Tecnológico de Monterrey

Inteligencia artificial avanzada para la ciencia de datos II (Gpo 101)

Profesor: Félix Ricardo Botello Urrutia

Actividad 3

Infrastructure Security for Cloud

Sofía Cantú Talamantes	A01571120
Ozner Leyva	A01742377
Nallely Serna	A00833111
Fernanda Perez	A01742102

Septiembre 2024

Seguridad en la Infraestructura Cloud

1. Riesgos, Vulnerabilidades y Estrategias de Mitigación

La adopción de infraestructuras cloud presenta desafíos de seguridad únicos que requieren un enfoque proactivo. Este análisis aborda los principales riesgos, métodos de ataque y estrategias de mitigación en entornos cloud.

I. Riesgos de Seguridad en la Infraestructura Cloud

1. Configuraciones Erróneas

   • Problema: Configuración inadecuada de recursos cloud.
   • Consecuencia: Exposición de datos y recursos a accesos no autorizados.
   • Factor agravante: Complejidad creciente en entornos multi-cloud.

2. Gestión Inadecuada de Accesos

   • Riesgo: Fallas en la gestión de identidades y accesos (IAM).
   • Problema específico: Incumplimiento del principio de mínimo privilegio.
   • Resultado: Exposición de sistemas sensibles a ataques.

3. Interfaces y APIs Inseguras

   • Vulnerabilidad: APIs mal configuradas o con protección insuficiente.
   • Consecuencia: Punto de entrada para manipulación de datos y recursos.

4. Amenazas Persistentes Avanzadas (APT)

   • Característica: Ataques sostenidos y sigilosos.
   • Objetivo: Acceso prolongado y movimiento lateral en la infraestructura.

II. Métodos de Ataque a la Infraestructura Cloud

1. Explotación de Configuraciones Incorrectas

   • Táctica: Búsqueda de permisos excesivos o almacenamiento sin cifrar.
   • Objetivo: Acceso no autorizado a datos.

2. Phishing y Compromiso de Credenciales

   • Método: Ingeniería social y ataques de phishing.
   • Meta: Obtención de credenciales para acceso ilegítimo.

3. Explotación de Vulnerabilidades de Día Cero

• Enfoque: Aprovechamiento de fallas de software no parcheadas.
• Riesgo: Exposición a ataques antes de la disponibilidad de parches.

III. Estrategias de Mitigación y Refuerzo de Seguridad

1. Modelo de Responsabilidad Compartida

   • Concepto: Delimitación clara de responsabilidades entre proveedor y cliente.
   • Proveedor: Seguridad de la infraestructura subyacente.
   • Cliente: Configuración de servicios y protección de aplicaciones y datos.

2. Optimización de Prácticas IAM

   • Enfoque: Implementación del principio de mínimo privilegio.
   • Acción: Auditorías frecuentes de accesos y permisos.

3. Cifrado Integral de Datos

   • Alcance: Cifrado en reposo y en tránsito.
   • Punto crítico: Gestión adecuada de claves de cifrado.

4. Segmentación de Redes y Monitoreo Continuo

   • Táctica: Limitación del movimiento lateral de amenazas.
   • Herramienta: Monitoreo constante de registros para detectar actividades sospechosas.

2. Concusión

La seguridad efectiva en entornos cloud requiere una estrategia integral que abarque configuraciones robustas, control de acceso estricto, cifrado avanzado y vigilancia constante. La colaboración entre proveedores y clientes, junto con la implementación de mejores prácticas, es esencial para mantener un entorno cloud seguro y resiliente frente a las amenazas en constante evolución.

Referencias

Doyle, K. (2024, April 22). *NSA debuts top 10 cloud security mitigation strategies*. Tripwire. https://www.tripwire.com/state-of-security/nsa-debuts-cloud-security-mitigation-strategies

Puzas, D. (2023, January 26). *9 cloud security risks, threats & challenges | crowdstrike*. CrowdStrike. https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-security-risks-threats-challenges/

Ramachandran, R. (2024, April 16). *Evolving threats to cloud computing infrastructure and suggested countermeasures*. ISACA. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/evolving-threats-to-cloud-computing-infrastructure-and-suggested-countermeasures

Top Threats. (2024, May 8). *Top threats to cloud computing 2024 | CSA*. Cloudsecurityalliance.org. https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024