# Dutch Railways Resilience Audit - Samenvatting

Door: Bescherming persoonlijke levenssfeer

## Achtergrond & Introductie

De IT-omgeving van de Nederlandse Spoorwegen wordt voornamelijk beheerd en geëxploiteerd door partijen gespecialiseerd in bedrijfskritische dienstverlening, onder het SPRONG-contract, waarin specifieke vereisten zijn opgenomen met dedicated IT-infrastructuur.

De Nederlandse Spoorwegen reisinformatie- en planningsdiensten werden stabiel ervaren totdat er op 3 april 2022 problemen optraden met de reisinformatie- en be- en bijsturingsdiensten, hierbij zijn de cruciale momenten op de tijdlijn de volgende:

- 09:37 – IT-infrastructuur fout.
- 12:00 – Defecte bovenleiding in Hoofddorp, besluit genomen om alle treindiensten stop te zetten.
- 12:38 – Herstel van de IT-infrastructuur.
- 13:30 – Succesvol herstel van de reisinformatie.
- 14:05 – Actueel beeld materieel blijkt niet te kloppen. Er missen dienstregelingsmutaties van spoornetbeheerder.
- 15:01 – Verwerking nieuw actueel verkeersplan van spoornetbeheerder mislukt.
- 18:46 – IT-specialisten starten handmatig applicatieherstel om resynchronisatiefouten te corrigeren.
- 21:10 – Succesvol functioneel herstel van het actuele beeld van de verkeerssituatie.

Dit incident veroorzaakte een grote storing en onderbreking van de landelijke treindiensten van NS en riep vragen op over de robuustheid en effectiviteit van de momenteel geïmplementeerde IT-weerbaarheid. Daarom is Bell Labs Consulting gevraagd om een onafhankelijke weerbaarheidsaudit uit te voeren waarvan de resultaten in dit document zijn samengevat.

De audit omvatte een end-to-end service keten audit inclusief een multi-vendor en multi-domein analyse, een architectuur- en technologiebeoordeling, kwantitatieve betrouwbaarheidsanalyse en een aanvullende operationele beoordeling. Dit om verbeteringen te identificeren om de algehele robuustheid van de kritische diensten van NS te verbeteren, de paraatheid te verbeteren, de operationele stabiliteit te herstellen, herhalingen te voorkomen en de medewerkers van het Nederlandse Spoorwegen en SPRONG-consortium te informeren over de algehele robuustheid van de oplossing. De controle was gericht op de volgende doelstellingen:

- End-to-end architectuur, servicebetrouwbaarheid en risicoanalyse.
- Operationele robuustheid inclusief het herstelproces van de gehele incidentlevenscyclus van 3 april 2022, onderverdeeld in het proces tot: a) Technisch herstel (datacenterfout) en b) Functioneel herstel (applicatie- en dataflowfout).
- Geprioriteerd verbeteringen en aanbevelingen.

### Back-up systeem functionaliteit

Bij de evaluatie van het incident rees de vraag waarom de beschikbare back-upsystemen faalden. Vanuit IT- en applicatieperspectief is redundantie onderdeel van de basisarchitectuurprincipes voor NS-systemen en -applicaties.

Om 9:37 uur trad er een uitzonderlijke fout op in een van de onderliggende infrastructuur componenten. Op dit specifieke fouttype was geen monitoring aanwezig en deze situatie was tevens niet onderkend als en aanleiding voor automatische uitwijk naar de backupsystemen. Het kostte voor de IT specialisten veel tijd om voor deze uitzonderlijke situatie de grondoorzaak te vinden. Uiteindelijk werd besloten om handmatig de uitwijk naar backupsystemen te activeren.

Om 12:38 werkt de infrastuctuur weer correct en werden applicaties en datastromen weer herstart.

Rond 14:05 uur werd geconstateerd dat het beeld in de systemen niet overeenkwam met het beeld buiten, er werden bijvoorbeeld nog steeds treinritten getoond die geannuleerd waren. Dit bleek te komen doordat mutatieberichten van de spoornetbeheerder vanaf 9:37 niet meer binnenkwamen bij NS.

De mutatieberichten van de spoornetbeheerder bleken inmiddels verloren gegaan te zijn en herstel van het actuele verkeersbeeld via reguliere mutatieverwerking lukte hierdoor niet. Er werd een nieuw actueel verkeersplan bij de spoornetbeheerder aangevraagd.

Om 15:00 uur werd dit actueel verkeersplan ingelezen, echter dit mislukte door fouten in de betreffende bijsturings applicaties bij NS.

Nu de reguliere transactie verwerking en het laden van een nieuw actueel verkeersplan beiden niet tot een actueel beeld van de werkelijke verkeerssituatie leidde werd rond 18:46 uur besloten om met applicatiespecialisten over te gaan tot handmatig herstel uiteindelijk resulterend in de actuele weergave van de toestand op het spoor in de be- en bijsturingssystemen rond 21:10 uur.

### Belangrijke bevindingen en aanbevelingen

Uit het onderzoek zijn verschillende bevindingen naar voren gekomen die vertaald worden naar aanbevelingen voor de NS of technologiepartner(s). Deze bevindingen en aanbevelingen zijn gegroepeerd op basis van de belangrijkste onderwerpen hieronder.

1. De keten van bedrijfskritische applicaties is complex en verdeeld over verschillende systemen en servicepartners. Er is een beperkte end-to-end architectuur weergave beschikbaar op tactisch en operationeel niveau, wat verbeteringen verhindert en de servicecontinuïteit negatief beïnvloedt in het geval van grote incidenten met meerdere toepassingen. Zorg voor een betrouwbare end-to-end bedrijfskritische servicearchitectuur met geografisch redundante infrastructuur, connectiviteit en applicaties. Zorg daarnaast ook voor goede monitoring op de afzonderlijke componenten in en over de gehele keten, met name gericht op de gegevensstromen en bijbehorende drempels (bandbreedte voor de gegevensstromen gebaseerd op business rules).

2. Operationele processen tussen alle servicepartners zijn aanwezig en worden onderhouden, maar op 3 april niet altijd nageleefd. Het wordt aanbevolen om een duidelijke RACI in te stellen voor rollen die betrokken zijn bij de incident-, probleem-, veranderings- en operationele beschikbaarheidsprocessen.
3. Menselijke besluitvormingsprocessen en handmatige interacties moeten in het monitoren en beheer van de IT infrastructuur verder worden verminderd. Door toepassing van automatische failover-oplossingen worden vertragingen en fouten voorkomen.
4. Test regelmatig de juiste werking van beveiligingsmechanismen, oefenprocedures en systeemfail-overs met alle partners in de gehele keten.
5. Applicaties moeten worden ontworpen volgens de best practices voor “redundantiemechanismen met hoge beschikbaarheid”. Lopende activiteiten om deze best practices te implementeren, waaronder automatische failover, moeten worden versneld.

De bevindingen, verbeteringen en aanbevelingen worden geprioriteerd en gedeeld met de NS en technologiepartner(s). De implementatie van de belangrijkste bevindingen is aan de gang om het risico op herhaling van het grote incident te minimaliseren. De overige bevindingen worden in nauwe samenwerking tussen alle betrokken partijen gepland.