

McAfee Intercept Database Edition

Sprawdzone funkcje zapobiegania włamaniom do serwerów baz danych

Wyzwanie

Dostęp w czasie rzeczywistym do informacji znajdujących się w serwerze bazy danych pozwala usprawnić procesy gospodarcze dotyczące klientów, pracowników i partnerów przedsiębiorstwa. Większa wygoda może jednak oznaczać zwiększoną podatność na włamanie. Badania przeprowadzone niedawno przez Evans Data Corp. wykazały, że serwery baz danych połączone do Internetu są w dużym stopniu narażone na ataki. Według badań, w 2001 r. ponad 20 procent projektantów baz danych stwierdziło przypadki naruszenia bezpieczeństwa. Ponadto z przeprowadzonej w 2001 r. ankiety wynika, że 12 procent respondentów padło ofiarą nieuprawnionego dostępu do informacji przechowywanych na serwerze bazy danych.

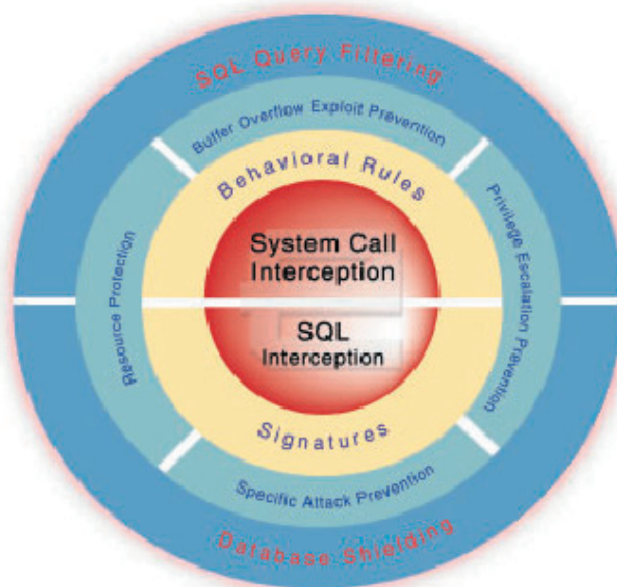
W ciągu zaledwie dziesięciu minut robak internetowy o nazwie SQL Slammer przeprowadził skuteczny atak na 90 procent wszystkich niezabezpieczonych hostów. Koszty usuwania szkód szacuje się na 750 mln do 1 mld USD. Nieautoryzowani użytkownicy, tacy jak hakerzy i niezadowoleni pracownicy, znajdują sposoby na uzyskanie dostępu i modyfikację danych, zasobów i plików programów w celu przeprowadzenia ataków czy zapewnienia sobie większych uprawnień. Dzisiejsze przedsiębiorstwa wymagają prewencyjnej ochrony zarówno przed najnowszymi technikami ataków na serwery, jak i metodami jeszcze nieodkrytymi. Biorąc pod uwagę, że serwer bazy danych jest podstawą każdego centrum przetwarzania danych, zabezpieczenie go przed znanymi i nieznanymi zagrożeniami jest sprawą o krytycznym znaczeniu dla przedsiębiorstwa.

Prezentujemy Intercept Database Edition

Zestaw funkcji zapobiegania włamaniom systemu McAfee® Intercept® został wzbogacony o prewencyjną ochronę serwerów baz danych. System Intercept Database Edition udostępnia przedsiębiorstwu sprawdzoną, łatwą do wdrożenia metodę ochrony zasobów i zapewnienia integralności serwerów baz danych. Oprogramowanie Intercept Database Edition bazuje na opatentowanych funkcjach ochrony oferowanych przez nasz sztanardowy produkt, Intercept Standard Edition. Dodatkowo udostępnia poszerzony zakres ochrony zarówno przed znanymi, jak i nieznanymi formami ataków, włącznie z bardzo popularnymi atakami typu SQL Injection. Intercept Database Edition blokuje bazę danych, by wymusić poprawne, a uniemożliwić niezgodne z regułami zachowanie, dzięki czemu system ten stanowi najbardziej rozbudowane i kompleksowe rozwiązanie do ochrony baz danych dostępne na rynku. Intercept jest jedynym systemem zapobiegania włamaniom tworzącym dostosowane do aplikacji mechanizmy i reguły przechwytywania treści, zapewniające ochronę aplikacji, systemów operacyjnych i danych przed zagrożeniami.

Intercept Database Edition:

- przechwytuje i selektywnie blokuje zapytania SQL, zanim zostaną one przetworzone przez bazę danych, co chroni integralność systemu
- osłania całą bazę danych, uniemożliwiając wykorzystanie luk w zabezpieczeniach i wymuszając poprawne zachowanie
- uniemożliwia włamywaczom wykorzystanie bazy danych do zaatakowania innych usług, plików, komputerów itp.



Oprogramowanie Intercept Database Edition bazuje na funkcjonalności systemu McAfee Intercept Standard Edition, zawierając ponadto unikatowy mechanizm SQL Interception Engine, który blokuje destrukcyjne zapytania SQL, zanim zostaną one przetworzone przez bazę danych. Łącząc filtrowanie zapytań i kompleksową osłonę bazy danych, wersja Database Edition zabezpiecza bazy danych przed znanymi i nieznanymi rodzajami ataków.

Oprogramowanie Intercept prewencyjnie chroni serwer bazy danych, analizując zapytania SQL kierowane do systemu operacyjnego, zanim zostaną one obsłużone. W przeciwieństwie do innych rozwiązań, ograniczających się wyłącznie do wykrywania ataków i informowania o nich po fakcie, Intercept posługuje się kombinacją reguł zachowań i sygnatur, zapobiegając zarówno znanym, jak i nieznanym formom ataków. Intercept to sprawdzony lider na rynku systemów zapobiegania włamaniom.

Korzyści

Ochrona zasobów

- chroni dane przedsiębiorstwa
- uniemożliwia niepowołanym osobom uzyskanie dostępu do serwera bazy danych poprzez wykorzystanie zapytań SQL
- uniemożliwia niepowołanym osobom wykorzystanie bazy danych jako przyczółka do ataku na inne zasoby.

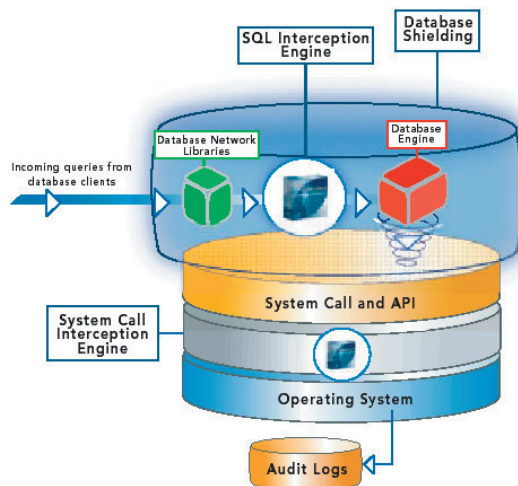
Krótszy czas przestoju

- uniemożliwia uzyskanie bez upoważnienia dostępu do serwera bazy danych
- zapobiega uzyskaniu dostępu do serwera za pomocą nowych, dotychczas nieznanych ataków
- blokuje najgroźniejsze znane formy ataków na bazy danych, które mogłyby zostać użyte do uzyskania całkowitej kontroli nad serwerem bazy danych

McAfee Enterecept Database Edition

Sprawdzone funkcje zapobiegania włamaniom do serwerów baz danych

Unikatowy mechanizm SQL Interception Engine przechwytyje zapytania SQL, wykorzystując integrację z samą aplikacją bazą danych. Mechanizm System Call Interception Engine jest zlokalizowany pomiędzy systemem operacyjnym a aplikacjami. Blokuje on wszelkie destrukcyjne działania i zapobiega włamaniom.



Jak działa Enterecept Database Edition?

Oprogramowanie Enterecept łączy w sobie kilka podstawowych technologii ochrony serwerów baz danych. Agenty programu Enterecept Database Edition instalowane są na każdym serwerze w przedsiębiorstwie w ramach architektury rozproszonej. System wykorzystuje nowoczesną, zaawansowaną technikę SQL Interception, pozwalającą na przechwytywanie wszystkich zapytań kierowanych do bazy danych i blokowanie tych, które stanowią zagrożenie. Mechanizm SQL Interception analizuje każde zapytanie pod kątem możliwego przepełnienia bufora, prób użycia techniki SQL Injection oraz innych prób nietypowej interakcji z bazą danych. Za pomocą tych informacji nadchodzące wywołania są dopasowywane do odpowiednich reguł zachowań oraz sygnatur znanych ataków. Następnie system blokuje zapytania wskazujące na zachowania destrukcyjne i takie, które pasują do jednej z sygnatur. Wszelkie działania prewencyjne są rejestrowane w systemie Enterprise Management System, a następnie udostępniane do wglądu i uwzględniane w raportach.

Baza danych reguł zawiera w pełni skonfigurowany szablon domyślny, wyposażony w rozbudowane funkcje dostosowywania. Użycie reguł domyślnych umożliwia szybkie wdrożenie. Na każdym serwerze instalowane są agenty, które następnie

są kontrolowane i aktualizowane za pośrednictwem systemu zarządzającego.

Funkcje

- Funkcja zapobiegania atakom umożliwia blokowanie destrukcyjnych działań, zanim doprowadzą one do powstania szkód.
- Bezpieczne, samodzielne agenty.
- Wstępnie skonfigurowany szablon reguł wyposażony w opcje dostosowawcze.
- Zapobieganie dostępowi bez upoważnienia do zasobów systemowych.
- Uzupełnienie istniejącej infrastruktury zabezpieczeń.

Ochrona przed atakami SQL Injection

System zapewnia ochronę przed powszechnym zagrożeniem bezpieczeństwa bazy danych: technikami SQL Injection. Wprowadzając specjalnie przygotowane instrukcje SQL do narażonych na takie ataki pól danych aplikacji, intruzi mogą uzyskać dostęp do poufnych danych, takich jak numery kart kredytowych, a także usunąć te dane, zmodyfikować je, a nawet zaatakować inne komputery w sieci, w której znajduje się dany serwer bazy danych. Enterecept Database Edition uniemożliwia takie ataki, dokonując weryfikacji zapytań SQL przed ich przetworzeniem przez bazę danych. Destructywny zapytania są odrzucane, dzięki czemu integralność bazy danych zostaje zachowana.

Ochrona przed konkretnymi atakami

— Uniemożliwia włamywaczom zakłócenie

działania bazy danych. Istnieją dziesiątki znanych ataków skutkujących awarią i/lub dostępem bez upoważnienia do serwerów baz danych. Za pomocą technologii SQL Interception oprogramowanie Enterecept blokuje takie ataki, zanim spowodują one szkody.

Ochrona bazy danych — Chroni bazy danych i przechowywane w nich dane przed dostępem bez upoważnienia. Ochrona bazy danych gwarantuje, że żaden proces poza samą bazą danych nie uzyska dostępu do środowiska wykonawczego, danych czy ustawień bazy danych. Ponadto, baza danych nie może uzyskać dostępu do zasobów niezwiązanych z bazą danych, dzięki czemu włamywacz nie jest w stanie wykorzystać jej do ataku na inne cele. Ochrona bazy danych jest więc warstwą ochronną, uniemożliwiająca zarówno penetrację z zewnątrz, jak i wykorzystanie serwera do niedozwolonych celów. W rezultacie zarówno znane, jak i nieznane próby ataków są blokowane w czasie rzeczywistym, zanim dotrą do serwera bazy danych i wywołają szkody. Potencjalni intruzi nie są w stanie odczytać ani zmodyfikować parametrów operacyjnych — nawet gdyby udało im się uzyskać dostęp do serwera z odpowiednimi prawami.

Wszystkie funkcje systemu Enterecept Standard Edition

— Oprogramowanie Enterecept Database Server Edition zawiera funkcje opisane wyżej, a także wszystkie funkcje udostępniane przez system Enterecept Standard Edition: zapobieganie znanym i nieznanym atakom, zapobieganie atakom bazującym na przepełnieniu bufora, ochrona zasobów oraz zapobieganie uzyskaniu nadmiernych praw dostępu.

Wymagania systemowe

Windows Database Server

- 200 MHz Pentium III lub lepszy
- 128 MB RAM lub więcej
- SQL Server 2000
- Windows 2000 Server lub Windows 2000 Advanced Server
- Windows NT 4 Server lub Enterprise Server, Service Pack 6a lub nowszy.

Network Associates, Enterecept, SecureSelect i PrimeSupport są zastrzeżonymi znakami towarowymi Network Associates Inc. i/lub przedsiębiorstw zależnych w Stanach Zjednoczonych i/lub innych państwach. Produkty marki Sniffer® są produkowane tylko przez Network Associates Inc. Pozostałe zastrzeżone i niezastrzeżone znaki towarowe są wyłączną własnością odpowiednich podmiotów. ©2003 Networks Associates Technology Inc. Wszelkie prawa zastrzeżone.