Le top 10 des menaces de sécurité des bases de données

Comment limiter les principales vulnérabilités des bases de données ?

L'infrastructure de la base de données d'une entreprise est sujette à un grand nombre de menaces. Ce document vise à aider les entreprises à mieux appréhender les menaces les plus critiques.
Ce document fournit une liste des 10 principales menaces, identifiées par notre centre d'experts.

Pour chacune de ces menaces, ce document décrit les informations de base, les principales stratégies de limitation des risques, ainsi que le dispositif de protection de la base de données fournies par la solution Imperva.

Les 10 principales menaces de sécurité des bases de données

1. Abus de privilège excessif
2. Abus de privilège légitime
3. Elévation de privilège
4. Exploitation de failles des bases de données vulnérables ou mal configurées
5. Injection SQL
6. Faiblesse de l'audit natif
7. Déni de service
8. Vulnérabilités des protocoles de communication des bases de données
9. Copies non autorisées de données sensibles
10. Exposition de données de sauvegarde

En se préoccupant de ces 10 menaces, les organisations répondront aux exigences mondiales de conformité et aux pratiques d'excellence de l'industrie en matière de protection des données et de limitation des risques.

Menace n° 1 – Abus de privilège excessif

Lorsque les utilisateurs (ou les applications) ont des privilèges d'accès à une base de données excédant les exigences de leur fonction professionnelle, ils peuvent abuser de ces privilèges à des fins malveillantes. Par exemple, un directeur d'université dont la fonction n'exige que la capacité à modifier les coordonnées des étudiants peut profiter de privilèges de mise à jour de bases de données excessifs pour modifier les notes.

L'utilisateur d'une base de données peut se retrouver avec des privilèges excessifs pour la simple raison que les administrateurs de bases de données n'ont pas le temps de définir ni de mettre à jour des mécanismes de contrôle granulaire des privilèges d'accès pour chaque utilisateur. Par conséquent, tous les utilisateurs ou les grands groupes d'utilisateurs ont des privilèges d'accès génériques définis par défaut qui excèdent largement les exigences de leur fonction spécifique.

Prévention des abus de privilège excessif – Elimination des droits excessifs et application d'un contrôle d'accès des requêtes

La solution à la menace présentée est l'élimination de tous droits excessifs. Ceci requiert la capacité à identifier les droits excessifs, c'est à dire les droits qui ne sont pas nécessaires à l'utilisateur pour remplir sa fonction. Cela s'effectue par l'extraction des droits depuis les bases de données, la corrélation des droits avec l'utilisateur professionnel et enfin par l'analyse de ces droits. C'est une procédure décourageante qui, si elle est effectuée manuellement, demande à la fois du temps et des ressources. Une solution automatisée peut réduire considérablement le temps et les ressources nécessaires et raccourcir la procédure d'analyse.
Afin de mieux appliquer les droits d'accès, des contrôles d'accès des requêtes granulaires sont également nécessaires. Le contrôle d'accès des requêtes fait référence à un mécanisme qui restreint les privilèges d'accès aux bases de données à un minimum requis d'opérations SQL (SELECTIONNER, METTRE A JOUR, etc.) et de données. La granularité du contrôle d'accès aux données doit être étendue du simple tableau, aux lignes et aux colonnes spécifiques à l'intérieur d'un même tableau. Un mécanisme de contrôle d'accès des requêtes suffisamment granulaire permettrait au directeur d'université malveillant décrit précédemment de mettre à jour les coordonnées des étudiants, mais déclencherait une alerte si ce dernier tentait de modifier les notes. Le contrôle d'accès des requêtes est utile non seulement pour détecter les abus de privilège excessif par des employés malveillants, mais aussi pour prévenir la plupart des 10 principales menaces décrites dans ce document. La plupart des implémentations de logiciels de bases de données intègrent un certain niveau de contrôle d'accès des requêtes (déclenchements d'alertes, sécurité au niveau des lignes, etc.), mais le caractère manuel de ces fonctionnalités « intégrées » les rend peu pratiques pour tous, à l'exception des déploiements les plus limités. Définir manuellement une règle de contrôle d'accès des requêtes pour tous les utilisateurs pour l'accès aux lignes, aux colonnes et aux opérations des bases de données prend simplement trop de temps. Pour rendre la situation plus difficile, les rôles des utilisateurs changeant au fil du temps, les règles de requêtes doivent être mises à jour pour refléter ces nouveaux rôles ! La plupart des administrateurs de bases de données auraient des difficultés à définir une règle de requêtes utile pour un petit nombre d'utilisateurs à un moment donné dans le temps. Ceci serait plus facile à définir pour des centaines d'utilisateurs au fil du temps. Par conséquent, la plupart des organisations attribuent aux utilisateurs un ensemble générique de privilèges d'accès excessifs pouvant être appliqués à un grand nombre d'utilisateurs. Des outils automatisés sont nécessaires pour que le contrôle d'accès des requêtes soit réellement appliqué.

SecureSphere Dynamic Profiling – Gestion des droits utilisateur et contrôle d'accès des requêtes automatisé

SecureSphere User Rights Management for Databases ou URMD (technologie de gestion des droits d'accès aux bases de données) permet l'attribution et la révision automatique des droits utilisateur, l'analyse des droits d'accès aux données sensibles et l'identification des droits d'accès excessifs et des utilisateurs inactifs basées sur le contexte organisationnel et l'utilisation réelle des droits utilisateur.

L'accès aux objets sensibles doit être autorisé sur la base du principe « besoin de connaître » et il est généralement défini par le contexte organisationnel des utilisateurs. En ajoutant des détails tels que le rôle et le département de l'utilisateur, les vérificateurs ont une totale visibilité sur la fonction professionnelle de l'utilisateur et le type de données auxquelles il/elle peut accéder. Les vues analytiques de la technologie URMD permettent aux vérificateurs de déterminer si les droits d'accès de l'utilisateur sont correctement définis et de supprimer les droits d'accès excessifs qui ne sont pas nécessaires aux utilisateurs pour remplir leur fonction.

En utilisant URMD, les organisations peuvent démontrer la conformité aux réglementations telles que SOX, PCI 7, et PCI 8.5 et réduire le risque de fuite de données. URMD est une option supplémentaire disponible sur les produits Imperva Database Security.

Les solutions SecureSphere Database Security d'Imperva fournissent également un mécanisme automatisé pour la définition et l'application de règles de contrôle d'accès des requêtes. La technologie **SecureSphere Dynamic Profiling** applique des algorithmes d'apprentissage automatisés pour créer des profils d'utilisation des requêtes pour chaque utilisateur et application accédant à la base de données. Chaque profil peut être étendu vers des modèles d'utilisation standard à chaque requête individuelle et à chaque procédure enregistrée. Les algorithmes d'apprentissage SecureSphere mettent continuellement à jour le profil d'utilisation au fil du temps pour éviter les réglages manuels lorsque les rôles des utilisateurs changent. Si un utilisateur lance une action qui ne correspond pas à son profil, SecureSphere enregistre l'événement, déclenche une alerte, et peut éventuellement bloquer l'action en fonction de la sévérité de l'alerte. Le changement de notes par le directeur d'université décrit précédemment serait facilement détecté par la technologie Dynamic Profiling. Le profil du directeur inclurait un ensemble de requêtes comprenant les changements classiques des coordonnées spécifiques des étudiants et peut-être un accès aux notes en lecture seule. Cependant, une tentative soudaine de modification des notes déclencherait une alerte.

Menace n° 2 – Abus de privilège légitime

Les utilisateurs peuvent également abuser de privilèges légitimes d'accès à une base de données à des fins non autorisées. Imaginez un éventuel fonctionnaire de la santé malveillant ayant des privilèges pour visualiser les dossiers médicaux des patients grâce à une application Web personnalisée. La structure de l'application Web limite normalement les privilèges des utilisateurs à la visualisation du dossier médical d'un seul patient. Les dossiers multiples ne peuvent pas être visualisés de manière simultanée et les copies électroniques ne sont pas autorisées. Cependant, le fonctionnaire malveillant peut contourner ces limitations en se connectant à la base de données en utilisant un client alternatif tel que MS-Excel. En utilisant MS-Excel et ses propres identifiants de connexion légitimes, le fonctionnaire peut récupérer et sauvegarder les dossiers médicaux des patients. Il y a peu de chances pour que de telles copies personnelles des bases de données des dossiers de patients respectent les règles sur la protection des données des patients définies par les institutions médicales. Il existe deux risques à prendre en considération. Le premier est le fonctionnaire malveillant qui tente de revendre les dossiers médicaux des patients. Le second (et peut-être le plus commun) est l'employé négligent qui récupère et sauvegarde un grand nombre de données sur son ordinateur client à des fins professionnelles légitimes. Une fois que ces données sont sauvegardées sur un autre ordinateur, elles deviennent vulnérables aux chevaux de Troie, au vol d'ordinateurs portables, etc.

Prévention des abus de privilège légitime – Compréhension du contexte d'accès aux bases de données

La solution à l'abus de privilège légitime est le contrôle d'accès aux bases de données qui s'applique non seulement aux requêtes d'accès spécifiques décrites précédemment, mais aussi au contexte d'accès aux bases de données. En appliquant une règle de contrôle pour les applications client, l'heure et la localisation de la requête d'accès, etc., il est possible d'identifier les utilisateurs qui utilisent des privilèges légitimes d'accès aux bases de données de manière suspecte.

SecureSphere Dynamic Profiling – Contrôle d'accès basé sur le contexte

En plus des données de la requête (voir la section Abus de privilège excessif décrite précédemment), la technologie SecureSphere Dynamic Profiling crée automatiquement un modèle de contexte d'accès normal aux bases de données. Les informations contextuelles spécifiques enregistrées dans le profil incluent l'heure de la requête d'accès, l'adresse IP source, le volume de données récupérées, l'application client, etc. Toute connexion à une base de données dont le contexte ne correspond pas aux informations définies dans le profil utilisateur déclenche une alerte. Par exemple, le fonctionnaire de la santé malveillant mentionné précédemment est repéré par SecureSphere non seulement en raison d'une utilisation inhabituelle de l'application client MS-Excel, mais aussi en raison du volume de données récupérées dans une seule et même session. Dans ce cas précis, les différences dans la structure de la requête non classique provenant de l'application MS-Excel déclencherait également une alerte pour violation au niveau de la requête (voir la section Abus de privilège excessif décrite précédemment).

Menace n° 3 – Elévation de privilège

Les auteurs d'attaques peuvent profiter des vulnérabilités des logiciels plate-forme de bases de données pour transformer les privilèges d'accès d'un utilisateur ordinaire en ceux d'un administrateur. Les vulnérabilités peuvent se trouver dans les procédures enregistrées, les fonctions intégrées, les implémentations de protocoles, voire même dans les données SQL. Par exemple, un développeur de logiciels travaillant dans une institution financière peut profiter d'une fonction vulnérable pour s'attribuer des privilèges administrateur d'accès aux bases de données. Avec des privilèges administrateur, le développeur malveillant peut désactiver les mécanismes d'audit, créer des comptes fantômes, transférer des fonds, etc.

Prévention d'élévation de privilège – technologie IPS et contrôle d'accès des requêtes

Les abus d'élévation de privilège peuvent être empêchés en combinant un système traditionnel de prévention des intrusions (IPS) et un contrôle d'accès des requêtes (voir la section Abus de privilège excessif décrite précédemment). La technologie IPS inspecte le trafic des bases de données pour identifier les modèles qui correspondent aux vulnérabilités existantes. Par exemple, si une fonction spécifique est connue pour être vulnérable, une technologie de type IPS peut soit bloquer tous les accès à la procédure vulnérable, ou (si possible) bloquer uniquement les procédures avec des attaques intégrées. Malheureusement, cibler uniquement les requêtes d'accès aux bases de données avec des attaques intégrées de manière précise peut s'avérer difficile en utilisant la technologie IPS seule. De nombreuses fonctions de bases de données vulnérables sont communément utilisées à des fins légitimes. Par conséquent, le blocage de toutes les occurrences de ces fonctions n'est pas recommandé. La technologie IPS sépare de manière précise les fonctions légitimes des fonctions intégrant des attaques. Dans beaucoup de cas, les variations infinies des attaques rendent cette distinction impossible. Dans ces conditions, les systèmes IPS peuvent être utilisés en mode alerte uniquement (et non en mode blocage) puisqu'il y a des chances d'obtenir des faux positifs. Pour améliorer la précision, la technologie IPS peut être combinée aux indicateurs d'attaques alternatifs tels que le contrôle d'accès des requêtes. La technologie IPS peut être utilisée pour vérifier si la requête d'accès à la base de données utilise ou non une fonction vulnérable, tandis que le contrôle d'accès des requêtes contrôle si la requête correspond ou non à un profil utilisateur classique. Si une seule requête indique un accès à une fonction vulnérable ou un profil utilisateur inhabituel, une tentative d'attaque est certainement en cours.

SecureSphere Privilege Elevation – Technologies intégrées IPS et Dynamic Profiling

SecureSphere intègre les technologies avancées IPS et Dynamic Profiling pour un contrôle d'accès des requêtes (voir la section Abus de privilège excessif décrite précédemment). Combinées, ces technologies fournissent une protection extrêmement précise contre l'élévation de privilège. La technologie SecureSphere IPS offre une protection contre les attaques visant les vulnérabilités identifiées grâce à des dictionnaires de signature pour tous les protocoles compatibles avec les solutions Snort®. Par ailleurs, l'organisation internationale de recherche sur la sécurité d'Imperva, le centre de défense des applications, fournit des protections spécifiques aux données SQL propriétaires pour s'assurer que SecureSphere représente la première solution mondiale de sécurité IPS des bases de données. Le service SecureSphere de mise à jour de la sécurité met automatiquement à jour les dictionnaires de signatures pour s'assurer que les protections les plus récentes sont continuellement appliquées. SecureSphere IPS bloque certaines attaques facilement

identifiables sans exiger aucune confirmation d'attaque supplémentaire. Cependant, si une requête spécifique peut être catégorisée comme suspecte uniquement, SecureSphere établit une corrélation entre la requête et les violations détectées par la technologie Dynamic Profile pour valider une attaque. Pour illustrer la manière dont SecureSphere intègre les technologies IPS et Dynamic Profiling, reprenons le cas de notre développeur de logiciels malveillant travaillant dans une institution financière mentionné précédemment. Imaginez que le développeur tente de profiter d'un dépassement de mémoire tampon dans la fonction d'une base de données pour insérer un code malveillant afin d'élever ses privilèges à ceux d'un administrateur de base de données. Dans ce cas, SecureSphere identifie deux violations simultanées. Tout d'abord, toute requête tentant d'accéder à une fonction vulnérable identifiée déclenche une alerte pour violation IPS. Par ailleurs, une requête inhabituelle déclenche une alerte pour violation de profil. En établissant une corrélation entre deux violations dans une seule requête d'accès à une base de données provenant du même utilisateur, une attaque est validée de manière très précise et une alerte de haute importance ou une action de blocage peuvent être appliquées.

Menace n° 4 – Exploitation des failles des bases de données vulnérables ou mal configurées

Les bases de données sont souvent vulnérables, non corrigées ou disposent de comptes et d'une configuration toujours définis par défaut. L'auteur d'une attaque qui tente d'exploiter la base de données test généralement les systèmes sur ces vulnérabilités, ce qui peut entraîner une violation de sécurité. Alors que les fournisseurs développent des packs de correction pour corriger les systèmes au niveau d'une vulnérabilité spécifique, les bases de données des entreprises demeurent librement exploitables. Lorsqu'un correctif est lancé, il n'est pas disponible immédiatement. Il existe différents aspects à prendre en considération au moment d'appliquer un correctif sur une base de données. Tout d'abord, l'organisation doit au préalable évaluer la procédure de correction du système avec le correctif en question, en tentant de comprendre comment le correctif affecterait le système. Parfois, un correctif peut être en contradiction avec un code déjà existant, ou il peut impliquer d'autres opérations. Ensuite, le système subit un temps d'arrêt lorsque le serveur de bases de données ne parvient pas à fournir aux utilisateurs un service afin de le corriger. Enfin, les grandes entreprises ayant des dizaines voire des centaines de bases de données doivent prévoir un plan de correction, en traitant en priorité les bases de données, celles-ci devant être corrigées en premier. Par conséquent, il n'est pas surprenant de voir que pour de nombreuses entreprises, la procédure de correction dure plusieurs mois, généralement entre 6 à 9 mois (durée établie sur la base des recherches menées par le groupe indépendant des utilisateurs d'Oracle ou IOUG*). Les accès aux bases de données, les administrateurs système et les administrateurs informatiques, les développeurs, tous jouent un rôle dans la procédure de correction. Alors que les ressources et le temps sont limités, les serveurs demeurent vulnérables pendant des mois après le lancement d'un correctif.

Des paramètres de compte et de configuration toujours définis par défaut sur une base de données de production peuvent être exploités par l'auteur d'une attaque. L'auteur d'une attaque peut tenter d'accéder à la base de données en utilisant un compte défini par défaut. Un paramètre d'audit faible peut permettre à l'auteur d'une attaque de contourner les contrôles d'audit ou de supprimer toutes traces de ses activités. Des modèles d'identification faibles permettent aux auteurs d'attaques de s'identifier comme les utilisateurs légitimes de bases de données en volant ou en obtenant les identifiants de connexion.

Prévention – Evaluation de la vulnérabilité et application de correctifs

Dans le but de limiter le risque de menace des bases de données non corrigées et vulnérables, il faut tout d'abord évaluer l'état de sécurité des bases de données et corriger toutes les vulnérabilités et les écarts de sécurité identifiés. Les entreprises devraient effectuer un balayage périodique des bases de données pour découvrir toutes vulnérabilités et correctifs manquants. Les évaluations de la configuration devraient fournir un aperçu clair de l'état de configuration actuel des systèmes de données. Ces évaluations devraient également identifier les bases de données qui ne respectent pas les règles de configuration définies. Tout correctif de sécurité manquant devrait être déployé le plus vite possible. Si une vulnérabilité est découverte alors que le correctif n'est pas encore disponible, soit parce qu'il n'a pas encore été lancé par le fournisseur ou parce qu'il n'a pas encore été déployé, une solution de correction virtuelle doit être définie. Une telle solution bloque les tentatives d'exploitation de ces vulnérabilités. La réduction de la fenêtre d'exposition obtenue grâce à l'application d'un correctif virtuel permettra de protéger la base de données des tentatives d'exploitation jusqu'à ce qu'un correctif soit déployé.

SecureSphere Vulnerability Assessments and Virtual Patching (solution d'évaluation des vulnérabilités et application de correctifs virtuels)

SecureSphere intègre une solution complète d'évaluation des vulnérabilités et de la configuration qui permet aux utilisateurs de programmer des balayages périodiques pour identifier les vulnérabilités, les correctifs manquants et les problèmes de configuration existants. La solution est régulièrement mise à jour grâce à un mécanisme automatisé de mise à jour De l' ADC Center, avec des évaluations des règles et des tests pour identifier les dernières vulnérabilités basées sur les recherches menées par le centre de recherche d'Imperva. SecureSphere permet également aux utilisateurs d'appliquer des correctifs virtuels pour bloquer toutes tentatives d'exploitation des vulnérabilités jusqu'à ce qu'un correctif soit déployé. Selon une recherche menée par le groupe indépendant des utilisateurs d'Oracle (IOUG), les organisations appliquent généralement ces correctifs virtuels au cours des 6 à 9 mois précédant le déploiement d'un correctif. SecureSphere peut limiter le risque d'exposition pendant la période requise pour déployer le correctif.

* http://ioug.itconvergence.com/pls/apex/f?p=201:1:4201959220925808

Menace n° 5 – Injection SQL

Dans une attaque par injection SQL, l'auteur insère généralement (ou « injecte ») des informations de bases de données non autorisées dans une chaîne de données SQL vulnérable. Généralement les chaînes de données visées incluent les procédures enregistrées et les paramètres d'entrée des applications Web. Ces informations injectées sont ensuite envoyées vers la base de données où elles sont exécutées. En utilisant l'injection SQL, les auteurs d'attaques peuvent obtenir l'accès illimité à l'ensemble d'une base de données.
Prévention de l'injection SQL. Trois techniques peuvent être combinées pour lutter efficacement contre l'injection SQL : La technologie de prévention des intrusions (IPS), le contrôle d'accès des requêtes (voir la section Abus de privilège excessif), et la corrélation d'événements. La technologie IPS peut identifier les procédures enregistrées vulnérables ou les chaînes d'injection SQL. Cependant, la technologie IPS seule n'est pas fiable puisque les chaînes d'injection SQL sont sujettes à des faux positifs. Les responsables de la sécurité qui compteraient uniquement sur la technologie IPS seraient bombardés d'alertes au sujet de « possibles » injections SQL. Cependant, en établissant une corrélation entre une signature d'injection SQL et un autre type de violation tel qu'une violation du contrôle d'accès de requête, une réelle attaque peut être identifiée de manière très précise. Une signature d'injection SQL et un autre type de violation ont peu de chance d'apparaître dans la même requête au cours d'une opération professionnelle classique.

Solutions SecureSphere de protection contre l'injection SQL
SecureSphere intègre les technologies Dynamic Profiling, IPS, et Correlated Attack Validation pour identifier avec une précision inégalée les attaques par injection SQL.
» Dynamic Profiling offre un contrôle d'accès des requêtes en créant automatiquement des profils pour chaque utilisateur et des modèles de requêtes classiques pour chaque application. Toutes les requêtes (telles qu'une requête d'attaque par injection SQL) qui ne correspondent pas à un profil utilisateur ou à un modèle d'application défini au préalable sont immédiatement identifiées.

» SecureSphere IPS inclut des dictionnaires de signatures de bases de données uniques spécialement conçus pour identifier les procédures enregistrées vulnérables et les chaînes d'injection SQL.

» Correlated Attack Validation établit une corrélation entre les violations de sécurité provenant de multiples couches de détection SecureSphere. En établissant une corrélation entre les multiples violations provenant d'un même serveur, SecureSphere peut détecter l'injection SQL avec un niveau de précision qui n'est pas possible dans le cas d'une utilisation d'une couche de détection unique. Considérez l'attaque par injection SQL de la procédure enregistrée décrite ci-dessous :

> exec ctxsys.driload.validate_stmt (« autoriser l'accès à la base de données à scott »). Par cette attaque, l'auteur (scott) tente de s'attribuer les privilèges administrateur d'accès à la base de données en intégrant une opération « autoriser » dans une procédure enregistrée vulnérable. SecureSphere traiterait cette attaque avec l'une des deux procédures en fonction de l'appartenance ou non de la procédure enregistrée à une fonction professionnelle requise.

Procédure enregistrée vulnérable non requise
Idéalement, les procédures enregistrées vulnérables ne sont utilisées par aucun utilisateur ou application. Si c'est le cas, la technologie SecureSphere IPS est suffisante pour identifier de manière précise et éventuellement bloquer toutes les tentatives de cette attaque. Les activités professionnelles classiques ne correspondront pas à une chaîne de caractères aussi complexe (...ctxsys.driload...).
Procédure enregistrée vulnérable requise

Dans certains cas, une procédure enregistrée vulnérable peut faire partie d'une fonction professionnelle requise. Par exemple, elle peut faire partie d'une application patrimoniale qui ne peut pas être modifiée. Dans ce cas, SecureSphere alertera tout d'abord les responsables de la sécurité sur l'utilisation de cette fonction. Ensuite, la technologie Correlated Attack Validation peut éventuellement être appliquée pour établir une corrélation entre les occurrences de cette signature et une liste des utilisateurs et applications autorisés à utiliser la procédure. Si un utilisateur non autorisé tente d'utiliser cette procédure, SecureSphere peut déclencher une alerte ou éventuellement bloquer la requête.

Menace n° 6 – Faiblesse de l'audit natif

Un enregistrement automatique de toutes les transactions de bases de données sensibles et/ou inhabituelles devrait être la base sous-jacente de tout déploiement de base de données. Une faible règle d'audit des bases de données représente un sérieux risque organisationnel à plusieurs niveaux.

» Risque au niveau des réglementations – les organisations utilisant de faibles mécanismes d'audit des bases de données (ou parfois inexistants) réaliseront de plus en plus qu'elles ne respectent pas les réglementations gouvernementales. La réglementation Sarbanes-Oxley (SOX) dans le domaine des services financiers et le Healthcare Information Portability and Accountability Act ou HIPAA (loi sur la portabilité et la comptabilité des soins de santé) dans le domaine de la santé ne sont que deux exemples de réglementations gouvernementales imposant des exigences claires au niveau de l'audit des bases de données.

» Dissuasion – à l'instar des caméras vidéo qui enregistrent les visages des personnes entrant dans une banque, les mécanismes d'audit des bases de données servent à dissuader les auteurs d'attaques qui savent que le suivi des audits des bases de données fournit aux enquêteurs des informations criminalistiques sur les auteurs d'un crime.

» Détection et récupération – les mécanismes d'audit représentent la dernière ligne de défense des bases de données. Si l'auteur d'une attaque parvient à contourner d'autres systèmes de défense, les résultats des audits peuvent identifier l'existence d'une violation après l'attaque. Les résultats des audits peuvent ensuite être utilisés pour faire un lien entre une violation et un utilisateur en particulier et/ou réparer le système.
Les plateformes de logiciels de bases de données intègrent généralement des fonctionnalités d'audit basiques mais elles présentent de multiples faiblesses qui limitent ou empêchent leur déploiement.

» Manque d'imputabilité des utilisateurs – lorsque les utilisateurs accèdent à une base de données via des applications Web (telles que SAP, Oracle E-Business Suite, ou PeopleSoft), les mécanismes d'audits natifs ne connaissent pas les identités des utilisateurs spécifiques. Dans ce cas, toutes les activités d'un utilisateur sont associées au nom de compte de l'application Web. Par conséquent, lorsque les résultats des audits natifs révèlent l'existence de transactions de bases de données frauduleuses, aucun lien ne peut être effectué avec l'utilisateur responsable.

» Dégradation des performances – les mécanismes d'audit de bases de données natives sont connus pour consommer les ressources de l'unité centrale et du disque dur. La dégradation des performances observée lorsque les fonctionnalités d'audit sont activées force de nombreuses organisations à réduire le nombre d'audits ou simplement à les supprimer.

» Séparation des fonctions – les utilisateurs ayant des droits d'accès administrateur (obtenus soit de façon légitime ou malveillante – voir la section Elévation de privilège) au serveur de bases de données peut facilement désactiver la fonctionnalité d'audit pour dissimuler une activité frauduleuse. Idéalement, les fonctions d'audit devraient être séparées de celles des administrateurs de bases de données et de celles de la plate-forme du serveur de bases de données.

» Granularité limité – de nombreux mécanismes d'audit natifs n'enregistrent pas les informations nécessaires pour prendre en charge la détection des attaques, les enquêtes criminalistiques et la récupération.
Par exemple, l'application client des bases de données, les adresses IP sources, les éléments de réponse des requêtes, et les requêtes ayant échoué (un indicateur important de reconnaissance d'attaque) ne sont pas enregistrés par de nombreux mécanismes natifs.

» Propriétaire – les mécanismes d'audit sont propres à la plate-forme du serveur de bases de données. Les résultats d'Oracle sont différents des résultats de MS-SQL, les résultats de MS-SQL sont à leur tour différents des résultats de Sybase, etc. Pour les organisations qui combinent les environnements de bases de données, cela élimine littéralement l'implémentation de procédures d'audit uniformes et évolutives dans l'entreprise.

Prévention des audits des faiblesses
Les dispositifs d'audit basés sur la qualité du réseau répondent à la plupart des faiblesses associées aux outils d'audit natifs.

» Hautes performances – les dispositifs basés sur la qualité du réseau peuvent appliquer une vitesse à la ligne sans aucune répercussion sur les performances de la base de données. En réalité, en rejetant la responsabilité des procédures d'audit sur les applications réseau, les organisations peuvent espérer améliorer les performances des bases de données.

» Séparation des fonctions – les dispositifs d'audit basés sur le réseau peuvent fonctionner indépendamment des administrateurs de bases de données, permettant ainsi de séparer de façon appropriée les fonctions d'audit des fonctions administratives. Par ailleurs, étant donné que les dispositifs du réseau sont indépendants du réseau lui-même, ils sont également invulnérables aux attaques par élévation de privilège lancées par des utilisateurs non-administrateurs.

» Audit multiplateforme – les dispositifs d'audit basés sur le réseau prennent généralement en charge les principales plateformes de bases de données permettant d'appliquer des critères uniformes et des procédures d'audit centralisées sur de grands environnements de bases de données hétérogènes. Combinées, ces caractéristiques réduisent les coûts d'exploitation du serveur de bases de données, les critères d'équilibrage de charge, ainsi que les coûts administratifs. Elles permettent également d'offrir une meilleure sécurité.

Fonctionnalités d'audit de SecureSphere
En plus des principaux avantages associés aux dispositifs d'audit basés sur le réseau décrits précédemment, SecureSphere offre un ensemble de fonctionnalités d'audit uniques qui rend cette solution différente des approches alternatives.

» La fonctionnalité Universal User Tracking rend les utilisateurs individuels responsables de leurs actions, même lorsqu'ils accèdent à la base de données via des applications Web commerciales (Oracle, SAP, PeopleSoft, etc.) ou personnalisées. Pour identifier les noms des utilisateurs des applications Web, une interface SecureSphere dédiée capture les informations de connexion à l'application, retrace les sessions utilisateur ultérieures, et établit une corrélation entre ces sessions et les transactions de bases de données. Les résultats d'audit obtenus incluent les noms des utilisateurs uniques des applications Web.

» La fonctionnalité Granular Transaction Tracking prend en charge la détection avancée des fraudes, les enquêtes criminalistiques et la récupération. Les informations de connexion incluent des informations telles que le nom de l'application source, le texte complet de la requête, les éléments de réponse de la requête, le système d'exploitation source, l'adresse IP source, et bien plus encore.

» La fonctionnalité Distributed Audit Architecture permet un suivi granulaire des transactions (voir le point précédent) tout en conservant la capacité à examiner de grandes banques de données; L'architecture de l'audit distribue les ressources de stockage et de calcul nécessaires entre les passerelles distribuées SecureSphere. Le serveur de gestion SecureSphere dispose d'un service d'audit ayant une vue d'ensemble sur la banque de données. Le serveur de gestion permet aux passerelles d'être gérées efficacement comme si elles ne formaient qu'une seule et même passerelle du point de vue du service d'audit. Des approches alternatives recommandent un enregistrement restreint des transactions ou forcent les administrateurs à gérer plusieurs dispositifs distribués de manière indépendante.

» La fonctionnalité External Data Archival automatise des procédures d'archivage de données à long terme. SecureSphere peut être configuré pour archiver de manière périodique les données sur des systèmes externes de stockage de masse. Les données peuvent éventuellement être compressées, cryptées ou signées avant l'archivage.

» La fonctionnalité Integrated Graphical Reporting fournit aux administrateurs un mécanisme flexible et facilement compréhensible pour analyser la piste d'audit. Ce mécanisme inclut des rapports préconfigurés qui répondent aux questions fréquemment posées au cours des audits, tout en offrant la possibilité de créer des rapports personnalisés pour répondre aux exigences spécifiques de l'entreprise. Une solution de rapport externe conforme à la connectivité de bases de données ouverte peut également être utilisée pour analyser les résultats d'audit SecureSphere.

» La fonctionnalité Local Console Activity Auditing est incluse dans la solution SecureSphere Database Agent. La solution SecureSphere Database Agent est un agent hôte léger installé sur le serveur de bases de données pour contrôler les activités administratives sur la base de données locale. Combinées, les solutions SecureSphere Database Agent et SecureSphere Gateways fournissent une piste d'audit complète ayant un impact négligeable sur, ou dans certains cas améliorant les performances de la base de données.

Menace n° 7 – Déni de service

Le déni de service (DOS - Denial Of Service) est une catégorie d'attaque générale par laquelle l'accès aux applications réseau est refusé à certains utilisateurs. Les conditions de déni de service peuvent être créées par de nombreuses techniques, parmi lesquelles beaucoup sont liées aux vulnérabilités mentionnées précédemment. Par exemple, le déni de service peut être obtenu en profitant de la vulnérabilité d'une plate-forme de bases de données pour faire tomber un serveur. D'autres techniques communes de déni de service incluent la corruption de données, l'engorgement du réseau, et la surcharge en ressources du serveur (mémoire, unité centrale, etc.). La surcharge des ressources est une technique très commune dans les environnements de bases de données. Les motivations qui se cachent derrière les attaques par déni de service sont aussi diverses. Les attaques par déni de service sont souvent liées aux tentatives d'extorsion par lesquelles un pirate informatique fait planter des serveurs à distance et de manière répétée jusqu'à ce que la victime place ses fonds sur un compte bancaire international. Le déni de service peut également être lié à une infection par un ver informatique. Quelle que soit la source, le déni de service représente une menace sérieuse pour de nombreuses organisations.

Prévention du déni de service
La prévention du déni de service requiert des protections à de multiples niveaux. Des protections au niveau du réseau, de l'application et de la base de données sont toutes nécessaires. Ce document met l'accent sur les protections spécifiques aux bases de données. Dans ce contexte spécifique aux bases de données, le déploiement du contrôle du taux de connexion, la technologie IPS, le contrôle d'accès des requêtes, et le contrôle du temps de réponse sont recommandés.

Solutions SecureSphere de protection contre le déni de service
» Les contrôles de connexion empêchent la surcharge en ressources du serveur en limitant les taux de connexion, les taux de requêtes, et autres variables pour chaque utilisateur des bases de données.

» Les technologies IPS et Protocol Validation (validation de protocole) empêchent les pirates informatiques d'exploiter les vulnérabilités de logiciels connues pour créer un déni de service. Le dépassement de mémoire tampon, par exemple, est une vulnérabilité de plate-forme qui peut être exploitée pour faire tomber les serveurs de bases de données. Reportez-vous aux sections Elévation de privilège et Vulnérabilités des protocoles de communication des

bases de données de ce document pour plus d'informations sur les technologies SecureSphere IPS et Database Communications Protocol Validation

» La technologie Dynamic Profiling fournit automatiquement un contrôle d'accès des requêtes pour détecter toutes requêtes non autorisées pouvant créer un déni de service. Les attaques par déni de service ayant pour cible les vulnérabilités de plate-forme, par exemple, pourraient provoquer les violations des technologies IPS et Dynamic Profile. En établissant une corrélation entre ces violations, SecureSphere peut obtenir une précision inégalée. Reportez-vous à la section Abus de privilège excessif pour de plus amples informations sur la technologie Dynamic Profiling.

» Response Timing (temps de réponse) – Les attaques de déni de service des bases de données visant à surcharger le serveur en ressources provoquent des réponses de bases de données différées. La technologie SecureSphere Response Timing détecte les délais de réponse pour une requête individuelle ainsi que pour l'ensemble du système.

Menace n° 8 – Vulnérabilités des protocoles de communication des bases de données

Un nombre croissant de vulnérabilités de sécurité sont identifiées dans les protocoles de communication des bases de données conçus par tous les fournisseurs de bases de données. Quatre des sept correctifs de sécurité inclus dans les deux derniers packs de correction IBM DB2 traitent des vulnérabilités des protocoles de type 1. De la même façon, 11 des 23 vulnérabilités de bases de données corrigées dans le dernier correctif trimestriel d'Oracle ont un rapport avec les protocoles. Les activités frauduleuses prenant pour cible ces vulnérabilités peuvent aller de l'accès aux données non autorisées, à la corruption de données, en passant par le déni de service. Le ver informatique SQL Slammer2, par exemple, a profité d'une faille sur le protocole du serveur Microsoft SQL pour forcer un déni de service. Pour rendre la situation plus difficile, aucun enregistrement de ces vecteurs de fraude n'existe dans la piste d'audit native puisque les opérations de protocole ne sont pas couvertes par les mécanismes d'audit de bases de données natives. Prévention des attaques de protocoles de communication des bases de données. Les attaques de protocoles de communication des bases de données peuvent être vaincues grâce à une technologie communément appelée validation de protocole. La technologie de validation de protocole décompose (désassemble) essentiellement le trafic des bases de données et le compare aux prévisions de trafic. Dans le cas où le trafic réel ne correspond pas aux prévisions, des alertes ou des actions de blocage peuvent être mises en place.

SecureSphere Database Communication Protocol Validation (technologie de validation de protocole de communication)
La technologie SecureSphere Database Communication Protocol Validation vérifie et protège contre les menaces de protocoles en comparant les protocoles de communications des bases de données réels aux structures de protocoles attendues. Aucune autre solution de sécurité ou d'audit de bases de données ne fournit cette possibilité. Elle est dérivée des recherches en cours du centre de défense des applications d'Imperva (ADC) sur les vulnérabilités et les protocoles de communication des bases de données propriétaires. Des fournisseurs d'applications et de bases de données y compris Oracle, Microsoft, et IBM ont attribué au centre de défense des applications d'Imperva la découverte de sérieuses vulnérabilités et de techniques de limitation ayant contribué à augmenter la sécurité de leurs produits. Sur la base de ces recherches, Imperva est capable d'intégrer des connaissances techniques sur les protocoles inégalées dans ses solutions SecureSphere.

Menace n° 9 – Copies non autorisées de données sensibles

De nombreuses entreprises s'efforcent de localiser et maintenir de manière appropriée un inventaire de toutes leurs bases de données. De nouvelles bases de données peuvent être créées sans que l'équipe responsable de la sécurité soit au courant et les données sensibles copiées dans ces bases de données peuvent être exposées si les contrôles nécessaires ne sont pas appliqués. Ces bases de données « cachées » peuvent contenir des données potentiellement sensibles telles que les détails des transactions, ainsi que les coordonnées des clients et des employés. Cependant, si les personnes chargées de la sécurité des données ne connaissent pas le contenu de ces bases de données, il est difficile de s'assurer que les contrôles nécessaires ont été appliqués. Que ce soit de manière intentionnelle ou non, les employés ou les pirates informatiques peuvent alors accéder illégalement aux données sensibles. Les anciennes bases de données qui ont été oubliées et laissées hors du champ d'évaluation sont un autre exemple. Si personne ne gère ces bases de données, les données sont laissées sans surveillance à la vue des regards indiscrets qui ne devraient pas accéder à ces données.

Prévention des copies non autorisées de données sensibles

Afin de maintenir un inventaire précis des bases de données et une localisation exacte des données sensibles, les organisations devraient identifier toutes les bases de données sur le réseau qui contient des données sensibles. La seconde étape consiste à trouver quels sont les types de données sensibles ou classifiées contenus dans les objets des bases de données. La classification de données représente deux difficultés majeures dont la première est de localiser les données sensibles parmi le grand nombre et les grandes tailles des tableaux. La seconde difficulté est de trouver les combinaisons de données qui en elles-mêmes sont considérées comme inoffensives, mais qui forment, une fois combinées avec d'autres données, une combinaison de données considérées comme sensibles. Afin de protéger de manière appropriée les données sensibles, les contrôles nécessaires doivent être définis conformément aux politiques d'accès aux données de l'organisation, une fois qu'un inventaire précis des bases de données et de la localisation des données sensibles est disponible.

SecureSphere Discovery and Classification

SecureSphere permet aux utilisateurs de programmer des balayages automatiques du réseau qui fournissent un inventaire complet de toutes les bases de données. Cette solution identifie également les nouvelles bases de données ou encore celles qui ont été modifiées, ce qui est utile pour le surfaçage de toutes les « fausses »bases de données. Les utilisateurs peuvent donc exiger le balayage du contenu des bases de données pour identifier les objets contenant des données sensibles. SecureSphere prend également en charge les types de données prêtes à être utilisées telles que les numéros de cartes bancaires ou les numéros de sécurité sociale (les utilisateurs peuvent également ajouter des types de données personnalisés). Afin de réduire le nombre de faux positifs, SecureSphere utilise des algorithmes de validation. Ceci permet également de repérer tous les nouveaux types de données sensibles ou classifiées.

Menace n° 10 – Exposition de données de sauvegarde

Les dispositifs de sauvegarde de bases de données auxiliaires ne sont généralement pas protégés contre d'éventuelles attaques. Par conséquent, plusieurs violations de sécurité importantes ont vu le jour, y compris le vol de disques durs et de bandes de sauvegarde de bases de données.

Prévention de l'exposition de données auxiliaires
Toutes les sauvegardes de bases de données devraient être cryptées. En réalité, certains fournisseurs ont suggéré que les futurs systèmes de gestion de bases de données ne devraient pas prendre en charge la création de sauvegardes non cryptées. Le cryptage des informations des bases de données de production en ligne est souvent suggéré, mais les performances et les inconvénients liés à la gestion des clés cryptographiques rend souvent cette solution peu pratique et sont généralement reconnus pour être un modeste substitut des contrôles de droits d'accès granulaires décrits précédemment.

Résumé
Bien que les informations des bases de données soient vulnérables à un grand nombre d'attaques, il est possible de réduire considérablement les risques en se concentrant sur les menaces les plus critiques. En s'occupant des 10 menaces principales décrites dans ce document, les entreprises répondront aux exigences de conformité et de limitation des risques des industries mondiales les plus réglementées.

#WP-TOP10DBTHREATS1110rev1