# *Comment améliorer la sécurité de vos bases de données Oracle ?*

Marco Anzile, ORACLE Switzerland

## Introduction

« Les entreprises doivent comprendre que personne n'est à l'abri d'un vol de données. Il peut s'écouler des semaines ou des mois avant que l'on identifie la brèche, quand l'intrusion, elle, n'a souvent pris que quelques minutes ou quelques heures », explique M. Baker,  principal auteur du rapport DBIR (Verizon Data Breach Investigation Reports). Ce rapport est disponible en anglais et en français, voir les ‘'Recommandations de lecture'' à la fin de l'article.

En résumé, ce rapport de 63 pages (voir figure 1) qui compile plus de 47'000 vols de données dans le monde sur les dix dernières années, nous montre que :

- 67% des vols ont lieu sur des serveurs, ce qui paraît logique, puisque les serveurs sont la cible naturelle des personnes ou organisations malintentionnées appelées « cybercriminels » dans cet article. On peut aussi noter que 33% des vols ont lieu sur des ordinateurs personnels ; mais cela représente une quantité des données volées nettement moindre. Bien sûr, tout dépend de la valeur (commerciale, concurrentielle, propriété intellectuelle ou autres telle que la réputation) de la donnée volée.

- 76% des vols ont pu se faire simplement par une faiblesse de la configuration des droits d'accès (abus de privilèges) ou un vol de ces droits d'accès (usurpation d'identité). Cela signifie simplement que la gestion des droits d'accès est généralement mal configurée, avec des mots de passe trop faibles et surtout mal comprise (notamment l'attribution des privilèges). Les vols des droits d'accès sont plus problématiques et se font par un scénario assez classique aujourd'hui, en quatre étapes :

  - Ciblage d'une personne de l'entreprise ayant des responsabilités systèmes grâce aux réseaux sociaux (par exemple, tapez DBA dans le moteur de recherche de Linkedin, sans même avoir un compte premium, et vous trouverez 433'032 occurrences de personnes ayant ce mot-clé dans leur profile).
  - Lui envoyer un faux courriel au nom d'un de ses collègues ou amis avec une justification bidon et un lien permettant d'installer un logiciel espion sur son poste de travail. Notez que l'on pourrait également le contacter physiquement et sympathiser, le corrompre ou faire pression sur lui…
  - Grâce au logiciel espion, récupérer des informations de connexions et des droits d'accès des systèmes dont il est responsable.
  - Utiliser ces informations pour se connecter directement sur les machines ciblées et voler les données.

- 69% des vols ont été découverts par des personnes ou sociétés externes à l'entreprise. Cela montre bien que les entreprises n'ont qu'une faible connaissance de ce qui se passe dans leurs bases de données et qu'elles ne sécurisent pas les données sensibles, mais les infrastructures en général. Il est donc essentiel d'avoir des outils de surveillance, d'alertes et de rapports automatisés et ne pas uniquement faire confiance aux utilisateurs (dont les accès peuvent être usurpés).

- 97% des vols auraient pu être évités grâce à des mesures simples, et nous allons voir, quelles sont ces mesures dans le chapitre suivant.

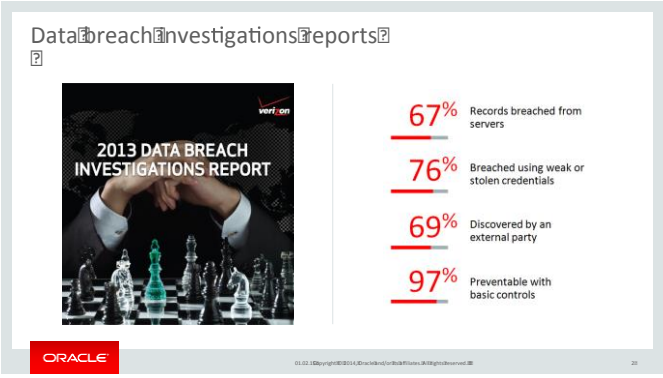


*Figure 1*

Donc, comment améliorer la sécurité de ses bases de données ? La méthodologie que nous proposons d'utiliser consiste à séparer les différents domaines composant un système de base de données et de les sécuriser individuellement, comme décrit dans la figure 2. Le but étant de passer d'un niveau standard à un niveau de sécurité plus élevé.

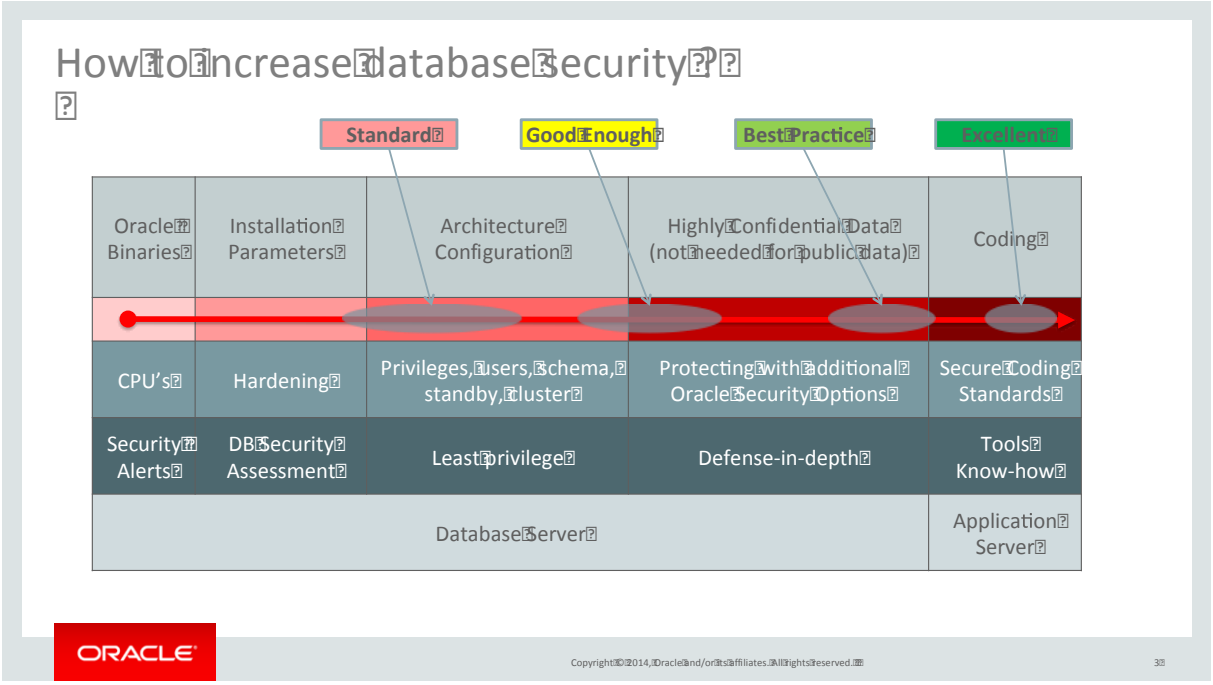


*Figure 2*

## 1. Oracle Binaries

La première étape pour sécuriser votre base de données est bien évidemment de regarder de plus près le noyau Oracle et donc les versions du logiciel installé. Durant les 5 ans de durée de vie (avec le Premier Support) d'une version de base Oracle, il y a 2 releases majeures (par exemple 12.1 et 12.2) dont 1 Patchset pour la release 1 (PS1 pour 12.1.0.2) et 3 Patchset pour la release 2.
Tout d'abord, il est recommandé d'être au dernier niveau de correctifs ou « patchs » appelés PSU (pour Patch Set Update), bien que cela ne soit pas toujours possible pour des raisons organisationnelles et/ou fonctionnelles, cela fait partie des bonnes pratiques d'administration d'une base de données. Ces PSU sont une installation complète des binaires et peuvent impacter différents composants telle que : Oracle Database Server, Oracle Grid Infrastructure, Oracle Database Client, etc.
Ensuite, il est recommandé d'appliquer les alertes de sécurité. Pour cela, Oracle a prévu des correctifs appelés CPU (pour Critical Patch Update) délivrés tous les trois mois (en fait, tous les mardis les plus proches du 17 des mois de janvier, avril, juillet et octobre) qui sont un ensemble de corrections de failles de sécurité du code Oracle (pas de correction de bugs, pas de nouvelles fonctionnalités, pas d'impact de performances). Ces failles sont classifiées en fonction de leur dangerosité, avec le système de notation CVSS (Common Vulnerability Scoring System), qui vous permettra d'évaluer la pertinence du CPU.

Les CPU ne corrigent pas de bugs comme les PSU et donc, sont plus petits et n'ont pas d'impacts fonctionnels qui nécessiteraient de faire des tests de régressions. Ces correctifs sont cumulatifs, c'est-à-dire qu'il suffit d'installer le dernier correctif pour être à jour. À noter également qu'un PSU, qui est

également cumulatif, contient le dernier CPU. Dernière remarque, les CPU s'appellent SPU (pour System Patch Update) à partir d'Oracle 12c.

Vous pouvez vous inscrire sur le site d'Oracle Technology Network pour recevoir les alertes de correctifs par courriel.

✓ ***Recommandations de lecture:***

***Oracle Technology Network – Security Alerts***
*http://www.oracle.com/technetwork/topics/security/alerts-086861.html*
***Common Vulnerability Scoring System***
*http://www.first.org/cvss*
***Voir les notes du support Oracle suivante :***

- *Patching Oracle Database Server (Doc ID 1446582.1)*
  - *Release Schedule of Current Database Releases (Doc ID 742060.1)*
  - *Oracle Recommended Patches -- Oracle Database (Doc ID 756671.1)*
  - *Lifetime Support and Support Policies - Oracle Database Overview (Doc ID 1351163.1)*

## 2. Installation/Parameters

Ensuite, il faut accorder une attention particulière aux paramètres d'initialisation de la base de données, des paramètres de configuration du réseau et de l'installation des binaires sur le système de fichiers. Pour cette étape de durcissement ou « hardening », il existe beaucoup de littérature, des blogues et des listes de vérification appelées « check-lists » (les plus connues étant SANS SCORE, DOD STIG, CIS Benchmark…) qui vont vous aider à parcourir ces paramètres et vous proposer de modifier les valeurs par défaut.

Depuis la version 11g, Oracle propose le « Security Guide » qui parcourt l'ensemble des points à vérifier pour sécuriser et renforcer sa base de données. Et notamment, les bonnes pratiques de durcissement des paramètres d'initialisation.

À noter également, qu'Oracle propose un service gratuit d'évaluation de votre niveau de sécurité sur une base de données. Ce service est appelé « DB Security Assessment » et ne demande pas beaucoup d'efforts de la part du client. En effet, il suffit d'exécuter un script sur la base qui récoltera des informations de paramétrage et d'envoyer le résultat à Oracle qui le fera analyser par ses experts en sécurité. Une présentation des faiblesses de sécurité et des recommandations associées sera ensuite présentée.

✓ ***Recommandations de lecture:***

***Oracle Security Guide***
*http://docs.oracle.com/database/121/DBSEG/toc.htm*

***Securing the Database Installation and Configuration***
*http://docs.oracle.com/database/121/TDPSG/tdpsg_install_config.htm#TDPSG60000*

**Voir la note du support Oracle suivante :**

- *Security Checklist: 10 Basic Steps to Make Your Database Secure from Attacks (Doc ID 1545816.1)*

## 3. Architecture/Configuration

Pour sécuriser cette partie, il faut avoir une connaissance approfondie de la compréhension de la définition des utilisateurs, de l'attribution des droits et de la définition des droits d'accès. C'est un travail auquel l'administrateur de la base de données (dont le savoir-faire sera mis à contribution) et les développeurs doivent collaborer étroitement.

Pour vous aider dans cette tâche, dans l'annexe A du «  Security Guide », Oracle propose un ensemble de bonnes pratiques de configuration et adopte la stratégie du « least privilège », c'est-à-dire de n'accorder que le minimum de privilèges à un utilisateur afin qu'il puisse effectuer sa tâche correctement. Il faut donc configurer des utilisateurs avec des comptes limités et contrôlés ainsi que de prévoir une séparation des tâches.

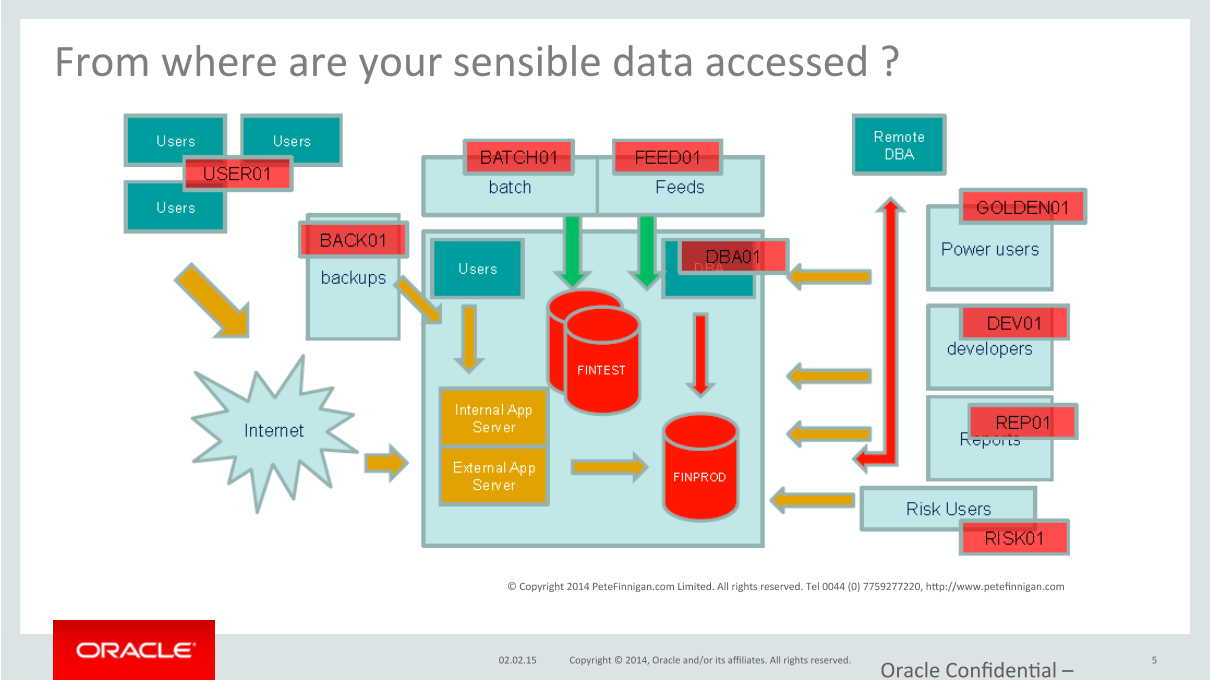


*Figure 3*

On voit très bien dans la figure 3 que la configuration du contrôle d'accès n'est pas si anodine, puisqu'il faut tenir des comptes : d'utilisateurs locaux, d'utilisateurs applicatifs, d'utilisateurs privilégiés, d'utilisateurs à distance, de tâches de fond, de processus de réplication, de sauvegarde, etc. La liste est longue et dépend de l'architecture en place.

Cette partie est également couverte par le service « DB Security Assessment » cité dans le paragraphe précédent.

On rappelle qu'il est important d'activer l'audit sur vos bases de données. Pour information, l'audit est activé par défaut depuis la 11g et il y a seulement un paramètre à configurer dans le fichier d'initialisation de la base. Oracle fournit les bonnes pratiques de configuration de l'audit des accès administratifs, des connexions, des privilèges et des objets dans le « Security Guide ». Remarquez que logiquement, l'audit des accès répond à la majorité des normes de conformité règlementaire (PCI-DSS, SOX, etc.).

- ✓ ***Recommandations de lecture:***

***A: Keeping Your Oracle Database Secure :***
*http://docs.oracle.com/database/121/DBSEG/guidelines.htm#DBSEG009*

***Voir les notes du support Oracle suivante :***

- *Oracle Password Management Policy (Doc ID 114930.1)*
- *Master Note For Privileges And Roles (Doc ID 1347470.1)*
- *Master Note For Oracle Database Auditing (Doc ID 1299033.1)*
- *Master Note For Oracle Database Authentication (Doc ID 1349896.1)*
- *All About Security: User, Privilege, Role, SYSDBA, O/S Authentication, Audit, Encryption, OLS, Database Vault, Audit Vault (Doc ID 207959.1)*

## 4. Data Security

Dans cette quatrième étape, on va se concentrer sur la sécurité des données elle-même et non de l'infrastructure. Pour cela, avant de définir quelles sont les options de sécurité à mettre en œuvre, il faut bien évidemment classifier les données de l'entreprise en fonction de leur niveau de sensibilité.

Cela permettra, premièrement d'avoir une vision globale des données sensibles, deuxièmement de savoir où elles se trouvent dans l'entreprise, troisièmement de savoir qui les produit et qui les utilise et quatrièmement d'implémenter des surcouches de sécurité en fonction du niveau de sensibilité des données. En effet, on ne va pas mettre en œuvre les mêmes outils pour sécuriser une base de données contenant des données publiques, internes, stratégiques, de clients ou des données de propriété intellectuelles car les investissements ne seront pas les mêmes. À ce sujet, il existe une littérature abondante, dont de nombreuses normes (par métier ou fonctionnelles) et des outils d'aide à la classification.

Comme on le voit dans la figure 3, une donnée sensible dans une table peut se retrouver dans plusieurs endroits assez rapidement dus au fonctionnement du moteur de base de données Oracle. En effet, on peut retrouver vos données dans des fichiers de trace, des fichiers d'historiques, des indexes, des fichiers de trace des serveurs applicatifs, sur des serveurs de tests, de développement et de reprise en cas de sinistre, et ainsi de suite, la liste est longue. Cette partie implique donc une connaissance approfondie de l'architecture du moteur de base de données et de son fonctionnement.

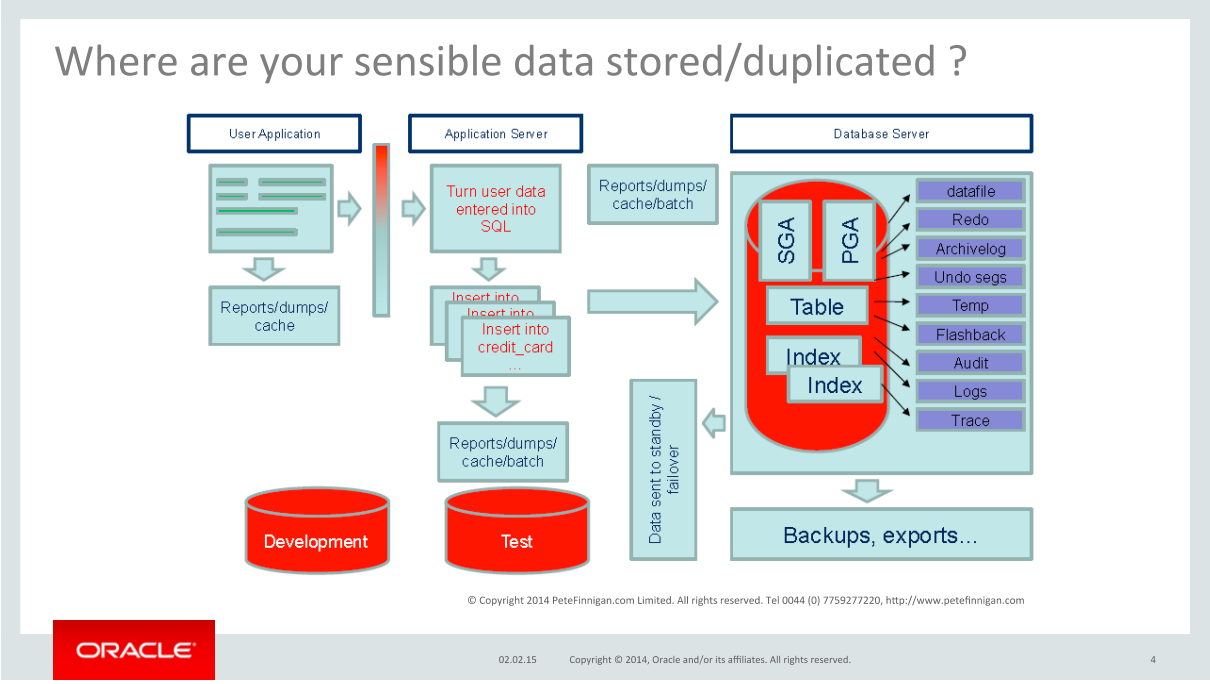


*Figure 4*

Depuis toujours, Oracle propose la technologie la plus pointue pour protéger les données où elles se trouvent - dans la base de données. Oracle propose une gamme complète de solutions de sécurité garantissant la confidentialité des données, la protection contre les menaces d'initiés et la conformité à la réglementation.

Dans l'approche « Defense-in-depth », Oracle propose différentes fonctionnalités, options, et extensions qui vont permettre de sécuriser directement les données. Les puissantes fonctions

de contrôle et de blocage des activités de base de données, de contrôle d'accès d'utilisateur privilégié et multicritères, de classification des données, de cryptage transparent des données, d'audit et de reporting consolidés, de gestion sécurisée des configurations et de masquage des données d'Oracle permettent de déployer des solutions fiables et économiques, sans avoir à modifier les applications. La figure 5 classe les solutions de sécurité Oracle selon trois piliers : Prévention (la menace est connue), Détection (contre les tentatives de vol en cours), Administration (renforcement des paramètres de l'installation) :

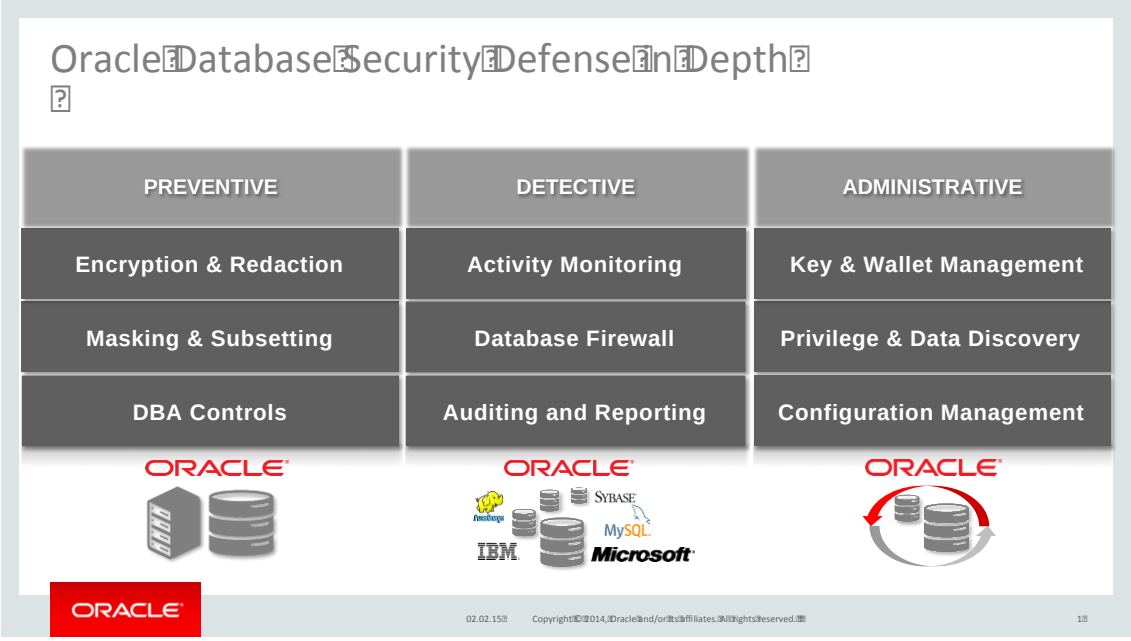


*Figure 5*

Deux exemples d'option de sécurité additionnelle :

Par exemple, des données sensibles stockées dans une table peuvent être vues au niveau du système de fichiers grâce un éditeur hexadécimal même si la base de données n'est pas démarrée. Le seul moyen de prévenir cette menace est de chiffrer les données au moyen de l'option Oracle Advanced Security.
Un autre exemple, très problématique aujourd'hui, est que l'administrateur système peut accéder à toutes les données d'une base de données grâce au rôle DBA (qui contient tous les privilèges). Pour résoudre ce défi, Oracle propose l'option Oracle Database Vault (c'est une surcouche de sécurité intégrée dans le noyau de la base de données) qui implémente une séparation des tâches forte, protège vos données sensibles des utilisateurs privilégiés ayant le rôle DBA et assure aussi la mise en œuvre des règles définissant par qui, quand, où et comment les applications, les bases de données et les données, peuvent être accédées.

✓ ***Recommandations :***

***Introduction to Oracle Database Security***
*http://docs.oracle.com/database/121/TDPSG/toc.htm*

***Voir les notes du support Oracle suivante :***

- *Master Note For Transparent Data Encryption ( TDE ) (Doc ID 1228046.1)*
- *Master Note For Oracle Database Vault (Doc ID 1195205.1)*
- *Master Note For Oracle Audit Vault [Document 1199033.1]*
- *Master Note For Enterprise User Security (Doc ID 1376365.1)*

## 5. Coding

La dernière partie à sécuriser est le code de l'application. En effet, une application qui n'a pas été développée dans les règles de l'art au niveau de la sécurité est une faille importante de sécurité par laquelle des cybercriminels peuvent passer. Ce code est généralement déployé sur un serveur applicatif, mais peut aussi être déployé dans la base de données. Voici par exemple, quelques aspects de sécurités qui doivent être pris en compte au niveau applicatif :

- Se protéger des techniques d'injection SQL
- Ne pas stocker de mot de passe en dur dans le code
- Transmission de l'utilisateur final au travers de comptes techniques applicatifs

Vous trouverez au chapitre 8 du « Oracle Security Guide » les bonnes pratiques de développement sécurisé (et donc la réponse aux deux exemples cités ci-dessus). Dans le cas des techniques d'injections SQL, elles sont utilisées avec succès malgré le fait qu'elles existent depuis plus de 12 ans. Apparemment, les développeurs ne sont pas encore tous formés à développer en ayant la sécurité comme objectif.

Dans la plupart des cas, on n'a pas accès au code, car c'est un logiciel qui a été acheté à un fournisseur. Dans ce cas, il faut placer un outil d'analyse de requêtes SQL entre le serveur applicatif et le serveur de base de données qui bloquera les requêtes litigieuses avant même qu'elles soient exécutées sur le serveur. Pour cela, Oracle propose Database Firewall.

Si l'application est un développement spécifique, il faut vérifier que les bonnes pratiques de développement sécurisé existent et soient appliquées. Il y a beaucoup de littérature également à ce sujet. Par exemple, Oracle développe ses propres produits avec des règles de bonne pratique de sécurité (pour information, c'est un document interne de 300 pages), avec l'utilisation intensive du package PL/SQL DBMS_ASSERT (qui permet de valider les saisies) et avec le logiciel « HP Fortify Static Code Analyser » pour valider le code.

Pensez également à protéger le code lui-même s'il contient des informations d'ordre de la propriété intellectuelle. Pour cela, il existe des logiciels de

- Scanning (pour chercher des vulnérabilités connues dans le code)
- Obfuscation (pour rendre votre code difficilement compréhensible pour un humain)
- Watermarking, birthmarking ou de checksum (pour s'assurer que le code n'a pas été modifié)
- Wrapping (pour le chiffrage du code, d'ailleurs Oracle propose un utilitaire « wrap.exe » pour le PL/SQL)

Dans la pratique, il faudra trouver un compromis entre les risques, la sécurité, la lisibilité et la performance du code.

La version Oracle 12c, en autres nouvelles fonctionnalités (plus de 500), des fonctions PL/SQL ont été revisitées pour plus de sécurité, et notamment les notions « definer rights », exécution d'une procédure avec les mêmes droits que le propriétaire de la procédure et « invoker rights », exécution d'une procédure avec les droits de l'utilisateur invoquant la procédure. Le support de la norme FIPS 140 pour les modules de chiffrements des données, le support de SHA-2 pour le chiffrage des mots de passe, un

moteur d'audit conditionnel unifié performant travaillant en mémoire et surtout des nouveaux rôles permettent une séparation des tâches encore plus granulaire.

✓ ***Recommandations de lectures:***

***Oracle Secure Coding Standards***
*http://www.oracle.com/us/support/assurance/development/secure-coding-standards/index.html*

***Changes in Oracle Database Security 12c Release 1 (12.1.0.2)***
*https://docs.oracle.com/database/121/DBSEG/release_changes.htm#DBSEG000*

***8. Managing Security for Application Developers***
*https://docs.oracle.com/database/121/DBSEG/app_devs.htm#DBSEG005*

***5. Security Guide***
http://docs.oracle.com/database/121/DBSEG/dr_ir.htm#DBSEG658

***Security Scanner***
http://www.pfclscan.com

***PL/SQL protection tool***
http://www.pfclobfuscate.com

## Conclusion

En conclusion, on voit que la sécurité des bases de données est complexe et nécessite une connaissance approfondie de l'architecture, de son fonctionnement ainsi qu'un travail de classification des données sensibles. La sécurité des données demande une discipline presque militaire pour y couvrir tous les aspects. Pour cela, une méthodologie est nécessaire et j'espère que cette approche pragmatique et simple en cinq étapes, vous aura aidé à y voir plus clair.

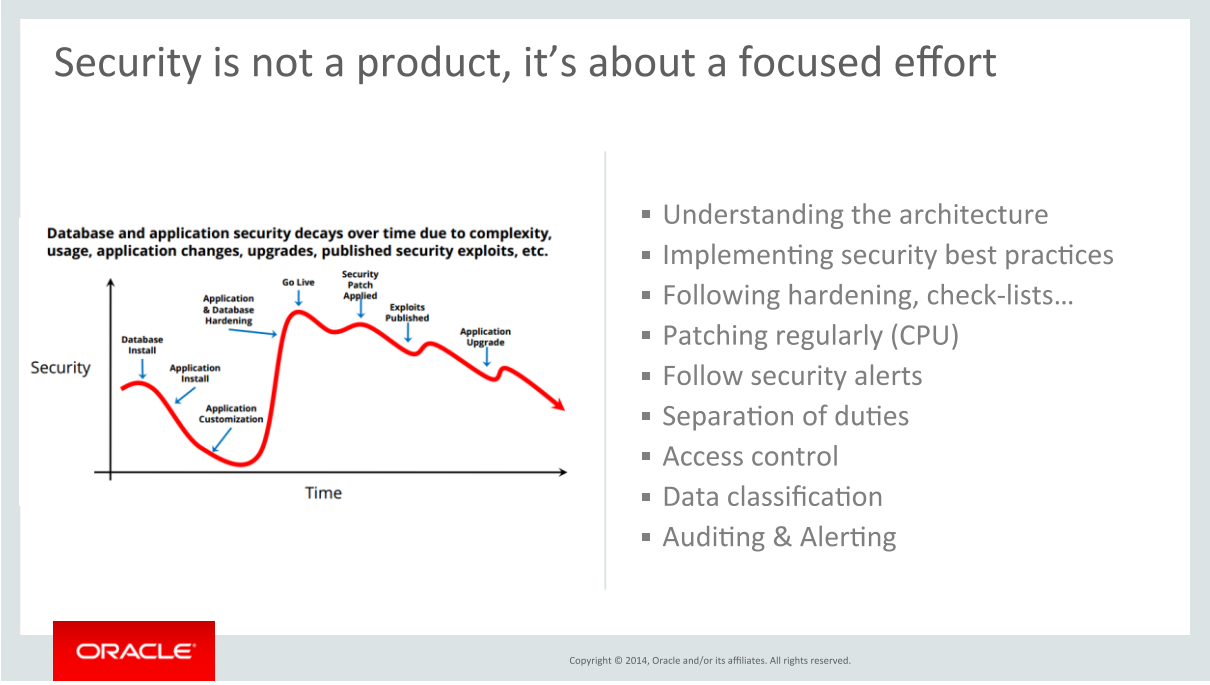


*Figure 6*

Pour terminer, la sécurité n'est pas un produit ou un ensemble de produits à installer, mais résulte d'une approche systémique et d'une attention régulière pour suivre les évolutions de la technologie, comme décrite dans la figure 6. L'affrontement entre les entreprises et les cybercriminels ne fait que commencer, et aujourd'hui, l'avantage est à ces derniers…

Pour une présentation détaillée des solutions de sécurité Oracle, d'un service gratuit d'évaluation de sécurité d'une base de données Oracle « DB Security Assessment » ou des propositions de mise-en-œuvre d'options de sécurité, vous pouvez contacter Oracle Suisse ou me contacter directement par email: marco.anzile@oracle.com

- ✓ ***Recommandations de lecture:***

***La Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI***
http://www.melani.admin.ch/?lang=fr

***Verizon Data Breach Investigation Reports***
http://www.verizonenterprise.com

***CVE, a dictionary of publicly known information security vulnerabilities and exposures***
http://cve.mitre.org/index.html

***The CERT Division***
http://www.cert.org/

***Computer Emergency Response Team - Industrie, Services et Tertiaire***
http://www.cert-ist.com/public/

***Open Security Foundation's DataLossDB***
http://datalossdb.org/

***Oracle Security Blog***
https://blogs.oracle.com/security