Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu

- **Co i kiedy archiwizować**
- **Jak tworzyć kopie zapasowe**
- **Przywracanie danych**
- **Najważniejsze zasady**

Backup i przywracanie danych

REDAKTOR GOŚCINNY

Dr. Eric Cole jest redaktorem gościnnym tego wydania biuletynu OUCH! Eric skupia się na usługach konsultingowych wspomagających organizacje we wdrażaniu rozwiązań, które pozwalają im się chronić. Jest również autorem i wykładowcą w SANS Institute.

WSTĘP

Kopie zapasowe to jeden z najlepszych i najważniejszych sposobów zapewnienia właściwej ochrony swoich danych. Są one ostatnią linią obrony kiedy nastąpi awaria dysku twardego, przypadkowe skasowanie ważnych plików lub w razie infekcji złośliwym oprogramowaniem. W tym wydaniu skupimy się na sposobach, jakimi można tworzyć kopie zapasowe i wypracować swoją własną strategię robienia backupów.

CO I KIEDY ARCHIWIZOWAĆ

Istnieją dwa podejścia do tworzenia kopii zapasowych danych, w zależności od tego co ma być archiwizowane: (1) wszystkie ważne dla Ciebie dane, takie jak dokumenty, zdjęcia czy filmy; albo (2) wszystko, włączając w to Twój system operacyjny i wszelkie zainstalowane programy oraz Twoje ważne dane.

W pierwszym przypadku proces tworzenia backupu jest uproszczony, natomiast podejście drugie sprawia że łatwiej jest odtworzyć wszystko sprzed całkowitej awarii systemu. Jeśli nie jesteś pewny tego co archiwizować, najlepiej archiwizuj wszystko.

Kolejną decyzją jaką musisz podjąć to określenie jak często będziesz tworzyć kopię zapasową swoich danych. Popularne okresy to: co godzinę, codziennie, co tydzień itp. Do stworzenia harmonogramu backupu użytkownikom komputerów domowych powinno wystarczyć użycie programów takich jak Apple Time Machine dla systemu Mac OS X, czy Microsoft Backup and Restore dla Windows. Z reguły jednorazowa konfiguracja takiej aplikacji jest wystarczająca, aby kopie zapasowe były wykonywane automatycznie i aby nie trzeba było pamiętać o całym procesie. Inne rozwiązania oferują ciągłą ochronę polegającą na natychmiastowym robieniu backupu, kiedy tylko nowostworzony lub zmodyfikowany plik zostanie zamknięty. Jeśli w Twojej organizacji jest wiele komputerów, możliwe że będzie potrzebne stworzenie własnego harmonogramu tworzenia kopii zapasowych. W takim wypadku dobrym podejściem jest nastawienie się na najgorszy scenariusz i określenie jak wielką utratę danych jesteśmy w stanie zaakceptować. Przykładowo, tworząc kopie zapasowe codziennie w przypadku awarii możesz stracić pracę z całego dnia, jeśli awaria nastąpi w późnych godzinach, niedługo przed kolejnym backupem. Wiele organizacji planuje wykonywanie dziennych backupów poza godzinami szczytu, tak aby zminimalizować obciążenie dla zwykłych operacji.

JAK TWORZYĆ KOPIE ZAPASOWE

Istnieją dwa miejsca, w których można robić kopie

Backup i przywracanie danych

zapasowe swoich danych: urządzenia fizyczne albo przechowywanie danych w chmurze. Przykładami urządzeń fizycznych są płyty DVD, dyski USB, taśmy magnetyczne lub dodatkowe dyski twarde. Unikaj tworzenia backupu na tym samym urządzeniu, na którym przechowujesz oryginalne pliki. Używając urządzeń fizycznych pamiętaj aby je właściwie oznaczyć zarówno wewnętrznie (w nazwie pliku) i zewnętrznie (na urządzeniu), tak aby można było z łatwością zidentyfikować kopię zapasową z konkretnej daty. Można również przechowywać lokalnie kopię danych w zamkniętym, ognio- i wodoodpornym pojemniku specjalnie przeznaczonym dla nośników z danymi. Jeszcze bardziej solidnym rozwiązaniem jest przechowywanie kopii zapasowych swoich danych poza lokalizacją gdzie przechowywane są oryginalne pliki. Jednak dla tworzenia kopii danych prywatnych wystarczy przechowywać je u kogoś z rodziny albo w bezpiecznym miejscu. Organizacje niekiedy korzystają z profesjonalnych usług transportu i przechowywania kopii zapasowych. Zależnie od tego jak wrażliwe są dane i gdzie będą przechowywane, można je dodatkowo zaszyfrować.

Wiele z tych kwestii da się pominąć za korzystając z backupów w chmurze. Tworzenie kopi zapasowej w chmurze bardzo często ogranicza się do zainstalowania i skonfigurowania aplikacji na komputerze. Po odpowiednim ustawieniu wszystkich opcji backupu, zarówno nowe jak i zmienione pliki będą kopiowane automatycznie na serwery centrum danych.

Na końcu musisz zdecydować jak daleko w przeszłość powinny sięgać Twoje kopie zapasowe. Użytkownicy domowi zazwyczaj nie muszą przechowywać swoich archiwów dłużej niż 30 dni wstecz. Niektóre organizacje mogą mieć specjalną politykę lub wymagania prawne na dłuższe okresy retencji danych albo obowiązek niszczenia starych kopii zapasowych. Jeśli archiwizujesz dane organizacji, upewnij się jakie zasady w niej obowiązują kontaktując się z odpowiednimi osobami z działów IT, prawnych albo odpowiedzialnych za bezpieczeństwo informacji. W przypadku wybrania metody przechowywania danych w chmurze, za ich magazynowanie najprawdopodobniej trzeba będzie zapłacić, zależnie od ich

Niezawodny backup to ostatnia linia obrony przed utratą Twoich danych.

ilości. Dlatego należy zwracać uwagę na ilość przechowywanych danych, aby nie zostać niemile zaskoczonym wysokim rachunkiem.

PRZYWRACANIE DANYCH

Tworzenie kopii zapasowych swoich danych to tylko połowa sukcesu. Musisz być pewny, że w razie awarii będziesz mógł je łatwo odzyskać. Wykonuj proces odzyskiwania danych regularnie, zupełnie jakbyś przeprowadzał ćwiczenia pożarowe, aby być pewnym, że kiedy będziesz potrzebował, wszystko zadziała tak jak należy. Przynajmniej raz w miesiącu sprawdź czy Twój program do tworzenia backupu na pewno działa przynajmniej próbując odtworzyć plik z kopii zapasowej. Aby wykonać bardziej rzetelne testy, szczególnie w organizacjach, można rozważyć przeprowadzenie pełnego odzyskania systemu aby zweryfikować czy jest to bezproblemowo wykonalne. Jeśli nie posiadasz wolnego sprzętu do testowania pełnego

Backup i przywracanie danych

odzyskania systemu, spróbuj odzyskać najważniejsze pliki i foldery i zapisać je w innej niż oryginalna lokalizacji. Następnie sprawdź czy na pewno wszystkie pliki zostały przywrócone i czy każdy z nich można otworzyć.

NAJWAŻNIEJSZE ZASADY

• Maksymalnie zautomatyzuj proces tworzenia kopii zapasowych, ale sprawdź czy wszystko należycie działa.

• Przywracając cały system albo odzyskując kluczowe pliki systemu operacyjnego upewnij się, że zaraz po tym ponownie zainstalowałeś wszystkie aktualizacje bezpieczeństwa, które ukazały się od czasu utworzenia backupu, zanim zaczniesz go normalnie używać.

• Przestarzałe kopie zapasowe powinny zostać zniszczone aby zapobiec dostaniu się ich w niepowołane ręce.

• Jeśli używasz rozwiązań które przechowują dane w chmurze, zorientuj się jakie zasady postępowania obowiązują w danej organizacji. Na przykład: czy dane które mają być składowane w chmurze dane powinny być szyfrowane? Kto może mieć dostęp do tych danych? Czy firma dostarczająca usługi zdalnego backupu wspiera odpowiednio mocne uwierzytelnianie?

• Gdy chcesz stosować silne kopie zapasowe, rozważ stosowanie zasady 3-2-1:

- Trzy: Jeśli cos jest warte zachowania, przechowuj oryginał i dwie dodatkowe kopie.
- Dwa: Używaj różnych rodzajów nośników dla swoich dwóch kopii zapasowych. Jeśli musisz użyć tego samego typu nośnika, postaraj się chociaż aby były to nośniki innego producenta dla każdej z kopii, tak aby zminimalizować możliwość defektów produkcyjnych.
- Jeden: Przechowuj jedną kopię danych poza lokalizacją, w której znajdują się oryginalne pliki.

ŹRÓDŁA

Niektóre odnośniki w biuletynie zostały skrócone przy użyciu usługi TinyURL dla lepszej czytelności tekstu. Dla zachowania bezpieczeństwa, OUCH! używa funkcji podglądu TinyURL, która pozwala podejrzeć docelowy adres odnośnika oraz pyta o pozwolenie przed wejściem na stronę o docelowym adresie.

Apple Time Machine:
http://preview.tinyurl.com/3wkytqs
Windows 7 Backup and Restore:
http://preview.tinyurl.com/ylghqgp
Cloud Backup: http://preview.tinyurl.com/3reftgv

DOWIEDZ SIĘ WIĘCEJ

Zasubskrybuj comiesięczny Biuletyn Bezpieczeństwa Komputerowego – SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS z zakresu 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 reagownia 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

Redakcja: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, Carmen Ruyle Hardy
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak and Paweł Jacewicz