Seguridad, ¿el talón de Aquiles del 5G?

Si la telefonía móvil de quinta generación corrige las fallas de 4G, el nuevo estándar acomodará servicios críticos en la ciudad inteligente o fábrica del futuro. La explosión en el número de objetos conectados también aumentará la superficie de ataque. En sí mismo, 5G está destinado a ser más seguro que el estándar actual.

Un teléfono inteligente 4G envía su Identidad de Suscriptor Móvil Internacional (IMSI) en claro, un número único que identifica a un usuario. Al presentarse como una estación base ficticia, un receptor IMSI puede interceptar estos datos confidenciales de forma remota. 5G cifrará la comunicación de los primeros intercambios. También frustrará los llamados ataques man-in-the-middle (HDM) que consisten, por ejemplo, en secuestrar un servidor DNS (suplantación de DNS) para redirigir su tráfico a un servidor DNS pirata y recuperar su contenido.

Por lo tanto, 5G en sí mismo no traerá nuevas vulnerabilidades. Por otro lado, los servicios innovadores que apoyará aumentarán la superficie de riesgo. Fábrica 4.0, ciudad inteligente , vehículos autónomos… Los usos asociados al 5G son especialmente críticos, conceptúan los expertos. Se deben implementar todos los mecanismos de seguridad posibles para asegurar las transmisiones sensibles. También existe un desafío de estandarización para que el mismo nivel de seguridad esté garantizado en toda la cadena por los diversos actores involucrados. En la ciudad inteligente de las comunicaciones sensibles se pueden intercambiar estos parámetros entre los directivos del agua y los gerentes de

electricidad, por ejemplo.

Botnets de objetos conectados zombis

Al densificar la red, 5G dará el puntapié inicial real al Internet de las cosas. Pero de nuevo, tenga cuidado con el peligro. Decenas de miles de millones de dispositivos inteligentes en la atención médica, la industria, los edificios inteligentes y el automóvil se conectarán mediante 5G, es nuestra nueva realidad.

Sin embargo, solo una pequeña parte de ellos tiene funciones de seguridad más allá de la contraseña. Resultado: los piratas informáticos podrían piratear fácilmente cientos o incluso miles de objetos conectados 5G, como cámaras de vigilancia IP o sensores industriales, con el fin de explotar su poder conectándolos en red (luego hablamos de botnets de objetos conectados zombies) en beneficio de la ola de ataques que se había desatado a finales de 2016 , que afectaron en particular a OVH cloud, solo para darnos una idea de lo que nos espera en términos de seguridad.

Se destaca la negligencia de los fabricantes. Están compitiendo para ser los primeros en poner nuevos objetos conectados en el mercado, pero la seguridad ocupa el segundo lugar. En general, hay una falta de cultura en ciberseguridad entre estos jugadores como en TI hace 20 o 30 años .

En su defensa, estos fabricantes están limitados por los pocos recursos a bordo y por un sistema operativo ajustado . Internet Society ha desarrollado un marco de confianza para IoT, Online Trust Alliance (OTA) , para ayudar a ambos fabricantes a integrar este enfoque, desde el diseño hasta todo el ciclo de vida del producto.

Microagentes e informática de borde

La responsabilidad también está en el campo empresarial. Un estudio de Check Point muestra que el 90% de ellos tienen objetos conectados que no son de confianza en sus redes. Con el auge de BYOD, la mayoría de las veces están conectados sin el conocimiento de los equipos de seguridad o de TI. No obstante, también existe el problema de delimitar el perímetro.

De forma incorrecta, los objetos conectados se consideran fuera de la red de la empresa. Algunos dependen de la producción, otros de los servicios generales y no del departamento de TI. Depende del CISO, que no debe depender del DSI sino de los riesgos, tomar esto sujeto de frente.

Si no se controla, las comunicaciones hacia y desde los dispositivos 5G pueden eludir la red corporativa y sus controles de seguridad. Con los ataques de rebote, cualquier objeto 5G puede proporcionar una puerta de entrada a la red IP tradicional. En los Estados Unidos, un casino ya ha sido

pirateado desde un termómetro de acuario conectado. La amenaza en los negocios podría provenir de una simple bombilla conectada o una máquina de café inteligente que advierte cuando es necesario recargarla.

Hay una serie de mejores prácticas dedicadas a proteger el IoT

En ausencia de seguridad «por diseño», se trata ante todo de modificar los parámetros y las contraseñas por defecto de tipo «admin» o «1234» y actualizar el firmware de los terminales.

Entonces es necesario elaborar un inventario exhaustivo de todos los objetos conectados presentes en la empresa y luego adoptar una estrategia de «contenerización». Las soluciones EMM (gestión de movilidad empresarial) permiten que solo los objetos autorizados accedan al sistema de información.

Así mismo, las empresas también podrían optar por abandonar su red cableada (LAN) o su infraestructura wifi en favor de 5G. Frente a esta conectividad inalámbrica permanente, los RSSI tienen todo un arsenal, desde la autenticación de usuarios hasta el cifrado, incluidos los firewalls. Sin embargo, el modelo de protección perimetral muestra sus límites ante estas nuevas amenazas y es necesario otro enfoque.

La seguridad debe ser constante, pero completamente escalable, para hacer frente al enorme ancho de banda de 5G, se trata de tener una prevención de amenazas avanzada para proteger los recursos de TI dondequiera que estén. Se aboga por el uso de complementos de seguridad que funcionen en cualquier entorno.

Estos micro-agentes pueden controlar cada atributo que entra y sale del dispositivo 5G mientras lo conectan a una arquitectura de seguridad consolidada para fortalecer la protección. Este enfoque va de la mano con el desarrollo de la informática de punta, que consiste en procesar los datos lo

más cerca posible de los objetos conectados en lugar de transferirlos a la nube para esta operación.

¿Lo peor por venir?

Sin embargo, las principales amenazas podrían llegar en una segunda fase con la llegada del llamado 5G independiente que se espera a partir de 2023. El núcleo de la red móvil se basará entonces exclusivamente en el nuevo estándar. Antes de eso, los operadores lo habrán virtualizado para ignorar la infraestructura subyacente. Al volverse programable, la red central se beneficiará por completo de 5G.

Con la técnica de corte de red, será posible desplegar componentes de red de forma dinámica. Esta softwareización de la red central tiene muchas ventajas, pero con contrapartes de seguridad. Lo que el operador gana en agilidad, pierde el control de la seguridad. Hasta entonces, el núcleo de la red consistía principalmente en equipos de hardware, cuya protección se facilitó. Una vez virtualizados, estarán mucho más orientados al exterior.

Se trata de automatizar y orquestar la política de seguridad

Debe ser una parte intrínseca de un despliegue y no debe estudiarse en un segundo paso. Esto supone una coordinación de los equipos de red y ciberseguridad, sabiendo que estos últimos pueden tener un impacto en la calidad del servicio. Acá por supuesto, nos referimos a las recomendaciones de Anssi y sus equivalentes británicos (NCSC) y estadounidenses (Nist). Tres agencias gubernamentales que abogan por un enfoque común de aseguramiento de redes, con foco en cinco pilares: identificación y análisis de riesgos, protección, detección de incidentes de seguridad, respuesta adecuada y, finalmente, recuperación de la calidad del servicio.

Leer también: ¿Cuál Será El Impacto De La Tecnología 5G En Los Centros De Datos? ; La guerra de los chips y semiconductores entre China y Estados Unidos ; Por qué Edge Computing es clave para el futuro de la alta velocidad