8 oplossingen voor veel voorkomende security risico's

Lees meer over:

- Hoe u industriële installaties tegen hackaanvallen of schadelijke software kunt beveiligen.
- Veel voorkomende security risico's en hun mogelijke beveiligingsmaatregelen.
- Technische én organisatorische security maatregelen.

PHOENIX CONTACT

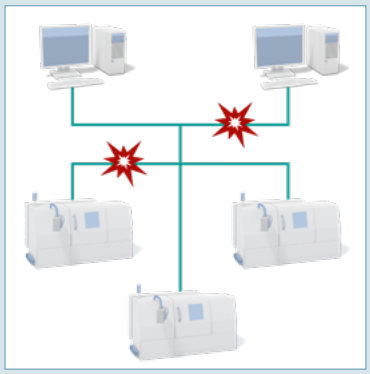
Een netwerkkoppeling biedt veel kansen, maar ook risico's

De voordelen van het koppelen van apparaten aan het netwerk zijn duidelijk. Maar door het steeds toenemende aantal netwerkkoppelingen en de daarmee gepaard gaande snelle samensmelting van IT en OT, ontstaan steeds meer potentiële aanvalsdoelen in bedrijfsnetwerken. Daarmee komen ook kritieke infrastructuren steeds vaker in het vizier van allerlei soorten cyberaanvallen.

De vraag is nu hoe we industriële installaties tegen hackaanvallen of schadelijke software kunnen beveiligen. Daarom volgen hieronder 8 veel voorkomende security risico's en hun mogelijke beveiligings-maatregelen.

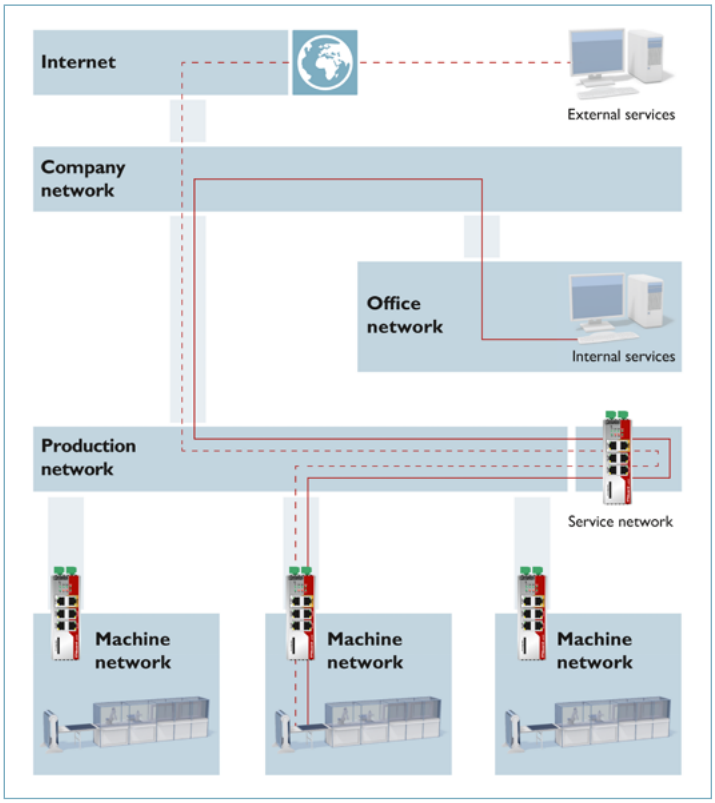
Inhoud

#1 Storingen veroorzaakt vanuit het kantoornetwerk



Risico: Storingen veroorzaakt vanuit het kantoornetwerk

Storingen en virussen, bijvoorbeeld uit de kantooromgeving, kunnen zich eenvoudig naar de productie verplaatsen.

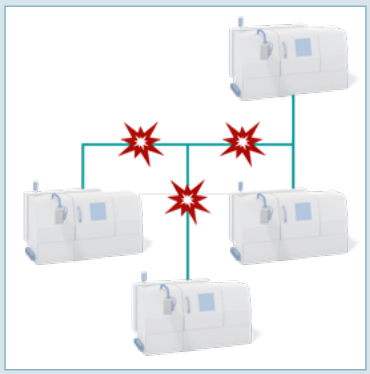


Network segmentation with mGuard security routers

Oplossing: Netwerksegmentatie

Door grote netwerken op te delen in kleine segmenten kan de data uitwisseling tussen de verschillende zones, bijvoorbeeld tussen productie en het kantoor of tussen verschillende systemen, beheerd worden. De afzonderlijke segmenten kunnen worden gerealiseerd met behulp van VLAN's of firewalls en voor de communicatie tussen de afzonderlijke netwerksegmenten moeten dan Routers of Layer 3-switches worden gebruikt. Hiermee voorkomen we dat typische netwerkfouten zich naar de rest van het netwerk verplaatsen.

#2 Kwaadaardige software

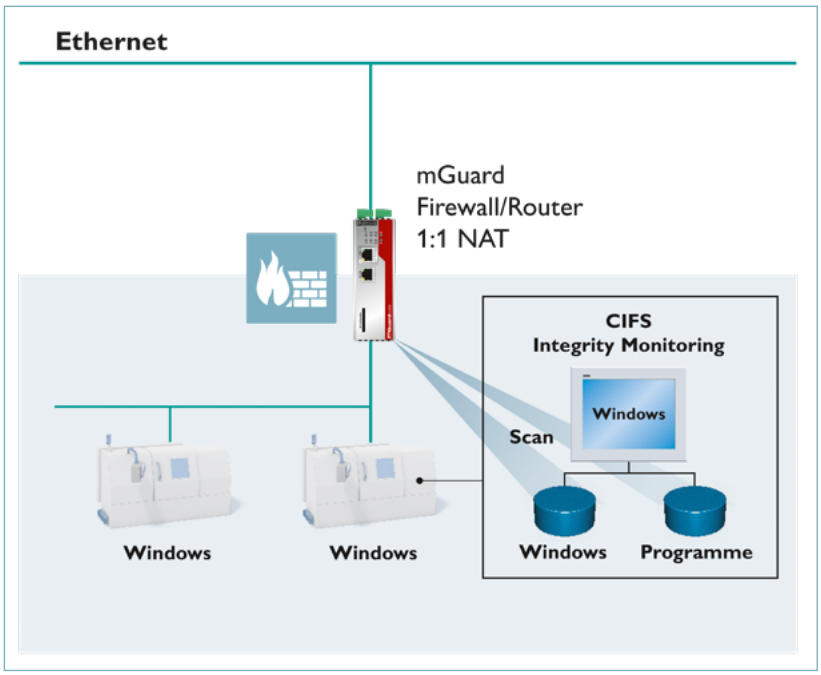


Risico: Kwaadaardige software

Kwaadaardige software is over het algemeen ontworpen om zich te verspreiden naar naburige systemen en deze ook te infecteren. Een voorbeeld hiervan is de WannaCry-malware die niet recentelijk gepatchte Windows-systemen infecteerde.

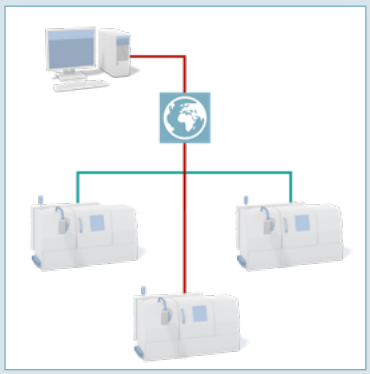
Oplossing: Communicatie beperken

De verspreiding van kwaadaardige software kan worden beperkt of voorkomen door firewalls te gebruiken. Als u alle communicatiemogelijkheden die technisch niet noodzakelijk zijn zou elimineren, zouden veel van deze aanvallen niet eens mogelijk zijn. Daarnaast helpt een industriële integriteitsbewaking (bv. CIM) u om wijzigingen en manipulaties van op Windows gebaseerde systemen, zoals besturingen, operator panels of pc's, tijdig te herkennen en in te dammen.



CIFS Integrity Monitoring

#3 Aanvallen van hackers

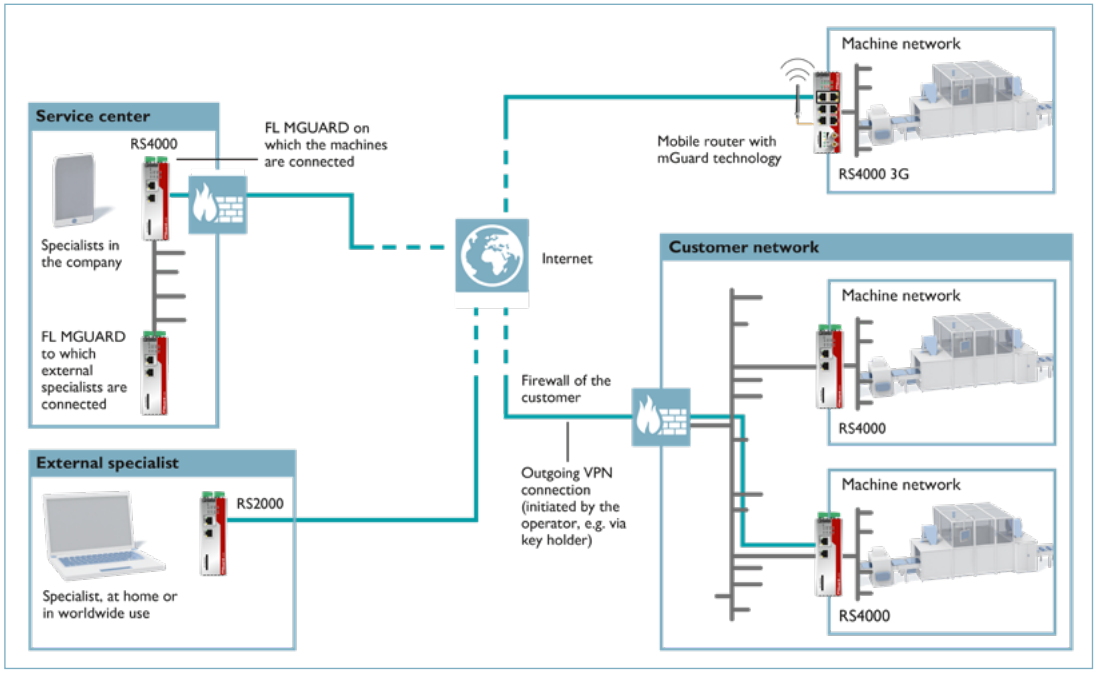


Risico: Aanvallen van hackers

Criminelen kunnen via een open internetverbinding data kopiëren of wijzigingen aan de installatie uitvoeren.

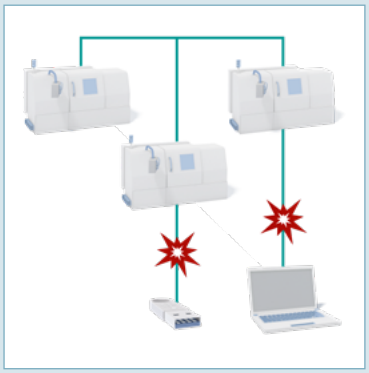
Oplossing: Versleutelde dataoverdracht

Het mag voor onbevoegden niet mogelijk zijn om via internet toegang te krijgen tot automatiseringssystemen. Dit kan worden gerealiseerd door gebruik van een firewall voor de internettoegang, welke al het inkomende verkeer en het uitgaande verkeer beperkt tot alleen de noodzakelijke, geautoriseerde verbindingen. Alle communicatie over een uitgestrekt gebied moet worden versleuteld, bijvoorbeeld via een Virtual Private Network met IPsec.



Secure remote maintenance with encrypted data transmission

#4 Geïnfecteerde hardware

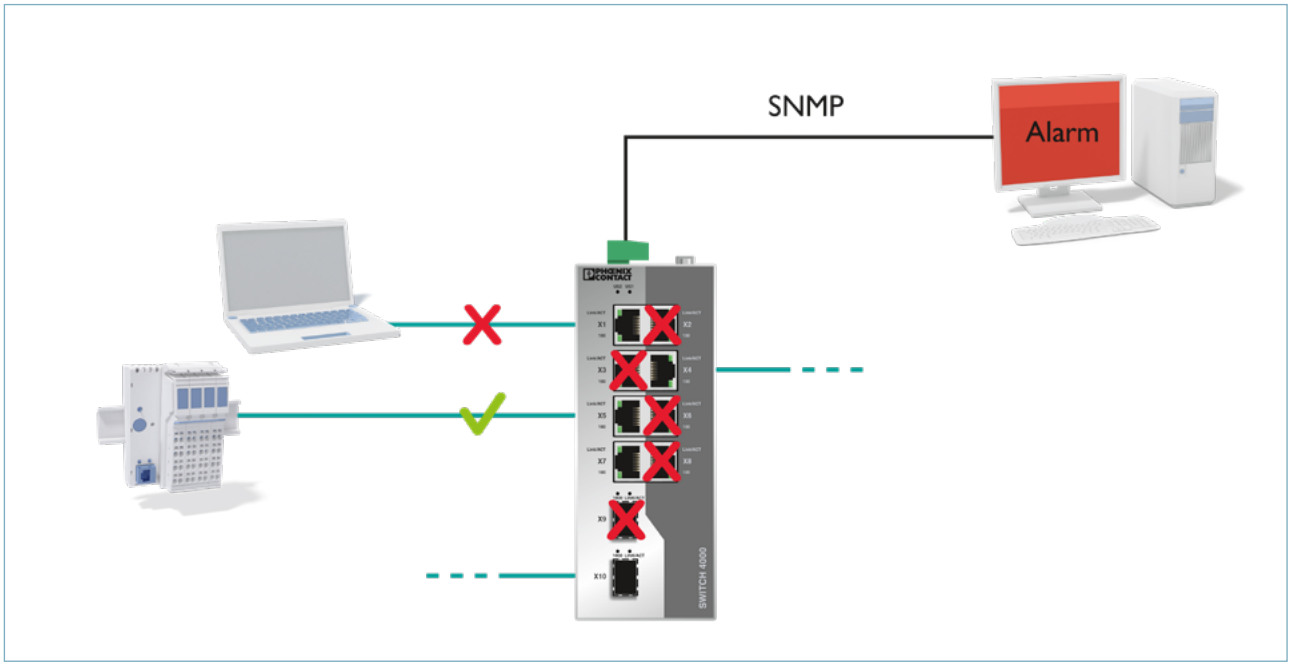


Risico: Geïnfecteerde hardware

Geïnfecteerde hardware, zoals USB-sticks of laptops, kunnen kwaadaardige software binnen het netwerk brengen.

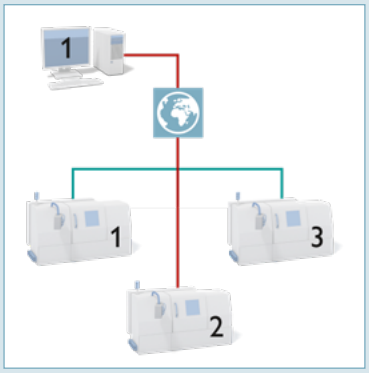
Oplossing: Ethernetpoorten beveiligen

Met de Port Security functie op managed switches kunt u instellen dat onbekende deelnemers geen data mogen uitwisselen met het netwerk. Ook moet u niet gebruikte ethernet poorten uit schakelen. Daarnaast bieden enkele managed switches de mogelijkheid om u via SNMP en meldcontacten te waarschuwen, wanneer zich een onbevoegd apparaat op het netwerk registreert.



Port disconnection and alerts via SNMP

#5 Onbevoegde toegang tot systemen



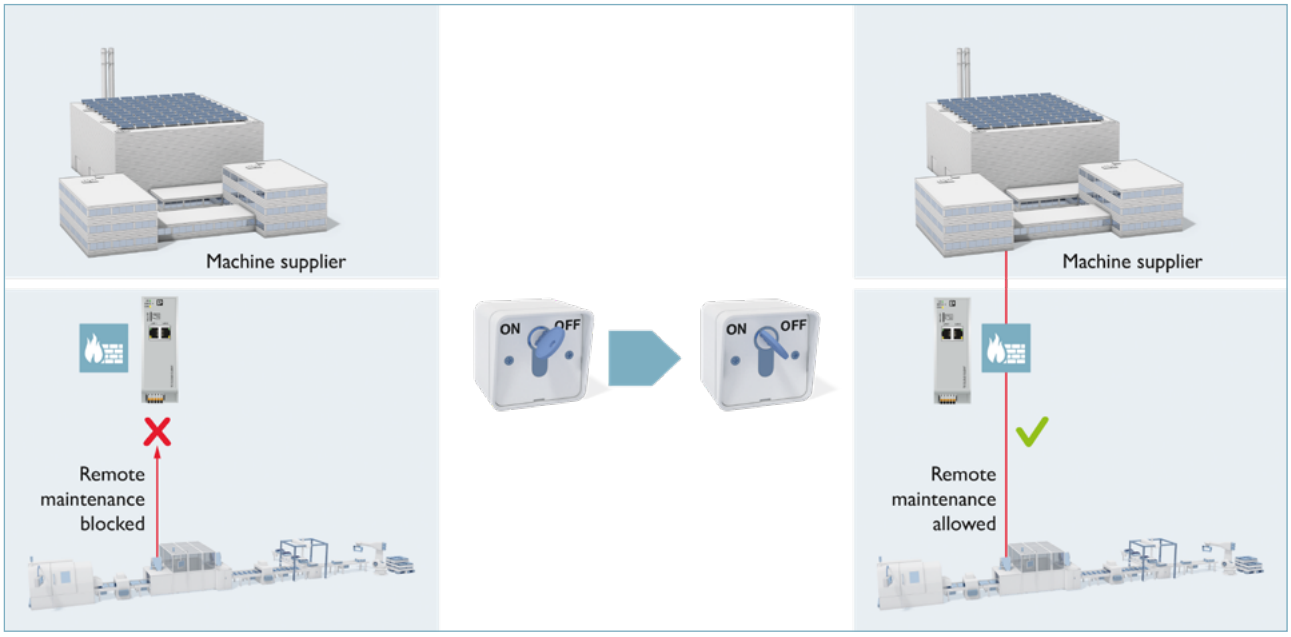
Risico: Onbevoegde toegang tot systemen

Er worden op afstand per ongeluk wijzigingen aangebracht in het verkeerde systeem.

Oplossing: Beveiligde toegang op afstand

Een beveiligde toegang op afstand tot een of meerdere machines kan met uiteenlopende, technologische oplossingen worden gerealiseerd. Enerzijds wordt de uitgaande communicatie versleuteld, bijv. door middel van IPsec of OpenVPN. Anderzijds kan via een sleutelschakelaar aan de machine het onderhoud op afstand worden geïnitieerd.

Zo wordt gewaarborgd dat aan de machine alleen wijzigingen worden doorgevoerd, wanneer dat ook werkelijk de bedoeling is. Tegelijkertijd maakt de sleutelschakelaar het mogelijk om bepaalde communicatie in het netwerk te blokkeren terwijl het onderhoud op afstand wordt uitgevoerd.



Controle of remote maintenance using a key switch

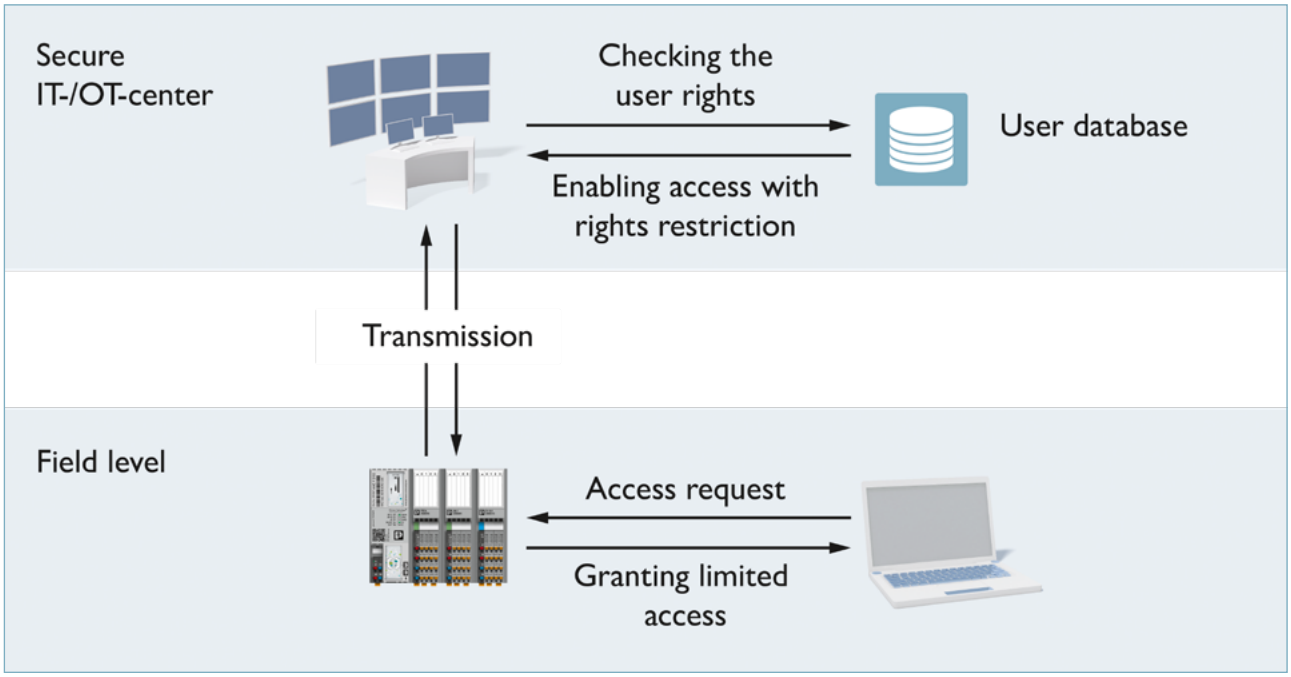
#6 Ontoereikend gebruikersbeheer

Risico: Ontoereikend gebruikersbeheer

Soms worden collectieve wachtwoorden gebruikt voor de toegang van gebruikers. Wanneer werknemers het bedrijf verlaten, worden deze wachtwoorden niet gewijzigd of wordt de toegang niet geblokkeerd. Het collectieve wachtwoord is dus bij veel gebruikers bekend en kan worden misbruikt.

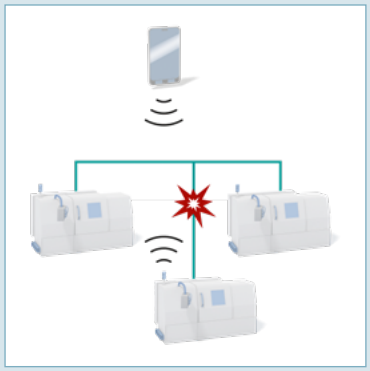
Oplossing: Centraal gebruikersbeheer

Dit probleem kan worden opgelost door centraal gebruikersbeheer, waarbij elke medewerker individuele toegangsrechten krijgt toegewezen. Veel apparaten van Phoenix Contact ondersteunen de integratie in centraal gebruikersbeheer.



Central user management with individual assignment of rights

#7 Draadloze apparatuur



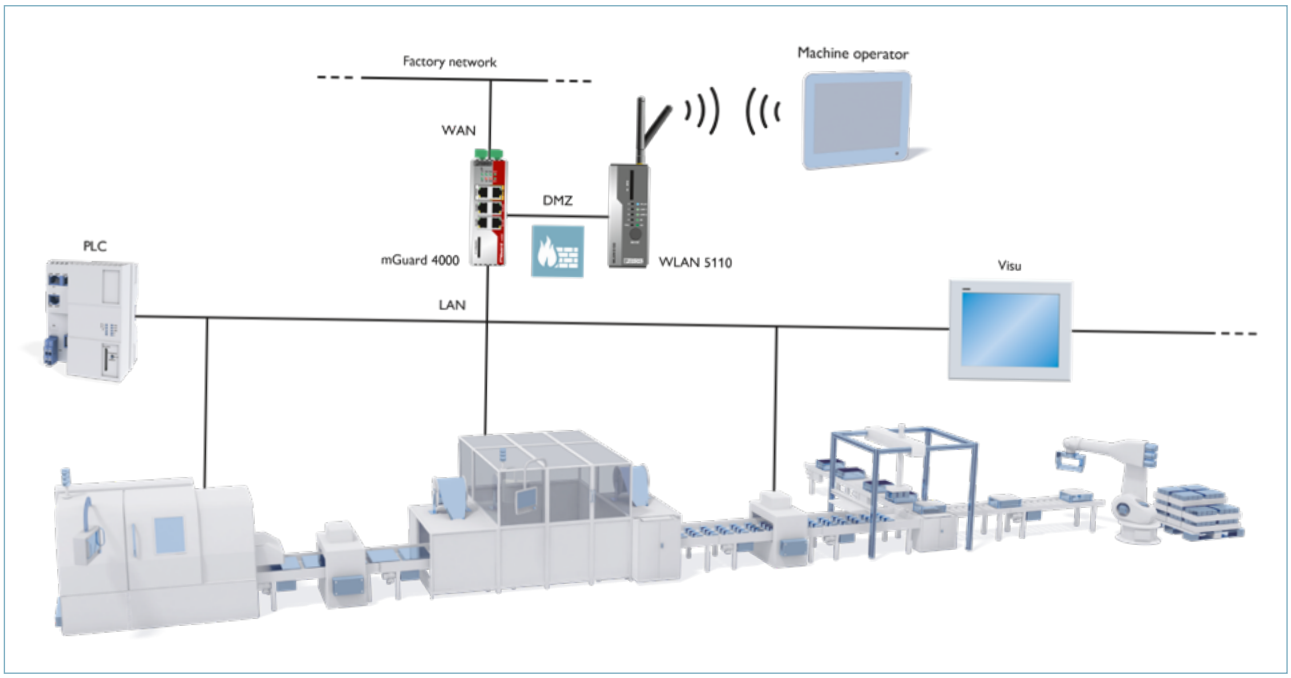
Risico: Draadloze apparatuur

Onbevoegde slimme apparaten maken zelf verbinding via WLAN.

Oplossing: Veilige WLAN-wachtwoordtoekenning

Wanneer WLAN-wachtwoorden bekend zijn en lange tijd niet zijn gewijzigd, maakt dit ook een ongecontroleerde toegang van derden mogelijk tot het netwerk. WLAN-componenten van Phoenix Contact maken daarom geautomatiseerd wachtwoordbeheer mogelijk via de machine-besturing (PLC). Zo kan een veilige WLAN-toegang in de vorm van eenmalige wachtwoorden, eenvoudig worden gerealiseerd.

Bovendien kan de WLAN-communicatie met een gedemilitariseerde zone (DMZ) worden beveiligd en zo van het resterende netwerk worden geïsoleerd.



Secure integration of mobile end devices with one-time passwords and DMZ

#8 Onjuiste of onveilige configuratie van het apparaat

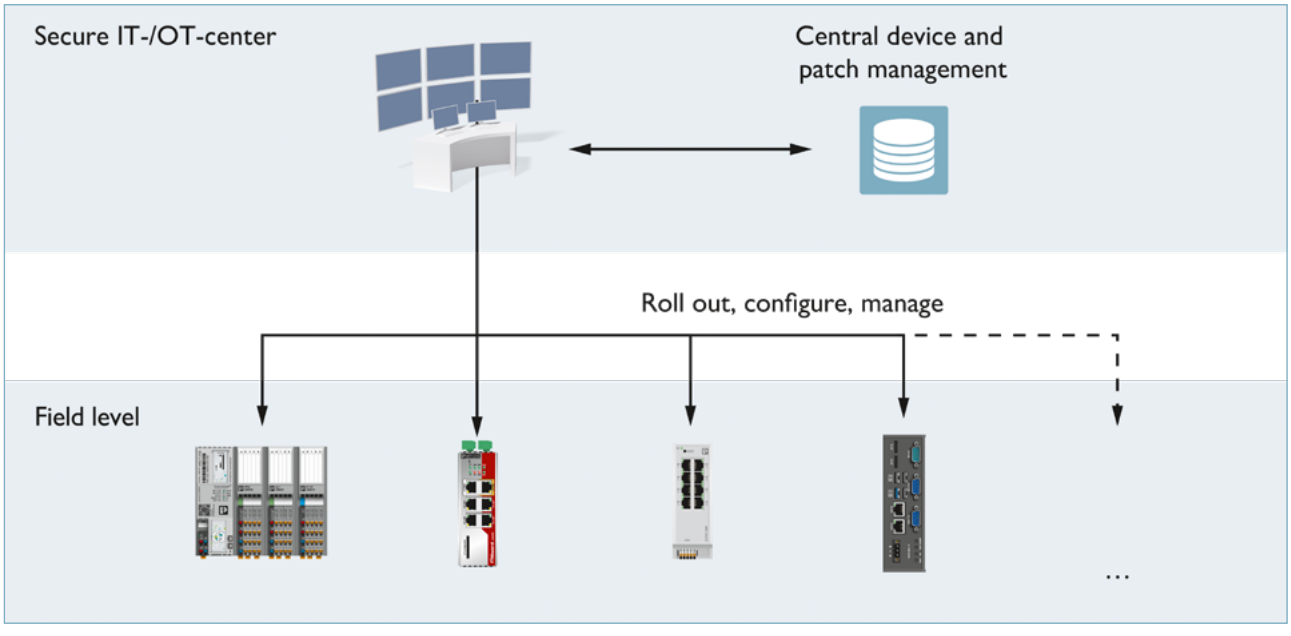
Risico: Onjuiste of onveilige configuratie van het apparaat

De standaardconfiguraties van apparaten zijn zo ontworpen dat ze gemakkelijk kunnen worden opgestart en correct functioneren. Beveiligingsmechanismen zijn hierbij soms van ondergeschikt belang.

Oplossing: Device and patch management

Als het gaat om het beheer van meerdere apparaten, kan intelligent en efficiënt 'device and patchmanagement' tijdrovende processen automatiseren en zo het risico van een onjuiste configuratie verminderen. Het biedt ondersteuning bij de configuratie, de uitrol en het beheer van apparaten en vermindert de risico's voor beveiliging en de naleving dankzij kortere patch- en upgradecycli.

Device and patch management maakt het mogelijk om alle beveiliging gerelateerde apparaatinstellingen centraal aan te maken en te beheren. Daarnaast biedt het ondersteuning voor firmware-upgrades.



Central patch and device management

Het gaat altijd om de combinatie van technische én organisatorische security maatregelen

Een goede beveiliging tegen cyberaanvallen is alleen succesvol wanneer op elkaar afgestemde technische én organisatorische maatregelen worden gecombineerd.

Daarom bieden wij u, behalve onze veilige producten, ook onze hulp aan zodat we er samen voor zorgen dat uw installaties en organisatie optimaal beveiligd zijn.

Onze experts helpen u graag met het oplossen van al uw Industrial Security vraagstukken.

→ Neem direct contact op voor een geheel vrijblijvende afspraak met een van onze specialisten.

CONTACT