Instituto Tecnológico y de Estudios Superiores de Monterrey

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

Equipo 4

Cloud computing | Actividad 3 - Infrastructure Security for Cloud

Integrantes:

Eliezer Cavazos Rochin A00835194

Facundo Colasurdo Caldironi A01198015

Saul Francisco Vázquez del Río A01198261

José Carlos Sänchez Gómez A01174050

Campus Monterrey **Fecha: 9/10/20**

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

Al tener una infraestructura cloud, se tiene que tomar en cuenta que esta tiene riesgos de seguridad como cualquier otra, en el caso de este tipo de infraestructura, puede ser por elementos tan sencillos como una brecha en la base de datos, una mala práctica de programación o ataques de personas con malas intenciones.

Todo este tipo de ataques no solo pone en riesgo la seguridad de los datos, sino que permite que actores con malas intenciones puedan explotar espacios de seguridad, logrando así el secuestro de cuentas de importancia, con las cuales puedan provocar aún más daño a la infraestructura, generando un peligro para el sistema entero. También existe el riesgo de pérdida de datos por fallos en el hardware, eliminación accidental o falta de copias de seguridad adecuadas en un aspecto físico, lo cual puede repercutir de manera negativa en la nube.

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

Un atacante puede explotar errores en la configuración de la infraestructura tales como robar credenciales mediante phishing, aprovecharse de las vulnerabilidades en APIs y servicios web. Las técnicas de phishing permiten a los atacantes robar credenciales y acceder a los servicios cloud como si fueran usuarios legítimos. Las APIs mal protegidas también son un objetivo frecuente, ya que los atacantes pueden aprovechar vulnerabilidades en estas interfaces para realizar operaciones no autorizadas o acceder a datos.

Una vez dentro, los atacantes pueden intentar escalar privilegios para acceder a recursos más críticos, también pueden instalar malware en la infraestructura o comprometer al proveedor de servicios en la nube. Las brechas en la virtualización, si no se gestionan adecuadamente, pueden permitir que los atacantes atraviesen las barreras entre inquilinos y accedan a datos de otros usuarios.

¿Cómo se pueden mitigar y reforzar estas vulnerabilidades?

Para poder prevenir y reforzar estas vulnerabilidades que se encuentran en la infraestructura, se pueden realizar diversas practicar para lograrlo, tales como la implementación de autenticación multifactorial o políticas de acceso, en donde se límite las credenciales de los usuarios, para evitar que puedan acceder a toda la información relevante, también, es importante asegurar que las diversas APIs tengan un acceso controlado y monitoreado, para poder proteger de intentos de acceso no autorizados y el hecho de seguir con las normativas tales como GDPR o ISO27001, los cuales se aseguran de un manejo adecuado de datos sensibles.

Otras acciones que se pueden realizar tienen que ver con costumbres de las personas, el mantener el software actualizado es crucial para evitar vulnerabilidades conocidas y el capacitar al personal para que puedan detectar este tipo de ataques.