Oracle Security

Markus Schmidt, Essential Bytes

Unsicherheit bei der Sicherheit?

essential BYTES

Agenda

- Grundlegende Gedanken
- Wo sind die Daten?
- Was können wir tun?
- Beispielhafte Maßnahmen

essential BYTES

Was ist schief gelaufen mit der Datenbanksicherheit?

- Internet und vernetzte Anwendungen
- Netzwerksicherheit schützt die Datenbank nicht
- Daten nicht mehr nur punktuell gespeichert sondern in großem Maß
- Bestimmungen sind verschärft worden
- Viele Installationen sind „default“ ohne Härtungsansatz
- Oracle liefert für den schnellen Einsatz eine „offene“ Datenbank
- Interne Angriffe nehmen zu

essential BYTES

Warum die Datenbank schützen?

- Oracle Datenbank mit immer zentralerer Rolle
  - Schlüsseldaten FI, HR, …
  - Alle Daten sind von Interesse.
- Prozesse werden von Datenbank getrieben
- Dramatische Auswirkungen durch Globalisierung
- Immer vollständigere Informationen in DB

ABER: kaum konkrete Maßnahmen für Schutz

essential BYTES

Kernprobleme

- Falsches Produkt installiert EE <> SE
- „Default“ – Installation
  - Features / Schemas / Konfiguration
- Schwache Passworte od. Defaults
- Kein Audit eingeschaltet (wie wollen Sie erkennen, dass ein Einbruch stattfindet?)
- Kein oder schwaches Berechtigungskonzept der Anwendungen
- DBAs verwenden SYS/SYSTEM und teilen sich Accounts
- Datenbank ist per TNS von überall zu erreichen
- …

essential BYTES

Was ist „Oracle Security“?

Wir müssen nicht die Oracle DB schützen.
Es ist nicht das Problem von Oracle.

Es geht um die Sicherheit und den Schutz **UNSERER** Daten für die **WIR** verantwortlich sind!

Die Daten müssen geschützt werden – es ist mehr zu tun als bloß ein „Patch“ einzuspielen und ab und zu nachzusehen.

essential BYTES

Wo sind die Daten?

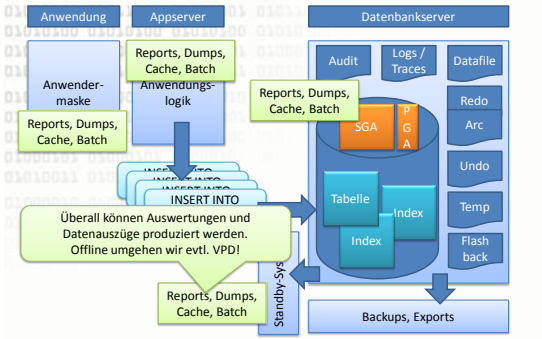
- Physikalisches Design
  - Controlfiles, PW-File, Initfile
  - Database Files
  - Redo logs / Archivelogs
  - Flashback
  - …
- Alle diese Dateien enthalten kritische Informationen zur Struktur, Daten, Passworte, etc.

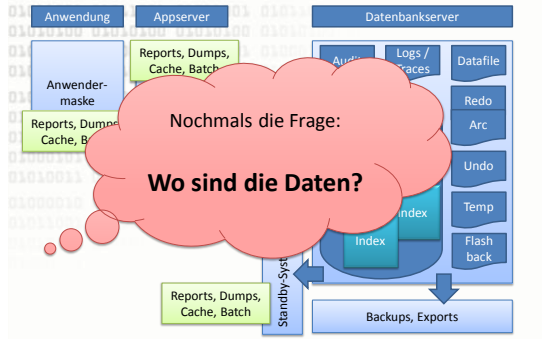
Wo sind die Daten?

- Logisches Design
  - Memory mit SGA, PGA, UGA
  - Pools, Heaps, Block Buffer, Dictionary Cache, Log Buffer
  - Prozesse die über Shared Memory kommunizieren
  - Blöcke, Segmente, Tablespaces, Objekte

Wo sind die Daten?

In der Datenbanktabelle!





Konsequenz: Daten sind nicht nur in der DB

- Es reicht nicht aus, nur punktuell für Schutz zu sorgen! Es gibt zuviele Angriffspunkte.
- Wissen Sie, wo überall die Daten sind?
- Wissen Sie, wer auf die Daten zugreift?
- Wissen Sie, wie auf Daten zugegriffen wird?
- Wenn wir die Zugriffspfade und die Speicherorte kennen, habe wir eine Chance gegen Angreifer.

Was können wir tun?

- Denken wie ein Hacker ☺
  - Was würde der tun?
  - Neugierig sein…
  - Hacker folgen keinen Regeln.
- Informationen nutzen
  - Oracle Security Documentation
  - Post Installation Documentation
  - Metalink / Oracle Support
  - Doku zu Internals, New Features, auch zu nicht sicherheitsbezogenen Aspekten!

essential BYTES

Was können wir tun?

- Tools nutzen
  - User Enumeration zum Erraten von Accounts
  - SID Guessing
  - Connect Brute Force
  - SYSDBA Brute Force
  - Listener Enumerators
  - Passwort Cracker
  - Default Password Tester
  - Scanners

essential BYTES

Was können wir tun?

- Webseiten
  - Zu Exploits
  - Bugs
  - Advisories
  - Blogs
- Bücher
- Checklisten

Wenn wir wissen, was passieren kann, können wir angemessen reagieren!

essential BYTES

Patches

- 95% aller Einbrecher nutzen bekannte Exploits
  - → wenn wir patchen, haben wir 95% abgewehrt…
  - → NEIN! Es ist wohl doch etwas komplexer.
- Insider-Attacken:
  2005 – 26%, 2009 – 43%, 2010 – 80%
  32% von vertrauten Partnern!
- Sind durch Patches die Probleme also gelöst?

essential BYTES

Warum können Daten gestohlen werden?

- Security bugs
  → Patchen. So einfach.
- Konfiguration
  → komplexer, weil anwendungsabhängig
- Feature Overload, breite Angriffsfläche
  → installierte Software
  → installierte Schemas
  → großes Problem!
- Defaults
  → reduzieren und vermeiden
  → Hauptproblem!!!

essential BYTES

Externe / Interne Angriffe

- Extern
  - Application Injection
  - Buffer Overflows
  - Protocol Attacks
  - DoS
- Intern
  - Physikalischer/Logischer Zugriff
  - Power User haben zuviel Rechte
  - Entwicklungsteam…
  - DBAs…

essential BYTES

Zugriff ist das Killerthema.

- Zugriff benötigt IP, SID, Account+PW
- TNSNAMES überall verfügbar.
  - Da stehen schon 2 Angaben drin!
  - Google-Suche: „filetype:ora tnsnames“
- Meist kann jeder auf die Server zugreifen
  - Verbindsversuch möglich
- Servicenamen leicht zu erraten
  - Orcl, Anwendungsname, prod, sapdb…
- Schwache Passwörter.

Beispiel: PUBLIC Privs

- PUBLIC wird immer umfangreicher
  - 9iR2 – 12.000 Privs
  - 10gR2 – 21.500 Privs, +77%
  - 11gR1 – 27.500 Privs, + 28%
  - 11gR2 – 28.200 Privs, + 1%
- Kein Read-only-User möglich!
  Jeder hat 28.200 Privs in 11gR2!
- Eines der größten Probleme

Beispielhafte Maßnahmen Betriebssystem

- Passworte suchen, z.B. in Skripten, cron
- Datenlecks suchen
- Konfiguration prüfen
- Rechte prüfen
  $ORACLE_HOME, Binaries, Datafiles, TNS, Traces, …
- Mitgliedschaft in Gruppen prüfen
  osoper, dba, oinstall, …
- „o“-Binaries
- Prozesslisten auf Passworte prüfen
- Exporte und Dumps suchen

Beispielhafte Maßnahmen Betriebssystem

- Dateiberechtigungen UTL_FILE_DIR
- External Tables, Dateiberechtigungen
- Alertlogs prüfen
- Traces prüfen
- Creation Skripts entfernen
- Unbenutze alte Versionen entfernen
- OS-Benutzer prüfen
- **DBA-Rechner prüfen, der ist gutes Angriffsziel !!!**

Beispielhafte Maßnahmen Netzwerk

- SQLNet Trace Files liefern interessante Infos
- XDB-Services nötig?
- XPT-Services (Data Guard) nötig?
- TNS sichern: Valid node checking
- Listener Password setzen nicht mehr empfohlen seit 11g! Dann nur lokaler Adminzugriff
- Listenener-Admin-Restrictions setzen
- Extproc nötig?

Beispielhafte Maßnahmen Datenbank

- Keine Seed-Datenbank verwenden.
- Eigenes Rollenkonzept erarbeiten
- **Keine** Standardrollen verwenden.
- Init-Parameter prüfen, z.B.
  UTL_FILE_DIR, REMOTE_OS_AUTHENT, OS_AUTHENT_PREFIX, O7_DICTIONARY_ACCESSIBILITY, SQL92_SECURITY, _SYSTEM_TRIG_ENABLED, RESOURCE_LIMIT, …
- Berechtigungen einschränken
- ANY und Unlimited vermeiden
- ALTER SESSION, ALTER SYSTEM einschränken
- Directories, External Tables, Libraries beschränken
- …

Mitarbeiter sensibilisieren

Sensibilisierung bei Security-Themen nötig. Nicht jeder ist sich den Auswirkungen bewusst.

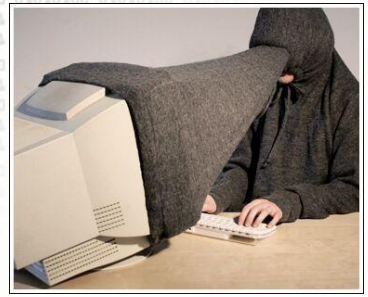
Fazit

Sorgloser Umgang mit den Systemen und der Datenbank verursacht die meisten Sicherheitslücken.

Es sind viele Bereiche zu berücksichtigen – zuviele für einen Kurzvortrag am Abend.

Ein paar Patche einspielen ist noch lange nicht genug.

Secure Environment



Essential Bytes
GmbH & Co. KG
Steinebühlstraße 30
77749 Hohberg

info@essential-bytes.de
www.essential-bytes.de
Tel. 0 78 08 / 943 93 50
Fax 07 81 / 20 55 15 54

Haben Sie noch Fragen?