Charla de Seguridad Digital para el Mundo Maker

"Entender los riesgos para protegerse sin paranoia"

[DrYouu]

Contents

1 Introducción: Tecnología y Seguridad en el Mundo Maker

Vivimos en una época fascinante para los makers: tenemos acceso a tecnologías que hace apenas unos años solo estaban en manos de gobiernos, laboratorios o grandes empresas. Podemos fabricar objetos, automatizar procesos, abrir puertas, crear redes de comunicación o incluso clonar dispositivos, todo con herramientas al alcance de cualquiera.

Pero esa accesibilidad también abre un nuevo frente de exposición: lo que podemos construir, otros también pueden explotarlo si no lo diseñamos con seguridad en mente.

El objetivo de esta charla es:

- Mostrar de forma práctica cómo herramientas como el Flipper Zero pueden ser utilizadas contra nosotros.
- Aprender a protegernos sin entrar en paranoia.
- Concienciar sobre los riesgos físicos derivados de vulnerabilidades digitales.
- Abordar la ética del hackeo y el uso responsable de herramientas de pentesting.

Además, lo haremos de forma participativa, con ejemplos escenificados y algunas pequeñas sorpresas prácticas sobre los asistentes.

2 El Flipper Zero: El Cuchillo Suizo del Pentesting Personal

2.1 ¿Qué es el Flipper Zero?

El Flipper Zero es un dispositivo multifunción diseñado inicialmente para investigadores de seguridad. Compacto, portable, versátil y muy intuitivo, ha ganado enorme popularidad tanto en entornos de pentesting como entre curiosos tecnológicos.

Permite interactuar con múltiples protocolos inalámbricos y electrónicos, muchos de ellos presentes en la vida cotidiana de cualquier ciudadano moderno.

2.2 Sus funciones principales incluyen:

- **Sub-GHz**: copiar y retransmitir señales de mandos a distancia de garajes, persianas, sistemas de alarma, etc.
- **RFID/NFC**: clonar tarjetas de acceso de edificios, oficinas, hoteles, gimnasios.
- **Infrarrojos (IR)**: controlar dispositivos electrónicos mediante señales de mando.
- **USB HID (BadUSB)**: simular un teclado o ratón al conectarlo a un ordenador.
- **GPIO**: interactuar directamente con hardware externo.
- **Bluetooth/BLE**: interactuar con dispositivos cercanos.

2.3 Desde el punto de vista de la víctima

Estas capacidades, usadas sin consentimiento, permiten:

- Interceptar y clonar dispositivos de acceso físico.
- Ejecutar comandos en dispositivos ajenos.
- Interferir en sistemas electrónicos sin contacto físico directo.

3 Escenificación 1: El Hotel Comprometido

Personajes

- **Víctima**: huésped en un hotel.
- **Atacante**: persona aparentemente amable en el vestíbulo.
- **Narrador**: introduce y explica la escena (puedes ser tú misma).

Guion escénico

Narrador:

Imaginemos una situación real que puede ocurrir en cualquier hotel. Nuestra víctima ha llegado al hotel y va a desayunar tranquilamente.

(La víctima se sienta en la mesa y deja su tarjeta RFID de la habitación en la mesa, junto al móvil.)

Narrador:

La tarjeta de acceso RFID está ahí, expuesta. Entra ahora el atacante. No necesita tocar nada. Solo pasa a escasos centímetros con un dispositivo similar a este (muestra el Flipper Zero) en modo de lectura de tarjetas.

(El atacante simula escanear con disimulo mientras pasa cerca.)

Narrador:

En segundos, ha copiado la tarjeta. Más tarde puede acercarse a la habitación cuando la víctima no esté y acceder sin dejar rastro de entrada forzada.

Mensaje clave

- Las tarjetas RFID de baja frecuencia (125 KHz) se copian fácilmente.
- Nadie sospecha de alguien que simplemente pasa cerca.
- Existen fundas protectoras baratas que bloquean este tipo de lectura.