

Mastering IT Complexity

# OT en de Cyberbeveiligingswet

van inzicht naar aantoonbare  
cyberweerbaarheid

Jasper Rappard & Jeroen van Es



# Sprekers

## Voorstellen



**Jasper Rappard**  
Cybersecurity Consultant  
Legian



**Jeroen van Es**  
CCO  
Nautilus OT

# Legian: kennispartner

Grip op IT- en OT-complexiteit

**30+** jaar ervaring

**400+** klanten en projecten

**150+** specialisten en generalisten

**5mil+** detacheringsuren

Flexibele expertise voor veilige, wendbare en efficiënte IT- en OT-omgevingen..

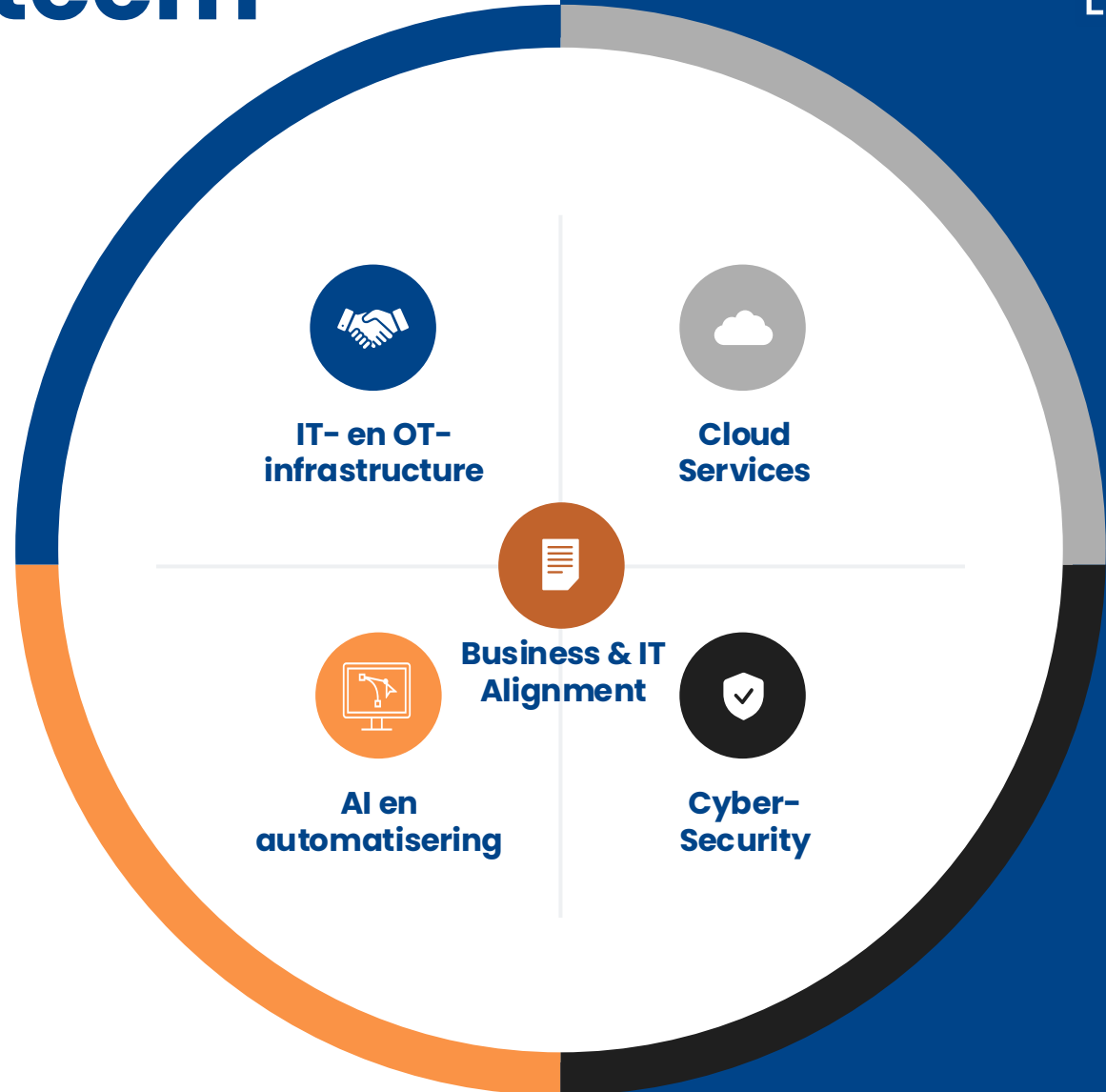
.. van tijdelijke versterking tot advies en implementatie.

LEGIAN

# Eén IT/OT-ecosysteem

## Vijf verbonden kennisdomeinen

Een integrale benadering voor veilige, efficiënte en wendbare bedrijfsvoering.



## Passief monitoringsplatform voor OT- en IoT-omgevingen

### Mid-market en mkb+

Cyberweerbaar zonder groot budget of team.

### 100% passief

Geen pakketinjectie, geen productieverstoring.

### Onafhankelijk

100% NL en EU gehost, geen Amerikaanse hyperscalers.

### Evidence, geen scores

Reproduceerbaar bewijs, beoordeling bij de consultant.

### Integraties

CMDB en SIEM platforms.

### Eén monitoringplatform

Zichtbaarheid, kwetsbaarheden en alerting.

# Van blinde vlek naar grip op OT

1. Helmpje op, helmpje af
2. IT in orde, OT buiten beeld
3. Cyberbeveiligingswet en OT
4. Van inzicht naar aantoonbare cyberweerbaarheid
5. Vragen

# Helmpje op, helmpje af..

Is jouw organisatie Cbw-plichtig?

JA



NEE



# Helpje op, helpje af..

Staat jouw organisatie al geregistreerd bij het NCSC?

JA



NEE



# Helpje op, helpje af..

Heb je OT in je organisatie?

JA



NEE



# Helmpje op, helmpje af..

Weet je welke OT-assets met je netwerk verbonden zijn?

JA



NEE



# Helmpje op, helmpje af..

LEGIAN

Ben jij verantwoordelijk voor security?

JA



NEE



”

**IT in orde. OT buiten beeld.**

# Maar wat verstaan we onder OT?

Operationele technologie is een ruim begrip. Het is breder dan de (maak)industrie.

- Energie
- Olie & gas
- Zorg
- Transport & logistiek
- Voedsel
- Gebouwbeheer
- Smart city
- Etc.



# Vóór de Cbw lag de focus op IT

Wat deden we onder andere al?

- Assets registreren
- Patches installeren
- Kwetsbaarheden scannen
- Netwerken segmenteren
- Monitoring inrichten



# OT: waar security nog blinde vlekken kent

Wat in IT vanzelfsprekend is, laten we in OT vaak liggen.

| IT                             | OT                                                                               |
|--------------------------------|----------------------------------------------------------------------------------|
| Patchmanagement                | “Die PLC draait al 12 jaar probleemlos. Daar blijven we af.”                     |
| Kwetsbaarheidsscans            | “Wat als die scan het productieproces verstoort?”                                |
| Assetmanagement                | “We weten niet welke PLC’s, HMI’s en sensoren actief zijn.”                      |
| Netwerksegmentatie             | “Het OT-netwerk is organisch gegroeid en voelt vertrouwd.”                       |
| Multi-Factor Authentication    | “Niet iedere OT-oplossing ondersteunt MFA.”                                      |
| Lifecycle management           | “Veel OT-apparatuur draait ver voorbij de reguliere lifecycle.”                  |
| Centrale logging en monitoring | “Niet alle OT-systemen genereren logs of leveren die centraal aan.”              |
| Configuratiebeheer             | “Configuraties staan verspreid bij leveranciers, engineers of lokale bestanden.” |



**IT en OT raken steeds meer verbonden.  
OT buiten beschouwing laten is geen  
houdbare keuze.**

# OT bleef draaien. Het risico groeide mee.

IT ondersteunt. OT maakt het mogelijk.

## Continuïteit

OT omvat machines, processen en dienstverlening. Een verstoring raakt direct de bedrijfscontinuïteit.

## Risico

Onbekende assets en afhankelijkheden bemoeilijken risico-inschatting en incidentrespons.

## Bestuurbaarheid

Management heeft begrijpelijke en toepasbare inzichten nodig om prioriteiten te bepalen.



**15 augustus 2026: De Cyberbeveiligingswet  
is van kracht.**

# Cyberbeveiligingswet

## In het kort

- **NIS2 – Europese richtlijn**

Verplicht lidstaten om essentiële en belangrijke entiteiten passende cybersecuritymaatregelen te laten nemen voor risicobeheersing en incidentpreventie.

- **Cyberbeveiligingswet – Nederlandse implementatie**

Vertaalt NIS2 naar Nederlandse verplichtingen, met als doel aan te sluiten bij de Europese eisen en de digitale weerbaarheid van Nederland te versterken.

# Cyberbeveiligingswet

## Vier pijlers

### Registratieplicht



**Registreren als  
NIS2-entiteit**

### Zorgplicht



**Aantoonbaar in  
control**

### Meldplicht



**Melden van  
incidenten**

### Toezicht



**Verantwoording  
op orde**

# 10 zorgplichtmaatregelen

Die dus ook voor OT gelden

1. Maak een risicoanalyse
2. Richt incidentrespons in
3. Bereid je voor op uitval
4. Beveilig je toeleveringsketen
5. Zorg voor goede cyberhygiëne
6. Beveilig netwerk- en informatiesystemen
7. Versterk personeel, toegang en assetbeheer
8. Gebruik sterke authenticatie, zoals passkeys
9. Stel een cryptografiebeleid op
10. Beoordeel de effectiviteit van je maatregelen

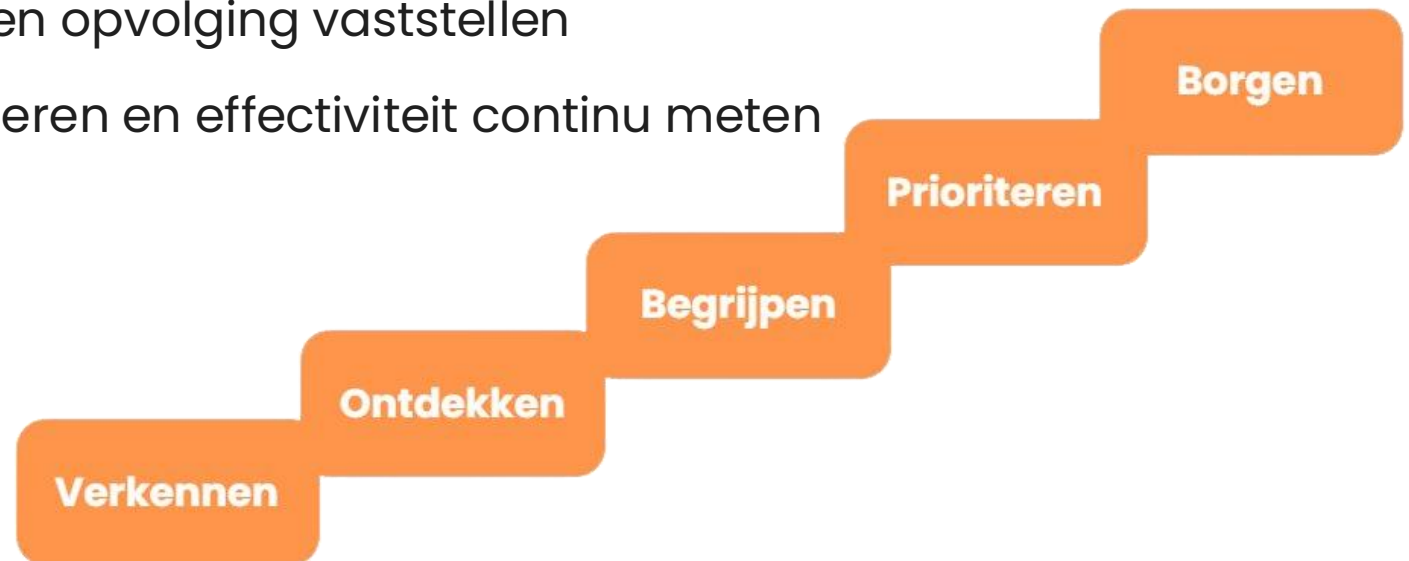


**Maar hoe kun je voldoen aan de eisen als je niet weet wat er in je OT-landschap aanwezig is?**

# Van inzicht naar grip op risico

Je kunt niet beschermen waar je geen inzicht in hebt

- Verkennen – Bestaande documenten en interviews
- Ontdekken – Technische netwerk assessment
- Begrijpen – Bevindingen in context plaatsen
- Prioriteren – Risico's identificeren en opvolging vaststellen
- Borgen – Maatregelen implementeren en effectiviteit continu meten



# Van inzicht naar bestuurbare opvolging

Een frisse blik maakt blinde vlekken zichtbaar

## Legian

- Duidt risico's, helpt prioriteren en vertaalt uitkomsten naar concrete maatregelen.
- Ondersteunt bij het opzetten van governance en borging binnen de organisatie.



## Nautilus OT

- Brengt OT- en IoT-assets continu in kaart, volledig passief en zonder verstoring.
- Signaleert risico's in het netwerkverkeer en levert bewijs richting de Cbw.



**Mét inzicht naar aantoonbare  
cyberweerbaarheid.**

# Vragen?

**Stel ze gerust of loop even langs stand 11.D060**