White Paper

Top 10 der Datenbankbedrohungen

So beheben Sie die wichtigsten Datenbankschwachstellen

Datenbankstrukturen in Unternehmen sind zahlreichen Sicherheitsbedrohungen ausgesetzt. Dieses Dokument soll Organisationen dabei unterstützen, den kritischsten dieser Bedrohungen wirksam zu begegnen. Es führt die vom Imperva Application Defense Center identifizierten zehn größten Sicherheitsbedrohungen auf. Zu jeder Bedrohung finden Sie Hintergrundinformationen, allgemeine Strategien zur Risikovermeidung und Informationen zum Datenbankschutz, der durch die Imperva SecureSphere Database Security Lösung zur Verfügung steht.

Top 10 der Datenbanksicherheitsbedrohungen

1. *Missbrauch übermäßiger Berechtigungen*
2. *Missbrauch legitimer Berechtigungen*
3. *Missbräuchliche Berechtigungserweiterung*
4. *Ausnutzen von Schwachstellen in fehlerhaft konfigurierten Datenbanken*
5. *SQL Injection*
6. *Unzureichender Audit-Trail*
7. *Denial of Service*
8. *Schwachstellen im Datenbankkommunikationsprotokoll*
9. *Nicht autorisierte Kopien vertraulicher Daten*
10. *Unzureichend geschützte Backup-Daten*

Organisationen, die all diesen Bedrohungen begegnen, erfüllen globale Compliance-Anforderungen und bewährte Industriestandards bezüglich Datenschutz und Risikominimierung.

Bedrohung 1 – Missbrauch übermäßiger Berechtigungen

Wenn Anwendern (oder Anwendungen) Berechtigungen für den Datenbankzugriff erteilt werden, die ihren Aufgabenbereich übersteigen, können diese Berechtigungen eventuell zu böswilligen Zwecken missbraucht werden. Ein Administrator in einer Universität, dessen Aufgabe es lediglich erfordert, Kontaktinformationen von Studenten zu pflegen, könnte z. B. seine übermäßigen Datenbankaktualisierungsberechtigungen dazu missbrauchen, Noten zu ändern.

Datenbankbenutzern werden oft übermäßige Berechtigungen aus dem einfachen Grund erteilt, dass Datenbankadministratoren nicht über die Zeit verfügen, abgestufte Kontrollmechanismen für die Zugriffsberechtigungen einzelner Benutzer zu definieren und auf dem neuesten Stand zu halten. Im Ergebnis führt dies dazu, dass allen Benutzern oder großen Benutzergruppen allgemeine Standardzugriffsberechtigungen erteilt werden, die weit über die Anforderungen ihrer Aufgaben hinausgehen.

Verhinderung des Missbrauchs übermäßiger Berechtigungen – Eliminierung übermäßiger Berechtigungen und Durchsetzung über die Zugriffssteuerung auf Abfrageebene

Um dieser Bedrohung wirksam zu begegnen, müssen alle übermäßigen Berechtigungen eliminiert werden. Dazu ist es zunächst erforderlich, übermäßige Berechtigungen zu identifizieren – Berechtigungen, die der Benutzer für seine Aufgaben nicht benötigt. Dies wird erreicht, indem Berechtigungen aus den Datenbanken extrahiert, mit den Benutzern abgeglichen und schließlich analysiert werden. Dieser Prozess stellt eine große Herausforderung dar und ist, sofern er manuell durchgeführt wird, sehr zeit- und ressourcenintensiv. Eine automatisierte Lösung kann den für den Analyseprozess erforderlichen Zeit- und Ressourcenaufwand erheblich reduzieren.

Um Zugriffsrechte besser durchsetzen zu können, wird zudem eine fein abgestufte Zugriffsteuerung auf Abfrageebene benötigt. Mit einer Zugriffssteuerung auf Abfrageebene ist ein Mechanismus gemeint, der die Datenbankberechtigungen eines Benutzers auf ein Mindestmaß benötigter SQL-Operationen (SELECT, UPDATE usw.) und Daten beschränkt. Die Granularität der Datenzugriffssteuerung muss dabei über die Tabelle hinausgehen und zwischen einzelnen Zeilen und Spalten innerhalb einer Tabelle unterscheiden können. Ein ausreichend granularer Zugriffssteuerungsmechanismus auf Abfrageebene würde es dem zuvor beschriebenen, in seinen Absichten fragwürdigen Universitätsadministrator zwar erlauben, Kontaktinformationen zu aktualisieren, aber eine Alarmmeldung erzeugen, würde er versuchen, Noten zu ändern. Eine Zugriffssteuerung auf Abfrageebene ist nicht nur hilfreich dabei, den Missbrauch übermäßiger Berechtigungen durch böswillige Zugriffe zu erkennen, sondern bietet zugleich Schutz gegen die meisten der anderen hier beschriebenen Top-10-Bedrohungen. Die meisten Datenbanksoftwareimplementierungen verfügen bereits über ein gewisses Maß an Zugriffssteuerung auf Abfrageebene (Trigger, Schutzfunktionen auf Zeilenebene usw.), diese integrierten Funktionen erfordern bei größeren Impelmentierungen allerdings ein hohes Maß an manuellen Konfigurationen. Solche Definitionen von Zugangsrichtlinien auf Abfrageebene für alle Benutzer über Datenbankzeilen, -spalten und -operationen hinweg ist zu zeitaufwendig. Doch damit nicht genug: Benutzerrollen ändern sich im Laufe der Zeit, sodass die Abfragerichtlinien aktualisiert werden müssen, um diesen neuen Rollen gerecht zu werden. Die meisten Datenbankadministratoren haben nicht ausreichend Zeit um für nur wenige Benutzer zu einem bestimmten Zeitpunkt sinnvolle Abfragerichtlinien zu definieren – von hunderten Benutzern, deren Aufgaben sich mit der Zeit ändern, ganz zu schweigen. Dies führt im Ergebnis meist dazu, dass Organisationen Benutzern eine Standardzugriffsberechtigung erteilen, mit denen eine große Anzahl an Benutzern arbeiten kann, die aber nicht maßgeschneidert und mit übermäßigen Rechten versehen ist Um eine echte Zugriffssteuerung auf Abfrageebene Realität werden zu lassen, sind automatisierte Tools erforderlich.

SecureSphere Dynamic Profiling – Benutzerrechtemanagement und automatisierte Zugriffssteuerung auf Abfrageebene

SecureSphere User Rights Management for Databases (URMD) ermöglicht es, Benutzerrechte automatisch zuzuweisen und zu prüfen, Berechtigungen für vertrauliche Daten zielgerichtet zu analysieren und übermäßige Berechtigungen sowie nicht aktive Benutzer basierend auf dem organisatorischen Kontext und der tatsächlichen Nutzung zu erkennen.

Der Zugriff auf vertrauliche Objekte wird basierend auf berechtigtem geschäftlichem Interesse gewährt, das sich normalerweise aus dem organisatorischen Kontext der Benutzer ergibt. Details wie die Benutzerrolle und Abteilung geben Prüfern Einblick über die geschäftliche Funktion eines Benutzers und die Art von Daten, auf die

dieser zugreifen darf. Mithilfe der Analyseansichten von URMD können Prüfer erkennen, ob Benutzerzugriffsrechte ordnungsgemäß definiert sind, und übermäßige Rechte, die der Benutzer nicht zur Durchführung seiner Aufgaben benötigt, entfernen.

URMD ermöglicht es Organisationen, ihre Compliance mit Regulierungen wie SOX, PCI 7 und PCI 8.5 nachzuweisen und das Risiko einer Datenzugriffsverletzung zu verringern. URMD ist eine Zusatzoption für die Datenbanksicherheitsprodukte von Imperva.

Die Imperva SecureSphere Datenbanksicherheitslösungen stellen darüber hinaus einen automatisierten Mechanismus bereit, um Zugriffssteuerungsrichtlinien auf Abfrageebene zu definieren und durchzusetzen. Die Dynamic-Profiling-Technologie von SecureSphere verfügt über einen automatischen Lernalgorithmus und erstellt für alle Benutzer und Anwendungen, die auf die Datenbank zugreifen, Benutzerprofile auf Abfrageebene. Profile umfassen allgemeine Nutzungsmuster ebenso wie jede einzelne Abfrage und gespeicherte Prozedur. Die Lernalgorithmen von SecureSphere aktualisieren laufend das Profil, um manuelle Anpassungen bei sich verändernden Benutzerrollen zu vermeiden. Sollte ein Benutzer einen Vorgang durchführen, der nicht zu seinem Profil passt, zeichnet SecureSphere dieses Ereignis auf, erzeugt eine Alarmmeldung und kann den Vorgang je nach Schweregrad optional blockieren. Der zuvor beschriebene Universitätsadministrator, der versucht, Noten zu ändern, wäre mit Dynamic Profiling einfach erkannt worden. Das Profil des Administrators würde eine Reihe von Abfragen umfassen, die den normalen Änderungen an bestimmten Kontaktinformationen von Studenten und gegebenenfalls einem Nur-Lese-Zugriff auf Noten entspricht. Ein plötzlicher Versuch, Noten zu ändern, würde jedoch eine Alarmmeldung auslösen.

Bedrohung 2 – Missbrauch legitimer Berechtigungen

Benutzer können auch legitime Datenbankberechtigungen für nicht autorisierte Zwecke missbrauchen. Nehmen Sie z. B. einen böswilligen oder unbedarften Krankenhausmitarbeiter an, der über die Berechtigung verfügt, über eine Webanwendung Daten einzelner Patienten abzufragen. Die Struktur der Webanwendung beschränkt Benutzer normalerweise darauf, Patientenakten nur einzeln aufzurufen – eine gleichzeitige Ansicht mehrerer Datensätze und elektronische Kopien sind nicht erlaubt. Der Mitarbeiter kann diese Beschränkungen jedoch umgehen, indem er sich mit einem alternativen Client wie MS-Excel an die Datenbank anmeldet. Mithilfe von MS-Excel und seinen legitimen Anmeldeinformationen könnte der Mitarbeiter alle Patientendatensätze abrufen und speichern. Derartige persönliche Kopien von Datenbanken mit Patientenakten werden die Datenschutzrichtlinien der Gesundheitsorganisation aller Wahrscheinlichkeit nach verletzen. In diesem Fall gibt es zwei Risiken, die in Betracht zu ziehen sind. Das erste Risiko ist ein böswilliger Mitarbeiter, der Patientendatensätze vielleicht gegen Geld verkaufen möchte. Das zweite (und vielleicht häufigere) Risiko ist ein fahrlässiger Mitarbeiter, der große Informationsmengen abruft und auf seinem Client-Gerät zu Arbeitszwecken speichert. Die jetzt auf dem Endgerät vorhandenen Daten sind dort Bedrohungen wie Trojanern, Laptopdiebstahl usw. ausgesetzt.

Missbrauch legitimer Berechtigungen verhindern – Verständnis für den Kontext des Datenbankzugriffs

Um den Missbrauch legitimer Berechtigungen zu verhindern, wird eine Datenbankzugriffssteuerung benötigt, die nicht nur bestimmte Abfragen berücksichtigt (wie oben beschrieben), sondern den Kontext des Datenbankzugriffs in Betracht zieht. Mit der Umsetzung von Richtlinien für Client-Anwendungen, Tageszeiten, Zugriffsorte usw. ist es möglich, Benutzer zu identifizieren, die legitime Datenbankzugriffsberechtigungen auf verdächtige Weise nutzen.

SecureSphere Dynamic Profiling – Kontextbasierte Zugriffssteuerung

Zusätzlich zu den Abfrageinformationen (siehe oben: übermäßige Berechtigungen) erstellt die Dynamic-Profiling-Technologie von SecureSphere ein Modell des Kontexts normaler Datenbanknutzungen. Zu den im Profil gespeicherten Kontextinformationen gehören die Tageszeit, die Quell-IP-Adresse, die Menge der abgefragten Daten, der Benutzer und weitere Informationen. Jede Verbindung, deren Kontext nicht mit den im Benutzerprofil gespeicherten Informationen übereinstimmt, löst einen Alarm aus. Der zuvor beschriebene Krankenhausmitarbeiter wird z. B. von SecureSphere nicht nur aufgrund der Verwendung von MS-Excel als Nicht-Standard-Client, sondern auch aufgrund der in einer einzigen Sitzung abgefragten Datenmenge erkannt. In diesem speziellen Fall würden die Abweichungen in der Struktur der Nicht-Standard-MS-Excel-Abfrage zudem eine Verletzung auf Abfrageebene auslösen (siehe oben: Missbrauch übermäßiger Berechtigungen).

Bedrohung 3 – Mißbrauch übermäßiger Berechtigungen

Angreifer können Schwachstellen der Datenbankplattformsoftware ausnutzen, um die Zugriffsberechtigungen eines normalen Benutzers in die eines Administrators umzuwandeln. Schwachstellen können in gespeicherten Prozeduren, integrierten Funktionen, Protokollimplementierungen und selbst in SQL-Statements auftreten. Ein Softwareentwickler in einer Finanzinstitution könnte z. B. eine Funktion mit Schwachstelle ausnutzen, um Administrationsberechtigungen für die Datenbank zu erlangen. Mit dieser Berechtigung könnte der böswillige Entwickler anschließend Prüfmechanismen umgehen, falsche Konten erstellen, Gelder transferieren usw.

Verhinderung von Berechtigungserweiterungen mit dem Ziel des Mißbrauchs – IPS und Zugriffssteuerung auf Abfrageebene

Die Erweiterung von Berechtigungen mit dem Ziel des Mißbrauchs lässt sich mit einer Kombination herkömmlicher Intrusion Prevention Systeme (IPS) und einer Zugriffssteuerung auf Abfrageebene (siehe oben: übermäßige Berechtigungen) verhindern. IPS untersucht den Datenbank-Verkehr und identifiziert Muster, die bekannten Schwachstellen entsprechen. Wenn die Schwachstellen einer bestimmten Funktion bekannt sind, kann ein IPS etwa jeden Zugriff auf die Prozedur mit Schwachstelle oder (sofern möglich) nur Prozeduren mit integrierten Angriffen blockieren. Leider reicht jedoch ein IPS alleine oft nicht aus, um gezielt die Datenbankabfragen mit Angriffen herauszufiltern. Viele für Angriffe anfällige Datenbankfunktionen werden häufig zu legitimen Zwecken genutzt. Alle Nutzungen derartiger Funktionen zu blockieren, ist daher keine Option. Das IPS muss in der Lage sein, legitime Funktionen von Funktionen mit integrierten Angriffen genau zu unterscheiden. In vielen Fällen macht die Vielzahl von Angriffsvarianten dies zu einer unmöglichen Aufgabe. In derartigen Fällen lassen sich IPS-Systeme nur im Alarmmodus (ohne Blockierung) verwenden, da zu oft false-positives auftreten. Um die Genauigkeit zu erhöhen, können IPS-Systeme mit alternativen Angriffserkennungsmethoden wie einer Zugriffssteuerung auf Abfrageebene kombiniert werden. IPS lässt sich verwenden, um zu überprüfen, ob bei Datenbankzugriffen anfällige Funktionen aufgerufen werden, während die Zugriffssteuerung auf Abfrageebene erkennt, ob die Anfrage dem normalen Benutzerverhalten entspricht. Wenn in einer einzelnen Anfrage sowohl ein Zugriff auf eine anfällige Funktion als auch ungewöhnliches Verhalten registriert werden, handelt es sich mit hoher Sicherheit um einen Angriff.

SecureSphere Privilege Elevation – Integriertes IPS und Dynamic Profiling

SecureSphere kombiniert ein weiterentwickeltes IPS-System und Dynamic Profiling für die Zugriffssteuerung auf Abfrageebene (siehe oben: übermäßige Berechtigungen). Diese Technologien ermöglichen einen extrem präzisen Schutz gegen die Erweiterung von Berechtigungen mit dem Ziel des Mißbrauchs. SecureSphere IPS verfügt über Snort®-kompatible Signaturdatenbanken für alle Protokolle und bietet Schutz vor Angriffen, die gegen bekannte Schwachstellen gerichtet sind. Die internationale Forschungsorganisation für Datensicherheit Application Defense Center von Imperva stellt proprietäre SQL-spezifische Schutzfunktionen zur Verfügung und gewährleistet, dass Sie mit SecureSphere die führende Datenbank-IPS-Sicherheitslösung der Welt nutzen. Der Aktualisierungsservice von SecureSphere Security hält alle Signaturdatenbanken auf dem neuesten Stand, um jederzeit Schutz auch vor den neuesten Bedrohungen zu bieten. SecureSphere IPS blockiert bestimmte einfach identifizierbare Angriffe online, ohne weitere Angriffsbestätigungen zu erfordern. Sollte eine Abfrage jedoch nur als verdächtig identifiziert werden können, korreliert SecureSphere die Abfrage mit zusammenhängenden Dynamic-Profile-Verletzungen, um den Angriff zu bestätigen. Lassen Sie uns zum erwähnten Softwareentwickler zurückkehren, um deutlich zu machen, wie SecureSphere IPS und Dynamic Profiling in die Sicherheitslösung integriert ist. Nehmen wir z. B. an, der Entwickler würde versuchen, einen bekannten Buffer-Overflow mit einer Datenbankfunktion zu nutzen, um schadhaften Code einzufügen. Sein Ziel besteht darin, seine Berechtigungen auf die eines Datenbankadministrators zu erweitern. In diesem Fall identifiziert SecureSphere zwei gleichzeitige Verletzungen. Zum einen löst jede Abfrage, die auf eine Funktion mit bekannten Schwachstellen zugreift, eine IPS-Verletzung aus. Zum anderen löst die ungewöhnliche Abfrage eine Profilverletzung aus. Indem beide Verletzungen in einer einzigen Datenbankabfrage des gleichen Benutzers korreliert werden, lässt sich ein Angriff mit extrem hoher Genauigkeit erkennen, sodass eine Alarmmeldung mit hoher Priorität ausgelöst oder der Vorgang blockiert werden kann.

Bedrohung 4 – Ausnutzen von Schwachstellen in fehlerhaft konfigurierten Datenbanken

Datenbanken mit nicht gepatchten Schwachstellen und Datenbanken, die noch über Standardkonten und Konfigurationsparameter verfügen, sind keine Seltenheit. Angreifer, die auf eine Datenbank zugreifen möchten, werden Systeme typischerweise auf diese Schwachstellen hin prüfen, sodass hier die Gefahr einer Sicherheitsverletzung gegeben ist. In der Zeit, in der ein Anbieter einen Patch für eine bestimmte Schwachstelle entwickelt, ist die Datenbank einer Organisation nicht gegen Angreifer geschützt. Auch wenn ein Patch freigegeben wurde, steht dieser vielleicht noch nicht sofort zur Verfügung. Beim Patchen einer Datenbank sind verschiedene Aspekte in Betracht zu ziehen. Eine Organisation muss zunächst den Patchvorgang für das System für diesen bestimmten Patch bewerten und verstehen, welche Auswirkungen sich auf das System ergeben. Es kann z. B. sein, dass der Patch bereits vorhandenen Code beeinträchtigt oder eine Work-Around-Möglichkeit eröffnet. Zudem wird der Patchvorgang Ausfallzeiten verursachen, in denen der Datenbankserver nicht für die Benutzer zur Verfügung steht. Große Unternehmen mit Dutzenden oder sogar hunderten von Datenbanken müssen schließlich eine zeitliche Abfolge für das Patching festlegen und Datenbanken eine Priorität zur Behebung der Schwachstelle zuordnen. Es sollte daher nicht überraschen, dass sich Patching-Vorgänge in vielen Organisationen über Monate hinziehen – typischerweise werden zwischen 6 und 9 Monate benötigt (basierend auf von der Independent Oracle User Group – IOUG* durchgeführten Studien). DBAs, System- und IT-Admins, Entwickler – alle diese Personen spielen beim Patching-Vorgang eine Rolle. Aufgrund dieser Beschränkungen hinsichtlich Ressourcen und Zeit bleiben Server oft noch Monate nach der Freigabe eines Patches angreifbar.

Standardkonten und Konfigurationsparameter, die aus einer produktiv genutzten Datenbank nicht entfernt worden sind, können von einem Angreifer ausgenutzt werden. Ein Angreifer kann versuchen, über ein Standardkonto Zugriff auf die Datenbank zu erlangen. Schwache Audit-Parameter können es einem Angreifer erlauben, Audit-Kontrollen zu umgehen oder Spuren seiner Aktivitäten zu verwischen. Schwache Authentifizierungsschemata ermöglichen es Angreifern, die Identität legitimer Datenbankbenutzer anzunehmen, indem Anmeldeinformationen gestohlen oder anderweitig erhalten werden.

Schwachstellenbewertung und Patching

Um Bedrohungen nicht gepatchter oder angreifbarer Datenbanken zu mindern, müssen zunächst der Sicherheitsstatus der Datenbanken bewertet und alle bekannten Schwachstellen und Sicherheitslücken beseitigt werden. Datenbanken sollten regelmäßig geprüft werden, um Schwachstellen und fehlende Patches zu identifizieren. Der derzeitige Konfigurationsstatus der Datensysteme sollte in Konfigurationsbewertungen klar ersichtlich sein. Diese Bewertungen sollten auch Datenbanken identifizieren, die definierten Konfigurationsrichtlinien nicht entsprechen. Fehlende Sicherheitspatches sollten so schnell wie möglich implementiert werden. Wird eine Schwachstelle erkannt und ist noch kein Patch verfügbar – sei es, weil dieser noch nicht vom Anbieter freigegeben oder bisher noch nicht implementiert wurde –, sollte eine virtuelle Patching-Lösung implementiert werden. Eine derartige Lösung blockiert Versuche, diese Schwachstellen auszunutzen. Die Minimierung des zeitlichen Verwundbarkeitsfensters durch virtuelles Patching schützt die Datenbank vor Angriffsversuchen, bis der Patch implementiert wird.

SecureSphere Vulnerability Assessments und Virtual Patching (Schwachstellenbewertung und virtuelles Patching)

SecureSphere verfügt über eine umfassende Schwachstellen- und Konfigurationsbewertungslösung, die es Benutzern ermöglicht, Systeme regelmäßig zu prüfen, um bekannte Schwachstellen, fehlende Patches und Fehlkonfigurationen zu entdecken. Die Lösung wird über automatische ADC-Updates regelmäßig aktualisiert und verfügt damit immer über die aktuellen Bewertungsrichtlinien und Tests, um die neuesten Schwachstellen zu entdecken. Grundlage dafür sind Untersuchungen, die im Forschungszentrum von Imperva durchgeführt werden – dem Application Defense Center (ADC). SecureSphere ermöglicht es Benutzern zudem, mithilfe virtueller Patches Angriffe auf Schwachstellen abzuwehren, bis der Patch implementiert wird. Die Implementierung von Patches nimmt gemäß einer Studie der Independent Oracle User Group (IOUG)* typischerweise 6 bis 9 Monate in Anspruch. SecureSphere kann das Risiko während der Zeit, die zur Implementierung des Patches benötigt wird, minimieren.

* http://ioug.itconvergence.com/pls/apex/f?p=201:1:4201959220925808

Bedrohung 5 – SQL Injection

Bei einem SQL-Injection-Angriff fügt der Angreifer typischerweise nicht autorisierte Datenbank-Statements in einen angreifbaren SQL-Datenkanal ein. Im Allgemeinen handelt es sich bei den Datenkanälen, die angegriffen werden, um gespeicherte Prozeduren und Eingabeparameter von Web-Applikationen. Die eingefügten Statements werden anschließend zur Datenbank weitergegeben und dort ausgeführt. Mithilfe von SQL Injection können Angreifer uneingeschränkten Zugriff zur gesamten Datenbank erlangen.

Verhinderung von SQL Injection – SQL-Injection-Angriffe lassen sich durch eine Kombination aus drei Techniken effektiv abwehren: Eindringlingserkennung (Intrusion Detection & Prevension- IPS), Zugriffssteuerung auf Abfrageebene (siehe: Missbrauch übermäßiger Berechtigungen) und Ereigniskorrelation. Mithilfe von IPS lassen sich angreifbare gespeicherte Prozeduren oder SQL Injection Strings erkennen. IPS alleine ist jedoch nicht zuverlässig genug, weil SQL Injection Strings viele false-positives erzeugen. Sicherheitsmanager, die sich ausschließlich auf IPS verlassen, würden mit zu vielen „möglichen" SQL-Injection-Alarmmeldungen konfrontiert. Kann eine SQL-Injection-Signatur jedoch mit einer anderen Verletzung wie einer Zugriffskontrollverletzung auf Abfrageebene korreliert werden, lassen sich tatsächliche Angriffe mit extrem hoher Genauigkeit identifizieren. Es ist unwahrscheinlich, dass eine SQL-Injection-Signatur und eine weitere Verletzung während einer normalen Geschäftsoperation gleichzeitig in derselben Abfrage auftreten.

SecureSphere SQL Injection Protection (SQL-Injection-Schutz)

SecureSphere kombiniert die Technologien Dynamic Profiling, IPS und Correlated Attack Validation und kann damit SQL-Injection-Angriffe mit unvergleichlicher Genauigkeit identifizieren.

- Dynamic Profiling bietet eine Zugriffssteuerung auf Abfrageebene. Dazu werden automatisch Profile der normalen Abfragemuster jedes Benutzers und jeder Anwendung erstellt. Jede Abfrage (wie z. B. die eines SQL-Injection-Angriffs), die nicht den normalen Benutzer- oder Anwendungsmustern entspricht, wird unmittelbar identifiziert.
- SecureSphere IPS verfügt über einzigartige Datenbanksignatursammlungen, die speziell darauf ausgelegt sind, angreifbare gespeicherte Prozeduren und SQL Injection Strings zu identifizieren.
- Correlated Attack Validation korreliert Sicherheitsverletzungen mehrerer Ebenen. Durch die Korrelation mehrerer Verletzungen des gleichen Benutzers ist SecureSphere in der Lage, SQL-Injection-Angriffe mit einer Genauigkeit zu erkennen, die mit einer einzigen Erkennungsmerkmal nicht zu erreichen ist. Betrachten Sie z. B. den unten gezeigten SQL-Injection-Angriff über eine gespeicherte Prozedur.

  ```
  exec ctxsys.driload.validate_stmt ('grant dba to scott')
  ```

  In diesem Angriff versucht der Angreifer (scott), sich selbst Datenbankadministratorrechte zu erteilen, indem er eine „grant"-Operation in eine anfällige gespeicherte Prozedur einbindet. SecureSphere würde diesem Angriff je nachdem, ob es sich bei der gespeicherten Prozedur um eine erforderliche Geschäftsfunktion handelt oder nicht, mit einem von zwei Prozessen begegnen.

  #### Anfällige gespeicherte Prozedur nicht erforderlich

  Idealerweise werden anfällige gespeicherte Prozeduren nicht von Anwendern oder Anwendungen genutzt. In diesem Fall, reicht SecureSphere IPS aus, um alle Instanzen dieses Angriffs zutreffend zu identifizieren und optional zu blockieren. In normalen Geschäftsaktivitäten treten derartig komplexe Zeichenstrings (...ctxsys. driload...) nicht auf.

  #### Anfällige gespeicherte Prozedur erforderlich

  In einigen Fällen ist die anfällige gespeicherte Prozedur Teil einer erforderlichen Geschäftsfunktion. Zum Beispiel kann diese Teil einer bestehenden Anwendung sein, deren Änderung nicht mehr möglich ist. In diesem Fall wird SecureSphere zunächst die Sicherheitsmanager auf die Verwendung dieser Funktion aufmerksam machen. Zudem lässt sich optional die Funktion Correlated Attack Validation verwenden, um das Auftreten dieser Signatur mit einer Liste von Benutzern und Anwendungen zu korrelieren, die diese Prozedur nutzen dürfen. Sollte ein nicht autorisierter Nutzer versuchen, die Prozedur zu nutzen, kann SecureSphere eine Warnmeldung erzeugen oder die Anfrage optional blockieren.

Bedrohung 6 – Schwacher Audit-Trail

Es sollte grundlegender Teil jeder Datenbankimplementierung sein, alle vertraulichen und/oder ungewöhnlichen Datenbanktransaktionen automatisch aufzuzeichnen. Schwache Datenbank-Audit-Richtlinien stellen auf vielen Ebenen ein ernsthaftes organisatorisches Risiko dar.

- Regulatorisches Risiko – Organisationen mit schwachen (oder manchmal nicht vorhandenen) Datenbank-Audit-Mechanismen werden zunehmend feststellen, dass sie behördlichen Regulierungsanforderungen nicht entsprechen. Vorschriften wie der Sarbanes-Oxley Act (SOX – ein US-Gesetz zur Prüfung und Dokumentation des internen Kontrollsystems) im Finanzsektor und der Health Insurance Portability and Accountability Act (HIPAA – eine US-Verordnung zum Schutz personenbezogener Gesundheitsdaten) im Gesundheitssektor sind nur zwei Beispiele behördlicher Regulierungen, die eindeutige Audit-Anforderungen an Datenbanken stellen.
- Abschreckung – Ähnlich wie Videokameras, die die Gesichter von Personen aufzeichnen, die eine Bank betreten, dienen Datenbank-Audit-Mechanismen dazu, Angreifer abzuschrecken. Diese wissen, dass Datenbank-Audit-Aufzeichnungen Ermittlern Beweismaterialien an die Hand geben, um Eindringlingen ein Verbrechen nachzuweisen.
- Erkennung und Wiederherstellung – Audit-Mechanismen sind die letzte Verteidigungslinie einer Datenbank. Sollte es einem Angreifer gelingen, andere Abwehrmaßnahmen zu umgehen, können Sicherheitsverletzungen nach ihrem Auftreten durch Audit-Daten identifiziert werden. Die Audit-Daten lassen sich anschließend verwenden, um die Sicherheitsverletzung einem bestimmten Anwender zuzuordnen und/oder das System zu reparieren.

  Datenbanksoftware-Plattformen verfügen in der Regel über grundlegende Audit-Merkmale, diese weisen jedoch oft mehrere Schwachstellen auf, die eine Implementierung beschränken oder ausschließen.
- Fehlende Benutzerüberwachung – Wenn Anwender über Web-Applikationen (wie SAP, Oracle E-Business Suite oder PeopleSoft) auf Datenbanken zugreifen, lassen sich spezifische Benutzeridentitäten mit nativen Audit-Mechanismen nicht identifizieren. In diesem Fall werden sämtliche Benutzeraktivitäten dem Account-Namen der Web-Applikation zugeordnet. Wenn betrügerische Datenbanktransaktionen also in nativen Audit-Logs aufgeführt werden, ist es nicht möglich, diese zum verantwortlichen Anwender zurückzuverfolgen.
- Leistungseinbußen – Native Datenbank-Audit-Mechanismen sind dafür bekannt, erhebliche CPU- und Festplattenressourcen zu belegen. Die mit der Aktivierung von Audit-Merkmalen einhergehenden Leistungseinbußen zwingen viele Organisationen dazu, Audit-Funktionen zurückzunehmen oder gleich vollständig zu deaktivieren.
- Pflichtentrennung – Anwender mit Administrationsrechten (ob legitim oder böswillig beschafft – siehe Erweiterung von Berechtigungen mit dem Ziel des Mißbrauchs) für den Datenbankserver können Audit-Funktionen einfach abschalten, um betrügerische Aktivitäten zu verschleiern. Audit-Pflichten sollten idealerweise von Datenbankadministratoren und der Datenbank-Server-Plattform getrennt werden.
- Begrenzte Granularität – Viele native Audit-Mechanismen zeichnen nicht alle erforderlichen Details auf, um Angriffe zu erkennen, den forensischen Nachweis zu führen sowie Systeme wiederherstellen zu können. Datenbank-Client-Anwendung, Quell-IP-Adressen, Query-Response-Attribute und fehlgeschlagene Abfragen (ein wichtiger Indikator für Ausspähungen vor einem Angriff) werden z. B. von vielen nativen Mechanismen nicht aufgezeichnet.
- Proprietäre Formate – Audit-Mechanismen einzelner Datenbankserver-Plattformen unterscheiden sich voneinander – Oracle-Logs unterscheiden sich von MS-SQL, MS-SQL-Logs unterscheiden sich von Sybase usw. Organisationen mit gemischten Datenbankumgebungen ist es daher nahezu unmöglich, einheitliche, skalierbare Audit-Prozesse über das gesamte Unternehmen hinweg zu implementieren.

Verhinderung schwacher Audit-Funktionen

Qualitativ hochwertige netzwerkbasierte Audit-Appliances weisen nicht die Schwachstellen auf, die mit nativen Audit-Tools verbunden sind.

- Hohe Leistung – Netzwerkbasierte Audit-Appliances arbeiten in Leitungsgeschwindigkeit, ohne die Datenbank-Performance zu beeinträchtigen. Durch eine Auslagerung der Audit-Prozesse auf Netzwerk-Appliances lässt sich die Datenbank-Performance sogar verbessern.
- Pflichtentrennung – Netzwerk-basierte Audit-Appliances sind unabhängig von der Datenbank-Administration, sodass es möglich ist, Audit-Pflichten ordnungsgemäß von administrativen Pflichten zu trennen. Die Netzwerkgeräte sind zudem vom Server selbst unabhängig, sodass sie gegenüber Angriffen zur Erweiterung von Berechtigungen, die von Nicht-Administratoren durchgeführt werden, unempfindlich sind.
- Plattformübergreifendes Auditing – Netzwerk-Audit-Appliances unterstützen im Allgemeinen alle führenden Datenbank-Plattformen und ermöglichen eine Implementierung einheitlicher Standards und zentralisierter Audit-Funktionen über große heterogene Datenbankumgebungen hinweg. Zusammengenommen können diese Attribute Datenbankserverkosten, Load-Balancing-Anforderungen und administrative Kosten senken. Und sie sorgen außerdem für eine höhere Sicherheit.

SecureSphere Audit-Funktionen

Zusätzlich zu den oben beschriebenen allgemeinen Vorteilen netzwerkbasierter Audit-Appliances bietet SecureSphere eine Reihe einzigartiger Audit-Funktionen, die sich von alternativen Ansätzen stark abheben.

- Universal User Tracking ermöglicht es, Vorgänge einzelnen Anwendern zuzuordnen – selbst, wenn sie über kommerzielle (Oracle, SAP, PeopleSoft usw.) oder benutzerdefinierte Web-Applikationen auf die Datenbank zugreifen. Um Benutzernamen von Web-Applikationen identifizieren zu können, erfasst eine speziell dafür entwickelte SecureSphere-Schnittstelle die Anmeldeinformationen der Applikation, verfolgt anschließende Webbenutzer-Sitzungen und korreliert diese mit Datenbank-Transaktionen. Die daraus erstellten Audit-Logs enthalten die eindeutigen Benutzernamen der Web-Applikation.
- Granular Transaction Tracking unterstützt Betrugserkennung, forensische und wiederherstellende Funktionen. Log-Details enthalten z. B. den Namen der Quellapplikation, den vollständigen Query-Text, Query-Response-Attribute, das Quellbetriebssystem, den Quell-Host-Namen und viele weitere Details.
- Distributed Audit Architecture ermöglicht eine granulare Nachverfolgung von Transaktionen (s. oben), lässt sich dabei jedoch trotzdem über große Rechenzentren hinweg skalieren. Die Architektur weist den verteilten SecureSphere Gateway-Appliances die benötigten Storage- und Rechenressourcen zu. Der SecureSphere Management Server bietet Audit-Personal eine einheitliche Ansicht des Rechenzentrums. Der Management Server ermöglicht es, viele Gateways effektiv so zu verwalten, als ob es sich aus der Sichtweise des Audit-Personals um ein einziges Gateway handelt. In alternativen Lösungen wird entweder empfohlen, nur ein eingeschränktes Transaktions-Logging durchzuführen, oder Administratoren sind dazu gezwungen, viele verteilte Geräte unabhängig voneinander zu verwalten.
- External Data Archive Funktionen automatisieren die Langzeitarchivierung von Daten. SecureSphere lässt sich so konfigurieren, dass Daten in regelmäßigen Abständen auf externen Massenspeichersystemen archiviert werden. Daten können vor der Archivierung optional komprimiert, verschlüsselt und mit Signatur versehen werden.
- Integrated Graphical Reporting stellt Administratoren einen flexiblen und leicht verständlichen Mechanismus zur Verfügung, um den Audit-Trail zu analysieren. Die Lösung enthält vorkonfigurierte Reports, die Antworten auf häufige Audit-Fragen geben. Zudem lassen sich individuelle Reports erstellen, um spezifischen Anforderungen des Unternehmens gerecht zu werden. SecureSphere Audit-Daten lassen sich alternativ auch mit einer ODBC-konformen externen Reporting-Lösung analysieren.
- Local Console Activity Auditing wird über den SecureSphere Database Agent bereitgestellt. Bei dem SecureSphere Database Agent handelt es sich um einen schlanken Host-Agenten, der auf dem Datenbankserver installiert wird, um lokale Aktivitäten des Datenbankadministrators zu überwachen. SecureSphere Database Agent und SecureSphere Gateways bieten zusammen einen umfassenden Audit-Trail, der die Datenbankperformance nur minimal beeinträchtigt und in einigen Fällen sogar verbessert.

Bedrohung 7 – Denial of Service

Denial of Service (DoS) ist die Bezeichnung für eine allgemeine Angriffskategorie, in der Angriffe dazu führen, dass berechtigten Anwendern der Zugriff auf Netzwerk-Applikationen und Daten verweigert wird. Denial of Service (DoS)-Zustände lassen sich über viele verschiedene Techniken hervorrufen – viele dieser Techniken nutzen dabei die zuvor bereits erwähnten Schwachstellen aus. Ein DoS lässt sich z. B. verursachen, indem Schwachstellen der Datenbankplattform genutzt werden, um einen Server zum Absturz zu bringen. Weitere verbreitete DoS-Techniken sind die Kompromittierung von Daten, eine Überflutung des Netzwerks mit Netzwerkverkehr und eine Überlastung von Serverressourcen (Speicher, CPU usw.). Ressourcenüberlastungen treten besonders häufig in Datenbankumgebungen auf. Die Motivationen, die hinter DoS-Angriffen stecken, sind ähnlich vielfältig. DoS-Angriffe kommen häufig in Zusammenhang mit Erpressungsversuchen vor, in denen ein Remote-Angriffs-Server die Datenbank wiederholt zum Absturz bringt, bis das Opfer Gelder auf ein internationales Bankkonto überweist. In anderen Fällen lassen sich DoS-Zustände auf eine Wurm-Infektion zurückführen. Unabhängig von der Ursache stellen DoS-Angriffe für viele Organisationen eine ernsthafte Bedrohung dar.

Verhinderung von Denial of Service

Ein Schutz vor DoS erfordert Maßnahmen auf verschiedenen Ebenen. Es müssen die Netzwerk-, die Anwendungs- und die Datenbankebene geschützt werden. In diesem Dokument geht es v. a. um datenbankspezifische Schutzmechanismen. In diesem datenbankspezifischen Kontext werden die Implementierung einer Verbindungsgeschwindigkeitskontrolle, eines IPS, einer Zugriffssteuerung auf Abfrageebene und einer Kontrolle der Antwortzeiten empfohlen.

SecureSphere DoS-Schutzfunktionen

- Connection Controls verhindert eine Überlastung von Serverressourcen, indem Verbindungs- und Abfragegeschwindigkeiten sowie andere Variablen für jeden Datenbankbenutzer begrenzt werden.
- IPS und Protocol Validation hindern Angreifer daran, bekannte Schwachstellen auszunutzen, um DoS-Zustände zu erzeugen. Ein Buffer Overflow ist z. B. eine häufige Plattformschwachstelle, die ausgenutzt werden kann, um Datenbankserver zum Absturz zu bringen. Umfassendere Beschreibungen der SecureSphere IPS- und Validierungstechnologien für Datenbankkommunikationsprotokolle finden Sie in den Abschnitten „Berechtigungserweiterungen zum Ziel des Mißbrauchs“ und „Schwachstellen von Datenbankkommunikationsprotokollen“ in diesem Dokument.
- Dynamic Profiling stellt automatisch eine Zugriffssteuerung auf Abfrageebene bereit, um nicht autorisierte Abfragen, die zu einem DoS führen können, zu erkennen. DoS-Angriffe, die z. B. auf Plattformschwachstellen abzielen, würden mit hoher Wahrscheinlichkeit sowohl IPS- als auch Dynamic-Profile-Verletzungen auslösen. SecureSphere korreliert diese Verletzungen und erreicht damit eine unvergleichliche Genauigkeit. Eine umfassendere Beschreibung von Dynamic Profiling finden Sie im Abschnitt „Missbrauch übermäßiger Berechtigungen“ in diesem Dokument.
- Antwortzeiten – Datenbank-DoS-Angriffe, die auf eine Überlastung von Serverressourcen abzielen, führen zu verzögerten Datenbank-Antworten. Die SecureSphere Response-Timing-Funktion erkennt Verzögerungen von Antworten auf einzelne Abfragen und des gesamten Systems.

Bedrohung 8 – Schwachstellen von Datenbankkommunikationsprotokollen

In Datenbankkommunikationsprotokollen werden immer mehr Sicherheitsschwachstellen entdeckt – betroffen sind alle Datenbankanbieter. Vier der sieben Sicherheits-Fixes in den letzten beiden IBM DB2 FixPacks betrafen Protokollschwachstellen1. Und auch 11 der 23 Datenbankschwachstellen, die im letzten vierteljährlichen Patch von Oracle behoben wurden, bezogen sich auf Protokolle. Betrügerische Aktivitäten, die auf diese Schwachstellen abzielen, reichen von nicht autorisierten Zugriffen auf Daten bis zu Datenkompromittierungen und DoS-Angriffen. Der Wurm SQL Slammer2 hat z. B. eine Sicherheitslücke im Microsoft SQL Server-Protokoll genutzt, um ein Denial of Service auszulösen. Noch schlimmer wird die Angelegenheit dadurch, dass im nativen Audit-Trail keine Aufzeichnungen dieser betrügerischen Aktivitäten vorhanden sind, weil native Datenbank-Audit-Mechanismen Protokolloperationen nicht abdecken. Verhinderung von Angriffen auf Datenbankkommunikationsprotokolle – Angriffe auf Datenbankkommunikationsprotokolle lassen sich mit einer Technologie abwehren, die als Protokollvalidierung bezeichnet wird. Die Protokollvalidierungstechnologie führt im Wesentlichen ein Parsing (eine Syntaxanalyse) des Datenbank-Traffics durch und vergleicht diese mit Erwartungswerten. Sollte der Datenverkehr nicht mit den Erwartungswerten übereinstimmen, werden Alarmmeldungen ausgelöst oder der Datenverkehr blockiert.

SecureSphere Database Communication Protocol Validation (Validierung von Datenbankkommunikationsprotokollen)

SecureSphere Database Communication Protocol Validation prüft den Netzwerkverkehr und schützt gegen Protokollbedrohungen. Dazu werden Datenbankkommunikationsprotokolle in Echtzeit mit erwarteten Protokollstrukturen abgeglichen. Keine andere Sicherheits- oder Audit-Lösung für Datenbanken bietet eine derartige Funktion. Die Funktion basiert auf den laufenden Forschungen des Imperva Application Defense Centers (ADC) über proprietäre Datenbankkommunikationsprotokolle und -schwachstellen. Datenbank- und Anwendungsanbieter – darunter Oracle, Microsoft und IBM – haben dem ADC die Entdeckung ernsthafter Schwachstellen und Bedrohungsminderungstechniken zu verdanken, die ihre Produkte sicherer gemacht haben. Imperva ist dank dieser Forschungen in der Lage, ein unvergleichliches Wissen über Protokolle in SecureSphere zu integrieren.

Bedrohung 9 – Nicht autorisierte Kopien vertraulicher Daten

Viele Unternehmen haben Schwierigkeiten damit, alle ihre Datenbanken ordnungsgemäß zu erfassen und zu warten. So kann es passieren, dass neue Datenbanken erstellt werden, ohne dass das Sicherheitsteam von diesen Datenbanken weiß. Wenn anschließend vertrauliche Daten in diese Datenbanken kopiert werden, sind diese einem Sicherheitsrisiko ausgesetzt, sofern die erforderlichen Kontrollen nicht implementiert werden. Derartige „verborgene" Datenbanken können potenziell vertrauliche Informationen wie Transaktions-, Kunden- und Mitarbeiterdetails enthalten. Wenn die verantwortlichen Personen jedoch kein Wissen über die Inhalte der Datenbanken haben, lässt sich nur sehr schwierig sicherstellen, dass geeignete Kontrollen implementiert sind. Unabhängig davon, ob dies absichtlich geschieht oder nicht: Vertrauliche Daten sind in diesen Fällen einem illegalen Zugriff durch Mitarbeiter oder Hacker ausgesetzt. Ein weiteres Beispiel sind alte Datenbanken, die vergessen und nicht in die Bewertung einbezogen wurden. Ohne eine Verwaltung dieser Datenbanken können Daten neugierigen Blicken von Personen ausgesetzt sein, die keinen Zugriff auf diese Daten haben sollten.

Identifizierung – Nicht autorisierte Kopien vertraulicher Daten

Um zu jedem Zeitpunkt über eine genaue Inventarliste ihrer Datenbanken und Speicherorte vertraulicher Daten zu verfügen, sollten Organisationen alle Datenbanken im Netzwerk, die vertrauliche Daten enthalten, identifizieren. In einem zweiten Schritt sollte erfasst werden, welche Arten von vertraulichen/klassifizierten Daten sich jeweils in den Datenbankobjekten befinden. Bei der Klassifizierung der Daten ergeben sich zwei große Herausforderungen: Zum einen müssen vertrauliche Informationen innerhalb der Vielzahl großer Tabellen aufgefunden werden. Zum anderen müssen Datenkombinationen von Daten identifiziert werden, die für sich alleine genommen unproblematisch sind, aber in Kombination mit anderen Daten als vertrauliche Informationen einzustufen sind. Nur so können vertrauliche Informationen angemessen geschützt werden. Sobald eine genaue Inventarliste der Datenbanken und Speicherorte vertraulicher Daten vorhanden ist, sollten anhand der Datenzugriffsrichtlinien des Unternehmens die entsprechenden Zugriffskontrollen eingerichtet werden.

SecureSphere Erkennung und Klassifizierung

SecureSphere ermöglicht es Anwendern, automatische Netzwerkscans zu planen, die eine vollständige Inventur aller Datenbanken zu liefern. Dabei werden auch neue oder geänderte Datenbanken identifiziert. Dies ist hilfreich, um „fragwürdige" Datenbanken zu entdecken. Anwender können anschließend einen Scan der Inhalte der Datenbank initiieren, um Objekte mit vertraulichen Daten zu identifizieren. SecureSphere erkennt bereits in der Voreinstellung Datentypen wie Kreditkarten- und Sozialversicherungsnummern (weitere Datentypen lassen sich hinzufügen). Um eine false-positive Zuordnung zu vermeiden, werden Validierungsalgorithmen eingesetzt. Zudem werden neue Instanzen vertraulicher/klassifizierter Daten hervorgehoben.

Bedrohung 10 – Unzureichend geschützte Backup-Daten

Speichermedien mit Datenbank-Backups sind Angriffen oft völlig ungeschützt ausgesetzt. In der Vergangenheit wurden daher immer wieder Bänder und Festplatten von Datenbank-Backups gestohlen, was zu ernsthaften Sicherheitsverletzungen geführt hat.

Verhinderung unzureichend geschützter Backup-Daten

Sämtliche Datenbank-Backups sollten verschlüsselt werden. Von einigen Anbietern ist sogar der Vorschlag zu hören, dass zukünftige DBMS-Produkte gar keine Erstellung unverschlüsselter Backups mehr unterstützen sollten. Oft wird auch vorgeschlagen, Informationen produktiv eingesetzter Datenbanken online zu verschlüsseln. Einbußen hinsichtlich der Performance und die Verwaltung von Verschlüsselungscodes machen derartige Lösungen jedoch oft unpraktisch, sodass diese nur eine unzureichende Alternative zu den oben beschriebenen granularen Zugangsberechtigungskontrollen darstellen.

Zusammenfassung

Datenbankinformationen sind zwar vielen verschiedenen Angriffen ausgesetzt, es ist jedoch möglich, Risiken durch eine Konzentration auf die wichtigsten Bedrohungen erheblich zu reduzieren. Wenn es Organisationen gelingt, den oben beschriebenen zehn wichtigsten Bedrohungen zu begegnen, erfüllen sie damit die Compliance- und Risikominimierungsanforderungen der meisten regulierten Branchen in der Welt.

ÜBER IMPERVA

Imperva ist der weltweite Marktführer für Datensicherheit. Tausende weltweit führender Unternehmen, Regierungsorganisationen und Serviceprovider verlassen sich auf Lösungen von Imperva, um Datenzugriffsverletzungen zu verhindern, Compliance-Anforderungen gerecht zu werden und Datenrisiken zu kontrollieren.

Imperva SecureSphere ist die marktführende Datensicherheits- und Compliance-Lösung. SecureSphere schützt sensible Daten vor Hackern und böswilligen Insidern, bietet eine schnelle und kosteneffektive Einhaltung regulatorischer Compliance-Anforderungen und etabliert einen reproduzierbaren Prozess zur Minderung von Datenrisiken.

Fuer weitere Informationen besuchen Sie http://www.imperva.de

Imperva
Herriotstrasse 1
60528 Frankfurt / Main
Germany
Tel: +49 69 67733 276
Fax: +49 69 67733 200

www.imperva.de