AdviceGroup LATAM

Claves Fundamentales
Zero Trust Security

1 Principio de "Nunca confiar, siempre verificar"

Este principio es la base de la herramienta, pues considera que ningún usuario o dispositivo es confiable, esté o no dentro de la red corporativa, por lo que cada intento de conexión debe ser verificado antes de ingresar.

Por medio de la implementación de la **autenticación multifactor (MFA)**, se evalúa de forma continua el contexto y políticas de acceso para cada solicitud.

2 Autenticación y autorización estricta

Zero Trust Security establece la **identidad de todos los usuarios y dispositivos** que pidan ingresar a los recursos de la organización. Para ello implementa sistemas de Gestión de Identidades y Accesos (IAM) que soporten la autenticación multifactor, Single Sing-On (SSO) y la autenticación basada en la ubicación, dispositivo y comportamiento

3 Principio de menor privilegio

Consiste en otorgar a los usuarios y dispositivos **solo los permisos necesarios para realizar funciones específicas.** Para ello es necesario definir roles y permisos detallados, utilizar controles de acceso basados en roles (RBAC) y revisar periódicamente los privilegios otorgados.

4 Segmentación de la red y microsegmentación

Dividir la red en segmentos más pequeños y controlar el flujo de tráfico entre ellos para limitar el movimiento lateral en caso de una brecha. Con la utilización de **firewalls de próxima generación,** tecnología de microsegmentación y políticas de control de acceso granular o control muy detallado para **aislar diferentes partes de la infraestructura.**

5 Monitoreo y registro continuo

A través de Zero Trust Security se logra **supervisar constantemente todas las actividades y accesos dentro de la red** para detectar comportamientos anómalos y posibles amenazas. Esto se logra con la implementación de soluciones de Seguridad de Información y Gestión de Eventos (SIEM), herramientas de detección y respuesta de endpoints (EDR) y análisis de comportamiento de usuarios (UBA).

6 Inspección y cifrado de tráfico

Inspeccionar todo el tráfico de información en la red y **cifrar los datos en tránsito para proteger la información contra intercepciones y manipulaciones** es vital para la seguridad. Zero Trust Security implementa protocolos seguros como TLS/SSL, inspección profunda de paquetes (DPI) y asegura que todos los datos sensibles estén cifrados.

7 Automatización y orquestación de seguridad

Automatizar las respuestas a incidentes y la implementación de políticas de seguridad para mejorar la eficiencia y reducir el tiempo de respuesta. Esto se logra al utilizar plataformas de orquestación, automatización y respuesta de seguridad (SOAR) que integren diferentes herramientas de seguridad y permitan acciones que se activan automáticamente, basadas en eventos predefinidos.

8 Visibilidad y control centralizado

Tener una **visión completa y unificada de todos los dispositivos, usuarios y flujos de tráfico** dentro de la infraestructura de TI. Para ello se requiere implementar dashboards centralizados que agreguen datos de diversas fuentes de seguridad, que permiten una gestión y análisis más efectivos.

9 Adaptabilidad y escalabilidad

La arquitectura de **Zero Trust Security debe ser adaptable a cambios en el entorno de TI y escalable** para crecer con la organización. Con ese fin, es necesario implementar soluciones basadas en la nube que faciliten la escalabilidad y diseñar políticas de seguridad que se ajusten dinámicamente según las necesidades de cada negocio.

Implementar **Zero Trust Security es fundamental en toda organización** porque reduce significativamente la superficie de ataque y limita el movimiento lateral de amenazas. Al verificar de forma continua la identidad de usuarios y dispositivos, se asegura el acceso a los recursos estrictamente necesarios, reduciendo el riesgo de ataques internos y externos.

¿Necesitas asesoría personalizada para tu organización? Haz una cita con nuestros asesores para implementar el enfoque Zero Trust Security en tu estrategia de TI.