Месечен бюлетин за Информационна Сигурност насочен към потребителите

OUCH!

В ТОЗИ БРОЙ...

- **Архивиране: Какво, кога и как**
- **Възстановяване**
- **Ключови моменти**

Архив и възстановяване

Преглед

Ако използвате компютър или мобилно устройство достатъчно дълго, рано или късно нещо ще се обърка, което ще доведе до загуба на вашите лични файлове, документи или снимки. Например, може случайно да изтриете файлове, да имате повреда в хардуера, да загубите устройство или да се заразите със злонамерен софтуер като „Ransomware“ (софтуер за изнудване). Във времена като тези, архивирането често е единственият начин, по който можете да изградите отново своя цифров живот. В този бюлетин ние обясняваме какво са резервните копия, как да архивирате данните си и как да разработите проста стратегия, която е подходяща за вас.

Гост-редактор

Кийт Палмгрен е професионалист в сферата на кибер сигурността с над 30 години опит в областта на ИТ сигурността. Той е старши инструктор към SANS и автор на SANS SEC301: “Въведение в сигурността на информацията”. Кийт ръководи и успешна практика за консултиране в областта на сигурността и е в Twitter: **@kpalmgren**.

Архивиране: Какво, кога и как

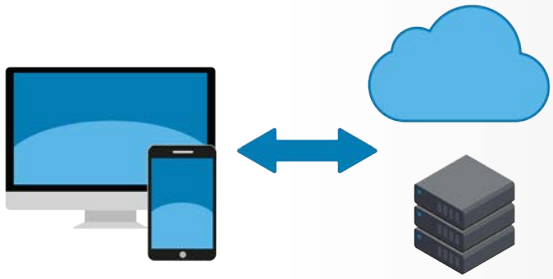
Архивите са копия на вашата информация, съхранени някъде другаде, но не и на вашия компютър или мобилно устройство. Когато загубите ценни данни, можете да ги възстановите от архивите си. За съжаление, твърде много хора не успяват да правят редовни резервни копия, въпреки че те са прости и евтини. Първата стъпка е да решите какво искате да архивирате. Има два подхода: (1) конкретни данни, които са важни за вас; или (2) всичко, включително цялата операционна система. Много от решенията за архивиране са конфигурирани по подразбиране, за да използват първия подход, те архивират данните от най-често използваните папки. В много случаи това е всичко, от което се нуждаете. Все пак, ако не сте сигурни какво да архивирате или искате да бъдете много внимателни, архивирайте всичко.

Второ, трябва да решите колко често да архивирате. Вградените програми за архивиране като Time Machine на Apple или Backup and Restore на Microsoft Windows ви позволяват да създадете график за автоматично създаване на резервни копия. Стандартните опции включват почасово, дневно, седмично и т.н. Други решения предлагат “непрекъсната защита”, при която нови или променени файлове се архивират всеки път, когато запишете документ. Като минимум ние препоръчваме автоматизирани ежедневни архиви.

Трябва също така да решите как ще направите резервно копие. Има два начина да направите резервно копие на данните си: физически носител или хранилище в облак. Всеки подход има предимства и недостатъци. Ако не сте сигурни кой подход да използвате, можете да използвате и двата едновременно. Физическите носители са устройства, които управлявате като външни USB устройства или Wi-Fi-достъпни мрежови устройства. Предимството

Архив и възстановяване

да използвате собствените си физически носители е, че ви позволяват да архивирате и възстановявате големи количества данни много бързо. Недостатъкът на такъв подход е, ако се заразите със злонамерен софтуер, като Ransomware, възможно е заразяването да се разпространи в архивите ви. Също така, ако ви сполети неприятност, като пожар или кражба, това може да доведе до загуба не само на вашия компютър, но и на резервните копия. По този начин, ако използвате външни устройства за архивиране, трябва да съхранявате копие от архива си на сигурно място извън дома. Уверете се, че резервните копия, които съхранявате извън дома си, са правилно надписани.



Автоматизираните, надеждни архивирания са често последната ви линия на защитата на вашите данни.

Облачните решения са онлайн услуги, които съхраняват вашите файлове в Интернет. Обикновено инсталирате приложение на компютъра си. След това приложението автоматично архивира файловете ви по график или когато ги промените. Предимството на облачните решения е тяхната простота, архивите често са автоматични и обикновено можете да получите достъп до файловете си отвсякъде. Също така, тъй като вашите данни се намират в облака, домашните неприятности като пожар или кражба няма да повлияят на вашето резервно копие. И накрая, резервните копия в облака могат да ви помогнат да се възстановите от заразяване със зловреден софтуер, като Ransomware, тъй като много облачни решения позволяват възстановяване от версии преди заразената. Недостатъците са, че може да отнеме много време за архивиране или възстановяване на много големи количества данни. Също така, неприкосновеността на личния живот и сигурността са важни. Услугата за архивиране предоставя ли сигурни контроли за сигурност, като например криптиране на данните ви и удостоверяване в две стъпки?

И накрая, не забравяйте мобилните си устройства. С мобилните устройства повечето от вашите данни, като например имейли, събития в календара и контакти, вече се съхраняват в облака. Конфигурациите на мобилното ви приложение, последните снимки и системните предпочитания обаче може да не се съхраняват в облака. Когато архивирате мобилното си устройство, не само съхранявате тази информация, но е по-лесно да прехвърляте данните си, когато надстроите до ново устройство. IPhone/iPad могат автоматично да се архивират в iCloud на Apple. Android или други мобилни устройства зависят от производителя или доставчика на услуги. В някои случаи може да се наложи да закупите мобилно приложение, специално разработено за архивиране.

Възстановяване

Архивирането на данните ви е само половината от битката. Трябва да сте сигурни, че можете да ги възстановите. Проверявайте периодично дали архивите ви работят, като извлечете файл и се уверите, че той е същият като оригинала. Също така, не забравяйте да направите пълно архивиране на системата преди основно надграждане

Архив и възстановяване

(като преминаване на нов компютър или мобилно устройство) или сериозна поправка (като подмяна на твърдия диск) и да се уверите, че данните са възстановими.

Ключови точки

- Независимо от това какви решения използвате за архивиране на данните си, направете така, че да автоматизирате архивите си и ги проверявайте периодично.
- При повторно изграждане на система от архивно копие, уверете се, че прилагате най-новите пакети и актуализации за сигурност, преди да ги използвате отново.
- Неактуалните архиви, които вече не са необходими, са отговорност; унищожавайте ги, за да предотвратите достъп на неоторизирани лица.
- Ако използвате облачно решение, проучете правилата и репутацията на доставчика и бъдете уверени, че те отговарят на изискванията ви. Например, криптират ли данните ви? Поддържат ли сигурно удостоверяване като удостоверяване в две стъпки?

НАУЧЕТЕ ПОВЕЧЕ

Абонирайте се за месечния бюлетин за информационна сигурност OUCH!, разгледайте архивните броеве на OUCH! и научете повече за решенията за информационна сигурност на SANS като ни посетите на securingthehuman.sans.org/ouch/archives.

Радослава Несторова (лингвист) и Николай Дачев (технически експерт) са екип, доказал се в областта на техническите преводи. Повече за нас можете да научите на нашите страници в LinkedIn:
https://www.linkedin.com/pub/radoslava-nestorova/6/6a2/962
https://www.linkedin.com/pub/nikolay-dachev/7b/5bb/96b

Ресурси

Ключови фрази:	https://securingthehuman.sans.org/ouch/2017#april2017
Удостоверяване в две стъпки:	https://securingthehuman.sans.org/ouch/2015#september2015
Облачна сигурност:	https://securingthehuman.sans.org/ouch/2016#november2016
Криптиране:	https://securingthehuman.sans.org/ouch/2016#june2016
Злонамерен софтуер за откуп:	https://securingthehuman.sans.org/ouch/2016#august2016

Редакторски колектив: Уолт Scrivens, Фил Хофман, Кати Кликнете, Черил Конли
Превод: Николай Дачев и Радослава Несторова

