Taustatietoa

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

16. toukokuuta 2024

Yritysten, koneiden ja tuotteiden suojaksi

Safety ja Industrial Security - Kaikki yhdestä paikasta

Ostfildern, 16. toukokuuta 2024 - **Security-loukkaukset eivät enää vaikuta vain IT-järjestelmiin, vaan yhä useammin myös tuotantoympäristöön (OT). Industrial Securityn alalla tapahtuviin vaaratilanteisiin kuuluu kohdennettujen hyökkäysten lisäksi myös tahatonta manipulointia. Industrial Securityn tehtävä tuotannossa on varmistaa koneiden käytettävyys sekä tietojen ja prosessien koskemattomuus ja luotettavuus. Sillä jos yritys ei hallitse tietojaan, yritys ja sen työntekijöiden turvallisuus on vaarassa: Ilman Securitya ei ole Safetya ja ilman Safetya ei ole ihmisten suojelua!**

EU:ssa lainsäätäjät ovat reagoineet kasvavaan uhkatilanteeseen: Yritystasolla **verkko- ja tietoturvadirektiivi NIS 2** edellyttää tietoturvallisuuden hallintajärjestelmän käyttöönottoa.

Uudessa koneasetuksessa 2023/1230 säädetään nyt koneiden ja järjestelmien suojaamisesta peukaloinnilta ja edellytetään turvatoimia koneen toiminnalliseen turvallisuuteen vaikuttaville osille.

Kyberkestävyyslaissa (Cyber Resilience Act, CRA) edellytetään Security-toimia tuotteille, joissa on digitaalisia elementtejä. Näitä ovat ohjausjärjestelmät, IO-järjestelmät ja muut koneissa käytettävät komponentit.

Yritykset, koneet ja tuotteet – koneiden valmistajat ja käyttäjät kohtaavat erilaisia haasteita ja erilaisia oikeudellisia vaatimuksia kaikilla tasoilla.

Riippumatta siitä, että lainsäätäjä on tehnyt Industrial Securitystä pakollista, on monia hyviä syitä käsitellä aihetta ja pyytää neuvoja varhaisessa vaiheessa. Tämä johtuu siitä, että monet prosessit ja koneiden toimintaolosuhteet suosivat manipulointia, ja ne olisi pikaisesti kyseenalaistettava ja muutettava. Esimerkiksi koneiden pitkä käyttöikä tarkoittaa usein sitä, että niihin liittyvät järjestelmät vanhenevat eivätkä jossain vaiheessa enää täytä uusimpia turvallisuusstandardeja. Näissä järjestelmissä on tietoturva-aukkoja, joita ei voida enää korjata, koska palveluntarjoaja ei enää toimita Security-päivityksiä. Haittaohjelmilta suojautumista ei useinkaan voida toteuttaa loppulaitteissa, koska osa niistä on liian vanhoja ja niiden suorituskyky kärsisi, mikä voi johtaa tuotannon keskeytymiseen.

Pilzin kattava palveluvalikoima

Viime kädessä tavoitteena on varmistaa, että liiketoiminta pysyy suojattuna, mutta yritysten on voitettava erilaisia haasteita tämän tavoitteen saavuttamiseksi: Tämä ulottuu sovellettavien oikeudellisten vaatimusten tunnistamisesta, järjestelmien heikkouksien tunnistamisesta ja poistamisesta, tietoisuuden lisäämisestä ja työntekijöiden kouluttamisesta aina tarkastusten myöhempään toteuttamiseen. Koska Security on "liikkuva kohde", on myös tarpeen tarkistaa säännöllisesti koneiden Industrial Securityn tila.

Automaatioyritys Pilz on mukautunut näihin vaatimuksiin ja kehittänyt koneenrakentajille ja käyttäjille kansainvälisesti palveluvalikoiman, joka kattaa kokonaisvaltaisesti kaikki ihmisen ja koneen suojeluun liittyvät näkökohdat. Tarjonta ulottuu perustiedoista ja perehdyttämisvälineistä sekä koulutuskursseista Industrial Security Consulting Serviceen (ISCS), jossa toteutetaan erityisiä hankkeita.

CESA - Certified Expert for Security in Automation -koulutuksen myötä Pilz on tarjonnut viime vuodesta lähtien kaksipäiväisen asiantuntijakurssin, joka antaa osallistujille uusimpiin standardeihin perustuvan kompaktin Security-osaamisen. Lisäksi käsitellään käytännön toimenpiteitä riskien vähentämiseksi, kuten kulunvalvontaa, verkkoturvallisuuden parantamista teknisin keinoin sekä organisatorisia toimenpiteitä turvallisuusriskien vähentämiseksi. Kokeen läpäistyään osallistujat saavat maailmanlaajuisesti tunnustetun TÜV-NORD CESA - Certified Expert for Security in Automation -sertifikaatin.

Uuden Industrial Security Consulting Service (ISCS) -palvelun myötä Pilz laajentaa koneiden turvallisuusteknistä tarkastelua Safetyn ja Securityn kokonaisvaltaiseen tarkasteluun. Pilz on kehittänyt koneiden toiminnallisen turvallisuuden alalla hyväksi havaittujen palvelumenetelmien ja IEC 62443 Security-standardisarjan pohjalta palveluvalikoiman, jonka käyttöönoton jälkeen yritykset ovat hyvin varustautuneita Industrial Securityn suhteen ja täyttävät voimassa olevat lakisääteiset vaatimukset.

Neljä moduulia, joilla parannat Industrial Securityä

ISCS koostuu neljästä moduulista: Suojelutarpeen analyysi, Industrial Security -riskinarviointi, Industrial Security -konsepti ja Industrial Security -järjestelmän todentaminen.

Suojaustarpeiden analysoinnin aikana Pilzin asiantuntijat määrittävät koneen tai laitoksen yksittäisten osien suojausvaatimukset ja niiden suojaustavoitteet. Toisessa vaiheessa, riskinarvioinnissa, tarkastellaan kaikkia riskejä ja niiden esiintymistodennäköisyyttä kunkin osa-alueen osalta järjestelmän koko elinkaaren aikana. Tämän jälkeen Pilzin asiantuntijat keskustelevat asiakkaan kanssa mahdollisista ratkaisuista heikkouksiin ja mahdollisiin vaaroihin.

Kolmannessa vaiheessa Pilzin asiantuntijat laativat Industrial Security -konseptin, joka sisältää strategioita ja toimenpiteitä hyökkäysten, manipuloinnin ja käyttövirheiden aiheuttamien riskien torjumiseksi ja lieventämiseksi. Järjestelmän jatkuvaa turvallista toimintaa varten luodaan myös käytäntöjä, sääntöjä ja ohjeita. Viimeisessä vaiheessa, Industrial Security -järjestelmän varmentamisessa, tarkistetaan toteutettujen vastatoimien tehokkuus.

Koneen käytettävyyden varmistaminen

Industrial Security Consulting Service lieventämään tai estämään verkkohyökkäyksiä. Myös tahattomasti käynnistettyjen Security-loukkausten laskee. Tämä puolestaan lisää koneiden käytettävyyttä ja varmistaa viime kädessä kustannussäästöt ja taloudellisen tehokkuuden säilymisen.

Ennen kaikkea ISCS varmistaa, että koneella työskenteleviä ihmisiä suojellaan asianmukaisilla turvatoimilla. Koska Security-tapahtumasta voi tulla este Safety-toimenpiteille. Esimerkiksi koneiden edessä oleva valoverho varmistaa, ettei käyttäjä astu vaaravyöhykkeelle. Jos hyökkääjä pystyy kuitenkin vaikuttamaan vastaavaan ohjaukseen ja -mekanismiin, valoverhon suojatoimintaa ei voida enää taata. Security suojaa Safetya!

Pilz tarjoaa näin ollen koneenrakentajille ja käyttäjille palveluvalikoiman, jossa otetaan huomioon kaikki ihmisen ja koneen suojeluun liittyvät näkökohdat.

Ratkaisun toteutuksen yhteydessä on järkevää tarkastella Safetya ja Securitya yhdessä. Sillä ilman Securitya ei ole Safetya ja ilman Safetya ei ole ihmisten suojelua.

Selkeästi säännelty: Kenellä on oikeus tehdä mitä koneella?

Koneen ja sen käyttäjien turvallisuus on kiinni ihmisten tai verkkojen kulkuaukkojen sääntelystä. Kulkuaukot on suojattava luvattomalta pääsyltä siten, että esimerkiksi koneen ollessa toiminnassa vaarallisella alueella ei ole henkilöitä. Jos valtuutettu koneen käyttäjä on tällä vaaravyöhykkeellä huoltotarkoituksessa, on varmistettava, että kukaan muu ei voi vaikuttaa järjestelmään samaan aikaan. Koska jopa järjestelmän hyvässä tarkoituksessa tapahtuvalla käytöllä tai huollolla – joko paikan päällä tai verkon kautta - voi olla kohtalokkaita seurauksia.

Tärkeä osatekijä on tunnistus ja pääsyoikeuksien hallinta (I.A.M.), jolla säännellään selkeästi valtuutuksia ja pääsyoikeuksia yrityksessä. Tähän kuuluvat organisatoriset toimenpiteet ja eritelmät sekä asianmukaiset turvatoiminnot. Pilzin PITreader kaltainen kulunvalvontajärjestelmä on tähän oikea tuotekomponentti. Näin käyttäjät voivat täyttää työntekijöiden suojelua, vastuuta, maksimaalista tuottavuutta ja tietosuojaa koskevat vaatimukset.

PITmode fusion toimintatavan- ja pääsyoikeuksien hallintajärjestelmä tarjoaa toiminnallisesti turvallisen toimintatilan valinnan ja koneiden ja järjestelmien kulunvalvonnan. Kukin käyttäjä saa vastuualueitaan ja pätevyyttään vastaavat koneen käyttöoikeudet RFID-koodatulla transponderilla. Siksi järjestelmää voivat käyttää ja valvoa vain valtuutetut henkilöt määritellyissä toimintatiloissa. Tämä tarjoaa korkeatasoisen suojan tahattomia toimia ja manipulointia vastaan.

Kun toimintatavan- ja pääsyoikeuksien hallintajärjestelmää täydennetään modulaarisen turvaporttijärjestelmän osilla, luodaan Safetyn ja Securityn näkökulmasta yhtenäinen kulunhallintakonsepti.

Paraskaan turvaportin suojaus on hyödytön, jos tietoja, asiantuntemusta ja toimintaprosesseja ei ole riittävästi suojattu

luvattomalta käytöltä ja manipuloinnilta ja jos hyökkääjä voi tunkeutua ohjausjärjestelmään.

Industrial Firewall suojaa pääsyä ulkopuolelta

Pilzin Industrial Firewall SecurityBridge -palomuurin tehtävänä on turvata pääsy automaatioverkkoihin ulkopuolelta. Se valvoo tietokoneen ja ohjausyksikön välistä tietoliikennettä ja vähentää siten hakkerihyökkäysten ja manipuloinnin hyökkäyspintaa. SecurityBridge suojaa Pilz-ohjausten lisäksi myös muiden toimittajien ohjauksia manipuloinnilta.

Pilz on vakuuttunut, että vain kokonaisvaltainen Securityn ja Safetyn tarkastelu voi taata kattavan suojan ihmisille ja koneille. Se, haluaako yritys puuttua Securityyn ja kuinka perusteellisesti, ei ole enää yrityksen harkinnassa. Security on lakisääteinen vaatimus. Koneenrakennusteollisuudessa Industrial Security ei ole vain IT:n tehtävä, vaan olennainen osa suunnittelua ja rakentamista. Securityn toteuttaminen jälkikäteen on aikaa vievää ja merkitsee yleensä käyttäjäystävällisyyden, toiminnallisuuden ja tuottavuuden heikkenemistä.

((Zeichen: 10 173))

((Kasten:))

Yleiskatsaus Industrial Securityä koskevaan EU:n lainsäädäntöön:

Erityisesti Euroopassa lainsäätäjät vastaavat uhkatilanteeseen useilla laeilla. Tämä tarkoittaa, että Euroopassa on maailman tiukimmat säädökset. Koordinointi muiden maiden kanssa on kuitenkin jo

käynnissä, ja tällaiset lait tulevat myös sinne. Industrial Securityn maailmanlaajuinen yhdenmukaistaminen on näin ollen odotettavissa.

NIS 2: Enemmän velvoitteita yritykselle

Verkko- ja tietoturva (NIS) on Euroopan unionin direktiivi, jolla pyritään vahvistamaan tietoverkkoturvallisuutta. Direktiivi on ollut voimassa vuodesta 2016, ja sitä on tähän mennessä sovellettu kriittisen infrastruktuurin tarjoajiin, kuten energia-, liikenne-, pankki- ja rahoituspalvelut, terveydenhuolto, juomaveden toimitus ja jakelu sekä digitaalinen infrastruktuuri. Näiden alojen palveluntarjoajien oli toteutettava "asianmukaiset varotoimenpiteet" Securityn osalta ja raportoitava vakavista tietoverkkoturvallisuuteen liittyvistä vaaratilanteista. Uusi verkko- ja tietoturvadirektiivi 2 EU 2022/2555 (NIS 2) edellyttää, että tulevaisuudessa huomattavasti useammat yritykset ryhtyvät riskinhallintatoimenpiteisiin kyberturvallisuuden alalla. NIS 2:ssa laajennetaan aloja esimerkiksi valmistus- ja tuotantoteollisuuteen, mukaan lukien koneenrakennus ja sähkölaitteiden valmistajat.

Se edelllyttää riskianalyysejä ja tietojärjestelmien, toimitusketjun suojaamisen ja henkilöstön turvallisuuden turvallisuuskäsitteitä. Se sisältää myös kulunvalvontaan ja järjestelmänhallintaan liittyviä käsitteitä sekä johdon pakollisen koulutuksen.

Euroopan parlamentti ja EU:n neuvosto hyväksyivät direktiivin vuoden 2022 lopussa. Muiden EU-direktiivien tavoin myös NIS 2 -direktiivi ei ole suoraan voimassa ja sitova yksittäisissä EU:n jäsenvaltioissa, vaan jäsenvaltioiden on saatettava se osaksi kansallista lainsäädäntöään. EU:n jäsenvaltioiden on saatettava direktiivi osaksi kansallista lainsäädäntöään 18. lokakuuta 2024 mennessä. Yritysten olisi hyvä käsitellä NIS 2 mahdollisimman pian ja tehdä yritykselle kattava Security-arviointi. Tähän kuuluu esimerkiksi

tietoturvallisuuden hallintajärjestelmän (ISMS) perustaminen. ISO 27001 -tietoturvastandardin mukainen sertifiointi on tässä yhteydessä hyödyllistä.

NIS 2 esimerkiksi tuulivoimaloissa: NIS 2:n myötä myös koneenrakentajien, kuten sähköntuotantolaitteiden (esim. tuuliturbiinien) valmistajien, on tulevaisuudessa noudatettava vaatimuksia. Tuulivoimalan valmistaja puolestaan tarvitsee automaatioratkaisuja, ohjaimia tai antureita. Tietyn koon ylittävät sähkökomponenttien valmistajat kuuluvat myös NIS 2:n piiriin. Ja koska NIS 2:ssa säädetään myös toimittajien huomioon ottamisesta, Pilzin kaltaisen yrityksen on myös huolehdittava turvallisista toimitusketjuista ja asetettava toimittajilleen vaatimuksia. NIS 2 kattaa siis koko toimitusketjun.

Uusi koneasetus: Ei CE-merkintää ilman Securityä

Konedirektiivi 2006/42/EY on erityisen tärkeä koneiden toiminnallisen turvallisuuden kannalta.

Koneiden valmistajien on jo pitkään täytynyt suorittaa vastaava vaatimustenmukaisuuden arviointimenettely ja CE-merkintä, jotta ne voivat tuoda koneita Eurooppaan.

Kesäkuussa 2023 julkaistu koneasetus on päivitetty vastaamaan tekniikan nykytilaa. Koska kyseessä on asetus, sitä ei tarvitse ensin saattaa osaksi kansallista lainsäädäntöä. Koneiden valmistajilla on 20. tammikuuta 2027 asti aikaa siirtyä uusiin vaatimuksiin ja noudattaa niitä määräajasta alkaen.

Koneasetus korvaa aiemman konedirektiivin, ja toisin kuin edeltäjänsä, siinä säädetään kyberturvallisuus pakolliseksi. Kun konedirektiivi käsitteli pelkästään Safetyä, koneasetuksessa Security-

tavoite on sisällytetty "olennaisiin terveys- ja turvallisuusvaatimuksiin" kuuluvaan kohtaan "korruptiolta suojautuminen": Tahaton tai tahallinen väärentäminen ei saa heikentää koneen turvatoimintoja.

Tämä uusi tie CE-merkintään herättää koneiden valmistajissa ja käyttäjissä useita uusia kysymyksiä, sillä niiden on tarkistettava nykyisiä Safety- ja Security-konseptejaan.

Kyberkestävyyslaki: Security koko tuotteen elinkaaren ajan

Yrityksen ja koneen tarkastelun lisäksi on ehdottoman välttämätöntä toteuttaa Security-toimia myös suoraan laitteissa (esimerkiksi ohjauksissa). Euroopan komissio esitti syyskuussa 2022 asetusluonnoksen, jonka tarkoituksena on lisätä tuotteiden kyberturvallisuutta. Tämä kyberturvallisuuslaki (CRA) on suunnattu sellaisten tuotteiden valmistajille, joissa on digitaalisia elementtejä (laitteistoja ja ohjelmistoja), eli itse asiassa lähes kaikille koneiden valmistajille. Tämä vaikuttaa sekä B2C-sektorin tuotteisiin, kuten älypuhelimiin tai robotti-imureihin, että B2B-sektorin tuotteisiin, kuten ohjausjärjestelmiin ja antureihin, sekä puhtaisiin ohjelmistotuotteisiin, kuten käyttöjärjestelmiin tai itse koneisiin.

Se, kuinka suuri vaikutus CRA:lla todellisuudessa on, riippuu siitä, mitä kriteerejä tuotteiden luokittelussa lopulta käytetään. Kyberkestävyyslain mukaan markkinoille saa nyt saattaa vain tuotteita, joilla varmistetaan asianmukainen kyberturvallisuuden taso – tuotteen koko tuotteen elinkaaren ajan. Security alkaa siis tuotteen kehityksestä. Pilz on myös jo muutaman vuoden ajan yhdenmukaistanut kehitysprosessinsa standardin IEC 62443-4-1 "Teollisuusautomaation ohjausjärjestelmien turvallisuus - osa 4-1:

Turvallisen tuotekehityksen elinkaarivaatimukset" kanssa ja kehittänyt esim. SecurityBridgen todistettavasti "turvallisesti".

((Zeichen: 5 826))

Abbildungen

Abb. 1

Grafik_aus_Prospekt_Schulungen_mit_Pilz_3c_ppt

Safety ja Security yhdeltä toimittajalta: Pilz tarjoaa kattavan valikoiman palveluja ja tuotteita koneiden Industrial Securityn varmistamiseksi.

Copyright: Pilz GmbH & Co. KG

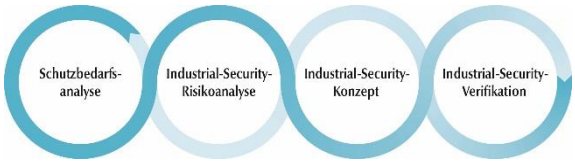
Abb.2:

F_Services_ISCS_two_men_tablet_in_discussion_get1150297892_cold1_v0

Pilz lanseeraa Industrial Security Consulting Service -palvelun ja tukee yrityksiä laitosten ja koneiden turvallisuuden parantamisessa.

Abb.3:

G_Cycle_Industrial_Security_de_v0



Pilzin Industrial Security Consulting Service koostuu neljästä moduulista: Suojelutarpeen analyysi, Industrial Security -riskinarviointi, Industrial Security -konsepti ja Industrial Security -järjestelmän todentaminen.

Abb.4:

F_Press_IAM_Man_using_PITreader_Key_Get1169337234_Get1169337153_cold1_v2

Kokonaisvaltainen tunnistus ja kulunhallinta sääntelee selkeästi käyttöoikeuksia ja -valtuuksia ja varmistaa siten turvallisuustoimintojen ja -toimenpiteiden eheyden - mukaan lukien Safety ja Industrial Security.

Abb.5:

F_security_robot_man_virtual_world_Fot208731449_cold1_2019_06_v2

Industrial Security tarkoittaa tuotanto- ja teollisuuslaitosten suojausta tahallisilta tai tahattomilta virheiltä. Sen tavoitteena on varmistaa koneiden ja laitosten käytettävyys sekä tietojen ja prosessien koskemattomuus ja luotettavuus.

Pilz – The Spirit of Safety

Pilz on globaali automaatiotekniikan tuotteiden, järjestelmien ja palvelujen toimittaja. Turvallisen automaation pioneerina Pilz luo turvallisuutta ihmisille, koneille ja ympäristölle. Vuonna 1948 perustettu perheyritys, jonka pääkonttori sijaitsee Ostfildernissä, on nykyään maailmanlaajuisesti edustettuna 2 500 työntekijän voimin 42 tytäryhtiössä ja sivuliikkeessä.

Teknologiajohtaja tarjoaa täydellisiä automaatioratkaisuja koneen Safetyä ja Industrial Securityä varten. Tuotevalikoimamme sisältää anturi-, ohjaus- ja käyttötekniikan täydellisiä automaatioratkaisuja – mukaan luettuna järjestelmiä teollisuuden tiedonsiirtoon, diagnosointiin ja visualisointiin. Salkun täydentää kansainvälinen palvelutarjonta, johon sisältyy neuvonta, suunnittelu ja koulutus. Pilzin ratkaisuja käytetään kone- ja laitosrakentamisen lisäksi lukuisilla muilla aloilla, kuten intralogistiikassa, pakkaustekniikassa, rautatietekniikassa ja robotiikassa.

www.pilz.com

Pilz sosiaalisessa mediassa:

Sosiaalisen median kanavillamme kerromme taustatietoa Pilzistä ja yrityksessä työskentelevistä ihmisistä ja jaamme uutisia automaatiotekniikan alalta.

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

Yhteystiedot lehdistölle:

Martin Kurth
Yritys- ja ammattilehdistö
Puh: +49 711 3409-158
m.kurth@pilz.de

Sabine Karrer
Yritys- ja ammattilehdistö
Puh: +49 711 3409-7009
s.skaletz-karrer@pilz.de

Eva Rößle
Ammattilehdistö
Puh: +49 711 3409-7147
e.roessle@pilz.de

Hansjörg Sperling-Wohlgemuth
Kongressi- ja luentohallinto
Puh: +49 711 3409-239
h.sperling@pilz.de