PANORAMA 80/180
Boletín #39

Algunos retos de seguridad y privacidad de datos en IoT

Un mundo conectado trae numerosos retos para **garantizar que los dispositivos y sensores no se conviertan en una amenaza para los usuarios** ya que es de suma importancia almacenar todos los datos de forma segura y respetar la privacidad de las personas.

Dicho esto, un reciente estudio de Deloitte destaca los principales retos en materia de seguridad y privacidad, acá se mencionan algunos :

Autenticación débil: La mayoría de personas utiliza los dispositivos IoT con contraseñas débiles y una autenticación insuficiente. Por lo cual es clave reforzar estos mecanismos de autenticación.

Falta de gestión integral: Los proveedores de servicios de IoT tienen que cubrir todos los aspectos de la gestión de datos y el ciclo de vida de los dispositivos de IoT. Esto se debe a que los propietarios de los dispositivos IoT pueden no gestionar por completo el firmware, el sistema operativo y las aplicaciones de un dispositivo IoT.

Falta de notificaciones: Algunos dispositivos de IoT carecen de aplicaciones y/o interfaces humanas de usuario para la gestión de los dispositivos, lo que impide que las personas afectadas puedan dar un consentimiento significativo para el tratamiento de su información personal. Por lo tanto, es imprescindible mostrar más notificaciones.

Lorem ipsum dolor

Capacidad de cifrado limitada: Los protocolos de cifrado deben ser eficientes. El sistema también debe abordar la creciente complejidad del movimiento de datos a través del mundo del IoT integrado.

Interfaz web insegura: La gran mayoría de las soluciones basadas en IoT tienen una interfaz web/móvil para consumir datos recogidos y enviarlos a través de proveedores de servicios. En este caso, la interfaz web es más propensa a una mala gestión de credenciales débiles por defecto, y vulnerabilidades de scripting entre sitios y de secuencias de comandos en sitios cruzados.

Actualizaciones de seguridad periódicas y aumento de amenazas: Teniendo en cuenta el volumen y la naturaleza de la integración en el mundo del IoT, la actualización periódica de seguridad es un proceso complejo.

Problemas de portabilidad e interoperabilidad de los datos con el bloqueo de los proveedores: Debido a los problemas de interoperabilidad, los consumidores se enfrentan al riesgo de quedar atrapados con un proveedor de servicios de IoT específico, lo que puede dificultar la flexibilidad de la portabilidad de datos para los clientes finales.

Disponibilidad continua: La capacidad de las plataformas de IoT para defenderse incesantemente de ataques implacables y persistentes, como los de denegación de servicio (DOS), es insuficiente, ya que todo un ecosistema subyacente de sistemas dependientes puede verse afectado. Por lo tanto, es importante garantizar la disponibilidad y la continuidad en la prestación de los servicios de IoT para evitar posibles fallos e interrupciones operativas.

Derechos de los interesados: IoT utiliza datos recogidos de diferentes fuentes y objetos para identificar a las personas. En estos casos, la titularidad y el ejercicio de los derechos de los de los datos se convierten en un reto tanto para el responsable como para el procesador de datos.

Fuente: Deloitte. 2021. Internet of Things (IoT): The rise of the connected world. Disponible en https://www2.deloitte.com/content/dam/Deloitte/in/Documents/-technology-media-telecommunications/in-tmt-IoT_Theriseoftheconnectedworld-

DATO CURIOSO

"Se estiman 83.000 millones de conexiones IoT para 2024"
(Juniper Research, 2020)

Juniper Research informó que el número total de conexiones IoT alcanzará los 83.000 millones en el año 2024. Esta cifra es superior a los 35.000 millones de conexiones que se registraron en 2020. Y el sector industrial es el que liderará el camino.

FUENTE:

Juniper Research. 2020. IOT CONNECTIONS TO R
EACH 83 BILLION BY 2024, DRIVEN B
Y MATURING INDUSTRIAL USE CASES.
Disponible en https://www.juniperresearch.
com/press/iot-connections-to-
reach-83-bn-by-2024

Si desea publicar en el boletín o en la página web, envíe sus artículos a Alianza80180@ccit.org.co