Las agencias estadounidenses especializadas en ciberseguridad e inteligencia han emitido un conjunto de sugerencias para abordar las inquietudes de seguridad relacionadas con la segmentación independiente de redes 5G («network slicing») y fortalecerlas frente a posibles amenazas.

> *«El panorama de riesgos en el contexto del 5G es dinámico; por ende, se requiere el uso de monitoreo avanzado, auditorías y otras capacidades analíticas para cumplir con los requisitos de nivel de servicio de la segmentación de redes a lo largo del tiempo»*, señalaron la Agencia de Ciberseguridad e Infraestructura y la Agencia de Seguridad Nacional de los Estados Unidos.

El 5G representa la quinta generación de estándares tecnológicos para redes celulares de banda ancha, ofreciendo mayores velocidades de transferencia de datos y menor latencia. La segmentación de redes («network slicing») es un modelo arquitectónico que permite a los proveedores de servicios móviles dividir su red en múltiples «segmentos» independientes para crear redes virtuales que atiendan a diferentes clientes y casos de uso.

El último aviso se basa en las recomendaciones previamente emitidas por las agencias en diciembre de 2022, advirtiendo que la segmentación de redes 5G podría exponer a los usuarios a diversas formas de ataques, como denegación de servicio, bloqueo de señales, robo de identidad y ataques de intermediarios adversarios, afectando en gran medida la confidencialidad, integridad y disponibilidad de los servicios de red.

Las preocupaciones relacionadas con la segmentación de redes 5G fueron detalladas en un informe publicado por Enea AdaptiveMobile Security en marzo de 2021, el cual resaltó el riesgo potencial de ataques de fuerza bruta para obtener acceso malicioso a un segmento y llevar a cabo ataques de denegación de servicio contra otras funciones de la red.

Después, en mayo de 2021, el gobierno de Estados Unidos advirtió sobre los riesgos significativos de ciberseguridad para las redes 5G debido a una implementación insuficiente de estándares de telecomunicaciones, amenazas a la cadena de suministro y debilidades en la arquitectura de los sistemas. Esto podría permitir que actores malintencionados exploten las vulnerabilidades para extraer información valiosa de sus víctimas.

En las últimas directrices, las autoridades identificaron tres vectores de amenazas prominentes en 5G: ataques de denegación de servicio en la capa de señalización, ataques de mala configuración y ataques de intermediarios adversarios. Para asegurar las implementaciones de red, se destacó la importancia de adoptar una arquitectura de confianza cero (Zero Trust Architecture – ZTA).

> *«Cumplir con la ZTA se logra en gran medida mediante la implementación de técnicas de autenticación, autorización y auditoría (AAA). Además, una correcta implementación de la autenticación y autorización también puede reducir los riesgos asociados con ataques de mala configuración»,* señalaron CISA y NSA.

Asimismo, las agencias subrayaron la importancia de reconocer las mejores prácticas reconocidas por la industria para implementar, diseñar, desplegar, operar, mantener, reforzar y mitigar el *«network slicing»* 5G, ya que esto afecta la calidad de servicio (QoS) y los acuerdos de nivel de servicio (SLAs).