Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu..

- **Backup: Co, kiedy i jak**
- **Odzyskiwanie danych**
- **Kluczowe punkty**

Backup i odzyskiwanie danych

Wstęp

Prędzej czy później najprawdopodobniej znajdziesz się w sytuacji, w której coś pójdzie nie po Twojej myśli i stracisz swoje prywatne pliki, dokumenty czy zdjęcia zgromadzone na urządzeniu. Może się tak stać choćby na skutek przypadkowego usunięcia niewłaściwych plików, awarii sprzętu, jego utraty lub zainfekowania złośliwym oprogramowaniem z rodziny Ransomware. W obecnych czasach kopie zapasowe są często jedynym sposobem na odbudowanie swojego cyfrowego świata. W tym biuletynie wyjaśnimy, czym są kopie zapasowe danych, jak je tworzyć oraz jak opracować właściwą dla siebie strategię zapobiegania utracie danych.

Redaktor gościnny

Keith Palmgren jest związany z cyberbezpieczeństwem od ponad 30 lat. Zajmuje stanowisko starszego instruktora SANS. Jest autorem kursu SANS SEC301; "Wprowadzenie do Bezpieczeństwa Informacji". Można znaleźć go na twitterze pod **@kpalmgren**.

Co kopiować, jak często oraz w jaki sposób

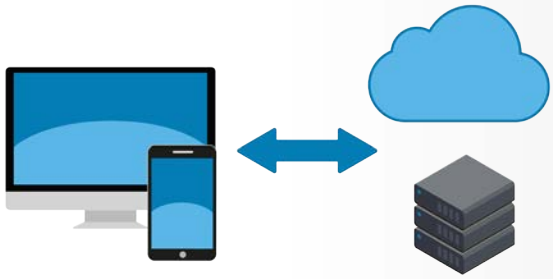
Kopia zapasowa (ang. backup), to klon danych z urządzenia , który jest przechowywany gdzie indziej niż ich oryginał. Kiedy stracisz ważne dane, można je odzyskać właśnie z kopii zapasowych. Niestety, większość ludzi nie wykonuje ich regularnie, mimo że jest to prosta czynność i nie wymaga kosztownych zasobów. W pierwszej kolejności powinieneś zdecydować jakie dane chcesz powielić. Istnieją dwa podejścia: pierwsze polega na zapisie konkretnych danych, które są dla Ciebie ważne, natomiast drugie to tworzenie kopii wszystkiego wraz z systemem operacyjnym. Większość narzędzi do wykonywania kopii zapasowych jest domyślnie skonfigurowana dla pierwszego podejścia i wykonuje kopię danych z najczęściej używanych lokalizacji. W większości przypadków to wystarcza. Natomiast jeśli nie masz pewności co powinieneś kopiować lub chcesz pozostać "super bezpieczny", kopiuj wszystko.

Kolejną decyzją będzie kwestia jak często tworzyć kopię zapasową danych. Najczęściej spotykane 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 na zasadzie "ustaw i zapomnij". Inne rozwiązania oferują "ciągłą ochronę", w których nowe lub zmodyfikowane pliki są natychmiast dodawane do kopii zapasowej.. Jako minimum zaleca się wykonanie kopii zapasowej codziennie.

Istnieją dwa sposoby, aby utworzyć kopię zapasową danych: zapisać je na zewnętrznym fizycznym nośniku lub na przestrzeni dyskowej w chmurze. Każdy z nich posiada swoje wady i zalety. Jeśli nie jesteś pewny, którą metodę wybrać, możesz stosować obie naraz. Nośniki fizyczne to każdy rodzaj sprzętu, taki jak zewnętrzne dyski USB lub urządzenia

Backup i odzyskiwanie danych

dostępne poprzez sieć WiFi. Zaletą korzystania z własnego nośnika fizycznego jest możliwość tworzenia szybkiej kopii zapasowej dużych zbiorów danych. Jednak jeśli komputer został zarażony złośliwym oprogramowaniem, np. ransomwarem, możliwe że infekcja przedostanie się również do kopii zapasowej. Ponadto w przypadku kataklizmu takiego jak pożar czy kradzież , możesz stracić nie tylko swój komputer, ale również kopię zapasową. Z tego powodu dobrze jest przechowywać kopię w innej lokalizacji niż komputer, w bezpiecznym miejscu. Upewnij się także, że kopia została odpowiednio opisana.



Zautomatyzowane, niezawodne kopie zapasowe to często ostatnia linia obrony Twoich danych.

Rozwiązania oparte o chmurę polegają na umieszczaniu kopii plików w internecie. Najczęściej instalowana jest wtedy aplikacja, która automatycznie tworzy kopię zapasową plików. W zależności od trybu robi to w oparciu o harmonogram lub po każdej modyfikacji. Zaletą tego rozwiązania jest automatyzacja procesu tworzenia kopii oraz dostęp do plików z dowolnego miejsca. W razie wystąpienia w domu nieszczęśliwego zdarzenia, pożaru lub włamania, kopia zapasowa będzie nadal bezpieczna. Co więcej, w przypadku infekcji złośliwym oprogramowaniem takim jak ransomware, możesz przywrócić dane do stanu sprzed zdarzenia. Wadą tego sposobu tworzenia backupów (w tym ich odzyskiwania) jest to, że ich tworzenie, zwłaszcza dla dużej ilości danych może być powolne. Ponadto zwróć uwagę na ochronę prywatności i bezpieczeństwo wybranego serwisu kopii zapasowej. Sprawdź czy usługa oferuje szyfrowanie danych oraz silne uwierzytelnianie.

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. Jednak niektóre dane mogą nie być archiwizowane automatycznie, np. konfiguracje aplikacji, najnowsze zdjęcia i ustawienia systemu. Poprzez tworzenie kopii zapasowej swojego urządzenia mobilnego, nie tylko zabezpieczasz informacje, ale również ułatwiasz sobie ich migrację w momencie zmiany urządzenia. 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 danych

Tworzenie kopii zapasowych to tylko połowa sukcesu. Musisz mieć pewność, że będzie można te dane odzyskać. Regularnie upewniaj się, że tworzone są prawidłowe kopie zapasowe, próbując odzyskać plik i weryfikując jego poprawność. Każdorazowo przed wprowadzeniem dużych modyfikacji systemowych lub sprzętowych lub przy wymianie sprzętu na nowy, upewnij się, że posiadasz pełną kopię systemu, którą jesteś w stanie odzyskać.

Backup i odzyskiwanie danych

Kluczowe punkty

- Niezależnie od wybranej metodyki wykonywania kopii zapasowych, zautomatyzuj ich tworzenie oraz sprawdzaj je cyklicznie.
- Podczas odzyskiwania systemu z kopii zapasowej, pamiętaj o zainstalowaniu najnowszych poprawek oraz aktualizacji zabezpieczeń przed jego ponownym użyciem.
- Usuwaj nieaktualne kopie zapasowe, by zmniejszyć ryzyko dostępu do nich osobom nieuprawnionym.
- 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? 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 securingthehuman.sans.org/ouch/archives 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

Źródła

Bezpieczne hasła:	https://securingthehuman.sans.org/ouch/2017#april2017
Dwustopniowe uwierzytelnianie:	https://securingthehuman.sans.org/ouch/2015#september2015
Bezpieczne korzystanie z chmury:	https://securingthehuman.sans.org/ouch/2016#november2016
Szyfrowanie:	https://securingthehuman.sans.org/ouch/2016#june2016
Ransomware:	https://securingthehuman.sans.org/ouch/2016#august2016

Editorial Board: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Polski przekład (NASK/CERT Polska): Sebastian Kondraszuk, Michał Strzelczyk, Jacek Sikorski

