Security

PILZ
THE SPIRIT OF SAFETY

Whitepaper

Ontheffing van aansprakelijkheid

Wij hebben ons whitepaper zeer zorgvuldig samengesteld. Deze bevat informatie over onze onderneming en over onze producten. Wij hebben alle informatie volgens de huidige stand van de techniek en naar eer en geweten verstrekt. Desondanks kunnen wij, voor zover ons geen grove nalatigheid te verwijten valt, geen aansprakelijkheid aanvaarden voor de juistheid en volledigheid van de informatie, omdat fouten ondanks alle zorgvuldigheid niet volledig kunnen worden voorkomen. In het bijzonder hebben de gegevens niet de juridische kwaliteit van toezeggingen of beloofde eigenschappen. Wij houden ons aanbevolen voor opmerkingen over eventuele onjuistheden.

Auteursrecht

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern
Duitsland

Overzicht

Vanwege de digitalisering van de fabriek worden installaties in toenemende mate gekoppeld. Hierdoor wordt ook het risico verhoogd dat belangrijke informatie door spionage wordt verkregen of gemanipuleerd. Voorheen werd in de automatisering hoofdzakelijk via veldbussen zoals CAN en fabrikantspecifieke protocollen gecommuniceerd. Om schade aan te richten, zou een aanvaller al in de fabriekshal moeten komen of via een telefoonlijn met een modem toegang tot een machine moeten krijgen. Omdat deze protocollen intussen in toenemende mate door Ethernet en IP-protocollen zijn vervangen, kunnen aanvallen nu dus ook via internet worden uitgevoerd.

De motieven variëren van terroristische bedoelingen, industriële spionage, de sabotage van installaties tot de afpersing van geldbetalingen. De activiteiten van de aanvaller worden vereenvoudigd doordat in de automatisering steeds vaker Open Source-software en softwarecomponenten voor consumenten worden gebruikt, die mogelijk zwakke punten bezitten waarmee de aanvallers bekend zijn. Ook daarom neemt security, dus de gegevensveiligheid, een steeds belangrijker plaats in.

Uit ervaring blijkt echter dat deze boodschap nog lang niet door iedereen juist wordt begrepen. Daarom worden in deze whitepaper de centrale aspecten van security toegelicht en aanzetten tot oplossingen voorgesteld die zich in de praktijk hebben bewezen. Hierdoor kunnen bijvoorbeeld machinebouwers, ontwerpers van installaties, installateurs en onderhoudspersoneel inzien welke rol hun producten en/of diensten spelen voor de security-strategieën van hun klanten en waarop ze moeten letten. Bovendien wordt hierbij ook het aspect van de functionele veiligheid (safety) betrokken. Want security en safety zijn twee zijden van dezelfde medaille, ofwel veiliger productieprocessen.

Inhoudsopgave

1. Security en safety

1.1. Definitie

Vroeger was security vrijwel uitsluitend een thema dat betrekking had op de klassieke informatietechnologie (IT). Tegenwoordig komen de IT- en automatiseringswereld echter steeds dichter samen. Hierdoor neemt de mate van netwerkvorming van productie-installaties en het gebruik van standaardprotocollen zoals Ethernet voor de fysieke overdracht van gegevens aanzienlijk toe. Bovendien kan middels gestandaardiseerde protocollen zoals OPC UA via IT-systemen toegang worden verkregen tot besturingen, waardoor de datacommunicatie nog opener wordt.
In de automatisering betekent de term 'security' met name de bescherming van machines en installaties tegen enige externe onbevoegde toegang evenals de bescherming van gevoelige gegevens tegen vervalsing, verlies en enige interne onbevoegde toegang. De bedreigingen komen uit de cyberwereld, waartoe zowel internet als de complete moderne informatie- en communicatietechnologie behoren. De controle begint als toegangscontrole bij de fabriekspoort en reikt tot het afweren van aanvallen door hackers. Evenwel zijn het, aldus de Duitse IT-veiligheidsexpert Ralph Langner, niet altijd de "kwaadwillenden" die schade aanrichten. Want veel security-fouten vinden onbedoeld plaats, bijvoorbeeld door bedieningsfouten van collega's en medewerkers.
Met de term 'safety' wordt de functionele veiligheid van installaties aangeduid, dus de bescherming van mens en milieu tegen voorzienbare bedreigingen die van machines kunnen uitgaan. Hierbij mogen restrisico's, die min of meer aanwezig zijn, de aanvaardbare niveaus niet overschrijden. Om dit te garanderen, worden onder meer componenten zoals veiligheidsrelais en veiligheidsschakelaars gebruikt, die ervoor zorgen dat de machine bij een probleem in een veilige toestand wordt gebracht, waardoor geen gevaar voor mens, machine en milieu wordt veroorzaakt.
Nadat de functionele veiligheid van een machine overeenkomstig de voorschriften van de Machinerichtlijn was goedgekeurd, hoefden de exploitanten van installaties zich over safety geen zorgen meer te maken, zolang daarna bij de machine geen belangrijke veranderingen meer werden uitgevoerd. Deze tijden zijn echter voorbij. Want door de bedreigingen uit de cyberwereld is security een onmisbaar element voor safety geworden.

1.2. Wisselwerkingen

Omdat productieprocessen door safety-functies kunnen worden onderbroken, wordt vaak geprobeerd deze – illegaal – te omzeilen, wat tot nu toe met name middels mechanische maatregelen is voorkomen. Een voorbeeld hiervan zijn verzegelde schroeven, die voorkomen dat veiligheidsschakelaars eenvoudig kunnen worden verwijderd. Tegenwoordig is het echter mogelijk deze manipulaties via het netwerk uit te voeren. Wanneer bijvoorbeeld een machine wegens een lichtscherm overschakelt naar een bepaalde toestand, kan het programma hiervan zodanig worden gewijzigd dat de betreffende gegevens niet meer worden geanalyseerd. Hierdoor is de beveiligingsfunctie uitgeschakeld, en blijft de machine ook in gevaarlijke situaties gewoon actief.
Anderzijds kunnen safety-mechanismen ook worden gebruikt om machines via het netwerk gericht tot stilstand te brengen. Hiervoor hoeft alleen de datacommunicatie te worden onderbroken. Want de safety-mechanismen controleren cyclisch of de netwerkdeelnemer aan de andere kant van de verbinding nog actief is. Zodra er geen antwoord volgt, stopt de

machine. Een mogelijkheid om dit te bewerkstelligen, zijn de reeds vermelde DoS-aanvallen die een overbelasting in het netwerk veroorzaken.
Via het netwerk worden echter niet alleen productieprocessen belemmerd, maar er dreigen ook nog andere risico's. Aanvallers kunnen als uitgangspunt gebruikmaken van safety-mechanismen die controleren of de aandrijving van een machine wordt aan- of uitgeschakeld. Als deze mechanismen zodanig worden veranderd dat de aandrijving continu loopt, kan dit ertoe leiden dat een machine in het ergste geval wordt vernield. Daarom worden kostenintensieve investeringsgoederen zoals windturbines vaak dubbel en drievoudig beveiligd.

2. Belang van security in de automatisering

2.1. Doelstelling

Vanwege initiatieven als Industrie 4.0, waarbij de netwerkvorming van essentieel belang is, vormen bedreigingen uit de cyberwereld een ernstig probleem voor producerende bedrijven. Weliswaar worden in principe alle op IT gebaseerde processen beveiligd, maar dit vergt veel werk en is duur. Daarom dient eerst te worden onderzocht welke risico's er daadwerkelijk bestaan. Want bij een security-strategie moeten uiteindelijk altijd de kosten en het nut voor de productiviteit van een bedrijf tegen elkaar worden afgewogen.
Security heeft als doel de beschikbaarheid van het netwerk en de apparatuur evenals de integriteit en vertrouwelijkheid van de gegevens te waarborgen. Hiertoe moeten bijvoorbeeld verdeelde besturingssystemen tegen zowel aanvallen zoals DoS-aanvallen als tegen software-, apparatuur- en bedieningsfouten worden beveiligd. Een andere mogelijkheid om productieprocessen te onderbreken is het manipuleren van de overdracht of opslag van gegevens, om welke reden de integriteit hiervan een belangrijke rol speelt. Maar ook een schending van de vertrouwelijkheid van gegevens kan zwaarwegende gevolgen hebben, bijvoorbeeld wanneer het toepassingsprogramma van een machine door spionage wordt verkregen, waarna deze vervolgens kan worden nagebouwd.

2.2. Meer dan IT-veiligheid

Om diverse bedreigingsscenario's flexibel het hoofd te kunnen bieden, worden tegenwoordig security-strategieën gerealiseerd die uit meerdere beveiligingslagen bestaan: in de kern bevinden zich de automatiseringscomponenten. Dan volgt het netwerk, via welk netwerk deze componenten met andere of bijvoorbeeld een ERP-systeem (Enterprise Ressource Planning) kunnen communiceren. De bovenste laag wordt gevormd door de fabriek, die door een firewall-concept naar buiten toe wordt afgeschermd.
Deze concepten zijn echter niet voldoende om installaties compleet te beveiligen. Want bedreigingen kunnen, zoals eerder vermeld, ook intern worden veroorzaakt. Daarom vormen de fysieke beveiliging tegen enige onbevoegde toegang tot netwerkapparatuur evenals firewalls en schakelaars de basis van elke security-strategie. Alleen wanneer deze apparaten niet vrij toegankelijk zijn, kan worden voorkomen dat ze ter plaatse kunnen worden gemanipuleerd. Een eenvoudige maar effectieve maatregel kan bijvoorbeeld zijn dat de netwerkapparatuur in afsluitbare schakelkasten of verdeelkasten wordt geïnstalleerd. Tegelijkertijd wordt hierdoor ook het risico van bedieningsfouten door onbevoegd personeel aanzienlijk gereduceerd.

2.3. Gevolgen voor de levenscyclus van installaties

Installaties kunnen een levenscyclus van 20 jaar en meer bezitten. Tot nu toe werden ze doorgaans gebruikt volgens het principe "Never change a running system". Dat wil zeggen dat wanneer een safety-mechanisme moest worden geactualiseerd, de besturing normaliter werd vervangen door een nieuw model van hetzelfde type. Want de functionele veiligheid is gegarandeerd zolang bij de machine geen essentiële veranderingen worden uitgevoerd. Deze veiligheid berust op statistische foutmodellen die aangeven hoe waarschijnlijk het is dat er een schadegeval optreedt. En hieraan verandert door de tijd heen zo goed als niets.
Security is daarentegen een "Moving Target". Hierbij gaat het er niet net als bij safety om dat een fout bijvoorbeeld met een waarschijnlijkheid van 1:100.000 optreedt, maar de verhouding kan ook 1:1 zijn wanneer een aanvaller eerst eenmaal in een netwerk is binnengedrongen. Bovendien worden steeds spitsvondiger methoden ontwikkeld om afweermaatregelen te bestrijden, en tot nu toe veilige algoritmen blijken plotseling onveilig. Zo was enkele jaren geleden de Data Encryption Standard (DES) een gangbare methode. Tegenwoordig raadt het BSI (overheidsinstantie voor veiligheid in de informatietechniek) aan deze methode niet meer te gebruiken. Hetzelfde geldt min of meer voor het hashing-algoritme MD5. En met kwantumcomputers zal het binnen niet al te lange tijd mogelijk zijn in enkele minuten of zelfs seconden cryptografische sleutels te berekenen, wat met de tegenwoordige computers nog een eeuwigheid zou duren.
Omdat security geen fysieke grootheid is, maar een "Moving Target", moeten de maatregelen tegen cyberbedreigingen voortdurend worden geactualiseerd. De verantwoordelijkheid hiervoor ligt in eerste instantie bij de exploitanten van installaties, voor wie gegevensveiligheid tegelijk een investeringsbescherming betekent. Want dankzij een effectieve security-strategie kunt u uw installaties net zolang als tot nu toe gebruiken. Omgekeerd zijn machinebouwers en fabrikanten van componenten verplicht de exploitanten direct te informeren over nieuwe veiligheidsproblemen en updates voor de software van hun apparatuur beschikbaar te stellen waarmee zwakke plekken kunnen worden verholpen. Dit vereist echter dat beide partijen gedurende de complete levenscyclus van de producten nauw samenwerken.

3. Bedreigingsvormen

3.1. Externe aanvallen

Op Ethernet gebaseerde automatiseringsnetwerken zijn blootgesteld aan veelzijdige bedreigingsscenario's, die echter aan de hand van het uitgangspunt kunnen worden gecategoriseerd. Want in feite bestaan er alleen externe en interne aanvallen evenals onbedoelde security-fouten, waarbij de motieven variëren.
Wanneer netwerken extern worden aangevallen, gebeurt dit doorgaans met kwade opzet. Hiertoe behoort bijvoorbeeld de sabotage van installaties. Welke gevolgen dit kan hebben, wordt verduidelijkt door een voorbeeld dat weliswaar is gepubliceerd, maar zonder "man en paard" te noemen: na een succesvolle aanval op een hoogoven in Duitsland moest deze uiteindelijk worden gesloopt omdat de gesmolten massa hard was geworden.
Een ander bedreigingsscenario dat negatieve gevolgen kan hebben, is industriële spionage. Wanneer bijvoorbeeld informatie over producten of productie-knowhow door spionage wordt verkregen, is mogelijk het concurrentievermogen van een onderneming in gevaar. Dit geldt ook

wanneer vertrouwelijke financiële gegevens en informatie over klanten, aanbestedingen en opdrachten worden ontvreemd.
Om aan wachtwoorden en toegangsgegevens te komen, maken aanvallers gebruik van deels perfect vervalste websites en e-mails, het zogeheten phishing. Wanneer de ontvangers niet op hun hoede zijn, wordt het de aanvallers gemakkelijk gemaakt. Daarom is het belangrijk dat ondernemingen hun medewerkers voor het thema security sensibiliseren en richtlijnen opstellen die voor iedereen bindend zijn.
Tenslotte is er recent steeds meer sprake van aanvallen die zonder meer met een criminele bedoeling worden uitgevoerd. Het favoriete middel is momenteel zogeheten ransomware, die bijvoorbeeld in Word-, PowerPoint- of Excel-bestanden kan zijn verborgen en via e-mail wordt verzonden. Wanneer een ontvanger deze opent, worden alle bestanden op zijn computer versleuteld. Bovendien kan de malware zich uitbreiden naar verdere apparatuur in het netwerk. De enige mogelijkheid om de gegevens weer terug te krijgen, bestaat uit de betaling van losgeld.

3.2. Interne aanvallen

Hoewel externe aanvallen altijd weer voor publiciteit zorgen, zijn interne aanvallen even gevaarlijk. Want zo kunnen security-strategieën in de ware zin van het woord worden omzeild. De bedoelingen van de aanvaller zijn min of meer gelijk aan de externe aanvallen, alleen de procedure is anders.
Eén mogelijkheid is bijvoorbeeld dat aanvallers in de onderneming binnendringen en daar bijvoorbeeld een vrije Ethernet-aansluiting zoeken om malware in het netwerk binnen te brengen. Hiervoor is een kleine USB-stick voldoende, die bij de controle bij de fabriekspoort niet opvalt.
Veruit vaker maken aanvallers echter gebruik van de situatie dat ook bij security de mens de meest zwakke schakel in de ketting is. Een effectieve methode om personeel te manipuleren is bijvoorbeeld het zogeheten social engineering.
Hierbij gaat het erom op arglistige wijze het vertrouwen van medewerkers te verkrijgen en hen als het ware als gewillig instrument te gebruiken. De kern hiervan is een voorafgaand grondig onderzoek, bijvoorbeeld op websites van ondernemingen, waarop vaak namen en functies van personeel te vinden zijn. Soms is het dan al voldoende wanneer een aanvaller tegenover een medewerker meldt dat hij met collega X heeft gesproken en dat deze heeft gezegd dat hij met hem contact moet opnemen om als personeelslid van het bedrijf door te gaan.

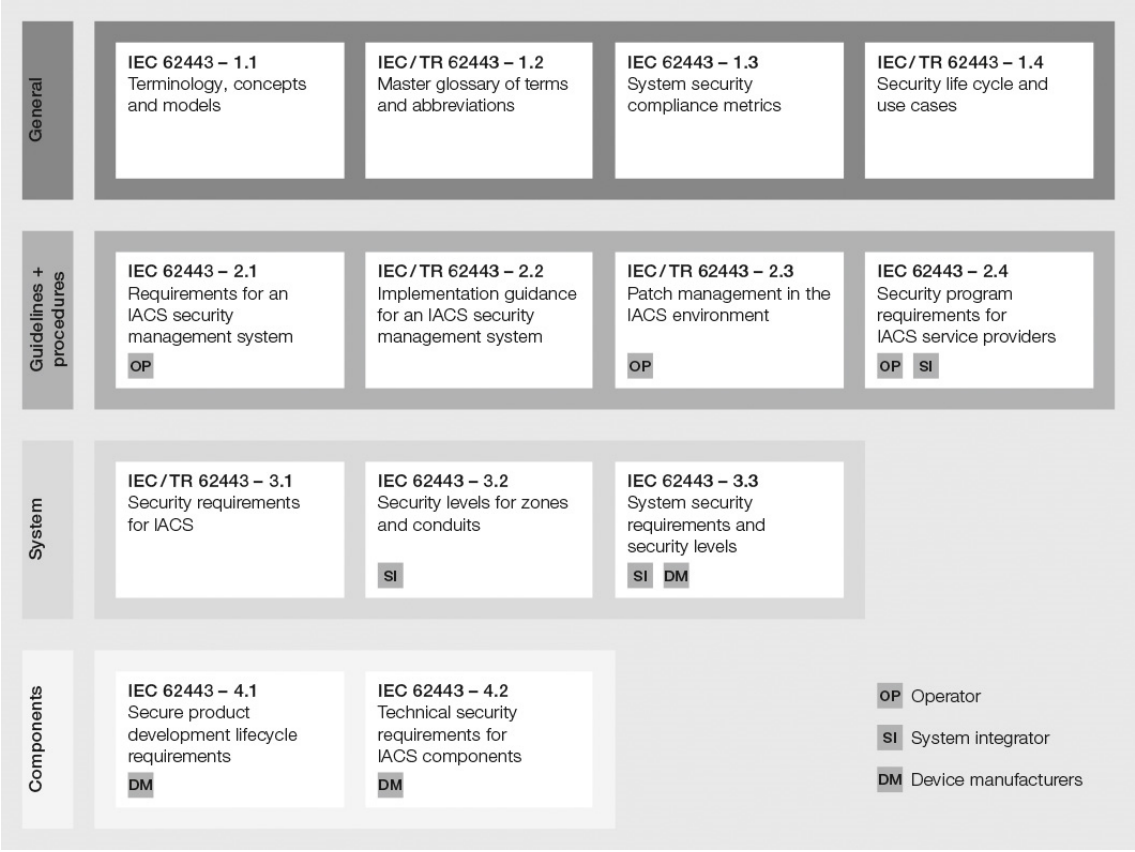
3.3. Onbedoelde security-fouten

De veruit meeste cybervoorvallen zijn noch het resultaat van externe, noch van interne aanvallen, maar vinden onbedoeld plaats. De gevolgen kunnen even zwaarwegend zijn als bij de twee andere bedreigingsscenario's, en kunnen dus bijvoorbeeld tot het uitvallen van netwerken of tot de verspreiding van gevoelige informatie leiden. De redenen zijn met name onjuist geconfigureerde apparaten en bedieningsfouten.
Daarom moeten de productiemedewerkers, die normaliter geen IT-experts zijn, overeenkomstig worden getraind. Bovendien worden netwerken ook zodanig gerealiseerd dat de gevolgen van onjuist geconfigureerde of onjuist bediende apparaten door een segmentatie, dus een verdeling in subnetwerken, en het gebruik van verschillende security-mechanismen worden beperkt.

4. Beoordeling van security

4.1. Normatieve basisprincipes

Security speelt in de klassieke IT al zeer lang een centrale rol, om welke reden er een reeks normen bestaan zoals de reeks van "ISO/IEC 27000 "Information technology - Security techniques - Information security management systems - Overview and vocabulary (ISO/IEC 27000:2016); German version EN ISO/IEC 27000:2017". Deze eisen zijn echter niet zonder meer van toepassing op de automatisering. Want hierbij staat de beschikbaarheid van gegevens op de eerste plaats, wat een essentiële voorwaarde voor feilloze productieprocessen is, terwijl in de IT de vertrouwelijkheid van gegevens de hoogste prioriteit heeft.
Om effectieve security-oplossingen voor de automatisering mogelijk te maken, zijn verschillende organisaties begonnen met het ontwikkelen van overeenkomstige normen. Hierin worden echter alleen deelaspecten zoals de begrenzing van security en safety beschreven. Bovendien zijn ze echter noch als ontwerp, noch als officiële norm beschikbaar, en zijn het dus eerder technische referenties.
Met de norm IEC 62443 "Industriële communicatienetwerken - IT-veiligheid voor netwerken en systemen" is er daarentegen sprake van een internationale normenreeks die reeds in delen is aangenomen en waarin de IT-veiligheid in de automatisering uitgebreid wordt behandeld. De



Afbeelding 1: norm IEC 62443

thema's variëren van de risicoanalyse en Best Practices (beproefde methoden) tot en met de veilige ontwikkeling van producten (Security by Design). Hierdoor vormt de norm IEC 62443

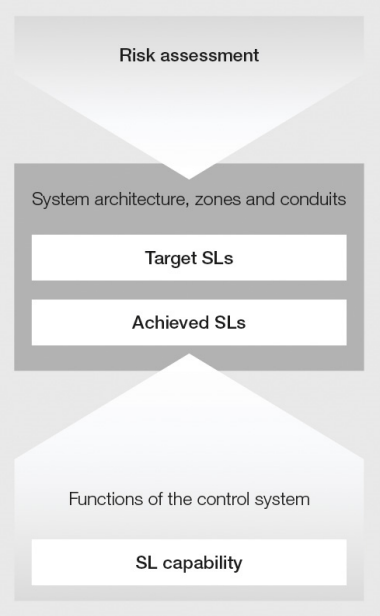
momenteel de beste oriëntatiehulp voor exploitanten van installaties en fabrikanten van apparatuur om security effectief te realiseren.
Het "ICS Security Kompendium" van de overheidsinstantie voor veiligheid in de informatietechniek (BSI) is met name bedoeld voor exploitanten van industriële besturingssystemen. Hierin worden zowel algemene basisprincipes als speciale eisen en relevante normen toegelicht. Bovendien worden passende maatregelen gepresenteerd en worden methoden beschreven hoe deze kunnen worden uitgevoerd.
Terwijl de norm IEC 62443 en het "ICS Security Kompendium" eerder geschikt zijn voor experts, maakt de VDI-richtlijn VDI/VDE 2182 een betrekkelijk eenvoudige toegang tot deze thematiek mogelijk. Bovendien hebben ook diverse ondernemingen uit de automatiseringsbranche publicaties uitgegeven, die inmiddels de omvang van een boek hebben. Vanwege de complexiteit van de industriële security is het beslist raadzaam – vooral wanneer het om de realisatie gaat – een beroep te doen op externe specialisten.

4.2. Risicoanalyse

Een security-strategie begint net als elke andere strategie met een inventarisatie, of anders geformuleerd: de exploitanten van installaties moeten zich eerst een beeld vormen van de

Afbeelding 2: projectstappen van de risicoanalyse

bedreigingen waaraan ze zijn blootgesteld evenals van de ondernemingswaarden die ze in de eerste plaats willen beveiligen. Bij de tweede stap worden vervolgens overeenkomstig IEC 62443 vijf beveiligingsniveaus gedefinieerd, die van 0 (geen gevaar) tot 5 (extreem gevaar) reiken, en waarvoor telkens verschillende eisen gelden. Hoe hier concreet aan kan worden voldaan, wordt echter niet vermeld.



Security Level	Protection
SL 0	No protection
SL 1	Protection against casual or coincidental violation
SL 2	Protection against intentional violation using simple means
SL 3	Protection against intentional violation using sophisticated means
SL 4	Protection against intentional violation using sophisticated means with extended resources

Afbeelding 3: Risk assessment

Als empirische formule geldt dat in principe alle apparaten die een Ethernet-aansluiting hebben, gevaar lopen. Want ze kunnen als het ware als toegangspoort voor externe en interne aanvallen dienen of het uitgangspunt van onbedoelde security-fouten zijn. Wanneer op deze apparaten bovendien gangbare besturingssystemen zijn geïnstalleerd, neemt het risico toe. Met name wanneer hiervoor geen veiligheidsupdates meer worden aangeboden. Om uit te vinden hoe dergelijke systemen succesvol kunnen worden aangevallen en welke malware hiervoor bestaat, is een onderzoek in zoekmachines vaak voldoende.
Een risicoanalyse is echter altijd slechts een momentopname. Want op elk moment kunnen nieuwe bedreigingen ontstaan waarmee rekening moet worden gehouden. Processors golden tot nu toe als onkritisch en hierbij werden onlangs veiligheidslekken ontdekt die onder de namen "Meltdown" en "Spectre" zijn samengevat en veel pc's gevoelig maken voor aanvallen. Hierdoor kwamen onder meer ook soft-PLC's (op software gebaseerde geheugenprogrammeerbare besturingen) binnen het vizier van aanvallers. Kortom: security is een permanent proces dat een lange adem vereist.

4.3. Tegenmaatregelen

Nadat de te beveiligen ondernemingswaarden zijn geïdentificeerd en geprioriteerd – een succesvolle aanval op een besturing heeft normaliter zwaarwegender gevolgen dan die op een visualiseringstool –, moet worden besloten hoe het hoofd moet worden geboden aan de bedreigingen.

Een uitstekende methode is om aanvallen en onbedoelde security-fouten van het begin af aan te voorkomen. Vanwege de complexiteit en dynamiek van de materie kan dit echter niet altijd worden bewerkstelligd. Want zelfs als specialisten de opdracht krijgen om voortdurend naar mogelijke zwakke plekken in het netwerk te zoeken, bestaat er uiteindelijk geen volledige zekerheid met betrekking tot alle eventualiteiten.
Daarom is het belangrijk dat security-problemen direct worden herkend en dat er terstond wordt gehandeld. Hiervoor kunnen onder meer alle gebeurtenissen in het netwerk worden geprotocolleerd (Event Logging) en vervolgens worden geanalyseerd. Zo kan bijvoorbeeld worden vastgesteld wanneer een aanval is gepleegd op een bepaald apparaat. Wanneer bijvoorbeeld onderhoudswerkzaamheden hebben plaatsgevonden op een moment waarop dit anders nooit gebeurt, moeten alle alarmklokken gaan luiden.
Wanneer een aanval succesvol was of de gegevensveiligheid al onbedoeld was geschonden, moet het probleem zo snel mogelijk worden verholpen en de oorzaak grondig worden geanalyseerd, zodat dit in de toekomst niet opnieuw kan gebeuren.

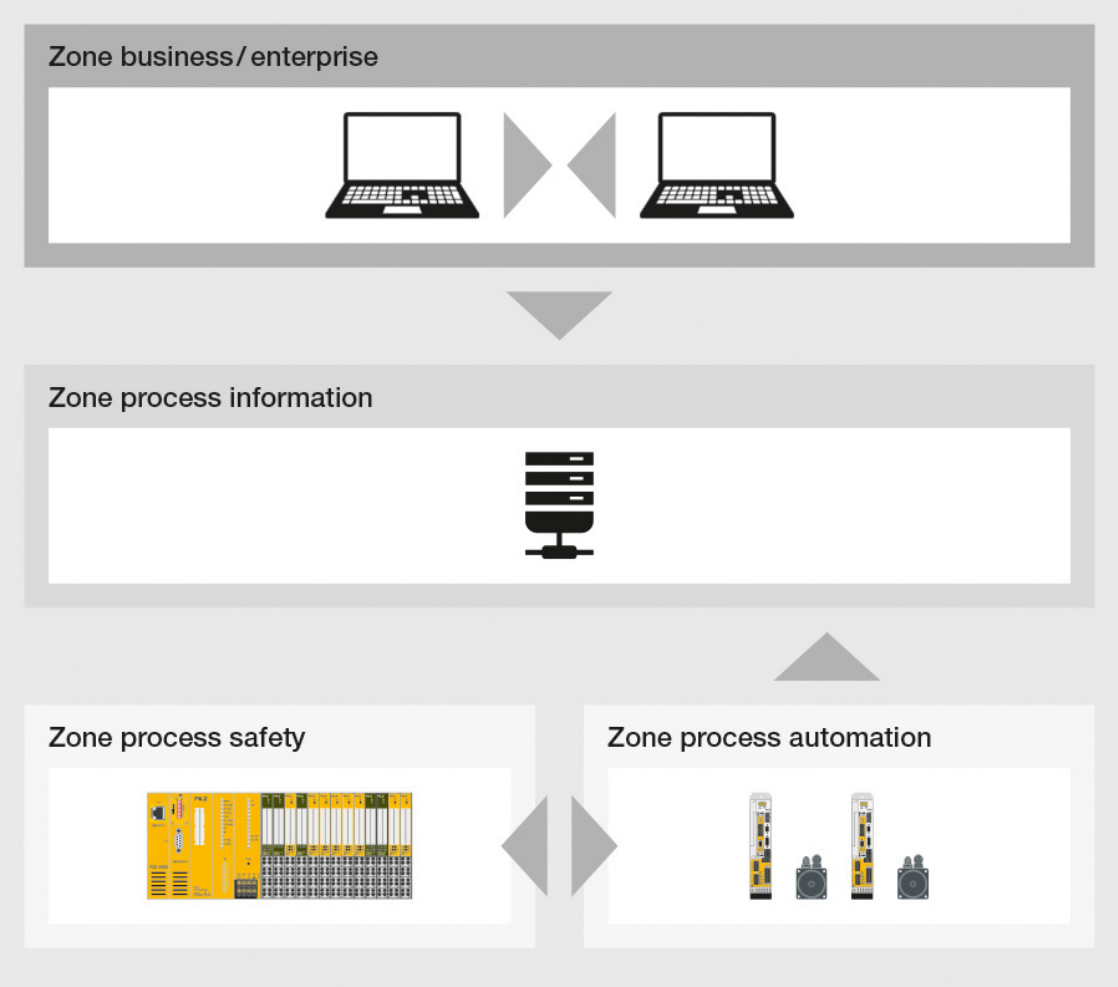
5. Realisatie van security-strategieën

5.1. Firewalls

Een maatregel om security-strategieën te realiseren, is de beveiliging van het netwerk door speciale apparaten. Hoewel ook routers en schakelaars veiligheidsmechanismen kunnen ondersteunen, spelen firewalls nog altijd een centrale rol. Hierbij gaat het ofwel om softwareoplossingen of om appliances (combinatie van hard- en software), die aan de hand van individueel gedefinieerde regels en met functies zoals Deep Packet Inspection of Intrusion Detection het complete dataverkeer bewaken.
Omdat firewalls normaliter op ingewikkelde wijze moeten worden geconfigureerd, is uitgebreide IT-kennis vereist, die bij de productie vaak ontbreekt. Daarom heeft Pilz met de SecurityBridge een op de industrie afgestemde firewall ontwikkeld die middels toepassingsspecifieke voorinstellingen volgens het plug-and-play-principe eenvoudig in gebruik kan worden genomen. Hiermee kunnen niet alleen besturingssystemen van Pilz tegen aanvallen en enige onbevoegde toegang worden beveiligd, maar kunnen ook procesgegevens met een geringe latentie worden overgedragen.
De meest effectieve security-apparaten hebben echter weinig nut wanneer ze niet vanaf het begin veilig zijn ontwikkeld en dit aspect ook gedurende de complete levenscyclus in acht wordt genomen – trefwoord Secure by Design. Want processors kunnen, zoals de voorbeelden Meltdown en Spectre aantonen, onverwachts niet meer veilig zijn. Bovendien is het altijd mogelijk dat malware in een productieproces wordt binnengeloodst en vervolgens in de producten wordt geïnstalleerd om later als achterdeur voor aanvallen te dienen. Om dergelijke scenario's te voorkomen, moeten de fabrikanten voortdurend zoeken naar nieuwe bedreigingen in de cyberwereld en – indien noodzakelijk – zo snel mogelijk aanvullende veiligheidsmechanismen in hun apparaten integreren en patches (veiligheidsupdates) beschikbaar stellen.

5.2. Segmentatie van het netwerk

Firewalls worden doorgaans aangebracht bij de overgang van een veilig naar een onveilig netwerk, bijvoorbeeld tussen een intranet en internet. Deze zogeheten perimeterbeveiliging bereikt echter snel haar grenzen wanneer het erom gaat te voorkomen dat malware zich als een epidemie over het complete netwerk uitbreidt en deze net als de gekoppelde installaties ontwricht.
Daarom voorziet de norm IEC 62443 in een onderverdeling van netwerken volgens het "Zones and Conduits"-model.



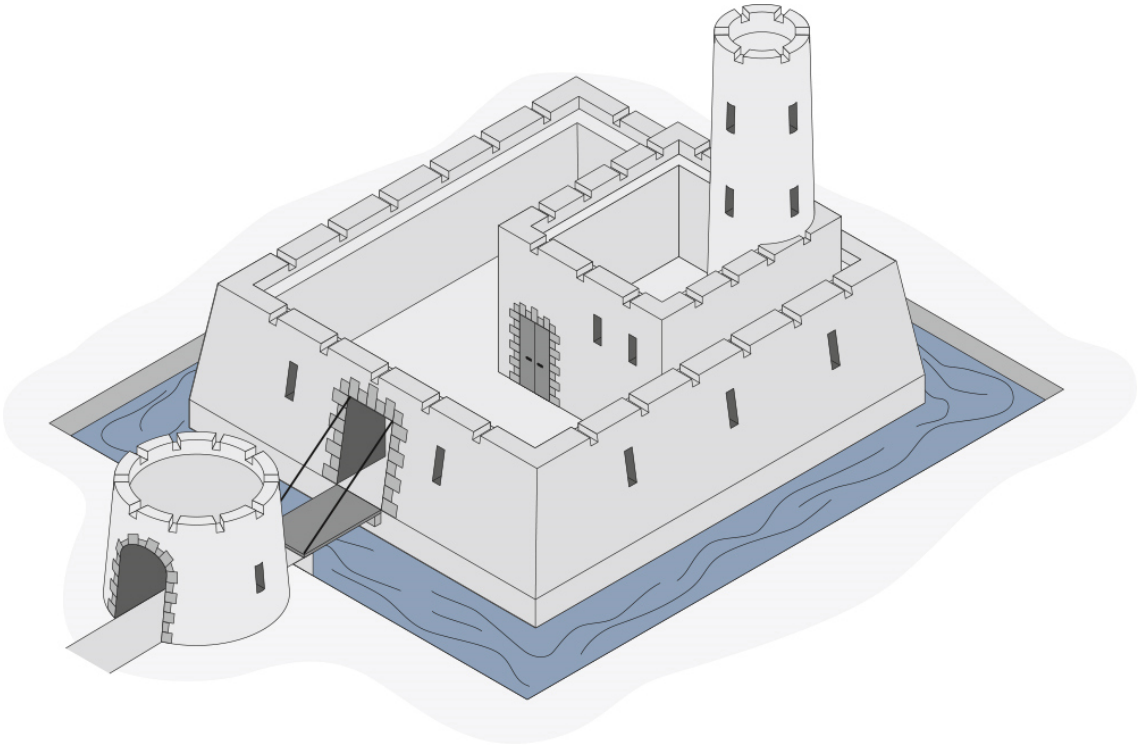
Afbeelding 4: "Zones and Conduits"-model

Hierdoor kunnen bijvoorbeeld het beheer- en het productienetwerk worden gescheiden. Indien nodig, kan ook dit netwerk worden gesegmenteerd, en wel tot afzonderlijke productiecellen. Hiervoor worden eerst zones geïdentificeerd waarin apparaten soortgelijke security-eisen hebben, waarna ze door firewalls of veilige routers van elkaar worden afgeschermd. Zo kan worden gegarandeerd dat via de leidingen (conduits) tussen de zones alleen die apparaten kunnen zenden en ontvangen die hiertoe gerechtigd zijn.
Wat dit in de praktijk betekent, wordt door het volgende voorbeeld verduidelijkt: onbedoelde security-fouten worden vaak door onjuist geconfigureerde apparaten veroorzaakt. De gevolgen zijn bijvoorbeeld een overdracht van gegevens of zogeheten broadcaststormen, die wederom

andere apparaten kunnen schaden. Wanneer netwerken daarentegen in beveiligde subnetwerken worden gesegmenteerd, wordt alleen schade toegebracht aan de apparaten in de zone waarin het probleem zich heeft voorgedaan. Dit geldt eveneens voor de gevolgen van abusievelijke of opzettelijke interne aanvallen.

5.3. Defense-in-Depth

Om het aanvallers zo moeilijk mogelijk te maken, kan het "Zones and Conduits"-model ook dienen als centraal element voor een diep gestaffelde verdediging (Defense-in-Depth) van het netwerk. Bij dit principe, dat bij de constructie van versterkingswerken wordt toegepast, worden indringers afgeweerd met telkens nieuwe en andere hindernissen. Zo konden burchten in de Middeleeuwen bijvoorbeeld zijn beschermd door grachten, valkuilen, ophaalbruggen, torens en meerdere muren.
De zones en leidingen van een netwerk zijn vergelijkbaar met de poorten van een burcht. De muren en andere hindernissen worden gevormd door de firewalls en veilige routers, die verschillende security-mechanismen ondersteunen. Hiertoe behoren bijvoorbeeld een toegangscontrole conform IEEE 802.1x en Access Control Lists, die onbekende apparaten en protocollen blokkeren. Bovendien bestaan er mechanismen die bij verdachte netwerkactiviteiten alarmen activeren of herkennen wanneer IP-pakketten met vervalste afzenderadressen worden verstuurd (IP-spoofing).



Afbeelding 5: verdedigingsniveaus aan de hand van het voorbeeld van een burcht

Hierdoor wordt gewaarborgd dat een aanvalsmethode alleen niet tot "succes" leidt. Om verder binnen te dringen in een netwerk moet een aanvaller dus altijd weer nieuwe, elkaar overlappende beschermlagen overwinnen. En zelfs wanneer hij erin zou slagen in het subnetwerk van een productiecel binnen te dringen, is het voor hem nauwelijks mogelijk om van daaruit doelen in aangrenzende subnetwerken aan te vallen.

5.4. Organisatorische maatregelen

Of producerende ondernemingen zichzelf beschermen tegen bedreigingen uit de cyberwereld, is, zoals reeds besproken, altijd een afweging van kosten en baten. In Duitsland bijvoorbeeld zijn hiertoe volgens de IT-veiligheidswet uitsluitend exploitanten van infrastructuren voor algemeen nut verplicht, waartoe bijvoorbeeld energie, verkeer en gezondheid behoren. Ook in andere landen bestaan vergelijkbare wettelijke voorschriften, in de VS bijvoorbeeld voor de beveiliging van stroomnetten.
Met het oog op de talloze bedreigingen is er veel voor te zeggen om installaties zowel tegen opzettelijke als onbedoelde security-fouten te beveiligen. Met uitgekiende firewall-concepten alleen is het probleem echter niet volledig opgelost. De complete onderneming moet security eerder als het ware internaliseren. Bovendien moeten er richtlijnen worden opgesteld die niet alleen voor alle medewerkers gelden, maar ook voor partners zoals fabrikanten van apparatuur en dienstverleners.
Bovendien is het belangrijk dat IT- en automatiseringsspecialisten nauw samenwerken, als gevolg waarvan zij vertrouwd moeten raken met de verschillende eisen en werkwijze van de telkens andere partij. Ten slotte dient er een organisatie te worden opgericht waarvan de leden verantwoordelijk zijn voor de gegevensveiligheid bij de productie en de voortdurende verbetering hiervan. Aan de top staat idealiter een security-functionaris die tot het hoogste leidinggevende niveau behoort of de hoogste leidinggevende(n) tenminste direct informeert.

5.5. Trainingen

"Wie ophoudt beter te worden, heeft het opgegeven om goed te zijn", aldus een succesformule die ondernemingen ook bij security ter harte zouden moeten nemen. Een mogelijkheid hiervoor bieden regelmatige trainingen, waarmee bijvoorbeeld het bewustzijn van medewerkers wordt verscherpt. Andere onderwerpen kunnen bijvoorbeeld informatie over actuele bedreigingen zijn of instructies over hoe bepaalde veiligheidslekken kunnen worden verholpen. Want alleen wanneer de security-deskundigheid gericht wordt uitgebreid, kan worden voorkomen dat medewerkers vanwege een ontbrekende kwalificatie onjuiste beslissingen maken.
Er zijn talloze aanbieders die security-trainingen geven. De seminars van Pilz, die zowel in de hoofdvestiging in Ostfildern bij Stuttgart als ook bij klanten of – in gecomprimeerde vorm – als webinar worden aangeboden, zijn met name bedoeld voor constructeurs van machines en ontwerpers van installaties. In de seminars wordt een fundamenteel overzicht geboden en wordt toegelicht hoe gevaren kunnen worden herkend en geminimaliseerd. De thema's variëren van netwerkarchitectuur, de authenticatie van netwerkdeelnemers en de versleuteling van gegevens tot en met een veilig onderhoud op afstand.

6. Samenvatting en vooruitblik

Om maximale security te bereiken, is het vooral belangrijk dat er exacte kennis bestaat omtrent de architectuur van het netwerk evenals de communicatieprotocollen en het type dataverkeer. Want alleen zo kunnen zowel externe als interne bedreigingen worden afgeweerd, ongeacht of ze opzettelijk of niet-opzettelijk zijn.
Vroeger was security eigenlijk alleen in de klassieke informatietechnologie (IT) een thema. Sinds in het kader van Industrie 4.0 in productie-installaties steeds vaker serieproducten op consumentengebied en complexe besturingssystemen worden toegepast, moet de automatisering hier echter ook rekening mee houden. Omdat de normen van de IT niet één op één kunnen worden overgedragen, zijn er nieuwe normen ontwikkeld, waarvan de norm IEC 62443 de belangrijkste is. Want hierin wordt gedefinieerd hoe een uitgebreide security-strategie voor de industrie stap voor stap kan worden ontwikkeld en gerealiseerd.
Tegelijkertijd moet in deze strategieën ook safety worden geïmplementeerd, omdat de functies hiervan uiteindelijk alleen kunnen worden gewaarborgd wanneer de betreffende gegevens betrouwbaar worden overgedragen. Immers, security-bedreigingen kunnen voortdurend veranderen en dus ook de tegenmaatregelen. Dat wil zeggen dat hoewel deze twee aspecten van de automatisering ook verder zelfstandig blijven, ze toch nauw op elkaar moeten worden afgestemd. Het goede bericht: wie al bekend is met safety, zal gemakkelijker omgaan met security, omdat de procedures op elkaar lijken.

Verklarende woordenlijst

Access Control List	Bij een Access Control List (ACL; Nederlands: toegangscontrolelijst) wordt bepaald in welke omvang afzonderlijke personen, computers of netwerken via welke diensten toegang hebben tot de router of schakelaar. Deze toegang kan worden vastgelegd voor afzonderlijke computers of netwerken en voor de betreffende toegangsmethode.
Broadcaststorm	Een broadcaststorm is een sterke opeenhoping van broadcastverkeer in een computernetwerk, die ertoe leidt dat geen netwerkverbindingen meer worden opgebouwd en bestaande verbindingen onderbroken kunnen worden. Een broadcaststorm kan ontstaan door een aanval, door een onjuiste configuratie of door een slecht netwerkdesign.
Deep Packet Inspection	Deep Packet Inspection staat voor een procedure in de netwerktechniek om datapakketten te bewaken en te filteren. Hierdoor kunnen spams worden bestreden en bovendien kan Deep Packet Inspection worden gebruikt voor de controle van overbelasting en een reductie van dataverkeer.
DES (Data Encrption Standard)	Data Encryption Standard, kortweg DES, is een gestandaardiseerde symmetrische versleutelingsmethode.
Intrusion Detection System	Met behulp van intrusiedetectie kunnen aanvallen die tegen een computersysteem of computernetwerk zijn gericht, tijdig worden herkend, zodat er snel tegenmaatregelen kunnen worden getroffen.
IP-spoofing	IP-spoofing betekent in computernetwerken het vervalsen van afzender-IP-adressen van IP-pakketten om het aangevallen IT-systeem een onjuiste identiteit voor te spiegelen. Elk IP-pakket bevat in de hoofdgegevens het afzenderadres. Een aanvaller kan dit afzenderadres in de hoofdgegevens zodanig vervalsen dat het lijkt of het pakket door een andere computer is verzonden. Veel protocollen van de TCP/IP-familie kunnen slechts via een IP-adres worden geverifieerd. Als deze is vervalst, kunnen veiligheidsmaatregelen zoals de op het IP-adres gebaseerde verificatie in het netwerk worden uitgeschakeld. IP-spoofing is hierbij slechts een type spoofing. Tegenwoordig vallen onder "spoofing" alle methoden waarmee verificatie- en identificatiemethoden worden omzeild waarbij vertrouwelijke adressen of hostnamen in netwerkprotocollen worden gebruikt.
Hashing-algoritme MD5	MD5 (Message Digest Algorithm 5) behoort tot de groep van mathematische eenwegfuncties. Dit betekent dat het niet

	eenvoudig mogelijk is op grond van het resultaat de ingangsparameters te achterhalen. Bij MD5 wordt een willekeurige hoeveelheid ingangsgegevens weergegeven op een waarde met een lengte van 128 bit. Bij een hash-algoritme wordt ervan uitgegaan dat het extreem moeilijk is twee ingangsdocumenten te vinden die dezelfde resultaatwaarde (collisie) leveren. In het geval van MD5 zijn sinds enige tijd zwakke plekken bekend waardoor een aanvaller collisies tot stand kan brengen.
Meltdown en Spectre	Meltdown en Spectre zijn veiligheidslekken die in microprocessors zijn ontdekt, waardoor een ongeautoriseerde toegang tot het geheugen van vreemde processen mogelijk is.
Netwerkstandaard IEEE 802.1x	IEEE 802.1X is een netwerkstandaard voor de authentificatie van gebruikers in IEEE-802-netwerken. Deze standaard fungeert als controlesysteem dat de gebruiker controleert voordat hij toegang krijgt tot het LAN- of WLAN-netwerk.
Security-doel: integriteit	Integriteit in verband met gegevens zorgt ervoor dat gegevens evenals de werkwijze van een systeem altijd correct zijn. Is integriteit gewaarborgd, dan kunnen ongeautoriseerde of onopgemerkte veranderingen direct worden herkend en uitgesloten.
Segmentatie van netwerken	Segmentatie betekent dat een netwerk in kleinere eenheden wordt opgedeeld. Deze eenheden worden vervolgens gekoppeld aan firewalls of andere apparaten waarmee de communicatie kan worden beperkt. Hierdoor worden zowel de gevolgen van broadcaststormen of andere "abusievelijke" gebeurtenissen als de gevolgen van aanvallen beperkt.

Lijst van afbeeldingen

Wij zijn internationaal vertegenwoordigd. Voor meer informatie kunt u onze homepage www.pilz.com raadplegen of contact opnemen met ons hoofdkantoor.

Hoofdkantoor: Pilz GmbH & Co. KG, Felix-Wankel-Straße 2, 73760 Ostfildern, Duitsland
telefoon: +49 711 3409-0, fax: +49 711 3409-133, e-mail: info@pilz.de, internet: www.pilz.com

PILZ
THE SPIRIT OF SAFETY