

9 SKUTECZNYCH PRAKTYK

dotyczących backupu

NET COMPLEX
2017/2018

Przestój w działalności przedsiębiorstwa jest drogi.

Do tego stopnia, że menedżerowie IT muszą zrobić wszystko co w ich mocy, aby zwiększyć czas pracy bez przestojów.

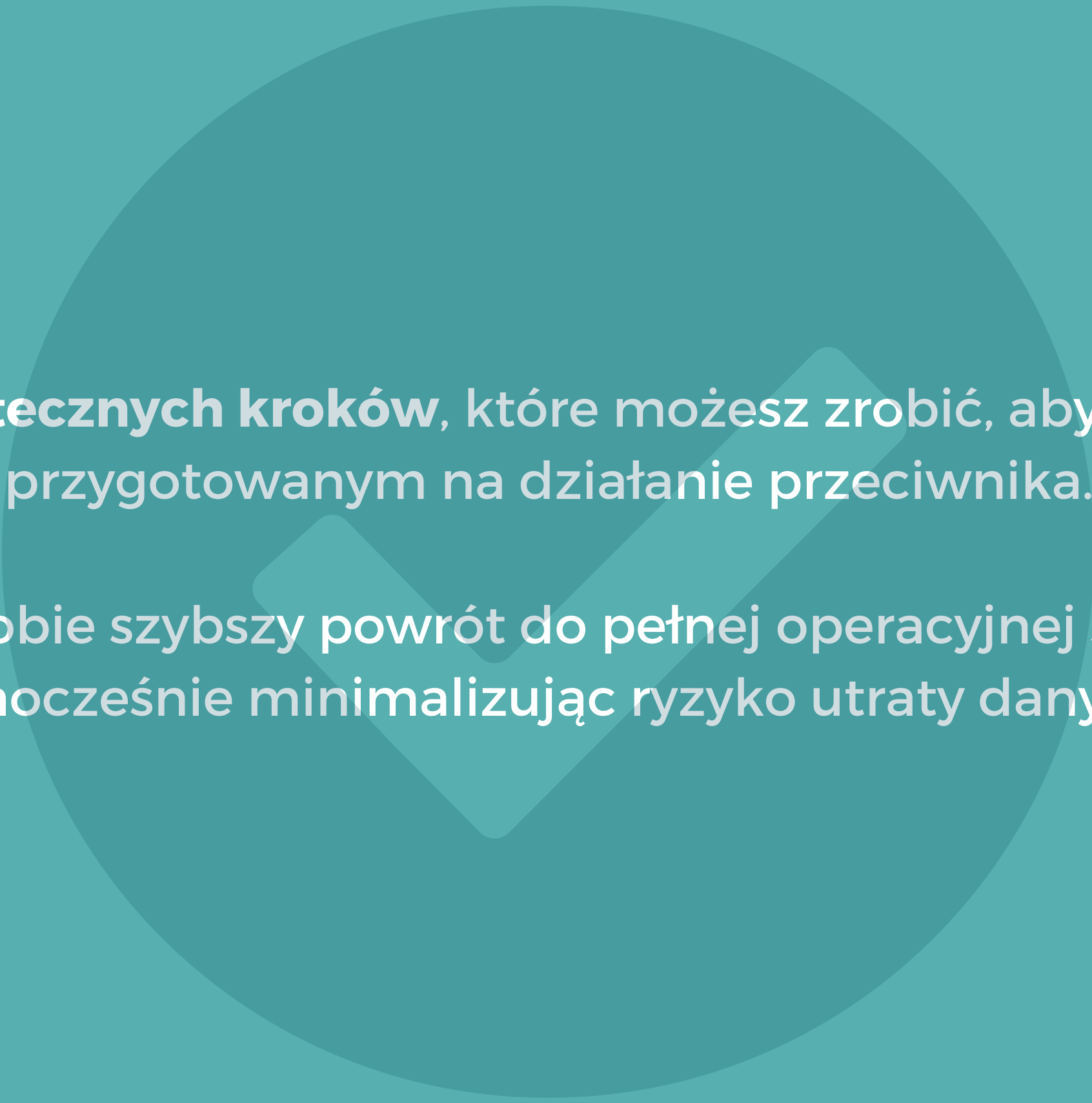
Nawet jeśli jesteś zadowolony z obecnego podejścia do tworzenia kopii zapasowych czy też odzyskiwania danych, wykonanie wskazanych 9 kroków może usprawnić pracę i pozwolić na działanie z jeszcze krótszymi przestojami. Nawet sam 1%-owy wzrost czasu pełnej sprawności może znacznie zmniejszyć ilość negatywnych skutków przestoju.



Większość osób myśli o kopii zapasowej, jako o strategii obronnej.

W obecnych czasach warto jednak nastawić się na atak wyprzedzający. Kiedy wygodnie rozsiądziesz się w fotelu, czekając, aż wydarzy się jakiś przestój, tak naprawdę nie będziesz wiedział, w jaki sposób zareagują plany naprawcze.





Oto **9 skutecznych kroków**, które możesz zrobić, aby być lepiej przygotowanym na działanie przeciwnika.

Zapewnij sobie szybszy powrót do pełnej operacyjnej sprawności, równocześnie minimalizując ryzyko utraty danych.

Szybkość i dynamika działania ransomware wzrasta bardzo szybko, wpływając na firmy każdej branży oraz każdej wielkości. W minionym roku 60% organizacji doniosło, że zostały dotknięte szkodami wyrządzonymi przez ransomware, a 70% z nich zapłaciło okup.

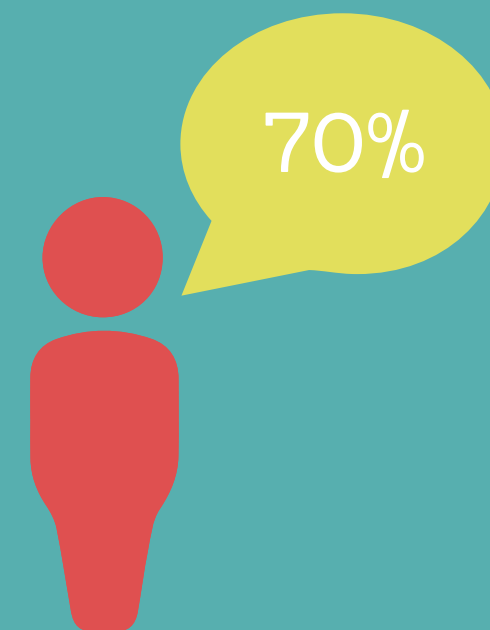
1

**Poznaj swojego przeciwnika -
najsilniejszym z nich
jest ransomware**

**Nie czekaj na czerwony
ekran - działaj!**

Ochrona antywirusowa oraz szkolenia pracowników są bardzo ważne, ale niewystarczające. Zagrożenia, pomimo wdrożenia wyżej wymienionych środków, nadal są skuteczne. Dlatego rozwiązanie dedykowane tworzeniu kopii zapasowych musi wykrywać aktywność ransomware. Dzisiejsze warianty szkodliwego ransomware opóźniają swoje ujawnienie się, aby zainfekować maksymalną liczbę plików i uzyskać jak największy okup.

Twoje rozwiązanie do tworzenia kopii zapasowych i odzyskiwania danych powinno aktywnie weryfikować możliwe infekcje plików podczas każdego wykonywania kopii zapasowej. Powinno szukać takich niuansów, jak duża liczba zmodyfikowanych plików, zmiany w systemie, które nie powinny występować oraz niewłaściwe tempo zmian. Po wykryciu Twój system do tworzenia kopii zapasowych powinien używać sztucznej inteligencji i uczenia maszynowego. W jakim celu? Aby zminimalizować liczbę fałszywych alarmów, rozpoznawać aktywną infekcję i powiadamiać administratorów o tym, by procedury odzyskiwania mogły się rozpocząć.



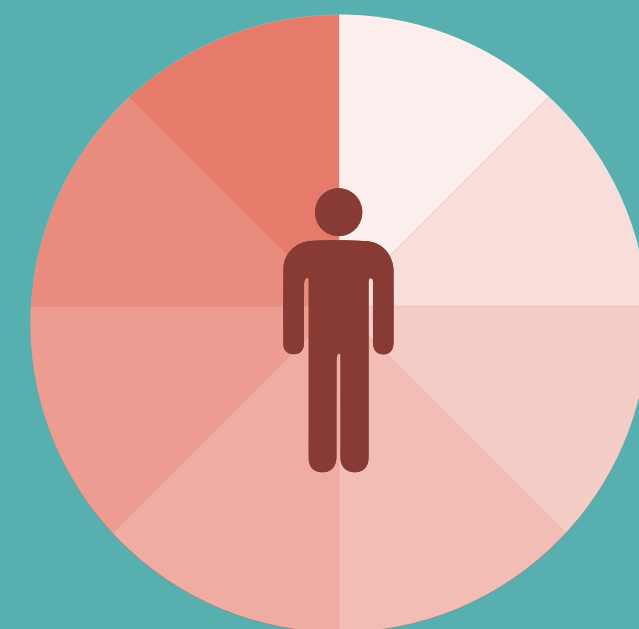
2

Nie zapominaj o backupie

Nie wiadomo kiedy wystąpi przestój, a nieudana kopia zapasowa może spowodować utratę danych. Zadbaj, aby tak się nie stało. Natomiast dbanie o to nie powinno odbywać się kosztem długotrwałego poświęcania Twojego cennego czasu i uwagi.

Nie musisz spędzać więcej niż 1 godzinę tygodniowo na zarządzaniu kopiami zapasowymi. Jeżeli wszystko działa sprawnie, powinieneś to po prostu wiedzieć. Jeśli występują jakiegolwiek problemy, powinieneś mieć wgląd w jasne do zrozumienia raporty, wskazujące newralgiczne punkty czy wymagające naprawy.

Stosowane przez Ciebie rozwiązanie do tworzenia backupu powinno nieustannie oceniać Twoje działania za pomocą e-mail i panelu administratora. Dobrze, aby pulpit nawigacyjny urządzenia miał możliwość dostosowywania umożliwiając organizowanie danych w dowolny sposób. Pełna kolekcja kopii zapasowych jest niezbędna do szybkiego odzyskiwania danych zapewniających realizację wyznaczonych celów.



Harmonogram tworzenia kopii zapasowych, to Twój przewodnik. Dobrze jest mieć pewność, że określanie harmonogramów i wykonywanie backupów jest procesem elastycznym - wspierającym cele biznesowe.

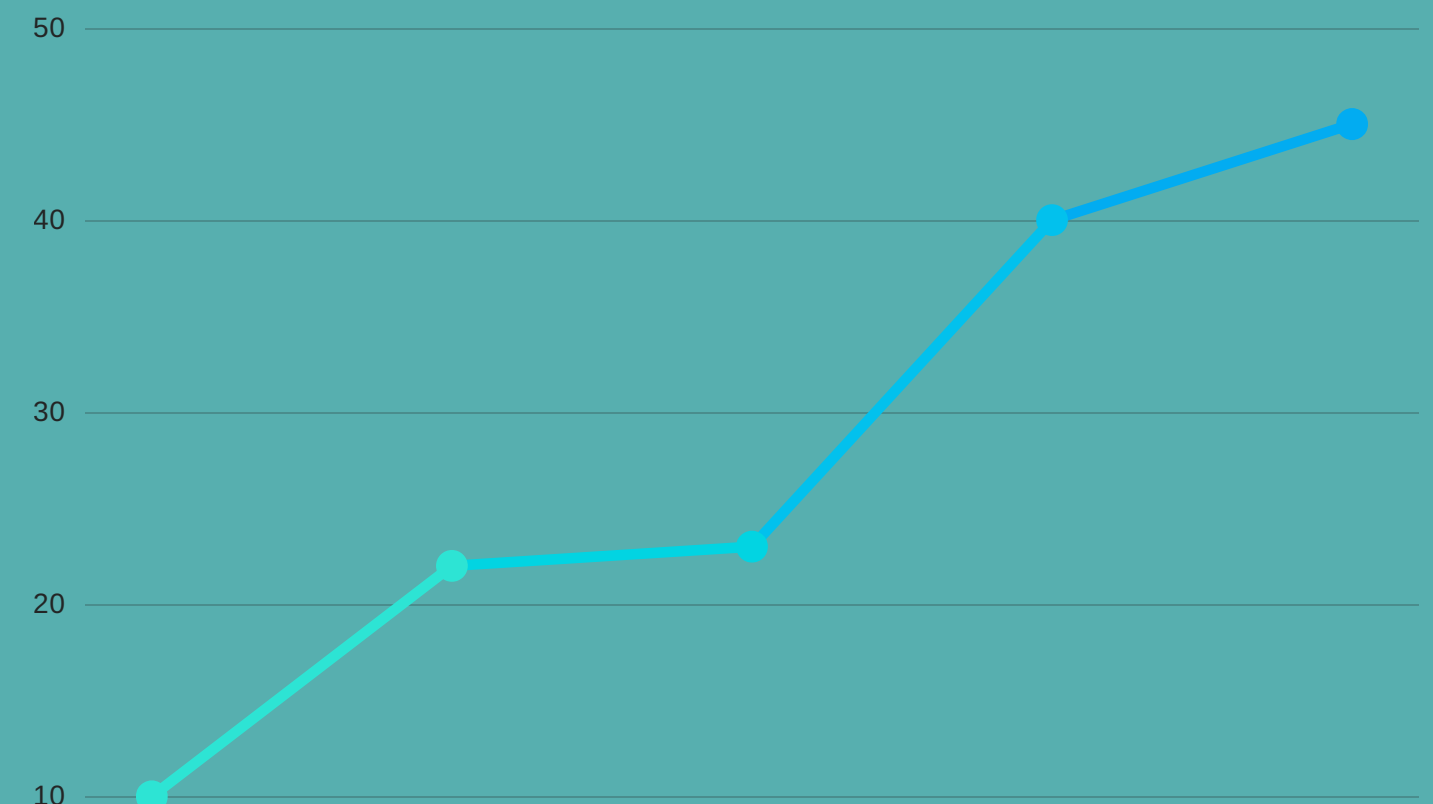
Rozwiązanie do tworzenia kopii zapasowych i odzyskiwania danych powinno oferować szeroki wachlarz możliwości planowania i wykonywania backupów. Tradycyjne sposoby pozwalają jedynie na ręczne wyznaczanie czasu, lokalizacji, celu i zasobów pamięci masowej. Co zyskujesz dzięki nowoczesnym metodom? Przede wszystkim tworzenie kopii w oparciu o cele biznesowe.

Określ swoje cele, zastanów się, gdzie chcesz przechowywać kopie zapasowe i daj systemowi działać – on sam obliczy resztę zmiennych wymaganych do spełnienia celów polityki spójności.

Dzięki temu Twój backup rzeczywiście może spełnić stawiane mu wymagania biznesowe.

3

Postaw na elastyczność



Kolekcja wykonanych kopii zapasowych w przedsiębiorstwie może być dosyć duża, a dział IT powinien pozwolić wyznaczonym administratorom na przetwarzanie danych w obszarze ich kompetencji. **Twoi użytkownicy najlepiej znają swoje dane, pozwól im więc zarządzać jak największą ich ilością.**

Rozwiązania do tworzenia kopii zapasowych i odzyskiwania danych, które obsługują dostęp oparty na rolach, dają administratorom wyznaczonych działów, kontrolę nad ich danymi - bez widoczności informacji dla innych grup.

Administratorzy, którym przyznano dostęp oparty na rolach, mogą odzyskać utracone pliki i zaplanować tworzenie kopii zapasowych spełniających ich wymagania produkcyjne oraz zarządzać własnymi kontami. Zapewnia to użytkownikom całkowitą samoobsługę.

4

Pozwól ekspertom wykonywać swoją pracę - zarządzanie oparte na rolach



Daj pracownikom przestrzeń - niech działy zarządzają kopiami zapasowymi we własnym zakresie.

5

Praktyka, praktyka i jeszcze raz praktyka - automatyczne testowanie

Testowanie polega na ćwiczeniu odzyskiwania, a zautomatyzowane testowanie - **ćwicz mądrze**. Jedynym sposobem, dzięki któremu dowiesz się w jaki sposób odzyskiwane są dane, jest regularne automatyczne testowanie – szczególnie po każdej zmianie w Twojej infrastrukturze.

Odzyskiwanie wydaje się być proste, jednak często powstają komplikacje - sporo aplikacji ma wiele poziomów, rozłożonych na różnych, wirtualnych i fizycznych maszynach. Wyobraź sobie, że chcesz przetestować odzyskiwanie nie tylko pojedynczej maszyny, ale to, jak wszystkie maszyny w aplikacji są odzyskiwane razem. **Powinieneś być pewien, że wszystkie zależności i działające na nich komponenty aplikacji można wyświetlać w odpowiedniej kolejności, bez żadnych komplikacji po awarii.**



6

**Zidentyfikuj kluczowych graczy -
oceń stan swoich aplikacji**

Aplikacje różnią się od siebie. Wybierz te, które mają największe znaczenie dla Twojej firmy, Aplikacje, które zarządzają zamówieniami klientów są znacznie ważniejsze niż te, które np. umożliwiają zwrot kosztów pracowniczych.

Rozwiązanie do tworzenia i odzyskiwania kopii zapasowych powinno umożliwić ustalenie kolejności odzyskiwania aplikacji. Jest to wymagane do lokalnego odtwarzania w centrum danych oraz do usług odzyskiwania DRaaS zlokalizowanego w chmurze.

Ty decydujesz o kolejności tego, co odzyskasz i kiedy to nastąpi.

7

Zbuduj plan działania - zobowiązanie do Service Level Agreement

Teraz, gdy wiesz, które aplikacje są krytyczne, możesz ustawić umowy SLA dla różnych klas aplikacji. W ten sposób informujesz swoich interesariuszy, jak szybko odzyskasz konkretne aplikacje i określasz maksymalną ilość danych, które można utracić w przypadku możliwego przestoju.

Twoje procedury testowe powinny porównywać przewidywane czasy odzyskiwania z zatwierdzonymi umowami SLA. Testowanie powinno odbywać się co najmniej raz w miesiącu i po każdej zmianie w infrastrukturze, np. po dodaniu nowych aplikacji lub serwerów. Raport odzyskiwania powinien być udostępniony i łatwy do zrozumienia przez kierownictwo.

Żaden plan naprawczy zlokalizowany wyłącznie w jednym miejscu nie może się powieść. Katastrofy takie jak powodzie, trzęsienia ziemi czy przerwy w dostawie energii elektrycznej, będą miały wpływ na działanie firmy czy też sam sposób odzyskiwania danych.

Druga kopia zapasowa jest potrzebna do obsługi odzyskiwania aplikacji.

Dla organizacji prowadzących działalność w jednym miejscu, chmura może okazać się dużo bardziej opłacalna niż np. finansowanie drugiej witryny.

Podczas gdy chmury hiperskalowe, takie jak Azure i AWS, mogą zaspokoić tę potrzebę, należy wziąć pod uwagę zalety specjalnie zbudowanej chmury DRaaS. Chmury DRaaS są budowane w celu optymalizacji wydajności, oferując specjalistyczne usługi. W przypadku tego typu chmury przekazujesz w outsourcing swoje wymagania DRaaS do ekspertów. Dzięki temu możesz skupić się na innych zadaniach, które spoczywają na Twoich barkach. Niektórzy oferują nawet umowy SLA dotyczące odzyskiwania, aby zwiększyć pewność, że przełączenia awaryjne zostaną wykonane poprawnie i na czas.

**Poznaj teren działania -
wtórne odzyskiwanie stron**



9

**Nie zapominaj, że istnieje coś takiego,
jak służba klientowi**

Jeżeli wystąpią problemy z Twoim backupem, możesz nie wiedzieć jak skonfigurować nową funkcję, a samo rozwiązanie również może wymagać serwisu...

Upewnij się, że usługodawca korzysta z zaawansowanych narzędzi, takich jak analizy predykcyjne w celu identyfikacji awarii sprzętu i oprogramowania, zanim wpłyną one na działanie kopii zapasowych. Poproś o ocenę poziomu zadowolenia z obsługi klienta, aby zobaczyć, co myślą inni.

Odkąd zagrożenie może uderzyć w dowolnym momencie, musisz dysponować rozwiązaniem obsługiwanym przez zespół dostępny przez telefon, czat, e-mail - 24h na dobę, 7 dni w tygodniu.

Podsumowując...

Musisz być w 100% pewien. Nie możesz pozwolić sobie na to, aby „mieć nadzieję”, że rozwiązanie do backupu, które posiadasz, będzie działało poprawnie.

Nadzieja nie jest strategią.

Przedstawiliśmy 9 aspektów, o które powinieneś zadbać, aby zredukować do minimum przestoje w firmie. Użyj dołączonej listy kontrolnej i sprawdź, czy Twoje rozwiązanie do tworzenia kopii zapasowych obsługuje te funkcje i zapewnia najszybszy możliwy czas działania.

Zastosowanie wcześniej opisanych praktyk chroni przed różnymi przyczynami przestoju - złośliwymi atakami, sabotażem pracowników oraz innymi nieprzewidzianymi, a potencjalnie destrukcyjnymi, zdarzeniami.

Nie czekaj - działaj!

lista kontrolna



świadomość
o ransomware



zarządzanie oparte
na rolach



zobowiązanie do
Service Level
Agreement (SLA)



nie przegap kopii
zapasowej



zautomatyzowane
testowanie



drugie odzyskiwanie
stron



elastyczność
w planowaniu
backupu



ocena stanu aplikacji



obsługa klienta,
na której możesz
polegać