Instituto Tecnológico y de Estudios Superiores de Monterrey
Campus Monterrey

Materia

Inteligencia artificial avanzada para la ciencia de datos II

Tarea

Actividad 3 - Infrastructure Security for Cloud

Estudiantes

Cleber Gerardo Pérez Galicia - A01236390

Juan Pablo Bernal Lafarga - A01742342

Jacobo Hirsch Rodríguez - A00829679

Eryk Elizondo González - A01284899

Profesor

Félix Ricardo Botello Urrutia

¿Cuáles son los riesgos de seguridad al tener una infraestructura cloud?

1. **Exposición o filtración de datos:** Los datos pueden ser expuestos o filtrados debido a configuraciones incorrectas o vulnerabilidades en la infraestructura.
2. **Acceso no autorizado:** Un usuario no autorizado puede acceder a datos internos, lo que puede comprometer la seguridad de la información sensible.
3. **Exceso de acceso por usuarios internos:** Un usuario autorizado puede tener demasiado acceso a los datos internos, lo que puede llevar a abusos o errores humanos.
4. **Ataques maliciosos:** Ataques como DDoS (Denegación de Servicio Distribuida) o infecciones de malware pueden dañar o destruir la infraestructura en la nube.
5. **APIs inseguras:** Las interfaces de programación de aplicaciones (APIs) inseguras pueden ser un punto de entrada para atacantes.

¿De qué manera un atacante puede acceder a los recursos y/o datos en una infraestructura cloud?

1. **Secuestro de cuentas:** Los atacantes pueden obtener acceso no autorizado a cuentas en la nube mediante técnicas como el phishing o el uso de credenciales robadas.
2. **Inyección de malware:** Los atacantes pueden explotar vulnerabilidades en la infraestructura de la nube o en las aplicaciones que se ejecutan en ella para inyectar malware.
3. **Configuraciones de seguridad incorrectas:** Las configuraciones incorrectas de seguridad, como permisos excesivos o configuraciones predeterminadas inseguras, pueden ser explotadas por atacantes para acceder a datos sensibles.
4. **Ataques de fuerza bruta:** Los atacantes pueden utilizar técnicas automatizadas para adivinar contraseñas y obtener acceso a cuentas protegidas por contraseñas débiles.
5. **APIs inseguras:** Las interfaces de programación de aplicaciones (APIs) inseguras pueden ser un punto de entrada para los atacantes, permitiéndoles acceder a datos y servicios en la nube.

¿Cómo se pueden mitigar y reforzar estas vulnerabilidades?

1. **Gestión de Identidades y Accesos Seguros:** Implementar prácticas seguras de gestión de identidades y accesos, como el uso de autenticación multifactor (MFA) y la gestión de privilegios mínimos.
2. **Gestión Segura de Claves:** Utilizar prácticas seguras para la gestión de claves, asegurando que las claves de cifrado estén protegidas y gestionadas adecuadamente.
3. **Segmentación de Red y Cifrado:** Implementar la segmentación de red y el cifrado de datos tanto en tránsito como en reposo para proteger la información sensible.
4. **Monitoreo y Alerta Continuos:** Establecer sistemas de monitoreo y alerta para detectar y responder rápidamente a cualquier actividad sospechosa o no autorizada.
5. **Actualización y Parcheo Regular:** Mantener todos los sistemas y aplicaciones actualizados con los últimos parches de seguridad para cerrar cualquier vulnerabilidad que pueda ser explotada.
6. **Capacitación de Empleados:** Capacitar a los empleados en políticas y procedimientos de seguridad adecuados para reducir el riesgo de errores humanos.

- Referencias.

¿Cómo funciona la seguridad en la nube? | Seguridad en la informática en la nube. (s. f.). CLOUDFLARE. https://www.cloudflare.com/es-es/learning/cloud/what-is-cloud-security/

Aqua Security. (2024, 23 julio). *Top 10 Cloud Attacks and What You Can Do About Them - Aqua*. Aqua. https://www.aquasec.com/cloud-native-academy/cloud-attacks/cloud-attacks/

NSA's top ten cloud security mitigation strategies. (s. f.). En *National Security Agency*. https://media.defense.gov/2024/Mar/07/2003407860/-1/-1/0/CSI-CloudTop10-Mitigation-Strategies.PDF