Más riesgos y controles del 5G

Siguiendo con el hilo del anterior post en el que comenté algunos de los riesgos del 5G, en este presentaré algunos riesgos más y los controles y medidas necesarias para mitigar esos riesgos.

Pero antes de todo, veo conveniente dejar claros algunos conceptos como riesgo, control, amenaza y vulnerabilidad. En el ámbito de la informática podemos definir el riesgo como la probabilidad de que ocurra un incidente de seguridad. Por otro lado, la amenaza es una acción que podría tener un potencial efecto negativo sobre un activo. Por sí sola la amenaza no provoca un daño, necesita de una debilidad o fallo en los sistemas para que se materialice el daño, a estas debilidades o fallos les llamamos vulnerabilidades. Por lo tanto, podemos decir que un riesgo es la probabilidad de que ocurra una amenaza utilizando una vulnerabilidad generando un daño [1].

Para mitigar estos riesgos, se emplean controles que permiten asegurar la calidad de nuestros sistemas y a su vez, estos controles necesitan ser auditados para asegurar que se cumplen como se deben.

Tras el apoyo del Consejo Europeo el 22 de marzo de 2019 para un enfoque concertado de la seguridad de las redes 5G, la Comisión Europea adoptó su recomendación sobre la ciberseguridad de las redes 5G el 26 de marzo de 2019. Esta recomendación pedía a los Estados miembros que completaran evaluaciones de riesgos y revisaran las medidas nacionales, trabajando juntos a nivel de la UE con el objetivo de concretar una evaluación de riesgos coordinada y preparar una "caja de herramientas" de posibles medidas de mitigación. Cada Estado miembro completó su propia evaluación de riesgos de sus infraestructuras de red 5G y transmitió los resultados a la Comisión y a ENISA. Gracias a esto se desarrolló una "caja de herramientas" de la UE para la mitigación de riesgos en cuanto a redes 5G [2].

Este documento comienza enumerando 9 riesgos fundamentales a tener en cuenta:

1. Mala configuración de redes.
2. Falta de controles de acceso.
3. Baja calidad del producto.
4. Dependencia de un solo proveedor dentro de redes individuales o falta de diversidad a nivel nacional.
5. Interferencia estatal a través de la cadena de suministro 5G.

6. Explotación de redes 5G por parte del crimen organizado dirigido a usuarios finales.
7. Interrupción significativa de infraestructuras o servicios críticos.
8. Fallo masivo de las redes debido a la interrupción del suministro eléctrico u otros sistemas de apoyo.
9. Explotación del IoT, teléfonos o dispositivos inteligentes.

Estos riesgos se pueden agrupar en diferentes escenarios. El primer y segundo riesgo hacen referencia a un escenario relacionado con una insuficiencia de medidas de seguridad. El tercero y cuarto están relacionados con la cadena de suministro. El quinto y sexto surgen de acciones negativas por parte de terceros actores. El séptimo y octavo riesgo surgen por el fallo de un sistema unido a la red 5G y por último, el noveno está relacionado con dispositivos para el usuario final. Tal vez este último riesgo sea uno de los que más se diferencia respecto a los riesgos que pudieran haber tenido y que siguen teniendo redes móviles de anteriores generaciones como el 4G y el 3G.

En el mismo documento también se plantean medidas que permiten mitigar los riesgos comentados anteriormente. A partir de estas medidas se pueden sacar los controles que aseguren la calidad de la red 5G. He realizado la siguiente tabla teniendo en cuenta el documento, seleccionando, resumiendo y adaptando el contenido:

Medidas	Controles	Riesgos Relacionados
Fortalecer el papel de las autoridades nacionales	Asegurar que las autoridades nacionales cuentan con los poderes necesarios para hacer cumplir con las medidas necesarias para asegurar la calidad y seguridad de la red.	R1, R2, R3, R4, R5, R6, R7
Ejecutar auditorías a MNO (Operador de Red Móvil)	Auditar o requerir auditorías a los operadores de redes móviles. Requerir a los operadores información detallada y actualizada de sus planes para el suministro de equipos 5G y participación de proveedores externos..	R1, R2, R3, R4, R5, R6, R7
Evaluar el riesgo y aplicar restricciones a operadores con alto riesgo	Realizar evaluaciones rigurosas del perfil de riesgo de todos los proveedores relevantes. Identificar activos clave críticos o sensibles. Aplicar restricciones para los activos clave definidos como críticos o sensibles.	R2, R5
Asegurar la diversidad de proveedores para MNO	Asegurar que cada MNO tiene una estrategia de múltiples proveedores adecuada que tenga en cuenta las limitaciones técnicas y los requisitos de interoperabilidad. Limitar cualquier dependencia importante de un solo proveedor. Evitar la dependencia de proveedores considerados de alto riesgo.	R4
Controlar el uso de MSP (Proveedores de Servicios Gestionados)	Aplicar restricciones en partes sensibles de la red 5G. Imponer disposiciones de seguridad mejoradas alrededor del acceso que se da a los MSP.	R2, R5
Asegurar la aplicación de requisitos de seguridad básicos	Asegurar que los MNO implementan buenas prácticas de seguridad no específicas de la red 5G. Asegurar que los MNO mantengan actualizada la información sobre la política operativa y de procedimientos de gestión de incidentes.	R1, R2, R3, R6, R7, R8, R9
Asegurar y evaluar la implementación de medidas de seguridad en estándares 5G existentes	Asegurar que los MNO y proveedores implementen medidas de seguridad existentes en los estándares de tecnología 5G. Asegurar que usan las medidas como línea de base de seguridad mínima.	R1, R2, R3, R6, R7, R9

Asegurar controles de acceso estrictos	Asegurar que se aplican controles estrictos de acceso a la red. Asegurar que se aplica el principio de privilegio mínimo. Asegurar que se aplica el principio de segregación de funciones. Asegurar la existencia de procedimientos para garantizar que las reglas están en vigor y evolucionan con la red.	R1, R2, R3, R5, R6, R7
Aumentar la seguridad de funciones de red virtualizada	Asegurar que los MNO siguen buenas prácticas de seguridad para las funciones de red virtualizada.	R1, R3, R6, R7
Garantizar una gestión, operación y monitorización seguros de 5G	Asegurar que los MNO ejecutan sus Centros de Operaciones de Red y/o Centros de Operaciones de Seguridad dentro del país y/o dentro de la Unión Europea. Asegurar que los MNO protejan adecuadamente el tráfico de gestión de la red.	R1, R2, R3, R5, R6, R7, R9,
Reforzar la seguridad física	Asegurar que se protege correctamente los componentes físicos críticos y partes sensibles de las redes 5G.	R6, R7
Reforzar la integridad del software, actualización y gestión de parches	Asegurarse de implementar herramientas y procesos adecuados que garantizan la integridad del software. Asegurar un seguimiento confiable de los cambios. Asegurar la realización de actualizaciones y parches de seguridad.	R1, R3, R5, R6, R7
Reforzar la resiliencia y los planes de continuidad	Asegurar que los MNO refuercen sus planes de resistencia y continuidad. Contar con planes de continuidad adecuados en caso de desastre.	R7, R8

En conclusión, los controles parecen estar muy dirigidos a los operadores de red móvil, esto puede expresar una clara preocupación por parte de estas empresas. Al final, dentro de un sistema compuesto por muchos agentes, el nivel de seguridad suele ser el del eslabón más débil y es donde hay que poner el foco. En mi opinión, estas medidas no serán suficientes para evitar que se materialicen ciertas amenazas ya que todo no se puede prever. Además, esta tecnología que posibilita que otras cojan fuerza, hace que ciertos

problemas solo salgan a la vista una vez que esté completamente implantada. Creo que todavía hay mucho trabajo por delante en cuanto al 5G.

Bibliografía

[1] <<Diferencias entre ataque, amenaza y vulnerabilidad en Ciberseguridad>>, EALDE, consultado el 12/11/2020, https://www.ealde.es/ataque-amenaza-vulnerabilidad-ciberseguridad/#:~:text=El%20concepto%20de%20vulnerabilidad%20en%20Ciberseguridad&text=Esta%20puede%20considerarse%20como%20la,de%20un%20sistema%20de%20informaci%C3%B3n.&text=Las%20amenazas%20representan%20un%20potencial,que%20se%20materialice%20ese%20da%C3%B1o

[2] <<EU Toolbox of risk mitigating measures>>, European Union, consultado el 12/11/2020, https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures