Recomendaciones y pautas de gestión de ciberseguridad de redes móviles

A medida que se desarrolla la economía digital, la ciberseguridad se está convirtiendo en la piedra angular de la economía digital, la economía digital crea nuevos modelos de negocio y aplicaciones que dependen en gran medida de las capacidades de las redes móviles. Por ejemplo, el Internet de las cosas (IoT), las ciudades inteligentes y las aplicaciones de la industria 4.0 dependen de redes móviles seguras, fiables y de alto rendimiento para recopilar, analizar y actuar sobre los datos en tiempo real. Las redes móviles proporcionan la infraestructura esencial para la comunicación y la transferencia de datos sin problemas, lo que permite a empresas y particulares acceder y compartir información al instante. Esta conectividad facilita el comercio electrónico, las transacciones financieras digitales, el trabajo remoto y la prestación de diversos servicios en línea, todos los cuales son componentes fundamentales de la economía digital. Por esta razón, es importante garantizar una red móvil segura y asegurarse de que exista una seguridad adecuada.

El esquema de aseguramiento de seguridad de equipos de red (NESAS, Network Equipment Security Assurance Scheme), definido conjuntamente por 3GPP y GSMA, proporciona un marco de aseguramiento de seguridad para toda la industria para facilitar mejoras en los niveles de seguridad en toda la industria móvil. NESAS define los requisitos de seguridad y un marco de evaluación para el desarrollo seguro de productos y los procesos del ciclo de vida del producto, así como el uso de casos de prueba de seguridad definidos por 3GPP para la evaluación de seguridad de los equipos de red.

NESAS proporciona una línea de base de seguridad para demostrar que el equipo de red cumple con una lista de requisitos de seguridad y se ha desarrollado de acuerdo con el desarrollo de proveedores y los procesos del ciclo de vida del producto que brindan garantía de seguridad. NESAS debe utilizarse junto con otros mecanismos para garantizar la seguridad de una red, en particular un conjunto adecuado de políticas de seguridad que abarquen todo el ciclo de vida de la red.

La GSMA también lleva a cabo análisis exhaustivos de amenazas con aportes en todo el ecosistema y fuentes públicas como el 3GPP, Agencia de Ciberseguridad de la Unión Europea (ENISA) y el Instituto Nacional de Estándares y Tecnología (NIST). Presenta un mapa de las amenazas potenciales para controles de seguridad adecuados y eficaces y recopila este análisis en la base de conocimientos sobre ciberseguridad móvil (MCKB). El CKB móvil es diseñado para ayudar a las partes interesadas clave a comprender las amenazas a la seguridad a las que se enfrentan las redes móviles de forma sistemática y objetiva, con orientación y mejores prácticas sobre la estrategia de gestión de riesgos y las medidas de mitigación de riesgos.

Para obtener más información, consulte el sitio web de GSMA y el enlace de documentos de NESAS y MCKB como se muestra a continuación:

Mintel(Ministerio de Telecomunicaciones y de la Sociedad de la Información) también elaboró una guía "Guía de seguridad de redes móviles" adjunta a los operadores móviles para evaluar el riesgo de la red.

Sistema de garantía de seguridad de equipos de red (NESAS) GSMA - Servicios industriales

Documentos de GSMA NESAS - Servicios industriales

Base de conocimientos sobre ciberseguridad móvil GSMA - Seguridad

Controles de seguridad de línea base GSMA FS.31 GSMA – Seguridad