BEZPIECZEŃSTWO DZIAŁANIA I KONTROLA PRODUKCJI

WPROWADZANIE

Pomimo ogromnego wzrostu indywidualnego przetwarzania na komputerach osobistych i stacjach roboczych w latach od opublikowania pierwszego wydania tego podręcznika w 1975 r., scentralizowane macierze dziesiątek, setek lub tysięcy komputerów wykorzystywanych w macierzach obliczeniowych i usługach w chmurze są nadal wykorzystywane w przedsiębiorstwach przetwarzanie w aplikacjach dedykowanych do podstawowej działalności przedsiębiorstwa. Ten rozdział koncentruje się na tym, jak bezpiecznie i skutecznie obsługiwać ważne komputery i sieci. Czytelnicy z doświadczeniem wojskowym zauważą, że bezpieczeństwo operacji w sektorze cywilnym różni się od określenia OPSEC (skrót wojskowy od „bezpieczeństwa operacyjnego") używanego w dyskursie wojskowym. Zgodnie z definicją Połączonych Szefów Sztabów Sił Zbrojnych Stanów Zjednoczonych „OPSEC stara się odmawiać przeciwnikowi prawdziwych informacji i zapobiegać prawidłowemu dedukowaniu przyjaznych planów". Określając, jakie operacje bezpieczeństwa i kontroli produkcji są wymagane dla dowolnego systemu, należy przeprowadzić dokładną analizę ryzyka; odniesienia można znaleźć w całym podręczniku. W celu przeprowadzenia szybkiej analizy pomocne może być użycie kilku innych powszechnie stosowanych akronimów wojskowych i wymienienie zagrożeń z ich perspektywy.

EMPCOA - najbardziej prawdopodobny kierunek działania wroga. Jaki jest najbardziej prawdopodobny sposób działania, który osoba atakująca podejmie przeciwko Twoim systemom?

EMDCOA - najbardziej niebezpieczny sposób działania wroga. Jaka jest najgorsza rzecz, jaką może osiągnąć napastnik?

Ważenie ich w ramach analizy ryzyka może ogromnie pomóc w podjęciu decyzji, jak wykorzystać ograniczone zasoby. Pomocny może być skrót METT-TC, który jest zasadniczo większą wersją inżynieryjnej triady kosztów, czasu i jakości. Istnieją różne wersje akronimu METT-TC, ale być może najbardziej przydatnym skrótem jest

* Misja (co musimy zrobić),

* Sprzęt (jakie posiadamy),

* Czas (do kiedy musimy to zrobić),

* Oddziały (którym mamy to zrobić),

* Teren (gdzie to robimy) i

* Kultura (możliwe względy kulturowe).

Każda część naszej analizy METT-TC powinna być oczywista, może z wyjątkiem kultury. Ignorowanie kultury zarządzania, polityki i społeczności w lokalizacjach, w których należy zainstalować mechanizmy bezpieczeństwa, jest częstym błędem, zwykle mającym tragiczne konsekwencje zarówno dla bezpieczeństwa, jak i kariery specjalistów ds. bezpieczeństwa. Bardzo ważne jest, aby móc precyzyjnie zdefiniować terminy związane z bezpieczeństwem operacji i kontrolą produkcji przed rozpoczęciem dyskusji na ich temat.

Czym są systemy produkcyjne?

System produkcyjny to taki, od którego przedsiębiorstwo zależy w zakresie krytycznych funkcji. Przykłady obejmują systemy do obsługi należności, rozrachunków z dostawcami, listy płac, zapasy, systemy produkcyjne, sterowanie procesami w czasie rzeczywistym, systemy wprowadzania danych,

internetowe interfejsy klienta dla handlu elektronicznego, krytyczne systemy informacyjne, przenośne systemy obsługi danych i systemy informacji zarządczej. To, co określa się jako krytyczne, to funkcja misji, a nie jednolita recepta. W związku z tym należności mogą być krytycznie ważną funkcją dla firmy produkcyjnej pracującej z niską marżą, z należnościami potrzebnymi do natychmiastowej zapłaty za kluczowe dostawy, ale mogą być mniej istotne dla małej grupy odnoszących sukcesy partnerów prowadzących firmę konsultingową.

Czym są operacje?

Operacje składają się z wymagań dotyczących kontroli, konserwacji i wsparcia systemów produkcyjnych. Personel operacyjny jest odpowiedzialny za takie funkcje jak:

* Integracja nowych systemów oprogramowania z istniejącą konfiguracją

* Uruchamianie programów i zadań wsadowych w celu aktualizacji baz danych i tworzenia raportów

* Instalacja nowych wersji programów produkcyjnych

* Utrzymywanie baz danych produkcyjnych dla maksymalnej wydajności

* Zarządzanie kopiami zapasowymi (tworzenie, etykietowanie, przechowywanie i usuwanie)

* Reagowanie na sytuacje awaryjne i przywracanie funkcjonalności

* Montowanie woluminów pamięci masowej taśm, kaset lub dysków w odpowiedzi na żądania użytkownika lub programu

* Obsługa specjalnych formularzy dla poszczególnych wydruków (np. blankietów czekowych)

* Zarządzanie wszystkimi aspektami sieci produkcyjnych, takimi jak konfiguracja routerów, mostów, bram, propagacja bezprzewodowa i zapory

Czym są programy komputerowe?

Program komputerowy to zestaw instrukcji, które informują komputer, co ma zrobić, aby wykonać zadanie. Programy komputerowe mogą być nabywane lub opracowywane wewnętrznie. Opracowane wewnętrznie programy przechowywane są w systemach komputerowych w dwóch podstawowych formach. Programy źródłowe mają postać, w jakiej zostały napisane (zakodowane) przez programistów komputerowych. Instrukcje w programach źródłowych są w językach takich jak COBOL, Visual BASIC, C++ i Java. Programy w języku źródłowym są przechowywane w plikach i przechowywane w folderach dyskowych zwanych bibliotekami źródłowymi lub bibliotekami programów. Programy wykonywalne zostały przekonwertowane z kodu źródłowego, poprzez kompilację lub interpretację, na program, który może wykonać komputer. Programy wykonywalne mogą być utrzymywane w dwóch osobnych formach: obiektowej i ładowanej. Program obiektowy to częściowo wykonywalny moduł, który musi być połączony z innymi wykonywalnymi modułami, takimi jak moduły wejścia/wyjścia, aby stać się modułem ładowalnym. Mówi się, że jako moduły ładujące programy są w formie wykonywalnej. Programy wykonywalne są przechowywane w bibliotekach produkcyjnych, z których są wywoływane w razie potrzeby. Nabyte programy są zazwyczaj w formie obiektu i obciążenia. Kod źródłowy jest własnością organizacji, która go opracowała i rzadko jest przekazywany przedsiębiorstwu przejmującemu. Gdy trzeba zmienić programy opracowane wewnętrznie, programiści pracują z kopiami programów źródłowych. Kopie są przechowywane w innej bibliotece, zwanej biblioteką programisty. Programiści wprowadzają zmiany w swojej kopii programów źródłowych i przechodzą przez proces rekompilacji i testowania, aż zmodyfikowany program będzie działał poprawnie. Gdy nabyte programy wymagają zmian, często z organizacją, od której nabyto programy, wystawiana jest

umowa na dokonanie modyfikacji. W niektórych sytuacjach wewnętrzni programiści generują nowe programy i interfejsy do pierwotnie nabytych programów. Wykorzystywane są te same biblioteki: biblioteki źródłowe dla kodu źródłowego, biblioteki produkcyjne dla modułów wykonywalnych oraz biblioteki programistyczne dla pracy w toku. Te biblioteki muszą być chronione. Utrata lub uszkodzenie może pociągać za sobą ogromne koszty i znaczne niedogodności; ich odzyskanie może wymagać dużo czasu i dużych nakładów.

Czym są procedury?

Procedury to zestawy instrukcji, które informują komputer, co ma robić w określonych sytuacjach. Różnią się od programów, ponieważ nie są kompilowane. Przechowywane w plikach lub bazach danych są wywoływane i interpretowane w razie potrzeby. Instrukcje proceduralne składają się z poleceń operacyjnych i parametrów. Polecenia operacyjne informują komputer, co ma robić, a parametry informują komputer, na którym encji ma działać. Job Control Language (JCL) jest przykładem języka proceduralnego. Instrukcje języka proceduralnego są często używane w systemach zarządzania bazami danych oraz w produktach zabezpieczających. Na komputerach osobistych pliki wsadowe (.BAT) są formą prostej procedury.

Czym są pliki danych?

Prawie wszystko, co jest przechowywane i utrzymywane w systemie komputerowym, ma formę pliku.2 Programy, procedury, informacje są przechowywane w plikach, używając pojęcia pliku w najszerszym tego słowa znaczeniu; czyli zbiór powiązanych elementów. To użycie stało się najbardziej widoczne w przypadku wszechobecnego komputera osobistego (PC). Pliki danych, w odróżnieniu od plików programów i innych typów, to te, które przechowują informacje. W środowisku PC pliki danych mogą być nazywane dokumentami. Dokumenty są tworzone przez edytory tekstu, arkusze kalkulacyjne, generatory grafiki i inne aplikacje. W środowiskach komputerów mainframe i średniej wielkości pliki danych są tworzone i obsługiwane przez aplikacje, takie jak płace, księgowość, inwentaryzacja, wprowadzanie zamówień i sprzedaż. Niektóre pliki danych są przejściowe; oznacza to, że są tworzone, używane i usuwane w krótkim czasie. W przypadku zgubienia lub uszkodzenia można je szybko zrekonstruować, bez większych trudności. Zwykle nie ma potrzeby ochrony plików przejściowych. Inne pliki, takie jak pliki główne lub bazy danych organizacji (grupy plików, które są połączone ze sobą za pomocą systemu zarządzania bazami danych lub DBMS), zawierają informacje, które są ważne, poufne lub praktycznie niezastąpione. Pliki te, generowane przez komputery PC, mainframe i średniej wielkości systemy komputerowe, muszą być chronione przez oprogramowanie zabezpieczające i procedury tworzenia kopii zapasowych, aby zapewnić ochronę przed utratą, zniszczeniem, kradzieżą, ingerencją i nieuprawnionym ujawnieniem.

ZARZĄDZANIE OPERACJAMI

Procesy efektywnego i wydajnego zarządzania operacjami mają bezpośrednie korzyści w zakresie zapewnienia informacji. W szczególności te aspekty zarządzania operacjami mają szczególną wartość dla poprawy i utrzymania bezpieczeństwa:

* Rozdzielenie obowiązków

* Zdefiniowanie roli oficera bezpieczeństwa lub administratora bezpieczeństwa

* Ograniczenie dostępu do centrum operacyjnego

* Definiowanie bezpiecznych procesów kontroli zmian

* Staranna kontrola nad oprogramowaniem dostarczonym zewnętrznie

* Zarządzanie zapewnieniem jakości i kontrolą jakości

Rozdział obowiązków

Rozdzielenie obowiązków jest kluczową kontrolą, którą należy stosować przy opracowywaniu i modyfikowaniu programów. W przedsiębiorstwach, w których istnieją systemy i działy programowania, które tworzą i utrzymują niestandardowe programy, każdemu indywidualnemu programiście przypisywany jest identyfikator użytkownika i hasło. W tych przedsiębiorstwach, w których programy są opracowywane i utrzymywane wewnętrznie, stale wprowadzane są zmiany w programach, aby sprostać zmieniającym się wymaganiom biznesowym. Zmodyfikowane programy wykonywalne, po rekompilacji i przetestowaniu przez programistów, przenoszone są z ich bibliotek do bibliotek produkcyjnych. Zmodyfikowane programy źródłowe są przenoszone do bibliotek źródłowych. Programiści są odpowiedzialni za utrzymanie aktualności bibliotek źródłowych, podczas gdy operacje komputerowe lub inna grupa funkcjonalna oddzielona od programowania mogą być odpowiedzialne za utrzymanie bibliotek produkcyjnych. Gdy zaktualizowany program wykonywalny jest przenoszony z biblioteki programisty do biblioteki produkcyjnej, dołączany jest przekaz, podpisany przez kierownika w dziale programowania. Szczególną konsekwencją rozdzielenia obowiązków jest to, że członek personelu operacyjnego powinien być zawsze zaangażowany w fazy analizy funkcjonalnej i definiowania wymagań dotyczących zmian w programach produkcyjnych. Perspektywa operacji nie zawsze jest jasna dla programistów, a takie kwestie, jak rejestrowanie, wycofywanie i odzyskiwanie, omówione w dalszej części tego rozdziału, należy zwrócić im uwagę na wczesnym etapie cyklu rozwoju i konserwacji. Niezwykle ważne jest, aby programiści i personel operacyjny zrozumieli, że w żadnym wypadku programiści nie mogą instalować zmian w systemach produkcyjnych bez odpowiednich testów i autoryzacji. Zarządzanie poprawkami zostało szczegółowo omówione w rozdziale 40 tego podręcznika.

Funkcjonariusz ds. bezpieczeństwa lub Administrator ds. bezpieczeństwa

Współczesne przedsiębiorstwa zazwyczaj obejmują kombinację zewnętrznych usług przetwarzania w chmurze, komputerów mainframe, komputerów średniej wielkości i sieci lokalnych (LAN) składających się z setek lub tysięcy stacji roboczych, komputerów PC, terminali i innych urządzeń, wszystkie połączone ze sobą i często połączone za pomocą tego samego zestawu w innych przedsiębiorstwach na całym świecie za pośrednictwem Internetu. Za zapewnienie i utrzymanie bezpieczeństwa plików, baz danych i programów odpowiada dział, jednostka lub mała grupa w mniejszych przedsiębiorstwach. Często kojarzony z tą funkcją tytuł to oficer bezpieczeństwa informacji (ISO) lub oficer bezpieczeństwa systemów informatycznych (ISSO). Ta osoba lub dział jest upoważniony do realizacji polityki bezpieczeństwa określonej przez kierownictwo wyższego szczebla przedsiębiorstwa. Szef ochrony jest upoważniony do zezwalania lub blokowania dostępu do plików, baz danych i programów. W języku oficera bezpieczeństwa tworzone i utrzymywane są procedury, które ustanawiają relacje między osobami, programami i plikami. Użytkownicy, programiści i technicy otrzymują uprawnienia pełnego dostępu, tylko aktualizacji, a nawet odczytu. Funkcjonariusz ds. bezpieczeństwa ma prawo do zmiany lub odebrania uprawnień .

Ogranicz dostęp do Centrum Operacyjnego

Fizyczny dostęp do centrum operacyjnego daje osobie ogromną moc do zakłócania systemów produkcyjnych. Taki dostęp musi być ściśle kontrolowany.

Potrzeba, nie status, determinuje dostęp

Fundamentalną zasadą skutecznego bezpieczeństwa jest to, że dostęp do obszarów o ograniczonym dostępie jest przyznawany na podstawie ról. Pracownicy, których role nie uzasadniają dostępu, powinni być wykluczeni z autonomicznego dostępu do systemów produkcyjnych. W szczególności dyrektorzy wysokiego szczebla, tacy jak prezes, dyrektor generalny, dyrektor finansowy, dyrektor operacyjny, dyrektor techniczny i wszyscy wiceprezesi, powinni zbadać swoje role i ustalić, czy powinni mieć możliwość wejścia do operacji ośrodek bez opieki; w większości przypadków taki dostęp jest nieuzasadniony. Ograniczenie własnego dostępu wyznacza ważny model dla innych aspektów polityki bezpieczeństwa i pokazuje, że to potrzeba, a nie status społeczny czy pozycja w hierarchii korporacyjnej, determinuje dostęp do zastrzeżonych obszarów. Kwestia ta jest również omówiona w rozdziale 45 dotyczącym praktyk i polityki zatrudnienia w niniejszym Podręczniku.

Podstawowe metody kontroli dostępu

Jak wyjaśniono wcześniej, kontrola dostępu zależy od identyfikacji i uwierzytelnienia (I&A). I&A może opierać się na:

* Czego brakuje innym (tokeny, takie jak klucze fizyczne lub karty inteligentne)

* Co wiadomo, czego inni nie wiedzą (identyfikatory użytkowników i hasła lub hasła)

* Czym różni się od innych (statyczne cechy biometryczne, takie jak odciski palców, wzory tęczówki, wzory siatkówki i rysy twarzy)

* Co robi się inaczej niż inni (dynamiczna biometria, taka jak wzorce głosu, wzorce pisania i dynamika podpisu)

Typowy układ bezpiecznego dostępu do centrum operacyjnego może obejmować klawiatury do wprowadzania określonego kodu lub czytniki kart zaprogramowane do przyjmowania posiadaczy określonych kart z paskiem magnetycznym, kart inteligentnych lub tokenów identyfikacji radiowej (RFID). Jeśli centrum operacyjne działa 24 godziny na dobę i zatrudnia pełnoetatowych pracowników, obecność operatorów zapewnia dodatkową warstwę bezpieczeństwa, aby zapobiec nieautoryzowanemu dostępowi. Zdalne monitorowanie wrażliwych obszarów zwiększa bezpieczeństwo, zniechęcając do nieautoryzowanego dostępu lub nieautoryzowanego zachowania i przyspiesza reakcję na ewentualny sabotaż.

Logowanie i odznakowanie odwiedzających

Odwiedzający obiekt, w którym znajdują się wrażliwe systemy, powinni być zalogowani (tj. ich tożsamość sprawdzona i odnotowana na piśmie) przy kontrolowanym wejściu i zaopatrzona w identyfikatory dla odwiedzających. W aplikacjach o wysokim poziomie bezpieczeństwa może być wymagane dodatkowe logowanie podczas wchodzenia do samego centrum operacyjnego. Aby zachęcić do zwrotu identyfikatorów dla gości, niektóre zasady bezpieczeństwa wymagają od gościa złożenia ważnego dokumentu, takiego jak prawo jazdy, ochroniarzom przy głównym wejściu. Skuteczność identyfikatorów dla gości jako sposobu identyfikacji osób niebędących pracownikami zależy wyłącznie od używania identyfikatorów przez cały czas przez cały personel; jeśli nienoszenie plakietki jest dopuszczalne i powszechne, złośliwy gość może po prostu ukryć plakietkę, aby uchodzić za upoważnionego pracownika. Czas logowania i wylogowania może być cennym dowodem kryminalistycznym w przypadku wykrycia nadużycia. Jednak takie zapisy można wykazać, że są wiarygodne tylko wtedy, gdy strażnicy odpowiedzialni za prowadzenie dzienników konsekwentnie weryfikują kompletność i poprawność wszystkich informacji wpisanych do dzienników. Nagrania wideo z wejścia, aby uchwycić twarz każdego odwiedzającego, a także dokładny czas przybycia i wyjazdu,

mogą być bardzo przydatne zarówno do identyfikacji oszustów, jak i do sprawdzenia, czy ochroniarze wykonują swoją pracę prawidłowo.

Towarzyszyć odwiedzającym

Żadnym odwiedzającym bez opieki nie należy zezwalać na poruszanie się po centrum operacyjnym lub w obiekcie, w którym znajduje się takie centrum. W obiektach o wysokim poziomie bezpieczeństwa ktoś musi nawet towarzyszyć gościowi w toalecie i czekać na gościa za drzwiami. Jeśli konsultant lub pracownik tymczasowy ma pracować nad projektem dłużej niż jeden dzień, może być dopuszczalne przyznanie tej osobie przepustki o ograniczonym dostępie do obszarów o niskim poziomie bezpieczeństwa; jednak obszary o wysokim poziomie bezpieczeństwa, takie jak centrum operacyjne, nadal wymagałyby towarzystwa takiej osoby. Kiedy jeden z autorów (Kabay) był dyrektorem obsługi technicznej dużego biura serwisowego w Montrealu w połowie lat 80., prezes firmy przybył niezapowiedziany w sobotni wieczór do drzwi centrum operacyjnego z gościem, aby go pokazać wokół centrum komputerowego. Młody operator wyjaśnił z pewnym niepokojem, że nazwisko prezydenta nie znajduje się na liście zatwierdzonych gości indywidualnych, więc nie zezwoli na wstęp (chociaż zaproponował, że zadzwoni do swojego szefa w celu uzyskania zezwolenia). Trzeba mu przyznać, że prezydent z wdziękiem przyjął ograniczenie - iw poniedziałek rano napisał list pochwalny dla operatora.

Procedury kontroli zmian z perspektywy operacyjnej

Gdy programiści wprowadzą zmiany w programach produkcyjnych, a cała dokumentacja i procedury testowe są kompletne, nowe wersje są formalnie przekazywane personelowi operacyjnemu w celu integracji z produkcją.

Przenoszenie nowych wersji oprogramowania do produkcji.

Menedżerowie operacyjni i personel muszą sprostać tym wymaganiom podczas przenoszenia nowych wersji oprogramowania do produkcji:

Identyfikacja — śledzenie używanego oprogramowania

Autoryzacja – kontrola zmian

Harmonogramowanie — minimalizowanie przerw w produkcji

Kopie zapasowe — zapewnienie, że wszystkie wymagane informacje są dostępne do przywrócenia poprzedniego stanu

Rejestrowanie — śledzenie wprowadzonych danych w celu odzyskania oraz błędów w celu zdiagnozowania problemów

Backout – powrót do poprzedniej wersji produkcyjnej w przypadku katastrofalnych błędów

Identyfikacja

Podstawą kontroli produkcji jest dokładna wiedza, które wersje oprogramowania produkcyjnego są w użyciu. Każdy moduł musi mieć unikalną identyfikację, która umożliwia natychmiastowe śledzenie między kodem wykonywalnym a kodem źródłowym; wszystkie zmiany w konkretnym module muszą być w pełni udokumentowane przez grupę programistyczną. Niepowtarzalne identyfikatory pozwalają procesowi zapewnienia jakości zapewnić, że do produkcji trafiają tylko te moduły, które zostały odpowiednio przetestowane. Większość zakładów produkcyjnych używa trzypoziomowego schematu numerowania do śledzenia wersji. Zazwyczaj wersja a.b.c (np. 7.13.201) jest definiowana w następujący sposób:

* c zmienia się za każdym razem, gdy cokolwiek — nawet błąd ortograficzny — jest zmieniane.

* b zmienia się, gdy menedżerowie programu decydują się na zgrupowanie wielu poprawek błędów w nowej wersji do wydania na produkcję.

* zmiany po dodaniu istotnych nowych funkcji; często kod źródłowy jest całkowicie przenumerowany, jeśli zmiany są wystarczająco duże.

Numer wersji kodu obiektowego musi być zgodny z numerem jego kodu źródłowego. Cały kod obiektowy powinien zawierać wewnętrzną dokumentację swojego numeru wersji, aby można było ją natychmiast ustalić, bez konieczności przeglądania potencjalnie niedokładnej dokumentacji zewnętrznej.

Autoryzacja

Muszą istnieć ścisłe procedury, aby uniemożliwić nieuczciwym programistom wprowadzenie zmodyfikowanego kodu do pakietu produkcyjnego. Oprócz niebezpieczeństw związanych z wprowadzaniem nieprzetestowanych lub nieudokumentowanych zmian, umożliwienie dowolnej osobie modyfikowania procesów produkcyjnych bez weryfikacji i autoryzacji przez odpowiedni łańcuch odpowiedzialności może pozwolić na wrogi kod, taki jak konie trojańskie i backdoory , który ma zostać wprowadzony do systemów.

Planowanie

Wdrożenie każdej nowej wersji systemu produkcyjnego wymaga starannego planowania i harmonogramowania. Personel operacyjny musi przygotować się na zmiany we wszystkich aspektach produkcji, które zależą od danego systemu; na przykład mogą wystąpić wymagania dotyczące nowych formularzy drukarskich, dodatkowych taśm magnetycznych i innych materiałów eksploatacyjnych, które należy zamawiać z wyprzedzeniem. Nowe prośby o interwencję operatora lub zmiany statusu i komunikatów o błędach podczas produkcji wymagają odpowiedniej dokumentacji i szkoleń. Wpływ na inne programy może wymagać specjalnych przygotowań, które muszą uwzględniać wymagania planowania innych systemów, których to dotyczy. Ponadto nowe wersje oprogramowania są często wdrażane natychmiast po głównych zadaniach produkcyjnych, takich jak przetwarzanie na koniec roku lub kwartalne, aby zachować spójność w okresie rozliczeniowym. Z tych wszystkich powodów planowanie jest niezwykle ważne dla bezproblemowego działania.

Kopie zapasowe

Podczas modyfikowania systemów produkcyjnych pracownicy operacyjni zwykle wykonują jedną lub więcej kompletnych kopii zapasowych (patrz rozdział 57 w niniejszym podręczniku) oprogramowania i danych, które mają zostać zmodyfikowane. Ta procedura jest niezbędna, aby umożliwić całkowite przywrócenie poprzedniego środowiska pracy w przypadku katastrofalnej awarii nowego oprogramowania i struktur danych. Menedżerowie i operatorzy systemów powinni mieć świadomość, że jeśli proponowane przez nich zmiany wymagają ponownego formatowania dysków w systemie produkcyjnym, muszą wykonać co najmniej dwie pełne kopie zapasowe, aby mieć pewność, że błąd w jednej z kopii zapasowych nie spowoduje katastrofy, gdy cały system do przywrócenia.

Rejestrowanie

Aby umożliwić odzyskiwanie lub wycofywanie bez utraty nowych danych i zmian w istniejących danych, które mogły zostać przeprowadzone przy użyciu nowego oprogramowania i struktur danych, wszystkie programy produkcyjne powinny zawierać funkcję rejestrowania. Rejestrowanie prowadzi dziennik

wszystkich informacji wymaganych do śledzenia zmian danych i ponownego generowania prawidłowej wersji danych przez zastosowanie wszystkich zmian do początkowego warunku początkowego.

Rejestrowanie wymaga synchronizacji z kopiami zapasowymi, aby uniknąć utraty lub uszkodzenia danych. Specjalne wymagania mogą istnieć, gdy nowa wersja systemu produkcyjnego wiąże się ze zmianami struktur danych; w takich przypadkach zastosowanie informacji o zmianach do starszych struktur danych może wymagać specjalnych programów użytkowych. Ponieważ programiści czasami zapominają o takich możliwościach, personel operacyjny powinien być przygotowany do przypominania personelowi programistycznemu o takich wymaganiach w fazie projektowania dla wszystkich zmian.

Tworzenie kopii zapasowych i odzyskiwanie

Czasami nowa wersja oprogramowania produkcyjnego jest niedopuszczalna i musi zostać usunięta ze środowiska produkcyjnego. Ta decyzja może zostać podjęta natychmiast lub może nastąpić po wprowadzeniu znacznej ilości danych i manipulacji danymi. W obu przypadkach operacje powinny mieć możliwość powrotu do poprzedniej wersji systemu produkcyjnego bez utraty danych. Proces ten obejmuje przywrócenie wcześniejszego kompletnego środowiska operacyjnego, z zsynchronizowanym oprogramowaniem i danymi, a następnie wykorzystanie plików dziennika do powtórzenia wprowadzania danych i modyfikacji danych od momentu przełączenia do momentu awaryjnego. Nie wszystkie zmiany, które zostały wprowadzone przy użyciu nowej wersji, koniecznie będą miały zastosowanie do poprzednich danych; na przykład, gdyby do bazy danych dodano nowe pola, dane przechowywane w tych polach nie byłyby przydatne w przypadku starszej, prostszej struktury danych. Podobnie, jeśli pola zostały usunięte w nowszej bazie danych, odzyskanie będzie wiązało się z podaniem wartości dla tych pól w starszej bazie danych. Wszystkie te funkcje muszą być dostępne w programach odzyskiwania i kopiach zapasowych, które powinny towarzyszyć każdej zmianie wersji w systemach produkcyjnych.

Używanie podpisów cyfrowych do walidacji programów produkcyjnych

W przypadku wykrycia nieautoryzowanego intruza lub niezadowolonego pracownika, który uzyskał dostęp do bibliotek produkcyjnych, konieczne będzie ustalenie, czy nie dokonano nieautoryzowanych modyfikacji programów produkcyjnych. Znaczniki daty i czasu w programach mogą rejestrować czas zmian, ale wiele środowisk operacyjnych umożliwia modyfikowanie takich informacji za pomocą narzędzi systemowych, które odczytują i zapisują bezpośrednio na dysku bez przechodzenia przez normalne wywołania systemowe. W takich przypadkach nie byłoby znacznika czasu ani wpisu w dzienniku. Jednym z rozwiązań, które zostało z powodzeniem zastosowane, jest zastosowanie sum kontrolnych do wszystkich komponentów produkcyjnych. Oprogramowanie do sum kontrolnych stosuje obliczenia do programów tak, jakby kody były po prostu liczbami; wyniki mogą być wrażliwe na zmiany tak małe jak pojedynczy bit. Jeśli jednak sumy kontrolne są obliczane w ten sam sposób dla wszystkich programów, dostęp do narzędzia sumy kontrolnej może umożliwić przestępcy zmianę modułu, a następnie uruchomienie narzędzia sumy kontrolnej w celu utworzenia odpowiedniej nowej sumy kontrolnej, ukrywając w ten sposób dowody zmiany. Aby utrudnić takie podstępy, sumy kontrolne można przechowywać w bazie danych. Oczywiście ta baza sum kontrolnych sama w sobie musi być chroniona przed nieautoryzowanymi zmianami, na przykład za pomocą szyfrowania. Przechowywanie sum kontrolnych może utrudnić ukrycie nieautoryzowanych zmian, ale także wydłuża łańcuch luk w zabezpieczeniach. Lepszym sposobem określenia, czy kod obiektowy lub kod źródłowy został zmodyfikowany, jest użycie podpisów cyfrowych. Podpisy cyfrowe są podobne do sum kontrolnych, ale wymagają wprowadzenia klucza prywatnego, który może i musi być chroniony przed ujawnieniem. Weryfikację podpisu cyfrowego można przeprowadzić przy użyciu odpowiedniego klucza

publicznego, który można udostępnić bez naruszania tajemnicy klucza prywatnego. Aby uzyskać więcej informacji na temat kluczy publicznych i prywatnych, zobacz Rozdział 7 o szyfrowaniu i Rozdział 37 o PKI i urzędami certyfikacji w niniejszym podręczniku. Gdy podpisy cyfrowe są używane do uwierzytelniania kodu, możliwe jest rutynowe sprawdzanie poprawności systemów produkcyjnych, pod warunkiem, że proces ten nie jest zbyt uciążliwy, aby można go było wykonać w ramach normalnego procesu produkcyjnego. Na przykład powinno być możliwe sprawdzenie poprawności wszystkich podpisów cyfrowych w czasie nie dłuższym niż kilka minut, zanim rozpocznie się codzienny cykl produkcyjny.

Korzystanie z oprogramowania dostarczonego zewnętrznie

Produkcja często wykorzystuje oprogramowanie spoza organizacji; Takie oprogramowanie może być komercyjnymi programami dostępnymi z półki (COTS) lub może składać się z programów zmodyfikowanych lub napisanych specjalnie dla organizacji przez dostawcę oprogramowania. W każdym razie oprogramowanie zewnętrzne stwarza szczególne problemy z zaufaniem zespołowi produkcyjnemu. Zdarzały się udokumentowane przypadki, w których produkcyjne wersje oprogramowania renomowanych firm programistycznych zawierały wirusy lub pisanki (nieudokumentowane funkcje, takie jak dobrze znany symulator lotu w MSExcel 97, który wyświetlał graficzny krajobraz zawierający monitor pokazujący nazwy zespołu programistów Excel). Ponadto niektórzy konsultanci publicznie przyznali, że celowo umieszczają kod konia trojańskiego (nieudokumentowane złośliwe oprogramowanie), który pozwala im na uszkodzenie danych lub dezaktywację programów zainstalowanych na stronach klienckich, jeśli nie uiścili opłat. W dużych centrach danych może być możliwe uruchomienie procedur zapewniania jakości na kodzie dostarczonym z zewnątrz (patrz rozdział 39 niniejszego podręcznika). Takie testy powinny obejmować monitorowanie pokrycia, w ramach którego zestaw testów sprawdza cały skompilowany kod odpowiadający każdej linii kodu źródłowego. Jednak rzadko zdarza się, aby grupa operacyjna posiadała zasoby niezbędne do takiego testowania. Wiarygodność autorskiego oprogramowania zewnętrznego napisanego lub przystosowanego specjalnie dla klienta może ostatecznie zależeć od umów prawnych pomiędzy dostawcą a użytkownikiem. Takie ograniczenia prawne mogą nie powstrzymać niezadowolonego lub nieuczciwego pracownika w organizacji dostawcy przed włączeniem szkodliwego kodeksu, ale przynajmniej mogą stanowić podstawę do odszkodowania w razie problemów.

Zweryfikuj podpisy cyfrowe w kodzie źródłowym, jeśli to możliwe

Jeśli zewnętrznie dostarczony kod jest dostarczany z biblioteką źródłową, a także ze skompilowanymi modułami, operacje powinny starać się, aby suplier dostarczał podpisy cyfrowe dla wszystkich takich programów. Podpisy cyfrowe pozwolą na uwierzytelnienie pochodzenia kodu i mogą utrudnić przestępcom dostarczenie zmodyfikowanego kodu użytkownikowi. Ponadto podpisy cyfrowe mogą wspierać niezaprzeczalność kodu (tj. dostawca nie będzie mógł wiarygodnie twierdzić, że nie dostarczył kodu), a zatem podpisy mogą być przydatne w razie potrzeby w postępowaniu sądowym.

Kompiluj ze źródła, gdy jest to możliwe

Tam, gdzie to możliwe, wysoce pożądana jest możliwość kompilowania plików wykonywalnych z kodu źródłowego na maszynie docelowej. Kompilacja ze źródła umożliwia procesom zapewniania jakości sprawdzenie źródła pod kątem nieudokumentowanych funkcji, które mogą stanowić naruszenie bezpieczeństwa, oraz ścisłe powiązanie plików wykonywalnych ze zweryfikowanym źródłem. Ponadto kompilacja w systemie lokalnym zapewnia, że wszystkie wywołania procedur systemowych zostaną spełnione przez połączenie z plikami wykonywalnymi, takimi jak biblioteki dołączane dynamicznie (DLL) dostarczane w bieżącej wersji systemu operacyjnego.Jednak kompilacja w systemie lokalnym ma dodatkowe implikacje komplikuje wdrażanie nowych aplikacji: ponieważ procedury systemowe

powiązane ze skompilowanym kodem mogą nie być identyczne z tymi używanymi podczas testów zapewnienia jakości producenta, organizacja klienta musi zaplanować własne testy zapewnienia jakości. Personel operacyjny powinien wyraźnie wyrazić tę preferencję dla kodu źródłowego osobie lub grupie kontrolującej nabywanie oprogramowania zewnętrznego. Więcej informacji na temat pisania bezpiecznego kodu znajduje się w rozdziale 38 tego podręcznika; Aby uzyskać informacje na temat bezpiecznego tworzenia oprogramowania i zapewniania jakości oprogramowania, zobacz Rozdział 39.

Kontrola jakości a zapewnienie jakości

Wspominano o zapewnieniu jakości jako o podstawowym filarze bezpieczeństwa operacji. Zapewnienie jakości odnosi się do procesów zaprojektowanych w celu zapewnienia i weryfikacji ważności programów produkcyjnych. Jednak inny aspekt jakości dotyczy grupy operacyjnej: jakość produkcji. Proces weryfikacji i zapewniania jakości wyników jest znany jako kontrola jakości.

Umowy o poziomie usług

W przeciwieństwie do prawdy matematycznej, nie ma absolutnego standardu jakości operacji obliczeniowych. Każda organizacja musi określić poziom jakości odpowiedni dla konkretnego zastosowania. Powszechnie przytaczaną zasadą w programowaniu i operacjach jest to, że istnieje złożona zależność między jakością, kosztem i czasem rozwoju: Zwiększanie jakości zwiększa zarówno koszt, jak i czas rozwoju; skrócenie czasu opracowywania zwiększa koszty, jeśli ma zostać zachowana jakość. Wynika z tego, że każdy system powinien zawierać definicję akceptowalnej wydajności; takie definicje są znane jako umowy dotyczące poziomu usług (SLA). Umowy SLA zazwyczaj zawierają minimalne i maksymalne limity wydajności, wykorzystania zasobów i jakości wydruku. Limity powinny być wyrażone w kategoriach statystycznych; na przykład „Czas odpowiedzi mierzony jako czas między naciśnięciem klawisza ENTER a wyświetleniem kompletnej odpowiedzi na ekranie powinien być krótszy niż trzy sekundy w 95 procentach wszystkich transakcji i nie może przekraczać czterech sekund w dowolnym momencie”. Umowy SLA mogą określać różne standardy dla różnych rodzajów transakcji, jeśli dyktują to potrzeby biznesowe użytkowników.

Monitorowanie wydajności

Wydajność systemu komputerowego zależy od pięciu elementów:

1. Czas dostępu i szybkość jednostki centralnej (CPU)

2. Czas dostępu i szybkość pamięci masowej (dysków)

3. Czas dostępu i szybkość szybkiej pamięci (RAM)

4. Projekt aplikacji

5. Dostępna przepustowość sieci

Grupy operacyjne powinny monitorować wydajność, aby zapewnić spełnienie wymagań umów SLA. Istnieją dwa podejścia do takiego monitorowania: (1) analiza plików dziennika oraz (2) przechwytywanie i analiza danych w czasie rzeczywistym. Pliki dziennika zaprojektowane z myślą o analizie wydajności mogą rejestrować dokładne czasy dowolnych interesujących zdarzeń; na przykład można mieć rekord w pliku dziennika, który pokazuje, kiedy konkretny użytkownik zainicjował żądanie odczytu określonych danych i inny rekord, który pokazuje, kiedy dane były wyświetlane na ekranie użytkownika. Taki poziom szczegółowości jest nieoceniony w przypadku analizy wydajności, ponieważ dane pozwalają analitykom spojrzeć na wszelkiego rodzaju transakcje i obliczyć statystyki dotyczące rozkładu czasów odpowiedzi. Z kolei dane te mogą być wykorzystywane do analizy trendów, która

czasami może uwydatnić problemy w strukturze programu lub danych, konstrukcji lub konserwacji. Na przykład zbyt długi czas wyszukiwania w tabeli danych może wskazywać, że system korzysta z dostępu szeregowego do danych, ponieważ został zaprojektowany bez odpowiedniego indeksu, który umożliwiałby szybki losowy dostęp do potrzebnych rekordów. Innym podejściem do monitorowania i analizy wydajności jest użycie monitorów w czasie rzeczywistym, które mogą ostrzegać personel operacyjny o nieprawidłowej wydajności. Na przykład program użytkowy może być zaprojektowany do obliczania czasu odpowiedzi w locie; wyniki mogą być wyświetlane numerycznie lub graficznie na desce rozdzielczej dla personelu operacyjnego. Wartości spadające poniżej określonego parametru mogą sygnalizować nienormalny stan za pomocą koloru lub dźwięku, aby ostrzec operatorów o spadku wydajności. Takie zintegrowane metryki wydajności umożliwiają najszybszą możliwą reakcję na problemy z wydajnością. Obszerne zestawy pomiarów w czasie rzeczywistym są czasami nazywane narzędziami świadomości sytuacyjnej. Nawet jeśli w aplikacjach brakuje zintegrowanych metryk wydajności, czasami można użyć narzędzi wydajności online na poziomie systemu do analizy aktywności systemu. W jednym przypadku w doświadczeniu jednego z autorów (Kabay), na przykład, dostawca oprogramowania w połowie lat 80. obiecywał czas odpowiedzi wynoszący 10 sekund lub mniej dla wszystkich transakcji, ale jedna konkretna operacja trwała 43 minuty. Ponieważ umowa SLA została naruszona, klient groził pozwaniem dostawcy za cały koszt rozwoju i trzyletnie opłaty za utrzymanie — w sumie 3,8 miliona dolarów (około 12 milionów dolarów w 2013 roku). Korzystając z internetowego narzędzia wydajności, szybko stało się oczywiste, że omawiana transakcja generowała ogromną ilość operacji we/wy na dysku (operacje odczytu i zapisu): 80 000 odczytów o dostępie swobodnym w określonym zestawie danych w celu odfiltrowania kilku rekordów docelowych przy użyciu pole bez indeksu. Zainstalowanie i używanie odpowiedniego indeksu oraz kompaktowanie zbioru danych w tym polu jako klucza podstawowego w celu zapewnienia szybkiego dostępu do bloków powiązanych rekordów skróciło czas odpowiedzi do 6 sekund

Zasoby monitorowania

Konsekwentne monitorowanie wykorzystania zasobów to jedna z najcenniejszych ról personelu operacyjnego. Operacje centrum danych powinny obejmować regularną analizę plików dziennika systemowego w celu śledzenia zmian liczby plików, ilości dostępnego wolnego miejsca na dysku, liczby zużytych cykli procesora, liczby operacji wymiany pamięci wirtualnej i mniej ezoterycznych wymagań dotyczących zasobów, takich jak liczba wydrukowanych wierszy lub stron, liczby żądanych montowań taśm, liczby używanych taśm kopii zapasowych itd. Dane te powinny być przedstawione na wykresach i poddane analizie trendów, aby przewidzieć, kiedy poszczególne zasoby zostaną nasycone, jeśli trend się utrzyma. Nawet prosty program do obsługi arkuszy kalkulacyjnych, taki jak Excel, może łatwo tworzyć linie regresji na wykresach. Operacje mogą następnie zmniejszyć zapotrzebowanie albo poprzez poprawę aspektów produkcji (np. optymalizacja programów tak, aby wymagały mniej zasobów) albo poprzez zwiększenie dostępnych zasobów (np. instalowanie uaktualnienia pamięci). Kolejny poziom analizy skupia się na konkretnych użytkownikach i grupach użytkowników. Każdą grupę funkcyjną korzystającą z systemów produkcyjnych należy przeanalizować oddzielnie, aby sprawdzić, czy występują nieciągłości w trendach wykorzystania zasobów. Na przykład określony dział może wykazywać stosunkowo powolny i stabilny wzrost liczby cykli procesora zużywanych w miesiącu — dopóki tempo wzrostu nie wzrośnie nagle dziesięciokrotnie. Jeśli taka stopa wzrostu miałaby się utrzymać, mogłaby przewyższyć wszystkie pozostałe wymagania systemowe razem wzięte; w związku z tym operacje zbadałyby sytuację, zanim spowodowałaby problemy. Przyczyną nieciągłości może być błąd programowania; na przykład może istnieć pętla logiczna w jednym z programów lub powtarzające się obliczenia, których wyniki powinny być przechowywane do ponownego wykorzystania. Jednak zmiana nachylenia wykorzystania procesora może być spowodowana wprowadzeniem nowych programów z szybko rosnącą bazą danych; w takich przypadkach operacje musiałyby działać, aby

sprostać nowym, dużym wymaganiom. Miejsce na dysku jest często kluczowym zasobem, który może powodować problemy. Jeśli użytkownicy nie usuną niechcianych plików, miejsce na dysku może zniknąć w zdumiewającym tempie. Problem ten potęgują złe praktyki programistyczne, które pozwalają na stałe utrzymywanie tymczasowych plików roboczych. Systemy zostały zaprojektowane z dziesiątkami tysięcy kolejno ponumerowanych tymczasowych plików roboczych, które po zakończeniu cyklu produkcyjnego nie spełniały żadnej funkcji, ale zostały nagromadzone przez kilka lat. Jedną z szeroko stosowanych metod ograniczania marnotrawstwa zasobów jest obciążenie zwrotne. Korzystając z plików logów systemowych i aplikacji, administracja systemu obciąża użytkowników poszczególnych systemów opłatą w oparciu o wykorzystanie przez nich różnych zasobów. Czasami takie obciążenia zwrotne są postrzegane jako śmieszne pieniądze, ponieważ są fikcją księgową – żadne pieniądze nie zmieniają właściciela. Jednak wymaganie od menedżerów starannego budżetowania zasobów obliczeniowych może naprawdę zwiększyć zainteresowanie przyziemnymi sprawami porządkowymi, takimi jak czyszczenie bezużytecznych plików. Jeśli system opłat zwrotnych obejmuje aspekty wydajności programu, takie jak liczba dysków we/wy, może nawet wpłynąć na programistów, aby odpowiednio zoptymalizowali swój projekt i kod. Optymalizacja jest właściwa, gdy łączne koszty optymalizacji są mniejsze niż oszczędności w zasobach i wzrost wydajności, które wynikają z wysiłków optymalizacyjnych, mierzonych w okresie życia aplikacji.

Monitorowanie jakości wyników

Ostatnim elementem kontroli jakości jest skrupulatne monitorowanie wszystkiego, co jest wytwarzane w centrum danych i wysyłane do użytkowników lub klientów. Chociaż obecnie dużo drukowania jest wykonywane na drukarkach lokalnych kontrolowanych przez użytkowników, w wielu sytuacjach grupa operacyjna jest odpowiedzialna za dokumenty, takie jak czeki płacowe, faktury i raporty o stanie kont. Każda grupa operacyjna musi wyraźnie przypisać odpowiedzialność za weryfikację jakości takich danych wyjściowych przed opuszczeniem centrum danych. Operatorzy powinni prowadzić staranne dzienniki, które odnotowują różne rodzaje błędów (np. rozdarty papier, nierówne formularze lub słabą jakość druku), aby kierownictwo mogło zidentyfikować obszary wymagające wyraźnej uwagi lub naprawy w celu poprawy jakości.

ZAPEWNIENIE ZAUFANEGO SYSTEMU OPERACYJNEGO

System operacyjny (OS) jest zwykle największym i najważniejszym przykładem oprogramowania dostarczanego zewnętrznie w centrum danych. Ponieważ system operacyjny wpływa na wszystko, co jest wykonywane w środowisku produkcyjnym, ważne jest, aby wiedzieć, że oprogramowanie jest godne zaufania. Do tego efektu, personel operacyjny stosuje procedury, aby zapewnić, że znane dobre oprogramowanie jest zawsze dostępne do ponownej instalacji w systemie. Systemy z takim oprogramowaniem są znane jako godne zaufania platformy komputerowe.

Tworzenie znanego dobrego nośnika rozruchowego

Prostą zasadą leżącą u podstaw znanego dobrego oprogramowania operacyjnego jest nieprzerwany łańcuch kopii systemu operacyjnego, które nigdy nie uruchamiały żadnego innego oprogramowania. Oznacza to, że operacje będą tworzyć nośnik startowy (taśma, kaseta, CD-ROM) natychmiast po zainstalowaniu znanego dobrego oprogramowania. Na przykład, jeśli nośnik rozruchowy V1B0 jest zdefiniowany jako wersja 1 systemu operacyjnego, gdy jest dostarczany przez producenta; jego instalacja wymagałaby określonych ustawień i parametrów dla konkretnej konfiguracji systemu. Natychmiast po zainstalowaniu V1B0, ale przed uruchomieniem jakiegokolwiek innego oprogramowania, operacje utworzyłyby nośnik V1B1 i odłożyły go na bok do późniejszego wykorzystania, gdyby V1B0 musiał zostać wymieniony.

Instalowanie nowej wersji systemu operacyjnego

Kontynuując ten przykład, jak utrzymywać znane dobre oprogramowanie operacyjne, może okazać się konieczne zainstalowanie nowej wersji systemu operacyjnego — powiedzmy wersji 2 na nośniku V2B0. Przed użyciem V2B0 operacje ponownie instalowałyby obecny znany dobry system operacyjny, powiedzmy z V1B1. Dopiero wtedy zostanie zainstalowany V2B0, a nowy nośnik startowy V2B1 zostanie utworzony natychmiast.

Łatanie systemu operacyjnego

Często, gdy konieczne jest zmodyfikowanie niewielkiej części systemu operacyjnego, zamiast instalowania całej nowej wersji, producenci proszą użytkowników o załatanie systemu operacyjnego. Programy poprawek modyfikują skompilowany kod w miejscu. Jeśli sumy kontrolne lub podpisy cyfrowe są używane do utrzymania integralności systemu operacyjnego, kody te będą musiały zostać ponownie wygenerowane po zastosowaniu poprawki. Jednak, aby utrzymać znany dobry stan, nakładanie łaty powinno przebiegać według sztywnej kolejności:

1. Załaduj aktualne znane dobre oprogramowanie z odpowiedniego nośnika (np. V2B1).

2. Zainstaluj poprawkę.

3. Natychmiast utwórz znany dobry nośnik rozruchowy przed uruchomieniem jakiegokolwiek innego oprogramowania (w naszym przykładzie tym nośnikiem będzie V2B2).

OCHRONA DANYCH

Dostęp do programów produkcyjnych i danych kontrolnych

Tak jak centrum operacyjne potrzebuje ograniczonego dostępu, tak też programy i dane produkcyjne. Z funkcjonalnego punktu widzenia istnieją trzy kategorie osób, które mogą mieć dostęp do programów i danych, od których zależy przedsiębiorstwo: użytkownicy, programiści i personel operacyjny.

Użytkownicy

Jedynymi osobami, które powinny mieć dostęp do odczytu i zapisu danych produkcyjnych, są ci użytkownicy przypisani do poszczególnych systemów, którym nadano określone uprawnienia dostępu. Na przykład, zwykle tylko personel działu kadr miałby dostęp do dokumentacji kadrowej; tylko pracownicy działu finansów mieliby pełny dostęp do wszystkich ewidencji rozrachunków z dostawcami i rozrachunkami z odbiorcami. Menedżerowie i inni użytkownicy z kadry kierowniczej mieliby dostęp do określonych podzbiorów danych, takich jak rekordy wydajności lub dane budżetowe. Oczywiście żaden użytkownik nie powinien mieć dostępu do zapisu w programach produkcyjnych.

Personel programujący

Programiści tworzą i utrzymują programy produkcyjne; naturalnie muszą mieć dostęp do wersji tych programów, nad którymi aktualnie pracują. Jednak programiści nie mogą mieć możliwości modyfikowania programów aktualnie używanych w produkcji. Wszystkie zmiany w programach produkcyjnych muszą być udokumentowane, przetestowane i zintegrowane ze środowiskiem produkcyjnym pod nadzorem personelu zapewnienia jakości, operacji i bezpieczeństwa. Programiści muszą być w stanie korzystać z realistycznych danych w swoich funkcjach rozwoju, konserwacji i testowania; jednak programiści nie powinni mieć uprzywilejowanego dostępu do zastrzeżonych danych. Na przykład programiści nie powinni mieć możliwości odczytywania poufnych plików z dokumentacji personelu lub dokumentacji medycznej lub modyfikowania danych produkcyjnych w systemie rozliczeń z dostawcami. Programiści mogą korzystać z wyciągów z produkcyjnych baz danych,

ale niektóre pola mogą wymagać losowania, aby zapobiec naruszeniom poufności. Programistom generalnie nie podobają się takie ograniczenia, ale zwykle skuteczny proces edukacji może przekonać ich, że utrzymywanie barier między systemami produkcyjnymi a rozwijanymi jest mądrą polityką.

Personel operacyjny

Tak jak programiści są odpowiedzialni za rozwój i utrzymanie systemów, tak personel operacyjny jest odpowiedzialny za używanie i kontrolowanie tych systemów. Pracownicy operacyjni wykonują takie zadania, jak planowanie, obsługa błędów, kontrola jakości, tworzenie kopii zapasowych, odzyskiwanie i zarządzanie wersjami. Jednak personel operacyjny nie powinien mieć możliwości modyfikowania programów produkcyjnych ani dostępu do wrażliwych danych w produkcyjnych bazach danych.

Oddzielanie danych produkcyjnych, rozwojowych i testowych

Z oczywistych względów testowanie z danymi produkcyjnymi i programami produkcyjnymi jest niedopuszczalną praktyką, z wyjątkiem sytuacji awaryjnych. Dlatego programiści, którzy tworzą nowe programy lub modyfikują istniejące programy, muszą przeprowadzać testy przy użyciu własnych bibliotek. Są one często nazywane bibliotekami testowymi. Doświadczeni programiści przechowują kopie programów źródłowych, za które są odpowiedzialni, a także kopie niektórych plików danych używanych przez programy i podzbiory innych programów we własnych bibliotekach testowych. Aby uniknąć naruszeń bezpieczeństwa, takie kopie i podzbiory danych uprzywilejowanych powinny być anonimizowane w stopniu niezbędnym do ochrony poufności. Na przykład system wykorzystujący dane osobowe może zastępować losowe liczby i ciągi identyfikatorów, nazwisk i adresów pracowników. Ważne jest, aby dołączyć znaczniki czasu do wszystkich plików i programów, w tym zarówno wersji produkcyjnych, jak i testowych. Ta praktyka służy do rozwiązywania problemów, które pojawiają się w związku z nieprawidłowym działaniem programu. Jeśli wszystkie programy i pliki mają sygnatury czasowe, może to być pomocne w ustaleniu, czy najnowsza wersja programu ładującego znajduje się w bibliotece produkcyjnej oraz czy pliki testowe i produkcyjne zostały zsynchronizowane. Testy końcowe przed wydaniem produkcyjnym mogą wiązać się z bardziej formalnym przeglądem przez niezależną sekcję lub dział zapewniania jakości; grupa ds. zapewnienia jakości może również kontrolować transfery programów do biblioteki produkcyjnej.

Kontrola dostępu użytkowników do plików i baz danych

Dostęp do plików musi być kontrolowany z dwóch powodów:

1. W aktach znajdują się informacje poufne, które nie powinny być udostępniane wszystkim.

2. Istnieją inne pliki, które są uważane za podlegające kontroli.

Informacje zawarte w tych plikach mogą być poufne, ale to nie jest powód kontrolowania dostępu do nich. Informacje zawarte w tych plikach muszą być kontrolowane, ponieważ ich zmiana jest nielegalna. Przykładem może być plik księgi głównej przedsiębiorstwa po zamknięciu ksiąg. Zmiana informacji w tych aktach zrodziła pejoratywne sformułowanie „gotowanie książek". Oryginalne kopie tych plików są tworzone na komputerze obsługującym codzienne transakcje przedsiębiorstwa. Jakiś czas po zamknięciu ksiąg na koniec miesiąca kopie tych akt są archiwizowane. W tej formie są one zapisaną historią przedsiębiorstwa i nie można ich zmienić. Przechowywanie tych wyrytych w kamieniu informacji historycznych, łączenie szczegółów i podsumowań w formacie bazy danych, aby były one dostępne w celu analizy, nazywa się hurtownią danych. W większości dużych przedsiębiorstw pliki te są tworzone na komputerach typu mainframe i średniej wielkości, chociaż obecnie coraz częściej stosuje się mikrokomputerowe serwery baz danych w sieciach LAN. W każdym razie kontrolowanie dostępu użytkownika do plików odbywa się na kilka sposobów, w zależności od tego, jakie typy dostępu

są dozwolone. Zdalny dostęp do produkcyjnych baz danych i plików online często odbywa się za pośrednictwem łączy dzierżawionych — wydzielone urządzenia komunikacyjne opłacane co miesiąc, w przeciwieństwie do łączy telefonicznych lub komutowanych, opłacanych w momencie użycia. Kontrolę dostępu można łatwo osiągnąć dzięki zastosowaniu zewnętrznych modułów oprogramowania zabezpieczającego, które z kolei zasilają bazę danych i oprogramowanie do obsługi plików, a ostatecznie oprogramowanie aplikacyjne. Na przykład w środowisku wykorzystującym oprogramowanie do obsługi zapytań i aktualizacji baz danych i plików online można zainstalować wiele różnych produktów oprogramowania zabezpieczającego. Takie produkty używają tak zwanych reguł lub schematów do sprawdzania poprawności identyfikatorów użytkowników i haseł, do autoryzacji typów transakcji oraz do umożliwienia dostępu do plików i baz danych. Wiele instalacji systemów informatycznych umożliwia zdalną komunikację dla wielu rodzajów transakcji. Różne osoby, w tym przedstawiciele handlowi wprowadzający informacje o zamówieniach i członkowie kadry kierowniczej, którzy chcą uzyskać dostęp do bieżących informacji z baz danych lub plików, korzystają z sieci publicznych, takich jak przewodowi lub bezprzewodowi dostawcy usług internetowych w hotelach, na lotniskach i w kawiarniach. Ten rodzaj dostępu zwiększa ryzyko naruszeń bezpieczeństwa. Powszechną praktyką jest obecnie korzystanie z wirtualnych sieci prywatnych (VPN), które składają się z zaszyfrowanych kanałów między urządzeniami przenośnymi a sieciami korporacyjnymi. Mimo to niektóre nieodpowiednie implementacje sieci VPN umożliwiają transmisję w postaci zwykłego tekstu początkowych informacji logowania, umożliwiając przechwycenie danych identyfikacyjnych i uwierzytelniających oraz wykorzystanie ich do nieautoryzowanego dostępu. Słabo zabezpieczony dostęp do sieci umożliwia również ataki typu man-in-the-middle na ruch użytkownika.

WALIDACJI DANYCH

Tak jak niezbędne jest posiadanie zaufanych systemów operacyjnych i oprogramowania aplikacyjnego do produkcji, grupa operacyjna musi być w stanie wykazać, że dane używane do produkcji są prawidłowe. Kontrole walidacji są zwykle przeprowadzane dynamicznie podczas wprowadzania danych i innych zadań przetwarzania. Niektóre kontrole ważności są przeprowadzane automatycznie przez oprogramowanie bazodanowe; na przykład niespójności między rekordami nagłówka a szczegółami mogą być zgłaszane jako błędy przez podsystemy bazy danych. Złe wskaźniki są zwykle natychmiast oznaczane przez oprogramowanie bazy danych jako błędy; przykłady zawierają:

* Wskaźniki z konkretnego rekordu głównego do rekordu szczegółowego z nieprawidłową wartością klucza lub do nieistniejącej lokalizacji

* Wskaźniki do przodu lub do tyłu z rekordu szczegółowego do rekordów, które mają niewłaściwą wartość klucza dla łańcucha lub które w ogóle nie istnieją

Jednak wiele błędów nie może zostać wyłapanych przez podsystemy bazy danych, ponieważ wiążą się one z określonymi ograniczeniami dotyczącymi aplikacji, a nie z błędami samej bazy danych. Na przykład niewłaściwe może być dopuszczenie do mieszania dwóch substancji chemicznych w kadzi procesowej, jednak w samych danych nie ma niczego, co oprogramowanie bazy danych rozpoznałoby jako uniemożliwiające zarejestrowanie tych dwóch wartości w zmiennych wejściowych. Programiści muszą uwzględnić takie ograniczenia w kontroli edycji; często te relacje między zmiennymi można zakodować w słowniku danych. Jeśli środowisko programistyczne nie pozwala na takie zależności, programiści muszą uwzględnić ograniczenia w tabelach przeglądowych lub w inicjalizacji zmiennych. Z punktu widzenia produkcji personel operacyjny musi uruchomić odpowiednie programy walidacyjne stworzone przez dostawców baz danych i programistów aplikacji, aby zapewnić jakość wszystkich danych produkcyjnych. Kolejne sekcje opisują bardziej szczegółowo co bierze udział w takich programach walidacji.

Kontrole edycji

Operacje powinny mieć dostęp do programów diagnostycznych, które skanują całe bazy danych w poszukiwaniu naruszeń kryteriów edycji. Na przykład, jeśli pole jest określone jako wymagające tylko znaków alfanumerycznych, ale nie znaków specjalnych, takich jak „#" i „@", wówczas częścią procesu diagnostycznego powinno być sprawdzanie każdego wystąpienia pola pod kątem zgodności z tymi regułami. Podobnie sprawdzanie zakresu (większy niż, mniejszy niż, większy lub równy, równy, mniejszy lub równy, pomiędzy) jest normalną częścią takich skanów. Tabele przeglądowe zawierające dozwolone i zabronione dane oraz kombinacje danych zapewniają dalsze wyrafinowanie bardziej złożonych relacji i ograniczeń. W każdym razie rolą personelu operacyjnego jest prowadzenie diagnostyki i identyfikacja błędów; korekta błędów powinna należeć do upoważnionych pracowników, takich jak administratorzy baz danych. Programy diagnostyczne powinny dostarczać szczegółowych informacji o każdym błędzie znajdującym się w plikach produkcyjnych. Takie szczegóły obejmują:

* Konfigurowalny widok rekordu lub rekordów stanowiących błąd, pokazujący niektóre lub wszystkie pola

* Unikalna identyfikacja takich rekordów według nazwy lub numeru pliku, numeru rekordu i opcjonalnie według fizycznej lokalizacji (cylinder, sektor) na dysku

* Kod błędu i opcjonalne pełnotekstowe opisy błędu, w tym dokładnie, które ograniczenia zostały naruszone

W idealnym przypadku program diagnostyczny powinien również umożliwiać naprawę błędu. Taka naprawa może być automatyczna, jak na przykład wstawienie prawidłowej sumy w nagłówku zamówienia, lub ręczna, zapewniając administratorowi bazy danych możliwość poprawienia szczegółowego rekordu, o którym wiadomo, że jest błędny.

Sprawdź cyfry i pliki dziennika

Inna forma weryfikacji opiera się na cyfrach kontrolnych. Programy mogą dodawać liczbowe lub alfanumeryczne wyniki manipulacji danymi do każdego rekordu lub do grup rekordów, gdy transakcje są zakończone prawidłowo. Znalezienie rekordów z niewłaściwymi cyframi kontrolnymi zasygnalizuje niespójności i potencjalne błędy w przetwarzaniu. Cyfry kontrolne są szczególnie przydatne do identyfikowania zmian w produkcyjnych bazach danych i innych plikach, które zostały wprowadzone za pomocą narzędzi, które omijają ograniczenia aplikacji. Na przykład większość baz danych zawiera stosunkowo proste narzędzie do tworzenia zapytań ad hoc, które umożliwia wyszukiwanie, wyszukiwanie szeregowe, widoki i proste raportowanie. Jednak takie narzędzia często zawierają możliwość modyfikowania rekordów zgodnie z ograniczeniami podsystemu bazy danych, ale całkowicie bez ograniczeń aplikacji. Jeszcze potężniejszy rodzaj narzędzia całkowicie omija system plików i działa poprzez wydawanie poleceń bezpośrednio do sterowników niskiego poziomu lub do oprogramowania układowego odpowiedzialnego za pamięć i dysk we/wy. W rękach niewłaściwych osób zarówno narzędzia bazodanowe, jak i systemowe mogą uszkodzić integralność danych. Jednak zwykle użytkownikom tych narzędzi trudno jest obliczyć prawidłowe sumy kontrolne, aby ukryć dowody ich modyfikacji. Procedura diagnostyczna, która ponownie oblicza sumy kontrolne i porównuje nowe wartości z wartościami przechowywanymi, może natychmiast wykryć takie nieautoryzowane manipulacje danymi. Jeśli to możliwe, sumy kontrolne w plikach dziennika powinny być łączone z jednego rekordu do drugiego, tak aby suma kontrolna dla każdego rekordu była obliczana przy użyciu sumy kontrolnej z poprzedniego rekordu oprócz danych w bieżącym rekordzie. Zmiana, dodanie lub usunięcie dowolnego wpisu w pliku dziennika wymaga od przestępcy zmodyfikowania wszystkich kolejnych sum kontrolnych, a porównanie zmodyfikowanego pliku dziennika z kopią

zapasową oryginalnego pliku dziennika może łatwo zidentyfikować manipulację, ponieważ istnieje tak wiele dowodów na to. Podobna technika sprawdzania poprawności i naprawiania danych wykorzystuje pliki dziennika bazy danych i aplikacji do rejestrowania informacji, takich jak obrazy przed i po zmodyfikowanych rekordach. Takie pliki dziennika mogą również zawierać specjalne rekordy znaczników do oznaczania różnych kroków w złożonych transakcjach; flagi te mogą umożliwić programom diagnostycznym dokładne określenie, kiedy transakcje zostały przerwane lub poddane innym formom niepowodzeń. Korzystając z tych plików dziennika, często można określić, które wadliwe transakcje należy usunąć, powtórzyć lub zakończyć. Komercyjne oprogramowanie integrujące dane jest dostępne dla szerokiej gamy platform i baz danych. Wyszukiwanie hasła „oprogramowanie integralności danych" w wyszukiwarce Google (www.google.com) pozwala znaleźć wiele odniesień do takich produktów.

Obsługa danych zewnętrznych

Przed użyciem danych dostarczonych przez organizacje zewnętrzne operacje powinny rutynowo sprawdzać czystość danych. Procedury diagnostyczne z grupy programistów powinny być dostępne do sprawdzenia wszystkich danych przed ich użyciem w przetwarzaniu wsadowym w celu aktualizacji produkcyjnej bazy danych. Te same zasady walidacji danych stosowane podczas sprawdzania produkcyjnych baz danych powinny mieć zastosowanie do wszystkich danych otrzymanych od klientów, dostawców, rządów i wszelkich innych organizacji. Można i należy napisać lub uzyskać specjalne programy walidacyjne w celu testowania danych otrzymanych na dowolnym nośniku, w tym taśmach, kasetach, dyskach wymiennych, dyskach CD-ROM, DVD i kanałach transmisji danych.

SYSTEMY OBLICZANIA I PRODUKCJI W CHMURZE

Historia komputerów produkcyjnych się powtarza: od lat 60. do 80. komputery były fizycznie tak duże i bardzo drogie, że wiele mniejszych organizacji zawierało umowy z biurami usługowymi, aby uzyskać dostęp do zasobów obliczeniowych. Połączenia fizycznie bliskie lokalizacje (np. rdzenie miejskie) często odbywały się za pomocą fizycznego kabla koncentrycznego lub skrętki. W przypadku bardziej odległych połączeń klienci podłączali swoje nieme terminale do komputerów typu mainframe za pomocą linii telefonicznych za pomocą modemów. Czasami komutowane połączenia telefoniczne przez zwykłą starą usługę telefoniczną (POTS) były ustalane na miejscu i dedykowane do połączenia – stąd nazywano je liniami dedykowanymi. Dziś, gdy zbliżamy się do połowy lat 2010, prędkość połączeń internetowych sięga 10 Gb/s – ogromnej przepustowości, która umożliwia zdalny dostęp do banków o mocy obliczeniowej o niemal niewyobrażalnej mocy.4 Organizacje wykorzystują możliwość tworzenia maszyn wirtualnych (wirtualizacji), które izolują od siebie współbieżne procesy, umożliwiając znacznie wydajniejsze współdzielenie scentralizowanych zasobów niż uruchamianie procesów na dedykowanych systemach we własnym zakresie. Niedrogie komputery (cienkie klienty) ze stosunkowo niewielką ilością oprogramowania aplikacyjnego i lokalną pamięcią dyskową mogą być używane do uzyskiwania dostępu do wszystkich niezbędnych programów i danych wymaganych dla działalności organizacji poprzez dostęp do usług w chmurze. W marcu 2013 r. analitycy branżowi powiedzieli: „W 2013 r. ponad 60% wszystkich przedsiębiorstw przyjęło jakąś formę przetwarzania w chmurze, według Gartner Research. Rynek chmury ma w tym roku wzrosnąć do 131 miliardów dolarów na całym świecie, czyli 18,5% w porównaniu z 11 miliardami dolarów w zeszłym roku. W raporcie State of the Cloud z 2013 r., w którym ankietowano ponad 1200 specjalistów IT, firma CDW-odsprzedawca IT stwierdziła, że 39% organizacji korzysta już z jakiejś formy rozwiązania w chmurze, co stanowi 11% wzrost w porównaniu z 2011 r." IDC poinformowało, że „W nadchodzących latach wpływ chmury obliczeniowej na gospodarkę będzie ogromny. Każdego roku coraz większy procent budżetów IT firm przeznaczany jest na chmurę. Obszerne badanie przeprowadzone przez International Data Corporation (IDC) … wykazało, że w 2011 roku firmy wydały 28 miliardów dolarów na usługi IT w chmurze publicznej. O

dziwo, oczekuje się, że wydatki na chmurę publiczną przekroczą 207 miliardów dolarów na całym świecie do 2016 roku…" Badacze przeanalizowali trendy w poszczególnych branżach:

* Bankowość: rosnące wykorzystanie chmury obliczeniowej

* Opieka zdrowotna: wolniejsza adopcja

* Produkcja: szczególnie silny wzrost w zakresie zarządzania relacjami z klientami (CRM) i wśród mniejszych firm

* Ubezpieczenie: rosnące wykorzystanie

* Komunikacja/media: szczególnie silny użytkownik przechowywania na żądanie

Gartner przewidział również, że „… do 2015 r. 10% ogólnych funkcji bezpieczeństwa IT w przedsiębiorstwach będzie dostarczanych w chmurze, z wyraźnym naciskiem na przesyłanie wiadomości, bezpieczeństwo internetowe i zdalną ocenę podatności na zagrożenia. Istnieje jednak również oczekiwanie, że w drodze pojawi się więcej, takich jak zapobieganie utracie danych, szyfrowanie, uwierzytelnianie, które są również dostępne jako technologie mające na celu wspieranie rozwoju przetwarzania w chmurze". Podobnie jak w przypadku biur serwisowych w przeszłości, przetwarzanie w chmurze stawia szczególne wyzwania w zakresie bezpieczeństwa operacji i kontroli produkcji.

* Wiarygodność pracowników zatrudnionych do obsługi poufnych i krytycznie ważnych danych jest poza zasięgiem organizacji klienta.

* Zasady zarządzania, monitorowanie, konserwacja oprogramowania, audyty — wszystko to potencjalnie może być obsługiwane wyłącznie przez pracowników dostawcy usług przetwarzania w chmurze.

* Praktyki Bring-your-own-device (BYOD) są ułatwione dzięki dostępowi do zdalnych usług w chmurze.

* Kwestie jakości usług (QOS) i szczegóły umów dotyczących poziomu usług (SLA) komplikują stosunki umowne między dostawcami a klientami.

Przetwarzanie w chmurze, podobnie jak biura obsługi, może zapewnić opłacalne ścieżki rozwoju dla mniejszych firm i może odciążyć technologię informacyjną wykorzystywaną do funkcji IT, które nie są postrzegane jako krytyczne, umożliwiając personelowi IT skoncentrowanie się na innowacyjnych, wysoce wydajnych aplikacjach, które mogą wyróżnić organizację na swoim rynku. Pozwalają na stopniowy wzrost mocy obliczeniowej bez zmuszania organizacji do podążania za funkcjami krokowymi przy dużych inwestycjach w znacznie większy sprzęt i zwiększonych kosztach operacyjnych. Jednak rozbudowa infrastruktury IT do centrów prowadzonych przez odrębne podmioty, kierujące się własnymi motywacjami zarobkowymi, wymaga starannej dbałości o bezpieczeństwo. Organizacje powinny co najmniej wdrożyć następujące zalecenia dotyczące utrzymania odpowiedniej kontroli nad swoim środowiskiem produkcyjnym, gdy znajduje się ono w lokalizacji zdalnej korzystającej z chmury obliczeniowej:

1. Podczas oceny wielu dostawców należy skontaktować się z klientami każdej firmy w celu osobistego omówienia ich doświadczeń z umowami o gwarantowanym poziomie usług i wydajności, otwartości komunikacji na temat kontroli produkcji, współpracy przy wizytach na miejscu oraz adekwatności i współpracy w rozwiązywaniu problemów.

2. Sprawdź poprawność szyfrowania wszystkich przechowywanych danych zastrzeżonych. Żadne dane w postaci zwykłego tekstu nie powinny być dostępne dla pracowników firmy hostingowej w chmurze

w dowolnym momencie — także podczas odszyfrowywania na maszynach wirtualnych działających na ich serwerach.

3. Upewnij się, że dla wszystkich internetowych transferów danych istnieją wirtualne sieci prywatne.

4. Jawnie przedyskutuj standardy aktualizacji dla całego oprogramowania, które Twoja organizacja planuje uruchomić w usłudze w chmurze. Czy jesteś odpowiedzialny za takie aktualizacje, czy jest to dostawca chmury?

5. Upewnij się, że całe oprogramowanie działające w chmurze w imieniu organizacji klienta przestrzega warunków licencji dostawców. Na przykład upewnij się, że licencja dla jednego użytkownika nie jest stosowana w Twoim imieniu do tysiąca jednoczesnych maszyn wirtualnych.

6. Zrozum i przeanalizuj obowiązujące planowanie ciągłości biznesowej (BCP) i planowanie odzyskiwania po awarii (DRP), aby zapewnić ciągłość działania w Twoim imieniu w przypadku wystąpienia problemów w lokalizacji dostawcy chmury. Czy w umowach podano dokładne warunki, które są dla Ciebie zadowalające? Czy istnieją przepisy dotyczące testowania adekwatności BCP i DRP?

7. Upewnij się, że umowa pozwala na audyty zewnętrzne, które może zainicjować klient. Niezależna ocena bezpieczeństwa, QOS i ciągłości działania (CoO) jest niezbędna dla ochrony klienta.

8. Omów zasady i praktyki bezpieczeństwa dostawców, w tym monitorowanie w czasie rzeczywistym pod kątem naruszeń (świadomość sytuacyjna), postępowanie ze złośliwym oprogramowaniem i analizę podatności, w tym testy penetracyjne.

9. Uważnie oceń procesy bilingowe: co determinuje okresowe wystawianie faktur – jednoczesnych użytkowników? Całkowita liczba sesji? Szczegółowe algorytmy mierzące takie elementy, jak dyskowe I/O, cykle procesora, zamiana do iz pamięci wirtualnej czy wykorzystanie przepustowości? Modeluj koszty, jeśli to możliwe, korzystając ze szczegółowych informacji z własnych istniejących systemów.

UWAGI KOŃCOWE

Do połowy lat 80. świat komputerów typu mainframe i minikomputerów różnił się od świata komputerów PC. Jednak od połowy lat 80. do tysiąclecia te światy połączyły się. Rozprzestrzeniły się sieci LAN, Internet zmienił sposób prowadzenia działalności, a mosty, routery i bramy umożliwiają przepływ informacji między platformami komputerowymi, niezależnie od ich typu. Wymagania bezpieczeństwa mają teraz uniwersalny zakres. Liczne warstwy oprogramowania i sprzętu oddzielają użytkownika i technika od informacji, do których potrzebują dostępu. Te warstwy same w sobie przyczyniają się do bezpieczeństwa, ponieważ wymagają pewnych umiejętności technicznych, aby uzyskać dostęp do informacji. Jak pisze się w 2008 r., umiejętność obsługi komputera szybko rośnie. Dzieci uczą się korzystać z komputerów w szkole podstawowej, a dziesiątki milionów pracowników codziennie korzysta z komputerów lub stacji roboczych, więc bezpieczeństwo zapewniane przez tę technologię nie jest tak znaczące, jak kiedyś. Bezpieczeństwo to także kwestia ekonomiczna. Jeśli osoba z wymaganymi umiejętnościami chce uzyskać dostęp do plików lub baz danych online, uniemożliwienie takiego dostępu jest niezwykle kosztowne. Nawet przy wysokich nakładach, sukces w osiągnięciu pełnego bezpieczeństwa nigdy nie jest gwarantowany. Niemniej jednak, jeśli wartość informacji i ich poufność uzasadniają dodatkowe wydatki, dostępne są produkty programowe, które wykorzystują złożone schematy wspierające bezpieczeństwo. W razie potrzeby bezpieczeństwo informacji można rozszerzyć do poziomu terenowego w ewidencji plików i baz danych online. Inne powiązane środki bezpieczeństwa, takie jak ochrona fizyczna, bezpieczeństwo komunikacji, szyfrowanie danych, techniki audytu, kontrola aplikacji systemowych i inne tematy, zostały omówione w innych rozdziałach niniejszego Podręcznika. Żadna miara nie może stać sama