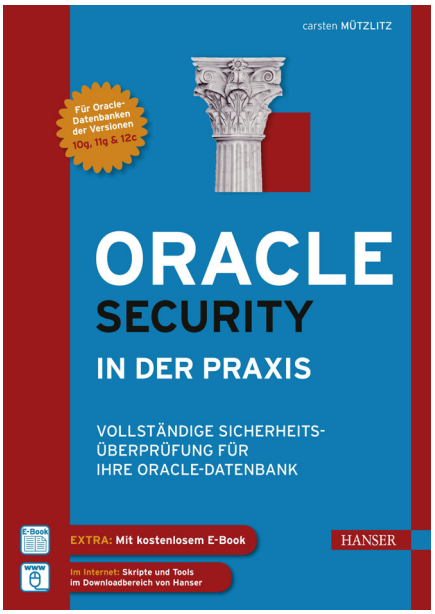
HANSER



Vorwort

zu

„Oracle Security in der Praxis“

von Carsten Mützlitz

ISBN (Buch): 978-3-446-43869-9
ISBN (E-Book): 978-3-446-43923-8

Weitere Informationen und Bestellungen unter
http://www.hanser-fachbuch.de/978-3-446-43869-9
sowie im Buchhandel

1 Vorbemerkung

Bevor ich gemeinsam mit Ihnen in die Details gehe und Ihnen zeige, wie man die Sicherheit einer Oracle-Datenbank überprüft, möchte ich ein persönliches Anliegen vorwegnehmen.

Wir alle sitzen im gleichen Boot, wenn es um unsere Daten geht. Ob wir nun Bäcker, Maler, Angestellte, Datenschutzbeauftragte, Vorstände, normaler Bürger oder Datenbank-Administratoren (DBAs) sind. Wir alle sind davon betroffen, dass unsere Daten in irgendeiner Datenbank eines Unternehmens oder einer Behörde gespeichert sind. Sobald wir einen Vertrag mit einer Firma/Versicherung/Bank abschließen oder einen Kauf im Internet tätigen, können wir davon ausgehen, dass unsere Daten in einer Datenbank gespeichert werden. Das ist eine Tatsache und betrifft uns alle, die wir Verträge und Geschäfte mit Dritten abschließen.

Glücklicherweise haben wir in Deutschland und der Europäischen Union (EU) Gesetze wie das Landesdatenschutzgesetz und das Bundesdatenschutzgesetz sowie einige Richtlinien, die vorschreiben, wie der Schutz personenbezogener Daten einzuhalten ist. Diese Gesetze sind kein Wunschkonzert, sondern müssen durch die Betreiber von Datenspeichern und Anwendungen umgesetzt werden. Für die IT-Abteilungen bedeutet das, Maßnahmen zu implementieren, um die Gesetze zu erfüllen und dadurch den bestmöglichen Datenschutz für unsere Daten zu gewährleisten. Ziel dieser Gesetze ist es, unsere Daten zu schützen. Das sollte jedem Verantwortlichen klar sein. So weit, so gut, aber warum erfährt man so oft aus der Presse, dass Daten gestohlen werden? Sind unsere Gesetze nicht gut oder die definierten Maßnahmen schlecht?

Meiner Meinung nach sind nicht die Gesetze in Frage zu stellen. Mittlerweile definieren diese Gesetze relativ gute Maßnahmen. Eher bin ich der Meinung, dass teilweise das fehlende Wissen und die Ignoranz einiger Menschen diese Vorfälle möglich machten. In den vielen Sicherheitsüberprüfungen von Datenbanken, die ich in den letzten 15 Jahren durchgeführt habe, ist mir immer wieder eines aufgefallen: *„Unsere Daten könnten sehr viel besser geschützt sein. Anforderungen und Maßnahmen aus den Gesetzen sind teilweise nicht implementiert oder durch ungeeignete Konzepte ausgehebelt.“* Es gibt viele Gründe für diese Aussage, doch der wichtigste Grund ist, dass der konsequente Blick auf die Sicherheit und den Datenschutz fehlt. Die Konzepte existieren. Gerade eine Oracle-Datenbank kann out-of-the-box alle Gesetzesanforderungen sofort realisieren. Aber leider werden die Konzepte nicht konsequent oder gar nicht umgesetzt.

Dieser Zustand macht mich sehr traurig und gleichzeitig betroffen, denn wie gesagt, es geht um **unsere** und somit auch um meine Daten. Das sollte sich jeder Datenbank-Administrator und Sicherheitsverantwortliche in den IT-Abteilungen bewusst machen.

Mit diesem Buch möchte ich erreichen, dass Ihre Daten besser geschützt werden, d. h., Sie werden viele Hinweise erhalten, wie man eine optimale Sicherheit einstellt. Die Oracle-Datenbank hat einen ungefähren Marktanteil von 50 %, d. h., jede zweite Datenbank, in der **unsere** Daten gespeichert werden, könnte eine Oracle-Datenbank sein. Somit möchte ich mit diesem Buch erreichen, dass zumindest jede zweite Datenbank in naher Zukunft eine erhöhte Sicherheit und Datenschutz implementiert und somit **unsere** Daten besser geschützt sind.

In diesem Buch finden Sie Konzepte und praktische Beispiele, die ich in den letzten Jahren entwickelt habe bzw. normale Empfehlungen als Oracle-Best-Practices darstellen. Diese Konzepte sind teilweise unabhängig von der Datenbankversion und auch dem jeweiligen Hersteller. Meinen Fokus in diesem Buch lege ich auf die Oracle-Datenbank in den Versionen 12c und 11g. Vieles funktioniert aber auch noch mit der Version 10g. Zusätzlich sollten Sie wissen, dass Sie in diesem Buch keine detaillierten Ausführungen zu altbekannten Konzepten finden werden. Ich möchte mich nicht zum tausendsten Male wiederholen, sondern setze voraus, dass Sie als Leser gewisse Grundkenntnisse im Umgang mit Oracle Datenbanken besitzen. Wenn nicht, finden Sie in der Oracle-Onlinedokumentation (siehe *http://docs.oracle.com*) genügend Lesestoff, um sich fehlende Grundkenntnisse anzueignen. Geschriebene Worte sind schnell veraltet, daher sind in diesem Buch die aktuellen Links aus der Oracle-Onlinedokumentation zur weiteren Vertiefung eingearbeitet.

Der Aufbau dieses Buchs ist sehr einfach gehalten. Als Erstes führe ich Sie in die Grundbedrohungen und Grundlagen der Datenbanksicherheit ein. Anschließend an diese Ausführungen beschreibe ich wichtige Lösungen, sogenannte Best Practices, für einen Standardbetrieb mit erhöhtem Schutz. In diesem Abschnitt finden Sie auch die herausragenden neuen Konzepte für die 12c-Oracle-Datenbank beschrieben. Im dritten Abschnitt des Buchs zeige ich Ihnen detailliert, welche Informationen von einer Oracle-Datenbank benötigt werden, um eine Aussage zu dem Datenbank-Sicherheitszustand machen zu können. Zusätzlich erfahren Sie, welche Erkenntnisse man gewinnen kann und welche Lösungen abgeleitet werden können. Darüber hinaus nehme ich eine Bewertung vor, die den Sicherheitszustand der Datenbank nach CVSS[1] bewertet. Und schließlich erfahren Sie, wie man die Tools ausführt, die zu einer Überprüfung der Sicherheit genutzt werden können. Die Tools ermöglichen es Ihnen, die Überprüfungen automatisiert auszuführen, und führen zu einem schnellen Ergebnis (siehe Hanser-Download-Bereich).

Danach sind Sie in der Lage, den Zustand Ihrer Datenbanken selbst zu bewerten und das Risiko kompakt an die verantwortliche Person in Ihrer Unternehmung zu melden, die dafür verantwortlich ist, Maßnahmen einzuleiten.

Das Ziel ist erreicht, wenn alle Oracle-Datenbanken, in denen personenbezogene oder andere sensible Daten gespeichert sind, einen erhöhten und gesetzeskonformen Datenschutz implementiert haben, sowie Prozesse aufweisen, die den guten Zustand der Datenbank erhalten.

---

[1] CVSS: Common Vulnerability Scoring System siehe *http://www.first.org/cvss* oder die Oracle-Erklärung zur Risikomatrix: *http://www.oracle.com/technetwork/topics/security/cvssscoringsystem-091884.html*

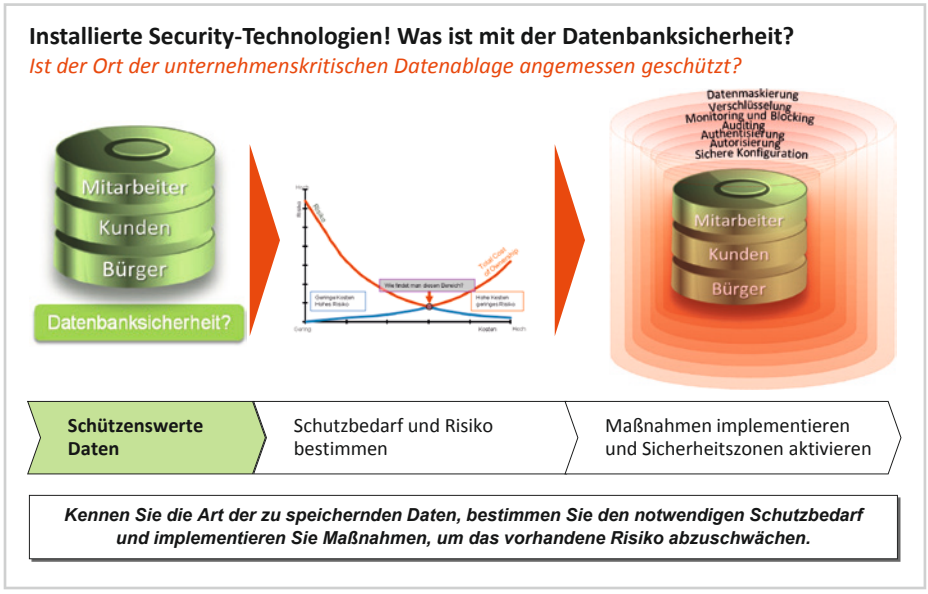


Bild 1.1 Datenbanksicherheit entsprechend dem Schutzbedarf einstellen

Bereits im Vorwort muss ich erwähnen, wie begeistert ich von der neuen Oracle-Datenbankversion 12c bin. Ich arbeite mit Oracle-Datenbanken seit der Version 6. Somit sind Oracle-Datenbanken seit über 20 Jahren ein wesentlicher Bestandteil meiner Beratertätigkeit. Es gibt wohl derzeit keine vergleichbare Datenbank am Markt, die aktuell über so hervorragende Sicherheitsfeatures und nutzbringende Konzepte verfügt wie die Oracle-Datenbank 12c. Es ist eine komplette Gewaltenteilung implementiert, die Netzwerkverschlüsselung und auch die starke Authentisierung (Kerberos, SSL, RADIUS) kann mit jeder Datenbankedition genutzt werden. Außerdem vorhanden sind eine hervorragende Mandantenfähigkeit (Oracle Multitenant) gerade mit den Pluggable Databases sowie viele zusätzliche Features, die die Sicherheit, Zuverlässigkeit und Verfügbarkeit abrunden und damit erheblich erhöhen, aber auch vereinfachen.

Trotz der vielen eindrucksvollen Funktionen und Konzepte einer Oracle-Datenbank ist es immer wichtig, diese korrekt anzuwenden und über das Wissen zu verfügen, was geht und was geht nicht. Oder sagen wir mal, was geht anders und besser. Und genau darum geht es in diesem Buch.

Ich möchte gerne mit den Worten eines bekannten Hackers die nächsten Kapitel einleiten: *„You don't need even a basic skill level to get in."*[2] Damit meinte Kevin Poulsen 1998, dass man kein Experte sein muss, um unerlaubten Zugriff auf Systeme zu erlangen. Diese Weisheit ist richtig, umso wichtiger ist es für die Administratoren, die Kontrolle über ihre Systeme zu behalten. Und hierfür ist die beste Maßnahme, wie Stephen Cobb bereits richtig formulierte: *„The best weapon with which to defend information is information."*[3] Damit meinte Stephen Cobb, dass man sich mit Wissen schützen kann.

[2] Kevin Poulsen, Internet Week, 23. März 1998
[3] Stephen Cobb, The NCSA Guide to PC and LAN Security, 1996

Ein scharsinniger Kunde sagte einmal zu mir: *„Kaum macht man es richtig, schon funktioniert es!“* In diesem Sinne viel Freude mit den nachfolgenden Seiten und den mitgelieferten Tools, die Sie unter dieser URL finden:

http://downloads.hanser.de