

ORACLE®

THE **INFORMATION** COMPANY

Tresch dm

Oracle Consulting,
Expert Services

Oracle adatbázis biztonságának megerősítése

Tapasztalatok

Tartalom

- Az „igazi” telepítések – amit láttunk
- A megerősítés területei
- Mire érdemes figyelni?
- Alapvetések
- A jövő megoldásai

Az Oracle Expert Services

- Oracle Expert Services: ha a rendszer nem az elvártaknak megfelelően működik, vagy elkel a szakértő kéz/fej/szem ...
- Egyik szolgáltatáscsomagunk az Oracle környezetek biztonsági megerősítése

Az „igazi” telepítések 1.

- Még kritikus környezetben is minden csomagot telepítünk...
 - *UTL_FILE, UTL_HTTP, UTL_TCP csomagok*
 - *Extproc funkcionalitás*
- A legtöbb kulcsfelhasználó vagy sématulajdonos dba jogokkal rendelkezik...
 - *Az adatfeldolgozó felhasználó,- ott is ahol üzletileg kritikus adatokat kezelnek - DBA, és a feltett kérdések, valamint az alkalmazás-architektúra ismeretében ezt sokszor nem is lehetett megváltoztatni.*
- Nincs naplózás, vagy a napló táblák nem védettek...
 - *Létrehoznak egy napló táblát, ebbe íródnak az események, de sem integritás sem más védelem nincs.*

Az „igazi” telepítések 2.

- Az audit – hát az jó, de minek?
 - *Ahol törvényi kötelezettség a naplózás, ott sem igazi audit napló készül, hanem van helyette egy log tábla.*
- Nem tipikusan RDBMS, de érdekes:
 - *Az interneten talált ~180 ezer telepített iAS szerver nagy része távolról is „felborítható”*
 - *Ha kiteszem a szerveremet a netre, akkor nem árt minél inkább “anonimizálni” – és ezt sem teszi meg szinte senki.*

A megerősítés területei 1.

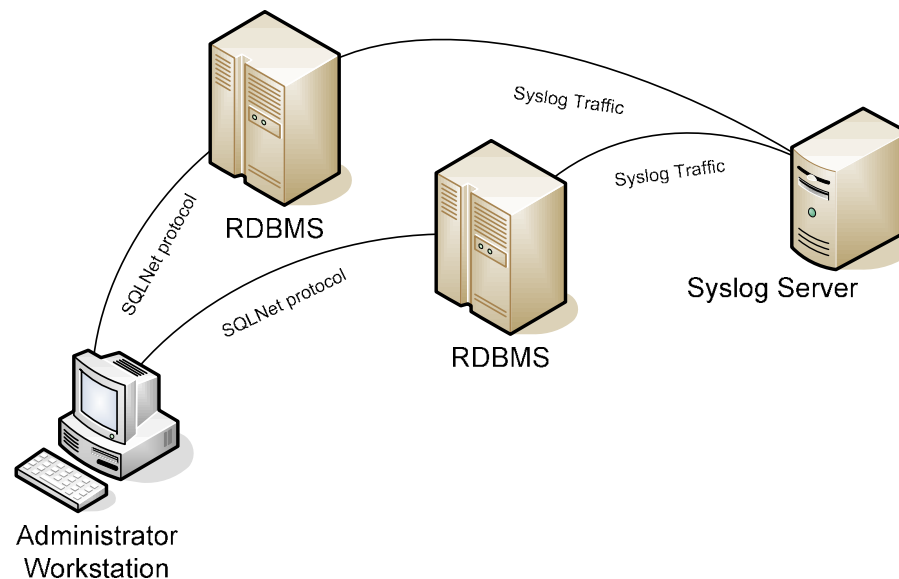
- Installáláskor
 - *Nem kell a user-nek oracle nevet adni*
 - *Nem kell a csoportnak oinstall nevet adni*
 - *Figyeljünk az umask-ra*
 - *Ne legyen senki más bejelentkezve a rendszerbe*
- Először operációs rendszer szinten kell tevékenykedni
 - *Minimalizált installálás után telepítsük az ORACLE-t, sok funkció nem szükséges az operációs rendszer csomagokból*
 - *Körül kell nézni a fájlrendszeren, hogy a jogosultságok megfelelően vannak e beállítva.*
 - *Ahol lehet használjunk sudo-t, hogy minimalizáljuk a korlátlan hozzáféréseket.*

A megerősítés területei 2.

- Az adatbázisból minden, nem szükséges funkciót el kell távolítani
 - *UTL_FILE, UTL_HTTP, UTL_TCP ... csomagok*
 - *Extproc funkcionalitás*
- Be kell állítani az auditot
 - *Az audit beállításához meg kell ismerkedni az alkalmazás funkcionalitásával. Tudnunk kell, hogy melyek a kritikus pontok a rendszerben, melyek azok a táblák, amelyekben „anomáliát” kell keresni, és tudnunk kell mi számít „anomáliának”.*
- Az auditot védeni kell
 - *Legbiztosabb az adatbázison kívülre auditálni*

A megerősítés területei 3.

- Az auditot syslogba irányítsuk, a syslogot meg egy másik szerverre, valahogy így



Alapvetések

- A fejlesztők vagy a rendszer tervezők a megmondható, hogy hogyan kell jól megtámadni a rendszert. – *kérdezzünk tőlük*
- Válasszuk szét a szerepköröket.
 - *A dba ne legyen egyben a rendszergazda is*
 - *A dba-k mind a saját nevükben dolgozzanak minden esetben*
- Mik ellen akarunk védekezni?
 - *Adat módosítás, adat törlés, adat beszúrás ... Attól függ melyik mire jó.*
- Hogyan akarunk védekezni?
 - *Vegyünk el minden jogot a felhasználóktól, csak a szükségeset kapják meg, ilyen szempontból a Connect és a Resource nem igazán jó párosítás.*

Alapvetések 2.

- A felhasználók jogainál néhány javaslat
 - Kerüljük azon jogosultságok alkalmazását, ahol a(z):
 - ANY szó szerepel.
 - ALL szó szerepel.
 - WITH ADMIN jogosultság szerepel.
 - WITH GRANT jogosultság szerepel.
 - CREATE PROCEDURE jogosultság szerepel.
 - ALTER SYSTEM jogosultság szerepel.
 - BECOME USER jogosultság szerepel.

Alapvetések 3.

- A paraméterezés csodákra képes, lássuk az init.ora egy két paraméterét
 - *audit_trail=os*
 - *audit_sys_operations=true*
 - *remote_os_authent= false*
 - *remote_os_roles= false*

Alapvetések 4.

- Az sqlnet.ora lehetőségei
 - *sqlnet_allowed_logon_versions=(9)*
 - *tcp.validnode_checking=yes*
 - *tcp.invited_nodes = (ip1,ip2,ip3)*
 - *interface binding*
- Az listener.ora lehetőségei
 - *save_config_on_stop_listener_name=false*

Hol vannak a hagyományos hardening határai?

- Egy biztos, ha támadni kell, akkor belülről fognak. (70-80%-ban)
- Mindíg a legolcsóbb az embert megvenni, ezért fontos a szerepkörök szétválasztása
- Túl sok audit = tű a szénakazalban
- Az audit napló elemzés és vizsgálat nélkül mit sem ér

A jelen/jövő megoldásai

- Ha biztonságra vágyunk:
 - Chipkártyás belépés
 - Rejtjelzett csatornák
 - Diszken tárolt adatok titkosítása
 - Kerberos Authentikáció
 - AD integráció
 - -> **Advanced Security**
 - Vége a DBA egyedi és korlátlan jogosultságának
 - -> **Database Vault**
 - Fejlett és biztonságosan tárolt log és audit szolgáltatások elemzésekkel
 - -> **Audit Vault**



Kérdések?

ORACLE®