Przywracanie z kopii zapasowych

Tworzenie kopii zapasowych jest kluczowym elementem każdego planu bezpieczeństwa cybernetycznego. Po zresetowaniu urządzenia do ustawień fabrycznych w ramach procesu przywracania możesz przywrócić dane i programy.

Twoje urządzenie będzie działać normalnie. Ponieważ większość ludzi nie musi regularnie przywracać danych z kopii zapasowych i ponieważ przywracanie jest zwykle wykonywane po wystąpieniu „złego" zdarzenia, które wymusiło konieczność przywracania, wiele osób po raz pierwszy doświadcza procesu przywracania z kopii zapasowych, gdy są bardzo zestresowani. W związku z tym ludzie są podatni na błędy podczas przywracania, co może prowadzić do tego ,że dane są tracone na zawsze. Na szczęście dowiesz się, jak przywrócić.

Będziesz musiał przywrócić

Szanse są bliskie 100 procent, że w pewnym momencie utracisz dostęp do jakiegoś pliku, do którego nadal potrzebujesz dostępu, a przywrócenie z kopii zapasowej uratuje Ci życie. Ale przywrócenie niekoniecznie jest proste. Przed wykonaniem odbudowy należy wziąć pod uwagę różne czynniki. Właściwe planowanie i wykonanie może mieć wpływ na odzyskanie utraconych danych i utratę jeszcze większej ich liczby.

Przywracanie z kopii zapasowych nie jest tak proste, jak wiele osób myśli. Poświęć trochę czasu na przeczytanie tego rozdziału przed wykonaniem przywracania.

Czekać! Nie przywracaj jeszcze!

Zauważyłeś, że brakuje niektórych danych, do których chcesz uzyskać dostęp. Zauważyłeś, że plik jest uszkodzony. Zauważyłeś, że jakiś program nie działa poprawnie. Więc powinieneś przywrócić z kopii zapasowej, prawda? Czekać! Przywracanie bez wiedzy, dlaczego wystąpił problem, może być niebezpieczne. Na przykład, jeśli masz infekcję złośliwym oprogramowaniem na komputerze, przywrócenie go, gdy złośliwe oprogramowanie jest nadal obecne, nie usunie zagrożenia i, w zależności od typu złośliwego oprogramowania i kopii zapasowej, może spowodować uszkodzenie plików w kopii zapasowej . Jeśli złośliwe oprogramowanie uszkodzi podstawowy magazyn danych, możesz utracić dane i nie mieć skąd je przywrócić! Na przykład osoby, które próbowały przywrócić dane z kopii zapasowych na zewnętrznych dyskach twardych, utraciły dane przez oprogramowanie ransomware. W momencie podłączenia zewnętrznego dysku do zainfekowanego komputera oprogramowanie ransomware rozprzestrzeniło się na kopię zapasową i również ją zaszyfrowało! Złośliwe oprogramowanie może również rozprzestrzeniać się na pamięć masową w chmurze. Samo posiadanie kopii zapasowej w chmurze nie jest powodem do przywrócenia, zanim dowiesz się, co się stało. Nawet w przypadku kopii zapasowych na nośnikach tylko do odczytu, których złośliwe oprogramowanie nie może zainfekować, próba przywrócenia ich przed zneutralizowaniem zagrożenia stwarzanego przez infekcję może stracić czas i potencjalnie dać złośliwemu oprogramowaniu dostęp do większej ilości danych do kradzieży. Przed przywróceniem danych z jakichkolwiek kopii zapasowych należy zdiagnozować źródło problemu, który powoduje konieczność przywrócenia. Jeśli na przykład przypadkowo usunąłeś plik i wiesz, że problem wystąpił z powodu twojego własnego błędu ludzkiego, z całą pewnością kontynuuj i przywróć.

Przywracanie z pełnych kopii zapasowych systemów

Pełna kopia zapasowa systemu to kopia zapasowa całego systemu, w tym pliku system operacyjny, programy / aplikacje, ustawienia i dane. Termin ten ma zastosowanie niezależnie od tego, czy urządzenie, którego kopia zapasowa jest tworzona, to smartfon, czy ogromny serwer w centrum

danych. W związku z tym proces przywracania odtwarza system, który jest faktycznie identyczny z tym, którego kopia zapasowa została utworzona w momencie tworzenia kopii zapasowej. (Nie jest to do końca prawdą w sensie absolutnym - na przykład zegar systemowy pokaże inny czas niż system pierwotny - ale jest to prawdą dla celów uczenia się o przywróceniu systemu).

Przywracanie na urządzenie komputerowe, na którym utworzono kopię zapasową. Przywracanie systemu z obrazu systemu działa najlepiej, gdy systemy są przywracane na to samo urządzenie komputerowe, z którego utworzono oryginalną kopię zapasową. Jeśli na przykład twój system został zainfekowany złośliwym oprogramowaniem i przywracasz na to samo urządzenie obraz utworzony przed infekcją złośliwym oprogramowaniem, system powinien działać dobrze. (Oczywiście straciłbyś pracę i inne aktualizacje wykonane od tego czasu, więc miejmy nadzieję, że wykonałeś ich kopię zapasową za pomocą jednej z metod opisanych w rozdziale 13.). Pełne przywrócenie systemu jest często nieodwracalne. Upewnij się, że chcesz go uruchomić, zanim to zrobisz. Przywracanie z pełnej kopii zapasowej systemu jest prawdopodobnie najszybszym sposobem na przywrócenie całego systemu, ale proces ten może zająć znacznie więcej czasu niż przywrócenie tylko kilku uszkodzonych plików. Jest również dużo bardziej prawdopodobne, że doprowadzi do przypadkowego usunięcia ustawień lub danych utworzonych od czasu ostatniej kopii zapasowej. W związku z tym pełnego przywracania systemu należy używać tylko wtedy, gdy jest naprawdę potrzebne. Jeśli przypadkowo usuniesz kilka plików lub nawet folderów, nie wykonuj pełnego przywracania systemu. Po prostu przywróć te pliki z kopii zapasowej, używając jednej z technik opisanych w dalszej części.

Przywracanie na inne urządzenie niż to, na którym utworzono kopię zapasową

Przywracanie systemu z obrazu często nie działa w systemie z zupełnie innymi komponentami sprzętowymi niż system, który był pierwotnie obrazowany. Ogólnie rzecz biorąc, im bardziej system różni się od systemu, który był obrazowany, tym więcej problemów można napotkać. Niektóre z tych problemów mogą ulec autokorekty. Jeśli na przykład przywracasz system ze sterownikami jednej karty graficznej do systemu z inną kartą graficzną, przywrócony system powinien zdać sobie sprawę, że zainstalowano niewłaściwe sterowniki i po prostu ich nie używać. Zamiast tego domyślnie korzysta ze sterowników wbudowanych w system operacyjny i umożliwia zainstalowanie sterowników dla właściwej karty (lub, w niektórych przypadkach, automatyczne pobranie ich lub wyświetlenie monitu). Niektóre problemy mogą nie zostać poddane autokorekty. Na przykład, jeśli komputer, którego kopia zapasowa została utworzona, używa standardowej klawiatury i myszy podłączonej przez USB, a urządzenie, do którego przywracasz, korzysta z zastrzeżonej klawiatury, która łączy się w inny sposób, może w ogóle nie działać po przywróceniu; może być konieczne podłączenie klawiatury USB do systemu w celu pobrania i zainstalowania sterowników zastrzeżonej klawiatury. Takie sytuacje stają się coraz rzadsze z powodu zarówno standaryzacji, jak i ulepszeń w nowoczesnych systemach operacyjnych, ale istnieją. Niektórych problemów nie da się naprawić. Jeśli spróbujesz przywrócić obraz systemu Maca na komputerze zaprojektowanym na przykład do uruchamiania systemu Windows, nie zadziała. Niektóre pakiety oprogramowania do tworzenia kopii zapasowych umożliwiają skonfigurowanie przywracania w celu zainstalowania oddzielnych sterowników lub wyszukania sterowników pasujących do sprzętu, na którym odbywa się przywracanie, w celu zastąpienia nieodpowiednich sterowników znalezionych w kopii zapasowej. Jeśli masz taką funkcję i masz trudności z przywróceniem jej bez niej, możesz spróbować. Pełna kopia zapasowa systemu może, ale nie musi, obejmować kopię zapasową całej zawartości na wszystkich dyskach podłączonych do systemu, a nie tylko na dyskach zamontowanych wewnątrz systemu. (Teoretycznie wszystkie takie dyski powinny być zawarte w obrazie systemu, ale termin obraz systemu jest często używany na oznaczenie obrazu wewnętrznych dysków twardych i dysków SSD). Jeśli urządzenie, dla którego masz obraz, ulegnie awarii, powinieneś móc użyć obrazu systemu do odtworzenia całego systemu, tak jak

był w momencie tworzenia kopii zapasowej. Gdy używasz odbudowanego systemu, powinien on działać dokładnie tak samo, jak poprzedni system w momencie tworzenia kopii zapasowej.

Oryginalne obrazy systemu

Jeśli chcesz przywrócić oryginalny obraz fabryczny systemu przed przywróceniem danych i programów, zapoznaj się z poprzednią częścią poświęconą wykonywaniu takich przywracania. Po przywróceniu ustawień fabrycznych jedna lub więcej (lub prawdopodobnie wszystkie) łatki i inne aktualizacje zabezpieczeń, które zainstalowałeś na urządzeniu, mogą zniknąć. Twoje urządzenie jest prawdopodobnie narażone na różne kompromisy. Dlatego natychmiast po przywróceniu należy uruchomić proces aktualizacji systemu operacyjnego (powtarzalnie, aż nie znajdzie żadnych potrzebnych aktualizacji), a także proces aktualizacji dowolnego oprogramowania zabezpieczającego (również powtarzalnie, dopóki nie znajdzie żadnych potrzebnych aktualizacji). Dopiero po wykonaniu tych czynności należy zainstalować inne oprogramowanie, przywrócić dane lub wykonać inne czynności online.

Późniejsze obrazy systemu

Przed przywróceniem z dowolnego obrazu systemu należy upewnić się, że jakikolwiek problem, który wymagał przywrócenia, nie pozostanie ani nie zostanie przywrócony podczas przywracania. Jeśli na przykład twój komputer został zainfekowany oprogramowaniem ransomware i usuwasz złośliwe oprogramowanie za pomocą oprogramowania zabezpieczającego, ale musisz przywrócić przestępnie zaszyfrowane pliki z kopii zapasowej, nie chcesz w końcu przywracać oprogramowania ransomware wraz z danymi. Jeśli wiesz na pewno, że obraz został wykonany przed pojawieniem się problemu, śmiało go wykorzystaj. Jeśli masz wątpliwości, jeśli to możliwe, przywróć urządzenie na dodatkowe urządzenie i przeskanuj je za pomocą oprogramowania zabezpieczającego przed wykonaniem właściwego przywracania. Jeśli nie masz dodatkowego urządzenia, które można przywrócić, i nie masz pewności, czy kopia zapasowa jest zainfekowana, możesz poprosić specjalistę, aby się przyjrzał.

Instalowanie oprogramowania zabezpieczającego

Po przywróceniu z obrazu systemu (czy to ustawień fabrycznych, czy późniejszego obrazu), pierwszą rzeczą, którą należy zrobić, jest sprawdzenie, czy jest zainstalowane oprogramowanie zabezpieczające. Jeśli tak nie jest, zainstaluj go. Tak czy inaczej, upewnij się, że uruchamiasz automatyczne aktualizacje, dopóki oprogramowanie nie będzie już wymagać aktualizacji. Zainstaluj oprogramowanie zabezpieczające przed podjęciem jakichkolwiek działań online lub przeczytaniem wiadomości e-mail. Jeśli nie masz zainstalowanego oprogramowania zabezpieczającego przed wykonaniem takich zadań, wykonanie ich może doprowadzić do naruszenia bezpieczeństwa urządzenia. Jeśli masz oprogramowanie zabezpieczające na płycie CD lub DVD, zainstaluj je stamtąd. Jeśli utworzyłeś napęd USB lub inny dysk z oprogramowaniem zabezpieczającym, możesz go stamtąd zainstalować. Jeśli nie, skopiuj oprogramowanie zabezpieczające na dysk twardy z dowolnego miejsca i uruchom je.

Oryginalny nośnik instalacyjny

W przypadku programów uzyskanych i zainstalowanych po zakupie urządzenia można je ponownie zainstalować po przywróceniu oryginalnego obrazu systemu lub nawet późniejszego obrazu utworzonego przed zainstalowaniem oprogramowania. W przypadku ponownej instalacji oprogramowania z dysku CD lub DVD wszelkie aktualizacje oprogramowania, które zostały wydane po utworzeniu dysku CD lub DVD, nie zostaną zainstalowane. Pamiętaj, aby skonfigurować program do automatycznej aktualizacji lub ręcznie pobrać i zainstalować takie aktualizacje. W niektórych przypadkach procedury instalacji oprogramowania mogą również pytać, czy chcesz, aby automatycznie

sprawdzały dostępność aktualizacji natychmiast po zakończeniu instalacji. Ogólnie rzecz biorąc, odpowiedź twierdząca jest mądrym pomysłem.

Pobrane oprogramowanie

Sposób ponownego zainstalowania programów, które zostały wcześniej zakupione i zainstalowane w pewnym momencie po zakupie urządzenia, zależy od lokalizacji oprogramowania:

* Jeśli masz kopię oprogramowania na pendrive'ie, możesz zainstalować ją ponownie z napędu, podłączając je do urządzenia, kopiując pliki na dysk twardy i uruchamiając instalację. Jeśli istnieje jakakolwiek możliwość, że pendrive jest zainfekowany złośliwym oprogramowaniem - na przykład przywracasz z powodu infekcji złośliwym oprogramowaniem i mogłeś w przeszłości włożyć pendrive do zainfekowanego komputera - przeskanuj go za pomocą oprogramowanie zabezpieczające, zanim cokolwiek z niego uruchomisz lub skopiujesz Zrób to z urządzenia z uruchomionym oprogramowaniem zabezpieczającym, które zapobiegnie rozprzestrzenianiu się infekcji po połączeniu dysku z maszyną używaną do skanowania.

* Jeśli skopiowałeś oprogramowanie na DVD lub CD, możesz zainstalować je z tego dysku. Pamiętaj, aby zainstalować wszystkie niezbędne aktualizacje.

* Jeśli zakupione oprogramowanie można ponownie pobrać z wirtualnej szafki, zrób to. W niektórych przypadkach ponownie pobrane oprogramowanie zostanie automatycznie zaktualizowane do najnowszej wersji. W innych przypadkach będzie to ta sama wersja, co oryginalnie zakupiona, więc pamiętaj o zainstalowaniu aktualizacji.

* Jeśli oprogramowanie można pobrać z oryginalnego źródła (oprogramowanie należące do domeny publicznej, oprogramowanie próbne aktywowane za pomocą kodu itp.), Możesz je ponownie pobrać. W niektórych przypadkach - na przykład, jeśli nowsze wersje wymagają uiszczenia opłaty za uaktualnienie - może być konieczne pobranie poprzedniej wersji. W każdym razie pamiętaj, aby zainstalować wszystkie aktualizacje dla wersji, którą instalujesz.

Przywracanie z pełnych kopii zapasowych danych

W wielu przypadkach warto przywrócić wszystkie dane na urządzeniu:

* Po przywróceniu z obrazu fabrycznego: po przywróceniu z obrazu fabrycznego i ponownym zainstalowaniu całego niezbędnego oprogramowania na urządzeniu nadal nie będzie żadnych (lub prawie żadnych) danych, więc musisz przywrócić wszystkie dane.

* Po niektórych atakach złośliwego oprogramowania: niektóre złośliwe oprogramowanie modyfikuje i / lub uszkadza pliki. Aby upewnić się, że wszystkie twoje pliki są takie, jak powinny, po infekcji, przywróć wszystkie dane z kopii zapasowej. Oczywiście to zakłada, że masz wystarczająco aktualną kopię zapasową, z której możesz to zrobić bez utraty pracy.

* Po awarii dysku twardego: Jeśli dysk twardy ulegnie awarii, w całości lub w części, zechcesz przenieść swoje pliki na inny dysk. Jeśli masz oddzielny dysk na dane niż dla systemu operacyjnego i programów - jak wiele osób to robi - pełne przywrócenie danych jest najłatwiejszym sposobem na przywrócenie. * Podczas przechodzenia na nowe, podobne urządzenie: Przywracanie z kopii zapasowej to łatwy sposób na umieszczenie wszystkich plików danych na nowym urządzeniu. Ponieważ niektóre programy przechowują ustawienia w folderach danych użytkownika, kopiując pliki bezpośrednio lub wykonując selektywne przywracanie z pliku

tworzenie kopii zapasowych jest zwykle lepszym rozwiązaniem. Ale ponieważ ludzie czasami nieumyślnie pomijają pliki podczas korzystania z takiej techniki, czasami używane są pełne odbudowy.

* Po przypadkowym usunięciu: ludzie czasami przypadkowo usuwają

duże porcje ich plików danych. Jednym z łatwych sposobów przywrócenia wszystkiego i nie martwienia się, czy wszystko „wróciło do tego, jak powinno" jest pełne przywrócenie wszystkich danych.

W przeciwieństwie do przywracania z pełnej kopii zapasowej systemu, przywracanie z pełnej kopii zapasowej danych nie przywraca 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. Wieloetapowy proces przywracania z obrazu fabrycznego, a następnie ponowna instalacja aplikacji i przywracanie danych może wydawać się bardziej żmudny niż zwykłe przywracanie z nowszego obrazu systemu, ale zwykle okazuje się również znacznie bardziej przenośny. Odzyskiwanie można zwykle przeprowadzić na urządzeniach, które znacznie różnią się od oryginalnego urządzenia, przy użyciu obrazów tych urządzeń (lub na nowe urządzenie), a następnie ponownej instalacji programów i przywrócenia danych.

Przywracanie z przyrostowych kopii zapasowych

Przyrostowe kopie zapasowe to kopie zapasowe utworzone po wykonaniu pełnej kopii zapasowej i zawierają kopie tylko tej części zawartości, której kopia zapasowa została zmieniona od czasu wykonania poprzedniej kopii zapasowej (pełnej lub przyrostowej). Niektóre uproszczone programy do tworzenia kopii zapasowych wykorzystują wewnętrznie przyrostowe i różnicowe kopie zapasowe, ale ukrywają przed nimi wewnętrzną pracę użytkowników. Wszyscy użytkownicy wybierają, które pliki lub typy plików mają zostać przywrócone i, jeśli to konieczne, które wersje tych plików, a system działa jak magia, ukrywając łączenie danych z wielu kopii zapasowych w wynikowym przywracaniu.

Przyrostowe kopie zapasowe systemów

Przyrostowe kopie zapasowe systemu to zasadniczo aktualizacje obrazów systemu (lub częściowych obrazów systemu w przypadku częściowych kopii zapasowych), które aktualizują obraz na dzień utworzenia kopii zapasowej. Przyrostowa kopia zapasowa systemu zawiera kopie tylko tej części systemu, która uległa zmianie od czasu uruchomienia poprzedniej kopii zapasowej (pełnej lub przyrostowej). Aby przywrócić z przyrostowej kopii zapasowej systemu:

1. Przywrócenie należy wykonać z ostatniej pełnej kopii zapasowej systemu.

2. Po zakończeniu odbudowy należy ją wykonać z każdej przyrostowej kopii zapasowej wykonanej od czasu utworzenia tego obrazu systemu został stworzony.

Nie zawarcie którejkolwiek z przyrostowych kopii zapasowych niezbędnych w kroku 2 może prowadzić do uszkodzenia brakujących programów, danych, składników systemu operacyjnego i problemów z niekompatybilnością oprogramowania. Większość nowoczesnych programów do tworzenia kopii zapasowych ostrzega (lub zapobiega) w przypadku próby pominięcia różnych operacji przyrostowych podczas przywracania z przyrostowej kopii zapasowej. Często jednak nie informują Cię, czy brakuje ci ostatniej kopii zapasowej lub kopii zapasowych w serii.

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

wykonaniu pełnej kopii zapasowej). Podczas gdy tworzenie serii różnicowych kopii zapasowych zwykle zajmuje więcej czasu niż tworzenie serii przyrostowych kopii zapasowych, przywracanie z różnicowych kopii zapasowych jest zwykle znacznie prostsze i szybsze. Aby odzyskać dane z różnicowej kopii zapasowej:

1. Wykonaj przywracanie z ostatniej pełnej kopii zapasowej systemu.

2. Po zakończeniu odbudowy wykonaj odbudowę z pliku najnowsza różnicowa kopia zapasowa.

Pamiętaj, aby przywrócić z ostatniej różnicowej kopii zapasowej, a nie z jakiejkolwiek innej różnicowej kopii zapasowej. Wiele systemów kopii zapasowych nie ostrzeże Cię, jeśli spróbujesz przywrócić kopię zapasową z innej kopii różnicowej niż najnowsza. Przed przywróceniem upewnij się, że używasz najnowszej wersji!

Ciągłe kopie zapasowe

Niektóre ciągłe kopie zapasowe są idealne do przywracania systemu. Podobnie jak obraz systemu, umożliwiają przywrócenie systemu do stanu, w jakim wyglądał w określonym momencie. Inne są okropne przy wykonywaniu przywracania, ponieważ pozwalają na przywrócenie tylko do najnowszej wersji systemu, która często cierpi z powodu konieczności odbudowy w pierwszej kolejności. W rzeczywistości normalnym zastosowaniem ciągłych kopii zapasowych jest reagowanie na awarie sprzętu, takie jak nagła przerwa w pracy dysku twardego, a nie odbudowa systemów po incydencie związanym z bezpieczeństwem. Ponadto, ponieważ ciągłe kopie zapasowe nieustannie przenoszą materiał z urządzenia, którego kopia zapasowa jest tworzona, do kopii zapasowej, wszelkie złośliwe oprogramowanie obecne w systemie głównym może znajdować się w kopii zapasowej.

Częściowe kopie zapasowe

Częściowe kopie zapasowe to kopie zapasowe części danych. Podobnie, częściowe kopie zapasowe nie są pełnymi kopiami zapasowymi na wypadek ataku złośliwego oprogramowania lub podobnego. Są jednak przydatne w innych sytuacjach i powinieneś wiedzieć, jak je przywrócić. Jeśli masz określony zestaw plików, które są wyjątkowo wrażliwe i wymagają tworzenia kopii zapasowych i przechowywania ich oddzielnie od reszty systemu, możesz użyć częściowej kopii zapasowej tych danych. Jeśli coś się stanie i będziesz musiał odbudować system lub przywrócić poufne dane, będziesz potrzebować oddzielnej częściowej kopii zapasowej, z której chcesz przywrócić. Cyfrowe klucze prywatne, które zapewniają dostęp do kryptowaluty, możliwości szyfrowania / odszyfrowywania wiadomości e-mail itp., Są często przechowywane na takich kopiach zapasowych wraz z obrazami niezwykle wrażliwych dokumentów

Często częściowe kopie zapasowe wrażliwych danych są wykonywane na dyskach USB, które są następnie zamykane w sejfach lub skrytkach depozytowych. Przywracanie z kopii zapasowej wymagałoby w takich przypadkach, aby osoba przywracająca otrzymała fizyczny dysk USB, co może oznaczać opóźnienie w przywracaniu. Jeśli potrzeba przywrócenia nastąpi o godzinie 18:00. Na przykład w piątek, a dysk znajduje się w skrytce depozytowej, która nie jest dostępna do 9 rano w poniedziałek, żądany materiał może pozostawać niedostępny dla użytkownika przez prawie trzy dni. Upewnij się, że przechowujesz częściowe kopie zapasowe w sposób, który pozwoli ci uzyskać dostęp do danych z kopii zapasowej, gdy ich potrzebujesz. Innym typowym scenariuszem dla wyspecjalizowanych częściowych kopii zapasowych jest użycie kopii zapasowej opartej na sieci - szczególnie w małej firmie - i użytkownik musi upewnić się, że ma kopię zapasową określonego materiału na wypadek problemów technicznych podczas podróży. Takie kopie zapasowe nigdy nie powinny być tworzone bez odpowiedniej autoryzacji. Jeśli uzyskano pozwolenie i utworzono kopię

zapasową, użytkownik w drodze, który ma problem techniczny wymagający przywrócenia danych, może wykonać przywrócenie, kopiując pliki z dysku USB (prawdopodobnie po odszyfrowaniu plików przy użyciu silnego hasło lub jakaś forma uwierzytelniania wieloskładnikowego).

Kopie zapasowe folderów

Kopie zapasowe folderów są podobne do częściowych kopii zapasowych, ponieważ zestaw elementów, których kopia zapasowa jest tworzona, to określony folder. Jeśli wykonałeś kopię zapasową folderu za pomocą narzędzia do tworzenia kopii zapasowych, możesz go przywrócić, korzystając z technik opisanych w poprzedniej sekcji. Proces przywracania jest inny, jeśli jednak utworzono odpowiednią kopię zapasową, po prostu kopiując folder lub zestaw folderów na dysk zewnętrzny (dysk twardy, dysk SSD, dysk USB lub dysk sieciowy). Teoretycznie wystarczy skopiować kopię zapasową folderu lub folderów do lokalizacji oryginalnego folderu. Jednak może to spowodować zastąpienie zawartości folderu podstawowego, więc wszelkie zmiany wprowadzone od czasu utworzenia kopii zapasowej zostaną utracone.

Kopie zapasowe dysków

Kopia zapasowa dysku jest podobna do kopii zapasowej folderu, ale zamiast folderu jest tworzona kopia zapasowa całego dysku. Jeśli wykonałeś kopię zapasową dysku za pomocą oprogramowania do tworzenia kopii zapasowych, możesz go przywrócić za pomocą tego oprogramowania. Jeśli utworzyłeś kopię zapasową dysku za pomocą oprogramowania do tworzenia kopii zapasowych, możesz go przywrócić za pomocą tego oprogramowania. Jeśli wykonałeś kopię zapasową dysku, kopiując zawartość dysku gdzie indziej, będziesz musiał ręcznie skopiować je z powrotem. Takie przywrócenie może jednak nie działać idealnie. Pliki ukryte i systemowe mogą nie zostać przywrócone, więc dysk rozruchowy, którego kopia zapasowa została utworzona i przywrócona w taki sposób, może nie pozostać bootowalna.

Kopie zapasowe dysków wirtualnych

Jeśli wykonałeś kopię zapasową zaszyfrowanego dysku wirtualnego, takiego jak dysk BitLocker zamontowany na komputerze, możesz przywrócić cały dysk w jednym ujęciu lub przywrócić poszczególne pliki i foldery z dysku.

Przywracanie całego dysku wirtualnego

Aby przywrócić cały wirtualny dysk w jednym ujęciu, upewnij się, że istniejąca kopia dysku nie jest zamontowana. Najłatwiej to zrobić, aby uruchomić komputer i nie montować żadnych dysków Bitlocker. Jeśli Twój komputer jest już uruchomiony, a dysk jest zamontowany, po prostu odłącz go:

1. Wybierz Startup ⇒ This PC.

2. Zlokalizuj zamontowany dysk Bitlocker.

Dysk jest wyświetlany z ikoną kłódki wskazującą, że jest zaszyfrowany.

3. Kliknij napęd prawym przyciskiem myszy i wybierz Wysuń. Po rozmontowaniu dysku znika on z listy dysków Ten komputer.

Po odmontowaniu dysku skopiuj kopię zapasową dysku do lokalizacji na dysku podstawowym i zastąp plik zawierający dysk. Następnie możesz odblokować i zamontować dysk.

Przywracanie plików i / lub folderów z dysku wirtualnego

Aby przywrócić pojedyncze pliki lub foldery z dysku wirtualnego, zamontuj kopię zapasową jako oddzielny dysk wirtualny i skopiuj pliki i foldery z kopii zapasowej na podstawowy, tak jakbyś kopiował pliki między dowolnymi dwoma dyskami. W idealnym przypadku należy wykonać kopię zapasową dysku wirtualnego przed zamontowaniem go i skopiowaniem z niego plików i / lub folderów, a po zamontowaniu zamontować go w trybie tylko do odczytu. Zawsze odłączaj dysk kopii zapasowej po skopiowaniu plików na podstawowy. Pozostawienie go zamontowanego - co z natury oznacza, że dwie kopie dużej części systemu plików są używane w tym samym czasie - może prowadzić do błędów ludzkich.

Radzenie sobie z usunięciami

Jednym z problemów związanych z przywracaniem z dowolnego przywracania, które nie zastępuje całkowicie danych nową kopią, jest to, że przywracanie może nie przywrócić usunięć. Na przykład, jeśli po wykonaniu pełnej kopii zapasowej usuniesz plik, utworzysz dziesięć nowych plików, zmodyfikujesz dwa pliki danych, a następnie wykonasz przyrostową kopię zapasową, przyrostowa kopia zapasowa może, ale nie musi, zarejestrować usunięcie. W przypadku przywracania z pełnej kopii zapasowej, a następnie przywracania z kopii przyrostowej, przywracanie z kopii przyrostowej powinno usunąć plik, dodać dziesięć nowych plików i zmodyfikować oba pliki do nowszej wersji. Jednak w niektórych przypadkach plik, który wcześniej usunąłeś, może pozostać, ponieważ niektóre narzędzia do tworzenia kopii zapasowych nie uwzględniają prawidłowo usunięć. Nawet jeśli wystąpi ten problem, zwykle nie jest krytyczny. Po prostu chcesz być tego świadomy. Oczywiście, jeśli w przeszłości usuwałeś poufne pliki, powinieneś sprawdzić, czy przywrócenie przywróciło je na komputer. (Jeśli zamierzasz trwale i całkowicie zniszczyć plik lub zestaw plików, powinieneś również usunąć go / je z kopii zapasowych).

Z wyłączeniem plików i folderów

Podczas przywracania nie należy przywracać niektórych plików i folderów. Prawdę mówiąc, nie powinno się ich tworzyć w pierwszej kolejności, chyba że utworzyłeś obraz dysku, ale w wielu przypadkach ludzie i tak tworzą ich kopie zapasowe. Poniżej przedstawiono przykłady niektórych takich plików i folderów, które można wykluczyć z typowych przywracania wykonywanych na komputerze z systemem Windows 10. Jeśli używasz oprogramowania do tworzenia kopii zapasowych, oprogramowanie prawdopodobnie wykluczyło te pliki podczas tworzenia kopii zapasowej. Jeśli kopiujesz pliki ręcznie, być może wykonałeś ich kopię zapasową.

* Zawartość Kosza

* Pamięci podręczne przeglądarki (tymczasowe pliki internetowe z przeglądarek internetowych, takich jak Microsoft Edge lub Internet Explorer, Firefox, Chrome, Vivaldi lub Opera)

* Foldery tymczasowe (często nazywane Temp lub tem i znajdują się w C: \, w katalogu użytkownika lub w katalogu danych oprogramowania

* Pliki tymczasowe (zwykle pliki o nazwach * .tmp lub * .temp)

* Pliki wymiany systemu operacyjnego (pagefile.sys)

* Informacje o obrazie systemu w trybie hibernacji systemu operacyjnego (hyberfil.sys)

* Kopie zapasowe (chyba że chcesz wykonać kopię zapasową kopii zapasowych), takie jak kopia zapasowa historii plików systemu Windows

* Kopie zapasowe plików systemu operacyjnego podczas aktualizacji systemu operacyjnego (zwykle znajdują się w C: \ Windows.old na komputerach z systemem Windows, na których zaktualizowano systemy operacyjne)

* Pliki pamięci podręcznej programu Microsoft Outlook (* .ost - pamiętaj, że dane lokalne programu Outlook należy wykonać kopię zapasową [* .pst]; w rzeczywistości w wielu przypadkach mogą tak 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, który ktoś mu podyktował, ale który użytkownik ma, od kiedy wszedł do jego katalogu smartfonów)

Kopie zapasowe w aplikacji

Niektóre aplikacje mają wbudowane funkcje tworzenia kopii zapasowych, które chronią Cię przed utratą pracy w przypadku awarii komputera, awarii zasilania i wyczerpania baterii oraz innych nieszczęśliwych wypadków. Niektóre takie aplikacje automatycznie monitują o przywrócenie dokumentów, które w przeciwnym razie zostałyby utracone w wyniku awarii systemu lub podobnej. Na przykład, gdy uruchamiasz program Microsoft Word po nieprawidłowym zamknięciu aplikacji, wyświetla listę dokumentów, które można automatycznie odzyskać - czasami nawet oferuje wiele wersji tego samego dokumentu.

Zrozumienie archiwów

Termin archiwum ma wiele znaczeń w świecie informatyki. Odpowiednie znaczenia opiszę w kolejnych sekcjach.

Wiele plików przechowywanych w jednym pliku

Czasami w jednym pliku można przechowywać wiele plików. Koncepcja dysków wirtualnych była jednak taka, że przechowywanie wielu plików w jednym pliku nie wymaga tworzenia dysków wirtualnych. Być może widzieliście na przykład pliki z rozszerzeniem .zip. Pliki ZIP, jak nazywane są takie pliki, są w rzeczywistości kontenerami, które zawierają jeden lub więcej skompresowanych plików. Przechowywanie wielu plików w takim kontenerze pozwala na znacznie łatwiejsze przenoszenie plików (pojedynczy plik ZIP załączony do wiadomości e-mail jest znacznie łatwiejszy w zarządzaniu niż 50 małych pojedynczych plików). Zmniejsza również (czasami znacznie) ilość miejsca na dysku i przepustowość Internetu niezbędną do przechowywania i przenoszenia plików. Jeśli chcesz przywrócić pliki z archiwum, możesz wyodrębnić wszystkie pliki z archiwum do głównego źródła lub otworzyć archiwum i skopiować poszczególne pliki do podstawowej lokalizacji, tak jak w przypadku wszelkich plików znalezionych w jakimkolwiek innym folderze. Pliki archiwów są dostępne w wielu różnych formatach. Niektóre pojawiają się automatycznie jako foldery w systemach plików Windows i Mac, a ich zawartość jako pliki i foldery w folderach. Inne wymagają specjalnego oprogramowania do przeglądania i ekstrakcji.

Stare dane na żywo

Czasami stare dane są przenoszone z systemów podstawowych i przechowywane w innym miejscu. Przechowywanie starych danych może poprawić wydajność. Na przykład, jeśli wyszukiwanie wszystkich elementów wiadomości e-mail oznacza przeszukiwanie wiadomości z 25 lat, będzie to trwało znacznie dłużej niż przeszukiwanie tylko ostatnich 3 lat. Jeśli prawie wszystkie odpowiednie

wyniki będą zawsze w ciągu ostatnich kilku lat, starsze e-maile można przenieść do oddzielnego archiwum, gdzie w razie potrzeby można uzyskać do nich dostęp i przeszukiwać je oddzielnie.

Jeśli używasz archiwizacji, weź to pod uwagę przy przywracaniu danych. Chcesz mieć pewność, że archiwa zostaną przywrócone do archiwów i że przypadkowo nie przywrócisz archiwów do głównych magazynów danych.

Stare wersje plików, folderów lub kopii zapasowych

Termin archiwa jest czasami używany w odniesieniu do starych wersji plików, folderów i kopii zapasowych, nawet jeśli te pliki są przechowywane w głównym magazynie danych. Ktoś, kto ma na przykład dziesięć wersji umowy, które zostały wykonane w różnych momentach, może przechowywać wszystkie wersje tych dokumentów programu Word w folderze Archiwum. Archiwizację tego rodzaju można przeprowadzić z jednego lub kilku z wielu powodów. Jednym z powszechnych powodów jest unikanie przypadkowego użycia starej wersji dokumentu, gdy powinna być używana aktualna wersja. Jeśli archiwizujesz, weź to pod uwagę przy przywracaniu danych. Przywróć wszystkie archiwa do ich właściwych lokalizacji. Możesz zobaczyć wiele kopii tego samego pliku w trakcie przywracania; nie zakładaj, że to błąd.

Przywracanie przy użyciu narzędzi do tworzenia kopii zapasowych

Przywracanie za pomocą oprogramowania do tworzenia kopii zapasowych jest podobne do procesu tworzenia kopii zapasowych za pomocą oprogramowania do tworzenia kopii zapasowych. Aby przywrócić za pomocą oprogramowania do tworzenia kopii zapasowych, które było używane do tworzenia kopii zapasowych, z których przywracasz, uruchom oprogramowanie (w niektórych przypadkach może być konieczne zainstalowanie oprogramowania na komputerze zamiast uruchamiania go z dysku CD lub podobnego) i wybierz Przywróć. Podczas przywracania upewnij się, że wybrałeś poprawną wersję kopii zapasowej do przywrócenia. Uważaj na fałszywe monity o przywrócenie! Różne formy złośliwego oprogramowania wyświetlają fałszywe monity informujące, że dysk twardy uległ jakiejś awarii i że musisz uruchomić routing przywracania, aby naprawić dane. Przywracaj tylko te programy, które otrzymałeś z wiarygodnego źródła i wiesz, że możesz im zaufać! Wiele nowoczesnych pakietów oprogramowania do tworzenia kopii zapasowych ukrywa podejście stosowane do tworzenia kopii zapasowych - pełne, różnicowe, przyrostowe itd. - od użytkowników i zamiast tego umożliwia użytkownikom wybranie wersji plików, które chcą przywrócić. Jeśli przywracasz za pomocą specjalistycznego oprogramowania do tworzenia kopii zapasowych i odzyskiwania, które zostało dostarczone z zewnętrznym dyskiem twardym lub urządzeniem półprzewodnikowym, którego używasz do tworzenia kopii zapasowych urządzenia, podłącz dysk, uruchom oprogramowanie (chyba że działa automatycznie) i postępuj zgodnie z instrukcjami monit o przywrócenie. Takie oprogramowanie jest zwykle proste w użyciu; przywracanie zwykle działa jak uproszczona wersja tego, która została wykonana przy użyciu innego oprogramowania do tworzenia kopii zapasowych. Odłącz dysk od systemu po wykonaniu przywracania!

Przywracanie z kopii zapasowej systemu Windows

Aby przywrócić dane z kopii zapasowej systemu Windows do oryginalnych lokalizacji, z których utworzono kopię zapasową danych, wykonaj następujące kroki:

1. Wybierz Start ⇒ Ustawienia ⇒ Aktualizacja i bezpieczeństwo ⇒ Kopia zapasowa.

2. Kliknij Przywróć pliki z aktualnej kopii zapasowej.

3. W przeglądarce systemu plików przejrzyj różne wersje folderów i plików lub wpisz i wyszukaj nazwę szukanego pliku.

4. Wybierz, co chcesz przywrócić.

5. Kliknij Przywróć.

Przywracanie do punktu przywracania systemu

Microsoft Windows umożliwia przywrócenie systemu do stanu, w jakim wyglądał w określonym czasie, w którym system operacyjny był obrazowany:

1. Kliknij przycisk Start i wybierz Ustawienia.

2. Wybierz Panel sterowania ⇒ System i konserwacja ⇒ Kopia zapasowa i przywracanie.

3. Kliknij Przywróć moje pliki, aby przywrócić pliki lub Przywróć pliki wszystkich użytkowników, aby przywrócić pliki wszystkich użytkowników (zakładając, że masz do tego uprawnienia).

Przywracanie z kopii zapasowej smartfona / tabletu

Wiele urządzeń przenośnych jest wyposażonych w możliwość automatycznej synchronizacji danych z chmurą, co umożliwia przywrócenie danych na nowe urządzenie w przypadku zgubienia lub kradzieży urządzenia. Nawet urządzenia, które nie mają wbudowanej takiej funkcji, prawie zawsze mogą uruchamiać oprogramowanie, które skutecznie udostępnia takie funkcje dla określonego drzewa folderów lub oprogramowanie, które skutecznie udostępnia takie funkcje dla określonego drzewa folderów lub dysku. Przy pierwszym uruchomieniu urządzenia z Androidem po przywróceniu ustawień fabrycznych może zostać wyświetlony monit z pytaniem, czy chcesz przywrócić dane. Jeśli tak, przywracanie jest dość proste. Odpowiedz tak. Chociaż dokładne procedury mogą się różnić w zależności od urządzenia i producenta, inne formy przywracania zazwyczaj wynikają z pewnego rodzaju następującego procesu:

Aby przywrócić kontakty z karty SD:

1. Otwórz aplikację Kontakty. Jeśli istnieje funkcja importu, wybierz ją i przejdź do kroku 4.

2. Wybierz Ustawienia z menu głównego (lub kliknij ikonę Ustawienia). Jeśli nie wyświetlasz wszystkich kontaktów, może być konieczne kliknięcie menu Wyświetl i wybranie Wszystkie kontakty.

3. Wybierz Importuj / Eksportuj kontakty (lub, jeśli ta opcja nie jest dostępna, wybierz Zarządzaj kontaktami, a następnie wybierz Importuj kontakty na następnym ekranie).

4. Wybierz opcję Importuj z karty SD.

5. Przejrzyj nazwę pliku kopii zapasowej listy kontaktów, a następnie kliknij na OK.

Kontakty są często archiwizowane (lub eksportowane do) plików VCF. Aby przywrócić multimedia (zdjęcia, filmy i pliki audio) z karty SD:

1. Za pomocą Menedżera plików otwórz kartę SD.

2. Kliknij, aby włączyć pola wyboru obok pliku lub plików, które chcesz przywrócić.

3. Aby skopiować pliki do pamięci telefonu, przejdź do menu i wybierz Kopiuj ⇒ Pamięć wewnętrzna.

4. Wybierz folder, do którego chcesz skopiować pliki lub utwórz folder i przenieś do niego.

5. Wybierz Kopiuj tutaj.

Przywracanie z ręcznych kopii zapasowych plików lub folderów

Aby przywrócić z ręcznej kopii pliku lub folderu, wystarczy skopiować plik lub folder z kopii zapasowej do głównego magazynu danych. (Jeśli nadpisujesz plik lub folder, możesz otrzymać ostrzeżenie od systemu operacyjnego). Po zakończeniu odłącz nośnik, na którym znajduje się kopia zapasowa, od głównego magazynu.

Korzystanie z kopii zapasowych danych przechowywanych na serwerach innych firm

Jeśli korzystałeś z możliwości tworzenia kopii zapasowych dostawcy zewnętrznego, u którego przechowujesz dane w chmurze lub z którego usług w chmurze korzystasz, możesz mieć możliwość przywrócenia swoich odpowiednich danych za pośrednictwem interfejsu udostępnionego przez dostawcę zewnętrznego. Jeśli korzystasz z zewnętrznego dostawcy usług chmurowych i nie wykonałeś kopii zapasowych, nadal możesz mieć możliwość przywrócenia danych. Skontaktuj się z dostawcą. Sam dostawca mógł wykonać kopię zapasową danych bez powiadamiania Cię. Chociaż nigdy nie powinieneś polegać na dostawcy usług w chmurze wykonującym kopie zapasowe, których nie zamówiłeś, jeśli jesteś w korku i kontaktujesz się z dostawcą, możesz (lub nie) być mile zaskoczony, gdy dowiesz się, że mają kopie zapasowe, z których może przywrócić.

Przywracanie kopii zapasowych do ich właściwych lokalizacji

Po przywróceniu z fizycznej kopii zapasowej musisz przywrócić ją do właściwej lokalizacji z kilku powodów:

* Nie chcesz, aby został zgubiony, jeśli kiedykolwiek będziesz go potrzebować.

* Nie chcesz, aby została skradziona.

* Chcesz mieć pewność, że nie podważasz żadnych strategii i procedur przechowywania, które mają na celu przechowywanie kopii zapasowych w innych lokalizacjach niż magazyny danych, których kopie zapasowe są tworzone.

Pamięć sieciowa

W idealnej sytuacji podczas przywracania z sieciowej kopii zapasowej dysk sieciowy należy zamontować jako tylko do odczytu, aby zapobiec możliwym uszkodzeniom kopii zapasowej. Ponadto pamiętaj, aby odłączyć się od sieciowej składnicy danych po zakończeniu przywracania. Upewnij się, że dowolny mechanizm używany do uruchamiania przywracania (na przykład oprogramowanie do tworzenia kopii zapasowych) ma odpowiednie uprawnienia sieciowe do zapisu w podstawowej lokalizacji przechowywania danych.

Przywracanie z kombinacji lokalizacji

Nie ma powodu, aby tworzyć kopie zapasowe tylko w jednej lokalizacji. Jednak przywracanie zwykle wykorzystuje kopie zapasowe tylko z jednej lokalizacji na raz. Jeśli musisz przywrócić dane z kopii zapasowych, które fizycznie znajdują się w więcej niż jednej lokalizacji, zachowaj szczególną ostrożność, aby nie przywrócić niewłaściwych wersji plików, ponieważ niektóre z nich mogą znajdować się na wielu kopiach zapasowych.

Przywracanie do nieoryginalnych lokalizacji

Jeśli chodzi o przywracanie danych, niektórzy ludzie decydują się na przywracanie do lokalizacji innych niż oryginalne, testują przywrócone dane, a następnie kopiują lub przenoszą je do oryginalnych

lokalizacji. Taka strategia zmniejsza prawdopodobieństwo nadpisania dobrych danych złymi danymi. Możesz pogorszyć zły dzień, jeśli stracisz część danych i odkryjesz, że kopia zapasowa danych jest uszkodzona. Jeśli następnie przywrócisz z tej kopii zapasowej oryginalne dane, a tym samym je uszkodzisz, utracisz jeszcze więcej danych.

Nigdy nie zostawiaj swoich kopii zapasowych podłączonych

Po przywróceniu nigdy nie pozostawiaj dysków twardych z kopiami zapasowymi ani dysków półprzewodnikowych podłączonych do systemów lub sieci, których kopie zapasowe są tworzone. Wszelkie przyszłe infekcje złośliwym oprogramowaniem, które zaatakują system główny, mogą 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 tworzysz kopię zapasową na nośniku wielokrotnego odczytu, na przykład na dyskach CD-R, po zakończeniu przywracania teoretycznie bezpiecznie jest pozostawić kopię zapasową na podłączonym dysku, ale nadal nie powinieneś tego robić. Chcesz, aby kopia zapasowa była łatwo dostępna we właściwej lokalizacji na wypadek, gdybyś kiedykolwiek jej potrzebował w przyszłości.

Przywracanie z zaszyfrowanych kopii zapasowych

Przywracanie z zaszyfrowanych kopii zapasowych jest zasadniczo takie samo, jak przywracanie z niezaszyfrowanych kopii zapasowych, z wyjątkiem tego, że przed przywróceniem należy odblokować kopie zapasowe. Kopie zapasowe chronione hasłem wymagają oczywiście wprowadzenia prawidłowego hasła. Kopie zapasowe chronione certyfikatami lub innymi bardziej zaawansowanymi formami szyfrowania mogą wymagać posiadania przez użytkownika elementu fizycznego lub certyfikatu cyfrowego w celu przywrócenia. W większości przypadków użytkownicy domowi dbający o bezpieczeństwo chronią swoje kopie zapasowe hasłami. Jeśli to zrobisz (a powinieneś), nie zapomnij swojego hasła.

Testowanie kopii zapasowych

Wielu ludzi sądziło, że mają odpowiednie kopie zapasowe tylko po to, aby odkryć, kiedy trzeba było przywrócić, że kopie zapasowe są 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. Przetestuj jednak pierwszą kopię zapasową utworzoną za pomocą dowolnego oprogramowania, sprawdź pliki autoodzyskiwania przy pierwszym użyciu programu Word itd. Niektóre programy do tworzenia kopii zapasowych są wyposażone w możliwość weryfikacji kopii zapasowych - to jest Niektóre programy do tworzenia kopii zapasowych mają możliwość weryfikacji kopii zapasowych - to znaczy po utworzeniu kopii zapasowej sprawdza, czy oryginalne dane i dane w kopiach zapasowych są zgodne. Przeprowadzenie takiej weryfikacji po wykonaniu kopii zapasowej znacznie wydłuża proces tworzenia kopii zapasowej. Warto jednak uruchomić, jeśli możesz to zrobić, ponieważ pomaga to upewnić się, że podczas procesu tworzenia kopii zapasowej nic nie zostało nieprawidłowo zarejestrowane lub w inny sposób uszkodzone.