Przykładowe tematy Prezentacji – Ataki na ICS/IoT

Poniżej przykładowe tematy prezentacji. Zachęcam również do znalezienia ciekawych case study dotyczących różnych ataków. Na Lab 6 proszę o przygotowanie krótkiej prezentacji 10-15min w grupach 1-3 osoby.

ICS (przemysł / OT)

- Stuxnet (Iran, 2010)
- BlackEnergy/KillDisk (Ukraina 2015)
- Industroyer/CrashOverride (Ukraina 2016)
- Industroyer2 (Ukraina 2022)
- TRITON/TRISIS (SIS/Triconex, 2017)
- PIPEDREAM/INCONTROLLER (framework na ICS, 2022)
- German Steel Mill (Niemcy, 2014)
- Colonial Pipeline (ransomware z wpływem na OT, 2021)
- Norsk Hydro / LockerGoga (2019)
- Oldsmar Water (USA, 2021)
- Unitronics PLC (wodociągi, 2023–2024)
- Iranian Khuzestan Steel (2022)
- Israeli Water Facilities (2020)
- Ransomware EKANS/SNAKE celujący w procesy ICS
- CODESYS runtime vulns - sterowniki PLC
- Schneider Modicon/Unity Pro case
- ICS w szpitalach: BMS/SCADA HVAC jako wektor ryzyka
- Itp.

IoT (konsumenckie / medyczne / automotive / BMS)

- Mirai / Hajime / Mozi / Reaper (IoT botnety)
- BrickerBot (permanentne „psucie” IoT)
- VPNFilter (SOHO routery/NAS)
- Verkada breach (kamery CCTV, 2021)
- Ring / Nest camera takeovers
- Jeep Cherokee (Uconnect, 2015)
- Tesla key-relay / BLE relays (różne lata)
- Ripple20 (stos TCP/IP Treck)
- URGENT/11 (VxWorks TCP/IP)
- AMNESIA:33 (stos TCP/IP w IoT)
- Kr00k / KRACK (Wi-Fi w IoT)
- Philips Hue/mostek Zigbee lateral movement
- Industrial IoT: MQTT brokerzy publicznie dostępne
- Smart building: KNX/BACnet/Modbus w BMS
- Medical IoT: Hospira infusion pumps
- Medtronic MiniMed insulin pumps (odwołania/alerty)
- St. Jude/Abbott pacemakers (komunikacja bezprzewodowa)
- Peloton API/telemetria użytkowników (privacy)
- SolarEdge/EV-chargers: ekspozycja interfejsów
- Itp.