Plan prezentacji

1. Wprowadzenie

- Czym są lokalne zagrożenia cyberbezpieczeństwa?
- Dlaczego są szczególnie istotne w codziennym życiu (biuro, dom, przestrzeń publiczna)?
- Cel prezentacji: podniesienie świadomości i przedstawienie realnych technik ataków

2. WiFi Sniffer

- Czym jest sniffing?
- Jakie dane mogą zostać przechwycone?
- Przykład: atak Man-in-the-Middle
- Legalne użycie vs. nadużycia
- Środki ochrony: VPN, silne szyfrowanie (WPA3), unikanie otwartych sieci

3. BadUSB

- Czym jest atak BadUSB?
- Jak wygląda atak z perspektywy użytkownika?
- Przykłady złośliwego działania (np. automatyczne wpisanie komend)
- Ochrona: blokowanie portów USB, fizyczna kontrola urządzeń, endpoint security

4. RFID/NFC

- Czym są systemy RFID/NFC i gdzie się je stosuje (np. karty miejskie, hotele, płatności)?
- Potencjalne zagrożenia: podsłuchiwanie, klonowanie, nieautoryzowany dostęp
- Przykład: atak na zamki hotelowe
- Zabezpieczenia: etui RFID, szyfrowanie komunikacji, ograniczenie zasięgu

5. Narzędzia ofensywne (Flipper Zero i inne)

- Czym są urządzenia haktywistyczne?
- Przykłady: Flipper Zero, HackRF One, Proxmark3, Ubertooth One
- Jakie ataki umożliwiają? (BadUSB, RFID emulacja, Bluetooth sniffing, piloty)
- Potencjalne ryzyka i zagrożenia
- Legalność i etyka użycia

6. Juice Jacking (Złośliwe ładowarki)

- Na czym polega atak Juice Jacking?
- Gdzie najczęściej się go spotyka (lotniska, centra handlowe)?
- Co może się stać po podłączeniu do publicznego portu USB?
- Jak się chronić? (power bank, tylko ładowanie, blokada danych USB)

7. Keyloggery sprzętowe

- Jak działają fizyczne keyloggery?
- Gdzie mogą być podłożone (komputery w bibliotece, w pracy)?
- Jak je rozpoznać i jak się chronić?
- Różnice między keyloggerem sprzętowym a programowym

8. Jak się chronić? (Zbiorcze podsumowanie)

- Silne hasła i uwierzytelnianie dwuskładnikowe
- Ograniczone zaufanie do publicznych portów, WiFi i urządzeń
- Stosowanie aktualizacji i oprogramowania zabezpieczającego
- Czujność wobec fizycznych manipulacji urządzeniami
- Edukacja i świadomość – najważniejsza obrona

9. Podsumowanie i źródła informacji

- Lokalne zagrożenia są realne i coraz bardziej zaawansowane
- Nowoczesne urządzenia mogą ułatwić ataki, ale też testować bezpieczeństwo
- Odpowiednia wiedza pozwala się skutecznie chronić
- Linki do wszystkich stron, które podałeś – uporządkowane tematycznie