

IoT: un campo de minas de seguridad

Al igual que cualquier tecnología en desarrollo, las empresas tienen dos opciones: esperar hasta que se establezca y estabilice, o probarlo mientras es nuevo. El peligro en la primera opción es que para cuando la tecnología esté estable, usted ya estará muy por detrás de los que adoptaron antes. Alternativamente, con la segunda opción enfrenta mucho más riesgo.

Hasta ahora, hay un riesgo de IoT que se ha destacado: la seguridad. Algunos casos presentan problemas de privacidad, como dispositivos que se usan para escuchar conversaciones. Otros casos sugieren un problema mayor para las empresas que desean construir soluciones de IoT: en los últimos años ha habido algunos casos importantes en los que se utilizaron miles de dispositivos conectados, en ataques DDoS o *ransomware*. Si bien estos ataques generalmente no representan una amenaza directa para la red en la que se ejecutan, generalmente el objetivo está en otra parte, todavía no sabemos con certeza a qué tipo de amenazas nos enfrentaremos en el futuro.

Entonces, ¿qué pueden hacer las empresas que adoptan el IoT para mitigar estos riesgos de seguridad?

Primero: seleccione cuidadosamente los dispositivos que trae a su infraestructura. Muchos dispositivos actuales no tienen la capacidad ni el espacio de almacenamiento para descargar e instalar actualizaciones de *firmware*. Esto significa que si tienen fallas de seguridad, no se podrán reparar con una actualización de *firmware*. Además, los dispositivos que tienen contraseñas simples son un riesgo, especialmente si la contraseña no se puede cambiar. Por lo tanto, cualquier dispositivo que conecte en su entorno debe tener lo siguiente: capacidad de instalar nuevo *firmware*, soporte activo del proveedor y funcionalidad para cambiar la contraseña del dispositivo.

Siguiente: manténgase al día con los avances realizados para el IoT. Siendo una tecnología en desarrollo, hay una serie de avances que encontrarán su camino hacia los dispositivos en los próximos meses y años. A medida que se lanzan nuevos dispositivos con nuevas capacidades, debe llevarlos a su entorno para reemplazar los dispositivos más antiguos.

Finalmente: como cualquier red, el IoT necesita ser monitorizado. Esto significa vigilar los datos que fluyen a través de la red, el ancho de banda y la latencia, y los dispositivos conectados. Una solución de monitorización le brinda una vista central de todos estos aspectos, lo que le permite detectar posibles problemas de seguridad antes de que ocurran.

Por ejemplo: PRTG Network Monitor proporciona dicha funcionalidad. Además de la monitorización tradicional como Netflow y SNMP, también ofrece la flexibilidad de monitorizar una amplia gama de dispositivos a través de varios sensores. [Dele un vistazo a esta descripción general](#) y conozca más sobre lo que PRTG Network Monitor puede hacer por usted.