Bakgrundsinformation

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

Skydd för företag, maskiner och produkter

Safety och industrial security – allt från ett och samma ställe

Ostfildern, oktober 2025 – **Säkerhetsincidenter drabbar inte längre bara IT-system, utan i allt högre grad även produktionsmiljön (OT). Incidenter inom industrial security omfattar inte bara riktade attacker utan även oavsiktlig manipulation. Uppgiften för industrial security i produktionen är att garantera tillgänglighet för maskiner och anläggningar samt integritet och sekretess för maskindata och processer. Det främsta skyddsmålet är dock funktionssäkerhet. Om företag inte har fullständig kontroll över sina uppgifter är det trots allt företaget och de anställdas säkerhet som står på spel: utan security ingen safety och utan safety inget skydd för människor!**

Inom EU har den ökande hotbilden uppmärksammats och lagstiftningen har anpassats därefter: På företagsnivå kräver **NIS 2-direktivet** åtgärder för att säkerställa en hög gemensam nivå av cybersäkerhet i unionen, t.ex. genom ett styrsystem för informationssäkerhet.

EU:s maskinförordning 2023/1230 föreskriver nu skydd mot manipulering för maskiner och system och kräver åtgärder för industrial security för de delar av maskinen som påverkar funktionssäkerheten.

Cyber Resilience Act (CRA) kräver säkerhetsåtgärder för produkter med digitala element. 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.

Toppmodern säkerhet

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. Etablerade processer och villkor för drift av maskiner kan gynna manipulation om de inte regelbundet ifrågasätts. 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.

Steg för steg mot förbättrad industrial security

I slutändan är målet att säkerställa att affärsverksamheten förblir skyddad, men företagen måste övervinna olika utmaningar för att uppnå detta: det sträcker sig från att identifiera de tillämpliga lagkraven, identifiera och eliminera sårbarheter i systemen, öka medvetenheten och utbilda medarbetarna för det efterföljande genomförandet av kontroller. Eftersom security är ett s.k. ”rörligt mål” är det också nödvändigt att regelbundet kontrollera maskinernas status vad gäller industrial security. Det är viktigt att ha tydliga ansvarsområden inom företaget och ett systematiskt arbetssätt som inbegriper att bygga upp nödvändig kompetens.

Automationsföretaget Pilz har anpassat sig till dessa krav och byggt upp en skräddarsydd serviceportfölj för maskintillverkare och användare internationellt, som på ett enhetligt sätt omfattar alla aspekter för skydd av människa och maskin. Experterna på Pilz känner till de aktuella lag- och standardiseringskraven och tar hänsyn till dem i sin rådgivning. För att bygga upp eller uppdatera säkerhetskunskapen i företagen kompletteras utbudet även med utbildningar. Den praktiska implementeringen sker med hjälp av produktlösningar från Pilz, till exempel Identification and Access Management - I.A.M. för ökad safety och industrial security.

Lägga rätt grund

För att säkerställa industrial security i de egna maskinerna behöver specialister inom maskin- och anläggningskonstruktion goda grundläggande kunskaper – särskilt vad gäller lagstiftning och gällande standarder. I utbildningen ”Grunderna inom industrial security” förmedlar Pilz den här kunskapen. Deltagarna får lära sig om security-hot, passande skyddsåtgärder och bästa praxis för att bättra förstå maskin- och nätverkssäkerhet. Det innebär att även nybörjare inom säkerhetsområdet kan lära sig vilka åtgärder de kan vidta för att effektivt skydda maskiner från cyberattacker och manipulation på maskinproduktionsnivå.

Med kvalificeringen ”CESA – Certified Expert for Security in Automation” erbjuder Pilz en tvådagars expertkurs som ger deltagarna fördjupade kunskaper inom security enligt de senaste standarderna, särskilt med avseende på standardserien IEC 62443 (Industriella kommunikationsnätverk – IT-säkerhet för nätverk och system). Dessutom tar utbildningen upp praktiska åtgärder för riskreducering, t.ex. åtkomstkontroll, ökad nätverkssäkerhet med tekniska medel samt organisatoriska åtgärder för att minska security-

risker. Deltagarna får lära sig att tillämpa standarden på rätt sätt och visa att deras automationssystem uppfyller kraven på cybersäkerhet. Efter godkänt slutprov får deltagarna det globalt erkända TÜV NORD-certifikatet som ”CESA – Certified Expert for Security in Automation”.

Omsätta teoretisk kunskap i praktiken

Med utgångspunkt i de teoretiska grunderna och utbildningarna består nästa steg för att stärka industrial security att tillämpa strukturerade, praktiskt orienterade processer. Rådgivning inom Operational Technology (OT) skapar en övergång från teori till genomförbara strategier. Med hjälp av en stegvis metod identifierar tjänsterna för industrial security sårbarheter i komplexa system och utvecklar åtgärder för att minimera riskerna. Detta resulterar i ett enhetligt säkerhetskoncept.

Fyra steg för ökad industrial security

OT-säkerhetsprocessen består av fyra steg: analys av skyddskraven, riskbedömning av industrial security, koncept för industrial security och verifiering av systemen för industrial security.

Under analysen av skyddskraven fastställer företaget skyddskraven för de enskilda ”tillgångarna” i maskinen eller systemet och 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. Nästa steg är att skapa ett detaljerat koncept för industrial security med strategier och åtgärder för att försvara sig mot och minska riskerna som orsakas av angrepp, manipulation och handhavandefel. 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,

systemverifieringen för industrial security, kontrolleras effektiviteten hos de genomförda motåtgärderna.

Säkra maskintillgängligheten

Tjänster för industrial security-processen bidrar till att mildra eller förhindra cyberattacker. Antalet oavsiktligt utlösta security-incidenter sjunker också. Detta ökar i sin tur maskinernas tillgänglighet och ger i slutändan kostnadsbesparingar och bibehållen ekonomisk effektivitet.

Detta tillvägagångssätt skyddar i första hand personer vid maskinen med lämpliga säkerhetsåtgärder. 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. Men om en angripare kan påverka motsvarande styrenhet och mekanism kan ljusridåns skyddsfunktion inte längre garanteras. Security skyddar safety!

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!

Tydliga regler: 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. Tillträdesplatser måste säkras mot obehörig åtkomst så att t.ex. inga personer befinner sig i riskområdet under driften. 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.

Endast en helhetssyn på safety och security kan garantera ett omfattande skydd av både 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.

((Antal tecken: 9 784))

((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 NIS 2-direktivet ((EU) 2022/2555 om åtgärder för en hög gemensam nivå av cybersäkerhet i hela unionen) kräver att betydligt fler företag vidtar åtgärder för hantering av cybersäkerhetsrisker i framtiden. 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 den nationella lagstiftningen. 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.

Ett exempel på NIS 2 i 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: ingen CE-märkning utan security

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 även 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 produktens hela 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.

Tillverkares skyldighet att rapportera utnyttjade sårbarheter gäller från och med 11 september 2026. Produkter med digitala element måste uppfylla kraven i CRA från och med 11 december 2027 för att få tillhandahållas på marknaden i EU. CRA är en EU-förordning och kommer därför att vara direkt tillämplig i EU:s medlemsländer

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”.

((Antal tecken: 6 062))

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 på sociala medier:

I våra kanaler på 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/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

Jenny Skarman
Fackpress
Tel: +49 711 3409-1067
j.skarman@pilz.de

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