

BACKUP W CHMURZE

Fakty i mity

Przyjrzeliliśmy się 10 popularnym mitom o backupie w chmurze

- Czy jest się czego obawiać?

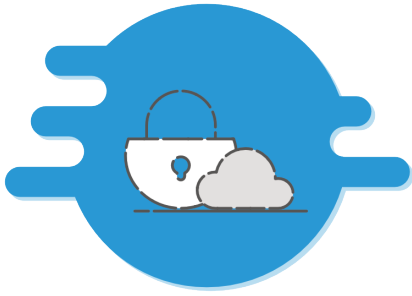


WPROWADZENIE

Firmy coraz chętniej przenoszą swoje zasoby do chmury, chociaż spora część przedsiębiorców ma co do niej mieszane uczucia. Z badań Xopero Software S.A wynika, że 58,3% przedsiębiorców uważa rozwiązania cloudowe za bezpieczne, a 41,7% spośród nich nie darzy chmury zaufaniem.

Pomimo obaw rynek rozwiązań chmurowych systematycznie rośnie. Według IDC z rozwiązań cloud computingu korzysta już 9 na 10 firm - wśród najbardziej popularnych nie sposób wymienić poczty czy narzędzi do współdzielenia i przechowywania danych, ale przedsiębiorcy powoli sięgają też po bardziej zaawansowane narzędzia. Do 2025 roku biznes umieści w chmurze 60% swoich danych.

Według 92% firm chmura ułatwia codzienną pracę. Cenią ją m.in. za automatyzację wielu procesów, dostępność oraz niskie koszty. Z drugiej strony wzbudza wspomnianą już nieufność w kwestiach związanych z bezpieczeństwem. Czy słusznie? W tym dokumencie postaramy się skonfrontować najczęstsze mity narosłe wokół backupu w chmurze z racjonalnymi argumentami.



Backup w chmurze jest mniej bezpieczny

Mit ten zakorzeniony jest w obawie przed przekazaniem istotnych danych firmowych poza jej siedzibę. Gdzie trafią dane? Do chmury... czyli dokąd? Odpowiedź na to pytanie pozwoli bardzo szybko rozwiązać wszelkie obawy.

Dostawcy rozwiązań do backupu korzystają z wyspecjalizowanych i zaufanych centrów danych - to w nich przechowywane są kopie zapasowe klientów. Centra zapewniają złożony i wysoki poziom bezpieczeństwa potwierdzony stosownymi certyfikatami i weryfikowany regularnymi audytami. To również infrastruktura dostosowana do ciągłej pracy urządzeń sieciowych oraz serwerów - odpowiednie wnętrza i budynki, zapewniające stałe dostawy energii agregaty prądotwórcze, procesy podtrzymywania zasilania (UPS), systemy klimatyzacji zapewniające właściwą temperaturę, wilgotność oraz czystość powietrza w pomieszczeniach. Wszystko starannie zaprojektowane i utrzymywane przez specjalistów. Wdrożenie takiego poziomu zabezpieczeń w pojedynczym przedsiębiorstwie jest nie tyle nieopłacalne, co wręcz niemożliwe.

Mówiąc już o samym bezpieczeństwie rozwiązań Xopero, nie sposób nie wspomnieć, że zanim dane trafią na serwer backupu w chmurze, a więc w momencie ich wysyłania z wykorzystaniem 128-bitowego certyfikatu SSL z komputera użytkownika, są szyfrowane algorytmem AES 256, uznanym za niemożliwy do złamania (korzystają z niego m.in.: banki przy realizacji transakcji płatniczych oraz amerykańska National Security Agency). Dane szyfrowane są przy użyciu klucza znanego klientowi lub klucza domyślnego (przechowywanego po stronie dostawcy rozwiązania do backupu). Czysto teoretycznie - jeżeli komuś udałoby się złamać zabezpieczenia i zdobyć dostęp do serwera - dane będą dla niego bezużyteczne. Proces deszyfryzacji zachodzi bowiem dopiero na komputerze użytkownika podczas przywracania danych.

Podsumowanie

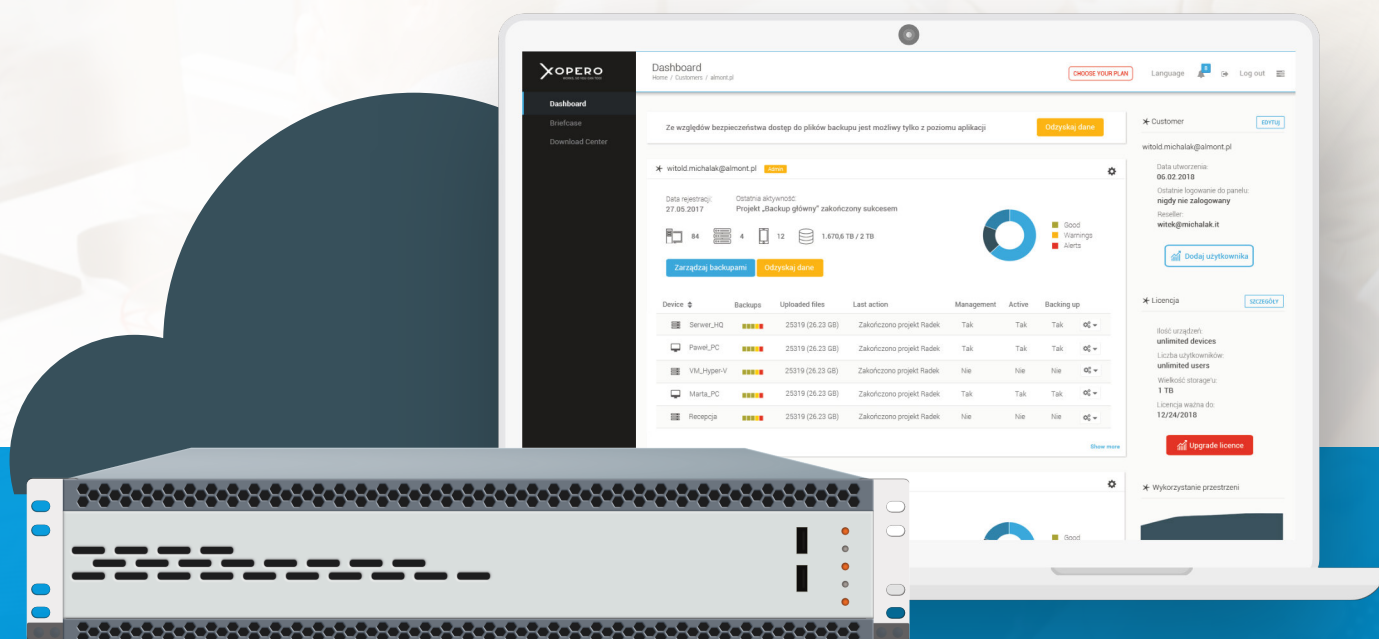
Wysokie standardy bezpieczeństwa, szyfrowanie danych, odpowiednia infrastruktura, monitoring 24/7, zespoły specjalistów, audyty bezpieczeństwa i zgodności z normami oraz certyfikaty sprawiają, że obawy o bezpieczeństwo danych firmowych przechowywanych w chmurze są nieuzasadnione.

Werdykt: **MIT JEST NIEPRAWDZIWIY.**



Xopero Cloud BACKUP W CHMURZE DLA FIRM

Zabezpieczaj kompleksowo biznesowe dane,
komputery, bazy danych, serwery, maszyny wirtualne



Prosta konfiguracja

Instalujesz aplikację
na urządzeniach, które
chcesz chronić i ustawiasz
automatyczny backup online



Brak limitów

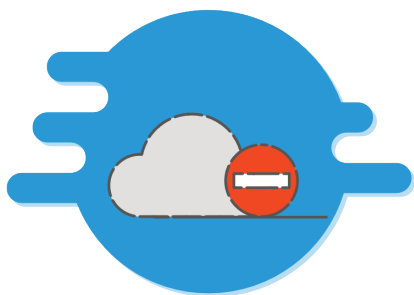
Nielimitowana liczba
urządzeń i wielkość storage'u
- ograniczone wyłącznie
Twoimi potrzebami..



Niskie koszty

Nie musisz inwestować
w drogą infrastrukturę - rób
kopie zapasowe w chmurze
i oszczędzaj.

Testuj za darmo



Dane w chmurze są mniej „dostępne”

Centra danych w których przechowywane są kopie zapasowe firmowych danych klasyfikowane są według dostępności (TIER). Zważywszy, że wyposażone są w redundantne (nadmiarowe) serwerownie, systemy zasilania i chłodzenia, zwielokrotnione połączenia sieci szkieletowej czy łącza internetowe do różnych operatorów nie może dziwić, że gwarantują dostęp do danych na poziomie 99,98% (TIER III) lub 99,99% (TIER IV). Czy dane mogą być bardziej dostępne? Czy ich przechowywanie w firmie może dać nam większą gwarancję i pewność?

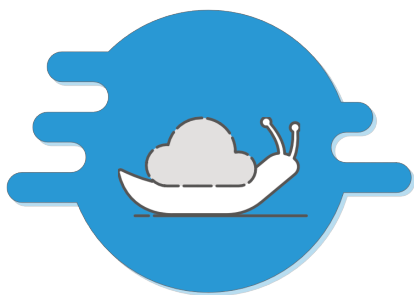
Co w przypadku awarii lub okresowych prac konserwacyjnych? Jak wówczas wyglądać będzie dostępność naszych danych?

Kopie zapasowe przechowywane w centrum danych są wielokrotnie zduplikowane. Przechowywane są nie tylko na kilku dyskach i w kilku różnych maszynach, ale również w więcej niż jednej fizycznej lokalizacji. Większość centrów danych posiada kilka lokalizacji co dodatkowo zabezpiecza dane przed różnymi zdarzeniami losowymi, klęskami żywiołowymi (jak powódź czy pożar), a także chwilowymi awariami czy pracami konserwacyjnymi. W przypadku ich wystąpienia w jednej lokalizacji, klient zawsze może pobrać swoje dane z drugiej.

Podsumowanie

Redundantna infrastruktura, wielokrotna duplikacja danych i blisko 100% gwarancja dostępności danych mówią same za siebie.

Werdykt: **MIT JEST NIEPRAWDZIWY.**



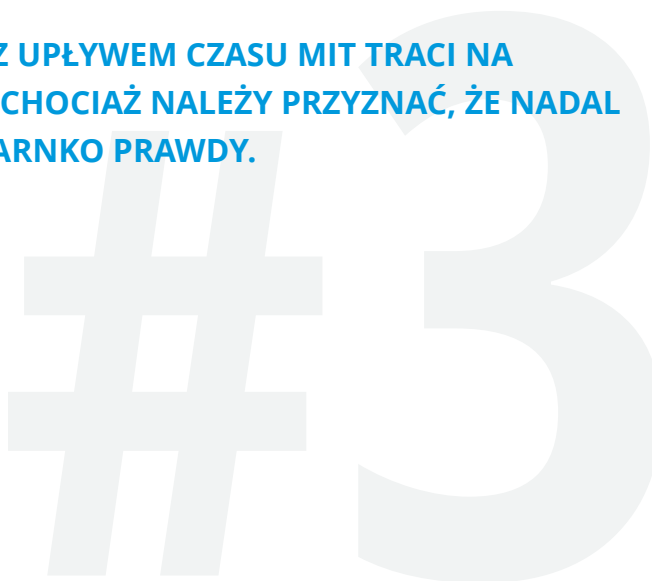
Backup wykonuje się wolno i długo...

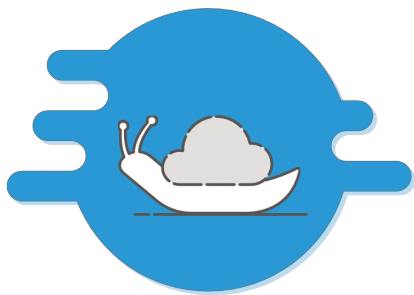
Backup w chmurze wymaga stabilnych oraz szybkich łączy internetowych. Szybkość jego wykonania zależy od prędkości łącza internetowego i choć czasy wolnego internetu bezpowrotnie minęły, to prawdą jest, że wykonuje się on nieco wolniej niż backup lokalny. Przedsiębiorcy często obawiają się również, że tworzenie kopii zapasowych wpłynie na prędkość internetu - rozwiązanie Xopero Cloud umożliwia taką konfigurację wykonywania backupu, aby wykorzystywał wyłącznie część łącza, nie ograniczając tym samym przepustowości.

Podsumowanie

Fakt, że w internecie oglądamy na co dzień seriale oraz filmy w jakości HD (w streamie) bez wieszania się i buforowania (co nie tak znowu dawno było nie do pomyślenia) świadczy o tym, że przesyłanie danych za pośrednictwem internetu nie stanowi obecnie problemu. Dynamiczny rozwój łączy internetowych, nowe technologie oraz rosnące standardy telefonii komórkowej (np. 5G) sprawiają, że może być pod tym względem tylko lepiej. Warto mieć to na uwadze.

Werdykt: **WRAZ Z UPŁYWEM CZASU MIT TRACI NA AKTUALNOŚCI, CHOCIAŻ NALEŻY PRZYZNAĆ, ŻE NADAL TKWI W NIM ZIARNKO PRAWDY.**





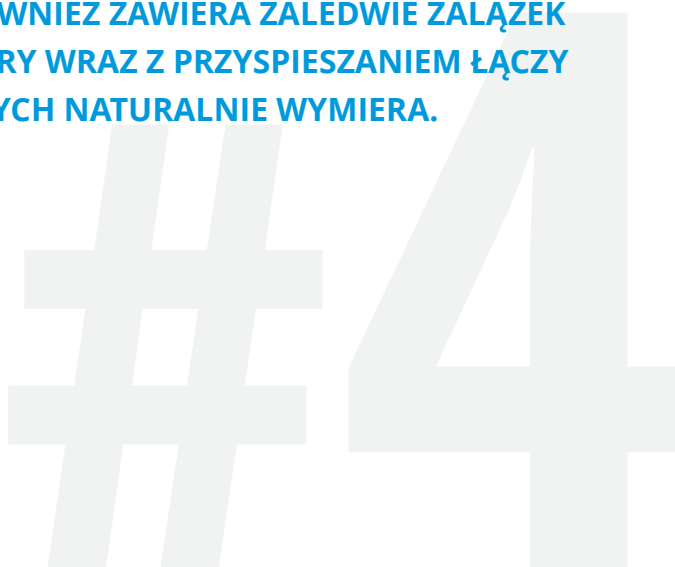
...podobnie jest z odzyskiwaniem danych

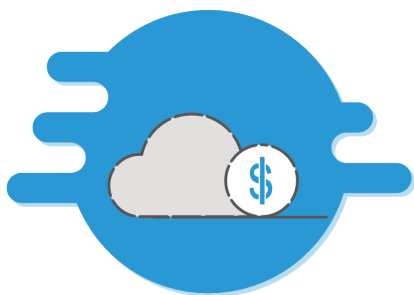
Odzyskiwanie danych z backupu w chmurze, podobnie jak tworzenie kopii zapasowej w tym ekosystemie wymaga stabilnych i szybkich łączy internetowych. Czas odzyskiwania zależy jednak nie tylko od przepustowości internetu, ale również od ilości przywracanych danych. Nie zawsze konieczne jest pobranie całej kopii backupu. Często utrata danych oznacza przypadkowe wykasowanie pojedynczego pliku lub folderu. W takich sytuacjach wystarczy pobrać z kopii zapasowej tylko utracone elementy, co nawet w przypadku wolniejszej sieci firmowej, nastąpi niemal natychmiastowo.

Podsumowanie

Postępujące procesy deduplikacji i kompresji danych, dynamiczny rozwój łączy internetowych oraz możliwość szybkiego przywracania wyłącznie wybranych plików i folderów sprawia, że "siła rażenia" tego mitu staje się znikoma.

Werdykt: **PODOBNIENIE JAK W PRZYPADKU WCZEŚNIEJSZEGO MITU, TEN RÓWNIEŻ ZAWIERA ZALEDWIE ZAŁĄŻEK PRAWDY, KTÓRY WRAZ Z PRZYSPIESZANIEM ŁĄCZY INTERNETOWYCH NATURALNIE WYMIERA.**





Backup w chmurze jest drogi

Cena jaką płaci się za przestrzeń w chmurze jest wyższa niż zakup równoważnego dysku - zgoda. Taka uproszczona kalkulacja nie uwzględnia jednak kosztów utrzymania lokalnej infrastruktury. Do serwera backupu należałoby doliczyć koszty otoczenia fizycznego, czyli pomieszczeń, prądu czy dodatkowych zabezpieczeń.

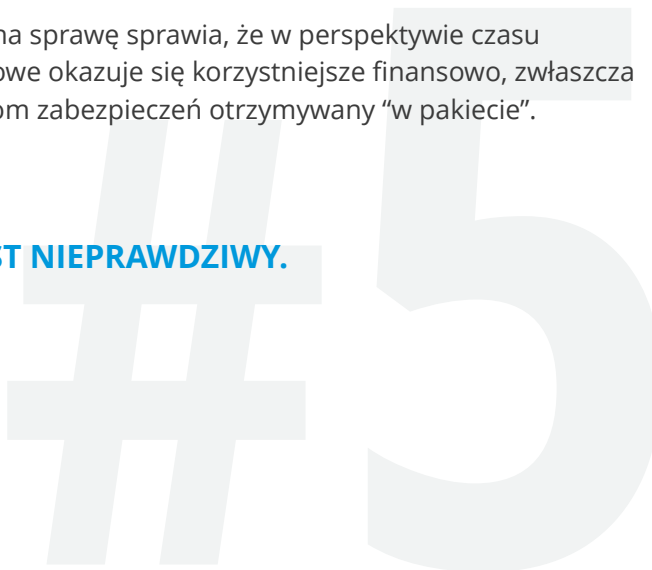
W przypadku rozwiązań chmurowych, w cenie otrzymujemy wspomniane już zabezpieczenia profesjonalnych centrów danych. Redundantna infrastruktura, duplikacja danych, monitoring 24/7, certyfikaty bezpieczeństwa, zabezpieczenie przed sytuacjami losowymi i katastrofami - to wszystko otrzymujemy w pakiecie i unikamy kosztów wdrożenia tego typu ochrony wewnętrznie w organizacji.

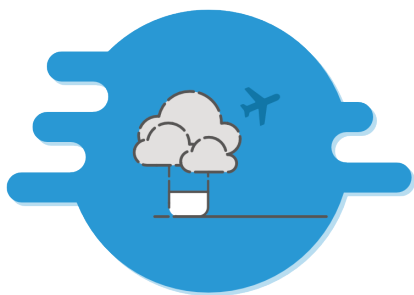
Pamiętajmy również, że korzystając z backupu w chmurze nie kupujemy przestrzeni na wyrost - płacimy tylko za realnie wykorzystane miejsce i dopiero wraz ze wzrostem potrzeb możemy zwiększyć ilość dostępnej przestrzeni. Można powiedzieć, że cloud backup jest rozwiązaniem "szytym na miarę" każdego biznesu.

Podsumowanie

Szersze spojrzenie na sprawę sprawia, że w perspektywie czasu rozwiązanie chmurowe okazuje się korzystniejsze finansowo, zwłaszcza uwzględniając poziom zabezpieczeń otrzymywany "w pakiecie".

Werdykt: **MIT JEST NIEPRAWDZIWIY.**





Backup w chmurze jest mniej wydajny...

...niż jego lokalny odpowiednik

Backup w chmurze napędzany jest przez tę samą technologię co rozwiązanie lokalne. Różnica polega przede wszystkim na miejscu przechowywania kopii zapasowych - lokalnie, w siedzibie firmy lub w chmurze. Każde z rozwiązań różni się nieco pod względem funkcjonalności, ale ciężko jednoznacznie stwierdzić, które z nich sprawdzą się lepiej. Wybór ekosystemu backupu powinien być poprzedzony analizą potrzeb i infrastruktury przedsiębiorstwa. Niemniej jednak, niezależnie od rodzaju backupu - w chmurze czy lokalnie - dane są zabezpieczone i możliwe do odzyskania w każdym momencie.

Podsumowanie

Skoro oba rodzaje backupów różnią się głównie miejscem składowania danych, kwestia wydajności jest mocno powiązana z potrzebami i wewnętrznymi uwarunkowaniami firmy.

Werdykt: **MIT JEST NIEPRAWDZIWIY.**

#6



Backup w chmurze jest skomplikowany w zarządzaniu...

...dużo bardziej niż jego lokalny odpowiednik

Oba rodzaje backupu - co już ustaliliśmy - napędza ta sama technologia, również ta odpowiedzialna za zarządzanie wykonywaniem kopii zapasowych. W jednym i w drugim rozwiązaniu istnieje możliwość centralnego, zdalnego zarządzania procesem tworzenia kopii zapasowej. W taki sam sposób definiuje się politykę tworzenia kopii bezpieczeństwa, określa dane i urządzenia do zabezpieczenia oraz harmonogram wykonywania backupu.

Podsumowanie

Jeżeli uświadomimy sobie, że podstawową różnicą między backupem lokalnym, a kopią w chmurze jest miejsce przechowywania danych, zrozumiemy, że nie ma to większego znaczenia dla funkcjonalności rozwiązań - również w aspekcie zarządzania.

Werdykt: **MIT JEST NIEZGODNY Z PRAWDĄ.**





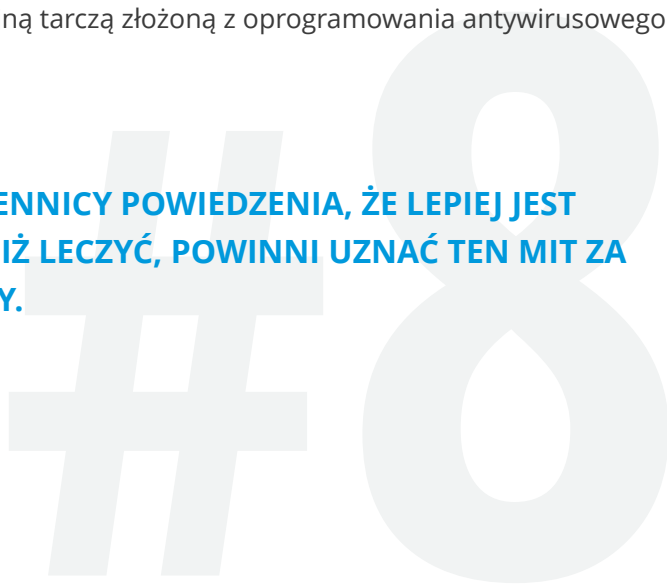
Antywirus uchroni mnie przed skutkami ataku ransomware

- *Antywirus i anty-malware to wystarczające zabezpieczenie przed ransomware, więc backup nie jest mi potrzebny.* - Niestety nie do końca... wielu przedsiębiorców jest przeświadczone, że antywirus skutecznie ochroni biznes przed atakiem ransomware. Co prawda producenci programów anty-malware stale ulepszają swoje produkty, ale nieustannie też mierzą się z coraz to większą pomysłowością przestępców i nowymi sposobami infekowania firmowych systemów komputerowych. To swego rodzaju nieustająca wojna. Oczywiście takie rozwiązania to podstawa i świetnie jeśli je posiadasz, ale nawet z nimi musisz liczyć się z tym, że możesz paść ofiarą tej walki. Co wtedy zrobisz? Jak widzisz, sam antywirus nie wystarczy. Przed skutkami ataków ochroni Cię backup. Zamiast płacić często horrendalnie wysoki okup, dzięki kopii w chmurze przywrócisz zaszyfrowane przez przestępców dane i...spokojnie wrócisz do swojej pracy. Antywirus i backup powinny być więc traktowane jako dwustopniowe zabezpieczenie Twoich danych przed ransomware.

Podsumowanie

Przezorny zawsze ubezpieczony... dlatego lepiej jest chronić dane firmowe za podwójną tarczą złożoną z oprogramowania antywirusowego oraz backupu.

Werdykt: **ZWOLENNICY POWIEDZENIA, ŻE LEPIJ JEST ZAPOBIEGAĆ NIŻ LECZYĆ, POWINNI UZNAĆ TEN MIT ZA NIEPRAWDZIWY.**





Cloud backup i cloud storage to dokładnie to samo

Przechowywanie danych w chmurze, czyli cloud storage to nie to samo co cloud backup, który jest procesem tworzenia kopii bezpieczeństwa danych firmowych by w wypadku awarii, ataku ransomware lub błędu pracownika móc je szybko odzyskać z kopii zapasowej, zapewniając tym samym ciągłość działania firmy.

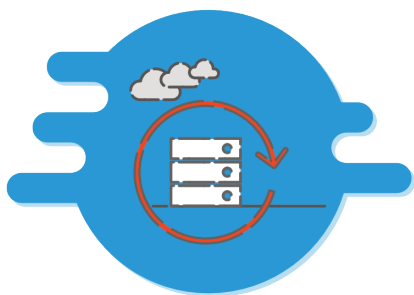
Cloud storage, którego popularnym przykładem są usługi Dropbox czy Google Drive, pozwala na przechowywanie kopii firmowych umów, faktur oraz dowolnych danych w chmurze. Nie zabezpiecza jednak firmowego serwera i komputera wraz ze zgromadzonymi danymi przed awarią, atakiem ransomware oraz błędem ludzkim.

Wykonując backup danych firmowych powstałą kopię bezpieczeństwa przechowujemy na storage'u. Nie są to jednak kopie wybranych plików czy dokumentów firmowych lecz specjalnie spreparowane pliki kopii bezpieczeństwa, które są zaszyfrowane, przechowywane w paczkach danych w formie pofragmentowanej (chunks), przez co pozostają „nieczytelne” dla osób trzecich. Backup w chmurze pozwala nam wykonać nie tylko kopie wybranych plików, ale również zabezpieczać całe dyski lub wybrane ich partycje przy pomocy backupu obrazu. W sytuacji, gdy dojdzie do uszkodzenia zbackupowanego dysku twardego w firmowym komputerze, zgromadzone dane oraz aplikacje odtworzymy z kopii bezpieczeństwa.

Podsumowanie

Powszechnie mylony ze sobą cloud storage i cloud backup to dwa zupełnie odmienne pojęcia. Przechowywanie danych w chmurze (cloud storage) to nowoczesna i wygodna alternatywa dla dysku przenośnego lub pendrive'a. Jednak jej utożsamianie z backupem danych w chmurze oraz zabezpieczeniem danych firmowych przed niespodziewanymi zdarzeniami jest olbrzymim nadużyciem.

Werdykt: **MIT JEST WYSOCE NIEPRAWDZIWY.**



Wykonując backup lokalnie, nie ma potrzeby robić kopii do chmury...

Dane firmowe chronić można nie tylko lokalnie lub w chmurze. Najskuteczniejszym sposobem ich ochrony jest połączenie obu tych rozwiązań w tzw. backup hybrydowy. Zyskuje się wówczas stabilność rozwiązań lokalnych z elastycznością chmury i 100% gwarancję bezpieczeństwa danych.

Kopia przechowywana lokalnie pozwala na szybkie przywracanie danych firmy w razie awarii czy ataku. Kopia w chmurze stanowi z kolei doskonałe zabezpieczenie na wypadek utraty backupu lokalnego w wyniku katastrofy takiej jak chociażby pożar czy powódź.

Podsumowanie

Chcąc spać spokojnie warto sięgnąć po backup hybrydowy, który jest spełnieniem złotej reguły tworzenia kopii zapasowych. Zasada „3-2-1” wskazuje bowiem, że dla zapewnienia bezpieczeństwa danych firma powinna posiadać co najmniej 3 kopie zapasowe przechowywane w co najmniej 2 różnych lokalizacjach z czego co najmniej jedna powinna mieścić się poza siedzibą firmy. Redundantna infrastruktura centrum danych i wielokrotna duplikacja danych sprawia, że w chmurze kopie zapasowe przechowywane są na kilku dyskach, w kilku różnych maszynach, a także w więcej niż jednej fizycznej lokalizacji, czyli w co najmniej dwóch różnych centrach danych.

Werdykt: **MIT MOŻNA UZNAĆ ZA NIEPRAWDZIWIY.**

