Achtergrondinformatie

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern
Duitsland/Germany
www.pilz.com

16 mei 2024

Bescherming voor bedrijven, machines en producten

Safety en industrial security – alles van één leverancier

Ostfildern, 16 mei 2024 - **Security-incidenten komen niet meer alleen bij IT-systemen, maar steeds vaker ook in de productieomgeving (OT) voor. Gerichte aanvallen en ook onbewuste manipulatie worden beschouwd als incidenten op het gebied van industrial security. De taak van industrial security bij de productie is om de beschikbaarheid van machines en installaties alsmede de integriteit en vertrouwelijkheid van machinale gegevens en processen te garanderen. Per slot van rekening geldt: als bedrijven niet de baas over hun gegevens zijn, staan de toekomst van het bedrijf en de veiligheid van de medewerkers op het spel: zonder security geen safety en zonder safety geen bescherming van mensen!**

In de EU heeft de wetgever gereageerd op de toenemende dreiging: de **richtlijn voor netwerk- en informatiebeveiliging NIS 2** vereist dat bedrijven een informatiebeveiligingsbeheersysteem implementeren.

De **nieuwe Machineverordening 2023/1230** schrijft nu voor machines en installaties de bescherming tegen corruptie voor en verlangt security-maatregelen voor de onderdelen van de machine die invloed op de functionele veiligheid hebben.

De **Cyber Resilience Act (CRA)** vereist security-maatregelen voor producten met digitale elementen. Daartoe behoren ook besturingen, IO-systemen en andere componenten die in machines worden gebruikt.

Bedrijven, machines en producten – op elk niveau hebben machinefabrikanten en -exploitanten te maken met verschillende uitdagingen en verschillende wettelijke kaders.

Ongeacht of de wetgever industrial security verplicht stelt, is er een aantal goede redenen om in een vroeg stadium met dit onderwerp aan slag te gaan en advies in te winnen. Veel processen en omstandigheden voor de werking van machines werken namelijk manipulatie in de hand en moeten dringend worden onderzocht en veranderd. Een lange levensduur van machines betekent bijvoorbeeld vaak dat de bijbehorende systemen verouderd raken en op een gegeven moment niet meer aan de huidige security-normen voldoen. Deze systemen hebben beveiligingslekken die niet meer kunnen worden gedicht, omdat de aanbieder geen security-updates meer levert. Ook kan de beveiliging tegen schadelijke software vaak niet op de eindapparaten worden geïmplementeerd, omdat deze soms te oud zijn en hun performance daardoor zou verslechteren met als gevolg dat er productieonderbrekingen kunnen optreden.

Uitgebreid dienstenaanbod van Pilz

Uiteindelijk gaat het erom dat de bedrijfsvoering beschermd blijft, maar daarvoor moeten bedrijven verschillende uitdagingen overwinnen: van het identificeren van de geldende wettelijke voorschriften, het detecteren en elimineren van zwakke plekken in systemen en het bewust maken en trainen van de medewerkers tot de aansluitende implementatie van controles. Aangezien security een "bewegend" doel is, moet bovendien de status van de industrial security van de machines regelmatig worden gecontroleerd.

Het automatiseringsbedrijf Pilz heeft zich ingesteld op deze eisen en voor machinefabrikanten en gebruikers een internationaal dienstenaanbod samengesteld dat alle aspecten voor de

bescherming van mens en machine omvat. Het aanbod varieert van fundamentele informatie en oriënterende hulpmiddelen tot trainingen en de Industrial Security Consulting Service (ISCS), waarbij concrete projecten worden uitgevoerd.

Met de training tot "CESA – Certified Expert for Security in Automation" biedt Pilz al sinds vorig jaar een tweedaagse experttraining aan, waarin de deelnemers compacte security-kennis volgens de huidige normen wordt bijgebracht. Bovendien worden er praktische risicobeperkende maatregelen, zoals toegangscontrole en het verbeteren van de netwerkbeveiliging met technische middelen, alsmede organisatorische maatregelen voor het verminderen van security-risico's behandeld. Als de deelnemers slagen voor het examen, ontvangen ze het wereldwijd erkende TÜV NORD-certificaat "CESA - Certified Expert for Security in Automation".

Met de nieuwe dienst Industrial Security Consulting Service (ISCS) breidt Pilz de veiligheidsbenadering van machines uit tot een holistische benadering van safety en security. Pilz heeft deze dienst op basis van de beproefde methoden voor diensten op het gebied van functionele machineveiligheid en op basis van de security-normenreeks IEC 62443 ontwikkeld. Nadat bedrijven gebruik hebben gemaakt van deze dienst, zijn ze goed uitgerust wat betreft industrial security en voldoen ze aan de huidige wettelijke voorschriften.

Vier modules voor meer industrial security

ISCS bestaat uit vier modules: analyse van de beschermingsbehoeften, industrial security-risicobeoordeling, industrial security-concept en industrial security-systeemverificatie.

Bij de analyse van de beschermingsbehoeften bepalen de experts van Pilz in het bedrijf de beschermingsbehoefte van de afzonderlijke

"assets" in de machine of installatie alsmede hun beschermingsdoelen. In de tweede stap, de risicobeoordeling, worden alle risico's en de waarschijnlijkheid van optreden beoordeeld en dit gebeurt voor elk deel gedurende de complete levenscyclus van het systeem. Aansluitend praten de experts van Pilz met de klant over oplossingen voor het beperken van de geïdentificeerde risico's en over mogelijke gevaren.

In de derde stap stellen de experts van Pilz een industrial security-concept op, met strategieën en maatregelen voor het afwenden en verminderen van risico's als gevolg van aanvallen, manipulatie en verkeerde bediening. Ook worden er policies, regels en richtlijnen voor de verdere veilige werking of opbouw van het systeem opgesteld. In de laatste stap, de industrial security-systeemverificatie, wordt de effectiviteit van de geïmplementeerde tegenmaatregelen gecontroleerd.

Machinebeschikbaarheid waarborgen

De Industrial Security Consulting Service helpt om cyberaanvallen te verminderen of te voorkomen. Ook het aantal onbedoeld veroorzaakte security-incidenten neemt af. Dit verhoogt de machinebeschikbaarheid en zorgt uiteindelijk voor kostenbesparing en het behoud van de rentabiliteit.

De ISCS zorgt er vooral voor dat mensen op de machine door middel van passende security-maatregelen zijn beschermd. Een security-incident kan namelijk een belemmering voor safety-maatregelen vormen. Zo zorgt een lichtscherm voor machines er bijvoorbeeld voor dat de operator niet een gevarenzone instapt. Als een hacker echter de bijbehorende besturing en het mechanisme kan beïnvloeden, kan de beschermende functie van het lichtscherm niet meer worden gegarandeerd. Security beveiligt safety!

Machinefabrikanten en gebruikers krijgen zo van Pilz een dienstenaanbod dat rekening houdt met alle aspecten van de bescherming van mens en machine.

Bij de concrete toepassing op de machine is een gemeenschappelijke benadering van safety en security dus zinvol. Want zonder security geen safety en zonder safety geen bescherming van mensen.

Duidelijk geregeld: wie mag wat doen op de machine?

De veiligheid van een machine en haar operators staat of valt met het regelen van de toegang – voor mensen of netwerken. Ingangen moeten worden beveiligd tegen onbevoegde toegang, zodat er bijvoorbeeld tijdens de werking van de machine geen personen in de gevarenzone aanwezig zijn. Als een geautoriseerde machineoperator zich voor onderhoudsdoeleinden in deze gevarenzone bevindt, moet ervoor worden gezorgd dat niemand anders tegelijkertijd toegang tot de machine krijgt. Want zelfs het goedbedoeld bedienen of onderhouden van een machine – ter plekke of via een netwerk – zou anders fatale gevolgen kunnen hebben.

Een belangrijke bouwsteen is het Identification and Access Management (I.A.M.), dat rechten en de toegang op machines en installaties in bedrijven duidelijk regelt. Daartoe behoren organisatorische maatregelen en voorschriften alsmede geschikte veiligheidsfuncties. Een toegangsautorisatiesysteem zoals dat PITreader van Pilz is daarbij de juiste productbouwsteen. Hiermee kunnen gebruikers voldoen aan de eisen op het gebied van werknemersbescherming, aansprakelijkheidsbescherming, maximale productiviteit en de bescherming van uw gegevens.

Met het bedrijfsmoduskeuze- en toegangsautorisatiesysteem PITmode fusion biedt Pilz de functioneel veilige bedrijfsmoduskeuze

en de regeling van de toegangsrechten op machines en installaties aan. Elke operator krijgt op een RFID-gecodeerde transponder de toegangsrechten tot de machine die bij zijn verantwoordelijkheden en kwalificaties passen. De installatie kan dus enkel door geautoriseerde personen in gedefinieerde bedrijfsmodi worden bediend en bestuurd. Op deze manier is er sprake van een hoge mate van bescherming tegen onbedoelde acties en manipulatie.

Als het bedrijfsmoduskeuze- en toegangsautorisatiesysteem wordt aangevuld met de componenten van een modulair heksysteem, ontstaat er een samenhangend toegangsconcept tot de machine – met het oog op safety en security.

De beste hekbeveiliging heeft geen zin als gegevens, knowhow en operationele processen onvoldoende tegen onbevoegde toegang en manipulatie zijn beveiligd en een hacker het besturingssysteem kan binnendringen.

Industriële firewall biedt beveiliging tegen toegang van buitenaf

De industriële firewall SecurityBridge van Pilz heeft als taak om automatiseringsnetwerken tegen toegang van buitenaf te beveiligen. Hij bewaakt het dataverkeer tussen pc en besturing en verkleint zo het aanvalsoppervlak voor aanvallen door hackers en manipulatie. SecurityBridge beveiligt niet alleen besturingen van Pilz tegen manipulatie, maar ook besturingen van andere leveranciers.

Pilz is ervan overtuigd dat alleen een holistische benadering van safety en security een uitgebreide bescherming van mens en machine kan garanderen. Of en in welke mate een bedrijf zich met security wil bezighouden, is niet langer iets dat het bedrijf naar eigen inzicht kan bepalen. Het is inmiddels wettelijk voorgeschreven. In de machinebouw is security in de vorm van industrial security niet alleen

de taak van de IT, maar een integraal onderdeel van het ontwerp en de constructie. Het achteraf implementeren van security is omslachtig en betekent meestal een verlies aan gebruiksvriendelijkheid, functionaliteit en productiviteit.

((tekens: 10.173))

((Kader:))

Een overzicht van de EU-wetgeving op het gebied van industrial security:

vooral in Europa reageert de wetgever met een aantal wetten op de dreiging. Hierdoor gelden in Europa de strengste voorschriften ter wereld. Maar er vindt al afstemming met andere landen plaats en ook daar zullen dergelijke wetten er komen. Er valt dus een wereldwijde harmonisatie op het gebied van industrial security te verwachten.

NIS 2: meer plichten voor bedrijven

NIS (Network and Information Security) is een richtlijn van de Europese Unie voor het versterken van de cyberveiligheid. Deze richtlijn is al sinds 2016 van kracht en gold tot nu toe voor aanbieders van kritieke infrastructuren, waaronder in de sectoren energie, verkeer, bankwezen en financiën, gezondheid, drinkwatervoorziening en -distributie en digitale infrastructuur. Aanbieders in deze sectoren moesten met het oog op security "passende veiligheidsmaatregelen" treffen en ernstige cyberveiligheidsincidenten melden. De nieuwe Netwerk- en Informatiebeveiligingsrichtlijn 2 EU 2022/2555 (NIS 2) verplicht in de toekomst aanzienlijk meer bedrijven om risicobeheersmaatregelen voor de cyberveiligheid te treffen. NIS 2

breidt de sectoren uit met bijvoorbeeld de producerende industrie, waaronder ook machinebouw en fabrikanten van elektrische apparatuur.

Risicoanalyses en veiligheidsconcepten voor informatiesystemen, de bescherming van de toeleveringsketen en de veiligheid van het personeel worden vereist. Ook concepten voor de toegangscontrole en het beheer van installaties horen erbij, evenals verplichte trainingen voor het management.

De richtlijn werd eind 2022 aangenomen door het Europees Parlement en de Raad van de EU. Zoals alle EU-richtlijnen is ook NIS 2 niet onmiddellijk van kracht en bindend in de afzonderlijke EU-lidstaten, maar moet deze richtlijn door de lidstaten worden omgezet in nationaal recht. De EU-lidstaten moeten de richtlijn voor 18 oktober 2024 omzetten in nationaal recht. Bedrijven doen er goed aan om zo snel mogelijk met NIS 2 aan de slag te gaan en een uitgebreide security-beoordeling voor het bedrijf uit te voeren. Daartoe behoort bijvoorbeeld het opzetten van een beheersysteem voor informatiebeveiliging (ISMS). In deze context is een certificering volgens de informatiebeveiligingsnorm ISO 27001 nuttig.

NIS 2 aan de hand van het voorbeeld van windturbines: met NIS 2 moeten in de toekomst ook machinefabrikanten, zoals een fabrikant van installaties voor stroomopwekking (bijvoorbeeld windturbines), aan de voorschriften voldoen. De fabrikant van de windturbine heeft bijvoorbeeld automatiseringsoplossingen, besturingen of sensoren nodig. Vanaf een bepaalde omvang vallen ook fabrikanten van elektrische componenten onder NIS 2. En aangezien NIS 2 ook voorschrijft dat er rekening moet worden gehouden met leveranciers, moet ook een bedrijf zoals Pilz zich om veilige toeleveringsketens

bekommeren en eisen aan zijn leveranciers stellen. NIS 2 bestrijkt dus de volledige toeleveringsketen.

De nieuwe Machineverordening: zonder security geen CE-markering

De Machinerichtlijn 2006/42/EG speelt een belangrijke rol in het kader van de functionele veiligheid.

Machinefabrikanten moeten van oudsher een passende conformiteitsbeoordelingsprocedure, eindigend met de CE-markering, doorlopen om machines in Europa te kunnen invoeren.

De in juni 2023 opnieuw als Machineverordening gepubliceerde voorschriften zijn op de huidige stand van de techniek gebracht. Aangezien het om een verordening gaat, hoeft deze niet eerst in nationaal recht te worden omgezet. Machinefabrikanten hebben tot 20 januari 2027 de tijd om over te stappen op de nieuwe eisen en hieraan te voldoen.

De Machineverordening vervangt de huidige Machinerichtlijn en stelt, in tegenstelling tot haar voorganger, cybersecurity verplicht. Waar de Machinerichtlijn uitsluitend betrekking had op de safety, is in de Machineverordening ook het beschermingsdoel security opgenomen onder "Protection against corruption" in de "Essential Health and Safety Requirements (EHSR)": de veiligheidsfuncties van een machine mogen niet worden beïnvloed door onopzettelijke of opzettelijke vervalsing.

Deze nieuwe weg naar de CE-markering werpt een aantal nieuwe vragen voor machinefabrikanten en -operators op, omdat ze hun bestaande veiligheidsconcepten voor safety en security zullen moeten herzien.

Cyber Resilience Act: security gedurende de gehele productlevenscyclus

Naast het beoordelen van het bedrijf en de machines is ook het direct implementeren van security-maatregelen in de apparaten (zoals besturingen) absoluut noodzakelijk. In september 2022 presenteerde de Europese Commissie een ontwerp van een verordening die de cyberveiligheid van producten moet vergroten. Deze Cyber Resilience Act (CRA) is gericht op fabrikanten van producten met digitale elementen (hard- en software) die met andere producten kunnen communiceren. Het gaat om producten uit zowel de B2C-sector, zoals smartphones of robotstofzuigers, als de B2B-sector, zoals besturingen en sensoren, maar ook op om pure softwareproducten zoals besturingssystemen of de machine zelf.

Hoe groot de impact van de CRA daadwerkelijk zal zijn, hangt af van welke criteria er uiteindelijk worden toegepast voor het classificeren van de producten. Volgens de CRA mogen er alleen nog maar producten op de markt worden gebracht die een passend cyberveiligheidsniveau garanderen – en wel gedurende de gehele levenscyclus van een product. Security begint dus bij de productontwikkeling. Pilz stemt zijn ontwikkelingsprocessen daarom sinds enkele jaren ook af op de IEC 62443-4-1 "Veiligheid voor industriële controle- en automatiseringssystemen – Deel 4-1: Lifecycle vereisten voor ontwikkeling van veilige producten" en heeft bijvoorbeeld de SecurityBridge aantoonbaar "secure" ontwikkeld.

((tekens: 5.826))

Afbeeldingen

Afb. 1

Grafik_aus_Prospekt_Schulungen_mit_Pilz_3c_ppt

Safety en security van één leverancier: Pilz heeft een uitgebreid oplossingsaanbod met diensten en producten voor industrial security op de machine.

Copyright: Pilz GmbH & Co. KG

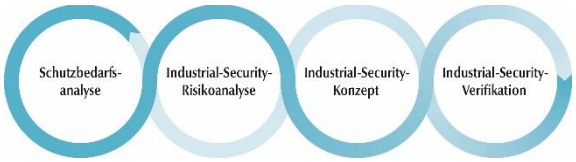
Afb. 2:

F_Services_ISCS_two_men_tablet_in_discussion_get1150297892_cold1_v0

Pilz lanceert dienst Industrial Security Consulting Service en helpt bedrijven om hun machines en installaties secure te maken.

Afb. 3:

G_Cycle_Industrial_Security_de_v0



De dienst Industrial Security Consulting Service van Pilz bestaat uit vier modules: analyse van de beschermingsbehoeften, industrial security-risicobeoordeling, industrial security-concept en industrial security-systeemverificatie.

Afb. 4:

F_Press_IAM_Man_using_PITreader_Key_Get1169337234_Get1169337153_cold1_v2

Een uitgebreid Identification and Access Management regelt de toegang tot de toepassing en garandeert zo de integriteit van

veiligheidsfuncties en -maatregelen – inclusief safety en industrial security.

Afb. 5:

F_security_robot_man_virtual_world_Fot208731449_cold1_2019_06_v2

Industrial security is de bescherming van productie- en industriële installaties tegen opzettelijke of onbedoelde fouten. Het doel is om de beschikbaarheid van machines en installaties alsmede de integriteit en vertrouwelijkheid van machinale gegevens en processen te garanderen.

Pilz – The spirit of safety

Pilz is een mondiale aanbieder van producten, systemen en diensten voor de automatiseringstechniek. Als pionier op het gebied van veilige automatisering creëert Pilz veiligheid voor mens, machine en milieu. Het in 1948 opgerichte familiebedrijf met hoofdkantoor in Ostfildern heeft op dit moment wereldwijd 2500 medewerkers in 42 dochterondernemingen en vestigingen in dienst.

De technologieleider biedt complete automatiseringsoplossingen voor safety en industrial security op de machine aan. Deze omvatten sensoren alsmede besturings- en aandrijftechniek – inclusief systemen voor de industriële communicatie, diagnose en visualisering. Een internationaal dienstenaanbod bestaande uit advies, engineering en trainingen completeert het portfolio. Oplossingen van Pilz worden niet

alleen in de machine- en installatiebouw, maar ook in heel veel andere branches zoals de intralogistiek, verpakkingsindustrie, spoorwegtechniek en robotica gebruikt.

www.pilz.com

Pilz op sociale netwerken:

Op onze socialmediakanalen geven wij achtergrondinformatie over het bedrijf en de mensen bij Pilz en brengen wij nieuws op het gebied van automatiseringstechniek.

www.pilz.com/facebook
www.pilz.com/X
www.pilz.com/xing
www.pilz.com/youtube
www.pilz.com/linkedin

Contactpersoon voor de pers:

Martin Kurth
Bedrijfs- en vakpers
Tel: +49 711 3409-158
m.kurth@pilz.de

Sabine Karrer
Vak- en bedrijfspers
Tel: +49 711 3409-7009
s.skaletz-karrer@pilz.de

Eva Rössle
Vakpers
Tel: +49 711 3409-7147
e.roessle@pilz.de

Hansjörg Sperling-Wohlgemuth
Congres- en presentatiemanagement
Tel: +49 711 3409-239
h.sperling@pilz.de