Is Your Database Secured?

Heli Helskyaho
Miracle Finland Oy
Finland

Keywords:

Database, Security

Introduction

Usually when talking about security people mention firewalls and virus protection. Database security is more difficult than that. The importance of security is unfortunately quite often seen only after something bad happens.

The Survey

IOUG made a survey to their members in 2013 about database security. The survey is called "DATA SECURITY: LEADERS VS. LAGGARDS 2013 IOUG ENTERPRISE DATA SECURITY SURVEY (By Joseph McKendrick, Research Analyst Produced by Unisphere Research, a Division of Information Today, Inc. December 2013)" and can be found and downloaded from Oracle pages. My experience reflects this survey very much and that's why I add my experience to the survey results in this presentation. All statistics are from the survey and all opinions and interpretations are mine.

Term

Database is the place where all the important data/information is stored. Some of this data/information is public and some is private. The data/information is *secured* from people who should not see it but those people who should have access to it will have it. The data/information has leaked/breached to somebody who does not have permissions to it either accidentally or on purpose.

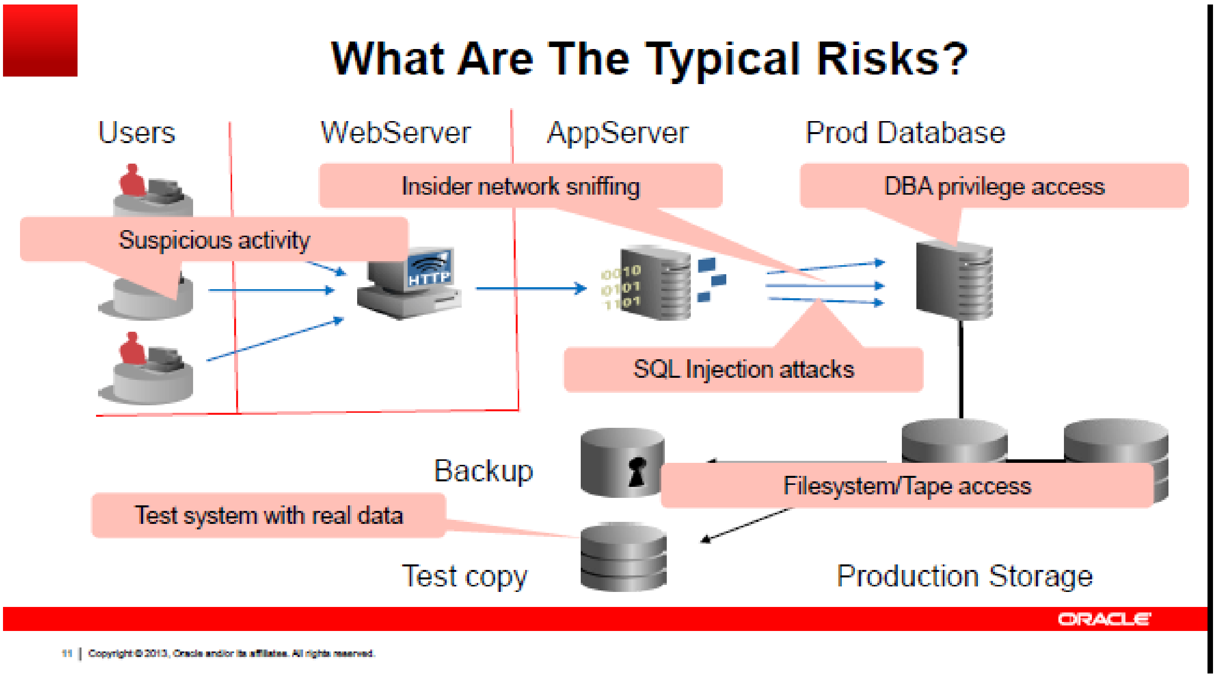
Why must the database be secured?

Usually the data/information is the most valuable asset of a company. If a unauthorized person has access to it:

- Competitors will have benefit
- Customers will be angry
- Reputation will be bad, image is gone
- ...
- Maybe even end of business.

Where does the data leak?

The data can leak while coming to database, while it is in the database, while going out the database or in any of the copies of the database. In this picture created by Jukka Männistö from Oracle Finland you can see the typical risks.



What Are The Typical Risks?

Users

WebServer

AppServer

Prod Database

Insider network sniffing

DBA privilege access

Suspicious activity

SQL Injection attacks

Backup

Filesystem/Tape access

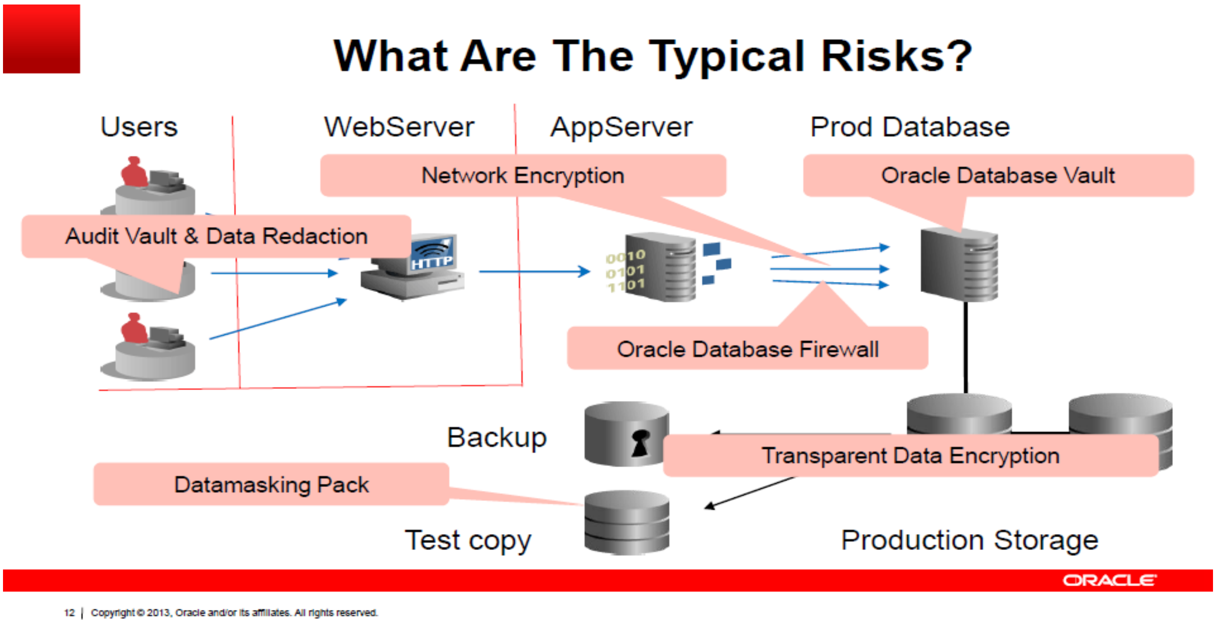
Test system with real data

Test copy

Production Storage

11 | Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

And in this picture also created by Jukka Männistö you can see what solutions Oracle has for those risks.



What Are The Typical Risks?

Users

WebServer

AppServer

Prod Database

Network Encryption

Oracle Database Vault

Audit Vault & Data Redaction

Oracle Database Firewall

Backup

Transparent Data Encryption

Datamasking Pack

Test copy

Production Storage

12 | Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

The Risk

In 2008 the survey shows that 20% thinks they might be in a risk of a data breach in the next 12 months. In 2013 36% sees that risk. The biggest risk seems to be a human error. The best way to prevent human errors are training, educating and implementing safeguards against data handling errors. 56% says they do not have any safeguards against administrator or developer data-handling errors and only 33% says they have.

Number of Databases and the data

The number of databases is growing. All the organizations have copies of their production databases: 69% has two or more copies. And 15% has five or more copies. 50% uses the production data in those copy databases, non-masked production data. Usually the non-production databases are not as well looked after as the production databases and getting the information from them is usually easier than from production. Number of databases can also lead to human errors. For instance an operation that was supposed to be done on test database is accidentally done in production database. Also the dump files or database links can cause a risk for leaking information.

Prevent

The first thing to prevent is when installing the database. Never install with default settings. Make sure the password is good, changes frequently, known by only limited number of people, maybe encrypted and never hardcoded. Hardcoded means that if you change the password the program does not work without changing it. Make sure the user privileges are designed, implemented as designed and maintained. Also make sure the privileges are implemented in the right level.

To be able to prevent a data leak you must know your data. In 2013 70% of the users said they are aware of all the databases with sensitive or regulated information. Those other 30% has no change to prevent anything before they know what they have to protect. The encryption is a good way to protect data in rest and data in motion. 70% encrypts data at rest in at least some of their databases, in 2008 the same number was 57%. A sad thing is though that in 2008 29% said they encrypt all the databases and in 2013 only 20% said the same. Most likely the growing number of databases has caused this change. In 2013 65% says they have encrypted data in motion in at least some of the databases while in 2008 52% said the same. Only 53% is using any kind of masking for sensitive data. To my experience the excuses for not using masking are something like this:

- Takes too much time
- Is too difficult
- Everybody has signed the NDA
- We trust our employees
- All these people have access to production anyway
- …

Detect

How do you know there has been a breach/leak? How do you know who did or did not do it?
Do you have monitoring in place? Only 39% can prove that privileged users were not tampering the sensitive data. 33% does not know how long it will take to detect and correct unauthorized database access or change. 29% says it takes 1-5 days. This is a very long time.

Administrate

Data Security Audits would be a good way to keep up the security level. Unfortunately security audits are not done quite often and the reason seems to be the long preparations for the audit.46% says it takes 1-5 days to prepare a database security audit.

Security Plan

The highest management in the company is responsible for the database security. The problem usually is that they do not understand what database security means and what risks have been taken in the company, at least not before it's too late. Every company should have a Security Plan approved by the management. The Security Plan should include for instance all the risks taken and plans on improving the security level. Security plan must be supported by the highest management.

The Media

Media is doing a good work on educating people on risks on security. In Washington Post there was an article: "Stop worrying about mastermind hackers. Start worrying about the IT guy" in October 17th, 2014: http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/17/stop-worrying-about-mastermind-hackers-start-worrying-about-the-it-guy

This article was about a security risk in Oracle Reports found by a security research Dana Taylor.
Dana Taylor found this problem and reported to Oracle as well as wrote a blog post about it: http://blog.netinfiltration.com/2014/10/15/massive-oracle-reports-data-exposures/
Afterwards she also posted about her recommended solution:
http://blog.netinfiltration.com/2014/10/18/operation-oracle-reports-anti-databreach/
In Washington Post they summarized that the problem was related to "mistakes in setting up popular office software" and "that computers need a 'Do-What-I-Mean' function". That means in short that if you installed the software with default settings you were in a risk. In the article they quoted Ben Caudill of Rhino Security Labs who said: "A lot of time organizations don't really know what's publicly accessible, and that becomes a real big problem.". In the article they also said: "Security issues typically get attention and resources, experts say, only when something goes wrong.". Oracle gave the solution to the problem but not many actually implemented it. Joseph Lorenzo Hall, chief technologist for the Center for Democracy & Technology, who said in the article: "To think that a local government IT administrator in a small town is going to be able to adequately protect from all threats is woefully misguided.". I think that in this article The Washington Post, a newspaper to common people, managed to describe all the concerns that were shown in the survey and more. Human error was 77% a risk for our data in the survey made in 2013 but if we do not do anything the number will be bigger in the next survey.

Contact address:

Heli Helskyaho
Miracle Finland Oy
Hermannin rantatie 12 A
00580 Helsinki, Finland

Phone: +358(0)503838152
Fax:

Email	heli@miracleoy.fi
Internet:	helifromfinland