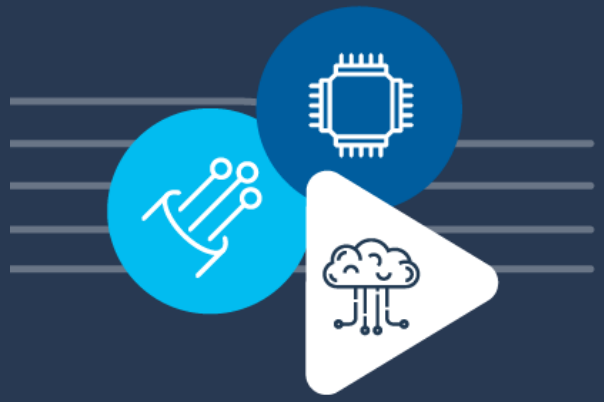


SuppliersDay
INFRABEL

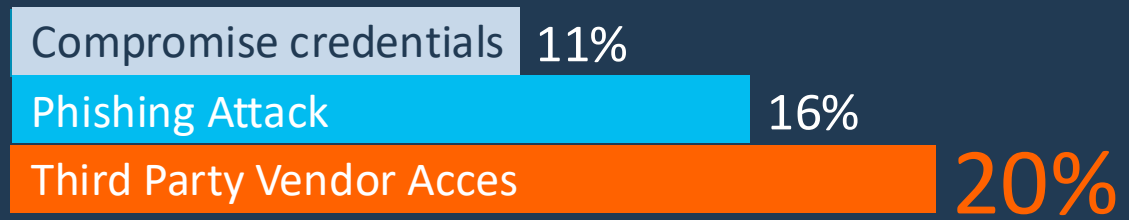
ICT


LIVE
TOUT LE TRAFFIC
EST INTERROMPU.
AUCUN TRAIN
NE CIRCULE.
Quai
Gpeer
11
BREAKING NEWS
CYBER ATTACK ON BELGIAN RAILWAYS
07:57
ALL TRAINS STOP DUE TO CYBERATTACK ON SIGNALING SYSTEMS

Waarom we op *jou* rekenen voor *onze* Cyber-Resilience

Belangrijkste vectoren 2025

32%
van de cyberaanvallen maakte gebruik van niet verbeterde softwarefouten



17x
Aanvallen gericht op de Supply Chain zijn nu 17 keer duurder om op te lossen dan directe datalekken (binnen het bedrijf zelf).

+ 1 week
72% van de bedrijven doen er meer dan een week over om hun werking volledig te herstellen. In sectoren waar veel op het spel staat, bedraagt de hersteltijd vaak meer dan zes weken.

20 tot 80 mia €
De verliezen zijn opgelopen tot ongeveer €20 tot €80 miljard in slechts 15 maanden als gevolg van grootschalige datalekken.

Een wettelijk en regelgevend kader

NIS2-wet

Infrabel is een Essentiële Entiteit in de zin van de NIS2-wet

Cyber Resilience Act

Alle digitale producten die Infrabel aankoopt, moeten voldoen aan de vereisten van de CRA

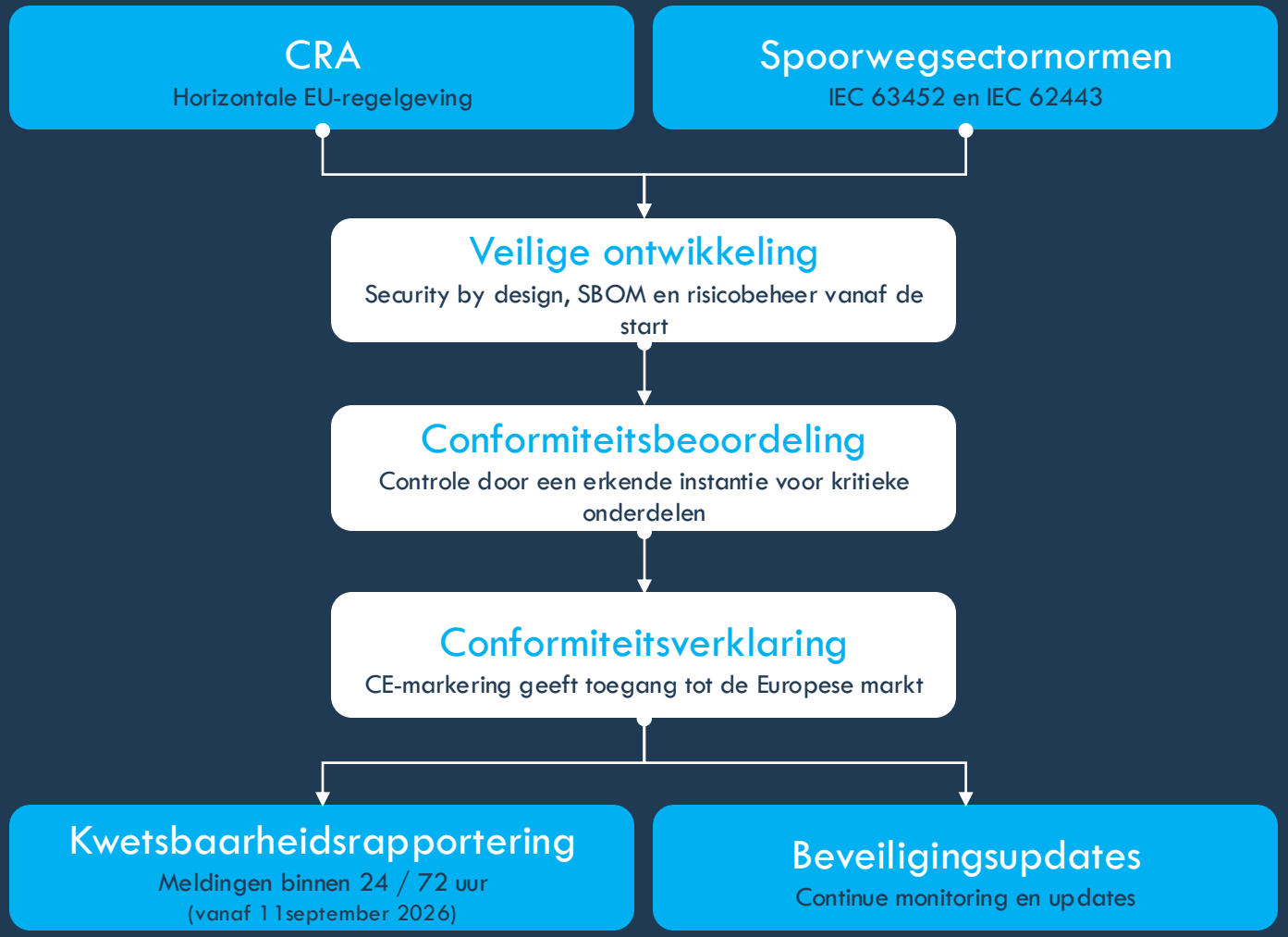
IEC 62443 //63452

De naleving van industrie- en sectornormen is essentieel voor kritieke oplossingen

AI Act

Naleving van de AI Act is verplicht

De impact van het CRA



De **CRA vervangt niet** wat we vandaag al doen volgens de IEC-normen en bestaande cybersecurityspecificaties.

De **CRA vult deze** referentiekaders **aan** en zorgt voor duidelijke traceerbaarheid tussen de Europese wetgeving en de sectornormen die de toezichthouders van ons verwachten.

Wat verwachten we precies van je?

1. Cyberbeveiligingscultuur en opleiding van het personeel
2. Cyberbeveiligingsbeheer en risicobeheer
3. Cyberbeveiliging vanaf het ontwerp en kwetsbaarheidbeheer

4. Continue bewaking, actieve detectie en reactie op incidenten
5. Cyberbeveiliging van de toeleveringsketen en derde partijen
6. Verbintenis, contractuele clausules en beheer van de verantwoordelijkheden

Onze uitdagingen

Modernisering van digitale spooroplossingen

In de **volgende 10 jaar** zal Infrabel zijn digitale oplossingen (FRMRS, New Signaling/IXL, enz.) moderniseren Maar **Cyber Resilience is vandaag al onmisbaar.**

Digitale, technologische en strategische soevereiniteit

Infrabel moet als kritieke spoorinfrastructuur zijn **soevereiniteit garanderen tegenover** digitale en Supply Chain-risico's.

Artificial Intelligence : vriend of vijand?

Volgens het rapport « *Global Cybersecurity Outlook 2026* » van het WEF zal artificiële intelligentie binnenkort de **belangrijkste drijvende kracht worden achter veranderingen** in cyberbeveiliging - al in de komende maanden.

Waarom we op jou rekenen om oplossingen in te zetten op basis van artificiële intelligentie

AI bij Infrabel: strategische opportuniteit, nieuwe vereisten

AI is overal op de werkvloer in opmars - maar in kritieke spoorinfrastructuur brengt **een slecht ontworpen, gekleurd of niet goed omkaderd systeem de veiligheid, naleving en het vertrouwen** in gevaar.

Strategische opportuniteiten

- Predictief onderhoud
- Verkeersoptimalisatie en incidentbeheer
- Anomaliedetectie
- Operationele beslissingsondersteuning

Nieuwe verantwoordelijkheden

- AI Act (EU 2024/1689) - transport geclassificeerd als **hoog risico**
- **Zware** sancties (AI Act)
- ISO 42001 - referentie voor IA maturiteit
- Datasoevereiniteit en uitlegbaarheid vereist

Een wettelijk en regelgevend kader

AI Act

Verplichte naleving
voor elk aan Infrabel geleverd AI systeem

GDPR

Strikte omkadering
van de persoonsgegevens en effectbeoordelingen

Soevereiniteit

Hosting en verwerking
binnen de Europese rechtsruimte of zelfs in onze eigen datacentra

ISO 42001

Referentie
om de AI-maturiteit van de leveranciers te beoordelen

Wat verwachten we precies van je?

Twee complementaire assen: AI-governance en AI-projecten

1. **Naleving AI Act: CE-markering en technische documentatie**
2. **ISO 42001:** IA-beleid, risicobeheer, certificering
3. **Ethiek & verantwoordelijke AI** : xAI, menselijk toezicht, opleiding

AI

4. **Betrouwbare AI**: uitlegbaarheid, robuustheid, validatie
5. **Beveiliging vanaf het ontwerp**: vijandig testen, beveiligde pipelines
6. **Souvereiniteit & IP** : data in EU, eigendom van de modellen

Uitvoeren van projecten met AI

Technische vereisten voor veilige, conforme en duurzame IA-projecten

1 Trustworthy AI

- Menselijk toezicht — “human in the loop”
- Robuustheid en precisie in realistische omstandigheden
- Uitlegbaarheid - xAI sterk aanbevolen

2 Security by Design

- Vijandige tests voor kritieke systemen
- Beveiligde en getraceerde data pipelines
- Continue bewaking & waarschuwingen

3 Data Governance

- Soevereiniteit - Europese rechtsruimte
- Intellectueel eigendom van de modellen
- Naleving van GDPR

4 Lifecycle & Maintenance

- Volledige technische documentatie
- Versiebeheer, traceerbaarheid, rollback mogelijk
- Kennisgeving van de kwetsbaarheden, beheer van het einde van de levensduur

Drie kernboodschappen

Naleving is niet onderhandelbaar

De AI Act is geen vodje papier. Doe nu het nodige voor de naleving door elk geleverd systeem.

Governance als basis

Naleving van de AI Act, ISO 42001, AI-beleid, risicobeheer: een sine qua non in kritieke spoorwegen.

Partnership & vertrouwen

We bouwen duurzame IA-partnerships op met toegewijde, volwassen leveranciers.

“We may have all come on different ships, but we’re in the same boat now.”

-Martin Luther King Jr.-