объемы данных. Недостатком является то, что если вы заразитесь вредоносным ПО, инфекция может распространиться на ваши резервные копии. Кроме того, в случае стихийного бедствия, например, пожара или кражи, вы можете потерять как свои резервные копии, так и свой компьютер.
Если вы используете внешние устройства для резервного копирования, храните копию вне офиса в безопасном месте и убедитесь, что ваши резервные копии правильно помечены. Для дополнительной безопасности рассмотрите возможность шифрования резервных копий.

Облачные решения — это онлайн-сервисы, которые создают резервные копии и хранят ваши файлы в Интернете. Как правило, вы устанавливаете приложение на свой компьютер. Затем приложение автоматически создает резервные копии ваших файлов либо по определенному расписанию, либо по мере их изменения или сохранения. Некоторыми преимуществами облачных решений являются их простота, автоматизация резервного копирования и доступ к файлам практически из любого места. Кроме того, поскольку ваши данные находятся в облаке, домашние бедствия, такие как пожар или кража, не повлияют на вашу резервную копию. Основным недостатком является потребляемая пропускная способность. Ваши возможности резервного копирования и восстановления зависят от объема резервных копий данных и скорости вашей сети. Не уверены, хотите ли вы использовать локальные или облачные резервные копии? Будьте особенно осторожны и используйте оба.

На мобильных устройствах большая часть ваших данных, таких как электронные письма, текстовые сообщения или фотографии, которые вы делаете, автоматически сохраняется в облаке. Однако конфигурации вашего мобильного приложения, системные настройки и другие файлы могут не храниться в облаке. Благодаря автоматическому резервному копированию вашего мобильного устройства вы не только сохраняете эту информацию, но и упрощаете перенос своих данных при переходе на новое устройство.

Дополнительные ключевые моменты

- Регулярно проверяйте работоспособность ваших резервных копий, извлекая и открывая файл.
- Если вы восстанавливаете систему из резервной копии, включая операционную систему, убедитесь, что вы повторно применили последние исправления и обновления безопасности, прежде чем использовать ее снова.
- Если вы используете облачное решение, выберите то, которое вам легко использовать, и изучите параметры безопасности. Например, поддерживает ли ваш поставщик облачных резервных копий двухэтапную проверку для защиты вашей учетной записи в Интернете?

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

Приглашенный редактор

Грег Шайдель (Greg Scheidel) — директор по кибербезопасности в Iron Vine Security с более чем 30-летним опытом работы в области ИТ и ИТ-безопасности. Он также является инструктором SANS, преподает архитектуру безопасности, проектирование и принцип нулевого доверия в SEC530. Вы можете связаться с ним в Twitter @greg_scheidel.

Ресурсы

Двухфакторная аутентификация: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/
Безопасное использование мобильных приложений: https://www.sans.org/newsletters/ouch/securely-using-the-cloud/
Менеджеры паролей: https://www.sans.org/newsletters/ouch/password-managers/
Цифровое наследование: https://www.sans.org/newsletters/ouch/digital-inheritance/

Роман Полаков