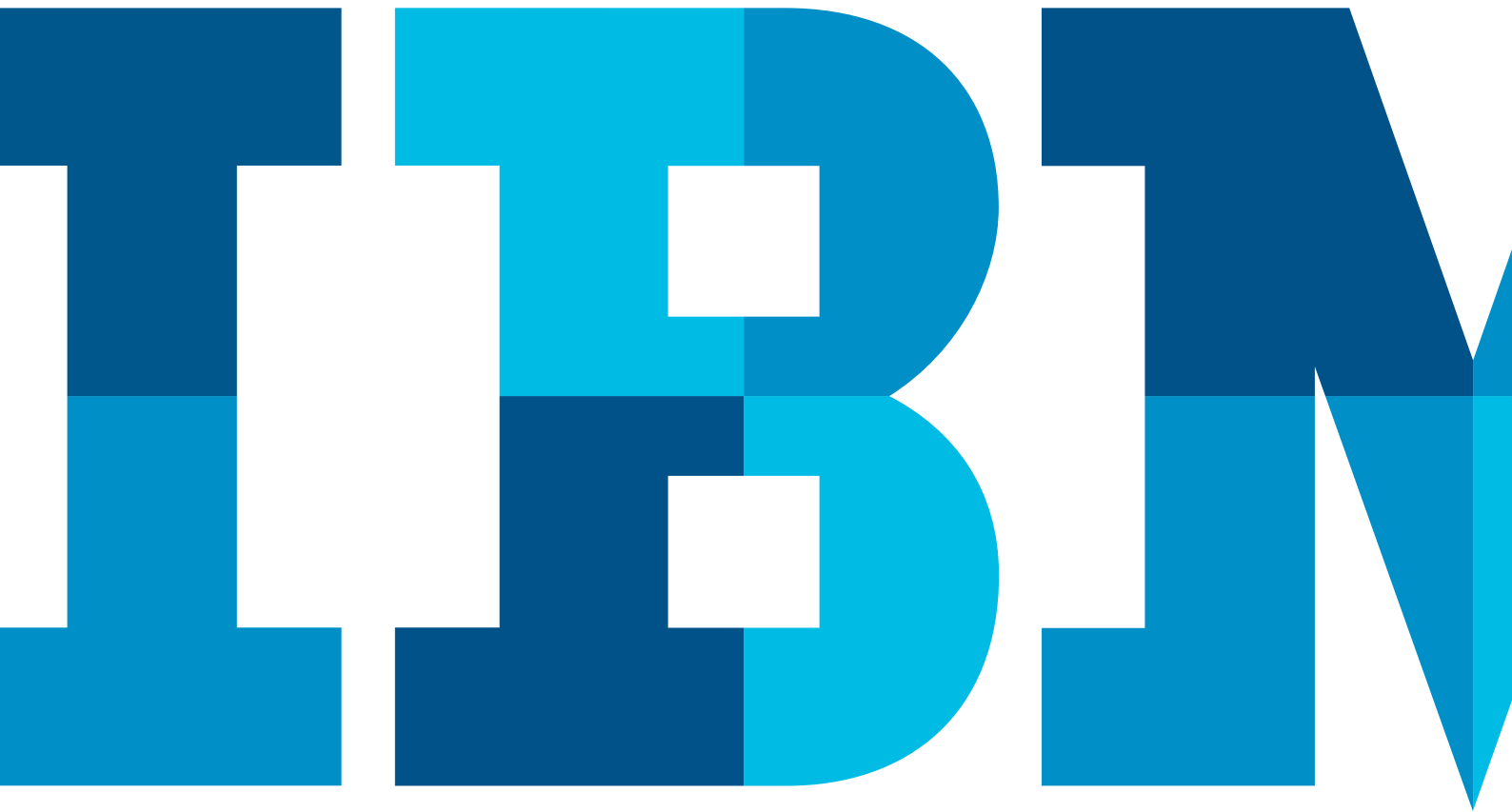


Acht Schritte zur ganzheitlichen Datenbanksicherheit

*Von Ron Ben Natan, Ph.D., IBM Distinguished Engineer,
CTO für den Bereich Integrated Data Management*



Cyberangriffe, Datenmissbrauch durch Insider und gesetzliche Vorgaben veranlassen Unternehmen, neue Wege zur Absicherung ihrer Unternehmens- und Kundendaten zu beschreiten. Diese Daten befinden sich in kommerziellen Datenbanksystemen wie Oracle, Microsoft SQL Server, IBM DB2 und Sybase. Das vorliegende Dokument stellt acht grundlegende Best Practices vor, die eine ganzheitliche Methodik zur Absicherung von Datenbanken sowie zur Einhaltung einschlägiger gesetzlicher Vorgaben wie SOX, PCI-DSS, GLBA und Datenschutzgesetzen bilden.

Datenbanken absichern, Compliance erzielen

Finanziell motivierte Angriffe, Datenmissbrauch durch Insider und gesetzliche Vorgaben veranlassen Unternehmen, neue Wege zur Absicherung ihrer Unternehmens- und Kundendaten zu beschreiten.

Weltweit werden sensible Daten zumeist in kommerziellen Datenbanksystemen wie Oracle, Microsoft SQL Server, IBM DB2 und Sybase gehalten – und folglich werden Datenbanken zum lohnenden Ziel für Kriminelle. Dies erklärt, warum SQL-Injektionsangriffe 2008 um 134 Prozent angestiegen sind. Wie in einem vor kurzem veröffentlichten IBM Bericht¹ vermerkt, entspricht dies einem Anstieg von wenigen tausenden Angriffen pro Tag auf mehrere hunderttausend täglich.

Doch es kommen weitere Probleme hinzu: Forrester² vermutet, dass 60 Prozent der Unternehmen beim Einspielen von Datenbanksicherheitspatches im Verzug liegen, während für 74 Prozent aller 2008 gemeldeten Schwachstellen von Webanwendungen – bei diesen handelt es sich primär um SQL-Injektionsschwachstellen – laut IBM auch Ende 2008 noch kein Patch verfügbar war.

„Man kann nicht absichern, was man nicht kennt. Man benötigt eine gute Abbildung der sensiblen Assets – und das gilt für die Datenbankinstanzen ebenso wie für die sensiblen Daten innerhalb der Datenbanken.“

Während bislang der Absicherung der Netzwerkperimeter und der Clientsysteme (Firewalls, IDS/IPS, Antivirus usw.) die meiste Aufmerksamkeit zuteil wurde, folgt jetzt der Übergang in eine neue Phase, in der Fachkräften des Bereichs Informationssicherheit die Aufgabe zufällt, den Schutz der Unternehmensdatenbanken vor Sicherheitslücken und unbefugten Änderungen zu gewährleisten.

Es gibt acht grundlegende Best Practices, die eine ganzheitliche Methodik zur Absicherung von Datenbanken sowie zur Einhaltung einschlägiger gesetzlicher Vorgaben wie SOX, PCI DSS, GLBA und Datenschutzgesetze bilden.

¹ "IBM Internet Security Systems X-Force® 2008 Trend & Risk Report," IBM Global Technology Services, En. 2009.

² "Market Overview: Database Security," Forrester Research, Feb. 2009.

1. Entdeckung

Man kann nicht absichern, was man nicht kennt. Man benötigt eine gute Abbildung der sensiblen Assets – und das gilt für die Datenbankinstanzen ebenso wie für die sensiblen Daten innerhalb der Datenbanken. Darüber hinaus gilt es, den Erkennungsprozess zu automatisieren, da sich der Standort der sensiblen Daten aufgrund neuer oder veränderter Anwendungen, Fusionen, Akquisitionen usw. fortlaufend ändert.

Durch eine interessante Wendung kann es auch dazu kommen, dass einige Erkennungstools aufgrund von SQL-Injektionsangriffen Malware in der Datenbank aufspüren. Neben der Preisgabe vertraulicher Informationen können durch SQL-Injektion entstandene Schwachstellen Angreifern die Möglichkeit bieten, weitere Angriffe in der Datenbank unterzubringen, die dann gegen Websitebesucher gerichtet werden können.

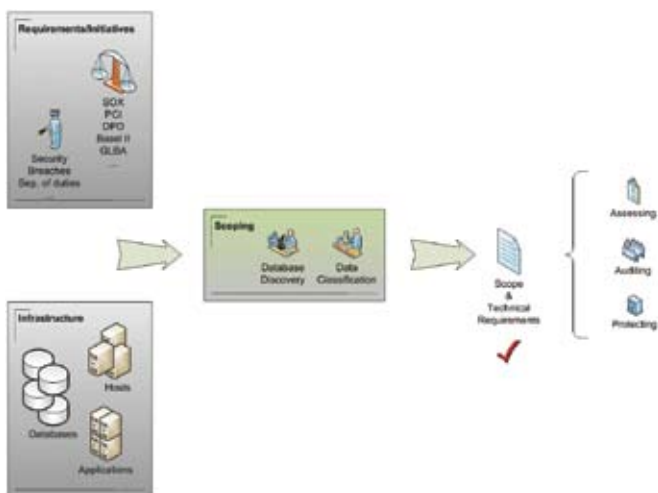


Abbildung 1. Nutzung von Erkennungstools für den Bootstrap einer Implementierung. Die Datenbankinstanzen müssen ebenso abgebildet werden wie der Ort, an dem sich die sensiblen Daten befinden.

2. Schwachstellen- und Konfigurationsbewertung

Wer sich gegen Sicherheitslücken (so genannte „Vulnerabilities“) wappnen will, muss die Konfiguration seiner Datenbanken überprüfen. Dazu ist zu kontrollieren, wie die Datenbank auf dem Betriebssystem installiert ist (beispielsweise durch Prüfen der Zugriffsrechte für Datenbankkonfigurationsdateien und für ausführbare Dateien) und welche Optionen für die Datenbank eingestellt sind (beispielsweise wie viele fehlgeschlagene Logins zur Accountsperrung führen oder welche Zugriffsrechte kritischen Tabellen zugewiesen wurden). Darüber hinaus ist zu verifizieren, dass keine Datenbankversionen mit bekannten Schwachstellen betrieben werden.

Traditionelle Schwachstellenscanner für Netzwerke sind hierfür nicht konzipiert, denn sie verfügen über keine integrierten Kenntnisse der Datenbankstrukturen und des zu erwartenden Verhaltens. Ebenso wenig können sie SQL-Abfragen ausgeben (mittels nachgewiesener Berechtigung zum Zugriff auf die Datenbank), um die Datenbankkonfiguration offenzulegen.



Abbildung 2. Anwendungsfall: Schwachstellenbewertung und Änderungsverfolgung

3. Absicherung

Das Ergebnis der Schwachstellenbewertung ist oft eine Zusammenstellung gezielter Empfehlungen. Dies ist der erste Schritt zur Absicherung der Datenbank. Zu den weiteren Elementen der Absicherung zählt das Entfernen aller nicht benutzten Funktionen und Optionen.

4. Änderungsaudit

Sobald die abgesicherte Konfiguration erstellt wurde, muss diese fortlaufend verfolgt werden, um sicherzustellen, dass diese nicht von der (sicheren) „goldenen“ Konfiguration abweicht. Dazu können Änderungsaudit-Tools eingesetzt werden, die Momentaufnahmen („Snapshots“) der Konfigurationen (sowohl auf der Betriebssystem- als auch auf der Datenbankebene) vergleichen und eine Warnmeldung ausgeben, wenn eine Änderung erfolgt, welche die Sicherheit der Datenbank beeinträchtigen könnte.

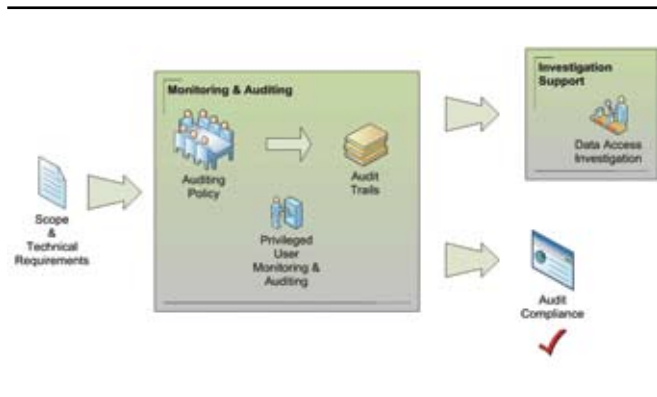


Abbildung 3. Anwendungsfall: Überwachung der Datenbankaktivität und Auditing

5. Database Activity Monitoring (DAM) – Überwachung der Datenbankaktivität

Die Echtzeitüberwachung der Datenbankaktivität ist der Schlüssel zur Gefahrenbegrenzung: Eindringversuche und Missbrauch werden sofort erkannt. DAM erkennt und meldet beispielsweise ungewöhnliche Zugriffsmuster, die auf einen SQL-Injektionsangriff, unberechtigte Änderungen an Finanzdaten, die Gewährung größerer Accountberechtigungen und Konfigurationsänderungen durch SQL-Befehle hindeuten.

Die Überwachung privilegierter Benutzer ist auch eine Voraussetzung für Data-Governance-Gesetze wie SOX und Datenschutzverordnungen wie PCI DSS. Diese ist ebenso wichtig für das Erkennen eines unbefugten Zugriffs, denn Angriffe führen häufig dazu, dass der Angreifer privilegierte Zugriffsrechte erhält – beispielsweise über Berechtigungsnachweise, die einer Geschäftsanwendung gehören.

DAM ist auch ein Grundelement der Schwachstellenbewertung, denn damit lassen sich traditionelle, statische Bewertungen um dynamische Bewertungen von Verhaltensschwachstellen erweitern, beispielsweise die gemeinsame Nutzung von Privilegien durch mehrere Benutzer oder eine übermäßig hohe Zahl fehlgeschlagener Datenbankanmeldungen.

„Nicht alle Daten und nicht alle Benutzer sind gleich. Benutzer müssen authentifiziert werden. Über jeden einzelnen Benutzer muss Rechenschaft abgelegt werden. Beim Management der Zugriffsrechte ist auf die Einschränkung des Datenzugriffs zu achten.“

Schließlich ermöglichen einige DAM-Technologien die Überwachung auf der Anwendungsschicht, so dass ein Betrug auch über mehrschichtige Anwendungen wie PeopleSoft, SAP und Oracle e-Business Suite statt nur über Direktverbindungen zur Datenbank erkennbar ist.

6. Audit

Für alle Datenbankaktivitäten, welche die Sicherheit bzw. die Datenintegrität tangieren oder bei denen sensible Daten angezeigt werden, müssen sichere, nicht anfechtbare Prüfprotokolle angelegt werden. Neben ihrer Schlüsselbedeutung für die Erfüllung gesetzlicher Vorgaben sind differenzierte Prüfprotokolle auch für forensische Untersuchungen wichtig.

Die meisten Unternehmen setzen derzeit auf eine Art manuelle Audits unter Nutzung traditioneller, nativer Datenbankprotokollfunktionen. Diese Verfahren erweisen sich aber aufgrund ihrer Komplexität und ihrer hohen, durch manuellen Aufwand verursachten Kosten oft als unzulänglich. Zu den weiteren Nachteilen zählen hohe Performanceeinbußen, die mangelnde Aufgabenteilung (DBAs können ungehindert die Inhalte von Datenbankprotokollen manipulieren und beeinträchtigen dadurch die Unanfechtbarkeit) und die Notwendigkeit des Kaufs großer Datenspeicherkapazitäten, um enorme Mengen ungefilterter Transaktionsdaten bewältigen zu können.

Erfreulicherweise steht heute bereits eine neue Klasse von DAM-Lösungen zur Verfügung, die differenzierte, DBMS-unabhängige Audits mit minimaler Beeinträchtigung der Performance bieten und die Betriebskosten durch Automatisierung, zentralisierte und DBMS-übergreifende Regelungen und Audit-Depots, Filterung und Komprimierung senken.

7. Authentifizierung, Zugriffskontrolle und Berechtigungsmanagement

Nicht alle Daten und nicht alle Benutzer sind gleich. Benutzer müssen authentifiziert werden. Über jeden einzelnen Benutzer muss Rechenschaft abgelegt werden. Beim Management der Zugriffsrechte ist auf die Einschränkung des Datenzugriffs zu achten. Und es gilt, diese Zugriffsrechte durchzusetzen – auch bei den am höchsten privilegierten Datenbankbenutzern. Ferner müssen auch die Berechtigungsberichte („User High Attestation Reports“) im Rahmen des formellen Auditprozesses regelmäßig geprüft werden.

8. Verschlüsselung

Mittels Verschlüsselung sind sensible Daten unlesbar zu machen, damit kein Angreifer von außerhalb der Datenbank unberechtigt auf die Daten zugreifen kann. Dazu zählen auch die Verschlüsselung der in Übertragung befindlichen Daten (der Angreifer soll nicht auf der Netzwerkschicht mitlauschen und auf Daten, die zum Datenbank-Client gesandt werden, zugreifen können) und die Verschlüsselung der ruhenden Daten (der Angreifer soll die Daten auch nicht per Zugriff auf die Mediendateien extrahieren können).

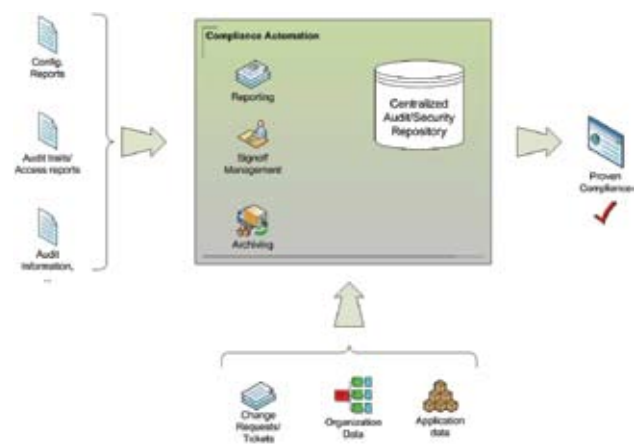


Abbildung 4: Management des gesamten Compliance-Lebenszyklus

Acht Schritte zur Datenbanksicherheit

1. Entdeckung
 2. Schwachstellen- und Konfigurationsbewertung
 3. Absicherung
 4. Änderungsaudit
 5. Database Activity Monitoring (DAM) – Überwachung der Datenbankaktivität
 6. Audit
 7. Authentifizierung, Zugriffskontrolle und Berechtigungsmanagement
 8. Verschlüsselung
-

Über den Verfasser

Dr. Ron Ben Natan verfügt über mehr als zwanzig Jahre an Erfahrung in der Entwicklung von Unternehmensanwendungen und Sicherheitstechnologie für renommierte Konzerne wie Merrill Lynch, J.P. Morgan, Intel und AT&T Bell Laboratories.

Dr. Ben Natan war auch als Berater für Datensicherheit und verteilte Systeme für Phillip Morris, Miller Beer, HSBC, HP, Applied Materials und die Streitkräfte der Schweiz tätig.

Dr. Ben Natan, IBM GOLD Consultant und promovierter Informatiker, ist ein Experte für verteilte Anwendungsumgebungen, Anwendungssicherheit und Datenbanksicherheit. Er hat zwölf Patente angemeldet und zwölf Fachbücher verfasst, darunter *Implementing Database Security and Auditing* (Elsevier Digital Press), das Standardwerk auf diesem Gebiet. Sein neuestes Buch wurde 2009 veröffentlicht und trägt den Titel *HOWTO Secure and Audit Oracle 10g and 11g* (CRC Press).

Über IBM InfoSphere Guardium

InfoSphere Guardium ist eine der marktführenden Lösungen zur Vermeidung von Datensicherheitslücken in Rechenzentren und zur Sicherstellung der Integrität von Unternehmensdaten. Die Unternehmensplattform von Guardium ist bereits in über 450 Kundenrechenzentren rund um den Globus installiert, darunter in den fünf größten Bankhäusern der Welt, bei vier der sechs weltgrößten Versicherer, in Ministerien und Behörden, bei zwei der drei weltgrößten Einzelhändler, in 20 renommierten Telekommunikationsunternehmen, bei zwei weltweit beliebten Getränkemarken, beim führenden PC-Hersteller, bei einem der drei führenden Automobilhersteller, in einem der drei weltweit führenden Luft- und Raumfahrtkonzerne und bei einem führenden Anbieter von Business-Intelligence-Software. InfoSphere Guardium war die erste Lösung, die gezielt die zentrale Schwachstelle bei der Datensicherheit anging: Die Datenbank. Die skalierbare, DBMS-übergreifende Unternehmensplattform schützt die Datenbanken in Echtzeit und automatisiert den gesamten Compliance-Auditing-Prozess.

Guardium ist Bestandteil des IBM InfoSphere Produktportfolios, IBM InfoSphere stellt eine einheitliche Informationsplattform bereit, die Daten und Inhalte aus verschiedenen Silos oder den Systemen verschiedener Anbieter unabhängig von ihrem Typ, ihrem Umfang oder ihrer Komplexität integriert, abgleicht, verwaltet und analysiert und sie den Benutzern, Anwendungen und Geschäftsprozessen im jeweiligen Kontext zur Verfügung stellt. So entsteht eine „Single Version of the Truth“, eine einzige, zuverlässige Version der Daten, die für alle Aspekte von Kunden, Produkten, Konten oder beliebiger anderer Gebiete eine verlässliche Grundlage darstellt. Die InfoSphere-Plattform stellt alle grundlegenden Bausteine für vertrauenswürdige Informationen bereit, einschließlich Datenintegration, Data-Warehousing, Stammdatenverwaltung und Information-Governance. Durch das modular ausgelegte Portfolio können Sie an einem beliebigen Punkt einsteigen und nach Ihren Vorstellungen InfoSphere-Softwarebausteine mit Komponenten anderer Anbieter kombinieren oder mehrere Bausteine zusammen implementieren.



IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustrasse 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

IBM, das IBM Logo, ibm.com, Guardium und InfoSphere sind Marken der International Business Machines Corporation. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Herstellern sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite „Copyright and trademark information“ unter [HYPERLINK](#)

ibm.com/legal/copytrade.shtml

Guardium ist eine eingetragene Marke und Safeguarding Databases, S-GATE und S-TAP sind Marken von Guardium.

Weitere Unternehmens-, Produkt- oder Servicenamen können Marken anderer Hersteller sein.

Vertragsbedingungen und Preise erhalten Sie bei den IBM Geschäftsstellen und/oder den IBM Business Partnern. Die Produktinformationen geben den derzeitigen Stand wieder. Gegenstand und Umfang der Leistungen bestimmen sich ausschließlich nach den jeweiligen Verträgen.

© Copyright IBM Corporation 2010
Alle Rechte vorbehalten.



Recyclingfähig, bitte der
Wiederverwertung zuführen
