Kyberbezpečnost v průmyslových zařízení (IoT a embedded)

Tomáš Martinec
tomas.martinec@metiosoftware.cz

METIO SOFTWARE


Medtronic
GEM III DR

Odolnost vůči hackování nedávno a dnes

- Ještě nedávno – Často ignorance
  - 2014 USA, výzkumníci snadno ovládli silniční infrastrukturu města; autority nepřipouští problém
  - 2015 USA, proveden prototypový útok ovlivňující řízení masy aut z internetu
- Dnes – Spíše akceptance problému a počátky systematického řešení
  - Jednotlivá odvětví začínají být regulována normami na kyberbezpečnost
    - ISO 27001, Common Criteria, IEC 62443, ETSI EN 303 645, mnoho dalších...
  - V ČR aplikován zákon o kybernetické bezpečnosti 181/2014
  - Významné zranitelnosti nicméně stále nijak vzácné
    - 2021 USA, Colonial Pipeline ransomware attack
    - 2020 www.root.cz, Inzulinová pumpa může být zranitelná bezdrátově

Proč bývá zabezpečení zanedbané?

1) Podfinancování nebo nevědomost
   - Veřejnost si nebývá ochotná připlatit za zabezpečení zařízení, které by se tak mohly i násobně zdražit.
   - Některé profesní domény, kde jsou nasazované embedded/IoT zařízení jsou obecně podfinancované a navyklé konkurovat nízkou cenou.
2) Nerozvinuté know-how
   - Pro mnoho výrobců zařízení je připojení k internetu zcela nová věc. Jejich zaměstnanci mají nízké know-how a povědomí o problematice kyberbezpečnosti.
3) Zvýšení komplexity managementu
   - Ve světle toho, že provoz firmy vyrábějící embedded/IoT zařízení bývá i bez řešení kyberbezpečnosti vysoce náročná úloha, tak se může management rozhodnout nově přidaný rozměr složitosti zcela vyignorovat.

Uvedení Metio Software s.r.o.

- Spin-off startup Sysgo s.r.o. dělající vývoj software na zakázku
- Aktuálně se profesionalizuje na služby ohledně kyberbezpečnosti embedded/IoT
  - Přehledové školení kyberbezpečnosti pro programátory a techniky

    „Školení určitě doporučuji, pomohlo mi získat úplně jiný pohled na věc - takový, o kterém jsem ani nevěděl, že existuje. Také mi pomohlo uspořádat si některé pojmy, naučil jsem se navrhovat bezpečnější hesla, dozvěděl jsem se o existenci nástrojů, které mi mohou být užitečné. Přeji ať neztrácíte elán do dalších školení.“

    Jan Konečný, RCD Radiokomunikace
  - Penetrační testování, Hardening embedded linuxu, …
  - Školení netechnických uživatelů (ve spolupráci s partnerskou firmou)

Prostor pro dotazy

Děkuji za pozornost

Tomáš Martinec
tomas.martinec@metiosoftware.cz