Una estrategia de seguridad de base de datos para prevenir realmente las violaciones de datos

Yonathan Mamani
yonathan@upt.pe

Luis Moreno
luis@upt.pe

Diego Layme
diego@upt.pe

1. ABSTRACT

El documento se centra principalmente en los problemas de seguridad que están asociados con el sistema de base de datos. La seguridad de los datos es uno de los desafíos más importantes y cruciales en el mundo digital. Se exige seguridad, privacidad e integridad de los datos en cada operación que se realiza en Internet. Siempre que se discute la seguridad de los datos, se encuentra principalmente en el contexto de la transferencia segura de datos a través de redes de comunicación no confiables. Pero la seguridad de los datos en las bases de datos también es importante. Con ataques cada vez más sofisticados y aumento del robo de datos internos, la seguridad de la base de datos merece un enfoque más fuerte que va más allá de la autenticación tradicional, la autorización y el control de acceso (AAA). Una sola intrusión que comprometa datos privados como números de tarjetas de crédito, números de seguridad social u otros datos financieros puede causar un daño inmenso a la reputación de una empresa, por no mencionar el inicio de juicios y multas regulatorias que pueden tener un impacto a largo plazo. La seguridad de la base de datos es la última línea de defensa, por lo que merece un mayor enfoque en la protección de datos privados contra ataques internos y externos de lo que los profesionales de TI han dado tradicionalmente. Con un número cada vez mayor de ataques internos y externos a aplicaciones corporativas y gubernamentales y un mayor cumplimiento de las normativas, la seguridad de los datos sigue siendo la principal prioridad para las organizaciones año tras año. Aunque muchas empresas están tomando medidas más enérgicas para proteger sus datos, aún existen vacíos importantes. el núcleo de las bases de datos que albergan las joyas de la corona corporativa. Muchas empresas no tienen una estrategia integral de seguridad de base de datos empresarial que pueda defenderse contra ataques sofisticados originados externa o internamente, rastrear datos confidenciales cuando se copian en múltiples ubicaciones o incluso cumplir con los requisitos reglamentarios emergentes más estrictos. Además, la mayoría de las empresas tienden a centrarse en los controles de detección en lugar de medidas preventivas cuando se trata de la seguridad de la base de datos, lo que las hace altamente estudiadas por algunas organizaciones de investigación y descubrió que algunas empresas en los Estados Unidos y Europa, que cubren servicios financieros, son vulnerables. En contraste, la investigación sugiere que las compañías que implementaron una solución de seguridad de base de datos completa e integrada con un fuerte énfasis en las medidas preventivas lograron mejores controles de seguridad, introdujeron un mayor grado de automatización en toda la empresa y tenían más confianza en la defensa contra ataques. Un experto en salud, manufactura, comercio minorista, telecomunicaciones, servicios públicos y medios acordaron que la seguridad de la base de datos era fundamental para su organización, y la mayoría estaba invirtiendo más tiempo y esfuerzo para mejorar los controles de la base de datos. Este trabajo de investigación describirá las infracciones recientes de la base de datos y examinará los errores comunes de seguridad cometidos por los administradores de la base de datos, el personal de seguridad y los desarrolladores de aplicaciones. También proporcionará una idea de cómo los hackers pueden aprovechar esos errores. Este documento luego describirá cómo una plataforma de seguridad de base de datos novedosa puede ayudar a alinear la base de datos con las políticas de seguridad; estrategia de seguridad de base de datos integral; medidas preventivas para la seguridad de la base de datos; detectar anomalías y realizar rutinas de seguridad; políticas de seguridad, estándares, separación de roles y disponibilidad; y aplique medidas de seguridad avanzadas (como auditorías

de bases de datos, monitoreo y evaluación de vulnerabilidades) a todas las bases de datos críticas que almacenan datos valiosos. En este documento presentaremos varios problemas en la seguridad de la base de datos, como los objetivos de las medidas de seguridad, las amenazas a la seguridad de la base de datos y algunas de las técnicas de seguridad comunes para los datos que se pueden implementar para fortalecer las bases de datos.

2. INTRODUCCION

Las organizaciones han llegado a confiar en la fluidez de información y los beneficios de la información sobre demanda. Sin embargo, con la omnipresencia y la inmediatez de la información viene el aumento Importancia de gestionar riesgos y proteger. Información de las amenazas de seguridad asociadas. La seguridad de la información se centra cada vez más en el insider - los usuarios de confianza autorizados (empleados, socios, contratistas y clientes) con las claves de las joyas de la empresa: propiedad intelectual. Mientras Estos usuarios son de confianza, no hay problema. Sin embargo, una vez que deciden usar sus privilegios para acceso inadecuado, las medidas de seguridad tradicionales No detectar o detener el robo de información [1]. El mayor potencial para el robo de datos ha forzado organizaciones a considerar el valor y los riesgos de Información y definir procesos y tecnologías para salvaguardarlos Esto es mucho más fácil decirlo que hacerlo; ya que la información no puede ser secuestrada en ”segura”paraísos, separados del uso diario, con el fin de protegerlo. Los usuarios no pueden ser restringidos de acceder información requerida por su organización definida. responsabilidades, a menos que las empresas estén dispuestas a proteger la información a riesgo de productividad y ingresos. Como la seguridad de la información no ofrece retorno inversiones, es poco probable que las organizaciones adopten políticas de seguridad de la información cuando vienen en el gastos de productividad e ingresos. Las organizaciones han adoptado sistemas de bases de datos como tecnología clave de gestión de datos para la toma de decisiones y las operaciones del día a día. Las bases de datos están diseñadas para mantener grandes cantidades de datos y gestión de datos. implica tanto la definición de estructuras para el almacenamiento de información y proporcionar mecanismos para Manipulación de la información.
Como los datos van a ser compartido entre varios usuarios el sistema debe evitar resultados anómalos y garantizar la seguridad de la información almacenada a pesar de los fallos del sistema y intentos de acceso no autorizado.

Los datos involucrados Aquí puede ser altamente sensible o confidencial, por lo tanto haciendo la seguridad de los datos gestionados por estos.

Los sistemas son aún más cruciales como cualquier violación a la seguridad. no afecta a una sola aplicación o usuario, pero puede tienen consecuencias desastrosas en la totalidad organización. Una serie de técnicas de seguridad tienen sido sugerido durante el período de tiempo para abordar el temas de seguridad. Estos pueden ser clasificados como accesos. control, control de inferencia, control de flujo y cifrado [2]. La variedad y volumen de datos recolectados, y la potencial para usar esto para mejorar nuestra vida diaria, seguir creciendo para el futuro previsible. Mientras que la Los beneficios potenciales son grandes, para numerosas aplicaciones. áreas, la privacidad de los datos y la seguridad de los datos deben ser dirigido para lograr los mayores beneficios mientras Proteger las libertades civiles. [3] Con lo aparentemente Flujo interminable de informes de noticias de hacks y datos fugas, una de las principales cuestiones de datos de 2014 que podemos Esperar que continúe en 2015 son grandes violaciones de datos. [3]. En Esta era de conectividad electrónica universal, de virus. y hackers, de escuchas electrónicas y fraude electrónico, de hecho no hay momento en el que La seguridad no importa. [4] El crecimiento explosivo en sistemas informáticos y sus interconexiones a través de Las redes ha aumentado la dependencia tanto de Organizaciones e individuos en la información. Almacenado y comunicado utilizando estos sistemas. Esta en a su vez, ha llevado a una mayor conciencia de la necesidad de proteger los datos y recursos de la divulgación, a garantizar la autenticidad de los datos y mensajes, y de protege los sistemas de ataques basados en la red [4] Asegurar la base de datos puede ser el más grande Acción que una organización puede tomar, para proteger sus activos. La base de datos más utilizada en una empresa La organización es la base de datos relacional. Los datos son un valioso recurso en una organización empresarial. Por lo tanto ellos tienen una gran necesidad de controlar estrictamente y manejándolo Como se discutió anteriormente, es el responsabilidad del DBMS para asegurarse de que los datos

Se mantiene seguro y confidencial, ya que el elemento que controla el acceso a la base de datos. Base de datos empresarial su infraestructura está sujeta a una gama abrumadora de amenazas la mayoría de las veces.

3. OBJETIVOS

Entender la importancia de una estrategia de base de datos y como prevenir las brechas de seguridad

4. MARCO TEORICO

- Data Base Management System (DBMS)
  Sistema de administración de bases de datos. Software que controla la organización, almacenamiento, recuperación, seguridad e integridad de los datos en una base de datos. Acepta solicitudes de la aplicación y ordena al sistema operativo transferir los datos apropiados.

- Base de datos

  Una base de datos es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. En este sentido; una biblioteca puede considerarse una base de datos compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta.

- Seguridad

  Ausencia de peligro o riesgo

- Estrategia

  una planificación de algo que se propone un individuo o grupo

- Administrador de base de datos
  Es aquel profesional que administra las tecnologías de la información y la comunicación, siendo responsable de los aspectos técnicos, tecnológicos, científicos, inteligencia de negocios y legales de bases de datos, y de la calidad de datos.

- Sistema de prevención de intrusos

  Un sistema de prevención de intrusos (o por sus siglas en inglés IPS) es un software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de prevención de intrusos es considerada por algunos como una extensión de los sistemas de detección de intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos.

- SQL
  es un lenguaje específico del dominio utilizado en programación, diseñado para administrar, y recuperar información de sistemas de gestión de bases de datos relacionales

5. ANALISIS

ESTRATEGIA INTEGRAL DE SEGURIDAD DE BASE DE DATOS

Una estrategia integral de seguridad de base de datos se centra sobre la protección proactiva de los datos de ataques internos y externos, minimizando la exposición de los datos a usuarios de TI privilegiados y protegiendo todas las bases de datos, incluida la producción y la producción. La mayoría de las empresas a menudo se centran en la seguridad de la red basada en el perímetro, ofreciendo la primera línea de defensa, pero la creciente complejidad del entorno y los ataques sofisticados requieren que las empresas tengan una visión más amplia de la seguridad de los datos. La seguridad de la base de datos, que es la última línea de defensa para los datos empresariales, necesita un mayor enfoque que otras capas de la pila de aplicaciones porque considera que las joyas de la corona son una clave para construir cualquier éxito. estrategia de seguridad de base de datos integral comprende de:

- Comprender qué datos deben protegerse, como números de tarjetas de crédito, números de la Seguridad Social, datos de clientes, información de identificación personal, salud protegida información, y propiedad intelectual.

- Comprensión de los requisitos de cumplimiento normativo aplicables, como SarbanesOxley (SOX), la Industria de tarjetas de pago (PCI), la Ley de responsabilidad y portabilidad de seguros de salud (HIPAA) y los reglamentos de la Unión Europea.

- Realizando un inventario de todas las bases de datos, Incluida la no producción.
- Descubrir y clasificar bases de datos en función de la sensibilidad de los datos.
- Establecimiento de políticas de seguridad para todas las bases de datos.
- Convertir las políticas en acciones y desplegarlas en bases de datos.
- Tomar las medidas de seguridad adecuadas, como encriptación, auditoría, control de acceso, monitoreo y enmascaramiento de datos.
- en busca de una solución de seguridad de base de datos completa que pueda implementar una base de datos robusta a un bajo costo.

A.Tres pilares clave de la base de datos integral estrategia de seguridad:

- Fundación Pilar- Comprende Del Descubrimiento, Clasificación, AAA, y Gestión de parches
- Pilar de detección, se compone de auditoría, Monitoreo, y evaluación de vulnerabilidad
- Pilar Preventivo - Comprende De Datos Cifrado, enmascaramiento de datos y base de datos Cortafuegos

Pilar de fundación

Cree una base sólida con AAA, descubrimiento y clasificación, y administración de parches. Comprender qué bases de datos contienen datos confidenciales es un requisito fundamental para cualquier estrategia de seguridad de base de datos. Las empresas deben realizar un inventario completo y continuo de todas las bases de datos, incluidas la producción y la no producción, y clasificarlas en categorías que deben respetar las mismas políticas de seguridad. Todas las bases de datos, especialmente las que contienen datos privados, deben tener una AAA sólida, incluso si el nivel de la aplicación tiene autenticación y autorización. La falta de una base AAA sólida debilita otras medidas de seguridad como la auditoría, el monitoreo y el cifrado. Además, los profesionales de seguridad de bases de datos deben parchar todas las bases de datos críticas de forma regular para eliminar las vulnerabilidades conocidas.

Pilar de detección

Establezca la detección de intrusiones con auditoría, monitoreo y evaluación de vulnerabilidad. Cada vez que los datos críticos cambian inesperadamente o se produce una actividad sospechosa de acceso a los datos, es fundamental que la organización inicie una investigación rápida para determinar qué sucedió. La auditoría de la base de datos brinda la capacidad de responder preguntas difíciles como ”¿quién cambió qué datos?”Y çuándo se modificaron”. Además, el monitoreo de seguridad de la base de datos proporciona alertas y protección en tiempo real, lo cual es esencial para defenderse contra ataques sofisticados. Finalmente, una evaluación de vulnerabilidad informa sobre las brechas de seguridad en el entorno de la base de datos, como contraseñas débiles o privilegios de acceso excesivos, que complementan la DBA y la supervisión de grupos de seguridad.

Pilar preventivo

Tome medidas preventivas con cifrado, enmascaramiento de datos y gestión de cambios. La seguridad preventiva es deseable para todas las bases de datos, pero es esencial para aquellos que tienen datos confidenciales. El objetivo es evitar el acceso no autorizado y la exposición de datos confidenciales. Las medidas de seguridad preventivas incluyen: 1) el uso de la red y el cifrado de datos en reposo para evitar la exposición de datos a miradas indiscretas, incluidas las de redes internas; 2) enmascarar datos privados en bases de datos que no sean de producción, como las de prueba, desarrollo y capacitación para evitar la exposición de datos a usuarios privilegiados, como evaluadores, desarrolladores y proveedores de outsourcing; y 3) requerir cambios en las estructuras de esquema realizadas como parte del desarrollo de la aplicación para seguir procedimientos formales que aseguren que solo se permiten los cambios aprobados en la producción.

B.Brechas de implementación de seguridad de base de datos

Las empresas, en su mayor parte, todavía dependen de la seguridad de la red para proteger sus bases de datos. Aunque esto puede evitar una intrusión muy básica en la infraestructura de la base de datos, la seguridad de la red no puede proteger los datos en las bases de datos. Especialmente a medida que más y más ataques contra bases de datos explotan el acceso legítimo a bases de datos al comprometer las aplicaciones y las credenciales del usuario. Hoy en día, los ataques a la información digital son más sofisticados, se producen desde lugares remotos en la Web y en velocidades de iluminación que hacen que sea difícil de detectar y responder antes de que el atacante se haya salido con la información. Aunque la mayoría de las empresas tienen una estrategia de seguridad de datos, muchas no tienen una estrategia de seguridad de base de datos que garantice la protección completa de las bases de datos críticas y la prevención de ataques [7]. A diferencia de la seguridad de la base de datos que se centra principalmente en las bases de datos, la seguridad de los datos es más amplia, ya que abarca bases de datos, aplicaciones de nivel medio, infraestructura y red en toda la pila de tecnología. La mayoría de las bases de datos son vulnerables a algún tipo de ataque, pero sin procesos y tecnologías de seguridad sólidos en su lugar, son objetivos fáciles. Si bien todos los productos DBMS empresariales ofrecen características de seguridad básicas, las empresas todavía necesitan políticas y procedimientos sólidos para proteger los datos. La seguridad de la base de datos no se trata solo de habilitar la auditoría y el monitoreo, se trata de establecer una estrategia integral que evite el acceso no autorizado a datos de piratas informáticos, aplicaciones e incluso a usuarios de bases de datos privilegiados. La mayoría de las empresas no tienen una estrategia de seguridad de base de datos en toda la empresa que realmente se centre en prevenir las violaciones de la base de datos Algunos tienen una estrategia de seguridad muy básica que solo abastece a una región geográfica particular o ciertas aplicaciones. Independientemente de cuán sofisticada sea su estrategia, la mayoría de las empresas no están haciendo lo suficiente para proteger sus bases de datos. Más bien pesimista, esto indica que solo una infracción hará que las personas presten más atención; hasta entonces, la seguridad de la base de datos no obtendrá la prioridad que necesita [11].

C. Establecer una base de seguridad de base de datos sólida, las empresas deben usar

- Descubrimiento y clasificación de bases de datos: la mayoría de las grandes empresas de hoy en día tienen cientos o miles de bases de datos para respaldar sus negocios. Algunos tienen hasta 15,000 bases de datos de producción, un volumen que a menudo crea un gran desafío de seguridad, especialmente si una gran cantidad de estas bases de datos contienen datos confidenciales. Algunas empresas solo implementan medidas de seguridad avanzadas en las bases de datos que son visibles para los auditores, dejando otras bases de datos vulnerables a los ataques. A muchas empresas grandes les resulta muy difícil hacer un seguimiento de cuántas bases de datos existen y qué bases de datos, tablas y columnas de producción y no producción contienen datos confidenciales. Esto es aún más problemático cuando se admiten aplicaciones heredadas con poca o ninguna documentación de base de datos, lo que deja a los DBA y al personal de seguridad sin saber qué columnas o tablas deberían proteger.

- Autenticación y autorización para controlar el acceso a la base de datos: la autenticación es el proceso de verificación de la identidad del usuario. Una identidad de base de datos se puede vincular a un directorio LDAP o al Directorio Activo de Microsoft para que los usuarios no tengan que ingresar sus credenciales nuevamente si ya se han autenticado. Los DBA deben verificar todos los nombres de inicio de sesión utilizados en las bases de datos de forma regular para garantizar que solo existan usuarios autorizados, deshabilitando aquellos que no están en uso. Idealmente, para imponer la separación de roles, un grupo distinto de los DBA debería crear inicios de sesión de usuarios. Incluso si una aplicación realiza la autenticación y la autorización, los DBA deben proteger las bases de datos al garantizar que solo existan cuentas de usuario activas en cada base de datos. Además, los DBA no deben usar la cuenta de usuario de DBA como predeterminado, sino solo cuando sea necesario; las organizaciones deben dar cuentas individuales a los DBA y hacer que

su actividad sea monitoreada por profesionales de seguridad y gestión de riesgos, al igual que otros usuarios. · Control de acceso para concretar el acceso a datos privados. El control de acceso garantiza que solo el personal autorizado tenga acceso a la información y tenga la capacidad de cambiar o eliminar datos. Los DBA deben crear roles que agrupen a los usuarios de acuerdo con sus privilegios de seguridad y los gobiernan asignándoles privilegios apropiados a cada rol. Las aplicaciones basadas en web que utilizan una identidad genérica de base de datos de administrador para obtener acceso a los datos en bases de datos representan una amenaza para la seguridad y, si es posible, se deben monitorear regularmente o cambiar a seguridad de nivel de usuario. De lo contrario, la creciente cantidad de ataques de inyección de SQL significará un mayor riesgo de exposición de datos privados e incluso corrupción en la base de datos; a medida que tales aplicaciones ejecutan comandos SQL en bases de datos con privilegios de nivel de administrador.

- Control de acceso avanzado para rastrear el uso de usuarios privilegiados. Más allá del control de acceso a datos tradicional, las empresas también deben tomar medidas avanzadas de control de acceso de seguridad para proteger los datos de usuarios privilegiados como administradores, desarrolladores, evaluadores y arquitectos. Además, las organizaciones deben segregar las tareas para garantizar que ningún usuario con privilegios tenga acceso completo a los datos privados, y deben habilitar la autorización basada en políticas multifactor siempre que sea posible. Los profesionales de la seguridad y la gestión de riesgos deben realizar un seguimiento de DBA y otras actividades de usuarios privilegiados

- Gestión de parches para protegerse contra vulnerabilidades. Todos los productos DBMS son vulnerables y, a menudo, lanzan parches de seguridad trimestralmente o según sea necesario a medida que el proveedor descubre vulnerabilidades. Si no se aplican todos los parches de seguridad actuales, se debilitan todas las demás medidas y procedimientos de seguridad. Todas las empresas deben aplicar parches de forma regular, pero solo después de probar las aplicaciones de base de datos afectadas para detectar problemas. Los profesionales de la seguridad y la gestión de riesgos también deben realizar un seguimiento de los parches de DBMS relacionados con la seguridad y notificar a los DBA su posible impacto en la seguridad.

D. Importancia de la prevención en lugar del enfoque en el seguimiento

Muchas empresas tienen algún nivel de auditoría de base de datos y capacidad de monitoreo implementado para muchas de sus bases de datos críticas. Las funciones nativas de auditoría y monitoreo de bases de datos que venían con el producto DBMS fueron implementadas generalmente por la mayoría, mientras que algunas tenían soluciones adicionales de terceros o proveedores de bases de datos. Curiosamente, muchas empresas confían en los firewalls de red y en el control de acceso a nivel de aplicaciones junto con el monitoreo de la base de datos para evitar violaciones de datos. Desafortunadamente, por supuesto, este enfoque no proporciona en realidad ataques de protección en tiempo real que exploten el acceso legítimo a la base de datos, como los ataques de inyección de SQL o el acceso directo que elude las aplicaciones que utilizan credenciales robadas, y se puede lograr fácilmente. Hasta que alguien realmente ataque las bases de datos directamente, es probable que el enfoque en la seguridad de la base de datos permanezca bajo. Las empresas creen que su primera línea de defensa, que incluye seguridad a nivel de red y de aplicación, es suficiente para defenderse contra ataques en tiempo real. La supervisión de la seguridad de la base de datos es el proceso y la tecnología de la actividad de supervisión en una base de datos para el acceso no autorizado, incluidos los fines fraudulentos para cumplir con los requisitos de cumplimiento, como SOX y PCI. Considerando que, la prevención es el proceso y la tecnología de tomar medidas proactivas para prevenir ataques de datos confidenciales en tiempo real. Ambos son igual de importantes, pero la prevención definitivamente debe ser la principal prioridad para todos. Definitivamente, la prevención es aún más importante que el monitoreo, que puede ser pasivo, ya sea un firewall y es más avanzado, a nivel de base de datos y a nivel de red.

E.Prevención de ataques de plataforma

Actualizaciones de software y prevención de intrusiones La protección de los activos de base de datos de los ataques de la plataforma requiere una combinación de actualizaciones de software regulares (parches) y sistemas de prevención de intrusos (IPS). Las actualizaciones proporcionadas por los proveedores eliminan las vulnerabilidades encontradas en la plataforma de base de datos a lo largo del tiempo. Desafortunadamente, las actualizaciones de software son proporcionadas e implementadas por las empresas de acuerdo con ciclos periódicos. Entre los ciclos de actualización, las bases de datos no están protegidas. Además, los problemas de compatibilidad a veces impiden las actualizaciones de software por completo. Para abordar estos problemas, se debe implementar IPS. Como se describió anteriormente, IPS inspecciona el tráfico de la base de datos e identifica los ataques dirigidos a las vulnerabilidades conocidas [12]

MEDIDAS PREVENTIVAS PARA LA SEGURIDAD DE BASES DE DATOS

Después de establecer una buena base de seguridad de base de datos, debe tomar medidas preventivas para proteger las bases de datos críticas. Estas medidas preventivas proporcionan una capa adicional de protección para las bases de datos de producción y no producción, lo que garantiza que haya protegido los datos privados de todos los usuarios no autorizados, incluidos los piratas informáticos. En esta era de conectividad electrónica universal, de virus y piratas informáticos, de escuchas electrónicas y fraude electrónico, no hay ningún momento en el que la seguridad no importe. Dos tendencias se han unido para hacer que el tema de esta investigación sea de vital interés. Primero, el crecimiento explosivo de los sistemas informáticos y sus interconexiones a través de las redes ha aumentado la dependencia tanto de las organizaciones como de los individuos de la información almacenada y comunicada mediante estos sistemas. Esto, a su vez, ha llevado a una mayor conciencia de la necesidad de proteger los datos y recursos de la divulgación, garantizar la autenticidad de los datos y mensajes, y proteger los sistemas contra ataques basados en la red. En segundo lugar, las disciplinas de criptografía y seguridad de la red han madurado, lo que lleva al desarrollo de aplicaciones prácticas y fácilmente disponibles para hacer cumplir la seguridad de la red [13].

Las medidas preventivas incluyen

- ifrado de la base de datos para proteger las bases de datos de producción: el cifrado es el proceso de transformación de datos mediante el uso de un algoritmo de cifrado para que sea ilegible. Puede implementar el cifrado de la base de datos en dos capas diferentes: 1) en la capa de red, que asegura los paquetes de datos en movimiento entre la base de datos y otros nodos, como los usuarios o las aplicaciones, protegiendo los datos privados contra miradas indiscretas que puedan estar indagando en el tráfico de la red, y 2) cifrado de datos atrasados, que se centra en los datos almacenados en la base de datos. A medida que abordan diferentes amenazas, estos enfoques de encriptación pueden implementarse de manera independiente. Por lo general, ninguno de los dos tiene un impacto en la funcionalidad de la aplicación. A diferencia del cifrado de red, el cifrado de datos en reposo tiene varias opciones de implementación, que incluyen nivel de columna, nivel de espacio de tablas, nivel de página y nivel de archivo. El cifrado de datos en reposo evita que cualquier persona que tenga acceso al archivo del sistema operativo subyacente vea los datos, ya que los DBMS generalmente almacenan los datos en texto sin cifrar.

- Enmascaramiento de datos para proteger datos en bases de datos que no son de producción: el uso o la copia de datos confidenciales de clientes, empleados o compañías de las bases de datos de producción para desarrollar o probar aplicaciones viola las leyes y regulaciones de privacidad de datos. La privacidad de los datos no se detiene con los sistemas de producción; también debe extenderse a entornos que no sean de producción, incluidas las pruebas, el desarrollo, el control de calidad (QA), la puesta en escena y las instancias de capacitación, donde sea que puedan residir los datos privados. Los profesionales de seguridad de bases de datos deben evaluar el uso de enmascaramiento de datos y la generación de datos de prueba para proteger los datos privados en entornos de prueba o cuando se subcontrata el desarrollo de aplicaciones.5

- Procedimientos de administración de cambios para proteger estructuras de bases de da-

tos críticas: la mayoría de las bases de datos se someten a cambios de esquema de forma regular para admitir los requisitos de aplicaciones y de negocio. En el pasado, el esquema u otros cambios en la base de datos en el entorno de producción requerían un cierre de la base de datos, pero las nuevas versiones de DBMS ahora permiten muchos de estos cambios mientras la base de datos está en línea, lo que crea un nuevo riesgo de seguridad. Los profesionales de seguridad de bases de datos deben seguir un procedimiento formal de administración de cambios para garantizar que los administradores cambien las bases de datos de producción solo después de la aprobación de la administración y que hagan un seguimiento de todos los cambios. Además, las organizaciones deben actualizar sus planes de recuperación y disponibilidad para hacer frente a la nueva contingencia de corrupción a los datos o metadatos que traen tales cambios.

DETECCIÓN DE ANOMALÍAS Y REALIZACIÓN DE CONTROLES DE SEGURIDAD RUTINARIOS

La comprobación periódica de las bases de datos para detectar anomalías en los datos y la actividad es un componente crítico de una estrategia integral de seguridad de la base de datos. Los datos y los metadatos en las bases de datos se pueden acceder, cambiar o incluso eliminar en cuestión de segundos. Para respaldar los estándares de cumplimiento normativo, como PCI, HIPAA, SOX y EU, los profesionales de la seguridad y la gestión de riesgos deben realizar un seguimiento de todos los accesos y cambios a los datos privados, como los números de tarjetas de crédito, números de seguridad social y los nombres y direcciones de las bases de datos críticas. Si los datos privados fueron cambiados o accedidos sin la autorización apropiada, las organizaciones deben responsabilizar a alguien. La seguridad de la capa de detección incluye:

- Auditoría de cumplimiento de bases de datos y alertas sobre anomalías de datos: aunque la auditoría de bases de datos ha existido durante décadas, su importancia no fue tan grande hasta hace poco. La auditoría verifica e informa de cualquier acceso, actualización y eliminación de datos. Produce una pista de auditoría que es esencial para cumplir con las regulaciones como SOX, PCI y HIPAA. No todas las bases de datos necesitan auditoría; por lo tanto, los profesionales de la seguridad y la gestión de riesgos solo deben permitir la auditoría de bases de datos selectivas. El problema de la auditoría con una sobrecarga significativa del sistema ha disminuido a lo largo de los años gracias a la innovación de DBMS y las soluciones de proveedores de terceros [16]. Hoy en día, muchas empresas realizan una extensa auditoría de la base de datos con una sobrecarga del sistema inferior al 10

- Monitoreo de la seguridad y defensa de la protección contra ataques en tiempo real: el monitoreo de la base de datos y la protección en tiempo real verifican actividades sospechosas y alertas a los profesionales de seguridad de bases de datos y profesionales de seguridad y administración de riesgos cuando ocurren. La supervisión de la base de datos protege de forma proactiva contra ataques a las bases de datos. A menudo, las grandes bases de datos críticas tienen cientos o incluso miles de conexiones por segundo, por lo que es humanamente imposible ver y detectar anomalías de seguridad. La supervisión y protección de la seguridad no solo alerta a los DBA sino que también bloquea las conexiones en tiempo real.

- Evaluación de la vulnerabilidad que comprueba la integridad y la configuración de las bases de datos: la simple instalación del software DBMS no crea un entorno seguro, incluso si el software proviene de un proveedor líder de DBMS. Los profesionales de seguridad de bases de datos deben reforzar el entorno definiendo las cuentas de usuario (en lugar de usar cuentas predeterminadas), garantizando la protección de archivos de la base de datos, habilitando la aplicación del control de acceso e instalando parches de seguridad de forma regular. Las evaluaciones de vulnerabilidad de la base de datos buscan agujeros de seguridad en las implementaciones de base de datos que resultan de no seguir los procedimientos de seguridad correctamente y resaltan los problemas que requieren atención [17]. Por ejemplo, una evaluación resaltará las contraseñas débiles, así como las tablas que tienen privilegios excesi-

vos.

POLÍTICAS DE SEGURIDAD, NORMAS, SEPARACIÓN DE FUNCIONES Y DISPONIBILIDAD

La estrategia de seguridad de la base de datos no se trata solo de auditoría y monitoreo; Es una estrategia integral que se enfoca en minimizar el riesgo, cumplir con los requisitos de cumplimiento normativo y defenderse contra ataques internos y externos. La seguridad de la base de datos necesita un enfoque más amplio que cubra los vacíos de seguridad, trabaje con políticas comunes y formalice los enfoques de seguridad. Cuando una organización decide proteger sus datos, implementa uno o más de los tres tipos de controles, tales como controles administrativos, controles físicos y controles lógicos [8]. Los controles administrativos (también llamados controles de procedimiento) consisten en políticas, procedimientos, normas y pautas escritas aprobadas. Los controles administrativos forman el marco para dirigir el negocio y administrar a las personas. Los controles físicos monitorean y controlan el entorno del lugar de trabajo y las instalaciones informáticas. También monitorean y controlan el acceso desde y hacia dichas instalaciones. Los controles administrativos y técnicos en última instancia dependen de los controles de seguridad física adecuados. una política administrativa que solo permita el acceso de los empleados autorizados al centro de datos no sirve para nada si no hay un control de acceso físico que impida que un empleado no autorizado acceda a la instalación. En un modelo tradicional, la organización es responsable de implementar estos controles físicos para asegurar la instalación de cómputo, al tiempo que separa la red y los entornos de trabajo, y establece salvaguardas ambientales [14]. Los controles lógicos (también llamados controles técnicos) utilizan software y datos para monitorear y controlar el acceso a la información y los sistemas informáticos. por ejemplo: las contraseñas, los firewalls basados en host y en la red, los sistemas de prevención de intrusiones, las listas de control de acceso y el cifrado de datos son controles lógicos [15]

La estrategia de seguridad de la base de datos debe:

- Integre con las políticas generales de seguridad de la información: las políticas de seguridad son fundamentales para cualquier estrategia de seguridad de base de datos exitosa. Los profesionales de la seguridad y la gestión de riesgos deben comprender las políticas generales de seguridad de la información y usarlas como base de todas las políticas de seguridad de la base de datos. Además, deben priorizar las soluciones de seguridad de base de datos que vienen con un amplio conjunto de políticas, especialmente las personalizables, ya que pueden ayudar a reducir el esfuerzo y el costo. También deben considerar implementar políticas diferentes para las bases de datos que contienen datos privados que para las que no lo hacen. Además, deben integrar la solución de seguridad de la base de datos con el sistema de tickets de la mesa de ayuda para apoyar las iniciativas de cumplimiento.

- Enfoque en los estándares de seguridad: los estándares son muy importantes al desarrollar una estrategia de seguridad de base de datos. Las profesiones de seguridad y riesgo deben considerar estándares de la industria como los Objetivos de control para la información y la tecnología relacionada (COBIT) y la Biblioteca de infraestructura de tecnología de la información (ITIL) para ayudar a definir la estrategia. Deben modificar estos estándares para satisfacer las necesidades de su organización, teniendo en cuenta el impacto del cumplimiento de diversos estándares como SOX, HIPAA, Gramm-Leach-Bliley Act (GLBA) y PCI, así como las aplicaciones e infraestructura existentes de su organización. Además, las organizaciones deben definir sus propios estándares y desplegarlos en toda la organización.

- Implementar la separación de roles: el cumplimiento normativo y los auditores destacan la importancia de la separación de roles, por lo que el personal diferente gestiona las bases de datos que aquellos que auditan o monitorean la actividad de seguridad. Forrester estima que los DBA dedican menos del 5 % de su tiempo a la seguridad de la base de datos, lo que crea una amenaza a la seguridad a menos que la organización implemente la separación de roles. Por lo general, los profesionales de seguridad monitorean la actividad de los DBA y otros usuarios privilegiados, revisan los registros de auditoría de la base de datos y crean inicios de sesión. Los profesio-

nales de la seguridad deben ocupar el puesto de analista de seguridad de la base de datos que pasa por alto la estrategia de seguridad de la base de datos, incluidas políticas, estándares y operaciones.

- Asegure la disponibilidad de la base de datos y los datos: los profesionales de la seguridad y la gestión de riesgos deben planificar las contingencias y articularse claramente en la recuperación de la estrategia de seguridad de la base de datos y en los procedimientos de disponibilidad de datos en caso de que una base de datos se caiga debido a un ataque. Los pasos deben incluir cómo recuperar las bases de datos, qué servidores y sistemas usar para garantizar la disponibilidad de las aplicaciones afectadas y cómo garantizar que los piratas informáticos no representen una amenaza para las bases de datos recuperadas.

Conclusion

Los datos de cualquier organización son una propiedad muy valiosa. La seguridad de los datos confidenciales es siempre un gran desafío para una organización en cualquier nivel. Las bases de datos son un objetivo favorito de los atacantes debido a sus datos. Hay muchas maneras en que una base de datos puede ser comprometida. Existen varios tipos de ataques y amenazas a partir de los cuales se debe proteger una base de datos. Para asegurar los datos que consideraciones debemos tener en cuenta, se mencionan en este documento y todas las técnicas que se utilizan recientemente para la seguridad de la base de datos.

References

[1] Defending From Within: How Insiders Threaten Data Privacy report by Informatics and Government Business Council. https://www.informatica.com/ content/dam/inform atica- com/global/amer/us/ collateral/executive- brief/defending-from-withingbc_executive-brief_2591.pdf.

[2] William Stallings Cryptography and Network Security: Principles and Practice Prentice Hall; 5 edition (14 Jan. 2010).

[3] Mohammed J. Novel Approaches to Big Data Management. ISSN 2348-1196 (print) International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online) Vol. 3, Issue 1, pp: (96- 105), Month: January - March 2015.

[4] Mohammed J. The State of Cryptography-A National Interest Perspective. ISO 9001:2008Certified International Journal of Engineering and Innovative Technology (IJEIT) Volume 4, Issue 8, February 2015.

[5] Imperva White Paper —Top Ten Database Threats 2014. http://www.imperva.com/ docs/WP_TopTen_Data base_Threats.pdf. International Journal of Computer Science Emerging Technologies (E-ISSN: 2044-6004) 368 Volume 2, Issue 3, June 2011, page(s); 368- 372.

[6] Tanya Bacca; Making Database Security an IT Security Priority A SANS Whitepaper – November 2009.

[7] 2012 future of cloud computing survey results – North Bridge http://northbridge.com/2012-cloud-computingsurvey.

[8] Iqra Basharat, Farooque Azam, Abdul Wahab Muzaffar,Database Security and Encryption: A Survey Study, International Journal of Computer Applications (0975 – 888) Volume 47– No.12, June 2012.

[9] Mr. Saurabh Kulkarni, Dr. Siddhaling Urolagin, —Review of Attacks on Databases and Database Security Techniques, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 11, November 2012.

[10]Networking and Security-Tech Soup for Libraries https://www.techsoupforlibraries.org/book/export /html/592

[11] Amichai Shulman; Top Ten Database Security Threats, How to Mitigate the Most Significant Database Vulnerabilities, 2006 White Paper.

[12] Mohammed J. (2015). The state of cryptography- a national interest perspective. International journal of engineering and innovative technology, 181- 192.

[13] Information Security http://en.wikipedia.org/wiki/information _security.

[14] Mohammed, J. (2014). Web and cloud security. International journal of engineering technology and advanced engineering.

[15] Kadhem, H.; Amagasa, T.; Kitagawa, H.; A Novel Framework for Database Security based on Mixed Cryptography; Internet and Web Applications and Services, 2009. ICIW '09. Fourth International Conference on; Publication Year: 2009, Page(s): 163 – 170.

[16] Iqra Basharat , Farooque Azam , Abdul Wahab Muzaffar —Database Security and Encryption: A Survey Study.