Data Governance

zarządzanie informacią w przedsiębiorstwie

Information Governance:

Information Governance: na straży informacji

Świat w ostatnich 10 latach przeszedł ogromne przeobrażenia. Czasami trudno je dostrzec, bo zmiany odbywają się ewolucyjnie. Komputery, Internet i informacja stanowią obecnie znacznie większą część naszego życia niż jeszcze kilka lat wcześniej. Przedsiębiorstwa, które dotychczas chroniły swoją informację, pilnując dostępu do kluczowych dokumentów, muszą sprostać znacznie większym, nieznanym wcześniej wyzwaniom.

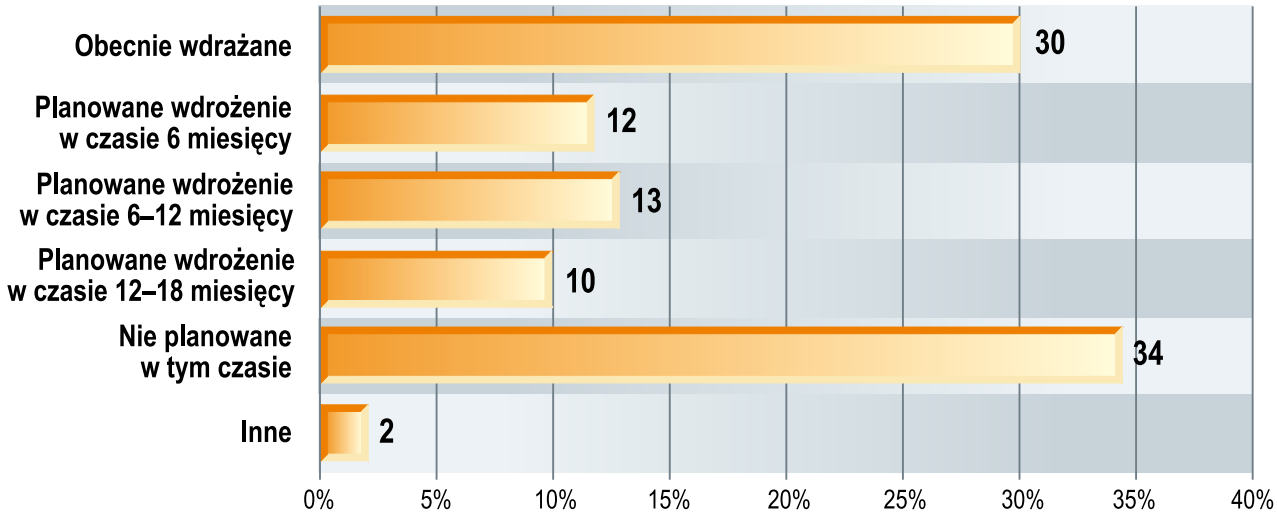
W świecie współczesnym cierpimy na nadmiar informacji, przez co bardzo trudno odróżnić informację prawdziwą od nieprawdziwej lub zmanipulowanej. Plotka – informacja nieprawdziwa, która jeszcze w ubiegłym stuleciu, zanim przekraczała granice państw, mogła być łatwo zdementowana, a przedsiębiorstwa miały dość dużo czasu by zapobiec degradacji wizerunku firmy, stanowi teraz znacznie większe zagrożenie.

W zakresie pełnego zastosowania metod i środków, które wdrożone są w standardach ochrony danych (Data Governance), IBM posiada całą gamę odpowiednich narzędzi. Nie zastąpią one standardów i praktyk biznesu, ale znacznie ułatwią ich implementację.

Nowe wyzwania w obszarze bezpieczeństwa danych

Obecnie informacja może rozprzestrzeniać się z prędkością fali elektromagnetycznej i być łatwo powielana i dystrybuowana przez portale społecznościowe i fora, które znajdują się poza wszelką kontrolą i cenzurą władz, nie mówiąc już o nadzorze ich ze strony przedsiębiorstw czy innych organizacji. Znamienny jest przypadek WikiLeaks, szeroko dyskutowany w mediach całego świata. Przez wiele miesięcy na stronach portalu tworzonego przez grupę niezależnych od nadzoru państw aktywistów pojawiały się miliony stron tajnych dokumentów, które trafiały tam za pośrednictwem anonimowych informatorów. Wystarczy wspomnieć, że od czasu gdy strona rozpoczęła swoją działalność w grudniu 2006 w niecały rok, do listopada 2007 opublikowano na niej już 1,2 mln dokumentów. Jednak strona WikiLeaks znana jest szerokiemu gronu internautów i postronnych słuchaczy mediów dopiero od jesieni 2010 r. To właśnie w listopadzie tamtego roku WikiLeaks opublikowało ponad 250 tys. depesz dyplomatycznych z amerykańskich ambasad na całym świecie. Wprawdzie tuż po publikacji strona WikiLeaks została zablokowana za pomocą rozproszonego ataku typu DoS (Denial of Service), jednak dokumenty skopiowano i opublikowano na setkach lustrzanych serwerów. W konsekwencji zablokowanie dystrybucji treści nie było już możliwe. Serwis, pomimo restrykcji ze strony serwisu transakcyjnego PayPal i szykanów ze strony władz różnych państw, działa bez przeszkód do dziś i m.in. 24 kwietnia 2011 ujawnił kolejne dokumenty, tym razem dotyczące więźniów z Guantanamo. Opublikowane informacje zawierały m.in. ocenę wywiadu na temat 779 ludzi, którzy od 2002 r. trafili do więzienia w tej amerykańskiej bazie. Przypadek WikiLeaks jest znamienny, bo pokazuje jak bardzo ważna jest ochrona informacji i zabezpieczenia przed ich wyciekiem. Nie można również stwierdzić z całą pewnością, jaka część informacji podawanych przez WikiLeaks jest prawdziwa, a jaka została specjalnie spreparowana przez służby lub organizacje i opublikowana na zasadzie „wycieku", by w ten sposób je uwiarygodnić. Przedsiębiorstwa stają zatem przed nowymi wyzwaniami dotyczącymi zarządzania informacją, które muszą być w szczególny sposób kontrolowane. Organizacja musi mieć też koncepcję radzenia sobie

Plany dotyczące wdrożenia strategii i narzędzi Data Governance



Źródło: 2010 IBM Information Governance Survey.

z sytuacjami kryzysowymi, związanymi zarówno z publikacją prawdziwych,
jak i nieprawdziwych lub zmanipulowanych informacji na swój temat.
Sytuacja, w której znalazły się przedsiębiorstwa, jest już codziennością, do której trzeba się dostosować. Nie ma od niej powrotu do tego, co było jeszcze kilka, kilkanaście lat temu. Szacuje się, że z Internetu korzysta obecnie 1,5 mld ludzi, a liczby te z każdym rokiem rosną. Szybki dostęp do Internetu możliwy jest już nie tylko w najbardziej uprzemysłowionych państwach, takich jak Stany Zjednoczone, Japonia czy państwa Unii Europejskiej, ale także w Kambodży czy Zimbabwe.

Strategia Data Governance

W celu wdrożenia zarządzania informacjami, organizacje potrzebują strategii Data Governance. Realizacja powinna skupiać się na dziedzinach, które pomagają w osiągnięciu celów biznesowych o najwyższym priorytecie. Podobnie jak w przypadku przedsiębiorstw miarą sukcesu strategii jest osiągnięcie celów – kluczowych wskaźników wydajności i ochrony danych. Działania te związane są z zapewnieniem dostępu do szczegółowych danych i uzyskaniem pełnej kontroli danych, do tego w jaki sposób trafiają do systemów i kto z tych systemów potem korzysta. Na przykład, nie można dopuścić do sytuacji, w której w firmie ubezpieczeniowej dane dotyczące rozliczeń z klientami wydostały się poza kontrolę pracowników działu rozliczeń. Standardy branżowe dla firm ubezpieczeniowych opisane są w systemie Solvency II. Po wykonaniu wielu analiz ryzyka działalności ubezpieczeniowej, analiz bankructw, analiz istniejących modeli wypłacalności wdrożonych w innych krajach przygotowano nowy system badania wypłacalności. Został on przedstawiony w 2001 r. przez Komisję Europejską w ramach Komitetu Europejskiego. Zawiera kluczowe dla wiarygodności firmy ubezpieczeniowej

Data Governance dla klienta: od braku kompleksowego rozwiązania zagadnień związanych z ochroną danych.

Nie zarządzany	Etap 1	Etap 2	System ochrony danych w pełni zarządzany
• Słaba jakość, konflikty • Niezintegrowany wgląd w dane klienta • Nieodseparowane dane dla tego samego klienta w różnych systemach • Utrzymywanie danych wielu klientów przez różne systemy • Brak wspólnej strategii synchronizacji • Brak ochrony danych dla MDM • Brak kontroli nad tym, kto może zmieniać istotne dane	• Wirtualny, zintegrowany wgląd w dane klienta (Global IDs) zapisywane w systemie - System of rekord (SOR). • Wspólne nazwy danych dla danych klienta w podglądzie wirtualnym. • Federacja danych i narzędzia do weryfikacji jakości danych. • Wsadowe sprawdzanie jakości danych w niektórych systemach operacyjnych. • Utrzymywanie danych klienta w wielu systemach operacyjnych. • Synchronizacja niektórych danych z użyciem SOR, web services lub SQL.	• W pełni zintegrowany zbiór danych klienta w hurtowni danych. • System MDM klienta jest systemem rekordów (SOR), ale nie systemem centralnie zarządzanym. • Zmiana przechwytywania danych ze wszystkich systemów przechowujących dane operacyjne. • Wszystkie dane klienta są zdefiniowane w słowniku biznesowym. • Weryfikacja i czyszczenie danych w procesie wsadowym i na żądanie. • Wspólne usługi dostępu do danych, integracja, federacja i synchronizacja danych klienta.	• W pełni zintegrowany zestaw danych klienta w centralnym repozytorium danych. • System MDM jest jednocześnie systemem wprowadzania danych (DES) i systemem przechowywania danych (SOR). • Wszystkie zatwierdzone zmiany danych są przenoszone do wszystkich systemów BI. • Wszystkie dane zdefiniowane są w słownikach biznesowych. • Dane chronione przez firewall i usługi ochrony danych. • Pełne użycie mechanizmów ochrony danych. • Wspólne mechanizmy dostępu do danych, federacji i synchronizacji. • Wspólne mechanizmy przetwarzania danych. • Ochrona prywatności danych i dostępu do danych.

wskaźniki, które w przypadku ich wycieku mogą zagrozić stabilności całej instytucji.

Efekty zarządzania bezpieczeństwem danych

W celu pomiaru skuteczności strategii ważne jest, aby efekty były mierzalne. Informacje zawarte w klasycznej karcie wyników (KPI) zarządzania w dużym stopniu odzwierciedlają realizację założonych celów. Ważnym elementem w strategii zarządzania informacjami jest ocena kierunku przepływu informacji – w jaki sposób przepływają one w organizacji.

W tworzeniu właściwej strategii ochrony danych ważne jest zadbanie o odpowiednią strukturę organizacyjną. Wprawdzie za ochronę informacji ostatecznie i tak odpowiedzialne jest kierownictwo, jednak zwykle zadania te delegowane są pracownikom przez CEO i CRO (Chief Risk Officer).

Zazwyczaj zarządzanie bezpieczeństwem informacji powierza się specjalnie powołanemu do tego ciału, którego celem jest „trzymanie kluczy" do najważniejszych informacji w przedsiębiorstwie i przydzielanie ich tylko właściwym osobom. Z punktu widzenia IT wiele działów i osób może być zaangażowanych w procesy związane z ochroną danych. Należą do nich:

- architekci systemowi
- analitycy odpowiedzialni za modelowanie danych
- programiści w zakresie jakości danych
- specjaliści od zarządzania treścią

Rolą IT jest nie tylko zapewnienie odpowiednich narzędzi, dzięki którym ochrona danych będzie możliwa, ale także wdrożenie standardów oraz polityki bezpiecznej wymiany danych i obiegu informacji. W kontekście wrażliwych danych, które podlegają ochronie, warto wymienić następujące cechy:

- definicja danych
- opis danych
- ograniczenia (polityka)
- synonimy
- terminy powiązane
- języki określające dane
- klasyfikacja wrażliwości danych, np. niskiej, średniej, wysokiej
- przypisana osoba odpowiedzialna za ochronę danych (tzw. steward)
- polityka jakości danych
- polityka prywatności
- polityka bezpieczeństwa
- polityka cyklu życia danych
- historia obejmująca zmianę nazw, definicji, ograniczeń, wersjonowanie
- występowanie danych (tabele, raporty)

Narzędzia

W zakresie pełnego zastosowania metod i środków, które wdrożone są w standardach ochrony danych (Data Governance), IBM posiada całą gamę odpowiednich

Tomasz Kotowski
Senior Software Sales Representative
Tomasz.kotowski@pl.ibm.com

Więcej informacji o rozwiązaniu:

Link

Narzędzie		Podstawowe funkcje
IBM InfoSphere Fundation Tools	Link	Definiowanie, modelowanie i generowanie usług do ochrony informacji - kluczowy komponent IBM InfoSphere Information Server.
IBM InfoSphere Business Glossary	Link	Definiowanie, zarządzanie i kontrola nazw i definicji danych, które mają być zarządzane.
IBM InfoSphere Data Architect	Link	Modelowanie danych.
IBM InfoSphere Discovery	Link	Wykrywanie danych we wszystkich źródłach danych.
IBM InfoSphere Information Analyzer	Link	Profilowanie jakości danych.
IBM InfoSphere FastTrack	Link	Projektowanie obiegu informacji, mapowanie i tworzenie usług integracji i oczyszczania danych.
IBM InfoSphere Metadata Workbench	Link	Monitorowanie przepływu danych.
IBM InfoSphere Information Server	Link	Integracja danych w heterogenicznych środowiskach.
IBM InfoSphere Blueprint Director	Link	Wykorzystywanie do tworzenia wzorców dla hurtowni danych.
IBM InfoSphere Quality Stage	Link	Czyszczenie danych i łączenie.
IBM InfoSphere DataStage	Link	Integracja i konsolidacja danych.
IBM InfoSphere Federation Server	Link	Federacja (łączenie) danych na żądanie.
IBM InfoSphere Services Director	Link	Publikacja danych do zarządzania.
IBM InfoSphere Guardium	Link	Monitoring baz danych w czasie rzeczywistym.
IBM InfoSphere Optim Data Privacy Solution	Link	Maskowanie danych w celu zachowania prywatności w środkowiskach nieprodukcyjnych.
IBM InfoSphere Optim Test Data Management Solution	Link	Zabezpieczenie środowisk testowych.
IBM InfoSphere Optim Data Growth Solution	Link	Inteligentna archiwizacja baz danych.
IBM InfoSphere Guardium Data Redaction	Link	Usuwanie danych wrażliwych z niezabezpieczonych obszarów.
IBM InfoSphere Tivoli Access Manager	Link	Zarządzanie bezpieczeństwem cyklu życia danych.

IBM Optim

Aplikacje biznesowe i bazy danych są nie tylko pomocą w prowadzeniu biznesu, ale wręcz stają się jego integralną częścią. Struktury aplikacji i danych stają się większe i bardziej złożone, co utrudnia zarządzanie nimi. Powoduje to również coraz większe koszty utrzymania oraz dodatkowe zagrożenia związane z koniecznością zapewnienia bezpieczeństwa przechowywanych danych i ich poufności. Rozwiązaniem tych problemów jest IBM Optim, który daje możliwość zarządzania danymi aplikacji przedsiębiorstw na każdym etapie cyklu ich życia.

IBM Optim poprawia wydajność baz danych, czym zarządza moduł Data Growth Management. Realizacja tego zadania odbywa się poprzez przenoszenie nieaktywnych lub rzadko wykorzystywanych fragmentów danych z zachowaniem powiązań relacyjnych i z możliwością ich odtwarzania oraz zapewnieniem bezpiecznego dostępu. Usprawnienie procesów osiągane jest dzięki modułowi Test Data Management, który odpowiada za tworzenie podzbiorów danych zapewniających lepszą wydajność, szybsze i tańsze niż powielone całe bazy danych (klony). Narzędzie zapewnia także łatwe odświeżanie, przywracanie i zarządzanie danymi w środowiskach testowych; automatyzację procesu porównywania danych.

O bezpieczny dostęp do danych wrażliwych dba moduł Data Privacy Protection. Umożliwia on zastępowanie danych poufnych danymi fikcyjnymi z propagacją zmian, testowanie i szkolenia z użyciem specjalnie przygotowanych danych poza chronioną infrastrukturą firmy oraz ochronę danych przekazywanych poza środowisko produkcyjne.

Funkcje IBM Optim

IBM Optim kompleksowo zarządza danymi przedsiębiorstwa. Funkcje rozwiązania odnoszą się do następujących obszarów:

Archiwizacja: obejmująca transakcje według wieku i statusu. Segregowanie historycznych informacji z bieżącej działalności i bezpieczne usuwanie ich z archiwum. Utrzymanie bazy produkcyjnej w zadanym rozmiarze, w celu uproszczenia obsługi i odzyskiwania pierwotnej prędkości pomimo przyrostu danych.

Klasyfikacja: stosowanie reguł biznesowych w celu uporządkowania aktywnych i nieaktywnych danych oraz odnośników do danych. Określenie i wdrożenie reguł polityki odnoszących się do tego, gdzie dane będą dostępne, gdzie należy je przechowywać, jak długo trzeba je utrzymać i kto może mieć do nich dostęp.

Ocena: ustalenie, gdzie dane aplikacji przyrastają najszybciej i ocena wpływu danych na tworzenie strategii obejmującej warstwową strukturę danych. Identyfikacja oraz rozwiązywanie potencjalnych problemów zanim wpłyną one negatywnie na wyniki finansowe.

Zarządzanie testowaniem danych: szybkie wdrażanie aplikacji poprzez usprawnienie sposobu tworzenia i administrowania środowiskami testowymi. Budowanie podzbiorów danych i migracja danych do powstałych w sposób realistyczny i w odpowiednim rozmiarze baz danych testowych. Eliminacja kosztów i wysiłku utrzymania wielu klonów bazy danych. Identyfikacja poufnych informacji, w celu ochrony prywatności.

Dostęp: umożliwia decydentom dostęp do właściwych danych, we właściwym czasie. Tworzenie zapytań i przeglądanie aktywnych, nieaktywnych danych oraz odnośników do danych. Wykorzystanie łatwych w użyciu formatek, ekranów i paneli. Generowanie standardowych i niestandardowych raportów. Przywracanie zarchiwizowanych transakcji, jeżeli przetwarzanie danych biznesowych staje się wymogiem.

Składowanie: składowanie danych aplikacji zgodnie z ich zmieniającą się wartością biznesową. Utrzymanie aktywnych transakcji w pamięci masowej o wysokiej dostępności. Zmiana danych raportowych na urządzeniach zabezpieczonych. Odzyskiwanie niewykorzystanych mocy produkcyjnych i maksymalizacja wartości istniejącej infrastruktury pamięci masowej.

Korzyści

Do najważniejszych korzyści wynikających z użycia IBM Optim należy zaliczyć zmniejszenie tempa wzrostu wielkości baz produkcyjnych oraz poprawę wydajności aplikacji biznesowych. Inne korzyści to:

- Uproszczenie i przyspieszenie migracji i aktualizacji, backupu i odzyskiwania ciągłości biznesowej po awarii.
- Przygotowanie danych z baz produkcyjnych do testowania, szkolenia i prac developerskich.
- Zapewnienie bezpieczeństwa dostępu do danych wrażliwych.

W efekcie IBM Optim przyczynia się do obniżenia kosztów posiadania infrastruktury IT.

Marek Raczyński
Advisory IT Specialist
Marek.Raczynski@pl.ibm.com

Więcej informacji o rozwiązaniu:

Link

Baza bezpieczeństwa

Firmowe bazy danych stanowią szczególnie cenne zasoby. IBM Guardium Infosphere to wyspecjalizowana platforma, zapewniająca ochronę informacji przechowywanej w firmowych systemach bazodanowych.

Z badania przeprowadzonego przez firmę ESG wynika, że przechowywana jest w nich bardzo duża liczba poufnych informacji. W bazach danych jest ich zdecydowanie więcej niż w innych typach repozytoriów. Jednocześnie z innych badań wykonanych przez IBM wynika, że ze wszystkich zdarzeń polegających na naruszeniu bezpieczeństwa aż 75% dotyczy baz danych.
Mimo to, nawet największe organizacje na świecie niedostatecznie dbają o bezpieczeństwo w tym obszarze. Dlatego coraz częściej uznaje się, że bazy danych to groźna i stale powiększająca się luka w firmowych systemach zabezpieczeń. Większość systemów zabezpieczeń, takich jak zapory ogniowe i systemy wykrywania włamań, koncentruje się na innych obszarach.
Z przytoczonych wcześniej badań wynika, że w ciągu ostatniej dekady 85% budżetów na zabezpieczenia było przeznaczone na ochronę przed atakami użytkowników zewnętrznych. Tymczasem ze statystyk wynika, że zdecydowana większość ataków pochodzi z wewnątrz organizacji. Przy tym ataki na bazy danych są trudne do wykrycia.

Kompletny zestaw

Ciekawych danych jest więcej. Przykładowo, aż 80% organizacji nie ma planów ochrony bazy danych. Zaledwie 20% firm korzysta z zaawansowanych technik pomiaru bezpieczeństwa. Spośród wszystkich naruszeń wewnętrznych, aż 80% dotyczy użytkowników uprzywilejowanych. Bazy nie mają zainstalowanych aktualnych uaktualnień i poprawek. Administratorzy poświęcają zaledwie 5% swojego czasu pracy na bezpieczeństwo. Można z tego wysnuć wniosek, że bazy danych, w zbyt dużym stopniu są zależne od manualnych procesów.
Dlatego budowa polityki bezpieczeństwa z użyciem technologii ochrony warstwy sieciowej, analizy i korelacji logów, zarządzania tożsamością i DLP (Data Leakage Protection) nie jest kompletna. Aktywna analiza bezpieczeństwa informacji musi uwzględniać implementację rozwiązania analizującego dostęp do danych na poziomie motoru bazodanowego. Rozwiązania klasy DAM (Database Activity Monitoring) zaczynają być wymagane przez różne regulacje, a coraz częściej stają się podstawowym narzędziem kontroli IT i użytkowników uprzywilejowanych.
Wdrożenie odpowiednich narzędzi pozwala na eliminowanie zagrożeń i ograniczanie ryzyka. „Odpowiednich" oznacza w tym wypadku oferujących pakiet składający się z mechanizmów skanowania i wykrywania podatności, testów penetracyjnych, monitorowania użytkowników, logowania, szyfrowania i technologii pozwalających egzekwować obowiązującą politykę bezpieczeństwa. Kompletną platformę integrującą takie narzędzia dostarcza IBM Guardium Infosphere. To najprostsze, a zarazem najbardziej zaawansowane rozwiązanie do ochrony informacji finansowych i produkcyjnych, danych dotyczących klientów i ich kart kredytowych, a także własności intelektualnej przechowywanej w systemach firmowych.
Lista najważniejszych funkcji oferowanych przez IBM Guardium Infosphere obejmuje lokalizowanie i klasyfikowanie wrażliwych informacji w bazach danych, monitorowanie i egzekwowanie polityki dostępu do wrażliwych danych, akcji uprzywilejowanych użytkowników, działań użytkowników aplikacji i zdarzeń, takich jak błędne logowanie, automatyzowanie procesów audytowych, a także ocenę podatności baz danych i niewłaściwych konfiguracji. Platforma wyposażona jest w mechanizmy pozwalające zaimplementować rekomendowaną konfigurację i zabezpieczyć ją przed wprowadzeniem zmian.
IBM Guardium Infosphere dostarcza kompletnego obrazu wszystkich transakcji w bazie danych za pomocą mechanizmu prezentującego działania użytkowników. Jest on zabezpieczony przed możliwością dokonywania zmian.

Dla małych i dużych

Patforma IBM Guardium Infosphere chroni przed nieautoryzowanymi, czy choćby tylko podejrzanymi, działaniami wykonywanymi przez uprzywilejowanych użytkowników i potencjalnych hakerów. Dostarcza także narzędzi do monitorowania potencjalnych nadużyć dokonywanych przez użytkowników końcowych aplikacji, takich jak Oracle E-Business Suite, PeopleSoft, SAP, a także oprogramowania tworzonego wewnątrz organizacji. Równocześnie rozwiązanie optymalizuje operacyjną efektywność przy wykorzystaniu skalowalnej, wielowarstwowej architektury, która automatyzuje i centralizuje zgodność pomiędzy całą infrastrukturą aplikacyjną a bazodanową. Warto też zauważyć, że rozwiązanie IBM nie ma wpływu na wydajność. Nie wymaga dokonywania żadnych zmian w bazie danych, a jego działanie nie zależy od natywnych logów bazy danych czy narzędzi wykorzystywanych do audytu. Co ważne, rozwiązanie IBM jest łatwo skalowane – od jednej bazy danych do tysięcy baz danych rozproszonych po centrach danych na całym świecie.

Więcej informacji o rozwiązaniu:

Link

Menedżer dostępu

Automatyzacja mechanizmów wewnętrznej kontroli nad uprawnieniami użytkowników pozwala osiągnąć równocześnie wysoki poziom bezpieczeństwa i ograniczyć koszty.

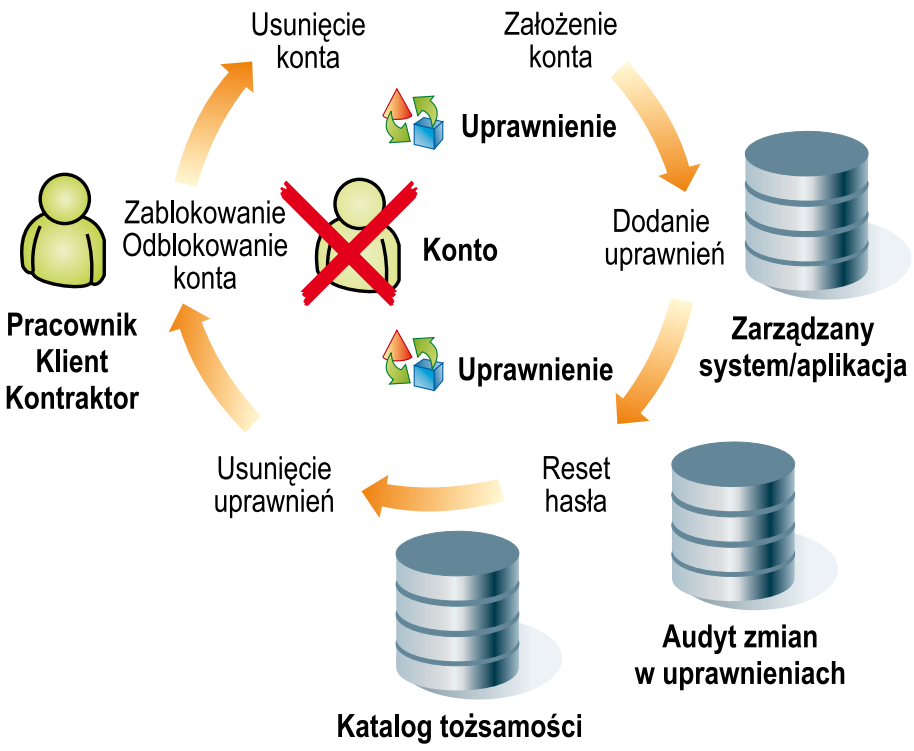
Udostępnianie informacji i systemów informatycznych klientom czy dostawcom za pośrednictwem Internetu stało się standardem w wielu branżach. Pozwala to przyspieszyć realizację procesów biznesowych i ograniczyć koszty związane z obsługą partnerów biznesowych. Zapewnienie dostępu do aplikacji w Internecie ma jednak również drugą, ciemniejszą stronę. Osiągane korzyści wiążą się bowiem z większymi wyzwaniami w zakresie bezpieczeństwa. Wyjątkowego znaczenia nabiera zagadnienie bezpiecznego zarządzania uprawnieniami przydzielanymi użytkownikom oraz udostępniania cennych danych.
Zadanie utrudniają zwykle wewnętrzne regulacje związane z bezpieczeństwem organizacji, a także akty prawne zobowiązujące do stosowania pewnych procedur czy rozwiązań. Nie jest łatwo zapewnić bezpieczeństwo, a przy tym sprostać wszystkim wymaganiom ekonomicznym. Obecnie każda inwestycja informatyczna musi być uzasadniona i zwrócić się w określonym czasie.

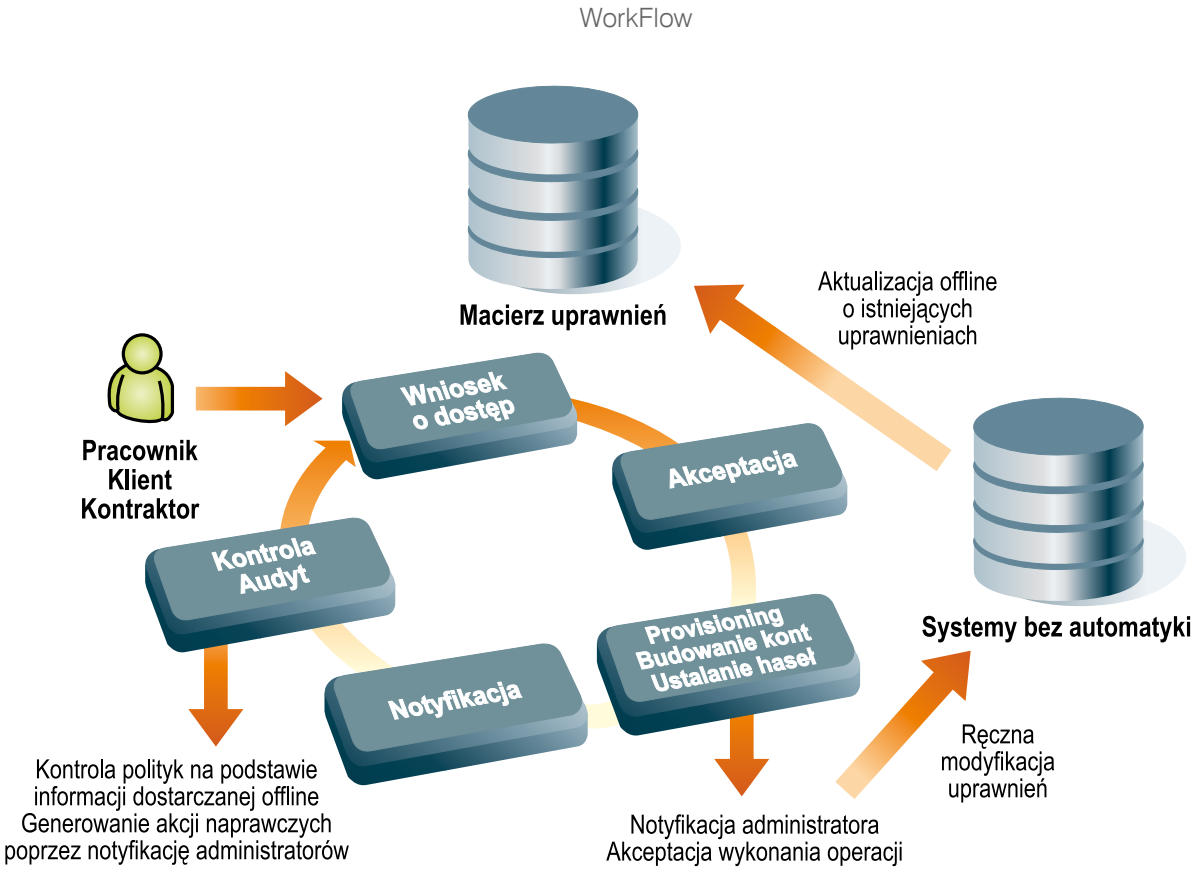
IBM Tivoli Identity Manager ułatwia sprostanie wyzwaniom. Pozwala na zarządzanie uprawnieniami użytkowników w heterogenicznych środowiskach informatycznych. System ułatwia automatyzowanie zadań związanych z zarządzaniem tożsamością i kontrolowanie praw dostępu dla ogromnej liczby użytkowników online. Jednocześnie zapewnia odpowiedni poziom bezpie-
czeństwa i dostarcza komplet informacji o aktywności użytkowników.

Kompletne rozwiązanie

IBM Tivoli Identity Manager to bezpieczne i zautomatyzowane rozwiązanie, działające na podstawie wypracowanej przez firmę strategii. Wzmacnia system zarządzania dostępem użytkowników. Wbudowane funkcje pozwalają na kompleksowe podejście do kwestii przyznawania dostępu zewnętrznym użytkownikom. Przykładowo
umożliwiają łatwe wnioskowanie o dostęp do ról i kont lub o uzyskanie precyzyjnie określonych uprawnień dostępu, np. do współużytkowanych folderów czy aplikacji internetowych. System oferuje sprawny interfejs samoobsługowy dla użytkowników. W prosty sposób można go dostosować do firmowych standardów, a także zintegrować z portalami
korporacyjnymi. Zawiera również udoskonalone mechanizmy powtórnej weryfikacji praw dostępu, które udostępniają szczegółowe informacje dotyczące strategii oraz
ich przestrzegania. Mecha-nizmy te można łatwo konfigurować. System dostarcza bogatego zestawu kreatorów i szablonów. Jedną z nowości jest przeznaczony dla audytorów tryb „tylko do odczytu". Ponadto pojawiła się zaprojektowana od nowa konsola zarządzania, dodatkowe raporty dotyczące zgodności ze strategiami oraz

Automatyzacja nadawania uprawnień





kreator niestandardowych raportów. Możliwe stało się zintegrowanie systemu z programem Tivoli Compliance Insight Manager, co pozwala na uzyskanie raportów kontrolnych z odniesieniami do przepisów i sprawdzonych procedur.

Ważne jest także, że oprogramowanie można szybko wdrożyć i nie wymaga ono długotrwałych szkoleń. Użytkownicy od początku dysponują zestawem gotowych, sprawdzonych procedur, które można wykorzystać od chwili rozpoczęcia pracy.

IBM Tivoli Identity Manager to bezpieczne i zautomatyzowane rozwiązanie, działające na podstawie wypracowanej przez firmę strategii. Wzmacnia system zarządzania dostępem użytkowników.

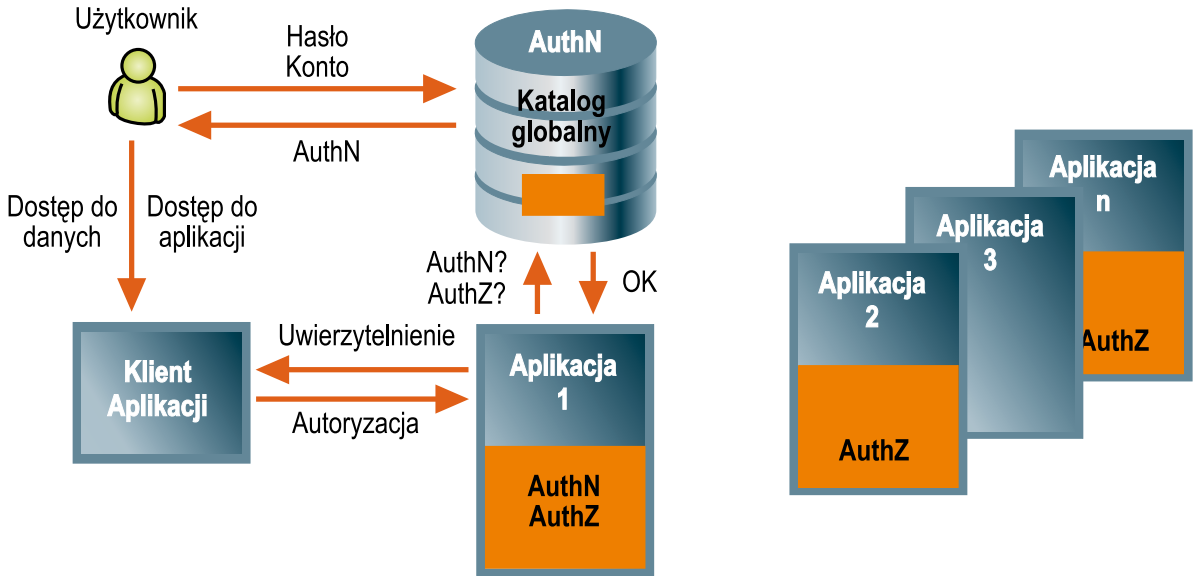
Efekty na wielu poziomach

Dyskusję o korzyściach warto zacząć od tego, że IBM Tivoli Identity Manager zapewnia szybki zwrot z inwestycji. Oprogramowanie nie tylko nadzoruje i egzekwuje udostępnianie użytkownikom odpowiednich zasobów, ale przy tym ma również wpływ na ograniczenie kosztów. Przede wszystkim decydują o tym niższe koszty administracji. Specjaliści nie muszą już poświęcać tak dużo czasu na zarządzanie tożsamością użytkowników. Wiele złożonych czynności, dzięki zaawansowanym funkcjom, staje się znacznie prostszych i można wykonać je szybciej. Redukcji ulega też liczba zadań wykonywanych ręcznie.

Zmniejszają się również koszty związane z help deskiem. Użytkownicy nie zgłaszają się tak często z problemami. O wiele rzadziej pojawiają się prośby o reset hasła. Funkcje samoobsługowe pozwalają na samodzielne wykonanie podstawowych czynności. Intuicyjny interfejs znacząco poprawia komfort użytkowników.

System wymusza eliminowanie nieużywanych kont i zwraca uwagę na użytkowników, którym mogły zostać przydzielone zbyt duże uprawnienia. Wsparcie formalnych procesów walidacji dostępu pozwala ograniczyć ryzyko związane z przyznawaniem dostępu do systemów i danych. Ewentualne problemy są błyskawicznie wykrywane. Implementowanie i modyfikowanie zasad przydzielania dostępu jest wyjątkowo proste. Przy tym gwarantuje dużą precyzję. Natomiast moduł odpowiedzialny za raportowanie dostarcza komplet informacji nie tylko na potrzeby wewnętrzne, ale także do wykorzystania na potrzeby sprawozdań wynikających z regulacji prawnych.

System pojedynczego logowania SSO



Różne implementacje pojedynczego systemu logowania SSO

System pojedynczego logowania SSO

Cechy rozwiązania:

- jedno konto, jedno hasło
- użytkownicy posługują się tylko jednym hasłem
- jedna prosta polityka kontroli siły haseł
- całkowita przezroczystość dla użytkownika
- duży koszt implementacji
- systemy, aplikacje, usługi wymagają znaczących zmian w budowie
- dla wielu aplikacji modyfikacja nie będzie możliwa ze względów technicznych bądź biznesowych

Federated SSO

Cechy rozwiązania:

- rozwiązanie ma sens tylko w przypadku istnienia Global lub Meta katalogów
- ograniczone zazwyczaj do aplikacji zintegrowanych w katalogach i katalogów wspierających protokoły federacyjne
- wsparcie dla Web Access Management
- brak jednego standardu usług federacyjnych
- duży koszt implementacji
- konieczność korelowania audytu w przestrzeniach federacyjnych

Enterprise SSO

Cechy rozwiązania:

- likwiduje problem zapamiętywania wielu haseł
- nazwy kont mogą się różnić
- kompletne rozwiązanie e-SSO może funkcjonalnie nie różnić się dla użytkownika od rozwiązania Global Login System przy ułamku kosztów w porównaniu z Global Login System
- scentralizowana i niejednorodna polityka haseł
- niskie koszty implementacji, bardzo krótki okres implementacji

Tivoli Identity Manager zapewnia szybki zwrot z inwestycji. Oprogramowanie nie tylko nadzoruje i egzekwuje udostępnianie użytkownikom odpowiednich zasobów, ale ma również wpływ na ograniczenie kosztów.

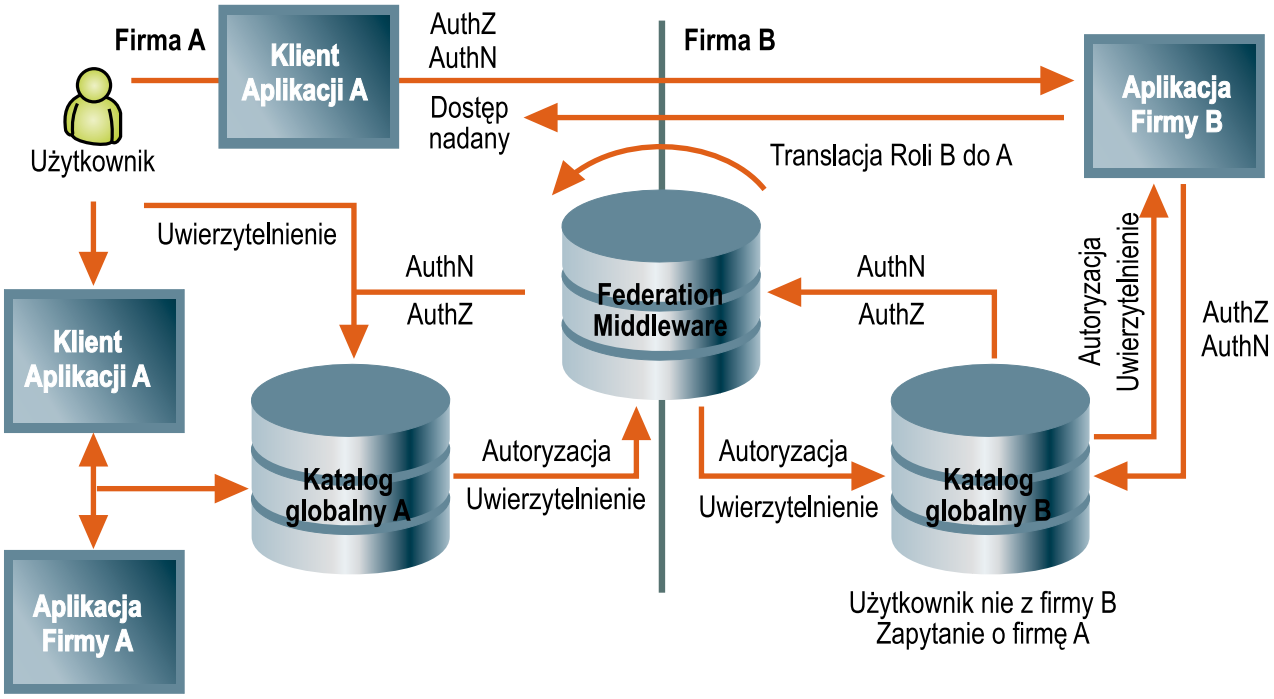
- prawidłowe działanie e-SSO wymaga, aby agent był zainstalowany na wszystkich stacjach roboczych, z których korzystają użytkownicy
- zwiększone koszty utrzymania

Zbigniew Szmigiero
Technical Specialist - Security
Zbigniew.szmigiero@pl.ibm.com

Więcej informacji o rozwiązaniu:

Link

Federated SSO



Enterprise SSO

1. Użytkownik uruchamia w aplikacji opcję zamiany hasła lub system automatycznie wymusza jego zmianę
2. Agent wykrywa takie zdarzenie i generuje nowe hasło zgodnie z polityką dla aplikacji
3. Agent zapisuje nowe hasło w bazie lokalnej i globalnej
4. Użytkownik zmienia hasło dla określonej aplikacji w Password Manager
5. Password Manager aktualizuje informację w haśle bazie globalnej
6. Baza lokalna jest aktualizowana w procesie synchronizacji, użytkownik jest automatycznie logowany w aplikacji z nowym hasłem

1. Baza uprawnień musi posiadać informację o AuthN
2. Jeśli baza uprawnień nie posiada informacji AuthN, użytkownik musi je wprowadzić za pierwszym razem


FORUM IT
14 marca 2011 r.
Hotel Hilton, Warszawa


zEnterprise
IBM