Bakgrundsinformation

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

16 maj 2024

Skydd för företag, maskiner och produkter

Safety & Industrial security – allt från ett och samma ställe

Ostfildern, 16 maj 2024 – **Det är inte längre bara IT-system som är föremål för security-incidenter, utan allt oftare även produktionsmiljön (OT). Till incidenter inom industrial security hör inte bara avsiktliga angrepp utan även omedveten manipulation. Uppgiften för industrial security i produktionen är att garantera tillgänglighet för maskiner och anläggningar samt integritet och sekretess för maskinella data och processer. Slutligen gäller följande: När företag inte har kontroll över sina data står företaget och medarbetarnas säkerhet på spel: Utan security finns ingen safety, och utan safety finns inget skydd för människor!**

Inom EU har lagstiftarna reagerat på det växande hotläget: På företagsnivå kräver **direktivet för nätverks- och informationssäkerhet (NIS 2)** enhetligt att ett system för hantering av informationssäkerhet implementeras.

Den **nya maskinförordningen 2023/1230** skyddar maskiner och anläggningar mot korruption, och kräver säkerhetsåtgärder för maskindelarna med avseende på funktionssäkerheten.

Cyber Resilience Act (CRA) kräver säkerhetsåtgärder för produkter som har digitala komponenter. Dit räknas bland annat styrningar, IO-system och andra komponenter som används i maskiner.

Företag, maskiner och produkter – På varje nivå finns olika utmaningar och olika rättsliga ramförhållanden för maskintillverkare och maskinoperatörer.

Oavsett om lagstiftaren gör industrial security obligatoriskt eller inte finns det flera bra anledningar att sätta sig in i ämnet i ett tidigt skede och få rådgivning. Flera processer och förutsättningar för att driva maskiner främjar nämligen manipulation, och därför är det viktigt att de undersöks och förändras. Till exempel leder en längre livslängd för maskiner ofta till att de tillhörande systemen åldras och till sist inte längre uppfyller gällande standarder för security. Dessa system har säkerhetsluckor som inte längre går att stänga eftersom leverantören inte längre tillhandahåller några säkerhetsuppdateringar. Skydd mot skadlig programvara kan ofta inte heller implementeras i slutenheterna eftersom de delvis är för gamla och prestandan skulle bli lidande, vilket skulle kunna leda till driftstopp i produktionen.

Omfattande tjänsteutbud från Pilz

Till sist handlar det om att affärsverksamheten förblir skyddad, men då måste företag hantera olika utmaningar: Det handlar om allt från att identifiera vilka rättsliga föreskrifter som gäller, upptäcka och åtgärda svaga punkter i system och skapa medvetenhet hos och utbilda de anställda till att implementera kontroller efteråt. Eftersom security är ett ”rörligt” mål är det dessutom nödvändigt med regelbunden kontroll av maskinens industrial security-status.

Automationsföretaget Pilz har anpassat sig efter de här kraven och tagit fram ett tjänsteutbud för maskintillverkare och operatörer över hela världen som tar med alla aspekter för skydd av människa och maskin i beräkningen på ett enhetligt sätt. Utbudet sträcker sig från grundläggande information, översikter och utbildningar till Industrial

Security Consulting Service (ISCS) där konkreta projekt implementeras.

Med kvalificeringen ”CESA – Certified Expert for Security in Automation” erbjuder Pilz sedan förra året en tvådagars expertkurs som ger deltagarna heltäckande security-kunskap baserat på aktuella standarder. Dessutom tar utbildningen upp praktiska åtgärder för riskreducering, t.ex. åtkomstkontroll, ökad nätverkssäkerhet med tekniska medel samt organisatoriska åtgärder för att minska security-risker. Efter att deltagarna har klarat provet får de det internationellt erkända TÜV NORD-certifikatet som ”CESA – Certified Expert for Security in Automation”.

Med det nya tjänsteutbudet Industrial Security Consulting Service (ISCS) utökar Pilz den säkerhetstekniska granskningen av maskiner till en helhetssyn på safety och security. Baserat på den beprövade metoden för tjänster inom funktionell maskinsäkerhet och standardserien för security, IEC 62443, har Pilz utvecklat sitt tjänsteutbud, och när detta implementeras är företag väl rustade när det gäller industrial security och uppfyller de aktuella lagkraven.

Fyra moduler för mer industrial security

ISCS består av följande fyra moduler: Skyddsbehovsanalys, industrial security-riskbedömning, industrial security-koncept och industrial security-systemverifiering.

Vid skyddsbehovsanalysen fastställer experterna från Pilz för företaget vilket skyddsbehov de enskilda ”tillgångarna” i maskinen eller anläggningen har samt deras skyddsmål. I det andra steget, riskbedömningen, tas alla risker och deras sannolikhet med i beräkningen, och detta görs för alla delområden i hela systemets livscykel. I anslutning till det diskuterar experterna från Pilz förslag till

lösningar för att minska de upptäckta riskerna och eventuella faror tillsammans med kunden.

I det tredje steget skapar experterna från Pilz ett industrial security-koncept med strategier och åtgärder för skydd mot och minskning av risker som sker genom attacker, manipulation eller felanvändning. Dessutom tar experterna fram policyer, regler och direktiv för att systemet ska kunna fortsätta drivas eller struktureras på ett säkert sätt. I det sista steget, industrial security-systemverifieringen, kontrolleras effektiviteten hos de genomförda motåtgärderna.

Säkra maskintillgängligheten

Industrial Security Consulting Service hjälper till att mildra eller förhindra cyberattacker. Antalet oavsiktligt utlösta security-incidenter sjunker också. Detta i sin tur ökar maskintillgängligheten, och i slutändan sparar det kostnader och bevarar lönsamheten.

Framför allt ser ISCS till att människor skyddas vid maskiner genom rätt security-åtgärder. En security-incident kan bli ett hinder för safety-åtgärder. Till exempel ser en ljusridå på en maskin till att operatören inte går in i ett riskområde. Om en angripare däremot tar över den motsvarande styrningen och mekanismen kan ljusridåernas skyddsfunktion inte längre garanteras. Security skyddar safety!

Maskintillverkare och operatörer får ett tjänsteutbud från Pilz som tar med alla aspekter för skydd av människa och maskin i beräkningen.

Vid konkret implementering på maskinen är det alltså vettigt att betrakta safety och security gemensamt. För utan security får vi ingen safety, och utan safety skyddas inte människorna!

Reglerat utan tvekan: Vem får göra vad på maskinen?

Säkerheten för en maskin och en operatör står och faller med regleringen av ingångarna – oavsett om det är för människan eller nätverket. Ingångar måste säkras mot obehörig åtkomst så att t.ex. inga personer befinner sig i riskområdet under driften. Om en behörig maskinoperatör befinner sig i riskområdet i underhållssyfte måste man kunna garantera att inga andra personer kommer åt anläggningen samtidigt. Även användning och underhåll av en anläggning som sker med välmening – oavsett på plats eller via ett nätverk – kan få allvarliga konsekvenser.

En viktig komponent är Identification and Access Management (I.A.M.), som tydligt reglerar behörigheter och åtkomster till maskiner och anläggningar hos företag. Dit hör organisatoriska åtgärder och riktlinjer samt lämpliga säkerhetsfunktioner. Ett åtkomstbehörighetssystem som PITreader från Pilz är en lämplig produktkomponent. Med det kan operatörer hantera kraven angående skydd för medarbetare, ansvarsskydd, maximal produktivitet samt dataskydd.

Med driftlägesväljar- och åtkomstbehörighetssystemet PITmode fusion erbjuder Pilz funktionssäkert driftlägesval och reglering av åtkomstbehörighet för maskiner och anläggningar. Med en RFID-kodad transponder frigörs maskinerna för varje operatör motsvarande deras egna ansvarsområden och kvalifikationer. Anläggningen kan alltså endast användas och styras av behöriga personer i definierade driftlägen. På så sätt får man en hög nivå av skydd mot oavsiktliga åtgärder och manipulation.

När driftlägesväljar- och åtkomstbehörighetssystemet utökas med komponenterna i ett modulärt skyddsgrindssystem uppstår ett enhetligt åtkomstkoncept för maskiner ur safety- och security-synvinkel.

Den bästa skyddsgrindssäkringen hjälper inte om data, kunskaper och drift inte är tillräckligt säkrade mot obehörig åtkomst och manipulation och en angripare kan tränga in i styrsystemet.

Industribrandvägg skyddar mot åtkomst utifrån

Industribrandväggen SecurityBridge från Pilz har till uppgift att säkra automationsnätverk från åtkomst utifrån. Den övervakar datatrafiken mellan datorn och styrningen och minskar på så sätt angreppsytan för hackerangrepp och manipulation. SecurityBridge skyddar inte bara Pilz-styrningar från manipulation, utan även styrningar från andra leverantörer.

Pilz är övertygade om att endast en helhetssyn på safety och security kan säkerställa ett omfattande skydd av människa och maskin. Om och i vilken utsträckning ett företag vill ägna sig åt security är inte längre en bedömningsfråga för företaget. Vid det här laget är det ett lagkrav. Inom maskintillverkning är security i form av industrial security inte bara en uppgift för IT, utan en integrerad beståndsdel i skisseringen och konstruktionen. Att implementera security i efterhand är alltid kostsamt och innebär oftast förluster i användarvänlighet, funktionalitet och produktivitet.

((Tecken: 10 173))

((Ruta:))

Överblick över EU-lagstiftning om industrial security:

Särskilt i Europa har lagstiftare reagerat på hotläget med en rad lagar. Därmed gäller världens strängaste riktlinjer i Europa. Men samordningen med andra länder är redan igång, och liknande lagar

kommer att träda i kraft även där. Vi kan därför förvänta oss en global harmonisering av industrial security.

NIS 2: Fler skyldigheter för företag

NIS (nätverks- och informationssäkerhet) är ett EU-direktiv för att stärka cybersäkerheten. Direktivet har funnits sedan 2016 men har hittills gällt för leverantörer inom kritisk infrastruktur, bland annat energi, transport, bank och finans, hälsa, dricksvattenförsörjning och digital infrastruktur. Leverantörer inom dessa sektorer har varit tvungna att vidta ”rimliga säkerhetsåtgärder” med avseende på säkerhet och rapportera allvarliga cybersäkerhetsincidenter. Det nya direktivet för nätverks- och informationssäkerhet 2 EU 2022/2555 (NIS 2) gör det till ett framtida krav för betydligt fler företag att vidta riskhanteringsåtgärder för cybersäkerhet. NIS 2 utökar sektorerna till t.ex. tillverkande/producerande verksamhet, bland annat maskintillverkning och tillverkare av elektrisk utrustning.

Det krävs riskanalyser och säkerhetskoncept för informationssystem, skydd för leveranskedjor och säkerhet för personalen. Hit räknas också koncept för åtkomstkontroll och hantering av anläggningar samt obligatoriska utbildningar inom hantering.

Direktivet antogs i slutet av 2022 i EU genom Europaparlamentet och rådet. Precis som alla EU-direktiv är inte heller NIS 2 omedelbart gällande och obligatoriskt i de enskilda medlemsländerna utan måste införlivas i nationell lagstiftning. Senast den 18 oktober 2024 måste EU-medlemsländerna föra över direktivet till sin nationella lagstiftning. Det är bra om företag tar itu med NIS 2 så snart som möjligt och genomför en omfattande security-bedömning för företaget. Dit hör t.ex. strukturen hos hanteringssystem för informationssäkerhet (ISMS). I det här sammanhanget kan en certifiering enligt informationssäkerhetsstandarden SS-EN ISO/IEC 27001.

NIS 2 i exemplet vindkraftverk: Med NIS 2 kommer även maskintillverkare, som t.ex. tillverkare av elproduktionsanläggningar (t.ex. vindkraftverk), att behöva uppfylla riktlinjerna i framtiden. Tillverkaren av vindkraftverket behöver i sin tur t.ex. automationslösningar, styrningar eller sensorer. Över en viss storlek omfattas även tillverkare av elektriska komponenter av NIS 2. Och eftersom NIS 2 också ställer krav på att leverantörer ska beaktas måste ett företag som Pilz också tänka på säkra leveranskedjor och ställa krav på sina leverantörer. NIS 2 täcker alltså hela leveranskedjan.

Den nya maskinförordningen: Utan security, ingen CE-märkning

Inom ramarna för funktionell maskinsäkerhet har maskindirektivet 2006/42/EG en särskild betydelse.

För att kunna importera maskiner till Europa har maskintillverkare alltid varit tvungna att gå igenom ett motsvarande förfarande för bedömning av överensstämmelse som avslutas med CE-märkning.

När den publicerades på nytt som maskinförordning i juni 2023 uppdaterades riktlinjerna till dagens tekniska nivå. Eftersom det är en förordning behöver den inte införlivas i nationell lagstiftning. Maskintillverkare har fram till 20 januari 2027 på sig att anpassa sig efter de nya kraven och uppfylla dem på brytdatumet.

Maskinförordningen ersätter det tidigare maskindirektivet, och till skillnad från dess föregångare gör den cybersäkerhet obligatorisk. Medan maskindirektivet enbart tog hänsyn till safety, ingår skyddsmål för security i förordningen under ”Protection against corruption” i ”Essential health and safety requirements EHSR”: Maskinens

säkerhetsfunktioner får inte försämras genom oavsiktlig eller avsiktlig manipulering.

Denna nya väg till CE-märkning skapar en rad nya frågeställningar för maskintillverkare och maskinoperatörer eftersom de måste omarbeta sina tidigare säkerhetskoncept för safety och security.

Cyber Resilience Act: Security under hela produktens livscykel

Förutom synen på företag och maskiner är det absolut nödvändigt att även security-åtgärder implementeras direkt i enheter (som t.ex. styrningar). I september 2022 presenterade EU-kommissionen ett utkast till en förordning som syftar till att höja cybersäkerheten för produkter. Cyber Resilience Act (CRA) riktar sig till tillverkare av produkter med digitala komponenter (maskin- och programvara) som kan kommunicera med andra produkter. Produkter från B2C-området, t.ex. smarttelefoner och robotdammsugare, berörs av förordningen, och det gör även produkter från B2B-området, t.ex. styrningar och sensorer, men också rena programvaruprodukter som operativsystem eller själva maskinen.

Hur stora effekter CRA faktiskt kommer att ha beror på vilka kriterier som i slutändan upprättas för att klassificera produkterna. Enligt CRA får endast produkter som garanterar en uppmätt nivå av cybersäkerhet under produktens hela livscykel släppas på marknaden. Security börjar alltså under produktutvecklingen. Sedan några år anpassar Pilz därför sina utvecklingsprocesser enligt IEC 62443-4-1, ”Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements”, och utvecklade t.ex. SecurityBridge bevisligen ”secure”.

((Tecken: 5 826))

Bilder

Bild 1

Grafik_aus_Prospekt_Schulungen_mit_Pilz_3c_ppt

Safety och security från ett och samma ställe: Pilz erbjuder ett omfattande lösningsutbud med tjänster och produkter inom industrial security för maskiner.

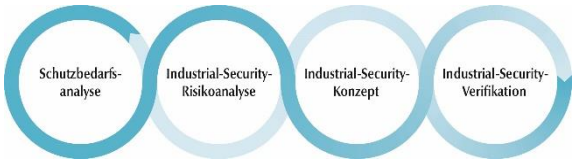
Bild 2:

F_Services_ISCS_two_men_tablet_in_discussion_get1150297892_cold1_v0

Pilz startar tjänsteutbudet Industrial Security Consulting Service och hjälper företag att göra sina maskiner och anläggningar säkra.

Bild 3:

G_Cycle_Industrial_Security_de_v0



Tjänsteutbudet Industrial Security Consulting Service från Pilz utgörs av fyra moduler: Skyddsbehovsanalys, industrial security-riskbedömning, industrial security-koncept och industrial security-systemverifiering.

Bild 4:

F_Press_IAM_Man_using_PITreader_Key_Get1169337234_Get1169337153_cold1_v2

Ett omfattande Identification and Access Management reglerar åtkomsten till tillämpningarna och garanterar därmed säkerhetsfunktionernas och -åtgärdernas integritet – inklusive safety och industrial security.

Bild 5:

F_security_robot_man_virtual_world_Fot208731449_cold1_2019_06_v2

Med industrial security avses att skydda produktions- och industrianläggningar mot fel som uppstår avsiktligt eller oavsiktligt. Målet är att säkerställa tillgängligheten för maskiner och anläggningar samt integriteten och sekretessen för maskinella data och processer.

Pilz – The Spirit of Safety

Pilz är en global leverantör av produkter, system och tjänster inom automationsteknik. Som pionjär inom säker automation skapar Pilz säkerhet för människa, maskin och miljö. Familjeföretaget grundades 1948 med huvudkontor i Ostfildern, men finns idag representerat över hela världen med 2 500 medarbetare i 42 dotterbolag och filialer.

Den ledande aktören inom teknik erbjuder kompletta automationslösningar för safety och industrial security för maskiner. Detta omfattar sensorteknik, styrteknik och driftteknik – inklusive system för industriell kommunikation, diagnostik och visualisering. Sortimentet avrundas med ett internationellt tjänsteutbud med rådgivning, projektering och utbildningar. Pilz lösningar används förutom inom maskin- och anläggningskonstruktion även inom många andra branscher som t.ex. intralogistik, förpackningsindustrin, järnvägsteknik och robotteknik.

www.pilz.com

Pilz i sociala medier:

I våra kanaler i sociala medier ger vi bakgrundsinformation om företaget och personerna som arbetar för Pilz, och rapporterar om vad som händer inom automationsteknik.

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

Presskontakt:

Martin Kurth
Företags- och fackpress
Tel: +49 711 3409-158
m.kurth@pilz.de

Sabine Karrer
Fack- och företagspress
Tel: +49 711 3409-7009
s.skaletz-karrer@pilz.de

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

Hansjörg Sperling-Wohlgemuth
Mässor och föredrag
Tel: +49 711 3409-239
h.sperling@pilz.de