REPRESENTACIÓN EN ESPAÑA

COMUNICADO DE PRENSA

Ciberseguridad de las redes 5G: La UE publica un informe sobre la seguridad de la Open RAN

Bruselas, 11 de mayo de 2022

Los Estados miembros de la UE, con el apoyo de la Comisión Europea y de ENISA, la Agencia de la UE para la Ciberseguridad, han publicado hoy un informe sobre la ciberseguridad de la red abierta de acceso por radio (Open RAN). Este nuevo tipo de arquitectura de red 5G facilitará en los próximos años una forma alternativa de desplegar la parte de acceso radioeléctrico de las redes 5G mediante interfaces abiertas. Esto supone otro paso importante en el trabajo coordinado a escala de la UE sobre la ciberseguridad de las redes 5G, que demuestra la firme determinación de seguir haciendo frente conjuntamente a los retos de seguridad de esas redes y de mantenerse al día de la evolución de su tecnología y arquitectura.

Los ciudadanos y las empresas de la UE que utilizan aplicaciones avanzadas e innovadoras posibilitadas por la 5G y las generaciones futuras de redes de comunicaciones móviles deben disfrutar del máximo grado de seguridad. A raíz del trabajo coordinado ya realizado a escala de la UE para reforzar la seguridad de las redes 5G con el conjunto de instrumentos de la UE sobre ciberseguridad de las redes 5G, los Estados miembros han analizado los aspectos de seguridad de la Open RAN.

Margrethe **Vestager**, vicepresidenta ejecutiva responsable de Una Europa Adaptada a la Era Digital, ha declarado: *«Nuestra prioridad y responsabilidad comunes es garantizar la oportuna implantación de las redes 5G en Europa, garantizando al mismo tiempo su seguridad. Las arquitecturas de Open RAN crean nuevas oportunidades de mercado, pero este informe muestra que también plantean graves problemas de seguridad, especialmente a corto plazo. Será importante que todos los participantes dediquen el tiempo y la atención suficientes para hacer*

frente a esos problemas retos, de modo que puedan hacerse realidad las promesas de la Open RAN».

Thierry **Breton**, comisario de Mercado Interior, ha añadido lo siguiente: *«En un momento en que las redes 5G se están implantando en toda la UE y nuestras economías dependen cada vez más de las infraestructuras digitales, es más importante que nunca garantizar un alto grado de seguridad de nuestras redes de comunicaciones. Eso es lo que hacemos con el conjunto de instrumentos de ciberseguridad de la 5G, y también es eso lo que, junto con los Estados miembros, hacemos ahora, en cooperación con los Estados miembros, en relación con la Open RAN con este nuevo informe. No corresponde a las autoridades públicas elegir una tecnología, pero es responsabilidad nuestra valorar los riesgos asociados a las distintas tecnologías. Este informe indica que la Open RAN brinda una serie de oportunidades, pero también plantea graves problemas de seguridad a los que aún no se hace frente y que no pueden subestimarse. Las posible implantación de Open RAN en las redes 5G de Europa no debe crear nuevos puntos vulnerables en ninguna circunstancia».*

Guillaume Poupard, director general de la Agencia Nacional de Ciberseguridad de Francia (ANSSI), ha comentado: *«Tras el conjunto de instrumentos de la UE sobre ciberseguridad de la 5G, este informe constituye otro hito en los esfuerzos del Grupo de Cooperación SRI por coordinarse y paliar los riesgos de seguridad de nuestras redes 5G. Este análisis en profundidad de la Open RAN contribuye a garantizar que nuestro enfoque común siga el ritmo de las nuevas tendencias y los problemas relacionados con la seguridad. Seguiremos trabajando para solucionarlos juntos».*

El informe constata que la Open RAN puede brindar posibles oportunidades en materia de seguridad, siempre que se cumplan determinadas condiciones. Gracias a una mayor interoperabilidad entre los componentes de la red de acceso por radio de diferentes proveedores, la Open RAN podría permitir una mayor diversificación de los proveedores dentro de las redes de la misma zona geográfica. Esto podría contribuir a que se cumpliera la recomendación del conjunto de instrumentos de la UE en materia de 5G de que cada operador tenga una estrategia adecuada de múltiples proveedores para evitar o limitar cualquier dependencia importante de un único proveedor. La Open RAN también podría contribuir a aumentar la visibilidad de la red gracias al uso de interfaces y normas abiertas, a reducir los errores humanos gracias a una mayor automatización y a aumentar la flexibilidad mediante el uso de soluciones de virtualización y basadas en la nube.

Sin embargo, el concepto de Open RAN sigue sin alcanzar su madurez y la ciberseguridad constituye aún un problema importante. Especialmente a corto plazo, al aumentar la complejidad de las redes,

la Open RAN agravaría una serie de riesgos de seguridad, tales como una exposición mayor a ataques y más puntos de entrada para los agentes malintencionados, un mayor riesgo de mala configuración de las redes y posibles repercusiones en otras funciones de red debido al uso compartido de recursos. El informe también señala que las especificaciones técnicas, como las desarrolladas por la Alianza de la Open RAN (O-RAN Alliance), no son suficientemente maduras y seguras en cuanto a su diseño. La Open RAN podría dar lugar a dependencias críticas nuevas o mayores, por ejemplo, en el ámbito de los componentes y la nube.

Para reducir estos riesgos y aprovechar las oportunidades potenciales de la Open RAN, el informe recomienda una serie de medidas basadas en el conjunto de instrumentos 5G de la UE, y en particular:

- utilizar las competencias en materia de regulación para poder controlar los planes de los operadores móviles de despliegue a gran escala de una Open RAN y, en caso necesario, restringir, prohibir o imponer requisitos o condiciones específicos para el suministro, el despliegue a gran escala y el funcionamiento de los equipos de Open RAN;
- reforzar los controles técnicos fundamentales, tales como la autenticación y la autorización, y adaptar el diseño en materia de control a un entorno modular en el que se supervise cada componente;
- evaluar el perfil de riesgo de los proveedores de Open RAN, los proveedores de servicios externos relacionados con la Open RAN, los proveedores de servicios o infraestructuras en la nube y los integradores de sistemas, y ampliar los controles y restricciones de los proveedores de servicios gestionados a dichos proveedores;
- corregir las deficiencias en la elaboración de especificaciones técnicas: el proceso debe ajustarse a los principios fundacionales de la Organización Mundial del Comercio (OMC)/Obstáculos Técnicos al Comercio (OTC) para la formulación de normas internacionales [1] y resolver las deficiencias en materia de seguridad;
- incluir los componentes de red de acceso por radio abiertos en el futuro régimen de certificación de la ciberseguridad de la 5G, actualmente en fase de elaboración, lo más tempranamente que sea posible.

Por lo que se refiere a la preservación y consolidación de las capacidades de la UE en este mercado, debe mantenerse una regulación tecnológicamente neutra para fomentar la competencia. En este marco, la financiación nacional y de la UE para la investigación y la innovación 5G y 6G podría servir para apoyar las oportunidades de los agentes de la UE para que compitan en igualdad de condiciones.

Además de la red de acceso por radio, también es importante abordar las posibles dependencias o la falta de diversidad en toda la cadena de valor de la comunicación para la diversificación del suministro.

En general, el informe recomienda un planteamiento prudente para avanzar hacia esta nueva arquitectura. Cualquier transición y coexistencia con tecnologías existentes y fiables debe llevarse a cabo concediendo tiempo y recursos suficientes para evaluar los riesgos con antelación, aplicar medidas paliativas adecuadas y definir claramente las responsabilidades en caso de fallo o incidente.

Contexto

La oportuna implantación de las redes 5G seguras es una de las principales prioridades de la Unión Europea. Para contribuir a este objetivo, los Estados miembros de la UE, con el apoyo de la Comisión Europea y de ENISA, han creado un método concertado en materia de ciberseguridad de las redes 5G. Mediante tal método, los Estados miembros de la UE evaluaron conjuntamente los principales riesgos relacionados con las redes 5G («evaluación coordinada de riesgos de la UE») y definieron un enfoque global y basado en el riesgo en forma de conjunto de instrumentos de la UE en materia de redes 5G, que se adoptó en enero de 2020. El conjunto de instrumentos de la UE sobre las redes 5G recomienda una serie de medidas comunes de reducción del riesgo.

Ese conjunto también comprende medidas estratégicas y técnicas y las actuaciones correspondientes para reforzar su eficacia. Entre las medidas fundamentales del conjunto de instrumentos figuran reforzar los requisitos de seguridad, evaluar los perfiles de riesgo de los proveedores, aplicar las restricciones pertinentes a los proveedores considerados de alto riesgo, incluidas las exclusiones necesarias para los activos clave considerados críticos y sensibles (tales como las funciones básicas de la red), y contar con estrategias para garantizar la diversificación de los proveedores y evitar dependencias.

Para continuar y profundizar el proceso de coordinación de la UE en materia de ciberseguridad de las redes 5G, la Estrategia de Ciberseguridad de la UE de diciembre de 2020 fijó tres objetivos clave: 1) garantizar una mayor convergencia en los planteamientos de reducción del riesgo en la Unión, 2) fomentar un constante intercambio de conocimientos y desarrollo de capacidades, y 3) promover la resiliencia de las cadenas de suministro y otros objetivos estratégicos de seguridad de la Unión.

Dentro de estos objetivos clave, el Grupo de Cooperación en materia de SRI seguirá supervisando y evaluando las cuestiones relacionadas con las nuevas tendencias y la evolución de la cadena de suministro de

la 5G. Puesto que la Open RAN es una tendencia del mercado en la evolución de las arquitecturas 5G y 6G, los Estados miembros han decidido llevar a cabo un análisis en profundidad de las consecuencias en la seguridad de la Open RAN para complementar el análisis coordinado de riesgos en materia de redes 5G.

Más información

Conjunto de instrumentos de la UE sobre la ciberseguridad de las redes 5G

Grupo de cooperación RSI