BUENDÍA RODRÍGUEZ VALENTINA

EL LADO OSCURO DE LOS DISPOSITIVOS INTELIGENTES: CÓMO HACKER UN IOT PARA APRENDER A PROTEGERLO

La ponencia presentada por Aleida Pérez, CEO de Tech Consulting, exploró los desafíos de ciberseguridad en el Internet de las Cosas (IoT) y las estrategias para mitigar riesgos.

Se destacó el origen del concepto de IoT, atribuido a Kevin Ashton, y su expansión a más de 221.7 millones de hogares con dispositivos inteligentes. La charla abordó los principales tipos de IoT y su impacto en la ciberseguridad, clasificándolos en:

- **IoT doméstico**, que incluye dispositivos como cámaras y asistentes inteligentes.
- **Sistemas de Control Industrial (ICS)**, empleados en infraestructuras críticas.
- **Tecnología Operativa (OT)**, orientada al monitoreo y control en procesos industriales.
- **Internet de las Cosas Médicas (IoMT)**, que abarca dispositivos médicos conectados.

Estos sectores demandan medidas específicas para garantizar la **Smart Ciberseguridad**, la cual debe proteger información personal y financiera, prevenir la propagación de ataques (movimiento lateral) y fortalecer la base de ataque.

Se identificaron como los dispositivos IoT más vulnerables los puntos de acceso inalámbricos, cámaras IP, impresoras, enrutadores y sistemas de VoIP, debido a componentes como el firmware, microcontroladores, memoria y almacenamiento.

Entre las amenazas comunes en la ciberseguridad del IoT, se subrayaron:

- Configuraciones predeterminadas inadecuadas.
- Ausencia de rutas de actualización seguras.
- Uso de tecnología inapropiada.
- Errores del usuario final.
- Robo y manipulación de datos.
- Incumplimientos legales o regulatorios.

La ponente también presentó casos emblemáticos de hackeos, como los realizados a cámaras Ring, sistemas HVAC y rifles inteligentes TrackingPoint, enfatizando que todos comparten un vector de ataque que facilita el ingreso a los sistemas.

Finalmente, se resaltó la importancia de establecer estándares de seguridad para IoT que aborden estas vulnerabilidades y aseguren la protección de los dispositivos y los datos asociados.

Aunque no se mencionaron directamente en la ponencia, las siguientes disciplinas matemáticas son fundamentales para abordar los desafíos de ciberseguridad en el IoT:

- **Teoría de Grafos:** Para modelar redes de dispositivos IoT y analizar posibles puntos de vulnerabilidad.
- **Estadística:** Detección de patrones anómalos en el comportamiento de dispositivos.
- **Álgebra Lineal:** Procesamiento de datos y modelado de señales en dispositivos IoT.