DISPOSITIVI IOT NEL MIRINO DEI CYBER CRIMINALI

Salvatore Corvaglia
salvatore.corvaglia@sysup.it
www.sysup.it

SCENARIO ATTUALE

- L'utilizzo dei dispositivi IoT cresce a dismisura in tutti i settori, dalle smart home fino alle smart city passando dalle smart factory.
- Nel 2018 la spesa mondiale in dispositivi IoT è stata di circa 800Mld $ → nel 2022 circa 1000Mld $ → nel 2023 potrebbe superare i 1100Mld $.
- Una rivoluzione tecnologica in corso i cui ambiti di applicazione interessano:
  - Enti pubblici → smart building, smart city, monitoraggio a livello sanitario
  - Imprese → smart factory, agricoltura 4.0, FoodTech, smart logistic
  - Consumatori → smart home, smart tv, smartwatch, smart car, smartphone
- Dietro la parola smart ci sono loro!

UTILI, FACILI DA INSTALLARE E CONFIGURARE MA…

- sono innumerevoli i vantaggi e i benefici che derivano dall'utilizzo di questi dispositivi, l'innovazione si affaccia su tutti i settori: sanità, educazione, logistica, infrastrutture critiche.

Sono alla base di servizi importantissimi !

- potenti e semplici da usare, molti dispositivi IoT sono plug & play, vengono installati e configurati senza preoccuparsi tanto di chi potrebbe utilizzarli e come.
- un loro malfunzionamento/compromissione potrebbe "costare" molto caro.
- E' necessario adottare delle precauzioni e implementare delle misure di sicurezza adeguate per proteggerli costantemente.

IL CUORE DEI DISPOSITIVI

- Sono numerose le tecnologie e i protocolli che alimentano i vari dispositivi IoT, spesso dietro il loro funzionamento ci sono intere piattaforme cloud a supporto e che offrono svariati servizi.
- Protocolli IoT e modalità di comunicazione dei dispositivi IoT (su vari livelli) con la rete:
  - AMQP (Advanced Message Queuing Protocol) → interazione tra sistemi tramite messaggi standard su scala industriale
  - CoAP (Constrained Application Protocol) → per dispositivi con capacità limitata per la connessione
  - DDS (Data Distribution Service) → comunicazioni peer-to-peer per eseguire operazioni
  - MQTT (Message Queue Telemetry Transport) → per comunicazioni su connessioni a banda ridotta verso posizioni remote
  - BLE (Bluetooth Low Energy)
  - Ethernet
  - LTE (Long Term Evolution)
  - NFC (Near Field Communication)
  - RFID (Radio Frequency Identification)
  - Wi-Fi/802.11
  - ...

➡ Sotto il cofano si nascondono sistemi complessi.

PROBLEMI E CRITICITA'

- Scarsa sicurezza dei dispositivi. Molti di questi oggetti sono affetti da grosse vulnerabilità e criticità di sicurezza già allo stadio progettuale. I costruttori privi di qualsiasi standard e obbligo normativo (almeno prima dell'avvento dello standard *ETSI TS 103 645* sulla sicurezza dei prodotti IoT destinati ai consumatori rilasciato dall' European Telecommunications Standards Institute) hanno immesso sul mercato **enormi quantità di device vulnerabili**.
- Nella maggior parte dei casi i sistemi operativi su cui girano i dispositivi IoT non sono aggiornabili perché il produttore non ha previsto questa funzionalità → senza aggiornare il sistema operativo **non è possibile applicare patch di sicurezza e risolvere le vulnerabilità.**
- Molti dispositivi IoT sono visibili in internet in quanto collegati a degli indirizzi IP pubblici, non sono dotati di sistemi di protezione e scambiano dati in continuazione alcuni dei quali anche sensibili e senza applicare crittografia → **privacy a rischio!**
- Una buona parte delle organizzazioni non è in grado di stabilire quali e quanti dispositivi IoT sono presenti nella propria rete, tanto meno verificare l'integrità di questi → **impossibile proteggere qualcosa che non si può vedere.**
- …

LE CONSEGUENZE

- Secondo l'ultimo Nokia Threat Intelligence Report nel 2020 i dispositivi IoT costituiscono oltre il 30% dei dispositivi infetti rispetto al 15% circa del 2019.
- I cybercriminali sfruttano le debolezze dei dispositivi IoT per veicolari attacchi molto potenti ai danni di aziende, organizzazioni e enti pubblici; lo fanno perché gli introiti che derivano da questo tipo di attività illecite sono molto cospicui.
- Gli attacchi diventano sempre più sofisticati ed evoluti ma soprattutto diventano sempre più frequenti: nella prima metà del 2018, si sono verificati più di 120mila attacchi da varianti di malware, il triplo rispetto a quelli registrati nel 2017 e il trend ovviamente è in crescita.
- L'IoT è uno dei principali obiettivi dei criminali informatici per due motivi in particolare:
  - **Diffusione massiccia di questi dispositivi su scala mondiale**
  - **Scarsa consapevolezza da parte delle aziende dei rischi a essi collegati**

COME PROTEGGERSI

- Avere completa visibilità degli dispositivi IoT presenti nella rete aziendale.
- Identificare e classificare i dispositivi sulla base delle criticità presenti: firmware obsoleti, password deboli/default, vulnerabilità note.
- Monitorare e analizzare costantemente il comportamento, il traffico e gli accessi ai dispositivi IoT per individuare e bloccare tempestivamente operazioni anomale e attacchi malware mirati.
- Segmentare la rete aziendale secondo l'approccio Zero Trust, a cui applicare automaticamente (grazie all'intelligenza artificiale e il machine learning) le adeguate policy di sicurezza tramite strumenti semplici e totalmente integrati, con l'obiettivo di:
  - **blindare il comportamento dei device alle sole operazioni consentite e necessarie**
  - **ridurre sensibilmente la superficie di attacco e limitare il movimento laterale tra i dispositivi IoT e IT**
  - **consentire l'accesso alle risorse aziendali da parte dei dispositivi IoT con privilegi minimi**

GRAZIE PER L'ATTENZIONE

Salvatore Corvaglia
salvatore.corvaglia@sysup.it
www.sysup.it