

Vitale infrastructuur: ketenuitval is grootste



Drinkwater, gas, elektriciteit, telefonie, internet, tv, radio, wegen, spoorwegen, stations, metro, havens, vliegvelden, geldautomaten. We hebben ons leven afhankelijk gemaakt van netwerken die nauw met elkaar zijn verbonden. Daardoor kan een klein ongeluk al grote gevolgen hebben. Om nog maar te zwijgen over een terroristische aanslag of een aanval via cyberspace. Een goede voorbereiding op zulke noodsituaties is dan ook geboden.

'Wereld in ban van internetvirus.' Zulke koppen staan vaker in de krant. Maar in maart ging het om het Conficker-virus, kwaadaardige software waarmee cybercriminelen complete landen kunnen ontregelen of offline halen. Elektronische oorlogsvoering dus, en allesbehalve een loos sensatiebericht. 'Het is een reële dreiging', zegt ir. Eric Luijff, die als *principal consultant* bij TNO strategisch onderzoek doet naar vitale infrastructuur. Hij weet van incidenten in de VS waar hackers met gemak de besturing van elektriciteitsnetwerken binnendrongen. 'Liefst 79 van de 80 pogingen waren succesvol; de tachtigste werd gestaakt omdat een groep hackers uit China langsij kwam.' En zo worden ook vitale infrastruc-

turen als de bediening van een stuwdam of kerncentrale van buitenaf bedreigd – alles wat op afstand bestuurd wordt.

Luijff en zijn team kijken naar de bescherming van vitale infrastructuur in brede zin. En daarnaast ook naar de technologische kwetsbaarheid van procescontrolesystemen. Luijff: 'Of het nu in de drinkwater- of de energiesector is of gebouwbeheersing, procesautomatisering wordt slimmer en beter. Maar procescontrolesystemen die hangen aan bedrijfsnetwerken worden daardoor ook kwetsbaarder. De man die verantwoordelijk is voor een waterzuiveringsinstallatie heeft thuis op zijn pc een virusscanner maar is niet opgeleid in informatiebeveiliging en bescherming tegen onbe-

voegde manipulatie van het drinkwatersysteem.' Omgekeerd snappen IT-mensen de procesbesturingswereld niet, stelt Luijff vast. 'Die hebben niks met kleppen en pompen. Denken dat je die wel met de hand kunt bedienen.' Die verschillende werelden aan elkaar knopen, ziet Luijff als een van zijn belangrijkste taken. 'Wij kunnen overheden en bedrijven adviseren op hoog abstract en strategisch niveau, bijvoorbeeld in het "Project Nationale Veiligheid" van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), maar wij zitten ook heel diep in specifieke infrastructuur. Als TNO brengen wij kennis in van opzij.'

BUSINESS CONTINUITY MANAGEMENT

De voorziening van drinkwater, gas, elektriciteit, telefonie, internet, tv en radio, wegen, spoorwegen, geld en betaalverkeer is voor zo'n tachtig procent in privé-handen. De beveiliging van de primaire processen is allereerst een zaak van die bedrijven zelf. Maar heel veel daarbij hangt nauw aan elkaar, benadrukt Luijff. Hij laat een schematische weergave van die wederzijdse systeemafhankelijkheid zien uit 2002: een ondoorzichtig spinnenweb. Een recente weergave van begin 2009 daarentegen is een helder

risico



CYBERCRIME

Ir. Eric Luijff werkte indertijd mee aan het rapport 'Bescherming Vitale Infrastructuur' van BZK, de eerste inhoudelijke analyse van de bescherming van de vitale infrastructuur in Nederland. In opdracht van de Nationale Infrastructuur tegen Cybercrime (NICC), waarbinnen een aantal private en publieke partijen samenwerken en Luijff ook actief is, schreef hij het boek *SCADA Good Practices for the Drinking Water Sector*. SCADA, voluit 'Supervisory Control And Data Acquisition', is de software waarmee je processen op afstand bestuurt. Luijff, trots: 'Dit boekje ligt overal, van Amerika tot Singapore. Het maakt ook andere sectoren bewuster van en weerbaarder tegen cybercrime-aanvallen. Er is zelfs een Italiaanse vertaling in de maak.' In internationaal verband is halverwege 2008 het project 'Designing an Interoperable European federated Simulation network for Critical InfraStructures' (DIESIS) gestart, een EU-project waarin TNO Europese modelleer- en simulatie-infrastructuur gaat ontwikkelen.

schema waarin energie en telecom eruit springen als de veruit belangrijkste initiators van cascade-uitval. 'We snappen het steeds beter', verklaart Luijff. 'We registreren vitale-infrastructuuruitval in een database, we brengen de gevolgen in kaart, we verzamelen berichten in de media om de gevoeligheid ervan te peilen.' Veel bedrijven hebben wel maatregelen getroffen, maar, gaat hij verder, 'toen eind 2006 de stroom uitviel rond de Elbe, en daarmee ook het mobiele telefoonnetwerk, kwamen trucks van Deutsche Telekom met reservemasten het gebied niet in doordat ze geen toegangspapieren hadden. En de autoriteiten waren mobiel niet bereikbaar. Dergelijke tweede-orde-effecten worden nauwelijks doordacht.' Ze komen vaak pas aan het licht als er iets ernstigs gebeurt. 'Een ramp op zijn tijd is input voor beleid', zoals ir. Edwin Matthijssen het uitdrukt. Als technisch consultant adviseert hij bedrijven over Business Continuity Management (BCM). 'Veel bedrijven doen wel iets aan risicomangement, maar de continuïteit van de business is maar al te vaak niet gefundeerd op beleid', stelt hij vast. 'Investeren in een methodische aanpak kost tijd en geld en verdient zich schijnbaar niet terug. Hoe groot de risico's zijn, realiseert men zich pas als er iets fout gaat.'

Voor al vitale infrastructuur kan een storing snel grote gevolgen hebben, zeker naarmate er meer gebruikers van afhankelijk zijn. In mei 2008 kampte KPN met een ongekend grote storing in het ATM-netwerk, de *backbone* van het landelijke ADSL-netwerk. Daardoor waren tienduizenden internetgebruikers twee dagen afgesloten van internet, televisie en telefoon. Zo'n netwerkstoring, de grootste ooit in Nederland, leidt niet alleen tot een miljoenschade maar ook tot reputatieschade, doordat hij breed wordt uitgemeten in de media. Ook in de energiesector of bij defensie is een goed geborgd BCM-proces cruciaal. 'Je moet een goed overzicht hebben van risico's en bewust afwegen welke risico's acceptabel zijn en welke niet, dus ook inzicht hebben in de impact bij een eventuele uitval', vertelt Matthijssen. 'De grootte van een risico is kans x impact. Een risico verlagen kan dus door kansverlagende en/of impactverlagende maatregelen.' Een voorbeeld van een impactverlagende maatregel is een *recovery*-plan dat een draaiboek bevat met wat te doen in een noodsituatie. Grootzakelijke klanten met bedrijfsnetwerken die verschillende vestigingen aan elkaar koppelen, eisen zelfs vaak zo'n plan. Maar zelfs de grootste partijen zijn zich

niet altijd bewust van risico's. 'Alle risico's wegnemen hoeft niet en kan niet, dat is technisch of financieel niet haalbaar. Als je de grootste risico's – de risico's waar je wakker van kunt liggen – maar aanpakt.' Zaak is om BCM te integreren in het reguliere proces, benadrukt Matthijssen. 'Zo houd je altijd een actueel overzicht van de meest kritieke risico's. De telecomsector is dynamisch, met steeds nieuwe technologieën en een snel veranderende markt waarin veel nieuwe diensten worden aangeboden. In zo'n wereld veranderen de risico's voortdurend.'

ONTSPORDE GOEDERENTREIN

Eind maart was het treinverkeer tussen Utrecht en Woerden een week geblokkeerd door een ontsporing van een goederentrein. Resultaat: vijf miljoen euro schade aan vijf kilometer spoor, plus de indirecte schade. 'Vijf ki-lo-me-ter', zegt TNO-onderzoeker ir. Menso Molag met nadruk. 'Die machinist merkte pas na vijf kilometer dat er wagons waren ontspoord. Dat was met ontsporingdetectie niet gebeurd. Maar dat kost zo'n tweeduizend euro per wagon. Dat vinden veel vervoerders te duur.' Molag doet bij TNO onderzoek naar veiligheids-

‘Een ramp op zijn tijd is input voor beleid’



analyse en veiligheidsmanagement voor productie, opslag en transport van gevaarlijke stoffen in relatie tot de ruimtelijke inrichting. Naast veiligheid is ook beschikbaarheid belangrijk, benadrukt hij. 'Anders hikken we straks tegen een totaalinfarct aan. Zeker als alle mensen ook nog de trein verruilen voor de auto.' Er worden ook maatregelen genomen: vanaf 2011 moeten alle chloortreinen in Europa op elke wagon ontsporingdetectie hebben. Een typisch voorbeeld van wat Molag ziet als een van de belangrijkste maatregelen om de vitale infrastructuur beter te beschermen: het veiliger en beter maken van de transportmiddelen zelf. Een ander voorbeeld daarvan is het aanbrengen van hittewerende bekleding om spoorketelwagens die brandbare gassen als LPG vervoeren, een maatregel die voor Nederlandse LPG-tankauto's al per 1 januari 2010 wordt ingevoerd. Wat chloortransport per trein betreft, nam Nederland meer fundamentele maatregelen. Het chloortransport door Nederland is helemaal beëindigd nadat Akzo met overheidssubsidie zijn chloorproductie verplaatste naar de chloorgebruikers. Zo kreeg ook DSM geld voor relocatie van zijn kunstmestfabriek van IJmuiden naar Geleen waardoor een einde komt aan het ammoniak-

transport per trein. Dit gebeurde na het regeringsstandpunt 'Ketenstudies ammoniak, chloor en LPG' uit 2004 waarvoor TNO in opdracht van vijf ministeries de risicoanalyses uitvoerde. Een derde maatregel is overstappen naar een andere vervoerswijze. 'Voor LPG-vervoer zou dat wenselijk zijn, omdat binnenvaart veiliger is dan het spoor', geeft Molag aan. 'Maar het is niet gelukt, omdat veel afnemers in Duitsland kleinere hoeveelheden nodig hebben en het vervoer per binnenschip daarvoor te grootschalig is.' LPG-vervoer per trein blijft, hoe risicovol ook, voorlopig nog een feit. Elk jaar gaan twintigduizend wagons gevuld met LPG van Rotterdam/Terneuzen naar Antwerpen en Duitsland. En daar komt dan de vierde mogelijke veiligheidsbevorderende maatregel om de hoek kijken: herroutering. 'Maar in Nederland heb je daar niet zoveel mogelijkheden voor', vertelt Molag. 'Spoorlijnen gaan hier altijd door steden. We hebben natuurlijk de Betuwelijn aangelegd, met een flinke afstand tussen spoor en bebouwing, maar die wordt niet genoeg gebruikt.' Nog niet. Juist vanwege de dichte bebouwing worden belangrijke doorgangsstations als in Utrecht, Breda en Arnhem mede door TNO grondig onderzocht op constructieve veiligheid en

toegankelijkheid voor brandbestrijding bij een onverhoopt treinongeval. 'Het is belangrijk dat een station beschikbaar blijft en niet na een ongeval maanden onbruikbaar is', verklaart Molag. Hij heeft voor het ministerie van VROM en de gemeente Rotterdam een uitgebreide interne en externe veiligheidstoets verricht naar het ontwerp van het nieuwe CS Rotterdam dat nu in aanbouw is. Molag: 'Daar worden ook veel woningen en kantoren omheen gebouwd. Het is een HSL-station. Het wordt een soort Schipholletje voor het spoorvervoer. Daardoor kan bij een explosie van een treinwagon of het vrijkomen van giftige gassen het aantal mogelijke slachtoffers aanzienlijk zijn. Net als de schade aan de bebouwing en kwetsbare infrastructuur.' Mogelijke maatregelen variëren van het aanbrengen van brandwerende wanden en alternatieve staal- en glas- of polycarbonaatconstructies in de overkapping tot het voorkomen van samenlading in de trein van brandbare vloeistoffen en LPG. Ontsporen is de belangrijkste ongevaloorzaak en daarom pleit Molag ervoor om wagons snel van ontsporingdetectie te voorzien. 'Daar heeft heel Nederland plezier van. Je hebt minder ongevallen en minder ernstige stremmingen op het spoor.'



IJKVIADUCT

Nogal wat bruggen en viaducten zijn oud of zelfs over hun verwachte levensduur heen. En dus niet meer betrouwbaar of slechts beperkt bruikbaar. Het ingieten van sensoren is een mogelijke methode, maar te duur gezien de vele kunstwerken die moeten worden doorgelicht. TNO onderzocht in het platform 'Ijkviaduct' enkele innovatieve en bestaande sensorprincipes. Zoals plaatsensoren, gekoppeld aan state-of-the-art datacommunicatie, data-interpretatie en assetmanagementtechnieken. In een demonstratieproef bleek zowel het constructieve, dynamische als het materiaalgedrag met hoge betrouwbaarheid in kaart te brengen. En daarmee de veiligheid van het infrastructurele object. De Ijkdijk is een soortgelijk project, maar dan gericht op het voorspellen van de stabiliteit van dijken.

Info: willy.peeten@tno.nl

KABELTUNNELS

Gasleidingen, telefoonkabels, waterleiding, elektriciteitskabels, glasvezel – er wordt wat van in de grond gestopt. Maar bij elke opnieuw geopende sleuf kunnen kabels worden doorgegraven of kapot gestoten. Gevolg: een compleet stadsdeel of bedrijventerrein zonder stroom, of ernstige ongevallen. Steeds vaker worden nu kabel- en leidingentunnels, een soort leidinggoten, aangelegd waarin de verschillende leidingen en kabels geordend naast elkaar liggen. Daarvoor heeft TNO een methodiek bedacht, vertelt ir. Mirjam Nelisse: 'We brengen de risico's in kaart van verschillende soorten tunnels, maar ook van de conventionele situatie.' Zoals bijvoorbeeld het effect van een lek van de ene leiding op het functioneren van de andere. 'Dat zit allemaal in een handig computertooltje.' Die kabeltunnels worden vooral aangelegd bij nieuw ontwikkelde gebieden zoals de Zuidas in Amsterdam. 'Bij dergelijke projectontwikkeling zijn een heleboel partijen betrokken die dan vanaf het begin op elkaar kunnen afstemmen wat er in moet en wanneer', wijst Nelisse als doorslaggevend voordeel aan.

DENKEN ALS EEN TERRORIST

Soortgelijke problemen doen zich voor bij spoortunnels maar ook bij wegtunnels waar het gaat om tankauto's met gevaarlijke stoffen. 'Het Nederlandse beleid is erop gericht om vervoer van gevaarlijke stoffen op hoofdwegen toe te staan en dan moet je nu eenmaal af en toe door een tunnel', schetst ir. Mirjam Nelisse. Zij doet bij TNO onderzoek naar risico's en veiligheid van vitale infrastructuur met de nadruk op tunnels – uiterst kwetsbare plekken, vooral als het gaat om brandbare en explosieve stoffen.

'De wens van Verkeer en Waterstaat is om zoveel mogelijk van de nu geldende beperkingen op te heffen. Terwijl het uiteraard heel belangrijk is dat tunnels open blijven. Een geblokkeerde tunnel is economisch zeer onverantwoord.' Voor het ministerie van Verkeer en Waterstaat inventariseerde Nelisse de mogelijk- en onmogelijkheden. 'We hebben rond de honderd maatregelen op een rij gezet, van heel futuristische tot praktische kortetermijnmaatregelen.' V&W stippelt nu aan de hand van dit rapport verder beleid uit om tunnels aan te passen.

Tunnels zijn, net als bruggen, stations en luchthavens, ook een gekend doelwit voor terroristische aanslagen. Net na de aanslagen

van 11 september 2001 in New York werden in Nederland na een dreigbrief liefst vier tunnels afgesloten, waaronder de Coentunnel en de Schiphol tunnel. Dat was voor TNO mede aanleiding om onderzoek te doen naar de bescherming van vervoersinfrastructuren tegen terroristische aanslagen. 'We hebben een specifieke vitale infrastructuur geanalyseerd in een geheim pilotproject', vertelt Nelisse. 'En we hebben een analysemethode opgesteld om te kijken welke objecten je wel en welke je niet kunt beschermen, welke soorten aanslagen mogelijk zijn bij een specifiek object en welke maatregelen je zou kunnen nemen.'

Daarvoor deed ze op locatie onderzoek. 'Je moet echt een andere bril opzetten en denken als een terrorist. En je moet beseffen dat je met een rugtas met vijftien kilo explosieven verder kunt doordringen op bijvoorbeeld een spoorwegstation dan met een auto of zelfs vrachtauto, waarin je een paar honderd kilo bommen mee kunt nemen. Een tunnel kun je ongestoord inrijden met een vrachtwagen maar een luchthaven is veel beter beveiligd, om maar twee extremen te noemen.' Met deze analysemethodiek kunnen beheerders zien waar zwakke plakken in de beveiliging zitten en de nodige maatregelen treffen. En ook hier

weer lopen die uiteen van toegankelijkheid (alle auto's door een röntgenpoort?) tot constructie: folie op glazen ruiten van vertrek- en aankomsthal om bij een bomaanslag versplintering in scherven tegen te gaan.

KETENUITVAL VOORKOMEN

Of het nu om stroomuitval, explosie, overstroming of aanslag gaat, de rode draad in de bescherming van vitale infrastructuur is een goede voorbereiding om ketenuitval te voorkomen. Luijff noemt ketenuitval de grootste bedreiging. 'Je kunt de ramp vergroten of hem beheerst houden door de dingen te snappen. Om de tweede-orde-effecten te voorkomen moet je ook de crisismanagers trainen. De private sector zou meer samen met het crisismanagement moeten oefenen. Of minstens vaker bij elkaar op bezoek gaan, elkaar leren kennen.'

Info: eric.luijff@tno.nl,
edwin.matthijssen@tno.nl,
menso.molag@tno.nl, mirjam.nelisse@tno.nl