OUCH! Wrzesień 2022

Biuletyn Bezpieczeństwa Komputerowego

Czy posiadasz kopie zapasowe?

Wstęp

Jeśli korzystasz z komputera lub smartfona wystarczająco długo, prędzej czy później nadejdzie czas, kiedy stanie się coś złego. Możesz przypadkowo usunąć dane lub pliki, które nadal są Ci potrzebne, dysk twardy może ulec awarii lub po prostu zgubisz swoje urządzenie. Co gorsze, złośliwe oprogramowanie może zainfekować urządzenie i usunąć lub zaszyfrować dane. W takich sytuacjach kopie zapasowe są często jedyną możliwością na odzyskanie utraconych danych.

Kopie zapasowe są niczym innym jak danymi potrzebnymi do odtworzenia oryginalnych danych w przypadku ich utraty. Są zapisane w dodatkowym miejscu poza urządzeniem, z którego korzystasz. W sytuacji, kiedy stracisz lub nie możesz uzyskać dostępu do swoich danych, możesz łatwo je przywrócić z tych kopii. Wiele plików, z których korzystamy jest automatycznie zapisywana w chmurze. Przykładem takich plików są dokumenty Microsoft Word zapisywane w usłudze One Drive, Dropbox lub Google Drive, lub zdjęcia zapisywane przy pomocy usługi Apple iCloud lub Zdjęcia Google. Jednak mimo tego nadal mogą istnieć dane, które nie są automatycznie zapisywane w Twojej kopii zapasowej; lub chcesz stworzyć dodatkowe kopie do osobistego użytku.

Co, kiedy i jak

Pierwszym krokiem przy tworzeniu kopii zapasowych jest decyzja jakie dane chcesz zachować: 1. szczególne dane, które są dla Ciebie ważne,2. wszystkie dane, być może nawet cały system operacyjny. Wiele rozwiązań do tworzenia kopii zapachowych jest domyślnie skonfigurowanych, żeby zapisywać dane tylko z najczęściej używanych folderów. Jeśli nie jesteś nie jesteś pewny co powinna zawierać Twoja kopia zapasowa lub chcesz zachować szczególną ostrożność, warto rozważyć opcję, która będzie zapisywać wszystkie dane.

Drugim krokiem jest decyzja jak często chcesz aktualizować zapisane dane. Wbudowane przez producentów rozwiązania pozwalają na stworzenie grafiku automatycznego tworzenia kopii zapasowych, przy pomocy mechanizmów "ustaw i zapomnij". Popularne opcje planowanego tworzenia kopii zapasowych to: co godzinę, codziennie i co tydzień. Innym rozwiązaniem, które oferuje "nieprzerwaną ochronę" jest natychmiastowe aktualizowanie plików w kopii zapasowej za każdym razem, kiedy są one edytowane lub zapisywane. Jako minimum bezpieczeństwa, zalecamy codzienną automatyczną aktualizację kopii zapasowych ważnych dla Ciebie plików.
Na sam koniec, pozostaje decyzja jak przechowywać kopie Twoich danych. Istnieją dwie możliwości: lokalne kopie zapasowe lub chmurowe kopie zapasowe. Lokalne kopie zapasowe zapisują dane na fizycznym urządzeniu, do którego masz dostęp. Może być to na przykład zewnętrzny dysk USB (pendrive) lub przenośny dysk twardy. Zaletą takiego rozwiązania jest możliwość odzyskania dużej ilości danych w krótkim czasie.
Wadą z kolei jest przykładowy scenariusz, kiedy Twój system zostanie zaatakowany przez złośliwe oprogramowanie, możliwe jest wtedy, że infekcja dosięgnie również urządzeń przechowujących kopie zapasowe. Dodatkowo, kopie takie są narażone na niebezpieczeństwa związane z niespodziewanymi wypadkami, jak na przykład pożar lub kradzież, podczas takich scenariuszy możesz stracić zarówno komputer jak i kopie zapasowe.
Jeśli wykorzystujesz zewnętrzne urządzenie do przechowywania swoich kopii, umieść je w bezpiecznej lokalizacji poza miejscem zamieszkania, pamiętaj również o ich właściwym oznaczeniu. Dodatkową warstwą zabezpieczenia będzie zaszyfrowanie kopii zapasowej.

Rozwiązania oparte o usługi chmurowe są serwisami internetowymi, które zapisują pliki w Internecie. Zazwyczaj, należy zainstalować na komputerze aplikację konkretnej firmy. Następnie aplikacja ta automatycznie tworzy kopie zapasowe plików według ustalonego grafiku lub za każdym razem kiedy edytujesz lub zapisujesz pliki. Niektóre z zalet takiego rozwiązania to prostota, możliwość automatyzacji tworzenia kopii i możliwość dostępu do plików z każdego miejsca na świecie, jeśli tylko masz dostęp do internetu. Ponadto, jako że dane nie są przechowywane w Internecie, niespodziewane wypadki takie jak pożar lub kradzież nie mają wpływu na nasze dane. Największą wadą takiego rozwiązania jest dodatkowe wykorzystanie limitu łącza internetowego. Może być to problematyczne zwłaszcza wtedy jeśli posiadamy umowę z miesięcznymi limitami dotyczącymi wykorzystania łącza. Twoje możliwości do tworzenia i odzyskiwania danych z kopii zapasowych są zależne od tego jak dużo danych chcesz zachować oraz od prędkości Twojego internetu. Nie jesteś pewny, z którego rozwiązania skorzystać? Najlepiej być podwójnie zabezpieczonym i użyć dwóch metod równocześnie.

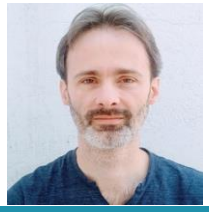
Jeśli chodzi o urządzenia mobilne, większość danych takich jak wiadomości email, sms lub zdjęcia są automatycznie przechowywane w chmurze zapewnianej producentów urządzenia. Jednak dane takie jak ustawienia aplikacji i systemu zazwyczaj nie są automatycznie zapisywane w kopiach zapasowych. Korzystając z automatycznych kopii zapasowych na urządzeniu mobilnym, nie tylko chronimy swoje dane ale również, o wiele łatwiej przeniesiemy swoje dane jeśli zechcemy kupić nowe urządzenie.

Dodatkowe rzeczy, o które należy mieć na uwadze

- Regularnie sprawdzaj czy kopie zapasowe działają w oczekiwany sposób. Sprawdź czy możesz odzyskać i otworzyć pliki z kopii zapasowej.
- Jeśli przywracasz cały system operacyjny z kopii zapasowych pamiętaj o zainstalowaniu najnowszych aktualizacji bezpieczeństwa przed ponownym użytkowaniem urządzenia.
- Jeśli korzystasz z rozwiązań chmurowych wybierz te, które jest dla Ciebie najprostsze w użytkowaniu oraz zapoznaj się z dodatkowymi opcjami bezpieczeństwa jakie ono oferuje. Na przykład, czy rozwiązanie które wybrałeś, wspiera dwustopniową weryfikację dostępu do danych?

Kopie zapasowe są prostym i nie drogim sposobem na ochronę cyfrowych danych.

Redaktor gościnny



Greg Scheidel jest dyrektorem ds. Cyberbezpieczeństwa w Iron Vine Security, posiada ponad 30 lat doświadczenia w dziedzinie informacji technologii i cyberbezpieczeństwa. Jest instruktorem kursu SANS dla SEC530, skupiającego się na nauczaniu o architekturze bezpieczeństwa, inżynierii i polityce "zero trust". Można go znaleźć na Twitterze @greg_scheidel.

Źródła

Zabezpieczenie kont online:
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt10571a9437cfe16e/6137f6abfbf2f03cb2533da7/ouch!_september_2021_one_simple_step_to_securing_your_accounts_Polish.pdf
Bezpieczne przechowywanie danych w chmurze:
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt608dc82396f5560b/61071fa90d73bb3ec5da9415/ouch!_Polish_august_2021_securely_using_the_cloud.pdf
Menedżer haseł:
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltee798afb2a08b806/604a692cacf0d53d70c5e0a6/202004-OUCH-Polish.pdf
Cyfrowa spuścizna:
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt801e959deab4f6cf/6048034dfef76d094c70314c/202001-OUCH-Polish.pdf

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz