Nadia Arellano G.
Ingeniera en Informática

Actividad – Sesión 2: Implementación y Evaluación de Seguridad en la Nube

Caso: Una empresa tecnológica ha migrado recientemente sus operaciones de TI a la nube para optimizar costos y mejorar la escalabilidad. Sin embargo, tras la migración, la empresa se enfrenta a varios problemas de seguridad debido a configuraciones incorrectas y falta de control sobre el acceso a los datos. El equipo de TI ha identificado tres incidentes de seguridad que afectan la confidencialidad, integridad y disponibilidad de sus datos en la nube. Como solución, han decidido aplicar los principios de CIA y revisar sus configuraciones de seguridad.

1. La empresa ha descubierto que algunos empleados no autorizados han accedido a datos confidenciales. ¿Cuál es la mejor medida para mejorar la confidencialidad y prevenir accesos no autorizados?
   (R). La mejor medida para mejorar la confidencialidad es en primer lugar implementar un control de acceso detallado basado en roles (RBAC) para permitir que solo los empleados autorizados según su función puedan acceder a ciertos datos. Además, es importante aplicar cifrado de datos tanto en tránsito como en reposo, porque incluso si ocurre una intrusión, la información no pueda ser leída ni utilizada por personas no autorizadas.

2. Durante una auditoría, el equipo de TI nota modificaciones no autorizadas en dato críticos debido a un ataque. ¿Qué medida de integridad podría haber prevenido esta situación?
   (R). Pienso que un sistema de verificación de integridad mediante hashing hubiese permitido detectar cualquier modificación no autorizada en datos críticos. También, se debió configurar alertas en tiempo real ante cambios sospechosos, esto hubiese permitido al equipo TI actuar rápidamente.

3. La empresa experimenta interrupciones del servicio debido a un ataque de denegación de servicio (DDoS). ¿Qué medida debería implementar para mejorar la disponibilidad y protegerse de futuros ataques?
   (R). Se debería implementar servidores redundantes con tolerancia a fallos y también un sistema de balanceo de carga, para que distribuya eficientemente el tráfico entre los servidores y evite la saturación de uno solo. Además, se debería complementar estas medidas con estrategias específicas de mitigación DDoS como herramientas de detección temprana de tráfico malicioso.