itomega

Kopie Zapasowe

Jak zabezpieczyć najcenniejsze zasoby firmy

Czy zabezpieczasz swoje dane?

Każda firma, która ma własną infrastrukturę informatyczną, posiada lub korzysta z serwera. Znaczna większość posiada też jakieś zasoby scentralizowane – przechowuje w jednym miejscu istotne dla organizacji dane. Najczęściej, w najprostszym wydaniu, są to pliki. Jednocześnie większość firm w niewystarczającym stopniu zabezpiecza te dane, a duża ich część nie robi tego w ogóle.

Typy serwerów

Serwer plików

Przedsiębiorstwa z reguły zaczynają swoją przygodę z serwerami od serwera plików. To jest **miejsce centralnego przechowywania danych, które są współdzielone między wszystkich użytkowników w grupie**. Użytkownicy, zamiast wymieniać się mailami z dużymi załącznikami, mają je umieszczone w katalogach na serwerze. Tam jest je nie tylko łatwiej dystrybuować i przesyłać, ale też zabezpieczać przed dostępem niepowołanych do tego osób.

Serwery z bazami danych

Z reguły, w drugim etapie, do takiego serwera plików dochodzi serwer z oprogramowaniem księgowym. W dalszej kolejności każda firma dorasta do serwera z systemem CRM, systemem ERP, zbierającym znacznie więcej danych niż zwykły system finansowo-księgowy. Ostatnim typem serwera, który często jest naturalnym następstwem rozrastania się firmy, jest serwer bazodanowy. To są bazy danych pod konkretne aplikacje, niezbędne przy oprogramowaniu typowo specjalistycznym.

Dodatkowym typem serwera, nie zawsze wykorzystywanym, ale mającym niewątpliwe zalety, jest serwer pocztowy. Często klientom poczta w hostingu po prostu przestaje wystarczać ze względu na np. poufność danych, czy potrzebę ścisłego zabezpieczenia tych danych.

Zabezpiecz dane

Przeciętna liczba serwerów w polskiej firmie to z reguły 3 maszyny, spełniające któreś z powyższych zadań. W obliczu takiego stanu rzeczy, zabezpieczenie newralgicznych danych w firmie jest wyzwaniem, które potrzebuje skutecznej i mądrej realizacji.
Jaka jest w związku z tym właściwa ochrona takich danych?

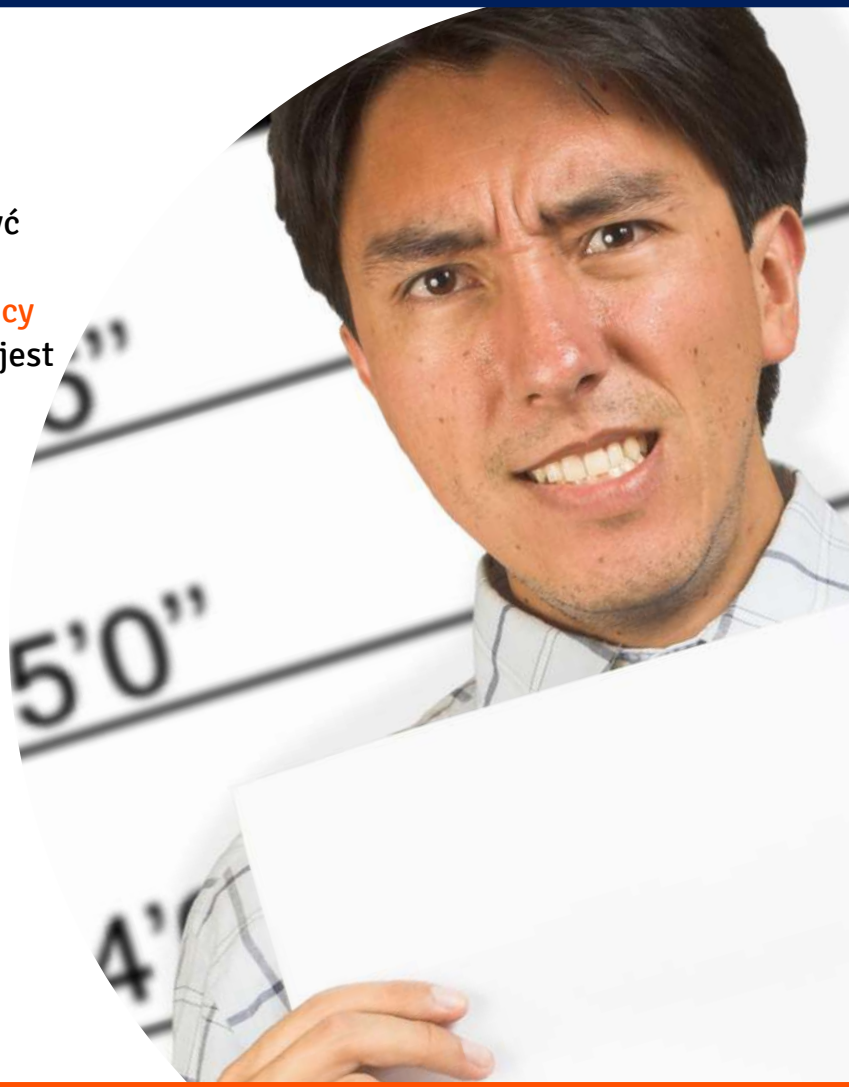
Co musisz wiedzieć

Scentralizowany system bazy danych

Wykonywanie kopii zapasowych na każdej stacji roboczej, które są w firmie może być kosztowne. Wymaga to dużo czasu, zasobów i wielu licencji na oprogramowanie. Robienie kopii zapasowych z jednego, scentralizowanego miejsca, do którego wszyscy mają bezpieczny dostęp, jest dużo tańsze i prostsze. Taką kopię zapasową wykonać jest łatwo i można to robić na bieżąco.

Zabezpieczenie przed niepowołanym dostępem

Dane, które posiada firma, to jeden z najcenniejszych posiadanych przez nią zasobów. Urządzenie, na którym się one znajdują stanowią z reguły ułamek tego kosztu – **sama „skrzynka", jaką jest serwer**, kosztująca wraz z oprogramowaniem nawet kilkanaście tysięcy złotych, mimo wszystko stanowi ułamek ceny, jaką warte są informacje na niej składowane. Dlatego właśnie to ich ochrona oraz zarządzanie dostępu do nich, **powinny być kluczowym elementem zabezpieczenia interesów firmy**.



Czas w IT

Przede wszystkim – odpowiedni interwał czasowy

Bardzo ważną, o ile nie kluczową kwestią przy wykonywaniu kopii zapasowych, często pomijaną lub lekceważoną, jest odpowiedni interwał czasowy ich wykonywania.
Przykład – firma wykonuje kopię zapasową raz w tygodniu z serwera plików. Załóżmy, że robi ją w piątek. W sytuacji, w której serwer „padnie” w czwartek, zostajemy z kopią zapasową z zeszłego piątku. Cztery dni pracy, w których kopia zapasowa nie była wykonywana – tych już nie odzyskamy.
Właściwa rekomendacja każdej firmy wdrażającej rozwiązania IT, jest następująca – kopie zapasowe powinny być robione przynajmniej raz dziennie.

Co to znaczy „stary serwer”?

Rynek potrzebuje uświadomienia w kwestii żywotności serwerów. Urządzenia powyżej pięciu lat, wbrew powszechnemu mniemaniu, to już serwery stare, obarczone dużym ryzykiem całkowitej awarii.

Zazwyczaj są już po gwarancji. Nawet jeden z najbardziej niezawodnych producentów urządzeń tego typu – Dell, daje na serwer gwarancje maksymalnie pięcioletnią. Firma jednoznacznie stwierdza, że przedłużenie gwarancji na kolejne lata jest niemożliwe. Trzeba w związku z tym zdawać sobie sprawę z tego, że po pięciu latach ryzyko awarii takiego sprzętu drastycznie wzrasta.

Budżet na tworzenie kopii zapasowych

Bardzo ważny elementem rozpatrywania bezpieczeństwa danych w firmie, jest posiadany przez firmę budżet. Tej konfrontacji nie da się nigdy uniknąć.

Dobre firmy IT przy każdym wdrożeniu prezentują zawsze rekomendacje „minimum”, „średnią” i „maksimum”. Każda z tych rekomendacji zawiera wszystkie wstępne wytyczne klienta – co chce mieć finalnie na tym serwerze zainstalowane, jak chce z tego serwera korzystać, ile osób będzie go używać i w perspektywie czasu – jak ten serwer ma działać. Miedzy innymi pod uwagę brane jest to, **czy zwiększona będzie liczba użytkowników lokalnych, czy raczej będą to przede wszystkim połączenia zdalne**. Czynników jest sporo, każdy trzeba przeanalizować i dobrać opcję optymalną.

Przykładem może być wspomniana częstotliwość wykonywania kopii zapasowych. Są sytuacje, w których rekomenduje się robienie kopii zapasowych codziennie, ale klient nie ma aktualnie zasobów, żeby taką inwestycję sfinansować. Wymaga to bowiem kupienia drogiego urządzenia i kosztownej licencji.

Świadomość zarządu firmy

Jeśli klienta na taką inwestycję nie stać, musi on być mimo wszystko świadomy ryzyka, jakie się z tym wiąże. Prowadząc w tym momencie doradztwo na poziomie biznesowym, często doradzany jest kilkuetapowy zakup, wykonywany w odstępach czasowych – jeden z nich można zrobić w jednym kwartale, drugie w drugim. Finalnie dążyć jednak powinno się do tego, żeby te najcenniejsze zasoby, które mamy w firmie, jakimi są poufne, ważne dane, były odpowiednio zabezpieczone.

Kopie zapasowe na serwerach dynamicznych

W serwerach plików kopie zapasowe tworzyć jest stosunkowo łatwo – jest to proste replikowanie wszystkich katalogów wraz z plikami w innej na innym, tożsamym nośniku danych.

Inaczej jest w przypadku serwerów bazodanowych, czy serwerów poczty – z nimi sytuacja jest dużo bardzie skomplikowana. Na takich bazach danych praca jest ciągła. Są one otwarte przez cały czas pracy firmy, aktualizowane i na bieżąco modyfikowane, dlatego też kopie zapasowe takich danych należy wykonywać w odpowiedni sposób. Kluczowe w przypadku ich powstawania jest to, aby umożliwić modyfikowanie danych przez użytkowników, mimo ich kopiowania, które w danym momencie się odbywa.

Zarządzanie kopią zapasową tych baz danych jest specyficzne. Są to skomplikowane procedury przyrostowych kopii, kopii na otwartych plikach, kopii logów, bez których bazy danych się nie odtworzy. **Trzeba mieć zaawansowaną wiedzę w zakresie IT**, żeby zrobić kopię zapasową sql, mysql'a czy postgresa, na których to działają najważniejsze programy dedykowane przedsiębiorcom.

Metody tworzenia kopii zapasowych

Są dwie powszechne metody wykonywania kopii zapasowych danych serwerowych. **Pierwsza**, to tradycyjny backup (czyli kopia) plików., **druga** to aktywowanie i utrzymywanie maszyny wirtualnej, która tworzy obraz całego serwera głównego. Więcej o obydwu z nich dowiesz się na kolejnych stronach.

Metoda 1
Tradycyjna kopia zapasowa – backup plików

Metoda 2
Zaawansowane kopie zapasowe – maszyna wirtualna

Tradycyjna kopia zapasowa

Punkt 17:00

To najbardziej znana metoda, działająca w najprostszy sposób. W firmie, która kończy pracę o 17:00, uruchamiany jest o tej porze skrypt, który kopiuje dane ze wskazanych miejsc z serwera na jakiś zewnętrzny nośnik (inny serwer, lokalizacje w chmurze lub dowolne inne urządzenie z pamięcią, podłączone do sieci).

Zasadniczą wadą takiego rozwiązania jest czas, potrzebny na uruchomienie całego środowiska po ewentualnej awarii. Najpierw musimy zadbać, żeby serwer „wstał", czyli zaczął normalnie działać, lub wytypować inne urządzenie, które tymczasowo lub na stałe przejmie jego funkcje. Na działającym urządzeniu musimy uruchomić oprogramowanie, zainstalować system operacyjny skonfigurować to środowisko i dopiero wtedy możemy przywrócić na nim dane.

Firmy korzystające z takiego rozwiązania nie zdają sobie z reguły sprawy, że uruchomienie środowiska zabezpieczanego w taki sposób będzie trwało znacznie dłużej niż spodziewanych „parę godzin". Samo odtworzenie serwera, wymiana lub naprawa części zamiennych, trwa 2 do 3 godzin, i to zakładając, że mamy już część zastępczą, która uległą awarii. Następnie należy odtworzyć oprogramowanie podstawowe, co trwa co najmniej dwie godziny. Instalacja Windowsa lub Linuxa trwa kolejne dwie godziny. Dopiero teraz można rozpocząć instalowanie oprogramowania docelowego. Nadal – jest to początek pracy, bo w tym momencie możemy dopiero rozpocząć odtwarzanie struktury serwera plików, co jest z reguły prawdziwą „dłubaniną". Ta kończy się z reguły po 5-6 dniach. To jest pokłosie prostego backup'u, polegającego na regularnym kopiowaniu ważnych plików.

Żadna firma nie chce „stać" przez 5-6 dni, tylko dlatego, że padł im centralny serwer z danymi. Mimo to większość firm nie jest świadoma, jak długo odzyskiwane są takie proste kopie zapasowe.

Zaawansowane kopie zapasowe

Szybkość i precyzja

Drugi sposób robienia kopii zapasowej, to aktywowanie i utrzymywanie maszyny wirtualnej – jest to oprogramowanie instalowane na serwerze (fizycznym bądź wirtualnym), które **tworzy i stale uaktualnia obraz całego serwera głównego**.

Wygląda to tak, że oprogramowanie do kopii zapasowych, z którego korzystamy, robi migawkę całego serwera – systemu podstawowego, systemu operacyjnego, zainstalowanego na nim oprogramowania (ERP, skrzynki pocztowej itd.), całej ich aktualnej konfiguracji oraz wszystkich plików z danymi na nim się znajdujących.

Kiedy dochodzi do awarii takiego serwera, wystarczy jedynie maszyna zastępcza. Może to być nawet chwilowo zwykły komputer, który na jakiś czas przejmie zadania serwera centralnego.

Instalujemy na nim oprogramowanie do odzyskiwania danych z maszyny wirtualnej, co trwa jedynie pół godziny. Na nim odtwarzamy już pełne środowisko wraz z systemem operacyjnym i oprogramowaniem – wszystko z utworzonej migawki. W ciągu dwóch do trzech godzin serwer jest w stanie pełnej funkcjonalności, pozwalającej na rozpoczęcie normalnej pracy.

Oprogramowanie to pozwala na odzyskanie nawet pojedynczego pliku z takiej migawki, jeśli będzie taka potrzeba. Jak widać, ponosząc koszt półtorej do trzech tysięcy złotych, w zależności od typu licencji, skracamy kilkunastokrotnie potencjalny czas odtworzenia serwera w przypadku jego awarii.

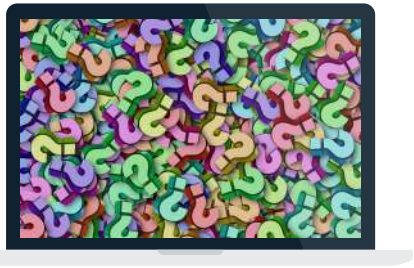
System RAID a kopia zapasowa

Klienci bardzo często mylą dyski pracujące w systemie RAID z systemem tworzenia kopii zapasowych. Mają serwer, w którym są z reguły cztery dyski twarde, pracujące w takim układzie, czyli kopiują się między sobą równolegle. Gdy jeden dysk ulega awarii, to drugi przejmuje jego rolę. Dysk zepsuty można spokojnie wymienić, bez zakłócania pracy całego układu. W ten sposób całość się odbudowuje i dalej funkcjonuje.

Jednak systemy RAID również są zawodne. Często użytkownicy bardzo mocno zawierzają takiemu rozwiązaniu, traktując je niemal jak twierdzę – są w nim cztery dyski, więc jak jeden się zepsuje, to są kolejne trzy. Prawdopodobieństwo tego, że dwa się zepsują naraz, jest wg nich praktycznie zerowe. Nie jest to niestety prawda, szczególnie w przypadku leciwych serwerów. **Częste są sytuacje, w których awarii ulega cały system, zwłaszcza w przypadku urządzeń pięcioletnich i starszych.**

Czy znasz procedury odzyskiwania danych w swojej firmie?

Często osoby decyzyjne w zarządach firm mają niewystarczające pojęcie o elemencie technicznym funkcjonowania ich firmy, np. jeśli chodzi o kopie zapasowe. Wiedzą, że coś takiego jest robione, ale to wszystko. Bardzo często jest to enigmatyczna świadomość – dział IT „coś tam" w tej kwestii robi.
Mało który zarząd jest jednak świadomy, jak będą wyglądały faktycznie procedury w przypadku awarii serwerów. Często firmy proszą o interwencje specjalistów od IT, mimo że mieli stale robioną kopię zapasową danych. W momencie jednak, w którym pojawiła się faktycznie awaria, okazało się, że te kopie nie nadawały się do niczego – źle zorganizowane, robione w zły sposób, i nienadające się do odtworzenia czegokolwiek.



Rozumieć ryzyko

Z dobrym zabezpieczeniem danych jest jak z ubezpieczeniem – płacimy wiele tysięcy złotych, żeby w przypadku nagłej szkody odzyskać przynajmniej częściej poniesionych strat.
Biorąc pod uwagę, że w przypadku awarii serwera przestój firmy może generować wielotysięczne straty, które potencjalnie pogrążą całą firmę, warto rozważyć inwestycję kilku-kilkunastu tysięcy złotych w odpowiednie rozwiązanie chroniące dane firmowe oraz systemy, na których oparte jest jej działanie. Właśnie w takich kategoriach należy rozpatrywać inwestycję w bezpieczeństwo IT, w tym w odpowiedni system tworzenia kopii zapasowych. Kto wie, może kiedyś ten drobny wydatek uchroni interesy i los całej organizacji.

Masz pytania? Chcesz wiedzieć więcej?

Od ponad 10 lat świadczymy kompleksową obsługę informatyczną dla sektora małych, średnich i dużych firm na terenie Warszawy.
Od 2017 roku jesteśmy zaangażowani we wdrażanie wymogów RODO w firmach.

Tomasz Janas
CEO, Itomega Sp. z o.o.
tomasz.janas@itomega.pl