Pyxis Cloud Security Approach

En la actualidad importante y cada vez más necesario seguir e implementar las buenas prácticas de Seguridad en Tecnología Informática. En particular para ambientes de Cloud, los proveedores cumplen con varios estándares de seguridad que aplican a sus centros de datos, aunque dejan la responsabilidad a sus clientes en mayor o menor medida sobre las configuraciones finales de seguridad.

Por otra parte es frecuente en la práctica que el abordaje de Cloud de muchas empresas sigue los lineamientos del negocio, sin tener en cuenta la Seguridad desde etapas tempranas de definición de la Arquitectura e Infraestructura.

Como consecuencia mas inmediata, un porcentaje muy alto de los incidentes de seguridad suceden debido a configuraciones de servicios precarias o con sus valores por defecto.

Cloud Security Approach propone una mirada obligatoria sobre la infraestructura y servicios desplegados en Cloud, así como también una visión con las premisas de Security by Default y Zero Trust para nuevas soluciones. A través del CSA se identifican y ponderan las oportunidades de mejora relacionadas con la infraestructura del cliente, recomendando un diseño que cumpla con buenas prácticas y estándares de seguridad actualizados.

A continuación se describen las fases que componen el CSA:

1.- Relevamiento de Situación Actual

Punto de partida para conocer la realidad del cliente, entender las necesidades y desafíos que actualmente tiene la infraestructura del cliente, así como los nuevos requerimientos y opciones de mejora que espera obtener. De esta manera se trabaja en conjunto en definiciones sobre las nuevas soluciones de Cloud que mejor se adapten al negocio. .

2.- Diseño de Infraestructura Segura

El desarrollo de infraestructuras de Cloud trae aparejado un conjunto de prácticas y formas de trabajo que no son totalmente comparables o equivalentes a los escenarios on-premise. Por lo cual es necesario entender como la realidad actual del cliente se adapta a un ambiente de Cloud. Se considerarán nuevas formas de acceso, la gestión de identidades y demás aspectos que hacen al diseño de la seguridad de la información en Cloud.

Esta es la principal fase del CSA, donde se define el diseño que mejor se ajusta a las necesidades del cliente teniendo en cuenta y priorizando la Seguridad según las mejores prácticas y experiencias en el área.

3.- Recomendaciones de Mejora

Luego de lograr un diseño acorde al cliente, se presentarán las recomendaciones de mejora haciendo hincapié en los beneficios que se obtendrán con la nueva infraestructura, las consideraciones que deberán tener y demás cambios que puedan implicar la nueva configuración.

4.- Acompañamiento en la Estrategia de Implementación

Confiamos en que esta fase generará el valor agregado mas importante para el cliente, donde se seguirán los lineamientos sugeridos en las fases anteriores, se logrará una nueva solución estable, confiable con las garantías de seguridad que se hayan acordado.

Acompañamos al cliente en estos primeros pasos, asesorándolo y despejando dudas que surjan ya en etapa de implementación.

Cloud Security
Approach

Más Información:
www.pyxis.tech/cloud-security