PAWEL KOWALSKI

DANE I BEZPIECZENSTWO

ESCAPE
MAGAZINE

Paweł Kowalski

DANE I BEZPIECZEŃSTWO

http://www.escapemag.pl

DANE I BEZPIECZEŃSTWO
Paweł Kowalski

Skład i łamanie:
Kamil "Cebula" Cebulski

Projekt i wykonanie okładki:
Maciej "Gilek" Kłak

Wydanie pierwsze
Jędrzejów 2003

ISBN: 83-917573-4-X

Wydawnictwo Publikacji Elektronicznych Escape Magazine
ul. Spokojna 14
28-300 Jędrzejów

e-mail: biuro@escapemag.pl
www: http://www.escapemag.pl

WSTĘP

Ochrona systemu komputerowego (a więc pojedynczego komputera lub sieci komputerowej) i przechowywanych w nim danych. Bezpieczeństwo można podnosić na wiele sposobów. Komputery chronione mogą być przed dostępem niepowołanych użytkowników - oprócz stosowania środków bezpieczeństwa polegających na fizycznym ograniczeniu takim osobom dostępu do sprzętu komputerowego wprowadzane są także zabezpieczenia programowe: konta, indywidualne prawa dostępu oraz hasła. Aby informacje nie mogły być przechwycone przez osoby trzecie, można je szyfrować (por. PGP). Przed przypadkową utratą danych chronią system komputerowy regularnie tworzone kopie zapasowe, a także urządzenia UPS. Jeżeli system komputerowy podłączony jest do internetu dostępu do niego broni firewall, zaś programy antywirusowe chronią przed atakiem malware.

Chroń swój system

Na pytanie o bezpieczeństwo danych w Windows 95/98 przeważnie można usłyszeć jedną odpowiedź: "Przejdź na Windows NT". Na szczęście istnieje kilka sposobów poprawienia zabezpieczeń bez kosztownej zmiany systemu. Większość tych sposobów nie kosztuje nic, oczywiście poza poświęceniem pewnej ilości czasu, można też wyłożyć kilka groszy na zakup jednego z wielu programów shareware, kontrolujących dostępność systemu. Nie ma zabezpieczeń doskonałych i prawdopodobnie zdeterminowany haker będzie mógł uzyskać dostęp do sytemu i zawartości dysków. Warto jednak wykorzystać wszelkie dostępne metody, aby niepowołanym osobom maksymalnie utrudnić dostęp do posiadanych zasobów.

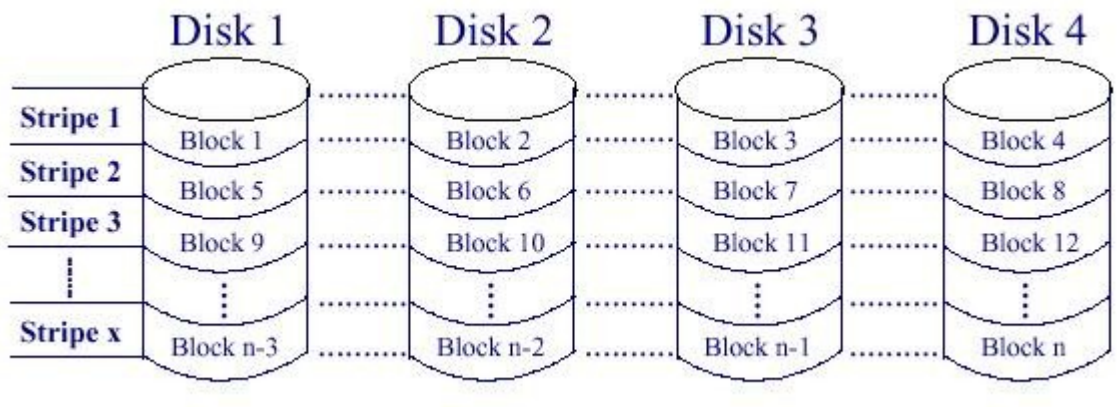
Podczas startu systemu na ekranie pojawia się okno z prośbą o wybór użytkownika i podanie hasła. Czy jest jedno z zabezpieczeń przed niepowołanym dostępem? Otóż nie. Wybór użytkownika pomaga tylko systemowi załadować odpowiednie spersonalizowane ustawienia systemu. Wystarczy nacisnąć klawisz Esc lub kliknąć przycisk Anuluj, aby uruchomić system z domyślnymi ustawieniami. Jak widać, nie jest to najlepsze zabezpieczenie przed niepowołanym dostępem. Można na szczęście w prosty sposób zabezpieczyć startowanie systemu, wykorzystując wygaszacz ekranu. Najpierw należy przygotować wygaszacz. Należy kliknąć na *Start | Ustawienia | Panel sterowania*, dwukrotnie Ekran. W oknie dialogowym, które się pojawi, przejdź na kartę Wygaszacz ekranu. Zaznaczyć opcję Ochrona hasłem i kliknąć przycisk Zmień. Należy podać nowe hasło, które związane będzie z wygaszaczem ekranu. Teraz należy sprawić, aby wygaszacz ekranu był uruchamiany.

Macierze dyskowe RAID.

Istotnym elementem każdej sieci komputerowej jest serwer sieciowy. Od niego w dużej mierze zależy wygoda pracy w sieci oraz bezpieczeństwo danych przechowywanych na serwerze. W celu poprawienia tych dwóch parametrów stworzony został w 1987 roku RAID (Redundant Array of Independent Drives). Zadaniem systemu RAID jest, w zależności od standardu, rozłożenie danych po pojedynczych dyskach. Dla systemu operacyjnego, a najczęściej nawet dla BIOSu, macierz dyskowa widziana jest jako jeden pojedynczy dysk. Ponieważ minimalna ilość dysków, które potrzebujemy na zrealizowanie macierzy RAID jest zależna od standardu RAID, na początek przyjrzyjmy się tym standardom

Standard RAID	Minimalna ilość dysków
RAID 0 (striping)	2
RAID 1 (mirroring)	2
RAID 2 (hamming)	3
RAID 3	3
RAID 4	3
RAID 5	3
RAID 10	4
RAID 50	6

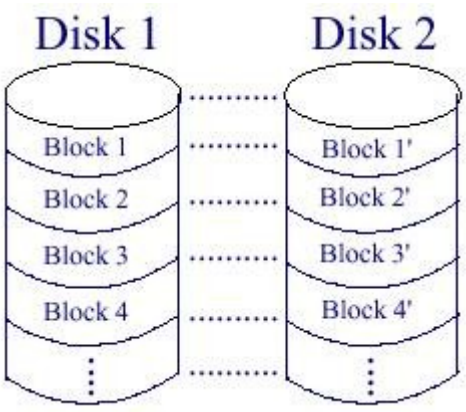
RAID 0 (stripping).



Dane przeznaczone do zapisu są dzielony na tzw. paski (stripes) o wielkości od 4KB do 128KB i zapisywane na różnych dyskach. RAID 0 wymaga minimum dwóch dysków. Zapisując plik, w wypadku RAID 0 opartego o dwa dyski, jego pierwsza część zostanie zapisana na pierwszym dysku, zaś druga na drugim dysku, trzecia część znów na pierwszym, następna na drugim itd. Przy odczycie danych, sytuacja wygląda podobnie: plik jest czytany z dwóch dysków równocześnie. Korzyść takiego rozwiązania jest oczywista - wydajność podsystemu dysków wzrasta teoretycznie o 100%, ponieważ do zapisu pliku każdy z dysków potrzebuje połowę czasu w porównaniu do zapisu całego pliku na jednym dysku. W praktyce, z powodu odpowiednich opóźnień, spowodowanych m.in. samym zarządzaniem macierzy RAID, nie osiągniemy wzrostu wydajności o 100%. W przypadku rozwiązań sprzętowych, wzrost wydajności o 90-95% okazał się być regułą. Wydajność można oczywiście stanowczo zwiększyć, stosując przy RAID 0 trzy, cztery lub więcej dysków, po których dane zostaną rozproszone.

RAID 0 posiada jednak zasadniczą wadę: jeśli utracimy któryś z dysków należących do macierzy RAID 0, tracimy wszystkie dane, ponieważ "z zewnątrz" macierz jest traktowana przez system operacyjny jako jeden dysk. RAID 0 jest więc najtańszym rozwiązaniem na "drastyczne" zwiększenie wydajności, należy go jednak stosować tylko przy odpowiednim regularnym zabezpieczeniu danych (backup).

RAID 1 (mirroring).

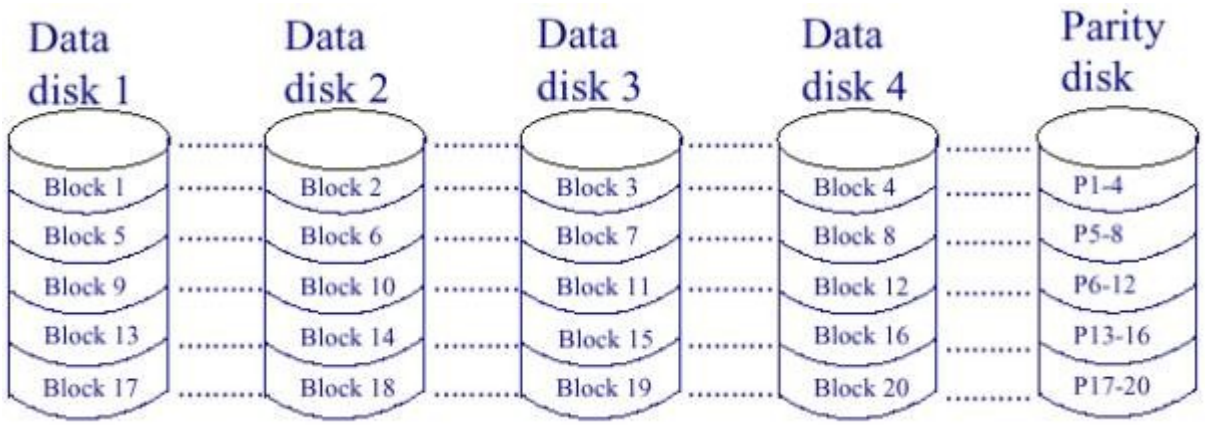


Poprzez "odzwierciedlenie" osiągamy pełną redundancje. Dane zapisywane na pierwszy dysk, są równocześnie też zapisywane na drugi dysk. Jeśli któryś z dysków zostanie uszkodzony, korzystamy z danych na drugim dysku. Rozwiązanie to przyczynia się co prawda do pełnego bezpieczeństwa danych, jednak ciągnie za sobą wysokie koszty (za każdy megabajt płacimy podwójnie) i z reguły obniżenie wydajności podsystemu dysków rzędu 5-10% podczas zapisu. Przy odczycie zaś często możemy zauważyć wzrost wydajności. RAID 1 stosowany jest w mniejszych serwerach pracujących na dwóch dyskach. Jeśli serwer ma dysponować większą ilością dysków, RAID 1 staje się stanowczo za drogim rozwiązaniem.

RAID 2 (hamming).

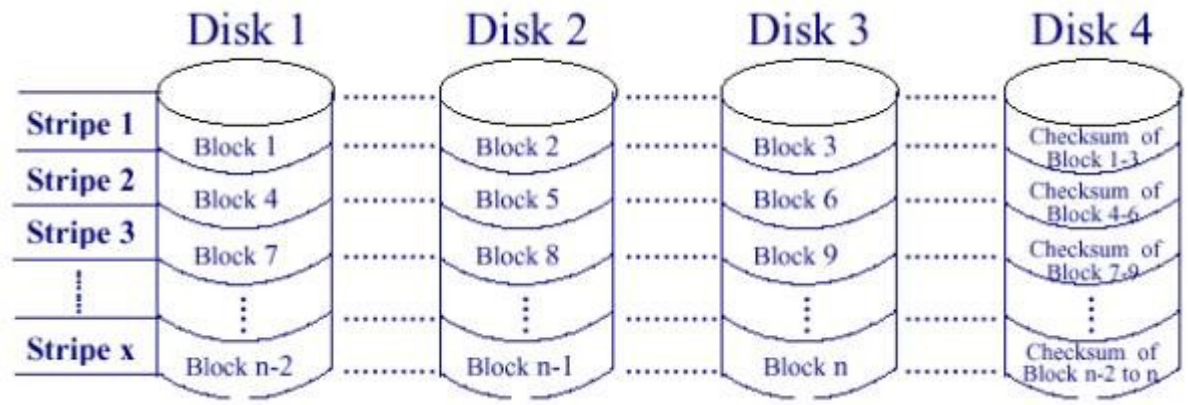
Standard RAID 2 opiera się o RAID 0, przy czym jeden lub więcej dodatkowych dysków jest używany na korekcję i rozpoznawanie błędów (ECC) (Error Checking and Correcting). RAID 2 "rozbija" plik na pojedyncze bajty i zapisuje je na dyskach obliczając przy tym ECC, które jest zapisywane na dodatkowych dyskach. Do obliczania ECC RAID 2 stosuje algorytm Hamminga. RAID 2 był używany w czasach, gdy dyski nie obsługiwały ECC. Dziś każdy dysk posiada własne mechanizmy korekty błędów jednobitowych i tym samym nie ma potrzeby na stosowanie macierzy RAID 2, która w praktyce nie przynosząc praktycznych zysków pod względem wydajności i bezpieczeństwa danych.

RAID 3.



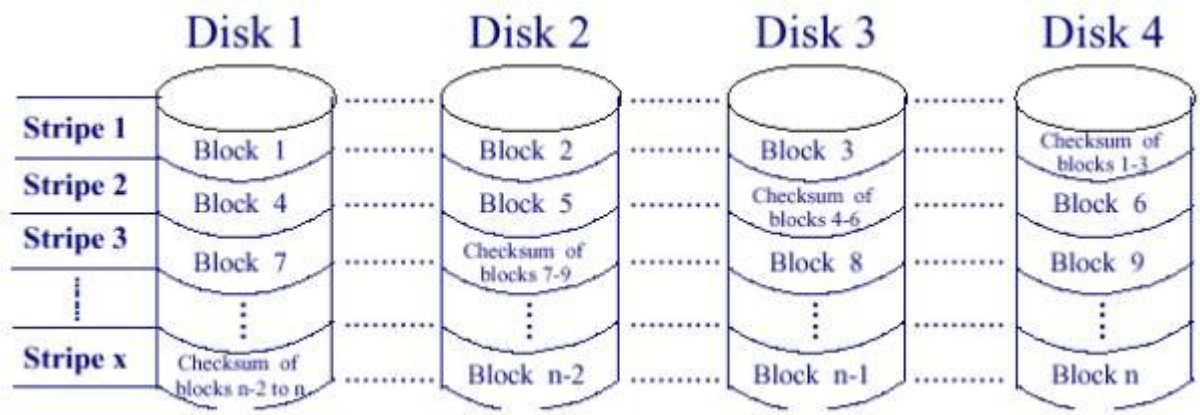
Podobnie jak RAID 2, RAID 3 zapisuje rozbija pliki na pojedyncze bajty i rozprasza je po dyskach. Do każdego bajta obliczana jest parzystość (parity), której zapis następuje na oddzielny dysk, przy czym ten dodatkowy dysk służy tylko i wyłącznie do zapisu parzystości. W wypadku utraty któregoś z dysków, za pomocą operacji XOR macierz jest w stanie z pozostałych danych i parzystości odtworzyć dane. Jeśli stracimy dysk zawierający parzystość, tracimy tylko zabezpieczenie - dane nadal są dostępne. Problem standardu RAID 3 polega na tym dodatkowym dysku parzystości. Każdy dostęp z zapis danych jest związany z tym dyskiem. Aby zwiększyć wydajność macierzy RAID 3, należy odejść od reguły stosowania identycznych dysków i na dysk parity użyć dysk szybszy niż pozostałe, ponieważ to zawsze ten dysk jest hamulcem całej macierzy. RAID 3 stosowany był w macierzach 2-4 dyski + dysk parity. Z dwóch powodów RAID 3 jest dziś już tylko sporadycznie stosowany. Po pierwsze z powodu niskiej wydajności związanej z dyskiem parity i po drugie dlatego, że dzisiejsze systemy operacyjne zapisują dane w blokach a nie w bajtach i niezbędne do konwersji obliczenia są zbyt czasochłonne.

RAID 4.



Ten standard jest podobny do RAID 3, tyle że zamiast bajtów zapisywane są bloki o wielkości 8, 16, 64 lub 128 KB a parzystość jest obliczana dla całego wiersza bloków. Można by również powiedzieć, że jest to RAID 0 z dyskiem na parzystość. RAID 4 pozwala, oprócz bezpieczeństwa danych, na znaczne zwiększenie wydajności podsystemu dysków w wypadku odczytu i zapisu dużych plików (sequential read/write). Przy tzw. rozproszonym zapisie i odczycie (duże ilości małych plików) wydajność macierzy RAID 4 drastycznie spada mimo użycia szybszego dysku dla parzystości.

RAID 5.



RAID 5, nazywany również Rotating Parity Array jest najczęściej stosowanym standardem RAID. Powodem tego jest najlepszy stosunek bezpieczeństwa danych i wydajności podsystemu dysków do kosztów. RAID 5 podobnie jak RAID 4 pracuje

na podstawie bloków i parzystości, która w odróżnieniu do poprzednich standardów RAID jest rozpraszana, tak samo jak same dane, po wszystkich dyskach. Zaletą tego rozwiązanie jest wyeliminowanie drastycznego zmniejszenia wydajności w przypadku rozproszonego zapisu czy odczytu, która występuje w przypadku RAID 4. Przy zapisie lub odczycie dużych plików, RAID 5 osiąga prawie tak samo wysoką wydajność jak RAID 4, co powoduje, że RAID 5 jest najczęściej stosowanym standardem RAID dla serwerów.

Jeśli macierz RAID 5 traci któryś z dysków, dane są nadal w pełni dostępne, ponieważ są rekonstruowane za pomocą parzystości zapisanej na pozostałych dyskach. Wydajność macierzy jest większa, ponieważ odpada problem "wplątywania" w każdą operację zapisu i odczytu dodatkowego dysku, tak jak jest to konieczne w RAID 3 i 4.

Przy standardach RAID zalecane jest stosowanie dla każdej macierzy tego samego modelu dysku, ale jeżeli chcemy wykorzystać dyski twarde, które już posiadamy, a każdy z nich jest inny, należy uwzględnić jedną ważną regułę: pojemność poszczególnych dysków będzie liczona względem najmniejszego dysku. Chcąc użyć dysku 2GB i dysku 1.6 GB na jedną macierz, 400 MB pierwszego dysku nie zostanie wykorzystana.

Zwróćmy jeszcze uwagę na kilka "sztucznych" standardów RAID.

RAID 10.

Często nazywany również RAID 0+1 lub RAID 0/1 jest to kombinacją RAID 1 i 0. Kontroler obsługujący ten standard pozwala np. na stworzenie dwóch "podmacierzy" RAID 0, które są obsługiwane jako pojedyncze dyski macierzy RAID 1 (mirroring). Koszt takiej macierzy są najwyższe ze wszystkich standardów RAID.

RAID 50.

Podobnie jak RAID 10, RAID 50 jest skrzyżowaniem dwóch standardów RAID: 5 i 0. Kontroler obsługujący ten standard, pozwala nam na stworzenie

prawdziwego monstrum pod względem wydajności i bezpieczeństwa danych. Pojedyncze macierze RAID 0 są traktowane jako dyski jednej macierzy RAID 5.

Odzyskiwanie danych

Jak wcześniej wspomniałem jednym z podstawowych zadań macierzy RAID jest odzyskanie danych w przypadku gdy któryś z dysków ulegnie uszkodzeniu. Sposób w jaki dane są rekonstruowane przedstawię na przykładzie macierzy RAID 5.

Disk 1	Disk 2	Disk 3	Disk 4	Disk 5
Parity for 1-4	Data block 1	Data block 2	Data block 3	Data block 4
Data block 5	Parity for 5-8	Data block 6	Data block 7	Data block 8
Data block 9	Data block 10	Parity for 9-12	Data block 11	Data block 12
Data block 13	Data block 14	Data block 15	Parity for 13-16	Data block 16
Data block 17	Data block 18	Data block 19	Data block 20	Parity for 17-20
Parity for 21-24	Data block 21	Data block 22	Data block 23	Data block 24
Data block 25	Parity for 25-28	Data block 26	Data block 27	Data block 28

Załóżmy że mamy do zapisania na dysku taką sekwencję danych: 6C7A79EDFC (01101100 01111010 01111001 11101101 11111100 dwójkowo). Na dyskach będzie to zapisane w następujący sposób:

Disk 1	Disk 2	Disk 3	Disk 4	Disk 5
00	01	10	11	00
01	10	11	10	10
01	11	01	10	01
11	10	11	11	01
11	11	11	00	11

Załóżmy że awarii ulegnie dysk 3. Rekonstrukcja danych zawartych na tym dysku będzie przebiegała w następujący sposób:

Z pierwszego wiersza tabeli (pierwszy pasek danych) bierzemy pierwszy bit zapisany na każdym dysku wykonujemy na nich operację XOR (ALBO) czyli sumę modulo 2 i przyrównujemy do zera. Wartość utracona na dysku 3 jest niewiadomą którą chcemy obliczyć. Mamy więc:

$0 \oplus 0 \oplus ? \oplus 1 \oplus 0 = 0$
$1 \oplus ? = 0$
$? = 1$

Operację powtarzamy dla drugiego bitu każdego dysku:

$0 \oplus 1 \oplus ? \oplus 1 \oplus 0 = 0$

$0 \oplus ? = 0$

$? = 0$

Następnie przechodzimy do drugiego wiersza (kolejne bloki danych) i powtarzamy operację do momentu gdy odzyskamy wszystkie dane z dysku.

RAID - Software

Jeżeli zamierzamy realizować RAID software'owo, procesor komputera przejmuje całą pracę związaną z zarządzaniem macierzy, obliczaniem parzystości i rozdzielaniem danych na "paski" (stripes). Szybkość i wydajność takiego rozwiązanie nie można mierzyć z dedykowanym sprzętem, jednak stanowi ono bardzo tanią możliwość zapoznania się z macierzami RAID i szczególnie przy standardach RAID 0 lub 1 jest w pełni wystarczające, by stanowczo zwiększyć wydajność podsystemu dysków przy stosunkowo niskim obciążeniu procesora.

W wypadku wyższych standardów (RAID 3,4,5 itd.) zalecane jest raczej stosowanie sprzętu a nie oprogramowania, przy czym ta reguła jest również w dużej mierze zależna od siły obliczeniowej, jaką nasz komputer posiada. Wyniki eksperymentów przeprowadzonych na macierzach sterowanych software'owo

wykazały, że obciążenie procesora w wypadku Linuxa wahało się między 15 a 32 %, co było w dużej mierze zależne od użytego rozwiązania. W przypadku dysków IDE obciążenie procesora znacznie wzrastało i w niektórych momentach procesor zostawał obciążony na grubo ponad 50%. Podobnie wyglądała sytuacja w przypadku Windows NT, przy czym obciążenie procesora w NT było mniejsze niż w Linuxie przy użyciu dysków SCSI. Przy dyskach IDE obciążenie procesora leżało z reguły na poziomie 25%.

Mając do dyspozycji serwer NT pracujący na dwóch procesorach Pentium III i trzech dyskach SCSI w macierzy RAID 5, obciążenie procesora było jak na serwer plików "znikome". Sytuacja ta powtarzała się również na innych dwuprocesorowych maszynach, z czego wnioskujemy, że NT w bardzo dobry sposób umie wykorzystać drugi procesor do takich "pobocznych" zadań.

Jeśli chodzi o bezpieczeństwo danych, to obydwóm systemom nie można nic zarzucić. Po symulowanych crashach dysków nie było większych problemów, choć taka macierz nie zachowywała się tak elegancko jak macierz sprzętowa, która po podpięciu dysku wymiennego sama się rekonstruowała w tle. W przypadku NT a szczególnie Linuxa niezbędna była ingerencja użytkownika, która w przypadku NT zajęła kilka godzin a w Linuxie prawie cały weekend...

RAID - Hardware

W przypadku sprzętowych macierzy RAID potrzebny jest nam odpowiedni kontroler. Przy kontrolerach RAID odróżniamy dwa rodzaje kontrolerów: kontrolery przeznaczone do instalacji wewnątrz komputera (np. PCI, EISA) i dedykowane kontrolery zewnętrzne.

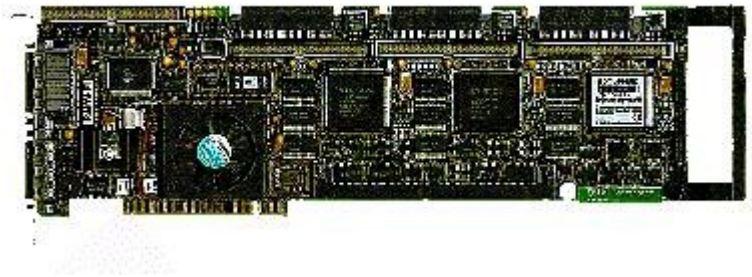
Dedykowane kontrolery macierzy RAID stosuje się w specjalnych obudowach przeznaczonych dla macierzy dysków i nie posiadających z reguły mocowań i miejsca

dla płyty głównej - całe miejsce zostaje przeznaczone na dyski twarde, redundantne zasilacze i odpowiednie chłodzenie dysków.

Wśród kontrolerów przeznaczonych do instalacji wewnątrz komputera znajdują się takie urządzenia jak ICP Vortex GDT 6xxx, Adaptec serii AAA-13x, Mylex AcceleRAID i Promise FastTrack (IDE).

Jednokanałowy AAA-131 Trzykanałowy AAA-133

Kontrolery serii AAA (131 i 133) firmy Adaptec, są pośrednim rozwiązaniem pomiędzy RAID sprzętowym a tym realizowanym przez oprogramowanie. W zależności od modelu, posiadają one jeden lub trzy kanały SCSI (istnieje również wersja OEM z dwoma kanałami), obsługują RAID 0, 1, 5 jak również RAID 10 i posiadają własny procesor, który w pełni przejmuje obliczanie parzystości. Rozwiązaniem pośrednim kontrolery te są z jednego powodu: ich procesor sam nie obsługuje podziału i rozproszenia danych po dyskach (striping) - tą pracę musi wykonać procesor komputera. Rozwiązanie firmy Adaptec nie jest więc w pełni przejrzyste, ale nadal stanowczo szybsze od rozwiązania czysto programowego. Ponadto kontrolery te obsługują do czterech megabajtów pamięci cache, co dodatkowo przyśpiesza dostęp do dysków. Uwzględniając cenę która wynosi około 1.500 PLN za model jednokanałowy i 2.800 PLN za model trzykanałowy, kontrolery te są idealnym rozwiązaniem dla mniejszych systemów NT i NetWare. Z czasem mają się również pojawić sterowniki dla Windows 95/98 i UNIX - na razie z tymi systemami kontrolery serii AAA nie współpracują, co w wypadku kontrolerów RAID nie jest niczym nadzwyczajnym: mało które kontrolery obsługują Windows 95/98.



ICP Vortex oferuje bardzo szeroką gamę kontrolerów RAID dla wszystkich standardów SCSI od 1 do 5 kanałów.

Firma ICP Vortex należy do czołówki specjalistów w dziedzinie RAID, co też widać po kontrolerach produkowanych przez tą firmę. Firma ta oferuje całą gamę kontrolerów, zaczynając od jednokanałowego kontrolera Fast SCSI obsługującego RAID 0 i 1 aż po kontrolery U2W obsługujący wszystkie standardy RAID i posiadające do pięciu kanałów.

W odróżnieniu od kontrolerów firmy Adaptec, modele GDT 6118 (trzy kanały) i GDT 6638 (jeden kanał) produkcji ICP Vortex nie tylko obsługują do 128 MB pamięci cache, ale również posiadają własny procesor RISC (i960), który przejmuje wszelkie obliczenia i operacje związane zarówno z parzystością jak i samym stripingiem. Ogromną zaletą tego rozwiązanie jest zarówno szybkość pracy, brak obciążenia procesora komputera i pełna przejrzystość względem systemu operacyjnego. Oznacza to, że system operacyjny widzi każdą macierz RAID jako zwykły dysk SCSI i kontrolery te współpracują z każdym systemem operacyjnym.

Takie w pełni profesjonalne rozwiązanie mają swoją cenę: niecałe 6.000 PLN dla wersji trzykanałowej lub 4.600 PLN dla wersji jednokanałowej. Mimo wysokiej ceny, można kupić również wersje obsługujące tylko RAID 0 i 1 takie jak GDT 6118, który posiada możliwość rozbudowy o wszystkie pozostałe standardy RAID. W odróżnieniu do innych super-wydajnych kontrolerów RAID (np. kontrolery firmy AMI), kontrolery firmy ICP Vortex pracują w każdym "nowszym" pececie.

Jak już wcześniej wspomniano, większość kontrolerów RAID jest dostępna również w wersjach wielokanałowych. Pomijając fakt, że do wielokanałowego kontrolera można podpiąć więcej urządzeń, oferują one jeszcze dwa zasadnicze walory: dla bezpieczeństwa danych można macierze zestawić tak, by każdy dysk danej macierzy znajdował się na własnym kanale. Następną zaletą kilku kanałów SCSI może się okazać wydajność. W testach przeprowadzonych na macierzy RAID 50, składający się z czterech "podmacierzy" RAID 0 po trzy dyski firmy IBM, pracujących przy 10.000 obrotach na minutę, gdy wszystko zostało podpięte do jednego kanału Ultra Wide podczas pomiarów szybkości okazało się, że macierz ma większą wydajność niż przepustowość Ultra Wide (40 MB/s). Tą samą macierz odtworzyliśmy w oparciu o U2W i również tutaj, mimo przepustowości 80 MB/s w testach można było zauważyć, że w niektórych momentach transfer osiągał 80 MB/s.

Dalszym dużym plusem sprzętowych kontrolerów RAID są Hot-Spare i Hot-Swap. Hot-Swap pozawala na wymianę dysku twardego podczas pracy. Hot-Spare zaś pozwala na wbudowanie dodatkowego dysku (lub dysków), które nie są używane na potrzeby macierzy. Jeśli któryś z dysków macierzy przestanie działać, ten dodatkowy dysk automatycznie wchodzi na jego miejsce. Podczas testów przeprowadzonych na pięciodyskowej macierzy RAID 5 i kontrolerów firm ICP Vortex i AMI, dysk automatycznie "wskoczył" na miejsce "zepsutego" dysku i po odbywającej się w tle rekonstrukcji macierzy (rebuild) po czterech godzinach (ICP Vortex) lub niecałych trzech (AMI) system był znów gotów na wypad następnego dysku. Całe "przedstawienie" było oczywiście niezauważalne dla użytkowników serwera - jedynie administrator walczył z przenikliwymi odgłosami alarmów kontrolerów. Na szczęście w kontrolerach AMI da się ten alarm wyłączyć...

Dodatkową funkcją obsługiwaną przez kontrolery RAID jest tzw. spanning. Służy on do łączenie kilku dysków (również różnej wielkości) w jeden dysk. Przeznaczeniem tego rozwiązania jest potrzeba przechowywania dużych plików (bazy danych, źródłowe dane video itp.), które nie mieszczą się na pojedynczym dysku.

W przypadku tego rozwiązania nie dysponujemy żadną redundancją czy zabezpieczeniem danych, mamy do dyspozycji jednak dużą ilość pamięci dyskowej. Jeśli potrzebny jest nam sam spanning, zakup kontrolera RAID nie jest konieczny. Większość serwerowych systemów operacyjnych obsługuje tę funkcje bez większego obciążenia procesora.

Wśród producentów kontrolerów dedykowanych RAID znajduje się m.in. Hewlett Packard. Jego produkt **HP SureStore E 12H** to szafa o wymiarach 578/425/310 ważąca 77 kg i pojemności 436 GB. Macierz oferuje unikalną technologię na rynku zwaną AutoRAID. Zastępuje ona ciągłe nadzorowanie danych w macierzy przez administratora, poprzez automatyczną migrację danych pomiędzy poziomami RAID oraz pamięcią cache. Dzięki temu użytkownik otrzymuje maksymalną możliwą wydajność macierzy. Modularna budowa umożliwia łatwą rozbudowę do 2,16 TB pojemności. HP gwarantuje 99,95% dostępności. Obsługuje standardy RAID 5 i 10.

Porównanie poziomów RAID

RAID Level	Data Availability	Read Performance	Write Performance	Rebuild Performance	Minimum Number of Drives Required*	Appropriate Uses
RAID 0	None	Very good	Very good	N/A	N	Noncritical data
RAID 1	Excellent	Very good	Good	Good	2N x X (X =number of RAID sets)	Small databases, database logs, critical information
RAID 2	Good	Very good	Good	Good	N + 1	Requires proprietary drives.
RAID 3	Good	Sequential I/O: Very Good Transactional I/O: Poor	Sequential I/O: Good Transactional I/O: Poor	Fair	N + 1 (N = at least 2)	Single-user data-intensive environments (such as video image processing)
RAID 4	Good	Sequential I/O: Good Transactional I/O: Good	Sequential I/O: Very Good Transactional I/O: Poor	Fair	N + 1 (N = at least 2)	Databases, other read-intensive transactional uses

RAID 5	Good	Sequential I/O: Good Transactional I/O: Very Good	Fair unless write-back cache is used	Poor	N + 1 (N = at least 2)	Databases, other read-intensive transactional uses
RAID 6	Excellent	Very good	Poor	Poor	N + 2	Small- and medium-sized highly available databases
RAID 10	Excellent	Very good	Fair	Good	2N x X (X = number of RAID sets)	Data-intensive environment (large records)
RAID 30, RAID 50	Excellent	Very good	Fair	Fair	N + 2 (N = at least 4, X = number of RAID sets)	Medium-sized transactional or data-intensive uses
* N = Storage space requirements of data						

Bezpieczeństwo w sieci

Udostępniając pliki i foldery w sieci Microsoft, można zwiększyć kontrolę na dostępnością zasobów systemu (uwaga: opisana tu metoda może nie dać spodziewanych rezultatów w innych rodzajach sieci, np. Netware). Otwórz Mój komputer, prawym przyciskiem myszy ikonę napędu, którego udostępnianie chcesz zmienić (można też wybrać jeden z folderów lub nawet pojedynczy plik). Z menu podręcznego wybierz Udostępnianie lub Właściwości i przejść na kartę Udostępnianie. Jeśli te opcje nie są widoczne, musisz włączyć możliwość udostępniania plików. Przejdź do *Start | Ustawienia | Panel* sterowania i dwukrotnie kliknij Sieć. Teraz kliknij przycisk Udostępnianie plików i drukarek. Zaznacz opcję Chcę mieć możliwość udostępnienia innym moich plików. Możesz też zaznaczyć drugie pole, jeśli chcesz udostępniać swoje drukarki. Kliknij przycisk OK. W oknie Właściwości na karcie Udostępnianie zaznacz pole Udostępniony jako. Możesz teraz wpisać nazwę, pod którą folder (lub plik) będzie widoczny w sieci i wybrać rodzaj udostępniania (Tylko do odczytu, Pełny, Zależny od hasła). Jeśli wybierzesz opcję Zależny od hasła, możesz podać dwa różne (najlepiej) hasła - podanie pierwszego będzie wymagane przy próbie dostępu do plików w trybie tylko do odczytu, podanie drugiego umożliwi pełny dostęp - z możliwością modyfikacji, zapisywania i usuwania plików. Ustal odpowiednie założenia. Krążek instalacyjny Windows 95 i 98/ME zawiera kilka przydatnych narzędzi, które nie są zwykle używane - z tego prostego powodu, że użytkownicy o nich nie wiedzą. Warto kiedyś poświęcić chwilę i przyjrzeć się bliżej zawartości krążka z napisem "Windows..." Jednym z takich narzędzi jest Edytor założeń systemowych, znany też jako poledit (od System Policy Editor). To bardzo przydatne narzędzie, zwłaszcza, jeśli komputer włączony jest do sieci lub korzysta z niego kilka osób. Wykorzystamy ten program do poprawienia zabezpieczeń systemu. Najpierw jednak konieczne jest utworzenie przynajmniej jednego profilu użytkownika, (jeżeli taki istnieje, możesz przejść do następnego akapitu). W Windows 95 otwórz Panel sterowania i dwukrotnie kliknij ikonę Hasła. Przejdź na kartę Profile użytkownika. Wybierz drugą opcję, tj. Użytkownicy mogą dostosować.... Jeśli chcesz,

zaznacz jedno lub dwa pola, które zostaną uaktywnione. Być może, trzeba będzie ponownie uruchomić system, przedtem jednak zostaniesz poproszony o podanie nazwy i hasła dla nowego użytkownika, następnie zostanie utworzony nowy profil. W Windows 98/ME sprawa jest dużo prostsza. Wystarczy dwukrotnie kliknąć pozycję Użytkownicy w Panelu sterowania - i postępować zgodnie ze wskazówkami

Jeśli do tej pory nie zainstalowałeś w swoim systemie Edytora założeń systemowych, to teraz jest dobry moment, aby to uczynić. Włóż krążek instalacyjny Windows do napędu. Kliknij opcję Dodaj/Usuń programy w oknie powitalnym. Na karcie Instalator systemu Windows kliknij przycisk Z dysku i wybierz plik poledit.inf z folderu *D:\tools\reskit\netadmin\poledit* (zamiast litery D może się pojawić, oczywiście, inna litera określająca napęd CD-ROM). W kolejnym oknie zaznacz obydwie dostępne opcje. Po chwili program poledit zostanie zainstalowany. Chociaż Edytor założeń systemowych to bezpieczne narzędzie, zrób mimo wszystko kopie zapasowe plików Rejestru - user.dat, system.dat i *.pwl. Dopiero po teraz można ze spokojnym sumieniem przejść do następnego etapu. Zrestartuj system. Gdy pojawi się okno wyboru użytkownika, kliknij przycisk Anuluj. W ten sposób uruchomisz system z domyślnymi ustawieniami - i bardzo dobrze, gdyż z takimi właśnie ustawieniami będą uruchamiać system potencjalni włamywacze. Dostosuj pasek zadań i menu Start, usuwając wszystkie te elementy, do których chcesz uniemożliwić dostęp. Przejdź do *Start | Programy | Akcesoria | Narzędzia systemowe | Edytor założeń systemowych*. Po uruchomieniu programu wybierz Plik | Otwórz Rejestr.

Dwukrotnie kliknij ikonę Użytkownik lokalny. Możesz teraz zaznaczyć wybrane opcje, włączające ograniczenia dostępu do zasobów systemowych. Należy jednak pamiętać o tym, aby zostawić możliwość anulowania wprowadzonych zmian w przyszłości, gdy np. powrócimy do jednego tylko, domyślnego profilu użytkownika (w takim przypadku system zostanie włączony z wszystkimi wybranymi przez nas ograniczeniami). Jak to zrobić? Przejdź do *Użytkownik lokalny | System | Ograniczenia*, kliknij przycisk Pokaż, następnie przycisk Dodaj, wpisz poledit.exe i kliknij dwa kolejne przyciski OK. Zapewnij sobie możliwość uruchomienia Edytora

założeń... w każdej sytuacji - pozostaw dostęp do polecenia Start | Uruchom. Od tej pory każda niepowołana osoba, która przedrze się przez powitalne okno wyboru użytkownika (np. naciśnie [Esc]) będzie musiała pracować z bardzo ograniczoną wersją Windows.Nie jest to, oczywiście, pełne zabezpieczenie przed niekontrolowanym dostępem do systemu, "przypadkowych" włamywaczy i dow cipnisiów może jednak z powodzeniem zniechęcić do myszkowania po programach i danych.

Ochrona plików

Chociaż istnieje wiele sposobów ochrony systemu, większość z nich może być kłopotliwa, a użytkownicy nie chcą zamieniać swego komputera w fortecę. W zupełności wystarczałaby ochrona kilku wybranych, krytycznych folderów lub nawet poszczególnych plików. Niestety, zabezpieczenie hasłem folderów lub plików nie jest możliwe w Windows 95/98. Można jednak zabezpieczyć ważne dane przed przypadkowym odczytaniem lub usunięciem (przypadkowym, nie celowym). Kliknij ikonę pliku lub folderu prawym przyciskiem myszy i wybierz właściwości z menu podręcznego. Zaznacz pola Ukryty i Tylko do odczytu, kliknij OK. Pomimo zaznaczenia tych opcji pliki ukryte wcale nie muszą być niewidoczne. Aby rzeczywiście znikły, wybierz (w Eksploratorze Windows) Widok | Opcje folderów, przejdź na kartę Widok i zaznacz opcję Nie pokazuj plików ukrytych. Kliknij OK. Warto też rozważyć przechowywanie najważniejszych plików na dyskietkach i innych nośnikach wymiennych (np. ZIP) - może się to okazać najprostszą metodą ochrony danych.

Narzędzia. Jeżeli ochrona danych i systemu jest bardzo istotna, można rozważyć użycie wyspecjalizowanych programów, które są, niestety, dość kosztowne. Umożliwiają nie tylko zabezpieczenie dostępu do plików i folderów hasłami, ale także szyfrowanie danych i fizyczne usuwanie szczególnie istotnych informacji (pamiętaj, że zwykłe [Delete] nie usuwa zawartości plików). Oto kilka takich aplikacji.

PGP

Słynny system szyfrujący, wykorzystujący dwa klucze - prywatny i publiczny. Istnieje kilka wersji darmowych szyfrujących pliki i np. listy elektroniczne, jest także dostępna nieco bardziej rozbudowana wersja shareware, sygnowana przez McAfee (producent znanego antywirusa).

MouseTrap

Prosty, mały, darmowy program blokujący kursor myszy na obszarze niewielkiego okna. Odblokowanie kursora, a więc i powrót do normalnej pracy jest możliwy dopiero po podaniu hasła.

F-Secure Desktop

Jeszcze jeden program wykorzystujący zaawansowane algorytmy szyfrujące do ochrony najbardziej tajnych danych. Wykorzystuje m.in. pomysłowy generator liczb losowych, polegający, mówiąc w skrócie, na badaniu ruchu myszy wewnątrz okna

More Properties

To mały, ale bardzo wygodny program do edytowania ustawień pracy systemu -- można go nazwać ulepszoną wersją Edytora założeń systemowych. Należy tylko pamiętać o kopii zapasowej plików Rejestru przed dokonaniem jakichkolwiek zmian.

Podglądactwo stosowane

Jeśli pracujesz z Windows 9x i Internet Explorerem w wersji co najmniej 4, możesz szybko przeglądać wiele typów plików multimedialnych wprost w otwartym oknie folderu. Wiąże się to, co prawda, z koniecznością wyświetlania zawartości folderów w trybie sieci Web, nielubianym przez wielu użytkowników, ale

jeśli chwilowo nie masz dobrej i szybkiej przeglądarki takich plików, warto spróbować. Przejdź do menu Widok i zaznacz opcję Jako strona sieci Web. Jeśli opis folderu pojawił się nad ikonami plików w postaci poziomego paska, powiększ okno folderu (rozciągnij w poziomie), a opis wraz z podglądem plików pojawią się po lewej stronie ikon. Niestety, nie wszystkie typy plików mogą być przeglądane (a raczej odgrywane) w ten sposób, np. filmy i pliki dźwiękowe. Można temu zaradzić. Otwórz folder *C:\Windows\Web* w Eksploratorze Windows. Wybierz Widok | Dostosuj ten folder. Zaznacz teraz opcję Utwórz lub edytuj dokument HTML i kliknij dwa kolejne przyciski Dalej. Strona HTML zostanie otworzona do edycji w Notatniku. Wybierz Wyszukaj |Znajdź, wpisz wantmedia i kliknij przycisk Znajdź następny. W wyniku poszukiwania powinien zostać zaznaczony fragment linii "var wantMedia = false". Zamień wyraz "false" na "true". Zapisz zmieniony plik i opuść Notatnik. Zamknij wszystkie otwarte okna Eksploratora.

Teraz możesz otworzyć folder z plikami dźwiękowymi lub animacjami i odtwarzać je w obszarze podglądu okna Eksploratora Windows.

Backup systemu

Gdy system Windows definitywnie odmawia współpracy, a niestety zdarza się to w najbardziej nieodpowiednich momentach, reanimacja systemu może się powieść, ale najgorszej ewentualności (czyli ponownej instalacji systemu) nie można wykluczyć. Nikomu nie trzeba chyba przypominać o konieczności regularnego tworzenia aktualnych kopii bezpieczeństwa danych - dokumentów, projektów itd. Warto także zastanowić się nad utworzeniem kopii systemu - łącznie z aplikacjami - - z której później można szybko odtworzyć stan sprzed awarii. Do przechowywania tego typu kopii można użyć krążka CD-R, CD-RW, dyskietki ZIP lub innego nośnika o dużej pojemności. Kopia systemu nie będzie zawierać dokumentów i danych te powinny być archiwizowane oddzielnie i znacznie częściej - w przeciwnym wypadku po restauracji uszkodzonego systemu możemy ujrzeć na dysku dokumenty w wersjach sprzed np. pół roku.

Do przygotowania kopii zapasowej najlepiej użyć jednego z wielu dostępnych programów - sposób "na piechotę" jest żmudny i łatwo wtedy o pomyłkę. Odpowiedniego programu nie trzeba szukać daleko - można wykorzystać Kopię zapasową, narzędzie znajdujące się na krążku instalacyjnym Windows 98. Włóż krążek do napędu, a gdy pojawi się okno powitalne, kliknij Dodaj / Usuń programy. Przejdź na kartę Instalator systemu Windows i kliknij opcję Narzędzia systemowe. Zaznacz pozycję Kopia zapasowa, kliknij OK, a następnie Zastosuj. Teraz można już przejść do tworzenia kopii. Wybierz Start | Programy | Akcesoria | Narzędzia systemowe | Kopia zapasowa.

Na pierwsze pytanie dotyczące nowego urządzenia, odpowiedz Nie. Teraz zaznacz opcję Utwórz nowe zadanie kopii zapasowej i kliknij przycisk OK. Zostanie uruchomiony Kreator kopii zapasowych - wybierz opcję Wykonaj kopię zapasową wybranych plików, folderów i dysków i kliknij przycisk Dalej. W tej chwili powinny zostać zaznaczone pliki i foldery, które chcesz archiwizować, chociaż wygodniej jest wybrać elementy, które archiwizowane nie będą, np. zaznacz dysk C, kliknij znaczek "+", a następnie usuń zaznaczenie tych elementów, które nie powinny znaleźć się w kopii zapasowej. Będą to z pewnością C:\Moje Dokumenty, C:\Windows\Dane aplikacji, C:\Windows\Ulubione i pliki z rozszerzeniem PST (wszystkie te pozycje należy i tak archiwizowane codziennie lub przynajmniej raz w tygodniu). Można także nie tworzyć kopii zapasowej folderów C:\Windows\Temporary Internet Files, C:\Windows\Temp i C:\Windows\Historia.

Po zakończeniu wybierania kliknij Dalej, zaznacz opcję Wszystkie wybrane pliki, ponownie kliknij przycisk Dalej. Teraz nadszedł czas, aby wybrać miejsce, w którym będziesz przechowywać kopię systemu. Jeżeli wybierzesz napęd CD-R lub CD-RW, musisz liczyć się z tym, że większości przypadków nie jest możliwe proste kopiowanie plików na nośniki CD-R i CD-RW - konieczne jest użycie specjalnych programów. Niektóre napędy, np. z dołączonym oprogra- mowaniem DirectCD, pozwalają kopiować pliki na krążek tak, jakby było to zwykłe kopiowanie między dyskami twardymi. Jeśli umieszczenie danych na krążku wymaga użycia programu do

wypalania płyt, wybierz tymczasową lokalizację kopii zapasowej na jednym z twardych dysków. Kliknij przycisk Dalej. W kolejnym, przedostatnim już oknie zaznacz obie opcje, kliknij Dalej, wpisz nazwę kopii i kliknij przycisk Rozpocznij. Kopia zapasowa tworzona jest automatycznie, nie należy jednak na długo opuszczać komputera podczas trwania tej procedury - mogą pojawiać się okna z pytaniami, na które trzeba odpowiedzieć (oczywiście, że chcesz umieścić w kopii zapasowej pliki Rejestru).

Gdy docelowy dysk okaże się za mały, zostaniesz poproszony o włożenie następnego. Jeśli tworzony plik będzie następnie wypalany na krążku za pomocą oddzielnego programu, można wcześniej pociąć plik na kawałki (np. wielkości 645 MB), odpowiedni do tego celu będzie bezpłatny program FileSplitter, do pobrania ze strony WWW (www.pcworld.pl/ftp). Po utworzeniu kopii zapasowej należy się jeszcze zaopatrzyć się w dyskietkę startową. O jej tworzeniu pisaliśmy już w PCWK Plus kilkakrotnie, a więc tym razem tylko krótkie przypomnienie (Windows 98): Przejdź do Start | Ustawienia | Panel sterowania | Dodaj | Usuń programy na kartę Dysk startowy. Kliknij przycisk Utwórz dysk.

Postępuj zgodnie z poleceniami w oknach dialogowych. Gdy nastąpi awaria, należy ponownie zainstalować "czysty" system Windows (ale razem z programem Kopia zapasowa) i sterowniki do napędu użytego podczas tworzenia kopii zapasowej. Teraz można już odtworzyć kształt systemu sprzed awarii

Pakiet NORTON UTILITIS 2000

Ochrona przed atakami hakerów i naruszeniem prywatności w sieci

Norton Personal Firewall 2000 chroni indywidualnych użytkowników komputerów przed nieautoryzowanym przesyłaniem oraz pobieraniem danych z Internetu, nie wymagając przy tym szczególnej konfiguracji lub skomplikowanej instalacji. Możliwość blokowania połączeń sprawia, że hakerzy nie mają dostępu do ważnych plików, haseł, numerów kart płatniczych lub rachunków bankowych oraz innych poufnych danych przechowywanych na domowym komputerze. Ponadto istnieje możliwość kontroli dostępu poszczególnych aplikacji do Internetu oraz alarmowania o próbach wysłania informacji przez programy, które nie posiadają odpowiednich uprawnień, np. „konie trojańskie". W programie Norton Personal Firewall 2000 zastosowano jedyną w swoim rodzaju, chronioną patentami technologię automatycznej konfiguracji zapory ogniowej dla najczęściej używanych aplikacji internetowych, co oszczędza czas i ogranicza ilość zbędnych alarmów. Użytkownicy mają możliwość wyboru gotowych ustawień zabezpieczeń lub dostosowania działania programu do własnych potrzeb za pomocą intuicyjnego kreatora reguł RuleAssistant.

Norton Personal Firewall 2000 oferuje zaawansowane funkcje ochrony danych niespotykane w konkurencyjnych produktach, takie jak: możliwość blokowania pobierania wybranych lub wszystkich apletów Java i kontrolek ActiveX. Program ponadto umożliwia tworzenie kompleksowych dzienników i statystyk zdarzeń, zawierających szczegółowe informacje dotyczące prób włamania, adresów IP potencjalnych włamywaczy oraz listę autoryzowanych połączeń. Dzięki uzyskanym w ten sposób danym możliwe jest zlokalizowanie źródła dokonywanych ataków.

Norton Personal Firewall 2000 jest obecnie jedynym zabezpieczeniem typu firewall, w którym zastosowano technologię przeznaczoną wyłącznie do ochrony prywatności danych. Pozwala ona na określenie, jakie informacje mają być traktowane jako poufne, np. numery kart kredytowych i rachunków bankowych, a następnie

skonfigurowanie programu Norton Personal Firewall 2000 w celu zabezpieczenia ich przed dostępem ze strony niebezpiecznych witryn WWW. Funkcja blokowania dostępu dla plików cookie z określonych stron sprawia, że użytkownik może zachować anonimowość podczas korzystania z sieci np. nie pozwalając na śledzenie sposobu poruszania się po zasobach Sieci. Norton Personal Firewall monitoruje i rejestruje, jakie dane osobiste zostały wysłane oraz kiedy były blokowane pliki cookie, adresy poczty elektronicznej i inne zdarzenia.

Norton Personal Firewall 2000 stanowi integralną część wielokrotnie nagradzanej rodziny kompleksowych zabezpieczeń internetowych firmy Symantec. W skład tej grupy zabezpieczeń wchodzą również programy Norton Internet Security 2000 2.0 oraz Norton Internet Security 2000 2.0 Family Edition, tworzące pierwszy i jedyny na rynku zintegrowany pakiet osobistych zabezpieczeń internetowych dla użytkowników indywidualnych.

OCENA STANU ZAGROŻENIA DLA SIECI WRAZ Z ANALIZĄ GŁÓWNYCH PRZYCZYN

W miarę, jak systemy komputerowe obsługujące biznes elektroniczny stają się coraz większe, bardziej dynamiczne i skomplikowane, lawinowo rośnie liczba zagrożeń dla ich bezpieczeństwa. NetRecon™ pomaga zabezpieczyć systemy e-biznesowe przedsiębiorstwa, eliminując najczęściej spotykane luki w zabezpieczeniach, zanim potencjalny intruz mógłby je wykorzystać do ataku.

Ocena stanu zagrożeń dla sieci

NetRecon jest narzędziem do oceny stanu bezpieczeństwa sieci, które znajduje luki w zabezpieczeniach, analizuje je i raportuje. Rozwiązanie to przeprowadza zewnętrzną ocenę stanu zabezpieczeń sieci; ocena taka odbywa się poprzez skanowanie oraz sondowanie usług działających w danej sieci. NetRecon symuluje najczęstsze scenariusze włamań lub ataków tak, aby zidentyfikować i wskazać "słabe punkty" sieci, sugerując jednocześnie właściwe działania naprawcze.

Droga ku przyszłości

Wykrywanie i wskazywanie luk w zabezpieczeniach za pomocą oceny ryzyka opartej na całościowej perspektywie sieci obecnie już nie wystarcza. Różnica między NetRecon a innymi skanerami polega na zastosowaniu jedynej w swoim rodzaju, oczekującej na przyznanie patentu technologii skanowania progresywnego, która zachowuje się wobec sieci i systemów jak sprytna szajka napastników — wykonując próby równolegle i dzieląc się uzyskanymi ze skanowania danymi w celu znajdowania głębiej ukrytych luk i niedociągnięć. Co więcej, rozwiązanie "uczy się" w miarę działania, modyfikując strategię infiltracji na podstawie uzyskanych już wyników.

NAJWAŻNIEJSZE FUNKCJE

Obsługa na poziomie całego przedsiębiorstwa

- Jedno narzędzie do skanowania wielu systemów operacyjnych, m.in. UNIX®, Windows 2000, Windows NT®, Windows® 95/ 98 i NetWare®, a także różnych protokołów, w tym TCP/IP, IPX/SPX
- Testowanie serwerów, zapór firewall, routerów, koncentratorów, usług nazewniczych oraz serwerów WWW
- Integracja z rozwiązaniem Enterprise Security Manager™ (ESM), zapewniająca pełną ocenę (hosta i sieci) oraz zgodność z polityką zabezpieczeń firmy

Skanowanie progresywne

- Równoległe przetwarzanie prób
- Współużytkowanie informacji o strategii infiltracji i wynikach uzyskanych podczas skanowania
- Drobiazgowa ocena pozwalająca znaleźć głębiej ukryte luki w zabezpieczeniach

Łatwy i szybki w obsłudze graficzny interfejs użytkownika

- Przegląd postępu skanowania na graficznym wyświetlaczu działającym w czasie rzeczywistym

Elastyczne funkcje raportowania

- Generowanie raportów zgodne z potrzebami użytkownika
- Obsługa szeregu formatów, m.in. Word, Excel oraz HTML, możliwych do przeglądania za pomocą przeglądarki
- Możliwość tworzenia niestandardowych raportów

Unikalna analiza ścieżki przebiegu zdarzeń

- Ilustracja dokładnej sekwencji działań, jakie intruz podjąłby w celu znalezienia lub wykorzystania luki zabezpieczeń
- Identyfikacja luk i sugestie odnośnie rozwiązania problemów

Aktualizacja w sieci WWW

- Dostępność najnowszych aktualizacji zabezpieczeń w sieci WWW

NetRecon jest jedynym rozwiązaniem analizującym przyczyny problemu, w którym sekwencja działań, które doprowadziłyby do odkrycia luki jest zobrazowana za pomocą jedynej w swoim rodzaju funkcji analizy przebiegu.

W odróżnieniu od innych narzędzi, które objaśniają tylko objawy problemów, NetRecon zapewnia pełną genezę przyczyn powstania luk w zabezpieczeniach. NetRecon nie przytłacza użytkownika tysiącami informacji – informuje po prostu, co było prawdziwą przyczyną powstania problemu. I robi to natychmiast...

DYNAMICZNE WYKRYWANIE WŁAMAŃ DO SIECI

Informacje ogólne

Coraz większej popularności inicjatyw z dziedziny biznesu elektronicznego w nowym tysiącleciu towarzyszy niestety wzrost liczby zagrożeń dla sieci. Systemy wykrywania włamań stanowią uzupełnienie dla zapór ogniowych typu firewall i rozwiązań kontroli dostępu, zapobiegając sondowaniu sieci, niewłaściwemu korzystaniu z systemów oraz innym szkodliwym działaniom popełnianym przez użytkowników wewnętrznych, zdalnych, a nawet uwierzytelnionych. Niezbędne jest zatem wdrożenie strategii zabezpieczeń, która zapewniałaby środki zaradcze względem zarówno zewnętrznych, jak i wewnętrznych ataków sieciowych.

Opis produktu

Dzięki rozwiązaniu NetProwler™ firmy Symantec przedsiębiorstwo może zdecydowanie wzmocnić linię swoich zabezpieczeń. Produkt ten w niewidoczny dla użytkowników sposób monitoruje ruch w sieci, zapobiegając naruszaniu zasad bezpieczeństwa i chroniąc zasoby wewnętrzne, w tym aplikacje zarówno standardowe, jak i specyficzne dla danej firmy. NetProwler odznacza się skalowalnością zarządzania przedsiębiorstwem, co pozwala na monitorowanie wielu segmentów sieci. Jest też wyposażony w jedyny w swoim rodzaju, oczekujący na przyznanie praw patentowych wirtualny procesor Stateful Dynamic Signature Inspection™ (SDSI), który w czasie rzeczywistym niweczy próby wykorzystania przez intruzów setek znanych i nowych luk w systemach zabezpieczeń. Korzystając z kreatora definicji ataku administratorzy sieci mogą z łatwością definiować i stosować nowe i niestandardowe sygnatury ataku, bez potrzeby wyłączania systemu.

NAJWAŻNIEJSZE FUNKCJE

- Zapewnia zarządzanie na poziomie całego przedsiębiorstwa w trzywarstwowej architekturze i z wykorzystaniem zaawansowanych możliwości raportowania za pomocą obsługi narzędzia Crystal Report

- W czasie rzeczywistym wykrywa i zapobiega setkom typowych ataków na systemy operacyjne i aplikacje
- Zapewnia funkcję profilowania sieci (Network Profiling), pozwalającą zainstalować i automatycznie skonfigurować produkt natychmiast „po wyjęciu z opakowania”
- Dzięki kompleksowemu kreatorowi dostosowywania sygnatur ataku chroni specyficzne aplikacje firmowe
- Gwarantuje możliwość automatycznego pobierania z sieci WWW aktualizacji oraz nowych sygnatur ataku, aby zabezpieczenia były zawsze gotowe do działania i aktualne
- Obsługując bazę danych SQL, zwiększa skalowalność i usprawnia zarządzanie danymi
- Tworzy szczegółowe opisy ataków oraz środków zaradczych, włącznie z umocnieniem zabezpieczeń zapory firewall
- Poprzez integrację z wielokrotnie nagradzaną aplikacją Intruder Alert™ firmy Symantec pozwala monitorować zdarzenia związane z bezpieczeństwem sieci i hosta w całym przedsiębiorstwie
- Poprzez zastosowanie technologii SDSI i obsługi wielu procesorów zapewnia maksymalną wydajność

Właściwości techniczne

- Funkcjonalność "prosto z pudełka". NetProwler potrafi w czasie rzeczywistym wykrywać setki zarówno typowych, jak i nowych ataków na aplikacje i systemy operacyjne, w żaden sposób nie obniżając przy tym wydajności aplikacji lub sieci. Jest wyposażony w funkcję profilowania, która usprawnia instalację i konfigurację, automatycznie wykrywając aplikacje i hosta sieci, a następnie dynamicznie stosując właściwe sygnatury ataków.
- Niestandardowe sygnatury ataków. Kreator definiowania niestandardowych sygnatur ataku pozwala na tworzenie przez użytkownika własnych sygnatur ataku, chroniących specyficzne aplikacje lub środowiska i zmniejszając lub całkowicie eliminując ich "słabe punkty". Interfejsy kreatora obsługują metodę

„przeciągnij i upuść" dla wyrazów kluczowych, prace zastrzeżone, operatory i łańcuchy arytmetyczne, co gwarantuje szybkie tworzenie i testowanie sygnatur.

- Dynamiczne aktualizacje. Firma Symantec aktualizuje bibliotekę sygnatur przynajmniej raz na miesiąc, dzięki czemu nowe sygnatury można instalować bez konieczności wyłączenia aplikacji i narażenia się na ryzyko ataku.
- Najnowocześniejsze techniki obrony. Częste uaktualnienia dostarczane przez zespół Infosecurity firmy Symantec sprawiają, że NetProwler zawsze chroni przed najbardziej aktualnymi zagrożeniami. Rozwiązanie zawiera opcje automatycznej reakcji, w tym: rejestrowanie sesji, przerywanie, przechwytywanie, raportowanie, alarmowanie oraz umacnianie zapory firewall. Rozległe możliwości obejmują także funkcje ogłaszania informacji na własną konsolę zdarzeń oraz przekazywanie raportów na pager, przez SNMP, e-mail lub HTML.

Wydajne filtrowanie treści i zabezpieczenie antywirusowe dla bram internetowych

NAJWAŻNIEJSZE CECHY

- Zabezpieczenie ruchu internetowego poprzez wysokowydajne, zintegrowane wyszukiwanie wirusów oraz filtrowanie treści na poziomie bramy.
- Maksymalna ochrona dzięki połączeniu działań prewencyjnych według harmonogramu z heurystyczną analizą treści, obejmująca zabezpieczenie antywirusowe i filtrowanie treści.
- Większa wydajność sieci i efektywność użytkowników przy jednoczesnym eliminowaniu niepożądanych treści i niebezpiecznych kodów.
- Obsługa strategii zabezpieczeń na platformach Windows NT®/2000 i Solaris®.

W miarę rozszerzania działalności internetowej firmy zauważają konieczność stosowania zabezpieczeń antywirusowych i systemów filtrowania treści. Zapewniając sobie ochronę przed wirusami przenoszonymi przez Internet i eliminując

wykorzystanie Internetu do celów niezwiązanych z prowadzoną działalnością, firmy nie tylko zabezpieczają zasoby i efektywność pracy, ale także zwiększają wydajność sieci i ograniczają zagrożenie konsekwencjami prawnymi wynikającymi z propagowania niewłaściwych treści w miejscu pracy. Symantec Web Security to obecnie jedyne zintegrowane rozwiązanie wykorzystujące standardowe i heurystyczne technologie wykrywania wirusów i filtrowania niepożądanych treści internetowych. Działając w oparciu o technologie opracowane i obsługiwane wyłącznie przez firmę Symantec system Symantec Web Security stanowi najlepsze rozwiązanie w zakresie filtrowania treści i zabezpieczeń antywirusowych dla większości popularnych systemów operacyjnych.

Wydajne jednoprzebiegowe wyszukiwanie wirusów i niepożądanych treści

Symantec Web Security zapewnia ochronę ruchu internetowego na poziomie bramy HTTP/FTP, oferując jednocześnie wysoką wydajność jednoprzebiegowego wyszukiwania wirusów, niebezpiecznego kodu i niepożądanych treści. Jest to obecnie jedyne rozwiązanie łączące heurystyczną analizę kontekstową z technikami opartymi na liście zadań w celu zapewnienia maksymalnej ochrony przed znanymi i nieznanymi zagrożeniami bezpieczeństwa oraz ograniczenia korzystania ze stron internetowych nie związanych z działalnością firmy.

Wiodące technologie ochrony antywirusowej i filtrowania treści internetowych.

Symantec Web Security to w pełni zintegrowany system zawierający rozwiązania jednego dostawcy. Zaimplementowane technologie skanowania i filtrowania zostały w całości opracowane i są wspierane przez firmę Symantec. Symantec Web Security korzysta z najważniejszych technologii firmy Symantec, takich jak NAVEX i Digital Immune System, zapewniając niezawodną ochronę antywirusową i krótki czasu reakcji na zagrożenia. Technologie te gwarantują najwyższy poziom automatycznego wykrywania i usuwania wirusów bez konieczności ponownego uruchamiania lub instalacji oprogramowania bramy internetowej po

dodaniu nowych mechanizmów skanowania. Symantec Web Security oferuje najbardziej zaawansowane filtrowanie treści internetowych i wykorzystuje międzynarodowe listy filtrowania adresów URL firmy Symantec oraz technologię analizy treści Dynamic Document Review™. Technologia ta oparta jest na opatentowanym procesie, który wykracza poza filtrowanie według słów kluczowych i jest pierwszym naprawdę wielojęzycznym rozwiązaniem do filtrowania w czasie rzeczywistym nieskategoryzowanych stron. Dzięki unikatowemu połączeniu zintegrowanych technologii Symantec Web Security zapewnia najdoskonalszą ochronę przed zagrożeniami z Internetu i spowodowanymi przez nie przestojami w działalności firmy.

Symantec Web Security stanowi pierwszą linię obrony przedsiębiorstwa przed wirusami z Internetu oraz spowodowanymi przez nie przerwami w działalności. Dzięki jednoprzebiegowemu skanowaniu danych HTTP i FTP pod kątem niebezpiecznego kodu i niepożądanych treści Symantec Web Security zwiększa efektywność pracy użytkowników oraz ogranicza ryzyko odpowiedzialności karnej i zagrożeń bezpieczeństwa związanych z przeglądaniem Internetu i pobieraniem plików.

Zwiększenie wydajności sieci

Symantec Web Security optymalizuje wykorzystanie przepustowości i zwiększa dostępność sieci. Jako składnik systemu Symantec Enterprise Security ogranicza ilość ruchu internetowego przechodzącego przez zapory sieciowe (firewall) i transmitowanego wewnątrz sieci. Tym samym zwiększa ogólną niezawodność i wydajność infrastruktury zabezpieczeń i zapewnia warstwie sieciowej tak samo wysoki poziom ochrony przed znanymi i nieznanymi zagrożeniami, jak w przypadku komputerów PC i innych warstw sieci chronionych przez produkty firmy Symantec.

Kompleksowe zarządzanie strategią zabezpieczeń internetowych

Symantec Web Security wykorzystuje elastyczny interfejs zarządzania polityką bezpieczeństwa w języku HTML, który umożliwia łatwą i intuicyjną instalację, konfigurację i zarządzanie z dowolnego miejsca w sieci poprzez przeglądarkę internetową. Wytyczne dotyczące korzystania z Internetu można z łatwością wdrażać i planować w całym przedsiębiorstwie dzięki konfigurowalnym ustawieniom filtrowania oferującym 31 zdefiniowanych kategorii, takich jak pornografia, sport, hazard oraz serwisy informacyjne. Ustawienia te można przypisywać określonym użytkownikom lub grupom, także według harmonogramu. Wszelkie działania związane z dostępem do Internetu można monitorować i analizować za pomocą kompleksowego zestawu wszechstronnych raportów z możliwością eksportu. Symantec Web Security to obecnie jedyne zintegrowane rozwiązanie do wyszukiwania wirusów i filtrowania treści, które obsługuje platformy Windows NT®/2000 i Sun Solaris®.

Ochrona informacji i filtracja wiadomości poczty elektronicznej.

Zabezpiecz swą firmę przed naruszeniami poufności informacji, utratą informacji, procesami sądowymi i niepożądanymi wiadomościami poczty elektronicznej za pomocą **Symantec Mail-Gear**.

Symantec Mail-Gear umożliwia ograniczenie strat cennej własności intelektualnej dzięki kompleksowemu, wieloplatformowemu i opartemu na regułach oprogramowaniu filtrującemu wiadomości poczty elektronicznej. Mail-Gear ułatwia ograniczenie ryzyka pociągnięcia swych użytkowników do odpowiedzialności prawnej dzięki przeszukiwaniu treści pod kątem niewłaściwych lub podlegających cenzurze słów, takich jak seks, rasista czy wulgaryzmy.

Mail-Gear umożliwia także zwiększenie wydajności i szerokości pasma, ponieważ przeciwdziała atakom zmierzającym do zaśmiecenia skrzynki pocztowej i oszustwom (fałszowaniu adresów e-mail).

Najważniejsze cechy

Przeszukiwanie i skanowanie treści

- Przeszukuje przychodzące i wychodzące wiadomości poczty elektronicznej pod kątem poufnych lub niepożądanych treści. Funkcja ta ułatwia przedsiębiorstwom chronienie poufnych informacji, ogranicza ryzyko pociągnięcia do odpowiedzialności prawnej i zwiększa produktywność.

Kompleksowe zarządzanie regułami

- Elastyczny interfejs tej funkcji sprawia, że ustalanie zasad dla użytkowników czy grup odbywa się łatwo i intuicyjnie. Mail-Gear umożliwia administratorom przyznanie użytkownikom różnych praw dostępu do poczty elektronicznej w zależności od tego, kim są i gdzie przebywają. Można na przykład określić, że niektórzy użytkownicy mogą wysyłać lub odbierać wiadomości poczty elektronicznej angażujące tylko te adresy lub domeny, które są wymienione na liście uprawnień.

Wyszukiwanie słów kluczowych

- Zaawansowane wyszukiwanie słów kluczowych, obejmujące także kombinacje słów i wyrażenia.

Dostosowywana baza danych

- Pozwala na konfigurowanie list słów dopasowanych do różnych użytkowników i grup.

Elastyczne prawa dostępu: listy uprawnień i zakazów

- Możliwość tworzenia różnych list, ustalających dokąd można wysyłać wiadomości poczty elektronicznej i skąd można je otrzymywać to cecha wyróżniająca Mail-Gear.

Filtrowanie niepożądanych typów plików

- Umożliwia definiowanie i blokowanie niepożądanych typów plików, takich jaki pliki wideo czy audio, które mogą znacznie obniżyć wydajność sieci.

Anti-Spam

- Blokowanie znanych adresów, spod których przychodzą niepożądane wiadomości pocztowe, a także filtrowanie pod kątem określonych słów kluczowych i wyrażeń. Zwiększa to produktywność i szerokość pasma.

Anti-Spoofing

- Zapewnia korzystanie z kont z wymaganym uwierzytelnieniem użytkownika i blokuje wysyłanie wiadomości anonimowych lub opatrzonych fałszywym adresem.

Harmonogram

- Ustala harmonogram dostępu do poczty elektronicznej, dzięki czemu użytkownicy koncentrują się na tych, z kim powinni się skontaktować w ciągu dnia. Po godzinach pracy dostęp jest swobodny.

Logowanie i sporządzanie raportów

- Śledzi transakcje poczty elektronicznej, a także archiwizuje wszystkie wiadomości. Mail-Gear oferuje kompleksowe narzędzia do logowania i sporządzania raportów.

Zarządzanie zdalne

- Bezpieczne zarządzanie zdalne za pomocą przeglądarki internetowej jest możliwe z dowolnego miejsca.

Poczta internetowa

Serwer poczty internetowej

- Wydajny serwer poczty elektronicznej (SMTP), który obsługuje wszystkie popularne standardy poczty internetowej.

Mobilni użytkownicy

- Klient WWW programu Mail-Gear zapewnia uniwersalny dostęp do poczty elektronicznej z dowolnego komputera wyposażonego w standardową przeglądarkę internetową. Ponieważ wszystkie wiadomości poczty elektronicznej są przechowywane na serwerze, użytkownicy nie muszą się już martwić o pozostawianie ich na komputerach, z których korzystają.

Blokowanie nieodpowiednio zachowujących się użytkowników

- Automatyzuje akceptowane reguły użytkowania za pomocą blokady automatycznej, która uniemożliwia działania jednostkom naruszającym firmowe reguły korzystania z poczty elektronicznej.

Współdziałanie z popularnymi klientami poczty

- Obsługuje popularne pakiety klientów poczty elektronicznej, takie jak Microsoft Outlook, Eudora czy Netscape.

Zdalne zarządzanie pocztą elektroniczną

- Wszelkimi aspektami związanymi z oprogramowaniem można zarządzać za pomocą przeglądarki internetowej.

PEŁNA OCHRONA - BEZKOMPROMISOWE BEZPIECZEŃSTWO

Informacje ogólne

Firmy i instytucje wprowadzające nowe modele gospodarcze, oparte na wykorzystaniu Internetu, łączą ze swymi zasobami informatycznymi klientów, partnerów i dostawców, gdyż jest to niezbędne do prowadzenia handlu elektronicznego i e-biznesu. To nowe, elektroniczne środowisko stwarza nowe szanse, ale też wiąże się z ryzykiem i wymaga odpowiedzialnych działań w celu ochrony własności przedsiębiorstwa. Zapora *Symantec Enterprise Firewall* zapewnia maksymalną, wszechstronną ochronę całej instytucji, nie powodując przy tym spadku wydajności sieci. Stanowi najlepsze zabezpieczenie przed niepożądanym wtargnięciem, jednocześnie dopuszczając do sieci przedsiębiorstwa akceptowany ruch, związany z jego działalnością.

Opis produktu

Symantec Enterprise Firewall zapewnia niezbędną ochronę całego przedsiębiorstwa, w tym interfejsu zewnętrznego między firmą a Internetem, intranetów firmowych, podsieci prywatnych oraz oddziałów terenowych. Znakomita architektura i funkcjonalność tego rozwiązania umożliwiają wszechstronną ochronę sieci przedsiębiorstwa oraz zapewniają pełną kontrolę informacji zarówno przychodzących, jak i wychodzących. Do weryfikacji informacji we wszystkich protokołach *Symantec Enterprise Firewall* wykorzystuje serwery proxy, działające na poziomie aplikacji.

Symantec Enterprise Firewall pracuje w systemach operacyjnych Windows NT®, Windows 2000, Solaris®. Zapewnia on kompleksową ochronę dzięki zintegrowaniu w swej architekturze serwerów proxy na poziomie aplikacji, obwodów sieciowych i filtrowania pakietów. Oprócz ochrony na poziomie protokołu, *Symantec Enterprise Firewall* charakteryzuje się intuicyjnym zarządzaniem, dużą wydajnością i zróżnicowaną gamą współpracujących ze sobą usług, co łącznie czyni z niego najbezpieczniejsze, najłatwiej zarządzane i najbardziej elastyczne rozwiązanie, zaspokajające potrzeby przedsiębiorstw w dziedzinie zabezpieczeń.

NAJWAŻNIEJSZE CECHY

- Umożliwia łatwe zarządzanie zaporami lokalnymi i zdalnymi za pomocą konsoli RMC (Raptor Management Console).
- Rozszerzenie ProxySecured Symantec Enterprise VPN firmy SYMANTEC łatwo integruje się z zaporą *Symantec Enterprise Firewall*, zapewniając bezpieczeństwo połączeń z oddziałami terenowymi i użytkownikami odległymi.
- Bogaty wybór doskonałych metod uwierzytelniania użytkowników pozwala elastycznie zastosować najlepszą metodę, zależnie od istniejącego już repozytorium.
- Zintegrowana z zaporą funkcja blokowania treści umożliwia filtrowanie sieci WWW oraz internetowych grup dyskusyjnych Usenet.
- W połączeniu z rozwiązaniem sprzętowym Fireproof Radware zapewnia wysoki poziom dostępności i wyrównywanie obciążenia, natomiast w połączeniu z oprogramowaniem Microsoft Cluster Server (do Windows NT) lub Veritas (do Solaris) daje wysoki poziom dostępności.
- Architektura zapewnia bogate możliwości zarządzania oparte na regułach, pozwalając administratorom na tworzenie reguł w dowolnej kolejności, bez obawy mimowolnego wprowadzenia luk w zabezpieczeniach.
- Rozszerzone funkcje logowania i raportowania umożliwiają tworzenie szczegółowych raportów statystycznych i opisujących trendy występujące w sesjach oraz prowadzenie dowolnych analiz.

- Zapora spełnia surowe wymagania zgodności operacyjnej między produktami różnych dostawców i ma certyfikat ICSA.
- Zapora rozszerza sieć przedsiębiorstwa, zapewniając szyfrowanie i uwierzytelnianie.

Nowości i usprawnienia w wersji 7.0:

- Programowa duża dostępność/równoważenie obciążenia

  Oprócz sprzętowego rozwiązania Radware, produkt oferuje nowe, zintegrowane funkcje dużej dostępności i wyrównywania obciążenia, co daje możliwość wyboru rozwiązania najlepiej dostosowanego do danego środowiska. Oba rozwiązania – sprzętowe i programowe – korzystnie wpływają na skalowalność platformy Symantec Enterprise Firewall i eliminują przestoje systemu.

- Ulepszone zabezpieczenia
  - Algorytm AES (Advanced Encryption Standard) – zaawansowany algorytm szyfrowania, gwarantujący wyższy poziom bezpieczeństwa i działający szybciej niż 3DES.
  - Dostęp tylko do odczytu – odseparowanie zadań administrowania zabezpieczeniami poprzez wyznaczenie osób mających dostęp do zapory ogniowej „tylko do odczytu", bez możliwości modyfikacji lub aktualizacji konfiguracji zapory.

- Nowe funkcje serwera proxy

  Dodatkowa obsługa następujących protokołów:
  - ESMTP (Extended Simple Mail Transfer Protocol), zapewniający dodatkową ochronę;
  - WEBDAV, stanowiący definicję metody wyszukiwania w Internecie dokumentów na podstawie tytułu, autora, słów kluczowych itp.;
  - T120 (protokół komunikacyjny w standardach telekonferencji H.323), udostępniający obsługę najnowszej wersji Microsoft NetMeeting®.

- Łatwiejsze zarządzanie

  Zawiera następujące nowe opcje konfiguracji dostępne z poziomu konsoli zarządzania Symantec Raptor™ Management Console:

  - Kreator klastrów – łatwiejsze definiowanie wielu identycznych zapór ogniowych i zarządzanie nimi jako jednym węzłem, odciążając administratorów.
  - Replikacja – nadawanie identycznych ustawień konfiguracji różnym zaporom ogniowym w klastrze, co ułatwia instalację.
  - Tworzenie kopii zapasowej – łatwiejsze tworzenie kopii zapasowej konfiguracji zapór ogniowych, a następnie odtwarzanie ich na wypadek ich uszkodzenia lub przypadkowej modyfikacji.

- Definiowanie łączących bramy tuneli VPN na podstawie nazwy DNS, a nie adresu IP, co upraszcza instalowanie oprogramowania klienckiego Symantec™ Enterprise VPN.

- Zaawansowana obsługa systemów operacyjnych Pełna gama możliwości Symantec Enterprise Firewall dla następującym platformom:
  - Solaris®7 i Solaris 8 dla serwera,
  - Windows® XP dla klienta VPN.

Właściwości techniczne

- **Technologia Application Proxy.** Zapewnia bezpieczny przepływ pakietów przez zaporę *Symantec Enterprise Firewall*. Pakiety wchodzące na stos TCP/IP poddawane są weryfikacji w siedmiu warstwach stosu, gdzie używane są różne techniki skanowania. Po zakończeniu wszystkich testów, jeżeli nie wystąpiły problemy, pakiety są uwalniane przez zaporę i przechodzą do kolejnego segmentu sieci.

- **Scentralizowane zarządzanie.** Konsola RMC (Raptor Management Console) upraszcza ustalanie reguł i zarządzanie przez zastosowanie technologii MMC (Microsoft Management Console). *Symantec Enterprise Firewall* wykorzystuje MMC do administrowania na platformach Windows NT. Specyficzna funkcja „zatrzaskiwania" (snap in) konsoli RMC umożliwia administratorowi zainstalowanie jej na dowolnej liczbie komputerów. Urządzenie zabezpieczające można skonfigurować, dostosowując je do zarządzania z wybranego komputera. RMC umożliwia zarządzanie scentralizowane, z równoczesnym połączeniem z wieloma urządzeniami zabezpieczającymi. W systemie operacyjnym UNIX zarządzanie jest realizowane z wykorzystaniem graficznego interfejsu użytkownika tego systemu. Narzędzia wykorzystujące wiersz poleceń pozwalają ponadto użytkownikowi na bezpieczne, zdalne logowanie do urządzenia zabezpieczającego oraz wyświetlanie informacji związanych z bieżącymi sesjami.

- **Integracja rozszerzenia ProxySecured PowerVPN Server Upgrade.** Oparty na standardach serwer PowerVPN® (IPSec, X.509, LDAP, potrójne szyfrowanie DES) umożliwia bezpieczne połączenia z oddziałami terenowymi i użytkownikami odległymi.

- **Uwierzytelnianie użytkownika.** Oferuje duży wybór skutecznych metod uwierzytelniania użytkownika (takich jak NT Domain, Radius itd.) oraz zapewnia elastyczność wyboru, w zależności od istniejącego już w środowisku użytkownika repozytorium. *Symantec Enterprise Firewall* obsługuje wiele różnych schematów uwierzytelniania:
    - OOBA (Out of Band Authentication — uwierzytelnianie autonomiczne). Umożliwia administratorowi określenie, dla dowolnego protokołu, schematu uwierzytelniania wymaganego do przejścia przez zaporę. Schemat OOBA jest realizowany za pomocą przeglądarki, która otwiera klientowi kanał dający mu dostęp do potrzebnego serwera.

- Windows NT Domain. *Symantec Enterprise Firewall* może uwierzytelnić użytkownika na podstawie upoważnienia związanego z jego domeną.
- Defender™ (żeton programowy lub sprzętowy), LDAP (Ligtweight Directory Access Protocol — prosty protokół dostępu do katalogów), BellCore Skey, Gateway Password, CryptoCard lub SecureID.
- Obsługiwane są również dwa inne protokoły uwierzytelniania — TACAS i Radius®.

- **Mechanizmy blokowania treści WebNOT i NewsNOT.** *Symantec Enterprise Firewall* stosuje technologię filtrowania adresów internetowych w celu blokowania dostępu do niepożądanych serwisów WWW. Administrator może ustalić dla określonych użytkowników różne reguły, uniemożliwiając lub ograniczając dostęp do witryn zawierających nagość, przemoc itd. Blokady te mogą być również stosowane w odniesieniu do grup dyskusyjnych. Technologia filtrowania adresów internetowych może być dostosowana do preferencji administratora. WebNOT® i NewsNOT® to jedyne zintegrowane z zaporą mechanizmy blokujące treści, które pozwalają na filtrowanie stron WWW i grup dyskusyjnych Usenet.

- **Wysoki poziom dostępności i wyrównywanie obciążenia.** Wybór jest bogaty — można zastosować rozwiązania programowe Veritas FirstWatch (do systemu Solaris), Microsoft Cluster Server (do NT) lub MCS Service Guard (do HP-UX), umożliwiające awaryjne przełączanie systemu, co zapewnia maksymalną dostępność i wydajność, albo rozwiązanie sprzętowe Radware, zapewniające wysoki poziom dostępności i wyrównywanie obciążenia. Ponadto zastosowanie odpornego na awarie rozwiązania sprzętowego Radware pozwala wyrównywać obciążenie zapory *Symantec Enterprise Firewall*, umożliwiając użytkownikom podział obciążenia ruchem między różne urządzenia zabezpieczające.

- **Zarządzanie oparte na regułach.** Ta wyjątkowa architektura pozwala administratorom tworzyć reguły dla sieci, spójne z regułami obowiązującymi w całym przedsiębiorstwie. Ponadto, dzięki unikatowym algorytmom optymalnego doboru, dopasowującym reguły dostępu do podejmowanych prób połączenia, administrator może tworzyć reguły w dowolnej kolejności, bez obawy mimowolnego wprowadzenia luk w zabezpieczeniach. *Symantec Enterprise Firewall* zawiera dające się konfigurować moduły zarówno dla poszczególnych użytkowników, jak i dla ich grup. Użytkownicy dołączający do określonej grupy natychmiast zaczynają podlegać regułom odnoszącym się do tej grupy. Jako przykłady takich reguł można wymienić: 1) dostęp do określonych serwerów, 2) dostęp do określonych klas współdzielonych plików oraz 3) dostęp ograniczony do określonych przedziałów czasowych.

- **Logowanie i raporty.** Pliki dzienników zapory *Symantec Enterprise Firewall* zawierają pewne informacje, które można wykorzystać do tworzenia szczegółowych raportów statystycznych lub opisujących trendy występujące w sesjach. Są to takie informacje, jak długość sesji, liczba przesłanych bajtów, pełne adresy internetowe, identyfikatory użytkowników i zastosowane metody uwierzytelniania. Plik dziennika w formacie ASCII jest natychmiast przedstawiany na konsoli RMC, co pozwala administratorowi przeglądać go w czasie rzeczywistym. Pliki dzienników są wymieniane co 24 godziny (okres ten można ustawiać) i mogą być importowane do innych aplikacji w celu sporządzania raportów, np. do Telemate.Net, co umożliwia graficzną ilustrację wykorzystania sieci.

- **Certyfikat ICSA.** Zapora spełnia surowe wymagania zgodności operacyjnej między produktami różnych dostawców. ICSA używa zapory *Symantec Enterprise Firewall* jako punktu odniesienia do porównywania wszystkich innych testowanych produktów.

- **Translacja adresów sieciowych.** *Symantec Enterprise Firewall* zawiera specjalne funkcje translacji adresów sieciowych (Network Address Translation — NAT). Pozwalają one administratorowi tworzyć listy dostępowe, dzięki czemu zgłoszenia w chronionej sieci, zarówno przychodzące, jak i wychodzące, są opatrzone ustalonymi adresami, a nie adresem urządzenia zabezpieczającego. Wybranym przez administratora adresem może być adres wewnętrznego komputera-klienta (jeśli wybierane są adresy dla sieci wewnętrznej) lub może nim być rzeczywisty adres serwera (jeśli znajduje się on w Internecie); może to być również adres dodatkowy z oficjalnego zakresu IP przedsiębiorstwa.

- **Kreatory.** *Symantec Enterprise Firewall* zawiera wiele nowych kreatorów, które ułatwiają administratorowi systemu zabezpieczeń kłopotliwe i skomplikowane zadania instalacyjne i konfiguracyjne.

Inteligentne rozwiązania chroniące przedsiębiorstwo przed Wirusami

Dla firm informatycznych obawiających się wirusów, które negatywnie wpływają na koszty, wiarygodność informatyczną i sprawność systemów, pakiet Norton AntiVirus Corporate Edition oferuje najlepsze w tej klasie zabezpieczenia antywirusowe nawet największych sieci rozległych. Skalowalna konsola administracyjna Symantec System Center zapewnia komunikację w czasie rzeczywistym z klientami oraz serwerami z jednego miejsca, umożliwiając wygodną dystrybucję nowych zestawów definicji wirusów. Zdolność do przeszukiwania komputerów, ustawiania blokowania oraz monitorowania aktywności systemu w dowolnym punkcie sieci zapewnia niezrównane zabezpieczenie przed atakiem. Jednocześnie technologia NAVEX™ firmy Symantec w znacznym stopniu obniża całkowite koszty eksploatacji, aktualizując mechanizmy programowe bez ponownego uruchamiania komputera. Pakiet Norton AntiVirus Corporate Edition oferuje w pełni zintegrowany zestaw łatwych w administrowaniu, najlepszych w swojej klasie produktów antywirusowych, zapewniając niezawodne, automatyczne wykrywanie, analizę oraz usuwanie makrowirusów w całej firmie, niezależnie od jej wielkości.

Dlaczego Norton AntiVirus Corporate Edition?

Tylko Norton AntiVirus Corporate Edition:

- Obniża koszty, podwyższając sprawność systemu.
- Ułatwia personelowi informatycznemu utrzymanie odpowiedniego poziomu usług serwisowych (Service Level Agreements).
- Upraszcza instalację komputerów biurkowych i serwerów plików oraz administrowanie nimi dzięki scentralizowanemu zarządzaniu różnymi platformami z jednej konsoli.
- Zapewnia zautomatyzowane, bezobsługowe zabezpieczenia przed makrowirusami, w tym aktualizacje oprogramowania zgodnie z harmonogramem, automatyczne dostarczanie plików definicji wirusów oraz

automatyczne łączenie z Ośrodkiem Badań nad Wirusami - Symantec Security Response (dawniej SARC™).

- Wykorzystuje NAVEX, wyjątkowe rozwiązanie instalujące nowe definicje wirusów oraz rozszerzenia mechanizmu skanująco-naprawiającego — bez konieczności ponownego instalowania czy odinstalowywania aplikacji — na wszystkie platformy występujące w firmie.

W komplecie

Na pakiet Norton AntiVirus Corporate Edition składa się cała rodzina sprawdzonych produktów, zespolonych w jedną konsolę, które można zakupić pojedynczo lub jako zestaw:

- Symantec System Center™ do zarządzania regułami oraz systemami z jednej konsoli.
- Norton AntiVirus Corporate Edition 7.6, najnowocześniejsze zabezpieczenie przed wirusami w systemach Windows® Me/98/95/3.x/2000/XP i Windows NT®, a także na serwerach i środowiskach stacji roboczych DOS.
- Norton AntiVirus Corporate Edition 7.6 for NetWare®, najnowocześniejsze zabezpieczenie przez wirusami dla serwerów NetWare.

Ponadto dostępne są osobno lub w pakietach następujące najlepsze w swojej klasie produkty:

- NAV for OS/2 Server and Client,
- NAV for Macintosh Client,
- NAV for Lotus Notes/Domino dla Windows NT/2000, Solaris, AIX, OS/400, OS/390,
- Symantec AntiVirus/Filtering for Microsoft Exchange dla Windows NT/2000,
- NAV for Lotus Notes/Domino dla OS/2,
- NAV for Gateways dla Windows NT/2000, Solaris,

- Symantec Web Security (dawniej NAV for Firewalls) dla Windows NT/2000, Solaris.

Norton AntiVirus Corporate Edition 7.6 for Windows XP/2000/NT/Me/98/95 and NetWare

- Integracja z Symantec System Center w celu zarządzania wszystkimi platformami Norton AntiVirus z jednego, centralnego miejsca, włączając mieszane domeny Windows NT i NetWare.

Zautomatyzowana analiza i reakcja

- Zapewnia automatyczne, bezobsługowe wykrywanie, analizę i usuwanie makrowirusów, dzięki czemu czas reakcji na szybko rozprzestrzeniające się zagrożenia jest znacznie krótszy, a sprawność systemu — znacznie lepsza. Nowa technologia zautomatyzowanej analizy firmy Symantec opracowała szczepionkę na wirusa Melissa w niespełna godzinę!

Serwer kwarantanny (Quarantine Server)

- Centralne zarządzanie wirusami przez skierowanie wszystkich nienaprawialnych, zainfekowanych wirusami plików w bezpieczny obszar serwera centralnego w celu dalszej kontroli.
- Wyższy poziom zabezpieczeń dzięki usunięciu wirusów z systemu głównego komputera, co zapobiega rozprzestrzenieniu się ich po całej firmie.

Konsola kwarantanny (Quarantine Console)

Umożliwia zdalne administrowanie serwerem kwarantanny, m.in.:

- wizualne śledzenie stanu plików podlegających kwarantannie, także tych wysłanych do ośrodka Symantec Security Response (dawniej SARC) w celu analizy i naprawy,
- testowanie szczepionek otrzymanych z Symantec Security Response,
- rozsyłanie szczepionek do klientów.

NAVEX

- Ponownie programuje mechanizm Norton AntiVirus pod kątem wykrywania nowych klas wirusów bez potrzeby mniejszych lub większych aktualizacji. Należy po prostu zaktualizować definicje wirusów i mechanizmy skanująco-naprawiające w celu poprawy zabezpieczeń, bez konieczności dinstalowywania obecnego oprogramowania lub wdrażania nowego.
- Obniża całkowite koszty eksploatacji. Dzięki aktualizacji mechanizmu wykrywania za pomocą jednego kliknięcia przycisku, możliwe jest skierowanie wysoko opłacanych pracowników do ważniejszych zadań.
- Skraca czas i zmniejsza liczbę problemów dzięki automatycznej instalacji na serwerze i stacjach roboczych podczas pobierania aktualizacji definicji wirusów, zapewniając taki sam stopień zabezpieczeń na wszystkich systemach.
- Oferuje natychmiastowe, bezproblemowe zabezpieczenie przed najnowszymi zagrożeniami ze strony wirusów, eliminując potrzebę oczekiwania na mniejsze lub większe aktualizacje produktu.
- Zapewnia zabezpieczenia w czasie rzeczywistym i na wszystkich platformach, i to nawet przed najbardziej skomplikowanymi wirusami. Jakiekolwiek utworzenie, skopiowanie lub zmiana pliku podlega sprawdzeniu przez moduł AutoOchrony (AutoProtect).

Przeszukaj i wyślij (Scan and Deliver) ***Rozwiązanie wyjątkowe!***
Zapewnia najszybszą analizę i reakcję na zagrożenia ze strony nowych wirusów. Po założeniu kwarantanny na nowy, nienaprawialny plik zainfekowany wirusem:

- Można w prosty i szybki sposób wysłać pocztą elektroniczną do Symantec Security Response plik podlegający kwarantannie.
- Symantec AntiVirus Research Automation (SARA) automatycznie przeanalizuje wirus, opracuje szczepionkę oraz wyśle poprawkę (definicję wirusa) z powrotem do firmy, i to zwykle w ciągu dwóch do ośmiu godzin.
- Można wysłać nową definicję do pojedynczego zainfekowanego klienta lub całej firmy.

- W tym samym czasie Symnatec Security Response opracuje nową definicję wirusa i udostępni ją wszystkim użytkownikom oprogramowania Norton AntiVirus na całym świecie.

Obsługa mikrodefinicji

- Umożliwia użytkownikom pobieranie tylko tych definicji wirusów oraz mechanizmów skanujących (jeśli wymagane do nowych definicji), które pojawiły się od chwili ostatniej aktualizacji. Możliwe jest pobieranie aktualizacji cotygodniowych, a nawet codziennych!
- Pozwala na prawie czterokrotnie szybszą pracę modułu LiveUpdate™, zmniejszając potrzebę pracy w trybie online.
- Eliminuje potrzebę regularnego pobierania dużych plików zawierających stare i nowe definicje.

Wykrywanie złośliwego kodu

- Zabezpiecza przed złośliwymi kodami ActiveX lub apletami Java™, jak również tzw. końmi trojańskimi, zapewniając ścisłą ochronę podczas korzystania z Internetu.

Wykrywanie i naprawianie plików skompresowanych

- Automatycznie wykrywa i usuwa wirusy znajdujące się w skompresowanych plikach, także w zagnieżdżonych, dzięki czemu nawet najlepiej ukryte wirusy nie przedostaną się do systemu. Obsługuje następujące formaty plików skompresowanych, spotykane w środowiskach komputerowych na całym świecie:
    - ZIP®,
    - LZH/LHA,
    - ARJ,
    - LZ,
    - MIME/UU,

  - CAB,
  - PKLite,
  - LZEXE.
- Zapewnia lepsze zabezpieczenie, dzięki czemu pobieranie plików z Internetu staje się znacznie bardziej bezpieczne.

Heurystyczna technologia Bloodhound™

- Automatycznie odszukuje nowe i nieznane wirusy, wykorzystując przełomową technologię heurystyczną. Bloodhound bada strukturę programu, jego logikę, instrukcje, pliki danych oraz pozostałe atrybuty, aby następnie, korzystając z procedury heurystycznej, ocenić prawdopodobieństwo infekcji wirusowej. Niezarażone pliki przechodzą procedurę bez problemu, zainfekowane zaś są powstrzymywane, zanim wyrządzą jakieś szkody.
- Zapewnia najlepsze obecnie zabezpieczenie, wychwytując wszystko, co może przypominać wirusa.
- Jest jedyną technologią certyfikowaną do wykrywania i usuwania nieznanych wirusów, na podstawie zestawień dostępnych pod adresem www.virusbulletin.com.

Automatyczna ochrona AutoProtect

- Oferuje stałe, dyskretne zabezpieczenie działające w tle systemu, automatyczne przeglądanie plików w chwili ich pobierania, otwierania, tworzenia, modyfikowania lub wykonywania.
- Zabezpiecza przed wirusami pochodzącymi z Internetu, intranetu, załączników poczty elektronicznej, dyskietek, dysków twardych, napędów CD-ROM, dysków sieciowych, dysków współdzielonych między komputerami.
- Pozwala spokojnie skupić się innych zadaniach, podczas gdy w tle działa Norton AntiVirus.

LiveUpdate

- Oferuje firmie szybki, prosty sposób na uzyskanie najnowszych definicji wirusów. Użytkownicy lub administratorzy podczas instalacji uruchamiają pierwszą sesję LiveUpdate i ustalają harmonogram przyszłych, wykonywanych automatycznie zadań.
- Dzięki temu stacje robocze i serwery są stale zabezpieczone przed zagrożeniami związanymi z najnowszymi wirusami. Codziennie odkrywanych jest około kilkunastu nowych wirusów, — dlatego właśnie aktualność ochrony antywirusowej ma znaczenie krytyczne!
- Pobieranie pakietów typu delta (różnicowych) od ostatniej aktualizacji przyczynia się do oszczędności związanych z pracą w trybie online oraz redukuje obciążenie pasma niezbędnego do transmisji przez sieć.
- Możliwa jest losowa aktywacja funkcji LiveUpdate, aby stacje klienckie nie pobierały aktualizacji jednocześnie blokując serwer i pasmo - zwiększa to przepustowość sieci!
- Możliwe jest ponowne uruchomienie niewykonanych zadań, aby stacje klienckie zawsze miały aktualne definicje nawet wtedy, gdy w zaplanowanym czasie aktualizacji nie było to możliwe.
- Kontynuacja pobierania uaktualnień od momentu przerwania połączenia - redukcja czasu pobierania aktualizacji nawet przy złej jakości połączeniu.

Administrator LiveUpdate

- Pozwala na wewnętrzne skonfigurowanie serwisu LiveUpdate, który:
    - pobiera aktualizacje definicji wirusów wprost od firmy Symantec w uprzednio określonym czasie lub w regularnych odstępach;
    - przekazuje definicje wirusów do wewnętrznego serwera centralnego;
    - umożliwia użytkownikom oraz administratorom szybkie i łatwe pobranie nowych definicji wirusów wprost na komputery biurkowe i serwery.
- Gwarantuje, że firma podlega stałemu zabezpieczeniu przed zagrożeniami związanymi z najnowszymi wirusami.

- Upraszcza administrację (wystarczy raz ustalić zadanie w harmonogramie LiveUpdate, a dalsza obsługa ze strony administratora staje się zbędna).
- Przynosi oszczędności dzięki możliwości ustalenia czasu aktualizacji na godziny poza szczytem.
- Redukuje ruch w sieci dzięki wyeliminowaniu potrzeby odwiedzania zewnętrznej witryny firmy Symantec w celu uzyskania nowych definicji wirusów.

Dysk awaryjny *(Rescue Disk)*

- Zapewnia bezpieczeństwo sieci, gdy wirus uniemożliwia rozruch systemu. Użytkownicy tworzą dyski rozruchowe wraz z zabezpieczeniami przed wirusami, które usuwają infekcję, gdy system Windows nie chce się uruchomić, i informują o błędach.