MATERIAŁ PRODUKTOWY

Rozwiązania backupu i ochrony danych

INNERGO

Rozwiązania backupu i ochrony danych

Sprawne działanie przedsiębiorstwa opiera się na łatwym dostępie do informacji z możliwością ich szybkiego przetwarzania. Wysokie tempo przyrostu danych generowanych przez firmy to również konieczność inwestycji w niezawodny system do ich ochrony. Przed podjęciem kluczowych decyzji w sprawie ochrony zbiorów danych swojej firmy, należy dowiedzieć się na czym polega taka ochrona, i jak dopasować rozwiązanie do potrzeb swojego przedsiębiorstwa.

Dlaczego należy chronić dane biznesowe?

Dynamiczny wzrost ilości informacji i powiększające się zbiory danych to ogromny potencjał dla rozwoju przedsiębiorstw. Analiza big data to identyfikacja nowych możliwości. Prowadzi do inicjowania przemyślanych i bardziej efektywnych działań biznesowych, a to przekłada się na wzrost konkurencyjności i zysków, oraz na zadowolenie klientów.

Ogromne tempo przyrostu danych wiąże się z nowymi wyzwaniami stawianymi przed firmami. Szczególną uwagę należy zwrócić na:

- wdrożenie systemu do ochrony danych, aby zapobiegać ewentualnym awariom, sytuacjom losowym, kradzieżom istotnych informacji biznesowych
- szybkość reagowania na wszelkie ewentualne zdarzenia dotyczące zbiorów danych (zniszczenie, uszkodzenie, utrata, kradzież itp.)
- umiejętność selekcji danych na te, z których aktywnie korzystamy, a także te, które już nie są aktywne, bądź zakończyliśmy ich przetwarzanie

Zarówno mniejsze, jak i większe przedsiębiorstwa coraz częściej decydują się na wdrożenie rozwiązania, które będzie chroniło firmowe bazy danych, nawet jeśli chronione informacje, czy systemy są mniej krytyczne. To podkreśla holistyczne spojrzenie na rozwój firmy, niezmiernie istotne w świecie biznesu.

Na czym polega ochrona danych, backup i archiwizacja?

Ochrona danych to pojęcie szersze od backupu danych i archiwizacji, ponieważ obejmuje dodatkowo zabezpieczanie danych, zarządzanie cyklem życia informacji, a także zapobieganie szkodliwemu oprogramowaniu, czy wirusom.

Backup polega na tworzeniu kopii zapasowych, które stanowią zabezpieczenie dla danych przetwarzanych na bieżąco. Informacje kopiowane są do wtórnego miejsca (zewnętrzne nośniki, serwery, chmura), aby w przypadku awarii lub zdarzenia zagrażającego danym biznesowym, zachować istotne dla firmy materiały.

Przedsiębiorstwa tworzą backup danych, zabezpieczając się przed wadliwym oprogramowaniem, uszkodzeniem danych, awarią sprzętu, złośliwym hackingiem, kradzieżą, błędami użytkowników lub innymi nieprzewidzianymi zdarzeniami.

Backupem możemy objąć między innymi serwery, desktopy, czy urządzenia mobilne. Dla tych wszystkich urządzeń może być tworzony backup całościowy, jak i backup częściowy dla wybranych katalogów, aplikacji, baz danych.

W przypadku całościowego backupu możemy liczyć na odtworzenie całego systemu, urządzenia lub w przypadku awarii danego sprzętu wykorzystać inny aby odzyskać dane. Częściowe kopie zapasowe zapewniają krótszy czas ich tworzenia ze względu na mniejszą ilość kopiowanych danych. Ponadto częściowe kopie zapasowe umożliwią granularne odzyskanie danych z baz danych lub aplikacji. Większość przedsiębiorstw wykorzystuje kombinację całościowych i częściowych backupów.

Archiwizacja danych to określenie często mylnie używane zamienne z terminem backup. Archiwizacja polega na przenoszeniu danych na inny nośnik lub serwer w celu ich segregacji biorąc pod uwagę ich aktualność, czy stan procesowania.

Według najlepszych praktyk backupu i archiwizacji, tworzenie kopii, bądź przenoszenie danych powinno być zawsze zaplanowane i występować co najmniej raz w tygodniu. Najlepszym terminem na takie działania są weekendy, bądź godziny po zamknięciu pracy biura, kiedy posiadane w zasobach firmy informacje nie są aktualnie przetwarzane.

Kto potrzebuje backupu i ochrony danych?

Każde przedsiębiorstwo, niezależnie od jego wielkości, posiada istotne dane biznesowe, bez których sprawne działanie firmy byłoby niemożliwe. Rozwój biznesu, wzrost konkurencyjności i wzrost zysków to wypadkowe analiz, kontaktów biznesowych i procesów sprzedażowych, czyli działań opierających się na przetwarzaniu danych przedsiębiorstwa.

Wdrożenie systemu do tworzenia backupu i ochrony danych nie powinno być uzależnione od ilości posiadanych zbiorów informacji w przedsiębiorstwie. Ochrona jest konieczna już wtedy, kiedy firma posiada małe ilości danych, ale są one krytyczne dla zachowania ciągłości procesów biznesowych.

Backup to rozwiązanie zarówno dla małych i dużych przedsiębiorstw i instytucji. Doskonale sprawdzi się np. w przedsiębiorstwach specjalizujących się w operacjach na danych, w przemyśle i zakładach produkcyjnych, w instytucjach administracji publicznej, szpitalach oraz służbie zdrowia, a także w energetyce i przedsiębiorstwach świadczących usługi komunalne.

Korzyści płynące z wdrożenia systemu backupu

Przedsiębiorstwa decydujące się na wdrożenie systemu backupu, stawiając na poprawę ochrony danych i systemów w firmie. Dzięki temu dostępność informacji znacznie wzrasta, zaś ryzyko biznesowe maleje. To pozwala na obniżenie kosztów i osiągniecie sukcesu w biznesie.

Narażenie danych na jakiekolwiek zagrożenia może spowodować ogromne straty, zakłócić działalność firmy lub nawet doprowadzić do awarii trwających procesów biznesowych.

Firmy stosują wiele narzędzi, których zadaniem jest ochrona danych. Korzyścią płynącą z backupu jest wzrost możliwości wykorzystania różnych działań do ochrony materiałów biznesowych firmy.

Inwestycja w system backupu przyczynia się znacząco do wzrostu efektywności operacyjnej firmy. Dzięki temu przedsiębiorstwa maksymalizują finansowe i niefinansowe wskaźniki stopnia realizacji swoich biznesowych celów.

5 pytań, które należy sobie zadać przed wyborem rozwiązania ochrony danych

Jak wiele i jakiego rodzaju informacje powinien obejmować backup w Twojej firmie?

Określenie ilości i rodzaju danych, wymagających kopii zapasowej to pierwszy i podstawowy krok podczas projektowania całego planu tworzenia backupu. W wyborze i selekcji danych warto korzystać z doświadczenia integratora ICT, który pomoże określić wagę danych informacji, a docelowo wybrać te, które wymagają backupu, bez konieczności kopiowania wszystkich informacji.

Ile czasu potrzeba do konfiguracji i obsługi wybranego przez Ciebie rozwiązania?

Najlepiej postawić na rozwiązanie, które będzie sprawowało kompleksową ochronę nad informacjami, a jednocześnie będzie proste w obsłudze i nie będzie pochłaniało ogromnej ilości pracy oraz czasu. Przykładem takiego rozwiązania może być oferta firmy Arcserve.

Jakiego rodzaju wsparcie będzie potrzebne?

Ogromną rolę odgrywa wybrane rozwiązanie wraz ze swoimi funkcjonalnościami, ale należy pamiętać o niezawodnej obsłudze narzędzia, która jest konieczna do prawidłowego rozwoju firmy. Innergo Systems, oferując usługę InnBACKUP, dokładnie podkreśla potrzeby, jakie wyrażają klienci. Integrator ICT przede wszystkim tworzy, przechowuje i zarządza kopiami zapasowymi. Przekazanie tych obowiązków swojemu integratorowi pozwala zaoszczędzić czas, który administratorzy IT mogą przeznaczyć na wspomaganie istotnych procesów przedsiębiorstwa. Korzystanie z usługi InnBACKUP daje pewność profesjonalnej ochrony danych i informacji koniecznych do sprawnego funkcjonowania firmy i zachowania ciągłości procesów biznesowych. Dzięki tej usłudze wszystkie usterki w systemach ICT są usuwane, co znacząco ogranicza wpływ awarii na działanie przedsiębiorstwa. Eliminacja konieczności odtwarzania konfiguracji od podstaw zwiększa efektywność kosztową firmy. Dodatkowo w ramach usługi zapewniony jest dostęp do informacji historycznych.

Jakie dane będziemy chcieli backupować w przyszłości?

Sukces firmy polega w głównej mierze na jej rozwoju. Dlatego tak, jak w przypadku każdego rozwiązania, które wdrażane jest na dłuższy czas, w przypadku systemów do ochrony danych również należy przewidzieć to, jak firma będzie funkcjonować w przyszłości, ile informacji będzie przetwarzać i jakiego rodzaju dane będą gromadzone.

Ile możemy zainwestować w system do backupu?

To pytanie jest złożone. Należy zwrócić uwagę na wartość inwestycji w ochronę danych i porównać ją z kosztami poniesionymi przy niedostatecznym zabezpieczeniu danych. Inwestowanie w rozwiązania backupu przyczynia się do wzrostu efektywności finansowej firmy, biorąc pod uwagę, jak często problemy wynikające z niezabezpieczonych danych, przekładają się bezpośrednio na późniejsze problemy przedsiębiorstwa. Przy wyborze systemu backupu warto przemyśleć, czy tańsza na pierwszy rzut oka opcja nie jest tylko na pozór tańsza, a w rzeczywistości nie zapewnia należytej ochrony informacji biznesowych i naraża firmę na dodatkowe koszty. Wybrane rozwiązanie powinno być przede wszystkim kompleksowe i odpowiadać na potrzeby danego przedsiębiorstwa.

Oferta Arcserve Unified Data Protection

Firma Arcserve stworzyła Arcserve Unified Data Protection – program zapewniający kompleksową ochronę danych w wirtualnych i fizycznych środowiskach.

Rozwiązanie to zasługuje na wyróżnienie przede wszystkim z trzech powodów:

- zunifikowana architektura nowej generacji, która w jednym narzędziu gromadzi wszystkie sposoby zabezpieczania danych;
- zarządzanie wszystkimi rozwiązaniami z poziomu jednej, łatwej w obsłudze konsoli;
- umożliwienie firmie łatwej skalowalności jej środowiska IT.

Arcserve UDP to jedno rozwiązanie, oferujące wiele działań tworzących kompleksową ochronę:

- Recovery Point Server (RPS) – serwer, który pełni funkcję backupu lub docelowej replikacji. Generuje, inwentaryzuje i usuwa nieaktualne kopie zapasowe, magazynuje zbiory danych, replikuje dane na inne urządzenia typu RPS, zarządza kopiami zapasowymi, przywraca dane, a także nadzoruje replikacje i wszelkie operacje o wysokiej dostępności.
- Globalna deduplikacja – dzięki temu procesowi, podczas tworzenia backupu przesyłane są tylko unikalne bloki danych. Pozwala to zaoszczędzić miejsce potrzebne do przechowywania backupu, skrócić czas okna backupowego jak również zoptymalizować wykorzystanie sieci.
- Zintegrowana replikacja – serwery RPS (Recovery Point Server) posiadają funkcjonalność replikowania wykonanych kopii zapasowych pomiędzy sobą. Dzięki temu możemy replikować wykonane backupy do zdalnych lokalizacji, czy do chmury.
- Instant Virtual Machines -funkcja umożliwiająca szybkie przywracanie usług przez uruchomienie maszyny wirtualnej bezpośrednio z pliku kopii zapasowej w zwykłej pamięci masowej
- Plany tworzenia kopii zapasowych – każdy plan zawiera instrukcje na temat tworzenia kopiowania zapasowych, ich replikacji, tworzenia drugorzędowych i trzeciorzędowych kopii danych (zazwyczaj poza terenem firmy), informacje dotyczące tworzenia i utrzymywania maszyn zarówno fizycznych, jak i wirtualnych, a także powiadomienia administratorów o powodzeniu lub niepowodzeniu backupu.
- Różnorodne opcje przechowywania danych – dane mogą być przechowywane na dysku lokalnym, serwerze zdalnym, serwerze NAS lub wirtualnym urządzeniu do przechowywania danych.
- Bare Metal Recovery (BMR) – mechanizm służący do odtworzenia środowiska systemowego po pełnej awarii sprzętowej serwera podczas którego dotychczasowy serwer zastępowany jest nowym. Pozwala na rozruch serwera w specjalnie przygotowanym środowisku uruchomieniowym, które wstępnie skonfigurowane samodzielnie podłączy się do systemu backupowego i umożliwi odzyskanie całości środowiska bezpośrednio z wykonywanych backupów.

Rozwiązanie proponowane przez Arcserve to kompleksowa ochrona wartościowych danych biznesowych przedsiębiorstwa z poziomu jednej, łatwej w obsłudze konsoli. Dzięki temu firma zyskuje pełną kontrolę nad działaniami prewencyjnymi, a także znacznie zmniejsza koszty związane z wdrożeniem wszystkich rozwiązań osobno.

Scenariusze wdrożeń

Przykład nr 1 – małe przedsiębiorstwo

Przedsiębiorstwo, w którym pracuje 40 osób, zlokalizowane jest w jednym mieście. Posiadają małą serwerownię, wyposażoną w sprzęt sieciowy, 3 serwery zwirtualizowane połączone w klaster Hyper-V oraz fizyczny serwer z systemem dla księgowości. Zasoby do serwerów udostępniane są z macierzy połączonej z serwerami poprzez parę przełączników SAN. W wirtualnym środowisku uruchomione jest kilkanaście systemów, wśród nich takie jak domena Active Directory, serwer plików, baza MS SQL, baza PostgreSQL.

Przedsiębiorstwo zdecydowało się na zakup appliance backupowego z zasobami computing'owymi, pozwalającymi na uruchomienie systemów bezpośrednio z backupu. Serwer fizyczny backupowany jest za pomocą agenta zainstalowanego w systemie operacyjnym, co pewien czas kopia zapasowa systemu księgowego zapisywana jest na taśmy, które z kolei przechowywane są w sejfie. Kopie zapasowe wirtualnych maszyn tworzone są bezagentowo.

Dodatkowo backupem zostały objęte desktopy, których jest 30. Globalna deduplikacja sprawia, że ograniczana jest ilość miejsca potrzebnego do przechowywania kopii zapasowych. Przesyłane są tylko unikatowe bloki danych, co skraca czas backupu desktopów oraz zmniejsza zużycie pasma sieciowego.

Appliance i oprogramowanie backupowe umożliwiają odtworzenie pojedynczych plików, odtworzenie całych baz danych lub przy użyciu alternatywnych narzędzi, pojedynczych wierszy, rekordów. Dla serwera Active Directory możliwe jest granularne odzyskiwanie obiektów oraz poszczególnych atrybutów. W przypadku awarii desktopa oprogramowanie backupowe umożliwia odzyskanie całej jego zawartości na innym sprzęcie, dzięki mechanizmowi Bare Metal Recovery (BMR). Funkcjonalność Instant Virtual Machines pozwala na uruchomienie systemu (wirtualnej maszyny lub serwera fizycznego) z backupu bezpośrednio na appliance w postaci wirtualnej maszyny. Minimalizuje to przestój systemu w przypadku awarii sprzętu, na którym został uruchomiony.

Każde przedsiębiorstwo, niezależnie od jego wielkości, posiada istotne dane biznesowe, bez których sprawne działanie firmy byłoby niemożliwe.

Wdrożenie systemu do tworzenia backupu i ochrony danych nie powinno być uzależnione od ilości posiadanych zbiorów informacji w przedsiębiorstwie.

Przykład nr 2 – duże przedsiębiorstwo

Firma posiada dwa główne oddziały oraz kilkanaście mniejszych zlokalizowanych w różnych miastach. W głównych lokalizacjach znajdują się serwerownie, w których działają systemy krytyczne dla działania firmy. Firma posiada sieć SAN, łączącą macierze i serwery. Serwery fizyczne z bazami danych Oracle i MS SQL. Sklastrowane środowisko wirtualne z wirtualnymi maszynami z systemami z rodziny Windows i Linux, na których znajdują się różne systemy między innymi poczta Exchange, domena Active Directory, strona WWW, CRM, ERP. W mniejszych lokalizacjach znajdują się po trzy serwery zwirtualizowane i pracujące w klastrze, na których działają systemy potrzebne do sprawnego funkcjonowania oddziału. Zasoby udostępniane są z macierzy podłączonej poprzez parę przełączników SAN do serwerów. Wszystkie lokalizacje połączone są poprzez VPN.

W dwóch głównych lokalizacjach wdrożono appliance backupowe, zapewniające backup środowiska serwerowo-macierzowego.

Kopia zapasowa serwerów fizycznych tworzona jest poprzez agenta zainstalowanego w serwerach, który integruje się z bazami danych, dzięki czemu backup baz danych jest konsystentny. Pozwala to na odzyskanie bazy danych z danego przedziału czasowego, odzyskanie pojedynczych plików, czy w przypadku awarii sprzętu odzyskanie całego systemu na innym serwerze, dzięki funkcjonalności Bare Metal Recovery (BMR).

Backup środowiska wirtualnego tworzony jest bezagentowo. Pozwala to na odzyskanie wirtualnej maszyny na dowolnym wirtualizatorze VMware vSphere lub Microsoft Hyper-V. Oprócz odzyskania całej wirtualnej maszyny możliwe jest odzyskanie pojedynczych plików, granularne odzyskiwanie elementów w systemie pocztowym Exchange oraz w domenie Active Directory. Dzięki integracji systemu backupowego z macierzami, backup wykonywany jest poprzez sieć SAN. Pozwala to na szybsze i efektywniejsze wykonanie kopii zapasowych.

Backup serwerów fizycznych, jak i wirtualnych maszyn tworzony jest inkrementalnie. Oznacza to, że przy wykonaniu kolejnych backupów przesyłane są tylko i wyłącznie zmiany jakie miały miejsce w danym systemie. Dodatkowo mechanizm globalnej deduplikacji dba o to, aby tylko unikalne dane zostały zapisane, dzięki czemu zapewnia oszczędność miejsca potrzebnego do przechowywania kopii zapasowych.

Appliance replikują backupy pomiędzy sobą, aby zapewnić szybkie odtworzenie danych w przypadku awarii jednej z serwerowni. Dzięki globalnej deduplikacji pomiędzy oddziałami przesyłane są tylko unikalne dane, przez co wykorzystanie pasma sieciowego jest zoptymalizowane.

W mniejszych lokalizacjach w ramach środowiska wirtualnego uruchomiona jest wirtualna maszyna z zainstalowanym oprogramowaniem do backupu. Repozytorium do przechowywania backupu znajduje się na osobnej macierzy przeznaczonej tylko i wyłącznie do tego celu. Kopie zapasowe maszyn wirtualnych tworzone są bezagentowo, a następnie replikowane do jednej z dwóch głównych lokalizacji. Mechanizm globalnej deduplikacji sprawia, że tylko unikalne bloki danych wysłane są do jednego z dwóch głównych oddziałów.

Dodatkowe dobre praktyki

chroniące dane firmy

Dbanie o rozwój firmy to oprócz stałej optymalizacji i wzrostu efektywności, świadomość istniejących zagrożeń, które mogą przerwać bezpieczną ciągłość biznesową. Taka świadomość pozwala zarówno kadrze zarządzającej, jak również pracownikom w porę przeciwdziałać niebezpieczeństwu, kierując się polityką bezpieczeństwa firmy.

Ogromne znaczenie ma również monitoring środowiska IT. Regularne oceny, planowanie działań prewencyjnych i ewaluacja wyników to ograniczenie przestojów i spowolnionej pracy sieci, poprawa efektywności finansowej, a także lepsze wykorzystanie zasobów ICT. Aby odciążyć specjalistów IT w firmie, usługę monitoringu można również outsourcować. InnMONITOR to propozycja Innergo Systems, która oprócz monitorowania infrastruktury IT, zapewnia także szybką identyfikację problemu i sugestię dalszych działań.

Stworzenie bezpiecznego miejsca pracy to wyzwanie dla pracodawców. Jeden pracownik zazwyczaj korzysta z wielu mobilnych narzędzi do pracy, jak smartfon, tablet, czy laptop. Istnieje rozwiązanie, które pozwala zarządzać wszystkimi urządzeniami mobilnymi w firmie – systemy MDM (Mobile Device Management). Dzięki nim administracja IT chroni korporacyjnych aktywów, zapobiega utracie danych przez każdego użytkownika, a także oszczędza mnóstwo czasu na konfiguracjach i aktualizacjach oprogramowania.

Ochrona danych firmowych to konieczność ze względu na ich ogromną wartość dla biznesu. Przedsiębiorstwa wprowadzają działania z zakresu ochrony danych, w tym backupu, archiwizacji i disaster recovery, aby niwelować zagrożenia i ich skutki, redukować koszty, a dzięki temu dbać o rozwój i sukces firmy.

Dane firmowe są niezwykle cenne zarówno dla efektywności operacyjnej oraz kosztowej. W związku z tym powinny być chronione przez najlepsze rozwiązania i systemy – takie, które zapewnią kompleksową ochronę i będą niezawodne w każdej sytuacji.