451 Research® | PATHFINDER REPORT

Przejęcie kontroli nad danymi pakietu Office 365

ZLECENIODAWCA:

VEEAM

MARZEC 2019

Informacje o tym raporcie

W raporcie z serii Pathfinder decydenci mogą znaleźć omówienie kwestii związanych z określoną technologią lub rodzajem zastosowań, prezentację korzyści biznesowych wynikających z wdrożenia, a także zalecenia dotyczące ważnych czynników wpływających na podejmowane decyzje i dalszych kroków w procesie decyzyjnym.

O AUTORZE

STEVEN HILL

STARSZY ANALITYK DS. PAMIĘCI MASOWEJ

Steven Hill jest starszym analitykiem ds. technologii pamięci masowej. Zajmuje się najnowszą generacją systemów hiperkonwergentnych, pamięci masowej w chmurze oraz rozwiązań z zakresu ciągłości działania i odzyskiwania po awarii przeznaczonych dla klientów korporacyjnych.

Streszczenie

Dla wielu klientów biznesowych nowoczesne aplikacje typu SaaS (Software-as-a-Service), takie jak pakiet Microsoft Office 365, mają dużą przewagę nad tradycyjnym modelem korzystania z oprogramowania, ale większa elastyczność licencjonowania w chmurze oraz dostępność współdzielonej chmurowej pamięci masowej rodzi nowe wyzwania z zakresu zarządzania danymi. Aplikacje działające w chmurze cechują się bardzo dużą dostępnością i odpornością na czynniki zewnętrzne, ale konieczność ochrony danych SaaS pakietu Office 365 przed takimi czynnikami ryzyka jak przypadkowe usunięcie, zagrożenia bezpieczeństwa i luki w zasadach przechowywania — a także przestrzegania stale ewoluujących przepisów prawa z zakresu nadzoru nad danymi — podtrzymuje zapotrzebowanie na tradycyjną ochronę i kontrolę, którą zapewniają automatycznie tworzone i weryfikowalne kopie zapasowe pakietu Office 365.

Dostawcy SaaS koncentrują się na ochronie własnej infrastruktury z myślą o dotrzymywaniu umów o poziomach usług (SLA), ale ochrona ta nie obejmuje danych klientów tworzonych i przechowywanych na tych platformach. Jest to zrozumiałe, jeśli wziąć pod uwagę potencjalne problemy prawne, stąd większość umów licencyjnych dostawców SaaS stanowi, że ochrona danych należy do obowiązków klienta, a nie dostawcy. Tak rodzi się niezmiernie ważne pytanie: „Co należy zrobić, aby zapewnić ochronę firmowych danych Office 365 i kontrolę nad nimi?”

Główne wnioski

- **Wiadomości e-mail i dokumenty pakietu Office 365 udostępniane oraz przechowywane w programach SharePoint, OneDrive i Teams to nowy rodzaj krytycznych danych biznesowych.** Punktem wyjścia wielu planów zapewnienia ciągłości działania/odzyskiwania po awarii jest ochrona najważniejszych baz danych i innych krytycznych aplikacji. Jednak nieusystematyzowane dane powstające w aplikacjach typu SaaS zaczynają przyrastać w tempie szybszym niż tradycyjna zawartość baz danych, a ich utrata lub zniszczenie może mieć równie katastrofalne konsekwencje.
- **Upowszechniło się błędne przekonanie, że dane SaaS przechowywane w chmurze są z natury bezpieczne.** Chmura publiczna jest bardzo niezawodna, a chociaż same platformy SaaS są wewnętrznie chronione przed przerwami w dostępie do usług, obowiązek zabezpieczenia i ochrony tych danych w chmurze oraz określenia zasad ich przechowywania spoczywa na kliencie.
- **Rozbudowane możliwości odzyskiwania i nadzoru stają się niemal równie ważne jak samo tworzenie kopii zapasowych danych.** Korzyści wynikające z wdrożenia platformy do backupu danych pakietu Office lub podobnych w dużej mierze wiążą się z odzyskiwaniem i zarządzaniem. Chociaż wchodzące w skład pakietu Office 365 programy SharePoint i OneDrive zawierają narzędzia do archiwizacji danych i konfigurowania odpowiednich przepływów pracy, funkcje te nie zastąpią backupu danych Office 365, który gwarantuje niezależność wszystkich danych od samej platformy oraz umożliwia zarządzanie nimi przy użyciu narzędzi zapewniających bardziej granularne odzyskiwanie, zabezpieczanie i nadzorowanie.

- **Ochrona danych będzie w coraz większym stopniu związana z nowymi wymogami prawnymi.** Tradycyjny backup danych ma jeden zasadniczy cel: zapobiec utracie danych. Jednak operacje eDiscovery oraz regulacje dotyczące prywatności, takie jak unijne ogólne rozporządzenie o ochronie danych (RODO) i uchwalona w 2018 r. ustawa California Consumer Privacy Act of 2018, kładą nowy grunt pod ochronę danych i nadzór nad nimi. Kopia zapasowa pakietu Office 365 może spełnić wiele istotnych wymagań z zakresu ochrony i bezpieczeństwa danych, a także stanowić wzorcowy zestaw danych do analizy, przy użyciu którego można zapewnić przestrzeganie przepisów zobowiązujących firmy do lokalizowania i ujawniania wszelkich danych zawierających informacje osobowe, a także okazania dowodu usunięcia takich danych.

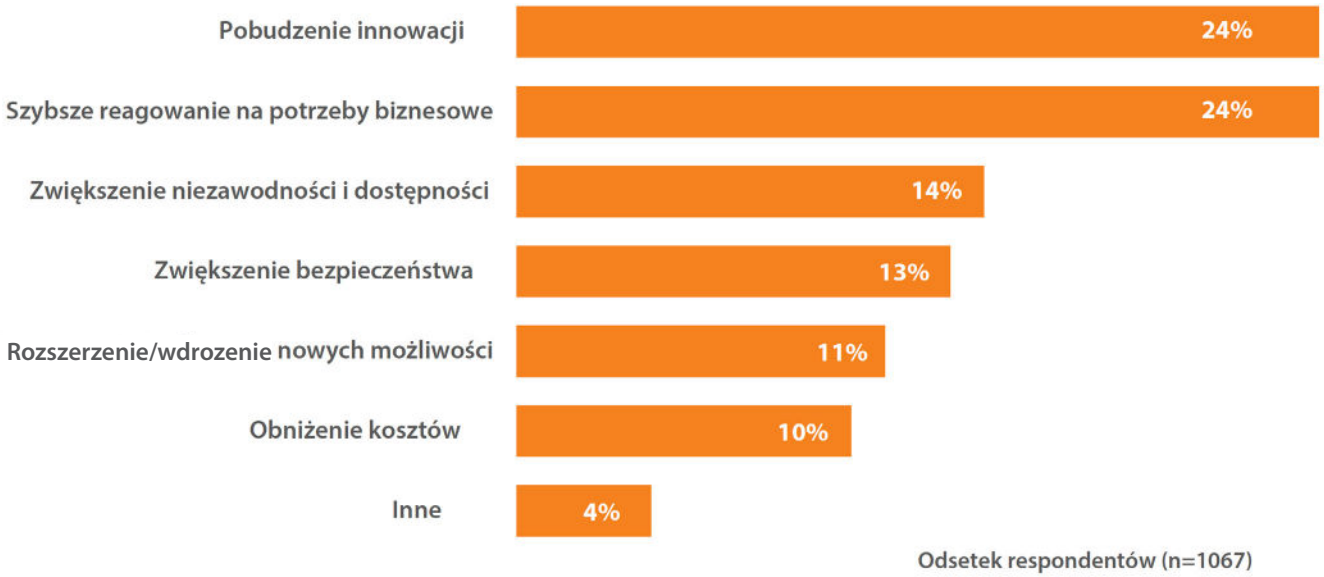
Ewolucja firmowych środowisk IT i nowa rola danych SaaS

W dzisiejszym biznesie opartym na technologiach IT pierwszorzędne znaczenie ma szybkość. Jest tak już od dziesięcioleci, a wdrożenie właściwej technologii w znacznym stopniu decyduje o sukcesie i rozwoju firm w niemal każdej branży. Obecnie nowy model chmurowy umożliwia firmom elastyczne korzystanie z aplikacji, infrastruktury, usług i danych, ale dla działów IT głównym zadaniem pozostaje znalezienie właściwego połączenia technologii, które umożliwi realizację celów biznesowych. Aby lepiej poznać te cele w skali całej branży, w ramach serwisu 451 Research Voice of the Enterprise (VotE) regularnie pytamy ponad 1000 pracowników działów IT przedsiębiorstw, co odgrywa najważniejszą rolę w ich środowiskach (ilustracja 1). Konsekwentnie okazuje się, że najistotniejsze czynniki to innowacje i szybkość reakcji.

Ilustracja 1. Najważniejsze cele firmowych działów IT na najbliższy rok

Źródło: 451 Research. Voice of the Enterprise: Digital Pulse, Vendor Evaluations 2018

P. Jaki jest najważniejszy cel działu IT w Państwa przedsiębiorstwie na najbliższe 12 miesięcy?



Oprogramowanie jako usługa (Software as a Service — SaaS) to jedna z głównych technologii opartych na chmurze, która przyczynia się do wzrostu innowacyjności i szybkości reakcji. Do najważniejszych zalet modelu SaaS należą elastyczne licencjonowanie i spójność wersji, które podnoszą wydajność i stopień interakcji użytkowników. Z perspektywy biznesowej trudno zanegować wygodę modelu SaaS, zwłaszcza w przypadku takich pakietów aplikacji jak Office 365, które udostępniają nie tylko funkcje tworzenia ważnych dokumentów biznesowych, e-maili i innych materiałów oraz zarządzania nimi, ale także mechanizmy współpracy w chmurze.

Dodatkowo pakiet Office 365 oferuje zintegrowane funkcje przechowywania danych w chmurze publicznej w ramach programów SharePoint, OneDrive i Teams, które zmniejszają zapotrzebowanie na lokalną pamięć masową oraz ułatwiają wspólny dostęp do danych na potrzeby współpracy. Rozpowszechniło się jednak błędne przekonanie, że dane klientów korzystających z modelu SaaS są chronione i bezpieczne, ponieważ znajdują się „w chmurze". Tymczasem tak po prostu nie jest, a umowa licencyjna dotycząca pakietu Office 365 wyraźnie stanowi, że odpowiedzialność za należyte środki ochrony danych ponosi klient. Właśnie w tym miejscu ważną rolę do odegrania mają działy IT przedsiębiorstw, które powinny pomóc najważniejszym interesariuszom w określeniu odpowiednich zasad ochrony, zabezpieczania, dostępności i przechowywania danych, a następnie przełożyć te ustalenia na właściwą kombinację technologii. Chociaż takie podejście może nieco skomplikować wdrożenie rozwiązania SaaS z perspektywy użytkowników, inwestycja w plan spójnej, hybrydowej ochrony danych zwróci się z nawiązką w przypadku przestoju systemów mogącego wpłynąć na dane krytyczne dla działalności firmy lub regulowane przepisami prawa.

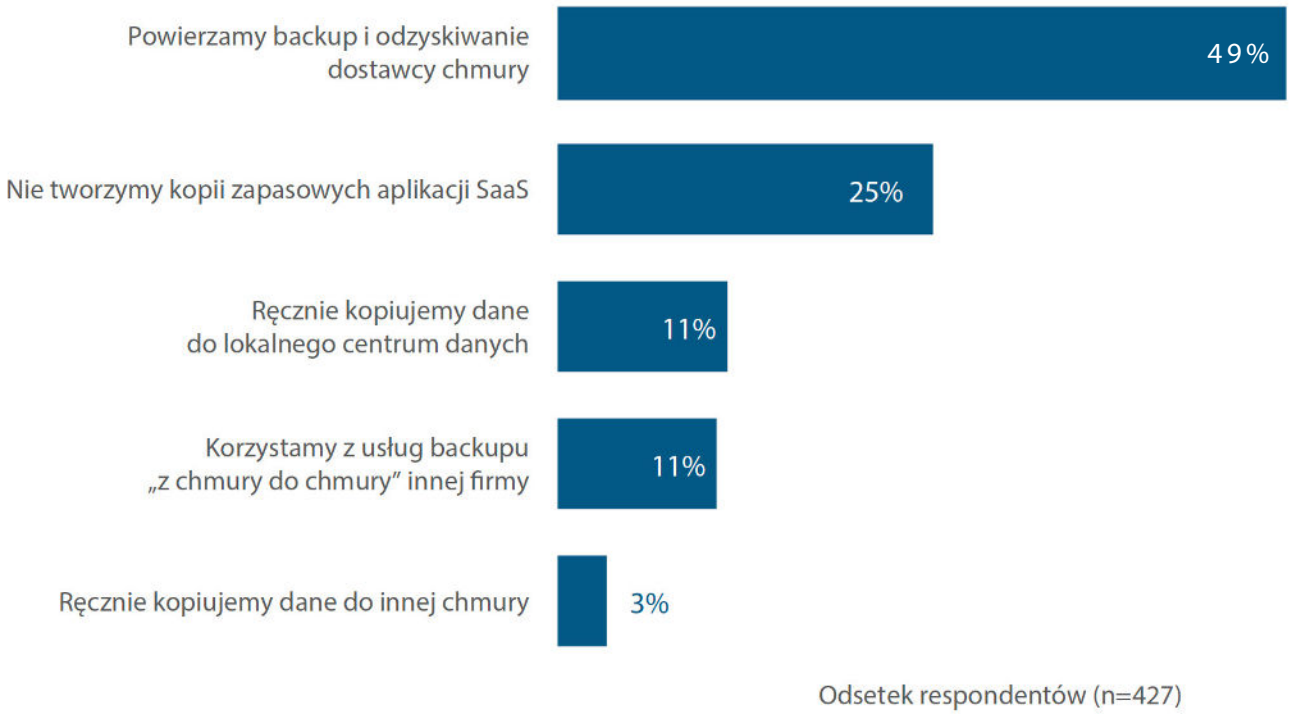
Backup danych SaaS w chmurze publicznej — problem z głowy?

Jest kilka powodów, dla których tworzenie kopii zapasowych pozostaje jednym z kluczowych elementów ochrony danych. I chociaż dostawcy rozwiązań SaaS koncentrują się na dbaniu o odporność infrastruktury i dostępność aplikacji na swoich platformach, do najlepszych praktyk z zakresu ochrony danych i zapewniania ich odporności na czynniki zewnętrzne wciąż należy tradycyjna reguła 3-2-1. W przypadku danych SaaS dynamika tego układu ulega zmianie, ponieważ dane oryginalne mogą powstawać i istnieć wyłącznie na platformie chmurowej dostawcy SaaS. Dlatego trzeba zadbać o ich backup w drugim, niezależnym miejscu — albo w odrębnej lokalizacji IaaS w chmurze, albo w środowisku lokalnym, jeśli tak wynika z wymogów prawnych obowiązujących w danej branży.

Chmurowe centra danych warstwy pierwszej są projektowane tak, aby zapewnić najwyższy poziom dostępności (w modelu 24/7/365), bezpieczeństwa i odporności, ale mimo tych najnowocześniejszych rozwiązań większość dostawców chmury często zaleca model, w którym ochronę przed przestojami osiąga się przez zastosowanie wielu centrów danych i/lub stref dostępności. Problem w tym, że model replikacyjny, którego ci dostawcy używają do ochrony własnych systemów, to nie to samo co niezależny backup danych SaaS klientów. Przedstawione poniżej dane uzyskane przez firmę 451 za pośrednictwem serwisu VotE pokazują istniejące wśród klientów różnice w ochronie danych generowanych na platformach SaaS i zarządzaniu nimi.

Ilustracja 2. Ochrona danych SaaS

Źródło: 451 Research. Voice of the Enterprise: Storage, Budgets and Outlook 2017
P. Jaka jest podstawowa strategia Państwa przedsiębiorstwa dotycząca ochrony danych aplikacji SaaS?



Jak wynika z pięciu opcji wymienionych na ilustracji 2, tylko 11% respondentów w znacznym stopniu odpowiada na podstawową potrzebę spójnego i zautomatyzowanego backupu. Chociaż tworzenie kopii zapasowych nie musi odbywać się w modelu „z chmury do chmury", zdecydowanie musi być niezależne od samej platformy chmurowej. Wszelkie kopiowanie ręczne jest nieefektywne i podatne na błędy, natomiast 25% respondentów, którzy w ogóle nie tworzą kopii zapasowych, naraża się na niebezpieczeństwo i wysokie koszty. Największy odsetek respondentów powierza backup i odzyskiwanie dostawcy chmury, ale takie rozwiązanie ma rację bytu tylko wówczas, gdy dostawca SaaS oferuje odrębne kompleksowe usługi tworzenia i odzyskiwania kopii zapasowych. Większości dostawców to nie dotyczy i to nieporozumienie może być dużym zagrożeniem dla krytycznych danych biznesowych. Ostatecznie problem sprowadza się do sprawdzonej w praktyce reguły, zgodnie z którą należy tworzyć kopię zapasową danych w drugim systemie/drugiej lokalizacji: metodą chmura-chmura lub chmura-środowisko lokalne.

Pakiet Office 365 i rosnące znaczenie przechowywanych w nim krytycznych danych biznesowych

Tradycyjnie najwyższy priorytet w obszarze zapewniania ciągłości działania/odzyskiwania po awarii dawano bazom danych — i słusznie. To logiczne, że jako główne aplikacje wykorzystywane w działalności przedsiębiorstw bazy danych są najważniejszym obiektem ochrony, jednak czasy się zmieniają. Obecne środowisko biznesowe jest coraz bardziej zależne od dokumentów, e-maili i innych krytycznych danych tworzonych, przechowywanych i udostępnianych w usłudze SaaS, jaką jest pakiet Office 365. Tego rodzaju informacje stanowią coraz wyraźniejszą większość wśród lokalnych i zdalnych danych, które są wytwarzane i przechowywane jako krytyczne zasoby nowoczesnych przedsiębiorstw.

Odruchowo można pomyśleć, że wszystkie rodzaje ochrony danych są do siebie podobne, ale ochrona infrastruktury Office 365 znacznie różni się od ochrony danych klientów utworzonych i przechowywanych w pakiecie Office 365. Dlatego tak ważne jest, aby dział IT pomógł w określeniu względnego znaczenia danych Office 365 dla działalności firmy, aby wybrać odpowiednie mechanizmy ochrony danych i nadzoru. I chociaż elastyczność współpracy wynikająca z przechowywania danych na współdzielonej platformie SaaS jest niewątpliwym plusem, dział IT tym bardziej powinien zadbać o odpowiednie zabezpieczenia, które uchronią te dane przed celowym włamaniem.

Ta dziura w ochronie danych nie umyka uwadze cyberprzestępców, którzy od pewnego czasu świadomie celują ataki ransomware i inne złośliwe działania w luki powstające na styku odpowiedzialności dostawców SaaS i przedsiębiorstw-właścicieli danych. Problem dostrzegają także organy regulacyjne, które coraz więcej uwagi poświęcają bezpieczeństwu danych. W 2018 r. firma 451 w ramach serwisu VotE zapytała klientów korporacyjnych o ich największe obawy związane z bezpieczeństwem z ostatnich 90 dni. Co ciekawe, obawy odnoszące się do zgodności z regulacjami branżowymi uplasowały się wyżej od tych dotyczących złośliwych ataków.

Ilustracja 3. Najważniejsze obawy dotyczące bezpieczeństwa informacji w ciągu ostatnich 90 dni

Źródło: 451 Research. Voice of the Enterprise: Information Security, Organizational Dynamics 2018
P. Jakie największe obawy dotyczące bezpieczeństwa informacji wystąpiły u Państwa w ciągu ostatnich 90 dni?

Większość powyższych obaw niemal dokładnie pokrywa się z typowymi lukami w zabezpieczeniach pakietu Office 365 i innych współdzielonych środowisk danych. Jednak ryzyko to można znacznie ograniczyć przez wprowadzenie schematu ochrony danych opartego na klasycznej regule backupu 3-2-1 oraz zaplanowanego tak, aby spełnić wymagania dotyczące wartości RTO i RPO. Przechowywane głównie w chmurze dane pakietu Office 365 są wygodne w użyciu i stosunkowo wysokodostępne, ale zgodnie z najlepszymi praktykami i tak należy co najmniej tworzyć ich kopie zapasowe w chmurze publicznej, na przykład Azure lub AWS, ewentualnie w środowisku lokalnym w celu zapewnienia łatwego dostępu i większej kontroli.

Dochodzimy tu do głównego uzasadnienia backupu, jakim jest odzyskiwanie danych. Rozwiązanie umożliwiające tworzenie kopii zapasowych pakietu Office 365 chroni dane przed utratą, ale na niewiele się przyda, jeśli odzyskiwalność danych będą ograniczać takie czynniki jak niska przepustowość, łączność czy granularność, nieudane operacje backupu bądź brak możliwości odzyskania danych do innej lokalizacji lub w innym formacie. Administratorzy IT odpowiedzialni za ochronę danych — w szczególności danych pakietu Office 365 — często stają przed całym zbiorem wyzwań, gdy pojawia się potrzeba odzyskania konkretnych danych z ogromnego repozytorium kopii zapasowych lub całych zestawów danych Office 365 po ataku ransomware. Jednak obowiązki administratora mogą także obejmować tak prozaiczne czynności jak odzyskiwanie użytkownikom pojedynczych e-maili lub plików. Właściwe narzędzia do szybkiego i efektywnego wykonywania tych czynności pozwalają zaoszczędzić cenny czas, który administrator może przeznaczyć na ważniejsze zadania biznesowe. Zasadniczo każdej strategii backupu pakietu Office 365 powinna odpowiadać strategia odzyskiwania, uwzględniająca mniej i bardziej poważne czynniki ryzyka utraty danych, zapewniająca możliwość odzyskiwania granularnego i kierowanego oraz obejmująca schemat testowania, który ewoluuje odpowiednio do zmian wprowadzanych w infrastrukturze, na platformie lub w wymaganych wartościach RTO i RPO.

Office 365 — archiwizacja, nadzór i operacje eDiscovery

Mimo pewnych podobieństw kopie zapasowe oraz archiwa różnią się od siebie i powinny być używane w różnych celach. W przypadku pakietu Office 365 dzięki mechanizmom archiwizacji danych SaaS można przenosić starsze, rzadziej używane dane do osobnej warstwy i tam nimi zarządzać. Wprawdzie tego rodzaju archiwizacja umożliwia konfigurowanie przepływów pracy opartych na regułach i wygodne zwiększenie pojemności pamięci masowej online na potrzeby pakietu Office 365, jednak nie zastąpi ona regularnego tworzenia kopii zapasowych. I chociaż dane przechowywane w tych archiwach raczej nie zmieniają się szybko, również im trzeba zapewnić ochronę przy użyciu strategii backupu 3-2-1.

Najnowszym zagrożeniem dla danych SaaS są wyzwania wynikające z przepisów o ochronie prywatności, takich jak RODO oraz ustawa California Consumer Privacy Act z 2018 r., która ma wejść w życie w 2020 r. Obowiązujące od 2018 r. RODO dotyczy przetwarzania danych osobowych pozyskanych w ramach dowolnej działalności gospodarczej na terenie UE, niezależnie od tego, czy przetwarzanie odbywa się na obszarze UE, czy poza nim. Rozporządzenie daje osobom mieszkającym w Unii większą kontrolę nad danymi. Indywidualne prawa obejmują możliwość zakazania przetwarzania danych w sposób wykraczający poza cel określony podczas ich pozyskania, prawo do bycia zapomnianym oraz możliwość cofnięcia zgody na zbieranie i wykorzystywanie danych osobowych.

Może to prowadzić do poważnych problemów, zwłaszcza gdy weźmie się pod uwagę ogromną ilość starszych danych zgromadzonych w całej branży. Konieczność zapewnienia odpowiedniej ochrony wszystkich tych e-maili, dokumentów i witryn oraz zarządzania nimi może przyprawić o ból głowy, ale jeśli chodzi o perspektywę biznesową, to w przypadku naruszenia przepisów ryzyko wynikające z *niezarządzania* danymi osobowymi może się okazać znacznie bardziej kosztowne niż rozwiązanie tego problemu. W RODO za naruszenie jego przepisów przewidziano kary finansowe sięgające 20 mln EUR lub 4% rocznych przychodów firmy, w zależności od tego, która z tych kwot jest wyższa. W USA w przyjętej w 2018 r. ustawie California Consumer Protection Act (CCPA) wprowadzono nieco inny model, zgodnie z którym każde naruszenie ustawy skutkuje karą finansową w wysokości 7500 USD. W praktyce oznacza to, że na przykład naruszenie CCPA dotyczące 500 000 kont może kosztować 3,75 mld USD.

Kolejną kwestią prawną stymulującą ochronę danych SaaS jest proces elektronicznego wyszukiwania informacji (eDiscovery), które firmy muszą przeprowadzać w ramach postępowań sądowych. Kiedy firma otrzymuje sądowe wezwanie do okazania danych biznesowych, dane te nagle stają się materiałem dowodowym, co wszystko zmienia. W zależności od zakresu wezwania firma musi następnie zidentyfikować, zachować, zebrać i przetworzyć te dane w celu ich przekazania zespołowi prawnemu, który z kolei analizuje ich zawartość i kontekst pod kątem treści wezwania, wyłącza dane poufne oraz przygotowuje komplet danych do przedłożenia sądowi. Tak zwany prawny obowiązek przechowywania dokumentów to proces polegający na zablokowaniu danych, tak aby nie zostały one usunięte ani zmodyfikowane podczas powyższych czynności. Aby mu sprostać, firma powinna mieć narzędzia niezbędne do zapewnienia odpowiednio drobiazgowej ochrony w trakcie przeszukiwania informacji w postaci elektronicznej (eDiscovery). Jednak z prawnego obowiązku przechowywania dokumentów należy korzystać selektywnie i chociaż pakiet Office 365 udostępnia szerokie możliwości w tym zakresie, pełna i niezależna kopia zapasowa danych SaaS może być optymalnym rozwiązaniem, jeśli chodzi o wyodrębnienie zestawu danych z określonego momentu do celów operacji eDiscovery. Niestety przepisy dotyczące materiału dowodowego mogą się znacznie różnić w zależności od jurysdykcji, więc przed udzieleniem odpowiedzi na sądowe wezwanie do przedstawienia dowodów w postaci cyfrowej firma powinna zawsze zwrócić się do doradcy prawnego, a następnie ściśle przestrzegać jego wskazań.

Niezależnie od tego, czy chodzi o względy prawne, czy inne przyczyny, uważamy, że firmom coraz bardziej będzie potrzebny lepszy wgląd i większa kontrola nad danymi przechowywanymi w chmurze i na platformach SaaS. Pakiet Office 365 oferuje klientom biznesowym połączenie wygody i elastyczności, a w sytuacji, gdy przechowywanie danych Office 365 w modelu SaaS staje się coraz popularniejsze wśród przedsiębiorstw, warto uzupełnić te atuty o odpowiednie rozwiązanie do ochrony danych. Zgodnie z autentycznym podejściem opartym na chmurze hybrydowej firma powinna traktować usługi i zasoby w chmurze publicznej jako rozszerzenie infrastruktury lokalnej oraz pamiętać, że sam fakt działania określonej aplikacji w chmurze nie unieważnia fundamentalnych zasad dotyczących ochrony danych, ciągłości działania i odzyskiwania po awarii.

Wnioski i zalecenia

Jeśli chodzi o takie aplikacje jak pakiet Office 365, dostawcy SaaS oferują przekonujące gwarancje dotyczące ochrony bazowej infrastruktury zgodnie z ustalonymi parametrami SLA, jednak ta ochrona nie obejmuje danych klientów tworzonych na tych platformach. Klienci muszą sami znaleźć rozwiązania, które uchronią ich dane przed zagrożeniami — na ich własnych warunkach, a nie w ramach ewentualnych ograniczeń narzucanych przez platformę SaaS. Z perspektywy działów IT wyzwanie polega na tym, aby zrozumieć zagrożenia związane z przechowywaniem danych na platformach SaaS oraz wdrożyć właściwe rozwiązania zapewniające ochronę, kontrolę i łatwy dostęp. Poniżej przedstawiono kilka ważnych kroków, które należy wykonać podczas rozważania ochrony danych pakietu Office 365.

- **Przyjąć do wiadomości, że w odniesieniu do pakietu Office 365 firma Microsoft zapewnia dostępność aplikacji i odporność infrastruktury na czynniki zewnętrzne, ale dane wciąż należą do klienta.** To klient odpowiada za ochronę swoich danych biznesowych i powinien określić model ich ochrony odpowiadający specyficznym potrzebom swojej firmy.
- **Rozważyć zakup niezależnego rozwiązania do backupu danych i ocenić dostępne produkty.** Jest to jeden z najlepszych sposobów na zabezpieczenie firmy przed ryzykiem utraty danych związanym z pakietem Office 365. Właściwe rozwiązanie zapewni ochronę przed takimi zagrożeniami jak przypadkowe usunięcie danych oraz wewnętrzne i zewnętrzne zagrożenia bezpieczeństwa oraz pozwoli spełnić wymogi prawne.
- **Określić i przetestować parametry SLA dotyczące odzyskiwania danych z udziałem interesariuszy ze sfery biznesowej (i działu IT).** Należy przetestować różne scenariusze odzyskiwania danych przy użyciu macierzystych narzędzi dostępnych na platformie SaaS i porównać je z wynikami uzyskanymi w przypadku produktów do backupu innych firm.
- **Dokładnie poznać regulacje i przepisy obowiązujące w danym otoczeniu biznesowym**. Przepisy dotyczące ochrony i bezpieczeństwa danych nieustannie się zmieniają, dlatego jednym z głównych celów wdrożenia planu ochrony danych powinno być zapewnienie zgodności z obowiązującymi przepisami.

Informacje o firmie 451 Research

451 Research to czołowa firma specjalizująca się w badaniach i doradztwie z zakresu technologii informatycznych. Koncentrując się na innowacjach technicznych oraz przełomowych wydarzeniach i procesach rynkowych, zapewniamy wartościową wiedzę liderom gospodarki cyfrowej. Ponad 100 analityków i konsultantów dostarcza tę wiedzę za pośrednictwem badań własnych, usług doradczych i wydarzeń na żywo, a grono odbiorców obejmuje ponad 1000 przedsiębiorstw z Ameryki Północnej, Europy i innych części świata. Firma 451 Research powstała w 2000 r. Ma siedzibę w Nowym Jorku i należy do 451 Group.

NOWY JORK
1411 Broadway
New York, NY 10018, USA
+1 212 505 3030

SAN FRANCISCO
140 Geary Street
San Francisco, CA 94108, USA
+1 415 989 1555

LONDYN
Paxton House
30, Artillery Lane
London, E1 7LS, Wielka Brytania
+44 (0) 203 929 5700

BOSTON
75-101 Federal Street
Boston, MA 02110, USA
+1 617 598 7200

451 Research®