

Požadavky IT/OT pro dodávaná výrobní zařízení

Tato specifikace slouží jako minimální požadavky na stroje, technologické celky a výrobní zařízení z pohledu připojení do podnikové sítě a bezpečného provozu zařízení z pohledu IT/OT. Jakékoli odchylky od těchto požadavků musí být předem schváleny IT a OT oddělením společnosti

1. Správa IP adres a síťové připojení

- Každé zařízení musí používat IP adresy přidělené OT oddělením společnosti Magna
- Adresy budou přidělovány na veškerou IP komunikaci v rámci zařízení. Není tedy možné, že na zařízení bude nastavená adresa například 192.168.1.1.
- Pro přidělení adresního rozsahu bude dodavatel kontaktovat v moment návrhu konstrukce/elektro schéma zařízení vedoucího pracovníka OT Magna Liberec. Rozsah adres bude přidělen na základě počtu jednotlivých zařízení s dostatečnou rezervou
- Připojení k síti může být realizováno pouze prostřednictvím infrastruktury schválené IT/OT Magna
- Pro připojení zařízení do podnikové sítě Magna bude uvolněna jedna zásuvka RJ-45, která bude připravena v blízkosti do 5 m od zařízení. Fyzické propojení mezi zařízením a podnikovou sítí Magna bude realizováno v dohodnutý termín s OT oddělením
- Je výslovně zakázáno použití modemů, GSM modulů nebo Wi-Fi

2. Řízení přístupu a autentizace

- V případě, že zařízení nebo technologický celek vyžaduje ověřování uživatelů, musí být technická implementace předem schválena.
- Musí být dodržovány aktuální Magna zásady účtů a hesel. Výchozí hesla musí být před spuštěním zařízení do zkušebního provozu změněna na bezpečné hodnoty. Hesla musí splňovat aktuální Magna požadavky na délku a složitost hesla. Defaultní ROOT a ADMIN účty nesmí být používány pro obsluhu služeb nebo běžnou administraci

3. Fyzické zabezpečení síťových rozhraní

- Všechna síťová rozhraní (Ethernet, USB, sériové porty) musí být jasně označena a dokumentována
- Nevyužitá nebo nepovolená rozhraní musí být deaktivována
- V rozvaděči stroje musí být na DIN liště místo pro instalaci Cisco switche (rozměry: V x Š x H; 15,2cm x 11,2cm x 13,5cm)

4. Synchronizace času

- Pro synchronizaci času zařízení zapojených do počítačové sítě je vyžadován Network Time Protocol (NTP) s nastavením na Magna NTP servery

5. Bezpečná komunikace a síťová segmentace

- Stroje musí podporovat pouze standardní průmyslové protokoly (OPC UA, MQTT, Modbus TCP, Profinet apod.)
- Je vyžadována segmentace síťového provozu pro izolaci logických celků

6. Logování a monitorování

- Každé zařízení musí podporovat logování bezpečnostních událostí a možnost exportu do SIEM systému Claroty
- Neautorizované požadavky o přístupy a změny konfigurace musí být logovány a monitorovány

7. Aktualizace a správa softwaru

- Dodavatel musí zajistit pravidelné bezpečnostní aktualizace firmwaru a softwaru po dobu životnosti zařízení
- Jakékoli aktualizace musí být předem schváleny OT oddělením

8. Princip nejmenších oprávnění (Least Privilege)

- Každý uživatel a proces musí mít pouze minimální oprávnění nutné pro vykonání dané operace
- Správní a servisní přístupy musí být přísně kontrolovány

9. Odolnost proti neoprávněné manipulaci

- Zařízení musí podporovat Secure Boot a ochranu proti neoprávněné manipulaci s firmwarem.
- Konfigurační soubory a přihlašovací údaje nesmí být udržovány v nezašifrované podobě

10. Ochrana proti neautorizovanému vzdálenému přístupu

- Vzdálený přístup je povolen pouze přes schválené bezpečnostní mechanismy (VPN s víceúrovňovou autentizací) pomocí standardních Magna nástrojů.
- Připojení k internetu realizuje Magna. Jakékoliv přímé připojení k internetu je zakázáno.

11. Dodržování bezpečnostních standardů

- Zařízení musí splňovat požadavky aktuálně platných standardů
- Dodavatel musí dodat dokumentaci o splnění těchto standardů a bezpečnostních opatření.