SIEMENS

BELANG VAN EEN GOEDE DEFINITIE VAN

Operational Technology in cybersecurity wet- en regelgeving

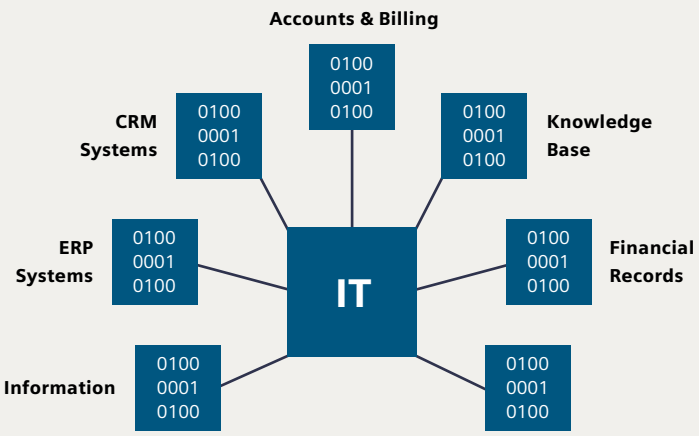
Gelijke spelregels voor een cybersecure industrie door middel van normen, toezicht, handhaving en samenwerking.

Operational Technology in cybersecurity wet- en regelgeving

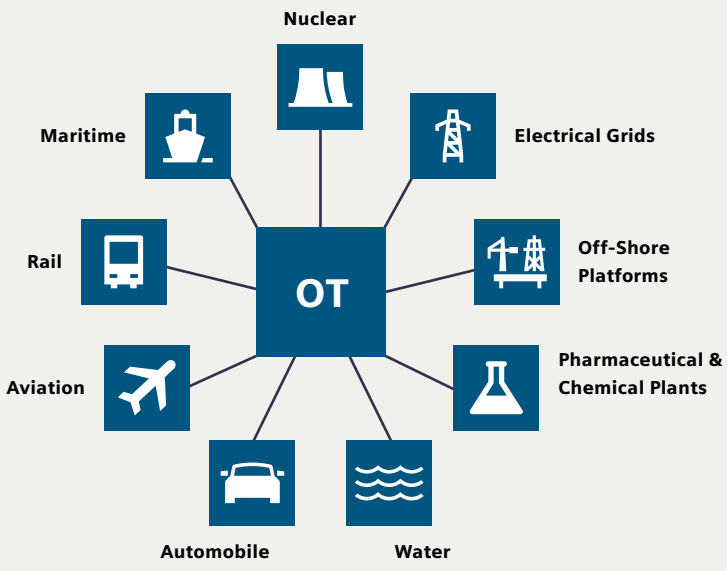
In deze mini-paper gaan wij in op het belang van OT-cybersecurity voor u als eigenaar van OT-systemen (naast uw IT-systemen) en/of als wet- en regelgevend instituut.

Onder Operational Technology wordt in deze paper verstaan: apparatuur en software voor de besturing binnen fabrieken, van bruggen, het spoorwegennet, onze drinkwatervoorziening, elektriciteit- en gasvoorzieningen enz.

IT - Information Technology



OT - Operational Technology



Charter of Trust

Digitalisering heeft vrijwel elk aspect van ons leven veranderd. Tegenwoordig zijn miljarden apparaten verbonden via het internet der dingen. Dit schept grote kansen, maar brengt ook grote risico's met zich mee. Om de digitale wereld veiliger te maken heeft Siemens de krachten gebundeld in het Charter of Trust. Deze unieke samenwerking tussen toonaangevende bedrijven heeft tot belangrijke verbeteringen geleid op het vlak van cybersecurity. De doelen voor de toekomst zijn ambitieus.

Het Charter of Trust (www.charteroftrust.com) focust op drie doelstellingen:

- De gegevens van personen en bedrijven beschermen
- Schade aan mensen, bedrijven en infrastructuren voorkomen
- Een betrouwbaar fundament creëren waarop het vertrouwen in een verbonden, digitale wereld wortel kan schieten en groeien

Versterken van de keten

De cyberrisico's in de toeleveringsketen nemen toe. Digitalisering van de industrie (versneld door de COVID-19-pandemie) leidt tot een grotere afhankelijkheid van een groeiend aantal externe partners, leveranciers, dienstverleners, aannemers enz. Een beveiligingsincident met één leverancier kan een volledig geïntegreerd supply chain-proces aanzienlijk verstoren.

We moeten dan ook kijken naar manieren om gemeenschappelijke kwetsbaarheden of afhankelijkheden beter te identificeren en hiaten in het beleid aan te pakken. Dit om de veiligheid en veerkracht van de toeleveringsketen te verbeteren. Deze aanpak kan een gemeenschappelijk certificeringsmechanisme op basis van internationale normen en certificeringsregelingen omvatten, evenals bredere holistische uitgangspunten voor cybersecurity, voortbouwend op door de industrie geleide aanbevelingen voor cybersecurity. Bijvoorbeeld de basisbeveiligingsvereisten van het Charter of Trust in de digitale toeleveringsketen.

NIS 2-richtlijn: kans op prominente plek voor OT

Per 9 november 2018 geldt de Wet beveiliging netwerk- en informatiesystemen (Wbni). De Wbni komt voort uit de NIS-richtlijn van de Europese Commissie. Het streven is de digitale weerbaarheid van Nederland, en in het bijzonder van vitale aanbieders, de rijksoverheid en digitale dienstverleners, te vergroten. De wet is erop gericht de gevolgen van cyberincidenten bij deze groepen te beperken en zo maatschappelijke ontwrichting te voorkomen. Ondanks deze wet- en regelgeving groeien de cyberrisico's.

Door de digitale transformatie van de maatschappij (versterkt door de COVID-19-crisis en nu ook de oorlog in Oekraïne) nemen de bedreigingen toe en ontstaan er nieuwe uitdagingen die aangepaste en innovatieve reacties vereisen. Om deze uitdagingen het hoofd te bieden en het achterblijven van de risicoperceptie van cybersecurity versus de werkelijke cyberdreiging op te lossen heeft de Europese Commissie een voorstel aangenomen voor een herziene richtlijn inzake de beveiliging van netwerk- en informatiesystemen (NIS 2-richtlijn).

Belang van prominente plek voor OT in wet- en regelgeving

Operational Technologie (OT) is tot nu toe in de cybersecurity wet- en regelgeving onderbelicht gebleven. De focus van cybersecurity regelgeving ligt van oudsher op het IT-landschap. Dit is een groeiend probleem aangezien we binnen (industrie)bedrijven steeds meer digitalisering met connected devices in de OT-omgeving zien. De cybersecurityrisico's aan de OT-zijde van bijvoorbeeld een Aanbieder van een Essentiële Dienst (AED) kunnen veel groter en ingrijpender zijn voor bedrijven en de maatschappij dan de cybersecurityrisico's aan de IT-zijde. De impact is enorm als onze elektriciteitsvoorziening voor meerdere dagen wordt platgelegd, ons drinkwater wordt vervuild of ons treinverkeer wordt stilgelegd.

Siemens roept de overheid op om naast IT- ook OT-cybersecurity een prominente plaats te geven en expliciet te benoemen in de Nederlandse implementatie van de NIS 2-richtlijn. Onderstaand een aantal redenen vanuit de praktijk bij onze klanten waarom dit van belang is.

Toegenomen cyberdreiging dwingt steeds meer bedrijven tot maatregelen

DI, 12/04/2022 - 07:57 • NIEUWS • SECURITY • *Door: Redactie WINMAG Pro*

45 procent onderzochte bedrijven heeft in 2022 al te maken gehad met cybercriminaliteit

Sterke stijging bedrijven (+55 procent) dat in 2022 doelwit was ten opzichte van vorig jaar

Het aantal Nederlandse bedrijven dat te maken heeft gehad met een cyberaanval is in de afgelopen maanden met ruim de helft toegenomen tot 45 procent. Terwijl in april 2021 bijna drie op de tien bedrijven zijn geconfronteerd met cybercriminaliteit, geldt dit nu al voor bijna de helft van de bedrijven. Dat blijkt uit onderzoek dat ABN AMRO heeft laten verrichten onder 233 zakelijke klanten die eind- of medeverantwoordelijk zijn voor de cyberveiligheid van hun bedrijf. Als gevolg van de verregaande digitalisering, die door corona in een stroomversnelling is gekomen, neemt het aantal potentiële toegangspunten voor cybercriminelen snel toe. Daarnaast worden zij steeds professioneler. Hoewel de gemeten toename in

Bron: https://www.winmagpro.nl/toegenomen-cyberdreiging-dwingt-steeds-meer-bedrijven-tot-maatregelen

Verwevenheid van IT en OT

Om beter inzicht te hebben, koppelen bedrijven steeds meer IT- en OT-systemen aan elkaar. Dit is niet alleen handig voor organisaties, maar óók voor hackers. Het is makkelijker om via de ene omgeving over te springen naar de andere omgeving en andersom.

Gebruik van verouderde en kwetsbare software

De karakteristieken van OT zijn anders dan die van IT (zie onderstaande figuur). OT-investeringen zijn vaak grote investeringen voor de lange termijn waarvan de beschikbaarheid over het algemeen erg hoog moet zijn. Dit betekent dat veel (productie)bedrijven werken met (ver)ouder(d)e OT die dringend een update nodig hebben. De productie stilleggen om updates uit te voeren is kostbaar. Hierdoor zitten er meer kwetsbaarheden in de software en is er sprake van een verhoogd cybersecurityrisico.

IT - Information Technology

Characterics	
Life time	3-5 Years
Availability req.	Medium, Delays accepted
Real time req.	Delays accepted
Physical Security	High (for critical IT)
Application of patches	Regular/scheduled
Anti-virus	Common/widely used
Security testing/audits	Scheduled and mandated

OT - Operational Technology

Characterics	
Life time	Up to 20 Years
Availability req.	Very High
Real time req.	Critical
Physical Security	Very much varying
Application of patches	Slow/none
Anti-virus	Uncommon
Security testing/audits	Occasional

Risicoperceptie blijft achter bij feitelijke dreiging

Hoewel de cyberdreiging is toegenomen, blijft de risicoperceptie van bedrijven hierbij achter, blijkt uit het onderzoek. "Terwijl in 2021 drie op de tien bedrijven aangaven cybercriminaliteit als groot risico te beschouwen, is dat dit jaar niet significant toegenomen. Dit betekent óók dat de digitale weerbaarheid van bedrijven slechts beperkt is toegenomen. De mate waarin bedrijven maatregelen treffen tegen cyberaanvallen hangt namelijk sterk samen met hun risicoperceptie. We zien dat

Bron: https://www.winmagpro.nl/toegenomen-cyberdreiging-dwingt-steeds-meer-bedrijven-tot-maatregelen

Weinig security-eisen voor hard- en software
Bij het aanschaffen van nieuwe (plug-and-play) OT letten bedrijven te weinig op cyberveiligheid. Vaak laat de security te wensen over. Een meer solide aanpak zou zijn om bepaalde cybersecuritystandaarden op te stellen waaraan alle nieuwe OT moet voldoen.

Onvoldoende monitoring
In de OT-omgeving monitoren bedrijven vaak nauwelijks op ongewoon gedrag van medewerkers of hardware waardoor hackers zich vrij kunnen bewegen tussen de OT-omgeving en de IT-omgeving of zelfs alle systemen kunnen gijzelen.

Ambitie EU: leider in cybersecurity
De EU heeft de ambitie om leider te worden op het gebied van cyberbeveiliging. Dit betekent dat cybersecurity 'default' moet worden voor producten en leveranciers van IT- en OT/IoT-producten maar ook voor het bedrijfsleven dat deze producten gebruikt. Dit gaat verder dan het kiezen van de juiste technologie. Het gaat ook om het inrichten van processen en het gedrag van medewerkers. Op dit moment is er ruimte om keuzes te maken over de benodigde mate van cybersecurity, ook bij de AED's. Cybersecurity kan binnen het bedrijfsleven en zeker bij de AED's geen optie meer zijn en omwille van de prijs worden uitgesloten of onderbelicht.

Digitale weerbaarheid NL bedrijven 'ondermaats' terwijl cyberdreiging toeneemt

13 april 2022 om 11:13 uur

Het Nederlandse bedrijfsleven moet een inhaalslag maken op het gebied van cybersecurity. De meeste organisaties hebben nog geen strategie voor digitale weerbaarheid en de securitybudgetten zijn vaak niet toereikend. Ook heeft Nederland een achterstand als het gaat om security-awarenesstrainingen. Dat blijkt uit een internationaal onderzoek van cyberbeveiliger Mimecast.

Bron: https://www.engineersonline.nl/nieuws/id35423-digitale-weerbaarheid-nl-bedrijven-ondermaats-terwijl-cyberdreiging-toeneemt.html

Het is belangrijk dat de overheid zorg draagt voor een gelijk speelveld als het gaat om cybersecurity. Belanghebbenden moeten gelijke markttoegang en concurrentievoorwaarden krijgen. Gelijke spelregels voor een cybersecure industrie door middel van normen, toezicht en handhaving. Op dit moment ontbreekt het aan eenduidige normen en richtlijnen en is het toezicht nog in ontwikkeling.

Om vertrouwen op te bouwen is een op consensus gebaseerde internationale aanpak het meest geschikt, waarbij alle betrokken partijen bij het standaardisatieproces worden betrokken en bij voorkeur marktpartijen een leidend positie geven in dit proces. Om de samenwerking op het gebied van internationale normen efficiënt te maken, biedt de ontwikkeling van normen onder de paraplu van bijvoorbeeld ISO en IEC een goede kans. Vervolgens moet de overheid bedrijven in alle sectoren actief stimuleren om hun bedrijfsprocessen te certificeren op basis van internationale normen zoals ISO 27001 en IEC 62443 en ervoor zorgen dat hun regelgeving verwijst naar diezelfde reeks gecoördineerde internationale normen.

Tot slot: Als de ambitie is om leider te worden op het vlak van cybersecurity dan is het noodzakelijk om cybersecurity op te nemen in nationale onderwijscurricula en permanente professionele ontwikkeling. Werknemers van elk niveau in de industrie en publieke sector moeten cyberbewust zijn in hun werk en in hun dagelijks leven. Siemens roept het bedrijfsleven en de overheid dan ook op om via sector-overschrijdende samenwerking een cyberveilige cultuur in elke organisatie te verankeren. De aanbevelingen vanuit de Charter of Trust kunnen hierbij ondersteunen.

War for talent serieus probleem

Een ander groot probleem dat de onderzoekers constateren, is het probleem van de ‘war for talent’. Volgens de meeste onderzochte bedrijven is het extreem moeilijk voldoende gekwalificeerd securitytalent te vinden. Meer dan de helft van de bedrijven geeft aan dat projecten zijn mislukt, omdat niet voldoende geschikt personeel voor handen was.

Daarnaast hebben bedrijven ook grote moeite securitypersoneel te behouden. Veel securityspecialisten staan onder grote druk en nemen vaak verantwoordelijkheden op zich waarvoor ze niet klaar zijn. Hierdoor staan zij onder extreme druk, wat vaak een reden is een andere baan te zoeken of overwegen.

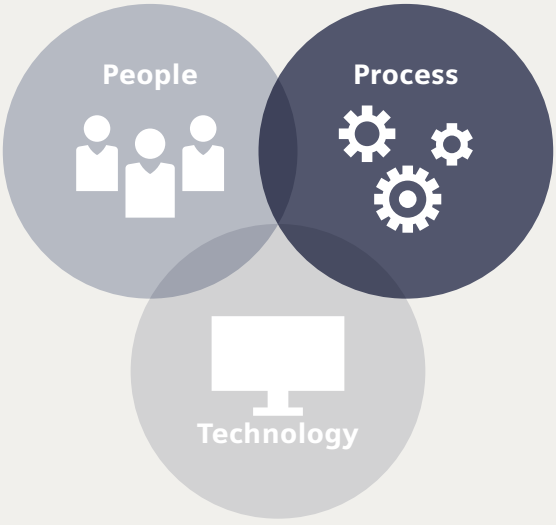
Bron: https://www.techzine.nl/nieuws/security/484805/cyberaanvallen-nemen-toe-en-securitytalent-wordt-schaarser/

Cybersecurity by design

Om het cybersecurityniveau te verhogen, moet beveiliging vanaf het begin worden ‘ingebouwd’ en overwogen in het product. Al in de ontwerpfase moet rekening worden gehouden met cybersecurity met als doel het toepassen van het hoogste passende niveau van beveiliging en gegevensbescherming. Dit om ervoor te zorgen dat het vooraf is geconfigureerd in het ontwerp van producten, functionaliteiten, processen, technologieën, operaties, architecturen en bedrijfsmodellen. Het principe moet meer omvatten dan alleen een product of technologie. Het is noodzakelijk om ook de dimensies ‘people’ en ‘process’ te integreren. Dit kan variëren van het aanbieden van basisbeveiligingstrainingen voor werknemers van een organisatie tot het volgen van veilige ontwikkelingsprincipes en het hebben van een goed cyberrisicobeheer. Dit helpt potentiële kwetsbaarheden, cyberrisico's en de daaraan verbonden kosten te voorkomen.

The operation model for cybersecurity:
Risk mitigation across these three dimensions

- → Awareness
- → Skills & Qualification
- → Competent resources
- → Follow the procedures



- → Governance
- → Security framework and policies
- → Operational processes
- → Compliance to standards
- → Audits

In dit kader is de Cyber Resilience Act relevant. Deze wordt verwacht in het derde kwartaal van 2022. Het doel van deze wet is om de consument en bedrijven te beschermen tegen onveilige producten. Dit moet gerealiseerd worden door het invoeren van cyberveiligheid-regels voor producenten en handelaars van materiële en immateriële digitale producten en bijbehorende diensten. Ook hier moeten OT- en I(o)T-producten en bijbehorende diensten gedefinieerd worden en binnen de scope van de wet vallen. Alleen dan wordt voorkomen dat niet alleen onveilige IT-producten maar ook OT-producten van de EU-markt worden geweerd en er gestandaardiseerde normen komen waaraan dergelijke producten moeten voldoen. Dit zal leiden tot een gelijker speelveld en bovenal een cyberveilige omgeving.

Meer informatie

Wilt u meer informatie over cybersecurity in relatie tot Operational Technology of heeft u vragen over cybersecurity in relatie tot Operational Technology, neem dan vrijblijvend contact op met uw contactpersoon binnen Siemens of:

→ Ivo van Nimwegen, Cybersecurity Manager
ivo.van.nimwegen@siemens.com
06 - 22 30 61 62

→ Ton Mes, Information Security Professional
ton.mes@siemens.com
06 - 22 25 04 78

→ Angelique Kuut, Government Affairs
angelique.kuut@siemens.com
06 - 31 64 13 60

→ Ruud Welschen, OT security services professional
ruud.welschen@siemens.com
06 - 55 84 49 11

Bijlage:

Wereldwijd

Wereldwijd onderzoek onder > 1.200 cybersecurityleiders toont een toename van gedetecteerde aanvallen en een toename van inbreuken. Vijfenzestig procent van de organisaties meldt dat ze te maken hebben met meer aanvallen en 49% zegt dat ze de afgelopen twee jaar te maken hebben gehad met een datalek (tegen 39% een jaar geleden).

Ransomware-aanvallen nemen toe en meer organisaties worden gedwongen te betalen. Van de respondenten die het slachtoffer werden van een succesvolle ransomware-aanval, betaalde 66% het losgeld en slechts 33% herstelde in plaats daarvan vanaf een back-up. Met name van degenen die nog niet het slachtoffer zijn geworden, denkt slechts 42% dat hun organisatie de aanvallers zal betalen, wat suggereert dat een aanzienlijk percentage overmoedig is.

$ 33,6 miljoen zijn de gemiddelde jaarlijkse kosten van door cybercriminaliteit veroorzaakte uitvaltijden in de onderzoeksgroep.

59% van de cybersecurityteams zegt dat ze veel tijd en middelen moeten besteden aan herstel. Bijna een derde van hun tijd wordt besteed aan het reageren op crises in plaats van zich voor te bereiden op aanvallen in de toeleveringsketen, ransomware en andere geavanceerde aanvallen.

Bron: https://www.splunk.com/en_us/blog/security/state-of-security-research-details-essential-strategies-for-the-year-ahead.html

---

In Nederland minder aandacht voor cybersecurity

Nederland scoort op veel vlakken minder goed dan de rest van de wereld. Bij maar dertig procent van de Nederlandse organisaties is vooruitgang geboekt in het afstemmen van de cyberstrategie op de bedrijfsstrategie in vergelijking tot vorig jaar. Bovendien is in Nederland minder vooruitgang gemaakt in het betrekken van de CEO bij cybersecurity (68% tegen 79% wereldwijd). Verder is de tijd die tijdens bestuursvergaderingen aan cybersecurity wordt besteed, wereldwijd meer toegenomen: 39% tegen 30% in Nederland.

Bedrijven hebben beperkt inzicht in de maatregelen die partijen waarmee ze samenwerken, nemen op het gebied van cybersecurity. Wereldwijd gaf minder dan de helft van de respondenten (40%) aan dat ze door formele reviews zicht hebben op mogelijke datalekken bij derde partijen. In Nederland ligt dit percentage op slechts 35.

Het managen van het risico rondom de software-supplychain (het leveren van software) scoort zelfs lager. Wereldwijd heeft 34% van de deelnemende organisaties hierop zicht door formele reviews. In Nederland is dat percentage twintig.

Bron: PWC, Cyber Digital Trust Insights NL 2022: https://www.pwc.nl/nl/actueel-en-publicaties/diensten-en-sectoren/technologie/bestuurders-niet-betrokken-cybersecurity.html