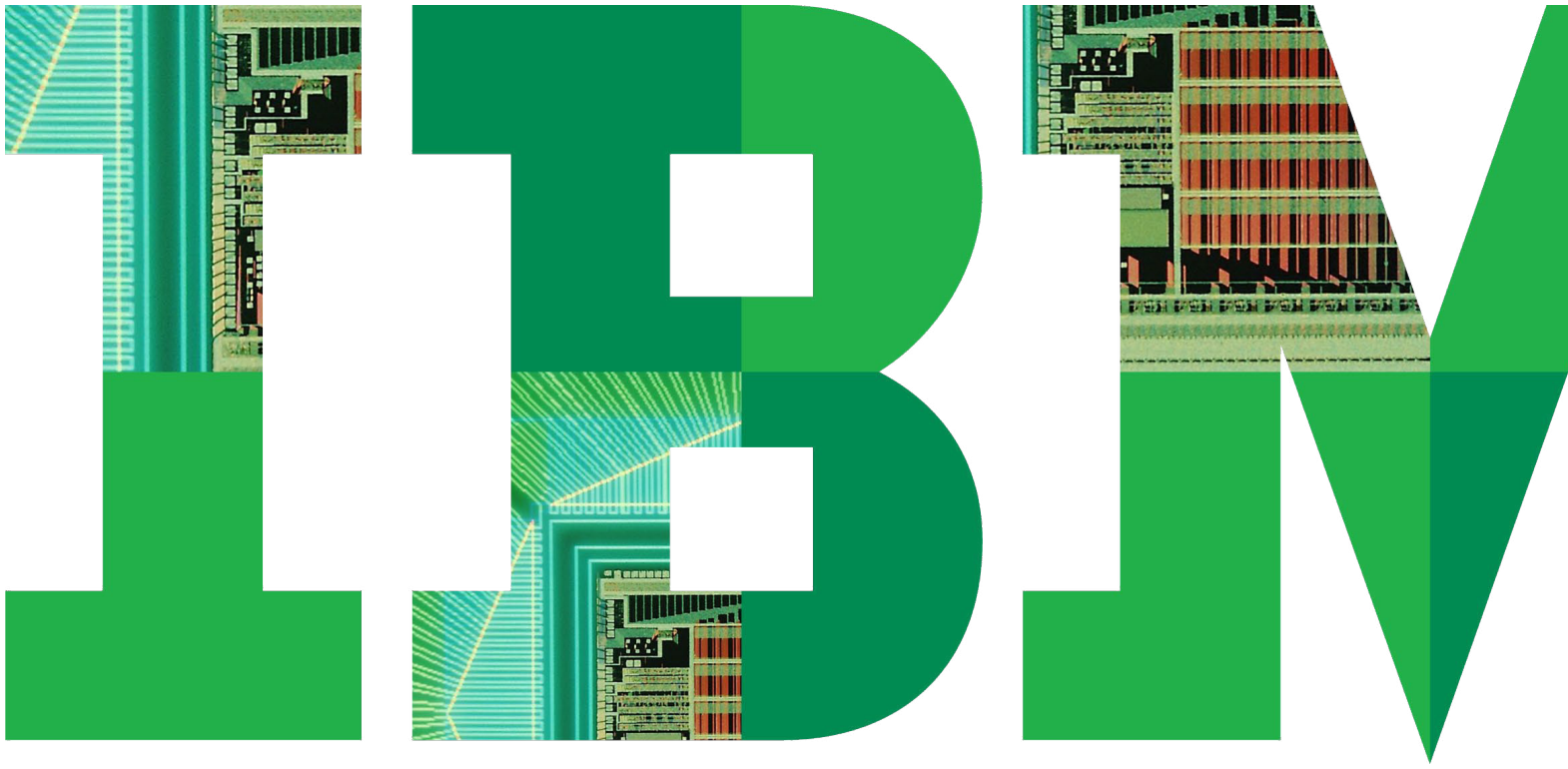
Protección contra ataques a la base de datos y amenazas de personas con acceso a información confidencial: Los 5 escenarios principales



El reto: La complejidad de salvaguardar las bases de datos

La seguridad de datos presenta un reto multi-dimensional donde los ambientes complejos incluyen una gran cantidad de sistemas para gestión de base de datos (DBMS), aplicaciones empresariales, plataformas de sistema operativo con múltiples rutas de acceso y niveles de permiso heterogéneos que han generado un conjunto aparentemente interminable de escenarios de amenazas y violaciones de seguridad.

Los tradicionales "enfoques tipo Fortaleza" como firewalls y sistemas IDS/IPS ya no son suficiente protección contra los atacantes del siglo XXI que fácilmente traspasan las barreras perimetrales. Estas medidas de seguridad no pueden diferenciar o evitar el tráfico que aparenta ser legítimo.

El reto: La complejidad de salvaguardar las bases de datos

Una de las razones por las que hay un mayor enfoque en la seguridad de bases de datos es que es que existe un desequilibrio dramático entre la complejidad de las plataformas actuales de sistemas para gestión de bases de datos – que continuamente han crecido en funcionalidad en los últimos 30 años- y los métodos usados para proteger estos sistemas críticos.

Para crear bases de datos más monitorearse, mejorarse y auditarse de funcionales, disponibles y capaces de soportar un gran número de transacciones, los proveedores han creado múltiples programas con una cantidad extremadamente grande de opciones de configuración, todas las cuales deben ser bien comprendidas y aseguradas para evitar violaciones de la información. La seguridad para bases de datos también ha avanzado, por supuesto, pero no a la misma velocidad. Las muchas características y servicios adicionales de los sistemas para gestión de bases de datos han traído nuevas vulnerabilidades y potencial de mal uso. Incluso más notorio resulta el desequilibrio entre conocimiento, habilidades, fuerza de trabajo y procesos. La mayoría de las organizaciones utilizan administradores de bases de datos (DBA) para administrar las bases de datos – la energía vital de las aplicaciones empresariales- y asegurar su disponibilidad, desempeño e integridad. Sin embargo, hay que considerar lo siguiente:

Forrester; calcula que actualmente sólo 20% de las empresas tienen una estrategia de seguridad de base de datos a nivel de toda la empresa en funcionamiento.

Fuente:Reporte de investigación Forrester; "Panorámica del mercado: Seguridad de Bases de Datos, 2011"

- ¿Qué porcentaje del tiempo del DBA se dedica a la seguridad de la información?
- ¿Qué tanto sabe el profesional de seguridad de la información promedio sobre bases de datos?
- ¿Qué verificaciones y balances existen para protegerse de los propios DBA (sin mencionar a otras personas con privilegios de acceso a información como desarrolladores, recursos subcontratados, personal de apoyo de proveedores, etc.)?
- ¿Cuántas organizaciones han implementado herramientas para monitorear y aplicar políticas de control de cambios respecto a cómo y cuándo se hacen cambios a estructuras y datos críticos?

La seguridad de datos, a nivel de base, no es un proyecto individual; es un proceso constante que debe administrarse, monitorearse, mejorarse y auditarse de manera continua a lo largo de toda la organización. La seguridad de datos debe implementarse como un proceso que se integra con otros procesos de seguridad (en particular, gestión de identidad y acceso y gestión de vulnerabilidad) al igual que otros procesos de negocios críticos.

En este libro electrónico se examinan los principales 5 escenarios y las mejores prácticas esenciales para evitar ataques a bases de datos y amenazas de personas con acceso a información confidencial. Las organizaciones que adoptan un enfoque proactivo requerirán una solución amplia que pueda ayudarles a reducir la complejidad del cumplimiento, al automatizar y centralizar controles cruzados en los sistemas de gestión de base de datos con el fin de satisfacer las regulaciones clave y leyes de protección de datos.

5 Escenarios principales:

Escenario 1: Evitar ataques externos

Escenario 2: Bloquear acceso de usuarios privilegiados a información sensible

Escenario 3: Identificar fraudes en la capa de aplicaciones (Oracle EBS, PeopleSoft, SAP, etc.)

Escenario 4: Garantizar acceso autorizado a bases de datos

Escenario 5: Detectar cambios no autorizados a bases de datos

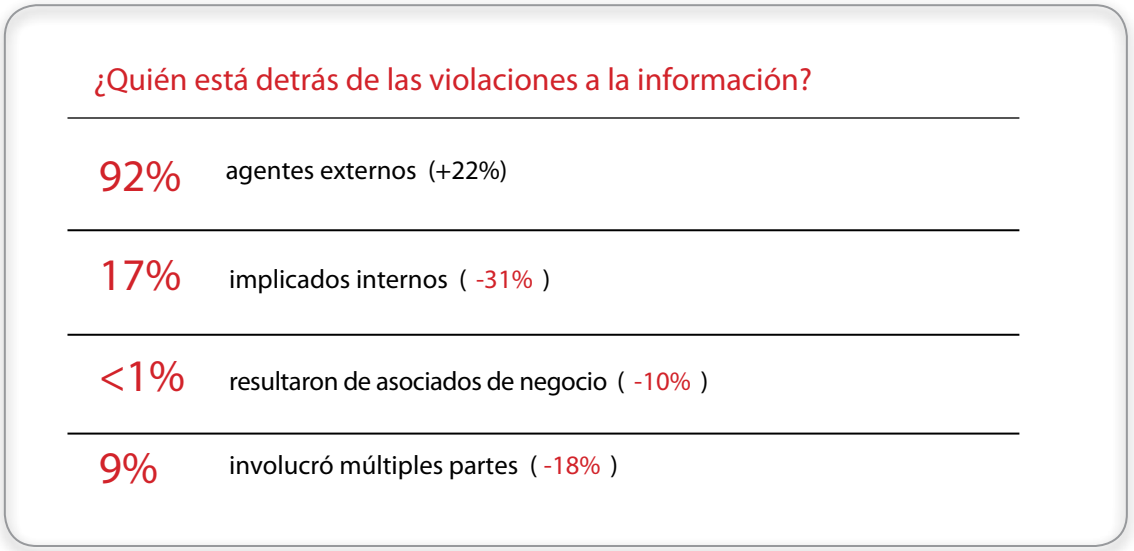
Evitar ataques externos

La mayor parte de la información sensible del mundo se almacena en bases de datos / almacenes de datos comerciales como Oracle, Microsoft SQL Server, IBM DB2, Informix, Sybase, MySQL, Netezza y Teradata - lo que hace de las bases de datos un blanco cada vez más buscado por los ciber - criminales.

Según el Reporte de Investigación de Violaciones de Información Verizon 2011, los ataques a servidores de datos representa-ron el 80% de las violaciones y 95% de los registros comprometidos durante 2010. De hecho, el reporte indica que ocurrieron más violaciones de la información en 2010 que en años anteriores (véase la Figura 1).

Las aplicaciones Web se han transformado y han mejorado la manera en que las empresas hacen negocios, pero también han hecho que las bases de datos estén más

Figura 1



La mayor parte de las violaciones a la información continúan originándose de fuentes externas. Verizon 2011

expuestas. La exposición existe porque la aplicación que utiliza los datos ahora sirve a un público mucho mayor y porque los usuarios no están limitados a empleados internos. Los atacantes tienen ahora una vía de entrada directa –a través de la aplicación, pasando las defensas perimetrales- al interior de la base de datos.

Violaciones a la información de alto perfil recientes incluyen ataques externos perpetrados por:

- Ciber-criminales, atacantes altamente motivados asociados con organizaciones criminales dispuestas a pagar en efectivo por información personal robada de las bases de datos de clientes.

- Ciber-espionaje dirigido a propiedad intelectual (PI) como diseño de nuevos productos, algoritmos, planes estratégicos y recursos estratégicos como petróleo, energía e infraestructura.

- Activismo, un nuevo fenómeno dirigido a determinados sitios, más por razones políticas que por ganancias financieras.

Estos ataques sortean las defensas perimetrales tradicionales al explotar vulnerabilidades de la aplicación web como inyección de código SQL o apalancando credenciales administrativas robadas para comprometer bases de datos administrativas.

La implementación de un monitoreo continuo a la base de datos y soluciones de seguridad ayudarán a evitar ataques externos como inyección de SQL en diversas maneras, todas las cuales pueden usarse simultáneamente para proporcionar una defensa en capas. Esto se logra mediante la creación y aplicación de políticas proactivas en tiempo real, como:

- Políticas de acceso que identifiquen comportamientos anormales mediante la continua comparación de actividad en la base de datos con una línea de base de comportamiento normal. Por ejemplo, un ataque por inyección de SQL típicamente mostrará patrones de acceso a base de datos no característicos de las aplicaciones estándar de la línea de negocios.

- Políticas de excepción basadas en umbrales definibles, como un número excesivo de intentos de conexión fallidos o errores de código SQL. Los errores SQL pueden indicar que un atacante está “echando un vistazo" a los nombres de las tablas principales, experimentando con comandos SQL al usar diferentes argumentos - como “Num_Tarj_Cred” o “Num_TC” - hasta encontrar un nombre de tabla válido que no produzca un error en la base de datos.

- Políticas de excepción basadas en códigos de error SQL específicos en la base de datos, como “ORA-00903: Nombre de tabla inválido” o bien “ORA-00942: La tabla o vista no existe.” Dichos códigos de error pueden ser indicativos de comportamiento de hackeo.

- Políticas de extrusión que examinan datos que salen de la base de datos respecto a patrones de datos específicos, como números de tarjeta de crédito o un alto volumen de registros devueltos que puedan indicar una violación.

- Firmas de políticas pre-configuradas que identifiquen intentos por explotar vulnerabilidades o funciones de sistema sin parches.

Escenario 2:

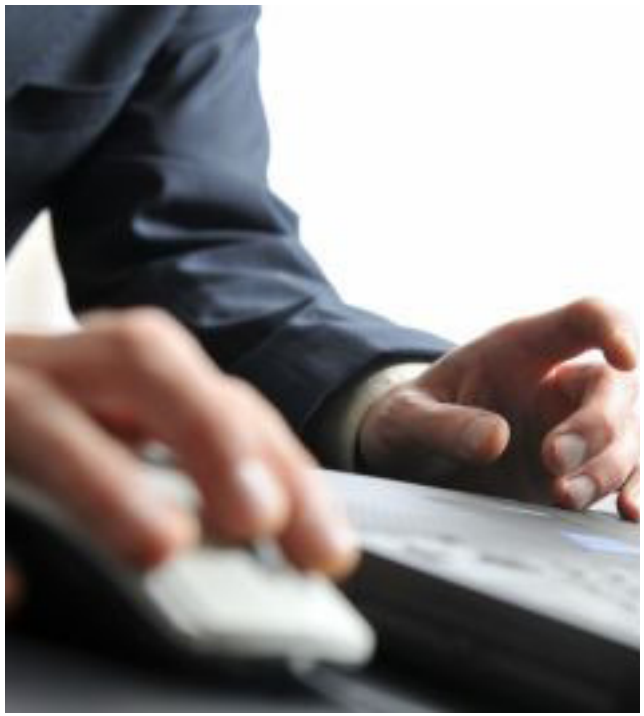
Bloquear acceso de usuarios con privilegios a información sensible

En la mayoría de los ambientes de TI, los usuarios con privilegios - como administradores de bases de datos, desarrolladores y personal subcontratado - pueden tener acceso sin restricciones a información sensible, con poco o ningún control de monitoreo de sus actividades. Estos "súper usuarios" pueden con facilidad sortear los puntos de control de seguridad a nivel de aplicación o de red.

Muchas organizaciones tienen políticas formales de seguridad de información que rigen la manera y el momento en que los usuarios con privilegios pueden acceder a los sistemas de bases de datos. Sin embargo, estas organizaciones carecen de controles de aplicación o visibilidad granular respecto a lo que realmente ocurre, exponiendo a fin de cuentas sus vulnerabilidades.

El acceso basado en roles y otros controles Integrados en los sistemas para gestión de bases de datos están diseñados para evitar que los usuarios finales tengan acceso a información sensible en bases de datos, pero no pueden evitar que los DBA y otros usuarios con privilegios, que tienen la capacidad de ejecutar cualquier comando en la base de datos, ejecuten algún comando u objeto de la base de datos como parte de su trabajo cotidiano.

Los desarrolladores de aplicaciones pueden acceder a la base de datos usando la cuenta que utiliza la aplicación misma (véase la figura 2) pero sin todas las molestas medidas de seguridad integradas en la aplicación. ¿Cómo identifica y maneja a una persona que está abusando de sus credenciales?



Escenario 2:

Para empeorar las cosas, se dificulta la asignación de responsabilidades, ya que los usuarios con privilegios con frecuencia comparten las credenciales usadas para acceder a los sistemas de bases de datos.

Las organizaciones que usan el ingreso a base datos nativo encuentran que este enfoque es poco práctico porque requiere cambios a la base de datos que afectan el desempeño y estabilidad de aplicaciones críticas para el negocio como ERP, CRM y sistemas para procesamiento de tarjetas de crédito. De igual manera, no se logra satisfacer el requerimiento de los auditores de separación de tareas, porque el acceso a base de datos no es controlado por personal de seguridad de TI y los administradores de bases de datos pueden darles la vuelta con facilidad.

Al desplegar una combinación de capacidades de monitoreo y bloqueo, proporcionadas por una solución de seguridad de base de datos, es posible controlar toda la actividad de la base de datos en la capa de red y en el servidor de base de datos mismo, evitando fugas de información en la fuente y cambios no autorizados a bases de datos críticas. Además, el uso de tecnologías de monitoreo en tiempo real puede dar el poder a las organizaciones de seguridad de TI para que de inmediato frustren el acceso no autorizado o sospechoso a bases de datos críticas, incluso por parte de usuarios con privilegios, mediante:

- Monitoreo de todas las transacciones en bases de datos para crear un rastro de auditoría continuo, detallado, que identifique el "quién, qué, cuándo, dónde y cómo" de cada transacción. Es requisito implementar políticas de acceso detalladas para regulaciones clave como Sarbanes-Oxley (SOX), el Estándar de Seguridad de la Industria de Pagos con Tarjeta (PCI-DSS), HIPAA/HITECH, NIST/FISMA SP 800-53 y leyes de protección de privacidad de datos estatales y locales.

- Análisis continuo de datos en tiempo real para identificar actividades no autorizadas o sospechosas y ejecutar acciones de respuesta que varían desde bloqueo de la transacción en tiempo real, hasta generación de una alerta para el equipo de seguridad.

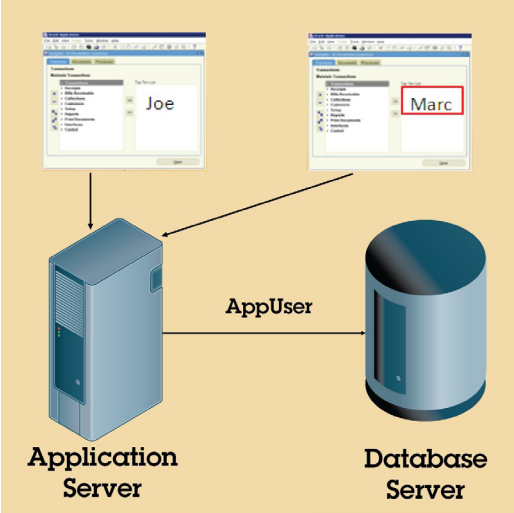
Escenario 3:

Identificar fraude en la capa de aplicaciones

Las aplicaciones multi capa como Oracle EBS, PeopleSoft, J.D. Edwards, SAP, Siebel, Business Intelligence, y los sistemas internos contienen la mayor parte de la información financiera, sobre clientes, empleados y propiedad intelectual más sensible de la empresa. Estos sistemas resultan los más difíciles de asegurar porque están altamente distribuidos y fueron diseñados para permitir acceso base web de personal interno y externo, como clientes, proveedores y socios.

Además, las aplicaciones multi capa enmascaran la identidad de los usuarios finales al nivel de transacción de base de datos, usando un mecanismo de optimización conocido como "pooling de conexión." Con el uso de conexiones en pool, la aplicación agrega todo del tráfico de usuarios dentro de unas pocas conexiones de base de datos que se Identifican

Figura 2



Problema: El servidor de aplicaciones usa una cuenta de servicio genérica (AppUser)para acceder a la base de datos que no identifica QUIEN (Joe o Marc) inició una transacción (pooling de conexión).

Identifican solamente mediante un nombre de cuenta de servicio genérico. El pooling de conexión dificulta la asociación de transacciones específicas con usuarios finales particulares. En consecuencia, resulta difícil rastrear transacciones fraudulentas. Finalmente, los usuarios con privilegios pueden acceder directamente a la información asociada con las aplicaciones empresariales, vía herramientas para el desarrollador como SQL *Plus, sorteando los controles dentro de la aplicación.

Sin monitoreo en la capa de aplicaciones, a las organizaciones les resulta difícil asociar transacciones específicas de base de datos con usuarios finales de una aplicación particular, dejando un gran hueco en su capacidad para detectar fraudes (y otros abusos de acceso legítimo) que ocurren vía las aplicaciones

Escenario 3:

empresariales. Con frecuencia se requiere este nivel de monitoreo para requerimientos sobre gobernabilidad de información, como SOX. Nuevos lineamientos para auditores del Consejo de Supervisión de Contabilidad de Empresas Públicas para cumplimiento con la ley Sarbanes- Oxley también subrayan el énfasis en controles anti fraude.

Mediante el monitoreo de la base de datos en tiempo real y una solución de auditoría, las organizaciones tienen la habilidad de capturar las transacciones directas y las indirectas. Se proporcionan capacidades para asegurar que se ejecuten transacciones vía conexiones en pool incluyendo la capa de aplicaciones asociadas, usando IDs en el rastro de auditoría y otras capacidades para identificar información como direcciones IP, nombre de registro de Dominio, etc. Estas capacidades, junto con el flujo de trabajo de cumplimiento automatizado, garantizan que las violaciones a la política se rastreen, investiguen y corrijan con facilidad.

Garantizar acceso autorizado a bases de datos

El acceso no autorizado a bases de datos con frecuencia pasa inadvertido, exponiendo datos sensibles y causando daños potenciales por miles de millones de dólares. Una estrategia sólida seguridad de la información y privacidad debe garantizar que la organización pueda identificar quiénes tienen acceso a la información, y garantizar que el acceso sea necesario para que una persona realice su trabajo.

Dos capacidades de soporte primarias son los controles de Autenticación y Autorización.

La autenticación es el proceso de identificar de manera única a una persona o sistema. El enfoque más típico es mediante el uso de una ID de usuario y contraseña. Al autenticar a los usuarios se asegura rendición total de cuentas por usuario y se administran los

privilegios para limitar el acceso a información; ésta debe aplicarse incluso a los usuarios de base de datos más privilegiados.

La autorización es el mecanismo para controlar qué información y qué acciones están disponibles para una persona en particular, y bajo qué circunstancias. Los mandatos regulatorios y requerimientos de seguridad exigen que las organizaciones adopten métodos de autenticación fuertes, con factores múltiples, con el fin de protegerse de acceso no autorizado y no identificado. Por ejemplo, los administradores de bases de datos deben estar autorizados sólo para realizar las funciones que necesitan para su trabajo. Sin embargo, el administrador de la base de datos no necesita acceso a los datos mismos.

Dentro de las bases de datos existe muchísima complejidad. Resulta muy difícil entender quién tiene acceso a qué información a través de qué roles y concesiones. Los auditores típicamente requieren que estos derechos se revisen de manera periódica. Así pues, una manera de ayudar a cumplir este requerimiento es mediante el escaneo automático de bases de datos seleccionadas para la recolección, organización,

Escenario 4:

distribución y revisión de información sobre derechos de usuarios –incluyendo los otorgados mediante roles y membresía a grupos.

Una solución de seguridad de base de datos construida con ese propósito incluye capacidades de reporte que agregan de manera automática información sobre derechos de usuarios a lo largo de toda la infraestructura heterogénea de la base de datos y también identifican qué usuarios tienen privilegios especiales particulares, qué nuevos derechos se han otorgado y quién los otorgó, y qué derechos tienen los usuarios particulares.

Escenario 5:

Detectar cambios no autorizados a la base de datos

Detectar cambios a la base de datos resulta importante desde el punto de vista de poner controles en torno a usuarios privilegiados. Sin embargo, también resulta importante desde la perspectiva de seguridad externa. Estos cambios pueden ser indicadores de que las bases de datos están comprometidas, pues los hackers con frecuencia hacen cambios a la base datos en el proceso de extraer datos o insertar malware.

En consecuencia, muchas organizaciones buscan monitorear sus infraestructuras de bases de datos usando controles automatizados y centralizados. Esto les permite rastrear todos los cambios a las bases de datos, incluso en ambientes complejos, heterogéneos y distribuidos, incluyendo cambios a:

- Estructuras de bases de datos como tablas, disparadores y procedimientos almacenados. Por ejemplo, puede detectar eliminaciones o inserciones accidentales de tablas críticas que impactan la gobernabilidad y calidad de las decisiones de negocios. Puede también de manera proactiva identificar actos maliciosos como "bombas lógicas" plantadas por empleados descontentos.

- Valores de datos críticos como información que afecta la integridad de las transacciones financieras.

- Objetos de seguridad y control de acceso como usuarios, roles y permisos. Por ejemplo, un contratista externo puede crear una nueva cuenta de usuario con acceso a bases de datos críticas y luego borrar toda la cuenta, eliminando todo registro de su actividad.

Escenario 5:

- Archivos de configuración de bases de datos y otros objetos externos que pueden afectar su postura de seguridad de bases de datos, tal como variables de ambiente/ registro, archivos de configuración (por ej., NAMES.ORA), archivos de comandos, archivos OS y ejecutables como programas Java.

Controles automatizados en tiempo real, implementados a través de una solución de seguridad de base de datos bien diseñada, pueden evitar acciones no autorizadas como: ejecución de búsquedas en tablas sensibles; cambio de valores de datos sensibles; añadir o eliminar tablas críticas (cambios de esquema) fuera de ventanas de cambio y creación de nuevas cuentas de usuarios y modificación de privilegios.

Otra mejor práctica consiste en utilizar la encriptación para que los datos sensibles resulten ilegibles, de manera que un atacante no pueda tener acceso a información de fuera de la base de datos. Esto se logra más fácilmente cuando se encriptan las bases de datos y archivos "en su lugar" vía el sistema operativo, a fin de evitar cambios costos y que consumen tiempo o la necesidad de re-arquitectura de la base de datos, archivos o redes de almacenamiento.

Conclusión

Las organizaciones deben construir programas para seguridad de información sólidos que los protejan y defiendan contra inyección de código SQL, scripting de sitios cruzados y violaciones de personas con privilegios de acceso a información basados en las mejores prácticas de seguridad y cumplimiento para bases de datos.

Según Forrester, "Cuando las empresas miran más allá de la auditoría y el monitoreo, muchas buscan un sólo proveedor que de soporte a todos sus requerimientos de seguridad de base de datos, incluyendo auditoría, asesoría de vulnerabilidad, enmascaramiento y encriptación y protección en tiempo real de la base de datos. Las soluciones de un sólo proveedor suelen ofrecer aplicación de políticas comunes entre sistemas de administración de base de datos heterogéneos, un tablero de monitoreo integrado, separación de roles superior y seguridad para base de datos de punta a punta para ambientes que pueden o no ser de producción.1

Los productos para seguridad de base de datos IBM® InfoSphere™ Guardium® proporcionan una solución robusta para el continuo monitoreo de acceso a bases de datos empresariales y simplifican las auditorías de cumplimiento con controles automatizados y centralizados para ambientes heterogéneos. El software InfoSphere Guardium de IBM ayuda a las organizaciones a:

- Evitar violaciones a la información, fraude de personas con acceso a la información y cambios no autorizados a información sensible.
- Monitorear usuarios con privilegios como administradores de bases de datos, desarrolladores y personal subcontratado
- Virtualmente eliminar el gasto indirecto y complejidad de las bitácoras de auditoría de los sistemas nativos para gestión de bases de datos
- Automatizar reportes de cumplimiento, evaluaciones de vulnerabilidad y configuración y descubrimiento de datos.
- Encriptar archivos en ambientes de base de datos.
- Enmascarar información confidencial en sistemas de prueba, capacitación y desarrollo.
- Redactar datos no estructurados en documentos, formatos y gráficas.

[1] Market Overview: Database Security, 2011, Forrester Research, Inc. Septiembre 19, 2011 | Actualizado: Septiembre 22, 2011

Para mayor información sobre cómo administrar la seguridad de bases de datos en su organización, visite

ibm.com/guardium

IBM Corporation Software Group Route 100
Somers, NY 10589 U.S.A.

Producido en los Estados Unidos de América
Enero 2012

IMB14130USEN