Rozbudowa i naprawa sieci. Wydanie V

Autorzy: Scott Mueller, Terry W. Ogletree, Mark Edward Soper
Tłumaczenie: Piotr Pilch, Przemysław Szeremiota
ISBN: 83-246-0474-X
Tytuł oryginału: Upgrading and Repairing Networks (5th Edition)
Format: B5, stron: 1440

Poznaj zasady działania sieci komputerowych i naucz się nimi administrować

- Projektowanie sieci komputerowych
- Protokoły komunikacyjne i urządzenia
- Przyłączanie komputerów do sieci
- Zarządzanie siecią

W ciągu ostatnich lat sieci komputerowe stały się niemal tak powszechne, jak telefony i telewizja. Wiedza dotycząca zasad ich działania, umiejętność zarządzania nimi lub chociażby korzystania z nich jest dziś niezbędna większości użytkowników komputerów – od korporacyjnych informatyków po entuzjastów technologii komputerowych, wdrażających je w swoich domach i małych biurach. Na szczęście wraz z rozwojem sieci ujednolicono protokoły komunikacyjne i zaimplementowano w systemach operacyjnych narzędzia niezbędne do podłączenia komputera do sieci. Nie oznacza to jednak, że korzystanie z sieci przestało być źródłem problemów.

Dzięki książce „Rozbudowa i naprawa sieci. Wydanie V" rozwiążesz wszystkie problemy, jakie kiedykolwiek napotkasz projektując sieć i administrując nią. Najnowsze wydanie tej książki, uzupełnione o wiadomości dotyczące sieci bezprzewodowych, technologii Bluetooth i Gigabit Internet oraz możliwości sieciowych systemu Windows XP, zawiera kompleksowe omówienie wszystkich zagadnień związanych z sieciami komputerowymi. Czytając tę książkę poznasz strategie projektowania sieci i doboru odpowiednich urządzeń oraz protokoły wykorzystywane do realizacji poszczególnych funkcji sieci. Nauczysz się administrować siecią, kontami użytkowników oraz dbać o bezpieczeństwo danych i komputerów.

- Topologie sieci
- Planowanie struktury sieci
- Okablowanie
- Dobór i konfiguracja urządzeń sieciowych
- Protokoły komunikacyjne
- Sieci bezprzewodowe Wi-Fi i Bluetooth
- Poczta elektroniczna
- Protokoły DNS i DHCP
- Zarządzanie użytkownikami w systemach Unix/Linux i Windows
- Drukowanie w sieci
- Ochrona sieci przed atakami z zewnątrz

Zostań administratorem doskonałym

Wydawnictwo Helion
ul. Kościuszki 1c
44-100 Gliwice
tel. 032 230 98 63
e-mail: helion@helion.pl

Spis treści

Rozdział 5.

Ochrona sieci: metody zapobiegania zagrożeniom

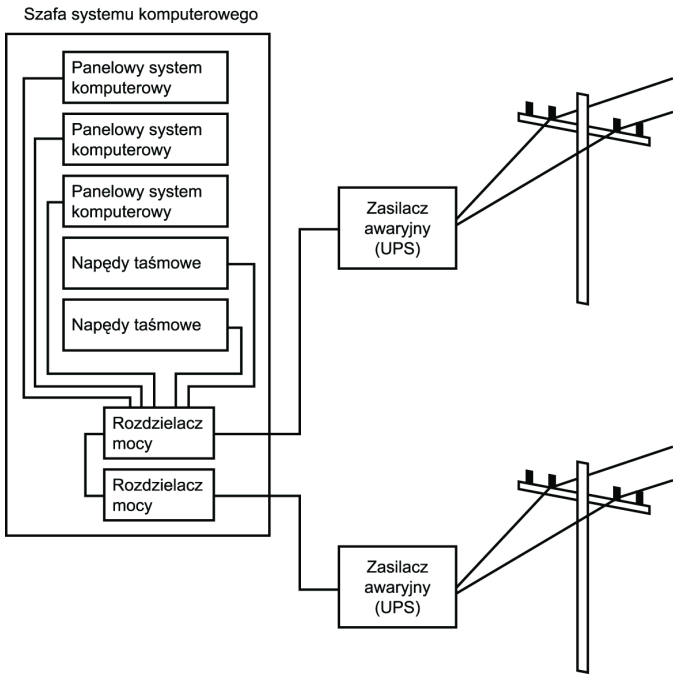
W tym rozdziale przyjrzymy się kilku ważnym ochronnym metodom zapobiegawczym, które można zastosować w sieci. Wielkość i budowa sieci będą miały wpływ na wybór jednej z metod omawianych w niniejszym rozdziale. Nie wszystkie metody są odpowiednie dla każdej sieci. Niektóre z nich — ze względu na wysoki koszt — nie nadają się do niewielkich sieci. Ponadto należy pamiętać, że podobnie do planowania rozbudowy samej sieci można również planować modernizację procedur i urządzeń chroniących sieć przed awariami i utratą danych.

Stabilizacja napięcia i zasilacze awaryjne UPS (Uninterruptible Power Supplies)

Bez prądu żadna sieć nie będzie w ogóle działała, natomiast w celu poprawnego funkcjonowania komputery wymagają stabilnego źródła napięcia. Zasilacz komputera może nie wytrzymać odebranego skoku napięcia, spowodowanego na przykład piorunem. Podobnie krótkotrwały spadek napięcia może doprowadzić do „zawieszenia się" komputera, a więc i utraty danych.

Duże systemy komputerowe stosowane w środowiskach korporacyjnych, takie jak średniej klasy serwery oraz komputery przemysłowe, również wymagają stabilnego źródła zasilania. W celu jego zapewnienia w większości dużych pomieszczeń komputerowych stosowane są duże zasilacze awaryjne UPS, których zadaniem jest pośredniczenie pomiędzy zewnętrznym źródłem zasilania a komputerami oraz innymi urządzeniami w serwerowni.

Przykładowo w większości przestronnych serwerowni komputery — niezależnie od tego, czy są to serwery PC czy większe systemy — są umieszczane w szafach panelowych wraz z napędami taśmowymi, dyskami oraz innymi urządzeniami peryferyjnymi. Szafa zawiera zazwyczaj jeden lub kilka rozdzielaczy mocy (PDU), zasilających zamontowane w niej urządzenia (rysunek 5.1).



Rysunek 5.1. *W celu zapobieżenia awarii zasilania sieci elementy zasilające są dublowane*

Na rysunku można zauważyć, że kilka używanych systemów komputerowych i napędów taśmowych umieszczono w jednej szafie. Dwa rozdzielacze mocy znajdujące się na dole szafy doprowadzają napięcie do wszystkich urządzeń w niej umieszczonych. Rozdzielacze są wzajemnie nadmiarowe, dzięki czemu w sytuacji, gdy jeden z nich ulegnie awarii, drugi będzie w dalszym ciągu doprowadzać napięcie do urządzeń. Każdy z rozdzielaczy mocy jest podłączony do oddzielnego zasilacza awaryjnego UPS, znajdującego się w pomieszczeniu. Jest to ważne z kilku powodów. Po pierwsze, nie wszystkie awarie zasilania wynikają z zewnętrznych problemów, takich jak wyłączona linia przesyłowa. Czasem awarii ulegnie sam zasilacz awaryjny. W trakcie rutynowych czynności konserwacyjnych lub instalacyjnych elektryk może odłączyć niewłaściwy kabel. Mysz może przegryźć przewody, powodując zwarcie. Mogą się zdarzyć przeróżne rzeczy, dlatego powinieneś „oczekiwać nieoczekiwanego".

Aby nadmiarowość sięgała dalej, każdy zasilacz awaryjny znajdujący się w serwerowni i używany przez systemy jest podłączony do niezależnego zewnętrznego źródła zasilania. A zatem jeśli złamie się drzewo i uszkodzona zostanie w ten sposób jedna linia zasilania, to w dalszym ciągu będzie dostępna dodatkowa linia, która za pośrednictwem drugiego zasilacza awaryjnego doprowadzi napięcie do urządzeń. Dzięki zapasowemu źródłu zasilania komputery i inne urządzenia podłączone do sieci nadal będą działały.

Energia to pieniądze

Istnieje takie stare powiedzenie: „pieniądze dają władzę"[1]. Odwrotna sytuacja również jest prawdziwa.

[1] W oryginale („*power is money*" i „*money is power*") gra słów, polegająca na wieloznaczności słowa „*power*", które oznacza zarówno władzę, jak i energię elektryczną — *przyp. tłum.*

Schemat przytoczony w poprzednim podrozdziale może wydać się przesadny dla administratora niewielkiej sieci złożonej z kilku komputerów PC, w której przestoje są dopuszczalne. Jednak w przypadku środowiska komputerowego, w którym wymagana jest bardzo wysoka dostępność — takiego, jak sieć dużej korporacji — koszt przestoju może być wyjątkowo wysoki z kilku powodów:

- Setki, a nawet tysiące pracowników stanie się bezproduktywnych, gdy komputery, których używają, będą pozbawione zasilania. Pracownicy w dalszym ciągu będą opłacani, nawet gdy nie będą mogli wykonywać swoich obowiązków. Dodaj złotówkę do złotówki i dojdziesz do wniosku, że każda minuta przestoju jest dość kosztowna.
- Klienci mogą nie być w stanie składać zamówień lub sprawdzać stanu realizacji zamówień już istniejących. Mniej lojalni klienci mogą po prostu zadzwonić do kogoś innego. Nikt nie lubi słyszeć: „właśnie teraz nasz serwer jest odłączony, proszę zadzwonić później". Po tym, jak klient skontaktuje się z innym dostawcą, możesz nawet już nigdy więcej się z nim nie spotkać. W efekcie stracisz nie tylko aktualne zamówienia, ale i wszystkie te, które mogły pojawić się w przyszłości.
- Niespodziewana awaria systemu spowodowana zanikiem zasilania może doprowadzić do uszkodzenia danych. Po przywróceniu zasilania identyfikacja uszkodzonych plików, a następnie ich przywrócenie do poprzedniego stanu z kopii zapasowych zapisanych na taśmach może czasem zająć wiele godzin, a nawet dni. Obecnie wiele dużych sieci, takich jak te należące do dostawców usług internetowych, zawiera dane o wielkości wyrażanej w terabajtach. Przywrócenie całej bazy danych może być bardzo kosztowne i czasochłonne. Taki dodatkowy przestój prawdopodobnie może kosztować więcej niż sama awaria zasilania, która do niego doprowadziła.

Jeśli masz do czynienia z tak wielkim środowiskiem, prawdopodobnie jesteś już świadom znaczenia gwarantowania ciągłej dostępności systemów komputerowych. Jeśli nie zadbasz o stabilne i pewne źródło zasilania, to wszystkie inne ochronne metody zapobiegawcze mogą przedstawiać niewielką wartość, gdy następnym razem dojdzie do zaniku napięcia.

Zasilacz awaryjny nie jest nieskończonym źródłem zasilania. Spełnia on rolę przewodu, przez który zewnętrzne źródło zasilania przesyła napięcie do systemów komputerowych. Działanie zasilaczy awaryjnych UPS polega na magazynowaniu energii w jednej lub kilku bateriach, dzięki czemu po nieoczekiwanej awarii zewnętrznego źródła zasilania w ciągu kilku milisekund mogą one przejść na zasilanie z baterii. Jednak baterie mogą być używane tylko przez określony czas. Jeśli jest używany tylko jeden zasilacz awaryjny, podłączony do jedynego źródła zasilania, pozwoli on na powiadomienie użytkowników o konieczności wylogowania się z systemów przez niego zasilanych oraz wyłączenie ich w sposób nie zagrażający uszkodzeniu danych. Co prawda nadal spowoduje to bezproduktywne oczekiwanie pracowników, ale nie pojawi się konieczność przywracania danych po usunięciu awarii zasilania.

W przypadku dużych sieci należy zaplanować dodatkowy poziom zabezpieczenia na wypadek zaniku zasilania, czyli generatory prądu oparte na silniku Diesla. Co prawda zasilanie przy ich użyciu dużej liczby stacji roboczych użytkowników byłoby zbyt kosztowne, ale mogą one posłużyć do podtrzymania pracy serwerów oraz rezerwowej pracowni, do której użytkownicy (przynajmniej najważniejsi) powinni się przenieść na czas awarii.

Przykładowo w większości sytuacji nie wszystkie aplikacje sieciowe odgrywają krytyczną rolę i muszą być dostępne przez 24 godziny na dobę i siedem dni w tygodniu. A zatem w zapasowe zasilanie powinny być wyposażone wyłącznie serwery o bardzo dużym znaczeniu. Jeśli masz do czynienia przykładowo z firmą handlową, to będzie Ci zależało na utrzymaniu dostępności serwerów (np. serwer WWW), które obsługują klientów. Inne aplikacje, takie jak edytor tekstu używany przez dział prawny czy działy realizujące inne zadania, mogą zostać przywrócone do działania później.

Interfejs ACPI (Advanced Configuration and Power Interface) a niezależne systemy zasilaczy awaryjnych UPS

W przypadku komputerów PC i niewielkich serwerów wystarczający będzie zakup niedrogich zasilaczy awaryjnych UPS, wartych kilkaset złotych. Mogą one być zastosowane w środowisku, w którym przestój jest dopuszczalny, ale uszkodzenie danych już nie. Konfiguracja typowego zasilacza awaryjnego, produkowanego np. przez firmę APC (American Power Conversion Corp), zajmuje zaledwie kilka minut. W zależności od modelu może on oferować zarówno zasilanie z baterii, jak i wybrane funkcje stabilizacji napięcia.

Trzeba wziąć pod uwagę, że stabilizatory i listwy przeciwprzepięciowe, choć mają uniemożliwiać przenikanie przepięć do chronionych systemów, nie zawsze działają zgodnie z zapewnieniami producenta. Tanie modele nabywane w niespecjalistycznych sklepach zazwyczaj nie oferują ochrony, o której wspominają producenci. Jeśli całe zabezpieczenie ma się opierać na prostym bezpieczniku, to przy jego zakupie należy odłożyć pieniądze na zakup nowego komputera — będzie potrzebny po najbliższym silnym wyładowaniu atmosferycznym. Tam gdzie nie ma miejsca dla rozbudowanych systemów UPS, realnym zabezpieczeniem może być jedynie prosty zasilacz awaryjny chroniący serwer czy inne ważne urządzenia sieciowe.

Należy mieć świadomość, że wszystkie urządzenia podłączone do komputera również muszą być chronione przed przepięciami itp. Jeśli Twój komputer został podłączony do zasilacza UPS oferującego taką ochronę, ale monitor i modem kablowy są podłączone bezpośrednio do gniazdka, a dopiero potem do komputera, to będziesz miał jedynie fałszywe poczucie bezpieczeństwa. W domu czy małym biurze z kablowym dostępem do internetu uderzenie pioruna w zewnętrzną instalację kablową może spowodować przeniesienie udaru przez okablowanie, a potem przez modem kablowy wprost do wnętrza komputera. Innymi słowy, wszystkie urządzenia podłączone do komputera wszelkimi sposobami powinny również być chronione zasilaczami awaryjnymi albo innymi porządnymi zabezpieczeniami.

Aby po zaniku napięcia i przejściu na zasilanie z baterii możliwe było poprawne zamknięcie systemu operacyjnego, kilka firm (najważniejsze z nich to Intel, Microsoft, a także inni producenci) opracowało interfejs ACPI (ang. *Advanced Configuration and Power Interface*). Interfejs ACPI jest dość obszerny i swoim zakresem obejmuje zarządzanie energią w laptopach i innego typu komputerach. Jednak interfejs ten oferuje też standardową metodę komunikacji niezależnego zasilacza awaryjnego z komputerem i w chwili, gdy UPS przełącza się na zasilanie z baterii, wymuszane jest wyłączenie systemu w sposób bezpieczny dla danych.

W celu uzyskania dodatkowych informacji na temat specyfikacji i innych danych dotyczących sposobu współpracy interfejsu ACPI z BIOS-em komputerów należy zajrzeć na stronę internetową znajdującą się pod adresem *http://acpi.info*. Na stronie zawarto też kilka narzędzi, takich jak kompilatory, które umożliwiają zastosowanie języka ASL (*ACPI Source Language*), służącego do tworzenia kodu zapisywanego w układach instalowanych na płycie głównej komputera. Co prawda czytanie informacji zawartych na stronie nie należy do przyjemności, ale zalecane jest to dla osób, które lubią wiedzieć, jak dane urządzenie działa. Na stronie zawarto też dekompilator, który może posłużyć do zamiany kodu maszynowego zapisanego w układzie z powrotem na kod języka ASL, co ma na celu uproszczenie jego analizy. Interfejs ACPI jest też dostosowywany do komputerów pracujących pod kontrolą systemu Linux. Dodatkowe informacje na ten temat można znaleźć na stronie *http://acpi.sourceforge.net/*.

Interfejs ACPI nie jest ograniczony wyłącznie do zewnętrznych zasilaczy awaryjnych. Specyfikacja uwzględnia też inne funkcje związane z zarządzaniem energią, które obecnie są standardowo obsługiwane przez większość systemów operacyjnych. Przykładowo jeśli w panelu sterowania systemów Windows 2000/XP/Server 2003 zostanie otwarte okno *Opcje zasilania*, to ustawienia, które można tam modyfikować, są powiązane z interfejsem ACPI. Kolejna interesująca funkcja zapewniana przez ACPI to uruchamianie komputera poprzez naciśnięcie dowolnego klawisza.

Komunikacja ta realizowana jest przez przyłączenie kabla zasilającego komputera do zasilacza awaryjnego, a także przez połączenie zasilacza i komputera specjalnym kablem szeregowym (albo kablem USB), a potem uruchomienie obsługi zasilacza awaryjnego w systemie operacyjnym. W systemach Windows 2000 i Windows Server 2003 tego typu usługa współpracuje z podłączonymi zasilaczami awaryjnymi, obsługującymi interfejs ACPI. Usługa taka jest też oferowana przez takie systemy, jak Windows 2000 Professional, Windows XP oraz niektóre wersje systemów Unix i Linux. Zasilacz awaryjny komunikuje się z usługą i nakazuje systemowi, aby zakończył działanie w standardowy sposób, gdy zostanie stwierdzony zanik napięcia i przejście na zasilanie z baterii. W niewielkich zasilaczach awaryjnych należy sprawdzić obecność następujących elementów:

- **Alarmy dźwiękowe**. Pamiętam, jak kilka lat temu obudził mnie alarm zasilacza awaryjnego. Okazało się, że spałem w trakcie huraganu. Cieszyłem się wówczas, że miałem zasilacz UPS — ocalił mój komputer i, przy okazji, być może mnie.
- **Wiele gniazd**. Większość małych zasilaczy awaryjnych pozwala na podłączenie do niego od dwóch do czterech urządzeń, dzięki czemu nie trzeba kupować oddzielnych zasilaczy UPS dla komputera, drukarki, routera itd. Takie rozwiązanie może być przydatne w środowisku małego biura SOHO (ang. *Small Office/ Home Office*), w którym urządzenia wymagające ochrony znajdują się blisko siebie. Dodatkowo przy zakupie zasilacza UPS należy szukać modeli umożliwiających ochronę podłączanych do komputera przewodów innych niż napięciowe, jak na przykład linia telefoniczna. Pamiętaj, że niektóre gniazdka zasilaczy UPS oferują tylko ochronę przeciwprzepięciową. Urządzenia mniej istotne dla sieci, takie jak drukarki, powinny być podłączane właśnie do tych gniazdek zasilacza.
- **Wskaźnik baterii**. Należy sprawdzić, czy zasilacz UPS zawiera mechanizm powiadamiania (zazwyczaj dioda sygnalizacyjna) o sytuacji, gdy bateria zostanie całkowicie naładowana lub jest w trakcie ładowania. Baterie nie podtrzymają napięcia w nieskończoność. Dodatkowo dioda powinna wskazywać, czy UPS doprowadza napięcie przy użyciu baterii czy zewnętrznego źródła prądu.

- **Wskaźnik przeciążenia**. Nawet pomimo tego, że UPS jest wyposażony w wiele gniazd, może nie być w stanie dostarczać wystarczającej mocy do podłączonych urządzeń. Dobrej jakości zasilacz awaryjny powiadomi (znów zazwyczaj przy użyciu diody) o zbliżeniu się do jego maksymalnych możliwości. W takiej sytuacji konieczne będzie zastosowanie więcej niż jednego zasilacza. W dokumentacji dołączonej do UPS powinno być podane natężenie prądu, jakie może być zapewniane przez urządzenie. Podobnie w dokumentacji dołączonej do komputerów i urządzeń peryferyjnych powinna się znajdować informacja dotycząca pobieranej przez nie energii. W celu sprawdzenia, czy zasilacz UPS jest w stanie spełnić wymagania, należy obliczyć całkowity pobór mocy.
- **Wyłącznik obwodu**. Jeśli zignorujesz wskaźnik przeciążenia, zasilacz powinien być wyposażony w automatyczny wyłącznik, który zwykle ma postać niewielkiego przycisku, który można ponownie włączać. Jeśli mimo powiadomienia o przeciążeniu w dalszym ciągu próbujesz uzyskać więcej mocy, niż zasilacz na to pozwala, UPS uruchomi wyłącznik i tym samym odetnie zewnętrzne źródło zasilania. Zasilacz przejdzie na pracę przy wykorzystaniu baterii, a podłączone urządzenia otrzymają sygnał do zakończenia pracy.

Co prawda duża liczba wytwórców produkuje i sprzedaje niewielkie zasilacze UPS, ale w celu uzyskania informacji na temat produktów (wraz z dokumentacją), które można zastosować w różnych przypadkach — począwszy od stacji roboczej, a skończywszy na w pełni wyposażonej serwerowni opartej na systemach zasilaczy UPS — warto zajrzeć na stronę internetową firmy American Power Conversion (*www.apc.pl*).

Przy podejmowaniu decyzji o zakupie zasilacza awaryjnego trzeba pamiętać, że możliwości tych produktów mocno windują ich ceny. Koszt zakupu zasilacza UPS należy porównać z kosztem wymiany urządzeń, które mają być chronione, ale także z kosztem przestoju, uszkodzenia danych itp.

Urządzenia sieciowe

Systemy zasilania awaryjnego nie są przeznaczone wyłącznie dla komputerów — w końcu niniejsza książka jest poświęcona sieciom. Nie zapomnij o routerach, przełącznikach i innych urządzeniach podłączonych do sieci. Co prawda w trakcie awarii zasilania dopuszczalny może być brak dostępu do drukarki, ale w przypadku komputerów nie będzie to miało większego znaczenia, czy działają, jeśli użytkownicy nie mogą się z nimi połączyć za pośrednictwem sieci. Tam gdzie ciągłe działanie sieci jest ważne dla działalności korporacji, routery i inne tego rodzaju urządzenia należy podłączać do tych gniazdek zasilaczy awaryjnych, na których UPS podtrzymuje zasilanie. Z kolei w domu czy małym biurze do podtrzymywanych gniazdek zasilacza awaryjnego można podłączyć nie tylko komputer, ale i router czy modem szerokopasmowy (kablowy, satelitarny, DSL itd.).

Monitorowanie sieci

Protokoły SNMP (ang. *Simple Network Management Protocol*) i RMON (ang. *Remote Monitoring*) są przydatnymi technologiami, służącymi do zarządzania nośnikiem danych stosowanym w dużych sieciach. W przypadku niewielkich sieci lokalnych, używanych

na przykład w domu, takie rozwiązania nie są wymagane. Jeśli urządzenie takie, jak modem kablowy lub modem DSL bądź router przestanie działać, to prawdopodobnie będzie możliwe szybkie stwierdzenie tego faktu. Dotyczy to również drukarki (może zabraknąć w niej tonera lub tuszu) i komputera lub komputerów (mogą się „zawiesić" lub ulec awarii). Jednak gdy sieć swoim zasięgiem obejmuje duży obszar geograficzny lub składa się z dużej liczby urządzeń i komputerów, to oba wymienione protokoły mogą być — wraz z konsolami zarządzania — użyte w celu ułatwienia zdalnego diagnozowania problemów i gromadzenia danych statystycznych dotyczących sieci. Protokoły SNMP i RMON mogą też okazać się przydatne do wykrycia usterki, zanim jeszcze stanie się ona powodem rzeczywistego problemu.

Podstawowym zadaniem protokołu SNMP jest zbieranie danych na temat komputerów i innych urządzeń podłączonych do sieci. Protokół jest używany wraz z konsolą zarządzania, spełniającą rolę centrum generowania raportów. Co prawda protokół RMON jest podobny do protokołu SNMP, ale oferuje dodatkowe funkcje, powiązane szczególnie ze zdalnymi urządzeniami. Poprzez wybranie odpowiedniej konsoli zarządzania można określić wartości progowe wybranych zdarzeń, takich jak obciążenie sieci, błędy i inne dane statystyczne, dzięki czemu po wystąpieniu jakichkolwiek anomalii automatycznie zostaną wygenerowanie ostrzegawcze alarmy.

►► Protokoły SNMP i RMON szczegółowo omówiono w rozdziale 49. — „Narzędzia do testowania i analizowania sieci". Jeśli zarządzasz dużą siecią za pomocą aplikacji służących do centralnego zarządzania, to wykorzystują one właśnie te protokoły do zbierania informacji o urządzeniach sieciowych oraz, w przypadku RMON, do ustawiania zmiennych w bazach MIB (ang. *Management Information Base*) tych urządzeń.

Kopie zapasowe stacji roboczych i serwerów

Czy kiedykolwiek zdarzyło Ci się stracić książkę adresową? Czy posiadałeś jej kopię? Jeśli korzystasz z laptopa lub urządzenia PDA (ang. *personal digital assistant*), pozwolę sobie na zadanie zmodyfikowanego pytania. Czy zdarzyło Ci się kiedyś stracić dane zapisane na komputerze PC? Czy wykonałeś wcześniej kopię zapasową? Może się to wydawać trywialne, ale jest to związane z najważniejszym zagadnieniem poruszonym w tym rozdziale.

Nic nie będzie bardziej dla Ciebie wartościowe niż poprawnie wykonana kopia zapasowa danych przechowywanych na wszystkich systemach komputerowych podłączonych do sieci. Nie ma znaczenia, czy wydałeś setki tysięcy złotych (lub nawet miliony) na zakup najnowocześniejszych macierzy dyskowych RAID (ang. *Redundant Array of Independent Disk*), gdzie na oddzielnych dyskach jest przechowywanych wiele kopii danych. Aby zapobiec klęsce żywiołowej spowodowanej utratą danych, wiele instytucji finansowych korzysta nawet z mechanizmu wykonywania lustrzanych kopii danych pomiędzy odległymi oddziałami, umieszczonymi w różnych miejscach kuli ziemskiej. Niezależnie od stopnia nadmiarowości w lokalnym systemie przechowywania danych istnieją inne powody, dla których należy utworzyć właściwy harmonogram regularnego wykonywania kopii zapasowych ważnych danych zapisanych na komputerach podłączonych do sieci.

Oto RAID!

Pierwotnie technologia RAID nosiła nazwę *Redundant Array of Inexpensive Disks* (*nadmiarowa macierz niedrogich dysków*). Zmiana nazwy została spowodowana tym, że większość dysków stosowanych w systemach RAID dużej skali może być kojarzona ze wszystkim, ale nie z niską ceną! Jeśli chcesz uzyskać więcej informacji na temat technologii RAID — począwszy od prostej konfiguracji dysków lustrzanych, a skończywszy na zestawach paskowych i kombinacji tych dwóch rozwiązań — zajrzyj na te strony: *http://SearchStorage.techtarget.com* (poszukaj tam artykułów z cyklu „The Essential RAID Primer"); *www.acnc.com/04_01_07.html* to adres witryny Advanced Computer and Network Corporation's z przewodnikiem „Get to Know RAID"; witryna AAA Data Recovery's publikuje pod adresem *www.aaa-datarecovery.com/raid_tutorial.htm* kolejny elementarz: „RAID Tutorial". To znakomite źródła informacji o rozmaitych odmianach macierzy RAID. Technologia RAID może być stosowana na dyskach ATE/IDE, SATA, SCSI i SAS.

Przy zakupie technologii RAID należy być świadomym, że termin RAID niekoniecznie musi oznaczać, że oferowane rozwiązanie posłuży do ochrony danych. Termin RAID swoim zasięgiem obejmuje kilka technologii dyskowych. Niektóre z nich umożliwiają utrzymywanie wielu kopii danych (np. zestawy lustrzane), natomiast pozostałe przyspieszają operacje odczytu i zapisu danych (np. zestawy paskowe). Jednocześnie obie technologie są stosowane w środowisku wymagającym krótkiego czasu dostępu do magazynów danych oraz zaawansowanych metod ich ochrony.

Co prawda technologia RAID zazwyczaj jest omawiana w takich książkach, jak *Naprawa i rozbudowa komputerów PC. Wydanie drugie* autorstwa Scotta Muellera, ale wspomniano też o niej w niniejszej publikacji, co wynika z ważnej roli, jaką odgrywa ona w obecnie spotykanych większych sieciach. Więcej informacji na temat technologii RAID zawarto w rozdziale 11. — „Urządzenia NAS i sieci SAN".

Nawet jeśli zastosujesz na przykład zestaw lustrzany lub inną technologię RAID, co zrobisz, gdy z nieba spadnie meteoryt, w dodatku dokładnie na Twoją serwerownię? Bum! Stracisz wszystkie komputery, dane i oczywiście kilku administratorów. Można kupić nowe komputery i zatrudnić nowych pracowników (oczywiście po odpowiednim szkoleniu), ale czy możesz odzyskać dane?

►► Dostępna jest jeszcze jedna technologia, która może okazać się przydatna, gdy awarii ulegnie cały system magazynowania danych znajdujący się w lokalnym oddziale. Sieci SAN (ang. *Storage Area Networks*) mogą posłużyć do replikacji danych pomiędzy lokacjami oddalonymi od siebie o kilka kilometrów. Istnieje również możliwość rozmieszczenia sieci SAN na znacznie większym obszarze geograficznym. Polega to na tunelowaniu danych przesyłanych w sieciach SAN przy użyciu takich protokołów sieci rozległych, jak ATM lub Frame Relay. W celu uzyskania dodatkowych informacji na temat sieci SAN należy zajrzeć do rozdziału 11.

W celu znalezienia bardziej praktycznego powodu, dla którego warto często wykonywać kopie zapasowe, wystarczy pomyśleć o użytkownikach. Kiedy ostatnio użytkownik usunął plik lub, co gorsza, cały katalog i prosił Cię o jego przywrócenie? Kopie zapasowe mogą Cię uchronić nie tylko przed skutkami awarii komputera i kataklizmów o charakterze naturalnym lub sztucznym. Czy naprawdę ufasz swoim użytkownikom? To duży błąd. Jak mówi stare powiedzenie, „ufaj każdemu, ale najpierw go sprawdź". W dużych organizacjach trudno zadowolić wszystkich pracowników. Badania wykazały, że większość awarii poszczególnych komputerów lub sieci jest spowodowanych przez lokalnych użytkowników. Sieć powinna być chroniona zarówno przed wewnętrznymi, jak i zewnętrznymi źródłami problemów.

Nic nie jest w stanie zastąpić dobrej kopii zapasowej, może z wyjątkiem nowej pracy. Utrata danych będących wynikiem miesięcy pracy, a nawet jednego dnia (zależnie od branży) bardzo podważa Twoje kompetencje i w prostej linii prowadzi do zmiany pracownika na Twoim stanowisku.

Nośniki archiwizujące — taśmy, dyski optyczne i twarde

Standardowa metoda wykonywania kopii zapasowych, stosowana przez większość firm, bazuje na taśmach o magnetycznym zapisie danych. Można się spotkać z każdego typu archiwizującym napędem obsługującym różne rodzaje taśm — począwszy od kasetowego formatu Travan, a skończywszy na bardziej nowoczesnych i pojemnych taśmach formatu DLT (ang. *Digital Linear Tape*). W niektórych instalacjach można się jeszcze natknąć na przestarzałe szpule 9-ścieżkowe. Przy wyborze nośnika archiwizującego należy kierować się następującymi kryteriami:

- Czy kopia zapasowa będzie przechowywana przez długi czy krótki okres czasu?
- Jeśli konieczna będzie operacja przywracania, to czy nośnik jest odpowiednio wydajny?
- Jaki jest koszt nośnika archiwizującego?
- Czy konieczna jest wymiana danych z innymi ośrodkami, takimi jak firmy zajmujące się przywracaniem danych po awarii i oferujące własne pomieszczenia?

Jeśli posiadasz dane tymczasowe i zależy Ci jedynie na przywróceniu systemów do poprzedniego stanu, niezbyt odległego w czasie, to można zastosować wiele typów nośników archiwizujących. Najprawdopodobniej Twój wybór będzie uzależniony od szybkości, z jaką będą tworzone kopie zapasowe, a następnie z jaką będą przywracane z nich dane. W takim przypadku prawdopodobnie taśma jest najlepszą propozycją. Dostępne są rozwiązania oparte na taśmach magnetycznych, oferujące bardzo dużą szybkość, które pozwalają na archiwizowanie i przywracanie danych w tempie kilku gigabajtów na godzinę. Taśma magnetyczna jest także odpowiednia do krótko- i długoterminowego przechowywania danych — przy założeniu, że jest przechowywana zgodnie z zaleceniami producenta. W przypadku długotrwałego składowania danych należy pamiętać o wybraniu nośnika obsługiwanego przez standardowe urządzenia. Przykładowo przez długi czas do wykonywania kopii zapasowych danych komputerowych używano 9-ścieżkowych taśm, traktowanych jako standard. Jednak jeśli na przykład ze względu na ustalenia odgórne konieczne jest przechowywanie kopii zapasowych przez wiele lat, należy również przechowywać napędy umożliwiające odczytanie danych na nich zapisanych.

W jednym z miejsc, w którym pracowałem, miałem do czynienia z firmą, która wydała ogromną sumę pieniędzy na przeniesienie danych ze sporej liczby starych, 9-ścieżkowych taśm na nowszy nośnik DLT. Od czasu do czasu napotykano na taśmę, której odczyt nie był możliwy. Większość danych odzyskano i teraz są one przechowywane w oczekiwaniu na następną kosztowną operację konwersji. Cóż, takie są wymagania rządu!

Gdy zamierzasz przechowywać dane przez dłuższy czas, to ze względu na szybki postęp technologiczny nie masz zbyt dużego wyboru. Jednak pamiętaj o wybieraniu technologii archiwizacji opracowanej przez zaufanego producenta, co do którego możesz być pewny, że będzie istniał na rynku przez następne kilka lat.

W sytuacjach awaryjnych czas wymagany do przywrócenia danych z kopii zapasowej może być bardziej istotny od ilości czasu potrzebnego do jej stworzenia.

Przykładowo istnieje możliwość poprawnego rozbicia zestawu lustrzanego i użycia jednego z jego dysków do stworzenia kopii zapasowej, a następnie ponownego przywrócenia tego zestawu przy wykorzystaniu oprogramowania systemu RAID. Takie rozwiązanie pozwala użytkownikom nieprzerwanie korzystać z systemu, który w minimalnym stopniu będzie ulegnie wpływowi wykonywanej operacji archiwizacji. Jeśli zostanie stworzony zestaw lustrzany złożony z trzech lub większej liczby dysków, to w trakcie wykonywania kopii zapasowej w dalszym ciągu będzie możliwe działanie mechanizmu odporności na awarie, ponieważ kopia aktualnych danych będzie znajdowała się na wielu dyskach.

W systemie RAID przywracanie danych może trwać tak samo jak operacja archiwizacji lub dłużej. Jest to uzależnione od zastosowanych kontrolerów dysków, oprogramowania sprzętowego i innych czynników. Przy wybieraniu technologii tworzenia kopii zapasowych nie należy zapomnieć o konieczności uwzględnienia operacji przeciwnej, czyli przywracania danych. Można nabyć zaawansowany i szybki podsystem dyskowy, oferujący wiele różnych poziomów technologii RAID, łącznie z archiwizacją w trybie *online*. Jeśli jednak przywracanie danych z wielu dysków trwa znacząco dłużej niż w przypadku pojedynczego dysku, to można się zastanowić nad rozwiązaniem alternatywnym.

Gdy dojdzie do najgorszego, czyli gdy nie tylko komputery, ale cały oddział padnie ofiarą jakiegoś kataklizmu, takiego jak pożar, należy mieć wtedy pewność, że używany nośnik archiwizujący jest kompatybilny z urządzeniami, które zostaną użyte w trakcie wykonywania procedury przywracania. Z łatwością można to przeoczyć podczas szukania dostawcy systemów czy pracowni awaryjnych. Nie należy do końca ufać dostawcy. Trzeba samemu wszystko sprawdzić. Weź taśmy z kopią zapasową i wykonaj w pracowni operację przywracania. Zmierz czas jej trwania. Upewnij się, że stosowany nośnik jest kompatybilny ze sprzętem dostawcy, a także sprawdź, czy napędy taśmowe (lub napędy innego typu) są wystarczająco szybkie, aby w krótkim czasie można było przeprowadzić operację odtwarzania.

Obecnie taśma magnetyczna nie jest jedynym typem nośnika archiwizującego. Dostępny jest bogaty asortyment nośników, począwszy od dysków magnetooptycznych, a skończywszy na dyskach CD i DVD. Problem z zapisywalnymi (jednokrotnie i wielokrotnie) dyskami CD i DVD polega na tym, że w dalszym ciągu w porównaniu z szybkością stosowanych taśm magnetycznych są zbyt wolne (nawet jeśli dysponujesz jednym z szybszych napędów), aby mogły być użyte na potrzeby operacji archiwizacji i przywracania. Pomimo to technologia zapisywalnych dysków CD i DVD jest stosunkowo niedrogim rozwiązaniem, które może posłużyć do wykonywania kopii zapasowych danych zapisanych na dyskach niewielkiego komputera, stosowanego w małym biurze SOHO. Ze względu na to, że pojemność dysków twardych jest wyrażana w gigabajtach, natomiast zapisywalnych dysków CD-R w megabajtach, powinno się je stosować w przypadku niewielkiej sieci firmowej lub domowej, gdzie zależy Ci jedynie na archiwizacji niewielkiej ilości danych. Z kolei na dysku DVD można nagrać 4,7 gigabajta (zapis jednowarstwowy) albo nawet 8,5 gigabajta (zapis dwuwarstwowy), przez co taki dysk lepiej nadaje się do archiwizowania większej ilości danych (co prawda, nie na potrzeby wykonywania pełnej kopii zapasowej dysków twardych, w przypadku których nadal najlepiej sprawdzają się napędy taśmowe).

Dyski wielokrotnego zapisu (RW), użyte do wykonania kopii zapasowej, pozwalają na dodawanie danych, wymazywanie ich i ponowne zastosowanie nośnika. W tym celu należy użyć jednego z wielu dostępnych obecnie na rynku programów służących do nagrywania danych na dyski CD i DVD (Nero Ultra Edition, Easy Media Creator itd.). W systemach Windows XP i Windows Vista można też korzystać z wbudowanych funkcji zapisu płyt CD. Ale oprogramowanie obsługujące te wbudowane funkcje nie jest ani tak wygodne, ani tak proste w obsłudze jak niektóre specjalizowane aplikacje; przede wszystkim zaś wbudowane oprogramowanie Windows XP nie pozwala zapisywać nośników DVD (nagrywarki DVD funkcjonują tak, jakby były nagrywarkami CD). Przy dostępności nagrywarek dwuwarstwowych dysków DVD w cenie poniżej 300 złotych modernizacja posiadanej nagrywarki nie stanowi wyzwania ekonomicznego. A trzeba pamiętać, że nagrywarki płyt DVD radzą sobie świetnie z zapisywaniem płyt CD-R i CD-RW, a do niektórych urządzeń tej klasy dołączane jest gotowe oprogramowanie do archiwizacji danych.

Ostatnio środkiem archiwizacji danych jest coraz częściej zewnętrzny dysk twardy. Wielu producentów oferuje takie dyski, podłączane do komputera za pośrednictwem złączy USB albo IEEE-1394 (niektóre dyski obsługują oba interfejsy). Najnowsze zewnętrzne napędy mają pojemności do 500 GB, a do większości z nich dołączane jest oprogramowanie archiwizujące. Niektóre oferują nawet automatyzację wykonywania kopii zapasowych — inicjuje się je przyciskiem na obudowie dysku zewnętrznego. Takie wykonywanie kopii zapasowych, z utrwalaniem starszych danych na dwuwarstwowych płytach DVD, to niezłe rozwiązanie problemu szybkiego wykonywania częstych kopii w połączeniu z koniecznością długotrwałego ich przechowywania.

Harmonogram wykonywania kopii zapasowych

Zanim zostanie wykonana kopia zapasowa, należy określić, jakie dane wymagają archiwizacji i przez jak długi okres czasu kopie muszą być dostępne na potrzeby operacji przywracania. Jeśli masz do czynienia z ciągle zmieniającym się środowiskiem pracy, w którym dane mające więcej niż kilka tygodni lub miesięcy są już bezwartościowe, nie będzie konieczne długotrwałe przechowywanie danych na taśmach lub innych nośnikach. Jednak w przypadku większości firm duże znaczenie ma możliwość odzyskania danych sprzed wielu miesięcy lub nawet lat, co ma na celu spełnienie określonych przez przepisy prawa wymagań finansowych lub proceduralnych. W takiej sytuacji należy stworzyć odpowiedni do potrzeb harmonogram wykonywania kopii zapasowych.

Można na przykład każdej nocy wykonywać pełną kopię zapasową danych przechowywanych na wszystkich systemach. Można też wykonywać pełną kopię zapasową raz w tygodniu, a w pozostałe dni kopie przyrostowe, czyli zawierające tylko te pliki, które uległy zmianie od czasu wykonywania ostatniej pełnej archiwizacji. Kombinacja pełnej kopii i przyrostowych kopii zapasowych pozwala na przywrócenie systemu do stanu, w którym się znajdował w dowolnej chwili wykonywania archiwizacji.

W tym przypadku, gdy zostanie wykonana kolejna pełna kopia zapasowa, kopie przyrostowe mogą być już niepotrzebne. Dzięki temu można wielokrotnie używać tych samych taśm. Częstotliwość, z jaką taśmy lub inne nośniki danych mogą być ponownie stosowane, jest określana mianem *częstości rotacji*. Ogólnie sprawdzająca się podstawowa procedura archiwizacji (której użycie zależy oczywiście od konkretnego środowiska) polega na cotygodniowym wykonywaniu kopii zapasowej wszystkich danych, a w pozostałe dni tygodnia

— kopii przyrostowych. Taka metoda archiwizacji umożliwia wykonywanie pełnej kopii zapasowej w czasie mniejszej aktywności użytkowników (np. w weekend). Taśmy przeznaczone na kopie przyrostowe mogą być ponownie użyte w kolejnym tygodniu, jeśli poprawnie wykonano pełną kopię zapasową.

Taśmy z pełnymi kopiami zapasowymi wykonywanymi co tydzień mogą być przechowywane przez miesiąc, a następnie ponownie wykorzystywane. Dodatkowo można przez dłuższy okres czasu przechowywać jedną z pełnych kopii zapasowych z danego miesiąca, ale zależy to od Twoich wymagań z tym związanych.

Metoda wykonywania pełnych i przyrostowych kopii zapasowych ma na celu zmniejszenie *okna archiwizacji*. Termin ten oznacza okres, podczas którego działa program archiwizujący, a użytkownicy nie wymagają dostępu do systemu. Jednak ze względu na ciągły wzrost zapotrzebowania na przestrzeń dyskową i całodobowy dostęp do danych można skorzystać z kolejnej technologii, która w takich sytuacjach może być przydatna. Jak już wcześniej w rozdziale wspomniano, w celu przeniesienia magazynów danych z serwerów mogą zostać użyte sieci SAN. Sieci te rozwiązują wiele problemów związanych ze standardowymi urządzeniami SCSI. Po pierwsze, interfejs SCSI pozwala na podłączenie do magistrali ograniczonej liczby urządzeń. Kolejnym ograniczeniem interfejsu jest też niewielka odległość, obsługiwana przez urządzenia SCSI. Sieci SAN pozwalają na podłączenie magazynów danych — zarówno dyskowych, jak i taśmowych — które znajdują się w znacznie większych odległościach od siebie, co nie powoduje zwiększenia czasu dostępu do danych. Sieci SAN mogą też posłużyć do odciążenia procesora serwera od zadań związanych z archiwizacją danych. Sieci SAN mogą zostać użyte do archiwizacji na taśmach danych przechowywanych na dyskach, bez konieczności interwencji serwerów, których ta operacja dotyczy.

Niezależnie od zastosowanej metody archiwizacji należy się upewnić, że spełnia ona wymagania użytkowników i aplikacji, z których oni korzystają. Ponadto należy zastosować określony typ mechanizmu, taki jak baza danych przechowująca informacje o każdej taśmie, dzięki czemu będziesz w stanie wyeliminować taśmę, której użyto już ustaloną liczbę razy. Taśmy magnetyczne zużywają się z każdym kolejnym ich wykorzystaniem i mogą nawet ulec uszkodzeniu, gdy są przechowywane w miejscu, którego temperatura i wilgotność przekraczają wartości graniczne zalecane przez producenta.

Przy użyciu kodów kreskowych lub poprzez zwykłe umieszczanie na taśmach etykiet z numerami seryjnymi można zidentyfikować taśmy w bazie danych i uaktualniać jej zawartość po każdorazowym użyciu taśmy. Kody kreskowe wykorzystywane są jako mechanizm identyfikacji taśm przez zautomatyzowane podajniki, ale warto o nich pomyśleć również wtedy, kiedy zmiana taśm w napędzie archiwizującym wykonywana jest ręcznie. Gdy czas eksploatacji taśmy osiągnął czas określony przez producenta jako maksymalny, to przy użyciu specjalnego narzędzia należy wymazać jej zawartość, tak aby odczytanie danych było niemożliwe, i wyrzucić ją do kosza. Ze względów bezpieczeństwa zaleca się stworzenie firmowej procedury dotyczącej pozbywania się wszystkich materiałów, np. wydruków i taśm. Kto będzie grzebał w Twoim śmietniku? Lepiej być pewnym niż przekazać komuś innemu wartościowe dane, należące do Twojej firmy.

Przechowywanie kopii zapasowej w innej fizycznej lokalizacji

Kopia zapasowa jest przydatna tylko wtedy, gdy jest przechowywana w bezpiecznym miejscu. Jeśli zależy Ci na przywróceniu tylko jednego pliku, ponieważ użytkownik popełnił błąd i usunął go, to — dysponując taśmą przechowywaną w serwerowni — możesz operację tę wykonać szybko i łatwo. Wystarczy umieścić taśmę w napędzie, przywrócić plik, a następnie powiadomić użytkownika. Jednak przechowywanie taśm archiwizujących w tym samym miejscu, w którym znajdują się komputery, nie zawsze jest dobrym rozwiązaniem. Przykładowo w przypadku jakiegokolwiek kataklizmu, takiego jak pożar, takie postępowanie może spowodować, że pozostaniesz bez kopii zapasowej. Zostaną stracone nie tylko komputery, ale również zarchiwizowane dane.

W przypadku danych o dużej wartości nośnik archiwizujący powinien zostać przewieziony do innej fizycznej lokalizacji jak najszybciej po wykonaniu kopii zapasowej. W takiej sytuacji, gdy dojdzie do kataklizmu, taśmy będą bezpiecznie przechowywane w innym miejscu i będą mogły zostać użyte do przywracania danych przy użyciu awaryjnego sprzętu lub po wymianie zniszczonego wyposażenia firmy.

Jakie są wymagania związane z przechowywaniem kopii w innej fizycznej lokalizacji? W zależności od potrzeb można przechowywać kopie zapasowe w kilku miejscach. Zastanów się najpierw, jak bezpieczne jest dodatkowe miejsce przechowywania kopii zapasowej, a następnie ile czasu będzie wymagane na dostarczenie nośnika archiwizującego. Na końcu należy określić koszt takiego rozwiązania. Oto kilka propozycji dodatkowych miejsc przechowywania:

- Skorzystaj z oferty firmy, która zajmuje się odbieraniem, przechowywaniem i dostarczaniem nośników archiwizujących. Istnieje wiele firm specjalizujących się w tym. W celu sprawdzenia, czy warunki oferowane przez wybraną firmę są odpowiednie do długotrwałego przechowywania wrażliwych nośników archiwizujących, należy osobiście się do niej wybrać. Poprzez zażądanie w różnych terminach próbnego dostarczenia taśm sprawdź, czy spełniany jest zadeklarowany czas reakcji. Upewnij się, że firma oferuje 24-godzinny dostęp do Twoich danych.
- Jeśli w przypadku wystąpienia jakiegoś kataklizmu będziesz korzystał z usług firmy udostępniającej awaryjne pracownie, może ona zaoferować również przechowywanie nośników archiwizujących w swoich pomieszczeniach. Dzięki temu w razie sytuacji awaryjnej można zaoszczędzić czas, ponieważ przed uaktywnieniem zapasowego środowiska roboczego nie będzie konieczne sprowadzanie taśm z innego miejsca.
- Jeśli pracujesz w dużej firmie, to praktyczniejsze może być przechowywanie nośników archiwizujących w jej innym oddziale. Pod uwagę powinna być brana szansa wystąpienia kataklizmu jednocześnie w kilku miejscach, a także warunki przechowywania w innej lokalizacji. Przykładowo jeśli oddziały znajdują się blisko siebie, może nie być to dobrym pomysłem — naturalny kataklizm, taki jak huragan lub powódź, mogą spowodować zniszczenie obu miejsc. Należy też uwzględnić koszt regularnego przesyłania taśm do innego oddziału firmy. Może się okazać, że tańsze będzie wynajęcie specjalistycznej firmy zajmującej się przechowywaniem taśm niż angażowanie pracowników w przewożenie ich z jednego oddziału do innego.

- Weź nośnik kopii albo zewnętrzny dysk twardy do domu i schowaj go pod łóżkiem. To nie jest żart! Miałem okazję pracować w niewielkiej firmie, w której menedżer ds. systemów zabierał comiesięczną kopię zapasową do domu i tam, pod łóżkiem, przechowywał ją do następnego miesiąca. To samo dotyczy małego biura prowadzonego w domu. Należy wziąć pod uwagę możliwość umieszczania cotygodniowej lub comiesięcznej taśmy z kopią zapasową w skrzynce depozytowej w lokalnym banku i traktować to jako metodę przechowywania danych w innym miejscu. Celem takich działań jest uzyskanie pewności, że dane są przechowywane z dala od systemu, na którym się znajdują. Dzięki temu zmniejsza się ryzyko wystąpienia kataklizmu, który zniszczy zarówno komputery, jak i kopie zapasowe zapisanych na nich danych.

Regularna konserwacja

Co prawda w rozdziale tym skupiłem się przede wszystkim na metodach zapobiegania zagrożeniom, ale ważne jest też regularne wykonywanie konserwacji komputerów i urządzeń sieciowych. Tego typu konserwacja zapobiega występowaniu awarii sprzętowych, spowodowanych intensywnie eksploatowanym lub przestarzałym sprzętem, który się psuje. Oto przykład: ponieważ wszystkie komputery — począwszy od niewielkich stacji roboczych, a skończywszy na dużych systemach montowanych w szafach — w celu zagwarantowania swobodnego przepływu powietrza wewnątrz systemu zapobiegającego przegrzaniu układów używają wentylatorów, to dodatkowo co jakiś czas powinno się sprawdzać, czy kurz i inne zanieczyszczenia nie są zasysane do środka obudowy i czy dzięki ładunkom elektrycznym nie przyczepiają do podzespołów.

Raz lub dwa razy w ciągu roku warto zdjąć obudowę i przy użyciu skompresowanego powietrza usunąć wszelkie zanieczyszczenia. Jest to zalecana metoda zapobiegawcza. W przypadku biura prowadzonego w domu dość łatwo o tym zapomnieć. Jeśli w domu znajduje się osoba paląca, to na przykład po jakimś czasie możesz stwierdzić, że dym papierosów może przyczynić się do powstania cienkiej warstwy kurzu nagromadzonego na komponentach komputera. Z własnego doświadczenia wiem, że powodem tego może też być kocia sierść. Co jakiś czas zdejmuj obudowę komputera. Zdejmij ją teraz i zajrzyj do środka, a następnie usuń brud. Nawet większe serwery, które znajdują się w zamkniętym pomieszczeniu, mogą wymagać czyszczenia co jakiś czas. Niezależnie od stopnia czystości pomieszczenia z komputerami należy sprawdzić, jaka ilość kurzu gromadzi się po upływie pewnego okresu czasu. Możesz być tym zaskoczony. Jest to jeden z problemów posiadania serwerowni, do której nikt nie zagląda. Warto więc od czasu do czasu odwiedzić takie pomieszczenie i skontrolować sytuację. Zawsze najlepiej wykryć problem, zanim w poważnym stopniu wpłynie on na używany sprzęt.

Napędy taśmowe wymagają okresowego czyszczenia, ponieważ taśma magnetyczna styka się z głowicami znajdującymi się wewnątrz urządzenia. Taśma czyszcząca powinna być stosowana z częstotliwością zalecaną przez producenta. Napędy taśm DLT zazwyczaj są wyposażone we wskaźnik świetlny, który zapala się, gdy na głowicy nagromadzi się taka ilość zanieczyszczeń, która może powodować występowanie błędów zapisu i odczytu. Jeśli taśma czyszcząca musi być używana częściej niż zaleca to producent, może się okazać

konieczne sprawdzenie, jakie taśmy były używane, zanim taki problem się pojawił. Możesz być w posiadaniu zużytej taśmy albo nawet napędu taśmowego, który należy ponownie skalibrować lub wymienić.

Tworzenie nadmiarowości w sieci

Bez znaczenia będzie rodzaj umowy serwisowej podpisanej z producentem, jeśli na sprowadzenie części zamiennych lub nowych urządzeń w miejsce uszkodzonych będzie on potrzebował wielu godzin lub dni. Z tego też powodu warto już na etapie projektowania zapewnić sieci nadmiarowość. Przykładowo jeśli awarii ulegnie router, to dodatkowa ścieżka sieci umożliwi użytkownikom uzyskanie w dalszym ciągu dostępu do wymaganych przez nich danych. W celu maksymalizacji dostępności systemów o dużym znaczeniu można zastosować serwery wyposażone w nadmiarowość bazującą na technologii klastrów.

◄◄ W rozdziale 2. — „Przegląd topologii sieciowych" — zawarto godne uwagi omówienie zastosowania topologii częściowej siatki, która może posłużyć do wyposażenia sieci w nadmiarowość. Zobacz punkt „Topologia siatki", a także podrozdziały „Tworzenie sieci wielosegmentowej i stosowane topologie" i „Topologia sieci wielowarstwowej".

Jeśli nie dysponujemy wystarczającą ilością czasu przeznaczoną na wymianę sprzętu (w porównaniu z kosztem związanym z opłacaniem użytkowników nie mogących wykonywać swoich zadań, kosztami powierzchni biurowej itp.), wartym rozważenia jest posiadanie na miejscu zapasowych urządzeń, które będą mogły szybko zastąpić ich uszkodzone odpowiedniki. W przypadku routera lub przełącznika operacja wymiany uszkodzonego urządzenia jest prosta. W tym celu należy — zgodnie z wcześniej przygotowaną szczegółową procedurą — dokonać ponownej konfiguracji, co pozwoli ponownie udostępnić sieć.

Planowanie przywracania pracy sieci

W sytuacji awaryjnej nic nie jest bardziej wartościowe (poza kopią zapasową) niż dobrze przemyślany plan przywracania pracy sieci. Tak naprawdę jest to ogólne określenie, ponieważ należy przygotować plany dotyczące awarii sieci lub serwera — począwszy od uszkodzenia pojedynczego dysku, poprzez niedostępność systemu komputerowego, a skończywszy na awarii całej sieci. W rozdziale 3. — „Strategie projektowania sieci" — zwrócono uwagę na to, że zawsze należy tworzyć dokumentację sieci i jej komponentów. W skład takiej dokumentacji powinny wchodzić procedury przywracania pracy sieci.

Cały problem z kataklizmami polega na tym, że nie można ich przewidzieć. Nie zawsze mają one miejsce w czasie normalnych godzin pracy, gdy jesteś w pełnej gotowości i sprawności. W środku nocy, po ciężkim dniu pracy, możesz zostać wezwany do przywracania systemu, co oznacza, że czeka Cię nieprzespana noc. Dobry plan przywracania pracy sieci po awarii jest przydatny dlatego, że dzięki niemu w trakcie całej operacji nie popełnisz błędów.

Dobry plan przywracania pracy sieci powinien uwzględniać następujące elementy:

- Dane kontaktowe pracowników, którzy będą odpowiedzialni za wykonywanie operacji przywracania oraz personelu, który powinien zostać o tym poinformowany. Należy tu wspomnieć o przedstawicielach klientów korzystających z przywracanego systemu. Pamiętaj o uaktualnianiu tego typu informacji.
- Dane kontaktowe producentów — zarówno sprzętu, jak i oprogramowania wchodzącego w skład systemu lub sieci. Należy w nich uwzględnić numery telefonów pomocy technicznej oraz dane kontaktowe pracowników lokalnego oddziału, którzy mogą być potrzebni przy odbudowie systemu i usuwaniu awarii.
- Szczegółowe procedury umożliwiające wyjście z sytuacji awaryjnej. Swoim zakresem mogą one obejmować całkowitą przebudowę określonego systemu poprzez ponowną instalację systemu operacyjnego i przywrócenie danych z kopii zapasowej zapisanej na taśmie. Plan przywracania pracy sieci powinien zawierać konfigurację routerów i innych urządzeń.
- Po usunięciu skutków kataklizmu zgodnie z opracowanym planem konieczne jest przeprowadzenie na systemie operacyjnym, urządzeniach i aplikacjach zestawu testów, mających na celu sprawdzenie, czy operacja przywracania pracy sieci została wykonana poprawnie.

Szacowanie kosztu metod ochrony

Niektóre z metod omówionych w niniejszym rozdziale są kosztowne. Z tego też powodu możesz mieć problemy z uzyskaniem od kierownictwa środków finansowych na ich zastosowanie. Aby sobie poradzić w takich sytuacjach, można wykonać kilka czynności.

Należy pamiętać o dokumentowaniu wszystkich przestojów każdego systemu znajdującego się w sieci i próbować określić ich koszt. Co prawda możesz nie być w stanie uzyskać informacji pozwalających określić, jaki wpływ przestoje mają na użytkowników, ale zazwyczaj jest możliwe ustalenie liczby tych przestojów. Zakładając, że użytkownicy pozbawieni dostępu do komputera lub sieci są w stanie wykonywać tylko pewien procent swoich codziennych obowiązków, spróbuj ustalić liczbę godzin straconych na skutek przestoju i pomnożyć ją przez średnią stawkę godzinową pracowników, którzy przez to ucierpieli. Najprawdopodobniej nie będziesz miał dostępu do wysokości stawek godzinowych innych pracowników. Jednak można sobie z tym poradzić poprzez pomnożenie liczby godzin przez minimalną średnią stawkę godzinową, a następnie — w przypadku uzyskania znacznej kwoty — poinformować o tym kierownictwo. Należy wspomnieć, że przy obliczeniach bazowano na minimalnej stawce. Ze względu na to, że osoby z kierownictwa najprawdopodobniej będą znały średnie zarobki używających komputera pracowników z dużym stażem, przekazany im wynik nadal będzie wiarygodnym oszacowaniem kosztu przestoju. Innymi słowy, jeśli w wyniku obliczeń opartych na stawce minimalnej uzyska się sporą wartość, to osoby z kierownictwa szybko dojdą do wniosku, że rzeczywista wartość będzie znacznie wyższa, dlatego też możesz liczyć na uzyskanie środków potrzebnych na zastosowanie metod zapobiegawczych.