Tworzenie kopii zapasowych

Chociaż tworzenie kopii zapasowych danych brzmi jak prosta koncepcja - i tak jest - w rzeczywistości wdrożenie wydajnej i skutecznej procedury tworzenia kopii zapasowych jest trochę bardziej skomplikowane. Aby poprawnie wykonać kopię zapasową, nie tylko musisz znać opcje tworzenia kopii zapasowych, ale musisz pomyśleć o wielu innych szczegółach, takich jak lokalizacja kopii zapasowych, szyfrowanie, hasła i dyski rozruchowe. W tym rozdziale dowiesz się o wszystkich szczegółach tworzenia kopii zapasowych i nie tylko.

Tworzenie kopii zapasowych jest koniecznością

W kontekście cyberbezpieczeństwa tworzenie kopii zapasowych odnosi się do tworzenia dodatkowej kopii lub dodatkowych kopii danych (które mogą składać się z danych, programów lub innych plików komputerowych) na wypadek uszkodzenia, utraty lub zniszczenia oryginału. Tworzenie kopii zapasowych jest jedną z najważniejszych zabezpieczeń przed utratą danych i ostatecznie może uchronić Cię przed poważnymi problemami, ponieważ prawie każdy, jeśli nie wszyscy, w pewnym momencie będą chcieli uzyskać dostęp do danych, do których on lub nie ma już dostępu. W rzeczywistości takie scenariusze występują regularnie. Czasami są wynikiem ludzkiego błędu, na przykład przypadkowego usunięcia pliku lub zgubienia komputera lub urządzenia pamięci masowej. Czasami są wynikiem awarii technicznej, takiej jak śmierć dysku twardego lub upadek urządzenia elektronicznego do wody. Czasami są wynikiem wrogich działań, takich jak infekcja ransomware. Niestety, wiele osób uważa, że tworzą kopie zapasowe wszystkich swoich danych tylko po to, aby dowiedzieć się, kiedy coś pójdzie nie tak, że nie mają odpowiednich kopii zapasowych. Nie pozwól, żeby ci się to przytrafiło. Pamiętaj, aby regularnie tworzyć kopie zapasowe - na tyle często, że gdybyś musiał przywrócić z kopii zapasowej, nie wpadłbyś w panikę. Ogólnie rzecz biorąc, jeśli masz wątpliwości, czy tworzysz kopie zapasowe wystarczająco często, tak nie jest. Nie myśl, że kopie zapasowe są dostępne, jeśli kiedykolwiek przegrasz dane. Pomyśl, że są przy Tobie, gdy tracisz dane. W pewnym momencie praktycznie każda osoba, która regularnie korzysta z urządzeń elektronicznych, straci dane.

Patrząc na różne typy kopii zapasowych

Kopie zapasowe można kategoryzować na wiele różnych sposobów. Jednym z ważnych sposobów rozróżniania różnych typów kopii zapasowych jest to, co jest kopiowane. W poniższych sekcjach omówiono różne typy kopii zapasowych oparte na tym podejściu.

Pełne kopie zapasowe systemów

Pełna kopia zapasowa systemu to kopia zapasowa całego systemu, w tym systemu operacyjnego, programów / aplikacji, ustawień i danych. Termin ten ma zastosowanie niezależnie od tego, czy urządzenie, którego kopia zapasowa jest tworzona, to smartfon, czy ogromny serwer w centrum danych. Technicznie rzecz biorąc, pełna kopia zapasowa systemu obejmuje kopię zapasową wszystkich dysków podłączonych do systemu, a nie tylko tych zamontowanych w jego wnętrzu - chociaż niektóre dyski są dołączane do systemu tylko od czasu do czasu i nie są potrzebne do podstawowego użytku. system, niektórzy mogą wykluczyć zawartość takich dysków z pełnych kopii zapasowych systemu, zwłaszcza jeśli są one podłączone do innych systemów lub są tworzone jako część kopii zapasowych innych systemów. Jednak dla większości użytkowników domowych pełna kopia zapasowa systemu oznacza dokładnie to, na co wygląda: tworzenie kopii zapasowej wszystkiego. Pełna kopia zapasowa systemu jest czasami nazywana obrazem systemu, ponieważ zasadniczo zawiera obraz systemu w postaci, w jakiej istniał w określonym momencie. Jeśli urządzenie, którego masz obraz, ulegnie awarii, powinieneś być w stanie użyć obrazu systemu do odtworzenia całego systemu, jaki był w momencie

tworzenia kopii zapasowej. Gdy używasz odbudowanego systemu, powinien on działać dokładnie tak samo, jak poprzedni system w momencie tworzenia kopii zapasowej. Pełne kopie zapasowe systemu to forma kopii zapasowej, z której zazwyczaj można najszybciej przywrócić cały system, ale ich utworzenie zajmuje więcej czasu niż inne formy kopii zapasowej. Zwykle wymagają również więcej miejsca do przechowywania. Jedno ważne zastrzeżenie: ponieważ kopia zapasowa systemu obejmuje ustawienia, sterowniki sprzętu itd., Przywracanie z obrazu systemu nie zawsze działa dobrze, jeśli przywracasz dane na inne urządzenie niż to, na które utworzono kopię zapasową. Jeśli na przykład wykonałeś zdjęcie laptopa z systemem operacyjnym Windows 7, a następnie nabyłeś nowsze urządzenie przeznaczone do systemu Windows 10, które ma inny sprzęt, przywrócony obraz systemu pierwszego urządzenia może nie działać dobrze na nowsze urządzenie. Odwrotna sytuacja jest jeszcze bardziej prawdopodobna: jeśli trzymasz stary komputer w szafie „na wszelki wypadek" i ta sytuacja na wszelki wypadek staje się rzeczywistością, próby przywrócenia obrazu z nowszej maszyny do starszej maszyny może zawieść całkowicie lub częściowo.

Obrazy systemowe są czasami określane jako duchy (przy czym duch jest również czasownikiem do tworzenia takich obrazów), szczególnie wśród techników. Nazwa pochodzi od jednego z oryginalnych pakietów oprogramowania do klonowania dysków dla komputerów PC.

Oryginalne obrazy systemu

Jednym ze specjalnych przypadków obrazów systemu jest oryginalny obraz systemu, znany również jako obraz fabryczny. Wiele nowoczesnych urządzeń komputerowych, takich jak laptopy, tablety czy smartfony, jest wyposażonych w obraz fabryczny, który można przywrócić. Oznacza to, że gdy kupujesz urządzenie, jest ono dostarczane z obrazem oryginalnej konfiguracji, którą otrzymujesz - w tym systemu operacyjnego, całego oryginalnego oprogramowania i wszystkich ustawień domyślnych - przechowywanym na ukrytej partycji lub innym mechanizmie przechowywania, który nie jest normalnie dostępny. użytkownikom. W dowolnym momencie możesz przywrócić ustawienia fabryczne i ustawić urządzenie tak, aby wyglądało identycznie, jak było, gdy było nowe. Gdy to zrobisz, urządzenie przywróci dane z ukrytego obrazu.Dwa ważne zastrzeżenia:

* Niektóre urządzenia zastępują obraz przywracania ustawień fabrycznych nowymi obrazami w przypadku niektórych aktualizacji systemu operacyjnego.

* W przypadku przywrócenia ustawień fabrycznych komputera wszystkie aktualizacje zabezpieczeń zainstalowane od momentu utworzenia pierwotnego obrazu fabrycznego nie będą obecne na przywróconym urządzeniu. Pamiętaj, aby zaktualizować system jak najszybciej po przywróceniu i przed przejściem do trybu online w jakimkolwiek innym celu!

Późniejsze obrazy systemu

Niektóre systemy tworzą również okresowe obrazy, z których można przywrócić bez konieczności powrotu do oryginalnych ustawień fabrycznych. Na przykład Windows 10 ma wbudowane takie możliwości.

Nigdy nie odtwarzaj z obrazu, chyba że wiesz, że wszelkie problemy, które wystąpiły i spowodowały konieczność przywrócenia, wystąpiły po utworzeniu tego obrazu.

Oryginalny nośnik instalacyjny

Oryginalny nośnik instalacyjny jest przeznaczony dla programów, które nabywasz i instalujesz po zakupie urządzenia. Jeśli oprogramowanie zostało dostarczone na płycie DVD lub CD, zapisanie fizycznego nośnika, na którym zostało dostarczone, umożliwi ponowne zainstalowanie

oprogramowania w przypadku problemu. Należy jednak pamiętać, że jeśli jakiekolwiek aktualizacje oprogramowania zostały wydane i zainstalowane po pierwotnej instalacji, konieczne będzie ponowne pobranie i ponowne zainstalowanie aktualizacji. Może to nastąpić automatycznie po ponownej instalacji lub może wymagać wysiłku ręcznego.

Pobrane oprogramowanie

Jeśli programy zostały nabyte od czasu zakupu urządzenia, prawdopodobnie niektóre lub wszystkie z nich zostały dostarczone do pobrania cyfrowego. Gdy oprogramowanie jest dostarczane do pobrania, program do pobierania nie otrzymuje fizycznej kopii. Jeśli jednak otrzymałeś oprogramowanie do pobrania, możesz zachować kopię pliku instalacyjnego, który posiadasz na co najmniej jednym z wielu różnych typów nośników, takich jak pendrive lub dysk CD lub DVD. Alternatywnie możesz przechowywać kopię na dysku twardym, ale pamiętaj, aby wykonać kopię zapasową tego dysku, jeśli jest częścią infrastruktury komputera. Ponadto niektóre sklepy, które sprzedają oprogramowanie do pobrania, przechowują kopie tego oprogramowania w wirtualnej skrytce, aby można było je pobrać później. Takie „kopie zapasowe" są przydatne, ale upewnij się, że wiesz, jak długo sklep będzie przechowywał produkt w Twojej szafce. Niektóre osoby miały poważne problemy, ponieważ polegały na takich „kopiach zapasowych" tylko po to, aby dowiedzieć się, że oprogramowanie nie było dla nich dostępne w czasie, gdy go potrzebowali. W przypadku plików muzycznych i wideo okres przechowywania przez dostawcę jest często teoretycznie nieograniczony lub przynajmniej tak długo, jak długo materiał jest dostępny do zakupu przez innych. W przypadku oprogramowania, w miarę wydawania nowych wersji i wycofywania starszych wersji (termin techniczny określający wycofywanie się dostawcy oprogramowania i ostatecznie zakończenie wsparcia dla przestarzałej wersji jego oprogramowania), okres przechowywania może być znacznie krótszy.

Pełne kopie zapasowe danych

Alternatywą dla wykonania pełnej kopii zapasowej całego systemu jest wykonanie pełnej kopii zapasowej danych w systemie, ale nie oprogramowania i systemu operacyjnego. (Ustawienia konfiguracyjne zarówno systemu operacyjnego, jak i różnych zainstalowanych programów są często przechowywane w folderach danych i uwzględniane w takich kopiach zapasowych). Wykonanie pełnej kopii zapasowej danych umożliwia użytkownikowi przywrócenie wszystkich danych za jednym razem, jeśli coś pójdzie nie tak. W zależności od narzędzia używanego do wykonania kopii zapasowej, użytkownik może być w stanie przywrócić również podzbiór danych - na przykład, wybierając opcję przywrócenia tylko jednego konkretnego pliku, który został przypadkowo usunięty. Przywrócenie z pełnej kopii zapasowej danych nie spowoduje przywrócenia aplikacji. Jeśli system wymaga całkowitej przebudowy, odzyskanie z pełnych kopii zapasowych danych prawdopodobnie wymaga wcześniejszego przywrócenia ustawień fabrycznych (lub późniejszego obrazu komputera) i ponownej instalacji całego oprogramowania

Jest to z pewnością bardziej żmudne niż zwykłe przywracanie z obrazu systemu. Jednocześnie jest też znacznie bardziej przenośny. Odzyskiwanie można zwykle przeprowadzić bez żadnych problemów na wielu urządzeniach, które znacznie różnią się od oryginalnego urządzenia. Zmniejsz prawdopodobieństwo naruszenia bezpieczeństwa przywracanego systemu, aktualizując ponownie zainstalowane oprogramowanie najnowszymi poprawkami natychmiast po przeprowadzeniu odpowiednich instalacji.

Przyrostowe kopie zapasowe

Kopie przyrostowe to kopie zapasowe utworzone po wykonaniu pełnej kopii zapasowej, które zawierają kopie tylko części danych (lub, w przypadku kopii zapasowej systemu, części całego systemu),

która uległa zmianie od czasu utworzenia poprzedniej kopii zapasowej (pełnej lub przyrostowej). biegać. Przyrostowe kopie zapasowe zwykle działają znacznie szybciej niż pełne kopie zapasowe, ponieważ w większości systemów zdecydowana większość plików danych nie zmienia się regularnie podstawa. Z tego samego powodu przyrostowe kopie zapasowe również zajmują mniej miejsca niż pełne kopie zapasowe. Aby jednak odzyskać dane, należy przywrócić ostatnią pełną kopię zapasową oraz wszystkie przyrostowe kopie zapasowe wykonane od ostatniej pełnej kopii zapasowej. Jeśli zdecydujesz się użyć przyrostowych kopii zapasowych, rozważ ograniczenie liczby takich kopii zapasowych, które tworzysz po wykonaniu pełnej kopii zapasowej. Na przykład, jeśli wykonałeś tylko jedną pełną kopię zapasową pierwszego dnia miesiąca kalendarzowego i wykonałeś przyrostowe kopie zapasowe we wszystkie kolejne dni, aż do rozpoczęcia następnego miesiąca, to jeśli coś poszło nie tak w ostatnim dniu miesiąca, prawdopodobnie będziesz musiał przywróć z aż 30 kopii zapasowych w celu odzyskania plików. Wiele osób (i wiele firm) decyduje się na tworzenie pełnych kopii zapasowych systemu w jeden z dni weekendu, a następnie tworzenie kopii przyrostowych w każdy inny dzień tygodnia, znajdując w ten sposób dobry środek między wzrostem wydajności podczas procesu tworzenia kopii zapasowych a potencjał żmudnego procesu odzyskiwania.

Kopie różnicowe

Kopie różnicowe zawierają wszystkie pliki, które uległy zmianie od czasu ostatniej pełnej kopii zapasowej. (Są one podobne do pierwszych z serii przyrostowych kopii zapasowych uruchamianych po utworzeniu pełnej kopii zapasowej). Seria różnicowych kopii zapasowych wymaga zatem więcej czasu na uruchomienie i zajmuje więcej miejsca w pamięci niż przyrostowe kopie zapasowe, ale mniej niż ta sama liczba pełnych kopii zapasowych. Odzyskiwanie z różnicowych kopii zapasowych może być szybsze i prostsze niż w przypadku przyrostowych kopii zapasowych, ponieważ przywracanie musi być wykonane tylko z ostatniej pełnej kopii zapasowej i ostatniej różnicowej kopii zapasowej. Jeśli zdecydujesz się użyć różnicowych kopii zapasowych, zastanów się, ile kopii zapasowych należy wykonać przed wykonaniem następnej pełnej kopii zapasowej. Jeśli różnicowa kopia zapasowa zacznie się rozrastać, nie będzie dużego wzrostu wydajności podczas tworzenia kopii zapasowej, a przywracanie zajmie znacznie więcej czasu niż w przypadku pełnej kopii zapasowej. Wiele osób (a także wiele firm) decyduje się na tworzenie pełnych kopii zapasowych systemu w jeden z dni weekendu, a następnie wykonywanie różnicowych kopii zapasowych w każdy inny dzień tygodnia.

Ciągłe kopie zapasowe

Ciągłe kopie zapasowe to kopie zapasowe, które działają w sposób ciągły. Za każdym razem, gdy wprowadzana jest zmiana w danych (lub w systemie i danych), tworzona jest kopia zapasowa tej zmiany. Ciągłe kopie zapasowe są świetne w przypadku awarii dysku twardego w systemie podstawowym - kopia zapasowa jest dostępna i aktualna - ale niewiele robią w przypadku infekcji złośliwym oprogramowaniem lub zniszczenia danych, ponieważ złośliwe oprogramowanie zwykle przenosi się do kopii zapasowej jako jak tylko zainfekuje system podstawowy. Jedynym wyjątkiem są złożone systemy tworzenia kopii zapasowych, które rejestrują każdą akcję tworzenia kopii zapasowej i mają możliwość jej cofnięcia. Te kopie zapasowe mogą cofnąć problematyczne fragmenty kopii zapasowych do momentu, w którym wystąpiły. Proces ciągłego tworzenia kopii zapasowych jest czasami nazywany synchronizacją (lub synchronizacją). Możesz zobaczyć to opisane jako takie na swoich urządzeniach elektronicznych lub w różnych pakietach oprogramowania.

Częściowe kopie zapasowe

Częściowe kopie zapasowe to kopie zapasowe części danych. W przeciwieństwie do pełnych kopii zapasowych, częściowe kopie zapasowe nie tworzą kopii zapasowych wszystkich elementów danych z systemu. Na przykład, gdyby system został całkowicie zamknięty, nie byłoby możliwości pełnego

odzyskania całej zawartości danych z częściowych kopii zapasowych wykonanych wcześniej w tym systemie. Częściowe kopie zapasowe mogą być realizowane w pełnym modelu przyrostowym, w którym pierwsza kopia w serii obejmuje wszystkie elementy wchodzące w skład zestawu zawartego w częściowej kopii zapasowej, a kolejne kopie zapasowe w serii obejmują tylko elementy z tego zestawu, które mają zmieniony. Częściowe kopie zapasowe można również zaimplementować jako zawsze pełne - w takim przypadku za każdym razem tworzone są kopie zapasowe wszystkich elementów zestawu zawartych w częściowej kopii zapasowej, niezależnie od tego, czy zmieniły się od czasu ostatniej kopii zapasowej. Częściowe kopie zapasowe nie są pełnymi kopiami zapasowymi na wypadek ataku złośliwego oprogramowania lub podobnego. Przydają się jednak w innych sytuacjach, na przykład w sytuacji, gdy określony zestaw plików wymaga oddzielnego archiwizowania ze względu na potrzeby konkretnej osoby lub grupy lub ze względu na wrażliwość materiału.

Na przykład, podczas gdy dział IT może wykonywać pełne i przyrostowe kopie zapasowe wszystkich plików na udostępnionym dysku sieciowym, księgowy, który potrzebuje stałego dostępu do określonego zestawu arkuszy kalkulacyjnych przechowywanych na tym dysku - i nie byłby w stanie pracować, gdyby te pliki stały się niedostępne - może utworzyć własną kopię zapasową tylko tych plików. Może wykorzystać swoje wsparcie, jeśli coś pójdzie nie tak, gdy jest w drodze lub pracuje w domu w weekend, bez konieczności niepotrzebnego przeszkadzania członkom działu wsparcia technicznego w swojej firmie, aby niepotrzebnie pracowali w niedzielę.

Kopie zapasowe folderów

Kopie zapasowe folderów są podobne do częściowych kopii zapasowych w sytuacjach, gdy zestaw elementów, których kopia zapasowa jest tworzona, to określony folder. Chociaż narzędzia do tworzenia kopii zapasowych mogą ułatwić tworzenie kopii zapasowych folderów, ku rozczarowaniu wielu profesjonalistów cyberbezpieczeństwa i działów IT wielu użytkowników wykonuje takie kopie zapasowe w sposób ad hoc, ręcznie wykonując kopię folderów na dysku twardym (lub SSD) na dyskach USB pod koniec każdego dnia roboczego i uważa takie kopie zapasowe za wystarczające zabezpieczenie w przypadku problemów. Teoretycznie oczywiście takie kopie zapasowe działają i można ich użyć do odzyskania wielu problemów. Rzeczywistość mówi jednak, że procedury tworzenia kopii zapasowych ad hoc prawie nigdy nie prowadzą do tworzenia prawidłowych kopii zapasowych: w niektóre dni ludzie zapominają o tworzeniu kopii zapasowych lub nie wykonują ich, ponieważ się spieszą, zaniedbują na powrót tworzyć kopie zapasowe niektórych materiałów, które powinni byli wykonać, przechowywać kopie zapasowe na niezabezpieczonych urządzeniach w niezabezpieczonych lokalizacjach lub zgubić urządzenia, na których są przechowywane kopie zapasowe - masz pomysł! Jeśli chcesz mieć pewność, że masz odpowiednie kopie zapasowe, gdy ich potrzebujesz – a w pewnym momencie prawdopodobnie będziesz ich potrzebować - nie polegaj na ad hoc kopie zapasowe folderów. Nigdy nie twórz kopii zapasowej folderu na tym samym dysku, na którym znajduje się oryginalny folder. Jeśli dysk ulegnie awarii, utracisz zarówno główne źródło danych, jak i kopię zapasową.

Kopie zapasowe dysków

Kopia zapasowa dysku jest podobna do kopii zapasowej folderu, ale w sytuacjach, w których tworzona jest kopia zapasowa całego dysku, a nie tylko folderu. Kopie zapasowe dysków ad hoc zapewniają pewną ochronę, ale rzadko zapewniają wystarczającą ochronę przed ryzykiem utraty danych. Nigdy nie przechowuj kopii zapasowej dysku na tym samym dysku, na którym znajduje się kopia zapasowa. Jeśli dysk ulegnie awarii, utracisz główne źródło danych i kopię zapasową.

Kopie zapasowe dysków wirtualnych

Jednym ze specjalnych przypadków tworzenia kopii zapasowych dysków jest sytuacja, w której osoba lub organizacja używa zaszyfrowanego dysku wirtualnego. Na przykład użytkownik może przechowywać swoje pliki na dysku BitLocker w systemie Windows. BitLocker to narzędzie wbudowane w wiele wersji systemu Windows, które umożliwia użytkownikom tworzenie wirtualnego dysku, który wygląda jak każdy inny dysk dla użytkownika, gdy jest używany, ale pojawia się jako jeden gigantyczny zaszyfrowany plik, gdy nie jest używany. Aby uzyskać dostęp do dysku, użytkownik musi go odblokować, zwykle wprowadzając hasło. Tworzenie kopii zapasowych takich dysków jest często wykonywane po prostu przez włączenie zaszyfrowanego pliku do pełnej, przyrostowej kopii zapasowej folderu lub dysku. W związku z tym cała zawartość zaszyfrowanego dysku jest kopiowana bez odwoływania się do nazwy i pozostaje niedostępna dla każdego, kto nie wie, jak otworzyć zaszyfrowany dysk. Wiele narzędzi do tworzenia kopii zapasowych oferuje kopie zapasowe dysków jako uzupełnienie bardziej ustrukturyzowanych form kopii zapasowych. Niektóre pakiety oprogramowania określają tworzenie obrazu całego dysku jako klonowanie. Chociaż taki schemat chroni zawartość zaszyfrowanego dysku, gdy znajdują się one w kopiach zapasowych, przy użyciu tego samego szyfrowania, które zostało użyte w przypadku kopii podstawowych, należy zwrócić uwagę na kilka zastrzeżeń:

* Nawet jeśli jedna mała zmiana została dokonana w jednym pliku na dysku wirtualnym, cały zaszyfrowany plik zostanie zmieniony. W związku z tym zmiana o 1 KB może łatwo doprowadzić do konieczności utworzenia kopii przyrostowej całego pliku o pojemności 1 TB.

* Kopia zapasowa jest bezużyteczna do odzyskiwania, chyba że ktoś wie, jak odblokować zaszyfrowany dysk. Chociaż szyfrowanie może być dobrym mechanizmem ochrony przed nieautoryzowanymi osobami szpiegującymi wrażliwe pliki w kopii zapasowej, oznacza to również, że sama kopia zapasowa nie jest w pełni użyteczna do odzyskiwania. Nietrudno sobie wyobrazić powstałe w wyniku tego problemy - na przykład, jeśli ktoś, próbując wykorzystać kopię zapasową kilka lat po jej pierwotnym utworzeniu, zapomina o kodzie dostępu lub osoba, która utworzyła kopię zapasową, jest niedostępna w momencie, gdy ktoś tego potrzebuje przywrócić z niego.

* Podobnie jak w przypadku wszystkich zaszyfrowanych danych, istnieje ryzyko, że gdy komputery staną się mocniejsze - a zwłaszcza gdy obliczenia kwantowe przejmą kontrolę - dzisiejsze szyfrowanie może nie zapewniać wystarczającej ochrony przed atakami siłowymi. Podczas gdy systemy produkcyjne bez wątpienia będą z czasem aktualizowane o lepsze możliwości szyfrowania (tak jak to było od czasu 56-bitowego szyfrowania w latach 90.), kopie zapasowe utworzone przy użyciu starej technologii szyfrowania i kluczy mogą stać się podatne na odszyfrowanie przez nieautoryzowane przyjęcia. Dlatego szyfrowanie może nie zawsze chronić poufne dane zawarte w kopiach zapasowych. Takie kopie zapasowe należy przechowywać w bezpiecznym miejscu lub niszczyć, gdy nie są już potrzebne.

Wyłączenia

Kopii zapasowej niektórych plików i folderów nie trzeba tworzyć, chyba że tworzysz obraz dysku (w takim przypadku obraz musi wyglądać dokładnie tak, jak dysk). Kopie zapasowe plików stronicowania systemu operacyjnego i innych plików tymczasowych, które nie służą na przykład w przypadku przywracania systemu, nie są konieczne. Poniżej znajdują się przykłady niektórych takich plików i folderów, które można wykluczyć z kopii zapasowych na komputerze z systemem Windows 10. Jeśli korzystasz z oprogramowania do tworzenia kopii zapasowych, prawdopodobnie zawiera ono wbudowaną listę domyślnych wykluczeń, która może przypominać tę listę:

* Kosz, który skutecznie tymczasowo tworzy kopie zapasowe usuniętych plików na wypadek, gdyby użytkownik zmienił zdanie o ich usunięciu

* Pamięci podręczne przeglądarki, które są tymczasowymi plikami internetowymi z przeglądarek internetowych, takich jak Microsoft Edge lub Internet Explorer, Firefox, Chrome, Vivaldi lub Opera

* Foldery tymczasowe, które często są nazywane tymczasowymi lub tymczasowymi i znajdują się w katalogu c: \, w katalogu użytkownika lub w katalogu danych oprogramowania

* Pliki tymczasowe, które zwykle mają nazwy * .tmp lub * .temp

* Pliki wymiany systemu operacyjnego, takie jak pagefile.sys

* Informacje o obrazie systemu w trybie hibernacji systemu operacyjnego, takie jak hyberfil.sys

* Kopie zapasowe (chyba że chcesz tworzyć kopie zapasowe kopii zapasowych), takie jak Historia plików systemu Windows

* Kopie zapasowe plików systemu operacyjnego są tworzone podczas aktualizacji systemu operacyjnego, tak jak zwykle znajduje się to w C: \ Windows.old na komputerach z systemem Windows które zaktualizowały swoje systemy operacyjne

* Pliki pamięci podręcznej programu Microsoft Outlook (* .ost), ale należy utworzyć kopię zapasową lokalnych magazynów danych programu Outlook (* .pst) (w rzeczywistości w wielu przypadkach mogą to być najbardziej krytyczne pliki w kopii zapasowej)

* Pliki dziennika wydajności w katalogach o nazwie PerfLogs

* Niepotrzebne pliki, które użytkownicy tworzą jako osobiste pliki tymczasowe do przechowywania informacji, na przykład plik tekstowy, w którym użytkownik wpisuje numer telefonu podyktowany mu przez kogoś, ale który od tego czasu wszedł do swojego katalogu smartfona.

Kopie zapasowe w aplikacji

Niektóre aplikacje mają wbudowane funkcje tworzenia kopii zapasowych, które chronią Cię przed utratą pracy w przypadku awarii komputera, awarii zasilania lub wyczerpania baterii. Jednym z takich programów jest Microsoft Word, który oferuje użytkownikom możliwość skonfigurowania częstotliwości zapisywania plików w celu Autoodzyskiwania. Dla większości ludzi ta funkcja jest dość cenna. Autor tej książki skorzystał nawet z tej funkcji podczas pisania tej książki! Chociaż mechanizm konfiguracji Autoodzyskiwania różni się w niektórych wersjach programu Word, w większości nowoczesnych wersji proces przebiega następująco lub podobnie: Wybierz Plik ⇒ Opcje ⇒ Zapisz i skonfiguruj opcje według własnego uznania. Kopie zapasowe w aplikacji zwykle trwają zaledwie kilka sekund, aby skonfigurować, normalnie działają bez aktywnego udziału i mogą zaoszczędzić wiele irytacji. W prawie wszystkich przypadkach należy włączyć tę funkcję, jeśli istnieje.

Odkrywanie narzędzi do tworzenia kopii zapasowych

Możesz używać wielu typów narzędzi do tworzenia, zarządzania i przywracania z kopii zapasowych. Narzędzia mogą na przykład zautomatyzować różne typy kopii zapasowych lub zarządzać procesem ciągłej synchronizacji kopii zapasowych. Narzędzia do tworzenia kopii zapasowych są dostępne w różnych przedziałach cenowych, w zależności od ich solidności i skalowalności.

Oprogramowanie do tworzenia kopii zapasowych

Oprogramowanie do tworzenia kopii zapasowych to oprogramowanie zaprojektowane specjalnie do uruchamiania i zarządzania kopią zapasową i przywracanie z kopii zapasowych. Można znaleźć wielu dostawców takiego oprogramowania, a ich dokładne funkcje różnią się w zależności od produktów i obsługiwanych przez nie platform (na przykład funkcje mogą się różnić w wersjach tego samego

pakietu oprogramowania do tworzenia kopii zapasowych dla systemów Windows i Mac). Niektóre oferty są przeznaczone dla użytkowników domowych, inne dla dużych przedsiębiorstw, a inne dla prawie wszystkich poziomów pośrednich. Za pomocą oprogramowania do tworzenia kopii zapasowych można ręcznie lub automatycznie tworzyć kopie zapasowe - to znaczy można je skonfigurować do tworzenia kopii zapasowych określonych systemów, danych, dysków lub folderów w określonym czasie, przy użyciu różnych modeli kopii zapasowych, takich jak pełne, przyrostowe itp. Kopie zapasowe można uruchamiać tylko wtedy, gdy komputer jest włączony. Upewnij się więc, że urządzenie, którego kopia zapasowa ma być utworzona, jest wtedy włączone! (Niektóre programy do tworzenia kopii zapasowych można skonfigurować w przypadku utraty kopii zapasowej tak, aby uruchamiały ją przy następnym uruchomieniu urządzenia lub bezczynności). Konfiguracja oprogramowania do tworzenia kopii zapasowych może zająć trochę czasu, ale po wykonaniu tej czynności często może proces tworzenia odpowiednich kopii zapasowych jest znacznie łatwiejszy niż jakakolwiek inna metoda tworzenia kopii zapasowych. Idealnie byłoby, gdybyś skonfigurował swoje systemy tak, aby automatycznie tworzyły kopie zapasowe w określonych momentach, aby mieć pewność, że faktycznie wykonujesz kopie zapasowe i nie zaniedbuj ich wykonywania podczas wykonywania wielu czynności, które pojawiają się w życiu. Nie myl tych ręcznych i automatycznych opcji z ręcznym i automatycznym kopiowaniem zadań. Jeśli właśnie pracowałeś nad jakimś ważnym projektem lub spędziłeś wiele godzin na tworzeniu nowej pracy na swoim komputerze, możesz chcieć wykonać dodatkową ręczną kopię zapasową, aby chronić swoją pracę i czas, który w nią zainwestowałeś.

Uważaj na fałszywe oprogramowanie do tworzenia kopii zapasowych! Osoby pozbawione skrupułów oferują bezpłatne oprogramowanie do tworzenia kopii zapasowych, które zawiera złośliwe oprogramowanie o różnej wadze, od irytującego oprogramowania reklamowego po infektory wykradające dane. Upewnij się, że otrzymujesz oprogramowanie do tworzenia kopii zapasowych (a także wszelkie inne używane oprogramowanie) z wiarygodnego źródła.

Oprogramowanie do tworzenia kopii zapasowych dla konkretnego dysku

Niektóre zewnętrzne dyski twarde i urządzenia półprzewodnikowe mają wbudowane oprogramowanie do tworzenia kopii zapasowych. Takie oprogramowanie jest często niezwykle intuicyjne i łatwe w użyciu, a użytkownicy mogą uznać je za najwygodniejszy sposób konfigurowania procedur tworzenia kopii zapasowych. Jednak trzy zastrzeżenia:

* Pamiętaj, aby nie pozostawiać dysku podłączonego do systemu, na którym znajduje się podstawowy magazyn danych.

* W przypadku korzystania z wersji oprogramowania do tworzenia kopii zapasowych dla konkretnego dysku może być konieczne zakupienie wszystkich dysków do tworzenia kopii zapasowych od tego samego producenta, aby nie komplikować procedur tworzenia kopii zapasowych i przywracania.

* Oprogramowanie przeznaczone do dysków jest mniej prawdopodobne, aby obsługiwać nowsze technologie, ponieważ pojawiają się one od innych dostawców, niż ogólne oprogramowanie do tworzenia kopii zapasowych.

Kopia zapasowa systemu Windows

System Windows jest wyposażony we wbudowane podstawowe oprogramowanie do tworzenia kopii zapasowych. Oprogramowanie ma kilka funkcji i dla wielu osób może być wystarczające. Korzystanie z kopii zapasowej systemu Windows jest z pewnością lepsze niż całkowity brak kopii zapasowej. Kopię zapasową systemu Windows można skonfigurować w dwóch miejscach:

* W aplikacji Ustawienia, w sekcji Aktualizacja i zabezpieczenia.

* Za pomocą tradycyjnego Panelu sterowania, który można uruchomić z menu Start. Kopia zapasowa i przywracanie to element w tradycyjnym widoku Wszystkie elementy lub w sekcji System i zabezpieczenia w widoku nowoczesnym.

Ponadto narzędzie do tworzenia kopii zapasowych plików systemu Windows automatycznie tworzy kopie zapasowe plików podczas ich modyfikacji. Możesz uzyskać dostęp do jego opcji konfiguracyjnych za pomocą opcji Historia plików w Panelu sterowania. Jeśli masz dużo miejsca na dysku i pracujesz wydajnie, upewnij się, że kopie zapasowe plików są tworzone dość często.

Kopia zapasowa smartfona / tabletu

Wiele urządzeń jest wyposażonych w możliwość automatycznej synchronizacji danych z chmurą - proces, który umożliwia przywrócenie danych na nowe urządzenie w przypadku zgubienia lub kradzieży urządzenia. Nawet urządzenia, które nie mają wbudowanej tej funkcji, prawie zawsze mogą uruchamiać oprogramowanie, które skutecznie udostępnia te funkcje dla określonego drzewa folderów lub dysku. Korzystanie z funkcji synchronizacji zapewnia doskonałą ochronę, ale oznacza również, że Twoje dane znajdują się w chmurze - co oznacza po prostu, że znajdują się na komputerze innej osoby - i są potencjalnie dostępne zarówno dla dostawcy usług chmurowych (w przypadku większości smartfonów dostawcą byłby Apple lub Google), a także jakimkolwiek agencjom rządowym, które żądają dostępu do odpowiednich danych uzbrojonych w nakaz, nieuczciwych insiderów lub hakerów, którym w jakiś sposób udaje się uzyskać do nich dostęp. Nawet jeśli nie popełniłeś żadnych przestępstw, rząd może nadal żądać Twoich danych w ramach procedur gromadzenia danych związanych z przestępstwami popełnionymi przez inne osoby. Nawet jeśli ufasz, że rząd nie nadużyje twoich danych, sam rząd doświadczył kilku naruszeń i wycieków danych, więc masz dobry powód, aby nie ufać mu, aby odpowiednio chronić twoje informacje przed kradzieżą przez inne strony, które mogą je wykorzystać. Zanim zdecydujesz, czy chcesz korzystać z synchronizacji, zastanów się nad zaletami i wadami.

Ręczne kopiowanie kopii zapasowych plików lub folderów

Ręczne kopie zapasowe są dokładnie takie, jak brzmią: kopie zapasowe wykonywane ręcznie, często przez kopiowanie plików, folderów lub obu z ich podstawowego dysku twardego (lub dysku SSD) do folderu sieciowego lub pendrive'a.

Ręczne tworzenie kopii zapasowych ma swój cel, ale używanie ich samodzielnie nie jest zazwyczaj dobrą strategią tworzenia kopii zapasowych. Ludzie nieuchronnie nie wykonują takich kopii zapasowych tak często, jak powinni, nie przechowują ich w odpowiedni sposób i często nie tworzą kopii zapasowych wszystkich elementów, które powinni przechowywać.

Automatyczne kopie zapasowe plików zadań lub folderów

Kopie zapasowe zadań automatycznych to zasadniczo ręczne kopie zapasowe na sterydach; są to ręczne kopie zapasowe, które są automatycznie uruchamiane przez komputer, a nie przez ludzi, którzy ręcznie je wyrzucają. Automatyzacja procesu tworzenia kopii zapasowej zmniejsza ryzyko zapomnienia lub braku kopii zapasowej z powodu pośpiechu, ale kopiowanie plików i folderów jest nadal ryzykowne, ponieważ jeśli niektóre poufne informacje z jakiegoś powodu nie są przechowywane we właściwym folderze, może nie ma kopii zapasowej. Jedynym możliwym wyjątkiem jest przypadek dysków wirtualnych. Jeśli ktoś zautomatyzuje proces kopiowania pliku zawierającego cały dysk na którym się znajduje lub przechowuje wszystkie swoje pliki danych, takie kopie zapasowe mogą być wystarczające. Jednak dla większości użytkowników domowych skonfigurowanie procedury automatycznego

kopiowania nie jest praktycznym rozwiązaniem. Korzystanie z oprogramowania do tworzenia kopii zapasowych jest znacznie prostszą i lepszą opcją.

Kopie zapasowe danych stron trzecich hostowane przez strony trzecie

Jeśli przechowujesz jakiekolwiek dane w chmurze lub korzystasz z usługi strony trzeciej do hostowania dowolnego ze swoich systemów lub danych, strona będąca właścicielem fizycznych i / lub wirtualnych systemów, w których znajdują się Twoje dane, może wykonać ich kopię zapasową lub nie - często bez Twoja wiedza lub aprobata. Jeśli na przykład przechowujesz dane na Dysku Google, nie masz absolutnie żadnej kontroli nad tym, ile kopii twoich danych przez Google. Podobnie, jeśli korzystasz z usługi strony trzeciej, takiej jak Facebook, wszelkie dane, które przesyłasz na serwery giganta mediów społecznościowych - niezależnie od ustawień prywatności, które ustawiłeś dla przesyłania (lub nawet jeśli je usunąłeś) - mogą zostać objęte kopią zapasową przez Facebooka do tylu kopii zapasowych, ile firma sobie życzy, w tak wielu różnych lokalizacjach, jak sobie tego życzy. W niektórych przypadkach kopie zapasowe innych firm przypominają kopie zapasowe dysków. Chociaż dostawca ma kopię zapasową Twoich danych, tylko Ty - strona będąca „właścicielem" danych - możesz je odczytać z kopii zapasowej w niezaszyfrowanej formie. Jednak w innych przypadkach dane z kopii zapasowej są dostępne dla każdego, kto ma dostęp do kopii zapasowej. To powiedziawszy, większość dużych firm zewnętrznych ma solidną nadmiarową infrastrukturę i systemy kopii zapasowych, co oznacza, że prawdopodobieństwo, że dane przechowywane w ich infrastrukturze pozostaną dostępne dla użytkowników, jest niezwykle wysokie w porównaniu z danymi w domach większości ludzi.

Wiedząc, gdzie wykonać kopię zapasową

Aby kopie zapasowe miały jakąkolwiek wartość, muszą być odpowiednio przechowywane, aby w razie potrzeby można było do nich szybko i łatwo uzyskać dostęp. Ponadto nieprawidłowe przechowywanie kopii zapasowych może poważnie naruszyć bezpieczeństwo informacji zawartych w kopiach zapasowych. Prawdopodobnie słyszałeś historie o niezaszyfrowanych taśmach zapasowych, które zawierały poufne informacje, które zostały zgubione lub skradzione. To powiedziawszy, nie ma jednego uniwersalnego podejścia do prawidłowego przechowywania kopii zapasowych. Możesz tworzyć kopie zapasowe w różnych miejscach, co skutkuje różnymi lokalizacjami przechowywania.

Lokalny magazyn

Przechowywanie lokalnej kopii kopii zapasowej - mającej miejsce w pobliżu domowego komputera lub łatwo dostępnej dla właściciela smartfona, tabletu lub laptopa - to dobry pomysł. Jeśli przypadkowo usuniesz plik, możesz szybko przywrócić go z kopii zapasowej. To powiedziawszy, nigdy nie powinieneś przechowywać wszystkich kopii zapasowych lokalnie. Jeśli na przykład przechowujesz kopie zapasowe w swoim domu, a Twój dom miałby zostać poważnie uszkodzony w wyniku klęski żywiołowej, możesz jednocześnie stracić podstawowy magazyn danych (na przykład komputer domowy) i kopie zapasowe. Kopie zapasowe należy zawsze przechowywać w bezpiecznym miejscu - nie na półce z książkami. Ognioodporny i wodoodporny sejf przykręcony do podłogi lub przymocowany do ściany to dwie dobre opcje. Należy również pamiętać, że dyski twarde i inne nośniki magnetyczne mają mniejsze szanse na przetrwanie niektórych katastrof niż dyski półprzewodnikowe, pendrive'y i inne urządzenia zawierające układy pamięci.

Przechowywanie poza siedzibą

Ponieważ jednym z celów tworzenia kopii zapasowych jest umożliwienie zachowania danych (i systemów) nawet w przypadku zniszczenia podstawowej kopii, chcesz mieć co najmniej jedną kopię zapasową poza siedzibą firmy - czyli w innej lokalizacji niż podstawowy magazyn danych. Istnieją różne

opinie co do tego, jak daleko od głównego magazynu należy przechowywać kopię zapasową. Zasadniczo ogólną zasadą jest przechowywanie kopii zapasowych na tyle daleko, aby klęska żywiołowa, która miała poważny wpływ na lokację główną, nie wpłynęłaby na drugą. Niektórzy ludzie przechowują kopię zapasową swoich danych w ognioodpornej i wodoodpornej torbie w sejfie. Sejfy bankowe zwykle są w stanie przetrwać klęski żywiołowe, więc nawet jeśli bank znajduje się stosunkowo blisko siedziby głównej, kopia zapasowa prawdopodobnie przetrwa, nawet jeśli nie będzie można jej odzyskać przez kilka dni.

Chmura

Tworzenie kopii zapasowych w chmurze zapewnia korzyści z przechowywania poza siedzibą firmy. Jeśli na przykład stracisz cały swój sprzęt i systemy w wyniku klęski żywiołowej, kopia twoich danych prawie zawsze będzie nadal istnieć w chmurze. Z praktycznego punktu widzenia istnieje również prawdopodobieństwo, że zespół ds. Bezpieczeństwa informacji u dowolnego dużego dostawcy pamięci masowej w chmurze ma znacznie większą wiedzę na temat zabezpieczania danych niż większość osób i ma do dyspozycji narzędzia, na które przeciętny człowiek nie może sobie pozwolić. zakup lub licencja. Jednocześnie tworzenie kopii zapasowych w chmurze ma swoje wady. Korzystając z kopii zapasowej w chmurze, polegasz na firmie zewnętrznej, która chroni Twoje dane. Chociaż strona ta może dysponować większą wiedzą i lepszymi narzędziami, jej głównym zmartwieniem nie jesteś Ty. Jeśli na przykład dojdzie do naruszenia i dotknie to dużych klientów, jego priorytetem może być zajęcie się ich obawami przed zajęciem się twoimi. Ponadto duże witryny są często głównym celem hakerów, ponieważ wiedzą, że takie witryny zawierają skarbnicę danych, znacznie większą niż to, co mogą być w stanie wydobyć z domowego komputera. Oczywiście, jeśli rząd wyda nakaz dostawcy chmury, organy ścigania mogą uzyskać kopie twoich kopii zapasowych - nawet w niektórych przypadkach, jeśli nakaz został doręczony, ponieważ wykazał prawdopodobną przyczynę tylko tego, że ktoś inny (a nie ty) popełnił przestępstwo. To powiedziawszy, dla większości ludzi tworzenie kopii zapasowych w chmurze ma sens, ponieważ zalety przeważają nad wadami, zwłaszcza jeśli szyfrujesz kopie zapasowe, przez co ich zawartość jest niedostępna dla dostawcy chmury. Jeśli chodzi o komputery, chmura naprawdę oznacza „komputery innych osób". Za każdym razem, gdy przechowujesz poufne dane, w tym poufne dane w kopiach zapasowych, w chmurze, tak naprawdę przechowujesz je na jakimś fizycznym komputerze należącym do kogoś innego. Dostawca chmury może oferować lepsze zabezpieczenia niż Ty sam możesz zaoferować, ale nie oczekuj, że korzystanie z chmury w magiczny sposób wyeliminuje zagrożenia dla cyberbezpieczeństwa.

Pamięć sieciowa

Tworzenie kopii zapasowych na dysku sieciowym oferuje połączenie funkcji z kilku wcześniejszych lokalizacji do przechowywania kopii zapasowych. Podobnie jak lokalna kopia zapasowa, sieciowa kopia zapasowa jest zwykle łatwo dostępna, ale być może z nieco mniejszą szybkością. Podobnie jak w przypadku kopii zapasowej poza siedzibą firmy, jeśli serwer sieciowy, na którym znajduje się kopia zapasowa, znajduje się poza siedzibą firmy, kopia zapasowa jest chroniona przed problemami z lokacją w pierwotnej lokalizacji danych. Jednak w przeciwieństwie do kopii zapasowych poza siedzibą firmy, jeśli nie masz pewności, że pliki znajdują się poza siedzibą firmy, mogą znajdować się w tym samym miejscu, co dane podstawowe. Podobnie jak w przypadku kopii zapasowych w chmurze, kopie zapasowe oparte na sieci można przywrócić na inne urządzenia w sieci. W przeciwieństwie do kopii zapasowej w chmurze może być dostępna tylko dla urządzeń w tej samej sieci prywatnej (co może być problemem lub, w niektórych sytuacjach, dobrą rzeczą z punktu widzenia bezpieczeństwa). Ponadto pamięć sieciowa jest często wdrażana z nadmiarowymi dyskami i automatycznymi kopiami zapasowymi, oferując lepszą ochronę danych niż wiele innych opcji przechowywania. Jeśli używasz sieciowej pamięci masowej do tworzenia kopii zapasowych, upewnij się, że dowolny mechanizm

używany do tworzenia kopii zapasowych (na przykład oprogramowanie do tworzenia kopii zapasowych) ma odpowiednie uprawnienia sieciowe do zapisu w magazynie. W wielu przypadkach może być konieczne skonfigurowanie loginu i hasła.

Mieszanie miejsc

Nie ma powodu, aby tworzyć kopie zapasowe tylko w jednej lokalizacji. Z punktu widzenia szybkiego przywracania danych, im więcej miejsc, w których masz bezpieczne kopie zapasowe danych, tym lepiej. W rzeczywistości różne lokalizacje zapewniają różne rodzaje ochrony zoptymalizowane pod kątem różnych sytuacji. Utrzymywanie jednej kopii lokalnej, aby można było szybko przywrócić przypadkowo usunięty plik, a także przechowywanie kopii zapasowej w chmurze, na przykład w przypadku klęski żywiołowej, ma sens dla wielu osób. Pamiętaj jednak, że jeśli przechowujesz kopie zapasowe w wielu lokalizacjach, musisz upewnić się, że wszystkie lokalizacje są bezpieczne. Jeśli nie masz pewności co do bezpieczeństwa jakiejś formy kopii zapasowej, uważaj i nie rób tam kopii tylko dlatego, że „im więcej kopii zapasowych, tym lepiej". Ponieważ różne lokalizacje kopii zapasowych mają różne mocne i słabe strony, korzystanie z wielu lokalizacji kopii zapasowych może lepiej chronić przed większą liczbą zagrożeń niż korzystanie z jednej lokalizacji.

Wiedząc, gdzie nie przechowywać kopii zapasowych

Nigdy, przenigdy nie przechowuj kopii zapasowych podłączonych do komputera lub sieci, chyba że masz inną kopię zapasową, którą chcesz odzyskać w przypadku ataku złośliwego oprogramowania. Ransomware, które infekuje komputer i sprawia, że pliki na nim są niedostępne, może zrobić to samo z dołączoną kopią zapasową. Po utworzeniu kopii zapasowej nigdy nie pozostawiaj dysków twardych ani dysków SSD z kopiami zapasowymi podłączonych do systemów lub sieci, których kopie zapasowe są tworzone. Każde złośliwe oprogramowanie, które infekuje system podstawowy, może również rozprzestrzenić się na kopie zapasowe. Usunięcie kopii zapasowej z połączenia z materiałem, którego kopia zapasowa jest tworzona, może spowodować różnicę między szybkim odzyskaniem danych po ataku ransomware a koniecznością zapłacenia przestępcy drogiego okupu. Jeśli utworzysz kopię zapasową na nośniku typu jednokrotnego, wielokrotnego odczytu, który jest obecnie najczęściej spotykany w postaci dysków CD-R i DVD-R, po sfinalizowaniu kopii zapasowej można bezpiecznie zostawić kopię zapasową na dołączonym dysku nagrywanie kopii zapasowej i ustaw dysk jako tylko do odczytu.

Szyfrowanie kopii zapasowych

Kopie zapasowe mogą łatwo stać się słabym punktem w łańcuchu bezpieczeństwa ochrony danych. Osoby, które sumiennie chronią swoje dane osobowe oraz organizacje, które starają się robić to samo ze swoimi poufnymi i zastrzeżonymi informacjami, często nie zapewniają takiego samego poziomu ochrony dokładnie tych samych danych, gdy znajdują się one w kopiach zapasowych, a nie w ich podstawowych Lokalizacja. Jak często słyszymy wiadomości, na przykład o danych wrażliwych, które są zagrożone, ponieważ znajdowały się w niezaszyfrowanej formie na taśmach kopii zapasowych, które zostały zgubione lub skradzione? Ogólnie rzecz biorąc, jeśli nie wiesz, czy zaszyfrować kopię zapasową, prawdopodobnie powinieneś. Pamiętaj, aby zaszyfrować kopie zapasowe, jeśli zawierają poufne informacje, co w większości przypadków tak jest. W końcu, jeśli dane są na tyle ważne, że można je zarchiwizować, istnieje duże prawdopodobieństwo, że przynajmniej część z nich jest poufna i powinna być zaszyfrowana. Pamiętaj tylko, aby odpowiednio zabezpieczyć hasło potrzebne do odblokowania kopii zapasowych. Pamiętaj, że może minąć trochę czasu, zanim rzeczywiście będziesz musiał użyć kopii zapasowych, więc nie polegaj na swojej pamięci, chyba że będziesz regularnie ćwiczyć używanie tego hasła do testowania kopii zapasowych.

Z praktycznego punktu widzenia wielu profesjonalnych administratorów systemów, którzy codziennie mają do czynienia z wieloma kopiami zapasowymi, nigdy nie widziało kopii zapasowej, która nie wymagałaby szyfrowania.

Ustalanie, jak często należy wykonywać kopie zapasowe

Nie ma jednej uniwersalnej reguły określającej, jak często należy tworzyć kopie zapasowe systemu i danych. Ogólnie rzecz biorąc, chcesz mieć pewność, że nigdy nie stracisz wystarczającej ilości pracy, która spowodowałaby znaczny ból serca.

Codzienne wykonywanie pełnej kopii zapasowej wymaga największej ilości miejsca na kopie zapasowe, a także zajmuje najwięcej czasu. Oznacza to jednak, że dostępnych jest więcej wszystkich kopii danych - więc jeśli kopia zapasowa uległaby uszkodzeniu w tym samym czasie co podstawowy magazyn danych, prawdopodobnie mniej danych zostało utraconych - i mniej kopii zapasowych jest wymaganych do wykonania systemu lub przywrócenie danych. Codzienne wykonywanie pełnej kopii zapasowej może być wykonalne dla wielu osób, zwłaszcza tych, które mogą wykonywać kopie zapasowe po godzinach pracy lub podczas snu w nocy. Taka strategia zapewnia najlepszą ochronę. Ponieważ ceny pamięci masowej gwałtownie spadały w ostatnich latach, koszt tego, który kiedyś był zaporowy dla większości osób, jest obecnie dostępny dla większości ludzi. Niektóre osoby i organizacje decydują się na cotygodniowe tworzenie pełnej kopii zapasowej i łączą tę kopię z codziennymi przyrostowymi lub różnicowymi kopiami zapasowymi. Pierwsza strategia zapewnia najszybszą procedurę tworzenia kopii zapasowych; ta ostatnia zapewnia szybszą procedurę odzyskiwania i zmniejsza liczbę kopii zapasowych potrzebnych do przywrócenia do maksymalnie dwóch zamiast siedmiu. Dodatkowo rozważ użycie ręcznych kopii zapasowych lub automatycznego schematu tworzenia kopii zapasowych w aplikacji, jeśli pracujesz nad ważnymi materiałami w ciągu dnia. Na przykład korzystanie z automatycznych kopii zapasowych w aplikacji w programie Word może uchronić Cię przed utratą godzin pracy w przypadku awarii komputera. Podobnie kopiowanie dokumentów do drugiej lokalizacji może zapobiec utracie znacznej ilości pracy w przypadku awarii dysku twardego lub dysku SSD. W przypadku aplikacji, które nie mają funkcji automatycznego tworzenia kopii zapasowych w aplikacji, niektórzy ludzie sugerują okresowe korzystanie z opcji menu Wyślij w systemie Windows lub Mac, aby wysyłać do siebie kopie plików, nad którymi pracują, pocztą elektroniczną. Chociaż nie jest to formalna strategia tworzenia kopii zapasowych, zapewnia sposób tworzenia kopii zapasowych w ciągu dnia między regularnymi kopiami zapasowymi i często robi to poza siedzibą firmy, zapewniając, że gdyby komputer nagle umarł, nie wystarczyłoby całego dnia pracy. zgubić się. Ogólnie rzecz biorąc, jeśli nie masz pewności, czy tworzysz kopie zapasowe wystarczająco często, prawdopodobnie nie .

Utylizacja kopii zapasowych

Ludzie i organizacje często przechowują kopie zapasowe przez długi czas - czasami zachowując materiały tak długo, że szyfrowanie używane do ochrony wrażliwych danych na nośnikach kopii zapasowych nie jest już wystarczające, aby odpowiednio chronić informacje przed wścibskimi oczami. W związku z tym konieczne jest, aby od czasu do czasu niszczyć kopie zapasowe lub tworzyć je ponownie. Zarówno formaty sprzętu, jak i oprogramowania zmieniają się w czasie. Jeśli tworzyłeś kopie zapasowe na taśmach w latach 80., na Bernoulli Boxes na początku lat 90. lub na dyskach Zip pod koniec lat 90., możesz mieć trudności z przywracaniem z kopii zapasowych dzisiaj, ponieważ możesz mieć problemy z uzyskaniem niezbędnego sprzętu, zgodnych sterowników i innego oprogramowania potrzebnego do odczytu kopii zapasowych na nowoczesnym komputerze. Podobnie, jeśli wykonałeś kopię zapasową danych wraz z różnymi programami DOS lub wczesnymi 16-bitowymi plikami wykonywalnymi Windows potrzebnymi do przetworzenia zawartości tych kopii zapasowych, możesz nie być w stanie przywrócić z kopii zapasowych na wielu nowoczesnych maszynach, które mogą nie

być w stanie uruchomić plików wykonywalnych. Oczywiście, jeśli wykonałeś pełny obraz systemu maszyny 20 lat temu, dziś będziesz miał trudności z przywróceniem z obrazu (możesz to zrobić za pomocą maszyn wirtualnych - coś znacznie przekraczającego poziom umiejętności technicznych większości użytkowników) . Nawet niektóre starsze wersje plików danych mogą nie działać łatwo. Na przykład dokumenty Word z połowy lat 90., które mogą być zainfekowane różnymi formami złośliwego oprogramowania, nie otwierają się we współczesnych wersjach programu Word, chyba że użytkownik zezwoli na taki dostęp, co może być trudne lub niemożliwe do wykonania w określonych środowiskach korporacyjnych. Formaty plików używane specjalnie przez oprogramowanie, które już dawno zniknęło całkowicie z rynku, mogą być jeszcze trudniejsze do otwarcia. W związku z tym stare kopie zapasowe mogą i tak nie mieć dla Ciebie dużej wartości. Tak więc, gdy kopia zapasowa nie jest już wartościowa lub gdy jej ochrona danych może być zagrożona, kopia nie jest już wartościowa lub gdy jej ochrona danych może być zagrożona, należy się jej pozbyć. W jaki sposób należy pozbyć się taśm, dysków itp. Z kopiami zapasowymi? Czy możesz po prostu wyrzucić je do kosza? Nie, nie rób. Może to całkowicie podważyć bezpieczeństwo danych w kopiach zapasowych. Zamiast tego użyj jednej z następujących metod:

* Nadpisywanie: różne programy będą kilkakrotnie nadpisywać każdy sektor nośnika pamięci (rzeczywista liczba razy zależy od poziomu bezpieczeństwa określonego przez użytkownika), co utrudni, jeśli nie uniemożliwi, późniejsze odzyskanie danych z wycofanych nośników.

* Rozmagnesowanie: różne urządzenia zawierające silne magnesy mogą być używane do fizycznego renderowania danych na nośnikach magnetycznych (takich jak dyski twarde i dyskietki) niedostępne po wystawieniu nośnika na działanie silnego pola magnetycznego.

* Spalanie: Często wystarczy spalenie nośnika pamięci w ogniu o wysokiej temperaturze, aby go zniszczyć. Nie próbuj tego samodzielnie. Jeśli chcesz realizować taką metodę, znajdź profesjonalistę z doświadczeniem. Proces spalania różni się w zależności od rodzaju zastosowanych mediów.

* Niszczenie: Cięcie nośnika na drobne kawałki. Idealnie, takie media powinny być całkowicie sproszkowane na pył. W każdym razie niszczenie za pomocą staromodnej niszczarki, która tnie nośnik na paski, generalnie nie jest uważane za bezpieczne usuwanie nośników, które nie zostało wcześniej nadpisane lub rozmagnesowane.

Nie potrafię przecenić wagi prawidłowego przechowywania i usuwania kopii zapasowych. Poważne wycieki danych wynikały z nośników kopii zapasowych, które zostały utracone po dłuższym przechowywaniu.

Testowanie kopii zapasowych

Wielu ludzi sądziło, że mają odpowiednie kopie zapasowe tylko po to, aby w czasie, gdy musieli przywrócić, że kopie zapasowe były uszkodzone. Dlatego testowanie kopii zapasowych jest krytyczne. Chociaż teoretycznie należy przetestować każdą utworzoną kopię zapasową i sprawdzić, czy każdy element z kopii zapasowej można przywrócić, taki schemat jest niepraktyczny dla większości ludzi. Należy jednak przetestować pierwszą kopię zapasową utworzoną za pomocą dowolnego oprogramowania, sprawdzić pliki autoodzyskiwania przy pierwszym użyciu programu Word i tak dalej. Niektóre programy do tworzenia kopii zapasowych mają możliwość weryfikacji kopii zapasowych - to znaczy po wykonaniu kopii zapasowej sprawdza, czy oryginalne dane i dane w kopiach są zgodne. Przeprowadzenie takiej weryfikacji po utworzeniu kopii zapasowej znacznie wydłuża proces tworzenia kopii zapasowej, ale warto ją przeprowadzić, jeśli możesz to zrobić, ponieważ pomaga to upewnić się, że nic nie zostało nieprawidłowo zarejestrowane lub w inny sposób nie uległo uszkodzeniu podczas procesu tworzenia kopii zapasowej.

Wykonywanie kopii zapasowych kryptowalut

Ponieważ kryptowaluta jest śledzona w księdze i nie jest przechowywana w banku, tworzenie kopii zapasowej kryptowaluty obejmuje tworzenie kopii zapasowych kluczy prywatnych używanych do kontrolowania adresów w księdze, w której znajduje się kryptowaluta, a nie tworzenie kopii zapasowej samej kryptowaluty. Często klucze nie są utrzymywane elektronicznie. Są wydrukowane na papierze i przechowywane w sejfie bankowym lub ognioodpornym sejfie. Dla tych, którzy używają portfeli sprzętowych do przechowywania kluczy do swojej kryptowaluty, kopia zapasowa urządzenia portfela jest często ziarenkiem odzyskiwania, czyli listą słów, które pozwalają urządzeniu odtworzyć klucze potrzebne do odpowiednich adresów. Powszechnie przyjmuje się, że lista słów powinna być zapisywana na papierze i przechowywana w sejfie bankowym i / lub sejfie, a nie elektronicznie.

Tworzenie kopii zapasowych haseł

Za każdym razem, gdy tworzysz kopię zapasową listy haseł, upewnij się, że robisz to w bezpieczny sposób. W przypadku ważnych haseł, które nie zmieniają się często i prawdopodobnie nie będą potrzebne w trybie pilnym, rozważ w ogóle nie zapisywanie ich w postaci cyfrowej. Zamiast tego zapisz je na kartce papieru i włóż ją do skrytki bankowej.

Tworzenie dysku rozruchowego

Jeśli kiedykolwiek będziesz musiał ponownie utworzyć system, będziesz potrzebować możliwości rozruchu komputera, więc w ramach procesu tworzenia kopii zapasowej powinieneś utworzyć dysk z tablicą rozruchową. W przypadku większości smartfonów i tabletów utworzenie dysku rozruchowego nie stanowi problemu, ponieważ zresetowanie urządzenia do ustawień fabrycznych spowoduje jego rozruch. Jednak taka prostota nie zawsze występuje w przypadku komputerów, więc podczas wykonywania pierwszej kopii zapasowej najlepiej byłoby utworzyć dysk rozruchowy, z którego można bezpiecznie uruchomić komputer (innymi słowy, bez złośliwego oprogramowania itp.). Większość pakietów oprogramowania do tworzenia kopii zapasowych przeprowadzi Cię przez ten proces, a niektórzy producenci komputerów zrobią to samo podczas pierwszego uruchomienia systemu. Różne pakiety oprogramowania zabezpieczającego są również rozprowadzane na rozruchowych dyskach CD lub DVD.