OUCH! | Серпень 2015

Щомісячник з інформаційної безпеки для користувачів

OUCH!

У ЦЬОМУ НОМЕРІ…

- Що копіювати та коли
- Як робити резервні копії
- Відновлення
- Ключові моменти

Резервне копіювання і відновлення

Огляд

Рано чи пізно, швидше за все, щось піде не так, і ви можете втратити свої особисті файли, документи або фотографії. Приклади включають в себе випадкове видалення файлів чи апаратний збій, втрату свого ноутбуку або зараження комп'ютера. У таких ситуаціях, резервне копіювання часто єдиний спосіб відновити ваше цифрове життя. У цьому випуску ми пояснюємо, що таке резервні копії, як робити резервне копіювання даних і як розробити стратегію, яка підходить саме вам.

Гість номера

Heather Mahalik є визнаним в промисловості судовим експертом, який фокусується на судово-медичній експертизі смартфонів. Вона є співавтором праць з прикладної мобільної криміналістики, технічний редактор навчання криміналістиці для платформ на базі Android і співавтором FOR585 Розширеної криміналістики смартфонів і судової експертизи FOR518 Macintosh для інституту SANS. Шукайте Heather в **Smarterforesnics.com** і Twitter: **heathermahalik**.

Що копіювати та коли

Резервні копії - це копії вашої інформації, які зберігаються в декількох місцях. Коли ви втрачаєте важливі дані, ви можете відновити ці дані з резервних копій. Проблема в тому, що більшість людей не виконує резервне копіювання, нажаль, тому що резервне копіювання може бути простими і недорогими. Є два підходи до вирішення питань, що потрібно зберігати: (1) конкретні дані, що важливі для вас; або (2) все, в тому числі всю вашу операційну систему. Перший підхід спрощує ваші резервні копії і економить простір на жорсткому диску, проте другий підхід є більш простим і всеосяжним. Якщо ви не впевнені, що обрати для резервного копіювання, то ми рекомендуємо зробити повну резервну копію.

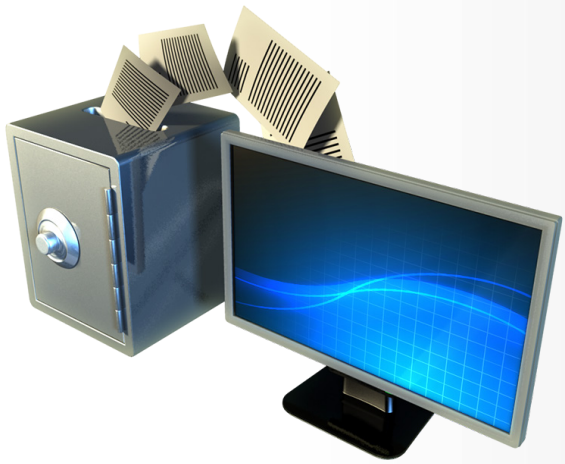
Ваше наступне рішення - вирішити, як часто ви будете робити резервне копіювання ваших даних. Загальні типові варіанти включають в себе: щогодини, щодня, щотижня і т.д. Для домашнього використання, особисті програми резервного копіювання, такі як Time Machine від Apple або Microsoft Windows Backup і Restore дозволять вам створити автоматичний "встановити параметри і забути" розклад резервного копіювання. Ці рішення мовчки роблять резервні копії ваших даних протягом дня, поки ви працюєте або далеко від комп'ютера. Інші рішення пропонують "безперервний захист", в якому нові або змінені файли відразу зберігаються, як тільки ви їх закриваете. Як мінімум, ми рекомендуємо вам робити резервне копіювання щодня. У кінцевому рахунку ви повинні відповісти на питання: "як багато інформації я можу дозволити собі втратити, якщо я буду повинен відновлювати її з резервної копії?"

Як робити рервні копії

Є два способи резервного копіювання даних: фізичні носії або хмара для зберігання даних. Фізичне медіа обладнання будь-якого типу, наприклад: DVD-диски, USB-накопичувачі або зовнішні жорсткі диски. Які би засіб зберігання інформації ви не вибрали, ніколи не зберігайте резервну копію ваших файлів в одному пристрої, який

Резервне копіювання і відновлення

містить оригінальні файли. В разі проблеми з фізичними носіями, якщо у вашій місцевості лихо (наприклад: пожежі або крадіжки), то ви можете не тільки втратити свій комп'ютер, але й резервні копії також. В такому разі ви повинні мати план, щоб зберігати резервні копії в безпечному місці. Якщо ви вже зберігаєте їх в безпечному місці, переконайтеся, що ви промаркували їх з тим, які данні там зберігаються, і коли вони були збережені. Для забезпечення додаткової безпеки вам необхідно шифрувати резервні копії.



Автоматизовані та надійні резервні копії - ваш останній рубіж оборони в захисті даних.

Рішення на основі хмари відрізняються, це сервіс, де ваші файли зберігаються в Інтернет. В залежності від того, скільки даних ви хочете зберегти, ви можете використовувати платні чи безкоштовні сервіси. Вони працюють шляхом встановлення програми на вашому комп'ютері, яка автоматично створює резервні копії файлів для вас. Перевага цього рішення полягає в тому, що, оскільки ваші резервні копії знаходяться в хмарі, в разі наприклад, якщо з вашим будинком станеться лихо, резервні копії будуть у безпеці. Крім того, ви можете отримати доступ до копії, або часто навіть тільки окремі файлів, практично в будь-якому місці, навіть під час подорожі. Недолік - відновлення резервної копії, збереженої в Хмарі може відбуватися повільніше, особливо якщо у вас є велика кількість даних. Якщо ви не впевнені, який варіант резервного копіювання краще для вас (з використанням фізичних носіїв або хмар), майте на увазі, ви завжди можете використовувати обидва рішення.

Нарешті, не забувайте про свої мобільні пристрої. Перевага мобільних пристроїв в тому, що більшість ваших даних вже зберігаються в хмарі, наприклад, ваша адреса електронної пошти, календар подій, контакти, тощо. Однак ви можете мати інформацію, яка не зберігається в хмарі, наприклад, конфігурації мобільних додатків, останні фото і системні налаштування. Виконуючи резервне копіювання вашого мобільного пристрою, ви не тільки зберігаете цю інформацію, але й піклуєтесь про легке відновлення пристрію, наприклад, в разі при оновленні до нової версії операційної системи. IPhone/IPad може виконувати резервне копіювання автоматично в ICloud Apple. Android або інші мобільні пристрої залежать від виробника пристрою чи постачальника сервіса. У деяких випадках вам, можливо, доведеться придбати мобільні додатки, розроблені спеціально для створення резервних копій.

Відновлення

Резервне копіювання даних це тільки півсправи; Ви повинні бути впевнені, що ви можете відновити інформацію. Перевіряйте кожен місяць, що ваші резервні копії працюють, шляхом відновлення файлів та перевірки вмісту. Крім того, не забудьте робити повну резервну копію системи перед будь-якими серйозними модифікаціями (такі як: переміщення на новий комп'ютер, або мобільний пристрій) або капітальний ремонт (такий, як заміна жорсткого диска) і переконайтеся, що їх можна відновити.

Резервне копіювання і відновлення

Ключові моменти

- Автоматизуйте резервне копіювання на стільки, на скільки це можливо, і постійно перевіряйте їх.
- При відновленні всієї системи з резервної копії, переконайтеся, що ви повторно встановили патчі і оновлення безпеки, перш ніж знову її використовувати.
- Застарілі резервні копії повинні бути знищені, щоб запобігти їх несанкціонованого доступу.
- Якщо ви використовуєте Хмарні рішення, ознайомтеся з дослідженням політики безпеки і репутацією постачальника рішення і переконатися, що вони відповідають вашим вимогам. Наприклад, чи шифруються резервні копії при збереженні? Хто має доступ до резервних копій? Чи підтримують вони двоступеневу автентифікацію?

About Crytek

Crytek is an independent videogame developer, publisher and technology provider with headquarters in Frankfurt am Main (Germany) and seven other studios around the world. Established in 1999, Crytek has created multiple award-winning titles, including the original Far Cry, the Crysis series, Ryse: Son of Rome and Warface. All of Crytek's games are developed using CRYENGINE, the company's cutting-edge 3D game technology, which is also the first choice of other leading developers and licensees when creating games for PC, Xbox One, PlayStation®4, Wii UTM, iOS and Android. Crytek's ongoing growth in the games-as-a-service market has extended the company's reach as they continue to deliver top quality interactive experiences to players through self-publishing platforms online.

ДІЗНАЙТЕСЯ БІЛЬШЕ

Підпишіться на OUCH! - Щомісячний журнал з інформаційної безпеки, отримаєте доступ до архівів OUCH! і дізнайтеся більше про рішення SANS в питаннях інформаційної безпеки на нашому сайті: http://www.securingthehuman.org.

Ресурси

Паролі:	http://www.securingthehuman.org/ouch/2015#april2015
Двоступенева автентифікація:	http://www.securingthehuman.org/ouch/2013#august2013
Безпека Хмарних сервісів:	http://www.securingthehuman.org/ouch/2014#september2014
Шифрування:	http://www.securingthehuman.org/ouch/2014#august2014
Порада дня:	http://www.sans.org/tip_of_the_day.php

Редакція: Білл Вайман, Уолт Скрівенс, Філ Хоффман, Боб Рудіс
Український переклад: Дмитро Коржевін