



IBM Global Services
Styczeń 2008

Wyjście poza taśmowe systemy kopii zapasowych.

Odpowiedź IBM na wyzwania w zakresie ochrony danych stojące przed średnimi firmami

Spis treści

- 2 ***Wprowadzenie***
- 2 ***Wyzwania w dziedzinie ochrony danych***
- 2 ***Niedobory zasobów i ryzyko***
- 3 ***Taśmowe systemy kopii zapasowych: popularne i problematyczne***
- 4 ***Ochrona danych użytkownika końcowego***
- 5 ***Lepsza alternatywa***
- 7 ***Istniejące rozwiązania pokazują skuteczność modelu usług na żądanie***
- 10 ***Rozwiązania i opcje dla ochrony danych serwerów***
- 11 ***Rozwiązania dla ochrony danych komputerów stacjonarnych i przenośnych***
- 12 ***Podsumowanie***

Wprowadzenie

Średnie firmy muszą zweryfikować sposób tworzenia kopii zapasowych dla ochrony danych przechowywanych w oddziałach i na komputerach PC przy użyciu systemów taśmowych i innych własnych rozwiązań. Ryzyko i potencjalne koszty — bezpowrotnej utraty kluczowych informacji, zakłóceń w funkcjonowaniu firmy, utraty klientów czy nieprzestrzegania wymogów narzuconych przepisami prawa — są zbyt duże. A przy rosnącej ilości krytycznych informacji biznesowych składowanych w oddziałach firmy i na komputerach użytkowników końcowych koszty ewentualnych awarii stają się coraz wyższe. Dlatego dla wielu średnich firm usługi ochrony danych na żądanie to rozsądne cenowo, praktycznie rozwiązanie uciążliwego problemu.

Wyzwania w dziedzinie ochrony danych

Średnie firmy stają w obliczu tych samych podstawowych problemów dotyczących ochrony danych jak duże firmy. Zagrożenia wynikające z braku ochrony danych oraz potencjalne koszty biznesowe mogą łatwo osiągnąć rozmiary katastrofy niezależnie od tego, czy firma pracuje na megabajtach czy terabajtach danych. Niestety, działy informatyki w średnich firmach zazwyczaj mogą oddelegować do obsługi tych problemów znacznie mniejsze zasoby niż w dużych firmach. Co gorsza, coraz częściej stoją one w obliczu takich samych wyzwań w dziedzinie ochrony danych rozproszonych. Wraz z rozwojem sieci oddziałów i rosnącym udziałem czasu pracy personelu w terenie rośnie ilość danych generowanych poza centralą firmy. Nie dysponując zasobami umożliwiającym samodzielne rozwiązanie tych problemów, wiele średnich firm zwraca się w kierunku zupełnie innego rodzaju rozwiązania: zakupu usługi zdalnej ochrony danych na żądanie.

Niedobory zasobów i ryzyko

Bycie małym nie chroni podmiotów świadczących usługi opieki zdrowotnej czy biur maklerskich przed kontrolowaniem stosowanych zasad przechowywania danych przez uprawnione organa. Zarzuty karne i procesy sądowe grożą każdemu. Do tego, awarie sieci energetycznej, wichury, powodzie czy podtopienia nie rozróżniają między firmami dużymi i małymi czy między korporacyjnymi centrami przetwarzania danych a oddziałami zajmującymi jedno piętro w budynku.

W skrócie

Lokalne kopie zapasowe nie chronią przed stratami powstającymi poza centrum przetwarzania danych.

Lokalne katastrofy mogą doprowadzić do zniszczenia zarówno podstawowych danych, jak i przechowywanych lokalnie kopii zapasowych.

Koszty nieodpowiedniej ochrony danych są wysokie. Gdy niechronione dane ulegną utracie, często trzeba je odtwarzać od zera. Jeśli firma polega na lokalnym systemie wykonywania kopii zapasowych na taśmach, każda strata mająca miejsce poza centrum przetwarzania danych jest poza kontrolą kierownictwa działu informatyki. Należy oczekiwać pogłębienia się tego problemu w najbliższych latach w związku z rozwojem średnich firm i zwiększaniem przez nie liczby oddziałów i filii. Trend ten jest spowodowany głównie zlecaniem obsługi procesów biznesowych poza firmę, integracją łańcuchów dostaw, rozwojem w kluczowych obszarach w ramach walki konkurencyjnej, fuzjami i przejęciami oraz globalizacją rynków. Oddziałom często brakuje odpowiedniego lokalnego wsparcia informatycznego. Przy ograniczonych zasobach zmuszonych do koncentrowania się na operacjach wykonywania kopii zapasowych i przywracania systemów po awariach odpowiednie zarządzanie danymi i ich ochrona schodzą na dalszych plan.

Taśmowe systemy kopii zapasowych: popularne i problematyczne

W większości średnich firm podstawową formą ochrony danych jest umieszczanie ich kopii zapasowych na nośnikach taśmowych. Metoda ta jest jednak niewystarczająca z wielu powodów:

- *Zawodna i losowa w działaniu; istnieje ryzyko uznania jej za niezgodną z różnymi wymogami prawnymi stawianymi firmom niezależnie od ich wielkości: krajowymi, regionalnymi, dotyczącymi papierów wartościowych czy zapewnienia ciągłości funkcjonowania.*
- *Trudności w centralnym zarządzaniu, ponieważ personel informatyczny może nie dysponować narzędziami monitorowania operacji wykonywanych w odległych ośrodkach i sprawdzać, czy kopie zapasowe są wykonywane i nie zawierają błędów.*
- *Ryzykowna, ponieważ taśmy często ulegają zagubieniu lub kradzieży, szczególnie podczas transportowania ich do bezpiecznych lokalizacji zewnętrznych.*
- *Obciążająca pod względem nakładów kapitałowych i zaangażowania zasobów: wymaga zakupu serwerów, taśm, napędów dyskowych i oprogramowania do wykonywania kopii zapasowych dla każdej lokalizacji.*
- *Powolna i skomplikowana — utrudnia stosowanie docelowych punktów odtwarzania (RPO) i docelowych czasów odtwarzania (RTO).*
- *Nie jest w stanie ochronić firmy przed poważną utratą danych, spadkiem wydajności pracy ani ustawowymi karami spowodowanymi nieodpowiednią ochroną danych.*

W skrócie

Wady taśmowych systemów wykonywania kopii zapasowych narażają firmy na poważne konsekwencje.

Firmy muszą zapewnić ochronę danych generowanych w oddziałach i filiach.

Wady taśmowych systemów wykonywania kopii zapasowych narażają firmy na poważne konsekwencje finansowe i biznesowe w postaci utraty danych, pogorszenia wydajności pracy i ustawowych kar.

Niektóre firmy wprowadziły procedury replikowania danych ponownie do centrali, gdzie mogą zostać zapisane na dyskach i podlegać centralnemu zarządzaniu. Takie rozwiązanie może być jednak zarówno drogie w implementacji, jak i skomplikowane w administrowaniu. Każdy oddział czy filię należy wyposażyć w sieciowe urządzenie pamięci masowej i oprogramowanie do replikacji. Rosną także koszty użytkowania sieci, ponieważ okresowe sesje wykonywania kopii zapasowych danych serwerów obciążają sieci rozległe (WAN) i lokalne (LAN), co może zakłócać przesyłanie danych kluczowych dla działalności firmy i znacznie pogarszać wydajność pracy użytkowników końcowych.

Ochrona danych użytkownika końcowego

Oddziały to tylko jeden z elementów w problematyce ochrony rozproszonych danych. Firmy muszą również chronić dane, które są generowane, pobierane i udostępniane przez gwałtownie rosnącą liczbę komputerów osobistych i urządzeń przenośnych.

Obecnie pracownicy mobilni generują ogromne ilości danych, często wiele kilometrów od centrali firmy i nadzoru personelu informatycznego. Ochrona i zabezpieczenie tych kluczowych i poufnych informacji, które obejmują m.in. dane klientów i informacje stanowiące własność intelektualną, staje się obowiązkiem wyłącznie tych zabieganych i często niewtajemniczonych w aspekty techniczne użytkowników końcowych.

Potrzeba zapewnienia ochrony takich danych jest paląca: komputery mogą zostać skradzione, doznać awarii dysków twardych czy ulec zarażeniu wirusami. Ponadto wiele aplikacji do zdalnego wykonywania kopii zapasowych danych komputerów znacznie obciąża przepustowość sieci i procesory samych komputerów, w efekcie spowalniając aplikacje biznesowe, wydłużając czasy reakcji w sieci, denerwując użytkowników i powodując spadek wydajności pracy.

W skrócie

Usługa ochrony na żądanie rozproszonych danych może zapewnić większą niezawodność i bezpieczeństwo.

Lepsza alternatywa

Szefowie działów informatycznych wielu średnich firm zdają sobie obecnie sprawę, że istniejące systemy ochrony rozproszonych danych są niewystarczające. Nie mają jednak zasobów pozwalających na samodzielne wprowadzenie i administrowanie lepszymi rozwiązaniami.

Na szczęście istnieje znakomita alternatywa: usługa ochrony na żądanie rozproszonych danych, która obejmuje automatyczne wykonywanie kopii zapasowych danych stacji roboczych i serwerów zlokalizowanych poza centralą, praktycznie w dowolnym miejscu sieci klienta bazującej na protokole IP, z zapewnieniem podwyższonej niezawodności i bezpieczeństwa.

Usługi te oferują szereg korzyści: niższe koszty, atrakcyjny wskaźnik rentowności inwestycji, wysoki poziom obsługi, poprawę parametrów utrzymania ciągłości biznesowej oraz możliwość dopasowania zakresu usług do zmieniających się potrzeb firmy.

Niższe koszty i atrakcyjny wskaźnik rentowności ROI

Oceniając wskaźnik rentowności inwestycji dla systemu ochrony danych w formie usług świadczonych przez zewnętrzną firmę, należy wziąć pod uwagę wszystkie koszty, jakie firma musiałaby ponieść w przypadku samodzielnego wdrażania takiego rozwiązania. Analiza powinna uwzględnić wzrost tych kosztów w czasie, co wynika z konieczności rozbudowy własnego systemu w odpowiedzi na rosnące wymagania. Oto pozycje kosztowe, które należy uwzględnić:

- *Nakłady kapitałowe, w tym na sieciowe urządzenia pamięci masowej, oprogramowanie, połączenia WAN oraz zewnętrzne fizyczne lokalizacje służące do przechowywania taśm z kopią zapasową danych.*
- *Koszty robocizny, w tym koszty przeszkolenia istniejącego personelu i zatrudnienia dodatkowego personelu technicznego odpowiadającego za wdrożenie, utrzymanie i administrowanie nową instalacją.*
- *Koszty ukryte wynikające z niewystarczającej ochrony danych i systemów (w tym koszty spadku wydajności pracy personelu informatycznego i użytkowników końcowych, utraconych przychodów, zaufania klientów i kar ustawowych).*

W skrócie

Usługa zdalnej ochrony danych na żądanie obejmuje udostępnienie urządzeń, oprogramowania i pomocy technicznej.

Usługi ochrony danych to atrakcyjna propozycja nie tylko dla dużych firm.

Odpowiedni usługodawca może zaoferować poziom ochrony rozproszonych danych, na który samodzielnie może sobie pozwolić bardzo mało średnich firm.

Usługa obejmuje udostępnienie urządzeń, oprogramowania i pomocy technicznej, dzięki czemu klient oszczędza na kosztach zarówno kapitału, jak i robocizny. Usługi wykonywania kopii zapasowych i odtwarzania danych są zazwyczaj realizowane z wykorzystaniem istniejących szerokopasmowych łączy internetowych klienta. Klient uiszcza miesięczną opłatę uzależnioną od ilości chronionych danych.

Model płacenia za wykorzystaną usługę nie tylko pomaga ograniczyć nakłady kapitałowe, ale również pozwala łatwiej i dokładniej przewidywać oraz planować przyszłe wydatki.

Usługi ochrony danych to propozycja, która może przynieść wymierne korzyści nie tylko dużym firmom. Średnie firmy, które przekażą odpowiedzialność za wykonywanie kopii zapasowych zewnętrznym usługodawcom, ograniczą koszty robocizny oraz przestoje związane z koniecznością wyłączenia serwerów i wymiany dysków.

Wysoki poziom obsługi, poprawa parametrów utrzymania ciągłości biznesowej
Co najbardziej istotne, odpowiedni usługodawca może zaoferować poziom ochrony rozproszonych danych, na który samodzielnie może sobie pozwolić bardzo mało średnich firm. Kierownicy działów informatycznych zyskują pewność, że kopie zapasowe będą wykonywane zgodnie z ustalonym harmonogramem dla wszystkich oddziałów, stacji roboczych i serwerów, z uwzględnieniem wymagań w zakresie docelowych punktów odtwarzania (RPO) i docelowych czasów odtwarzania (RTO).

Usługa ochrony danych może również obejmować całodobowe wsparcie techniczne i monitorowanie, na co większości średnich nie stać, ale wraz z globalizacją działalności jest im to coraz częściej potrzebne. Kopie zapasowe danych mogą być przechowywane w odległym ośrodku usługodawcy przeznaczonym do odtwarzania systemów po awarii. Takie rozwiązanie zwiększa szanse utrzymania ciągłości funkcjonowania firmy w przypadku awarii wyłączającej z działania oddział, a nawet centralę.

W skrócie

Unowocześnianie systemów ochrony danych wraz z rozwojem potrzeb firmy

Dla działów informatycznych większości firm konieczność zaspokojenia rosnących potrzeb firmy w dziedzinie ochrony danych to ciągła walka o środki i źródło poważnych wydatków. Skalowalność rozwiązań jest szczególnie istotna dla średnich firm, które mają tendencję do rozwijania się gwałtownymi skokami tak pod względem organizacyjnym, jak i ilości generowanych i przetwarzanych danych.

Model usług na żądanie umożliwia administratorom z działów informatyki znacznie dokładniejsze prognozowanie i planowanie przyszłych kosztów.

Usługi na żądanie zawierają z założenia elementy nadmiarowości, zapasowej pojemności i elastyczności, dzięki czemu pozwalają zaspokoić oczekiwania firm o praktycznie dowolnej wielkości oraz szybko i płynnie skorygować zakres wykorzystywanych zasobów górę lub w dół zgodnie z aktualnymi potrzebami. Płacąc wyłącznie za wykorzystywane usługi, firma unika nakładów na zakup i utrzymanie urządzeń, które często są obciążone w zbyt małym lub dużym stopniu. Dodatkowa zaleta modelu usług na żądanie to stworzenie pracownikom działów informatycznych możliwości znacznie dokładniejszego prognozowania i planowania przyszłych kosztów.

Usługa zdalnej ochrony danych pozwala zabezpieczyć dane umieszczone na serwerach, komputerach osobistych i laptopach rozproszonych po całej firmie.

Istniejące rozwiązania pokazują skuteczność modelu usług na żądanie

Jednym z takich zdalnych systemów ochrony danych na żądanie jest usługa IBM zdalnej ochrony danych z pakietu Usług IBM w zakresie ochrony danych (IBM Information Protection Services) . Usługa pozwala zabezpieczyć dane umieszczone na serwerach, komputerach osobistych i laptopach rozproszonych po całej firmie i w różnych lokalizacjach. Kopie zapasowe danych są umieszczane automatycznie za pośrednictwem istniejącej sieci IP klienta w naszych znakomicie zabezpieczonych centrach przetwarzania danych.

Usługa zdalnej ochrony danych jest opłacana na zasadach subskrypcji, zapewniając wysoką przewidywalność i rozsądną wysokość kosztów ponoszonych przez klientów. Obejmuje sprzęt, oprogramowanie i pomoc operacyjną niezbędną do szybkiego i sprawnego wdrożenia skutecznej strategii ochrony danych. Taka metoda pozwala wyeliminować koszty badań i rozwoju, wdrożenia, zatrudnienia i szkoleń związane z wprowadzeniem systemu wewnątrz firmy, a jednocześnie znacznie przyspieszyć moment rozpoczęcia korzystania z usługi.

W skrócie

Codziennie wykonywanie kopii zapasowych to z założenia szybki, ekonomiczny i wygodny sposób zapewnienia jednorodnej ochrony danych.

Kopie zapasowe danych są wykonywane automatycznie codziennie, dzięki czemu cała operacja przebiega bardzo szybko i w niewielkim stopniu obciąża sieć klienta. Usługa została pomyślana jako szybki, ekonomiczny i wygodny sposób zapewnienia spójnego mechanizmu ochrony danych rozproszonych po różnych serwerach, stacjach roboczych, oddziałach i filiach firmy przy ograniczeniu niezbędnych nakładów na infrastrukturę sieciową.

Usługa może być atrakcyjna cenowo dla firmy praktycznie każdej wielkości — od globalnych korporacji z wieloma filiami do małych i średnich firm, ponieważ klienci płacą jedynie za ilość danych zabezpieczanych poprzez kopie zapasowe.

Oto najważniejsze zalety naszych usług zdalnej ochrony danych:

Klienci mogą oddelegować personel do innych zadań oraz znacznie ograniczyć koszty zarządzania wykonywaniem kopii zapasowych i przywracaniem danych z tych kopii.

- **Zwiększone możliwości redukcji kosztów i poprawy wskaźnika ROI.** Urządzenia i wsparcie techniczne są udostępniane klientom z wykorzystaniem centrów przetwarzania danych odpornych na awarie, co wyraźnie ogranicza potrzebę nakładów z ich strony na sprzęt i oprogramowanie. Opłata za korzystanie opiera się na ilości danych klientów wymagających ochrony. Ta optymalizacja użycia zasobów pozwala na bieżąco kontrolować ponoszone koszty. A ponieważ operacje ochrony kluczowych danych są zautomatyzowane, klienci mogą oddelegować personel do innych projektów oraz znacznie ograniczyć koszty zarządzania wykonywaniem kopii zapasowych i odtwarzaniem danych z tych kopii.
- **Ochrona danych firmy w odległej lokalizacji.** Usługa zdalnej ochrony danych przewiduje niezawodne i sprawne codzienne wykonywanie i umieszczanie w odległej lokalizacji kopii zapasowych danych serwerów i stacji roboczych na potrzeby zapewnienia ciągłości działania firmy i przywracania systemów po awarii praktycznie niezależnie od lokalizacji chronionych danych (oddziały, urządzenia przenośne itd.).
- **Wysokie poziomy obsługi i poprawione parametry utrzymania ciągłości biznesowej.** Procesy wykonywania kopii zapasowych kluczowych danych i przywracania tych danych są realizowane i zarządzane przez 24 godziny 365 dni w roku.
- **Nieinwazyjne, skalowalne narzędzia wykonywania kopii zapasowych.** Zaawansowane technologie pozwalają ograniczyć ilość pasma wykorzystywanego dla operacji ochrony danych klienta, a w efekcie zoptymalizować działanie komputerów i sieci. Usługa zdalnej ochrony danych jest realizowana w wykorzystaniu infrastruktury o wysokiej pojemności, która umożliwia dynamiczne reagowanie na zmieniające się potrzeby klienta spowodowane rosnącymi wolumenami danych.

W skrócie

Dzięki rozwiązaniom na żądanie procesy ochrony i dostępu do danych mogą być realizowane niezwykle sprawnie.

Nasze odporne na awarie centra przetwarzania danych ochronią dane klientów nawet w przypadku najbardziej dramatycznych klęsk żywiołowych.

- **Większa elastyczność użytkowania.** *Intuicyjne aplikacje i interfejsy w postaci portalu internetowego ułatwiają personelowi automatyczne wykonywanie kopii zapasowych danych i odtwarzanie danych z tych kopii zaledwie kilkoma kliknięciami myszy.*
- **Szybsze wykonywanie kopii zapasowych i odtwarzanie bez stosowania taśm.** *Systemy taśmowe mogą być powolne, nieprzyjazne w obsłudze i zawodne. Dzięki usłudze zdalnej ochrony procesy ochrony i dostępu do danych mogą być realizowane niezwykle sprawnie.*
- **Elastyczne opcje przechowywania kopii danych i długoterminowej archiwizacji.** *Usługa zdalnej ochrony danych pomaga klientom zdefiniować konkretne zasady przechowywania danych oparte na kryterium czasowym (w skali dnia, tygodnia, miesiąca i roku), dopasowane do indywidualnych potrzeb firmy wynikających z wymogów ustawowych. Ponadto oferuje opcję archiwizowania wszystkich danych na taśmach z przeznaczeniem do długotrwałego przechowywania.*
- **Bezpieczeństwo i zgodność z wymaganiami ustawowymi.** *W usłudze zdalnej ochrony danych jest stosowane szyfrowanie 128 bitowym kluczem AES (Advanced Encryption Standard). To bardzo bezpieczny mechanizm, ponieważ zapewnia możliwość dostępu do danych wyłącznie uprawnionym osobom. Ponadto nasze odporne na awarie centra przetwarzania danych ochronią dane klientów nawet w przypadku najbardziej dramatycznych klęsk żywiołowych, stanowiąc pod tym względem jedną z najbezpieczniejszych opcji dostępnych na rynku. Oferowana przez nas usługa zdalnej ochrony danych uzyskała certyfikat SAS 70 (Statement on Auditing Standards 70) typu II. To kolejne potwierdzenie, iż wykonywane za jej pomocą kopie zapasowe spełnią wymogi biznesowe i regulacyjne.*
- **Współpraca z różnymi platformami.** *Usługa zdalnej ochrony danych może współpracować z różnymi systemami operacyjnymi Microsoft® Windows®, UNIX® i Linux®, najważniejszymi systemami bazodanowymi takimi jak Oracle, Microsoft Exchange i SQL oraz maszynami wirtualnymi VMware, Microsoft i Sun.*

W skrócie

Błyskawiczne lokalne przywrócenie danych w ośrodku dotkniętym awarią pozwala spełnić coraz bardziej restrykcyjne wymagania dotyczące docelowych czasów odtwarzania RTO.

W celu skrócenia czasu przywracania do lokalizacji klienta można szybko wysłać urządzenie zawierające kopię zapasową danych klienta.

Rozwiązania i opcje dla ochrony danych serwerów

Opcja Stałego Urządzenia Lokalnego dla ochrony danych serwerów

Opcja Stałego Urządzenia Lokalnego dostępna w ramach usługi zdalnej ochrony danych zapewnia błyskawiczne przywracanie danych w ośrodku. Jest to odpowiedź na coraz większe oczekiwania klientów w zakresie docelowych czasów odtwarzania RTO. Opcja jest realizowana przez zainstalowanie wstępnie skonfigurowanego urządzenia pamięci masowej w sieci LAN klienta. W ten sposób przywrócenie sprawności serwera zajmuje kilka godzin, a nie dni.

Opcja Całkowitego Odtworzenia dla serwerów

Opcja Całkowitego Odtworzenia dostępna w ramach usługi zdalnej ochrony do zdalna, automatyczna usługa, umożliwiająca przywrócenie systemów operacyjnych i aplikacji serwera „od zera” nawet 80% szybciej niż przy tradycyjnych metodach. Opcja stanowi niezawodne i ekonomiczne narzędzie pozwalające na szybkie przywrócenie systemów kluczowych dla funkcjonowania firmy.

Opcja Szybkiego Startu dla serwerów

Opcja Szybkiego Startu dostępna w ramach usługi zdalnej ochrony danych to lokalny i wyposażony w zaawansowane zabezpieczenia mechanizm ochrony danych przeznaczony dla dużych oddziałów firm lub central średnich firm, który pozwala zdecydowanie ograniczyć czas i obciążenie sieci wymagane zazwyczaj przy pierwotnym wykonywaniu kopii zapasowej za pośrednictwem Internetu. Jego działanie polega na zebraniu lokalnej kopii danych, a następnie zaimportowaniu powstałej kopii na platformę usługodawcy.

Gdy dane znajdują się już na platformie usługowej IBM, generowanie przyrostowych kopii zapasowych za pośrednictwem Internetu trwa ułamek czasu potrzebnego na wykonanie kopii wszystkich danych.

Opcja Szybkiego Odtworzenia dla serwerów

Opcja Szybkiego Odtworzenia dostępna w ramach usługi zdalnej ochrony danych to wyposażony w zaawansowane zabezpieczenia mechanizm przywracania po awarii przeznaczony dla dużych oddziałów firm lub central średnich firm. W razie nieprzewidzianego wyłączenia serwera lub całego ośrodka do podstawowej lub awaryjnej lokalizacji klienta można błyskawicznie wysłać urządzenie zawierające kopię zapasową danych klienta. Zastąpienie przesyłania znacznych ilości danych do odtworzenia za pośrednictwem Internetu opisywanym rozwiązaniem pozwala znacznie skrócić czas przywracania dużych serwerów.

W skrócie

Kopie zapasowe danych są wykonywane automatycznie codziennie.

Rozwiązania dla ochrony danych komputerów stacjonarnych i przenośnych
W odniesieniu do stacjonarnych i przenośnych stacji roboczych usługa zdalnej ochrony danych oferuje zdalne internetowe narzędzia do wykonywania i odtwarzania z kopii zapasowych, które uwzględniają kluczowe wymagania w zakresie ochrony danych, zapewnienia ciągłości działania firmy i kosztów stawiane przez duże i średnie firmy.

Dane z komputerów stacjonarnych i laptopów klienta podlegają codziennej procedurze wykonywania kopii zapasowych za pośrednictwem istniejącej infrastruktury sieciowej w starannie zabezpieczonym zewnętrznym ośrodku składowania danych. Informacje kluczowe dla działalności firmy są centralnie administrowane, lepiej chronione i łatwiej dostępne w razie potrzeby.

Pod względem operacyjnym usługa zdalnej ochrony danych działa bardzo szybko i efektywnie. Ponieważ transmisja obejmuje wyłącznie dane, które uległy zmianie od ostatniej sesji wykonywania kopii zapasowych, usługa pozwala znacznie ograniczyć użycie pasma związane w wykonywaniem tych czynności. To z kolei oznacza mniejsze obciążenie poszczególnych komputerów i całej sieci, umożliwiając personelowi w organizacji klienta normalną pracę w trakcie procesu wykonywania kopii. Zasadniczo użytkownicy mogą wykonywać kopie zapasowe danych i odtwarzać dane z kopii w dowolnym momencie, bez pomocy personelu działu informatycznego, korzystając jedynie z intuicyjnego interfejsu użytkownika usługi zdalnej ochrony danych. Wystarczy zalogować się w aplikacji i wskazać dane, dla których mają zostać wykonane kopie lub, które mają zostać odtworzone. Dzięki możliwości wybierania indywidualnych plików lub całych folderów zazwyczaj można przywrócić różne wersje tego samego pliku z dowolnej kopii zapasowej wykonanej w ciągu ostatnich 30 dni.



© Copyright IBM Corporation 2008

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Wyprodukowano w Stanach Zjednoczonych
01-08
Wszelkie prawa zastrzeżone

IBM i logo IBM są znakami towarowymi lub
zastrzeżonymi znakami towarowymi firmy
International Business Machines Corporation w
Stanach Zjednoczonych i/lub innych krajach.

Nazwy innych firm, produktów lub usług mogą
być ich znakami towarowymi lub znakami
usługowymi.

Zawarte w tym dokumencie odniesienia do
produktów lub usług IBM nie oznaczają, że są
one dostępne we wszystkich krajach, w których
działa IBM.

Podsumowanie

Średnie firmy muszą zweryfikować sposób tworzenia kopii zapasowych dla ochrony danych przechowywanych w oddziałach i na komputerach PC przy użyciu systemów taśmowych i innych własnych rozwiązań. Ryzyko i potencjalne koszty — bezpowrotnej utraty kluczowych informacji, zakłóceń w funkcjonowaniu firmy, utraty klientów czy nieprzestrzegania wymogów narzuconych przepisami prawa — są zbyt duże. A przy rosnącej ilości krytycznych informacji biznesowych składowanych w oddziałach firmy i na komputerach użytkowników końcowych koszty ewentualnych awarii stają się coraz wyższe.

Usługa zdalnej ochrony danych może pomóc uniknąć kosztów spowodowanych utratą danych przez udostępnienie średnim firmom ekonomicznego narzędzia do ochrony rozproszonych danych.

Więcej informacji

Aby dowiedzieć się więcej o usłudze IBM zdalnej ochrony danych z pakietu Usług IBM w zakresie ochrony danych (IBM Information Protection Services – Remote Data Protection), skontaktuj się z przedstawicielem handlowym IBM lub odwiedź następującą witrynę:

ibm.com/services/continuity