Überprüfung von Oracle-Datenbanken nach dem BSI Grundschutz-Standard

Inhalt

- BSI Grundschutz Datenbanken
- Überprüfung der Datenbanken mit dem McAfee Security Scanner for Databases (DSS)

BSI: B 5.7 Datenbanken

BSI: B 5.7 Datenbanken

Der BSI Grundschutz legt die Prozesse und Maßnahmen zum Schutz der Datenbanken nicht genau fest, sondern gibt Empfehlungen, was bei der Überprüfung zu beachten ist.

Diese Empfehlungen können unterschiedlich ausgelegt werden und müssen (z.B. Länge der Passworte, …) an den Schutzbedarf angepasst werden.

https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/baust/b05/b05007.html

Vieles ist Ansichtssache…

BSI: B 5.6 Anschlag

Die technischen Möglichkeiten, einen Anschlag zu verüben, sind vielfältig: **geworfene Ziegelsteine, Explosion durch Sprengstoff, Schusswaffengebrauch, Brandstiftung**. Ob und in welchem Umfang eine Institution der Gefahr eines Anschlages ausgesetzt ist, hängt neben der Lage und dem Umfeld des Gebäudes stark von ihren Aufgaben und vom politisch-sozialen Klima ab. Unternehmen und Behörden, die in politisch kontrovers diskutierten Bereichen agieren, sind stärker bedroht als andere. Institutionen in der Nähe üblicher Demonstrationsaufmarschgebiete sind stärker gefährdet als solche in abgelegenen Orten. Für die Einschätzung der Gefährdung oder bei Verdacht auf Bedrohungen durch politisch motivierte Anschläge können in Deutschland die Landeskriminalämter oder das Bundeskriminalamt beratend hinzugezogen werden.

https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/g/g05/g05006.html

Frage?

Welches Oracle-Feature/ Produkt hilft gegen Anschläge (nach BSI 5.6)

BSI <-> Oracle Mapping

Von Oracle existiert ein Dokument, das die verschiedenen Oracle Produkte auf die BSI Standards mappt.

	Daten-bank EE	Sonstiges
G 5.6 (Anschlag)	**X**	UCM, IRM, IPM

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Extern/BSI-Oracle-Mapping.pdf?__blob=publicationFile

BSI Grundschutz
Datenbanken (B 5.7)

Gefährdungen der Datenbank

- Organisatorische Mängel
- Menschliche Fehlhandlungen
- Technisches Versagen
- Vorsätzliche Handlungen

Organisatorische Mängel

- G 2.22 - Fehlende Auswertung von Protokolldaten
- G 2.26 - Fehlendes oder unzureichendes Test- und Freigabeverfahren
- G 2.38 - Fehlende oder unzureichende Aktivierung von Datenbank-Sicherheitsmechanismen
- G 2.39 - Mangelhafte Konzeption eines DBMS
- G 2.40 - Mangelhafte Konzeption des Datenbankzugriffs
- G 2.41 - Mangelhafte Organisation des Wechsels von Datenbank-Benutzern
- G 2.57 - Nicht ausreichende Speichermedien für den Notfall
- G 2.110 - Mangelhafte Organisation bei Versionswechsel und Migration von Datenbanken

Organisatorische Mängel I

- **G 2.22 - Fehlende Auswertung von Protokolldaten**
  - Test, ob Oracle Auditing aktiviert ist
  - Test, ob Oracle SYS Auditing aktiviert ist
- **G 2.38 - Fehlende oder unzureichende Aktivierung von Datenbank-Sicherheitsmechanismen**
  - Überprüfung, ob die sicherheitsrelevanten Datenbank-Parameter richtig gesetzt sind
- **G 2.39 - Mangelhafte Konzeption eines DBMS**
  - Überprüfung ob Spiegelung der Redo-logs, Aktivierung Archivelog, ... Aktiviert sind
- **G 2.40 - Mangelhafte Konzeption des Datenbankzugriffs**
  - Direkter Zugriff auf die Datenbank (z.b. mittels Daten AWR/Auditing/...)
  - zu viele Rechte (Rechte-Report), z.b. DBA

Organisatorische Mängel II

- **G 2.41 - Mangelhafte Organisation des Wechsels von Datenbank-Benutzern**
  - Überprüfung der Oracle Profile (Passwort-Alter, ...)
  - Klassifikation der Benutzer in verschiedene Gruppe (Verfahrensuser, Persönlicher Benutzer, DBA Benutzer, ...)

Menschliche Fehlhandlungen

- G 3.6 - Gefährdung durch Reinigungs- oder Fremdpersonal
- G 3.16 - Fehlerhafte Administration von Zugangs- und Zugriffsrechten
- G 3.23 - Fehlerhafte Administration eines DBMS
- G 3.24 - Unbeabsichtigte Datenmanipulation
- G 3.80 - Fehler bei der Synchronisation von Datenbanken

Menschliche Fehlhandlungen

- **G 3.16 - Fehlerhafte Administration von Zugangs- und Zugriffsrechten**
  - Überprüfung der Kennungen, die SYS.AUD$ verändern dürfen
  - Überprüfung der Tabelle SYS.MON_MOD$ auf Veränderungen von SYS.AUD$
- **G 3.23 - Fehlerhafte Administration eines DBMS**
  - Test, ob DDL Trigger verwendet wird
  - Überwachung ungültiger Kennungen (Expired/Locked/…)

Technisches Versagen

- G 4.26 - Ausfall einer Datenbank
- G 4.27 - Unterlaufen von Zugriffskontrollen über ODBC
- G 4.28 - Verlust von Daten einer Datenbank
- G 4.30 - Verlust der Datenbankintegrität/-konsistenz

Technisches Versagen

- **G 4.27 - Unterlaufen von Zugriffskontrollen über ODBC**
  - Direkter Zugriff auf die Datenbank (z.b. mittels Daten AWR/ Auditing/...)
  - Test, ob Logon-Trigger existiert

Vorsätzliche Handlungen

- G 5.9 - Unberechtigte IT-Nutzung
- G 5.10 - Missbrauch von Fernwartungszugängen
- G 5.18 - Systematisches Ausprobieren von Passwörtern
- G 5.64 - Manipulation an Daten oder Software bei Datenbanksystemen
- G 5.65 - Verhinderung der Dienste eines Datenbanksystems
- G 5.131 - SQL-Injection

Vorsätzliche Handlungen I

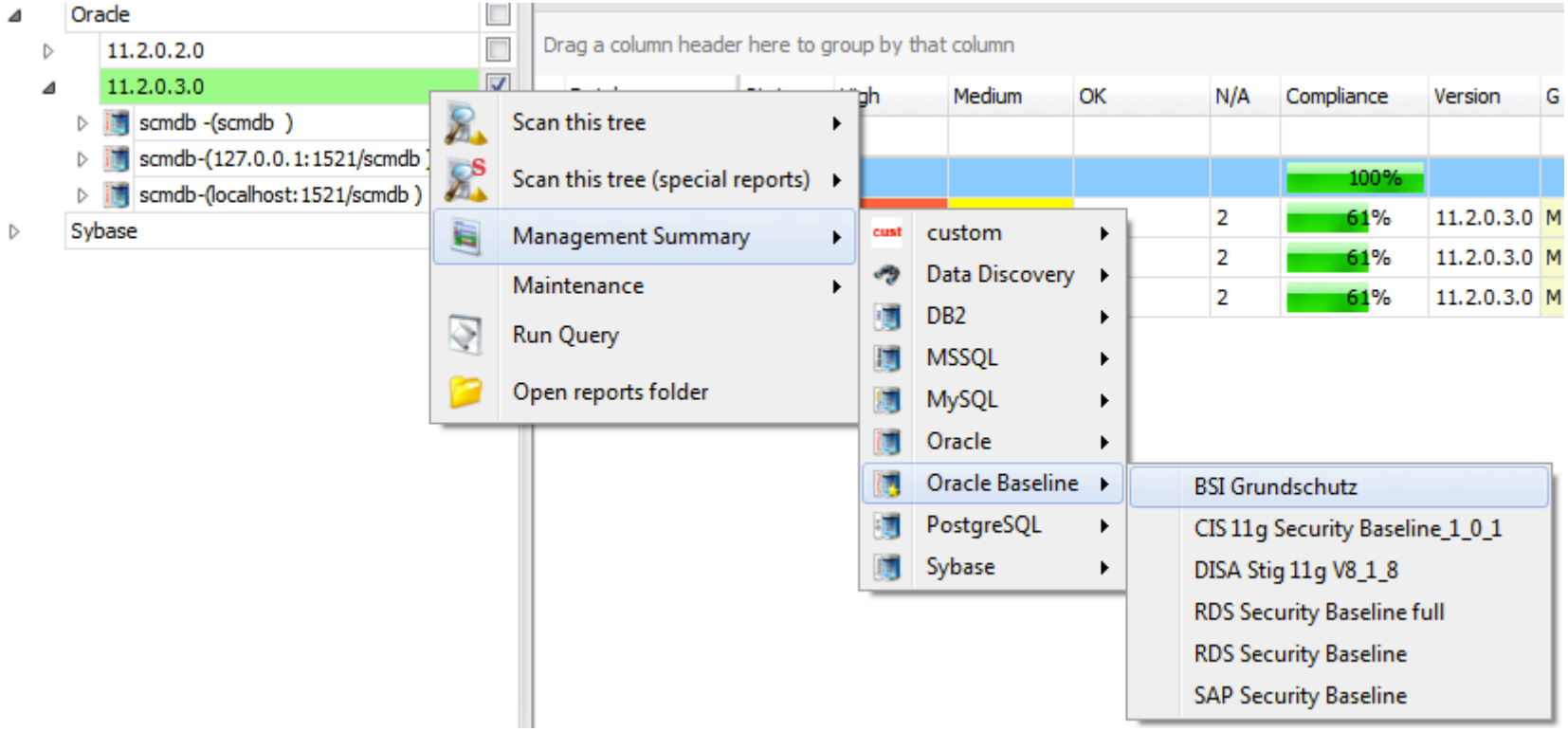
- **G 5.9 - Unberechtigte IT-Nutzung**
  - !!! Überprüfung der Passworte auf schwache Passworte
  - Passworte sollten nicht im Klartext angezeigt werden
- **G 5.18 - Systematisches Ausprobieren von Passwörtern**
  - Existenz und Stärke der Passwort-Verifikation-Funktion
  - Überprüfung des Passwort-Alters
- **G 5.64 - Manipulation an Daten oder Software bei Datenbanksystemen**
  - Test auf Hintertüren

Vorsätzliche Handlungen II

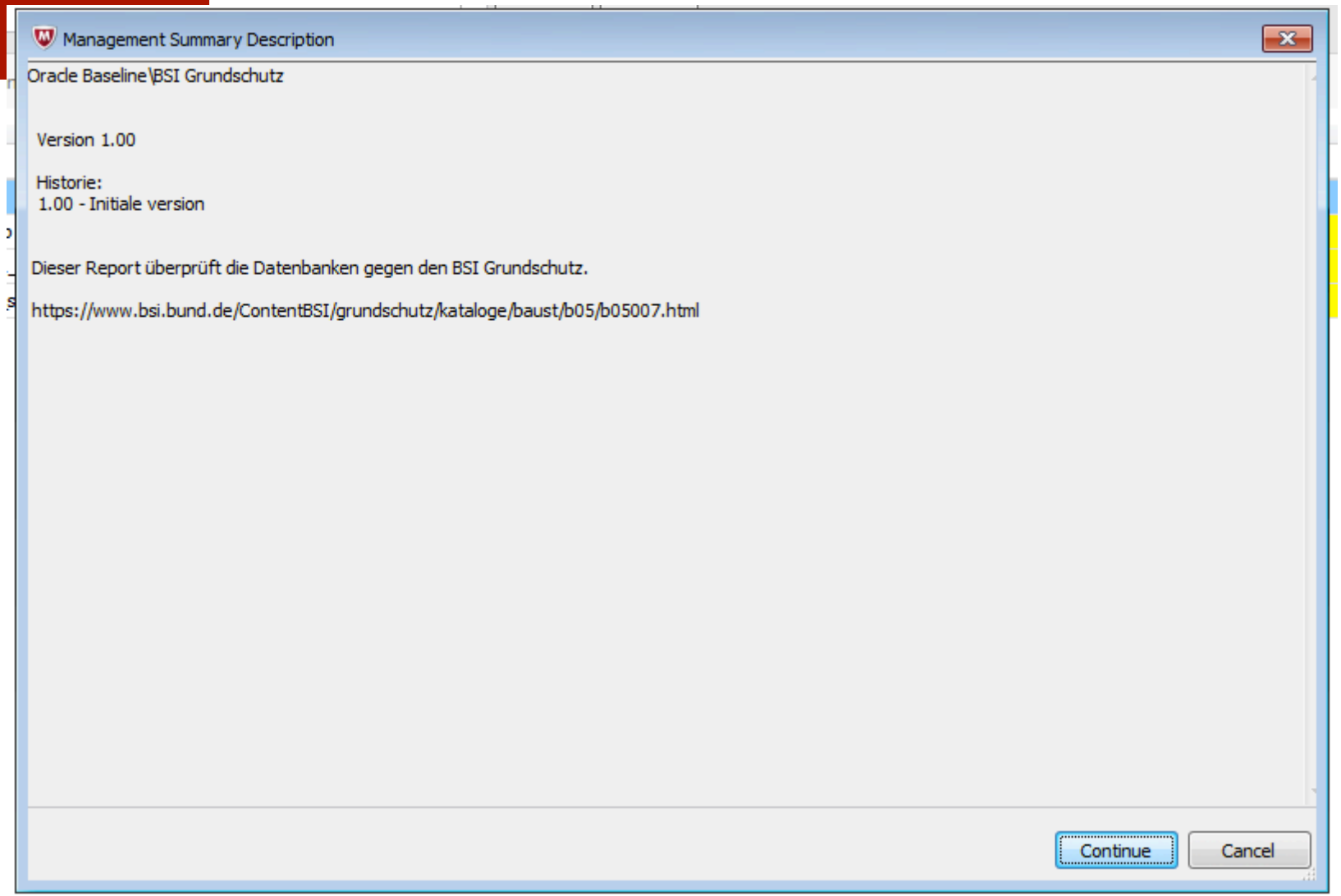
- **G 5.65 - Verhinderung der Dienste eines Datenbanksystems**
  - Test, welche Datenbank Dienste (z.b. xmldb, ...) installiert sind
  - Test, ob Resource Management aktiviert ist
  - Test auf fehlende Patches
- **G 5.131 - SQL-Injection**
  - Existenz eines Error Trigger
  - Test auf Public-Privilegien die von SQL Injection Angriffen ausgenutzt werden

Überprüfung mehrerer Datenbanken

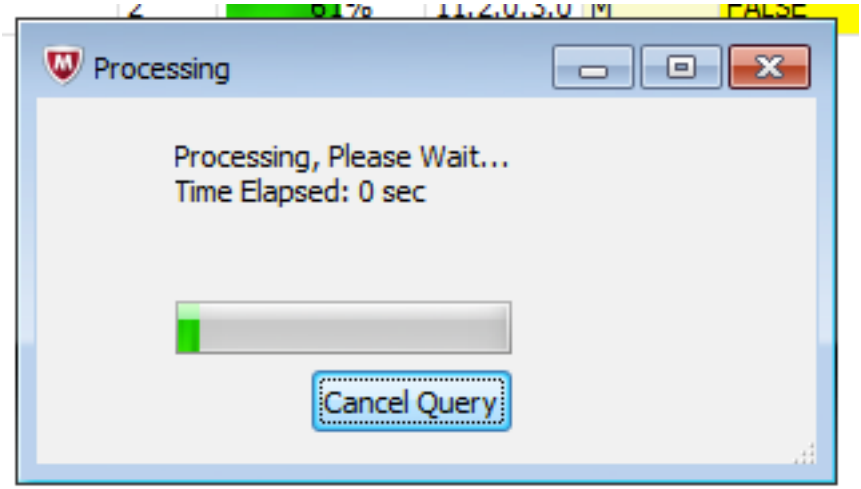
Auswahl der Überprüfung



Report Details



Fortschritt



Ergebnisse

McAfee Security Scanner for Databases - Build 1516 (EnterpriseUnlimited)

Configuration | Scan | Tools | Help

Wizard | Manual | Network | Oracle | Oracle | MSSQL | DB2 | Sybase | Bookmarks

Configuration | Enumeration | Information | Bookmark

List All | DB | DSP | Hierarchy

Databases
- Vendor
  - DB
    - DB2
    - MSSQL
    - Oracle
      - 11.2.0.2.0
      - 11.2.0.3.0
        - scmdb -(scmdb)
        - scmdb-(127.0.0.1:1521/scmdb)
        - scmdb-(localhost:1521/scmdb)
    - Sybase

DB Summary | DB Browser | DB Query | OS Command | Output

Oracle Baseline\BSI Grundschutz

Find | Clear

Drag a column header here to group by that column

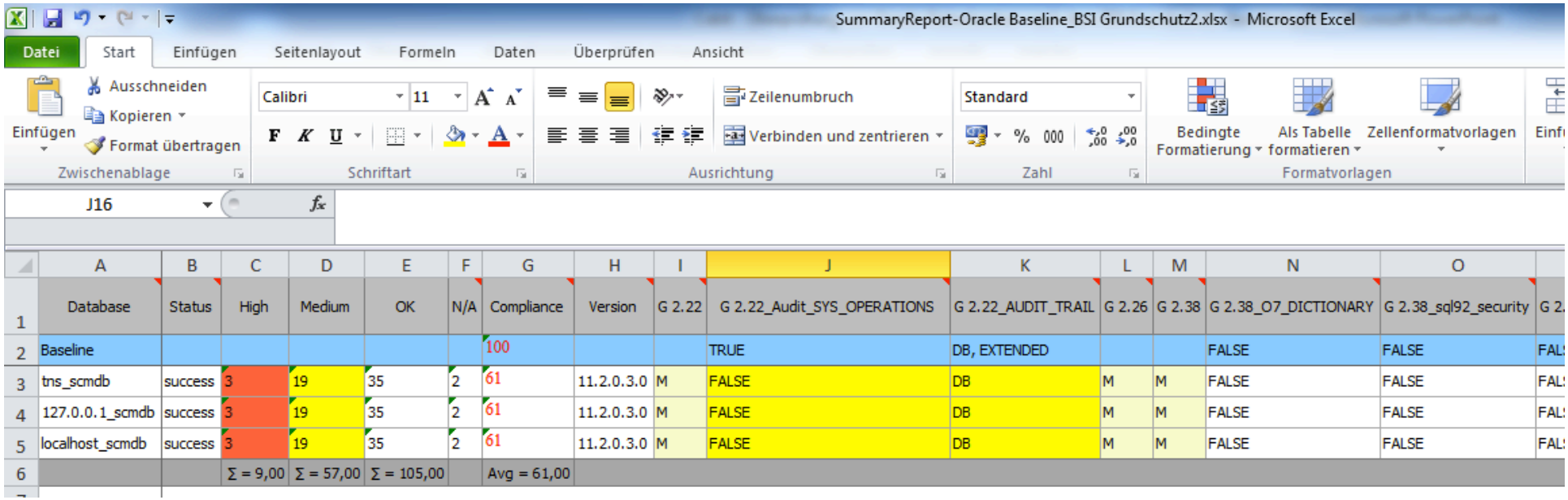
Database	Status	High	Medium	OK	N/A	Compliance	Version	G 2.22	G 2.22_Audit_SYS_OPERATIONS	G 2.22_AUDIT_TRAIL	G 2.26	G 2.38	G 2.38_O7_DICTIONARY	G 2.38_sql92_sec
Baseline						100%			TRUE	DB, EXTENDED			FALSE	FALSE
tns_scmdb	success	3	19	35	2	61%	11.2.0.3.0	M	FALSE	DB	M	M	FALSE	FALSE
127.0.0.1_scmdb	success	3	19	35	2	61%	11.2.0.3.0	M	FALSE	DB	M	M	FALSE	FALSE
localhost_scmdb	success	3	19	35	2	61%	11.2.0.3.0	M	FALSE	DB	M	M	FALSE	FALSE

Σ = 9,00 | Σ = 57,00 | Σ = 105,00 | Avg = 61,00

Save | Load | Compare Table | Diff Table

Number of Rows in Table 4 Time Elapsed: 9 seconds.

Export nach Excel



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Database	Status	High	Medium	OK	N/A	Compliance	Version	G 2.22	G 2.22_Audit_SYS_OPERATIONS	G 2.22_AUDIT_TRAIL	G 2.26	G 2.38	G 2.38_O7_DICTIONARY	G 2.38_sql92_security
2	Baseline						100			TRUE	DB, EXTENDED			FALSE	FALSE
3	tns_scmdb	success	3	19	35	2	61	11.2.0.3.0	M	FALSE	DB	M	M	FALSE	FALSE
4	127.0.0.1_scmdb	success	3	19	35	2	61	11.2.0.3.0	M	FALSE	DB	M	M	FALSE	FALSE
5	localhost_scmdb	success	3	19	35	2	61	11.2.0.3.0	M	FALSE	DB	M	M	FALSE	FALSE
6			Σ = 9,00	Σ = 57,00	Σ = 105,00		Avg = 61,00								

Mehr Informationen zum Thema Datenbank-Sicherheit am McAfee Stand…

Danke

- Kontakt:

Red-Database-Security GmbH

Bliesstr. 16

D-.66538 Neunkirchen

Germany