Securing Oracle Databases

Security Baseline Roadshow

Jonathan Intner, Global Head of Database Security

NYOUG, 6 June, 2007

NOVARTIS

Agenda

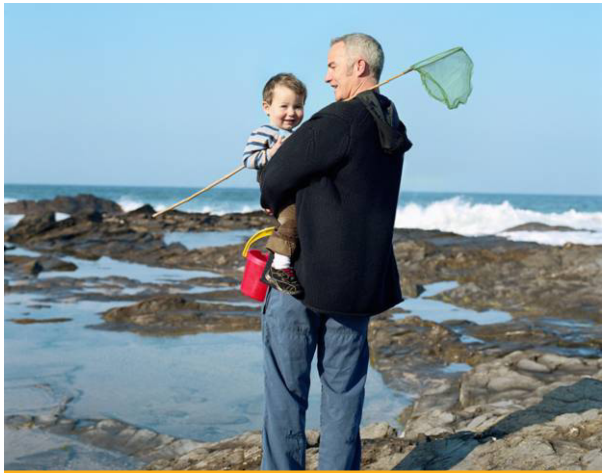
About Novartis

Non-Technical

Technical

Novartis at a Glance

- Novartis is a world leader in the research and development of products to protect and improve health and well-being.
- The company has core businesses in pharmaceuticals, vaccines, consumer health, generics, eye care and animal health.
- It invested approximately USD 5.4 billion in research and development (R&D) and employs approximately 26,000 people in the US. Globally Novartis employs approximately 101,000 people in more than 140 countries
- The global headquarters are in Basel, Switzerland and US Pharmaceuticals headquarters are in New Jersey



Key Facts

Invested in R&D: **USD 5.4 bn**

US Employees: **26,000**

Global Employees: **101,000**

Countries: **140**

Headquarters: **Basel**

Improving People’s Lives

Our products provide treatment for a broad range of disease areas that include:

- **Cardiovascular, endocrine and respiratory diseases:** *H*igh blood pressure, Arteriosclerosis, High cholesterol, Diabetes, Renal failure, Asthma
- **Central nervous system (CNS) disorders:** *S*chizophrenia, Epilepsy, Alzheimer's disease, Parkinson's disease, Attention deficit hyperactivity disorder, Migraine
- **Dermatology:** Fungal disease, Psoriasis
- **Oncology/hematology:** Cancer therapy, Metastatic bone disease
- **Ophthalmics:** Age-related macular degeneration, Glaucoma, Dry eye, Ocular allergies, Other eye disorders
- **Rheumatism/bone and hormone replacement therapy:** *A*rthritis, Osteoporosis
- **Transplantation:** Prevention of acute rejection in organ transplants

Agenda

About Novartis

Non-Technical

- Document creation
- Roles and Responsibilities
- Rollout
- Implementation
- Well-known folks in Oracle Database Security

Technical

Document Creation

- Constituencies
- Process
- Not all databases require the same level of security
- Well-known folks in Oracle Database Security
  - Pete Finnegan
  - Cesar Cerrudo
  - David and Niall Litchfield:
    - David Litchfield’s great book, The Oracle Hacker's Handbook: Hacking and Defending Oracle.

Levels of Security

- Not all data requires the same level of security.
- What is the “Right” level?
- Data has different requirements:
  - Availability
  - Confidentiality
  - Exposure
  - Integrity

Roles and Responsibilities

- Customers
- DBAs
- Application Teams
- Four ways to divide up the tasks:
  - Solely the DBAs
  - Solely the Application Teams
  - Shared between the DBAs and Application Teams
  - Each of the DBAs and the Application Teams have their own sets of responsibilities.

Rollout

- Site visits:
  - Locations:
    - Two sessions at the corporate HQ in Europe.
    - Four at different locations around the US.
  - Technical audience
  - Non-technical audience
- Conference calls:
  - For non-technical audience that didn’t get a site visit

Implementation

- Personally implemented for one location.
- Once I became global, assisted several locations.
- Developed a self-assessment process.

Agenda

About Novartis

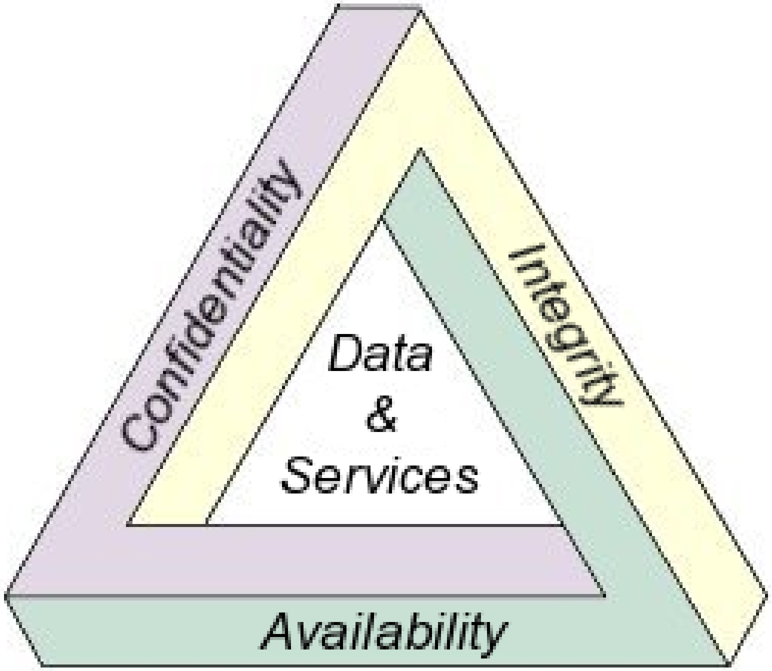
Non-Technical

Technical

- Quick discussion of the security “triangle”
- Detailed discussion of recommended best practices

CIA Triad

- Confidentiality
- Integrity
- Availability



Areas

- Account Management
- Auditing, Logging and Monitoring
- Backup
- Passwords in scripts and script management
- Separation of duties
- Software Version
- Test and Development Databases
- Other

Account Management

- User accounts must be created (& removed!) with a process
- Must use a Quality Password
  - Length and complexity with $ORACLE_HOME/rdbms/admin/utlpwdmg.sql.
  - FAILED_LOGIN_ATTEMPTS
  - PASSWORD_LOCK_TIME
- Don’t use Identified Externally
  - Identified Globally should be OK.
  - If using Identified Externally, then **must** set REMOTE_OS_AUTHENT to FALSE.

Account Management (continued)

- Don’t grant system privileges with admin option nor object privileges with grant option.
- Vendor activities that need SYS or SYSTEM should be done as scripts.
- Remove or lock unused default Oracle accounts.
- DBAs should have their own accounts, rather than using SYS or SYSTEM (except where SYS or SYSTEM are necessary).

Auditing, Logging and Monitoring

- Availability Monitoring. This is the classic DBA activities, for example:
  - Unexpected database startups and shutdowns.
  - Status of background processes.
  - Space utilization
  - Etc.
- Security Auditing:
  - Auditing of behaviors that occur when someone is trying to crack into your system.
  - Oracle Audit Vault
    - Or similar vendor products

Backup and Recovery

- The backup strategy that is selected must match the customer’s recovery requirements.
- It is probably wise to store backups offsite.
- TEST, TEST, TEST:
  - Standard database recovery.
  - Disaster recovery.

Passwords in scripts and script management

- Don't store passwords in plain text (in world readable command files)
- Don't pass passwords as arguments on the command line:
  - Put the passwords into
    - scripts (for SQL*Plus) or
    - parfiles (for export, import or SQL*Loader)
  - Use OPS$ORACLE accounts.
  - Use a construct like:

    ```
    echo <password> | <oracle-program> <username> <command line arguments>
    ```

Separation of duties

- Important regulatory concept.
  - Audit Vault supports this for audit-related data.
  - DBAs having their own IDs, instead of SYS or SYSTEM does as well.
- Often a staffing problem (for critical data, need separate Development and Production Support Teams)
- Access to critical data, like Personally Identifiable Information (PII), should be severely limited:
  - Perturb PII data.

Software Version/Production & non-Production

- Try to be on a version of Oracle that is supported by the Critical Patch Updates (CPUs).
  - As of the April 2007 CPU:
    - 9.2.0.7 & 9.2.0.8
    - 10.1.0.4 & 10.1.0.5
    - 10.2.0.2 & 10.2.0.3
  - Examine the CPU to see if it impacts the products you have installed:
    - Important security principle: only install what you need!
    - Configuration Management (ideally) or Inventory Management (minimally)
- Production databases should be separated from Test and Development

Other

- TNS Listener should be secured:
  - 9i and below:
    - Password protect it or
    - Disable runtime changes by setting ADMIN_RESTRICTIONS_<listener-name> to FALSE.
  - In 10g, per MetaLink Note# 260986.1, only the user that installed the software can administer the listener.
- Don’t use actual database and server names where they might be read by others, e.g.,
  - Internet newsgroups, for example, Oracle-L.
  - Don’t let contractors use the CSI#s from their previous customers!

Other (continued)

Be careful with PUBLIC grants:

- Try to avoid them for Application Objects
  - Better to use roles.
- Consider revoking access from PUBLIC for *some* Oracle-supplied stored procedures

Consider revoking from PUBLIC

- Execute privilege should be revoked from PUBLIC to the following stored procedures owned by SYS:
  - utl_file
  - utl_tcp
  - utl_http
  - utl_smtp
  - dbms_random
  - dbms_lob
  - sys.initjvmaux
  - dbms_job
  - dbms_scheduler
  - owa_util
- All privilege should be revoked from PUBLIC to the following stored procedures owned by SYS:
  - dbms_sql
  - dbms_sys_sql

?

References

- Slide 10: Diagram retrieved from http://en.wikipedia.org/wiki/CIA_Triad on 4 May, 2007
- Slide 21:
  - Center for Internet Security Benchmark for Oracle 9i/10g available here: http://www.cisecurity.org/
- Other sources for security checklists:
  - NIST Security Configuration Checklists Repository, http://checklists.nist.gov/repository/1006.html
- Finnegan:
  - http://www.petefinnigan.com/
- David Litchfield:
  - http://www.databasesecurity.com/
- Oracle-L:
  - http://www.freelists.org/archives/oracle-l/