La Autenticación Multifactor ya no es suficiente: la relevancia del enfoque Zero Trust

Ciudad de México, 16 de abril de 2024.- La autenticación multifactor (MFA) alguna vez fue considerada la piedra angular de la protección de datos sensibles para las compañías en todo el mundo. Sin embargo, con la evolución constante de las amenazas cibernéticas y la creciente sofisticación de los ciberdelincuentes, la eficacia de la MFA comienza a cuestionarse y la necesidad de un cambio de paradigma en la manera de proteger a las compañías se hace cada vez más relevante.

La realidad es que la identidad de los usuarios, aunque fundamental, está cada vez más expuesta a riesgos y vulnerabilidades. Datos de Netskope indican que en la actualidad alrededor del 70% de las opciones de MFA son vulnerables a ataques de ingeniería social y phishing.

"En un panorama de amenazas cibernéticas en constante evolución, es vital que las empresas reconozcan la necesidad de adoptar un enfoque más holístico en su estrategia de seguridad. Si bien la autenticación multifactor ha sido una herramienta valiosa en la protección de datos sensibles, la realidad es que ningún método único puede garantizar una protección completa. Es hora de que las organizaciones adopten un enfoque que vaya más allá de la simple autenticación y considere todos los aspectos de la seguridad cibernética actual", considera Neil Thacker, CISO EMEA de Netskope.

De acuerdo con Netskope, y ante dicho contexto, para avanzar hacia el siguiente nivel en materia de combate al cibercrimen se requiere la adopción del modelo Zero Trust. Este enfoque parte del principio fundamental de que ninguna entidad, ya sea usuario o dispositivo, puede ser completamente confiable. Por lo tanto, en lugar de basarse exclusivamente en la identidad del usuario, Zero Trust adopta una estructura holística que considera múltiples factores y capas de seguridad.

- ¿Cuáles son los factores que contempla este enfoque?

Más allá de la autenticación de identidad como medida de seguridad, Zero Trust se basa en un esquema descentralizado. Entre los principales elementos que toma en cuenta para garantizar una infraestructura de confianza cero segura y sólida, destacan:

1. Dispositivo: Debido a que la seguridad no solo depende de quién es el usuario, sino también de qué dispositivo está utilizando, Zero Trust diferencia entre dispositivos corporativos y personales, evaluando sus actualizaciones, el nivel de protección con el que cuenta (como los parches y antivirus que tiene instalados) y sus configuraciones de seguridad, antes de otorgar acceso.

2. Ubicación: En un mundo cada vez más conectado y con el aumento del trabajo remoto, es crucial anticiparse a los intentos de acceso desde ubicaciones inusuales. Zero Trust debe ser capaz de detectar y alertar sobre patrones de acceso sospechosos, como intentos de inicio de sesión desde ubicaciones geográficas dispares. De ese modo, incluso aunque las

contraseñas, biométricos y pasos de seguridad sean correctos, el sistema alertará sobre un intento de inicio sospechoso.

3. Aplicación: Con la proliferación de servicios en la nube, es esencial que las organizaciones aprueben y controlen las aplicaciones utilizadas, mitigando así el riesgo de pérdida de datos debido al uso de aplicaciones no autorizadas.

Datos de la compañía revelan que a nivel global las empresas utilizan hasta 800 aplicaciones para complementar sus procesos; muchas de ellas están basadas en la nube y el 97% son instaladas y utilizadas en el día a día de la compañía sin la supervisión del equipo de TI.

4. Actividad: Zero Trust no solo se trata de autenticar al usuario, sino también de vigilar de cerca las acciones realizadas dentro de las aplicaciones y entre ellas. De ese modo la protección no se detiene una vez que el acceso se autoriza, sino que se monitorea de manera constante el comportamiento del usuario al interior de la red, para detectar oportunamente cualquier patrón de sospecha.

Esto es relevante considerando que, de acuerdo con Netskope, más del 20% de los usuarios de redes empresariales mueven datos entre distintas plataformas de nube, tanto dentro como fuera de la empresa; el 35% de esa data se puede considerar como “sensible”.

5. Datos: El núcleo de la confianza cero son los datos. Por ello se basa en cifrar la data, tanto en tránsito como la que se encuentra inactiva, y monitorea los patrones de acceso a dichos datos para detectar anomalías, independientemente de la identidad del usuario. Esto incluye medidas para automatizar la categorización de datos y la implementación de controles específicos si se requiere.

En conclusión, la adopción de un enfoque Zero Trust integral es fundamental para garantizar la seguridad cibernética en un entorno cada vez más complejo y dinámico. No se trata solo de proteger los datos, sino también de permitir la innovación y la adaptación a las necesidades comerciales en constante evolución.

Como un reconocimiento hacia la innovación en ciberseguridad de Netskope y con respecto a la implementación de Zero Trust en la región de Latinoamérica, y en todo el mundo, la empresa fue recientemente acreditado por CRN como una de las 20 empresas más populares de ciberseguridad en IA, ubicándola en el puesto #9 en la lista "The 20 Hottest AI Cybersecurity Companies: The 2024 CRN AI 100".

Este reconocimiento subraya el compromiso de Netskope con la innovación, incluida la implementación de capacidades de inteligencia artificial y aprendizaje automático en su plataforma de acceso seguro a la nube, así como el impulso de Zero Trust para mejorar la prevención de pérdida de datos y detectar amenazas generadas por IA.

Acerca de Netskope

Netskope es la compañía líder mundial en SASE que ayuda a las organizaciones a aplicar los principios de confianza cero (zero trust) y las innovaciones de IA/ML para proteger los datos y defenderse de las ciberamenazas. Rápida y fácil de usar, la plataforma Netskope proporciona acceso optimizado y seguridad en

tiempo real para personas, dispositivos y datos en cualquier lugar. Netskope ayuda a los clientes a reducir riesgos, acelerar el rendimiento y obtener una visibilidad inigualable de cualquier actividad en la nube, la web y las aplicaciones privadas. Miles de clientes confían en Netskope y en su potente red NewEdge para hacer frente a las amenazas cambiantes, los nuevos riesgos, los cambios tecnológicos, los cambios organizativos y de red, y los nuevos requisitos normativos. Para saber cómo Netskope ayuda a los clientes a estar preparados en su viaje SASE, visite https://www.netskope.com/es/