Ежемесячник по информационной безопасности для всех

OUCH!

В ЭТОМ ВЫПУСКЕ…

- Резервные копии: что, когда и как сохранять
- Восстановление
- Ключевые моменты

Резервное копирование и восстановление

Обзор

Если вы пользуетесь компьютером или мобильным устройством достаточно давно, то рано или поздно что-то случится с вашим устройством, и вы потеряете свои личные файлы, документы или фотографии. Например, файл может быть случайно удален; может произойти аппаратный сбой; устройство может быть потеряно или заражено вирусом, например, программой-вымогателем. Во всех этих случаях резервная копия будет единственной возможностью восстановить данные. В этом выпуске мы расскажем о резервном копировании, как правильно его делать и как разработать простую, подходящую для вас стратегию.

Об авторе

Кит Палмгрен – профессионал компьютерной безопасности с 30 летним стажем. Он является старшим инструктором Института SANS и автором курса SEC301 «Введение в информационную безопасность». Кит успешно работает как консультант по информационной безопасности. Он ведёт блог в Twitter: **@kpalmgren**

Резервные копии: что, когда и как сохранять

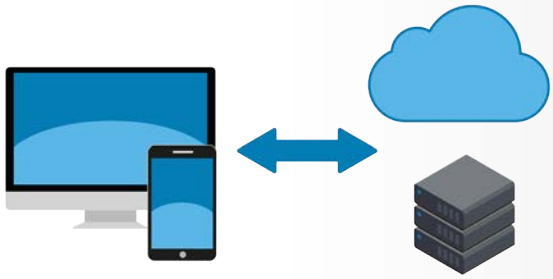
Резервные копии – это копии данных с вашего компьютера, которые хранятся вне вашего компьютера или мобильного устройства. Если вы потеряете ценные данные, то вы легко сможете их восстановить из резервной копии. К сожалению, многие люди не делают резервные копии регулярно, хотя делать их просто и недорого. Прежде всего, вам нужно решить, что именно вы будете копировать. Существует два варианта: (1) только нужную вам специфическую информацию или (2) абсолютно все, включая операционную систему. Многие программы резервного копирования по умолчанию используют первый вариант и копируют данные из наиболее часто используемых папок. В большинстве случаев этого вполне достаточно. Но если вы не знаете точно, что именно хотите копировать или хотите быть абсолютно уверены, то в таком случае следует копировать абсолютно всё.

Второй шаг – частота создания резервных копий. В большинстве компьютеров есть программы по автоматическому созданию резервных копий, например, Apple Time Machine или Microsoft Window's Backup and Restore, позволяют создать автоматическое расписание, по принципу «настрой и забудь». Наиболее популярные опции настроек: почасово, ежедневно, еженедельно и т.д. Другие решения предоставляют возможность «непрерывной защиты», когда каждый новый или измененный файл немедленно добавляется в резервную копию каждый раз, как вы его сохраняете. Мы рекомендуем делать резервные копии как минимум ежедневно.

© SANS Institute 2017

Резервное копирование и восстановление

Следующий шаг – это решить, где вы будете хранить резервные копии. Существует два варианта: физический носитель или облачное хранилище данных. У каждого из этих способов есть свои преимущества и недостатки. Если вы не уверены, какой вариант выбрать, то можете использовать оба способа. Физические носители - это устройства, которые вы можете контролировать, например, внешние диски, USB флешки или сетевые устройства с доступом через Wi-Fi. Преимущество использования физического носителя в том, что вы можете копировать большой объем данных достаточно быстро. Недостатки заключаются в том, что в случае заражения вирусами, такими, как программы-вымогатели, резервные копии будут тоже повреждены. В случае бедствия, пожара или ограбления, вместе с компьютером или устройством вы можете потерять и свои резервные копии. Поэтому, выбрав этот способ хранения резервных копий следует предусмотреть безопасное место для хранения носителей в удалённом, безопасном месте. Не забудьте пометить ваши устройства с резервными копиями.



Автоматическое создание надёжных резервных копий – последняя линия защиты ваших данных.

Облачные хранилища данных – сервисы, позволяющие хранить данные онлайн. Как правило, нужно установить приложение сервиса на свой компьютер. Это приложение будет копировать данные с компьютера по заданному вами расписанию или по мере того, как вы обновляете ваши файлы. Преимущество данного способа заключается в его простоте использования: данные копируются автоматически, и вы можете получить доступ к ним из любой точки мира. Кроме того, данным, хранящимся на облаке не страшны пожары и ограбления. Они также позволят вам восстановить данные в случае заражения компьютера программой-вымогателем, при условии, что есть резервная копия незараженных файлов. Недостаток в том, что для копирования большого объема данных требуется много времени. Кроме того, важна конфиденциальность и безопасность. Использует ли поставщик услуги такие опции защиты данных, как шифрование и двухступенчатую аутентификацию?

Поговорим о мобильных устройствах. Большая часть информации с мобильных устройств, такой, как электронная почта, расписание и контакты всегда хранится на облаке. Но ваши настройки приложений, новые фото и настройки системы могут не попасть на облако. Поэтому резервная копия не только поможет сохранить все данные, но и упростит перенос данных на новое устройство. В устройствах iPhone/iPad резервные копии автоматически сохраняются на Apple's iCloud. На устройствах Android всё зависит от производителя или поставщика услуг связи. В некоторых случаях необходимо приобрести специальное приложение для создания резервных копий.

© SANS Institute 2017

Резервное копирование и восстановление

Восстановление

Сохранение данных – это только половина успеха: вам нужно убедиться, что вы можете восстановить данные с копии. Рекомендуется периодически проверять возможность восстановления файлов из копии. Также следует делать полную копию операционной системы при подготовке к серьёзным изменениям и обновлениям (например, переносе данных на новый компьютер или устройство) или при серьёзном ремонте (например, замене жёсткого диска) и убедиться в том, что копия функциональна.

Ключевые моменты

- Независимо от того, какой вариант хранения данных вы выбрали, настройте автоматическое создание копий и регулярно их проверяйте.
- При восстановлении системы из резервной копии убедитесь, что установили последние обновления и настройки безопасности.
- Старые копии следует уничтожить, чтобы предотвратить доступ к ним посторонних лиц.
- Если вы используете облачное решение, изучите политики и репутацию поставщика услуг, чтобы быть уверенным в том, что они соответствуют вашим требованиям. Например, используется ли шифрование данных? Кто имеет доступ к информации? Используют ли они надёжную двухступенчатую аутентификацию?

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

Парольные фразы:	https://securingthehuman.sans.org/ouch/2017#april2017
Двухступенчатая верификация:	https://securingthehuman.sans.org/ouch/2015#september2015
Безопасность при использовании «облака»:	https://securingthehuman.sans.org/ouch/2016#november2016
Шифрование:	https://securingthehuman.sans.org/ouch/2016#june2016
Программы-вымогатели:	https://securingthehuman.sans.org/ouch/2016#august2016

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: Уолт Скривенс, Фил Хоффман, Кэти Клик, Шерил Конли
Русский перевод: Александр Котков, Ирина Коткова

© SANS Institute 2017