ASIR 2024/2025

SAD

TAREA 0 - UT1

Realizado por:

Alejandro Abellán García

Información de ataques al Internet de las Cosas (IoT)

1. Explosiones de dispositivos electrónicos: Recientemente, se han reportado incidentes en los que dispositivos como busca y walkie-talkies han explotado. Se sospecha que estos incidentes fueron provocados intencionalmente para causar daño a los usuarios. Este tipo de ataques subraya la necesidad de mejorar la seguridad en los dispositivos IoT para prevenir manipulaciones maliciosas.

Causas:

- **Manipulación maliciosa**: Los dispositivos pueden ser alterados intencionalmente para causar daño físico.
- **Defectos de fabricación**: Problemas en el diseño o fabricación pueden llevar a fallos catastróficos.

Consecuencias:

- **Daño físico**: Riesgo de lesiones a los usuarios.
- **Pérdida de confianza**: Los consumidores pueden perder la confianza en la seguridad de los dispositivos IoT.

Impacto en la seguridad del IoT:

- **Necesidad de mejores controles de calidad**: Asegurar que los dispositivos sean seguros desde el punto de vista físico.
- **Implementación de medidas de seguridad**: Protección contra manipulaciones maliciosas.

2. Crecimiento de amenazas IoT: Un informe de Kaspersky ha revelado un aumento significativo en las amenazas dirigidas a dispositivos IoT. En los primeros seis meses de 2024, se identificaron más de 700 anuncios de servicios de ataques DDoS en la dark web. Esto indica que los dispositivos IoT son cada vez más objetivos de ciberataques, lo que resalta la importancia de implementar medidas de seguridad robustas.

Causas:

- **Aumento de dispositivos conectados**: Más dispositivos IoT en uso significa más objetivos potenciales.
- **Falta de seguridad**: Muchos dispositivos IoT tienen medidas de seguridad insuficientes.

Consecuencias:

- **Ataques DDoS**: Los dispositivos IoT pueden ser utilizados para lanzar ataques de denegación de servicio.
- **Robo de datos**: Los atacantes pueden acceder a información sensible a través de dispositivos IoT comprometidos.

Impacto en la seguridad del IoT:

- **Necesidad de medidas de seguridad robustas**: Implementar cifrado, autenticación y actualizaciones regulares.
- **Conciencia y educación**: Informar a los usuarios sobre la importancia de la seguridad en sus dispositivos IoT.

3. Obsolescencia y vulnerabilidades: Según ESET, más de 5.600 millones de dispositivos IoT podrían ser vulnerables a ciberataques en los próximos cinco años debido a la obsolescencia y la falta de actualizaciones de seguridad. Muchos dispositivos IoT no reciben actualizaciones regulares, lo que los deja expuestos a nuevas amenazas y vulnerabilidades.

Causas:

- **Falta de actualizaciones**: Muchos dispositivos IoT no reciben actualizaciones de seguridad regulares.
- **Obsolescencia programada**: Los dispositivos pueden volverse obsoletos rápidamente, dejando de recibir soporte.

Consecuencias:

- **Vulnerabilidades explotables**: Los dispositivos sin actualizaciones son más susceptibles a ataques.

- **Aumento del riesgo**: Un gran número de dispositivos vulnerables puede ser explotado en ataques masivos.

Impacto en la seguridad del IoT:

- **Políticas de actualización**: Necesidad de políticas que aseguren actualizaciones regulares y soporte a largo plazo.
- **Diseño seguro**: Crear dispositivos con seguridad integrada desde el diseño.