Red Attack - Die Katastrophe in der Datenbank

Gunther Pippèrr
GPI Consult
München

Schlüsselworte
Datenbank Sicherheit

Einleitung

Was kann ein User mit genügend Rechten in der Datenbank anrichten?

Mit welchen Tricks und Hintertüren kann eine Datenbank-Umgebung so bearbeitet werden, dass der Betrieb langsam aber sicher in der Katastrophe endet?

Wie kann sich ein Angreifer tarnen, damit er und der Angriff möglichst spät entdeckt wird?

Welche Fallen lassen sich in der System-Umgebung auslegen, um Spuren zu verwischen?

Was können wir aktiv dagegen unternehmen, um uns vor diesen Szenarien zu schützen?

Wo müssen wir ansetzen, um unserem System noch vertrauen zu können?

Im Vortrag werden in einer Live Demonstration die Möglichkeiten aufgezeigt, wie ein potentieller Angreifer vorgehen kann.

Auf Basis dieses Wissen wird demonstriert, wie sich proaktiv entsprechende Schutzmaßnahmen aufbauen lassen, um die Katastrophe zu verhindern. In einer überwiegenden Live Demo wird die Datenbank Stück für Stück auseinander genommen um Awareness für Datenbank Sicherheits-Probleme zu erzeugen.

Das Ganze soll neben einem gewissen Unterhaltungswert auch eindringlich die Gefahren des zu leichtsinnigen DBA’s aufzeigen.

Das Szenario

Ein Anwender bzw. Administrator hat viele Rechte in der DB Umgebung erworben und überlegt sich nun, da er die Firma bald verärgert verlässt, was er so alles mit seinen Rechten anfangen kann.

Sein Ziel ist es dabei natürlich nicht aufzufallen. Der Schaden soll erst möglichst lange nach seinem Austritt auftreten.

Wo kann er nun dazu in der DB Umgebung starten?

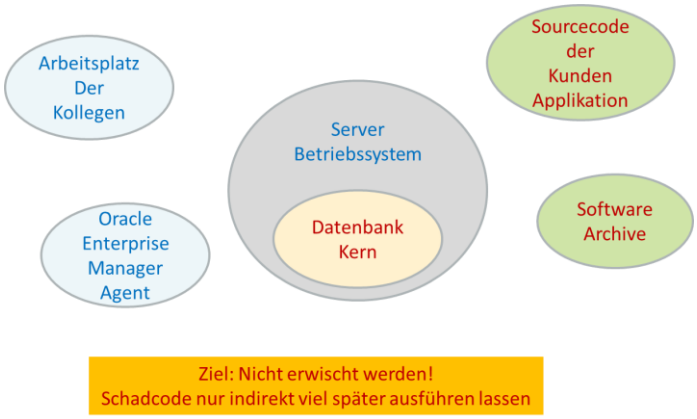

Abb. 1: Wo können wir unsere Abschiedsgeschenke hinterlassen?

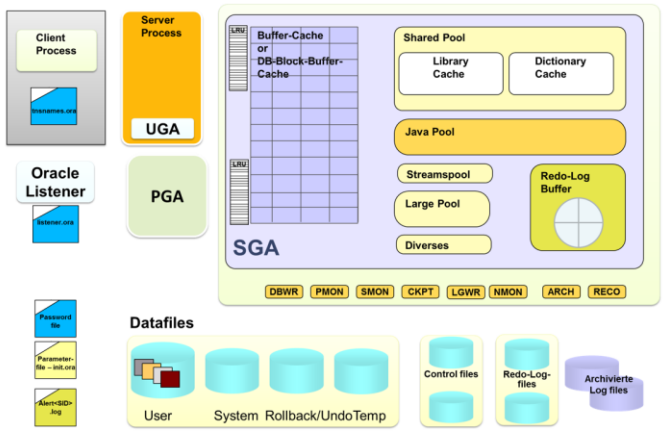

Abb. 2: Auf welcher Ebene der Datenbank wollen wir ansetzen?

Am einfachsten ist es am Anfang auf dem Oracle Support Portal nach guten und einfach zu findenden Bugs zu suchen.

Basierend auf diesen Bugs lassen sich dann schon einfach die ersten „Überraschungen“ in der DB Umgebung einbauen.

Verstecken und Tarnen

Im ersten Schritt müssen wir uns überlegen, wie und wo wir die „Überraschungen“ im System verstecken, so dass es möglichst lange dauert bis das Ganze aktiv wird.

Mit etwas Aufwand:

- In die Sicherungs-Skripte einbauen
- In ETL Jobs verstecken
- Im Source Code der Applikation
- Zum Beispiel in den Deployment Skripte verstecken
- Init.ora Debug Parameter „_oradbg_pathname“ und Events verwenden

Sehr einfach:

- Ganz altmodisch glogin / login.sql von SQL*Plus und TOAD verwenden
- Password verify function in der Datenbank

Was wollen wir anrichten?

Je nach unserer Intention muss im nächsten Schritt überlegt werden was umgesetzt werden soll.

Nur Verwirren und Ärgern

- Init.ora Parameter verbiegen
- Passwort File löschen
- Prozess und File Rechte verändern
- Compliance Lücken wieder öffnen
- Für das nächste Lizenz Audit nicht lizensierte Features aktivieren
- Zeitzone der DB verstellen
- Unsichtbare Objekte in der DB Anlegen

Datenbank vernichten

- Data Dictionary manipulieren
- Bit Fehler in den Control-/ Daten Dateien erzeugen
- Datenbank verschlüsseln

Schon das Entfernen eines Zeichens kann zuverlässig den Neustart eines Oracle RAC Clusters verhindern.

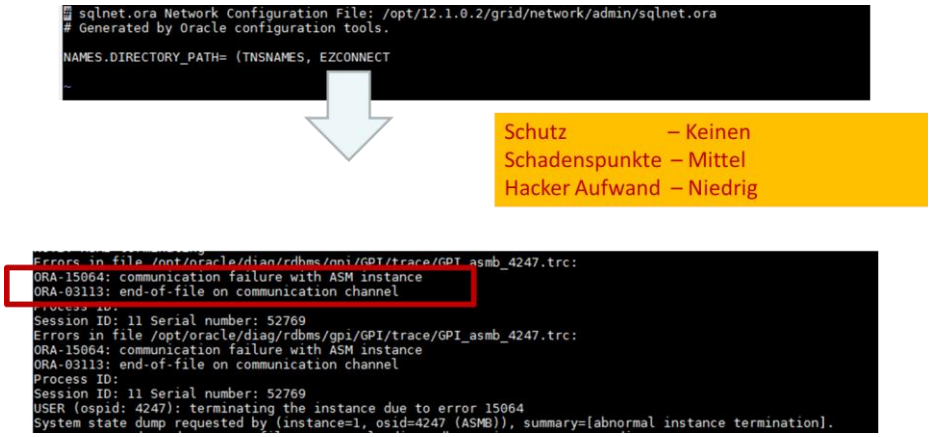

Abb. 3: Ein kleiner Tippfehler führt zur Katastrophe

Eine einfache Veränderung im SPFile führt dazu das kein Neustart mehr möglich ist:

```
alter system reset compatible scope=spfile sid='*';
alter system set audit_file_dest='.' scope=spfile sid='*';
```

Neben diesem ersten Bespielen werden noch mehr einfache Möglichkeiten aufgezeigt, den Betrieb der Datenbank nachhaltig zu stören bzw. die Datenbank entscheidend zu manipulieren.

Wie können wir uns schützen – Ist Schutz überhaupt möglich?

Wurden hier unrealistisch Szenarien vorgestellt?

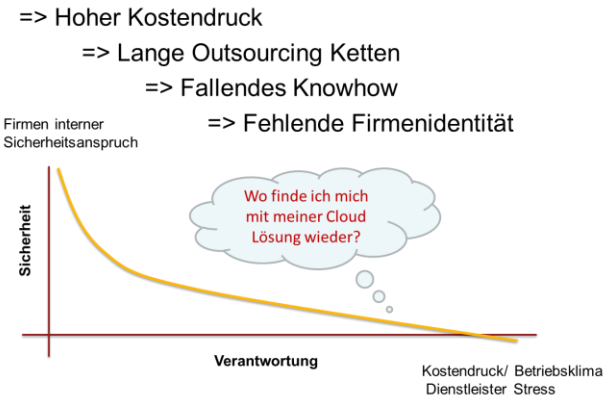

Abb. 4: Sicherheit und Verantwortung hängen eng zusammen

Wie können wir uns schützen?

Vertrauensvolles Personal

- Loyal
- Gut ausgebildet
- Gut bezahlt
- Nicht überarbeitet

Verständnisvolles Management

- Sicherheit kostet Mühe => Kosten
- Sicherheit gilt für alle => Stichwort iPhone für den Chef!

Effektives Monitoring – Früherkennungssysteme

- Stichwort IDS wie unter Linux Tripwire
- Proaktiv auf Veränderungen reagieren

Fazit

Die heutigen Systeme, unabhängig vom Hersteller oder der Funktion, sind in Ihrer Komplexität viel zu empfindlich gegenüber Fehlern in der Konfiguration und der Systemumgebung.

Immer noch gehen die meisten Systeme (bzw. ihre Entwickler) davon aus, dass wir noch in einer heilen Welt leben, allen trauen können und auf Fehlerbehandlung verzichten können.

Kleinste Manipulation führen daher schnell zu einer Katastrophe, ob bewusst oder unbewusst herbeigeführt.

Technisch lässt sich zwar einiges härten und überwachen, aber ein effektiver Schutz gegen all diese Bedrohungen ist nur möglich mit hoch motivierten und zufriedenen Mitarbeitern,

Kontaktadresse:

Gunther Pippèrr
GPI Consult
Schwanthalerstr. 82
D-80336 München

Telefon: +49 (0)89 53 026 418
Mobil: +49(0)171 8065113
E-Mail gunther@pipperr.de
Internet: **http://www.pipperr.de/dokuwiki/doku.php**