

Kopie bezpieczeństwa – o czym warto pamiętać?

W poniższym artykule skupiamy swoją uwagę na bezpieczeństwie danych w firmach. Publikacja wyjaśnia po krótku czym są kopie bezpieczeństwa i dlaczego należy je wykonywać, a także jak zaplanować wdrożenie i zarządzanie systemem, by przyniósł on zamierzone efekty. Artykuł wskazuje nowe technologie, które wypierają te starsze, oraz przedstawia problem organizacji backup w kwestii procedur. Całość stanowi świetny wstęp do weryfikacji posiadanego systemu backup'owego lub zaplanowania go od nowa.

Nikomiu nie trzeba tłumaczyć jak ważny w obecnych czasach jest szybki dostęp do aktualnych danych w prężnie działającym przedsiębiorstwie. W dobie Internetu i aplikacji webowych awaria serwera udostępniającego dane tysiącom klientów bądź komputera dyrektora finansowego, który jako jedyny w firmie może wysłać przelew tysięcy Euro, może spowodować wielkie straty dla przedsiębiorstwa. Oczywiście jeżeli chodzi o serwery, w szczególności te korporacyjne służące tysiącom osób, zwykle konfigurowane są w klastry, przełączając z uszkodzonego na sprawny w razie awarii jednego z nich.

Inaczej zwykle wygląda jednak sytuacja w sektorze SMB, gdzie oszczędności finansowe nie pozwalają na zaawansowane rozwiązania. W każdym jednak wypadku szybki dostęp do kopii bezpieczeństwa plików, bazy danych bądź świeżej kopii obrazu całego serwera oraz opracowane i sprawdzone procedury ich odzyskiwania, warte są znaczących inwestycji w każdej firmie, która dba o jakość swojej infrastruktury IT oraz wiarygodność wobec klientów.

CZYM JEST KOPIA BEZPIECZEŃSTWA?



Kopia bezpieczeństwa – to zautomatyzowany proces zabezpieczenia danych poprzez ich kopiowanie, celem późniejszego odtworzenia (odzyskania) w przypadku ich uszkodzenia lub utraty.

Często z pojęciem kopii bezpieczeństwa używa się zamiennie terminu archiwizacja, co jednak nie jest jednoznaczne, gdyż archiwizacja, to proces długotrwałego przechowywania różnych danych, np. księgowych, finansowych.

Jakie są przyczyny uszkodzeń i/lub utraty danych?

Jest ich wiele, różnią się często w zależności od rodzaju nośnika, można je jednak uogólnić:

- czynnik ludzki – główny powód, który stoi za utratą danych; może to być błąd administratora, działanie użytkownika, bądź osoby niepowołanej, działanie zwykle niezamierzone,
- nieprawidłowe warunki pracy, niezgodne z zaleceniami producentów sprzętu (nieprawidłowa wilgotność, temperatura, obciążenie pracy, złe ustawienie),
- szkodliwa działalność oprogramowania – wirusy, trojany, włamania do komputerów,

- zbyt duże oszczędności finansowe prowadzące do stosowania do celów produkcyjnych sprzętu i oprogramowania przeznaczonego przez producentów do zastosowań domowych, bądź stosowanie rozwiązań przestarzałych, zużytych,
- awarie zasilania – nieprawidłowe zabezpieczenia sprzętu przed zanikiem napięcia i jego jakością,
- katastrofy naturalne,
- kradzieże.

Każda utrata danych powoduje powstanie skutków, które mają bezpośrednie przełożenie na działanie przedsiębiorstwa. Konsekwencji takich może być wiele, obejmują one m.in. :

- brak dostępu klientów do usług świadczonych przez firmę powoduje utratę jej wiarygodności, co pociąga za sobą wymierne skutki finansowe,
- reorganizacja pracy – utrudnienia w funkcjonowaniu przedsiębiorstwa,
- utrata kontaktów biznesowych,
- trudności w rozliczaniu się firmy z bieżących zobowiązań,
- problemy z odzyskaniem licencji oprogramowania, w szczególności jeżeli było to oprogramowanie OEM,
- konsekwencje osobowe.

Mimo wprowadzenia systemu kopii bezpieczeństwa w firmie, nagminnie zdarza się, że jest on wdrażany przez osoby niemające odpowiedniej wiedzy na jego temat, bez dobrego planu i wcześniejszego projektu. Sam zakup odpowiedniego systemu jest najważniejszą decyzją, która warunkuje następne zdarzenia związane z możliwością przywrócenia pełnej sprawności firmie po awarii.

Zakup oprogramowania należy uwzględnić w procesie planowania całego systemu backupu i jego projektowania. Większość specjalistów IT ma już w tej dziedzinie pewne doświadczenie i sprawdzone w praktyce, ulubione produkty i producentów sprzętu oraz oprogramowania do backupu. Problem jednak w tym, że wraz ze zmianami, które następują w przedsiębiorstwie nie zawsze zachodzą zmiany niezbędne w systemie kopii bezpieczeństwa – dokupienie dodatkowych licencji, dysków do serwera plików i inne. Wszystko to należy przewidzieć już na etapie planowania zakupu i dostępnego budżetu, projektowania systemu, tworzenia procedur kopii bezpieczeństwa oraz zawrzeć w dokumencie SLA (Service Level Agreement). Zakupiony pakiet sprzętowo-programowy musi zakładać rozwój firmy i umożliwiać łatwą rozbudowę, by nie trzeba było „łatać” go kolejnymi drogimi, specjalistycznymi rozwiązaniami innych producentów, najczęściej niezgodnymi ze sobą. Co raz częściej jednak widać otwartość na popularne na rynku rozwiązania i wynikowe formaty plików backupu, co umożliwia bardziej elastyczne zarządzanie posiadanymi już kopiami w różnych formatach, np. obrazy .vmc, .pvs, .sv2, .spf, .tib., można przekonwertować do formatu .vmx w aplikacji VMWareConverter.

Wybór właściwego sprzętu i oprogramowania przeznaczonego do tworzenia kopii bezpieczeństwa powinien wynikać z wcześniejszej wnikliwej analizy przedsiębiorstwa: posiadanej przez niego infrastruktury, używanych aplikacji, krytycznych usług i punktów działania firmy, założonego budżetu inwestycyjnego. Zbyt często firmy nie mając świadomości własnych wymagań i możliwości zawierają „fachowym” poradom sprzedawców wychwalających swoje produkty jako remedium na wszystkie bolączki przedsiębiorstwa, co kończy się na pierwszej próbie dostosowania tego „uniwersalnego” rozwiązania do swoich potrzeb.

Zakupiony software i hardware zwykle stanowią początek wdrożenia systemu backupu w firmie. Sam zakup nie oznacza jeszcze rozwiązania problemu posiadania przez firmę rzetelnych kopii bezpieczeństwa najważniejszych danych.

W związku z tym warto wspomnieć o najczęstszych błędach przy projektowaniu systemu backupu, do których należą m.in.:

- minimalizm, zbytnia oszczędność osób odpowiedzialnych za inwestycje w firmie – co skutkuje niedopasowaniem systemu do rzeczywistych potrzeb firmy, najczęściej spowodowane brakiem jasnego określenia wymogów firmy co do jakości, zawartości, dostępu, retencji, RTO/RPO (ang. Recovery Time Objective/Recovery Point Objective) kopii bezpieczeństwa,
- brak planowania skalowalności systemu – bardzo szybko może okazać się, że zaprojektowany system jest niewystarczający, np. za wolny - kopia nie nadąża wykonać się w okienku backupowym (BW-Backup Window), nośniki mają za małą pojemność (np. taśma DAT, LTO) i trzeba je zbyt często wymieniać, np. kilka razy dziennie, nie ma możliwości dołączenia dodatkowych elementów, czy nośników danych, np. kontrolerów, dysków,
- zły dobór medium transmisyjnego LAN/SAN/iSCSI i innych w odniesieniu do infrastruktury przedsiębiorstwa,
- nachodzenie na siebie zaplanowanych zadań (jobów) backupu blokujących wykonanie kolejnych,
- brak zarządzania cyklem życia taśm i innych nośników kopii bezpieczeństwa, co prowadzi do ich nagłego, nieprzewidzianego zużycia i braku nośników zastępczych,
- niezapewnienie redundancji w rozwiązaniu backup'u, zarówno sprzętowego jak i programowego serwerów, urządzeń sieciowych, zasilających, łącza internetowego,
- brak planu działania awaryjnego, w razie uszkodzenia sprzętu, utraty danych.

STARE I NOWE TECHNOLOGIE BACKUP'U



Gdy przedsiębiorstwo ma już wdrożony i sprawdzony system kopii bezpieczeństwa zwykle trwa przy nim bez wglądu na zmieniające się możliwości i nowe technologie. Przeważnie wynika to z dużych inwestycji poniesionych na zakup i wdrożenie systemu. Gdy wszystko działa dobrze, trudno przekonać zarządzających finansami o możliwości czy konieczności zmian. Prędzej czy później te zmiany są jednak konieczne. W większości przypadków firma nie stoi w miejscu i rozwija się. Pojawiają się nowe systemy operacyjne, ilość danych ciągle rośnie, a sprzęt starzeje się.

W dobie wirtualizacji taśma może nie zdawać już egzaminu, a szybkość odzyskiwania plików ma duże znaczenie. Dobrze więc trzymać rękę na pulsie i prześledzić nowe rozwiązania w dziedzinie kopii zapasowych, tym bardziej, że mogą przyczynić się do sprawniejszego działania firmy i oszczędności finansowych. Mając na myśli nowe technologie przedstawione zostaną dwa rozwiązania rzadko stosowane w sektorze SMB, a z racji ich coraz mniejszych kosztów oraz nowych funkcjonalności stają się konkurencyjne dla odchodzących po woli do lamusa ich poprzedników.

Backup online (w chmurze) – dzięki znacznemu przyspieszeniu i niższej cenie łącz internetowych, jest obecnie bardzo ciekawą propozycją do rozważenia. Oferowany przez firmy zewnętrzne najczęściej w formie SaaS – Software as a Service – oprogramowanie jako usługa, gdzie aplikacja jest przechowywana i udostępniana przez producenta użytkownikom poprzez Internet .

Głównymi atutami wykonywania kopii online, są:

- brak konieczności ponoszenia dużych wydatków na zakup sprzętu,
- projektowania systemu kopii zapasowych,
- możliwość backupu zdalnych lokacji i urządzeń mobilnych bez konieczności skomplikowanej konfiguracji,
- wysoki poziom bezpieczeństwa danych.

Przechowywaniem i ochroną skopiowanych już plików zajmuje się centrum danych, znajdujące się zwykle w dobrze zabezpieczonym budynku, wyposażonym w instalacje chroniące przed pożarem, brakiem napięcia czy nawet katastrofami naturalnymi. Właściciel danych, płacąc abonament, nie martwi się o ich bezpieczeństwo oraz nie musi ponosić nakładów na sprzęt czy specjalistów odpowiedzialnych za kopie bezpieczeństwa.

Cena tej stosunkowo nowej formy backupu jest bardzo konkurencyjna biorąc pod uwagę brak konieczności ponoszenia dodatkowych inwestycji (zakładając, że łącze internetowe nie wymaga zwiększenia przepustowości). Na rynku dostępnych jest wiele firm oferujących usługi kopii bezpieczeństwa online. Duża część z nich zachęca do korzystania z ich usług poprzez oferowanie bezpłatnego konta do backupu stosunkowo małej ilości danych 1-5 GB.

Przykładowe firmy oferujące kopie bezpieczeństwa online i ceny:

- IDrive – pojemność: 500GB, opłata miesięczna: 50\$, roczna: 500\$,
pojemność: 1000GB, opłata miesięczna: 80\$, roczna: 800\$
- FSecure – pojemność – bez limitu dla jednego komputera, opłata roczna: 190,55 zł

Backup online nie jest jednak dla każdego. Przy dużych ilościach danych (powyżej kilkuset GB), żadne łącze internetowe nie może zapewnić koniecznej przepustowości, toteż w korporacjach używa się zwykle systemów mieszanych, korzystających np. z zainstalowanych na zdalnych komputerach użytkowników programowych agentów, przesyłających po sieci LAN/WAN dane do serwera centralnego, który posiada już stacjonarny system backupu – np. serwer plików, bibliotekę taśmową.

Virtual Tape Library (VTL) – zintegrowane rozwiązania sprzętowo-programowe koncentrujące się na wykonywaniu kopii bezpieczeństwa. Zawarte najnowocześniejsze techniki kompresji/dekompresji wraz z wysokiej wydajności sprzętem, obsługującym dopiero wchodzące na rynek technologie 8Gb światłowodu i 10Gb sieci Ethernet – iSCSI pozwalają na wykonywanie kopii znacznie większej ilości danych w krótszym czasie niż dotychczas. Nazwa „wirtualny napęd taśmowy” nie jest pomyłką. Mimo, że nośnikiem zapisu jest tu dysk twardy, to przykładowy VTL emuluje ponad 50 bibliotek taśmowych i 30 typów taśm. Jest to o tyle ważne, że pozwala zintegrować obecny system kopii bezpieczeństwa korzystający ze streamerów i bibliotek taśmowych z nowym – opartym na macierzy dyskowej. Ponadto możliwe jest bezbolesne przejście z korzystania z taśm magnetycznych na przechowywanie plików na dyskach.

Wielkość macierzy dostępna dla plików waha się w zależności od rynku, na jaki dane urządzenie jest kierowane. W chwili obecnej są to wartości od kilku TB do 1 PB. Wydajność to 1.6 GB/s, ponad 5.8 TB/h dla 1 noda. Dla porównania - prędkości zapisu najnowszej taśmy LTO5

wynosi 140 MB/s – 50,4 GB/h. Nie biorąc pod uwagę innych czynników (np. szybkość łącza przesyłającego pliki kopii), korzyść z wykorzystania VTL to ponad 10-krotny przyrost prędkości backupu. Natomiast minusem tego rozwiązania (w porównaniu do wcześniej przedstawionej kopii bezpieczeństwa w „chmurze”) jest głównie wysoki koszt samego urządzenia. Konieczność projektowania systemu backupu również jest wymagana, lecz głównie w przypadku, gdy wcześniej nie był stosowany inny system kopii bezpieczeństwa. Jeżeli wirtualnym napędem VTL zastępujemy napęd taśmowy, wdrożenie go powinno być zadaniem łatwym i szybkim.

W obu przedstawionych rodzajach nowoczesnych systemów kopii bezpieczeństwa używana jest technologia deduplikacji, mająca na celu ograniczenie ilości przesyłanych danych na serwer kopii bezpieczeństwa. Dotychczas stosowanymi, popularnymi metodami oszczędności czasu wykonywania kopii i zasobów na ich przechowywanie były i są kopie przyrostowe oraz wcześniejsze przygotowanie plików dużej objętości np. poprzez kompresję. Sprzęt i oprogramowanie pełniące funkcje deduplikacji, wyszukują powtarzające się ciągi danych w plikach lub blokach na dysku, zastępując duplikaty jedynie odwołaniem do jednej wersji zawierającej te same dane. W obecnych czasach, gdy ilość danych koniecznych do zabezpieczenia zwiększa się w tempie wykładniczym a okienka backupu (okres czasu w jakim możemy wykonać zadanie backupu) pozostają takie same lub zmniejszają się, deduplikacja może być zbawienna. Pozwala zaoszczędzić od kilku do nawet dziewięćdziesięciu procent miejsca i czasu transferu w zależności od użytej formy deduplikacji, nośnika zapisu i przesyłu danych.

O CZYM NIE PAMIĘTAMY – OLA, SLA, RPO, RTO?

W polskich firmach niezbyt popularne są dokumenty dotyczące procedur związanych z IT, czy też ogólnie rzecz biorąc same procedury. Niestety często można spotkać nieprzykładających należytej uwagi do kwestii kopii bezpieczeństwa prezesów nawet dużych firm oraz informatyków zakładających bezawaryjność i pewność wdrożonego przez siebie rozwiązania.

Procedury są wykorzystywane w codziennym działaniu większości korporacji, jednak nie tylko one je stosują. Są także wyjątki i w dużych strukturach, gdzie problematyczne może okazać się odzyskanie pojedynczych plików z komputera jednego z tysięcy użytkowników, chociażby dlatego, że straty te mogą być wliczone w koszty działalności jako mniejsze od zakupu maksymalnie wydajnego systemu kopii bezpieczeństwa wszystkich danych przedsiębiorstwa.

Spisane instrukcje, których powinny się trzymać osoby odpowiedzialne za dany dział IT, konkretne działania, terminy i czasy poszczególnych czynności rutynowych i podejmowanych w razie awarii zawarte są w dokumencie OLA (Operation Level Agreement). Stanowi on listę funkcji i czynności, za jakie odpowiedzialne są konkretne osoby wraz z określonym czasem trwania poszczególnych etapów realizacji zadań, np. osoba odpowiedzialna za wymianę nośnika kopii zapasowej, czas trwania odzyskania plików i dział/osoba odpowiedzialna za tę czynność, przywrócenie funkcjonowania bazy danych, wznowienia działania aplikacji przez odpowiednie osoby czy działy, itd.

Umowa między działem IT lub firmą outsourcingową a zarządem firmy dotycząca czasu reakcji na awarię poszczególnych składowych systemu IT w firmie to SLA (Service Level Agreement), np. po awarii sprzętowej serwerów, muszą one zacząć działać ponownie w ciągu 5 godzin, bądź w tym samym czasie powinna być zapewniona ich funkcjonalność na sprzęcie zastępczym.

Zarówno jeden jak i drugi dokument wymaga dokładnego opracowania i rzetelnego stosowania. Umożliwiają one łatwy audyt jakości pracy danego działu oraz funkcji IT w przedsiębiorstwie, wyciągnięcie konsekwencji i wniosków oraz korekty samych procedur.

Z dokumentami tymi ściśle związane są pojęcia RPO/RTO:

RPO – Recovery Point Objective – określa do którego punktu w przeszłości będziemy odzyskiwać kopię bezpieczeństwa. Wskazuje częstotliwość kopiowania danych czyli czas co jaki firma jest w stanie poświęcić dane, by wrócić do działającej kopii, np. czas 15 minut oznacza, że co 15 minut musimy robić kolejną kopię, by stracić jedynie 15 minut pracy w razie awarii.

RTO – Recovery Time Objective – oznacza maksymalny czas na odzyskanie poprawnych, działających danych.

Określenie RTO wraz z RPO i zawarcie ich w dokumencie operacyjnym OLA jak i przełożenie ich na język umowy serwisowej SLA zapewnia przedsiębiorstwu solidne podstawy zapewnienia należytej ochrony posiadanych danych.

Posiadając już opracowane procedury i dokumenty OLA i SLA, kolejnym etapem jest przestrzeganie zawartych w nich uzgodnień, terminów oraz rutyn i nadzór nad prawidłowym ich wykonywaniem. Dobrze, gdy zostanie powołany do tego odpowiedzialny zespół, gdyż nic nie jest w stanie zastąpić dobrej kopii bezpieczeństwa.

Przedstawione po krótkce zagadnienia związane z kopiami bezpieczeństwa miały na celu uzmysłowienie czytelnikom zachodzących zmian na rynku oraz popełnianych przez menedżerów błędów, z którymi autor tego artykułu zetknął się podczas pracy zawodowej w środowisku polskich i europejskich firm różnej wielkości. Niezależnie od skali przedsięwzięcia natknąć się można na niefrasobliwość specjalistów oraz oszczędności firm co do inwestycji w sprzęt a także zasoby ludzkie.

W polskim sektorze SMB zauważona została niska świadomość zagadnienia kopii bezpieczeństwa i ich dużej roli w przedsiębiorstwie, często bagatelizowanie tego tematu oraz małe nakłady, a właściwie oszczędności na infrastrukturze IT.

Zwrócono uwagę na interesujące formy wykonywania kopii bezpieczeństwa – online - w chmurze i wirtualny napęd taśmowy (VTL), jako następcę popularnego streamera i serwera plików.

Artykuł opracował **Maciej Ochal**,
MCSA, Support Online Sp. z o.o.

Źródła:

1. http://pl.wikipedia.org/wiki/Software_as_a_Service
2. <http://www.falconstor.com>
3. <http://www.idrive.com>
4. http://itpedia.pl/index.php/RPO_i_RTO.



Firma **Support Online** świadczy usługi informatyczne dla firm oraz instytucji. W ramach obsługi IT oferujemy instalację, konfigurację i zarządzanie programami backup'owymi. Jeśli są Państwo zainteresowani wsparciem w tym zakresie lub innymi usługami informatycznymi – zapraszamy do kontaktu.

Support Online Sp. z o.o.
tel. + 22 335 28 00
e-mail: support@so.com.pl
www.support-online.pl