

CIVIELE TECHNIEK

Vakblad voor grond-, weg- & waterbouwkunde en verkeerstechniek
jaargang 66 nummer 5/6 2012



Thema

Duurzaam Beheer
& Onderhoud

**BREEAM-NL Infra
Richtlijn**

CO₂-Prestatieladder

Energie uit de snelweg

RailVacuDrill

**Risicogestuurd beheer
bij Rijkswaterstaat**

**EXTRA KATERN:
Innovatieve,
duurzame materialen**

Onderbouwd risico-inzicht in kwaadwillend handelen (Deel 1)



Verbinden security aan risicogestuurd beheer en onderhoud bij RWS

Panorama Hartelkering

Rijkswaterstaat heeft al enige jaren ervaring met risicogestuurd beheer en onderhoud van haar belangrijkste objecten. Deze aanpak is onlangs uitgebreid met een security risicoanalyse-aanpak. Dit geeft mogelijkheden om de kansen op falen van een object door kwaadwillend handelen te vergelijken met andere faalkansen. Beslissingen over de security (of beveiliging) worden daarmee in samenhang genomen met andere investering- en beheerbeslissingen voor het object.

Dit eerste deel van het artikel gaat in op de risicogestuurde beheeraanpak van Rijkswaterstaat in relatie tot integrale veiligheid en security. Het tweede deel (dat verschijnt in de volgende uitgave) gaat dieper in op de security risicoanalyse-aanpak. Met security heb je te maken met een denkende mens als opponent. Hoe schat je de kansen in van kwaadwillend handelen en hoe krijg je een realistisch en onderbouwd risicobeeld?

Probabilistisch Beheer en Onderhoud (ProBO) is, binnen Rijkswaterstaat, de naam van de werkwijze van beheren en onderhouden van objecten waarmee continu aangetoond wordt dat aan de gestelde RAMS prestatie-eisen wordt voldaan. RAMS staat voor de samenhang tussen de aspecten betrouwbaarheid (reliability), beschikbaarheid (availability), onderhoudbaarheid (maintainability) en veiligheid (safety). Kenmerken van deze methode zijn dat beheer en onderhoud gebaseerd worden op risico's die het prestatieniveau van een object of systeem

beïnvloeden en dat de relatie tussen de prestatie-eisen en het prestatieniveau van het areaal transparant en traceerbaar wordt gemaakt. Deze systematische aanpak is vooral van belang voor besluitvorming rond beheersing van incidenten die nauwelijks tot niet voorkomen. Via deze methode is de beheerder blijvend 'in control' over zijn areaal, kan duidelijk worden gemaakt dat het areaal aan wet- en regelgeving voldoet en worden de kosten en opbrengsten van onderhoud geoptimaliseerd. ProBO is door Rijkswaterstaat in eerste

instantie toegepast op stormvloedkeringen, maar wordt nu ook toegepast op naar andere gebieden als bij tunnels in rijkswegen.

Aanpak van risicogestuurd beheer en onderhoud

ProBO vraagt enerzijds kwantitatieve eisen voor betrouwbaarheid en beschikbaarheid voor het object en anderzijds om een prestatieanalyse van het object. Deze prestatieanalyse is een risicoanalyse die aangeeft welke risico's het prestatieniveau van het object bedreigen, zodat



gerichte beheersmaatregelen kunnen worden genomen. De risicoanalyse bestaat uit:

- een systeem- en functiebeschrijving voor een object;
- een Failure Mode & Effect Analysis (FMEA);
- het in kaart brengen van mogelijke externe gebeurtenissen;
- het in kaart brengen van het menselijk handelen in het systeem. Dit kan menselijk falen zijn, maar ook effectief ingrijpen;
- het in kaart brengen van mogelijk afhankelijk falen;
- het in kaart brengen van mogelijk software-falen;
- het opstellen van een kwalitatief risicoanalysemodel (foutenboom);
- het kwantificeren van dit model;
- het vastleggen hiervan in een rapportage;
- het hanteren van een eenduidig revisiebeheer.

Vanuit de eerste risicoanalyse start de cyclus van continue beheersing van het prestatieniveau van het object. De noodzakelijke beheer- en onderhoudactiviteiten die uit de risicoanalyse blijken, worden gepland, uitgevoerd en gemeten. Vervolgens wordt het verschil tussen



Westerscheldetunnelbouw (Tineke Dijkstra)

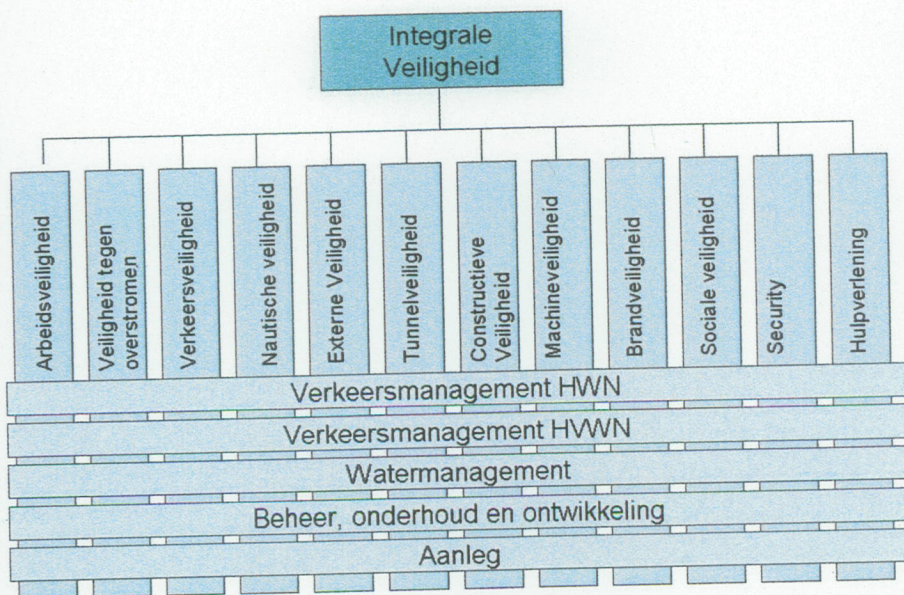
eisen en gemeten prestaties vastgesteld en vinden verbeteracties plaats. Hierna wordt deze cyclus opnieuw doorlopen.

Bepalen van extern verstorende gebeurtenissen

In eerste instantie werd ProBO toegepast op systeemeigen verstorende gebeurtenissen: uitval van elektriciteit, hydrauliek, civiel, menselijk falen. Daarna is



Brug Twentekanaal (Thomas Fasting)



de aanpak uitgebreid met externe gebeurtenissen die mogelijk tot falen leiden. Bijvoorbeeld brand, blikseminslag, wind of te veel of te weinig water. Met een korte brainstorm via de 'screening analyse externe risico's' is een gestructureerde en praktische evaluatie mogelijk op relevante externe risico's. Een extern risico dat in ieder geval bij de ProBO-analyse betrokken moet worden is security, ofwel moedwillige verstoring.

Sturen op integrale veiligheid

Binnen Rijkswaterstaat worden alle relevante veiligheidsthema's in samenhang beheerst, dit wordt integrale veiligheid genoemd.

Security wordt binnen Integrale Veiligheid gedefinieerd als de bescherming of beveiliging van inrichtingen, personen en infrastructuur tegen moedwillige verstoringen. Voor objecten die maatschappelijk vitale processen zoals het

keren en beheren van oppervlaktewater ondersteunen, is de Handreiking Risicoanalyse van het voormalige NAVI van toepassing. Voor download zie www.adviescentrumbvi.nl/domeinkennis_downloads.htm

Security risicoanalyse-aanpak Start: Karakteriseren object

Voor elke risicoanalyse geldt als eerste stap om vast te stellen wat de ongewenste topgebeurtenis is. Hierbij kan gedacht worden aan het aantal doden/gewonden, economische schade, milieuschade, financiële schade of reputatieschade. Ook voor de maatlat van iedere schadesoort moet een norm worden gevonden. Binnen de ProBO-systematiek is helder wanneer er over objectfalen kan worden gesproken (bijvoorbeeld doorbraak dam, niet kunnen sluiten van waterkering). Daarbij hoort ook een analyse van de gebruiksomstandigheden van het object door zowel geautoriseerde als ongewenste gebruikers. Tot slot wordt een beeld gevormd van de beveiligingsmaatregelen en van herstelvermogen.

Vervolg risicoanalyse: Vaststellen relevante dreigingsscenario's

Er zijn potentieel veel mogelijkheden van kwaadwillend handelen op het object. Denk alleen al aan het ongeautoriseerd verblijven, vandalisme, koperdiefstal, brandstichting, het al dan niet via digitale weg vernielen of ongeautoriseerd bedienen van het object, explosies of het onder dwang bedreigen van bedienaars van het object. Om een onderbouwd dreigingsbeeld te krijgen is het nuttig om vanuit de mogelijke opponenten te redeneren. Wie heeft mogelijk een belang bij het object en wat is dat belang? Ieder type opponent heeft een repertoire aan mogelijke daden dat zeker 80 procent van het gedrag voorspelt. Door dit mogelijke gedrag in relatie tot het object in kaart te brengen wordt een realistisch dreigingsbeeld opgebouwd waarop het securityplan kan worden gebaseerd. Een vandaal heeft andere motieven dan een crimineel, activist, gefrustreerde medewerker, verwarde persoon of terrorist. Type opponenten verschillen daarbij in soorten daden tegen het object, aanvalsplan, kennis, middelen en kracht. Vanuit ervaringen met en kennis over type opponenten kunnen type daden tegen het object als zeer waarschijnlijk tot zeer onlogisch worden gekenmerkt.



Sluis Eefde (Thomas Fasting)

De meest logische combinaties van type opponenten en type daden worden in een 'dader-daad matrix' aangekruist en daarna concreet gemaakt in scenario's. Een scenario bestaat uit de volgende componenten:

- Wie is de kwaadwillende? Kennis hierover zegt iets over motieven van de kwaadwillende, over de mogelijkheden die hij tot zijn beschikking heeft (waaronder kennis en kunnen) en modus operandi.
- Wat gaat kwaadwillende doen, wat is de aanval?
- Welk onderdeel van de asset wordt aangevallen?

Het effect geeft aan:

- Welk type effect kan ontstaan en wat is de grootte van het effect? In dit effect zijn de bestaande effect beper-

kende maatregelen (vooral redundantie en herstellvermogen) meegenomen.

- Binnen de ProBO-securityanalyse worden alleen de effecten benoemd en gemeten die de functie van het object bedreigen. De overige effecten, zoals bijvoorbeeld reputatieschade, worden bij ProBO niet in beschouwing genomen.
- Welke security-scenario's kunnen tot falen leiden?

De kans geeft de kwantitatieve kanswaarde aan. Bij het schatten van de kans is het dadertype dominant en wordt het uitgevoerd vanuit een expertbenadering waarbij argumenten rondom het scenario worden benoemd. Deze argumenten kunnen de kans vergroten, de kans reduceren of een neutrale werking hebben.

Het opgebouwde inzicht bestaat dan uit een overzicht met per regel een scenario, het effect, de kans en de kansargumenten.

Vervolgartikel

Het tweede en afsluitende deel van het artikel gaat over de wijze waarop kansen vanuit kwaadwillend handelen worden geschat, hoe deze in de kansschatting van ProBO worden geïntegreerd, wat de mogelijkheden zijn om securityrisico's te verlagen en wat de opbrengst is van het verbinden van security met risicogestuurd beheer en onderhoud op infrastructuur objecten. ■

Martijn Flinterman, senior-adviseur Veiligheidsmanagement en Security, Rijkswaterstaat Dienst Infrastructuur; Joris Hutter, consultant, Coöperatief Adviescentrum Bescherming Vitale Infrastructuur U.A.

Scenario			Effect		Kans		
Wie? (kwaadwillende)	Wat/hoe?	Asset (tegen wat gericht?)	Effect	Falen?	Kanswaarde	Argumenten waarom kwaadwill. scenario WEL uitvoert	Argumenten waarom kwaadwill. scenario NIET uitvoert

- 1 American Nuclear Society (2007), External-Events PRA methodology, La Grange Park, Illinois: American National Standard.



Stuw Amerongen (Tineke Dijkstra)

CIVIELE TECHNIEK

Vakblad voor grond-, weg- & waterbouwkunde en verkeerstechniek
jaargang 66 nummer 7 2012

Thema Geotechniek

**Techniek binnen HBO
verwatert**

**Biogrout:
stand van zaken**

**Met GIS alle gegevens
in kaart**

**Ondergronds bouwen
in de stad**

Geologische quickscan

**Prognoses van
trillingshinder**

**Historie:
Artesische putten**

**HERA: wereldprimeur
asfaltproductie**





Brug bij Zaltbommel (sloop oude brug)

Onderbouwd risico-inzicht in kwaadwillend handelen (Deel 2)

Verbinden security aan risicogestuurd beheer en onderhoud bij RWS

Rijkswaterstaat heeft al enkele jaren ervaring met risicogestuurd beheer en onderhoud van haar belangrijkste objecten. Dit wordt bij Rijkswaterstaat Probabilistisch Beheer en Onderhoud genoemd of kortweg ProBO. Deze aanpak is onlangs uitgebreid met een security-risicoanalyse-aanpak. Dit geeft mogelijkheden om de kansen op falen van object door kwaadwillend handelen te vergelijken met andere faalkansen. Beslissingen over security worden daarmee in samenhang genomen met andere investerings- en beheerbeslissingen voor het object.

Het eerste in juni 2012 gepubliceerde artikel ging in op de risicogestuurde beheeraanpak van Rijkswaterstaat met de relaties naar integrale veiligheid en security. Dit tweede en afsluitende artikel gaat dieper in op de security-

risicoanalyse-aanpak. Hoe schat je de kansen in van kwaadwillend handelen en hoe krijg je een realistisch en onderbouwd risicobeeld? Bij security heb je te maken met een denkende mens als opponent.

Security-scenario's voor beeldvorming over realistische risico's

De security-risicoanalyse-aanpak verloopt in grote lijnen volgens de aanpak van het voormalig Nationaal Adviescentrum Vitale Infrastructuur ([44](http://www.advies-</p></div><div data-bbox=)

centrumbvi.nl/domeinkennis_downloads.htm).

Er zijn potentieel veel mogelijkheden van kwaadwillend handelen op een infrastructuurobject. Denk alleen al aan het ongeautoriseerd verblijven, vandalisme, koperdiefstal, brandstichting, het al dan niet via digitale weg vernielen of ongeautoriseerd bedienen van het object, explosies of het bedreigen van bedienaars van het object. Om een onderbouwd dreigingsbeeld te krijgen is het nuttig om vanuit de mogelijke opponenten te redeneren. Wie heeft mogelijk een belang bij het object en wat is dat belang? Ieder type opponent heeft een repertoire aan mogelijke daden dat zeker 80 procent van het gedrag voorspelt. Door dit mogelijke gedrag in relatie tot het object in kaart te brengen wordt een realistisch dreigingsbeeld opgebouwd, waarop het security-plan kan worden gebaseerd.

Een vandaal heeft andere motieven dan een crimineel, activist, gefrustreerde medewerker, verwarde persoon of terrorist. Typen opponenten verschillen daarbij in soorten daden tegen het object, aanvalsplan, kennis, middelen en kracht.

Vanuit ervaringen met en kennis over type opponenten kunnen type daden tegen het object als zeer waarschijnlijk tot zeer onlogisch worden gekenmerkt.

De meest logische combinaties van typen opponenten en typen daden worden in een 'dader-daad-matrix' aangekruist en daarna concreet gemaakt in scenario's. Eerst worden door een security expert de mogelijke typen opponenten (daders) opgeschreven. Vervolgens worden de daden die zij zouden kunnen verrichten opgeschreven. Een scenario bestaat uit de volgende componenten:

- Wie is de kwaadwillende? Kennis hierover zegt iets over motieven van de kwaadwillende, over de mogelijkheden die hij tot zijn beschikking heeft (waaronder kennis en kunnen) en modus operandi;
- Wat gaat kwaadwillende doen, wat is de aanval?
- Welk asset wordt aangevallen?

Het effect geeft aan:

- Welk type effect kan ontstaan en wat is de omvang ervan? Hierin zijn de

bestaande effectbeperkende maatregelen (vooral redundantie en herstellvermogen) meegenomen.

- Binnen de ProBo-security-analyse worden alleen de type effecten benoemd en gemeten waarop ProBo meet bij het object. Dit zijn de vastgelegde eisen op betrouwbaarheid en beschikbaarheid. Overige type effecten als bijvoorbeeld financiële schade en reputatie worden in voorliggende aanpak niet in beschouwing genomen.
- Is er sprake van falen? Vanuit ProBo is de grenswaarde benoemd van een effect. Welke security-scenario's kunnen tot falen leiden?

De kans geeft de kwantitatieve kanswaarde aan. In deze beoordeling is het dadertype dominant. Het schatten van de waarschijnlijkheid is minder 'hard' en wordt uitgevoerd vanuit een expertbenadering waarbij argumenten rondom het scenario worden benoemd. Deze argumenten kunnen een kansvergroten, kansverkleinende, dan wel kansneutrale werking hebben.



ouw Sluiskiltunnel

Het opgebouwde inzicht bestaat dan uit een overzicht met per regel een scenario, het effect, de kans en de kansargumenten.

Scenario			Effect		Kans		
Wie (kwaad- willende)	Wat/hoe	Asset/ doelwit (tegen wat gericht)	Effect	Falen?	Kans-waarde	Argumenten waarom kwaadwillende scenario WEL uitvoert	Argumenten waarom kwaadwillende scenario NIET uitvoert

Schatten van het effect

Een scenario moet beeldend en goed voorstelbaar zijn. In algemene zin is daarna het schatten van het mogelijke effect van een security-scenario goed uitvoerbaar. Dit gebeurt met kennis van de objectbeheerders en vanuit de risicoanalyses van ProBo. In een workshop worden, onder leiding van een security expert, de 'zware' scenario's besproken en objectbeheerders geven aan of deze scenario's vanuit daderperspectief mogelijk zijn en hoe zij met deze scenario's zullen omgaan om (vervolg) schade zoveel mogelijk te beperken. Vanuit deze workshop wordt het helder of een scenario ook tot gedefinieerd objectfalen leidt.

Een uniform afwegingskader op alleen het meten van objectfalen heeft ook een beperking. Kleinere security-dreigingen die niet tot gedefinieerd objectfalen leiden, kunnen dusdanige effecten (milieu, politiek, gezondheid, reputatie) hebben, dat deze vanuit een andere optiek beheersbaar moeten worden gemaakt. Dit is te ondervangen door vast te leggen welke belangen en belanghebbenden er zijn en hoe ze worden behartigd en bediend.

Schatten van de kans

Het schatten van de kans is veel lastiger. Zoveel als mogelijk worden daarbij incidentcijfers gebruikt. Voor daders als vandalen, stenengooiers vanaf viaducten en metaaldieven zijn incidentcijfers beschikbaar. Voor andere scenario's, denk aan internationaal terrorisme, zijn weinig cijfers beschikbaar, omdat deze nu eenmaal nauwelijks voorkomen.

De analyse wordt dan aangevuld met expertmeningen. Bij deze analyse is niet zozeer kennis van het object, maar kennis van dreigingen in Nederland van betekenis. Na een eerste basis kansschatting vanuit de cijfers worden door workshopdeelnemers zoveel mogelijk factoren genoemd rondom het scenario. Daarna is er discussie of een

factor kansvergroterend, kansverkleinend of kansneutraal is.

Factoren die de kans beïnvloeden

Het schatten van de kans is per dadergroep verschillend. Relevante factoren zijn:

- Waar bevindt het dadertype zich? In de buurt van een woonwijk zijn meer potentiële vandalen. Een object dat daar enkele kilometers van verwijderd is, loopt een veel kleinere kans om te worden getroffen door vandalisme.
- Hoe vaak slaat een dergelijk dadertype toe?
- Wat zijn alternatieve doelen voor de dader?
- Wat maakt een object aantrekkelijk voor de dader?
- Wat voor kennis is nodig en hoe toegankelijk is deze voor de opponent?
- Wat voor hulpmiddelen zijn nodig en hoe moeilijk zijn deze verkrijgbaar?
- Wat beïnvloedt de doelwitselectie?
- Wat zijn, voorafgaand aan de daad, de mogelijkheden tot verkenning van het object?
- Wat zijn de toegangsmogelijkheden voor een dader?
- Wat zijn de mogelijkheden voor een dader, nadat hij de daad heeft gepleegd? (vlucht, verhandelbaarheid van opbrengst, media-aandacht, et cetera).

Bij de kansinschatting is het nuttig om de fasering van een daad in betrekking te nemen:

- Een dader zal eerst het object als doelwit moeten kiezen. Hoe groot is de kans dat een object wordt gekozen, als er voor de dader aantrekkelijkere doelwitten bestaan?
- Na de keuze van het doelwit zal verkenning plaatsvinden. Een terrorist zal uitgebreid verkennen, een crimineel zal mogelijk direct vanuit verkenning zijn daad uitvoeren. Als het de dader moeilijk wordt gemaakt om te verkennen (bijvoorbeeld door hem uit de anonimiteit te halen, kennisverga-

ring moeilijk te maken) bestaat de kans dat de opponent, afhankelijk van dadertype, afziet van de daad (ontmoediging).

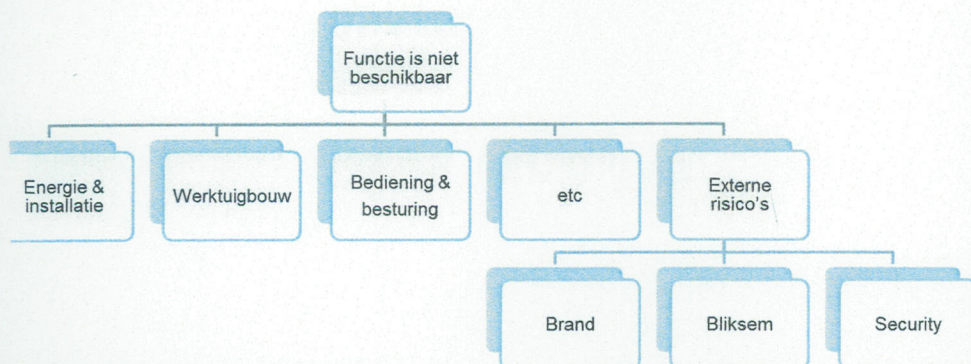
- Na besluit tot uitvoering van de daad moet zo nodig toegang worden verschaft en wordt de daad uitgevoerd. Hoe groot is de kans dat de dader succesvol zal zijn?

Deze methodiek van kansinschatting is getest op een object van Rijkswaterstaat. Daarbij is de volgende redeneerlijn gevolgd. Eerst is geschat hoe groot de kans is dat vanuit internationaal terrorisme een aanslag in Nederland plaatsvindt. Daarna is de kans geschat op een aanslag op infrastructuur in plaats van op een ander doelwit. Tot slot is een basiskans geschat op een doelwit in de waterhuishouding in Nederland. Daarbinnen zijn de diverse terroristische opties ten opzichte van elkaar geschat.

De kansschattingen op een incident door een andere opponent, bijvoorbeeld een gefrustreerde medewerker, een crimineel of vandaal, zijn op overeenkomstige wijze opgebouwd. Eerst zoveel mogelijk vanuit cijfers en daarna aangevuld met specifiek kansvergroterende of kansverkleinende argumenten.

Opnemen van security kansgetal in ProBO-foutenboom

Het geheel is een security risicobeeld met scenario's, effecten en kansen. Geïdentificeerde dreigingen die niet raken aan de Ongewenste Topgebeurtenis, zoals gebruikt binnen ProBO, worden voor besluitvorming overgedragen aan de objectbeheerder. Het kansgetal moet daarbij dezelfde 'vorm' hebben als de overige kansgetallen die ProBO gebruikt. Op die wijze kan ook een security incident als (basis)gebeurtenis (event) in de foutenboom worden opgenomen. Bij Rijkswaterstaat bekijkt de faalkansanalist waar het security-incident in de foutenboom thuishoort.



In veel situaties kan security als onderdeel van de externe risico's worden gemodelleerd. Daarbij grijpt security direct in op de niet-beschikbaarheid van het object.



Het is ook mogelijk om een security-gebeurtenis aan een specifieke component te koppelen. Een denkbeeldig object heeft een kwetsbare kabel die zowel kan uitvallen door een te hoog voertuig als door een vandaal, een koperdief of een terrorist. In dit voorbeeld is het rekenkundig en communicatief sterker om de verstorende gebeurtenissen direct aan deze component te verbinden. Als voor deze kwetsbare kabel redundantie aanwezig is in het systeem, bijvoorbeeld in de vorm van een back-up kabel, dan móet zelfs gemodelleerd worden zoals in deze laatste figuur.

Beperken van de security-risico's

Na het opbouwen van een risicobeeld kunnen mogelijkheden worden bedacht om te grote risico's van scenario's te verkleinen. Risicobeperking kan onder andere plaatsvinden op de volgende manieren:

- Vergroten van redundantie. Met deze strategie wordt de slagingskans van de kwaadwillende verlaagd;
- Verkleinen van hersteltijd. Met deze strategie worden de (economische) gevolgen verlaagd;

- Verbeteren van de beveiliging. Met deze strategie wordt de slagingskans van de kwaadwillende verlaagd.

Bij het verbeteren van de beveiliging kan gedacht worden aan:

Van de radar blijven

In generieke zin zal het niet lukken om het object 'onzichtbaar' te maken voor mogelijke opponenten. Wat wel kan is voorkomen dat over kwetsbaarheden wordt gepubliceerd, waardoor ze minder snel als doelwit zullen worden uitgekozen.

Dader ontmoedigen

Veel maatregelen hebben als doel om de opponent te ontmoedigen. Het kan hem vooral in de verkenning lastig worden gemaakt door bijvoorbeeld:

- hem uit de anonimiteit te halen (detecteren, aanspreken, traceerbaar maken, verlichten);
- de benodigde kennis vertrouwelijk te houden;
- de toegang voor de opponent te bemoeilijken;



- een overdaad aan beveiligingsmaatregelen te tonen (perceptie van pakkans).

Dader stoppen

Hiervoor dient de toegang/aanval te worden gesignaleerd en moet snel een interventie worden opgeroepen die bij machte is om de dader tegen te houden. Na signalering moeten barrières hem afremmen, om de interventie een kans te geven om op tijd bij het doelwit te komen.

Daad stoppen

Als de daad kan worden gestopt heeft deze geen effect meer op het object (bijvoorbeeld een muur om het doelwit die deze tegen een kogel beschermt). In algemene zin worden de kosten van de beschreven typen maatregelen steeds

hoger. Het eenvoudigste is om van de radar te blijven, het stoppen van de daad is meestal de meest kostbare maatregel. Bij de verschillende scenario's kan worden aangegeven wat het nieuwe risico zal zijn (effect, kans) bij het gebruik van additionele maatregelen.

Resultaten van aanpak

De aanpak om security-risicoanalyse te verbinden met de aanpak op risicogestuurd beheer en onderhoud, heeft voor Rijkswaterstaat de volgende resultaten:

- Via security-scenario's wordt helder en begrijpelijk gemaakt welke kwaadwillende handelingen tot objectfalen kunnen leiden.
- Er is een onderbouwde argumentatie op de waarschijnlijkheid van deze scenario's.

- Er is een uniform afwegingskader op risico's die tot objectfalen leiden. Hierdoor wordt het ook eenvoudiger om beslissingen te nemen. Wat is effectiever: extra schilderbeurt ter voorkoming van corrosie of een extra hekwerk ter voorkoming van een security incident?
- Realistisch inzicht in waar het om gaat: geen dubbeltjes beveiligen met euro's. ■

Martijn Flinterman, senior-adviseur Veiligheidsmanagement en Security, Rijkswaterstaat Dienst Infrastructuur; Joris Hutter, consultant, Coöperatief Adviescentrum Bescherming Vitale Infrastructuur U.A.

Foto's: Beeldarchief Rijkswaterstaat

NIEUWS UIT DE MARKT



Samenwerking dynamisch verkeersmanagement en parkeren

Vialis en Nedap gaan samenwerken om de verkeersdoorstroming in Nederlandse steden te verbeteren en het parkeren te vergemakkelijken. Vialis, een dochter van VolkerWessels, koppelt haar ViValdi-systeem voor dynamisch verkeersmanagement met het SENSIT-systeem voor draadloze parkeerdetectie van Nedap. De samenwerking start per direct. Vialis helpt steden op het gebied van dynamisch verkeersmanagement. Een groot

aantal gemeenten in Nederland maakt gebruik van ViValdi om verkeersstromen te optimaliseren. Het systeem staat in verbinding met verkeersgerelateerde technologieën, zoals verkeersregelininstallaties (VRI) en bewegwijzeringsystemen. Nedap levert draadloze sensoren SENSIT die de parkeerbezetting in kaart brengt. De samenwerking tussen Vialis en Nedap moet ervoor zorgen dat automobilisten naar vrije parkeerplekken in de stad worden verwezen. Dit vermindert het zoekverkeer en verbetert de benutting van de bestaande parkeercapaciteit. Het systeem dat dynamisch verkeersmanagement en parkeren integreert wordt nog niet in Nederland gebruikt.

Eerste Hillblocks op dijk bij Stavenisse

Bij het Zeeuwse Stavenisse wordt voor het eerst de innovatieve dijksteen Hillblock toegepast. Rijkswaterstaat en het waterschap Scheldestromen doen er een proef-

project met het duurzaam bekleden van dijken. Het proefvak met Hillblocks meet 4.000 vierkante meter. Het Hillblock is een betonnen taludblok en biedt grote milieutechnische voordelen. Voor de productie is 30 procent minder beton nodig dan in conventionele dijkstenen. Dat beton is ook milieuvriendelijker van samenstelling. Het lichtere gewicht, een slimmer productieproces en efficiënter transport zorgen voor de nodige CO₂-vermindering. Door de bijzondere vormgeving van het Hillblock ontstaan bovendien holle ruimten die leefruimte bieden aan flora en fauna, zowel boven als onder water. Proeven hebben aangetoond dat de nieuwe dijksteen de oploop van de golven tegen de dijk met 30 procent of meer doet afnemen. Het Hillblock is, met andere woorden, een golfremmer. Dit in tegenstelling tot conventionele dijkbekleding. Het werk in de Stavenissepolder wordt uitgevoerd door de aannemerscombinatie AVK/De Klerk en is dit najaar klaar.
www.hillblock.com

Bezoek Civiele Techniek op de Infra Relatiedagen in Gorinchem op 30 oktober tot en met 1 november: Stand nr 109