SPRZĘTOWE ELEMENTY BEZPIECZEŃSTWA

Sprzęt komputerowy zawsze odgrywał główną rolę w bezpieczeństwie komputerów. Z biegiem lat ta rola wzrosła dramatycznie, ze względu zarówno na wzrost mocy obliczeniowej, pojemności pamięci i możliwości komunikacyjnych, jak i na zmniejszenie kosztów i wielkości komponentów. Wszechobecność tanich, wydajnych i wysoko połączonych urządzeń komputerowych stanowi poważne wyzwanie dla bezpieczeństwa komputerowego. Jednocześnie wyzwania stawiane przez duże, scentralizowane systemy komputerowe nie zmniejszyły się. Zrozumienie elementów sprzętowych komputerów ma zatem kluczowe znaczenie dla dobrze rozumianego rozumienia bezpieczeństwa komputerowego.

PROJEKT BINARNY

Chociaż istnieją duże różnice między architekturami komputerów i konstrukcjami sprzętu komputerowego, wszystkie mają co najmniej jedną wspólną cechę: wykorzystują one unikalnie zakodowaną serię impulsów elektrycznych do reprezentowania dowolnej postaci w ich zasięgu. Podobnie jak kod Morse'a z kropkami i myślnikami, kody impulsów komputerowych mogą być połączone razem w celu przekazania informacji alfabetycznej lub numerycznej. Jednak w odróżnieniu od alfabetu Morse'a komputerowe ciągi impulsowe mogą być również łączone w operacjach matematycznych lub manipulacja danymi. W 1946 r. Dr John von Neumann, w Institute for Advanced Study of Princeton University, po raz pierwszy opisał w formalnym raporcie, w jaki sposób można zastosować binarny system liczb w komputerowych implementacjach. System binarny wymaga kombinacji tylko dwóch cyfr, 0 i 1, aby reprezentować dowolną cyfrę, literę lub symbol, a przez to dowolną grupę cyfr, liter lub symboli. W przeciwieństwie do tradycyjnego systemu dziesiętnego który wymaga kombinacji 10 różnych liczb, od 0 do 9, liter od a do z, oraz dużej liczby symboli, aby przekazać te same informacje. Von Neumann zdawał sobie sprawę, że elementy elektryczne i elektroniczne można uznać za posiadające tylko dwa stany, włączane i wyłączane oraz że te dwa stany mogą odpowiadać 0 i 1 systemu dwójkowego. Jeśli włączanie i wyłączanie elementu komputerowego odbywało się z dużą szybkością, otrzymane wyniki napięcia lub prądu najlepiej byłoby opisać jako impulsy. Pomimo 60 lat intensywnych innowacji w sprzęcie komputerowym i wprowadzenia niektórych optycznie opartych metod reprezentacji danych, charakter tych elektrycznych impulsów i sposób ich obsługi pozostają ostateczną miarą dokładności i niezawodności komputera.

CHARAKTERYSTYKA IMPULSÓW

Idealnie, kształt fali pojedynczego impulsu powinien być prostoliniowy, o płaskim wierzchołku, o dokładnie określonym czasie trwania, amplitudzie i zależności fazowej od innych impulsów w szeregu. To wyjątkowa zaleta komputerów cyfrowych, że można je zaprojektować tak, aby działały z ich pierwotną dokładnością, pomimo znacznego pogorszenia charakterystyki impulsów. Błędy będą jednak występować, gdy pewne limity zostaną przekroczone, a tym samym naruszona zostanie integralność danych. Ponieważ te błędy są trudne do wykrycia, ważne jest ustalenie harmonogramu konserwacji zapobiegawczej i rygorystyczne jej przestrzeganie. Tylko w ten sposób operatorzy mogą wykryć pogorszoną wydajność zanim będzie wystarczająco ostry, aby wpłynąć na niezawodność.

OBWODY

Aby generować impulsy o pożądanych właściwościach i prawidłowo nimi manipulować, wymagane są elementy o jednolitej jakości i niezawodności. Aby obniżyć koszty produkcji, ułatwić konserwację i wymianę, a ogólnie poprawić niezawodność, projektanci komputerów starają się używać jak najmniej różnych rodzajów komponentów i włączać dużą liczbę każdego typu do dowolnej maszyny. Komputery pierwszej generacji używały aż 30 000 lamp próżniowych, głównie w półdozenowych typach

elementów logicznych. Podstawowymi obwodami były klapki lub bramki, które wytwarzały impuls wyjściowy za każdym razem, gdy dany zestaw impulsów wejściowych był obecny. Jednakże, lampy próżniowe generowały intensywne ciepło, nawet w stanie czuwania. W konsekwencji, użyteczny czas działania między awariami był stosunkowo krótki. Wraz z rozwojem diod półprzewodnikowych i tranzystorów komputery stały się znacznie mniejsze i znacznie chłodniejsze niż ich poprzedniczki lamp próżniowych. Dzięki postępowi w projektowaniu logiki, pojedynczy typ bramki, taki jak obwód Nie-I (NAND), mógłby zastąpić wszystkie inne elementy logiczne. Uzyskana w ten sposób poprawa kosztów i niezawodności została przyspieszona dzięki zastosowaniu monolitycznych układów scalonych. Nie mniej ważna jest ich znacznie większa szybkość działania. Od tego czasu między awarie obwodów elektronicznych komputera są zwykle niezależne od liczby wykonanych operacji, co oznacza, że przepustowość wzrasta bezpośrednio wraz z prędkością; prędkość jest definiowana jako szybkość, z jaką komputer uzyskuje dostęp, porusza się i manipuluje danymi. Ostatecznym ograniczeniem prędkości komputera jest czas wymagany do przejścia sygnału z jednego elementu fizycznego do drugiego. Przy prędkości 299 792 458 metrów na sekundę (186 282 mil na sekundę) w próżni, sygnał elektryczny przesuwa się o 3,0 metra lub 9,84 stopy w 10 nanosekundach (0,000 000,01 sekundy). Gdyby komponenty były tak duże, jak były pierwotnie, a w konsekwencji tak odległe od siebie, dzisiejsze nanosekundowe prędkości komputera byłyby oczywiście niemożliwe, podobnie jak zwiększona przepustowość i niezawodność, które są obecnie powszechne.

KODOWANIE

W typowej aplikacji dane mogą być tłumaczone i ponownie tłumaczone automatycznie na kilka różnych kodów tysiące razy na sekundę. Wiele z tych kodów reprezentuje wcześniejsze technologie zachowane ze względu na kompatybilność wsteczną i wyłącznie ekonomiczne. W każdym danym kodzie każdy znak pojawia się jako określona grupa impulsów. W każdej grupie każda pozycja impulsu jest znana jako bit, ponieważ reprezentuje jedną z dwóch cyfr binarnych, 0 lub 1. Bajt to nazwa oryginalnie zastosowana do najmniejszej grupy bitów, które można odczytać i zapisać (dostęp lub adres) jako jednostkę. Dzisiaj bajt jest zawsze uważany przez konwencję za 8 bitów. W nowoczesnych systemach bajt jest postrzegany jako jednostka pamięci dla jednego amerykańskiego standardowego kodu wymiany informacji (ASCII), chociaż nowsze systemy, takie jak Unicode, które obsługują międzynarodowe znaki akcentowane i wiele innych symboli, używają do 4 bajtów na znak . Zgodnie z konwencją większość ludzi używa prefiksów metrycznych (kilo-, mega-, giga-, tera-) do wskazania kolekcji bajtów; zatem KB odnosi się do kilobajtów i jest zwykle definiowany jako 1024 bajty. Poza polem przetwarzania danych K zwykle wskazywałby na mnożnik 1000. Ze względu na niejednoznaczność definicji zaproponowano Amerykański Narodowy Instytut Norm i Technologii (NIST), a w 2000 r. Powołała Międzynarodową Komisję Elektrotechniczną i nowy zestaw jednostek do przechowywania informacji lub komputera. Jednostki te są ustalane przez serię przedrostków skazujących potęgę 2; w tym schemacie KB oznacza kibibity i odnosi się wyłącznie do 1024 (2^{10} lub ~ 10^3) bajtów. Jednakże, kibibity, mibibity (2^{20} lub ~10^6), gibibity (2^{30} lub ~10^9) i tebibity (2^{40} lub ~ 10^{12}) są terminami, które nie są jeszcze szeroko stosowane. Ponieważ tłumaczenia między systemami kodowania są realizowane z niewielkim kosztem, brakuje prawdziwej zachęty do ujednolicenia różnych systemów. Jednak wszystkie ruchy danych i tłumaczenia zwiększają prawdopodobieństwo błędów wewnętrznych, dlatego też kontrole parzystości i testy ważności stały się niezbędne.

PARZYSTOŚĆ

Redundancja jest kluczem do bezbłędnego przetwarzania danych. Uwzględniając dodatkowe bity we wcześniej określonych lokalizacjach, niektóre rodzaje błędów można wykryć natychmiast, sprawdzając te metadane (dane o oryginalnych danych). W typowej aplikacji dane przesuwają się tam i z powrotem wiele razy, między pamięcią podstawową, pamięcią dodatkową, urządzeniami wejściowymi i

wyjściowymi, a także za pośrednictwem łączy komunikacyjnych. Podczas tych ruchów dane mogą utracić integralność przez upuszczenie 1 lub większej liczby bitów, poprzez wprowadzenie wprowadzonych dodatkowych bitów i losowe zmiany w określonych bitach. Aby wykryć niektóre z tych zdarzeń, bity parzystości są dodawane przed przeniesieniem danych i są sprawdzane później.

PIONOWE KONTROLE NADMIAROWOŚCI

W tym stosunkowo prostym i niedrogim schemacie, początkowo ustalane jest, czy w każdym znaku powinna być parzysta lub nieparzysta liczba "1" bitów. Na przykład, używając binarnie kodowanej reprezentacji dziesiętnej liczby "5", stwierdzamy, że 6-bitowa grupa impulsów 000101 zawiera dwie 1-nki, parzystą liczbę. Dodając siódmą pozycję do grupy kodu, możemy mieć albo rodzaj parzystości. Jeśli wybrano nieparzystą parzystość, 1 zostanie dodane w pozycji najbardziej na lewo od pozycji kontrolnej:

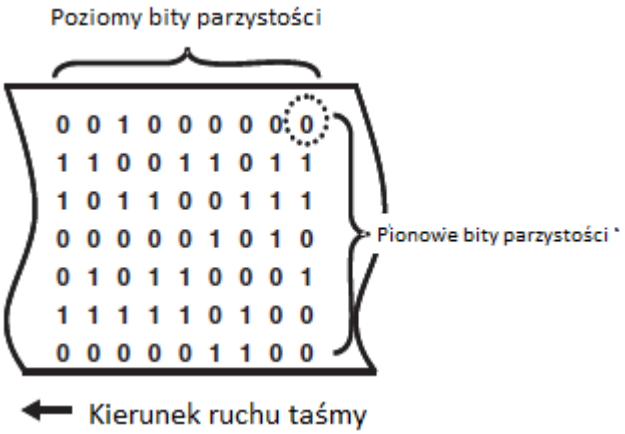
Nieparzystość parzystość 1000101 trzy 1-nki

Parzysta parzystość 0000101 dwie 1-nki

Po każdym ruchu liczba 1 bitów byłaby zliczana, a jeśli nie była liczbą nieparzystą, przyjmowany byłby błąd, a przetwarzanie wstrzymane. Oczywiście, jeśli 2 bity lub dowolna liczba parzysta zostały niewłaściwie przesłane, żaden błąd nie zostałby wskazany, ponieważ liczba bitów "1" byłaby wciąż nieparzysta. Aby rozwiązać problem niejednolitości każde z nich 4-, 5-, 6-, 7-, 8- i 16-bitowe grupy kodów mogą mieć dodatkowy bit dodany do sprawdzania parzystości. Ponadto może występować niespójność nieparzystości lub parzystości między producentami, a nawet między różnymi urządzeniami pochodzącymi od jednego dostawcy.

POZIOME TESTY NADMIAROWOŚCI

Błędy mogą nie zostać wykryte przez samą kontrolę redundancji pionowej (VRC), z powodów właśnie omówionych. Dodatkowym zabezpieczeniem, szczególnie przydatnym w transmisji danych i rejestrowaniu nośników, takich jak taśmy i dyski, jest kontrola podłużnej redundancji (LRC). Dzięki tej technice dodatkowy znak jest generowany po pewnej z góry określonej liczbie znaków danych. Każdy bit w dodatkowej postaci zapewnia parzystość dla odpowiadającego mu wiersza, tak jak robią to pionowe bity parzystości dla odpowiednich kolumn. Tu przedstawiamy oba typy, ponieważ zostałyby zapisane na 7-ścieżkowej taśmie magnetycznej.



Jeden kawałek został zakreślony, aby pokazać, że jest niejednoznaczny. Ten bit pojawia się na przecięciu wiersza parzystości i kolumny parzystości i musi być z góry ustalony, aby był poprawny dla jednego lub drugiego, ponieważ może nie być poprawny dla obu. Na ilustracji niejednoznaczny bit jest poprawny w przypadku nieparzystego wymogu parzystości kolumny znaku VRC; jest niepoprawny dla

równej parzystości LRC bitowy rząd. W praktyce pionowe paski kontrolne byłyby dołączone do każdej kolumny znaków, jak pokazano, ale bity podłużne byłyby zgodne z blokiem danych, który może zawierać od 80 do kilkuset znaków. Gdy możliwe jest użycie zarówno LRC, jak i VRC, każdy pojedynczy błąd danych w bloku będzie zlokalizowany na przecięciu niepoprawnych bitów parzystości wiersza i kolumny. Wskazany bit może następnie zostać poprawiony automatycznie. Ograniczenia tej metody są następujące: (1) wielokrotnych błędów nie można skorygować, (2) błędu w niejednoznacznej pozycji nie można skorygować, oraz (3) błędu, który nie generuje zarówno wskazania VRC, jak i LRC, nie można skorygować.

CYKLICZNE KONTROLE NADMIAROWOŚCI

Gdy koszt błędu danych może być wysoki, uzasadniony jest dodatkowy koszt cyklicznych kontroli nadmiarowych (CRC). W tej technice stosuje się stosunkowo dużą liczbę nadmiarowych bitów. Na przykład każdy 4-bitowy znak wymaga 3 bitów parzystości, podczas gdy 32-bitowe słowo na komputerze wymaga 6 bitów parzystości. Dodatkowe miejsce jest wymagane w pamięci głównej i dodatkowej, a transmisja trwa dłużej niż bez takich kontroli. Zaletą jest jednak to, że każdy pojedynczy błąd może być wykryty, zarówno w bicie danych, jak i w bicie parzystości, a jego lokalizacja może być pozytywnie zidentyfikowana. W prostym elektronicznym procesie uzupełniania niepoprawne 0 jest konwertowane na 1 i na odwrót.

KODY SAMOKONTROLI

Stosuje się kilka rodzajów kodów, które z natury zawierają zdolność sprawdzania podobną do tej w systemie parzystości. Typowym z nich jest kod 2 do 5, w którym każda cyfra dziesiętna jest reprezentowana przez bitową konfigurację zawierającą dokładnie dwa 1 i trzy 0. Jeżeli test parzystości polegałby na zliczaniu 1s, aby sprawdzić, czy ich liczba była nieparzysta czy parzysta, test 2 na 5 wskazywałby błąd, gdy liczba 1 była mniejsza lub równa 2.

OPERACJE SPRZĘTOWE

Wejście, wyjście i przetwarzanie to trzy podstawowe funkcje każdego komputera. Aby chronić integralność danych podczas tych operacji, dostępnych jest kilka funkcji sprzętowych.

* Read-after-write. W napędach dyskowych i taśmowych powszechną praktyką jest odczytywanie danych natychmiast po ich zarejestrowaniu i porównywanie ich z oryginalnymi wartościami. Każda niezgodność oznacza błąd, który wymaga przepisania.

* Echo. Dane przesyłane do urządzenia peryferyjnego, do terminala zdalnego lub do innego komputera mogą być generowane w celu wygenerowania sygnału zwrotnego. To echo jest porównywane z oryginalnym sygnałem, aby zweryfikować poprawność odbioru. Zawsze jednak istnieje ryzyko wystąpienia błędu w sygnale zwrotnym i fałszywego oznaczenia błąd w oryginalnej transmisji.

* Przepełnienie. Maksymalny zakres wartości numerycznych, które może pomieścić dowolny komputer, jest ustalany na podstawie jego projektu. Jeśli program jest nieprawidłowo skalowany lub wymagana jest operacja niemożliwa, taka jak dzielenie przez zero, wynik operacji arytmetycznej może przekroczyć dopuszczalny zakres, powodując błąd przepełnienia. Wcześniejsze komputery wymagały zaprogramowanych instrukcji wykrywania nadmiarowości, ale teraz ta funkcja jest ogólnie dostępna i jest realizowany przez elementy sprzętowe na poziomie maszyny. Nadmiarowość w ramach programów aplikacyjnych musi być nadal przetwarzana w oprogramowaniu. (Faktycznie, niewykonanie tego może spowodować, że oprogramowanie będzie nadużywane przez złośliwe strony.)

* Walidacja. W dowolnym systemie kodowania komputerowego niektóre wzorce bitowe mogą być nieprzypisane, a inne mogą być nielegalne. Na przykład w IBM System / 360 Extended Binary Coded Decimal Interchange Code (EBCDIC) liczba 9 jest reprezentowana przez 11111001, ale 11111010 jest nieprzypisany. Kontrola parzystości nie wykryłaby drugiej grupy jako błędnej, ponieważ obie mają tę samą liczbę 1 bitów. Sprawdzenie ważności odrzuci jednak konfigurację drugiego bitu jako niepoprawną. Podobnie niektóre wzorce bitów reprezentują przypisane kody instrukcji, podczas gdy inne tego nie robią. W jednym komputerze instrukcja zamiany liczb w formacie spakowanym na liczby dziesiętne strefowe to 11110011 lub F3 w zapisie heksadecymalnym; 11110101 lub F5 jest nieprzypisane, a sprawdzenie ważności spowoduje zatrzymanie przetwarzania za każdym razem ta instrukcja została przetestowana.

* Replikacja. W wysoce wrażliwych aplikacjach, dobrą praktyką jest zapewnienie sprzętu do backupu na miejscu, do natychmiastowego przełączenia w przypadku awarii komputera podstawowego. Z tego powodu rozsądnie jest zachować dwa identyczne, mniejsze komputery zamiast zastępować je jedną jednostką o równoważnej lub nawet większej mocy. Odporne na awarie lub odporne na awarię komputery korzystają z dwóch lub więcej procesorów pracujących jednocześnie, dzielących ładunek i wymieniających informacje o bieżącym statusie powtarzających się równolegle procesów. Jeśli jeden z procesorów zawiedzie, inny kontynuuje przetwarzanie bez pauzy.

Wiele wrażliwych aplikacji, takich jak systemy rezerwacji biletów lotniczych, ma szerokie możliwości transmisji danych. Ważne jest, aby cały ten sprzęt był duplikowany, a także same komputery. (Awaria systemu rezerwacji biletów lotniczych, jeśli może przekroczyć stosunkowo niewielką liczbę godzin, może doprowadzić do awarii samej linii lotniczej). Wymiana powinna być również natychmiast dostępna dla urządzeń peryferyjnych. W niektórych systemach operacyjnych konieczne jest poinformowanie systemu, że urządzenie jest wyłączone i ponowne przypisanie jego funkcji do innej jednostki. W bardziej wyrafinowanych systemach uszkodzone urządzenie jest automatycznie wycinane i wymieniane. Na przykład nowojorska giełda obsługuje i utrzymuje dwa identyczne systemy transakcyjne, aby niepowodzenie systemu podstawowego nie powodowało żadnych zakłóceń w handlu.

PRZERWANIA

Sekwencja operacji wykonywanych przez system komputerowy jest określona przez grupę instrukcji: program. Jednak wiele zdarzeń występujących podczas operacji wymaga odchyleń od zaprogramowanej sekwencji. Przerwania są sygnałami generowanymi przez elementy sprzętowe, które wykrywają zmienione warunki i inicjują odpowiednie działanie. Pierwszym krokiem jest natychmiast zapisanie statusu różnych elementów we wstępnie przypisanych miejscach pamięci. Określone zapisane wzorce bitów, potocznie zwane słowami statusu programu, zawierają informacje niezbędne do zidentyfikowania przez komputer przyczyny przerwania, podjęcia działania w celu jej przetworzenia, a następnie powrotu do właściwej instrukcji w sekwencji programu po przerwaniu wyczyszczone.

RODZAJE PRZERWAŃ

Pięć rodzajów przerwań jest w powszechnym użyciu. Każdy z nich ma znaczenie w ustanawianiu i utrzymywaniu integralności przetwarzania danych

Przerwania wejścia / wyjścia : Przerwania wejścia / wyjścia (I / O) są generowane za każdym razem, gdy dostępne jest urządzenie lub kanał, który był zajęty. Ta zdolność jest niezbędna, aby uzyskać bezbłędne wykorzystanie zwiększonej przepustowości zapewnianej przez buforowanie, nakładanie przetwarzania i multiprogramowanie. Po każdym przerwaniu wejścia / wyjścia sprawdza się, czy dane

zostały odczytane lub zapisane bez błędów. Jeśli tak, można rozpocząć następną operację wejścia / wyjścia; w przeciwnym razie inicjowana jest procedura odzyskiwania po błędzie. Liczba przypadków wystąpienia tych błędów powinna być tak, aby pogorszona wydajność mogła zostać wykryta i skorygowana.

Wywołania supervisora : Organ nadzorczy lub monitor jest częścią oprogramowania systemu operacyjnego, który kontroluje interakcje między wszystkimi elementami sprzętu i oprogramowania. Każda prośba o odczyt lub zapis danych jest zaplanowana przez przełożonego, gdy zostanie do tego wezwany. Przerwania we / wy są również obsługiwane przez wywołania nadzorców, które koordynują je za pomocą żądań odczytu / zapisu. Ładowanie, wykonywanie i kończenie programów są inne ważne funkcje inicjowane przez wywołania superwizora.

Przerwanie kontroli programu : Niewłaściwe użycie instrukcji lub danych może spowodować przerwanie kończące program. Na przykład próba podziału przez zero i operacje powodujące przepełnienie arytmetyczne są anulowane. Nieprzypisane kody instrukcji, próby uzyskania dostępu do chronionej pamięci i nieprawidłowe adresy danych są innymi rodzajami wyjątków, które powodują przerwania w sprawdzaniu programu.

Przerwy w kontroli maszyny : Wśród wyjątków, które spowodują, że przerwania sprawdzania maszynowego są błędy parzystości, uszkodzone sektory dysku, odłączenie urządzeń peryferyjnych i wadliwe moduły obwodów. Ważne jest, aby postępować zgodnie z odpowiednimi procedurami, aby wyczyścić kontrole maszyny bez utraty danych lub błędu przetwarzania.

Przerwania zewnętrzne : Przerwania zewnętrzne są generowane przez działanie zegara, przez naciśnięcie klawisza przerywania lub przez sygnały z innego komputera. Gdy dwie centralne jednostki przetwarzania są ze sobą połączone, sygnały przechodzące między nimi inicjują zewnętrzne przerwania. W ten sposób sterowanie i synchronizacja są utrzymywane w sposób ciągły, podczas gdy programy, dane i urządzenia peryferyjne mogą być współdzielone i koordynowane. W komputerach typu mainframe zegar elektroniczny jest zwykle uwzględniany w centralnej jednostce procesora dla wpisów czasowych dzienników zadań i pomiarów z upływem czasu. Jako interwał czasowy zegar można ustawić tak, aby generował przerwanie po określonym czasie. Ta funkcja powinna być używana jako środek bezpieczeństwa, zapobiegający pozostawaniu na komputerze wrażliwych zadań na wystarczająco długo, aby umożliwić nieuprawnione manipulowanie danymi lub instrukcjami.

PUŁAPKOWANIE

Pułapkowanie to rodzaj odpowiedzi sprzętowej na przerwanie. W celu wykrycia wyjątku, bezwarunkowa gałąź zostaje przeniesiona do pewnej z góry określonej lokalizacji. Instrukcja przekazuje kontrolę do procedury nadzoru, która inicjuje odpowiednie działanie.

PAMIĘĆ I PRZECHOWYWANIE DANYCH

Tak jak ludzki umysł podlega aberracjom, tak samo jest z pamięcią komputera. W interesie bezpieczeństwa i integralności danych opracowano różne środki terapeutyczne dla kilku rodzajów przechowywania.

PAMIĘĆ GŁÓWNA

Pamięć o dostępie swobodnym (RAM) i jej pochodne, takie jak dynamiczna pamięć RAM (DRAM), synchroniczna pamięć DRAM (SDRAM, wprowadzona w 1996 r. i działająca z częstotliwością 133 megaherców [MHz]) oraz DDR-3 (SDRAM z podwójną przepływnością danych w 2005 r. i działający z częstotliwością 800 MHz) należy dzielić niezbędną jakość łatwego i szybkiego dostępu do odczytu i

zapisu danych. Niestety, ta niezbędna cecha jest jednocześnie potencjalnym źródłem trudności w utrzymaniu integralności danych przed niechcianymi operacjami odczytu / zapisu. Problemy są znacznie zintensyfikowane w środowisku multiprogramowania, szczególnie przy dynamicznym przydzielaniu pamięci, gdzie istnieje możliwość, że jeden program zapisze nieprawidłowo dane innego użytkownika w pamięci. Ochrona przed tym typem błędu musi być zapewniona przez system operacyjny. Jedna forma ochrony wymaga podziału pamięci głównej na bloki lub strony; na przykład 2048 ośmiobitowych bajtów każdy. Strony mogą być oznaczone jako tylko do odczytu, jeśli zawierają stałe, tabele lub programy, które mogą być udostępniane przez wielu użytkowników. Ponadto stronom, które mają być niedostępne, z wyjątkiem wyznaczonych użytkowników, można przypisać blokadę za pomocą odpowiednich instrukcji programu. Jeśli odpowiedni klucz nie zostanie uwzględniony w programie użytkownika, dostęp do tej strony zostanie odrzucony. Ochronę można zapewnić wyłącznie przed pisaniem lub przed czytaniem i pisaniem.

PAMIĘĆ TYLKO DO ODCZYTU

Jedną z wyróżniających cech pamięci głównej jest bardzo duża prędkość, z jaką dane mogą być wprowadzane lub odczytywane. Zestaw procedur sekwencyjnych, które realizują tę i inne funkcje, to program, a programista ma pełną swobodę łączenia ważnych instrukcji w znaczący sposób. Jednak niektóre operacje, takie jak uruchamianie systemu lub uruchamianie, są często i rutynowo wymagane i mogą być wykonywane automatycznie przez wstępnie zaprogramowaną grupę elementów pamięci. Elementy te powinny być chronione przed nieumyślnymi lub nieautoryzowanymi zmianami. W tym celu opracowano klasę elementów pamięci, które po zaprogramowaniu nie mogą być w ogóle zmienione lub wymagają stosunkowo długiego czasu. Elementy te nazywane są pamięcią tylko do odczytu lub ROM; proces, w którym instrukcje sekwencyjne są ustawione na te elementy, jest znany jako mikroprogramowanie. Technikę tę można wykorzystać, gdy integralność danych jest chroniona przez wyeliminowanie możliwości błędu programisty. Warianty tej zasady obejmują programowalne pamięci tylko do odczytu (PROM) i kasowalna, programowalna pamięć tylko do odczytu (EPROM), z których wszystkie łączą mikroprogramowanie z nieco większym stopniem elastyczności niż sama pamięć tylko do odczytu. Dane na tych układach można zmienić za pomocą specjalnej operacji, często nazywanej flashowaniem (dosłownie ekspozycja na silne światło ultrafioletowe, różni się ona od używanej obecnie pamięci flash do przechowywania takich danych, jak cyfrowe pliki muzyczne i zdjęcia cyfrowe - wrócimy do temat pamięci flash później).

PAMIĘĆ DODATKOWA

Termin "pamięć wtórna" tradycyjnie był używany do opisywania przechowywania, takiego jak dyski magnetyczne, dyskietki, taśmy i kasety z taśmą. Chociaż dyskietka magnetyczna o pojemności 1,44 megabajta (MB) jest przestarzała, to magnetyczny dysk twardy o pojemności do terabajtów pozostaje istotnym elementem praktycznie wszystkich komputerów, a zewnętrzne dyski twarde o pojemności terabajta wielkości książki w miękkiej oprawie są teraz dostępne od ręki za kilkaset dolarów. Nowszym opracowaniem są dyski optyczne, takie jak wymienna, kompaktowa pamięć tylko do odczytu (CD-ROM), oryginalnie udostępniona we wczesnych latach 80-tych, która jest przydatna do długoterminowego przechowywania danych archiwalnych na poziomie około 700 MB na płycie. Hybrydowe formy również istnieją, na przykład płyty CD-R, które można zapisać raz, oraz płyty CD-RW, które obsługują wielokrotne odczyty i zapisy. Cyfrowy dysk wideo (DVD), lub tak jak go zmieniono, cyfrowy uniwersalny dysk, został wprowadzony w 1997 roku i zapewnia pojemności od 4,7 gigabajta (GB) na dysk do 30 GB do archiwizacji danych. Dyski optyczne o większej pojemności wykorzystują technologię Blu-ray wprowadzoną w 2002 roku i mogą przechowywać po 25 GB na stronę; zwykle są używane do dystrybucji filmów, ale dyski BD-R (jednorazowego użytku) i BD-RE (wielokrotnego zapisu) mają duży potencjał w zakresie uogólnionego przechowywania danych. Najnowszym dodatkiem do

pamięci dodatkowej jest pamięć RAM, która symuluje dyski twarde, znane jako pamięć flash. Pochodzący z elektrycznych EPROM (EEPROM) i wprowadzony przez firmę Toshiba w latach 80-tych, ten rodzaj pamięci istnieje obecnie w wielu różnych formatach, w tym stosunkowo niedrogich tokenach Universal Serial Bus (USB) o pojemnościach pamięci teraz w zakresie gigabajtów. Urządzenia te pojawiają się jako zewnętrzne dyski po podłączeniu do komputera osobistego typu plug-and-play. Innym formatem pamięci flash są małe karty o wielu rozmiarach znaczków pocztowych, które można umieszczać w telefonach komórkowych, aparatach fotograficznych, drukarkach i innych urządzeniach, a także komputerach. Zabezpieczenia sprzętowe opisane wcześniej, takie jak nadmiarowość, ważność, parzystość i odczyt po zapisie, mają znaczenie dla zachowania integralności pamięci wtórnej. Te zabezpieczenia są wbudowane w urządzenie i zawsze działają, o ile nie są wyłączone lub działają nieprawidłowo. Inne środki ostrożności są opcjonalne, takie jak standardowe procedury wewnętrznego etykietowania napędów, taśm i dysków. Standardowe wewnętrzne etykiety mogą zawierać numery identyfikacyjne, liczbę rekordów oraz daty utworzenia i wygaśnięcia. Chociaż pomocne, zewnętrzne etykiety z tworzywa sztucznego lub papieru na nośnikach nagrywalnych nie są wystarczającym zamiennikiem generowanych komputerowo etykiet, magnetycznie wpisanych na samym nośniku i automatycznie sprawdzane za pomocą zaprogramowanych instrukcji. Innym środkiem bezpieczeństwa, który czasami jest podważany, jest ochrona przed zapisem na nośnikach wymiennych. Blokady sprzętowe uniemożliwiają zapisywanie do nich. Te blokady powinny zostać aktywowane natychmiast po usunięciu nośnika z systemu. Niewykonanie tej czynności spowoduje zniszczenie danych, jeśli te same media zostaną niewłaściwie użyte przy innej okazji. Dyski twarde, dyski optyczne i karty pamięci flash są klasyfikowane jako urządzenia do bezpośredniego dostępu (DASD). W przeciwieństwie do taśm magnetycznych z ich wyłącznie sekwencyjnym przetwarzaniem, DASD mogą przetwarzać dane zarówno losowo, jak i sekwencyjnie. Ta możliwość jest niezbędna w operacjach online, w których nie można sortować transakcji przed przetworzeniem. Wadą bezpośredniego dostępu jest to, że może istnieć mniejsza kontrola nad wpisami i większa szansa na degradację systemu niż w przypadku sekwencyjnego przetwarzania wsadowego. Jedno z możliwych źródeł błędów DASD wynika z dużej prędkości obrotowej nośnika zapisu oraz, z wyjątkiem urządzeń head-per-track, również ruchu głowic. Aby zminimalizować tę możliwość, obszary na powierzchni zapisu mają swoje adresy magnetycznie wpisane. Gdy komputer kieruje dane do odczytu z lub do określonej lokalizacji, adres w pamięci głównej jest porównywany z odczytem z DASD. Tylko wtedy, gdy będzie zgoda, operacja zostanie wykonana. Poprzez odpowiednie programowanie można zapewnić integralność danych. Oprócz sprawdzania adresu, można dokonać porównania na numerach identyfikacyjnych lub na kluczowych polach w każdym rekordzie. Chociaż dodatkowy czas przetwarzania jest zwykle nieistotny, może nastąpić znaczna poprawa w zakresie prawidłowego księgowania transakcji. Kilka innych środków bezpieczeństwa często włącza się do DASD. Jedna jest podobna do funkcji ochrony w pamięci głównej i polega na określaniu "zakresów" dla każdego zestawu danych. Jeśli te wartości, które są po prostu górną i dolną granicą adresów pliku danych, zostaną przekroczone, zadanie zostanie przerwane. Kolejny środek bezpieczeństwa wynika z faktu, że uszkodzone obszary na powierzchni dysku mogą powodować błędy niewykrywalne podczas normalnych operacji. Aby zminimalizować tę możliwość, dyski powinny być testowane i certyfikowane przed użyciem, a następnie okresowo. Dalsze informacje są dostarczane przez systemy operacyjne, które rejestrują liczbę napotkanych błędów dysku. Ponowne formatowanie lub wymiana musi zostać zamówiona, gdy błędy przekroczą wcześniej określony poziom. Wiele dysków twardych komputerów osobistych ma teraz pewną formę samokontroli, analizy i raportowania (SMART). Opracowany na podstawie wcześniejszych technologii, takich jak IBM Predictive Failure Analysis (PFA) i Intellisafe firmy Compaq, producenta dysków Seagate, Quantum i Conner, SMART może ostrzegać operatorów o potencjalnych problemach z napędem. Niestety wdrożenie SMART nie jest znormalizowane i ma potencjał prewencyjny prognozy dotyczące konserwacji i awarii są często pomijane. Zauważ, że SMART

różni się od zakresu technologii stosowanych do ochrony dysków twardych przed awariami. Awaria głowicy występuje, gdy komponent odczytujący dane z dysku faktycznie dotyka powierzchni dysku, potencjalnie uszkadzając go i dane na nim przechowywane. Wiele dysków twardych ma systemy, które umożliwiają wycofanie głowic z dysku przed wystąpieniem takiego kontaktu. Te środki ochronne osiągnęły punkt gdzie aktywny dysk twardy może być noszony przy względnym bezpieczeństwie jako część odtwarzacza muzyki i wideo (np. Apple iPod lub Microsoft Zune)

CZAS

W sali komputerowej i wielu biurach zazwyczaj dominuje zegar ścienny. Nie ma wątpliwości, że ten wskaźnik czasu rzeczywistego ma znaczenie w planowaniu i regulowaniu funkcji ludzi i maszyn, ale wewnętrzne czasy działania komputera są ważniejsze dla bezpieczeństwa.

SYNCHRONICZNY

Wiele operacji komputerowych jest niezależnych od pory dnia, ale musi utrzymywać dokładne relacje z jakimś wspólnym czasem i ze sobą. Przykłady tej synchronizacji obejmują działanie bramek, przerzutników i rejestrów oraz transmisję danych z dużą prędkością. Synchronizację uzyskuje się na różne sposoby. W przypadku bram i innych elementów obwodu, zegary elektroniczne zapewniają dokładność rozmieszczonych impulsów z wysoką częstotliwością, podczas gdy napędy dyskowe i taśmowe są utrzymywane z prędkością znamionową przez serwomotory sterujące w oparciu o częstotliwość linii elektroenergetycznej. Ze wszystkich błędów komputerowych najtrudniejsze do wykrycia i skorygowania są prawdopodobnie te spowodowane niespójnościami czasowymi. Wewnętrzne zegary mogą wytwarzać 1 miliard impulsów na sekundę (zwanych 1 gigahercem [GHz]) lub więcej, gdy komputer jest włączony. Utrata nawet pojedynczego impulsu lub jego losowe odkształcenie lub opóźnienie może spowodować niewykryty błędy. Bardziej kłopotliwy jest fakt, że nawet jeśli zostaną wykryte błędy, ich przyczyny mogą nie zostać zidentyfikowane, chyba że przypadkowe błędy czasowe stają się częste lub spójne. Przykład podstępnego charakteru usterek czasowych jest konsekwencją fluktuacji mocy elektrycznej, gdy napięcie spada poniżej normy. Podczas tych nieustalonych zmian napięcia dyski mogą zwolnić; jeśli sektory są rejestrowane, ich rozmiar fizyczny będzie odpowiednio mniejszy. Następnie, po przywróceniu prawidłowego napięcia, nieprawidłowe rozmiary sektorów mogą powodować błędy danych lub utratę danych.

ASYNCHRONICZNY

Niektóre operacje nie występują w ustalonych odstępach czasu i dlatego są określane jako "asynchroniczne". W tym trybie sygnały generowane po zakończeniu jednej akcji inicjują następującą. Przykładowo, transmisje danych o niskiej prędkości, takie jak te, które używają zwykłych modemów, są zwykle asynchroniczne. Zakodowane sygnały generowane przez przypadkowe naciśnięcie klawiszy klawiatury są niezależne od impulsów zegarowych

NATURALNE ZAGROŻENIA

Aby zachować dokładność i aktualność wyników komputerowych, komputery muszą być chronione przed zagrożeniami środowiskowymi.

AWARIA ZASILANIA

Prawdopodobnie najczęstszą przyczyną przestoju komputera jest awaria zasilania. Nieobecności i zamglenia są widocznymi oznakami kłopotów; niewykryte skoki napięcia są znacznie częstsze, chociaż nie mniej niszczące. Błyskawica może wytwarzać impulsy napięciowe na liniach komunikacyjnych i liniach energetycznych o wystarczającej amplitudzie, aby zniszczyć sprzęt lub przynajmniej losowo

zmienić dane. Nagłe burze i intensywne upały lub chłód nakładają nadmierne obciążenia na generatory. Spadek napięcia sieciowego może spowodować awarię komputera lub urządzenia peryferyjnego. Nawet jeśli nie, mogą pojawić się szkodliwe skoki napięcia, gdy dodatkowe generatory zostaną przełączone, aby przenosić większe obciążenia. Tam gdzie jest to uzasadnione, wskaźnik nagrywania może być wykorzystywany do wykrywania fluktuacji linii elektroenergetycznej. Takie monitorowanie jest często zalecane, gdy systemy komputerowe mają niewyjaśnione, błędne błędy. W każdym momencie, gdy sygnalizowane są warunki braku tolerancji, wyjścia komputera powinny być starannie sprawdzane, aby zapewnić integralność danych. Jeśli takie zdarzenia występują często lub aplikacja jest wrażliwa należy rozważyć jeden pomocniczy sprzęt do zarządzania energią. Są to zarówno proste regulatory napięcia i kondycjonery linii, jak i zasilacze awaryjne (UPS).

CIEPŁO

Utrzymujące się wysokie temperatury mogą spowodować nieprawidłowe działanie podzespołów elektronicznych lub ich całkowite zawieszenie. W związku z tym klimatyzacja jest niezbędna, a wszystkie urządzenia muszą być odpowiednie, niezawodne i prawidłowo zainstalowane. Jeśli do komputera dostarczone jest zapasowe zasilanie, musi ono być również dostępne dla klimatyzatorów. Na przykład po trzęsieniu ziemi w San Francisco w 1989 roku komputery stacjonarne i serwery sieciowe w co najmniej jednej głównej siedzibie firmy zostały uszkodzone przez brak synchronizacji między klimatyzacją a zasilaniem. Klimatyzacja została znokautowana przez trzęsienie, a budynek został ewakuowany, ale komputery pozostały włączone. Wiele nie udało im się uratować na poziomie układów i płyt głównych w ciągu następnych kilku dni, ponieważ temperatura w nieochłodzonych biurach była zbyt wysoka. Często nierozpoznaną przyczyną przegrzania jest niedrożność kratek wentylacyjnych. Wydruki, taśmy, książki i inne przedmioty nie mogą być umieszczane na szafkach, w których mogą uniemożliwić swobodny przepływ powietrza. Termometr cyfrowy to dobra inwestycja dla każdego pomieszczenia, w którym używane są komputery. Obecnie wiele urządzeń elektronicznych zawiera termostaty odcinające moc, jeśli temperatura wewnętrzna przekracza granicę niebezpieczeństwa.

Wilgotność

Każda ekstremalna wilgotność może być szkodliwa. Niska wilgotność - poniżej około 20 procent - powoduje gromadzenie ładunków elektrostatycznych, które mogą wpływać na impulsy danych. Ponieważ zjawisko to jest nasilone przez wykładzinę, podłogi w pomieszczeniach komputerowych powinny być wolne od dywanów lub pokryte wykładziną antystatyczną. Wysoka wilgotność - powyżej około 80 procent - może prowadzić do kondensacji, która powoduje zwarcia w obwodach elektrycznych lub koroduje metalowe styki. Aby zapewnić działanie w granicach dopuszczalnych wartości granicznych, należy zainstalować regulatory wilgotności i przechowywać ciągłe wartości pomiarowe.

Woda

Woda wprowadzana przez deszcz, powodzie, rury rozrywane i tryskacze napowietrzne prawdopodobnie była odpowiedzialna za bardziej rzeczywiste uszkodzenie komputera niż pożar lub inny pojedynczy czynnik. Należy zachować ostrożność podczas lokalizacji urządzeń komputerowych, w prowadzeniu rur wodociągowych i przy wyborze środków gaśniczych, aby zminimalizować to znaczące niebezpieczeństwo. Niedostępność wody - na przykład po awarii głównej - spowoduje prawie natychmiastowe wyłączenie komputerów typu mainframe chłodzonych wodą. Centra danych o znaczeniu krytycznym powinny być przygotowane na tę ewentualność. Przykładowo, kiedy rzeka Des Moines wylała w 1993 r., powodując, że budynki mieszkalne w wieżowcu zostały ewakuowane z głównej siedziby głównej grupy finansowej, ale nie z powodu wody w budynku. Budynek pozostawał

wysoki i suchy, ale powódź zmusiła miejską elektrownię do zamknięcia, pozbawiając budynek wody niezbędnej do chłodzenia. Po powodzi firma zainstalowała w piwnicy zbiornik na wodę o pojemności 40 000 galonów, aby zapobiec ponownemu wystąpieniu tego problemu

BRUD I PYŁ

Cząsteczki obcych substancji mogą zakłócać prawidłowe działanie taśm magnetycznych i napędów dysków, drukarek i innych urządzeń elektromechanicznych. Wszystkie wloty powietrza muszą być filtrowane, a wszystkie filtry muszą być utrzymywane w czystości. Filiżanki kawy wydają się być szczególnie niestabilne w środowisku komputerowym; wraz z jakimkolwiek innym jedzeniem lub piciem, powinny one zostać całkowicie zakazane. We wszystkich obszarach, w których używany jest sprzęt komputerowy, należy rygorystycznie egzekwować zasady dobrego gospodarowania

PROMIENIOWANIE

Wiele już napisano o niszczącym działaniu pól magnetycznych na taśmach lub plikach dyskowych. Jednakże, ponieważ natężenie pola magnetycznego zmniejsza się gwałtownie wraz z odległością, jest mało prawdopodobne, że uszkodzenie może być spowodowane tylko przez duże magnesy trzymane bardzo blisko zarejestrowanych powierzchni. Na przykład przechowywanie dysku CD lub DVD przez przymocowanie go do szafki na dokumenty za pomocą magnesu nie jest dobrym pomysłem, ale zwyczajne przejście obok lodówki ozdobionej magnesami, trzymając CD lub DVD, prawdopodobnie nie spowoduje żadnych uszkodzeń. Rozprzestrzenianie się sygnałów bezprzewodowych może narazić dane na błędne impulsy. Biura powinny być świadome potencjalnych zakłóceń między telefonami bezprzewodowymi, telefonami komórkowymi, bezprzewodowymi punktami dostępu do Internetu i urządzeniami peryferyjnymi oraz mikrofalami. Radioaktywność może stanowić poważne zagrożenie dla personelu, ale nie dla komputera lub nośnika zapisu.

PRZESTÓJ

Istotne jest prawidłowe funkcjonowanie centrum przetwarzania danych, w którym regularna konserwacja prewencyjna odbywa się regularnie, a także dokładne zapisywanie czasu i przyczyny, że dowolny element komputera nie działa. Im częściej komputer jest wyłączony, tym bardziej operatorzy będą nadążać za zaplanowanymi obciążeniami. W takich warunkach omijane są kontrole, stosowane są skróty, oraz błędy ludzkie mnożą się. Należy przestudiować zapisy dotyczące przestojów, aby wykryć niekorzystne tendencje i wskazać sprzęt, który musi zostać poddany przeglądowi lub zastąpiony, zanim przestaną być nadmierne. Jeśli nieplanowane przestoje się wydłużą, konserwacja zapobiegawcza powinna zostać rozszerzona lub poprawiona do momentu odwrócenia tendencji

KOMUNIKACJA

Jednym z najbardziej dynamicznych czynników w bieżącym użytkowaniu komputera jest rozprzestrzenianie urządzeń i systemów transmisji danych. Są to między innymi: od modemów telefonicznych po sieci przewodowe, od telefonów komórkowych z obsługą Internetu po bezprzewodową sieć Ethernet 802.11, a także Bluetooth, podczerwień, osobiści cyfrowi asystenci (PDA), odtwarzacze muzyczne i nowe technologie, które pojawiają się niemal co miesiąc. Komputery, które nie działają co najmniej w niepełnym wymiarze godzin w trybie połączonym, mogą być rzadkością. Konieczność przyspieszania informacji na duże odległości zwiększa się proporcjonalnie do wielkości i rozproszenia geograficznego podmiotów gospodarczych; konieczność zachowania integralności i bezpieczeństwa danych oraz trudność w tym zakresie wzrastają jeszcze szybciej. Główne zagrożenia, przed którymi należy się chronić, to błędy ludzkie i mechaniczne, nieautoryzowane przystąpienie, zmiana i sabotaż. Termin "akcesja" odnosi się do umiejętności odczytu danych

przechowywanych lub przesyłanych w systemie komputerowym; może być przypadkowe lub celowe. "Zmiana" jest świadomym wprowadzaniem nieautoryzowanych lub niepoprawnych danych. "Sabotaż" jest zamierzonym aktem niszczenia lub uszkadzania systemu lub danych w nim zawartych. W przypadku każdego z tych zagrożeń narażenie i środki zaradcze będą zależeć od sprzętu i urządzeń.

TERMINALE

W tych dyskusjach terminal jest dowolnym urządzeniem wejścia / wyjścia, które obejmuje urządzenia do odbierania, wyświetlania, komponowania i wysyłania danych. Przykłady obejmują komputery osobiste i wyspecjalizowane urządzenia, takie jak jednostki zatwierdzania kart kredytowych. Przesyłanie danych odbywa się między komputerami, między terminalami lub między komputerami i terminalami. Same terminale mogą być klasyfikowane jako nieme lub inteligentne. Niemy terminale mają niewiele możliwości przetwarzania lub przechowywania i są w dużej mierze zależne od komputera hosta dla tych funkcji. Inteligentne terminale zwykle obejmują pamięć dyskową i możliwości mniej więcej odpowiadające komputerowi osobistemu. Oprócz znacznie ulepszonych możliwości komunikacyjnych, są one w stanie działać samodzielnie. W najprostszym z terminali jedynym zabezpieczeniem przed błędami transmisji jest niemożność rozpoznawania znaków nieuwzględnionych w prawidłowym zestawie i wyświetlanie znaku zapytania lub innego symbolu, gdy się pojawi. Niemal każdy terminal może być wyposażony w funkcję wykrywania błędu parzystości pionowej. Bardziej zaawansowane terminale są w stanie wykryć dodatkowe błędy za pomocą podłużnych i cyklicznych znaków redundancji, a także za pomocą kontroli parzystości i ważności. Oczywiście wykrywanie błędów to tylko pierwszy krok w utrzymywaniu integralności danych. Korekcja błędów jest zdecydowanie ważniejszą częścią, a retransmisja jest najczęściej stosowaną techniką korekcji. Inteligentne terminale i komputery osobiste są zdolne do szybkiej transmisji i odbioru. Mogą wykonać skomplikowane testy danych przed żądaniem retransmisji, lub mogą być zaprogramowane, aby wewnętrznie poprawić błędy. Techniki samokorygujące wymagają kodów działających w przód, takich jak kod cykliczny Hamminga. Są one podobne do wykrywających błędy cyklicznych kodów nadmiarowych, z tym, że wymagają jeszcze więcej nadmiarowych bitów. Chociaż korekcja błędów jest droższa i zwykle wolniejsza niż wykrywanie z retransmisją, jest przydatna w pewnych okolicznościach. Przykłady obejmują układy simplex, w których nie jest możliwy sygnał zwrotny, oraz układy półdupleksowe, w których czas obrócenia linii od transmisji do odbioru jest zbyt długi. Korekta do przodu jest również konieczna, gdy błędy są tak liczne, że retransmisje zatykają obwody, z niewielką lub żadną użyteczną przepustowością informacji. Należy zachować bardziej efektywne wykorzystanie inteligentnych terminali i komputerów osobistych integralność danych przez szyfrowanie. Mogą być również stosowane do kompresji lub zagęszczania. Zmniejszenie liczby znaków w komunikacie zmniejsza prawdopodobieństwo wystąpienia błędu, a także czas potrzebny na transmisję. Jedna technika zastępuje długie łańcuchy spacji lub zer za pomocą znaku specjalnego i liczby liczbowej; procedura jest odwracana podczas odbierania danych. Wreszcie, inteligentny terminal lub mikroprocesor może być używany do kodowania lub odczytywania danych, gdy poziom bezpieczeństwa wymaga kryptografii. Wszystkie terminale każdego typu, w tym komputery osobiste komputerów stacjonarnych i notebooków (komputery PC), mają co najmniej jedną wspólną cechę: konieczność ochrony przed sabotażem lub nieautoryzowanym użyciem. Chociaż zasady ustalania właściwej fizycznej lokalizacji i procedury ograniczania dostępu są zasadniczo takie same jak te, które dotyczą centralnego komputera, rzeczywiste problemy z odległymi terminalami są jeszcze trudniejsze. Pojedyncze lokalizacje, niewystarczający nadzór i łatwiejszy dostęp dla większej liczby osób zwiększają prawdopodobieństwo naruszenia bezpieczeństwa.

URZĄDZENIA PRZEWODOWE

Dostępne są cztery typy urządzeń przewodowych: dostęp telefoniczny, dzierżawione linie, cyfrowe linie abonenckie (DSL) i przekaźniki kablowe. Zarówno powszechne nośniki, jak i niezależne systemy mogą wykorzystywać różne media do transmisji danych. Rosnące zapotrzebowanie na większą szybkość i lepszą jakość transmisji danych spowodowało wykorzystanie kabli koncentrycznych i światłowodowych, podczas gdy stacje mikrofalowe i satelity komunikacyjne często są określane jako łącza bezprzewodowe w systemach przewodowych. Zasadniczo decyzje dotyczące wyboru usługi opierają się na ilości danych, które należy obsłużyć, oraz na związanych z nimi kosztach, ale względy bezpieczeństwa mogą być jeszcze ważniejsze.

LINIE TELEFONICZNE

Nadal szeroko stosowane w terminalach kart kredytowych i debetowych, linie telefoniczne zostały zastąpione w wielu innych aplikacjach za pośrednictwem łączy dzierżawionych, linii DSL i kabli obsługujących ruch internetowy. Połączenia telefoniczne są nawiązywane między modemami działającymi na zwykłych liniach głosowych, zwanych czasami zwykłymi usługami telefonicznymi (POTS). W przypadku, gdy dostęp telefoniczny do sprzętu nadal istnieje, na przykład w celu konserwacji określonego sprzętu, niezbędne są odpowiednie kontrole w celu ochrony zarówno sprzętu, jak i integralności innych systemów, do których może być podłączony. Dostęp do portów telefonicznych może uzyskać każdy, kto ma telefon w dowolnym miejscu na świecie, a praktyka wybierania w czasie wojny w celu wykrywania modemów jest nadal używana przez osoby szukające nieautoryzowanego dostępu do sieci organizacji. (Wirtualne wybieranie numerów polega na wybieraniu bloków numerów w celu ustalenia, które z nich odpowiadają jako modemy lub faksy, numery te są rejestrowane i mogą zostać wybrane później w celu uzyskania nieautoryzowanego dostępu do systemów lub usług.) Zalecenia:

*Skompiluj dziennik nieautoryzowanych prób wejścia i używaj go, aby zniechęcić do dalszych wysiłków.

* Skompiluj dziennik wszystkich dostępów do poufnych danych i sprawdź ich odpowiedniość.

* Wyposaż wszystkie terminale w wewnętrzne generatory identyfikacyjne lub urządzenia odbierające odpowiedzi, aby nawet właściwe hasło zostało odrzucone, jeśli zostanie wysłane z nieautoryzowanego terminalu. Technika ta może wymagać dostępności autoryzowanego serwera kopii zapasowych w przypadku awarii głównego urządzenia.

* Podaj użytkownikom osobistą identyfikację oprócz hasła, jeśli wymaga tego poziom bezpieczeństwa. Dodatkowym zabezpieczeniem może być magnetycznie pasiasta lub skomputeryzowana karta plastikowa, którą należy włożyć do specjalnego czytnika. Wartość takich kart jest ograniczona, ponieważ mogą z nich korzystać wszyscy, bez względu na to, czy są autoryzowani, czy nie. Aby spełnić wysokie wymagania bezpieczeństwa, należy wziąć pod uwagę inne zależne od sprzętu identyfikatory biometryczne, takie jak odciski dłoni i wznowienia głosu.

* W razie potrzeby skorzystaj z urządzenia oddzwaniania, które uniemożliwia stacji zdalnej bezpośrednie wejście do komputera. Zamiast tego urządzenie wybiera numer dzwoniącego z wewnętrznej listy zatwierdzonych numerów telefonów, aby nawiązać połączenie.

Przy odpowiedniej dyscyplinie hasła można zminimalizować problemy związane z akcesją, zmianą i sabotażem danych. Jednak jakość przesyłu jest bardzo zmienna. Wbudowany w publiczny system telefoniczny jest automatycznym mechanizmem ustalania trasy, który kieruje sygnały przez niekontrolowane ścieżki. Odległość i liczba przechodzących punktów przełączania oraz szansa na obecność przesłuchań, stanów przejściowych i innych produktów szumowych będą miały

nieprzewidywalny wpływ na częstość występowania błędów. Opisane wcześniej systemy parzystości są skutecznym sposobem ograniczenia takich błędów.

LINIE DZIERŻAWIONE

Linie dzierżawione od wspólnego przewoźnika do wyłącznego użytku jednego abonenta nazywane są liniami dedykowanymi. Ponieważ są one bezpośrednio połączone między określonymi punktami, zwykle nie można ich uzyskać przez sieć dial-up. Tradycyjnie dzierżawione linie były miedzianymi, ale można również wynająć światłowodowe i koncentryczne linie kablowe punkt-punkt. Podłączanie jest technicznie wykonalną metodą uzyskiwania dostępu do łączy dzierżawionych, ale jest droższe, trudniejsze i mniej wygodne niż wybieranie przez przełączaną sieć. Łącza dzierżawione są z reguły bezpieczniejsze niż te, z których można łatwo wybrać na czas wojny. Do tego zwiększonego poziomu bezpieczeństwa łączy dzierżawionych dodaje się zapewnienie odbioru o wyższej jakości. Problemy związane z niepewnymi ścieżkami transmisji i przejściowymi przejściami są eliminowane, chociaż inne źródła błędów nie są. W konsekwencji kontrola parzystości pozostaje minimalnym wymogiem.

CYFROWE LINIE ABONENCKIE

Spadając gdzieś pomiędzy linią dzierżawioną a POTS, cyfrowa linia abonencka oferuje cyfrową transmisję lokalnie za pośrednictwem zwykłych linii telefonicznych, które mogą być wykorzystywane jednocześnie do transmisji głosu. Jest to możliwe, ponieważ zwykłe miedziane linie telefoniczne mogą przenosić, przynajmniej na krótkich dystansach, sygnały znajdujące się w zakresie znacznie wyższych częstotliwości niż ludzki głos. Modem DSL jest używany przez komputer do przełączania się do najbliższego przełącznika telefonicznego, w którym to momencie transmisja danych przechodzi do szkieletu Internetu. Komputery połączone z Internetem za pośrednictwem DSL komunikują się za pomocą protokołu TCP / IP i są określane jako hosty, a nie terminale. Są narażone na kompromis poprzez szeroki zakres exploitów. Jednak niewiele z tych zagrożeń jest włączanych przez sam DSL. Podobnie jak w przypadku łączy dzierżawionych, podsłuch jest możliwy, ale inne ataki, takie jak wykorzystanie słabych punktów w implementacjach TCP / IP na komputerach hosta, są łatwiejsze.

NOŚNIKI KABLOWE

Wszędzie tam, gdzie dostępna jest telewizja kablowa (TV), te same kable światłowodowe lub koncentryczne, które przenoszą sygnał telewizyjny, mogą również służyć do szybkiej transmisji danych. Zalety tej technologii obejmują prędkości pobierania, które w przypadku kabli koncentrycznych przekraczają 50 megabitów na sekundę, lub w przypadku kabla światłowodowego - przekraczają 100 gigabitów na sekundę. Wady wynikają z faktu, że połączenia z operatorem mogą być współdzielone przez innych abonentów w tej samej lokalizacji. O ile usługodawca nie ogranicza dostępu, być może zgodnie z umową dotyczącą jakości usług, wielu abonentów może jednocześnie korzystać z Internetu, co spowalnia szybkość transmisji. Jeszcze poważniejsza jest możliwość naruszenia bezpieczeństwa, ponieważ wiele komputerów w sąsiedztwie może współdzielić część wirtualnej sieci lokalnej, a zatem każdy z nich jest potencjalnie dostępny dla każdego innego węzła w tej sieci. Z tego powodu połączenia kablowe powinny być zaporą ogniową. Szczegóły dotyczące zapór ogniowych i ich zastosowań. Innym powodem używania zapór jest to, że połączenia kablowe są zawsze włączone, zapewniając maksymalną możliwość hakerów dostępu do nienadzorowanego komputera. \

KOMUNIKACJA BEZPRZEWODOWA

Transfery danych między wielonarodowymi korporacjami rozwijają się bardzo szybko, a transoceaniczne sieci radiowe i telefoniczne okazały się zbyt kosztowne, zbyt wolne, zbyt zatłoczone i podatne na błędy, aby zapewnić odpowiednią obsługę. Ważną alternatywą jest satelita komunikacyjny.

Orbitując nad Ziemią, satelita odbija sygnały radiowe o bardzo wysokiej częstotliwości, które mogą przenosić program telewizyjny lub dane komputerowe z równą prędkością i łatwością. W przypadku komunikacji na krótszych dystansach koszty usług przewodowych typu "common-carrier" były tak wysokie, że sprzyjały konkurencyjnym technologiom. Jedno z nich, radiowe łącze mikrofalowe, jest używane w wielu sieciach. Jedną z cech takich transmisji jest to, że mogą być odbierane tylko na bezpośredniej linii wzroku z anteny nadawczej lub retransmisyjnej. Z takimi stacjami naziemnymi punkt-punkt, czasami trudno jest ustawić promienie radiowe tam, gdzie nie mogą zostać przechwycone; z transmisją satelitarną i bezprzewodową jest to niemożliwe. Jest to istotny problem w przypadku technologii bezprzewodowej sieci lokalnej opartej na standardach IEEE 802.11 i powszechnie znanej jako Wi-Fi (marka należąca do Wi-Fi Alliance, termin ten jest skrótem od wierności bezprzewodowej). Potrzeba bezpieczeństwa jest w konsekwencji większa, a skramblery lub enkodery kryptograficzne są niezbędne do przekazywania poufnych danych. Ze względu na szerokie pasma na częstotliwościach mikrofalowych możliwe są niezwykle szybkie szybkości przesyłania danych. Dzięki pionowym, podłużnym i cyklicznym znacznikom sprawdzania nadmiarowości można wykryć prawie wszystkie błędy, ale przepustowość pozostaje wysoka.

KRYPTOGRAFIA

Presja konkurencyjna w biznesie, polityce i sprawach międzynarodowych nieustannie stwarza sytuacje, w których moralność, prywatność i prawa wydają się ustępować przed zniewalającą chęcią zysku. Informacja, ze względu na nią samą lub za cenę, jaką przynosi, jest pożądanym towarem. Jesteśmy przyzwyczajeni do widoku samochodów pancernych i uzbrojonych strażników przewożących pieniądze, ale często nieocenione dane są przenoszone z niewieloma środkami ostrożności. Kiedy liczba komputerów i kompetentnych techników była niewielka, ryzyko związane z nieostrożnym przetwarzaniem danych nie było może duże. Teraz jednak istnieje bardzo duża populacja dobrze poinformowanych osób komputerowych, a wśród nich osoby chętne i zdolne do wykorzystania swojej wiedzy do nielegalnych celów. Inni znajdują stymulację i satysfakcję w pokonywaniu intelektualnego wyzwania, które dostrzegają w pokonaniu środków bezpieczeństwa komputerowego. Pozyskiwanie informacji w nieautoryzowany sposób jest stosunkowo łatwe, gdy dane są przesyłane między lokalizacjami. Jedną z metod zniechęcania do tej praktyki lub uczynienia jej kosztownym wartą wysiłku jest kryptograficzne kodowanie danych przed transmisją. Ta technika jest również przydatna w zachowaniu bezpieczeństwa plików wewnątrz urządzenia do przechowywania danych. Jeśli wszystkie ważne pliki byłyby przechowywane na nośnikach magnetycznych lub optycznych tylko w szyfrach kryptograficznych, częstość kradzieży i odsprzedaży byłaby niewątpliwie mniejsza. Można używać wielu rodzajów szyfrów, w zależności od ich kosztu i wymaganego stopnia bezpieczeństwa. Teoretycznie każdy kod może zostać złamany, biorąc pod uwagę wystarczającą ilość czasu i sprzętu. W praktyce, jeśli szyfr nie może zostać złamany dość szybko, zakodowane dane mogą stać się bezwartościowe. Ponieważ jednak sam klucz może zostać użyty do rozszyfrowania późniejszych wiadomości, konieczne jest częste zmienianie kodów lub kluczy.

BACKUP

Podobnie jak w przypadku większości problemów, głównym celem bezpieczeństwa komputerowego powinno być zapobieganie, a nie leczenie. Niezależnie jednak od tego, jak wielki wysiłek ten się uda, nigdy nie można zagwarantować pełnego sukcesu. Istnieją cztery powody takiego stanu rzeczy:

1. Nie każdy problem można przewidzieć.

2. Jeżeli koszt uniknięcia określonej szkody przewyższa koszt odzyskiwania, środki zapobiegawcze mogą nie być uzasadnione.

3. Środki zapobiegawcze, przenoszone do skrajności, mogą nakładać niemożliwe ograniczenia na wydajność i wydajność operacji. W związku z tym konieczne może być uniknięcie takich środków, których celem jest zdarzenie, którego statystyczne prawdopodobieństwo wystąpienia jest niewielkie.

4. Nawet w optymalnych warunkach starannie opracowane plany mogą zbłądzić. W prawdziwym świecie niepewności i ludzkiej omylności, gdzie występuje aktywna lub nieumyślna ingerencja, jest niemal pewne, że w takim czy innym momencie najlepsze środki ostrożności okażą się nieskuteczne.

Uznając niemożność zapobiegania wszelkim niepożądanym działaniom i zdarzeniom, konieczne jest zaplanowanie odpowiednich sposobów na ich wyleczenie. Plany takie muszą obejmować tworzenie kopii zapasowych dla personelu, sprzętu, zasilania, urządzeń fizycznych, danych i oprogramowania. Plany tworzenia kopii zapasowych powinny być oceniane pod kątem:

* Priorytety ustalone dla każdego wniosku, aby zapewnić ich właściwe przypisanie i faktyczne przestrzeganie.

* Czas wymagany do przywrócenia aplikacji o wysokim priorytecie do stanu pełnego funkcjonowania.

* Stopień pewności, że plany można faktycznie zrealizować w razie potrzeby. W przypadku ważnych aplikacji alternatywne plany powinny być dostępne w przypadku, gdy plan podstawowy nie może zostać wdrożony.

* Stopień bezpieczeństwa i integralności danych, które będą istniały, jeśli faktycznie zostaną wprowadzone plany tworzenia kopii zapasowych.

* Stopień, w jakim obserwuje się zmiany warunków wewnętrznych lub zewnętrznych, oraz szybkość, z jaką plany są modyfikowane w celu odzwierciedlenia takich zmian.

Przydzielanie priorytetów przed faktyczną awarią jest kluczowym i niezwykle ważnym procesem. W większości organizacji nowe aplikacje mnożą się, a stare rzadko są odrzucane. Jeśli plany tworzenia kopii zapasowych próbują objąć wszystkie miejsc pracy, prawdopodobnie nie osiągną żadnego. Właściwe wykorzystanie priorytetów pozwoli na realistyczne planowanie, a ważne zadania zostaną wykonane na czas i po akceptowalnych kosztach.

PERSONEL

Problemy związane z codzienną pracą komputera wymagają planów awaryjnych dla personelu, od którego zależy działanie sprzętu. Choroby, zwolnienia, zwolnienia, awanse, rezygnacje, nadgodziny i dodatkowe zmiany to tylko niektóre z powodów, dla których rozważni menedżerowie nieustannie zajmują się problemem tworzenia kopii zapasowych personelu. Te same praktyki, które sprawdzają się w codziennych problemach, mogą dostarczyć wskazówek dotyczących awaryjnych planów tworzenia kopii zapasowych.

SPRZĘT

Kopia zapasowa sprzętu dla centrów danych może przybierać różne formy:

* Wiele procesorów w tym samym miejscu, aby chronić przed utratą usługi z powodu awarii jednego urządzenia

* Duplikaty instalacji w pobliskich obiektach tej samej firmy

* Utrzymywanie programów w kompatybilnym biurze usług, w trybie testowym lub w trybie gotowości

* Umowa na wykonanie kopii zapasowej w obiekcie przeznaczonym do odzyskiwania po awarii

* Odwrotna umowa z podobną instalacją w innej firmie

Prawdopodobieństwo, że dwa procesory lokalne są jednocześnie wyłączane z powodu błędów wewnętrznych, jest bardzo małe. W związku z tym większość instalacji nierzadko pozostaje w tyle w aplikacjach o znaczeniu krytycznym. Jednak ten rodzaj kopii zapasowej nie zapewnia ochrony przed awarią zasilania, pożarem, wandalizmem ani żadną katastrofą, która mogłaby uderzyć w dwa lub więcej procesorów naraz. Katastrofy z 11 września 2001 r. dowiodły, że nawet bardzo mało prawdopodobne wydarzenie może się zdarzyć. W przypadku zduplikowanych procesorów w różnych, ale często posiadanych witrynach, istnieje małe prawdopodobieństwo, że oba te czynniki oddziałują na te same siły. Chociaż współczynnik bezpieczeństwa zwiększa się wraz z odległością dzielącą je, trudność w transporcie ludzi i danych staje się większa. Alternatywna strona musi reprezentować kompromis między tymi sprzecznymi celami. Ponadto należy zachować pełną kompatybilność sprzętu i oprogramowania, nawet jeśli spowoduje to nadmierne obciążenie operacyjne jednej z instalacji. Krótko po 11 września wiele nowojorskich firm finansowych powróciło do pracy z alternatywną stroną komputerową na rzece Hudson. Wsparcie zapewniane przez biura obsługi może być niezwykle skuteczne, szczególnie jeśli wybór obiektu jest starannie wykonany. Chociaż biura usług progresywnych często ulepszają zarówno sprzęt, jak i oprogramowanie, prawie nigdy nie robią tego w sposób, który by powodował problemy ze zgodnością dla dotychczasowych klientów. Po przetestowaniu programów można je przechowywać w trybie offline na taśmie lub dysku za niewielką opłatą. Zaktualizowane matryce można obracać w bibliotece biura serwisowego, zapewniając kopie zapasowe danych poza siedzibą, a także możliwość natychmiastowej pełnej operacyjności. Efektywne wsparcie sprzętowe jest również dostępne w niezależnych obiektach utworzonych specjalnie w tym celu. W jednym typie obiektu jest odpowiednia przestrzeń, moc, klimatyzacja i linie komunikacyjne, aby pomieścić bardzo duży system. Większość producentów jest w stanie zapewnić niemal każdą konfigurację w krótkim czasie, gdy katastrofa trafi do cennego klienta. Koszty tego rodzaju rezerwowego punktu bazowego są udostępniane przez wielu użytkowników, tak aby wydatki były minimalne do momentu pojawienia się faktycznej potrzeby. Jeżeli jednak dwóch lub więcej podmiotów udostępniających dane jest geograficznie blisko, ich urządzenia mogą przestać działać w wyniku tego samego pożaru, powodzi lub awarii zasilania. Przed zawarciem umowy na taki obiekt należy przeanalizować ten potencjalny problem; alternatywą może być całkowicie fałszywe poczucie bezpieczeństwa. Kilka firm, których instalacje zostały uszkodzone lub zniszczone 11 września, zostały w krótkim czasie dostarczone przez ich dostawców kompletnemu sprzętowi zastępczemu. Inny typ zaplecza jest już wyposażony w komputery, napędy dyskowe i taśmowe, drukarki, terminale i linie komunikacyjne, dzięki czemu może natychmiast zastąpić niesprawny system. Koszty gotowości za tę usługę są znacznie wyższe niż w przypadku instrumentu bazowego, ale zapewnienie ożywienia w możliwie najkrótszym czasie jest znacznie większe. Tutaj również rozsądne byłoby zbadanie prawdopodobieństwa, że więcej niż jeden klient będzie wymagał instalacji w tym samym czasie i zażądać zapewnienia spełnienia własnych potrzeb. Kilka firm z powodzeniem skorzystało z tego typu kopii zapasowych i odzyskiwania po awarii po 11 września. Backup przez wzajemne porozumienie był przez wiele lat akceptowaną praktyką, choć nieczęsto wystawianą na próbę. Niestety wielu menedżerów wciąż polega na tym przestarzałym zabezpieczeniu. Trzeba przetrwać tylko jedną istotną zmianę oprogramowania systemu operacyjnego uświadomienie sobie, że kiedy się pojawia, ani czas, ani skłonność nie są dostępne do modyfikowania i testowania programów innej firmy. Nawet drobne zmiany w sprzęcie i oprogramowaniu które ciągle odbywają się w większości instalacji, mogą sprawić, że będą niezgodne. Jednocześnie, zgodnie z ustawą o chorobie Parkinsona, obciążenia zawsze się rozszerzają, aby wypełnić dostępny czas i udogodnienia. W konsekwencji wielu, którzy wierzą, że mają odpowiednie zabezpieczenie, dostanie tylko niemiłą niespodziankę, jeśli spróbują skorzystać z przywileju.

MOC

Niezbędnym elementem każdej instalacji przetwarzania danych jest energia elektryczna. Kopie zapasowe mocy na komputery osobiste i małe serwery dzięki zasilaczom bezprzerwowym są rozsądne pod względem kosztów i dość skuteczne. W przypadku komputerów typu mainframe i dużych serwerów dostępnych jest kilka typów kopii zapasowych. Główną determinantą w wyborze powinno być całkowite koszty przewidywanych przestojów i powtórzeń w porównaniu do kosztu kopii zapasowej, aby je wyeliminować. Czas przestoju i czas ponownego uruchomienia mogą być ekstrapolowane z zapisów poprzednich doświadczeń. Problemy związane z energią elektryczną można sklasyfikować według rodzaju i czasu trwania. Problemy z zasilaniem, ponieważ wpływają na komputery, składają się z amplitudy, częstotliwości i kształtu fali, których czas trwania wynosi od ułamków milisekundy do minut lub godzin. Długotrwałe przestoje zazwyczaj spowodowane są silnymi wiatrami, lodem, błyskawice, pojazdy niszczące linie energetyczne lub awarie sprzętu, które uniemożliwiają pracę całej podstacji. W przypadku komputerów typu mainframe w centrach danych zwykle możliwe jest, choć kosztowne, zlecenie dostawy energii z dwóch różnych podstacji, z których jedna działa jako zapasowa. Innym rodzajem ochrony są generatory benzynowe lub wysokoprężne. Dostępne są elementy sterujące, które wykrywają awarię zasilania i automatycznie uruchamiają silnik. Pełną prędkość osiąga się w mniej niż minutę, a wyjście generatora może zasilać komputer w razie potrzeby przez kilka dni. Kilka sekund opóźnienia w przełączaniu źródeł zasilania wystarcza, aby przerwać działanie programów uruchomionych na komputerze i zniszczyć pliki danych. Aby tego uniknąć, zaprojektowano "nieprzerwane" źródło zasilania. W jednej wersji linia prądu przemiennego zasila prostownik, który dostarcza prąd stały do falownika. Falownik z kolei napędza silnik synchroniczny sprzężony z alternatorem, którego wyjście AC zasila komputer. Podczas gdy prostownik dostarcza prąd stały do falownika, ładuje on również duży zestaw baterii o dużej ładowności. Po wykryciu usterki na głównej linii zasilającej akumulatory są natychmiastowo i automatycznie przełączane, aby napędzać silnik synchroniczny. Ponieważ ogromny odpływ baterii może ją wyczerpać w ciągu kilku minut, należy również zapewnić generator diesla. Zalety tego projektu to:

* Zmiany w częstotliwości linii, amplitudzie i przebiegu nie docierają do komputera.

* Przełączenie z linii energetycznej na baterię jest niewykrywalne przez komputer. Programy działają, a żadne dane nie są tracone.

* Milisekundowe skoki i inne stany przejściowe, które mogą być odpowiedzialne za uszkodzenie sprzętu i niewykryta utrata danych, są całkowicie tłumione.

TESTOWANIE

Najważniejszym aspektem każdego planu tworzenia kopii zapasowych jest jego skuteczność. Czy to zadziała? Błędem byłoby czekać na awarię, aby się dowiedzieć. Jedyną sensowną alternatywą jest systematyczne testowanie. Jedna forma testu jest podobna do próby kostiumowej, z rzeczywistą awarią ściśle symulowaną. W ten sposób można korzystać ze sprzętu, ludzi i procedur, dopóki praktyka nie zapewni biegłości. Okresowo po tym testy powinny być powtarzane, aby zmiany sprzętu, oprogramowania i personelu nie osłabiły kopii zapasowa.

PROCEDURY ODZYSKIWANIA

Procedury wymagane do odzyskania od dowolnego problemu systemowego będą zależeć od natury problemu i od zastosowanych środków tworzenia kopii zapasowych. Odzyskiwanie sprzętu sięga od natychmiastowej i w pełni automatycznej, poprzez ręczną naprawę lub wymianę komponentów, po budowę, wyposażenie i obsadzenie całkowicie nowego centrum danych. Prawie każde centrum danych to kolekcja sprzętu z opcjami, modyfikacjami, dodatkami i funkcjami specjalnymi. Jeżeli konieczna będzie wymiana sprzętu, musi być dostępna aktualna lista konfiguracji i ustalone wcześniej procedury

ponownego zamawiania. Jeszcze lepszą praktyką byłoby utrzymywanie aktualnej listy pożądanych urządzeń, które mogłyby być podstawą do wymiany. Prawdopodobnie wymiana byłaby szybsza i potężniejsza, ale należy zaplanować dodatkowy czas na szkolenie i konwersję.

ROZWAŻANIA MIKROKOMPUTERA

Działają cztery czynniki w celu zintensyfikowania problemów związanych ze sprzętem, ponieważ dotyczą małych komputerów:

1. Dostępność

2. Wiedza

3. Motywacja

4. Szansa

DOSTĘPNOŚĆ

Dostępność jest konsekwencją pracy małych komputerów w szeroko otwartym środowisku biurowym, a nie w kontrolowanym centrum danych. Żaden ochroniarz, specjalne odznaki, pułapki-pułapki, kamery, bibliotekarze taśmowi ani nadzorujący zmiany nie ograniczają dostępu do sprzętu lub nośników danych w biurze, tak jak robią to w typowym centrum danych.

WIEDZA

Wiedza i jej brak są równie niebezpieczne. Z jednej strony, gdy komputery osobiste przenikają środowisko biurowe, wiedza techniczna staje się szeroko rozpowszechniana. Kiedy ta wiedza była ograniczona do stosunkowo niewielu ekspertów komputerowych, których można było łatwo kontrolować, jej rosnąca uniwersalność sprawia, że kontrola jest niezwykle trudna, a nawet niemożliwa. Z drugiej strony, gdy komputery są obsługiwane przez osoby o minimalnej wiedzy i umiejętnościach, prawdopodobieństwo naruszenia bezpieczeństwa przez błąd i nieumyślność znacznie wzrosło.

MOTYWACJA

Motywacja istnieje w wielu formach. Jest obecny wszędzie tam, gdzie można przekierować cenny majątek dla osobistych korzyści; powstaje, gdy prawdziwa lub wyobrażona niesprawiedliwość wywołuje pragnienie zemsty; i może po prostu być formą autoekspresji. Nielegalne przekierowanie aktywów korporacyjnych zawsze zapewniało możliwości kradzieży; teraz, gdy wielu pracowników posiada komputery w domu, wartość skradzionego sprzętu, programów i danych może zostać zrealizowana bez udziału osób trzecich. Gdy do równania zostanie dodana strona trzecia i zostanie uwzględniony kwitnący rynek skradzionych danych osobowych, potencjał kradzieży danych, przestępstwa o niskim ryzyku i wysokim zysku, jest bardzo duży. Komputery i sieci są również celem sabotażu, a także kradzieży danych. Opieranie się na takich systemach przez rządy, wojsko, wielkie korporacje i innych postrzeganych społecznych i gospodarczych problemów oznacza, że przestępcze działania będą prawdopodobnie kontynuowane. Ponieważ komputery osobiste są teraz częścią tych systemów, są także łączem z polityką lub praktyką, której nie akceptuje jedna lub więcej grup ludzi. Motywacja do sabotowania komputerów osobistych jest bardziej prawdopodobna w najbliższym czasie, niż do zaniku. Trzecią motywacją do łamania zabezpieczeń komputera jest wyzwanie i podekscytowanie. Niezależnie od tego, czy próbują przezwyciężyć techniczne przeszkody, bezkarnie łamać prawo, czy też po prostu przekroczyć zakazany teren, niektórzy hakerzy uznają te wyzwania za nieodłączne i stają się hakerami przestępczymi. Oglądanie aktów z rozbawioną tolerancją lub nawet

łagodną dezaprobatą jest całkowicie niezgodne z wielkością potencjalnych szkód i świętości pokonanych barier zaufania. Ponieważ technologia istnieje, aby zablokować wszystkich, oprócz najbardziej zdeterminowanego i sprawnego technicznie hakera przestępczego, brak ochrony wrażliwych systemów jest coraz częściej postrzegany jako zaniedbanie.

MOŻLIWOŚĆ

Przy tak wielu komputerach osobistych w prawie każdym biurze, praktycznie bez nadzoru w godzinach pracy, a już na pewno w żadnym innym czasie, możliwości są obfite w przypadku dwóch rodzajów naruszeń bezpieczeństwa: celowych przez osoby posiadające wiedzę techniczną i niezamierzone przez osoby bez nich.

ZAGROŻENIA DLA MIKROKOMPUTERÓW

Do najważniejszych zagrożeń dla mikrokomputerów należą:

* Obrażenia fizyczne

* Kradzież

* Energia elektryczna

* Elektryczność statyczna

* Komunikacja danych

* Konserwacja i naprawa

OBRAŻENIA FIZYCZNE

Mikrokomputery i ich urządzenia peryferyjne nie są odporne na uszkodzenia. Napędy dysków są bardzo podatne na awarie w wyniku uderzenia; klawiatury nie mogą tolerować zabrudzeń lub nieostrożnego obchodzenia się z nimi. Istotne jest, aby komputery były uznawane za delikatne instrumenty i aby były odpowiednio traktowane. Nawet w centrum danych kontrolowanym przez dostęp, gdzie jedzenie i napoje są oficjalnie zakazane, często zdarza się, że kawa rozlewa się po ustawieniu na lub w pobliżu sprzętu operacyjnego. W niekontrolowanym środowisku biurowym rzadko zdarza się, aby nie narażać komputerów osobistych na bezpośrednie niebezpieczeństwo oblodzenia potencjalnie szkodliwymi płynami. Problem pogłębia powszechna praktyka niezabezpieczania nośników , takich jak płyty CD i DVD leżące na tej samej powierzchni, na których łatwo może się dostać do nich żywność i napoje. Chociaż całkowite wyeliminowanie tych praktyk może być niemożliwe, większa dyscyplina ochroni nośniki danych i sprzęt przed zanieczyszczeniem. Jak wspomniano w rozdziale dotyczącym ciepła, uszkodzenie może również wynikać z blokowania otworów wentylacyjnych niezbędnych do odpowiedniego chłodzenia. Takie otwory mogą być nieskuteczne poprzez umieszczenie urządzenia zbyt blisko ściany lub, w przypadku laptopów, na miękkich powierzchniach, takich jak dywany, które blokują otwory wentylacyjne na podstawie maszyny. Otwory na obudowy komputera a wyświetlacze w kształcie rurek katodowych są zbyt często pokryte papierami lub książkami, które uniemożliwiają swobodny przepływ powietrza chłodzącego. W wyniku tego wzrasta wewnętrzna temperatura sprzętu, co powoduje nieprawidłowe działanie komponentów marginalnych, otwarte styki przerywane, błędy i ostatecznie usterek systemu lub ustaje.

KRADZIEŻ

Możliwości kradzieży komputerów osobistych i ich nośników danych są znacznie większe niż w przypadku ich większych odpowiedników. Pliki zawierające zastrzeżone informacje lub drogie

programy są łatwo kopiowane na nośniki wymienne tak małe jak znaczek pocztowy i pobierane z lokalu bez pozostawiania śladów. Zewnętrzne napędy dyskowe są na tyle małe, że można je przenosić w etui lub etui attachée, a nowe dyski USBUS wyglądają jak breloczki dla niewtajemniczonych. Powszechna praktyka polegająca na zabraniu komputerów przenośnych do domu na wieczór lub pracę w weekend ostatecznie unieruchamia nawet najbardziej sumiennych strażników. W biurach bez strażników problem jest jeszcze trudniejszy. Bez ustanawiania policyjnego stanu nieustannej inwigilacji, co należy zrobić, aby zniechęcić do kradzieży? Sprzęt może być przykuty lub przykręcony do biurka lub zamknięty w szafkach zbudowanych do tego celu. Większa staranność w nagrywaniu i śledzeniu numerów seryjnych, częstszych zapasów oraz ciągły program edukacji może pomóc. Przede wszystkim istotne jest rozpoznanie wielkości problemu na wystarczająco wysokim poziomie zarządzania, aby do jego rozwiązania zastosować odpowiednie zasoby. W przeciwnym razie nadal będzie wzrastać zapotrzebowanie na zyski korporacyjne.

MOC

Nawet w kontrolowanym centrum danych, utrata zasilania, przerwy w zasilaniu, skoki napięcia, spadki napięcia i przepięcia oraz inne zakłócenia zasilania elektrycznego stanowią zagrożenie. Sytuacja jest znacznie gorsza w typowym biurze, w którym komputery osobiste są podłączone do istniejących gniazd, z niewielką lub żadną myślą o konsekwencjach złej energii. Niektóre z podstawowych środków ostrożności, które należy podjąć, to:

* Eliminowanie lub przynajmniej kontrolowanie użycia przedłużaczy, kostek i wielu listew wylotowych. Każda jednostka na tej samej linii elektroenergetycznej może zmniejszyć napięcie dostępne dla wszystkich pozostałych, a każdy z nich może powodować zakłócenia na linii.

* Dostarczanie regulatorów napięcia linii i kondycjonerów linii, gdy jest to konieczne, aby utrzymać moc w wymaganych granicach.

* Zakaz używania odkurzaczy lub innych urządzeń elektrycznych podłączonych do tej samej linii energetycznej co komputery lub urządzenia peryferyjne. Takie urządzenia wytwarzają wysoki poziom szumu elektrycznego, oprócz zaników napięcia.

* Prawidłowe podłączenie wszystkich przewodów uziemiających. Jest to szczególnie ważne w starszych biurach wyposażonych w dwustykowe gniazda, które wymagają wtyczek adapterów. Trzeci przewód wtyczki musi być podłączony do stałego uziemienia w celu zapewnienia bezpieczeństwa personelu, a także do redukcji szumów elektrycznych. Ponadto stosowanie UPS-ów jest wysoce zalecane dla wszystkich komputerów i urządzeń pomocniczych. Urządzenia te są dostępne w pojemnościach od około 200 watów dla komputerów PC do praktycznie nieograniczonych rozmiarów dla komputerów typu mainframe. Podczas działania linii zasilającej UPS może kondycjonować linię, usuwając zakłócenia elektryczne, zwisy, skoki i przepięcia. Gdy napięcie sieci spadnie poniżej ustawionej wartości lub gdy całkowicie zaniknie moc, UPS konwertuje prąd stały z wewnętrznych baterii na prąd przemienny wymagany do zasilania związanego z nim sprzętu. W zależności od jego wartości znamionowej i obciążenia, UPS może zapewnić zasilanie w stanie gotowości przez kilka minut do kilku godzin. Jest to wystarczający czas, aby wyłączyć komputer normalnie lub w trybie w przypadku dużych instalacji, aby generator silnika został umieszczony online. Usługi wykwalifikowanego elektryka powinny być wykorzystywane wszędzie tam, gdzie istnieje możliwość wystąpienia problemów z zasilaniem elektrycznym.

ELEKTRYCZNOŚĆ STATYCZNA

Po pokryciu podłogi dywanem w suchy dzień, iskra, która przeskakuje z czubka palca do komputera, może być lekko szokująca dla osoby, ale dla komputera może spowodować poważną utratę pamięci, degradację danych i nawet zniszczenie komponentów. Efekty te są jeszcze bardziej prawdopodobne, gdy ludzie dotykają komponentów wewnątrz komputera bez odpowiedniego uziemienia. Aby temu zapobiec, dostępnych jest kilka środków:

* Użyj nawilżacza, aby utrzymać względną wilgotność powyżej 20%.

* Usuń zwykłe dywany. Wymień w razie potrzeby na typy bez statycznych.

* Użyj maty antystatycznej pod krzesłami i biurek.

* Użyj paska uziemiającego przy każdej klawiaturze.

* Podczas instalowania lub naprawy podzespołów urządzeń elektronicznych należy nosić bransoletkę uziemiającą.

Dotknięcie paska uziemiającego przed uruchomieniem komputera spowoduje odprowadzenie ładunków elektrostatycznych przez podłączony przewód uziemiający, co spowoduje spłukiwanie urządzenia okresowo natryskiem antystatycznym. Niektóre kombinacje tych środków chronią personel, sprzęt i dane przed czasami niejasnymi, ale zawsze rzeczywistymi niebezpieczeństwami elektryczności statycznej.

PRZESYŁANIE DANYCH

Chociaż komputery osobiste pełnią znaczące funkcje w trybie autonomicznym, ich użyteczność znacznie się zwiększa dzięki komunikacji z komputerami mainframe, narzędziami informacyjnymi i innymi małymi komputerami, zdalnie przez linie telefoniczne lub Internet lub przez sieci lokalne. Wszystkie problemy bezpieczeństwa związane z komunikacją na komputerach mainframe dotyczą komputerów osobistych z dodatkowymi komplikacjami. Aż do pojawienia się komputerów osobistych prawie wszystkie terminale komunikujące się z komputerami typu mainframe były "głupie". Oznacza to, że funkcjonowały one podobnie do maszyn typu teletype, z możliwością tylko wprowadzania lub drukowania znaków, po jednym na raz. W rezultacie znacznie trudniej było złamać zabezpieczenia komputera mainframe, celowo lub przypadkowo, niż w przypadku dzisiejszych w pełni inteligentnych komputerów osobistych. Obraz tysięcy dedykowanych hakerów wybierających łatwo dostępny komputer. Numery dostępu lub sondowanie adresów internetowych, nielegalna zabawa i gry lub nielegalne zyski finansowe nie są mniej niepokojące niż rzeczywiste. Dostępne są środki zaradcze, w tym:

* Szyfrowanie dwukierunkowe

* Częste zmiany hasła

* Automatyczne oddzwanianie przed zalogowaniem

* Badanie nieudanych logowań

* Monitorowanie tablic ogłoszeniowych hakerów

* Zapory ogniowe ograniczające ruch do i z komputera

* Oprogramowanie antywirusowe

Ustawodawstwo, które sprawia, że dyrektorzy i wyżsi rangą urzędnicy są osobiście odpowiedzialni za straty korporacyjne, którym można było zapobiec, powinno mieć znaczący wpływ na przezwyciężenie

obecnej inercji. Roztropność mówi, że należy podjąć działania zapobiegawcze, a nie działania korygujące po takich stratach

KONSERWACJA I NAPRAWA

W przypadku każdego elementu systemu komputerowego należy przestrzegać regularnego programu konserwacji profilaktycznej. Powinno to obejmować zaplanowane czyszczenie napędów dysków i ich głowic magnetycznych, klawiatur, i drukarki. Istotnym elementem każdego programu konserwacji zapobiegawczej jest częsta wymiana filtrów powietrza w każdym urządzeniu. Jeśli nie zostanie to zrobione, przepływ czystego, chłodnego powietrza będzie utrudniony, a niepowodzenie prawie na pewno spowoduje. Opcje konserwacji komputerów osobistych, w kolejności malejącej terminowości, obejmują:

* Zarządzanie na miejscu przez stałych pracowników

* Utrzymanie na miejscu przez strony trzecie na mocy rocznej umowy

* Naprawa na wezwanie, z lub bez umowy

* Usługa przewozowa

* Usługa poczty elektronicznej

Ponieważ komputery osobiste są coraz częściej stosowane w funkcjach, które wpływają na samo istnienie firmy, ich utrzymanie i naprawa wymaga większej uwagi kierownictwa. Nadmiarowe urządzenia i kopie zapasowe w miejscu instalacji zawsze będą skuteczne, ale dłuższy czas na naprawy zewnętrzne nie będzie już możliwy. W przypadku większości aplikacji biznesowych "pożyczkobiorcy" lub "zamiennicy" powinni być natychmiast dostępni, aby przestój odbędzie się do absolutnego minimum. Kierownictwo musi ocenić znaczenie każdego funkcjonującego komputera osobistego i wybrać odpowiednią politykę utrzymania i napraw. Dostępność, wiedza, motywacja i możliwości to szczególne czynniki, które zagrażają każdej instalacji komputera osobistego. Do czasu rozwiązania każdego z tych czynników żaden system nie może być uznany za bezpieczny.

WNIOSEK

Tu chodziło głównie o środki, za pomocą których elementy sprzętowe systemu przetwarzania danych wpływają na bezpieczeństwo i integralność jego działań. Wiele zabezpieczeń stanowi integralną część samego wyposażenia; inni wymagają świadomego wysiłku, determinacji i zaangażowania. Skuteczny program bezpieczeństwa, który zapewnia zarówno zmniejszone prawdopodobieństwo katastrofy komputerowej, jak i łagodzenie skutków szkód, nie może zostać zaprojektowany ani wdrożony bez znacznych nakładów czasu i pieniędzy. Podobnie jak w przypadku innych rodzajów unikania strat, premia powinna być oceniana na podstawie oczekiwanych kosztów. Jednakże, po podjęciu decyzji, nie można dopuścić do wygaśnięcia tego równoważnika polisy ubezpieczeniowej. Składki muszą być nadal wypłacane w formie okresowych testów, ciągłej aktualizacji i stałej czujności.

LISTA KONTROLNA OCHRONY SPRZĘTU

MAINFRAME

* Czy przy wyborze nowego sprzętu bierze się pod uwagę wymagania dotyczące bezpieczeństwa i integralności?

* Czy wymuszono harmonogram konserwacji profilaktycznej?

* Czy w dzienniku przechowywane są wszystkie awarie komputera i nieplanowane przestoje?

* Czy istnieje osoba odpowiedzialna za przeglądanie dziennika i inicjowanie działań?

* Czy w miarę możliwości stosowane są kontrole parzystości?

* Czy istnieje ustalona procedura rejestrowania błędów parzystości i odzyskiwania z nich?

* Czy kody są stosowane do przodu lub do korekty błędów, gdy są uzasadnione ekonomicznie?

* Czy operatorzy postępują zgodnie z zalecanymi procedurami po błędzie odczytu lub innym zatrzymaniu maszyny?

* Czy wszystkie interwencje operatora są rejestrowane i wyjaśniane?

* Czy jest przechowywany protokół zadania i czy jest on porównywany regularnie z autoryzowaną listą zadań?

* Czy licznik interwału służy do zapobiegania nadmiernie długim biegom?

* Czy są używane funkcje chroniące pamięć masową, takie jak blokady danych i stronicowanie tylko do odczytu?

* Czy klucze do blokad danych oprogramowania są odpowiednio chronione?

* Czy podjęto środki ostrożności, aby zapobiec utracie danych z ulotnej pamięci podczas przerw w zasilaniu?

* Czy obowiązują standardowe wewnętrzne i zewnętrzne procedury etykietowania taśm i dysków?

* Czy pierścienie zabezpieczające przed zapisem są zawsze usuwane z rolek taśmy natychmiast po użyciu?

* Czy istnieje zasada, że nowe taśmy i dyski muszą być przetestowane lub certyfikowane przed użyciem? W regularnych odstępach czasu?

* Czy taśmy i dyski są odnawiane lub wymieniane, zanim wydajność spadnie?

* Czy klimatyzatory są odpowiednie do szczytowych obciążeń termicznych? Czy klimatyzacja jest bezpieczna?

* Czy istnieje harmonogram częstych zmian filtrów?

* Czy wszystkie generatory elektryczności statycznej zostały wyłączone?

* Czy wyeliminowano wszystkie źródła wody?

* Czy w całym obiekcie egzekwuje się dobre gospodarowanie?

* Czy dostęp do terminali danych jest ograniczony?

* Czy terminale i otaczające je obszary są często badane w celu wykrycia niedbale pozostawionych haseł?

* Czy prowadzony jest dziennik z nieudanymi próbami wprowadzenia komputera z terminali?

* Czy dziennik jest używany do zapobiegania kolejnym próbom?

* Czy prowadzony jest rejestr wszystkich udanych wpisów do poufnych danych?

* Czy dziennik służy do weryfikacji autoryzacji?

* Czy terminale są wyposażone w automatyczne generatory identyfikacyjne?

* Czy procedury testowe są wystarczające do zapewnienia wysokiej jakości transmisji danych?

* Czy kryptografia lub szyfrowanie są używane do ochrony poufnych danych?

* Czy sformułowano kompletny plan tworzenia kopii zapasowych? Czy jest często aktualizowany?

* Czy plan tworzenia kopii zapasowych obejmuje szkolenie, przekwalifikowanie i przekwalifikowanie personelu?

* Czy dostępna jest kopia zapasowa na miejscu dla centralnej jednostki przetwarzania? Dla urządzeń peryferyjnych?

* Czy witryna kopii zapasowej informuje o wszystkich zmianach w konfiguracji sprzętowej i systemie operacyjnym?

* Czy twoja strona zapasowa ma wystarczająco dużo wolnego czasu na zaspokojenie twoich potrzeb w nagłych wypadkach?

* Czy monitorujesz napięcie i częstotliwość linii zasilającej?

* Czy znane są efekty zaniku, zaciemnienia i zaciemnienia?

* Czy dostępne jest wcześniejsze ostrzeżenie, a jeśli tak, czy istnieje lista kontrolna działań, które należy podjąć?

* Czy są używane korektory mocy? Regulatory napięcia? Urządzenia do kondycjonowania linii? Błyskawica iskier?

* Czy dostępna jest moc zapasowa? Podwójna dostawa podstacji? Generatory silników? Bezprzerwowe zasilacze?

* Czy sprzęt zapewnia automatyczny restart i odzyskiwanie po awarii zasilania?

* Czy plany tworzenia kopii zapasowych są testowane realistycznie? W częstych odstępach czasu?

MIKROKOMPUTERY

* Czy dyski wymienne są zawsze przechowywane w zamkniętym pojemniku, gdy nie są zamontowane w napędzie?

* Czy nie wolno umieszczać jedzenia lub napojów na lub w pobliżu sprzętu komputerowego?

* Czy komputery osobiste są bezpiecznie zamocowane, aby zapobiec upuszczeniu lub kradzieży?

* Czy otwory wentylacyjne są wolne?

* Czy utrzymywane są dokładne zapasy?

* Czy zasilanie elektryczne jest prawidłowo okablowane?

* Czy dostępne są zasilacze bezprzerwowe?

* Czy elektryczność statyczna została wyeliminowana?

* Czy transmisja danych jest bezpieczna?