SIEMENS

WHITEPAPER

Cyberweerbaarheid van de industrie: Schijnveiligheid?

Over de auteur

Emma Plak behaalde in 2024 haar Masterdiploma in Global Criminology aan de Universiteit Utrecht. Haar thesis met de titel *"Threats to operational security: protect or neglect"* is een kwalitatief onderzoek naar digitale veiligheid en verantwoordelijkheid binnen de industrie. Hoe wordt de verantwoordelijkheid van managers voor digitale veiligheid ervaren? Om antwoord te krijgen op deze vraag hanteerde Emma drie kwalitatieve onderzoeksmethoden, waaronder semigestructureerde interviews met het management van bedrijven uit de industriële sector. In deze White Paper vatten we de belangrijkste inzichten samen. De vermelde interviewbronnen en onderzoeksdetails zijn niet publiek beschikbaar, maar bekend bij de betrokkenen.

Inhoudsopgave

1 Motivatie

Criminologie gaat over het gedrag van delinquenten in de maatschappelijke, antropologische en psychologische context. In een snel digitaliserende samenleving neemt cybercriminaliteit sterk toe. Steeds vaker hebben hackers het gemunt op OT-systemen (Operationele Technologie), die door de integratie met IT-systemen kwetsbaarder geworden zijn voor cyberaanvallen.

Voor criminologen is OT-security een nog jong, maar belangrijk onderzoeksterrein. Cyberaanvallen op OT-systemen kunnen een enorme impact hebben op de samenleving. Ze staan in de top 5 van mondiale risico's die tot sociale ontwrichting kunnen leiden. Zo probeerde in 2021 een hacker in Florida het water in een drinkwatervoorziening te vergiftigen door er een gevaarlijke hoeveelheid natriumhydroxide (bijtend soda) aan toe te voegen. De aanvaller verschafte zich op afstand toegang tot de drinkwatervoorziening. Dankzij het snelle ingrijpen van een leidinggevende van de faciliteit raakte het drinkwater niet vergiftigd en was er geen dreiging voor de volksgezondheid. Dit is een voorbeeld hoe *ransomeware* uit IT-omgevingen in OT-omgevingen *killware* kan zijn.

Een onschuldige slok water.
Cyberaanvallen op kritieke OT-infrastructuur kunnen de hele wereld ontregelen.

Ook de industriële sector krijgt steeds vaker te maken met cyberaanvallen op OT-systemen. Onder meer geopolitieke spanningen vergroten de dreiging. Behalve individuele bedrijven loopt de hele supply chain gevaar wanneer netwerken en apparatuur onvoldoende beschermd worden. De voedselbeschikbaarheid en -veiligheid kunnen door een cyberaanval ernstig verstoord worden.

Door nieuwe wet- en regelgeving worden bedrijven verplicht hun OT beter te beveiligen. Wet- en regelgeving is een katalysator voor de implementatie van een bedrijfsklimaat waarbinnen verantwoording jegens cybersecurity een hogere plaats krijgt en de cyberweerbaarheid toeneemt. In hoeverre zijn productiebedrijven al voorbereid op nieuwe wet- en regelgeving? Emma Plak slaat vanuit global criminology de brug tussen mens en techniek en legt de cybersecurity-kwetsbaarheden bloot. De conclusies kunnen dienen als een kader voor de industrie.

2

Externe dreiging versus interne weerbaarheid

Hoewel de externe dreiging – het risico om slachtoffer te worden van een cyberaanval – toeneemt, is zo'n 60 procent van de Nederlandse bedrijven zich onvoldoende bewust van de schade die een OT-hack kan veroorzaken. Hierdoor worden te weinig of niet-adequate maatregelen genomen om de organisatie tegen een cyberaanval op de OT te beschermen.

Source: Gartner
743174_C

Figuur 1: The 10 Operational Technology Security Controls (Gartner, 2021).

De bovenstaande figuur (Gartner, 2021) laat zien welke stappen er nodig zijn om de OT-security op orde te brengen.

Stap één is het in kaart brengen van de verantwoordelijkheden voor cybersecurity. Wie moet wat doen binnen de organisatie? Zelfs de beste beveiligingstechnologie is ontoereikend als mensen niet weten wat hun verantwoordelijkheden zijn. Emma Plak vroeg middenmanagers van de industrie hoe zij hiertegen aankijken om inzicht te krijgen in hun gedrag. Uit hun antwoorden destilleerde zij twee risico's ten aanzien van de OT-beveiliging:

- → Versnippering van verantwoordelijkheid
- → Gebrek aan kennis

Dit kan leiden tot een gevoel van schijnveiligheid.

2.1. Risico 1: Versnippering van verantwoordelijkheid

De geïnterviewden geven aan zich bewust te zijn van de cyberrisico's die de organisatie loopt. Met de juiste kennis en adequate werkwijzen kan dit risico volgens hen gereduceerd worden. Tegelijkertijd is niet duidelijk *wie* hierin *welke* verantwoordelijkheid heeft. Dit blijkt uit het volgende citaat:

> "Ik heb daar waarschijnlijk een rol in, maar ik zou niet weten wie de hoofdverantwoordelijkheid heeft."

In een aantal gevallen leggen de geïnterviewden de verantwoordelijkheid neer bij een andere partij:

> "Dat moet toch eigenlijk vanuit het hogere management komen?"

Het bovenstaande citaat is een voorbeeld van neutralisatietechniek: door een beroep te doen op in dit geval een hogere autoriteit neutraliseert men de eigen rol. Versnippering van verantwoordelijkheid kan er echter toe leiden dat er onvoldoende toezicht wordt gehouden op digitale veiligheid. Het levert meer ruis op dan oplossingen.

2.1.1. Verantwoordelijkheidsvacuüm

Wanneer verantwoordelijkheden en rollen niet duidelijk zijn, loopt de organisatie het risico in een *grijze zone* terecht te komen, waarin niemand zich bezighoudt met de monitoring en inspectie van de OT. Er ontstaat een verantwoordelijkheidsvacuüm (Lindeman, 2012; Wolswinkel and Spronk, 2019) waardoor problemen onopgelost blijven.

> "Misschien is het wel mijn verantwoordelijkheid, maar dan moet dat nog gezegd worden."

Uit het bovenstaande citaat komt het verantwoordelijkheidsvacuüm duidelijk naar voren. Naar anderen wijzen betekent dat men zichzelf niet verantwoordelijk voelt en dus ook geen actie onderneemt.

> "Het is veel te gefragmenteerd door de organisatie. Mensen hebben geen idee wie ze moeten contacteren."

Bedreiging

→ Middenmanagers hebben de neiging hun verantwoordelijkheid voor OT-security uit te besteden en te verwaarlozen. Ze weten niet wie waarvoor verantwoordelijk is.

“The oldest and strongest kind of fear is fear of the unknown.”

H.P. Lovecraft

2.2. Risico 2: Gebrek aan kennis

Uit de interviews blijkt ook dat cybersecurity nog vaak wordt gezien als een ‘IT-issue’ en minder relevant wordt geacht voor de OT. Dit valt af te leiden uit het volgende citaat:

> “Het is een ver-van-je-bed show, wat is nou de kans dat het ons gebeurt?”

Met als bijkomend risico dat mensen niet altijd de juiste kennis hebben op het gebied van OT-security. Hiervoor is men vaak afhankelijk van externe partijen zoals technologieleveranciers en consultants van buiten de organisatie.

> “Ik kan niet zeggen of mijn netwerk secure is, want ik heb daar de kennis niet voor. Hiervoor zijn we aangewezen op expertise van externe deskundigen.”

Naast interviews met het middenmanagement uit de industrie analyseerde Emma Plak gesprekken tussen het middenmanagement en een technologieleverancier. Ook hieruit blijkt dat de kennis van OT-security binnen de organisatie ontoereikend is. Niet altijd zijn bedrijven zich hiervan bewust. Vaak geeft een deel van de organisatie de indruk deze kennis in huis te hebben en ermee bezig te zijn, maar zonder mandaat en volledig zicht op de problematiek.

Deze *schijnkennis* creëert als een soort sluipmoordenaar een blinde vlek voor cybersecurity, wat onveilige situaties in de hand werkt.

Bedreiging

→ Het beveiligen van de procesautomatisering vereist specifieke kennis. Niet altijd zijn bedrijven zich bewust dat ze deze kennis niet in huis hebben. Waardoor een blinde vlek kan ontstaan voor de productie.

2.3. Schijnveiligheid

Schijnverantwoordelijkheid en -kennis kunnen leiden tot het onterechte gevoel dat de OT-security binnen de organisatie geborgd is. De dingen lijken veilig, maar zijn het in werkelijkheid niet.

> "Misschien heb ik een beetje een vals gevoel van veiligheid."

Een vals gevoel van veiligheid veroorzaakt onrust, frustratie en kan het vertrouwen in de organisatie beschadigen. Terwijl cybercriminelen steeds slimmer en dynamischer worden, lijkt de eigen organisatie het tempo niet bij te kunnen houden. Hierdoor kan een gevoel van machteloosheid ontstaan ten aanzien van cybercriminaliteit. Alsof een ongrijpbaar orgaan de macht overneemt en een kleine groep in de greep houdt. Met vaak ontevredenheid richting de eigen organisatie als gevolg.

Bedreiging

- → Door onterechte verantwoordelijkheid en valse kennis lijkt de OT-beveiliging geborgd te zijn, zonder dat er concrete acties worden ondernomen.
- → Dit wordt in stand gehouden door de organisatiestructuur.
- → Als gevolg hiervan kan de productieveiligheid in het gedrang komen.

> "Wij zien ook wel dat onze huidige werkwijze niet toekomst-bestendig is en we realiseren ons dat er risico's zijn. Maar hoe krijg je dit bij het hoger management voor het voetlicht?"

De roep om duidelijkheid over verantwoordelijkheden en kennis sluit aan bij de *responsibiliseringstheorie* van Rik Peeters, onderzoeker bij de Nederlandse School voor Openbaar Bestuur, die verklaart dat uitbesteding van verantwoordelijkheden, bijvoorbeeld via nieuwe wetgeving, kan leiden tot versnippering van verantwoordelijkheden en daarmee tot onduidelijkheden.

Bedreiging

- → Met nieuwe wet- en regelgeving legt de Europese overheid druk op organisaties om hun OT-beveiliging op orde te brengen. Wanneer mensen binnen organisaties ervan uitgaan dat iemand anders dit wel zal doen, ontstaat een vals gevoel van veiligheid met alle risico's van dien.

3

Discrepantie in veiligheidsbewustzijn

Uit het vorige hoofdstuk onthouden we de onbalans tussen externe dreigingen en intern bewustzijn en verantwoordelijkheid voor en kennis van OT-security. Dit in tegenstelling tot IT-security en persoonsveiligheid waar organisaties vaak wél beleid voor en grip op hebben. In dit hoofdstuk zoomen we in op enkele oorzaken, waarna we in het volgende hoofdstuk oplossingen aandragen om deze kloof versneld te dichten.

3.1. IT/OT: Een wereld van verschil

Productiebedrijven worden dagelijks op meerdere terreinen met veiligheid geconfronteerd. Te beginnen met de persoonlijke veiligheid van medewerkers en het veilig houden van productie-processen. De geïnterviewden geven aan dat hun organisatie hier breed op ingericht is. Voorbeelden zijn het gebruik van Persoonlijke Beschermingsmiddelen (PBM), het verplicht volgen van protocollen en veilige looproutes door de productiehal.

> "Op het gebied van persoonlijke veiligheid en procesveiligheid hebben wij meerdere beveiligingslagen."

	Protecting	Priority	Update Frequency	Operating System	Protocols	Cyber Criminal Motivation	Cyber Attack Mission
IT	Data	1. Confidentiality 2. Integrity 3. Availability	High	Standardised	Standardised	Monetisation	IT Stack Specific
OT	Asset	1. Safety & Environment 2. Availability 3. Integrity 4. Confidentiality	Very Low	Proprietary	Proprietary	Disruption	Industry Specific

Gevraagd naar cyberbeveiliging vertellen de geïnterviewden in eerste instantie over hun IT-security, die goed geregeld is. Hiermee houdt zich binnen de organisatie een specifiek team bezig. Dit is niet het geval voor de OT-security.

> "Je weet gewoon dat IT beter beveiligd is omdat daar een bepaald team bij betrokken is. Maar OT-beveiliging moet van onze kant komen."

Bedreiging

- → Middenmanagers zien de verantwoordelijkheid van operationele technologieën als iets dat vooral te maken heeft met persoonsveiligheid.
- → OT-security staat niet hoog op de prioriteitenlijst.

3.2. Invloed van procesautomatisering

Hoe komt het dat IT-beveiliging en persoonsveiligheid in organisaties vaak beter geborgd zijn dan OT-beveiliging? Dit valt deels te verklaren door de enorme inhaalslag die OT de laatste jaren ten opzichte van IT heeft gemaakt op het gebied van automatisering en digitalisering. Dit vraagt om nieuwe vaardigheden van zowel operators als managers. Naarmate proceskennis steeds meer 'ingebakken' zit in automatiseringsoplossingen verschuift de verantwoordelijkheid van operators van uitvoerende taken (bedienen van machines) naar toezichthoudende taken. Hiertoe moeten ze het gehele proces kunnen overzien, monitoren en analyseren.

Geautomatiseerde en gedigitaliseerde productiesystemen vereisen regelmatige updates als men ze cybersecure wil houden. Een idee waaraan de OT-wereld nog steeds moet wennen. Om verstoringen te voorkomen en de continuïteit te borgen, wordt van oudsher binnen productieomgevingen niet regelmatig gepatcht. Dit blijkt ook uit de interviews van Emma Plak:

> "We geven er de voorkeur aan om iets te installeren, en als het dan werkt blijven we eraf."

3.3. Invloed van vergrijzing

De geïnterviewde middenmanagers zien een aantal obstakels om binnen de organisatie snel de benodigde kennis en vaardigheden te kunnen verwerven. Eén daarvan is vergrijzing. Dit heeft een negatieve impact op zowel de interne dynamiek als het bewustzijn van digitale veiligheid.

> "Wij hebben de vereiste kennis niet en het is moeilijk deze te verwerven. Mijn hele team bestaat uit mensen op leeftijd. Ik ben al blij dat ze een computer kunnen gebruiken."

Voor ouderen gaan de technologische ontwikkelingen vaak te snel om ze nog kunnen te volgen. Jongere generaties hebben hier meer affiniteit mee.

4

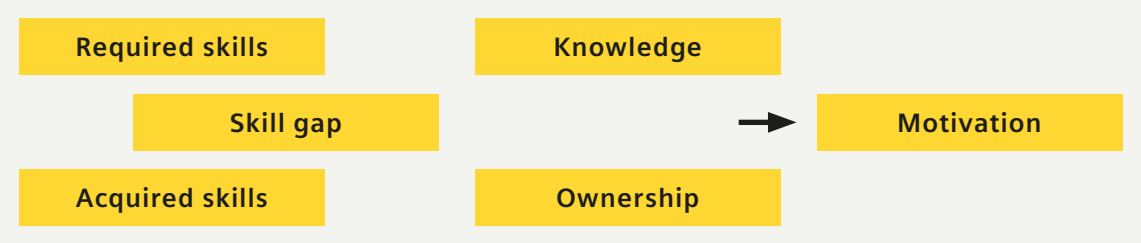
De cirkel doorbreken

Schijnkennis en -verantwoordelijkheid leiden tot schijnveiligheid. In organisaties waar OT-security geen prioriteit krijgt, stagneert uiteindelijk ook het bewustzijn voor deze problematiek. Wat kunnen bedrijven doen om het tij te keren en hun OT-security versneld naar een hoger niveau te tillen?

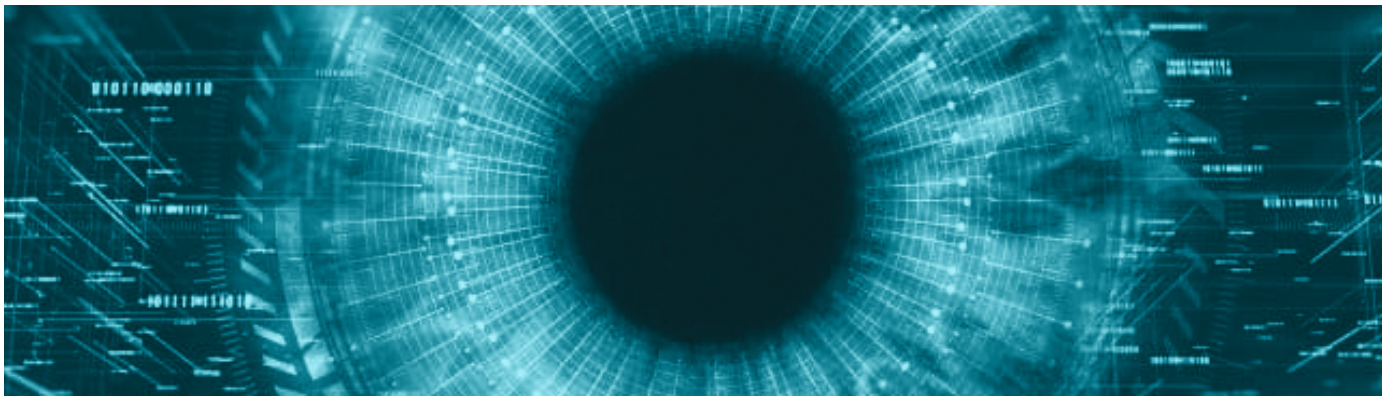
4.1. Het belang van motivatie

Motivatie is cruciaal voor organisaties om de cirkel te doorbreken. Medewerkers moeten kansen krijgen om nieuwe vaardigheden aan te leren die door de automatisering van productieprocessen noodzakelijk geworden zijn. Uit het vorige hoofdstuk blijkt dat er een discrepantie ontstaan is tussen de vereiste werkzaamheden en inzichten van medewerkers en hun werkelijke werkzaamheden en inzichten. Dit leidt tot demotivatie en onwil om uitdagingen op te pakken (Shanthi & Sharma, 2019).

Werkgevers hebben er alle belang bij deze 'skill gap' weg te werken door hun medewerkers bij te scholen. Zij zullen hierdoor gemotiveerder worden om een veilige werkomgeving en daarmee ook veiligheid voor de samenleving te borgen.



Figuur 2



4.2. Het belang van vertrouwen

In het vorige hoofdstuk bleek hoe procesautomatisering leidt tot een verschuiving van verantwoordelijkheid. Het overnemen van menselijke handelingen door machines maakt bedrijven afhankelijker van techniek om hun fabriek te kunnen runnen. Daarmee worden ze ook financieel en bedrijfsmatig afhankelijk.

> "Een ongeplande shutdown kost algauw 40.000 – 80.000 euro per uur."

Door de verschuivende afhankelijkheidsrelaties wordt vertrouwen in technologie een essentiële succesfactor. Diverse wetenschappelijke onderzoeken hebben aangetoond dat mensen niet met nieuwe (automatiserings-)technologie willen werken als ze er geen vertrouwen in hebben. Dit omvat óók vertrouwen in het vermogen van de organisatie om met deze technologie om te gaan en het tempo van de automatisering bij te kunnen houden. Hier sluit het thema 'opleiden en bijscholen' naadloos bij aan

4.3. Prioriteiten stellen

Helaas hebben organisaties vaak andere prioriteiten dan het dichten van de bovengenoemde skill gap. Ze geven bijvoorbeeld de voorkeur aan trainingen op andere gebieden. Trainingen in OT-security worden ervaren als 'duur' en roepen vanwege de vergrijzende werknemersgroep weerstand op. Bovendien zijn de resultaten niet zichtbaar op de korte termijn. Een ander tegenargument is dat er sowieso al 'trainingsmoeheid heerst en men werknemers niet wil overbelasten'.

> "Een diepgaande training zou kunnen helpen, maar je kunt je voorstellen dat we met ons team veel trainingen doen. Dit zijn mensen die elke dag met hun handen bezig zijn, zij weten wat er moet gebeuren. Als we het zouden doen, zouden we klachten krijgen. Het is niet eenvoudig."

Op basis van dergelijke argumenten worden investeringen in cybersecuritymaatregelen (waaronder trainingen) uitgesteld of voor zich uitgeschoven. Problemen worden vermeden onder het mom van 'onwetendheid is gelukzaligheid'. Verantwoordelijkheden worden niet omgezet in eigenaarschap. Het bewustzijn voor externe bedreigingen groeit langzaam, maar door andere prioriteiten binnen organisaties en nalatigheden wordt er geen actie meer ondernomen.

Des te belangrijker is het volgens Emma Plak de cultuur van de organisatie beetje bij beetje te veranderen om een strakke verantwoordelijkheid voor OT-beveiliging te creëren.

5 Conclusie en aanbevelingen

Uit het onderzoek van Emma Plak blijkt dat het middenmanagement van productiebedrijven een sleutelrol speelt in het beveiligen van de OT, maar deze uitdaging niet alleen kan oplossen. Samenwerking binnen en buiten de organisatie is belangrijk.

5.1. Investeren in kennis en technologie

Door te investeren in bewustwording, trainingen, protocollen en afspraken kunnen organisaties hun medewerkers de stap laten maken van bewustwording naar gedragsverandering. Hierdoor wordt de blinde vlek met betrekking tot valse kennis en verantwoordelijkheid zichtbaar en kunnen medewerkers een concretere rol opnemen in de verantwoordelijkheden voor het beschermen van de kritieke infrastructuur. Dit is voor industriebedrijven cruciaal om een veilige en betrouwbare keten te borgen.

Trainingen voor management & technologie voor Cybersecurity:

sitrain-learning.siemens.com/NL/nl

5.2. Samenwerking met externen

Hierbij kunnen productiebedrijven mede een beroep doen op de kennis van OT-fabrikanten. Procesautomatisering heeft geleid tot nieuwe relaties tussen productiebedrijven en technologieleveranciers. Deze is gebaseerd op verschillende kennisniveaus, waardoor mensen soms langs elkaar heen praten en geen oplossingen vinden voor problemen. Het gevaar bestaat dat hierdoor de OT-beveiliging langer wordt verwaarloosd.

Siemens heeft een netwerk van partners om zich heen verzameld om bedrijven op alle vlakken te kunnen ondersteunen. Zowel qua business consultancy als technische realisatie. In overleg bekijken welke partner het beste aansluit bij de samenwerking.

siemens.com/global/en/company/partners/industry/solution-partners.html

xcelerator.siemens.com

5.3. Wederzijds vertrouwen

Een kans ligt volgens Emma Plak in het aanvullende karakter van de nieuw ontstane rollen in de relatie. Dit wil zeggen dat productiebedrijven en leveranciers wederzijds afhankelijk zijn van elkaar. Zo hebben fabrikanten specifieke bedrijfskennis van hun klanten nodig om automatiseringsoplossingen op maat te kunnen maken. Om het optimale uit deze samenwerking te kunnen halen is het belangrijk dat er wordt toegewerkt naar vertrouwen in elkaar.

Binnen zo'n 'trust relationship' borgt men samen een feilloze productie door regelmatig kennis en informatie te delen. Dit kan in de vorm van een end-to-end servicegericht partnerschap, een transparante en goed gefundeerde samenwerking, die wordt gekenmerkt door een hoge mate aan loyaliteit. Door OT-security op deze manier professioneel op te pakken, kan men het vlottrekken en financieel aantrekkelijk maken. Productiebedrijven die erin slagen hun klassieke organisatiestructuur te doorbreken, zullen hier op verschillende terreinen de vruchten van plukken: ze zijn in controle, effectief en hebben hoog gemotiveerde medewerkers.

charteroftrust.com
siemens.com/cybersecurity-industry

5.4. Wat zegt de overheid

Het Nationaal Cybersecurity Centrum (NCSC) publiceert de vijf basisprincipes van digitale weerbaarheid.

1. Brengt je risico's in kaart – dus ook je veiligheid en omgeving risico's rond je productie.
2. Bevorder veilig gedrag – dat begint met duidelijke rollen in de organisatie.
3. Bescherm systemen, applicaties & apparaten – dus ook in je productieomgeving.
4. Beheer toegang tot data en diensten – dus ook voor onderhoud aan je productiemiddelen.
5. Bereid je voor op incidenten – dus vooral een langdurige uitval van je gehele productieketen.

ncsc.nl/wat-kun-je-zelf-doen/basis-principes

Figuur 3: Charter of Trust

6 Verantwoording

Om recht te kunnen doen aan de complexiteit van het onderwerp en rekening te kunnen houden met context en nuances is gekozen voor kwalitatief onderzoek. Hierbij zijn drie verschillende onderzoeksmethoden toegepast:

Gestructureerde interviews: op basis van diepte-interviews met business unit managers is het verantwoordelijkheidsgevoel voor digitale veiligheid binnen de industrie in kaart gebracht. Er is bewust gekozen voor gesprekken met vertegenwoordigers van het middenmanagement, die als schakel tussen het hoger management en de uitvoerende teams een sleutelpositie hebben in het bereiken van de strategische doelstellingen van de organisatie. Dit brengt ook verantwoordelijkheid ten aanzien van digitale veiligheid met zich mee.

Niet-participerende observatie: hierbij is de interactie rond het thema 'digitale veiligheid' geobserveerd, zowel binnen de groep van geïnterviewden als in gesprekken tussen de geïnterviewden en een OT-leverancier.

Discoursanalyse: een analyse van de wijze waarop men op papier over de thematiek communiceert.

De combinatie van bovenstaande onderzoeksmethoden leidt tot een holistisch beeld van de verantwoordelijkheidsgevoelens rondom Cybersecurity en verhoogt de objectiviteit van het onderzoek.

Bronvermelding

The 10 Operational Technology Security Controls – Gartner: gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we

Contact

Neem voor meer informatie over onze activiteiten op het gebied van OT-security contact op met:

Ruud Welschen
Industrial cybersecurity consultant
ruud.welschen@siemens.com
siemens.com/cybersecurity-industry

Siemens Nederland N.V.

Prinses Beatrixlaan 800
2595 BN Den Haag

Postbus 16068
2500 BB Den Haag

Tel (0)70 333 3333

www.siemens.nl