Planes detallados de tecnología

McAfee
An Intel Company

PROTECCIÓN DE BASES DE DATOS

Incrementar la seguridad ante los ataques y vectores de pérdida de información actuales

ARQUITECTURA DE REFERENCIA SECURITY CONNECTED

NIVEL 1 2 **3** 4 5

Security Connected

El marco Security Connected de McAfee permite integrar distintos productos, servicios y asociaciones para reducir los riegos de forma efectiva, eficiente y centralizada. Basado en más de dos décadas de prácticas de seguridad probadas, el enfoque Security Connected ayuda a las organizaciones de todos los tamaños y segmentos, de todas las zonas geográficas, a mejorar sus condiciones de seguridad, optimizar la seguridad para conseguir una mayor rentabilidad y alinear estratégicamente la seguridad con las iniciativas empresariales. La arquitectura de referencia Security Connected ofrece una ruta concreta desde las ideas hasta la implantación. Utilícela para adaptar los conceptos de Security Connected a sus riesgos, infraestructura y objetivos empresariales. En McAfee dedicamos todos nuestros esfuerzos a la búsqueda constante de nuevas soluciones y servicios que garanticen la total seguridad de nuestros clientes.

Incrementar la seguridad ante los ataques y vectores de pérdida de información actuales

Situación actual

En el año 2010, la cifra de fugas de datos llegó a su máximo histórico y el 47% de los ataques tardó minutos u horas en llegar desde el punto de entrada al de riesgo. Otro 44% lo consiguió en días, de acuerdo con el informe de 2011 sobre investigaciones de fugas de datos realizado por Verizon y el Servicio Secreto de Estados Unidos. Es decir, los malos consiguen entrar, y con rapidez. Y los buenos responden con lentitud. En el 38% de los casos se tardó semanas en descubrir el peligro y en el 36%, meses[1]. Es mucho tiempo para que los delincuentes pudieran apoderarse de lo que querían y escapar.

Los malos actúan en un plazo de tiempo de minutos y días, y los buenos en semanas o meses. ¿Cómo es posible que se muevan con tanta rapidez? Usando tácticas nuevas. El hacking (50%) y el malware (49%) fueron las más utilizadas. Además, el informe concluye que los delincuentes están persiguiendo objetivos de bajo perfil, organizaciones más pequeñas con sistemas peor protegidos, en lugar de dar el gran golpe a servidores con millones de registros.

Con frecuencia los delincuentes reciben la ayuda involuntaria de los empleados. Gracias a la ingeniería social y al robo de credenciales, los delincuentes pueden encontrar con facilidad la forma de parecer empleados con acceso legítimo. Y con bases de datos tan valiosas y una economía tan deprimida, el soborno también funciona. Según el mismo informe, pedir dinero y el soborno fueron las tácticas sociales utilizadas con más frecuencia el año pasado. Por tanto, no se puede confiar en la protección del perímetro para defender las bases de datos ni en que los empleados hagan lo correcto.

Preocupaciones principales

Las bases de datos no solo almacenan información crítica si no que suelen estar conectadas a múltiples sistemas que prestan servicios esenciales para las empresas. Cualquier interrupción del servicio, fuga o pérdida de datos involuntaria tiene la posibilidad de detener las operaciones de toda una empresa y perjudicar su reputación. Además, dado que las bases de datos guardan información sujeta a normativas y confidencial, una fuga normalmente se traduce en incumplimiento de las mismas y en un enorme coste de recuperación, en la pérdida de confianza de los consumidores y posiblemente en la pérdida drástica de la capitalización bursátil.

Para proteger los datos confidenciales frente a las amenazas externas e internas, se necesita visibilidad en tiempo real de la actividad de las bases de datos. En la actualidad, la mayoría de las organizaciones aprovechan las ventajas de las herramientas de inicio de sesión y auditoría inherentes a las bases de datos para protegerlas, pero estas herramientas no son las adecuadas contra las tácticas modernas de hacking e ingeniería social. Para poder proteger correctamente las bases de datos frente al código malicioso y la pérdida de información, es necesario abordar los siguientes temas:

- **La supervisión de la actividad y de los cambios**. Todas las bases de datos responden a comandos. Si un comando es el adecuado para el usuario que solicita datos, funcionará correctamente. Dado que los delincuentes y las herramientas son cada vez más sofisticados, los agresores pueden evadir las técnicas de detección típicas y aumentar sus privilegios. Los controles de acceso poco estrictos facilitan trabajo de los agresores. Típicamente, el nivel de acceso concedido a los usuarios sobrepasa en gran medida los derechos de acceso al sistema que necesitan o que sus puestos requieren. Cuentas viejas y un control poco riguroso de la creación de cuentas nuevas significan más puertas a las que los delincuentes pueden llamar. Primero atacan las contraseñas predeterminadas y demasiado sencillas y después aumentan los privilegios. Se ha demostrado que la supervisión de la actividad basada en la red no es adecuada para resolver este problema dado que los métodos de acceso local pueden evitar los sistemas de supervisión basada en la red.

- **Las herramientas de auditoría**. Las funciones de inicio de sesión y auditoría nativas de las bases de datos se quedan muy cortas para proporcionar la visibilidad necesaria. La mayoría no captura los cambios realizados, los privilegios utilizados, los administradores responsables o los cambios al sistema. Además, las actividades de inicio de sesión y auditoría integradas en las bases de datos pueden ser un obstáculo para el rendimiento. Son funciones diseñadas para supervisar, no para proteger, y los administradores pueden desactivarlas y eliminar así el valor que las herramientas nativas podrían aportar.
- **Evitar las interrupciones debidas a parches**. Los ingresos, el tiempo de actividad y la disponibilidad ganan la partida a la seguridad. Algunas organizaciones tienen ciclos de aplicación de parches superiores a los 12 meses. Cada año aparecen cientos de amenazas nuevas, pero dada la naturaleza crítica de las bases de datos, el tiempo de inactividad no es una opción. Las organizaciones quieren estar protegidas continuamente sin aplicar parches a las bases de datos.
- **La distribución de servicios en Internet**. Dado que las organizaciones empiezan a adoptar los servicios distribuidos en Internet, las bases de datos deben adaptarse para poder acceder a ellas y supervisarlas utilizando servicios web, no solo desde la red local.
- **Las pruebas de cumplimiento de normativas sectoriales, de la Administración e internas**. Dependiendo de la función de las bases de datos, puede ser necesario cumplir, informar y mantener las directivas de una serie de regulaciones tales como la DSS del PCI, Sarbanes-Oxley, HIPAA, SAS 70, GLBA y FERPA. Y si se hacen negocios en otros países, estos también tienen requisitos de control de la privacidad y financiero. Además, las organizaciones pueden haber elaborado sus buenas prácticas y estándares operativos, y los ejecutivos esperan que los cuadros de mando muestren la situación con respecto a las normas de la Administración pública.

Elementos para tomar una decisión

Las respuestas a las siguientes preguntas pueden influir en la arquitectura:

- ¿Qué normativas debe cumplir la organización?
- ¿Cómo se mide e informa del cumplimiento de las normativas de las bases de datos?
- ¿Existen bases de datos en sistemas operativos de 64 bits? ¿Cuáles son?
- ¿Se sabe el nivel de seguridad de las bases de datos?
- ¿Con qué frecuencia se aplican parches a las bases de datos?

Descripción de la solución

Todas las organizaciones dependen de las bases de datos para operar. Si no confiamos en que los proveedores de los sistemas operativos los protejan, ¿por qué nos conformamos con las herramientas de los proveedores para que nos ayuden a proteger las bases de datos más valiosas? Las bases de datos tienen desafíos exclusivos y normalmente la implantación de las directivas y normas de seguridad se ha dejado en manos de los administradores. Con la cifra de fugas procedentes de bases de datos en los titulares de los periódicos, debe considerarse una forma nueva de hacer las cosas que asegure que la integridad está protegida frente al código malicioso y, triste pero cierto, frente a los empleados de confianza.

Para resolver estas preocupaciones, la solución debe cumplir con los siguientes requisitos:

- **La supervisión de la actividad y de los cambios**. La solución debe poder supervisar el comportamiento y la actividad de todas las bases de datos desde una posición estratégica exterior a ellas. Si la supervisión se lleva a cabo solo dentro de las bases de datos, los administradores podrían desactivar la función (deliberada o involuntariamente). También debe poder terminar las sesiones que violen las directivas, enviar alertas a una consola gestionada centralizadamente y poner en cuarentena a los usuarios maliciosos o que no cumplen las normativas. Debe poder detectar las técnicas de evasión e impedir que actúen.
- **Las herramientas de auditoría**. De forma similar, las herramientas de auditoría no son eficaces si los administradores pueden desactivarlas. La solución debe proteger las funciones de inicio de sesión y auditoría desde el exterior de las bases de datos para garantizar que los registros se obtienen y están disponibles para analizarlos. Durante el análisis forense posterior a un incidente, esta pista de auditoría puede ayudar a saber la cantidad de datos que se han perdido y a conocer mejor las actividades maliciosas. La solución debe ser capaz de entregar pistas de auditoría e informes que cumplan con SOX, PCI y con otros requisitos de auditoría de cumplimiento de las normativas.
- **Evitar las interrupciones debidas a parches**. La solución debe poder detectar los ataques que intentan explotar las vulnerabilidades conocidas y los vectores de amenazas más frecuentes. Debe configurarse para enviar alertas o terminar la sesión en tiempo real. Esperar a que el proveedor de las bases de datos entregue los parches u omitir su instalación para evitar la pérdida de productividad hace que las bases de datos sean vulnerables a muchos vectores de amenazas. El concepto de parche virtual puede ayudar a proteger contra los ataques de día cero y las vulnerabilidades recientemente descubiertas, y puede implantarse sin interrumpir el funcionamiento de las bases de datos, protegiendo la información confidencial hasta que el parche pueda aplicarse.

- **La distribución de servicios en Internet**. Basarse en el análisis del tráfico de red para identificar las infracciones de las directivas es imposible o ineficiente en las arquitecturas distribuidas y muy dinámicas que se utilizan en la virtualización de centros de datos y la prestación de servicios desde Internet. Una solución debe configurarse de forma que se ponga en marcha automáticamente junto con cada nueva base de datos, solicite la directiva de seguridad en función de los datos que alberga y a continuación empiece a enviar las alertas oportunas al servidor de administración. Incluso si la conexión a la red se interrumpe, los datos todavía estarán protegidos mediante la aplicación de directivas locales.
- **El cumplimiento de las normativas sectoriales, de la Administración e internas**. Dado que las normativas y las regulaciones cambian, los informes que deben guardarse también tienen que cambiar. La solución debe proporcionar plantillas para cumplir las normativas, las que se guardan con los últimos controles y directrices de las violaciones. También debe poder identificar las amenazas cuando aparecen e informar de las medidas preventivas para reducir el riesgo y cumplir con las responsabilidades. Las plantillas preconfiguradas deben incluir la DSS del PCI, Sarbanes-Oxley, HIPAA y SAS-70, todas ellas visibles desde la plataforma administrada centralizadamente.

Tecnologías utilizadas en la solución de McAfee

McAfee ofrece dos productos especialmente diseñados para proteger las bases de datos, McAfee® Vulnerability Manager for Databases y McAfee Database Activity Monitoring. La administración centralizada de McAfee ePolicy Orchestrator® (McAfee ePO™) une estos dos productos en una sola plataforma de gestión de la seguridad y de cumplimiento de las normativas para toda la infraestructura.

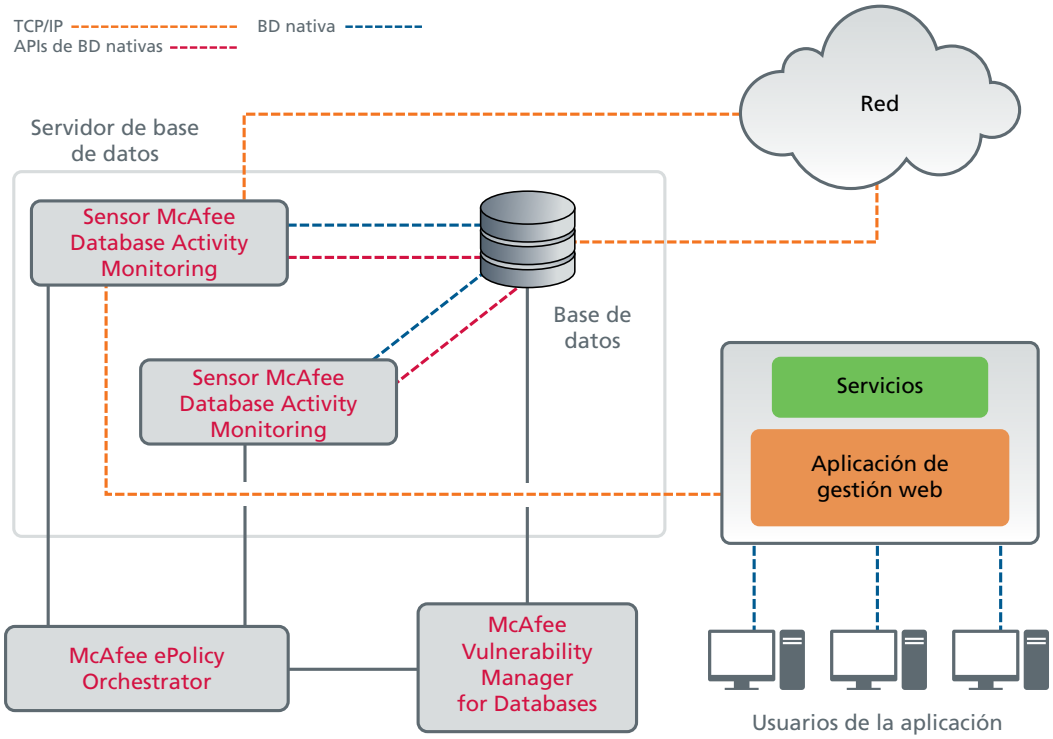
McAfee Vulnerability Manager for Databases permite realizar más de 3.000 exploraciones de vulnerabilidades en los sistemas de bases de datos más importantes como SQL Server, DB2 y MySQL. Al mejorar la visibilidad sobre las vulnerabilidades de las bases de datos (y ofrecer recomendaciones expertas para subsanarlas), reduce la probabilidad de que se produzcan fugas de datos perjudiciales y permite ahorrar costes, ya que allana el terreno de cara a las auditorías de cumplimiento de las normativas. Vulnerability Manager for Databases ayuda a reducir la superficie de ataque identificando las debilidades típicas que buscan los hackers y los delincuentes, tales como contraseñas sencillas, compartidas y cuentas predeterminadas. Para mantener el registro de eventos sospechosos y responder a ellos, informará de la versión y los parches, los objetos que han sufrido cambios, los privilegios modificados y de las pistas forenses de las herramientas de hackers comunes.

A diferencia de las auditorías o los análisis de registros básicos, que solo informan a posteriori de lo que ha ocurrido, las funciones de supervisión y prevención de intrusiones en tiempo real detienen las fugas de datos antes de que provoquen daños. Más de 380 reglas definidas previamente abordan problemas específicos para los que existen parches de los proveedores de las bases de datos, así como perfiles de ataque genéricos. Las plantillas predefinidas para directivas pueden personalizarse para sean compatibles con las reglas de acceso y los procesos de las bases de datos adecuados y que cumplan las normativas.

Las alertas se envían directamente al panel de supervisión con todos los detalles de las infracciones de las directivas necesarios para corregirlas. La configuración se puede ajustar de forma que las infracciones de alto riesgo terminen automáticamente las sesiones sospechosas y pongan en cuarentena a los usuarios maliciosos, lo que da tiempo al equipo de seguridad para investigar la intrusión.

Los ataques dirigidos a la información valiosa almacenada en las bases de datos pueden proceder de otras partes de la red, de usuarios locales conectados al propio servidor e incluso de los procedimientos almacenados o activadores en el interior de la propia base de datos.

McAfee Database Activity Monitoring utiliza sensores basados en memoria para supervisar la actividad y detectar los tres tipos de amenazas con una única solución no intrusiva. Las actualizaciones de parches virtuales para las vulnerabilidades nuevas que se van descubriendo se proporcionan con regularidad y se aplican sin necesidad de detener la base de datos. De este modo se protege la información confidencial hasta que el proveedor de la base de datos publique un parche y este se pueda aplicar. La información sobre las actividades y los eventos puede utilizarse después para demostrar durante las auditorías que se cumplen las normativas y para mejorar la seguridad general.



La protección especializada permite a McAfee evaluar las vulnerabilidades de las bases de datos y supervisar posibles acciones maliciosas y de riesgo.

McAfee Vulnerability Manager for Databases

Diseñado para acelerar los análisis iniciales y generar informes listos para usarse como respuesta a los requisitos de la mayoría de las normativas, McAfee Vulnerability Manager for Databases puede descubrir y analizar múltiples bases de datos desde una sola consola. Localiza e identifica las tablas que contienen información confidencial y realiza un análisis de puertos rápido que indica la versión de la base de datos y el estado de los parches. Además de detectar la solidez de las contraseñas (si son sencillas, predeterminadas y están compartidas), puede analizar las contraseñas con hash almacenadas como SHA-1, MD5 o DES. También comprobará la susceptibilidad a los riesgos específicos de las bases de datos, como la inyección SQL, el desbordamiento de búfer y el código PL/SQL malicioso o inseguro. A continuación presenta los hallazgos en forma de informes preconfigurados para las normativas más comunes.

McAfee Database Activity Monitoring

McAfee Database Activity Monitoring es un sensor de tamaño reducido, un agente de software que se instala en los propios servidores de bases de datos y supervisa toda la actividad. El sensor es un proceso independiente escrito en C++ que se ejecuta en los host de bases de datos. Se instala utilizando herramientas estándar de la plataforma (RPM, PKG, DEPOT, BFF o EXE) en una cuenta de usuario del sistema operativo distinta. El sensor identifica automáticamente todas las instancias de bases de datos del equipo y puede supervisar varias instancias, incluso diferentes tipos de bases de datos, en el mismo host.

Cuando se ejecuta, el sensor se conecta a la misma área de memoria caché SQL que la instancia utilizando mecanismos y APIs de solo lectura, y lleva a cabo la supervisión con un bucle de sondeo de muestras de memoria. En cada ciclo de muestreo, el sensor analiza las sentencias en ejecución y las anteriores de todas las sesiones de la instancia y, utilizando una directiva predefinida que recibe del servidor, determina de qué sentencias hay que alertar o cuáles bloquear. Las sentencias que incumplen la directiva se envían a la consola de administración como alertas en tiempo real. El sensor también puede configurarse para terminar las sesiones en caso de que se produzcan violaciones específicas y poner a los usuarios en cuarentena. No es intrusivo y consume pocos recursos de CPU (menos del 5% de un solo núcleo de CPU, incluso en equipos multinúcleo). Las funciones de prevención del sensor se implantan utilizando APIs nativas de las bases de datos que permiten terminar las sesiones sin poner en riesgo la integridad de los datos.

McAfee ePolicy Orchestrator (McAfee ePO)

McAfee ePO permite que la distribución de software y la gestión de directivas se lleven a cabo de forma centralizada y automática. McAfee Vulnerability Manager for Databases se integra en el panel de McAfee ePO para facilitar la elaboración centralizada de informes y de resúmenes de todas las bases de datos. McAfee ePO también se conecta a McAfee Database Activity Monitoring para proporcionar una sola vista y facilitar la generación de informes.

Impacto de la solución

Si implanta una protección especializada en los vectores de ataque y en la pérdida de información de bases de datos, puede mejorar la capacidad de detectar y defenderse de los ataques externos, así como reducir las posibilidades de correr riesgos o de sufrir interrupciones desde el interior de la red.

McAfee proporciona visibilidad y protección en tiempo real frente a todos los orígenes de los ataques supervisando y enviando alertas de los eventos sospechosos. Tanto si la amenaza procede de la red, de usuarios locales que han iniciado sesión en el mismo servidor, como del interior de las bases de datos, McAfee ayuda a reducir el riesgo y el incumplimiento de las responsabilidades deteniendo los ataques antes de que produzcan algún daño. La aplicación de parches virtuales a las vulnerabilidades recientemente descubiertas de las bases de datos las protege de inmediato sin interrumpir su actividad.

Las plantillas y las reglas predefinidas, las verificaciones automatizadas y actualizadas, y las interfaces basadas en el asistente aceleran el despliegue y contribuyen a que la arquitectura de seguridad de las bases de datos se audite de forma eficiente y sencilla.

Recursos adicionales

www.mcafee.com/es/products/database-security/index.aspx
www.mcafee.com/es/products/vulnerability-manager-databases.aspx
www.mcafee.com/es/products/database-activity-monitoring.aspx
www.mcafee.com/es/products/epolicy-orchestrator.aspx

Para obtener más información sobre la arquitectura de referencia Security Connected, visite: www.mcafee.com/es/enterprise/reference-architecture/index.aspx.

Acerca del autor

Uy Huynh es el Director General de ingeniería de ventas de McAfee. Es responsable de asegurar que su equipo elabore las soluciones y diseños de seguridad adecuados, y las buenas prácticas para ayudar a los clientes a mejorar las condiciones de seguridad y a proteger los activos digitales más importantes. Uy es un experto en seguridad que ha trabajado con grandes clientes Fortune 100 como HP, Oracle, ATT y McKesson para seleccionar los productos de seguridad idóneos que satisfacen sus complejos requisitos.

Antes de incorporarse a McAfee, dirigió y creó la organización de técnica de sistemas de Foundstone. Durante esa etapa, desarrolló las buenas prácticas para gestionar las vulnerabilidades y los riesgos de grandes redes y sistemas. Antes de trabajar en Foundstone, fue consultor senior en ISS, donde desarrolló una serie de soluciones, políticas y tecnologías de seguridad para grandes organizaciones.

[1] http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

McAfee, S.A.
Avenida de Bruselas nº 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8535
www.mcafee.com/es

38600bp_protecting-databases-L3_1111