General Data Protection Regulation

Kontrola bezpečnostních nastavení a bezpečnostní politika pro technologie Oracle

David Krch
Principal Consultant, Expert Services
Oracle Consulting

Září 2016

ORACLE
CONSULTING

ORACLE

Kontrola bezpečnostních nastavení pro technologie Oracle

Oracle Database | Oracle WebLogic | Oracle Service Bus

- Rychlé a přehledné zhodnocení
- Identifikace **chybných bezpečnostních konfigurací** technologií Oracle
  - Technologická bezpečnost
    - Klíčová pro celkovou bezpečnost systému
    - Eliminace možných chybných konfigurací
    - CVSS scoring identifikovaných rizik
    - Doporučení
    - Lze využít jako podklad pro navazující službu **Standardizace Bezpečnosti produktů Oracle**
- Službu lze doplnit podrobným **auditem přidělených uživatelských oprávnění**
  - Identifikace účtů se silnými oprávněními, úroveň přístupu k datům
  - Přehled o **zabezpečení aplikačních dat**

Kontrola bezpečnostních nastavení pro technologie Oracle

Výstupy

- Dokument
  - identifikovaná rizika
  - jejich CVSS scoring
  - doporučení
- Prezentace
  - podrobná prezentace výsledků auditu

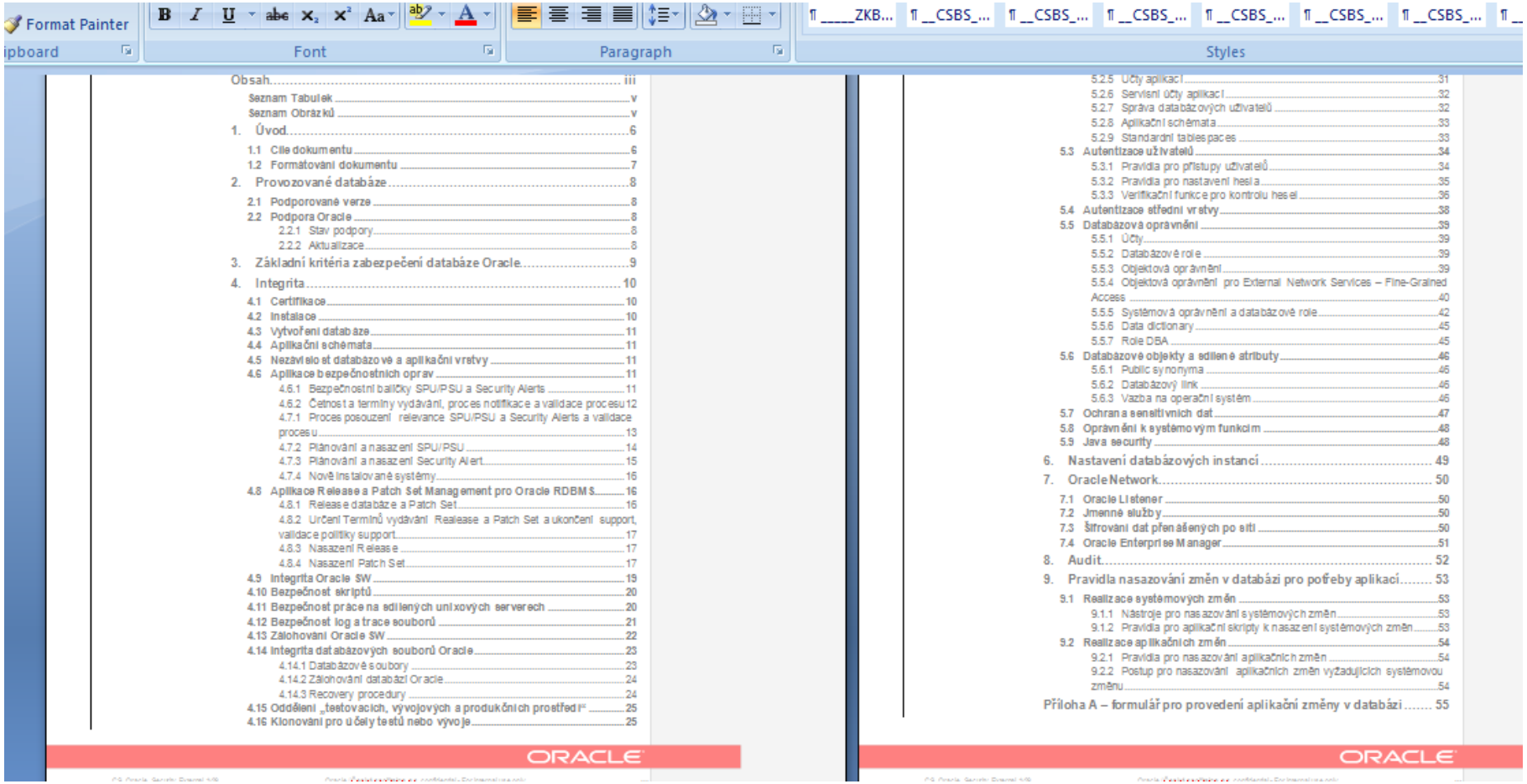
Audited Area	Evaluation	Score	Risk Treatment priority	Risk Treatment
Installed Components	Risk Exists	4.6	Medium	*Uninstall unnecessary components*
Security patches	Risk Exists	7.1	High	*Apply latest security patches, establish procedures for security patches management*
Authentication	OK	0.0	N/A	*N/A*
User password	OK	0.0	N/A	*N/A*
Password management	OK	0.0	N/A	*Use case sensitive passwords, setup password function for XXX_TEMP profile*
SYSDBA and SYSOPER roles	OK	0.0	N/A	Check if user XXX needs SYSDBA privilege
Batch task securing	Risk Exists	4.3	High	*Implement secure password store*
Database dictionary securing	OK	0.0	N/A	*N/A*
Database privileges	Risk Exists	4.0	Medium	*RMAN account shouldn't have a DBA role, verify the usage of OPS$XXXX account,XXXX has excessive privileges*
Public privileges	OK	0.0	N/A	*N/A*
Run-time facilities securing	OK	0.0	N/A	*N/A*
Oracle Listener securing	Risk Exists	1.7	Low	*Implement admin restrictions*
External Procedures securing	Risk Exists	4.6	Medium	*Check Extproc usage*
TNS Listener Poison Attack	Risk Exists	7.5	High	*Implement Oracle recommendation for listeners*
Database Auditing	Risk Exists	4.6	Medium	*Enable audit AUDIT_SYS_OPERATIONS*

Bezpečnostní politika pro technologie Oracle

- Podrobný bezpečnostní standard pro technologie Oracle
  - Obecná bezpečnostní politika je obvykle málo konkrétní
- Upraven na základě požadavků a situace konkrétního zákazníka, zapracovává
  - Naše zkušenosti
  - Stávající normy a postupy zákazníka
  - Národní, Industriální a jiné požadavky – PCI-DSS, ZoKB, EU GDPR
- Implementuje víc úrovní zabezpečení (např. ZKB, non-ZKB, PCI-DSS)
- Včetně **stanovení bezpečnostních požadavků na dodavatele pro technologie Oracle**
  - Standard má **externí a interní část**
  - Externí slouží pro definici požadavků na řešení dodavatelů

Bezpečnostní standard pro Oracle Database

Co zahrnuje – 2 dokumenty, 60 stránek, 70+ kontrolovaných parametrů



Framework pro zabezpečení pravidelného monitoringu

- **Aplikace umožňují sledovat a evidovat soulad se standardem**
  - Vazba na konkrétní pravidla standardu
  - Definovaná pravidla pro Oracle DB a MW
  - Porovnání s předchozím stavem
  - Identifikace chyb z pohledu předepsané konfigurace i oprávnění
  - Evidence nálezů, možnost jejich klasifikace

- **Správa nálezů a výjimek**
  - Jednotlivé nálezy lze dále zpracovávat
  - Díky správě výjimek již v následných auditech řešíte jen nové nálezy
- **Lokální vývoj a podpora**, provozováno ve významných bankách v ČR

Oracle Database Security Compliance Report

General Info

DBNAME	Db, Version	PSU	Oldest Audit Date	Hostname	Platform	PCI Mode	Captured Date
orcl	12.1.0.2.0	-- NONE --	27.11.2013 00:06:31	db12c.cz.oracle.com	Linux x86 64-bit	No	16.12.2014 13:07:50

Script Info

Standard Version	Config Download Date	Script Version
1.1	16.12.2014 13:06:33	1.20141216

Report Summary

Chapter Name	Cust. Compliance
3.2.1.7 Mandatory OS groups exist - dba, oinstall, oper	PASSED
3.8.1.4 Oracle Software Integrity - write permission for others not allowed	FAILED
3.8.1.5 Files in ORACLE_HOME must be owned by oracle:dba	PASSED
3.8.1.6 File permissions of the redundant files in $ORACLE_HOME/bin/ (oracleO, tnslsnr0, ...) have to be set to 0000 when no patch rollback is necesary anymore.	FAILED
3.11.1.2 Privileges on DIAGNOSTIC_DEST/diag and its subdirectories	PASSED
3.11.1.1 Directories background_dump_dest, user_dump_dest and core_dump_dest must beowned by oracle:dba with permissions rwxr-x---	PASSED
3.11.1.3 Privileges on AUDIT_FILE_DEST files - not for Unified Auditing	PASSED
	PASSED
	FAILED
	PASSED
	PASSED
	PASSED

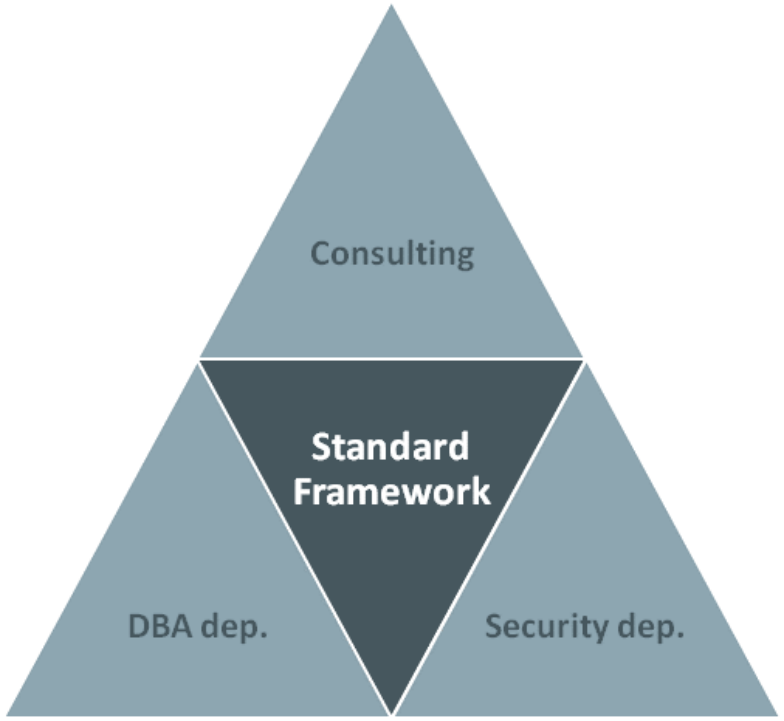
Detailed Report - Failed Items - Selected Section

3.8.1.4 - Oracle Software Integrity - write permission for others not allowed

	Edit	Privileges	Owner	Group	Name	Exception, Task, Comment	Cust. Compliance
☐	✎	-rwxrwxrwx	oracle	oinstall	/u01/app/oracle/product/12.1.0.2/dbhome_1/javavm/doc/readme.txt	Ex:Broader privileges required by Application ABC (DKRCH/30.11.2015)	PASSED(ex)
☐	✎	-rwxrwxrwx	oracle	oinstall	/u01/app/oracle/product/12.1.0.2/dbhome_1/javavm/doc/javadoc.zip		FAILED
☐	✎	-rwxrwxrwx	oracle	oinstall	/u01/app/oracle/product/12.1.0.2/dbhome_1/rdbms/doc/README_rdbms.htm		FAILED

Dodávka

- Kontrola bezpečnostních nastavení
  - Rychlá jednorázová kontrola
  - Základní **podklad pro standardizaci**
- Bezpečnostní politika
  - Vstupem jsou **bezpečnostní směrnice** organizace
  - Standard Oracle je upraven na základě požadavků a **situace konkrétního zákazníka**
- Framework pro zabezpečení pravidelného monitoringu
  - Připraven na základě odsouhlasené Bezpečnostní politiky
  - Možná **integrace na SIEM řešení**




ORACLE®