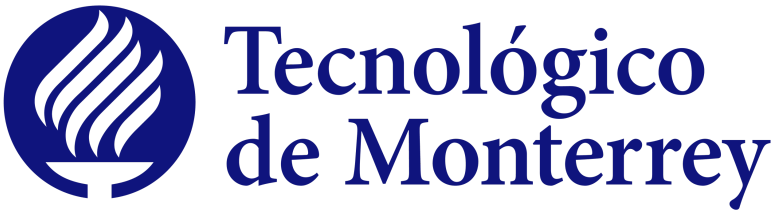
Instituto Tecnológico y de Estudios Superiores de Monterrey
Campus Monterrey



Inteligencia artificial avanzada para la ciencia de datos II
TC3007C, Grupo 101

Nombre del profesor: Félix Ricardo Botello Urrutia

Cloud computing | Actividad 3 - Infrastructure Security for Cloud

Equipo 6 | Integrantes:

Oskar Arturo Gamboa Reyes	| A01173648
Ricardo Salinas	| A01284657
Oscar Gutiérrez Araiza	| A00832992
Erika Martínez	| A01028621
Marcelo de Luna	| A00832239

Octubre 2024

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

- **Visibilidad limitada:** Cuando se mueven cargas de trabajo, datos o activos a la nube, las empresas pierden un cierto nivel de visibilidad de las operaciones en red. Esto se debe, fundamentalmente, a que la responsabilidad de la administración se traslada al proveedor.
- **Malware:** Existen estudios que muestran que casi el 90 % de las empresas tienen más probabilidades de experimentar filtraciones de datos a medida que aumenta el uso de la nube.
- **Pérdida de datos:** Si el proveedor experimenta un ataque, se pueden perder datos en el proceso.
- **Privacidad:** Por defecto, los sistemas en la nube, suelen permitir el acceso a usuarios a gran escala, por lo que es conveniente implementar medidas de seguridad para limitar el acceso y la manipulación de según qué datos o información almacenada en la nube.
- **Evaluación inadecuada de los riesgos:** Es importante llevar a cabo una evaluación exhaustiva que garantice que la empresa tiene una comprensión completa del alcance del trabajo necesario para pasar a la nube sin problemas de seguridad.
- **Pérdida del gobierno.** Con el uso de infraestructuras en la nube, el cliente cede el control al proveedor cloud en cuestiones que afectan a la seguridad de la información.

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

Los ataques de este tipo pueden ser de muchas diferentes maneras, dependiendo de lo que se quiera lograr y el tipo de compañía que sea, estos son algunos ejemplos:

- **Aumento de privilegios:** una común técnica de seguridad en las empresas es la limitación de privilegios y accesos a los usuarios, y por medio de un aumento de privilegios, los atacantes pueden llegar a acceder a información sensible de la empresa con facilidad.
- **Robo y fuga de datos:** en el momento que un atacante logra tener acceso a las plataformas de una empresa, los datos en general se ven en peligro, ya que estos pueden ser fácilmente recolectados y eliminados del software.
- **Man-In-The-Middle:** este concepto se define como un atacante teniendo acceso a la comunicación entre la empresa y un cliente, esta infiltración le puede dar acceso a tanto los datos de la empresa como los del cliente, lo cual hace muy importante la implementación de robustos filtros de seguridad.
- **Robo de Tokens: l**as empresas que cuentan con identificación por medio de tokens pueden llegar a sufrir el robo de estas, lo cual le da un fácil acceso a los atacantes y dejan vulnerables los sistemas.

- **Poca Supervisión:** Se tiene que mantener un monitoreo constante de las sesiones de los usuarios, ya que se pueden identificar usuarios que dejan sus sesiones activas por largos periodos de tiempo, lo cual puede indicar un canal fácil de acceder para los atacantes, también se puede detectar actividad maliciosa y retirarla lo antes posible.

3. ¿Cómo se pueden mitigar y reforzar estas vulnerabilidades?

- **Aumento de privilegios:**
  - Implementar el principio de privilegios mínimos (PoLP), para que los usuarios solo tengan acceso a los recursos mínimos necesarios para realizar actividades y tareas.
  - Utilizar Control de Acceso Basado en Roles (RBAC) para limitar permisos en función de los roles específicos.
  - Activar autenticación multifactor (MFA) para todas las cuentas de alto privilegio, esto ayuda a hacer más difícil el acceso.

- **Robo y fuga de datos:**
  - Cifrado de datos, asegurando que los datos sensibles no sean posibles leerlos aunque estén en la posesión del atacante.
  - Implementar un sistema de detección y prevención de fugas de datos (DLP) para monitorear y bloquear la exfiltración no autorizada.
  - Agregar alertas de seguridad para actividades sospechosas o inusuales, como transferencias masivas de datos o en horas inesperadas.

- **Man-In-The-Middle (MITM):**
  - Usar protocolos de comunicación seguros como HTTPS (TLS) y cifrado de extremo a extremo.
  - Implementar certificados SSL y configurar políticas estrictas de seguridad (HSTS).
  - Habilitar la validación de certificados para garantizar la autenticidad de las comunicaciones entre clientes y servidores.
  - Utilizar redes privadas virtuales (VPNs) o redes privadas en la nube (VPCs) para añadir una capa adicional de seguridad en las comunicaciones internas y evitar que queden expuestas en el caso de haber una brecha.

- **Robo de Tokens:**

    - Implementar rotación frecuente de tokens y establecer una caducidad corta para los tokens de acceso.
    - Evitar almacenamiento de tokens en texto plano en el navegador o dispositivos de los usuarios.
    - Habilitar autenticación multifactor (MFA) para la emisión de tokens, reduciendo el riesgo si un token es comprometido.

- **Poca Supervisión**:
    - Implementar monitoreo continuo y análisis de registros de actividad, utilizando herramientas de SIEM (Security Information and Event Management) para identificar comportamientos inusuales.
    - Habilitar alertas automáticas cuando se detecten sesiones activas por un tiempo inusualmente largo o actividad fuera de horario.
    - Forzar cierre automático de sesiones inactivas para evitar que los atacantes se aprovechen de sesiones abandonadas.

Referencias

OWASP Foundation. (2022). *OWASP Cloud-Native Application Security Top 10*. OWASP. https://owasp.org/www-project-cloud-native-application-security-top-10/

Bhargav, A. (2024). A guide to NIST SP 800-53: 20 steps to compliance. AppSecEngineer. https://www.appsecengineer.com/blog/a-guide-to-nist-sp-800-53-20-steps-to-compliance

Goulding, T. (2023). *What you need to know about NIST 800-53, least privilege, and PAM*. Delinea. https://delinea.com/blog/nist-800-53-security-privacy-privileged-access

Joint Task Force. (2022). *Assessing security and privacy controls in information systems and organizations* (NIST SP 800-53A Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53Ar5

Canle Fernández, E. (2022). *Riesgos de seguridad en cloud computing*. Tokio School. https://www.tokioschool.com/noticias/riesgos-seguridad-cloud-computing/