WiFi 6, las empresas no deben de minimizar riesgos en seguridad

El Wifi 6 traerá consigo mayores beneficios para las empresas, gracias a la rapidez que se traducirá en mayor productividad, por ejemplo. Pero su adopción también implica riesgos y debe encender los focos rojos en el uso de los dispositivos IoT (Internet of Things) que dependen de esta red.

Se sabe que **un dispositivo IoT comprometido puede servir como un trampolín para que un atacante se propague a través de la red y robe o destruya información confidencial.**
Erick Muller, consultor en Software de Seguridad en Aruba Networks, coincide con que veremos grandes beneficios con el WiFi 6, pero también con ello, asegura citando la Ley de Moore, cualquier cosa con una dirección IP ahora debe considerarse una amenaza potencial. “Aunque el WiFi 6 presenta nuevas funciones de seguridad increíbles, también hace que la WLAN sea aún más compatible con IoT y **la seguridad que los rodea se ha quedado rezagada con respecto a la capacidad de los hackers para penetrar en estos dispositivos**. Los delincuentes pueden controlar de forma remota los equipos inteligentes, creando atascos de tráfico en las carreteras, interrumpiendo la red eléctrica o interrumpiendo los robots industriales”, asegura.

Muller, resalta que a pesar de su poder de cómputo, cosas como sensores, controles, equipos, etc., son cada vez más vulnerables, debido a que rara vez llevan una protección mínima más allá de un ID de usuario y contraseña instalados de fábrica (y fáciles de adivinar), que rara vez se cambian. Además, **estos dispositivos no se registran, por lo que no hay señal ni alerta para indicar que se han comprometido**.

Soluciones
Ante un ataque a bases de datos con información crítica, es importante que los dispositivos de IoT estén conectados a la red que los equipos de seguridad.

Para la seguridad del Internet de las Cosas, esto significa convertir la red en el “sensor” donde el tráfico sin procesar se elabora a través de un motor de inspección profunda de paquetes diseñado para recopilar cientos de elementos de comportamiento relevantes, como el volumen de tráfico, el ciclo de trabajo, los destinos, los puertos, los protocolos, etc.

La información sobre el tráfico se pasa luego a los modelos de aprendizaje automático, para construir una línea de referencia de comportamiento normal para que las desviaciones se puedan detectar fácilmente. Cuando los modelos de aprendizaje automático ven suficiente evidencia de que un ataque está en curso, se genera una alerta para que el analista la revise.

Piense en una cámara que está enviando el doble de paquetes que lo que normalmente hace. O un control de edificio que intenta conectarse a sistemas que nunca ha visto.

Estos dos primeros pasos son cruciales para detectar incidentes relacionados con IoT y requieren una sólida experiencia en el dominio de la red y una ciencia de datos comprobada en conexiones cableadas, inalámbricas, WAN y remotas.

Las decisiones correctas y las acciones apropiadas se basan en la eliminación de falsos positivos y

en proporcionar al analista no solo la señal de ataque correcta, sino también la evidencia de respaldo asociada.