ICT GROUP
ICT Netherlands
Smarter Solutions

OT is stuk –
repareer alleen wat nodig is

Hoe de CSIR OT weer toekomst geeft

7-10-2025 | PvIB | Marco Rijkschroeff

Even voorstellen

Ir Marco Rijkschroeff CISSP
Business Consultant
OT Cybersecurity
ICT Nederland / ICT Group

- 20+ jaar ervaring security IT en OT
  - Waterschappen
  - Rijkswaterstaat
- Trainer Security by Design, CSIR

Beveiliging vanaf het Begin

Beveiliging als prioriteit

Beveiliging moet vanaf het begin centraal staan bij digitale projecten om risico's effectief te minimaliseren.

Integratie in ontwerp

Als beveiliging direct in de ontwerpfase wordt meegenomen, zijn dure en ingewikkelde aanpassingen later te voorkomen.

Voorkomen van schade

Het negeren van beveiliging kan leiden tot ernstige risico's en aanzienlijke financiële schade voor organisaties.

Agenda (1/2)

01	Invoering CSIR bij Gemeente, Waterschap of Provincie
02	Waarom CSIR en BIO2?
03	Wat valt er onder de CSIR?
04	Stappenplan invoering CSIR
05	Praktijkvoorbeeld hack Object brug

Agenda (2/2)

06	Eisen aan objectbeheerder
07	Maatregelenpakketten + beveiligingsplan
08	Weerstandsniveau 2 – Externe Toegang
09	Top 10 risico's CSIR
10	Afsluiting & Takeaways

- In het blauwe kader tips toegevoegd nav Q+A

Baseline voor IT

BIO2 verplicht normenkader

Informatiebeveiliging binnen de overheid

Gebaseerd op ISO 27001/27002

met aanvullende overheidsmaatregelen

Doel: een gemeenschappelijk basisniveau van informatieveiligheid en vertrouwen in de keten

BIO2 als Baseline

BIO2 wordt verplicht via wetgeving (voor overheid)
Cyberbeveiligingswet (Cbw)

IT: hanteer de BIO2
OT: CSIR toepassen, altijd naast BIO2

De beheersmaatregelen uit NEN-ISO/IEC 27002 en de BIO kunnen, waar nodig én gelijkwaardig worden vervangen of gecombineerd met beheersmaatregelen uit andere normen en richtlijnen, zoals voor zorginformatie de **NEN 7510** en voor Operationele Technologie (OT) de **CSIR** en IEC 62443 Industriële cybersecurity.

BIO2 als Baseline

BASELINE INFORMATIEBEVEILIGING OVERHEID 2

BIO 2

24 september 2025, versie 1.2 definitief

BIC

Rijksoverheid

VNG

BIO2 wordt verplicht via wetgeving (voor overheid)

Cyberbeveiligingswet (Cbw)

IT: hanteer de BIO.

OT: CSIR toepassen, altijd risicoanalyse BIO2

De bestuursorganen passen uit NEN-ISO/IEC 27002 en de BIO kunnen, waar nodig én gelijkwaardig worden aangevuld of gecombineerd met beheersmaatregelen uit andere normen en richtlijnen, zoals voor informatie de **NEN 7510** en voor Operationele Technologie (OT) de **CSIR** en IEC 62443 Industriële cybersecurity.

Doel CSIR: Veiligheid, beschikbaarheid én betrouwbaarheid van vitale processen.

Waarom een Baseline voor informatiebeveiliging

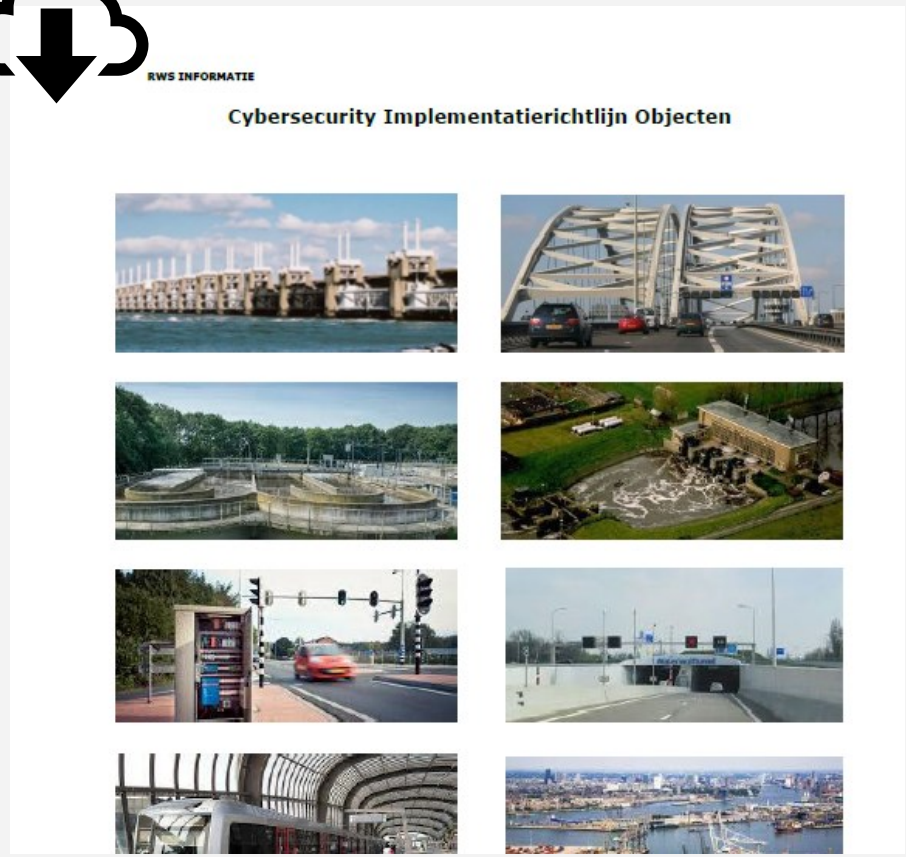
CSIR =
Cybersecurity Implementatierichtlijn Objecten

Praktische uitwerking voor OT/IA
(Industriële Automatisering)

- Verkeersregelinstallaties
- Bruggen
- Gemalen
- ...

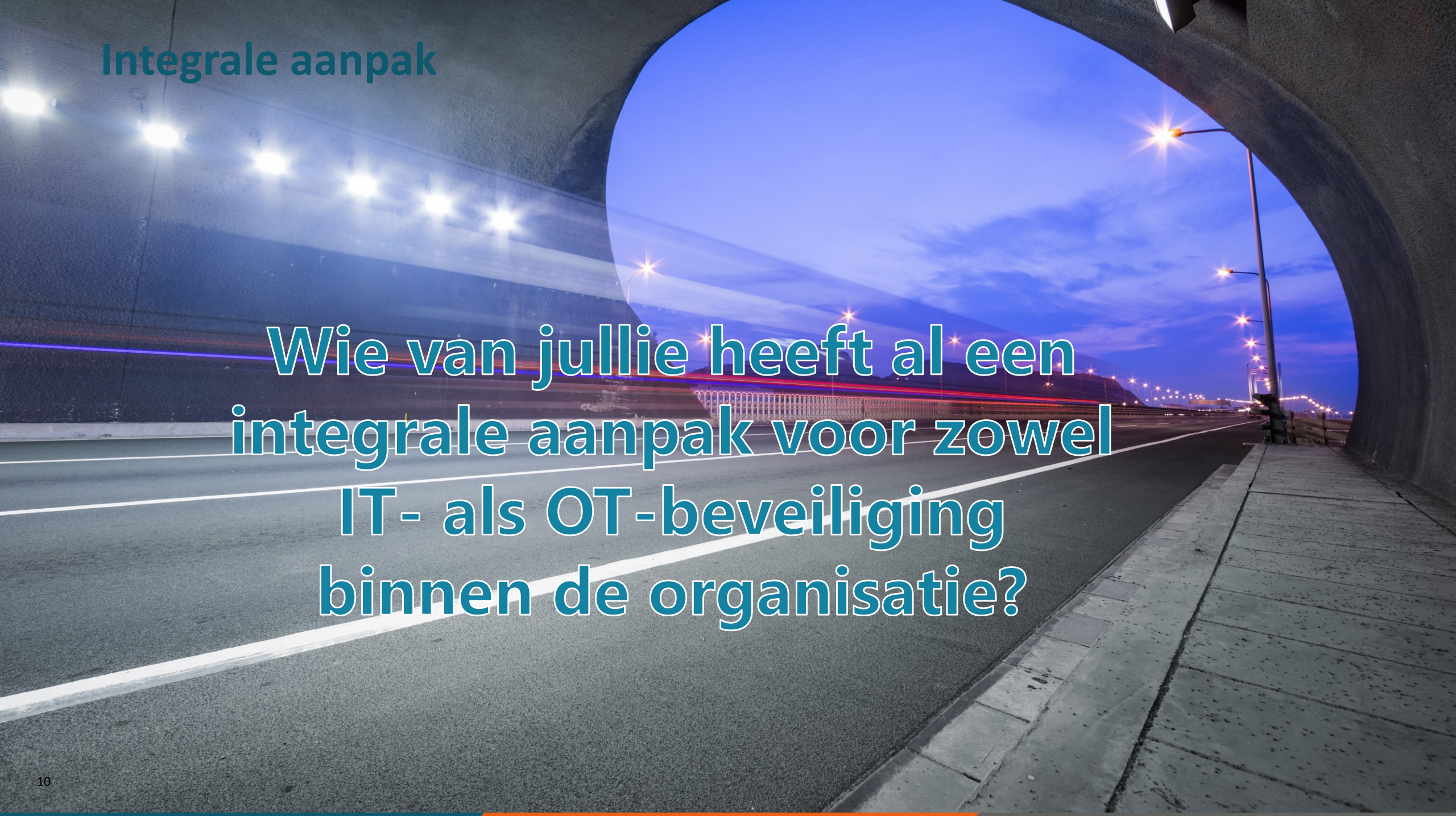
De CSIR vertaalt de BIO2 naar de praktijk van
OT-systemen en voegt eisen toe uit IEC 62443

CSIR: CyberSecurity ImplementatieRichtlijn | CERT-WM



https://www.cert-wm.nl/documenten-overheden

Integrale aanpak



Wie van jullie heeft al een integrale aanpak voor zowel IT- als OT-beveiliging binnen de organisatie?

Verantwoordelijkheid Cybersecurity

- Waarom heeft (in mijn ogen) een top down aanpak voor security de voorkeur?

Het senior management (de asset owner)
Motivatie

- Verantwoordelijk voor het (blijven) functioneren van de asset om de primaire functies te leveren
- Borgen dat de medewerkers voldoende tijd krijgen om security maatregelen te borgen in de lifecycle (en te documenteren)

Pas als de verantwoordelijke op de hoogte is van de security risico's, is de verantwoordelijke in staat deze verantwoordleijkheid te dragen.

Verantwoordelijkheid Cybersecurity

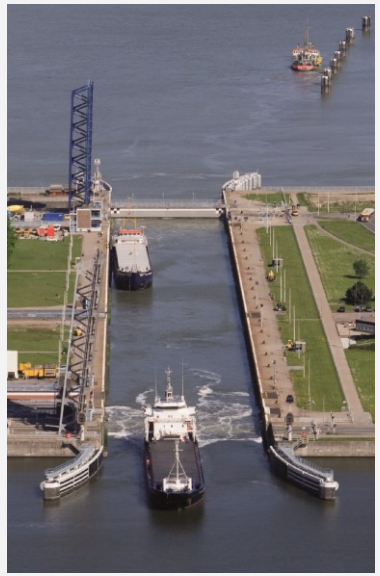
- Waarom heeft (in mijn ogen) een top down aanpak voor security de voorkeur

Het senior management (de asset owner)
Motivatie
- Verantwoordelijk voor het (blijven) functioneren van de asset om de primaire functies te leveren
- Borgen dat de medewerkers voldoende tijd krijgen om security maatregelen te borgen in de lifecycle (en te documenteren)

Pas als de verantwoordelijke op de hoogte is van de security risico's, is de verantwoordelijke in staat zijn verantwoordelijkheid te dragen.

Soms is het vinden van de verantwoordelijke (asset owner) een uitdaging!

Wat valt er onder de CSIR? Scope?



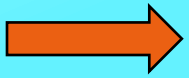
Alle OT-objecten: verkeersregelinstallaties, bruggen, gemalen, sluizen, etc.

Zowel bestaande als nieuwe objecten.

Geldt ook voor alle netwerk- en informatiesystemen direct nodig voor de aansturing.

Best passende baseline voor gekoppelde informatiesystemen?

- Wat is de meest passende beveiligings baseline voor gekoppelde informatiesystemen?



Alle systemen in het IV domein (kantoor automatisering) moeten voldoen aan de BIO2 baseline.
Op basis van het Risico van gekoppelde systemen kunnen wel maatregelen (vooral voor verhoogde beschikbaarheid) genomen worden.
Denk b.v. aan:

- *Off-line redundant systeem*
- *Data-overdracht via systemen in de DMZ*
- *Continue validatie en filtering bij dataoverdracht*

Best passende baseline voor gekoppelde informatiesystemen?

- Wat is de meest passende beveiligings baseline voor gekoppelde informatiesystemen?

Alle systemen in het IV domein (kantoor automatisering) moeten voldoen aan de BIO2 baseline.
Op basis van het Risico van gekoppelde systemen kunnen wel maatregelen (vooral voor verhoogde beschikbaarheid) genomen worden.
Denk b.v. aan:
- *Off-line redundant systeem*
- *Data-overdracht via systemen in de DMZ*
- *Continue validatie en filtering bij datatoverdracht*

Je wil ten slotte security incidenten voorkomen zoals die van Maersk (2017), AH (Kaashack)! En LandRover (2025)

Stappenplan invoering CSIR

1. Inventarisatie & Classificatie
    - Alle OT-objecten in kaart brengen
    - Scope bepalen
    - Risicoanalyse (BIA)
    - Functieboxen en weerstandsniveau bepalen
2. Leveranciers contracteren
3. Implementatie maatregelenpakketten (CSIR hoofdstuk 1 & 2)
4. Opstellen beveiligingsplannen
5. Borging in ISMS

Gedurende de Life cycle

- Audits, testen, continue verbetering

Assetmanagement

Wie heeft al een actuele CMDB voor OT-assets?

Hoe houden jullie deze actueel?

= *essentieel uitgangspunt voor monitoring en detectie*

Wie heeft al een actuele CMDB voor OT-assets?

- Wie heeft al een actuele CMDB voor OT-assets?

Nog geen 10% van de aanwezigen staken hun hand (min of meer) op…..

Automatiseer het inventariseren van de assets! Het zal helaas voorlopig veel sneakerwerk blijven…

Eisen voor Objectbeheerder

Objectbeheerder draagt zorg voor en ziet erop toe dat waar nodig in de beheer en onderhoudscontracten met onderaannemers:

a. geheimhouding is opgenomen;
b. training- en opleidingsvereisten alsmede overige benodigde certificeringen zijn beschreven;
c. screening van personeel is geregeld (bijv. VOG);
d. beschreven is dat de beveiligingshuisregels van Opdrachtgever strikt in acht moeten worden genomen;
e. een concrete procedure is vastgelegd met betrekking tot incidentresponse en voor escalatieprocedures met de leverancier (24*7) en dat deze bij alle betrokkenen bekend is;
f. de procedures voor fysieke toegang tot objecten en ruimten, alsook de logische toegang tot systemen zijn vastgelegd;
g. de registratie en rapportage van beveiligingsincidenten is geregeld;
h. beschreven is dat handelingen van medewerkers en systemen worden gelogd en gemonitord ;
i. de procedure “Toegang Derden” van de objecteigenaar voor de logische toegang tot netwerken en systemen moet worden gevolgd. De tijdelijke toegang tot de systemen ten behoeve van ondersteuning dient geautoriseerd te zijn en handelingen dienen te worden gelogd.
j. beschreven is dat onderhoud en wijzigingen op ICS/SCADA systemen alleen uitgevoerd mogen worden vanaf systemen

Praktijkvoorbeeld – Bruggen

Een brug wordt op afstand bediend.

Stel: er is onvoldoende netwerksegmentatie. Indien een aanvaller toegang heeft tot het kantoornetwerk en er geen goede afscherming van het OT gedeelte is. Kan je bij de KA dan kan ook toegang krijgen tot de brugbesturing.

Oplossing:

- Asset-inventarisatie *(weet wat je beveiligt)*
- Fysieke/logische scheiding van netwerken
- Strikte toegangscontrole *(+unieke accounts)*
- Monitoring en logging

Maatregelen Externe logische Toegang

Cybersecurity Implementatie Richtlijn

2.2 Maatregelen logische toegang

Mens		Weerstandsniveau			
No.	Vereiste	1	2	3	4
LM11	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel wordt verwezen naar paragraaf 2.7 de maatregelen-set “bewustwording en training” van de Cybersecurity Implementatierichtlijn Objecten.	X	X	X	X

Procedures en Organisatie		Weerstandsniveau			
No.	Vereiste	1	2	3	4
LP1	Er kunnen controles worden uitgevoerd op de naleving van het logische toegangsproces.	X	X	X	X
LP2	Er dient door het management erop toe te worden gezien dat: a. de toegang voor de bedienaars en beheerders tot ICS/SCADA en overige ondersteunende ICT-systemen uitsluitend plaatsvindt, rol gebaseerd en op basis van het ‘need to have’ en 'segregation of duties' principe; b. de toewijzing en het gebruik van privileges van administrators en systeembeheerders beperkt dienen te blijven tot het strikt noodzakelijke; c. fysieke toegang tot objecten en ruimten waar zich informatie, software en andere bedrijfsmiddelen (o.a.	X	X	X	X

Maatregelen Externe logische Toegang

Cybersecurity Implementatie Richtlijn

2.2 Maatregelen logische toegang

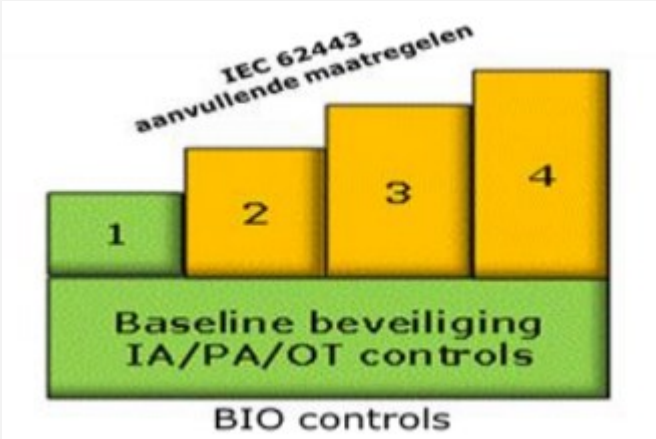
Techniek		Weerstandsniveau			
No.	Vereiste	1	2	3	4
LT1	De logische toegang tot informatiesystemen en netwerk dient plaats te vinden na het succesvol doorlopen van het identificatie, authenticatie en autorisatieproces (IAA), waarbij de IAA-gegevens in principe in versleutelde vorm worden uitgewisseld en opgeslagen.	X	X	X	X
LT2	De toegang tot ICS/SCADA en overige ondersteunende ICT-systemen is geblokkeerd, tenzij het expliciet is toegestaan.	X	X	X	X
LT3	Voor bedienaars, beheerders en systemen worden unieke ID's gehanteerd zodat uitgevoerde handelingen terug te leiden zijn tot een persoon of systeem.	X	X	X	X
LT4	Voor bedienaars, beheerders, software processen en systemen worden unieke ID's gehanteerd zodat uitgevoerde handelingen terug te leiden zijn tot een persoon, software proces of systeem.			X	X
LT5	Het aantal gelijktijdige sessies dat kan worden opgezet door enige gebruiker (mens, software-proces of apparaat) dient te worden beperkt en instelbaar te zijn.	X	X	X	X

b. de toewijzing en het gebruik van privileges van administrators en systeembeheerders beperkt dienen te blijven tot het strikt noodzakelijke;
c. fysieke toegang tot objecten en ruimten waar zich informatie, software en andere bedrijfsmiddelen (o.a.

Maatregelen Externe logische Toegang

Risico verminderen voor onbevoegde digitale toegang

- Externe toegang tot OT-systemen alleen bereikbaar via centrale, beveiligde voorzieningen.
- MFA verplicht voor remote toegang vanaf onvertrouwd
- Gebruik van unieke accounts, geen generieke logins
- Aanvraag toegang procedureel vastgelegd en aangevraagd met een wijzigingsverzoek of enrollment
- Toegang wordt automatisch beëindigd
- Authenticatiegegevens worden centraal beheerd en periodiek gecontroleerd
- Regelmatige review van toegangsrechten
- Logging van alle externe toegang, minimaal 6 maanden bewaren
- Monitoring van remote sessies door SOC/SIEM
- Alleen geautoriseerde apparatuur mag verbinding maken (device control)



Maatregelen vastgelegd in het Cybersecurity beveiligingsplan

Dit zijn CSIR maatregelen (weerstandsniveau 2)

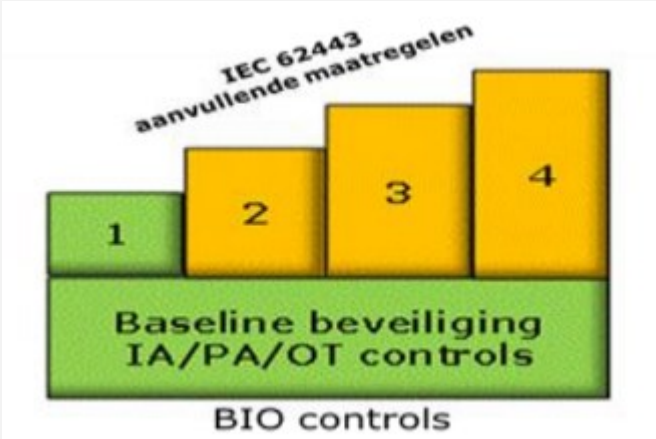
Maatregelen Externe logische Toegang

Risico verminderen voor onbevoegde digitale toegang

- Externe toegang tot OT-systemen alleen bereikbaar via centrale, beveiligde voorzieningen.
- MFA verplicht voor externe toegang vanaf onvertrouwd
- Gebruik van unieke accounts, geen generieke logins
- Aanvraag toegang procedureel vastgelegd en aangevraagd met een wijzigingsverzoek of enrollment
- Toegang wordt automatisch beëindigd
- Authenticatiegegevens worden centraal beheerd en periodiek gecontroleerd
- Regelmatig review van toegangsrechten
- Logging van alle externe toegang, minimaal 6 maanden bewaren
- Monitoring van remote sessies door SOC/SIEM
- Alleen geautoriseerde apparatuur mag verbinding maken (device control)

Maatregelen vastgelegd in het Cybersecurity beveiligingsplan

Dit zijn CSIR maatregelen (weerstandsniveau 2)



Risico gestuurd werken!
= verantwoorden
waarom je keuzes maakt

Risico analyse: IT heeft BIV, hoe dat je dat bij OT?

- Hoe doe je een risico analyse in de OT?

Slechte IT Risico analyses beperken zich vaak tot de impact (schade) van het niet functioneren van het systeem maar vergeten de echte schade voor de ‘klant’ te duiden. (burgers/bedrijven/ketenpartners)

De CSIR gaat uit van meer impactcategorien op bais van de RAMSSHEEP methodiek.
Zie de CSIR 3.0 bladzijde 151
Bijlage C - Best practice voor risico inschatting bij CSIR afwijkingen

Voer een risicoanalyse altijd uit met een multidisciplinair team, liefst met de eindverantwoordelijke!

Risico analyse: IT heeft BIV, hoe dat je dat bij OT?

- Hoe doe je een risico analyse in de OT?

Slechte IT Risico analyses beperken zich vaak tot de impact (schade) van het niet functioneren van het systeem maar vergeten de echte schade voor de 'klant' te duiden. (burgers/bedrijven/ketenpartners)

De CSIR gaat uit van meer impactcategorien op basis van de RAMSSHEEP methodiek.
Zie de CSIR 3.0 bladzijde 51
Bijlage C - Best practice voor risicoclassificatie bij CSIR afwijkingen

Voer een risicoanalyse altijd uit met een multidisciplinair team, liefst met de eindverantwoordelijke!

Vraag de senior medewerker van het object waar je de stekker uit moet trekken om het object z.s.m. te beschadigen...

Uitgangspunt Cybersecurity

1. Uitgangspunt
   - Beveiliging maakt integraal onderdeel uit van elk proces, systeem of product en dit in de lifecycle
   - Infraclassificatie objecten met cybersecurity weerstandsniveau's
   - Maatregelen voor Mens, Proces & Organisatie en Techniek
   - Focus op preventie, detectie en response
   - (Internationale) standaarden ISO 27001, IEC 62443
   - Cybersecurity contractueel geborgd (VSP, VSE)
2. Uitwerking van security doelstellingen is transparant en toetsbaar voor de marktpartijen en toezichthouders

→ Cybersecurity Beveiligingsplan

Cybersecurity Dilemma

Hoe ga je om met oude objecten, die afwijken van de security baseline?

Repareer alleen wat nodig is

Repareer de grootste security risico's

Cybersecurity Beveiligingsplan

Cybersecurity Beveiligingsplan / Cybersecurity Dossier [20XX]

voor

[beheerobject(en)]

Rijkswaterstaat

hetWaterschapshuis

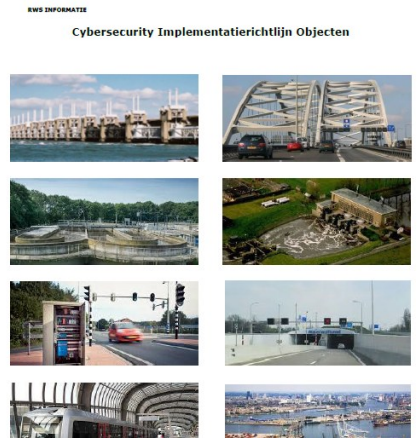
Opdrachtnemer/Uitvoerder	
Naam	
Functie	
Datum	
Status	
Classificatie	Vertrouwelijk (*na invulling door ON*)
Paraaf	

5.1.1.1	De uitwerking van de controls voor de IA/PA/OT dient vastgelegd en onderhouden te worden in de template "Cybersecurity Dossier/Cybersecurity Beveiligingsplan". Bij uitbesteding dient het "Cybersecurity Dossier/Cybersecurity Beveiligingsplan" ter acceptatie te worden voorgelegd aan de verantwoordelijke. Een template voor het "Cybersecurity Dossier/Cybersecurity Beveiligingsplan" is beschikbaar.
5.1.1.1	De werking van de beschreven maatregelen in het Cybersecurity Dossier/Cybersecurity Beveiligingsplan/security by design documentatie dient in lijn met de PDCA cyclus jaarlijks geëvalueerd en waar nodig geactualiseerd te worden..

Cybersecurity Beveiligingsplan

CSIR in een notendop (1-3)

Gericht op de 10 grootste risico's in infra.



1. Niet geautoriseerden hebben fysieke toegang tot bedien- en technische ruimten

2. Niet geautoriseerden hebben logisch toegang tot de ICT en ICS/SCADA-systemen

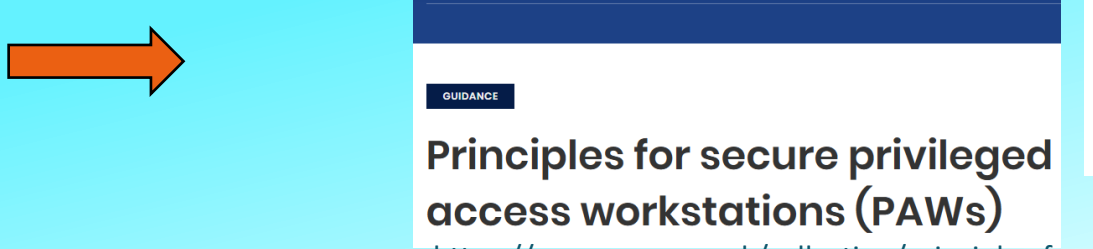
3. Informatie over zwakke plekken in de beveiliging en beveiligingsincidenten ontbreekt alsmede een handelingsperspectief

CSIR in een notendop (4-5)

Gericht op de 10 grootste risico's in infra.

4. Niet geautoriseerden hebben (via Internet of draadloze toepassingen) toegang tot het datanetwerk

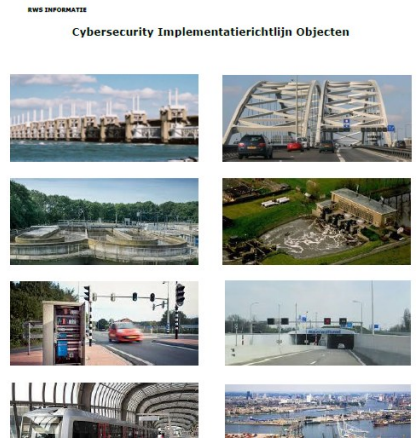
5. ICT en ICS/SCADA-systemen bevatten kwetsbaarheden en zijn vatbaar voor malware



https://www.ncsc.gov.uk/collection/principles-for-secure-paws

CSIR in een notendop (6-7)

Gericht op de 10 grootste risico's in infra.

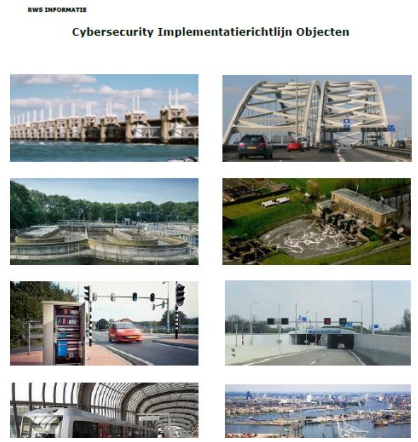


6. Het niet kunnen detecteren en analyseren van afwijk
   op het datanetwerk en de zich voorgedane incidente
   logging en monitoring

7. Risico's geïntroduceerd door bedien en of onderhoudsmedewerkers. Deze zijn zich niet bewust van onveilige situaties, beschikken niet over de juiste opleiding en training, hebben geen geheimhoudingsverklaring getekend of beschikken niet over een recente verklaring omtrent het gedrag

CSIR in een notendop (8-10)

Gericht op de 10 grootste risico's in infra.



8. Functionele wijzingen brengen onvoorziene veiligheic beveiligingseffecten met zich mee en kunnen zelfs de functionele werking van ICT en ICS/SCADA-systemer volledig doen uitvallen

9. De handhaving en de effectiviteit van de Cybersecurity maatregelen is niet gewaarborgd alsmede de structurele borging bij onderaannemers

10. Bij systeemstoringen of functionele wijzigingen is er geen terugvaloptie (geen back-up en recovery proces)

Cybersecurity Dilemma's

- Wat doe je als een leverancier geen patches meer levert voor een verouderde (brug)besturing?

  → Neem alternatieve compenserende maatregelen en/of
  Accepteer het rest Risico (door senior management oftewel de asset owner)

- Wie is verantwoordelijk voor de cybersecurity van een object dat door meerdere partijen wordt beheerd?

  → Senior management/asset owner

CSIR Takeaways

Begin klein, leer en schaal op
Blijf in gesprek met collega's, leveranciers en ketenpartners
Begin bij de start:

Security is geborgd:

- Business case
- Architectuur en Ontwerp
- Contracten
- Life cycle

Dank u wel!

Marco Rijkschroeff
Specialist OT Cybersecurity

marco.rijkschroeff@ict.nl
Creating a smarter world | ICT Group

Aanpak met de Security Baseline voor infra en water

CSIR is praktisch en noodzakelijk voor veilige OT binnen de overheid