Grundlegende, ganzheitliche Methodiken zur Absicherung von Datenbanken unter Einhaltung der Datenschutzgesetze

Kathegorie
SQL Server, Software, WHY_INVESTIGATOR

Jeanne
Renard

Dieser Artikel befasst sich mit grundlegenden Methodiken zur Absicherung Deiner Datenbank unter Einhaltung der aktuellen Datenschutzgesetze.
In Zeiten von Cyberangriffen und (digitalem) Datenmissbrauch, aus Neugierde oder finanzieller Absicht, ist diese Absicherung obligatorisch für die Geheimhaltung unserer Kunden- und unternehmensinternen Daten! Egal ob wir unsere Datenbanken mit Oracle, Microsoft SQL Server, IBM DB2 oder Sybase speichern – wir helfen Dir gerne bei der Verschlüsselung und zeigen Dir hier erste Tipps und Tricks auf, wie Du die gesetzliche Vorgaben des Datenschutzes wie SOX, PCI-DSS oder GLBA einhalten kannst. Diese neue Art der Absicherung (bislang kennen wir ausschließlich Firewalls, IDS/IPS, Antivirus usw.) gewährleistet die Informationssicherheit und schließt damit alle Sicherheitslücken und verhindert den Eingriff von unbefugten Usern.

Übrigens:
mithilfe des WHY_INVESTIGATORs kannst Du etwa alle Bewegungen auf Deiner SQL Server Datenbank nachvollziehen und in einfachen Schritten fremde User und fälschliche Bewegungen automatisiert nachvollziehen!
Motivation für diesen Beitrag sind die steigenden Zahlen von Hackerangriffen. Schon 2008 sind die SQLInjektionsangriffe um 134% gestiegen, das entspricht einem Anstieg auf mehrere hunderttausend Angriffe pro Tag. Außerdem liegen aktuell vermutlich mehr als die Hälfte der Unternehmen beim Einspielen von Datenbanksicherheitspatches im Verzug, vor allem bei Webanwendungen.

Mainzer Datenfabrik GmbH
Rotterdamer Platz 2, 55120 Mainz
info@madafa.de
madafa.de
+49 6131 3331612

Wie erkennen wir die Schwachstellen, die abgesichert werden müssen?

Allen voran solltest Du als DBA ein gutes und sensibles Auge für Deine Datenbanken und (deren) Daten sowie Benutzer und deren Zugriffsrechte haben! All diese Variablen sind flexibel und genau deswegen kann sich der Standort und Erkennungsprozess fortlaufend ändern. Hier eignet sich ein automatisierter Erkennungsprozess, um zu verhindern, dass größere "Schäden" wie etwa die Preisgabe vertraulicher Informationen auftreten.

Alle Daten und alle Benutzer sind individuell zu betrachten und behandeln. Benutzer müssen **authentifiziert** werden und der DBA sollte über jeden einzelnen Benutzer, der Rechenschaft ablegen muss, Bescheid wissen, bevor die Automatisierung beginnt. Der DBA ist außerdem angehalten, auf die Einschränkung der Datenzugriffe zu achten und Zugriffsrechte minimal zu halten – selbst bei den am höchsten privilegierten Datenbankbenutzern. Die **Zugriffskontrolle** ist also mit die wichtigste Aufgabe des **Bereichtigungsmanagements**. Eine Dokumentation von Berechtigungsberichten (User High Attestation Reports) und eine regelmäßige, formelle Überprüfung des formellen Auditprozesses bleibt dabei nicht aus.
Empfehlenswert für die Absicherung unserer Datenbank ist neben dem Entfernen von Funktionen, der genauen Überprüfung der Benutzer und Optionen, die nicht genutzt werden, auch die Verwendung von Tools zur Gefahrenbegrenzung, auf die wir im letzten Abschnitt genauer eingehen.

Wie erkennen wir Schwachstellen, die wirklich Schwachstellen sind?

Sicherheitslücken (Vulnerabilities) in der Struktur Deiner Datenbank sind oftmalig der Grund für Hackerangriffe, da diese die Möglichkeiten des Eindringens in die Datenbank sofort erkennen können. Um diese Sicherheitslücken unter Kontrolle zu haben und Dich zukünftig gegen Angriffe zu wappnen, solltest Du die Konfiguration Deiner Datenbank genau prüfen.
Hierzu stelle Dir folgende Fragen:

1. Wie ist die Datenbank auf dem aktuellen Betriebssystem installiert?
2. Welche Zugriffsrechte haben die Datenbankkonfigurationsdateien?
3. Welche Optionen für die Anzahl fehlgeschlagener Logins bis zur Accountsperrung sind eingestellt?
4. Welche Zugriffsrechte habe ich für kritische Tabellen an welche Benutzer freigegeben?
5. Kann ich aktuell bekannte Schwachstellen erkennen und sofort lösen?
6. Befindet sich die Datenbank auf dem aktuellsten Patch-Stand?

Traditionelle **Schwachstellenscanner** für Netzwerke gibt es nicht, da jede Datenbankstruktur individuell ist und es keine "Rezeptur" für die Erkennung gibt, allerdings gibt es Automatisierungs-Tools, auf die wir im Verlauf dieses Artikels eingehen.

Überprüfung Deiner Datenbank

Für alle Datenbankaktivitäten sollten sichere, nicht anfechtbare Prüfprotokolle angelegt werden, um die Sicherheit und Datenintegrität zu gewährleisten und um sensible Daten zu sichern. Dies ist für die Erfüllung gesetzlicher Vorgaben notwendig, aber auch besondere Prüfprotokolle für etwa forensische Untersuchungen sind vorstellbar.
Es gibt die Möglichkeit, Datenbanken manuell zu überwachen, etwa mit traditionellen, nativen Datenbankprotokollfunktionen. Allerdings sind hier die Kosten sehr hoch und auch der Aufwand der Mitarbeiter fast schon unnötig, auch im Hinblick auf das Preis-Leistungs-Verhältnis. Es gibt defitinitiv einfachere, kostengünstigere und vor allem auch sichere Varianten der Kontrolle. Durch manuelle Eingriffe ist das Risiko einer Manipulation durch DBAs (Datenbankadministratoren/Datenbankadministratorinnen) höher.
Die neusten DAM-Lösungen mit differenzierter, Datenbankmanagementsystem(DBMS)-unabhängiger Überprüfung, bieten eine Regulierung der Betriebskosten durch Automatisierung, zentralisierte und DBMS-übergreifende Regelungen und Audit-Depots, Filterung und Komprimierung.

Mainzer Datenfabrik GmbH
Rotterdamer Platz 2, 55120 Mainz
info@madafa.de
madafa.de
+49 6131 3331612

Tools zur Gefahrenbegrenzung Deiner Datenbank

Wie bereits erwähnt ist eine Echtzeitüberwachung der Schlüssel zur Gefahrenbegrenzung, denn dadurch können Eindringversuche und Fremdeinwirkung direkt erkannt werden.

Database Activity Monitoring (DAM) etwa kann ungewöhnliche Zugriffsmuster erkennen, die auf einen SQL-Injektionsangriff, unberechtigte Änderungen an Finanzdaten, die Gewährung größerer Accountberechtigungen und Konfigurationsänderungen durch SQL-Befehle hindeuten. Die Überwachung der Benutzer ist Voraussetzung für Data-Governance-Gesetze wie SOX und Datenschutzverordnungen wie PCI DSS, die es zu berücksichtigen gibt.

DAM eignet sich auch zur **Schwachstellenbewertung**, um Verhaltensschwachstellen genau zu erkennen und bei der gemeinsamen Nutzung von Privilegien auffällige Benutzer differenzieren zu können, etwa durch eine übermäßig hohe Zahl fehlgeschlagener Datenbankanmeldungen. Diese DAM-Technologien ermöglichen die Überwachung der Anwendungsschicht, sodass auch ein Betruf über mehrschichtige Anwendungen wie PeopleSoft, SAP und Oracle e-Business Suite statt nur über Direktverbindungen zur Datenbank erkennbar ist.

Mit Hilfe einer **Verschlüsselung** können sensible Daten geschützt und unlesbar gemacht werden, damit unberechtigte Nutzer auf keinen Fall Zugang zu diesen Daten hat. Schon bei der Übertragung der Daten sollten diese geschützt werden, damit der Angreifer nicht auf die Netzwerkschicht zugreifen können.

Auch hier möchten wir erneut auf den WHY_INVESTIGATOR aufmerksam machen, der alle Bewegungen auf Deiner Datenbank dokumentieren und speichern kann, damit Du jede Veränderung nachvollziehen kannst. Dieses Tool eignet etwa, um Momentaufnahmen Deiner Konfiguration zu speichern und Warnmeldungen auszugeben, sobald eine kritische Änderung erfolgt ist, die die Sicherheit Deiner Datenbank beeinträchtigen könnte.

Mainzer Datenfabrik GmbH
Rotterdamer Platz 2, 55120 Mainz
info@madafa.de
madafa.de
+49 6131 3331612