Auteurs: Bart Gijsen, Sterre den Breeijen, Robert Seepers, Ruggero Montalto, en Bram Poppink zijn allen werkzaam bij de unit ICT van TNO. Jeroen van der Ham is werkzaam bij het NCSC en de Design & Analysis of Communication Systems (DACS) groep van de universiteit Twente. Samen werkten ze in 2020 aan een verkennend onderzoek naar de status van herstelvermogen bij Nederlandse organisaties. Voor vragen en opmerkingen, mail naar bram.poppink@tno.nl.

ICT herstelvermogen: de stand van zaken

Herstelvermogen is het vermogen van een organisatie om haar bedrijfsvoering snel en goed weer op te pakken na een cyberaanval of niet-intentioneel ICT-incident. Uit inventarisatie onder Nederlandse organisaties blijkt dat herstelvermogen een bekend en ingebed concept is. Er blijkt ook ruimte voor verbetering van herstelvermogen te zijn, vooral ten aanzien van het periodiek bijstellen van incidentscenario's, oefenen van risicovollere scenario's en het inrichten van collectief herstelvermogen.

ICT-voorzieningen worden gebruikt om de uitvoering van bedrijfsprocessen mogelijk te maken. De toename van het gebruik van IT in de afgelopen decennia heeft ertoe geleid dat zeer veel organisaties afhankelijk zijn geworden van correct functionerende ICT. Zonder correct functionerende ICT kunnen bepaalde bedrijfsprocessen, of zelfs gehele organisatieketens, verstoord raken. Het voorkomen van verstoringen – doelbewust als gevolg van een cyberaanval of incidenteel – met betrekking tot de beschikbaarheid, vertrouwelijkheid en integriteit van ICT is daarom belangrijk. In het verleden is veel aandacht besteed aan het voorkomen van dergelijke verstoringen door het treffen van preventieve maatregelen. Dit levert echter nooit een garantie op correct functionerende ICT aangezien preventieve maatregelen nooit volledig dekkend zijn. In het geval van een verstoring zal de ICT goed hersteld moeten worden. Dit vermogen om ICT te herstellen is, in vergelijking met preventieve of responsieve maatregelen, onderbelicht.

In dit kader heeft TNO, in samenwerking met het NCSC, verkennend onderzoek gedaan naar de huidige stand van zaken op het gebied van herstelvermogen. Het doel van dit onderzoek is om zicht te krijgen op de huidige stand-van-zaken op het gebied van herstelvermogen binnen Nederlandse organisaties en mogelijke aanknopingspunten voor verbetering te identificeren. Als onderdeel van dit onderzoek is er eerst bepaald wat er precies bedoeld wordt met herstelvermogen (in vergelijking met o.a. cyberweerbaarheid) en wat typerend zou zijn aan adequaat ingericht herstelvermogen. Deze beelden zijn vervolgens getoetst aan de huidige herstelinrichting van een negental organisaties door middel van kwalitatief onderzoek (op basis van interviews). In de volgende paragraaf gaan we eerst in op de definitie van herstelvermogen. Vervolgens bespreken we wat er van belang is voor een adequate inrichting van herstelvermogen. In de daaropvolgende paragraaf lichten we toe welk type organisaties zijn geïnterviewd, waarna we de bevindingen op basis van deze interviews bespreken. Aansluitend gaan we wat dieper in op de aanknopingspunten voor verbetering, naar aanleiding van deze bevindingen. We sluiten af met een conclusie en een vooruitblik op mogelijk vervolgonderzoek.

Wat is herstelvermogen?

Het herstellen van verstoorde ICT is een concept dat terug te vinden is in onder andere cyberweerbaarheid en business continuity management. Laatstgenoemde onderwerpen zijn echter een stuk breder dan het herstellen van ICT en omvatten typisch ook het opstellen van preventieve en repressieve maatregelen. Aangezien het primaire doel van dit onderzoek zich beperkt tot het herstellen van verstoorde ICT wordt de scope van herstelvermogen een stuk enger gedefinieerd. Specifiek wordt binnen dit onderzoek de volgende definitie gehanteerd:

Herstelvermogen, is de mate waarin een organisatie efficiënt en effectief in staat is om functionaliteit, die voorzien wordt door ICT, weer beschikbaar te maken.

Deze definitie verdient enige onderbouwing. Om te beginnen met *functionaliteit, die voorzien wordt door ICT:* met herstel wordt uiteindelijk beoogd om bepaalde functionaliteiten te herstellen. We beperken ons, in het kader van dit onderzoek, daarbij tot dergelijke functionaliteiten die geleverd worden door ICT. Denk hierbij aan diensten die een organisatie kan leveren waarbij er een directe relatie is tussen ICT en dienst (e.g. het leveren van software diensten), maar ook aan bedrijfsprocessen die gebruik maken van informatiesystemen (e.g. administratie).

Figuur 1: Fases van herstelvermogen.

Het herstellen van ICT functionaliteit dient *efficiënt en effectief* te gebeuren. De middelen die ingezet worden voor herstel dienen op te wegen tegen de negatieve impact van een incident. Herstel dient doeltreffend en binnen passende tijd te worden uitgevoerd. Zoals later in dit artikel wordt toegelicht is een onderdeel hiervan de mate waarin een organisatie baat heeft bij 'acuut herstel' of 'duurzaam herstel'.

Een *organisatie* is afhankelijk van bovenstaande functionaliteiten (voorzien door ICT) om diensten te kunnen leveren. Elke organisatie is eindverantwoordelijk voor de door haar geleverde diensten en de daarvoor gebruikte functionaliteit en daarbij het herstel van deze functionaliteit. Hiervoor is in de definitie expliciet de term 'organisatie' opgenomen, refererend aan de organisatie die de diensten levert.

Wat is van belang voor het adequaat inrichten van herstelvermogen?

Goed herstelvermogen kenmerkt zich door een set activiteiten die voor, tijdens en na een incident uitgevoerd moeten worden. Er worden hierbij typisch drie fases onderscheiden zoals ook weergegeven in figuur 1.

In al deze fases vindt er een samenspel plaats tussen techniek,

processen en mensen. In de techniek zijn oplossingen te vinden om ICT-functionaliteit te herstellen, bijvoorbeeld door het aanbrengen van redundantie. Het daadwerkelijke herstel (e.g. het uitvoeren van technische maatregelen) moet worden uitgevoerd volgens bepaalde processen en procedures. Een van deze processen is hierbij het besluiten welke functionaliteit er wanneer en hoe hersteld moet worden, veelal belegd bij een crisisteam binnen een organisatie. Deze processen worden uiteindelijk uitgevoerd door mensen. Neem bijvoorbeeld het herstellen van gecompromitteerde data, die veroorzaakt zou kunnen zijn door een ransomware aanval. Om deze data op een effectieve en efficiënte manier te kunnen herstellen moet er o.a.:

- *Voorafgaand* aan een dergelijk incident, een data back-up infrastructuur worden ingericht die het mogelijk maakt om data op een later tijdsstip te herstellen. Als onderdeel van deze voorbereiding moeten er ook processen en procedures worden opgesteld om dit herstel uit te kunnen voeren;
- *Tijdens* een incident zal er een inventarisatie gemaakt moeten worden van de data die getroffen is door de aanval. Op basis van de impact die de aanval heeft op de organisatie zal er een besluit moeten worden genomen (in teamverband) over hoe de getroffen functionaliteit en data het beste hersteld kan worden. Hierbij worden de juiste processen en procedures bepaald en gevolgd (bijv. een draaiboek dat beschrijft hoe de data uit technisch perspectief moet worden hersteld). Vaak is de uitvoer van het herstel een iteratief proces;
- *Na* het herstel moet de organisatie van de gelegenheid gebruikmaken om te evalueren hoe het herstel is verlopen. Deze evaluatie wordt vervolgens gebruikt om de getroffen maatregelen en gevolgde herstelprocessen, waar mogelijk, aan te scherpen.

In deze fases – voorbereiding, uitvoering en leren van uitvoering – zijn een aantal specifieke activiteiten te benoemen die uitgevoerd kunnen worden om een verbeterd herstelvermogen te bereiken. In de komende paragrafen worden deze activiteiten per fase kort toegelicht. Vervolgens worden er nog een aantal aspecten benoemd die belangrijk zijn voor herstelvermogen, maar van toepassing zijn op al deze fases.

Voorbereiden op herstel

Het voorbereiden op herstel is cruciaal voor efficiënt en effectief herstel ten tijde van een incident. Door zoveel mogelijk herstelmaatregelen in de techniek en processen kan er ten tijde van een incident snel geschakeld worden. In de voorbereidende stap kan bijvoorbeeld een inventarisatie gemaakt worden van mogelijke incidenten, kan techniek worden ingericht die bij het herstel gebruikt kunnen worden (e.g. back-ups, monitoring system, etc.) en kan een herstelplan geschreven worden om uit te voeren ten tijde van een specifiek incident. Ook is het mogelijk om samenwerking op te zetten met ketenpartners en eventuele gezamenlijke beschermingstechnieken voor het tijdelijk uitwijken van ICT-functionaliteit.

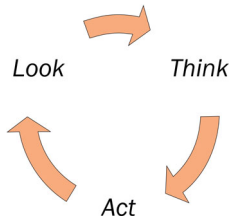
Herstel-in-uitvoering

De herstel-in-uitvoering fase begint zodra er vastgesteld wordt dat er een incident gaande is. Bijvoorbeeld wanneer een monitoringsysteem een afwijking detecteert, of een klant meldt dat een online service niet langer beschikbaar is. Afhankelijk van het type incident en de impact op de bedrijfsvoering zullen bepaalde keuzes gemaakt moeten worden. Kan dit zelf opgelost worden, of is een leverancier verantwoordelijk? Kan de 'pre-disruption state' snel hersteld worden, of is het zinvoller om eerst alternatieve functionaliteit in te zetten in plaats van de verstoorde functionaliteit? Deze keuzen tijdens uitvoering van herstel hangen sterk af van de organisatorische drijfveren, het type functionaliteit die verstoord is, en welke oorzaak hieraan ten grondslag ligt.

De fase 'herstel-in-uitvoering' vormt hiermee de kern van het herstelvermogen. Het herstel-in-uitvoering is daarbij een iteratief proces waarbij er stapsgewijs wordt toegewerkt naar een oplossing. Een representatie van dit proces is geïllustreerd in figuur 2:

- **Look:** Observeer en onderzoek wat er aan de hand is. Onder deze deelfase vallen onder andere het (steeds beter) zicht krijgen op het incident en de impact die dit heeft op de organisatie;
- **Think:** Bepaal mogelijke acties om het herstel uit te voeren. Er zal hierbij gezocht moeten worden naar de balans tussen de snelheid en duurzaamheid van herstel. Dat wil zeggen, snelle oplossingen zijn er typisch op gericht om de functionaliteit zo snel mogelijk weer aan te bieden, maar zullen zich slechts in beperkte mate richten op het voorkomen van vervolgincidenten. Langzamere (maar duurzamere) oplossingen richten zich erop om de functionaliteit in het vervolg ook beter te kunnen garanderen, maar vereisen doorgaans enige tijd om geïmplementeerd te worden. Naast het bepalen van specifieke herstelacties wordt er binnen deze fase ook gecontroleerd of het

incident nog voldoende onder controle is, of dat er moet worden geëscaleerd.
- **Act:** Voer de herstelacties uit. Indien de functionaliteit hersteld is, zal er hierbij voor enige tijd een 'verhoogde dijkbewaking' plaatsvinden om zeker te zijn dat het herstel goed is uitgevoerd.



Figuur 2 - Fases tijdens de uitvoer van herstel, een iteratief proces.

Leren van uitvoering

Als een incident is verholpen en de functionaliteit is hersteld volgt een evaluatie om verbeteringen te identificeren en waar nodig te implementeren. Belangrijk voor deze evaluatie is dat alle voorgaande processtappen goed zijn gedocumenteerd en vastgelegd. Zowel de aanleiding naar het incident, het incident zelf als de uitvoering van herstel dienen geëvalueerd te worden. Eventuele tekortkomingen die het incident teweeg hebben gebracht, of het herstel hebben belemmerd, dienen aangescherpt te worden, mits de kosten op wegen tegen de baten. Bijvoorbeeld een aanpassing in de herstelprocessen of getroffen technische maatregelen.

Overige belangrijke aspecten

Er zijn een aantal aspecten belangrijk voor de inrichting van herstelvermogen welke van toepassing zijn op het algemeen herstelvermogen. Dit zijn Training en oefening, het afstemmen met ketenpartners en collectief herstelvermogen.

Zoals eerder beschreven is herstelvermogen een samenspel tussen techniek, processen en mensen. Training is een middel dat gebruikt kan worden om ervoor te zorgen dat de medewerkers de juiste kennis hebben en weten wat er van hen verwacht wordt. Denk hierbij aan kennis op zowel het gebied van expertise (e.g. crisismanagement of technisch incidentbeheer) als herstelprocessen. Het oefenen van incidenten is daarbij een belangrijk aspect om te toetsen of deze kennis beheerst wordt. Daarbij kunnen oefeningen gebruikt worden om ervaring op te doen met de technische herstelmaatregelen en herstelprocessen, en om eventuele tekortkomingen hierin te identificeren nog vóór een incident plaatsvindt.

Een ander belangrijk aspect zijn de relaties met andere organisaties. Ondanks dat herstelvermogen primair betrekking heeft op het herstel van de functionaliteit binnen de eigen organisatie, is het afstemmen met ketenpartners een onderdeel van het herstel. Bijvoorbeeld wanneer functionaliteiten afhangen van (ICT) diensten die geleverd worden door een externe leverancier. Het afstemmen met dergelijke ketenpartners kan vooraf worden geformaliseerd in contracten en/of SLAs en gedurende en na een incident zal er tussen ketenpartners moeten worden afgestemd.

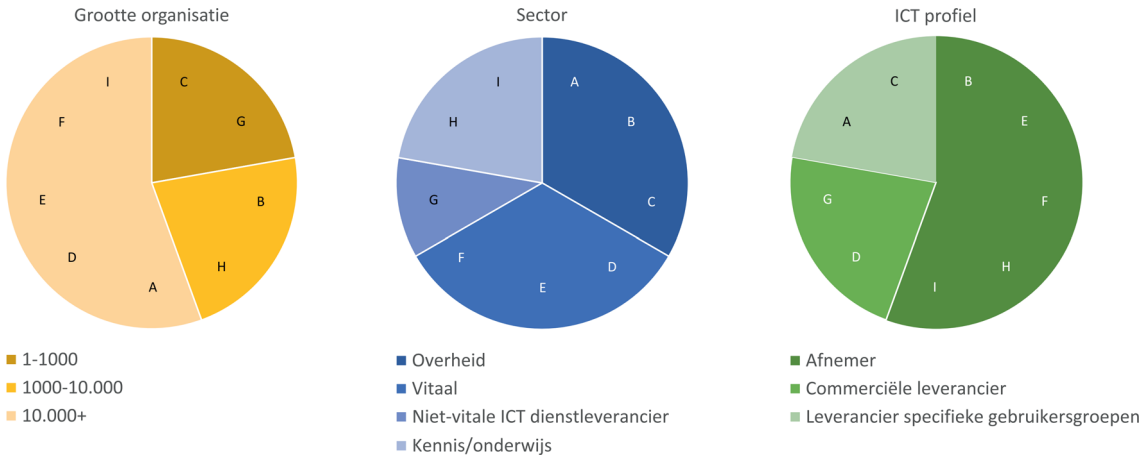
Ten slotte kan een organisatie ook samenwerken met andere organisaties welke niet directe leveranciers of afnemers zijn, bijvoorbeeld soortgelijke organisaties in dezelfde sector. Dit collectief herstelvermogen is de mate waarin organisaties gezamenlijk optrekken om hun herstelvermogen (beter) in te richten. De twee geïdentificeerde manieren waarop collectief herstelvermogen bedreven kan worden zijn: collectief leervermogen, bijv. informatiedeling tussen sectorpartners over bepaalde incidenten en advies richting de inrichting van het herstelproces); en collectief herstel, bijvoorbeeld de inrichting van sector-gezamenlijke uitwijkfaciliteiten.

Wat doen Nederlandse organisaties op het gebied van herstelvermogen?

Om inzicht te krijgen in de stand van zaken op het gebied van herstelvermogen zijn interviews afgenomen bij negen verschillende organisaties. Deze organisaties blijven anoniem en de bevindingen van de interviews zijn zo goed als mogelijk onherleidbaar naar specifieke organisaties en personen opgeschreven. In de komende paragrafen wordt er eerst een beknopt, geanonimiseerd overzicht gegeven van de (types) organisaties die bij dit onderzoek betrokken zijn geweest, waarna er wat dieper gekeken wordt naar de meest belangrijke bevindingen van dit onderzoek.

Selectie interviewkandidaten

Bij veel organisaties is herstelvermogen belegd bij meerdere personen met verschillende taken. Vanwege het verkennende karakter van dit onderzoek is er voor gekozen om inzichten te inventariseren bij personen met verschillende rollen en verantwoordelijkheden bij de organisaties, waaronder business continuity managers en information security officers. De negen betrokken organisaties zijn actief in verschillende sectoren: overheid, vitale dienstverlening, niet-vitale ICT-dienstverlening, en kennis/onderwijs. Vijf van de negen organisaties kunnen gekenmerkt worden als primair afnemer van ICT-diensten, twee organisaties worden gekenmerkt als commerciële ICT-dienstleverancier, en twee organi-



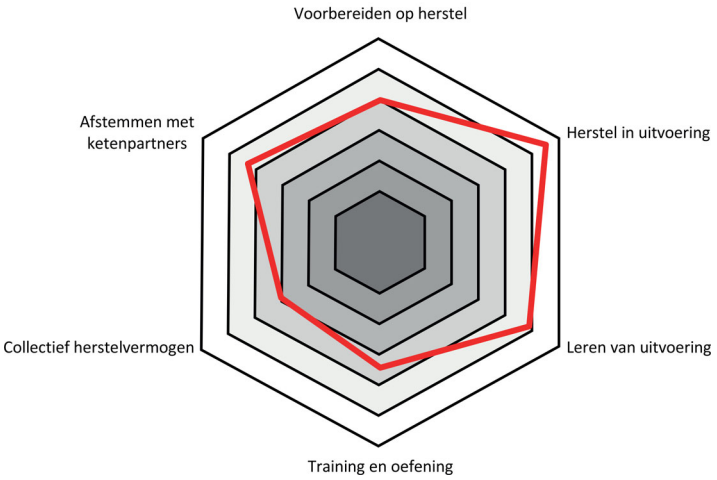
Figuur 3 - Categorisering van de geïnterviewde organisaties.

saties worden gekenmerkt als leverancier aan specifieke gebruikersgroepen (b.v. aan Rijksoverheid organisaties). De grootte van de organisaties varieert in omvang van minder dan 1.000 tot meer dan 10.000 medewerkers.

In figuur 3 staat de categorisering van de geïnterviewde organisaties grafisch weergegeven. Individuele organisaties worden hier aangegeven met de letters 'A' tot en met 'I'.

Status-quo herstelvermogen

Na een analyse van alle interviews is geconcludeerd dat herstelvermogen bij alle geïnterviewde organisaties is ingeregeld en al voor langere tijd wordt opgepakt in de vorm van een samenvoeging / integratie van business continuity management en cyber security. Het valt op dat de awareness en het commitment bij het management een belangrijke indicator voor goed ingericht herstelvermogen is. De organisaties waarbij het herstelvermogen slechts beperkt tot recht kwam gaven allen aan dat herstelvermogen niet door de gehele organisatie leeft. In deze gevallen wordt herstelvermogen vaak gezien als een `feestje voor de ICT afdeling', terwijl herstel meer elementen raakt dan puur ICT. Door het gebrek aan awareness en commitment bij het hogere management zijn er bij deze organisaties onvoldoende mensen en middelen beschikbaar om herstelvermogen in de breedte op te kunnen pakken.
Een belangrijke drijfveer voor het management om zich te committeren aan herstelvermogen kan gekoppeld worden aan de mate waarin ICT van direct belang is voor de business continuity, maar ook specifieke richtlijnen vanuit wet- en regelgeving. Het herstelvermogen van een organisatie hangt hierbij ook sterk samen met het ICT-profiel van de organisatie. Vooral bij organisaties waarbij het primaire bedrijfsbelang sterk afhangt van ICT-continuïteit worden vergaande herstelmaatregelen getroffen.
Daarbij wordt ook opgemerkt dat de awareness bij het management (tijdelijk) kan opleven door recente (grote) incidenten bij eigen of vergelijkbare organisaties. De ransomware aanval op Universiteit Maastricht leidde tot vragen bij het management van veel van de geïnterviewde organisaties: `kan dit ook bij ons gebeuren?'. Dergelijke situaties kwamen in de breedte van de geïnterviewde organisaties voor, ongeacht hoe goed het herstelvermogen is ingericht.
De algemene bevindingen die voortkomen uit de interviews zijn geïllustreerd in figuur 4. Dit radardiagram geeft weer in hoeverre het herstelvermogen van de organisaties zich gemiddeld gezien verhoudt tot de belangrijkste aspecten die eerder in dit artikel zijn beschreven. Daarmee geeft deze grafiek een eerste beeld bij de huidige stand van zaken op het gebied van herstelvermogen binnen Nederlandse organisaties. Wat opvalt uit deze grafiek is dat de gemiddelde organisatie goed scoort op het aspect `herstel in uitvoering' . Voor 'voorbereiden op herstel', `collectief herstelvermogen' en `training en oefening' lijkt er nog de meeste ruimte voor verbetering te zijn.



Figuur 4 - Algemene bevindingen herstelvermogen. Hoe verder van het centrum verwijdert des te beter dit aspect er over het algemeen voor staat bij de geïnterviewde organisaties. Deze beoordeling is gebaseerd op een kwalitatieve analyse.

Een geconstateerde tekortkoming bij het voorbereiden op herstel is dat incidentscenario's slechts in beperkte mate periodiek worden bijgesteld. De meeste organisaties herzien deze scenario's pas zodra er een (grootschalig) incident plaatsvindt in de eigen organisatie of daarbuiten, zoals de Citrix-crisis of de ransomware aanval bij de Universiteit van Maastricht. Meerdere organisaties komen er bij deze incident-gedreven heroverweging achter dat sommige scenario's achterhaald zijn. Veelvoorkomende reden voor deze incident-gedreven aanpak is een gebrek aan toegewezen tijd en middelen om deze activiteit periodiek uit te voeren.
Op het gebied van collectief herstelvermogen komt er uit de interviews naar voren dat er vooral behoefte is, maar nog een beperkte implementatie. Vooral bij de vitale infrastructuur organisaties wordt hier al wel over nagedacht, bijvoorbeeld over de inrichting van gezamenlijke ICT-voorzieningen voor sectorpartners in geval van calamiteiten. Door een gebrek aan directe noodzaak en best-practices, maar ook vanwege juridische complicaties wordt hier nog geen concrete invulling aan gegeven. Daarnaast geven meerdere organisaties aan dat er behoefte is om van elkaar te leren op het gebied van herstelvermogen.

Alle organisaties geven aan dat herstel met enige regelmaat wordt beoefend. Er blijkt hier echter wel een terughoudendheid om risicovolle technische oefeningen uit te voeren, vanwege de lastig te voorspellen impact op de bedrijfsuitvoering. Hoewel eenvoudige technische maatregelen wel worden geoefend worden complexere technische herstelvoorzieningen nauwelijks getest.

Aanknopingspunten voor verbetering en vervolg

Aanvullend op de verbeteringen die organisaties voor hun eigen herstelvermogen doorvoeren, kunnen collectieve verbeteracties meerwaarde bieden. Het is bijvoorbeeld aannemelijk dat een organisatie minder aanleiding zal voelen om periodiek haar risico- en dreigingsprofielen aan te passen, indien dit gedaan wordt op basis van slechts de ervaringen vanuit die ene organisatie zelf. Indien de organisatie meer zicht krijgt op relevante ervaringen en getroffen maatregelen bij andere organisaties, dan ontstaat een meer accuraat dreigingsbeeld dat aanleiding kan zijn voor frequentere aanpassingen van het risico- en dreigingsprofiel. Het Cybersecuritybeeld Nederland (opgesteld door de NCTV in samenwerking met het NCSC) is een voorbeeld dat hieraan bijdraagt. Vooralsnog blijft het echter een uitdaging om een uniformere manier te vinden om relevante dreigingsinformatie op een vertrouwde wijze beschikbaar te maken voor andere organisaties, die voldoende gedetailleerd is om concreet toegepast te kunnen worden.

Het oefenen van realistische, grootschalige incidenten blijkt door individuele organisaties te worden ingeschat als te risicovol, hoewel het herstelvermogen zou kunnen verbeteren. Ook het concretiseren van collectief herstelvermogen zou volgens sommige geïnterviewde organisaties verbeterd kunnen worden. Wellicht dat het gebruik van collectieve (grootschalige) ICT testfaciliteiten, die dermate realistisch zijn dat ze als uitwijk faciliteit gebruikt zouden kunnen worden in geval van een calamiteit, een eerste stap zijn om aan deze tekortkoming tegemoet te komen. Voor een dergelijk (potentieel kostbaar) initiatief ter verbetering van collectief herstelvermogen is nog de vraag welke partijen bereid zijn om deze uitdaging als eerste op te pakken.

Conclusies en vervolgonderzoek

Dit artikel heeft een beknopte inzage gegeven in de huidige stand van zaken met betrekking tot herstelvermogen binnen Nederlandse organisaties. Er zijn hierbij een aantal belangrijke bevindingen verwoord over de rol die management awareness- en commitment speelt bij het herstelvermogen. Daarbij zijn er een aantal aanknopingspunten geschetst die het herstelvermogen van organisaties kunnen versterken.
Dit verkennende onderzoek heeft zich beperkt tot het herstelvermogen van de ICT functionaliteit van een select aantal organisaties. Het is de ambitie om dit verkennend onderzoek in de toekomst op twee manieren te verbreden. Ten eerste is gedurende het onderzoek het voorstel naar voren gekomen om de geïnventariseerde stand van zaken verder uit te werken naar self-assessments. Met deze self-assessments kunnen ook andere organisaties een inschatting maken over hoe hun herstelvermogen er voor staat en tips ontvangen voor verbetering. Daarnaast is voor veel organisaties ook OT (Operationele Technologie) van belang voor hun kernbedrijfsprocessen. Een inventarisatie van OT herstelvermogen is dan ook nodig om de stand van zaken op het gebied van herstelvermogen bij Nederlandse organisaties te completeren.