Lectura 10: Best Practices for Database Security

Diego Granados Retana 2022158363

Bases de datos II

3 de noviembre, 2023

Responda las siguientes preguntas:

¿Por qué se deben implementar controles que garanticen "compliance" en bases de datos?

Existen regulaciones sobre cómo se almacenan los datos, cuándo se acceden y quién tiene acceso. Algunas de estas regulaciones incluyen General Data Protection Regulation (GDPR), Sarbanes-Oxley Act (SOX), Health Insurance Portability and Accountability Act (HIPPA), Gramm-Leach-Bliley Act (GLBA) y Payment Card Industry and Data Security Standard (PCI DDS) (Liquibase, 2018). Si no se cumplen estas regulaciones, la compañía se expone muchos castigos y también desventajas. Primero, tendrán que pagar muchas multas y penalizaciones. Segundo, muchas de las regulaciones exigen usar herramientas de monitoreo, lo cual puede a su vez permitir ver problemas de rendimiento. Finalmente, la compañía se expone a que roben la información de sus usuarios. Esto no solo es un problema muy serio ya que puede llevar a que a los usuarios les roben dinero o sus cuentas, sino que también pierde la credibilidad de la compañía en los clientes y afecta negativamente los ingresos.

¿Qué papel juega los sistemas de Observabilidad en garantizar el "compliance" con estándares como HIPPA y PCI DSS? Comente como los controles específicos pueden ser monitoreados con un sistema como Prometheus

Los sistemas de observabilidad o monitores de actividad son fundamentales porque dan a conocer mucha información que se necesita para cumplir con las regulaciones. Analizan las consultas de la base de datos en tiempo real y pueden diferenciar entre operaciones normales y ataques (Lane, s.f.). Obtienen información de diferentes fuentes, dan análisis y alertan o incluso detienen alguna actividad inusual. Se puede rastrear cuáles índices y tablas se usan, verificar cuáles consultas son las que duran más, cuáles se están haciendo a una hora específica, cuáles consultas está haciendo un usuario específico, entre otros (LogicMonitor, 2022). Por ejemplo, si a la 1 de la mañana se aumenta un uso de CPU y de memoria con consultas a la tabla que almacena la información de los clientes, es muy posible que nos estén robando la información. Además, en los logs de inicios de sesión podemos ver si alguien se metió al sistema a una hora extraña. Por eso, los sistemas observabilidad ayudan a mantener control de la información sensible y su acceso, lo que evita la pérdida de ingresos y el robo de información privada.

¿Por qué "Separation of Duties" es importante para el manejo de bases de datos? ¿Está bien qué una persona tenga control completo sobre todos los sistemas?

Separation of duties es muy importante evita que se realicen acciones en interés de las personas a cargo de la base de datos, como por ejemplo no registrar un pago cuyo dinero será robado. Entre más personas tengan que revisar la integridad de la base de datos, ese tipo de inconsistencias es más difícil que aparezcan detectadas, a menos que todos los encargados sean corruptos. Por eso, muchas compañías contratan

servicios de auditoría que realizan los análisis e informes de los aspectos financieros, ya que estas tienen el interés de detectar la mayor cantidad de falencias de seguridad posible y no tienen la habilidad de esconder sus delitos. El separation of duties es importante en términos de seguridad, ya que agrega más capas de protección a la base de datos. Una sola persona no debe el acceso completo a la base de datos, ya que si su cuenta es comprometida, el intruso puede robar todos los datos, borrarlos, desencriptarlos y causar otra gran cantidad de problemas. Si hay más personas a cargo de la base de datos y una sola no tiene acceso completo, si hackean la cuenta de una, solo podrán acceder a lo que esta tiene permiso y no a toda la base de datos.

Tomando en cuenta lo estudiado en clases acerca de seguridad de bases de datos (desde seguridad física hasta aplicación) y este artículo, ¿Que controles consideran que fallaron dando como resultado el faltante de aproximadamente 3200 millones de colones en el Banco nacional? ¿Con lo estudiado en este curso que controles y sistemas implementarían para evitar este tipo de problemas?

En primer lugar, no se separaron las tareas correctamente, ya que es posible que los que estaban encargados de contabilidad del banco podían obviar algunas transacciones sin que alguien más se diera cuenta. De acuerdo con Mora, el dinero se les había dado en custodia a los sospechosos, por lo que tal vez se requirieron aún más personas u otra entidad a cargo del dinero (Mora, 2023). También, no se revisó el caso a tiempo. Se hizo una revisión en agosto, la cual señaló indicios del problema. El 3 de octubre se levantó la alerta, pero fue hasta el 24 de octubre que se confirmó la falta del dinero. Por otro lado, es posible que el dinero no falte y que sea un error contable. En este caso, está claramente fallando la consistencia del sistema contable. Al ser un sistema de banco, tal vez lo más seguro es que cada transacción sea aislada o por lo menos que haya un locking muy estricto de los recursos, con el fin de que no se pierdan transacciones. También, muy posiblemente no se revisaron los logs y si estos se habían guardado correctamente en la base de datos.

Referencias:

Lane, A. (n.d.). Database Monitoring Best Practices: Using DAM Tools. TechTarget. Retrieved November 2, 2023, from https://dokumen.tips/documents/best-practices-for-database-3-of-12-sponsored-by-best-practices-for-database-security.html?page=3

Liquibase. (2018, May 9). Database Compliance & Security: What You Need to Know. Liquibase.com. Retrieved November 2, 2023, from https://www.liquibase.com/blog/database-compliance-security

LogicMonitor. (2022, August 2). What is database monitoring, and why is it still important? https://www.logicmonitor.com/blog/what-is-database-monitoring-and-why-is-it-still-important

Mora, A. (2023, October 24). Banco Nacional confirma faltante de más de 3200 millones de colones de su bóveda. Delfino.cr. Retrieved November 2, 2023, from https://delfino.cr/2023/10/banco-nacional-confirma-faltante-de-mas-de-3200-millones-de-colones-de-su-boveda