IoT zařízení (Internet of Things)

IoT zařízení jsou fyzické objekty vybavené senzory, softwarem a síťovou konektivitou, které jim umožňují sbírat a vyměňovat si data s jinými systémy přes internet nebo lokální síť. V naší firmě nám IoT pomáhá zvyšovat efektivitu provozu a komfort pracovního prostředí.

Kategorie IoT v naší firmě

Naše IoT ekosystémy dělíme do tří hlavních skupin podle jejich účelu:

1. Smart Office (Chytrá kancelář)

Slouží k optimalizaci pracovního prostředí a úspoře energií:

- **Chytré osvětlení a HVAC:** Automatická regulace světla a teploty na základě přítomnosti osob (protokoly Zigbee/WPAN).
- **Rezervační systémy:** Tablety u zasedacích místností propojené s firemním kalendářem přes **WLAN**.
- **Senzory kvality ovzduší:** Monitorování hladiny CO2 pro zajištění zdravého a produktivního prostředí.

2. Logistika a Asset Tracking

Sledování majetku a pohybu zboží v reálném čase:

- **RFID čtečky:** Automatizovaný příjem a výdej materiálu ze skladu bez nutnosti manuálního skenování.
- **GPS trackery:** Sledování polohy firemních vozidel a cenných zásilek přes **WAN**.
- **Smart Tagy:** Lokalizace sdíleného vybavení (např. projektory, měřicí přístroje) v rámci budovy.

3. Průmyslové IoT (IIoT)

Monitorování a správa technické infrastruktury:

- **Senzory v serverovně:** Sledování vlhkosti, teploty a úniku vody v rámci **správy infrastruktury**.
- **Smart Metery:** Měření spotřeby elektrické energie a vody pro potřeby reportingu udržitelnosti.

Síťová konektivita a protokoly

IoT zařízení využívají různé komunikační standardy podle nároků na dosah, spotřebu energie a datovou propustnost:

Technologie	Dosah	Využití
Wi-Fi (IoT-Net)	Střední	Kamery, interaktivní displeje, chytré spotřebiče.
Bluetooth / Zigbee	Krátký	Bezdrátové senzory, chytré žárovky, zámky.
LoRaWAN / Sigfox	Dlouhý	Venkovní senzory, monitorování parkovišť.
NB-IoT / LTE-M	Globální	Mobilní trackery využívající operátorské 4G/5G sítě.

Kybernetická bezpečnost IoT

IoT zařízení jsou často nejslabším článkem sítě, proto v rámci **kybernetické bezpečnosti** striktně dodržujeme:

- **Izolace (Segmentace):** Všechna IoT zařízení jsou uzavřena ve speciální VLAN (SSID: `IoT-Devices`) bez přístupu k citlivým datům v systémech Jira nebo HR portál.
- **Změna továrního nastavení:** Žádné zařízení nesmí být připojeno s výchozím heslem (např. admin/admin).
- **Pravidelné aktualizace:** Firmware všech IoT prvků je centrálně aktualizován pod dohledem **IT oddělení**.
- **Šifrování:** Data přenášená z IoT zařízení do cloudu musí být šifrována (TLS/SSL).

Integrace do firemních procesů

Data z IoT zařízení jsou integrována do našich stávajících workflow:

- **Automatický Alerting:** Pokud senzor detekuje kritickou teplotu v serverovně, automaticky se založí incident s vysokou prioritou v systému **Jira**.
- **Analytika:** Data o obsazenosti kanceláří se vizualizují v rámci reportů pro vedení firmy za účelem optimalizace nákladů na prostory.

> **Důležité upozornění:** Je přísně zakázáno připojovat do firemní sítě jakákoliv soukromá IoT zařízení (chytré konvice, osobní meteorologické stanice apod.) bez předchozího písemného schválení IT oddělením.

— **Související stránky:** ZIF, Kybernetická bezpečnost, WLAN, WPAN, IT Podpora, Jira, WAN

From:
https://serviceit.cz/ - **IT ENCYKLOPEDIE**

Permanent link:
https://serviceit.cz/doku.php?id=iot_zarizeni

Last update: **2026/01/01 16:01**