Zabezpiecz swój magazyn

Bezpieczeństwo danych w systemach komputerowych (Cz. 1)

Jak bardzo jesteśmy uzależnieni od komputerów i jak ważne dane na nich przechowujemy - zwykle uświadamiamy sobie, gdy jest już za późno. Niniejszy artykuł jest początkiem serii poświęconej ochronie danych i bezpieczeństwu w systemach komputerowych.

Choć wszyscy użytkownicy są zgodni, że informacje na ich komputerach są bezcenne, rzadko spotyka się, aby ktoś zabezpieczał je przed zniszczeniem. Analogicznie jest w większych firmach, gdzie administratorzy w pełni ufają stworzonemu przez siebie systemowi komputerowemu, nie zdając sobie sprawy z czyhających nań zagrożeń. Człowiek nienauczony doświadczeniem, bezgranicznie wierzy w niezawodność komputerów i dopiero czas pokazuje, jak bardzo się mylił. Według TANDBERG DATA egzystują tylko dwa rodzaje danych: te, które zostały zarchiwizowane oraz te, które nie zostały JESZCZE utracone. Zanim więc zaczniemy wyrywać sobie włosy z głowy i płakać nad rozlanym mlekiem warto zwrócić uwagę na ogromne niebezpieczeństwa grożące naszym zasobom i... w porę się zabezpieczyć. W tej części artykułu opisane zostały najpopularniejsze zagrożenia mogące powodować utratę danych.

Przyczyny utraty danych

Najczęstszą przyczyną utraty danych są niewątpliwie **uszkodzenia sprzętowe** (78%), głównie mechaniczne, dysków twardych. Nie ma dysków bezawaryjnych! Nawet te najdroższe, najlepszej jakości, wyprodukowane przez najlepsze światowe firmy, mogą stać się źródłem awarii i prowadzić do utraty danych. I to wg praw Murphy'ego właśnie w najmniej pożądanym momencie. Awarie dysków można podzielić na dwie grupy - w zależności od objawów uszkodzeń - a w konsekwencji na sposób ewentualnego odzyskania chociaż części danych. Jeśli nagle system informuje nas o sprzętowych problemach z odczytem danych na dysku oznacza to, że prawdopodobnie bezpowrotnie straciliśmy już część danych, a w kolejnych minutach, bądź dniach stracimy wszystko. Wtedy natychmiast należy ratować zbiory, zaczynając oczywiście od tych najważniejszych. Jeśli system nie chce już poprawnie startować, uruchamiamy komputer z dyskietki systemowej i kopiujemy pliki pod DOS'em. Drugą grupę awarii dyskowych bardzo łatwo poznać. Po włączeniu komputera system bardzo długo czeka na zgłoszenie się twardego dysku, po czym zwykle nic nie znajduje. Często towarzyszą temu: głośnie stukanie lub wręcz zgrzytanie. Można się domyślić, że w tym momencie szanse na odzyskanie jakichkolwiek danych bez pomocy wykwalifikowanych (i bardzo drogich) specjalistów praktycznie nie istnieją.

Istnieje kilka środków zapobiegawczych, zmniejszających ryzyko pojawienia się awarii sprzętowych. Jedną z nich jest montaż urządzeń UPS (uninterruptable power supply). Nie tylko chronią one komputer przed nagłym zanikiem zasilania, ale również przed niebezpiecznymi skokami napięcia, które mogą prowadzić do uszkodzeń sprzętu. Bardzo ważna jest dobra wentylacja komputera, w tym chłodzenie lub zapewnienie odpowiedniego przepływu powietrza dyskom twardym. Obecnie produkowane dyski odprowadzają znaczne większe ilości ciepła niż kiedyś (dla uproszczenia można przyjąć, że tym bardziej dysk się grzeje, im większa jest prędkość obrotowa jego talerzyków). Należy pamiętać również o tym, aby nie narażać dysku (całego komputera) na drgania, zwłaszcza podczas pracy. Bardzo dużą ostrożność należy zachować podczas przenoszenia komputera, czy też transportu.

Awarie dysków można wykryć nawet na 24 godziny przed ich pojawieniem się, korzystając ze specjalnej technologii zwanej **S.M.A.R.T.** odpowiedzialnej za autokontrolę stanu technicznego dysku (skuteczność oceniana jest na 30 do 40%). W chwili obecnej praktycznie wszystkie produkowane dyski są z nią kompatybilne. Dzięki niej, za pomocą odpowiednich programów (np.: **SIGuardian** - *http://www.siguardian.com*, **ActiveSMART** - *http://www.ariolic.com*), możliwe jest sprawdzanie na bieżąco, wykrywanie wszelkich nieprawidłowości w działaniu dysku i powiadamianie użytkownika o niebezpieczeństwie.

Jednym ze sposobów, zapewniających 100% ochronę danych przed skutkami awarii, jest stosowanie macierzy dyskowych RAID. Skrót RAID pochodzi od Redundant Array of Independent Disks i ma na celu poprawienie wydajności systemów dyskowych oraz zwiększenie bezpieczeństwa zapisywanych danych. Zasada działania standardu **RAID** polega na odpowiednim połączeniu wielu dysków w jedną całość. W ramach standardu RAID rozróżnia się kilka trybów pracy dysków. Poniżej opisano najczęściej używane:

- RAID 0 (*Disk Striping*) - Dane dzielone są na odpowiedniej wielkości bloki i zapisywane rotacyjnie na wszystkich podłączonych dyskach (blok 1 na pierwszym dysku, blok 2 na drugim itp., przy czym w macierzy mogą pracować dwa lub więcej dysków). Uzyskuje się przez to znaczy wzrost szybkości transferu danych, zarówno przy zapisie jak i odczycie, natomiast powiększa się możliwość utraty danych wskutek awarii - jeden zepsuty dysk w macierzy powoduje utratę wszystkich danych.
- RAID 1 (*Mirroring*) - RAID dokonuje lustrzanej kopii danych na wszystkich podpiętych do niego dyskach. Innymi słowy, w czasie rzeczywistym tworzone są kopie bezpieczeństwa danych, natomiast nie ma poprawy wydajności dysków.
- RAID 5 - w tym trybie dane zapisywane są w blokach, tak jak w trybie 0, ale dla podniesienia bezpieczeństwa, co kilka bloków zapisywane są informacje o parzystości. Dzięki temu uzyskuje się poprawę wydajności, a jednocześnie zabezpiecza przed awarią dysków (system, dzięki informacjom o parzystości potrafi odtworzyć brakujące dane). Należy jednak zwrócić uwagę na to, że tylko jeden dysk w macierzy naraz może ulec uszkodzeniu. Jednoczesne uszkodzenie dwóch dysków powoduje utratę danych. Minimalnie w tym trybie należy podłączyć 3 dyski twarde. RAID 5 jest trybem stosowanym najczęściej w serwerach.

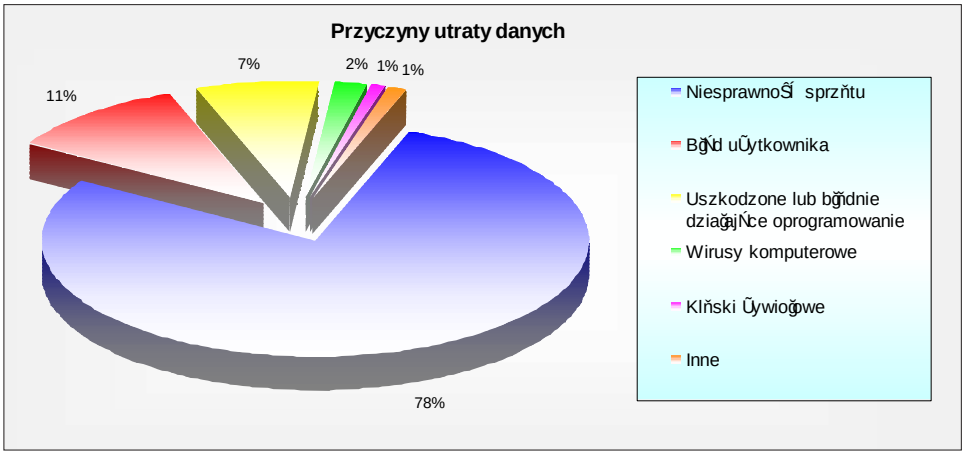
RAID występuje w wersji sprzętowej (kontrolery) lub programowej (standar-

dowo obsługiwane np. przez Windows NT 4, 2000 i XP). Dokładne sposoby wykorzystanie tej technologii zostaną opisane w następnych numerach "Logistyki".

Drugim, co do wielkości zagrożeniem są **błędy popełniane przez użytkowników** (11%). Ich przykłady można mnożyć: przypadkowe zmazanie katalogu, bądź pliku, format dysku, upuszczenie dysku, czy całego komputera (np. laptopa), "majsterkowanie" przy otwartym komputerze, itp. Osobiście znam również zdarzenie, gdy przy przenoszeniu komputera przypadkowo przełączono zasilanie z 220V na 110V.

Sposoby ochrony przed takimi awariami są dość proste (praktyka jednak pokazuje, że rzadko stosowane): nie jesteś pewny - nie ruszaj, zapytaj specjalisty, oraz nigdy nie przenoś komputera w trakcie jego pracy (mowa tu o komputerach stacjonarnych), ani nie ruszaj niczego w jego wnętrzu bez uprzedniego odłączenia wtyczki zasilającej. Oczywiście, identycznie jak w poprzednim przypadku, w obliczu katastrofy pozostaje tylko sięgnąć po... aktualną kopię zapasową danych.

Błędy oprogramowania (7%) to kolejne zagrożenie dla naszych danych. Jest kilka źródeł powstawania takich awarii. Jednym z nich jest nagłe wyłączenie komputera w czasie jego pracy, np. w wyniku zaniku napięcia, powodujące przerwanie w połowie zapisu pliku, co może doprowadzić do jego całkowitego uszkodzenia. Innym jest uruchomienie programu, który przypadkowo, błędnie spowoduje ingerencję w pliki na dysku, bądź w tablicę alokacji plików, w efekcie czego zajdą tam nieodwracalne zmiany. Czasem próba naprawy jakiegoś błędu na dysku niezbyt dobrym lub niesprawdzonym oprogramowaniem kończy się jeszcze większymi szkodami. Okazuje się również, że aplikacje, nawet wiodących producentów software'u, potrafią w określonych przypadkach zniszczyć bezpowrotnie przetwarzane przez siebie dane lub pliki, w których dane te były przechowywane. Spotkałem się z takim problemem, gdy podczas zapisu pliku w programie MS Excel nagle system się zawiesił. Po zresetowaniu komputera okazało się, że plik nie daje się otworzyć - Excel nie rozpoznawał nawet formatu zapisu, nie mówiąc o jakichkolwiek danych, a były to informacje zbierane przez 2 lata.... Jak więc przeciwdziałać takiemu zagrożeniu? Jedyna droga - to częste tworzenie kopii zapasowych danych.



Rys. 1. Procentowy wykres wszystkich przyczyn utraty danych. *Źródło: Ontrack*

Wirusy komputerowe stanowią czwarte, co do wielkości (2%) zagrożenie utratą danych. Przenoszone przez pocztę, foldery sieciowe, dyskietki, mogą nie tylko pokazywać dziwne komunikaty, powodować spowolnienie systemu i rozsyłać swoje kopie z wykorzystaniem wpisów pobranych z książki adresowej użytkownika, ale także usuwać pliki, zmieniać ich kod czy nawet formatować dysk. W obecnych czasach jedynym środkiem zapobiegawczym przeciwko wirusom jest dobry program antywirusowy, skanujący komputer w trybie rzeczywistym, uaktualniany codziennie.

Klęski żywiołowe (1%). Trzęsienie ziemi, powódź - to typowe kataklizmy, w wyniku których oczywiste są straty tak i sprzętu, jak i w wielu wypadkach danych. Jednak rzadko kto zdaje sobie sprawę z zagrożenia, jakim jest uderzenie pioruna. Źle zabezpieczona przez dostawcę sieć energetyczna, czy telefoniczna może doprowadzić do doszczętnego spalenia podłączonego doń komputera. Zapobiegać tego rodzaju katastrofom można w następujący sposób: przede wszystkim należy zamontować dobrej klasy UPS. Ochroni to sieć energetyczną przed przepięciami - w przypadku silnego przepięcia spali się tylko UPS. Jeżeli natomiast chcemy korzystać z modemu w miejscu, gdzie przyłącze telefoniczne doprowadzane jest liniami napowietrznymi, musimy zaopatrzyć się w model najlepiej zewnętrzny, o wysokich parametrach szczególnie w zakresie przepięć. Przeciwko utracie danych możemy zabezpieczyć się wykonując kopie zapasowe, które będą przechowywane poza murami domu, budynku, np. w skrytce bankowej.

W obliczu tylu zagrożeń okazuje się, że najlepszą, najskuteczniejszą i sprawdzoną metodą zabezpieczenia danych okazuje się tylko **dobrze prowadzona polityka archiwizacji danych**. W jaki sposób wykonywać kopie zapasowe i na jakie nośniki - o tym w następnym artykule.

Maciej Niemir

9 sierpnia 2002 r. weszło w życie rozporządzenie Ministra Infrastruktury (Dz. U. nr 117, poz. 1010), określające rodzaj informacji i zakres danych, których może żądać od przewoźników drogowych organ wydający licencje i zezwolenia. Ma on prawo zobowiązać przewoźnika drogowego do podania informacji i dokumentów potwierdzających spełnienie warunków do prowadzenia działalności. Pytania mogą dotyczyć: daty rozpoczęcia (lub zaprzestania) wykonywania transportu drogowego objętego licencją; rodzaju wykonywanych przewozów; liczby pojazdów i zatrudnionych kierowców; danych osoby zarządzającej. Na żądanie Ministra Infrastruktury lub organu wydającego licencje i zezwolenia należy ponadto dostarczyć stosowane taryfy i ceny, dane liczbowe o ilości przewiezionych osób, towarów (w ujęciu kwartalnym, półrocznym, rocznym) z podziałem na transport zarobkowy i niezarobkowy. Dodatkowo Minister Infrastruktury może zażądać od wybranych przewoźników systematycznego udzielania danych statystycznych dla monitoringu rynku przewozów drogowych.

Iwo Nowak