

IX Seminarium PLOUG
Warszawa
Maj 2004

(Nie)bezpieczeństwo instalacji Oracle – 7 grzechów głównych

Wojciech Dworakowski

SecuRing
wojciech.dworakowski@securing.pl

Od kilku lat zajmuję się ocenami bezpieczeństwa systemów informatycznych. Wykład będzie krótkim przeglądem najczęściej spotykanych podatności w instalacjach Oracle, z jakimi miał do czynienia zespół mojej firmy. W większości instalacji można zauważyć te same błędy. Dotyczy to zwłaszcza baz, które działają już od kilku lat i na których bezpieczeństwo ma wpływ nie tylko sposób konfiguracji początkowej ale również proces codziennego administrowania bazą. Poniżej opisuję kilka błędów, według mnie najczęściej popełnianych, które można spotkać w eksploatowanych produkcyjnie systemach Oracle

1. Brak poprawek

Za największą bolączkę eksploatowanych w Polsce systemów Oracle uważam wyjątkową wręcz niechęć administratorów do nakładania poprawek związanych z bezpieczeństwem. Większość systemów posiada tylko poprawki niezbędne do stabilnego działania oprogramowania na danej platformie systemowej. Poprawki związane z bezpieczeństwem nie są z reguły aplikowane. Taka sytuacja może dziwić – zwłaszcza jeśli weźmie się pod uwagę jakiego rodzaju zagrożenia mogą się wiązać z nienałożonymi poprawkami na oprogramowanie Oracle. Firmie tej (jak każdej innej) zdarzały się dość horendalne błędy umożliwiające łatwe zwiększenie przywilejów w bazie, zakłócenie funkcjonowania oprogramowania, czy przejęcie uprawnień w systemie użytkownika z jakiego prawami działa oprogramowanie Oracle.

Przykład 1:

Początkowo – w bazie w wersji 9 istniał błąd pozwalający dowolnemu użytkownikowi uzyskać dostęp do danych z przywilejami DBA. Błąd tkwił w nieprawidłowo zaimplementowanej składni LEFT OUTER JOIN, która pojawiła się w wersji 9. Przykład zapytania wykorzystującego ten błąd:

```
select a.username,a.password from sys.dba_users
a left outer join sys.dba_users b on
b.username = a.username
```

Przykład 2:

Jeśli na port na którym nasłuchuje Listener wyślemy nieudokumentowaną komendę SERVICE_CURLOAD, to na większości platform spowoduje to obciążenie systemu w 100% i zawieszenie procesu Oracle Listener. Błąd istnieje we wszystkich wersjach do (włącznie) 9i Release 2.

Z rozmów przeprowadzonych z administratorami Oracle wynika, że obawiają się oni obniżenia stabilności, czy wręcz zniszczenia instalacji w wyniku nałożenia poprawki. Jednak uważam że nie może to usprawiedliwiać braku uaktualniania systemów przetwarzających z reguły dość ważne dane. Temat strategii nakładania poprawek porusza artykuł „Dylematy administratora Oracle”, który opublikowałem w 27 numerze PLOUG’tek. Jest on dostępny pod adresem: <http://www.ploug.org.pl/gazetka/27/12.htm>

Mam nadzieje że sytuacja ta się zmieni choćby dzięki temu, że Oracle w najnowszym Enterprise Manager, wprowadziło funkcjonalność zarządzania poprawkami.

2. Użytkownicy/hasła standardowe

Drugą – równie groźną bolączką są użytkownicy i hasła standardowe. Wiadomym jest, że produkty Oracle przy instalacji zakładają bardzo wielu użytkowników w bazie. Są to zarówno konta potrzebne do administracji systemem (SYS, SYSTEM), konta demo (np. SCOTT) a także konta potrzebne do prawidłowego działania pewnych funkcji systemu (np. CTXSYS, MDSYS). W Internecie można znaleźć dość pokaźne listy takich kont i towarzyszących im haseł. Problem potęguje fakt, że część z tych kont posiada standardowo w systemie przywileje DBA lub bardzo bliskie DBA (np. CTXSYS z hasłem CTXSYS). Często spotykam też instalacje z hasłami SYS/CHANGE_ON_INSTALL i SYSTEM/MANAGER z tym że są to z reguły instalacje nieprodukcyjne (developerskie lub testowe). W tym miejscu zaznaczę, że warto dbać choćby w stopniu podstawowym o bezpieczeństwo instalacji testowych czy developerskich, bo również w nich bywa że są przetwarzane istotne dane. Zdarza się np. że do bazy testowej jest odtwarzana cała zawartość bazy produkcyjnej (łącznie z danymi) po to żeby dokładnie przetestować jakąś nową funkcjonalność.

Jeśli chodzi o ten typ podatności to sytuacja znacznie się poprawiła od wersji 9i. W nowszych wersjach, większość kont standardowych jest blokowana w końcowej fazie instalacji bazy.

3. Za duże uprawnienia użytkowników

Kolejny bardzo często spotykany błąd do zbyt duże uprawnienia użytkowników. Niektóre instalacje sprawiają wręcz wrażenie, że administrator bezgranicznie ufa swoim użytkownikom a system nadawania ról i przywilejów to tylko zbędny balast utrudniający pracę. W ocenianych przez nasz zespół instalacjach często znajdujemy dość dużo kont z nadaną rolą DBA. Innym przykładem są konta z nadanymi przywilejami „ANY” (SELECT ANY TABLE itp.). Z reguły nie analizujemy tego czy zestaw przywilejów danego użytkownika pozostaje w zgodzie z zasadą najmniejszych uprawnień koniecznych do wykonania zadań użytkownika, jednak nadawanie ponad 10 użytkownikom roli DBA czy przywilejów „ANY” wydaje się przesadą.

Z wywiadów z administratorami wynika, że tego typu sytuacje są pozostałością po działaniach administracyjnych lub (co gorsza!) po działaniach typu „gaszenie pożaru”. Czyli: „jeśli komuś coś nie działa to nadaję mu rolę DBA lub dodaję „ANY” do zestawu przywilejów i problem na razie mam z głowy, a w między czasie sprawdzę co nie działało”. Z reguły takie „chwilowe” zmiany pozostają na lata.

Do dobrych praktyk administracyjnych powinny należeć okresowe przeglądy przywilejów. Można to zrobić półautomatycznie za pomocą prostych skryptów PL/SQL.

4. Brak profili

Do dobrych praktyk związanych z zarządzaniem bezpieczeństwem systemów informatycznym należy ograniczanie ilości błędnych prób uwierzytelniania do systemu oraz wymuszanie na użytkownikach stosowania silnych haseł i wymuszanie okresowego zmieniania tych haseł. Wszystko to ma na celu ograniczenie możliwości przechwycenia kont użytkowników przez intruza.

W systemach Oracle służy do tego mechanizm profili. W większości instalacji z jakimi miałem do czynienia mechanizm ten nie był wogóle wykorzystywany. W standardowej konfiguracji istnieje tylko jeden profil – DEFAULT a wszystkie parametry w tym profilu mają wartość UNLIMITED. Taka standardowa konfiguracja powoduje, że potencjalny intruz ma nieograniczoną liczbę prób zgadywania hasła a ponieważ użytkownicy nie muszą zmieniać okresowo hasła, to intruz nie jest również ograniczony czasem. Daje to intruzowi nieograniczone możliwości łamania haseł metodą brute force. Na domiar złego w standardowym profilu DEFAULT nie ma włączonego wymuszania siły haseł.

Warto przy tej okazji wspomnieć, że bardzo częstą sytuacją spotykaną przez nasz zespół podczas przeglądów baz Oracle jest stosowanie trywialnych haseł (np. identycznych jak login użytkownika).

5. Listener bez hasła

Ustawienie hasła na dostęp administracyjny do Listenera jest podstawową zasadą zabezpieczania instalacji Oracle. Listener nie zabezpieczony hasłem umożliwia wiele prostych ataków, których skutkiem może być np. wyłączenie Oracle Listenera, wykonanie dowolnego kodu w systemie czy uzyskanie zdalnego dostępu do serwera Oracle. Ataki na Oracle Listener opisałem w artykule: Wybrane metody ataków na Oracle 8i (<http://www.ploug.org.pl/gazetka/23/11.htm>). Ustawienie hasła powoduje, że aby wydawać dla Listenera komendy administracyjne, należy najpierw uwierzytelnić się hasłem. Utrudnia to przeprowadzenie skutecznych ataków.

W znacznej części instalacji produkcyjnych administratorzy ustawiają hasło Listenera, jednak w przypadku serwerów testowych i developerskich najczęściej te hasło nie jest stosowane.

6. Brak admin_restrictions

O ile ustawienie hasła na Listener jest dość powszechną praktyką, o tyle żadko można spotkać dodatkowe środki zabezpieczające ten kluczowy serwis, takie jak np. włączenie parametru AD-

MIN_RESTRICTIONS. Bez ustawienia w konfiguracji Listenera tego parametru, Listener będzie akceptować komendy administracyjne wydawane zdalnie. Komendy te to np. wyłączenie listenera, zmienienie plików logów, itd. Najczęściej ta funkcjonalność nie jest wymagana a mało który administrator wyłącza ją.

7. Demo

Ostatnim – bardzo groźnym błędem jaki można spotkać w instalacjach Oracle jest obecność skryptów, kont i przykładów demo w instalacjach produkcyjnych. Szczególnie groźne są skrypty demo dostępne zdalnie przez HTTP w instalacjach Oracle HTTP Server czy Oracle Application Server. Skrypty te umożliwiają zdobycie dużej wiedzy o instalacji Oracle oraz często umożliwiają wykonywanie nieuprawnionych działań w systemie. W wielu skryptach demo dostarczanych z OHS i 9iAS istnieje możliwość skutecznego ataku na dane metodą SQL-injection (prezentowałem te możliwości wielokrotnie na warsztatach corocznych konferencji PLOUG).

Nikogo nie muszę chyba przekonywać, że zawartość demo w instalacjach produkcyjnych jest niewskazana.

8. Podsumowanie

Wielu administratorów, zwłaszcza nie specjalizujących się w bezpieczeństwie IT, uważa że do wykorzystania dziur w Oracle potrzebna jest „wiedza tajemna”. Sytuację pogarsza fakt, że administratorzy czują się relatywnie bezpieczni, bo systemy Oracle działają z reguły w sieci LAN i nie są wystawione bezpośrednio do Internetu. Pamiętajmy jednak o tym że Oracle często stanowi backend dla systemów wystawionych do Internetu, a poza tym z niezależnych badań wynika że 70% ataków na systemy informatyczne jest przeprowadzana z wewnątrz sieci. Z opanowanej wcześniej stacji roboczej, lub za pośrednictwem nieuczciwego pracownika. Mam nadzieje że powyżej przytoczone przykłady (a to tylko czubek góry lodowej) pomogą uzmysłowić stopień zagrożenia.

Najwięcej błędów i uchybień znajduje się w instalacjach Oracle, które są eksploatowane od kilku lat (a takie instalacje nie należą do rzadkości). Twierdzenie to jest prawdziwe nie tylko w przypadku instalacji Oracle. Wynika to z tego, że podczas zadań administracyjnych bywają stosowane rozwiązania tymczasowe, które pozostają w systemie. Rozwiązania te z reguły mają za zadanie uruchomienie jakiejś funkcjonalności a nie podniesienie czy choćby zachowanie poziomu bezpieczeństwa instalacji. Stąd właśnie wynika proces „starzenia się” instalacji systemów produkcyjnych. Zwłaszcza gdy zadania administracyjne nie są ściśle wyznaczone odpowiednimi procedurami.

Do dobrych praktyk administracyjnych powinno należeć zabezpieczenie systemu Oracle zaraz po zainstalowaniu (hardening) oraz okresowe sprawdzanie bezpieczeństwa instalacji. Jest to jedyny sposób na utrzymanie zakładanego poziomu bezpieczeństwa.