Breve historia de la confianza cero: de la pizarra a la Casa Blanca

Las organizaciones están recurriendo a la confianza cero para satisfacer las exigencias de las empresas moderna. Para comprender lo revolucionaria que es la arquitectura de confianza cero, las organizaciones deben examinar la evolución de la confianza cero y cómo transforma fundamentalmente el pensamiento de hace décadas sobre las redes y la seguridad empresarial.

Creación de los muros del perímetro de red

1987

Los ingenieros de Digital Equipment Corporation (DEC) publican el primer artículo sobre la tecnología de cortafuegos, iniciando así décadas de pensamiento de seguridad de red de castillo y foso.

Separación básica mediante segmentación de red

1990

Los intentos iniciales surgen para segmentar la red utilizando VLAN o subredes, un enfoque extremadamente limitado sin autenticación, con restricciones mínimas y pocas capacidades de seguridad interna. Cualquier restricción implementada se omite fácilmente.

Se añade el control de acceso a la red

2001

La IEEE Standards Association publica el protocolo 802.1X para el control de acceso a la red (NAC). Impulsado por la adopción de WLAN, proporciona conexiones de red autenticadas y da acceso a nivel de red (LAN/VLAN), pero es complejo y difícil de implementar ampliamente.

La semilla de la confianza cero está ya plantada

2004

Se crea el Foro Jericho. Reconoce que los usuarios y las aplicaciones están abandonando la red corporativa e introduce los primeros conceptos de confianza cero a través del principio de desperimetrización.

Nace la confianza cero

2010

El analista John Kindervag presenta el modelo de confianza cero en un documento para Forrester Research. Traslada la autenticación y la seguridad en línea, y sugiere la segmentación de las sesiones. Sigue centrándose en el acceso a la red y traslada el perímetro al interior de la misma.

Google define su propio modelo

2014

La iniciativa BeyondCorp de Google reimagina la arquitectura de seguridad tras el ataque de la Operación Aurora, lo que lleva al despliegue de confianza cero en toda la empresa.

Zscaler traslada la confianza cero a la nube

2016

Zscaler presenta la primera solución de confianza cero entregada en la nube, que permite a las organizaciones eliminar la superficie de ataque externa y minimizar el potencial de movimiento lateral, lo que simplifica fundamentalmente la implementación de la confianza cero.

Gartner entra en acción

2019

Gartner introduce el concepto de Secure Access Service Edge (SASE) o perímetro de servicio de acceso seguro) y revitaliza el concepto de confianza cero, redefiniéndolo como Zero Trust Network Access (ZTNA).

El NIST define un marco estándar de confianza cero

2020

El NIST publica el documento SP 800-207 como marco unificado para establecer una arquitectura de confianza cero (ZTA) e introduce el primer cambio real de la definición de confianza cero en el contexto de la red.

Gartner define un camino seguro

2021

Gartner especifica los componentes de seguridad de SASE como una nueva categoría de mercado, conocida como Security Service Edge (SSE) o perímetro de servicio de seguridad.

El gobierno de EE. UU. exige la confianza cero

2022

La Oficina de Gestión y Presupuesto exige la adopción de principios de confianza cero para todas las agencias para 2024.

Profundice en la historia de la confianza cero y hacia dónde se dirige.

Leer la documentación técnica

Experience your world, secured.

Zscaler, Inc.
120 Holger Way
San José, CA 95134
+1 408.533.0288
www.zscaler.es