ezú elektrotechnický zkušební ústav

Kybernetická bezpečnost inteligentních budov. Znamená chytřejší svět také bezpečnější svět?

Bc. Michal Hager

Obsah

- Kybernetická bezpečnost inteligentních budov dnes
- Chytřejší svět = bezpečnější svět?
- Incidenty a hrozby
- V čem je zabezpečení inteligentních budov odlišné?
- Kdo je za bezpečnost inteligentních budov odpovědný?
- Jaké je řešení?
- Kybernetická bezpečnost inteligentních budov zítra

ezú elektrotechnický zkušební ústav

Kybernetická bezpečnost inteligentních budov dnes

- Pojem inteligentní budova
- Bariéry bránící většímu rozmachu inteligentních budov
- Soukromí a bezpečí
- Technologie jsou (téměř) připraveny
- Chybějící průmyslové standardy pro bezpečnost IoT zařízení

Chytřejší svět = bezpečnější svět?

- ANO
  - Ochrana před požárem
  - Kontrola vstupu (přístupu)
  - Programy umělé inteligence ochraňující obyvatele a jejich zdraví
  - Péče o seniory, péče o děti
  - Monitoring elektroinstalace a spotřeby (el. energie, vody…)
  - Dohled nad každým koutem budovy

Chytřejší svět = bezpečnější svět?

- NE
  - Špatně zabezpečené prvky infrastruktury
  - Problémy samotných výhod
    - HVAC
    - Systémy zabezpečení
    - Samotná chytrá zařízení
- Jaký je tedy závěr?

Incidenty a hrozby

- Tři hlavní cíle útočníků
- Zaznamenané incidenty
  - Napadení chytrých televizorů Samsung
  - Linuxový červ Darlloz
  - Zapojení televizorů, domácích směrovačů i ledničky do botnetu
  - Kompromitace bezpečnostního systému
  - Hacknutí připojených termostatů
- Další vektory možných útoků

V čem je zabezpečení inteligentních budov odlišné?

- Zařízení musí komunikovat jak přes Internet, tak i s dalšími zařízeními
- Zařízení nemají dostatečný výkon pro provádění šifrování
- Většina zařízení je ,,uzavřená“ a určená ke speciálním účelům, vyžadující tak specifický přístup k bezpečnosti
- V domácnosti není nikdo, kdo by bezpečnost spravoval
- Malé povědomí lidí o bezpečnosti inteligentních budov, IoT
- Stále se jedná o nepříliš probádanou oblast

Kdo je za bezpečnost inteligentních budov odpovědný?

- Role výrobce zařízení
- Role dodavatele OS
- Role dodavatele vestavěných zařízení (např. čipů)
- Role specializovaných bezpečnostních společností
- Role konečného uživatele
- Role poskytovatele síťových služeb
- Shrnutí

Jaké je řešení?

- Maximalizace bezpečnosti
- Analýza rizik
- Kvalitní a důvěryhodné prvky zabezpečení a jejich vhodná integrace
- Hardware řešení třetích stran
- Testování jednotlivých prvků a celé infrastruktury
- Proškolení samotných obyvatel objektu
- Zacházet s chytrými zařízeními jako s PC
- Prozatím nekupovat nezabezpečená zařízení

ezú elektrotechnický zkušební ústav

Kybernetická bezpečnost inteligentních budov zítra

- Předpovědi:
  - Gartner: 30 miliard zařízení
  - Cisco: 50 miliard zařízení
  - Morgan Stanley: 75 miliard zařízení
- Větší míra využití biometrie
- Úplně nový svět?

ezú elektrotechnický zkušební ústav

Děkuji za pozornost!