Publicado en CDMX el 17/08/2023

# [Hillstone Networks explica todo lo que se tiene que saber acerca de Zero Trust](http://www.notasdeprensa.es)

## Hace dos años se produjo uno de los ataques de ransomware más impactantes en la economía digital: la invasión de los sistemas de la empresa norteamericana de petróleo y gas Colonial Pipeline. Después de investigar, se descubrió que la brecha fue una VPN que aún estaba operativa pero que no se había utilizado durante algún tiempo. Lo más probable es que las credenciales de este usuario de VPN se hayan filtrado en la Dark Web y, tras varios intentos, el grupo de cibercriminales DarkSide logró su objetivo

 Hillstone Networks considera que cuando se habla del concepto Zero Trust Network Access es fundamental comprender que la VPN sigue viva y activa en este modelo. La diferencia es que el modelo ZTNA se basa en el concepto de privilegio mínimo: "nunca confíes, siempre verifica". El objetivo es proporcionar acceso mínimo a los recursos y usuarios. No importa si el usuario está dentro o fuera del perímetro. Con cada acceso, varias funciones de autenticación y verificación de contexto desafían al usuario a demostrar que tiene las credenciales necesarias. ZTNA comprueba la fiabilidad del punto desde el que los usuarios y dispositivos acceden a los recursos, estén donde estén. En cierto sentido, el acceso se ha convertido en el nuevo perímetro de la red. El modelo ZTNA no confía en ningún usuario o dispositivo por defecto. Este enfoque aumenta la seguridad de la organización al detectar múltiples amenazas y bloquear accesos no autorizados. • Phishing y exploits. Según un informe de Verizon, el factor humano y las tácticas de ingeniería social como el phishing representan el 82% de los puntos de entrada. Al autenticar, validar y probar constantemente a los usuarios y dispositivos, ZTNA puede reducir la probabilidad de un ataque exitoso. • Ransomware y botnets. Estos ataques operan ganando un punto de apoyo en la red y luego moviéndose lateralmente para obtener acceso a datos valiosos. ZTNA puede proporcionar microsegmentación para restringir el acceso y bloquear el movimiento lateral no autorizado, lo que limita los efectos del ataque. • Hacks de Man-in-the-Middle (MitM). La fuerza laboral remota aumenta en gran medida el riesgo de ataques MitM, donde el ciberdelincuente puede robar información confidencial, secuestrar recursos y más. A través de la verificación continua del usuario, el dispositivo y el contexto, el modelo de confianza cero puede evitar el inicio de un ataque MitM. • Amenazas internas. Los empleados y socios comerciales con acceso a la red son responsables hasta del 20% de las filtraciones de datos. El acceso con privilegios mínimos a través de ZTNA, junto con la verificación del estado del dispositivo, el conocimiento del contexto y la microsegmentación, pueden ayudar a reducir la probabilidad de daño a través de estos canales. • Ataque DoS/DDoS. Los ataques de denegación de servicio pueden inmovilizar una organización. Por lo general, estos ataques comienzan con el escaneo de puertos u otro descubrimiento para identificar vulnerabilidades. ZTNA protege eficazmente el entorno digital de usuarios no autorizados, lo que también evita que los atacantes descubran infracciones. "En 2023, el alcance de la exposición aumentará, no solo porque habrá más datos en línea, sino porque surgirá una nueva clase de amenazas con la adopción de IA a escala. Por ejemplo, cuando se trata de ChatGPT, el mantra Zero Trust (no confíes fácilmente) será fundamental. La generación de contenido de IA hace que sea imposible confiar en el contenido por principio. Este es otro enfoque de Zero Trust que aún se está diseñando", comentó André Kupfer, líder de ingeniería de ventas de LATAM en Hillstone Networks.

**Datos de contacto:**

Carlos Soto

CEMPR Digital

5532322068

Nota de prensa publicada en: [https://www.mexicopress.com.mx/hillstone-networks-explica-todo-lo-que-se](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Telecomunicaciones Programación Ciberseguridad



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)