# Retos de la tecnología 5G para la ciberseguridad de las empresas

Hiperconectividad, baja latencia, mayor ancho de banda, bajo consumo, un aumento exponencial de la velocidad… El despliegue de la quinta generación de telefonía móvil va a suponer una auténtica revolución en todos los ámbitos, desde el doméstico hasta el industrial: en muy poco tiempo, el 5G permitirá dar un impulso a proyectos de Smart City, vehículo autónomo, expansión de dispositivos IoT, automatización industrial, el vídeo en 3D, la generalización del Edge Computing que permitirá un consumo de servicios en la nube con mayor velocidad…

A medida que avance este despliegue nuestras vidas estarán más interconectadas; tendremos acceso a mucha más información de manera casi inmediata, y veremos más cerca algunas tecnologías que hasta ahora nos parecían propias del cine de ciencia ficción.

**Retos a los que se enfrenta el ecosistema empresarial con el 5G**

Como ocurre con cualquier cambio tecnológico que se encuentra en proceso de transición, el 5G también constituye una oportunidad para que los ciberdelincuentes encuentren vulnerabilidades y puedan lanzar sus ataques contra las empresas. Estos son algunos de los retos a los que se enfrentan:

- **Aumento de los puntos de entrada,** a través de dispositivos cuyo uso se está extendiendo como es el caso del IOT. Existen infinidad de soluciones Internet of Things que ya se aplican en el mundo de la empresa, la salud o la industria. El crecimiento exponencial de dispositivos conectados aumenta el nivel de exposición de las empresas a los ciberriesgos. Además, muchos de estos dispositivos se fabrican en un modelo *low-cost* sin las necesarias medidas de ciberseguridad y abren una brecha por la que se pueden colar los ciberdelincuentes. Un dispositivo IoT conectado puede compartir datos sensibles por sí mismo, desde información médica procedente de un hospital hasta datos de clientes gestionados por sistemas CRM o equipamientos de mantenimiento industrial. Cuando se generalicen las redes 5G, su mayor ancho de banda aumentará la capacidad para añadir dispositivos IoT o de cualquier otro tipo conectados que exigirán, en consecuencia, soluciones de ciberseguridad fácilmente escalables, que permitan monitorizarlos de una manera integral y establecer medidas de prevención o contención adecuadas.
- **Mayor ancho de banda**. El aumento del ancho de banda será, precisamente, una de las pruebas de seguridad a las que tendrá que someterse la nueva tecnología cuando avance su despliegue por el aumento consecuente del flujo de información. A la hora de transmitir datos, las redes actuales están más limitadas en cuanto a capacidad y velocidad de transmisión. Sin embargo, la quinta generación de telefonía móvil ampliará notablemente el carril por el que discurra la información; eso ayudará a que se transmita con mayor rapidez, y a que el tiempo de respuesta sea mucho menor. En cambio, la mayor capacidad de transmisión también aumenta la exigencia de

seguridad. El reto más importante en este sentido estará en conseguir que las soluciones de seguridad no supongan un cuello de botella en las comunicaciones.

- **La concentración de proveedores aumenta el impacto**. Tal y como se desprende del informe publicado por la Agencia Europea de la Ciberseguridad, la concentración de proveedores de estas redes móviles en grandes operadores, constituye un reto por el nivel de exposición a un mayor volumen de usuarios impactados en caso de ataque y el efecto agravado de la detección de puntos débiles en dichos proveedores de red por parte de los ciberdelincuentes. En este sentido, se habla de la disponibilidad y la integridad de las propias redes como retos importantes.

**Mecanismos que permiten una navegación segura con el 5G**

Para evitar estas situaciones tanto proveedores de servicio como fabricantes deben poner en marcha mecanismos que permitan una navegación segura. En cualquier caso, y aunque por el momento el despliegue efectivo de las redes 5G se limita al ámbito urbano, recordamos **algunas medidas de seguridad generales** que las empresas deben adoptar desde ya.

- **Instalar antivirus actualizados**. Es imprescindible que todos los dispositivos cuenten con un antivirus actualizado de forma permanente.
- Instalar las últimas actualizaciones de software del fabricante, que incluyen parches de seguridad adaptados a posibles vulnerabilidades.
- **Utilizar redes VPN**. Estas redes impiden el acceso a los equipos de personas ajenas a la organización, especialmente cuando se utilizan equipos remotos o se accede desde redes públicas.
- **Establecer contraseñas seguras.** Es muy importante mantener una política de seguridad estricta con respecto a las contraseñas, que deben contener caracteres alfanuméricos.
- **Mantener actualizados los dispositivos IoT.** Cualquier dispositivo IoT que se utilice en el ámbito profesional o doméstico es susceptible sufrir un ataque y debe llevar instaladas las últimas actualizaciones que incluya el fabricante.

La quinta generación de la telefonía móvil se encuentra a la vuelta de la esquina: iniciativas como el Proyecto 5G Euskadi, en el que participa el Basque CyberSecurity Centre, ya han comenzado a desplegar esta tecnología en los parques tecnológicos y, dentro de muy poco, será una realidad en la mayoría de los ámbitos de la sociedad.