Umfang der Datenbanksicherheit

Hintergründe zu Pro und Contra von Maßnahmen zur Datenbanksicherheit

Debatten zur Sicherheit und Standardisierung werden schon immer geführt und dienen auch der Eindämmung des Wildwuchses. Leider werden diese Themen innerhalb der Unternehmen oft mit Einschränkungen und Behinderungen in Verbindung gebracht. In der Diskussion um Cloud- und Mobile-Computing rückt neben der Standardisierungsdebatte auch das Thema Sicherheit wieder in den Mittelpunkt. Obwohl Sicherheit in den meisten Unternehmen intensiv diskutiert wird, hapert es immer noch an der Umsetzung und der nachfolgenden Überprüfung. Selten werden als notwendig erachtete Anforderungen konsequent durch Maßnahmen umgesetzt, obwohl die Realisierung eines entsprechenden Sicherheitskonzeptes von allen Verantwortlichen grundsätzlich befürwortet wird.

Die wesentlichen Ursachen der zögerlichen Implementierung von Datenbanksicherheit lauten:

1. Relevante Vorschriften und Regularien sowie die daraus resultierenden Anforderungen an die Datenbanksicherheit sind häufig nicht bekannt.
2. Dem mit den Sicherheitsmaßnahmen einher gehende finanzielle und personelle Aufwand stehen keine direkten Einsparungen oder Verbesserungen im Betrieb gegenüber und ein Return-on-Investment ist kaum berechenbar. Somit sind die anfallenden Kosten sehr schwer zu rechtfertigen.
3. Häufig sind Sicherheitsmaßnahmen mit Einschränkungen bei der Nutzung und Administration verbunden mit der Folge, dass bei vielen konkreten Maßnahmen die Akzeptanz der betroffenen Personen fehlt.

Grundsätzlich beginnen Sicherheitsanforderungen und Schutzbedürfnis bei den Daten

Obwohl Datenbankadministratoren und Applikationsverantwortliche die Notwendigkeit von Sicherheitsmaßnahmen nie grundsätzlich verneinen werden und in allgemeinen Diskussionen sogar oft sehr hohe Anforderungen an die Datenbanksicherheit stellen, reduzieren sie doch ihre Anforderungen spätestens dann, wenn Aufwände und Kosten thematisiert werden.

Zur Umsetzung einen sinnvollen Sicherheitsniveaus ist zu allererst eine Aufstellung erforderlich, welche Daten in welchen Systemen überhaupt vorhanden sind und welche Schutzbedürfnisse mit der Verarbeitung und Speicherung dieser Daten verbunden sind. Relevante Gesetze und Regularien (z.B. für personenbezogenen Daten Bundesdatenschutzgesetz (BDSG), für Kreditdaten PCI-DSS, für Banken und Finanzinstitute Basel II/III) müssen hierzu bekannt sein und ihre Relevanz muss zunächst für die in den jeweiligen Systemen vorliegenden Daten geprüft werden.

Somit ist der erste Schritt zum Ausbau der Datenbanksicherheit eine Sicherheits-Klassifizierung der Daten nach Verfügbarkeit, Vertraulichkeit, Integrität (Korrektheit) und Nachweisbarkeit der Informationen. Sehr hilfreich für die Kategorisierung und Klassifizierung der Daten sind die IT-Grundschutz Unterlagen und Tools vom Bundesamt für Sicherheit in der Informationstechnik (BSI).

Im Rahmen dieser Arbeiten werden Daten den genannten Kategorien entsprechend ihrer Relevanz zugeordnet. Auf Basis dieser Klassifizierung lassen sich nun die notwendigen Schutzmaßnahmen ableiten und geeignete Sicherheits-Lösungen auswählen.

Ist die Datenbanksicherheit nur ein Kostenfaktor ohne jeden finanziellen Nutzen?

Zunächst einmal ist Sicherheit ein Kostenfaktor und abgesehen von einzelnen Spezialfällen lassen sich weder Einsparungen noch Effektivitätssteigerungen erzielen.

In Analogie zu einer Versicherung dienen Sicherheitsmaßnahmen lediglich der Absicherung für den Schadenfall und die anfallenden Kosten für die Sicherheit müssen immer im Verhältnis zur Eintrittswahrscheinlichkeit und möglichen Schadenshöhe betrachtet werden.

So lange kein Angriff erfolgt und auch niemand außerhalb seiner Berechtigungen Zugriff auf Systeme ausübt, wären auch keine umfangreichen Sicherheitsmaßnahmen notwendig. Kommt es jedoch zu einem Schadensfall, übersteigen in der Regel die Kosten ein Vielfaches der für die Sicherheitsmaßnahmen angefallen Kosten. Hinzu kommt, dass bei Verstößen gegen Regularien zudem noch hohe Strafen gegen die Geschäftsführung verhängt werden können und ein Sicherheits-Schadensfall im Extremfall sogar das Ende für ein Unternehmen bedeuten kann.

Sicherheitsmaßnahmen unter Berücksichtigung von Administrierbarkeit und Benutzbarkeit

Häufig sind Sicherheitsmaßnahmen mit Einschränkungen bei der Nutzung und Administration verbunden mit der Folge, dass bei vielen konkreten Maßnahmen die Akzeptanz der betroffenen Personen fehlt.

Eine wesentliche Sicherheitsmaßnahme ist z.B. die Trennung von Zuständigkeiten für Aufgaben und Tätigkeiten zwischen verschiedenen Rollen bzw. Personen („Segregation of Duties“). Grundsätzlich sollten sicherheitsrelevante Änderungen immer auf mindestens zwei Rollen verteilt werden, die durch unterschiedliche Personengruppen abgebildet werden. Dies gilt insbesondere für Aufgaben, die umfassende Privilegien benötigen. Ein Administrator sollte z.B. die Datenbank, aber nicht die Daten administrieren können. Solch eine klare Trennung zwischen Infrastrukturbereitstellung/-Administration und der Verarbeitung der Daten verhindert, dass vorhandene Privilegien missbraucht werden und unzulässige Zugriffe auf oder Änderungen von sensitiven Informationen erfolgen können.

Hierbei wird deutlich, dass bei der Umsetzung von Sicherheitsmaßnahmen auch immer die Aspekte Administrierbarkeit und Benutzbarkeit zwingend berücksichtigt werden müssen, um eine ausgewogene Balance zwischen diesen drei Bereichen und damit einen optimalen Einsatz der IT zu ermöglichen sowie die Akzeptanz von Sicherheitsmaßnahmen bei Nutzern und Administratoren zu gewährleisten.

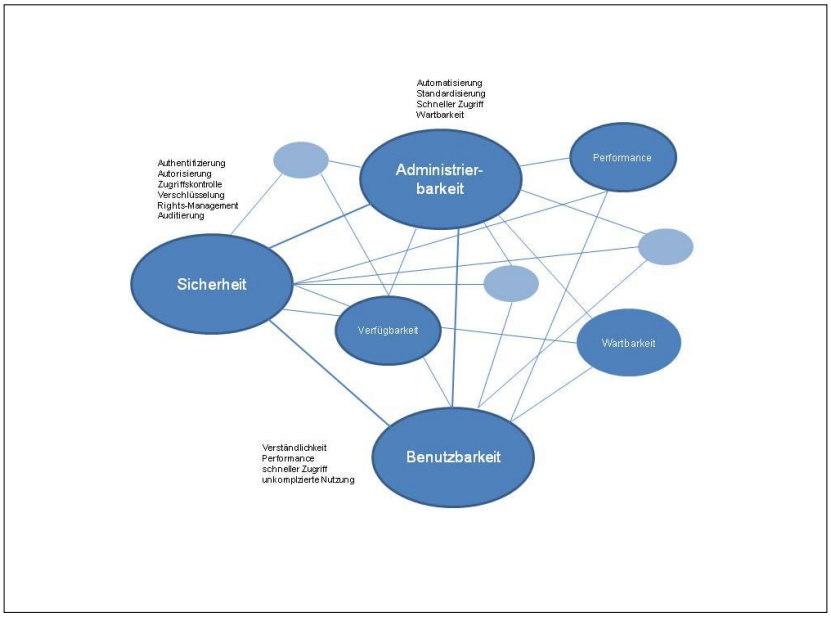

Abb.1: Anforderungsgeflecht an Sicherheitsimplementierungen

Sicherheitsaspekte bei Datenbanken

Da ein Großteil der umfangreichen und oft sensiblen Unternehmensdaten in kommerziellen Datenbanksystemen wie Oracle, Microsoft SQL Server, IBM DB2 und Sybase Datenbanken gehalten werden, stellen diese Systeme zunehmend ein lukratives Ziel für kriminelle Aktivitäten dar. Stand bisher die Absicherung der Netzwerkperimeter und der Clientsysteme (Firewalls, IDS/IPS, Antivirus etc.) im Fokus der IT Sicherheitsaktivitäten, sollte nun die nächste Phase, die den Schutz der Unternehmensdatenbanken vor Sicherheitslücken und unbefugten Zugriffen und Änderungen zum Gegenstand hat, folgen.

Zur Absicherung von Datenbanken sowie zur Einhaltung von gesetzlichen Vorgaben insbesondere, wenn sensitive und personenbezogene Daten gem. § 3 (1) BDSG innerhalb der Datenbanken gespeichert werden, die vor unberechtigten Zugriffen geschützt werden müssen, lässt sich auf Basis der Best Practices zur Datenbanksicherheit, die eine ganzheitliche Methodik bilden, recht einfach ein durchgängiges Sicherheitskonzept zum Schutz sensitiver Daten in Datenbanken aufbauen.

Umfang der Datenbanksicherheit

Die wesentlichen Aspekte im Rahmen der Datenbanksicherheit lauten:

- Härtung der Datenbanksysteme
- Trennung der Zuständigkeiten (Segregation of Duties)
- Authentifizierung, Autorisierung, Zugriffskontrolle und Berechtigungsmanagement
- Verschlüsselung (Netzwerk, Datensatz, Export, Backup und File)
- Anonymisierung von sensitiven Daten für Test und Abnahme
- Audit der Datenbankaktivität
- Rückgriff und Wiederherstellung von historischen Daten
- Schutz vor Angriffen durch SQL-Injection

Um ein sinnvolles Maß an Sicherheit für Datenbanken zu erreichen, ist in der Regel eine Kombination aus organisatorischen und technologischen Anforderungen umzusetzen. Sowohl die Datenbankhersteller als auch Drittlieferanten bieten hierzu zahlreiche Funktionen und Produkte an, die technologisch optimal auf die jeweilige Datenbank abgestimmt sind.

Weitere Informationen zum Thema Datenbanksicherheit finden Sie unter:

Best Practices zur 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