POLITECHNIKA CZĘSTOCHOWSKA

WYDZIAŁ INŻYNIERII MECHANICZNEJ I INFORMATYKI

LOKALNE I ROZLEGŁE SIECI KOMPUTEROWE

„ADMINISTRACJA I BEZPIECZEŃSTWO SIECI”

W.I.M. i I. Informatyka
Rok IV gr. VI
Puchała Marcin
Piech Jarosław

Obowiązki administratora:

1. Czynności wstępne:
    - wybór bazy sprzętowej
    - instalacja i konfiguracja serwera na bazie sieciowego systemu operacyjnego – np. Linux
    - określenie warunków łącza internetowego
    - założenie sieci komputerowej - wybór rodzaju sieci oraz konfiguracja urządzeń sieciowych
    - konfiguracja stacji roboczych
    - zapewnienie zdalnego dostęp do sieci firmowej
    - instalacja programów użytkowych

2. Czynności administracji ciągłej:

    - zarządzanie kontami użytkowników, uprawnienia
    - system haseł
    - bezpieczeństwo w dostępie do internetu, firewalle
    - ochrona antywirusowa
    - sprawdzanie logów systemowych
    - aktualizacja oprogramowania pod kątem bezpieczeństwa sieci i serwera (kompilacja jądra systemu)
    - monitoring i nadzorowanie pracy sieci
        - kontrola platformy sprzętowej
        - kontrola platformy programowej
    - backup danych

3. Prawa Administratorów:

        - aktywowanie bądź dezaktywowanie usług dodatkowych
        - dostęp do wszystkich urządzeń sieciowych
        - dbanie o zgodność z prawem oraz normami moralnymi treści udostępnianych przez Członków sieci za pomocą serwerów
        - blokowanie dostępu do sieci Internet bądź usług dodanych w przypadku naruszenia przez Członków sieci Regulaminu
          a w szczególności w przypadku zalegania z opłatami (dotyczy głównie sieci akademickich i blokowych)

I. Zarządzanie kontami użytkowników, uprawnienia

Zadaniem każdego administratora jest zarządzanie kontami użytkowników. Do zadań administratora należy dodawanie nowych użytkowników, usuwanie nieaktualnych, zmiana haseł, zmiana uprawnień (w zależności od potrzeb), przydzielanie użytkowników do poszczególnych grup.
Konto jest to nic innego jak zbiór danych użytkownika znajdujący się w katalogu domowym lub rozproszonej bazie danych. Każde konto jest dostępne pod unikalną nazwą, którą podajemy podczas logowania. Fakt ten sprawia, że poszczególni użytkownicy nie wchodzą sobie w drogę i nie mogą odczytywać danych nie należących do nich (chyba, że właściciel plików lub root zadecyduje inaczej). Najważniejszym kontem w systemie jest oczywiście konto root, które jest tworzone podczas instalacji.

Podstawowe uprawnie to: zapis, odczyt, uruchamianie. Uprawnienia należy nadawać poszczególnym użytkownikom według określonych zasad. Jedną z zasad jest nadawanie minimalnych uprawnień i zwiększanie ich w zależności od potrzeb.

II. System haseł

System haseł jest najpopularniejszym sposobem identyfikacji i potwierdzania użytkownika w systemie komputerowym. Jest on szeroko stosowany zarówno w klasycznych systemach wielodostępnych jak i sieciowych systemach odległego dostępu. Ogólnie metoda ta pozwala stwierdzić, że użytkownik wydaje się być tym za kogo się podaje. O ile w przypadku systemów wielodostępnych, bazujących na klasycznych terminalach znakowych (łącza szeregowe), systemy haseł są stosunkowo bezpieczne o tyle w środowisku sieciowym są one bardzo proste do złamania.

- Istnieje możliwość łatwego nasłuchiwania połączenia sieciowego w celu pozyskania kombinacji identyfikator-hasło. Sztandarowym przykładem jest telnet. Odpowiednie programy typu LanWatch, IPtrace czy snoop są prostym narzędziem pozwalającym odczytać hasło. Klasyczne połączenie telnet nie jest bowiem kodowane i hasło wprowadzane jest do sieci „żywym" tekstem.
- Najprostszym sposobem pozyskania haseł jest zainstalowanie na swoim własnym koncie konia trojańskiego udającego pracę programu login (np. w UNIX). Program ten może być napisany w klasycznym shell-u i - jak to czyni system operacyjny - prosić o identyfikator i hasło. Dane te są zapamiętywane na dowolnym pliku, a następnie program wyświetla informację o niepoprawnej kombinacji identyfikator-hasło i wywołuje normalny program login. Użytkownik niczego nie podejrzewając rozpoczyna logowanie na terminalu a po komunikacie o błędzie uznaje, że się pomylił. Jego hasło jest już na pliku „złośliwego kolegi".
- Typowym sposobem łamania haseł jest tzw. „Dictionary Attack" (atak poprzez słownik). Polega on na próbkowaniu programu autoryzującego całym słownikiem danych. Jeżeli weźmiemy pod uwagę, że w przypadku klasycznego systemu UNIX maksymalna długość hasła wynosi 8 znaków, a funkcja haszująca używa tylko siedmiu bitów znaczących otrzymujemy klucz o długości 56 bitów. Ponieważ większość użytkowników stosuje „normalne" hasła, pole poszukiwań może być zawężone tylko do np. małych liter - odpowiada to sytuacji używania klucza o długości 19 bitów. Tego typu hasła są dość łatwe do złamania za pomocą słowników. Przykładem ataku poprzez słownik jest program COPS (Computer Oracle Password and Security), który używa tej metody do diagnozowania skuteczności zabezpieczeń poprzez hasła.
- Użytkownicy grup roboczych bardzo często pożyczają hasła koledze, a ci skrzętnie je zapisują np. na karteczkach przyklejonych do terminala. W takim przypadku nie

istnieje potrzeba stosowania żadnych specjalnych technik hakerskich - wystarczy umieć czytać.

Istnieją oczywiście techniki pozwalające pracować z hasłami w sposób bardziej bezpieczny. Do najpopularniejszych z nich należą:

- W przypadku sporadycznych połączeń z odległymi komputerami stosowana jest technika ważności hasła tylko dla jednego połączenia Zakłada się, że przy nawiązywaniu łączności hasło zostanie podsłuchane i dlatego przed opuszczeniem odległego systemu użytkownik zobowiązany jest do zmiany swojego hasła.
- Wiele systemów operacyjnych ma możliwość narzucenia użytkownikom odpowiedniej polityki haseł. Co pewien okres czasu hasła ulegają przedawnieniu i użytkownik zmuszany jest do wprowadzenia nowego hasła. System wymaga stosowania odpowiednio ważonej kombinacji liter i znaków specjalnych. Administrator ma także możliwość przedawniania ważności kont (haseł).
- Bardzo bezpiecznym mechanizmem haseł są karty magnetyczne weryfikujące dostęp. Wygenerowane hasła charakteryzuje bardzo trudna do złamania kombinacja i odpowiednia długość (użytkownik nie musi pamiętać hasła - musi mieć kartę). Rozwiązania te są powszechnie stosowane np. w bankach i jak się można domyślać nie należą do najtańszych.
- Systemy jednokrotnych haseł. W systemach o hierarchicznej, protegowanej strukturze dostępu użytkownik może być zmuszony do ustalenia dużej ilości haseł w zależności od typu danych i aplikacji. Doprowadza to do ironicznej sytuacji, w której duża ilość haseł staje się niebezpieczna w użyciu. Wyobraźmy sobie użytkownika, który musi korzystać z 50 haseł - musi on je gdzieś zapisać, a w takim przypadku jedno hasło gwarantujące dostęp do różnych elementów i aplikacji systemu jest na pewno bezpieczniejsze.
- Systemy haseł jednokrotnego użycia należą do jednych z najbardziej technologicznie zaawansowanych rozwiązań. Szeroko stosowanym przekładem tej metody są karty mikroprocesorowe SecurID opracowane przez Security Dynamics. Każdy użytkownik posiada swoją kartę (małe urządzenie elektroniczne), która generuje hasło - weryfikowane przez dedykowany serwer - na podstawie tzw. PIN-u (stałego identyfikatora). Hasło ważne jest przez okres tylko 60-ciu sekund.

III. Bezpieczeństwo w dostępie do internetu, firewalle

Bezpieczeństwo w dostępie do netu

Nawet najlepsze oprogramowanie czy sprzęt nie uchronią naszych zasobów jeżeli nie będziemy zdawać sobie sprawy z tego co i przed czym chcemy chronić.
Bezpieczeństwo jest bardzo drogie, bowiem straty mogą być bardzo duże. Jednakże w wielu przypadkach może okazać się, że zastosowanie podstawowych zasad bezpieczeństwa jest niemalże wystarczające dla spełnienia naszych założeń polityki bezpieczeństwa.

Dlaczego nasza sieć potrzebuje zabezpieczeń?

Jako nowoczesna firma, dostrzegająca wagę i korzyści płynące z prowadzenia działalności w sieciach publicznych, podłączamy się do Internetu. Zamykamy wszystko na „potężne klucze" i idziemy spokojnie spać. Czy aby jednak nie zostawiliśmy otwartego okna - naszego podłączenia do Internet?

Większość przestępstw komputerowych związanych z włamaniami do systemów komputerowych nie jest raportowana - trochę „ze wstydu", trochę z bojaźni przed utratą wiarygodności i prestiżu. Statystyki są jednak alarmujące:

- Zgodnie z CERT NASK w okresie 03.96 - 09.96 7% komputerów w polskim Internecie było próbkowanych pod względem możliwości realizacji włamania. Na nasze szczęście tylko ok. 1% z tych komputerów uległ udanemu atakowi hakerów. Dane dotyczą oczywiście tylko zgłoszonych wydarzeń (incydentów). Najczęściej spotykanymi typami ataków były próby wykorzystania:
  - słabości wynikających z mechanizmów stosowanych w systemach rozproszonych takich jak NIS;
  - „słabe hasła";
  - słabości protokołu HTTP stosowanego w serwerach WWW;
  - „dziury" w oprogramowaniu systemowym (najczęściej sendmail).

Co możemy stracić? - w gruncie rzeczy zależy kim lub czym jesteśmy.

- Możemy przyjść rano do pracy i zobaczyć, że nas serwer Internetu znajduje się w stanie inicjacji początkowej z dość zaskakującym komunikatem „missing operating system" i nasze połączenie ze światem jest nieczynne.
- Możemy także pozbyć się centralnej bazy haseł i nikt nie będzie mógł podłączyć się do serwera.
- Możemy stracić dane związane z „tajnym projektem" lub udostępnić włamywaczowi konta naszego banku do dowolnej dyspozycji.

Niektóre elementy bezpieczeństwa sieciowego

- Najbardziej oczywistym sposobem ochrony naszych zasobów jest po prostu ochrona fizyczna wrażliwych elementów naszego systemu komputerowego takich jak np. pomieszczenie, w którym pracuje serwer, czy stacja robocza administratora sieci. Nigdy nie zakładajmy, że nikt poza jednym guru nie zna się na skomplikowanych poleceniach.
- Następny poziom zabezpieczeń to bezpieczeństwo systemu operacyjnego. Często słyszymy, że systemy takie jak UNIX czy Microsoft Windows NT uzyskały certyfikat klasy C2. Oznacza to, że systemy te wyposażono w mechanizmy kontroli dostępu, gwarantowania zezwoleń na czytanie i zapis kartotek oraz plików przez określonych użytkowników oraz notowanie (auditing) dostępów i autoryzacji.

Poziomy bezpieczeństwa - Orange Book

W dokumencie „Trasted Computer Standards Evaluation Criteria", znanym także jako „Orange Book", Departament Obrony USA zdefiniował siedem poziomów bezpieczeństwa komputerowego systemu operacyjnego. Klasyfikacja ma charakter „zawierania" (wyższe poziomy mają wszystkie cechy poziomów niższych).

- **D1** Najniższy poziom bezpieczeństwa
- **C1**
- **C2** Poziom ten gwarantuje automatyczne rejestrowanie wszystkich istotnych - z punktu widzenia bezpieczeństwa - zdarzeń i zapewnia silniejszą ochronę kluczowych danych systemowych takich jak np. baza danych haseł użytkowych.
- **B1**
- **B2**
- **B3**
- **A1** Jest to najwyższy poziom bezpieczeństwa.

Bezpieczne IP

Jedną z metod próby globalnego zabezpieczenia transmisji w sieciach bazujących na protokole TCP/IP jest tzw. IP Security lub IP Sec, która de facto jest zbiorem protokołów opracowanych przez IETF (Internet Enginnering Task Force) a udokumentowanym w RFC 1825-1829.

Standard ten gwarantuje autentyczność, prywatność i integralność danych działając na poziomie jądra IP. Niewątpliwą zaletą takiego rozwiązania jest zatem jego skuteczność w odniesieniu do każdej aplikacji sieciowej, niezależnie od tego, czy jest to poczta elektroniczna czy telnet. IP Sec zdefiniowano dla IPv4 (aktualnie stosowanego systemu adresowania IP), ale włączono go jako standardową własność do IPv6.

Wdrożenie IP Sec polega na używaniu dwu opcjonalnych nagłówków IP:

- AH - Authentication Header, dedykowany do stwierdzania autentyczności i integralności danych,
- ESP - Encapsulating Security Payload zapewniający prywatność (szyfrowanie).

Nagłówki mogą być używane rozłącznie albo wspólnie w zależności od potrzeb.
Specyfikacja IPS Sec umożliwia komunikującym się stronom na uzgodnienie odnośnych parametrów (mechanizm identyfikacji, algorytm szyfrowania, klucz, czas ważności połączenia, etc.), na bazie odpowiedniego pola w nagłówkach IP, tzw. SPI (Security Parameter Index). Dzięki temu istnieje możliwość ominięcia wszelkich restrykcji eksportowych USA, bowiem zamiast standardowego szyfrowania DES można uzgodnić np. 40-bitowy RC4. Jedynym nie ustalonym parametrem IP Sec jest sposób dystrybucji kluczy. Aktualna propozycja wskazuje na tzw. ISA Key Management Protocol (ISAKMP, Oalkey), ale na obecnym etapie używane są „ręczne" sposoby wymieniania kluczy. Jak dotąd jedynym komercyjnym pakietem posiadającym wdrożenie IP Sec i IPv6 jest OnNet32 for Windows z FTP Software.

„Firewall'e - Ściany ognia"
Systemy firewall chronią naszą sieć na kilku poziomach, a także umożliwiają wdrożenie zupełnie nowych własności:

- Użytkownicy wewnętrzni mogą mieć dostęp do wszystkich (lub wybranych) usług Internet, natomiast użytkownicy zewnętrzni nie będą mieli dostępu do jakiegokolwiek zasobu naszej sieci lokalnej.
- Usługi takie jak e-mail, ftp, WWW mogą być dozwolone dla ruchu zewnętrznego tylko w odniesieniu do specyficznego komputera. Daje to nam otwartość na świat jednocześnie chroniąc i ukrywając inne zasoby sieciowe.
- Zaawansowane systemy identyfikacji i kontroli tożsamości są skuteczną metodą zabezpieczenia określonych zasobów przed nieupoważnionym dostępem zarówno w odniesieniu do użytkownika jak i aplikacji. Często istnieje możliwość połączenia procesu identyfikacji z systemami kart elektronicznych (np. SecurID).
- Wszystkie wydarzenia są bardzo detalicznie monitorowane i rejestrowane, a niektóre z nich generują natychmiastowe alarmy.
- Pakiety mogą podlegać badaniu jeszcze przed ich pojawieniem się w systemie operacyjnym. Są niejako zdejmowane wprost z karty sieciowej. Jeżeli nie spełniają zasad polityki bezpieczeństwa są natychmiast odrzucane.
- Zawierają mechanizmy ukrywania adresów IP komputerów chronionej sieci lokalnej, tłumaczenia adresów IP (np. niepoprawnych adresów Internet na poprawne) lub translacji grupy wewnętrznych adresów IP do jednego lub kilku adresów zewnętrznych. Daje to m.in. wielkie możliwości podłączenia dużych sieci lokalnych do Internet z wykorzystaniem tylko jednego, przydzielonego nam adresu IP.
- Wiele systemów ma możliwość konstrukcji wirtualnych sieci prywatnych - VPN (Virtual Private Network), opartych na metodach szyfrowania transmisji danych. Oznacza to, że możemy utworzyć swoją sieć prywatną na bazie publicznych mediów takich jak Internet. Pozwala to np. łatwo połączyć różne, odległe oddziały firmy w jedną bezpieczną sieć. Niekiedy istnieje możliwość kodowania tylko niektórych typów

usług (jak np. telnet) pozostawiając inne w normalnej postaci, co pozwala utrzymać efektywność całego systemu.

Każdy system firewall wprowadza oczywiście pewne obciążenie i obniża efektywność pracy.

Sposób realizacji danego firewall'a zależy głównie od jego sposobu działania, możemy tutaj wyróżnić dwa główne typy firewall'i :

- zapory sieciowe na poziomie sieci\pakietu (filtry pakietów)
- zapory sieciowe na poziomie aplikacji\usługi (bramy pośredniczące, proxy)

Zapory sieciowe na poziomie sieci (filtry pakietów)

Działają na najniższym poziomie czyli na pakietach IP. Firewall`e te korzystają z danych dostępnych w każdym pakiecie IP, czyli :

- adres źródłowy
- adres przeznaczenia
- numer protokołu
- numer portu źródłowego
- numer portu przeznaczenia
- zawartość pakietu
- typ pakietu

Najczęściej filtrowanie pakietów wykonywane jest na poziomie routerów z funkcjami filtrowania.

Do zalet firewall`i filtrujących można zaliczyć :

- niezależność od systemu i aplikacji - do korzystania z firewall`a nie jest konieczna specjalna konfiguracja stacji roboczych
- zabezpieczenie przed podszywaniem i atakami odmowy obsługi - zaawansowane firewalle filtrujące mogą zabezpieczać przed atakami tego typu
- duża łatwość stosowania - wystarczy podłączyć i zdefiniować reguły
- jeśli sieć jest podłączona łączem stałym router i tak jest niezbędny więc utworzenie z niego firewall`a jest rozwiązaniem tanim i naturalnym - cały ruch musi przejść przez router (i firewall jednocześnie)
- możliwe jest ukrycie sieci wewnętrznej przed światem zewnętrznym za pomocą translacji adresów (NAT)

Oprócz zalet firewall`e filtrujące mają swoje wady :

- w przypadku zdefinowania dużej ilości szczegółowych reguł filtrowania przy małej mocy obliczeniowej routera przy dużym natężeniu ruchu może spaść jego wydajność
- niektóre routery są podatne na atak podszywania
- niezbędne jest dokładne zdefiniowanie usług, które mamy przepuszczać oraz tych, które chcemy odrzucić.

Zapory sieciowe na poziomie aplikacji\usługi (bramy pośredniczące, proxy)

W przypadku firewall'i działających na poziomie aplikacji następuje całkowite oddzielenie sieci wewnętrznej od zewnętrznej na poziomie aplikacji. Każda aplikacja, która chce połączyć się z wewnątrz sieci ze światem zewnętrznym łączy się z firewall'em, który wykonuje dopiero połączenie z danym adresem na zewnątrz sieci chronionej (do Internetu). Na zewnątrz nie jest przekazywana żadna informacja o nadawcy pakietu, firewall wykonuje połączenie ze swoim adresem IP uruchamiając własnego klienta danej usługi i dostarczając zwróconych danych do programu klienta wewnątrz sieci, który żądał połączenia.

Zaletami takiego firewall'a są

- większa kontrola nad poszczególnymi usługami
- zapewnia doskonałe bezpieczeństwo pod warunkiem poprawnej konfiguracji

- możliwość buforowania danych na firewall'u (np. stron www) pozwalające na znaczne przyspieszenie dostępu do często używanych danych

Wśród wad firewall'i działających na poziomie aplikacji należy wymienić :

- konieczność skonfigurowaniu aplikacji proxy dla każdej usługi sieciowej (FTP, telnet, HTTP, mail)
- konieczność skonfigurowania każdej stacji klienckiej
- korzystanie z aplikacji obsługujących funkcję proxy, co czasami może powodować konieczność zmian w oprogramowaniu i przystosowaniu go do obsługi firewall'a

IV. Ochrona antywirusowa

Zagrożenie wirusami i korporacyjne systemy antywirusowe

Z roku na rok rośnie liczba wirusów komputerowych oraz innych złośliwych tworów takich jak konie trojańskie czy też robaki internetowe. Spowodowane jest to:

- wzrostem popularności technik komputerowych,
- szerokim dostępem do nich,
- łatwą wymianą wiedzy na temat wirusów
- popularnością wirusów pisanych w językach wysokiego poziomu
- Internet, który jest obecnie najpopularniejszym medium wymiany informacji, a jednocześnie jest najczęstszą drogą ataków.

Szalejący w 2000 r. Love Bug, z jego 50 odmianami, był jak dotąd najdroższym wirusem. Jego koszt szacuje się na 8,7 mld USD. W 1999 r. najwięcej kłopotów przysporzył firmom wirus Melissa (1,2 mld USD strat) i Explorer (1 mld USD strat). Koszty utraconych korzyści, kalkulowane do całkowitych strat związanych z wirusem, są jednak znacznie większe.

Od pewnego czasu eksperci zajmujący się wirusami komputerowymi ostrzegają przed rosnącym niebezpieczeństwem wynikającym z możliwości infekcji komputerów poprzez odwiedzenie strony WWW. Zarażenie wirusem odbywa się poprzez uruchomienie kodu ActiveX lub Java i z powodu łatwości dostępu do stron WWW jest rzeczywiście poważnym zagrożeniem.

Kolejnym, coraz bardziej popularnym zagrożeniem są wirusy rozsyłane w załącznikach poczty. Ich popularność i łatwość rozprzestrzeniania się (najczęstszą formą działania tych wirusów jest właśnie rozsyłanie samego siebie do adresatów z książki adresowej programu pocztowego) w połączeniu z niską świadomością użytkowników powoduje olbrzymie zagrożenie.

Na szczęście, w walce z wirusami możemy wykorzystać wiedzę i doświadczenie firm, które tworzą oprogramowanie antywirusowe. O tym, że posiadanie takiego oprogramowania jest obecnie niezbędne przekonujemy się zwykle po pierwszym zdarzeniu, kiedy w wyniku niszczycielskiej działalności wirusa tracimy dane czy też zaufanie partnerów.

W zależności od zastosowania, programy antywirusowe możemy podzielić na jednostanowiskowe (do użytku domowego i w bardzo małych firmach) oraz oprogramowanie korporacyjne (wyposażone w rozbudowane możliwości skalowania oraz centralnego zarządzania), które właściwie można nazwać *systemem antywirusowym*. Niezależnie od zastosowania, dobry program/system antywirusowy powinien posiadać następujące cechy:

- Możliwość uaktualniania bazy wzorców wirusów - od tego zależy, czy oprogramowanie jest w stanie wykryć i usunąć najświeższe, krążące w sieci wirusy,
- Możliwość automatycznej aktualizacji silnika wyszukującego (search engine) a nawet całego oprogramowania,
- Skanowanie nie tylko pamięci komputera, plików na dysku, początkowych sektorów dysku (boot sector) ale również zawartości przesyłek pocztowych, czy też ruchu HTTP,
- Ciągle aktywny monitor - rezydentny program który skanuje wszystkie pliki otwierane podczas pracy z systemem komputerowym, np.: pliki na dysku i dyskietkach, pliki na

dyskach sieciowych, załączniki poczty, pliki ściągane ze stron WWW czy też przy użyciu FTP.

W korporacyjnych systemach antywirusowych, kluczową rolę odgrywa możliwość centralnego zarządzania systemem antywirusowym:

- rozsyłania uaktualnień,
- gromadzenia logów,
- monitorowanie aktywności,
- zdalnego uruchamiania skanowania dysków

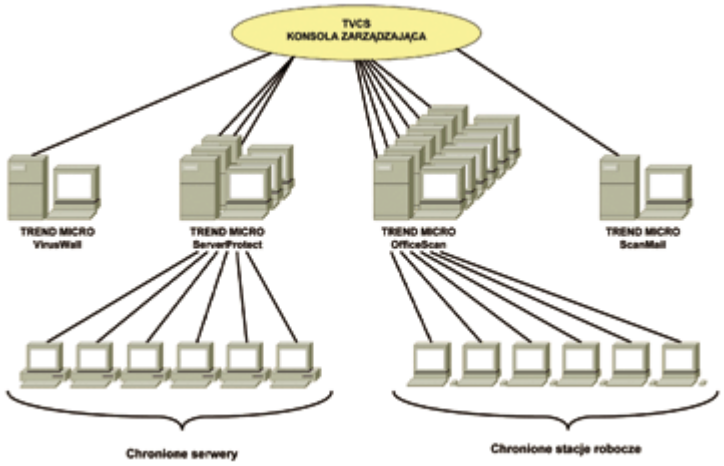
Wsparcie producenta oprogramowania - możliwość wysłania pliku do zespołu profesjonalistów, którzy są w stanie usunąć wirusa; szybkie pojawianie się nowych baz wzorców wirusów; bezpieczeństwo inwestycji czyli gwarancja otrzymywania aktualizacji baz wirusów i oprogramowania.

Opis możliwości na przykładzie systemu antywirusowego firmy **Trend Micro.**

Posiada ono modularną budowę oraz duże możliwości skalowania które można zastosować do budowy kompletnego systemu ochrony antywirusowej zarówno w małej firmie jak i w wielooddziałowej, rozbudowanej korporacji.

Firma Trend Micro posiada w swej ofercie również programy umożliwiające filtrowanie poczty pod względem występowania określonych słów kluczowych, zarządzające dostępem do stron WWW oraz blokowaniem dostępu do określonych grup stron oraz oprogramowanie służące do blokowania niebezpiecznego kodu ActiveX a także Java na stronach WWW.

Kluczowym elementem nowoczesnych systemów antywirusowych jest oprogramowanie spełniające funkcje konsoli zarządzającej.



Schemat struktury logicznej systemu antywirusowego Trend Micro

Najważniejsze cechy Trend VCS:

- zarządzanie oprogramowaniem antywirusowym poprzez sieć komputerową z wykorzystaniem jednego interfejsu WWW
- raporty i statystyki dotyczące wirusów z całego obszaru sieci
- możliwość generowania alarmów i powiadamiania administratorów z wykorzystaniem różnych metod komunikacji (np.: e-mail)
- jeden, wspólny punkt aktualizacji bazy wirusów, oprogramowania oraz patchów dla rodziny oprogramowania antywirusowego Trend Micro
- możliwość przechowywania informacji w serwerze LDAP (Lightweight Directory Access Protocol)
- łatwa instalacja i wdrożenie agentów
- centralna baza zdarzeń w systemie: data, typ serwisu (e-mail, HTTP, FTP)

Dzięki grupowaniu wszystkich komputerów z zainstalowanym oprogramowaniem antywirusowym Trend Micro w domeny, administrator może łatwo zarządzać tysiącami maszyn.

System komputerowy jest zabezpieczony przeciwko wirusom tylko na tyle na ile jest zabezpieczony najsłabszy element w tym systemie. Zdalna aktualizacja daje pewność, że wszystkie komputery korzystają z aktualnych wersji oprogramowania (również aktualizowanego zdalnie) oraz posiadają aktualne bazy wirusów.

Uwagę należy zwrócić również na zabezpieczenie takich newralgicznych punktów sieci jak serwery plików, poczty czy po prostu bram internetowych. Oprogramowanie firmy Trend Micro zostało stworzone właśnie w tym celu.
Najważniejsze jego cechy to:

- wykrywanie i usuwanie wirusów z całego ruchu wchodzącego i wychodzącego SMTP, HTTP oraz FTP w czasie rzeczywistym,
- powiadamianie nadawcy, odbiorcy i administratora w przypadku wykrycia wirusów,
- automatyczna aktualizacja baz wirusów oraz oprogramowania przeszukującego,
- interfejs konsoli zarządzającej umożliwia zarządzanie z poziomu przeglądarki WWW,
- współpraca z dowolnym serwerem poczty elektronicznej,
- wykrywanie potencjalnie niebezpiecznych kontrolek ActiveX oraz kodu Javy i możliwość blokowania Javy oraz ActiveX. Filtrowanie kodu ActiveX i Javy

V. Sprawdzanie logów systemowych

1. Zasada działania logów,

Logi systemowe: Jest to swego rodzaju "dziennik pokładowy", który zawiera informacje o akcjach lub operacjach wykonywanych w systemie. Należy dołożyć najwyższych starań, aby pliki z logami były bezpieczne i nikt nie mógł w nie ingerować bez naszej wiedzy (najlepiej robić ich kopię zapasową lub przechowywać na osobnej maszynie). Jest to najważniejsze źródło wiedzy przy włamaniach i wykrywaniu przyszłych włamań.
Bez logów wykrycie i usunięcie wielu problemów może okazać się niemożliwe.
W przypadku włamania logi można odtworzyć i spróbować odkryć metodę włamania oraz źródło ataku. Logi mogą być również dowodem w postępowaniu karnym.

2. Ręczne przeglądanie logów,

Spora grupa administratorów nie sprawdza regularnie logów swych systemów i byliby zdziwieni, jak cenne informacje można w ten sposób pozyskać. Jednakże, zanim powiemy o tym jakie informacje można zdobyć za pomocą standardowych mechanizmów logowania, zajmiemy się tym, jak zabezpieczyć logi.
Informacje z logów systemowych są praktycznie nic nie warte, o ile nie mamy pewności że nie zostały podmienione bądź zmodyfikowane. Musimy mieć do nich całkowite zaufanie. Pierwszą rzeczą, jaką z reguły robi intruz po włamaniu i osiągnięciu uprawnień administratora, jest zmodyfikowanie logów. Większość obecnie używanych rootkitów (np. cloak), podczas instalacji wymazuje ślady ataku z logów. Tak więc intruz nie musi nawet angażować swojego czasu - "czarną robotę" odwala za niego automat. Niektóre z narzędzi idą o jeden krok dalej - podmieniają programy obsługujące podsystem logowania na własne wersje, które nie zdradzają działań intruza. Tak więc pierwszym krokiem, przed zgromadzeniem danych z logów do analizy, powinno być zabezpieczenie podsystemu logowania.

W praktyce, oznacza to zastosowanie zdalnego serwera logowania. Niezależnie od tego jak bezpieczny jest twój system, nie możesz ufać logom zgromadzonym na dyskach, jeśli intruz uzyska prawa administracyjne. Jeśli nawet intruz nie będzie wiedział jak zastosować bardziej wyrafinowane metody zacierania za sobą śladów, to wystarczy, że złośliwie usunie

cały system - odzyskanie informacji z logów będzie w takim wypadku dosyć trudne. **Żeby bronić się przed tego typu metodami należy gromadzić logi lokalnie i jednocześnie zdalnie, na innym systemie**. Dobrze by było, żeby serwer gromadzący logi był systemem dedykowanym tylko i wyłącznie do tego zadania i żeby gromadził dane ze wszystkich źródeł informacji (serwerów, urządzeń, itp.). Jeśli koszta są dosyć ważną sprawą, to można zbudować taki centralny log serwer przy pomocy systemów Open Source. Serwer logowania powinien być maksymalnie zabezpieczony, z wyłączonymi wszystkimi usługami z wyjątkiem usług niezbędnych do gromadzenia logów z innych systemów. Pamiętajmy także o tym, że system ten powinien być odseparowany od Internetu (np. przez wyfiltrowanie na firewallu lub umieszczenie w osobnej sieci fizycznej).

Ślady skanów

Przeglądając logi możemy się dowiedzieć, czy nasze systemy były skanowane w poszukiwaniu jakiejś usługi. Większość script kiddies przeszukuje sieci po to by znaleźć usługę, o której wiedzą że jest "dziurawa". Jeżeli logi pokazują, że do większości twoich systemów ktoś próbował się połączyć z tego samego adresu IP, na ten sam port TCP lub UDP, to przeważnie oznacza skan w poszukiwaniu znanej słabości danej usługi. Po prostu intruz dysponuje exploitem na jakieś oprogramowanie (np. MS Telnet) i poszukuje potencjalnej ofiary.

Czy udało im się włamać?

Gdy wykryliśmy skanowanie naszych systemów, warto sprawdzić czy tylko na tym skończyła się aktywność intruza w naszej sieci. W większości wypadków intruz będzie próbował wykorzystać jakiś exploit.

Ataki tego typu da się zidentyfikować w logach o ile demon wysyłający zdarzenie przekaże do podsystemu logowania cały cytat z błędną komendą a nie tylko informacje że wystąpił błąd.

Jednakże ciężko jest stwierdzić, czy próba zakończyła się sukcesem. Jednym ze śladów potwierdzających włamanie będą połączenia ze zdalnego systemu do atakowanego hosta. Innym śladem mogą być dziwne, nie znane nam konta systemowe, czy też konta z dużymi przywilejami systemowymi, których sami nie ustawialiśmy. Z reguły zaraz po włamaniu do systemu intruz usuwa ślady włamania z logów i podmienia system logowania na swoją wersję.

3. Programowe przeglądanie logów, na przykładzie Kene Security Monitor

Kene Security Monitor jest ciągłym skanerem, sprawdzajacym stan bezpieczeństwa. KSM analizuje logi bezpieczeństwa wszystkich dostępnych serwerów i stacji roboczych. Używając elementów sztucznej inteligencji, KSM przygląda się wielokrotnym próbom logowania się, stara się wykryć maskowanie użytkownika oraz inne niestandardowe zachowania się, mogące być potencjalnym źródłem problemów. KSM natychmiast powiadamia administratora na e-mail, pager lub w inny sposób.

Ważniejsze własności:

- Ciągłe monitorowanie stanu bezpieczeństwa
- Możliwość zwrócenia specjalnej uwagi na konkretnych użytkowników, stacje lub pliki
- Automatyczne powiadomienie administratora i osoby odpowiedzialnej za bezpieczeństwo w razie wykrycia podejrzanego zachowania
- Proste raporty stanu bezpieczeństwa
- Centralizacja monitoringu dla wszytkich serwerów i stacji roboczych

Czuwający skaner:

KSM jest serwisem ukierunkowanym na konkretne komputery, który aktywnie kontroluje stan sieci. Składa się z trzech elementów:

- konsoli, instalowanej zwykle na komputerze administratora,
- serwera kontroli, instalowanego na serwerze sieci,

- agentów, instalowanych na poszczególnych stacjach.

KSM identyfikuje próby zgadywania haseł lub ich łamania, zmian uprzywilejowania, podejrzanego przeglądania plików i inne tego typu niestandardowe zachowania mogące świadczyć o próbach włamania.

Odkrywanie prób włamań:
Mając baczną uwagę na specyficzne zachowania się użytkowników, administrator może być szybko powiadomiony o próbie włamania, zanim do niego dojdzie. KSM może kontrolować następujące aspekty:

- zdefiniowane przez administratora profile włamań;
- wielokrotne próby logowania się zakończone niepowodzeniem;
- wielokrotne próby czytania plików zakończone niepowodzeniem z powodu braku dostępu;
- "ciekawość" użytkowników oraz przeglądanie plików;
- próby użycia zabronionych usług;
- obecność plików o niezidentyfikowanym ID użytkownika;
- maskowanie się użytkowników;
- nadużywanie ID administartora;
- nadmierne przywileje użytkowników.

Monitorowanie użytkowników, stacji i plików:
KSM może zwracać baczniejszą uwagę na pewne, wydzielone klasy użytkowników, stacji lub plików. Własność ta pozwala na objęcie ściślejszą ochroną użytkowników, którzy posiadają dane wymagające szczególnej ochrony.
Szybkie powiadamianie:
W chwili wykrycia charakterystycznych objawów, KSM natychmiast zawiadamia administratora poprzez sygnał ostrzegawczy na konsoli, stosowny list oraz w inny uprzednio zdefiniowany sposób.
Monitorowanie sieci z jednego miejsca:
Dzięki KSM możemy monitorować stan bezpieczeństwa całej sieci (poszczególnych stacji i serwerów) z jednego miejsca. Możemy również wybrać odpowiedni sposób prezentacji przekazywanych przez KSM raportów. Raporty nt. stanu bezpieczeństwa są przesyłane przez poszczególne elementy systemu KSM w czasie rzeczywistym, dając wgląd administratorowi w aktualny stan bezpieczeństwa.

4. IDS – czyli Intrusion Detection System na przykładzie - snorta

Statycznemu podejściu do zabezpieczenia komputerów od kilku lat przeciwstawiana jest filozofia "obserwuj i reaguj", której kluczowym punktem są narzędzia wykrywające symptomy ataku i podejmujące przeciwdziałanie lub przynajmniej informujące właściciela czy administratora systemu o zagrożeniu. Pakiety programowe reprezentujące pierwsze podejście są dostępne za darmo od dawna. Opisywany tu Snort należy do tej drugiej kategorii - jest pakietem IDS (Intrusion Detection System) . Snort może działać jako sniffer, umożliwiając bieżące podglądanie tego, co dzieje się w sieci; użytkownik może też zapisać wybrane pakiety. Na podstawie bazy sygnatur program może wykrywać różne rodzaje ataków na systemy komputerowe. Pakiet ma otwartą architekturę. Obecnie dostępne rozszerzenia umożliwiają np. zapisy do wielu typów baz danych (PostgreSQL, MySQL, Oracle czy inne - poprzez ODBC), tradycyjnych dzienników systemowych lub plików XML, powiadamianie administratora o zdarzeniach krytycznych poprzez mechanizm WinPopup czy protokół SNMP. Baza sygnatur dla Snorta jest również dostępna bezpłatnie i uaktualniana na bieżąco, w miarę pojawiania się kolejnych zagrożeń.

IDS składa strumień pakietów TCP w spójną sesję, w której treść można zajrzeć w poszukiwaniu symptomów ataku.
Główny mechanizm systemu detekcji zagrożeń polega na porównywaniu przetworzonych pakietów i ich zrekonstruowanych strumieni z bazą sygnatur. System detekcji porównuje cechy pakietu ze zbiorem reguł. Jeśli cechy pakietu dopasowują go do którejś z reguł, zostaje podjęta odpowiednia akcja.
Reguły identyfikowania ataku pozwalają na podjęcie trzech rodzajów akcji: przepuszczenia pakietu (pass), zapisania informacji do dziennika (log) oraz ogłoszenia alarmu (alert).
Oprócz przeszukiwania treści pakietów możemy badać pod różnymi kątami ich nagłówki, m.in. pola i kody ICMP, pole TTL, rozmiary fragmentacji czy numery sekwencji.

VI. Aktualizacja oprogramowania pod kątem bezpieczeństwa sieci i serwera

Nie łudźmy się, że raz zainstalowany system będzie wiecznie sprawny i tak samo bezpieczny. Wraz z upływem czasu odkrywane są nowe błędy w oprogramowaniu, naprawiane są stare - za kilka miesięcy nasz podłączony do Internetu komputer może być celem ataków ludzi z całego świata. Mówiąc bardziej brutalnie, poziom zabezpieczeń naszej stacji roboczej maleje z każdym dniem. Dlatego oprócz stosowania generalnych zasad właściwego użytkowania, należy co jakiś czas odwiedzić stronę producentów używanego oprogramowania. Możemy tam zasięgnąć informacji o ewentualnych odkrytych lukach oraz o aktualnych wersjach programów nie posiadających usterek.
Producenci zazwyczaj umieszczają tzw. serwis-paki oraz innego rodzaju łaty systemowe które zawierają najnowsze aktualizacje zabezpieczeń i aktualizacje dotyczące niezawodności oraz działania systemu. Nowe oprogramowanie zawiera aktualizacje, które rozwiązuje problemy wykryte przez klientów lub wewnętrzny zespół testerów firmy.

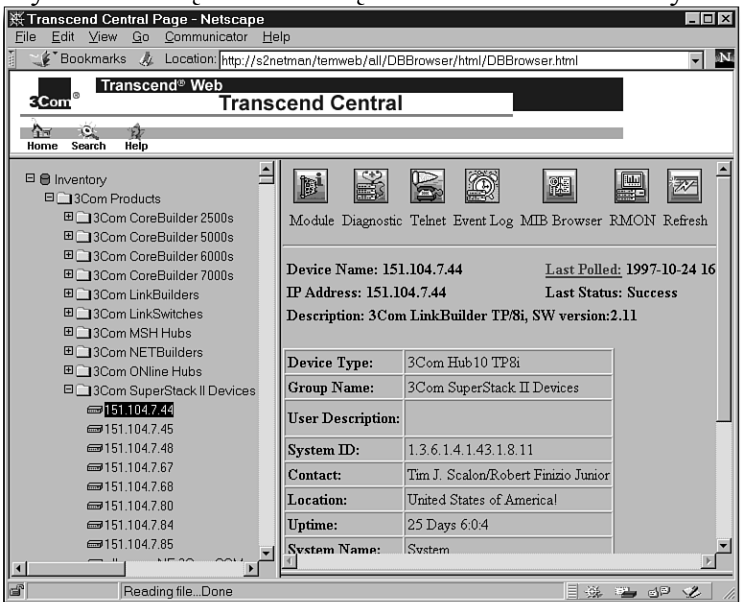
VII. Monitoring i nadzorowanie pracy sieci (kontrola platformy sprzętowej, kontrola platformy programowej)

Tradycyjne zarządzanie siecią
Dobra sieć pracuje w sposób niezauważalny. Serwer realizuje żądania klientów szybko i bez żadnych specjalnych czynności użytkowników korzystających z zasobów sieciowych. Ponieważ konstruktorzy uczynili ten system przezroczystym, problemy związane z okablowaniem, konfiguracją, projektem i utratą parametrów często nie występują lub nie są zgłaszane do momentu katastrofalnej awarii. Dwa słowa „sieć padła” są w stanie zamrozić krew w żyłach każdego administratora sieci.
W części poświęconej zarządzaniu opisane zostaną techniki i narzędzia do zarządzania siecią i jej kontroli. Przedstawionych zostanie pięć – nieco na siebie zachodzących – poziomów systemów zarządzania siecią:

1. narzędzia do zarządzania,
2. system kontroli i raportów o całej sieci,
3. system kontroli i raportów dla koncentratora,
4. analizy protokołów i pomiary ruchu,
5. analizy statystyczne.

Dziedzina systemów zarządzania siecią wprawia w zakłopotanie, głównie z powodu dwóch głównych i kilku podrzędnych kategorii produktów noszących w nazwie określenie „zarządzanie siecią”. Pierwsza kategoria to pakiety programów narzędziowych, których celem jest ułatwienie pracy administratora sieci. Pakiety te, oferowane przez kilka firm – w tym Intela, Novella i Microsoft – obejmują najczęściej ochronę antywirusową sieci oraz narzędzia do inwentaryzacji i dystrybucji oprogramowania. Ponadto pakiety te mogą mieć również

funkcje w rodzaju zdalnej kontroli sieci poprzez modem, możliwości inwentaryzacji sprzętu i dodatkowych zabezpieczeń.
Pakiety te są przydatne, ale dotyczą one tylko jednej strony zarządzania siecią. Druga strona to wszechstronne raporty i kontrola stanu sieci. W szczególności obejmuje to otrzymywanie raportów z routerów, sieci Frame Relay i innych urządzeń sieci szkieletowej. Światowym liderem – jeśli chodzi o możliwości i funkcje zarządzania – jest SystemView IBM. Podobne cechy oferują również Optivity Nortela/Bay Networks, Spectrum Enterprise Cabletrona, OpenView Hewletta-Packarda czy Transcend firmy 3Com. Na rysunku poniżej pokazano ekran z centralnego systemu zarządzania siecią Transcend Central firmy 3Com.

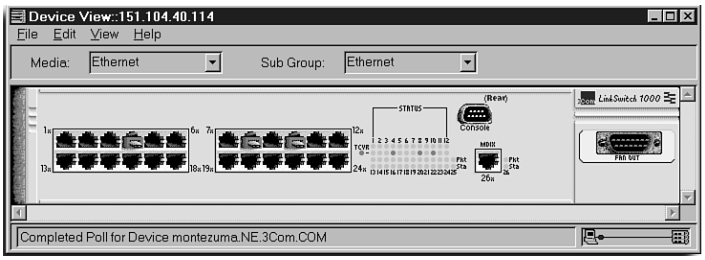


System Transcend Center
Pokazany na rysunku Transcend Central firmy 3Com jest przeznaczony do zarządzania siecią korporacyjną pełną routerów i innych urządzeń. Z poziomu tego głównego ekranu można eksplorować całą sieć, uzyskując raporty z poszczególnych urządzeń.

Pakiet ManageWise Novella to oprogramowanie zupełnie niezależne od sprzętu. Produkty innych firm z branży oprogramowania, takie jak LANDesk Manager Intela, Systems Management Server Microsoftu i Norton Administrator for Networks Symanteca, koncentrują się na funkcjach związanych z kosztami użytkowania systemu, na przykład dystrybucją i inwentaryzacją oprogramowania i pomiarami ruchu.
Najnowszym wynalazkiem we wszystkich produktach do zarządzania siecią jest przeglądarkowy fronton. Niezależnie od tego, czy mamy do czynienia z siecią korporacyjną czy z pojedynczym routerem, możemy przeglądać raporty i konfigurować podstawowe aspekty działania poprzez przeglądarkę w swoim komputerze.

Na wielu poziomach sieci mają miejsce działania związane z generowaniem raportów i kontrolą, które udostępniają wskaźniki pozwalające na ocenę bieżącej kondycji sieci.
W największych sieciach są hierarchie urządzeń i programów, które generują raporty o statucie i problemach na kilku poziomach, kierując je w górę do centralnego systemu raportów i zbierania danych.
Niektóre produkty, na przykład systemy raportów o ruchu dla koncentratorów, dostarczają doskonałych informacji o pojedynczych urządzeniach i nie muszą ich wymieniać z innymi urządzeniami.
Najniższy poziom sieciowych urządzeń generujących raporty to urządzenia z własnymi procesorami i programami w pamięci ROM, które tworzą raporty o ilości i jakości

przesyłanych w konkretnym punkcie sieci. Te urządzenia z wewnętrznymi raportami to koncentratory sieci LAN, mosty, routery, serwery zdalnego dostępu, serwery wydruków, multipleksery, nadajniki radiowe i modemy telefoniczne. Ich wewnętrzne procesory i programy zbierają informacje statystyczne i wysyłają raporty o statusie do programów zarządzających średniego szczebla, które mogą działać praktycznie na dowolnym komputerze w sieci. Rysunek poniżej przedstawia ekran pokazujący, co się w danej chwili dokładnie dzieje w koncentratorze sieci Ethernet.



Aplikacja obsługi koncentratora 3Com
Przy pomocy tej aplikacji można w pełni kontrolować działanie koncentratora. Kontrolki migają, a wtyczki w gniazdkach odpowiadają faktycznym połączeniom, jakie można by zobaczyć, gdyby obserwator zechciał podejść do koncentratora. W programie dostępne są również widoki statystyk i pewne funkcje kontrolne.

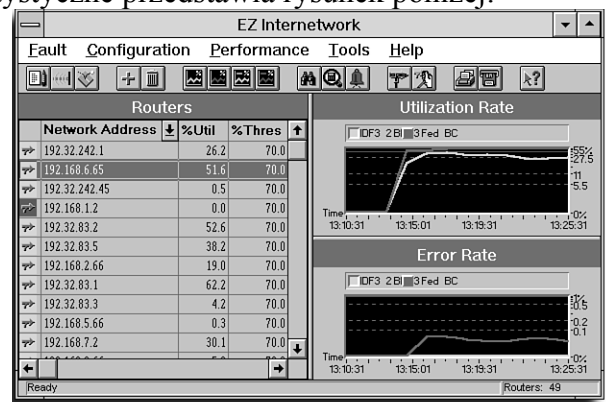
Alarmy i akronimy
Dla całej branży zarządzania i kontroli sieci charakterystyczne są dwie cechy: zaufanie do koncepcji alarmów i irytująca tendencja to powszechnego używania skrótów. Nie trudno zrozumieć koncepcję alarmów, ale wiele więcej czasu zajmuje poznanie używanych skrótów.
Użycie alarmów dotyczących działania sieci polega na poinstruowaniu oprogramowania o konieczności powiadomienia administratora w sytuacji, kiedy wydarzy się coś nadzwyczajnego. Zdarzeniem odbiegającym od normy może być wartość praktycznie każdego innego parametru – zaczynając od temperatury wewnątrz obudowy urządzenia na napięciu w linii zasilającej kończąc. Oprogramowanie do zarządzania siecią i jej kontroli może reagować na sytuacje alarmowe poprzez ich rejestrację w specjalnym rejestrze lub przekazania na pager administratora powiadomienia w postaci specjalnego kodu opisującego problem.

Główne funkcje zarządzania:

- **Zarządzanie awariami** obejmuje wykrywanie problemów, podejmowanie odpowiednich działań w celu ich wyizolowania i usunięcia i udostępnia komunikaty opisujące aktywne połączenia i stan wykorzystywanego sprzętu.
- **Zarządzanie konfiguracją** to nadzór nad konfiguracją poszczególnych urządzeń i sieci jako całości oraz ewentualne zmiany konfiguracji; zarządzanie konfiguracją jest blisko powiązane z zarządzaniem awariami, ponieważ zmiana konfiguracji to podstawowa technika określania awarii.
- **Zarządzanie wydajnością** dotyczy zliczania poszczególnych pozycji, na przykład pakietów, żądań dostępu do dysków i dostępu do określonych programów.
- **Zarządzanie bezpieczeństwem** obejmuje powiadamianie osób odpowiedzialnych o próbach nieuprawnionego dostępu na poziomie okablowania, sieci, serwera plików i zasobów.
- **Zarządzanie rozliczaniem** to naliczanie opłat za korzystanie z sieci przez użytkowników.

Systemem kontroli i raportowania używanym dziś w wielu głównych sieciach jest Simple Network Management Protocol (*SNMP*).

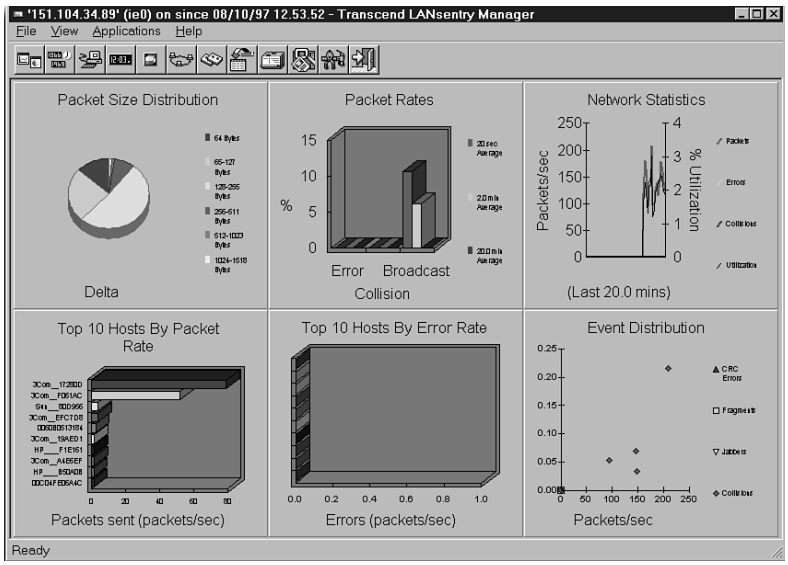
SNMP działa dobrze zarówno w sieciach Departamentu Obrony USA, jak i w sieciach komercyjnych używających TCP/IP. Są metody umożliwiające zastosowanie SNMP nawet w najmniejszych sieciach LAN łączących komputery PC. Zgodny z SNMP program administracyjny OpenView Hewletta-Packarda jest sprzedawany pod różnymi nazwami przez wiele firm. Cabletron ma system SNMP o nazwie Spectrum, który wykorzystuje moduły sztucznej inteligencji do stosowania skomplikowanych reguł i reagowania na otrzymywane raporty o zdarzeniach sieciowych. Oryginalnym i wciąż jednym z najlepszych graficznych systemów do zarządzania siecią jest Optivity Nortela/Bay Networks. Ekran z tego programu zawierający raporty statystyczne przedstawia rysunek poniżej.



Wielkie systemy i aplikacje

Ekran programu Optivity przedstawia w prawej części okna statystyki wybrane z listy znajdującej się w lewej części okna. Raporty statystyczne – jak te pokazane na rysunku – ułatwiają optymalizację architektury sieciowej i planowanie budżetu na zakup nowego sprzętu i połączeń.

Urządzenia w sieci zarządzanej zgodnie z SNMP dzielą się na agentów i stacje zarządzające. Agenty to urządzenia, które przesyłają raporty do stacji zarządzających. Głównym zadaniem agenta jest gromadzenie informacji statystycznych i składowanie ich w bazie informacji zarządzania (*Management Information Base – MIB*). Dla różnych typów baz MIB istnieją standardowe formaty danych, a niektóre firmy przechowują dodatkowe informacja w tak zwanych rozszerzeniach MIB. Jedną z bardziej popularnych baz MIB jest Remote Monitoring lub RMON MIB. Ten rodzaj bazy MIB jest używany w wielu urządzeniach, które kontrolują różne segmenty sieci LAN. Widok aplikacji z oknem RMON MIB przedstawia rysunek poniżej.



Raport z bazy RMON MIB
Raport z bazy RMON MIB zawiera szereg statystyk o objętości i jakości danych monitorowanych przez bazę MIB. Bazę taką można znaleźć w wielu urządzeniach sieciowych – w tym w pudełkach zwanych sondami (*probe*) – których jedynym zadaniem jest generowanie raportów.

Segmenty z bazami RMON MIB
Należy podkreślić konieczność dzielenia sieci na segmenty w celu poprawienia wydajności i niezawodności. Pytanie tylko, skąd wiadomo, co się dzieje w odległym segmencie? Aby się dowiedzieć, najlepiej kupić koncentrator z wbudowaną obsługą bazy RMON MIB lub użyć w różnych segmentach osobnego urządzenia zwanego sondą. Sonda zawiera mały procesor z oprogramowaniem obsługującym bazę RMON MIB. Jej jedyną funkcją jest raportowanie tego, co się dzieje w sieci.
Standard baz MIB odwołuje się do urządzeń zgodnych ze specyfikacją RMON, aby objąć informacje diagnostyczne o awariach w standardowych sieciach, planowanie i funkcje dostosowywania wydajności. RMON to standardowa specyfikacja branżowa, która udostępnia większość funkcji oferowanych przez współczesne niestandardowe analizatory sieci i protokołów.
W celu stworzenia wszechstronnej bazy informacji, dostawcy mogą instalować niewielkie procesory wykonujące program RMON MIB w najróżniejszych urządzeniach podłączonych do sieci. Do kabla sieci LAN można podłączyć kieszonkowych rozmiarów urządzenie zwane sondą (*probe*), które wygeneruje raport i prześle go do stacji zarządzającej.

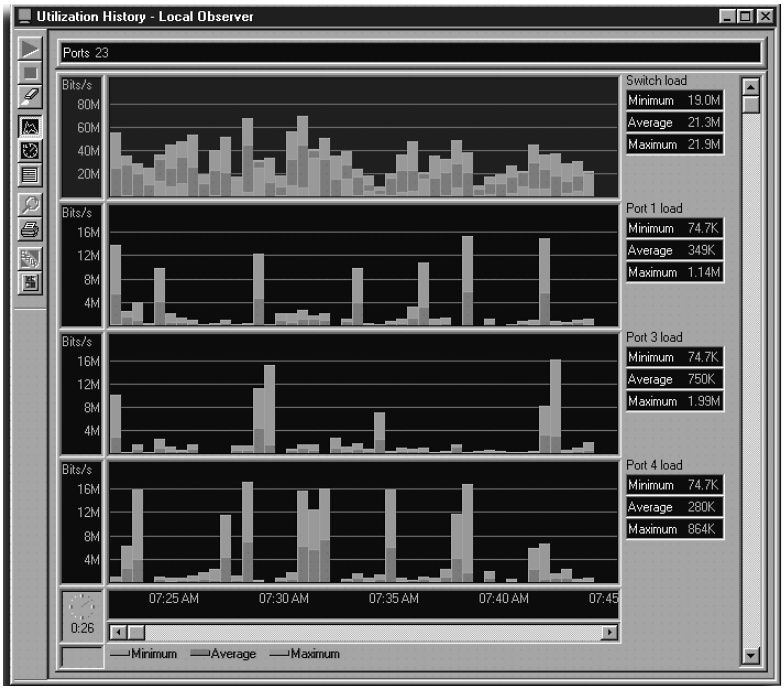
Dzięki bazom RMON MIB administratorzy sieci mogą zbierać informacje z odległych segmentów sieci w celu rozwiązywania problemów i monitorowania wydajności. Baza RMON MIB udostępnia:

- Bieżące i historyczne statystyki ruchu dla segmentu sieci, dla danego hosta w segmencie i ruchu pomiędzy hostami.
- Uniwersalny mechanizm alarmów i zdarzeń umożliwiający określanie wartości progowych i powiadamianie administratora o zmianach w funkcjonowaniu sieci.
- Wydajne i elastyczne narzędzia filtrowania i przechwytywania pakietów, których można użyć do stworzenia kompletnego, rozproszonego analizatora protokołów.

Agentami używającymi baz RMON MIB lub sprzętem z wbudowanymi bazami MIB mogą być koncentratory, routery, serwery plików i węzły sieciowe wszelkiego typu. Niczym dziwnym nie jest fakt posiadania przez agenta – w rodzaju koncentratora czy routera – własnego procesora specjalnie przeznaczonego do zbierania i przechowywania informacji statystycznych.
Stacja zarządzająca „odpytuje" każdego agenta i inicjuje transmisję zawartości bazy MIB. Na stacjach zarządzających działa najczęściej system Windows z uwagi na graficzny interfejs użytkownika lub jakaś wersja Uniksa, ponieważ Unix jest powszechnie kojarzony z protokołami IP i UDP używanymi podczas transmisji pomiędzy agentami a stacjami zarządzającymi.

Raporty z koncentratora
W topologii okablowania 10Base-T i Token-Ring, centralny koncentrator jest ważnym punktem sieci. Ponieważ przez koncentrator przechodzi cały ruch – nawet ruch, który omija serwer plików, i przechodzi między stacją a serwerami wydruków lub serwerami komunikacyjnymi – mikroprocesor w koncentratorze może monitorować wszelką aktywność w sieci i generować na tej podstawie raporty. Ten sam procesor może również zaoferować administratorowi sieci pewien poziom kontroli nad połączeniami sieciowymi.
Produkty te nie dekodują ruchu przechodzącego przez koncentratory i przełączniki. Skomplikowane zadania związane z dekodowaniem realizują urządzenia nazywane

analizatorami protokołów. Analizatory protokołów, które wychwytują i dekodują pakiety, oferują niektóre podobne funkcje, jednak trzeba sporo popracować, aby uzyskać informacje za pomocą tych środków i nie dają one obrazu sieci „z lotu ptaka", takiego jaki zapewniają koncentratory.
Systemy raportów i kontroli działające na poziomie kabla sieciowego nie dekodują pakietów, a zatem nie stwarzają one żadnych zagrożeń dla bezpieczeństwa danych lub haseł. Analizatory protokołów mają zastosowanie w sieciach, w których programiści pracują nad zaawansowanym oprogramowaniem i sprzętem sieciowym, natomiast systemy raportów i kontroli mają zastosowanie niemal w każdej sieci.. Rysunek poniżej przedstawia raporty dotyczące ruchu dla różnych portów przełącznika.

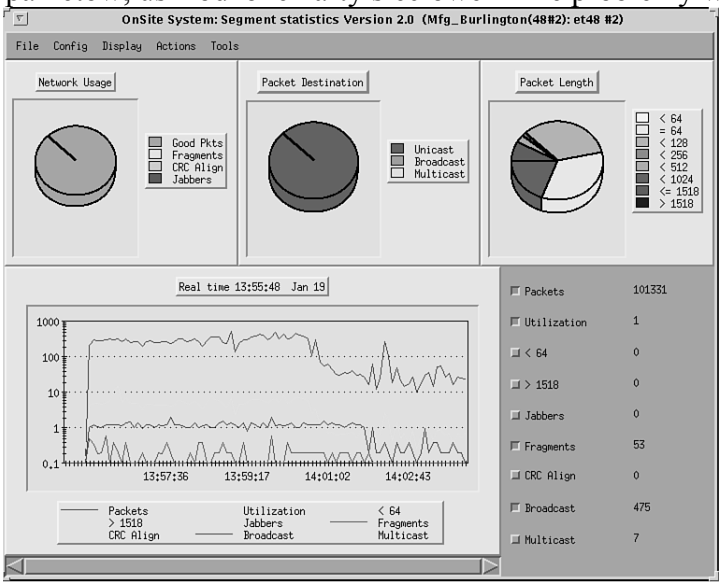


Ekran programu Network Instruments Observer
Ekran programu Network Instruments Observer przedstawia dane o ruchu dla różnych portów przełącznika o określonych porach dnia. Ten rodzaj informacji jest przydatny przy planowaniu konfiguracji sieci i może dać argumenty na rzecz rozbudowy sieci, a także może pomóc wykryć niewłaściwe wykorzystanie sieci.

Produkty te same w sobie mają wszelkie możliwości w zakresie raportów i kontroli, jakich większość organizacji będzie kiedykolwiek potrzebowała, jeśli jednak ktoś spodziewa się, że sieć będzie się rozwijała, przybędzie serwerów, bram i mostów oraz połączeń do sieci rozległych, wkrótce można pomyśleć o zwiększeniu liczby poziomów raportów.
Osiągnięcie pełnej zgodności sieci z protokołem SNMP to niezły pomysł, ale najlepszą rzeczą, jaką można zrobić jest instalacja systemu raportów i kontroli w najniższej, sprzętowej warstwie sieci.

Karty sieciowe przy pracy
Kluczowym elementem we wszystkich narzędziach do analizy protokołów i pomiarów ruchu jest karta sieciowa, która łączy komputer z siecią. Zestaw układów na takiej karcie informuje oprogramowanie o każdym przychodzącym pakiecie, dokonuje translacji formatów danych i przesyła odbierane dane do pamięci RAM, tak aby oprogramowanie mogło je dalej przetwarzać. Układy te realizują również funkcję testowania okablowania.

Układ zestawów produkcji National Semiconductor na typowej karcie ethernetowej może zgłosić siedemnaście różnych błędów dotyczących kontroli transmisji, odbioru i formatu pakietów. Najczęściej występujące błędy dotyczą tak zwanych pakietów runt, które mają za mało bitów i pakietów dribble, które mają dobrą liczbę bitów, ale nie kończą się równym bajtem.
Kiedy karta sieciowa podczas nadawania pakietu wykryje kolizję z pakietem z innej stacji, wysyła sygnał blokady (*jam signal*) – to jest cztery do sześciu bajtów dowolnych danych – aby zapewnić, że wszystkie inne stacje również wykryją kolizję. Wszystkie karty odbierające ten sygnał zgłaszają go programom monitorującym jako kolizję. Mierniki ruchu w sieci LAN przyjmują te raporty od kart sieciowych typu Ethernet lub podobne raporty od kart ARCnet lub Token-Ring i przekształcają je w przydatne wykresy i raporty.
Zarówno systemy zarządzania ruchem w koncentratorach, jak i mierniki ruchu działające poprzez karty sieciowe udostępniają praktyczny i szeroki obraz sieci. Mierzą one natężenie i objętość strumienia danych płynącego poprzez sieć. Rysunek poniżej przedstawia statystyki, takie jak fragmenty pakietów, uszkodzone karty sieciowe i inne problemy w okablowaniu.



Ekran programu Optivity
Ekran z programu Optivity firmy Nortel/Bay Network obrazuje ruch w sieci i dzieli go według fragmentów pakietów, pakietów z uszkodzonych kart sieciowych, rozmiaru pakietów i innych kategorii.

Statystyki serwera
Statystyki bez interpretacji i intuicji są niewiele warte, jednak jeśli ktoś posiada te umiejętności, może dzięki statystykom wiele zdziałać. Sieci to dynamiczne systemy operacyjne. Ich działanie można opisywać poprzez pewne parametry. Administratorzy mogą korzystać z nich do planowania rozbudowy, określania podstawy do porównań, wykrywania problemów we wczesnych stadiach i argumentacji na rzecz budżetów.
Mnóstwo współczesnych programów dostarcza administratorom sieci LAN surowych i przetworzonych danych statystycznych. Uważna analiza tych danych pozwala administratorom stworzyć produktywne i wydajne środowisko sieciowe.

Funkcje zarządzania określają produkt
Trudno jest wypuścić wyjątkowy produkt, na przykład kartę sieciową, który ma być tani i zgodny ze standardami. Dlatego takie firmy, jak Hewlett-Packard, Intel i 3Com wyróżniają swoje karty sieciowe, wyposażając je w funkcje zarządzania i monitoringu. Funkcje te są oczywiście bardzo pożądane przede wszystkim w kartach przeznaczonych dla serwerów.

Wskaźniki mierzone przez te programy to:

- objętość przestrzeni dyskowej zajmowanej przez poszczególne aplikacje, użytkowników lub centra kosztów,
- poziom aktywności dla określonych programów lub plików,
- czas połączenia dla konkretnych użytkowników lub komputerów,
- liczba zadań drukowania (przedstawiana na kilka sposobów),
- obciążenie serwera w określonym czasie,
- kilkadziesiąt innych parametrów.

Dane statystyczne zbierane za pomocą oprogramowania monitorującego tworzą obraz codziennej działalności, który można wykorzystać jako podstawę do rozwiązywania problemów w sieci i jako platformę do planów na przyszłość. Programy te umożliwiają również kompilację i formatowanie informacji o sieci LAN, dzięki czemu można porównywać dane statystyczne przed wystąpieniem problemu i po nim albo przed zmianą i po niej. Informacje takie są przydatne do wykrywania problemów, do określania potrzeb i do budżetowania.

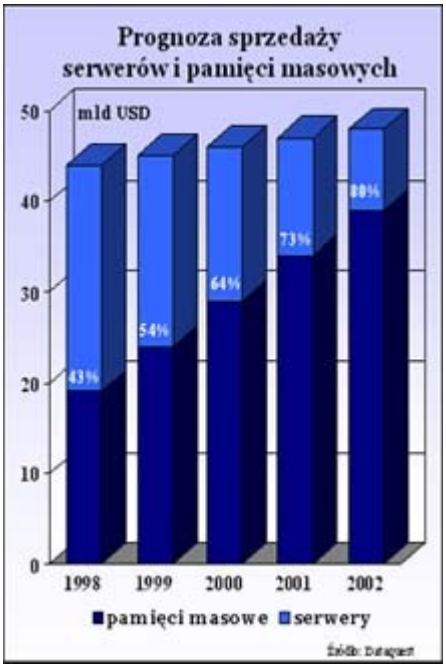
Zestawy programów do zarządzania siecią składają się z wielu narzędzi, które, mniej lub bardziej, współpracują ze sobą w celu przedstawienia wszechstronnego obrazu kondycji sieci. Elementy takich pakietów są bardzo zróżnicowane pod względem możliwości – od prostych programów monitorujących cykle procesora serwera plików do programów inwentaryzujących oprogramowanie i sprzęt, które mogą wygenerować raport o numerach przerwań używanych przez karty sieciowe we wszystkich komputerach w sieci.

Rozległa dziedzina zarządzania siecią obejmuje do 15-20 kategorii narzędzi (niektórzy twierdzą, że więcej). Jednak główny nurt obejmuje pięć podstawowych obszarów: oprogramowanie inwentaryzacyjne (w tym liczące oprogramowanie), monitoring ruchu, monitoring klientów PC, monitoring serwerów i dystrybucja oprogramowania użytkowego.

Tak jak sieciowe programy użytkowe, sieciowe programy narzędziowe są zaprojektowanie z myślą o ułatwieniu pracy administratora i zwiększeniu ogólnej produktywności poprzez wskazywanie problemów w sieci.

VIII. Backup danych

Gromadzenie, przetwarzanie i analizowanie danych jest stałym i nieodłącznym elementem działalności każdej firmy i każdego przedsiębiorstwa. Dane elektroniczne składowane w aplikacjach biznesowych, e-biznesowych, w systemach bazodanowych oraz jako pliki użytkowników na dyskach serwerów są nieustannie narażone na utratę. Jak pokazują statystyki około 50% użytkowników systemów komputerowych nie stosuje żadnych zabezpieczeń, licząc że problem utraty danych ich nie dotyczy i nigdy ich nie spotka. Niestety prędzej lub też później, z różnych przyczyn przydarza się to każdemu. A po wystąpieniu awarii krytycznej najczęściej jest już za późno, koszt odtworzenia utraconych danych jest bardzo wysoki, a bardzo często danych tych już nie można odzyskać.



Aby zwiększyć niezawodność i zredukować ryzyko utraty danych należy zastosować odpowiednie zabezpieczenia:

- System backup'u,.
- System archiwizacji,
- Macierze dyskowe RAID,
- Systemy klastrowe serwerów,

Wszystkie systemy wymienione powyżej doskonale się uzupełniają, ale jeden nie może zastąpić drugiego. Każdy z tych systemów ma inną funkcję do wypełnienia, a dopiero ich połączenie gwarantuje pełny sukces w zakresie zabezpieczania i ochrony danych. Rozwiązanie backup'u ma za zadanie zabezpieczyć dane przed ich utratą spowodowaną trwałym uszkodzeniem serwera , awarią dysku lub całej macierzy dyskowej jak również ma pozwolić na odtworzenie przypadkowo skasowanych plików. Systemy archiwizacji umożliwiają przechowywanie wybiórczych danych na nośnikach magneto-optycznych przez bardzo długi okres czasu. Systemu macierzy dyskowych RAID chronią przed awariami pojedynczych dysków czyniąc, iż taka awaria jest niezauważalna dla zwykłego użytkownika. Systemy klastrowe replikują w trybie rzeczywistym pracujące serwery.

Strategie backupu

Backup pojedynczy zakłada wykonywanie kopii bezpieczeństwa danych na pojedynczej taśmie (lub innym typie nośnika). W czasie tworzenia kopii dane nie są w żaden sposób chronione! Awaria dysku twardego w czasie backupu powoduje utratę danych i utratę kopii bezpieczeństwa.

Bezpieczniejsza odmiana tej strategii zakłada wykorzystanie dwóch nośników lub zestawów nośników. Kolejne kopie bezpieczeństwa są wykonywane na kolejnych nośnikach, przy czym trzecia kopia zamazuje kopię pierwszą itd. Użytkownik może stracić niektóre dane, jeżeli awaria dysku twardego nastąpi w momencie tworzenia kopii bezpieczeństwa, ale nie traci całego systemu i wszystkich danych.

Jednak wszystkie strategie, w których nośnik lub mały zestaw nośników jest cyklicznie wykorzystywany do tworzenia kopii danych są - prawdę mówiąc - bezużyteczne. Zamazanie ostatniej lub przedostatniej kopii danych powoduje zniszczenie poprzednich wersji plików. Nie możemy więc odtworzyć danych np. sprzed tygodnia.

Wady tej nie mają profesjonalne metody tworzenia kopii bezpieczeństwa danych wykorzystujące schematy rotacji. Obecnie dwie najpopularniejsze metody rotacji nośników to Dziadek-Ojciec-Syn (Grandfather-Father-Son) oraz Wieża Hanoi. Strategie te zakładają tygodniowe wykonywanie pełnej kopii danych oraz dzienne wykonywanie kopii przyrostowych lub różnicowych. Gwarantują, że dane z różnych dni będą zapisywane na różnych taśmach, pozwalają na tworzenie historii plików.

Backup pełny polega na archiwizacji wszystkich danych, niezależnie od czasu, kiedy były archiwizowane po raz ostatni. Czas wykonania kopii bezpieczeństwa jest długi, ale ponieważ wszystkie potrzebne dane mogą być odzyskane z jednej tasiemki, czas potrzebny na uruchomienie serwera po awarii jest stosunkowo krótki. Backup pełny jest zazwyczaj stosowany w połączeniu z backupem przyrostowym lub różnicowym.

Backup różnicowy (differential) jest to tworzenie kopii zapasowej plików, które zostały zmodyfikowane po ostatnim pełnym backupie. Operacja kopiowania plików trwa stosunkowo krótko, wzrasta w skali tygodnia. Za to odtworzenie systemu po awarii trwa dłużej, bo zazwyczaj potrzebne są do tego dwie kasety - z ostatniego tygodnia oraz najbardziej aktualna - z ostatniego dnia.

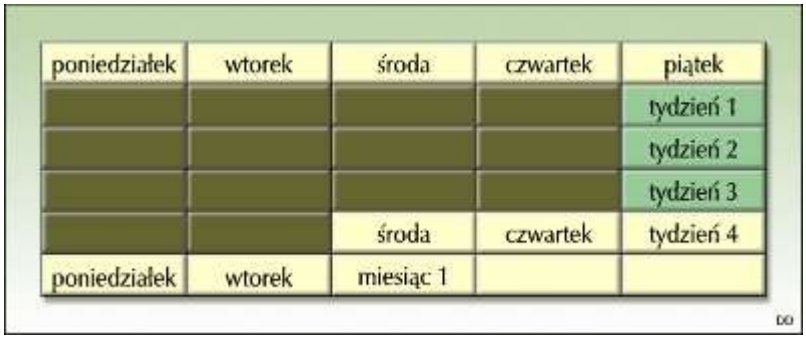
Backup przyrostowy (incremental) jest najszybszym sposobem wykonania kopii bezpieczeństwa, kopiowane są pliki, które zostały zmodyfikowane po ostatnim backupie pełnym lub przyrostowym. Czas potrzebny do odtworzenia danych jest dłuższy niż w przypadku backupu pełnego i różnicowego, zwykle potrzeba do tego kilku tasiemek.

Backup delta to bardzo rzadko stosowana odmiana backupu przyrostowego, pozwalająca na dalsze skrócenie operacji backupu. Kopiowane są nie całe pliki, lecz tylko te ich fragmenty, które zostały zmodyfikowane od czasu ostatniego backupu.

Strategia backupu Dziadek-Ojciec-Syn

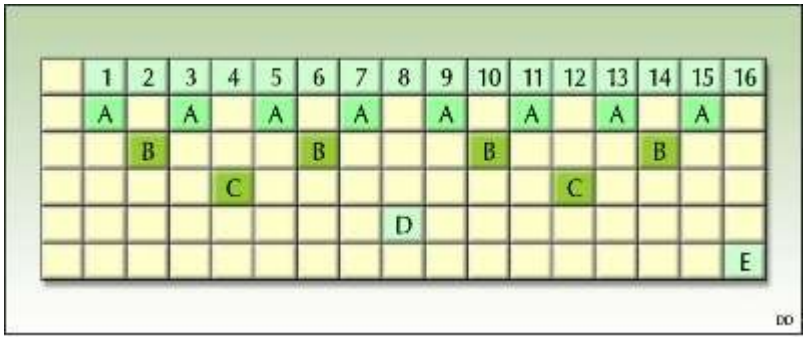
zakłada wykorzystanie 21 (dla 5-dniowego tygodnia pracy) taśm lub zestawów taśm. Cztery taśmy oznaczamy: poniedziałek, wtorek, środa, czwartek. Na tych taśmach sporządzane będą

przyrostowe lub różnicowe kopie danych. Kolejne pięć taśm należy oznaczyć: tydzień 1, tydzień 2, tydzień 3, tydzień 4, tydzień 5. Na tych tasiemkach należy sporządzić pełną kopię w każdy piątek. Pozostałych dwanaście taśm należy oznaczyć kolejnymi nazwami miesięcy. Na koniec każdego miesiąca trzeba na odpowiedniej tasiemce zapisać pełną kopię bezpieczeństwa danych. Taśmy z kopiami miesięcznymi powinny być przechowywane poza siedzibą firmy.



Strategia backupu Wieża Hanoi

wymaga od osoby odpowiedzialnej za wykonywanie kopii bezpieczeństwa żelaznej konsekwencji i pełnego skupienia. Zakłada dodawanie nowego nośnika lub nowego zestawu nośników w sposób cykliczny, przy czym dla każdego kolejnego nośnika długość cyklu jest dwa razy dłuższa niż dla poprzedniego. W tej metodzie rotacji nośnik (lub zestaw nośników) A rozpoczyna schemat rotacji i jest używany w sposób cykliczny co drugi dzień. Drugi nośnik B jest dołączany do schematu rotacji w pierwszy wolny dzień, w którym nie jest wykorzystywany nośnik A i jest używany cyklicznie co czwarty dzień. Trzeci nośnik C jest dołączany do schematu rotacji w pierwszy wolny dzień, w którym nie jest wykorzystywany ani nośnik A, ani nośnik B, i jest używany cyklicznie co osiem dni. Do schematu rotacji można dołączać kolejne nośniki - D, E itd. Najbardziej aktualne kopie danych znajdują się na nośnikach o najkrótszym cyklu, im dłuższy cykl zapisu danych na nośniku tym starsza kopia danych jest na nim zapisana. Podobnie jak w metodzie Dziadek-Ojciec-Syn, nośniki z długim cyklem zapisu danych należy przechowywać poza siedzibą firmy, aby uchronić je przed skutkami lokalnych katastrof.



Dziesięć przestróg dotyczących backupu danych

1. Nie lekceważ wartości danych - decydują o istnieniu firmy.
2. Nie wybieraj najtańszych rozwiązań i opcji - możesz za to drogo zapłacić.
3. Nie kupuj nowego sprzętu ze względu na cenę, najważniejsze, aby wybrane rozwiązanie było dostosowane do potrzeb firmy.
4. Nie pozwalaj na tworzenie tylko jednej kopii krytycznych danych.
5. Nie przechowuj nośników bez okresowego sprawdzania, czy warunki ich przechowywania są zgodne z zaleceniami producenta.
6. Nie używaj nośników "podejrzanych" lub uszkodzonych.
7. Sprawdzaj regularnie jakość nośnika.
8. Nie używaj nowych nośników bez uprzedniego ich sprawdzenia.
9. Nie przechowuj i nie transportuj nośników bez opakowania.
10. Upewnij się, że co najmniej dwie osoby są przeszkolone i wiedzą, co robić w razie awarii systemu.

Dziesięć przykazań dotyczących backupu danych

1. Opracuj zasady zabezpieczania danych w firmie.
2. Upewnij się, że dostęp do kopii bezpieczeństwa mają tylko właściwe osoby.

3. Zamów niezależną ekspertyzę swoich potrzeb w profesjonalnej firmie.
4. Twórz regularnie kopie bezpieczeństwa i sprawdzaj poprawność algorytmów wykonywania kopii.
5. Przechowuj i regularnie rotuj zestaw kopii bezpieczeństwa poza siedzibą firmy - uchroni to dane przed skutkami lokalnych katastrof.
6. Wykonuj regularne próby odtwarzania całego systemu, ale nie na serwerze produkcyjnym!
7. Zainstaluj oprogramowanie antywirusowe i regularnie aktualizuj zbiór z definicjami wirusów.
8. Jednoznacznie opisuj nośniki zawierające kopie bezpieczeństwa, przestrzegaj zaleceń producentów dotyczących ich użytkowania i przechowywania.
9. Upewnij się, że masz zapasowy napęd lub że masz zagwarantowaną natychmiastową wymianę uszkodzonego napędu na sprawny.
10. Przygotuj i aktualizuj Awaryjny Zestaw Naprawczy zawierający: dysk startowy, oprogramowanie diagnostyczne, wersję instalacyjną systemu operacyjnego, wersję instalacyjną programu do backupu danych, aktualne wersje sterowników, zapasowe nośniki.

Urządzenie	Koszt urządzenia	Pojemność nośnika	Koszt nośnika	Szybkość	Komentarz
3,5" stacja dyskietek	Wbudowana w wiekszości komputerów	1,44 MB - nośnik wymienny	0,50$	Wolna	Dobre rozwiązanie przy małych ilościach danych. Tani, przenośny nośnik.
CD-R/W	149-299 (wbudowany w wielu nowych komputerach)	do 700 MB - nośnik wymienny	1$	Średnia	Bardzo dobre urządzenie do backup'u. Przy większej ilości danych, możliwe wykorzystanie wielu dysków.
Dysk twardy (główny)	Brak dodatkowych kosztów. Wbudowany we wszystkich komputerach.	do 160 GB. Powszechnie poniżej 20 GB.	Nośnik niewymienny	Szybka	Dobre rozwiązanie do przechowywania kopii zapasowych plików. Brak możliwości stworzenia backup'u całego systemu. Ewentualnie można wykorzystać połączone komputery w sieci do przechowywania kopii na innych komputerach.
Dysk twardy (dodatkowy)	50-599 instalowany wewnątrz, bądź nazewnątrz komputera	do 160 GB	Nośnik niewymienny	Szybka	Nowe dyski twarde są tanie i stosunkowo proste w instalacji. Urządzenia zewnętrzne są wygodniejsze w instalacji, jednak kosztują więcej.
Napędy ZIP	149$ (czasem spotykane w nowych komputerach)	100 MB lub 250 MB	10$ - nośnik wymienny	Wolna	Jest to najbardziej popularny rodzaj dyskietek dużej pojemności
Napędy taśmowe	od 299$ do ponad 3000$	4GB do 110 GB	od 10$ (4 GB) do 100$ (110 GB) - nośnik wymienny	Szybka	Doskonały, wysokiej pojemności, wymienny nośnik. Najczęściej używane rozwiązanie do backup'u.
Backup Internetowy	Wykorzystywane łącze internetowe	Nieograniczona pojemność, jednak koszty i prędkość połączenia z Internetem stanowią ograniczenie	około 20$ miesięcznie za 500 MB	Średnia - głównie zależy od przepustowości łączy Internetowych	Jeżeli posiadamy łącze Internetowe, nie ma żadnych dodatkowch urządzeń.
Drukarka	Wystarczy drukarka	Nieograniczona ilość kartek	15$ za 500 stron, 40$ tusz/toner	Bardzo wolna	Backup w formie papierowej jest i tak lepszy od braku kopii zapasowej