Best Practices zur Datenbanksicherheit

Die Datenbanksicherheit wird in vielen Unternehmen immer noch recht stiefmütterlich behandelt – und das obwohl heute eine solide Datenbank von zentraler Bedeutung für eine gut organisierte und konsolidierte IT-Landschaft ist und nicht autorisierte Zugriffe leicht zu einem Abfluss von Informationen oder zu Missbrauch und Löschung wichtiger Daten führen können mit häufig existenzbedrohenden Auswirkungen für das Unternehmen.

Dabei lässt sich auf der Basis der nachfolgenden Best Practices zur Datenbanksicherheit, die eine ganzheitliche Methodik bilden, recht einfach ein durchgängiges Sicherheitskonzept zum Schutz sensitiver Daten in Datenbanken aufbauen.

1. Entdeckung

Da sich nur das absichern lässt, was auch bekannt ist, wird eine umfassende Abbildung der sensiblen Assets wie Datenbankinstanzen in der Produktions-, Referenz-, Test-, Abnahme- sowie Staging-Umgebung sowie der sensiblen Daten innerhalb dieser Datenbanken benötigt.

2. Schwachstellen- und Konfigurationsbewertung

Mittels spezialisierter Tools lassen sich Datenbanken nach bekannten Schwachstellen und Konfigurationsmängeln einfach durchsuchen, um so einen ersten Status zur Sicherheit der eingesetzten Datenbanksysteme sowie Handlungsempfehlungen als ersten Schritt zur Absicherung und Implementierung eines Mindestsicherheitsstandards der Datenbank zu erhalten.

Sowohl diese Handlungsempfehlungen als auch herstellerspezifische Empfehlungen zur Datenbanksicherheit sollten nun Bestandteil von konkreten Sicherheitsanforderungen für Datenbanksysteme im Unternehmen werden.

3. Absicherung – Systemhärtung

Durch die Umsetzung der konkreten Sicherheitsanforderungen für Datenbanksysteme kann nun unter Berücksichtigung der vorliegenden Systemumgebung durch Härtung der Datenbanksysteme die Sicherheit des Unternehmens mit recht wenig Ressourcenaufwand sichergestellt werden.

4. Änderungsaudit – Security Reporting

Nach der Erstellung einer abgesicherten Konfiguration ist es nun ratsam diese in regelmäßigen Abständen zu überprüfen, um sicherzustellen, dass sie im Laufe der Zeit nicht von der sicheren Konfiguration abweicht.

Das Security Reporting stellt hierzu technische Informationen über den Sicherheits- und Compliance-Status zur Verfügung und generiert Warnmeldungen, sobald Änderungen erfolgt sind, welche die Sicherheit der Datenbanken beeinträchtigen könnte.

5. Audit der Datenbankaktivität

Neben den bereits beschriebenen Maßnahmen zur Datenbanksicherheit, sollte auch nicht auf das Audit der Datenbankaktivität („Database Activity Monitoring (DAM)“) zur Gefahrenbegrenzung verzichtet werden, wodurch Eindringversuche und Datenmissbrauch zeitnah erkannt werden können.

Zu allen Datenbankaktivitäten, mit Auswirkungen auf Sicherheit und Datenintegrität oder bei denen sensible Daten angezeigt werden, ist die Erstellung von sicheren und nicht anfechtbaren Prüfprotokollen notwendig. Diese differenzierten Prüfprotokolle sind neben ihrer Schlüsselrolle für die Erfüllung gesetzlicher Vorgaben auch für forensische Untersuchungen sehr hilfreich.

6. Trennung von Zuständigkeiten

Zentrales Thema eines Sicherheitskonzepts ist die Trennung von Zuständigkeiten für Aufgaben und Tätigkeiten (“Segregation of Duties”). Dies gilt insbesondere für Aufgaben, die umfassende Privilegien benötigen. Z.B. sollte ein DBA die Datenbank, aber nicht die Daten administrieren können. Solch eine klare Trennung zwischen Infrastrukturbereitstellung/-administration und der Verarbeitung der Daten dient der Verhinderung von Rechtemissbrauch.

7. Authentifizierung, Autorisierung, Zugriffskontrolle und Berechtigungsmanagement

Authentifizierung (Identifizierung und Legitimierung des Zugriffs) und Autorisierung (Festlegung und Überprüfung der Zugriffsrechte) sind sicherzustellen. Im Rahmen der Zugriffskontrolle als integraler Bestandteil der Datenbanksicherheit sollten die per Autorisierung vergebenen und überprüften grundlegenden Lese- und Schreibberechtigungen auf Daten durch zusätzliche Mechanismen weiter eingeschränkt werden.

8. Verschlüsselung der Daten

Damit kein Angreifer von außen unberechtigt auf sensible Daten zugreifen kann, sind diese Daten mittels Verschlüsselung unlesbar zu machen. Hierzu gehört die Verschlüsselung der Datenübertragung zwischen Datenbank-Client und Datenbank und zwischen Datenbanken untereinander, um zu verhindern, dass der Angreifer auf der Netzwerkschicht mit lauschen kann sowie die Verschlüsselung der Daten auf Mediendateien.

9. Anonymisierung von Daten

In Test- und Abnahmeumgebungen muss häufig mit den gleichen Datenbeständen wie in der Produktion gearbeitet werden. Solche Daten sind unbedingt zu anonymisieren, indem sie unwiderruflich verändert werden, damit sie in solchen Umgebungen genutzt werden dürfen, ohne dass noch zusätzliche Schutzmaßnahmen notwendig wären. Das gleiche gilt für den Fall, dass aus vorgelagerten Prozessen sensitive Daten bezogen, aber für die Weiterverarbeitung nicht unbedingt benötigt werden.

10. Rückgriff und Wiederherstellung von historischen Daten

Häufig ist es notwendig, darüber Auskunft geben zu können, welchen Wert ein Datenfeld zu einem bestimmten Zeitpunkt z.B. vor einer Datenänderung gehabt hat. Dieses Erfordernis gilt häufig in Bereichen mit rechtlicher Relevanz. Der Zugriff auf solche historischen Daten kann mit gewissem Entwicklungsaufwand innerhalb von Applikationen realisiert oder mittels entsprechender Datenbankmechanismen genutzt werden.

11. Schutz vor Angriffen durch SQL-Injection

Insbesondere im Rahmen von Web-Applikationen muss dem Schutz vor Angriffen auf die Datenbank durch SQL-Injection ein besonderes Augenmerk geschenkt werden. Da in vielen unsicheren Anwendungen die über Eingabemasken eingegebenen Zeichenketten zusammen mit SQL-Befehlen lediglich zu kompletten SQL-Statements zusammengesetzt und direkt auf der Datenbank ausgeführt werden, können Angreifer durch bestimmte Eingaben das resultierende SQL-Statement so manipulieren, dass unerwünschter Code in den Datenbanken ausgeführt wird.

Links zu den angesprochenen Begriffen:

- Begriff Authentifizierung
- Begriff Autorisierung
- Abgrenzung der Begriffe Anonymisierung und Pseudonymisierung

Weitere Informationen zum Thema Datenbanksicherheit finden Sie unter:

Umfang der Datenbanksicherheit: http://www.consulting.edilog.de/datenbanksicherheit.html
Datenbanksicherheit im IT-eXpert NETWORK: http://www.it-experts.edilog.de/leistungsportfolio/datenbanksicherheit/

Haben Sie noch Fragen? Dann rufen Sie uns doch einfach an unter **0221/6903870** oder senden Sie eine E-Mail mit Ihren Wünschen an: **consulting@edilog.de**

Impressum

Datum: November 2013
Autor: Jürgen Esser
Kontakt:
consulting@edilog.de
www.consulting.edilog.de