



OKPT

KENNISPLATFORM TUNNELVEILIGHEID

Onze taken



1. Bibliotheek - website
2. Helpdesk - Q&A
3. Inventarisatie
- 4. Kennis delen**
5. Publieks-communicatie



1.



2.



3.



4.



5.

Ons team



Harry de Haan
Coördinator



Daan Seesing
Specialist niet-Rijkstunnels



Karin Clement
Managementondersteuner



Niels Veen
ICT-faciliteiten

+ flexibele schil



Marije Bockholts



Jan Küchel

Agenda

12:00 uur Welkom en KPT

12:10 uur Tunnelveiligheid & Cybersecurity

door Cedric Both en Marc van der Zandt

13:00 uur(?) Vragen

Marc van der Zandt
Compliance made easy

SAFE
SECUR

Cedric Both
IT & OT Specialist

NEXT LEVEL SPECIALISTS

DATA**DIGEST**

NIS2

Cyberbeveiligingswet

Waarom we hier zijn

Tunnelveiligheid & Cybersecurity

De invoering van de Europese Cyberbeveiligingswet (NIS2) raakt tunnelbeheerders direct — maar de kern van dit verhaal is niet de wet, het is de basishygiëne die je toch al aan je klant en publiek verschuldigd bent.

- 1 Val je onder de wet?
- 2 Wat betekent dat concreet?
- 3 Hoe leg je dat vast — voor jezelf, de toezichthouder én de rechter?

Waarom NIS2 nu op de agenda staat

De Europese Cyberbeveiligingswet (NIS2) verplicht organisaties in kritieke en belangrijke sectoren — mogelijk óók tunnelbeheerders — tot een aantoonbaar niveau van digitale weerbaarheid.

1

Val je onder de wet?

Bepaal of jouw organisatie als essentieel of belangrijk wordt aangemerkt — sector, omvang en type dienst zijn bepalend.

2

Wat houdt het in?

Een zorgplicht (passende beveiligingsmaatregelen) én een meldplicht (incidenten tijdig melden bij de toezichthouder).

3

Wat is de onderliggende vraag?

Heb je je basishygiëne — richting klant en publiek — eigenlijk al op orde, los van wat de wet voorschrijft?

De echte drijfveer is niet compliance zelf, maar goed geregeld zijn richting klant en publiek — de wet is daarbij een aanleiding, geen doel.

Zorgplicht, meldplicht — en het dossier dat overblijft

Zorgplicht

Passende technische en organisatorische maatregelen nemen, risicogebaseerd en aantoonbaar — vooraf, niet achteraf.

Meldplicht

Significante incidenten binnen de wettelijke termijnen melden bij de toezichthouder (eerste melding vaak binnen 24 uur).



Bij een groot incident telt je dossier

Als het toch misgaat, vraagt je klant, de toezichthouder — en in het ergste geval de rechter — niet alleen wát er gebeurd is, maar of je vooraf redelijkerwijs had gedaan wat van je verwacht mocht worden.

Een op orde zijnd compliencedossier — assets, risico's, maatregelen, besluiten — is dan het verschil tussen aantoonbare zorgvuldigheid en het ontbreken daarvan.

Weet wat je hebt, voordat je het beveiligt

1 Asset-inventarisatie

- SCADA, camera's, sensoren, verlichtingsbesturing, PLC's, netwerkkapparatuur — wat draait er allemaal?
- Wat is verbonden met internet of externe netwerken, direct of indirect?
- Welke leveranciers/integrators hebben remote toegang voor support of onderhoud?

Veel organisaties ontdekken hier verbindingen die niemand meer kent of documenteert.

2 Risico-classificatie

- Wat is veiligheidskritisch (brandmelding, ventilatie, nooddeuren) versus 'alleen' operationeel (tol, statistieken)?
- Wat is de impact bij uitval of manipulatie — verkeershinder, gevaar voor leven, reputatieschade?

Geeft een prioriteitenlijst — in plaats van overal gelijk beginnen.

Quick wins en duidelijke eigenaarschap

3

Quick wins: weinig kosten, veel opbrengst

Credentials:

Standaard wachtwoorden op apparatuur — vaak nog fabrieksinstellingen.

Segmentatie:

Eén plat netwerk, of zijn OT en IT al gescheiden? VLAN-scheiding is al een grote sprong.

Remote access:

Toegang van leveranciers: via VPN met MFA, of staat er een RDP-poort open naar buiten?

4

Governance: wie is verantwoordelijk

- Wijs een eigenaar aan van de asset.
- Elke asset moet zijn toegewezen.

Laat je extern toetsen — en vermijd deze valkuilen

5 Extern laten toetsen

- Een nulmeting of quick-scan door een gespecialiseerd bureau geeft een objectief beeld — zonder dat je alle expertise zelf in huis hebt.
- Dit hoeft geen volledige pentest te zijn: een risico-assessment op basis van interviews en documentatie is al waardevol.

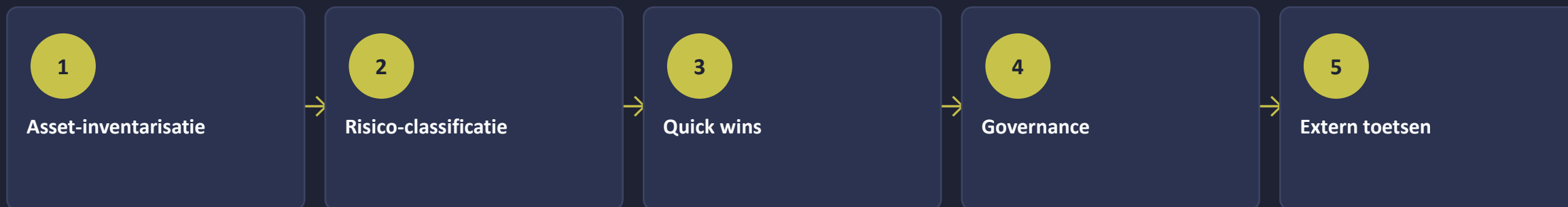
Precies het soort vraag om aan gespecialiseerde partijen te stellen: hoe pak je een eerste assessment in de praktijk aan?

× Wat je beter niet doet

- × Meteen een grote, dure end-to-end oplossing kopen zonder eerst te weten wat je beveiligt.
- × Wachten tot NIS2 voor jou 'verplicht' wordt — de basis helpt sowieso, los van wetgeving.

Begin met zicht, niet met een oplossing

Krijg eerst zicht op wat je hebt en wat het meest kritiek is, voordat je investeert in oplossingen. Dat is precies het soort vraag die je aan gespecialiseerde begeleiders kunt stellen — hoe zij zo'n eerste assessment in de praktijk aanpakken bij tunnelbeheerders die nog aan het begin staan.



Basishygiëne op orde = goed voor je klant, je publiek — én je compliancedossier als het er ooit op aankomt.

De praktijk leunt nu veelal op alleen Cybersecurity richtlijnen



BIO & CSIR (IEC 62443)

- Men wijst nu vaak direct naar de richtlijnen en denk dat daarmee alles afgehecht is.
- Verantwoordelijkheden worden vaak naar de Aannemer/onderhoudspartij gedelegeerd en daarmee is het dan “klaar”
- Vaak is de Opdrachtgever zelf nog helemaal niet in staat om mee te doen in de process-flow van Cybersecurity.



Verouderde systemen

- De richtlijnen zijn makkelijk toepasbaar bij een nieuw object of een renovatie. Maar het is niet eenvoudig toepasbaar bij bestaande objecten.
- Er zijn nog veel systemen die verouderd zijn, maar toch moeten blijven draaien. Daar is niet eenvoudig van te zeggen “die moeten nu per direct voldoen of geupdate worden”.
- Het ontbreekt regelmatig aan een pragmatische insteek en daarbij is er ook nog gebrek aan goede kennisdeling en uitwisselen van ervaringen.

Hoe zou het anders kunnen?



Risico classificatie & Assets in kaart

- Maak samen met elkaar een duidelijke inventarisatie van de Risico's en bepaald hoe "erg" deze zijn. Denk bijvoorbeeld aan de weerstandniveau's van RWS, maar niet alles hoeft meteen naar het hoogste niveau.
- Werk met elkaar samen om alle Assets goed in kaart te brengen, zodat ook duidelijk wordt waar precies Risico's zitten die wellicht afgedicht moeten worden.
- Met de nieuwe wetgeving zul je met elkaar moeten gaan samenwerken om tot de juiste inzichten te komen en werkbare oplossingen te bedenken.



Hoe om te gaan met de verouderde systemen?

- Weet om welke systemen het gaat binnen ieder object. Ook na nieuwbouw of renovatie verouderen de systemen vrijwel direct. Er moeten dus aan het begin afspraken gemaakt worden hoe de systemen onderhouden kunnen worden.
- Het is niet perse erg dat er verouderde systemen draaien, er zijn genoeg relatief simpele en kostenefficiënte oplossingen te bedenken om het toch veiliger te maken. Continu inzicht in de actuele toestand helpt hierbij.
- Maak het niet te moeilijk en hou een pragmatische insteek. Alles helemaal dicht willen timmeren en alles afsluiten van de buitenwereld is niet noodzakelijk. Werk met elkaar samen om de beste oplossing te vinden.

**Logic will get you from A to B,
imagination will take you everywhere**
– Albert Einstein

**SAFE
SECUR**

NEXT LEVEL SPECIALISTS 
DATA DIGEST