Biuletyn Bezpieczeństwa Komputerowego

Czy robisz kopie zapasowe?

Wstęp

Używając komputera lub urządzenia mobilnego prędzej czy później 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.

Co kopiować, jak często oraz w jaki sposób

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. Pierwszym krokiem jest podjęcie decyzji, jakich plików chcesz zrobić kopię zapasową: (1) konkretne dane, które są dla Ciebie ważne; lub (2) wszystko, w tym cały system operacyjny. 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, najlepiej archiwizuj wszystko.

Musisz zdecydować jak często robić kopie zapasowe. 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. Zaleca się wykonanie kopii zapasowej codziennie.

Powinieneś zdecydować, w jaki sposób chcesz wykonać 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 zewnętrzne dyski USB lub urządzenia 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.

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. Każda z metod posiada swoje wady i zalety. Jeśli nie jesteś pewny, którą metodę wybrać, możesz stosować obie naraz.

W przypadku urządzeń mobilnych większość danych 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.

Kluczowe punkty

- **Tworzenie kopii zapasowej to zaledwie połowa sukcesu, musisz mieć pewność, że jest ona prawidłowa i zdatna do użycia. Testuj okresowo, czy kopie zapasowe działają poprawnie.**
- **Podczas odzyskiwania systemu z kopii zapasowej, pamiętaj o zainstalowaniu najnowszych poprawek oraz aktualizacji zabezpieczeń przed jego ponownym użyciem.**
- **Jeśli używasz rozwiązania w chmurze, zbadaj dokładnie politykę i reputację dostawcy oraz upewnij się, że spełnia on Twoje wymagania. Na przykład czy wspiera on silne uwierzytelnianie, takie jak dwustopniowa weryfikacja?**

Tworzenie kopii zapasowych jest prostym i tanim sposobem ochrony Twojego cyfrowego życia.

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

Redaktor wydania

Matt Bromiley *jest specjalistą w zakresie cyberbezpieczeństwa oraz reagowania na incydenty w sieci. Jest również instruktorem SANS, który prowadzi zaawansowane zajęcia z zakresu reagowania na incydenty oraz ich wyszukiwania (FOR 508 i FOR572). Możesz się z nim skontaktować na Twitterze* @mbromileyDFIR.

Źródła

Tworzenie haseł w prostszy sposób:	https://www.sans.org/u/TqR
Ochrona przed złośliwym oprogramowaniem:	https://www.sans.org/u/TqW
Cyberbezpieczny Dom:	https://www.sans.org/u/Tr1