

Veilige OT-toegang in een hypergeconnecteerde wereld

24 juni 2026, 15:02

Annanda Rath

Identiteits- en toegangsbeheer voor geconnecteerde industriële omgevingen

Industrie 4.0 transformeert de productiesector. Ze zorgt voor meer efficiëntie, betere prestaties en een sterker concurrentievermogen. Hoe meer machines en systemen met elkaar worden verbonden, hoe groter het risico op cyberbeveiligingsproblemen wordt. Moderne beveiligingsoplossingen worden door technische beperkingen vaak niet ondersteund op verouderde OT-apparaten. Veilige identificatie en toegangscontrole vormen daarom een essentiële beveiligingslaag. Nieuwe regelgeving, zoals NIS2 en de Cyber Resilience Act (CRA), maakt deze uitdaging nog urgenter.

Belangrijke onderdelen van veilig toegangsbeheer voor OT-systemen

Veilig OT-toegangsbeheer omvat verschillende, elkaar aanvullende maatregelen:

1. **Gecentraliseerde identiteitsdatabase:** een gecentraliseerde database koppelt identiteiten van mensen aan die van apparaten. Dat voorkomt dat onbeheerde, ongeautoriseerde apparaten en onbekende bedrijfsmiddelen op de fabrieksvloer verschijnen.
2. **Veilige toegang op afstand:** veilige bastionhosts en industriële gedomilitariseerde zones (iDMZ's) schermen OT-netwerken af van het openbare internet. Hierdoor kunnen technici op afstand onderhoudswerkzaamheden uitvoeren zonder het netwerk rechtstreeks bloot te stellen.
3. **Geavanceerde authenticatie:** aanvalbestendige multifactorauthenticatie (MFA) beveiligt zowel lokale als externe aanmeldingen. Dat is vooral belangrijk voor accounts waarmee kritieke besturingsopdrachten kunnen worden gegeven. Authenticatie op basis van certificaten kan extra bescherming bieden zonder de bedrijfscontinuïteit te verstoren.
4. **Beheer van geprivilegieerde toegang en minimale rechten:** toegangsgegevens moeten veilig worden beheerd. Sessies op afstand kunnen indien nodig worden gevolgd of opgenomen. Gebruikers krijgen alleen de rechten die nodig zijn om hun specifieke taken uit te voeren.
5. **Continue monitoring en controle:** continue monitoring houdt gebruikersactiviteiten bij en registreert configuratiewijzigingen. Regelmatige controles sporen inactieve accounts en buitensporige rechten op voordat ze veiligheidsrisico's veroorzaken.

6. **Zero Trust-architectuur:** een Zero Trust-aanpak is gebaseerd op het principe 'nooit vertrouwen, altijd controleren'. Elke sessie, gestart door een persoon of machine, moet worden geauthenticeerd en geautoriseerd voordat toegang wordt verleend.



Belangrijkste kenmerken van het demonstratieproject

Het door ons ontwikkelde toegangscontrolesysteem combineert deze technologieën en biedt geavanceerde beveiligingsmogelijkheden:

- **Veilige gebruikersidentificatie en toegangscontrole:** SSI maakt gedecentraliseerd identiteitsbeheer, door de gebruiker beheerde gegevens en privacybeschermende authenticatie mogelijk via selectieve openbaarmaking.
- **Betrouwbare registratie van toegangsgegevens:** blockchaintechnologie zorgt voor een manipulatiebestendige registratie van inloggebeurtenissen en garandeert goede traceerbaarheid.
- **Ondersteuning voor audits en naleving:** verifieerbare en onveranderlijke gegevens ondersteunen audits en helpen organisaties te voldoen aan de steeds veranderende regelgeving op het vlak van cyberbeveiliging.
- **Mogelijkheid tot offline authenticatie:** de oplossing ondersteunt veilige authenticatie, zelfs wanneer apparaten tijdelijk niet zijn aangesloten op IT- of OT-netwerken.

SecuWeb: oplossingen voor OT-beveiligingsuitdagingen

Binnen het [SecuWeb-project](#) pakken Sirris en zijn partners deze uitdagingen aan met praktijkgericht onderzoek en innovatie. Het project onderzoekt methoden, technologieën en procedures die veilige identificatie en toegangscontrole mogelijk maken voor gebruikers en operatoren in OT-omgevingen. Door opkomende technologieën zoals Self-Sovereign Identity (SSI), Solid en blockchain te combineren, ontwikkelde het projectteam een geavanceerd demonstratiemodel voor identiteitsbeheer en toegangscontrole.

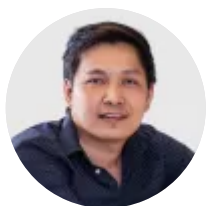
[Ontdek het SecuWeb-project](#)

Sluit u aan bij het SecuWeb-project als industriële partner

Wilt u innovatieve cyberbeveiligingsoplossingen verkennen in een industriële omgeving? Binnen het [SecuWeb-project](#) zijn we op zoek naar industriële partners om samen te werken aan praktijkgerichte use cases en nieuwe benaderingen voor identiteits- en toegangsbeheer in OT-omgevingen te valideren. Laten we uw uitdagingen bespreken en ontdekken hoe deze technologieën uw organisatie kunnen ondersteunen.

[Contacteer ons](#)

Auteurs



Annanda Rath