Informatyka. Projekty. Rozwiązania.

Backup danych – dobra praktyka czy upierdliwy obowiązek?

Co zrobić z uciążliwym backupem?

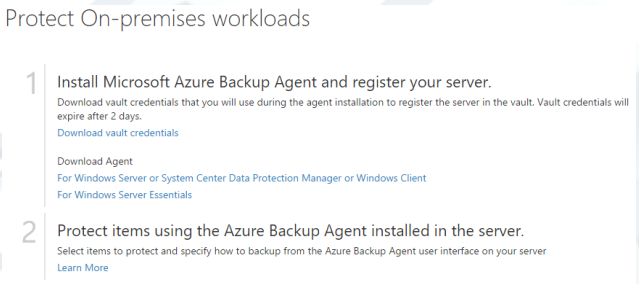
Czasami wymogi prawne, czasami zasady działania macierzystej grupy czy korporacji, a czasami po prostu zdrowy rozsądek skłaniają mniejsze i większe organizacje do przechowywania kopii wybranych danych poza własną siedzibą. Choć jest to „dobra praktyka", to wiele organizacji, porównując prawdopodobieństwo wystąpienia takiego przypadku z kosztami przechowywania danych na zewnątrz firmy, nie podejmuje działań zmierzających do wdrożenia takiego rozwiązania.

Popularne tasiemki, pomimo ciągle najlepszego stosunku ceny nośnika do jego pojemności, wymagają specjalistów, drogich urządzeń i odpowiedniego oprogramowania. I tak najsłabszym ogniwem systemu backupu jest człowiek, gdyż nie działa automatycznie.

Jak w pełni zautomatyzować bezpieczeństwo danych w zewnętrznym repozytorium?

Istniejąca obecnie infrastruktura sieciowa i przepustowość łączy internetowych oraz technologia backup-u, wykorzystująca ciągłe kopie przyrostowe i tylko jedną pierwotną kopię pełną, umożliwiają wykonywanie kopii zapasowych najważniejszych danych i przesyłanie ich do repozytorium w chmurze.

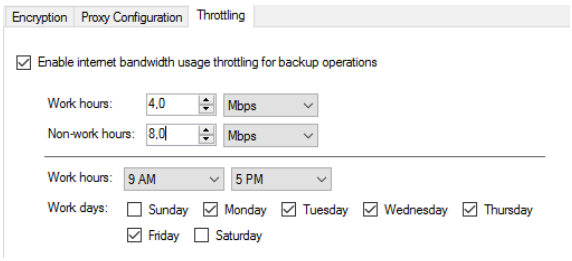
Stosunkowo niedawno na rynku tego typu usług pojawiła się firma Microsoft wraz z mającą wiele funkcjonalności chmurą Azure.



Jedną z tych funkcjonalności jest usługa o nazwie Azure Backup. Pod tą prostą nazwą i bardzo przyjazną nawet dla nie-informatyków konfiguracją, polegającą na wykonaniu kilku kroków – które zajmują, począwszy od

RavNet Sp. z o.o.
www.ravnet.pl
e-mail: biuro@ravnet.pl

rejestracji w Azure, a skończywszy na uruchomieniu zadania pierwszej kopii dosłownie kilkanaście minut–, kryje się bardzo rzetelne i użyteczne narzędzie pozwalające na zabezpieczaniu wybranych danych zarówno z serwera, jak i końcówek.



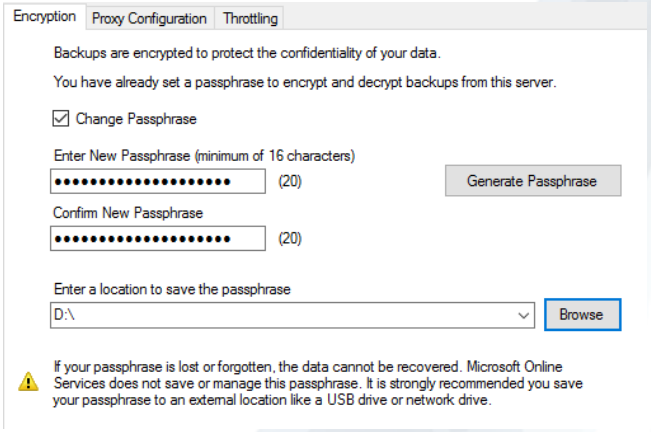
Jakie są koszty tej usługi?

W każdej firmie można wytypować pewną pulę newralgicznych danych, które będą podstawą do przywrócenia jej funkcjonowania w przypadku sytuacji kryzysowej. Dane takie to zazwyczaj tylko część wszystkich przechowywanych na serwerach plików, baz czy ich dodatkowych kopii – szczególnie w małej lub średniej firmie. Na przykład, koszt zapełnionej przestrzeni o rozmiarze 512 GB przy 1 źródle to tylko 27,23 € miesięcznie, przy czym jest to szacowana cena maksymalna. Przeważnie cała przewidywana przez nas przestrzeń nie jest zajmowana od razu, a Azure kieruje się zasadą, że klient płaci tylko za wykorzystane zasoby, więc opłata – przynajmniej w początkowym okresie – zazwyczaj będzie niższa. Podana cena obejmuje również koszt *agenta*, który odpowiada za autentykację, szyfrowanie i wykonywanie zadania kopii wskazanych danych. Zakup usługi można zrealizować np. poprzez zakup tzw. tokenów w ramach licencji grupowej Open (1 token=około 85 Euro). Wykorzystanie tych środków nie zależy od czasookresu lecz utylizacji przestrzeni w miesiącu rozrachunkowym. Praktyka wskazuje, że zabezpieczone za pomocą 1 tokena dane z laptopów handlowców są chronione przez kilka miesięcy.

Najczęstsze wątpliwości.

Przenoszenie danych do chmury może nasuwać wątpliwości związane z przepustowością łącza internetowego czy też bezpieczeństwem informacji, które należy wziąć pod uwagę.

Pierwsza wątpliwość dotyczy pierwszego pełnego backupu, który ma zazwyczaj duże rozmiary w porównaniu z przepustowością typowych łączy internetowych. Druga wątpliwość to dostępność łącza w trakcie wykonywania kopii zapasowej. Rozwiązaniem jest *throttling*, czyli możliwość ograniczenia pasma wykorzystywanego na backup zależnie od pory doby, co zapewnia odpowiednio



długi czas na wykonanie pierwszej kopii, nawet w godzinach pracy organizacji. Kolejne kopie przyrostowe są już małe i potrzeba znacznie mniej czasu na ich tworzenie. Jeżeli jednak pierwotny backup jest zbyt duży, istnieje możliwość dostarczenia go do Datacenter Microsoft za pośrednictwem wyspecjalizowanego przewoźnika w odpowiednio przygotowanej przy pomocy agenta formie. Trzecia wątpliwość to zapewnienie poufności, dlatego przesyłane i przechowywane w Azure dane są szyfrowane silnym kluczem, którego fraza generująca jest przechowywana tylko po stronie klienta, co uniemożliwia dostęp do zawartości danych administratorom Microsoft-u oraz niweluje potencjalne zagrożenia na całej drodze przesyłania danych. Poza tymi najważniejszymi funkcjami sam agent pozwala na bardzo elastyczne ustawienia retencji kopii zapasowych, począwszy od dni, a skończywszy na latach. Kopia może być synchronizowana do trzech razy dziennie, a jeżeli zaistnieje taka potrzeba, może zostać włączona replikacja do zapasowego Datacenter

Microsoft, co pozwala na jej zabezpieczenie geograficzne.

Jako administrator z wieloletnim doświadczeniem mogę powiedzieć, że otrzymałem nowe narzędzie, które niewielkim nakładem kosztów (kilkanaście euro miesięcznie) pozwala dodatkowo podnieść jakość zabezpieczenia newralgicznych danych, a w niektórych przypadkach może stać się głównym sposobem ich zabezpieczania.

Patryk Prymowicz
Dyrektor ds. wdrożeń w firmie RavNet. Problemem backup-ów i bezpieczeństwa baz danych zajmuje się od ponad 15 lat.
patryk.prymowicz@ravnet.pl