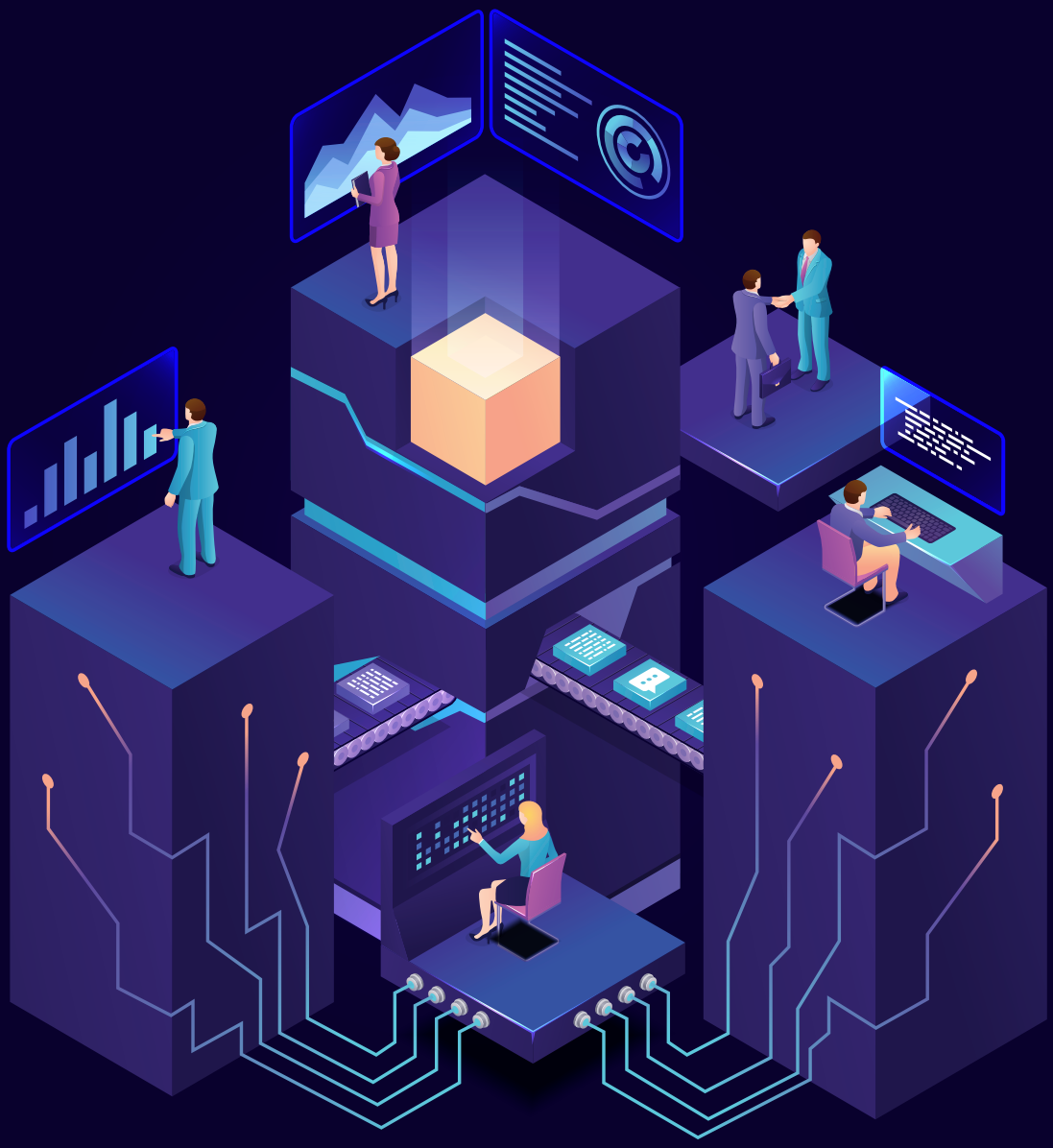
Samodzielny audyt procesów Disaster Recovery.

Czy Twoja organizacja jest przygotowana na wypadek utraty danych?



Opracowanie merytoryczne:

beyond.pl

Partner:

PURESTORAGE®

Sprawdź poziom przygotowania Twojej organizacji na sytuację awarii infrastruktury IT, która może skutkować utratą danych. Samodzielnie wykonaj audyt procesów disaster recovery i dowiedz się w jakich obszarach Twoja firma jest przygotowana na uruchomienie procesów odzyskiwania danych, a które powinna jeszcze poprawić.

Odpowiedz na 32 pytania z listy kontrolnej i sprawdź stan przygotowania Twojego przedsiębiorstwa.

Dlaczego warto się zaudytować?

Usprawnisz procedury

Wskazówki i rekomendacje podniosą poziom przygotowania Twojej organizacji na wypadek awarii skutkującej utratą danych.

Zidentyfikujesz wadliwe obszary

Wykonując samodzielnie audyt dowiesz się, które obszary w zakresie disaster recovery wymagają uwagi i optymalizacji.

Wyeliminujesz błędy

Zbadasz występowanie różnego rodzaju błędów i braków w procesach, które możesz wyeliminować.

Zredukujesz następstwa awarii IT

Odpowiednio wdrożony i egzekwowany Disaster Recovery Plan pozwoli Twojej organizacji ograniczyć następstwa wystąpienia krytycznych sytuacji.

Odkryjesz nowe możliwości

Porady i podpowiedzi zwrócą uwagę na nowe technologie i rozwiązania w obszarze disaster recovery, które dostępne są na rynku polskim.

Skorzystasz z bezpłatnych konsultacji

Skorzystaj z bezpłatnych konsultacji, w ramach których eksperci Beyond.pl zarekomendują działania w obszarze przygotowania wydajnej infrastruktury IT na potrzeby disaster recovery.

Pytania i wskazówki

Jeśli chcesz wiedzieć czy Twoja firma jest dobrze przygotowana na wystąpienie awarii IT i proces odzyskiwania danych, odpowiedz na poniższe pytania. Zaznacz jedną z trzech odpowiedzi, aby naliczyła się punktacja.
W niektórych przypadkach odpowiedzi zostaną uzupełnione automatycznie jako efekt wcześniejszych odpowiedzi. Jednak każda odpowiedź może zostać samodzielnie zmieniona. Po uzupełnieniu wszystkich odpowiedzi zostanie naliczona finalna punktacja, na podstawie której poznasz stan przygotowania Twojej organizacji w zakresie disaster recovery.

1. Zakres organizacyjny:

a. Dokumenty i procedury:

Czy masz plan odzyskiwania danych oraz systemów IT po awarii infrastruktury IT (Disaster Recovery Plan)?
Disaster Recovery Plan (DRP) to dokument zawierający zestaw procedur niezbędnych do przywrócenia działania firmy w przypadku poważnej awarii IT. Dowiedz się więcej o Disaster Recovery Plan

○ TAK ○ NIE ○ NIE WIEM

Czy plan disaster recovery był testowany w ciągu ostatnich 12 miesięcy?
Aby plan odtwarzania po awarii był skuteczny, należy go regularnie testować. Poznaj dobre praktyki i profesjonalne podejście do wykonania testów DRP. Dowiedz się więcej o testowaniu Disaster Recovery Plan

○ TAK ○ NIE ○ NIE WIEM

Czy plan disaster recovery jest regularnie weryfikowany i aktualizowany?
Należy aktualizować wszystkie dokumenty zawierające procedury odzyskiwania danych po awarii. Pod koniec każdego testu powinno się wykonać podsumowanie, które określi jak Twoje zespoły poradziły sobie z testem. Udokumentuj wszystkie wyniki i wprowadź niezbędne usprawnienia.

○ TAK ○ NIE ○ NIE WIEM

Czy zostały zidentyfikowane krytyczne systemy w firmie?
Krytyczne systemy to systemy, które zapewniają biznesową ciągłość działania – są to m.in. systemy ERP, CRM czy systemy produkcyjne i magazynowe. Opisz je procedurą DRP i regularnie poddawaj testom sprawność przywrócenia ich do działania na wypadek nagłych zdarzeń.

○ TAK ○ NIE ○ NIE WIEM

Czy został określony czas, w jakim musi nastąpić przywrócenie do działania krytycznych systemów IT?
Przywrócenie działania krytycznych systemów rozumiane jest jako stan sprzed awarii, w pełnej zgodności integracji i dostępności danych. Kluczowe jest określenie dwóch wskaźników (RTO i RPO), które określają maksymalne przedziały czasowe konieczne do odzyskania danych oraz wznowienia działania systemów. Więcej o wskaźnikach RTO i RPO dowiesz się tutaj

○ TAK ○ NIE ○ NIE WIEM

Pytania i wskazówki

Czy została wytypowana osoba odpowiedzialna za "opiekę" nad planem disaster recovery?

Konieczne jest wytypowanie zespołu odpowiedzialnego za podjęcie natychmiastowych działań w przypadku wystąpienia awarii. Zespół ten powinien być wspierany przez specjalistów IT, którzy znają się na infrastrukturze informatycznej i mogą wskazać problemy dotyczące sprzętu, oprogramowania lub systemów. Zespół ds. DR jest odpowiedzialny za tworzenie kopii zapasowych danych oraz dysponuje listami oprogramowania i kluczami licencyjnymi wymaganymi do przywracania systemu.

◯ TAK ◯ NIE ◯ NIE WIEM

Czy opracowano kalkulację ryzyka związanego z utratą danych i systemów IT?

Kalkulacja ryzyka powinna uwzględniać zagrożenia takie jak: błędy ludzkie, katastrofy naturalne, błędy technologiczne, sytuacje ekonomiczne i brak stabilności politycznej z określeniem prawdopodobieństwa ich wystąpienia oraz poziomem wpływu na funkcjonowanie Twojego biznesu.

◯ TAK ◯ NIE ◯ NIE WIEM

Czy opracowano analizę wpływu awarii na biznes?

Analiza wpływu awarii na biznes to diagnoza krytycznych procesów biznesowych w danej organizacji wraz z wyceną kosztu niedostępności usług. Różnica pomiędzy analizą wpływu na biznes a diagnozą ryzyka jest taka, że ta pierwsza określa, jaki wpływ na działalność operacyjną organizacji będzie miało przerwanie procesów biznesowych. Z kolei diagnostyka ryzyka mierzy prawdopodobieństwo wystąpienia zagrożeń i ich wpływ na procesy biznesowe.

◯ TAK ◯ NIE ◯ NIE WIEM

Czy umowy i ubezpieczania zostały skonstruowane w sposób uwzględniający pokrycie kosztów przerwania działalności, napraw, zatrudnienia dodatkowych pracowników, wynajmu tymczasowych pomieszczeń i sprzętu?

W sytuacji kiedy dojdzie do awarii, a Twoi dostawcy zrozumieją, że zapłacisz każdą cenę za krytyczne usługi czy produkt, musisz się liczyć z tym, że wielu podniesie swoje stawki w obliczu niekorzystnych okoliczności.

◯ TAK ◯ NIE ◯ NIE WIEM

b. Personel

Czy personel wie jaką rolę pełni w przypadku wystąpienia awarii?

Każdy pracownik powinien znać zakres swoich kompetencji i wiedzieć, co zrobić jeśli zaobserwuje symptomy awarii. Jest to o tyle ważne, że szybka reakcja pozwoli szybciej opanować sytuację i zminimalizować szkody.

◯ TAK ◯ NIE ◯ NIE WIEM

Czy pracownicy wiedzą, kto jest odpowiedzialny za reagowanie w nagłych wypadkach awarii IT?

Czas reakcji jest kluczowy i może wpłynąć na przebieg awarii. Zapewnienie kontaktu, który bez zbędnego opóźnienia zareaguje o każdej porze, pozwala sprawnie opanować krytyczną sytuację oraz zredukować jej następstwa.

◯ TAK ◯ NIE ◯ NIE WIEM

Czy personel wie jak się zachować, gdy zaistnieje awaria IT?
Niezależnie od pełnionej roli każdy z pracowników powinien wiedzieć, co ma robić w przypadku awarii IT. Ścisłe stosowanie się do procedur pozwoli uniknąć chaotycznych i nieprzemyślanych działań. Zespół wsparcia Beyond.pl reaguje na podstawie wypracowanych procedur i doświadczenia wyniesionego z obsługi zdarzeń u klientów.

○ TAK ○ NIE ○ NIE WIEM

2. Zakres techniczny:

a. Budynki i lokalizacje:

Czy krytyczne komponenty podstawowej infrastruktury IT (primary infrastructure) są przechowywane poza siedzibą firmy?
Utrzymywanie kluczowej infrastruktury IT wraz z krytycznymi danymi/systemami poza siedzibą firmy (np. w zewnętrznym data center) uodparnia organizację na efekty potencjalnych awarii, katastrof i innych nieprzewidzianych zdarzeń.

○ TAK ○ NIE ○ NIE WIEM

Czy kopie zapasowe krytycznych systemów IT są przechowywane poza siedzibą firmy (tzw. secondary site)?
Przechowywanie kopii zapasowych poza siedzibą firmy, chroni organizację na wypadek nieprzewidzianych zdarzeń w siedzibie. Ważne, aby lokalizacja serwerów z kopiami zapasowymi była inna niż podstawowa. Poznaj ofertę naszego Disaster Recovery Center

○ TAK ○ NIE ○ NIE WIEM

Czy podstawowa infrastruktura IT i kopie zapasowe są przechowywane w dwóch różnych i niezależnych od siebie lokalizacjach?
Ulokowanie podstawowej infrastruktury IT i kopii zapasowych w dwóch różnych lokalizacjach jest fundamentalną zasadą w projektowaniu polityki Disaster Recovery.

○ TAK ○ NIE ○ NIE WIEM

Czy lokalizacja budynku, w którym są utrzymywane kopie zapasowe była weryfikowana pod kątem potencjalnych ryzyk?
Lokalizacja kopii zapasowych w budynkach na terenach zalewowych, w pobliżu traktów kolejowych, lotnisk czy budynków stanowiących bezpośrednie zagrożenie jak stacja benzynowa zwiększa ryzyko wystąpienia katastrofy (np. powódź, pożar, wybuch, etc.)

○ TAK ○ NIE ○ NIE WIEM

Pytania i wskazówki

Czy poprawność działania instalacji grzewczych i chłodzących w budynku, w którym utrzymywane są kopie zapasowe jest regularnie kontrolowana?

Pęknięcie rury i zalanie pomieszczeń to wysoce prawdopodobne zdarzenie. Regularne kontrole instalacji ograniczają ryzyko zalania budynków i zniszczenia infrastruktury IT.

◯ TAK ◯ NIE ◯ NIE WIEM

Czy budynek, w którym utrzymywane są kopie zapasowe, jest wyposażony w zabezpieczenia przeciwpożarowe?

Nie wszystkie firmowe data center posiadają systemy przeciwpożarowe. Zabezpieczenia tego typu gwarantują, że nagłe pojawienie się ognia zostanie szybko wykryte, pożar się nie rozprzestrzeni a firmowe dane nie zostaną zniszczone.

◯ TAK ◯ NIE ◯ NIE WIEM

Czy budynek, w którym utrzymywane są kopie zapasowe, jest wyposażony w system monitoringu i bezpieczeństwa?

Budynki wyposażone w taki system są monitorowane i chronione całodobowo. Dodatkowo, obiekty wyposażone są w systemy zdalnego monitorowania parametrów pracy urządzeń z funkcją natychmiastowego powiadamiania Centrum Nadzoru. Znacząco obniża to ryzyko wystąpienia nieprzewidzianych sytuacji. Beyond.pl Data Center 2 to pierwsze data center w Unii Europejskiej i jedyne w Europie Centralnej z certyfikatem Rated 4 ANSI/TIA-942. Dowiedz się więcej

◯ TAK ◯ NIE ◯ NIE WIEM

Czy budynek, w którym zlokalizowane są kopie zapasowe, jest wyposażony w zasilanie zapasowe?

Zanik zasilania to jedna z najczęstszych awarii w firmowych i zewnętrznych data center, zatem obiekty tego typu muszą być wyposażone w system zasilania zapasowego. Jeżeli zasilanie zapasowe opiera się o generatory na silniku diesla należy mieć zakontraktowane dostawy paliwa na wypadek awarii. Zasilanie (energia elektryczna) to również istotny element kosztowy, który stanowi znaczącą część utrzymania podstawowych lub zapasowych centrów danych. Data Center 2 Beyond.pl należy do najbardziej energooszczędnych obiektów przetwarzania danych w Polsce, który oferuje PUE na poziomie 1.2. Dowiedz się więcej

◯ TAK ◯ NIE ◯ NIE WIEM

Czy budynek, w którym utrzymywane są kopie zapasowe, jest wyposażony w niezależne łącza telekomunikacyjne od wielu dostawców?

W przypadku świadczenia usług disaster recovery gwarancja stabilnej łączności z ośrodkiem podstawowym i szybki transfer danych jest jednym z kluczowych elementów wyboru dostawcy. Beyond.pl jest dostawcą neutralnym telekomunikacyjnie, oferując dostęp do globalnych operatorów klasy Tier 1, największego w Polsce punktu wymiany ruchu internetowego EPIX oraz do wielu regionalnych i lokalnych dostawców Internetu. Więcej o neutralności komunikacyjnej Beyond.pl tutaj

◯ TAK ◯ NIE ◯ NIE WIEM

Czy budynek, w którym utrzymywane są kopie zapasowe, jest wyposażony w więcej niż jedno wejście telekomunikacyjne?

Wyposażenie budynku w więcej niż jedno wejście telekomunikacyjne gwarantuje utrzymanie łączności z ośrodkiem podstawowym w przypadku mechanicznego uszkodzenia jednego łącza. W przypadku uszkodzenia jednej z tras druga zapewnia łączność. Data Center 2 Beyond.pl dysponuje dwoma niezależnymi wejściami telekomunikacyjnymi.

◯ TAK ◯ NIE ◯ NIE WIEM

Pytania i wskazówki

b. Technologie i infrastruktura IT:

Czy wdrożono firmową politykę bezpieczeństwa IT?

Polityka bezpieczeństwa IT to dokument określający cele, strategie i działania zapewniające odpowiedni poziom bezpieczeństwa IT organizacjom.

◯ TAK ◯ NIE ◯ NIE WIEM

Czy wdrożono proces zarządzania podatnościami?

Podatnościami określamy niebezpieczeństwa zachodzące w trakcie codziennej eksploatacji infrastruktury i oprogramowania (np. mechaniczne uszkodzenie sprzętu czy ataki hakerskie). Wdrożenie odpowiedniego procesu zarządzania podatnościami skutecznie ograniczy lub całkowicie zapobiegnie większości ryzyk.

◯ TAK ◯ NIE ◯ NIE WIEM

Czy wdrożono proces zarządzania aktualizacjami (patch management)?

Dzięki implementacji procesu zarządzania aktualizacjami możesz w łatwy sposób zarządzać aktualizacjami wraz z kontrolą ich wersji oraz zapewnić swojej organizacji możliwość sprawnego wdrażania aktualizacji oprogramowania.

◯ TAK ◯ NIE ◯ NIE WIEM

Czy oprogramowania antywirusowe są na bieżąco aktualizowane?

Oprogramowanie antywirusowe powinno być regularnie aktualizowane. Dzięki temu ograniczysz ryzyko ataków hakerskich opartych na exploitach (różnorodnych atakach, które wykorzystują luki w zabezpieczeniach komputerów lub sieci) i zapewnisz organizacji wyższy poziom bezpieczeństwa antywirusowego.

◯ TAK ◯ NIE ◯ NIE WIEM

Czy personel wsparcia IT nadzoruje infrastrukturę podstawową fizycznie na miejscu w trybie 24/7/365?

Im szybciej wsparcie IT zareaguje na wystąpienie awarii lub problemów technicznych, tym możliwe będzie szybsze uporanie się z nimi i ograniczenie kosztów późniejszego przywracania operacyjności Twojej organizacji.

◯ TAK ◯ NIE ◯ NIE WIEM

Czy personel wsparcia IT nadzorujący firmowe kopie zapasowe jest dostępy 24/7/365 lub na żądanie?

Dostępność i szybkość reakcji wsparcia IT umożliwia szybsze uporanie się z awarią lub problemami technicznymi, tym samym ograniczysz koszty późniejszego przywracania operacyjności Twojej organizacji.

◯ TAK ◯ NIE ◯ NIE WIEM

Czy przepływ danych w systemach IT jest monitorowany?

Dzięki monitorowaniu przepływu danych w systemach IT zapewnisz organizacji możliwość efektywniejszego wdrożenia planu disaster recovery.

◯ TAK ◯ NIE ◯ NIE WIEM

Pytania i wskazówki

Czy proces zużycia i eksploatacji infrastruktury IT jest monitorowany?
Im dłuższy czas użytkowania sprzętu, tym większe ryzyko jego awarii i utraty danych.

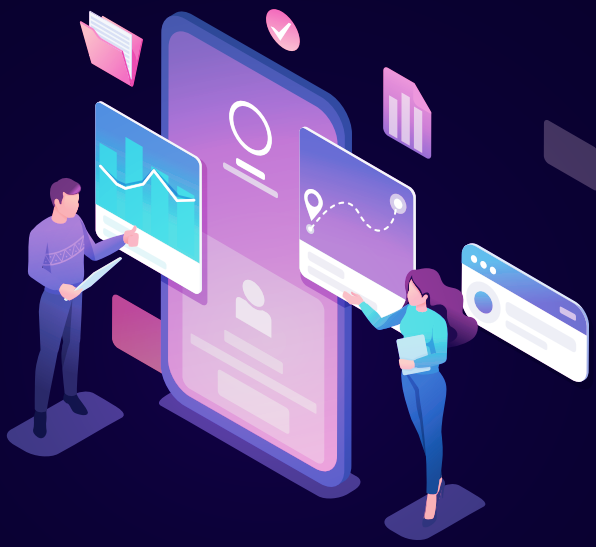
◯ TAK ◯ NIE ◯ NIE WIEM

Czy wykorzystywane systemy IT replikują się synchronicznie pomiędzy dwiema niezależnymi lokalizacjami?
Replikacja synchroniczna zapewnia zapis danych w dwóch miejscach jednocześnie, dzięki czemu żadna informacja nie zostanie utracona w przypadku awarii w centrum danych.

◯ TAK ◯ NIE ◯ NIE WIEM

Czy systemy IT, które są replikowane działają w trybie active-active serwując dane dla aplikacji z dwóch niezależnych lokalizacji równocześnie?
Dzięki takiej architekturze podwajasz wydajność systemów oraz zapewniasz ciągłość działania biznesu w przypadku jakiejkolwiek awarii.

◯ TAK ◯ NIE ◯ NIE WIEM



SPRAWDŹ WYNIK!

Rekomendacje

TWÓJ WYNIK

OBLICZ

NA PODSTAWIE UZYSKANEGO WYNIKU OCEŃ POZIOM PRZYGOTOWANIA TWOJEJ ORGANIZACJI DO ODZYSKANIA DANYCH W PRZYPADKU AWARII INFRASTRUKTURY IT. PRZECZYTAJ NASZE REKOMENDACJE.

Wynik: 22 – 32 punkty

To świetny wynik! Wygląda na to, że procedury disaster recovery zostały opracowane i wdrożone. Aby mieć pewność, że wszystkie aspekty działają prawidłowo, możesz skontaktować się z naszym ekspertem. Dowiedz się, co jeszcze można poprawić w przypadku utrzymania infrastruktury IT na potrzeby kopii zapasowych.

Wynik: 16 – 21 punktów

Całkiem dobrze! Wynik wskazuje, że Twoja organizacja wdrożyła pewne aspekty disaster recovery. Niemniej, istnieją obszary, które mogą zostać usprawnione. Skorzystaj z konsultacji z ekspertem Beyond.pl i określ co możesz poprawić w zakresie infrastruktury IT, aby zwiększyć poziom przygotowania w obszarze Disaster Recovery.

Wynik: 10 – 15 punktów

Jest sporo do zrobienia! Uzyskany wynik wskazuje, że Twoja organizacja dopiero rozpoczyna przygotowania w kierunku wdrożenia procedur disaster recovery. Nie spoczywaj na laurach, masz jeszcze wiele rzeczy do zrobienia. Skonsultuj się z Beyond.pl, aby porozmawiać o usługach BaaS (backup as a service) i DRaaS (disaster recovery center as a services). Dzięki naszemu wsparciu podniesiesz poziom przygotowania Twojej organizacji na wypadek utraty danych.

Wynik: poniżej 10 punktów

Czas na natychmiastowe działanie! Poziom przygotowania Twojej organizacji na wypadek utraty danych wymaga poprawy. Dodatkowo, umów się na konsultacje z Beyond.pl, aby ustalić kwestie związane z przygotowaniem infrastruktury IT na potrzeby utrzymywania kopii zapasowych.

Konsultacje

Skorzystaj z bezpłatnych konsultacji w zakresie przygotowania infrastruktury IT na wypadek uruchomienia procesów odzyskiwania danych.
Prześlij wypełniony dokument na adres: kontakt@beyond.pl.

W ramach projektu oferujemy 3 godziny bezpłatnych konsultacji z przedstawicielami Beyond.pl, aby zaproponować rozwiązania dostosowane do Twojego poziomu przygotowania organizacji na wypadek konieczności uruchomienia procesów odzyskiwania danych.

Konsultacje zostały podzielone na dwa bloki:

1. Analiza wyników audytu i pogłębiony wywiad stanu obecnego (2 godziny)
2. Rekomendacja rozwiązań w zakresie usług DR na bazie ustalonych założeń podczas wywiadu (1 godzina)

Jak możesz skorzystać z bezpłatnych konsultacji?

1. **Wyślij wypełniony dokument na adres: kontakt@beyond.pl**
2. **Ustal termin pierwszych konsultacji**
3. **Konsultacje: Analiza wyników i pogłębiony wywiad**
4. **Konsultacje: Wyniki i rekomendacje działań**
5. **Wzrost poziomu przygotowania organizacji na wypadek utraty danych i dostępu do systemów IT**

Nie czekaj! Zgłoś się już dziś. Dostępność eksperta jest ograniczona*.

kontakt@beyond.pl
+48 61 667 48 90

*Beyond.pl zastrzega sobie prawo do całkowitego zaprzestania świadczenia bezpłatnych konsultacji w każdym czasie, bez podania przyczyn.