

Tożsamość usługowa

Impulsem do wdrożenia systemu zarządzania tożsamością w itelligence, były regularne prace związane z audytami systemów – m.in. wymagania ISO 27001 czy ustawy Sarbanesa-Oxley – oraz codzienne kłopoty z posługiwaniem się wieloma hasłami przez różnych administratorów. **MARCIN MARCINIAK**

itelligence jest firmą usługową, jej najważniejszymi klientami są firmy, które wykorzystują system SAP. Systemów tych jest prawie 100, a do tego dochodzą systemy operacyjne, bazy danych, systemy zarządzające i monitorujące. Do każdego z nich trzeba się często zalogować, odczytać logi i dokonać prac związanych z ich utrzymaniem. Zgodnie z wymaganiami większości norm jakości i bezpieczeństwa, pracownicy itelligence używają kont imiennych. W rozproszonym środowisku wymagało to kilkudziesięciu hasel dla każdego z administratorów.

Narastające problemy

Na potrzeby ewidencji oraz kontroli nad procesem przyznawania uprawnień do systemów opracowano w oparciu o Lotus Notes autorski system o nazwie Baza Uprawnień. Do pewnego momentu przy okazji audytów analizowano wszystkie systemy, potem gdy liczba obsługiwanych systemów rosła o kolejne setki – obecnie jest ich razem ponad 500 – życie wymusiło losowanie badanych systemów, gdyż ilość danych podlegających analizie wykraczała poza możliwości działów audytu. Na początku szukano jeszcze rozwiązań, które umożliwiłyby zmniejszenie liczby tworzonych kont. Gdzie to było możliwe, korzystano z kont domenowych, a w bazach danych stosowano uwierzytelnienie przy użyciu autoryzacji systemu operacyjnego.

Punktem zwrotnym był moment, gdy firma itelligence zaczęła obsługiwać klientów SOX i J-SOX. Wymagania ustawy Sarbanesa-Oxley w obszarze zarządzania uprawnieniami są bardzo rygorystyczne

i nie dopuszczają sytuacji, w której osoby nieuprawnione choćby przez moment mają dostęp do systemów IT. Jest to wnikliwie sprawdzanie co najmniej raz w roku podczas audytów SAS70. Każda istotna rozbieżność w tej materii może skutkować negatywnym wynikiem audytu i utratą certyfikatu, a razem z nim – klientów. Takie ryzyko było nie do zaakceptowania dla zarządu.

Firma potrzebowała narzędzia, które usprawniłoby proces dostępu do wielu systemów. Ostatecznie wybrano IBM Tivoli Identity

Pracownik itelligence otrzymuje w miarę potrzeb dostęp do systemu service desk, folderów sieciowych z dokumentami ISO, poczty, domeny Active Directory i dodatkowych dostępuów.

Manager (TIM). W krótkim czasie uruchomiono połączenia między TIM a systemami klientów. Najważniejsze było podłączenie systemów SAP, ale dołączono też bazy danych i systemy operacyjne, na których SAP jest zainstalowany. Oprócz systemów wchodzących w skład środowisk SAP, uruchomiono także połączenia z pozostałymi zarządzanymi systemami. Wśród zarządzanych systemów operacyjnych należałoby wymienić Windows, różne dystrybucje Linuxa i Unix. Bazy danych podłączone do TIM zaś to

Microsoft SQL Server, IBM DB2 i Oracle. Dodatkowo firma wdrożyła integrację z Cisco ACS, RSA SecureId i Lotus Notes/Domino.

Integracja

Najważniejszym dla itelligence agentem pakietu TIM jest ten, który integruje się z aplikacjami SAP. Więcej niż połowa działalności itelligence to obsługa firm korzystających z tej technologii, w różnych wersjach i konfiguracjach. Agent SAP występuje wyłącznie w wersji dla Windows, co sprawiało problemy w firmach, które nie wykorzystują żadnego serwera Microsoftu w podsieci SAP i nie życzą sobie żadnej maszyny z Windows w tej podsieci. Agent został więc zainstalowany w podsieci itelligence.

Aby TIM mógł się skomunikować z SAP, niezbędne jest zainstalowanie dostarczanego razem z agentem tak zwanego transportu dostosowanego do konkretnej wersji systemu SAP. Każdy z mandantów SAP (SAP clients) jest z punktu widzenia TIM osobną usługą. Po stronie SAP, niezbędne jest utworzenie konta typu „Communication” lub „System”, za którego pomocą agent będzie zarządzał użytkownikami. Niekiedy uprawnienia w SAP mogą posiadać bardzo okrojone uprawnienia, przykładowo dla celów audytu wystarczy konto, które nie będzie miało uprawnień do usuwania innych kont. Tak opracowana konfiguracja podwyższa bezpieczeństwo pracy.

Za pomocą natywnego agenta obsługiwane są systemy Windows, usługi Active Directory, baza SQL Server i aplikacje SAP. Co ciekawe, agenta TIM dla SAP można

zainstalować wyłącznie na platformie Windows, natomiast przy jego pomocy można zarządzać wszystkimi edycjami i wersjami SAP, niezależnie od platformy serwera. Pozostałe systemy można obsłużyć za pomocą Tivoli Directory Integrator, który zrealizuje połączenie pomiędzy TIM a docelowym systemem. Mechanizmy DI są elastyczne, w ten sposób można zintegrować wiele systemów, w tym takie, które nie są i nie będą oficjalnie wspierane przez producenta. itelligence realizuje połączenie pomiędzy DI a systemami Debian Linux, CentOS, bazami Oracle oraz innymi aplikacjami, w tym portalem SAP. Wykorzystano narzędzia do bardzo różnych aplikacji i baz wliczając MaxDB czy nawet SQLite, przy czym standardowe bazy, które nie są natywnie wspierane przez TIM, mogą być zarządzane alternatywnie przez JDBC. Jednym z obecnie aktywnych projektów jest integracja systemu elektronicznych kart dostępowych z Tivoli Identity Manager.

Dostęp dla pracowników

Oprócz dołączania kolejnych systemów do TIM, jednym z typowych procesów w firmie jest przyjęcie nowego pracownika. Dotychczas tworzono dużo dokumentów, które wymagały zatwierdzenia. Obecnie pierwszym etapem przy wdrożeniu pracownika jest utworzenie tożsamości w TIM. Nie jest to jeszcze konto czy dostęp do konsoli, ale referencja do wszystkich kont. Typowo przydzielanie uprawnień i dostępuów odbywa się za pomocą ról biznesowych, których uprawnienia się sumują. Razem z rolami, TIM zarządza także dostęпами, takimi jak np. dostęp do zasobów zarządzanych przez Active Directory lub baz Lotus Notes. Pracownik otrzymuje dostęp do systemu service desk, folderów sieciowych z dokumentami ISO, konto poczty elektronicznej i domeny Active Directory oraz dodatkowe dostępy, w miarę potrzeb. W standardowym modelu jest to kilkanaście kont, ale gdy przyjmowany jest pracownik na stanowisko np. starszego administratora, który ze względu na charakter swojej pracy musi mieć ok. 100 kont.

W chwili zaś rozwiązania umowy o pracę, wszystkie konta, do których pracownik miał dostęp, powinny zostać zablokowane. W tradycyjnym modelu nie jest to proste. W itelligence wystarczy obecnie zawieszenie tożsamości, skutkujące

automatycznym zablokowaniem dostępu do zarządzanych systemów. Czas reakcji jest liczony w minutach, przy czym zgłoszenie zawieszenia konta może zrobić prawie każdy pracownik w przypadku ważnych podejrzeń (np. kradzieży hasła). Decyzję o docelowym zablokowaniu lub usunięciu kont podejmuje właściwy dyrektor.

Pierwsze koty za płoty

Pierwsze problemy dotyczyły połączenia pomiędzy agentami oraz systemami SAP. Wynikały one głównie z braku doświadczenia współpracujących specjalistów z systemami SAP. W szczególności chodziło o tzw. transporty SAP. Pojawiały się też problemy z systemem SAP UME, który jest platformą aplikacyjną w języku Java, ale i te zostały szybko rozwiązane. Obecnie połączono ponad 150 systemów SAP, typowe połączenie nowego systemu zajmuje dziś tylko kilka minut. Inne zasoby, np. systemy operacyjne Windows i UNIX/Linux nie sprawiały problemów, czasami wymagały tylko dopra-

cowania konfiguracji optymalnej z punktu widzenia bezpieczeństwa.

Najpoważniejsze okazały się jednak kłopoty z komunikacją w bardzo specyficznej topologii połączeń. Ze względów bezpieczeństwa, ruch między podsieciami został zablokowany, sieci wykorzystywały różne adresacje. Stosowana podwójna zmiana adresu byłaby problemem, gdyby komunikacja wymagała dynamicznie otwieranych portów. Na szczęście wystarczy otwarcie konkretnych portów, agent nie używa portów zwrotnych.

Ważnym problemem było szybkie i niezawodne blokowanie konta we wszystkich systemach na podstawie zgłoszenia z TIM. W domyślnej konfiguracji serwer TIM łączył się z zarządzanym systemem i blokował konto, ale była to komunikacja jednorazowa. Zmianą wprowadzoną przy wdrożeniu systemu była pętla, która powodowała kilkukrotne komunikowanie się. Skutkiem wykonania pętli jest skuteczne i potwierdzone zablokowanie dostępu albo zgłoszony alert o problemach z komunikacją. ▸

Bezpieczeństwo przede wszystkim

System zarządzania tożsamością jest najważniejszym elementem systemu, odpowiedzialnym za bezpieczeństwo wszystkich zarządzanych zasobów. Dlatego firma zastosowała ponadstandardowe środki bezpieczeństwa. Serwery Tivoli Identity Management zostały zainstalowane w oddzielonej podsięci. Wybrano platformę Red Hat Linux eksploatowaną w wirtualizowanym środowisku VMware, zapewniającym wysoką dostępność dzięki mechanizmowi klastrowania VMotion.

Do każdego ze środowisk klienckich zrealizowano wirtualną sieć prywatną IPSec. Połączenie jest zrealizowane w taki sposób, że reguły zapór sieciowych blokują każdy ruch z wyjątkiem połączenia pomiędzy agentami TIM a współpracującym z nimi serwerem. Przy tym projekt topologii połączeń wyklucza całkowicie inną komunikację, nie jest możliwe żadne połączenie pomiędzy sieciami

poszczególnych klientów. Agent TIM komunikuje się z serwerem przy pomocy szyfrowanego połączenia SSL, nasłuchuje wyłącznie jednego adresu IP, pod którym jest widoczny serwer. Komunikacja jest zabezpieczona certyfikatami, zatem podszywanie się jest praktycznie niemożliwe.

Do serwera Tivoli Identity Management, w celach administracyjnych lub przy zmianie hasła, można się zalogować wyłącznie z dedykowanej podsięci, z użyciem dwuskładnikowego uwierzytelnienia tokenami RSA SecurID. Centralizowany dostęp umożliwił zrealizowanie mocnej polityki haseł, znacznie lepszej niż najmocniejsza używana przez klientów. Dzięki temu administratorzy nie muszą pilnować zmian hasła w każdym z systemów, logując się w każdym z nich za pomocą swojego, aktualnego, mocnego i dobrze pilnowanego hasła.