SIEMENS

AANDACHTSPUNTEN VANUIT OT-SECURITY

Van NIS2 naar Wbni

Hoofdpunten

- De mondiaal groeiende cyberdreiging raakt niet alleen informatietechnologie (IT), maar ook operationele technologie (OT), zoals apparatuur en software voor het aansturen van slimme fabrieken, *smart buildings* en cruciale infrastructuur (waaronder bruggen, het spoor en sluizen). Ook dit soort objecten wordt steeds meer verbonden met het internet.
- Het duurt gemiddeld 200 dagen voordat getroffen partijen doorhebben dat er hackers in hun interne OT-omgeving zitten. De (privacy)schade is dan vaak al niet meer te overzien.
- Om deze groeiende risico's te kunnen mitigeren, moeten in de nationale implementatie van de NIS2-richtlijn vanuit OT-veiligheid enkele cruciale punten worden meegenomen:
    1. Het opnemen van een specifieke definitie van OT in de Wbni, inclusief een heldere differentiatie tussen technische, organisatorische en operationele maatregelen.
    2. Een verwijzing naar IEC62443 (of een andere vergelijkbare norm).
    3. Een prominente plek voor OT in risicoanalyses (in de eigen organisatie en supply chain).

Elke elf seconden

Digitalisering is niet meer weg te denken uit ons dagelijkse leven. Over de hele wereld zijn miljarden apparaten, gebouwen, machines en voorzieningen verbonden met het internet. Dit heeft een enorme impact op onder andere de maakindustrie, het transport, slimme steden, de publieke infrastructuur en de voedselproductie.

Digitalisering genereert zowel kansen als bedreigingen. Nieuwe kansen zitten in gebruikersgemak, betere toegang, meer kennis en efficiëntie, en hogere productiviteit. In de industrie is dit bijvoorbeeld zichtbaar in het tempo van automatisering, het stroomlijnen van maakprocessen met geavanceerde sensoren, real-time informatie, de optimalisatie van aanvoer- en leveringsketens, minder menselijke fouten en beter voorraadmanagement. En gebouwen worden 'slimmer' door de inpassing van allerlei sensoren en regelsystemen, waaronder klimaatregelaars en sensoren met een ethernet-aansluiting.

Maar naast deze nieuwe kansen is er ook een toenemende bedreiging voor de continuïteit van bedrijven en is de cybersecurity onvoldoende. Ondanks publiek-private inspanningen groeit de kloof tussen cyberdreigingen en digitale weerbaarheid. Ten opzichte van 2021 is het aantal cyberaanvallen in Nederland met **55% toegenomen**, en heeft bijna de helft van alle Nederlandse bedrijven te maken gehad met cyberdreiging. Op mondiaal niveau wordt **elke elf seconden** een bedrijf slachtoffer van ransomware. De jaarlijkse **schade** van cybercriminaliteit bedraagt inmiddels **5,5 biljoen euro**.

Belang OT neemt snel toe

Deze groeiende cyberdreiging raakt niet alleen informatietechnologie (IT), maar ook **operationele technologie (OT)**, waaronder apparatuur en software voor het aansturen van fabrieken, gebouwen, allerlei vitale sectoren (drinkwater, gas, elektriciteit) en cruciale infrastructuur. Hoewel OT en IT zich van origine op andere domeinen richten - bij OT ligt de nadruk meer op het waarborgen van de veiligheid en functionaliteit van fysieke machines en taken - zijn beide netwerktypen steeds sneller en verder geïntegreerd. Maar daarmee openen ze ook een veel breder scala aan cyberdreigingen.

Bovendien leidt de groei van het aantal slimme en verbonden producten ertoe dat een simpel cyber-beveiligingsprobleem bij een enkel product gevolgen kan hebben voor de gehele toeleveringsketen. Dit komt mede omdat het onderhoud van OT-systemen minder regulier is, omdat bij oefeningen en/of werkzaamheden direct een hele keten moet worden stilgelegd. Dit maakt OT een gewild doelwit van hackers.

Uit het onderzoek *The State of Industrial Cybersecurity* blijkt dat **89%** van de elektriciteits-, olie-, gas- en productiebedrijven in 2021 te maken heeft gehad met cyberaanvallen die van invloed waren op de productie en **energievoorziening**. Een aanvullende conclusie is dat de OT-beveiligingsfunctie gemiddeld gezien

minder volwassen leek dan de IT-beveiligingsfunctie. Een gemiddelde OT-aanval leverde **2,8 miljoen euro** schade op. Een groot risico voor wie bedenkt dat het gemiddeld **200 (!) dagen** duurt voordat bedrijven/instellingen door hebben dat er is ingebroken in hun OT-omgeving, met alle gevolgen van dien.

NIS2 richtlijn: OT komt te weinig aan bod

Dit groeiende dreigingsbeeld heeft de Europese Commissie gestimuleerd tot het aannemen van een herziene richtlijn inzake de beveiliging van netwerk- en informatiesystemen (NIS2). NIS2 verhoogt cybersecurityeisen, verbreedt de scope van vitale sectoren en streeft naar meer harmonisatie tussen de 27 EU-lidstaten. Siemens steunt de ontwikkeling van de NIS2-richtlijn, alsmede de implementatie ervan op nationaal niveau. Tegelijkertijd signaleert Siemens ook dat de richtlijn sterk is gericht op IT en veel minder op OT, en dat deze onduidelijkheid voor grote risico's en het niet meenemen van talrijke kwetsbaarheden zorgt. Door het niet expliciet benoemen van OT in de reikwijdte van de Wbni voorziet Siemens dat noodzakelijke cybersecuritymaatregelen voor OT-omgevingen door bedrijven worden uitgesloten of als minder belangrijk beschouwd. Dit komt vooral doordat de verantwoordelijkheid van IT en OT bij (industriële) bedrijven in de regel strikt gescheiden is. Implementatie van de Wbni zal in de regel daarom toegewezen worden aan het IT domein. Ook is de ervaring van Siemens dat cyberrisico’s binnen de OT nog niet structureel worden meegenomen in het risicomanagementraamwerk van bedrijven.

Siemens deelt daarom graag een aantal aanbevelingen rond het OT-domein waarvan het hoopt dat deze bij de nationale implementatie van de NIS2-richtlijn (vermoedelijk in de Wbni) worden meegenomen. Op dit moment staat in de Wbni geen enkele definitie of verwijzing naar OT. Het is cruciaal om dit te repareren als de NIS2-richtlijn (met een bredere scope qua vitale sectoren, verscherpte beveiligingseisen voor bedrijven en een zorgplicht) in nationale wetgeving wordt omgezet. Ook omdat 60% van alle bedrijven volgens Gartner en Agentschap Telecom nog in de awareness fase zit op het gebied van OT-security.

Siemens steunt de ontwikkeling van de NIS2-richtlijn, alsmede de implementatie ervan op nationaal niveau.

Aanbevelingen voor de **nationale implementatie van NIS2**

1A NIS2 is een open richtlijn die erg op IT-security is gericht. De term Operational Technology (OT) wordt niet concreet benoemd, wat ook geldt voor de specifieke aandachtspunten die bij OT-security horen. Ook in de huidige (nog aan te passen) Wbni staat nergens een definitie van of een verwijzing naar OT. Siemens bepleit om de nationale implementatie van de NIS2 richtlijn te gebruiken om OT specifiek te benoemen in de Wbni (in Artikel 4) door de tekst in lid 1C (definitie van network and information systems) uit te breiden met OT. Voorgestelde definitie:

"alle hardware-, software- en firmwarecomponenten van een systeem, die worden gebruikt om fysieke operationele processen real-time te benaderen, te detecteren, te monitoren of te wijzigen door directe controle en bewaking van fysieke apparaten, oftewel operationele technologie".

1B In de NIS2-richtlijn is in Artikel 18, lid 1 aan 'technische en organisatorische maatregelen' ook 'operationele maatregelen' toegevoegd. Dat is positief, maar iets verderop gaat de richtlijn niet ver genoeg: '...to manage the risks posed to the security of network and information systems which those entities use for their operations...'. Deze formulering is nog te algemeen om genoeg aandacht voor OT-security zeker te stellen. 'Operations' kan immers ook als operations voor het IT-domein gelezen worden. OT moet ook hier specifiek worden benoemd. De oplossing hiervoor ligt in het aan-passen van Artikel 7, lid 1:

***Essentiele en belangrijke aanbieders** nemen passende en evenredige technische, relevante, **operationele** en organisatorische maatregelen om de risico's voor de beveiliging van hun netwerk- en informatiesystemen te beheersen. De maatregelen in **zowel het IT- als OT-domein** zorgen, gezien de stand van de techniek, voor een niveau van beveiliging dat is afgestemd op de risico's die zich voordoen.*

2 Positief is wel dat in de NIS2-richtlijn, artikel 18, lid 2 de minimale basismaatregelen uiteen worden gezet waaraan bedrijven moeten voldoen die onder de NIS2-richtlijn vallen. Siemens bepleit om in de nieuwe Wbni naar dit artikel te verwijzen, daarbij wel rekening houdend met de nuanceverschillen tussen IT en OT, waarvoor speciale kennis vanuit het OT-domein in acht moet worden genomen:

- Scan tools voor IT-omgevingen zijn niet voldoende voor OT-omgevingen. Hiertussen moet worden gedifferentieerd.
- Beter aangeven hoe bedrijven kunnen aantonen dat ze cybersecuritymaatregelen hebben genomen op het vlak van OT. In de basis zijn de maatregelen hetzelfde als bij IT, maar er zit wel verschil in de scope. Bevat het Information Security beleid van een bedrijf naast IT bijvoorbeeld ook OT en zijn de techneuten getraind etc.?

- Vulnerability handling vraagt om extra garanties van OT-leveranciers. Hoe weet een afnemer bijvoorbeeld dat patches worden geïnstalleerd of kwetsbaarheden afdoende gerapporteerd? En hoe beoordeel je of er voldoende interne expertise aanwezig is of dat security by design wordt toegepast? Meer duidelijkheid is hier nodig.
- Beter aangeven hoe de doeltreffendheid van beleidslijnen en procedures (testen en audits) beoordeeld kan worden voor de OT-omgeving. Een auditor zou naar bewijs kunnen vragen: dat het ISMS ook OT in de scope heeft benoemd, dat de servicecontracten met de OT-leveranciers ook cybersecurity afspraken bevatten, dat de inkoopafdeling cybersecuritycontractvoorwaarden hanteert etc.
- Binnen IT en OT worden in principe dezelfde encryptietechnieken en principes toegepast, maar veel al bestaande OT-omgevingen staan dat niet toe. Bovendien verschilt de levensduur van een OT-systeem sterk van een IT-systeem -> 3/5 om 20 jaar). Met deze omstandigheid moet rekening worden gehouden.
- Qua bescherming ligt bij IT de nadruk op het beschermen van data, maar dat is bij OT geen noodzaak. Bij OT moet juist worden voorkomen dat systeemgedrag wordt ondermijnd dan wel gemanipuleerd. In de juridische uitwerking moet hiermee rekening worden gehouden.

3 Er zijn belangrijke nuanceverschillen tussen IT en OT waarvoor speciale kennis en aandacht vanuit het OT-domein in acht genomen moet worden in de toepassing van genoemde maatregelen. Om dit in de Wbni verder te verduidelijken en meer richting te geven aan betrokken organisaties, beveelt Siemens aan om in Artikel 7, lid 2 een verwijzing naar de IEC62443 norm (of een vergelijkbare norm) te maken.

IEC62443 is een internationale reeks normen gericht op cybersecurity voor operationele technologie in automatiserings- en controlesystemen. Het wordt mondiaal geaccepteerd door toezichthouders en auditors.

Grote OT-hacks in de laatste periode: **maatschappelijke schade neemt toe**.

2021 | Colonial Pipeline

Colonial Pipeline (het grootste oliepijpleidingsbedrijf in de VS) legt alle pijpleidingen stil na een cyberaanval. Dit leidt tot grote brandstoftekorten aan de Oostkust.

2021 | De Mandemakers Groepv

Ransomewareaanval op De Mandemakers Groep. Alle aangesloten bedrijven kunnen dagenlang geen meubels leveren. Keukens moeten met potlood worden getekend.

2021 | LOG4J

Ernstige kwetsbaarheid (met catastrofale potentie) geconstateerd in Java. Wereldwijd verwerkt in talrijke producten en toepassingen.

2021 | Waterzuiveringsinstallatie

Aanval via Teamviewer op waterzuiverings-installatie in Florida. Zeer vroege detectie voorkomt dodelijke slachtoffers.

2021 | Solarwinds

Verwoestende aanval op Solarwinds. Onder de slachtoffers zitten grote vissen zoals CISCO, Microsoft, Intel, het Pentagon, de Amerikaanse ministeries van Financiën en Justitie.

2022 | Olieterminals

Meerdere olieterminals in Europa getroffen door cyberaanval.

Over Siemens

Siemens is een technologie en softwarebedrijf dat zich richt op industrie, infrastructuur, transport en gezondheidszorg. Wij ontwikkelen technologie die waarde toevoegt. Denk aan efficiëntere fabrieken, veerkrachtige toeleveringsketens, slimmere gebouwen, schoner vervoer en geavanceerde gezondheidszorg. Door de echte wereld en de digitale wereld te verbinden, stellen wij onze klanten in staat hun industrieën en markten te transformeren en helpen wij hen het leven van alledag voor miljarden mensen te veranderen.

Siemens wordt beschouwd als een van de meest prominente cyberaanvalsdoelen in de industrie, met name door de wereldwijde bekendheid en het brede productportfolio. Siemens hoort mondiaal gezien bij de bedrijven die de meeste zeer gevoelige infrastructuur hebben ontwikkeld.

Voor meer informatie, neem contact op met Angelique Kuut, Government Affairs bij Siemens en te bereiken via 06 31 64 13 60 of angelique.kuut@siemens.com

Siemens Nederland N.V.
Prinses Beatrixlaan 800
2595 BN Den Haag
Postbus 16068
2500 BB Den Haag
Tel (0)70 333 3333
Fax (0)70 333 2917

www.siemens.nl