Publicado en Madrid el 11/09/2023

Smart Cities vs ciberataques: una lucha pendiente de ganador en 2023

Check Point Software alerta de la necesidad de optimizar las medidas de protección en este ámbito y señala que controlar todos los dispositivos conectados, proteger la infraestructura, mejorar la protección de datos, conocer los riesgos de la cadena de suministro, contar con la última tecnología e incrementar el grado de la seguridad son los principales retos

Las ciudades inteligentes se están convirtiendo en una realidad más que en un concepto, y la integración de la tecnología en las infraestructuras cotidianas se ha convertido en la norma. Utilizan el potencial que ofrecen las Tecnologías de la Información y la Comunicación (TIC) para impulsar de manera más eficiente un desarrollo sostenible y mejorar la calidad de vida de sus ciudadanos, de hecho se estima que en 2024 habrá más de 1.300 millones de conexiones a Internet de red de área amplia en estas Smart Cities, según datos de ABI Research.

Check Point® Software Technologies Ltd. (NASDAQ: CHKP), un proveedor líder de soluciones de ciberseguridad a nivel mundial, alerta de que el nivel de complejidad de estas infraestructuras digitales no hace más que incrementarse, lo que significa que cualquier servicio digital implementado por un gobierno u empresa será más vulnerable que nunca a los ciberataques. Esto se debe a que el uso de grandes redes conectadas ofrece a los ciberdelincuentes más endpoints que nunca y la oportunidad perfecta para saltar de un sistema expuesto al siguiente.

Las ciudades inteligentes se enfrentan a retos de ciberseguridad únicos. Las redes son utilizadas a diario por entidades públicas y privadas, particulares y miles de dispositivos IoT. La enorme cantidad de datos que se intercambian a través de estas redes requiere una estrategia de seguridad rigurosa. Algunos de los principales retos son:

Controlar todos los dispositivos conectados: una multitud de aparatos IoT que controlan todo, desde CCTV y gestión de semáforos hasta datos personales y financieros de empresas, podrían estar conectados a una red en cualquier momento. En teoría esto suena ideal para una comunicación y gestión sin fisuras, pero en la práctica ofrece a los ciberdelincuentes miles de posibles puntos de entrada para lanzar un ataque.

Proteger cada operación de la infraestructura: la automatización aporta muchos beneficios a todo tipo de operaciones para las ciudades inteligentes, reduciendo la necesidad de control humano directo sobre dichos sistemas. El aumento de sensores implica más conexiones que supervisar y gestionar. Estas podrían verse como más objetivos a comprometer a través de vulnerabilidades.

Mejorar la protección de datos: los datos están en el corazón de cualquier ciudad inteligente y son fundamentales para llevar a cabo las operaciones diarias. Sin embargo, muchas carecen de los procesos adecuados para garantizar que esta información se gestiona de forma segura. Si una base

de datos no se controla correctamente, puede resultar fácil para los ciberdelincuentes atacarla y ponerla en peligro, con la consiguiente filtración o robo de datos confidenciales.

Conocer los riesgos de la cadena de suministro de las TIC y de los proveedores: Esto fue particularmente evidente durante la reciente vulnerabilidad de 'zero-day' encontrada en el software de transferencia de archivos MOVEit, que posteriormente fue explotada como parte de un ataque de ransomware a gran escala. Los atacantes siguen centrándose en los eslabones más débiles y, por lo tanto, atacar los sistemas de infraestructuras inteligentes está destinado a ser un objetivo lucrativo. Para combatirlo, es fundamental que se adopten prácticas seguras por diseño y por defecto.

Contar con la última tecnología: muchas ciudades tienen infraestructuras y redes construidas con tecnología obsoleta, lo que las hace susceptibles de sufrir ciberataques. Garantizar que los sistemas estén al día con las últimas actualizaciones de software y parches de seguridad es primordial. Este aspecto es fundamental para el éxito de cualquier ciudad inteligente y disponer de sistemas resistentes debe ser una prioridad.

Incrementar el grado de la seguridad: vinculado directamente a la tecnología obsoleta, contar con protocolos de seguridad ineficaces expone a las ciudades inteligentes a sufrir numerosas amenazas maliciosas. Esto deja a los ciudadanos y a las organizaciones a merced de filtraciones de datos, robos de identidad y pérdida de información sensible. Proteger la infraestructura existente con medidas de seguridad sólidas podría evitar una brecha potencialmente desastrosa.

"El mundo avanza a una velocidad que pocos pueden seguir y las ciudades no podían ser menos. Ahora que la tecnología está cada vez más presente en todas las actividades diarias de una gran urbe, es imprescindible implementar las medidas de ciberseguridad necesarias. Cuantos más dispositivos conectados estén en la red, mayores probabilidades de vulnerabilidad tendrá. Es imprescindible que el nivel de protección sea óptimo desde el principio, para que no se produzca ninguna brecha de seguridad", alerta Eusebio Nieva, director técnico de Check Point Software para España y Portugal.

Datos de contacto:
Everythink PR
Everythink PR
91 551 98 91

Nota de prensa publicada en: Madrid

Categorías: Nacional Sociedad Madrid Software Ciberseguridad Dispositivos móviles Sostenibilidad Urbanismo Arquitectura