Ignacio Gabriel Bugueño Córdova

Consulta 4: ¿Qué aspecto(s) considera relevante(s) para ser tratado(s) en materia de ciberseguridad?

"Basado en el documento “Baseline Security Recommendations for IoT, in the context of Critical Information Infrastructures“. Table 3. pp 34. (2017). ENISA (The European Union Agency for Network and Information Security), se consideran como relevantes los siguientes aspectos en materia de Cyberseguridad, siendo descrita cada amenaza en cada una de las categorías correspondientes.

Categoría: Ataques/Abusos

-Malware: referido a programas informáticos diseñados para realizar acciones no deseadas y no autorizadas en un sistema sin el consentimiento del usuario.

-Secuencias de Exploit: código diseñado para aprovechar un punto vulnerable y acceder a un sistema. La detección de esta amenaza es difícil y en los entornos IoT puede tener distintos grados de impactos.

-Ataques dirigidos: ataques diseñados con un objetivo específico, lanzados durante un período de tiempo prolongado y llevados a cabo en numerosas fases. Su objetivo principal es permanecer ocultos para obtener la mayor cantidad de información/datos confidenciales.

-Denegación de Servicio Distribuido (DDoS): varios sistemas atacan un único objetivo para saturarlo y dejarlo inoperativo. Puede llevarse a cabo empleando varias conexiones, colapsando un canal de comunicación.

-Falsificación de dispositivos maliciosos: esta amenaza es difícil de detectar, puesto que resulta complicado diferencias un dispositivo falso de uno original. Estos dispositivos cuentan normarlmente backdoors que pueden emplearse para atacar otros sistemas TIC en el entorno.

-Ataques a la privacidad: estas amenazas afectan tanto a la privacidad del usuario como a la exposición de los elementos en red a personal no autorizado.

-Modificación de información: el objetivo es manipular la información para causar caos u obtener beneficios económicos.

Categoría: Eavesdropping/Intercepción/Secuestro

-Man in the middle: se trata de un ataque de intercepción activa en el que el atacante se posiciona en medio de la comunicación entre dos víctimas, haciéndolas creer que están hablando directamente entre sí.

-Secuestro de protocolo de comunicación IoT: toma del control de una sesión de comunicación existente entre dos elementos de la red. El intruso tiene acceso a información, incluyendo contraseñas.

-Intercepción de información: intercepción y modificación no autorizada de procesos de comunicación privada, como llamadas telefónicas, mensajería instantánea o correos electrónicos.

-Reconocimiento de red: obtención pasiva de información sobre la red: dispositivos conectados, protocolo empleado, puertos abiertos, servicios en uso, entre otros..

-Secuestro de sesión: robo de la conexión de datos actuando como host legítimo con el objetivo de robar, modificar o eliminar los datos transmitidos.

-Reproducción de mensajes: este ataque emplea una transmisión de datos válida de manera maliciosa, enviándolos repetidamente o retrasándolos, con el propósito de dejar inoperativo el dispositivo objetivo."

Consulta 5: ¿Qué condiciones específicas considera relevantes para la protección de IoT?

"Basado en el documento “Baseline Security Recommendations for IoT, in the context of Critical Information Infrastructures“. Table 3. pp 34. (2017). ENISA (The European Union Agency for Network and Information Security), se consideran como relevantes las siguientes amenazas a tener en consideración para la protección de IoT.

Categoría: Caídas

-Caídas de red: interrupción o fallo en el suministro de red, de manera intencionada o accidental. Dependiendo del segmento de la red afectado y del tiempo necesario para recuperar el servicio, la importancia de esta amenaza varía de alta a grave.

Activos afectados: infraestructura y comunicaciones.

-Fallos de dispositivos: amenaza de fallo o avería en los dispositivos de hardware.

Activos afectados: dispositivos IoT.

-Fallo del sistema: amenaza de fallo de los servicios o aplicaciones de software.

Activos afectados: dispositivos IoT, plataforma y backend, otros dispositivos del ecosistema IoT.

Categoría: Fallos/averías

-Vulnerabilidades del software: en términos generales, los dispositivos IoT tienden a ser vulnerables debido a contraseñas débiles seteadas por defecto, errores de software y errores de configuración, suponiendo un riesgo para la red. Esta amenaza suele estar vinculada con otras, como secuencias de exploit, y se considera una amenaza grave.

Activos afectados: dispositivos IoT, otros dispositivos del ecosistema IoT, plataforma y backend, infraestructura, aplicaciones y servicios.

-Fallos de terceros: errores en un elemento activo de la red ocasionados por una configuración no adecuada de un elemento que guarda relación directa con este.

Activos afectados: dispositivos IoT, otros dispositivos del ecosistema IoT, plataforma y backend, infraestructura, aplicaciones y servicios.

Categoría: Ataques físicos

-Modificación de dispositivos: manipulación de dispositivos, por ejemplo, mediante comunicaciones de puertos, aprovechando aquellos que quedan abiertos.

Activos afectados: comunicaciones, dispositivos IoT.

-Destrucción del dispositivo: sucesos como robo del dispositivo, ataques con explosivos, vandalismo o sabotaje, que puedan dañar el dispositivo.

Activos afectados: dispositivos IoT, otros dispositivos del ecosistema IoT, plataforma y backend, infraestructura."