Nadia Arellano G.
Ingeniera en Informática

Actividad – Sesión 4: Análisis de Caso de Fallos de Seguridad en la Nube

Caso
Exposición de datos confidenciales debido a configuraciones incorrectas de permisos.

1. **Identificación de Causas y Consecuencias:** Describe las causas del fallo en el caso. ¿Cuáles fueron las consecuencias para la empresa y sus usuarios?
   (R). Las causas del fallo fueron por una configuración incorrecta de permisos de acceso. Los datos confidenciales quedaron accesibles debido a que no se realizaron ni revisaron correctamente las configuraciones de los permisos. Además, la ausencia de cifrado en tránsito como en reposo permitió que los datos quedaran expuestos en texto claro. Las consecuencias para la empresa fueron pérdida de confianza por parte de sus clientes, posibles sanciones legales por incumplimiento normativo (como GDPR si aplica) y daño reputacional. Para los usuarios, hubo riesgo de robo de identidad, fraude y uso indebido de su información personal.

2. **Análisis de Medidas de Prevención:** ¿Qué medidas de prevención habrían evitado este fallo? Justifica tu respuesta.
   (R). Para evitar este fallo, se debieron aplicar medidas de prevención tales como: revisión y configuración adecuada de permisos de acceso usando controles basados en roles (RBAC), configurar cifrado de datos en reposo y en tránsito y realizar auditorías regulares de configuraciones de seguridad. Estas medidas se justifican porque están alineadas con los principios de confidencialidad y forman parte de las buenas prácticas recomendadas por normas como ISO 27001.

3. **Propuesta de Solución y Plan de Acción:** Proporciona un plan de acción breve que incluya las medidas que tomarías para que la empresa se recupere del fallo y prevenga futuros incidentes similares.
   (R). Plan de acción para recuperación y prevención:
   - Realizar una contención inmediata revocando el acceso público al recurso afectado y notificar a los usuarios afectados si corresponde a la legislación vigente.
   - Revisar y corregir todas las configuraciones de acceso en la nube, aplicando el principio de mínimo privilegio y controles basados en roles.
   - Asegurar que todos los datos sensibles estén cifrados, tanto en tránsito como en reposo.
   - Realizar capacitaciones al equipo de TI en configuración segura de servicios en la nube y concientizarlos sobre seguridad.
   - Establecer auditorías periódicas y herramientas de monitoreo que alerten sobre cambios no autorizados en la configuración.

Nadia Arellano G.
Ingeniera en Informática

4. **Reflexión y Lecciones Aprendidas:** Reflexiona sobre la lección principal que se puede aprender de este caso. ¿Por qué es importante implementar las medidas de seguridad en la nube?

   (R). La lección principal de este caso es que la seguridad en la nube no puede depender de configuraciones predeterminadas. La falta de revisión de permisos y la ausencia de medidas como el cifrado pueden provocar consecuencias legales y reputacionales graves. Es importante implementar medidas de seguridad en la nube para proteger la confidencialidad de los datos, evitar vulnerabilidades y fortalecer la confianza de los clientes.