OUCH! | Sierpień 2015

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM WYDANIU..

- **Czego kopię zapasową tworzyć i kiedy to robić**
- **Jak tworzyć kopię zapasową**
- **Odzyskiwanie**
- **Kluczowe punkty**

Backup i odzyskiwanie danych

Wstęp

Prędzej czy później najprawdopodobniej spotka Cię taka sytuacja, że coś pójdzie nie po Twojej myśli i stracisz swoje osobiste pliki, dokumenty lub zdjęcia. Może się tak stać choćby na skutek przypadkowego usunięcia niewłaściwych plików, awarii sprzętu, utraty laptopa czy zainfekowania komputera. W obecnych czasach kopie zapasowe są często jedynym sposobem na odbudowanie swojego cyfrowego świata. W tym biuletynie wyjaśnimy, czym są kopie zapasowe, jak tworzyć kopie zapasowe swoich danych oraz jak opracować właściwą dla siebie strategię.

Redaktor gościnny

Heather Mahalik jest uznaną w branży ekspertką kryminalistyki informatycznej skupiającą się na analizie smartfonów. Jest współautorką opracowania "Practical Mobile Forensics", redaktorką techniczną Learning Android Forensics i współautorką kursów FOR585 "Advanced Smartphone Forensics" i FOR518 "Macintosh Forensics" dla Instytutu SANS. Możesz śledzić Heather na **Smarterforesnics.com** i na Twitterze **@heathermahalik**.

Czego kopię zapasową tworzyć i kiedy to robić

Kopie zapasowe, zwane także backupem, to kopie informacji, które są przechowywane gdzie indziej niż ich oryginał. Kiedy stracisz ważne dane, można je odzyskać właśnie z kopii zapasowych. Niestety, większość ludzi nie wie jak wykonywać kopie zapasowe. A szkoda, ponieważ czynność ta jest prosta i nie wymaga specjalnych zasobów. Istnieją dwie szkoły co do tego, co należy przechowywać w kopii zapasowej: (1) konkretne dane, które są dla Ciebie ważne; lub (2) wszystko, w tym cały system operacyjny. Pierwsze podejście optymalizuje tworzenie kopii zapasowych i oszczędza miejsce na dysku, jednak drugie podejście jest prostsze i bardziej wszechstronne. Jeśli nie masz pewności którą wersję wybrać, zalecamy tworzenie kopii zapasowych wszystkiego, czyli zarówno danych jak i systemu operacyjnego.

Kolejną decyzją będzie kwestia jak często tworzyć kopię zapasową danych. Popularne opcje to co godzinę, codziennie, co tydzień, itd. Istnieją programy do użytku domowego przeznaczone do tworzenia kopii zapasowych, takie jak Time Machine firmy Apple lub Microsoft Windows Backup and Restore. Pozwalają one tworzyć automatyczne harmonogramy tworzenia kopii zapasowych w stylu "ustaw i zapomnij". Rozwiązania te po cichu wykonują kopię zapasową danych podczas pracy lub kiedy jesteś z dala od komputera. Inne rozwiązania oferują "ciągłą ochronę", w których nowe lub zmienione pliki są natychmiast dodawane do kopii zapasowej, gdy tylko zostają zamknięte. Jako minimum zaleca się wykonanie kopii zapasowej codziennie. Pytanie na które musisz sobie odpowiedzieć to: "Jak wiele informacji mogę sobie pozwolić stracić?"

Jak tworzyć kopię zapasową

Istnieją dwa sposoby, aby utworzyć kopię zapasową danych: zapisać je na zewnętrznym fizycznym nośniku lub na przestrzeni dyskowej w chmurze. Nośniki fizyczne to każdy rodzaj sprzętu, taki jak DVD, dysk USB lub zewnętrzny dysk twardy. Niezależnie od tego jaki rodzaj nośnika wybierzesz, nigdy nie twórz kopii zapasowych plików na tym samym

Backup i odzyskiwanie danych

urządzeniu, które zawiera oryginalne pliki. Wadą nośników fizycznych jest to, że w przypadku przechowywania nośnika z kopią w tym samym miejscu co komputer z oryginalnymi danymi, jeśli zdarzy się kradzież czy pożar, możesz stracić nie tylko swój komputer, ale również kopię zapasową. Dlatego dobrze jest przechowywać kopię zapasową poza lokalizacją w której znajduje się komputer, w bezpiecznym miejscu, opatrzoną opisem z informacją co zostało na niej nagrane i kiedy. Dla dodatkowego bezpieczeństwa, zalecamy szyfrowanie swoich kopii zapasowych.

Zautomatyzowane i niezawodne kopie zapasowe to często ostatnia linia obrony w ochronie Twoich danych.

Odmiennym rozwiązaniem jest tworzenie kopii zapasowych w chmurze, co polega na tym, że nasze pliki są przechowywane gdzieś w Internecie. W zależności od ilości danych, które chcemy tam zapisać, usługa może być płatna. Korzystanie z niej polega na zainstalowaniu na komputerze programu, który automatycznie tworzy kopie zapasowe plików. Zaletą tego rozwiązania jest to, że dane są przechowywane w chmurze i jeśli zdarzy się jakieś nieszczęśliwe zdarzenie w domu, kopia zapasowa jest nadal bezpieczna. Ponadto mamy dostęp do kopii zapasowych i ich pojedynczych plików z każdego miejsca, na przykład w podróży. Wadą tego sposobu tworzenia backupów (w tym ich odzyskiwania) jest to, że mogą być one wolniejsze, zwłaszcza jeśli składujemy dużą ilość danych. Jeśli nie masz pewności, która opcja tworzenia kopii zapasowych będzie najlepsza dla Ciebie (nośnik fizyczny lub chmura) pamiętaj, że zawsze możesz korzystać z obu sposobów jednocześnie.

Nie zapomnij też o swoich urządzeniach mobilnych. W ich przypadku zaletą jest to, że większość Twoich danych, takich jak e-mail, zdarzenia z kalendarza czy kontakty, i tak jest już przechowywana w chmurze, nawet bez Twojej świadomości. Jednak są dane, które nie są archiwizowane automatycznie, takie jak konfiguracje aplikacji mobilnych, najnowsze zdjęcia i ustawienia systemu. Poprzez tworzenie kopii zapasowej urządzenia mobilnego, nie tylko zachowujemy te informacje, ale łatwiej jest przywrócić ustawienia osobiste urządzenia, na przykład podczas aktualizacji do nowej wersji. IPhone czy iPad może automatycznie zrobić kopię zapasową do usługi iCloud firmy Apple. W przypadku Androida i innych urządzeń mobilnych zależy to od producenta lub usługodawcy. W niektórych przypadkach może być konieczny zakup aplikacji mobilnej przeznaczonej specjalnie do tworzenia kopii zapasowych.

Odzyskiwanie

Tworzenie kopii zapasowych danych to tylko połowa sukcesu. Musisz mieć pewność, że będzie można te dane odzyskać. Co miesiąc sprawdzaj czy zapisywanie kopii zapasowych działa poprzez próbę odzyskania pliku i zweryfikowanie czy jego zawartość jest poprawna. Ponadto zawsze wykonuj pełną kopię zapasową systemu przed każdą poważną aktualizacją (taką jak przenosiny do nowego komputera czy urządzenia mobilnego) lub poważną naprawą (jak wymiana dysku twardego) i sprawdzaj czy da się ją odzyskać.

Backup i odzyskiwanie danych

Kluczowe punkty

- Zautomatyzuj tworzenie kopii zapasowych i sprawdzaj je regularnie.
- Podczas odzyskiwania całego systemu z kopii zapasowej, pamiętaj o zainstalowaniu najnowszych poprawek i aktualizacji zabezpieczeń zanim zaczniesz używać go ponownie.
- Pamiętaj o ewentualnej odpowiedzialności związanej ze zbyt długim przechowywaniem danych. Przestarzałe kopie zapasowe powinny zostać zniszczone, aby ustrzec się przed dostępem nieupoważnionych użytkowników.
- Jeśli używasz rozwiązania w chmurze, zbadaj dokładnie politykę i reputację dostawcy oraz upewnij się, że spełnia on Twoje wymagania. Na przykład, czy szyfruje przechowywane dane? Kto ma dostęp do Twoich kopii zapasowych? Czy wspiera on silne uwierzytelnianie, takie jak dwustopniowa weryfikacja?

Dowiedz się więcej

Zasubskrybuj comiesięczny biuletyn o bezpieczeństwie komputerowym SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS dotyczące bezpieczeństwa komputerowego i osobowego.
Odwiedź http://www.securingthehuman.org i dowiedz się więcej.

Polski przekład

CERT Polska jest zespołem działającym w strukturach NASK powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w polskiej sieci Internet. Należy do organizacji FIRST, w ramach której współpracuje z podobnymi zespołami na całym świecie.
WWW: http://www.cert.pl
Twitter: @CERT_Polska
Facebook: http://facebook.com/CERT.Polska

Przydatne linki

Nowe oblicze hasła:	http://www.securingthehuman.org/ouch/2015#april2015
Dwustopniowe uwierzytelnianie:	http://www.securingthehuman.org/ouch/2013#august2013
Bezpieczne korzystanie z chmury:	http://www.securingthehuman.org/ouch/2014#september2014
Szyfrowanie:	http://www.securingthehuman.org/ouch/2014#august2014
Porada Dnia SANS (ang.):	http://www.sans.org/tip_of_the_day.php

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak, Paweł Jacewicz, Łukasz Siewierski

