Anna van Buerenplein 1
2595 DA Den Haag
Postbus 96800
2509 JE Den Haag

www.tno.nl

T +31 88 866 00 00

TNO-rapport

TNO 2020 R12064

Herstelvermogen binnen IT infrastructuren

Een definitie, belangrijke aspecten, en status-quo analyse

Datum	10 december 2020
Auteur(s)	Sterre den Breeijen, Robert Seepers, Bart Gijsen, Ruggero Montalto, Bram Poppink
Aantal pagina's	39 (incl. bijlagen)
Aantal bijlagen	1
Opdrachtgever	NCSC
Projectnaam	NCSC Kennisopbouw 2020
Projectnummer	060.43105

Anna van Buerenplein 1
2595 DA Den Haag
Postbus 96800
2509 JE Den Haag

www.tno.nl

T +31 88 866 00 00

Dit rapport is een direct resultaat van het onderzoek verricht in de meerjarige (2020-2022) onderzoekssamenwerking tussen het NCSC en TNO. Dit rapport is tot stand gekomen door inhoudelijke en richting gevende bijdrage van het NCSC (onder andere Jeroen van der Ham), de deelname aan interviews door negen verschillende Nederlandse organisaties, en de inhoudelijke inbreng van het TNO projectteam (de auteurs van dit rapport, zie management samenvatting).

Het rapport is op de NCSC website gepubliceerd, onder het thema onderzoek: www.ncsc.nl/onderzoek.

Dit rapport is op de TNO website gepubliceerd onder het thema Cyber Security: het belang van een integrale oplossing.

Management samenvatting

Titel :	Herstelvermogen binnen IT infrastructuren
Auteur(s) :	Sterre den Breeijen, Robert Seepers, Bart Gijsen, Ruggero Montalto, Bram Poppink
Datum :	10 december 2020
Opdrachtnr. :	NCSC
Rapportnr. :	TNO 2020 R12064

Herstelvermogen speelt een cruciale rol in de cyberweerbaarheid van organisaties, waaronder de doelgroep organisaties van het NCSC. In de meerjarige onderzoekssamenwerking tussen het NCSC en TNO is herstelvermogen daarom aangewezen als een belangrijk onderwerp voor kennisopbouw. In 2020 is binnen deze onderzoekssamenwerking een verkennend onderzoek uitgevoerd naar de status van herstelvermogen voor IT-infrastructuren bij Nederlandse organisaties. De aanpak en resultaten van dit onderzoek staan beschreven in dit rapport.

In het onderzoek zijn eerst de belangrijke aspecten van herstelvermogen in kaart gebracht en is een definitie van herstelvermogen geformuleerd:

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

Vervolgens zijn er negen interviews afgenomen bij verschillende typen organisaties met een eigen IT-infrastructuur om te achterhalen wat de stand van zaken is op het gebied van herstelvermogen. Na een analyse op basis van de hiermee opgehaalde informatie zijn de belangrijke aspecten van herstelvermogen aangescherpt en kon geconcludeerd worden dat herstelvermogen bij alle geïnterviewde partijen wordt opgepakt, vaak in de vorm van een samenvoeging van Business Continuity Management en Cyber Security.

Een belangrijke indicator voor goed ingericht herstelvermogen is awareness en commitment bij management. Als deze ontbreken, zijn er onvoldoende mensen en middelen om herstelvermogen in de breedte goed in te richten. Belangrijke drijfveren voor het management om middelen toe te wijzen aan de inrichting, en het verbeteren van, herstelvermogen zijn:

- het directe belang van IT voor de bedrijfscontinuïteit; en
- wetgeving.

Vooral bij organisaties waarbij het primaire bedrijfsbelang sterk afhangt van IT-continuïteit worden vergaande herstelmaatregelen getroffen. Verder hebben recente, grote incidenten bij eigen, of vergelijkbare, organisatie veel invloed op de awareness bij het management.

Op basis van de analyse is er ook ruimte voor verbetering geïdentificeerd. Het NCSC zou op onderstaande punten mogelijkerwijs vervolgstappen kunnen ondernemen:

- het periodiek bijstellen van incidentscenario's;

- het (vaker) oefenen van realistische scenario's met mogelijkerwijs risicovolle technische gevolgen; en
- het verder uitwerken en opstarten van concreet collectief herstelvermogen.

Aandacht voor het periodiek bijstellen van incidentscenario's is belangrijk omdat uit de interviews is gebleken dat de meeste organisaties incidentscenario's pas herzien en bijstellen wanneer er een (grootschalig) incident plaatsvindt in de eigen organisatie of daarbuiten.

Daarnaast kan het oefenen van realistische grootschalige incidenten het herstelvermogen van organisaties verbeteren. Namelijk, eenvoudige technische maatregelen worden wel degelijk geoefend, soms ook on-the-job, maar er is terughoudendheid om risicovolle technische oefeningen uit te voeren, vanwege de lastig te voorspellen impact op de bedrijfsuitvoering. De mogelijkheid om complexere technische herstelvoorzieningen te testen is daardoor beperkt.

Ook het concretiseren van collectief herstelvermogen kan bijdragen aan de verbetering van herstelvermogen. In de interviews zijn wel voorbeelden naar voren gekomen van informatiedeling, maar geen praktische voorbeelden genoemd van gezamenlijk optrekken richting herstel. Vooral bij de vitale infrastructuur organisaties wordt hier al wel over nagedacht, bijvoorbeeld over de inrichting van gezamenlijke IT-voorzieningen voor sectorpartners in geval van calamiteiten. Dit levert dan wel weer juridische complicaties op, zoals onduidelijkheid over aansprakelijkheid.

Bovendien bieden sommige conclusies handelingsperspectief voor het NCSC. Namelijk, beïnvloeding van de awareness en commitment bij het management van organisaties kan leiden tot de verbetering van herstelvermogen. De volgende twee conclusies zijn hiervoor relevant:

- nieuws is een belangrijke drijfveer voor het herzien van de eigen inrichting van herstelvermogen; en
- wet- en regelgeving is een belangrijke drijfveer voor het inrichten of verbeteren van herstelvermogen.

Nieuws blijkt een belangrijke drijfveer voor het herzien van de eigen inrichting van herstelvermogen. Niet alleen recente incidenten bij de eigen organisatie leiden tot bewustwording, maar ook incidenten bij andere organisaties die via de media binnenkomen kunnen inzichten creëren. Dergelijke incidenten beïnvloeden de perceptie over de kans op een incident. Deze perceptie is door NCSC beïnvloedbaar, bijvoorbeeld door bepaalde incidenten specifiek uit te lichten via gepubliceerde dreigingsbeeld en/of via de media.

Wettelijke regelgeving is door een aantal organisaties genoemd als belangrijke drijfveer voor het inrichten van herstel maatregelen. Voor het NCSC biedt dit handelingsperspectief om herstelvermogen te beïnvloeden in gereguleerde sectoren via toezichthouders.

Inhoudsopgave

1 Inleiding

In de afgelopen jaren heeft er een paradigmaverschuiving plaatsgevonden in het cybersecuritylandschap: het is niet langer de vraag óf een organisatie kwetsbaar is voor incidenten, maar het is de vraag wannéér een organisatie getroffen zal worden door een incident. Op het moment dat een organisatie getroffen wordt door een incident is het herstelvermogen van deze organisatie van cruciaal belang.

Binnen de context van dit onderzoek is het onderwerp *herstelvermogen* in eerste instantie afgebakend als het vermogen van een organisatie om haar bedrijfsvoering zo snel en goed mogelijk weer op te pakken (te herstellen) nadat deze getroffen is door een cyberaanval of niet-intentioneel incident met gevolgen voor de ICT. Zonder degelijk ingericht herstelvermogen is het mogelijk dat een incident op één organisatie kan leiden tot een cascade effect in een gehele (vitale) dienstketen.

Herstelvermogen is binnen de NCSC onderzoeksagenda[1] voor de periode 2019-2022 aangewezen als een belangrijk onderwerp gegeven de cruciale rol die herstelvermogen speelt in de cyberweerbaarheid van haar doelgroep organisaties, waaronder de vitale infrastructuur organisaties.

In de NCSC onderzoeksagenda zijn onderwerpen geïdentificeerd waar kennisopbouw of verbetering relevant geacht wordt. Zo is er nog geen volledig beeld van welke aspecten relevant zijn voor herstelvermogen (denk aan aspecten zoals technische inrichting, organisatie-inrichting, collectief herstelvermogen[2] en leren-van-de-fouten). Ook is het niet duidelijk in hoeverre de doelgroepen van het NCSC hun herstelvermogen op orde hebben. Het NCSC ziet een rol voor zichzelf op dit gebied door advies te kunnen geven over de inrichting van herstelvermogen. Voldoende kennis van dit onderwerp is hiervoor een randvoorwaarde.

In dit kader heeft TNO verkennend onderzoek verricht ten gunste van kennisopbouw op het onderwerp herstelvermogen. Dit onderzoek is daarbij primair bedoeld om te bepalen hoe herstelvermogen is ingericht bij organisaties in Nederland, zowel binnen de doelgroep van het NCSC (Rijksoverheid en vitale infrastructuur) als daarbuiten. Ook is geanalyseerd waar de belangrijkste gaten zitten in het herstelvermogen van de doelgroep als geheel.

Dit document beschrijft achtereenvolgens
- de aanpak van het onderzoek, in hoofdstuk 2;
- definitie en belangrijke aspecten van herstelvermogen, in hoofdstuk 3;
- bevindingen op basis van de opgehaalde informatie in interviews met de (doelgroep) organisaties, in hoofdstuk 4; en
- conclusies, inclusief mogelijke vervolgstappen voor het NCSC, en de ambities voor vervolg onderzoek, in hoofdstuk 5.

[1] https://www.ncsc.nl/documenten/publicaties/2019/september/26-9-2019/ncsc-onderzoeksagenda-2019-2020

[2] Collectief refereert hier aan de mate waarin organisaties gezamenlijk optrekken richting herstel.

2 Aanpak

In dit hoofdstuk wordt de aanpak van het onderzoek omschreven. Het onderzoek is uitgevoerd aan de hand van de volgende taken:

1. Het komen tot een definitie van herstelvermogen en identificeren van de belangrijke aspecten van herstelvermogen;
2. Het afnemen van interviews bij diverse organisaties; en
3. Een analyse aan de hand van de afgenomen interviews.

Om tot een definitie van herstelvermogen te komen (taak 1) zijn interviews en brainstorm sessies gehouden met TNO experts, en is een literatuurscan uitgevoerd. Bij de literatuurscan zijn vooral raamwerken betreffende Resilience Engineering[3] (weerbaarheid) en IT Service Continuity Management[4] waardevol gebleken. De definitie waartoe gekomen werd, is op 14 april besproken tijdens een werksessie met het NCSC. In deze sessie is de definitie van herstelvermogen gepresenteerd, inclusief de belangrijke aspecten hiervan. De input van het NCSC (in de vorm van feedback en nieuwe ideeën) tijdens deze werksessie is verwerkt en een uiteindelijke definitie van Herstelvermogen is omschreven in een tussentijdse deliverable. De definitie en belangrijke aspecten van herstelvermogen staan omschreven in het volgende hoofdstuk *3* Herstelvermogen – Definitie en belangrijke aspecten.

Vervolgens zijn interviews afgenomen om de stand van zaken rondom herstelvermogen bij organisaties te inventariseren (taak 2). Er zijn negen interviews afgenomen bij verschillende organisaties, zowel onderdeel van de doelgroep van het NCSC als daarbuiten. Sectoren waar deze organisaties onder vallen zijn: Rijksoverheid, vitale infrastructuur organisaties, clouddienst providers en kennis- en onderwijsinstellingen. In paragraaf 2.1 zal verder worden ingegaan op de selectie van interview kandidaten en zullen de kenmerken van deze organisaties op geanonimiseerde wijze worden weergegeven.

De interviews zijn semigestructureerd afgenomen, waarbij gebruik werd gemaakt van vooraf opgestelde interview vragen met mogelijkheid om daarvan af te wijken. De vooraf opgestelde vragen zijn geformuleerd gebruikmakend van de eerder opgestelde belangrijke aspecten van herstelvermogen. De inzichten uit elk interview zijn vastgelegd in een interviewverslag.

Bij ieder interview waren één of twee vertegenwoordigers van de te interviewen organisatie aanwezig. Bovendien waren er tenminste twee TNO projectleden aanwezig voor het stellen van de vragen en voor de verslaglegging. Ook is bij bijna alle interviews een NCSC afgevaardigde aanwezig geweest, om het gesprek toe te horen en additionele vragen te stellen.

Na het interview is het interviewverslag voorgelegd aan de geïnterviewde personen ter verificatie en waar nodig zijn aanpassing doorgevoerd. Ook is het verslag ter verificatie opgestuurd naar de aanwezige NCSC afgevaardigde.

Na het afronden van alle interviews en interviewverslagen is een analyse uitgevoerd (taak 3). De belangrijke aspecten van herstelvermogen zijn hierbij puntsgewijs vergeleken over

[3] Cyber Resiliency Engineering Framework | The MITRE Corporation
[4] ITIL Version 3 Chapters (hci-itil.com)

de organisaties heen. Hierbij is rekening gehouden met het type organisatie: commercieel of overheid, primair leverancier van IT of afnemer van IT, vitaal of niet vitaal, doelgroep organisatie of niet doelgroep organisatie. Daarnaast is de focus gelegd op het identificeren van gedeelde gaten in herstelvermogen, trends en mogelijke aanleiding tot collectief herstelvermogen. De resultaten zijn na deze analyse geanonimiseerd en op zodanige wijze verwerkt in dit document dat het niet naar afzonderlijke organisaties herleidbaar is. De bevindingen van deze analyse staan in hoofdstuk 4 Bevindingen beschreven.

2.1 Selectie en kenmerken van geïnterviewde organisaties

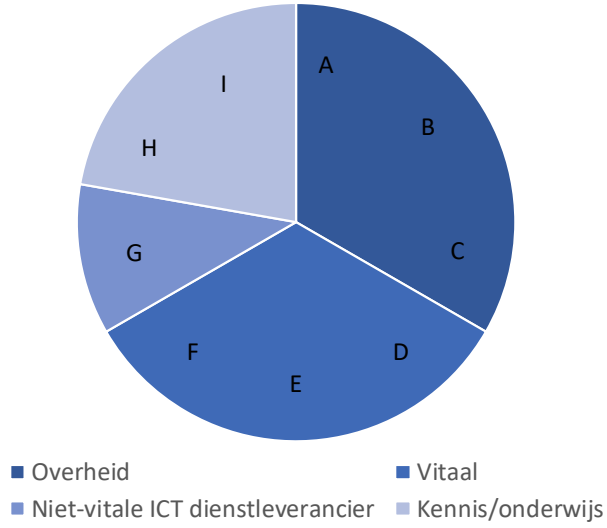
Om de stand van zaken rondom herstelvermogen bij organisaties te inventariseren zijn er interviews afgenomen bij verschillende organisaties. Gegeven de verkennende aard van dit onderzoek is de keuze gemaakt om hier een breed pallet van typen organisaties voor te benaderen. Met deze organisaties is afgesproken dat hun interviews anoniem verwerkt worden.

Bij de selectie van te-benaderen organisaties zijn er een aantal selectiecriteria opgesteld. In de komende paragrafen worden deze criteria verder beschreven. Gegeven de afspraak tot anonimiteit worden deze organisaties hierbij aangeduid met de letters ‘A’ tot en met ‘I’.

Vanwege de verkennende aard van dit onderzoek is per organisatie getracht één à twee vertegenwoordigers aan tafel te krijgen welke een integraal beeld hebben van de stand van zaken van herstelvermogen bij de eigen organisatie. Dit heeft er toe geleid dat de interviewkandidaten verschillende rollen en verantwoordelijkheden hebben bij de eigen organisatie, waaronder information security officers en business continuity managers.

2.1.1 Sector

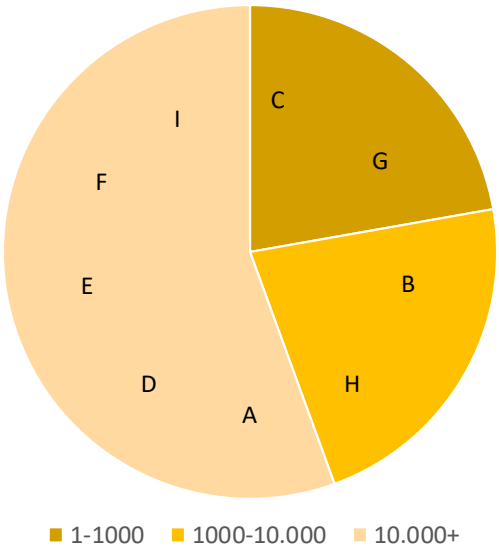
De primaire doelgroep van het NCSC zijn organisaties binnen de Rijksoverheid als ook de vitale infrastructuur. Binnen het onderzoek zijn hierom verschillende organisaties geïnterviewd die in één van deze sectorcategorieën vallen. Daarnaast zijn er een aantal organisaties geïnterviewd die geschaard zijn in de sector “kennis-/onderwijsinstelling” en “niet-vitale ICT dienstverlening”. Deze organisaties zijn betrokken om breder beeld te kunnen schetsen bij de status van herstelvermogen in Nederland. Daarnaast biedt dit de mogelijkheid om de status van herstelvermogen van de primaire doelgroep van het NCSC te vergelijken met organisaties die hierbuiten vallen. Figuur 1 illustreert de vertegenwoordiging van de verschillende geïnterviewde organisaties per sector.



Figuur 1: Vertegenwoordiging geïnterviewde organisaties per sector

2.1.2 Organisatiegrootte

Er zijn organisaties van verschillende groottes betrokken om te kunnen achterhalen of er verschillen zitten tussen kleine en grote organisaties. Figuur 2 geeft een indicatie van de grootte van de verschillende geïnterviewde organisaties.



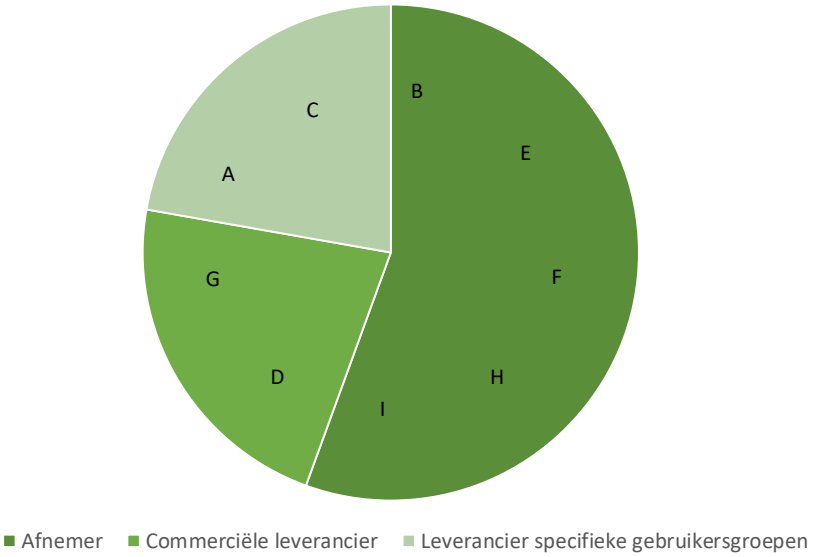
Figuur 2: Aantal medewerkers van de geïnterviewde organisaties.

2.1.3 Relatie met ICT

Elk van de geïnterviewde organisaties maakt gebruik van ICT om haar diensten te kunnen verlenen. Er is hiervoor onderscheid gemaakt in de volgende types organisatie:

- **Afnemer:** Organisaties die ICT primair gebruiken als ondersteuning voor hun dienstverlening.
- **Commercieel dienstverlener:** Organisaties waarvan het aanbieden van ICT onderdeel is van de primaire dienstverlening.
- **Leverancier specifieke gebruikersgroepen:** Organisaties die ICT aanbieden binnen een beperkte gebruikersgroep (e.g. regie-organisaties).

Figuur 3 geeft weer hoe de geïnterviewde organisaties deze groepen vertegenwoordigen.



Figuur 3: Relatie tussen geïnterviewde organisaties en ICT.

3 Herstelvermogen – Definitie en belangrijke aspecten

Om een uitspraak te kunnen doen over de stand van zaken op het gebied van herstelvermogen bij Nederlandse organisaties is het van belang scherp te krijgen wat we verstaan onder 'herstelvermogen'. In dit hoofdstuk wordt hiertoe eerst beschreven wat verstaan wordt onder herstelvermogen, in paragraaf 3.1 Definitie van Herstelvermogen. Vervolgens wordt er in paragraaf 3.2 Deelaspecten inrichting herstelvermogen ingegaan op de belangrijkste aspecten en deelaspecten die nodig zijn om herstelvermogen goed in te richten. Deze (deel)aspecten worden in Hoofdstuk 4 gebruikt om de huidige status van herstelvermogen bij de geïnterviewde organisaties te analyseren.

3.1 Definitie van Herstelvermogen

Om tot een werkbare definitie van herstelvermogen te komen is er gebruik gemaakt van verschillende bronnen – waaronder publicaties en frameworks die betrekking hebben op cyber resilience en/of herstel. Hieruit is een eerste definitie afgeleid, die verder is aangescherpt op basis van een werksessie met deelnemers van het NCSC en TNO. De uitkomst hiervan is de onderstaande definitie van herstelvermogen:

> *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 is bewust breed opgezet aangezien herstelvermogen een heel scala aan facetten raakt: van diensten die geleverd worden door een bedrijf tot data-back-ups, en van tijdelijk herstel tot duurzame vernieuwing. In de komende paragrafen worden de belangrijkste nuances in deze definitie verder uiteengezet.

3.1.1 Functionaliteit, die voorzien wordt door ICT

Herstel kan alleen plaatsvinden als er iets beschadigd is, waarbij "iets" alleen relevant is, wanneer deze een bepaalde functionaliteit levert. Denk hierbij aan informatie, informatiesystemen en/of diensten. We beperken ons, in het kader van dit onderzoek, tot dergelijke functionaliteiten die geleverd worden door ICT. *Functionaliteit, voorzien door ICT* werkt naar behoren als de beschikbaarheid, vertrouwelijkheid en integriteit van functionaliteit zoals informatie, informatiesystemen en -diensten, kan worden gegarandeerd.

Een incident met impact op *functionaliteit, voorzien door ICT*, betekent dus niet altijd dat een dienst of systeem het niet meer doet. Een voorbeeld hiervan is een cyberaanval. Op het moment dat er ontdekt wordt dat er een indringer een bedrijfsnetwerk is binnengekomen, kunnen alle systemen en diensten nog werken, en is de beschikbaarheid dus niet aangetast. Wel is de vertrouwelijkheid verstoord en mogelijk ook de integriteit van informatie, waardoor de *functionaliteit, voorzien door ICT* verstoord is, en herstel noodzakelijk is. Toch krijgt herstelvermogen een brede toepassing aangezien er ook niet-intentionele verstoringen zijn, buiten het cybersecurity domein, die onder de definitie vallen.

We maken een onderscheid tussen repressie (het beperken van impact van een incident) en herstel (het herstellen na inperking). Het laatste valt binnen de scope van herstelvermogen. Het doel van herstel na repressie is primair om de *functionaliteit, voorzien door ICT* weer beschikbaar te maken. Namelijk, herstel van een specifiek

informatiesysteem, is niet een doel op zich als er een alternatief informatiesysteem dezelfde functionaliteit kan leveren. Sterker nog, een belangrijk aspect van goed ingericht herstelvermogen is het inbouwen van redundantie in *functionaliteit, voorzien door ICT*.

Herstel betekent niet per se dat men na een incident toewerkt naar de “pre-disruption state” van de functionaliteit. Vaak is het zo dat een herconfiguratie van informatie, informatiesystemen en -diensten na een incident noodzakelijk is om de beschikbaarheid, vertrouwelijkheid en integriteit op een duurzame manier te kunnen garanderen (dat wil zeggen dat de functionaliteit op een manier wordt ingericht dat een soortgelijke uitval van functionaliteit in de toekomst niet meer voorkomt).

3.1.2 Efficiënt en effectief

Het herstellen van functionaliteit, voorzien door ICT dient *efficiënt en effectief* te gebeuren. Dit refereert aan dat*:*

- de middelen die ingezet worden voor herstel opwegen tegen de negatieve impact van een incident;
- dat het herstel doeltreffend is;
- binnen een passende tijd wordt uitgevoerd; en
- passend duurzaam is.

Belangrijke succesfactoren hierbij zijn de status van voorbereiding van herstelvermogen en het adapterend en lerend vermogen van een organisatie.

Herstellen na een incident kent doorgaans gradaties. Vaak is er een balans tussen de snelheid van herstel en de duurzaamheid. Snelle oplossingen zijn vaak niet duurzaam, en duurzame oplossingen zijn vaak niet snel gevonden en in de praktijk gebracht. Afhankelijk van de impact van een incident op de functionaliteit, voorzien door ICT, dient men te bepalen wat de beste optie is: herstellen tot een minimaal acceptabel functionaliteitsniveau, tot het gewenste functionaliteitsniveau, iets daartussen, of eerst het minimaal acceptabele en daarna herstellen tot het gewenste functionaliteitsniveau.

3.1.3 Organisatie

Als organisatie heb je invloed op de functionaliteit die je als organisatie zelf levert, maar ook op de mate waarin de organisatie afhankelijk is van functionaliteit geleverd door anderen. Als organisatie ben je eindverantwoordelijke voor de door jou geleverde diensten en de daarvoor gebruikte functionaliteiten. Hiervoor is in de definitie expliciet “de organisatie” opgenomen, refererend aan de organisatie die de diensten levert.

Er zijn veel situaties denkbaar waarbij een organisatie slechts een deelfunctionaliteit levert in een groter geheel (zoals een keten). Soms heeft een incident met impact op functionaliteit geleverd door één organisatie ook effect op een organisatie overstijgend proces, of zelfs een negatief cascade effect op de functionaliteit geleverd door andere organisaties. Wanneer het belang van herstel van het organisatie overstijgende proces even groot, of groter, is dan het herstel van de functionaliteit bij één specifieke organisatie kan het wenselijk zijn om samen te werken bij het herstellen van het organisatie overstijgende proces. Dit kan bijvoorbeeld het geval zijn bij een keten in de vitale infrastructuur, waarbij het maatschappelijke belang van de functionaliteit die deze keten van organisaties levert groter is dan het herstel van functionaliteit bij één van de organisaties na een incident.

De mate waarin organisaties gezamenlijk toewerken naar herstel noemen we *collectief herstelvermogen*. Voor *collectief herstelvermogen* is de noodzaak tot herstel (incidenten)

en de kwaliteit van herstel (efficiënt en effectief) vergelijkbaar als bij “individueel” herstelvermogen. Wat bij individueel herstelvermogen niet noodzakelijk is, maar bij collectief herstelvermogen wel, is dat er afspraken gemaakt moeten worden tussen organisaties, vooral over de te herstellen functionaliteit en de verantwoordelijkheden van herstel.

Zowel afstemming met ketenpartners als collectief herstelvermogen worden verder toegelicht in paragraaf 3.2.5.2 Afstemming met ketenpartners en collectief herstelvermogen.

3.1.4 Herstelvermogen in relatie tot andere begrippen

Herstelvermogen, zoals gedefinieerd in dit onderzoek is sterk gerelateerd, maar niet synoniem, aan twee andere begrippen: weerbaarheid en business continuity management. Hieronder wordt de relatie van herstelvermogen tot deze twee begrippen uitgelegd.

3.1.4.1 Weerbaarheid

Weerbaarheid, digitale weerbaarheid of cyber resilience, wordt vaak beschreven als het vermogen van organisaties om de bedrijfsvoering voldoende goed te blijven uitvoeren ondanks het optreden van (vijandige) digitale incidenten. Het MITRE CREF[5] omschrijft bijvoorbeeld dat weerbaarheid bestaat uit het anticiperen op cyber dreigingen, het continueren van operatie ondanks cyber dreigingen, het herstellen van cyber dreigingen, en het adapteren naar aanleiding van cyber dreigingen. Het is een relatief nieuw, innovatief en opkomend vakgebied. Binnen dit vakgebied worden maatregelen ten aanzien van (geavanceerde) cyber dreigingen vaak expliciet behandelt.

Herstelvermogen is een onderdeel van weerbaarheid. Echter, herstelvermogen, zoals gedefinieerd in dit onderzoek, is meer dan slechts de herstelactiviteiten zoals vaak verwoord binnen het vakgebied weerbaarheid. Dit klinkt in eerste instantie wellicht contra-intuïtief, maar komt voort uit het feit dat we in dit onderzoek ook de anticiperende, evaluerende/adapterende, en nog een aantal overige activiteiten (e.g. collectief herstelvermogen) ten gunste van herstel meenemen in dit onderzoek. Hier zal verder op worden ingegaan in hoofdstuk 3.2 Deelaspecten inrichting herstelvermogen.

3.1.4.2 Business Continuity Management

Business Continuity Management (BCM) is een relatief klassiek vakgebied met als doel om de bedrijfsvoering zo continue als mogelijk uit te voeren, of anders te hervatten binnen vooraf afgesproken tijdschalen. Het is een al langer gevestigd vakgebied met focus op het beheersen van alle risico’s die de bedrijfsvoering in gevaar kunnen brengen. Het adresseert alle risico’s die de bedrijfsvoering bedreigen en focust daarbij niet specifiek op incidenten met een bepaalde oorzaak (e.g. cyber aanvallen). De BCM aanpak is vooral geschikt voor herstel na grote, mogelijk catastrofale, incidenten. Voor de inrichting van herstelvermogen ten aanzien van kleinere, wederkerende incidenten worden alternatieve vergelijkbare aanpakken gehanteerd, zoals het ITIL IT Service Continuity Management. Binnen het BCM vakgebied worden maatregelen ten aanzien van (geavanceerde) cyber dreigingen hooguit impliciet behandelt.

Herstelvermogen overlapt grotendeels met Business Continuity Management (BCM) met enkele verschillen. Maatregelen met als doel om incidenten te voorkomen (preventief) of beperken (repressief) zijn wel onderdeel van BCM, maar vallen niet onder de definitie van

[5] Cyber Resiliency Engineering Framework | The MITRE Corporation

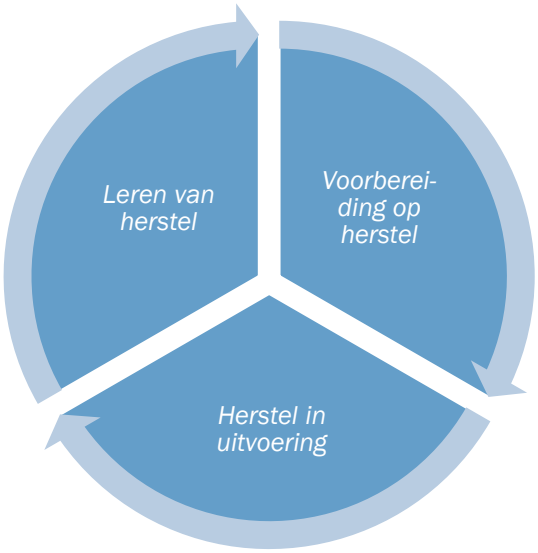
herstelvermogen. Ook richt BCM zich vooral op continuering of hervatting van de “pre-disruption state” en is daardoor minder gericht op het aanpassen (adapteren) van middelen naar aanleiding van incidenten. Adapteren en aanpassen naar aanleiding van incidenten is wel een belangrijke component van herstelvermogen, zoals in detail zal worden uitgelegd in hoofdstuk 3.2.4 Leren van uitvoering.

3.2 Deelaspecten inrichting herstelvermogen

De definitie in de vorige paragraaf geeft aan dat goed herstelvermogen er voor zorgt dat functionaliteit (voorzien door ICT) op een efficiënte en effectieve manier hersteld wordt. In deze paragraaf wordt verder ingegaan bij wat er nodig is om het herstelvermogen goed in te richten. Hiervoor wordt eerst een beknopt overzicht gegeven van de kernactiviteiten die voor, tijdens en na het herstel behoren te worden uitgevoerd, waarna de belangrijke aspecten van deze activiteiten in meer detail worden beschreven.

3.2.1 Beknopt overzicht herstelactiviteiten

Goed herstelvermogen wordt gekenmerkt door een set activiteiten die voor, tijdens en na een incident uitgevoerd moeten worden. We onderscheiden hierbij dus drie fases als onderdeel van het herstelvermogen: voorbereiding op herstel, herstel in uitvoering en leren van herstel – zoals ook geïllustreerd in Figuur 4: Fases van herstelvermogen.



Figuur 4: Fases van herstelvermogen

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.

Dit samenspel kan verder worden toegelicht aan de hand van een voorbeeld. Neem een scenario waarbij data gecompromitteerd wordt als gevolg van een ransomware-aanval.

Om deze data op een effectieve en efficiënte manier te kunnen herstellen, zijn de volgende acties nodig in de drie herstelfases:

- **Voorafgaand** aan de aanval moet er 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 (e.g. 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 om de getroffen maatregelen en gevolgde herstelprocessen, waar mogelijk, aan te scherpen.

In de volgende subsecties worden eerst de drie hoofdfases van herstelvermogen verder toegelicht. Hierbij worden ook de belangrijkste deelactiviteiten per fase beschreven (met name geënt op de techniek en processen) en hoe deze relateren aan het herstelvermogen. Vervolgens wordt er verder ingegaan op een aantal onderwerpen die belangrijk zijn voor het herstelvermogen maar een algemener karakter kennen en daarbij niet direct onder één van deze drie hoofdfases vallen. Dit zijn de onderwerpen “Training en oefening” en “Afstemming met ketenpartners en collectief herstelvermogen”.

3.2.2 Voorbereiden op herstel

Voordat er een incident plaatsvindt, moeten er verschillende activiteiten worden uitgevoerd om herstel-in-uitvoering zo goed mogelijk te faciliteren. Zo zullen er verschillende technische maatregelen getroffen moeten worden (e.g. het inrichten van data-back-ups), maar ook organisatorische maatregelen (e.g. het opstellen van processen en procedures om deze back-ups snel te kunnen herstellen). In de komende deelsecties wordt er verder ingegaan in de verschillende deelactiviteiten die getroffen dienen te worden ter voorbereiding op herstel.

3.2.2.1 Dreigingsbeeld en risico inschatting

Het inrichten van de verschillende maatregelen moet passen bij het risico dat een organisatie wil mitigeren ten aanzien van ICT. Door goed zicht te hebben op de dreigingen voor een organisatie kan er een goede inschatting gemaakt worden in hoeverre herstelmaatregelen getroffen moeten worden voor de verschillende functionaliteiten. Hoe belangrijker de functionaliteit voor de organisatie, hoe stringenter de maatregelen zouden moeten zijn. Denk hierbij bijvoorbeeld aan het garanderen van een hoge uptime van geleverde diensten, of het garanderen dat missie-kritieke data altijd behouden blijft.

Voor het inschatten van de juiste herstelmaatregelen zijn de volgende aspecten van belang:

- Een organisatie moet goed op de hoogte zijn van welke functionaliteiten (voorzien door ICT) ze heeft en hoe en in hoeverre deze bijdraagt aan de bedrijfsvoering;
- Er moet een goed beeld zijn bij de verschillende dreigingen ten aanzien van deze organisatie en de (door ICT-geleverde) functionaliteiten. Deze dreigingen kunnen zowel van digitale of fysieke origine zijn en kunnen bewust of incidenteel van aard

zijn. Denk bijvoorbeeld aan een ransomware-aanval, maar ook voorzieningen die incidenteel uitvallen door, e.g., een stroomstoring.
- Op basis van het bovenstaande moet er een risico-inschatting gemaakt worden en bepaald in hoeverre deze risico's gemitigeerd moeten worden. Herstelmaatregelen zijn onderdeel van deze mitigerende maatregelen.

Het periodiek en incidenteel aanscherpen van bovenstaande aspecten is van belang voor effectief en efficiënt herstelvermogen. Dit staat organisaties toe om de (getroffen) herstelmaatregelen zo nauw mogelijk af te stemmen op haar risicoprofiel.

3.2.2.2 Technische herstelmaatregelen

Afhankelijk van het type incident waarop organisaties zich voorbereiden zullen verschillende technische maatregelen getroffen worden. Deze maatregelen kunnen op verschillende niveaus getroffen worden. Zo kunnen er redundante hardware-infrastructuren ingericht worden (bijvoorbeeld in een active-active of active-passive configuratie), maar ook maatregelen op data-niveau (het maken van back-ups of redundante hosting).

Goed herstelvermogen wordt gekenmerkt door een passende inrichting van deze technische maatregelen ten aanzien van het risicoprofiel en de daarbij passende hersteleisen (zoals beschreven in de vorige paragraaf).

3.2.2.3 Organisatorische maatregelen

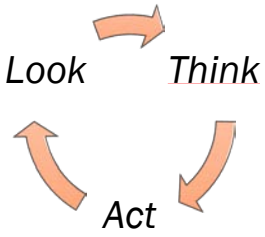
De technische maatregelen zoals in de hierboven aangegeven paragraaf maken het mogelijk om herstel uit te kunnen voeren. Tijdens het uitvoeren van herstel is het echter ook van belang om te weten wie dit herstel uitvoert, en hoe. In paragraaf 3.2.3 worden de verschillende deelactiviteiten voor tijdens het herstel nader beschreven. Om deze soepel te laten verlopen, moet er vooraf duidelijk worden beschreven hoe deze activiteiten moeten worden uitgevoerd, door wie en met welk mandaat. Denk hierbij aan zowel procedurebeschrijvingen om (technisch) herstel uit te voeren, het beleggen van verantwoordelijkheden en de inrichting van een crisisteam. Ook moeten er, in het geval dat er externe leveranciers betrokken zijn (e.g. externe hostingpartijen) afspraken gemaakt worden over het uitvoeren van herstel bij een incident (o.a. doorlooptijd).

Goed herstelvermogen wordt gekenmerkt door het vastleggen van een set organisatorische maatregelen voordat een incident zich voordoet, waardoor die het herstel-in-uitvoering zo goed mogelijk wordt gefaciliteerd.

3.2.3 Herstel-in-uitvoering

De fase 'herstel-in-uitvoering' vormt de kern van het herstelvermogen; zoals de naam suggereert wordt de verstoorde functionaliteit in deze fase daadwerkelijk hersteld. Deze fase begint met het detecteren van een verstoring en sluit af wanneer deze hersteld is. Het herstel-in-uitvoering is daarbij een iteratief proces waarbij er stapsgewijs wordt gewerkt naar een oplossing. Een representatie van dit proces is geïllustreerd in Figuur 5 en bestaat uit:

- *Look:* Observeer en onderzoek wat er aan de hand is;
- *Think:* Bepaal mogelijke herstelacties; en
- *Act:* Voer de herstelacties uit.



Figuur 5: Fases tijdens de uitvoer van herstel, een iteratief proces

In de komende subsecties worden de verschillende deelactiviteiten binnen deze fase verder beschreven. Let op dat deze activiteiten typisch cyclisch worden doorlopen: Sommige activiteiten brengen bijvoorbeeld nieuwe informatie aan het licht, waardoor bepaalde activiteiten opnieuw uitgevoerd zullen worden.

3.2.3.1 Incidentdetectie

Het herstel-in-uitvoering begint met de detectie van een incident. Er zijn verschillende manieren om incidenten op te merken. Zo kunnen:

- Klanten contact opnemen in het geval een geleverde dienst direct is verstoord;
- Technische verstoringen opgemerkt worden door middel van technische monitor-tooling (Denk hierbij aan tooling om periodiek te verifiëren of alle servers die offline zijn, maar ook de detectie van cyber-security incidenten door middel van end-point agents); en
- Het eigen personeel of een toeleverancier aan de bel trekken, bijvoorbeeld wanneer er stroomuitval wordt geconstateerd.

Goed herstelvermogen wordt gekarakteriseerd door een divers pallet aan mogelijkheden om incidenten te detecteren, passend bij de herstelbehoefte van de organisatie.

3.2.3.2 Impactanalyse

Bij constatering van een incident zal niet direct duidelijk zijn wat het effect en de impact hiervan is. Een klant die belt over een verstoorde inlogdienst duidt bijvoorbeeld op een directe belemmering van de primaire dienstverlening. De melding van dit incident maakt echter nog niet duidelijk of dit de enige dienst is die getroffen is, of dit de enige klant is die getroffen is, en wat de oorzaak is van dit incident. En andersom zou een puur technisch incident dat er op het eerste oog ‘onschuldig uitziet’ best grote gevolgen hebben voor de bedrijfsvoering.

Verschillende types incident zullen veelal verschillende impact hebben op bedrijfsvoering of andere IT-systemen. De activiteit ‘impactanalyse’ is erop gericht om in kaart te brengen wat de scope en effect is van het incident. Dit omvat zowel:

- Het scoren van (bekende) incidenten op hun verwachtte impact, bijvoorbeeld op basis van lessons learned of het bestaande draaiboek.
- Het uitvoeren van analyse om een scherper beeld te krijgen bij de oorzaak van het incident en daarmee mogelijk de bredere scope en effect van de verstoring.

Hoe sneller onderzocht kan worden welke systemen er verstoord zijn, hoe sneller deze hersteld kunnen worden. Goed herstelvermogen hangt in dat kader samen met de mogelijkheid tot het snel en effectief analyseren van de impact.

3.2.3.3 Escalatie

Als onderdeel van de impactanalyse (of: op basis van meerdere incidentmeldingen) kan blijken dat er meer aan de hand is dan in eerste instantie ingeschat. In deze gevallen moet er geëscaleerd kunnen worden. Een verstoring aan de infrastructuur kan bijvoorbeeld in eerste instantie een technisch probleem lijken, maar als meerdere systemen getroffen zijn (en meerdere klanten hier last van krijgen) dan ligt de oplossing mogelijk niet meer in enkel het volgen van technische herstelprocedures. Over sommige zaken zal een technisch team zelf kunnen besluiten, maar over incidenten met grote impact, zal besluitvorming hogerop in de organisatie gebeuren.

Het is belangrijk om in dergelijke situaties op een goede manier te kunnen escaleren, binnen eigen organisatie, maar ook naar leverancier of juist afnemers. Er moet dan duidelijk zijn naar wie, op welke wijze en wanneer er geëscaleerd kan worden.

3.2.3.4 Besluitvorming

Gedurende het herstelproces moeten verschillende besluiten gemaakt worden, zoals:

- Of nieuwe inzichten van een incident aanleiding geven tot escalatie;
- Welke expertise er betrokken moet worden binnen een herstelteam.
- Of de organisatie meer baat heeft bij snel-maar-tijdelijk herstel, of dat er juist langzamer-maar-duurzamer hersteld moet worden;

Goed herstelvermogen kenmerkt zich door een organisatie die snel en efficiënt dergelijke besluiten kan nemen en daarbij het mandaat heeft om hierop te sturen. Het gebruik maken van een gestandaardiseerde besluitmethode kan daarbij een positieve factor zijn.

3.2.3.5 Acuut en duurzaam herstel

Zoals in de vorige paragraaf al beschreven kan er een keuze gemaakt worden uit snel-maar-tijdelijk herstel, of juist langzamer-maar-duurzamer herstel. Met eerstgenoemde wordt gedoeld op de functionaliteit zo-snel mogelijk weer beschikbaar te maken waarbij het voorkomen van toekomstige uitval van dezelfde functionaliteit niet de eerste prioriteit heeft. Langzamer-maar-duurzamer herstel richt zich erop om de functionaliteit op een andere manier in te richten waardoor bijvoorbeeld toekomstig uitval minder waarschijnlijk. Dit type herstel is typisch duurzamer, maar kan minder snel gerealiseerd worden. Het kan daarbij ook het geval zijn dat het eerste herstel met de nodige hand-en-spandiensten wordt gedaan voor acuut herstel en, in navolging van het tijdelijk herstel, er een duurzamere oplossing wordt getroffen.

De gekozen vorm van herstel moet passen bij de mate waarin de functionaliteit van belang is voor de organisatie en in hoeverre deze acuut gemist kan worden.

3.2.3.6 Gebruik van draaiboeken in de praktijk en improvisatie

Herstel-in-uitvoering kan, naast acuut/duurzaam, gecategoriseerd worden door gestandaardiseerd (‘volgens een draaiboek’) en geïmproviseerd. In de eerste vorm wordt er gebruikt van gestandaardiseerde, vastgelegde processen. Deze processen kunnen daarbij gaan over hoe een bepaalde functionaliteit typisch hersteld moet worden, maar ook (zoals eerder beschreven) over welke besluiten er wanneer genomen moeten worden, en door wie. Het is echter niet mogelijk om alle mogelijke herstelacties tot in detail te beschrijven en uit te voeren. In het geval dat een herstel plan niet voldoende toegeschreven blijkt te zijn voor een bepaald type incident, of minder effectief blijkt dan verwacht, dan zal de organisatie zich moeten berusten op haar improvisatievermogen.

Denk hierbij aan het betrekken van relevante expertise die vanuit hun eigen perspectief ideeën kunnen aandragen om het herstel uit te voeren.

Goed herstelvermogen kan gekenmerkt worden door een draaiboek dat het merendeel van de processen, procedures en rolbelegging beschrijft en waarbij er gebruik gemaakt wordt van relevante expertise om, waar mogelijk, deze processen ter plekke te improviseren/toespitsen op het incident.

3.2.3.7 Verslaglegging tijdens incidenten

Gedurende een incident worden verschillende acties uitgevoerd en beslissingen gemaakt. Door deze vast te leggen wordt het mogelijk om gedurende het herstelproces:

- Meer inzicht te geven in de impact en scope/effect van een incident; en
- Een overdracht te doen tussen uitvoerende personen (bijvoorbeeld bij langdurige herstelacties).

Daarnaast maakt verslaglegging het mogelijk om na afloop van een incident beter te evalueren en lering te trekken uit het verloop van het herstel. Verslaglegging tijdens incidenten kan heel breed zijn, maar ook beperkt. Voorbeelden die vastgelegd kunnen worden zijn: oorzaak van incident, uitgevoerde herstelacties en gevolgen daarop, besluitvorming en andere procesmatige punten zoals communicatie met klanten.

3.2.3.8 Verhoogde dijkbewaking na herstel

Na het treffen van een bepaalde herstelactie kan het verstandig zijn om gedurende enkele tijd deze specifieke functionaliteit en andere functionaliteiten die hier nauw aan raken, scherper de aandacht te vestigen. Zo wordt sneller opgemerkt als een incident toch niet afgelopen blijkt te zijn, of als de herstelacties andere, onvoorziene gevolgen hebben.

3.2.4 Leren van uitvoering

Wanneer een incident afgerond is, gaat de laatste fase in: leren van uitvoering. Het primaire doel van deze fase is om terug te kijken naar het uitgevoerde herstel (evaluatie) en om te kijken hoe dit in de toekomst verbeterd kan worden (lessons learned). Deze geleerde lessen kunnen betrekking hebben op alle aspecten die genoemd zijn in dit hoofdstuk – van de inrichting van technische maatregelen tot besluitvorming en verslaglegging. Een belangrijk aspect is dat deze lessons learned ook lessons implemented worden. Dat wil zeggen, niet alleen constateren wat er beter kon, maar aanpassingen maken (in bijvoorbeeld de herstelinrichting of het algemene herstelplan) om herhaling te voorkomen.

3.2.5 Overige aspecten

In de vorige subsecties zijn de drie hoofdfases van herstel en de daaronder vallende deelactiviteiten nader beschreven. Er zijn echter een aantal activiteiten die ook van belang zijn voor het herstelvermogen, maar die niet direct vallen onder een van deze hoofdfases. Deze activiteiten zijn “Training en oefening”, “afstemmen met ketenpartners” en “collectief herstelvermogen” en worden in de komende subsecties nader beschreven.

3.2.5.1 Training en oefening

De deelactiviteiten die beschreven zijn voor de drie hoofdfases van herstel vereisen allen een bepaalde mate van expertise van de daarbij betrokken medewerkers. Zo vereist de activiteit “besluitvorming” om een bepaalde mate van stressbestendigheid en aansturingsvaardigheden, terwijl de daadwerkelijke uitvoer van herstelwerkzaamheden vragen om meer technische expertise. Als onderdeel van het herstelvermogen zullen

organisaties hiertoe ervoor moeten zorgen dat de medewerkers die betrokken worden bij het herstel op voorhand de juiste training hebben gehad. Bijvoorbeeld dat ze weten welke processen zich op welk moment afspeelt, weten wat er tijdens die processen van hen verwacht wordt en dat ze de juiste kennis hebben om hun rol te vervullen.

Als onderdeel van training zal er ook geoefend moeten worden met het herstel. Een dergelijke oefening gaat in wezen uit van een fictief incident waarbij de verschillende herstelstappen worden doorlopen. In de breedste zin kan een dergelijke oefening tekortkomingen in het herstelvermogen blootleggen. Specifieker dient een dergelijke oefening één of meerdere van de volgende doelen:

- Het beproeft de mate van expertise en ervaring bij de betrokken medewerkers, waarbij gaten in opleiding kunnen worden ontdekt;
- Het beproeft de getroffen technische maatregelen en processen voor het daadwerkelijk herstel. Hiermee kunnen tekorten in de processen of technische inrichting van herstelmaatregelen aan het licht worden gebracht;
- Het beproeft de processen met betrekking tot de organisatie (e.g. besluitvorming en escalatie) en kan daarbij gebruikt worden om deze aan te scherpen;
- Het kan de organisatie scherp en slagvaardig houden.

Daarnaast kan het houden van oefeningen noodzakelijk zijn voor compliance aan bepaalde standaarden. Een goede oefening zal echter nooit puur compliance-gedreven zijn en trachten om een of meerdere van bovenstaande punten te adresseren. De waarde van oefeningen zit hem in het opstellen van een realistisch scenario en het inbedden van geleerde lessen. Daarnaast kan er een keuze worden gemaakt over het vooraf aankondigen van een oefening of niet, als ook de effect en scope van het oefenscenario, afhankelijk van het doel van de oefening.

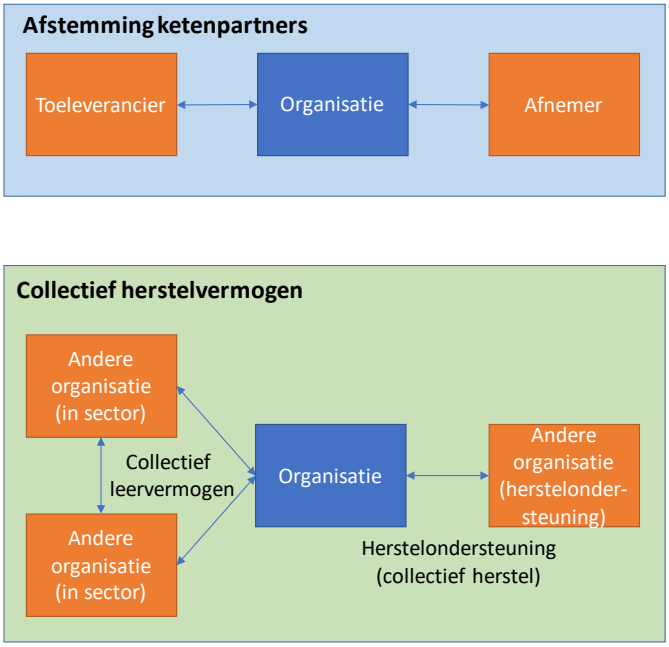
3.2.5.2 Afstemming met ketenpartners en collectief herstelvermogen

Binnen de eerder gegeven definitie van herstelvermogen en in alle bovenstaande paragrafen is er uitgegaan van de kennis en kunde van een enkele organisatie om zorg te dragen voor haar eigen herstel. Een organisatie opereert echter nooit in een vacuüm en zal altijd relaties hebben met andere organisaties, zoals leveranciers, afnemers of concurrenten. Binnen deze relaties zijn een aantal raakvlakken te noemen die relevant zijn voor het eigen herstelvermogen. Deze zijn, zoals ook geïllustreerd in Figuur 6, het afstemmen met ketenpartners en collectief herstelvermogen:

- **Afstemmen met ketenpartners:** Een verstoring van één organisatie kan negatieve effecten hebben in ketenverband (richting een afnemer). Het is daarom belangrijk om met ketenpartners (directe leveranciers en afnemers) afspraken te maken. Goed herstelvermogen eist bijvoorbeeld dat er met ICT-dienstleveranciers op voorhand afspraken gemaakt worden over hersteleisen (o.a. technisch en communicatie) en dat deze vastgelegd worden in een SLA. Bovendien, bij constatering van een incident moeten getroffen partners zo snel mogelijk geïnformeerd worden zodat er geen cascade van incidenten ontstaat.

- **Collectief herstelvermogen:** Collectief herstelvermogen is de mate waarin organisaties samen optrekken richting herstel. Collectief herstelvermogen wordt in dit onderzoek onderverdeelt in twee deelaspecten:
    - **Collectief leervermogen** is de mate waarin organisaties van elkaar leren en de bereidheid om (gegeneraliseerde) inzichten en conclusies uit incident evaluaties met andere partijen te delen.

- **Collectief herstel** is de mate waarin organisaties samenwerken om te herstellen van een incident met impact op één of meerdere van deze organisaties. De veronderstelling is dat samenwerking bij herstel, i.p.v. individueel/solitair herstel door organisaties, voor sommige incidenten effectiever kan zijn.



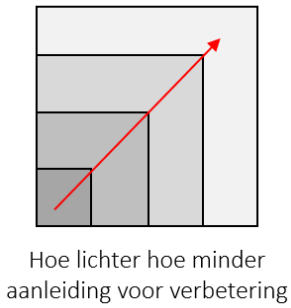
Figuur 6: Herstelvermogen en relaties met andere organisaties.

4 Bevindingen

Het belangrijkste doel van dit onderzoek is het bepalen van de status-quo van herstelvermogen bij relevante organisaties voor het NCSC. Zoals beschreven in hoofdstuk 2 Aanpak, wordt deze status-quo analyse gebaseerd op interviews met 9 verschillende organisaties. In dit hoofdstuk worden de bevindingen o.b.v. deze interviews besproken.

De bevindingen zijn opgesplitst in verschillende onderwerpen. Allereerst zal besproken worden wat de drijfveren voor het inrichten van herstelvermogen zijn volgens de geïnterviewden, in paragraaf 4.1. Vervolgens zal de inrichting van herstelvermogen bij de geïnterviewde organisaties besproken worden in paragraaf 4.2. Vervolgens zullen in de paragrafen 4.3 tot en met 4.5 overige belangrijke aspecten van herstelvermogen worden behandeld, respectievelijk Training en oefening, Afstemming met ketenpartners Collectief herstelvermogen

Bovendien zullen we in dit hoofdstuk, maar ook in hoofdstuk 5 Conclusies en vervolgonderzoek, gebruik maken van spindiagram visualisaties om de stand van zaken bij de geïnterviewde organisaties intuïtief weer te geven. Deze spindiagrammen zullen een overzicht geven van (deel)aspecten van herstelvermogen. Per aspect zal een rode lijn aangeven hoe dit aspect kwalitatief is beoordeeld, waarbij we onderstaande redenatie hanteren:



Figuur 7: Redenatie van de kwalitatieve beoordeling in de spindiagram visualisaties (in volgende paragrafen) van herstelvermogen (deel)aspecten.

De bovenstaande figuur kan geïnterpreteerd worden als de legenda voor de visualisaties in de komende hoofdstukken. In deze visualisaties zijn de (deel)aspecten van herstelvermogen beoordeeld o.b.v. de opgehaalde informatie in interviews. Des te dichter de rode lijn bij het centrum is geplaatst des te meer aanleiding voor verbetering, en dus des te verder de rode lijn verwijdert is van het centrum des te minder aanleiding voor verbetering is ingeschat. Iedere beoordeling van een (deel)aspect is gebaseerd op een gedegen kwalitatieve beoordeling. Hierbij zijn de conclusies gebaseerd op *alle* interviews, meegenomen in de relatieve beoordelingen van de (deel)aspecten. De visualisaties zijn bedoeld om de lezer in één oog opslag inzicht te geven in de relatieve stand van zaken van de (deel)aspecten van herstelvermogen. Ook zal in hoofdstuk 5 Conclusies en vervolgonderzoek een totaal overzicht worden gegeven van de relatieve stand van zaken van alle (deel)aspecten van herstelvermogen. In Appendix 1 – Verantwoording van visualisaties wordt uitgelegd hoe de relatieve beoordelingen van de (deel)aspecten van herstelvermogen tot stand zijn gekomen, en welke conclusies daar aan ten grondslag hebben gelegen.

4.1 Drijfveren herstelvermogen

Elke organisatie zal een bepaalde drijfveer hebben om herstelvermogen in te richten. Alle organisaties geven aan dat het inrichten van herstelvermogen nodig is om:

1. De (markt)positie van de organisatie te waarborgen, bijvoorbeeld omdat de IT-infrastructuur (direct) bijdraagt aan de bedrijfsvoering; en/ of
2. Te voldoen aan wet- en regelgeving.

Uit de interviews komt naar voren dat organisaties die moeten voldoen aan strenge wet- en regelgeving (o.a. financiële instellingen) en organisaties waarbij IT van primair belang is voor de bedrijfsvoering (o.a. de cloud leverancier en telecom) hun herstelvermogen relatief beter op orde hebben. Organisaties die een minder directe relatie kennen tussen IT en bedrijfsvoering lijken minder voorbereid te zijn op incidenten.

Er is hierbij ook een relatie te trekken tussen de drijfveren en het beeld van het hoger management. Uit de interviews blijkt dat er bij organisaties die een minder volwassen inrichting van herstelvermogen hebben, er een cultuur lijkt te heersen dat herstelvermogen een 'ICT-feestje' is, met slechts beperkte commitment vanaf hoger management, en beperkte geldstromen die hiervoor beschikbaar worden gesteld. Dit zorgt ervoor dat bepaalde aspecten (zoals het bepalen van relevante dreigingen en incident-impactbepaling zoals besproken in de komende secties) minder sterk kunnen worden uitgevoerd en/of er minder middelen beschikbaar zijn.

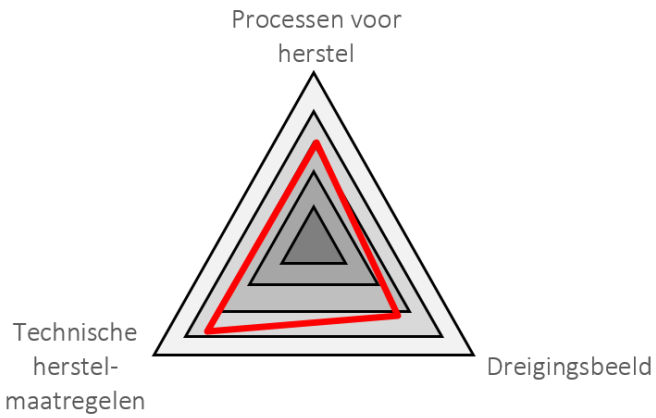
Daarnaast blijkt uit de interviews dat grootschalige incidenten (zoals de ransomware-aanval op de Universiteit van Maastricht) op alle lagen in de organisatie vragen oproept over de inrichting van herstelvermogen en de aandacht vestigen op het algemene belang van goed herstelvermogen, en daardoor de organisatie specifieke inrichting hiervan.

4.2 Herstelvermogen proces

De inrichting van herstelvermogen bij de geïnterviewde organisaties is onderverdeeld aan de hand van de drie fases zoals beschreven in hoofdstuk 3.2.1 Beknopt overzicht herstelactiviteiten: voorbereiden op herstel, herstel-in-uitvoering en leren van uitvoering. De conclusies die getrokken zijn over de inrichting van herstelvermogen op basis van het analyseren van de interviews zijn op een zo logisch mogelijke wijze onderverdeeld onder deze drie fases.

4.2.1 Voorbereiden op herstel

In onderstaande figuur staan de relatieve beoordelingen van de drie deelaspecten van *voorbereiden op herstel* weergegeven. In de komende alinea's worden de conclusies voor deze deelaspecten tekstueel toegelicht.



Figuur 8: Kwalitatieve beoordeling van de drie deelaspecten van Voorbereiden op herstel

4.2.1.1 Dreigingsbeeld en risico-inschatting

Het vaststellen van een dreigingsbeeld (bijvoorbeeld met welke verstoringsscenario's er rekening moet worden gehouden) en het inschatten van de risico's die gepaard gaan met dit beeld zijn nodig om de juiste herstelmaatregelen en processen in te richten.

Uit de interviews komt naar voren dat vrijwel alle organisaties rekening houden met een breed assortiment van types dreigingen, waaronder:

- Fysieke oorzaken, zoals stroomuitval of relevante geografische oorzaken (zoals het potentieel neerstorten van een vliegtuig op een datacenter in de buurt van Schiphol);
- Digitale oorzaken, zoals ransomware/DDoS aanvallen en onbeschikbaarheid van applicaties/internetvoorzieningen; en
- Menselijke oorzaken, zoals grootschalige ziektemelding door het nieuwe coronavirus.

Voor de verschillende dreigingsbeelden worden dreigingsscenario's bepaald. Een geïnterviewde partij met een versnipperd (decentraal) bestuurskarakter geeft aan dat het lastig is om intern de juiste scenario's af te stemmen, omdat de verschillende takken binnen de organisatie elk hun eigen dreigingen kennen. Een andere organisatie met soortgelijke structuur heeft een oplossing gezocht in de vorm van delegatie.

Idealiter worden scenario's periodiek herzien en aangepast aan de huidige stand van zaken. Het blijkt echter dat de meeste organisaties hun scenario's pas herzien wanneer er een (grootschalig) incident plaatsvindt in de eigen organisatie of hierbuiten, zoals de Citrix-crisis of de ransomware aanval bij de Universiteit van Maastricht. Meerdere organisaties komen er bij deze incident-gedreven heroverwegingen achter dat een aantal scenario's achterhaald zijn. Een reden voor deze incident-gedreven aanpak wordt niet door alle organisaties gegeven, maar de beschikbaarheid en toewijzing van middelen aan deze activiteit lijken onderdeel van de oorzaak te zijn.

Als onderdeel van het scenario-schetsen wordt er een inschatting gemaakt van de potentiële impact op de bedrijfsvoering. Er worden verschillende parameters genoemd die hierbij meegewogen worden, gerelateerd aan in hoeverre het een directe impact heeft op

de geboden dienstverlening en in hoeverre het een impact heeft op de onderliggende bedrijfsprocessen. Voor veelvoorkomende incidenten of incidenten waarop geanticipeerd wordt, worden bij de meeste organisaties een prioritering afgeleid. Daarbij vormen de scenario-schetsen het middel om de juiste herstelmaatregelen en processen in te richten.

4.2.1.2 Getroffen technische herstelmaatregelen

De technische herstelmaatregelen gaan over de inrichting van de ICT om een incident zo snel mogelijk het hoofd te kunnen bieden. We onderscheiden hierin maatregelen die 'actief' zijn (zoals een dubbel-ontsloten datacentrum met een active-active inrichting, waarbij er bij uitval van één datacentrum geen directe verstoring voor de bedrijfsvoering is) en maatregelen met een meer passief karakter (zoals het kunnen terugzetten van data back-ups).

Bij elk van de geïnterviewden lijkt het erop dat er goed is nagedacht over de te treffen technische maatregelen. Veelal zijn deze afgestemd op de impact van een verstoring op de bedrijfsvoering en de ingeschatte impact en prioritering. De maatregelen zijn hierbij vooral ingericht op het verhelpen van enkelvoudige verstoringen (denk aan een duaal uitgevoerd datacentrum). De geïnterviewde onderwijsinstelling geeft daarnaast aan dat het versnipperde karakter van de organisatie het lastig maakt om de juiste maatregelen te treffen, omdat het bijvoorbeeld niet duidelijk is welke data er zijn. Dit valt samen met de moeite om de relevante scenario's te schetsen zoals benoemd in de vorige sectie.

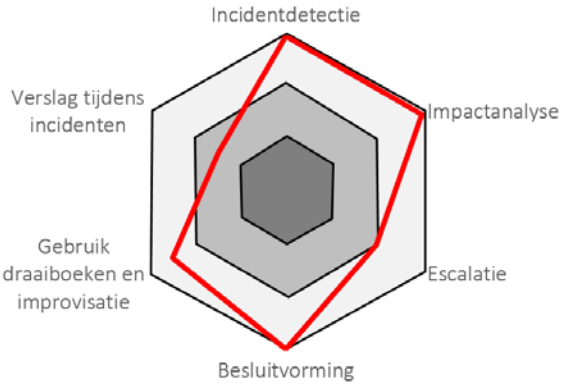
4.2.1.3 Processen voor herstel

Naast het inrichten van technische maatregelen, zijn er ook processen nodig om tijdig en correct te kunnen herstellen. Deze processen, als ook de belegging van verantwoordelijkheden horend bij rollen en individuen, worden voorafgaand aan een incident vastgelegd. Deze paragraaf beschrijft de algehele bevindingen op dit onderwerp; in paragraaf *4.2.2 Herstel-in-uitvoering* wordt er verder ingegaan op specifieke processen en rolverdelingen.

Op het gebied van procesinrichting geven de meeste organisaties aan dat er standaard draaiboeken zijn om bepaalde types incidenten op te lossen. Echter, per organisatie verschillen de herstelplannen wel. Bij organisaties die zelf veel techniek in beheer hebben, zoals de commerciële organisaties die geïnterviewd zijn, zijn de herstelplannen van veel voorkomende incidenten erg uitgebreid en zijn specifieke werkacties opgenomen. Bij organisaties die vooral techniek en digitale diensten afnemen, kan het zijn dat een herstelplan minder uitgebreid is en vooral verwijst naar de leverancier.

Naast processen voor het afhandelen van een incident hebben alle organisaties ook processen voor escalatie (van incident naar crisis) en om de juiste expertise bij elkaar te brengen om een crisis te bestrijden. Er worden meerdere manieren gebruikt om de juiste expertise te vinden. Sommige organisaties houden lijsten bij met wie-waarvoor verantwoordelijk is, waar andere organisaties meer gaan in ad hoc groeperingen op basis van bekende expertise. Wel geven alle organisaties mandaat bij het crisisteam, zodanig dat de crisis prioriteit krijgt in de afhandeling boven de reguliere gang van zaken.

4.2.2 Herstel-in-uitvoering



Figuur 9: Kwalitatieve beoordeling van de zes deelaspecten van Herstel-in-uitvoering

In onderstaande paragrafen worden alle belangrijke deelactiviteiten van herstel-in-uitvoering behandeld.

4.2.2.1 Incidentdetectie

Bij alle organisaties blijken er passende mechanismen aanwezig te zijn om incidenten in kaart te brengen. Het is mogelijk om te observeren aan de hand van technische en handmatige metingen of meldingen van meetsystemen, klanteninput en input van eigen personeel.
Bij de meeste organisaties lijkt de incidentmelding terecht te komen bij de juiste persoon, bijvoorbeeld door vast te leggen per IT-component wie daarvoor benaderd kan worden bij problemen.

4.2.2.2 Impactanalyse

Bij vrijwel alle organisaties blijken er passende mechanismen aanwezig te zijn om de impact (scope en effect) van een incident te bepalen en op waarde te schatten. De meeste organisaties geven aan dat de impact van een incident veelal wordt bepaald door de kritikaliteit van de asset die is geraakt. De kritikaliteit komt daarbij voort uit een kritikaliteitsanalyse die al in de voorbereidingsfase wordt gemaakt. Zo kan het zijn dat de impactinschatting de ‘crisiscode’ bepaalt aan de hand waarvan een crisisteam wordt ingericht, er geëscaleerd wordt of er externen worden betrokken. De impactanalyse kan ook leidend zijn bij de prioritering van herstel. De organisaties hanteren de uitkomst van de impactanalyse consistent over alle herstelfasen heen, vanaf bij het bekend worden van het incident tot aan de implementatie van uit een incident geleerde lessen.

Bij veel organisaties wordt er een scheiding gemaakt van taken. De technici kijken naar wat technisch geraakt is en de medewerkers op business niveau controleren de vooraf geschatte impactbepaling in de praktijk, en zorgen voor communicatie (intern en extern). Voor de technische impactanalyse scoren de meeste organisaties volgens een standaardlijst (gerelateerd aan ITIL impact scores). In een aantal interviews werd gemeld dat de impactanalyse parallel wordt uitgevoerd aan de root cause analysis.

4.2.2.3 Escalatie

Bij sommige organisaties zijn van tevoren de verschillende escalatiestappen omschreven. De meeste organisaties geven aan dat in de beslissing om te escaleren ook de incidentscope en effect meegenomen worden. Een aantal organisaties geven aan dat escalatie soms automatisch gebeurt, bijvoorbeeld als een klein incident vaker voorkomt,

andere organisaties geven aan dat escalatie door een persoon, zoals een calamiteitenmanager, met bijbehorend mandaat gedaan kan worden.

Eén organisatie heeft een expliciete escalatiedesk, die in geval van incident verantwoordelijk is voor in- en opschaling en regie voert voor administratieve zaken als logging en documentatie.

4.2.2.4 Besluitvorming

De meeste organisaties geven aan dat de wijze waarop besluiten worden genomen, afhankelijk is van het type incident. Als er namelijk een klein, technisch incident is, kan dat door de technici opgelost worden. Hoe dit besloten is, is niet in de interviews zelf naar voren gebracht. Verschillende organisaties geven aan een gestandaardiseerde besluitvorming methode te gebruiken, waarbij de BOB(OC) methode (Beeldvorming, Oordeelsvorming, Besluitvorming, Opdracht, Controle) vaak genoemd worden.

De organisaties die technische diensten leveren, of zelf verantwoordelijk zijn voor hun technische inrichting, voeren veelal het herstel van kleine technische incidenten onmiddellijk zelf uit, volgens vooropgesteld herstelplan. Is het incident groter, met grotere gevolgen voor bedrijfsvoering, dan worden beslissingen bij bijna alle organisaties door hoger management genomen, of door bijvoorbeeld een zogenaamde calamiteiten- of crisismanager, veelal geadviseerd door de betrokken technici. Bij organisaties die zelf minder techniek in beheer hebben en een klein technisch team hebben, of voornamelijk afnemer zijn van techniek, worden beslissingen over herstel ook genomen door hoger management, of een eerder genoemde calamiteiten- of crisismanager. Een uitzondering hierop zijn de zogenoemde managerloze organisaties. Deze organisaties vertrouwen op kennis en kunde van de experts, die dan ook bevoegd zijn voor het nemen van beslissingen.

4.2.2.5 Gebruik van draaiboeken in de praktijk en improvisatie

Bijna alle geïnterviewde organisaties geven aan dat er gebruik wordt gemaakt van vooraf opgestelde herstelplannen, zoals eerder besproken in paragraaf 4.2.1.3. Ook geven partijen aan dat het herstel van kleine technische incidenten geautomatiseerd mogelijk is. Dit voorkomt dan ‘ongecontroleerde IT-aanpassingen’.

Op het moment dat een draaiboek onvoldoende toereikend is, geven alle organisaties aan dat er ruimte is voor improvisatie. De mate van improvisatie hangt hierbij samen met hoe goed een herstelplan vooraf opgesteld is. Eén organisatie geeft aan dat herstelplannen niet of nauwelijks toereikend zijn, hierdoor is improvisatie voor hen zelfs essentieel.

Daarnaast geven alle organisaties aan dat improvisatie essentieel is voor onverwachte incidenten met grote impact. Er is dan ook ruimte voor improvisatie, bijvoorbeeld door experts. Dit maakt het ook mogelijk om af te wijken van vooraf opgestelde herstelplannen, als duidelijk is dat dit essentieel is voor herstel.

4.2.2.6 Verslaglegging tijdens incidenten

De meeste partijen geven aan dat er procedures zijn voor verslaglegging of logging, van zowel incident, besluitvorming, als herstelhandelingen. De eerder genoemde BOB-methode als handvat voor besluitvorming wordt ook door diverse organisaties gebruikt als methode voor logging.
Wat niet duidelijk bleek uit de interviews, is de kwaliteit van de logging. Of er bijvoorbeeld altijd uitgebreide logging plaatsvindt tijdens een incident of crisis, of dat alleen kort de besluitvorming vastgelegd wordt is niet duidelijk. Ondanks dat dit een belangrijke bron kan zijn om uit te putten bij het leren van de uitvoering.

4.2.2.7 Verhoogde dijkbewaking na herstel

Een enkele organisatie meldt dat er na uitvoering van herstelacties een periode ingegaan wordt, meestal van enkele uren, van verhoogde dijkbewaking. Dit wordt ingevuld door extra controles, voordat de evaluatiefase start.

4.2.2.8 Acuut en duurzaam herstel

Veel organisaties geven aan dat er onderscheid gemaakt wordt tussen korte termijn, dus instant herstel, en volledig herstel. Dit zijn vooral de geïnterviewde partijen die zelf veel IT in beheer hebben. Deze organisaties focussen zich dan eerst op het veilig en werkbaar maken van de functionaliteit, en daarna wordt de functionaliteit volledig hersteld, bijvoorbeeld door een re-roll inrichting of patchmanagement. Een aantal organisaties geven hierbij aan dat dit mede afhankelijk is van de prioritering op basis van impactanalyse en verwachte duur van herstel.
Dit onderscheid wordt in mindere mate gemaakt bij organisaties die veel van hun IT-services hebben uitbesteed. In dat geval worden soms afspraken gemaakt met leveranciers over welk type herstel acceptabel is voor welke systemen.

4.2.3 Leren van uitvoering

Figuur 10: Kwalitatieve beoordeling van de twee deelaspecten van Leren van uitvoering

4.2.3.1 Evaluatie incident en herstel

Post-mortum incidentevaluatie is een belangrijk element van continue verbetering van crisis management en herstelvermogen: “never waste a good crisis”. Alle geïnterviewde organisaties geven aan dat zij incidentevaluaties uitvoeren. Voor sommige organisaties hangt het uitvoeren van de evaluatie, en de mate van diepgang van de evaluatie, af van de ernst van het incident. Ook geeft bijna de helft van de organisaties aan dat evaluaties niet altijd gedaan worden als gevolg van een combinatie van prioriteitstelling en beperkte bemensing. Commerciële organisaties geven daarentegen aan dat ze grondige evaluatie uitvoeren van ernstige incidenten om de continuïteit van hun dienstverlening te verbeteren. Zowel door sommige commerciële als niet-commerciële organisaties wordt bij de uitvoering van de evaluatie wel eens een externe organisatie betrokken, afhankelijk van de ernst en de toedracht van het incident.

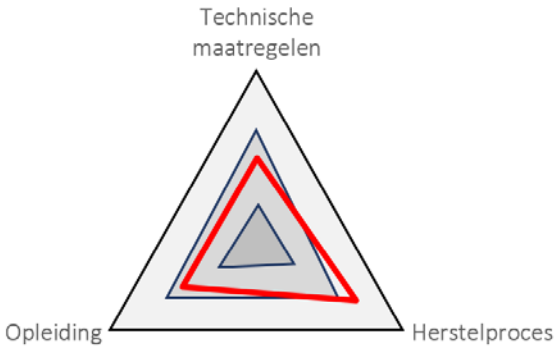
In de meeste incidentevaluaties is het vaststellen van de oorzaak van het falen van de IT een vaststaand onderdeel. Daarnaast besteden veel organisaties ook aandacht aan evaluatie van de crisis management procedure en de communicatie tijdens het proces.

4.2.3.2 Lessons learned en lessons implemented

Afhankelijk van de inzichten uit de incidentevaluaties worden deze inzichten gerapporteerd aan relevante betrokkenen binnen de organisatie. Bijvoorbeeld, technische oorzaken van een IT-incident of kwetsbaarheden in de IT-architectuur die bij een incidentevaluatie naar voren komen, worden gerapporteerd en afgehandeld door de IT-afdeling. Bij incidenten die

grotere impact op de bedrijfsvoering hebben gehad, zijn meer afdelingen betrokken en wordt ook gerapporteerd aan hoger management. Bij het implementeren van geïdentificeerde verbeteringen geven organisaties aan dat er kosten / baten afwegingen worden gemaakt.

4.3 Training en oefening



Figuur 11: Kwalitatieve beoordeling van de drie deelaspecten van Training en oefening

In geen enkel interview is aangegeven dat er onvoldoende kennis of resources beschikbaar waren om een IT-incident op te lossen, noch dat er aanleiding was om te concluderen dat er onvoldoende aandacht is geweest voor opleiding of training van crisisbeheersingspersoneel. In de meeste gevallen wordt training van kennis en vaardigheden ten aanzien van herstelvermogen gezien als onderdeel van oefeningen of training-on-the-job. Slechts twee organisaties geven aan dat zij een expliciet crisismanagement training & opleiding programma aanbieden aan hun medewerkers.

Naast het opleiden en trainen van personeel is het beproeven van de eigen herstelvermogen inrichting, ofwel oefenen, van belang. Oefenen kan o.b.v. de opgehaalde informatie in de interviews logischerwijs opgedeeld worden in het beproeven en verbeteren van 1) technische maatregelen en 2) het herstelproces zelf. In onderstaande paragrafen worden beide aspecten van *oefenen* besproken.

4.3.1 Technische maatregelen beproeven

Alle partijen voeren testen uit met technische maatregelen tegen IT uitval, zoals redundantie maatregelen, data back-ups en het gecontroleerd uitwijken van applicaties tussen data centers. Deze testen betreffen relatief kleinschalige, simpele oefeningen van eenvoudige maatregelen.

Er is bij alle partijen terughoudendheid om meer risicovolle oefeningen uit te voeren in verband met de lastig te voorspellen impact op bedrijfsprocessen. Bijvoorbeeld, testen van de noodstroomvoorziening van een data center, door de primaire stroombron uit te schakelen, worden niet gedaan. Ook noemt een aantal organisaties voorbeelden van testen die niet gedaan worden omdat deze de stabiliteit van externe IT-diensten (van klanten of zakelijke partners) in gevaar kunnen brengen. De terughoudendheid hierbij is begrijpelijk, maar geeft ook de grens aan van de praktische haalbaarheid van oefeningen van het technisch herstelvermogen. De mogelijkheid om complexere technische herstelvoorzieningen te testen is daardoor beperkt.

4.3.2 Herstelproces beproeven

De meeste organisaties geven aan dat er geoefend wordt op crisis- en herstelmanagement, wat verder gaat dan het testen van technische maatregelen. Hierbij wordt bijvoorbeeld geoefend op bekendheid met crisis procedures, rol- en taakverdeling en communicatie, zowel binnen het crisisteam als extern, met leveranciers en klanten. Afhankelijk van de doelstelling van de oefening worden diverse voorbeelden van oefenvormen genoemd, zoals scenario-gebaseerde simulatie, een red-team cyber oefening of een table-top waarin herstelplannen geëvalueerd worden.

Het opstellen van realistische oefenscenario's is niet triviaal en enkele organisaties geven aan dat niet elke oefening daarom succesvol is. Om goed invulling te geven aan crisisoefeningen betrekt een aantal organisaties, waaronder alle geïnterviewden uit de vitale infrastructuur, ook regelmatig externe partijen bij het opstellen van oefeningen en trainingen.

4.4 Afstemming met ketenpartners

Herstelvermogen vergt ook afstemming met ketenpartners, zoals leveranciers en afnemers. Eén van de geïnterviewden geeft expliciet aan dat er tijdens de inkoop van diensten al rekening wordt gehouden met eisen rondom herstelvermogen en dat deze worden vastgelegd in de SLA met hun IT-leverancier. Bij een andere organisatie waarbij de bedrijfsvoering intern is ingericht in diverse takken, worden die andere delen van de organisatie ook gezien als 'ketenpartner'. Vanuit dat oogpunt worden ook afspraken gemaakt wat de eisen zijn rondom herstelvermogen, dit wordt dan ook besproken in een centraal overleg.

In een ander interview werd aangegeven dat er ook geoefend wordt op crisis management en herstel met klanten en/of met leveranciers. Bij de oefeningen met leveranciers betreft het niet de grote IT of cloud dienstverleners, maar de kleinere, meer specialistische IT-leveranciers. Hierbij werd aangegeven dat de toezichthouder ook sterk aanmoedigt om oefeningen samen met ketenpartners uit te voeren.

4.5 Collectief herstelvermogen

Collectief herstelvermogen is op basis van de interviews onder te verdelen in een tweetal onderdelen: collectief leervermogen en collectief herstel.

Collectief leervermogen is de behoefte om van elkaar te leren en de bereidheid om (gegeneraliseerde) inzichten en conclusies uit incident evaluaties met andere partijen te delen. Sommige geïnterviewden geven aan dat deze behoefte bestaat. Onder kennisinstellingen blijkt de gemeenschappelijke aansluiting via SURF een positieve rol te spelen ten aanzien van informatiedeling. Andere organisaties geven aan dat verschillende belangen van organisaties in de keten (zoals klant versus leverancier of commerciële concurrenten) een belemmering kunnen vormen voor het delen van details over de toedracht van een crisis.

Van collectief herstel werden in de interviews geen praktische voorbeelden genoemd. Wel is in de gesprekken met de organisaties die vallen onder vitale infrastructuur, genoemd dat er afspraken worden gemaakt met toezichthouders hierover. Ook denken deze organisaties zelf na over gebruik van gezamenlijke IT-voorzieningen voor sectorpartners in geval van calamiteiten. Op dit vlak wordt ruimte voor verbetering gezien, maar ook wordt

aangegeven dat collectieve herstelvoorzieningen juridische complicaties kan opleveren (bijvoorbeeld aansprakelijkheid).

5 Conclusies en vervolgonderzoek

In dit hoofdstuk worden de conclusies van het verkennend onderzoek uiteengezet. Ook wordt de ambitie voor vervolgonderzoek besproken.

5.1 Algemene conclusies

Het blijkt dat herstelvermogen bij alle geïnterviewde organisaties is ingeregeld in de vorm van een samenvoeging / integratie van Business Continuity Management (BCM) en Cyber Security. Daarbij lijkt het erop dat de Business Continuity Management aspecten van herstelvermogen al voor langere tijd worden opgepakt, volgens een klassiekere benadering, en zijn de Cyber Security aspecten van herstelvermogen daar later aan toegevoegd.

Een belangrijke indicator voor goed ingericht herstelvermogen is awareness en commitment bij management. Als deze ontbreekt, zijn er onvoldoende mensen en middelen om herstelvermogen in de breedte op te kunnen pakken. Belangrijke drijfveren voor het management zijn het directe belang van IT voor business continuity (je wilt herstellen om primaire bedrijfsprocessen terug te zetten) en wetgeving (je moet herstellen om aan wet- en regelgeving te voldoen).

De getroffen herstelmaatregelen hangen sterk af van het IT-profiel van de organisatie. Zo lijkt de positie van de organisatie in de IT-dienstketen, en of de gebruikte IT wordt gekocht/afgenomen/ontwikkelt door de organisatie zelf, veel invloed te hebben op de getroffen herstelmaatregelen. Vooral bij organisaties waarbij het primaire bedrijfsbelang sterk afhangt van IT-continuïteit worden vergaande herstelmaatregelen getroffen.

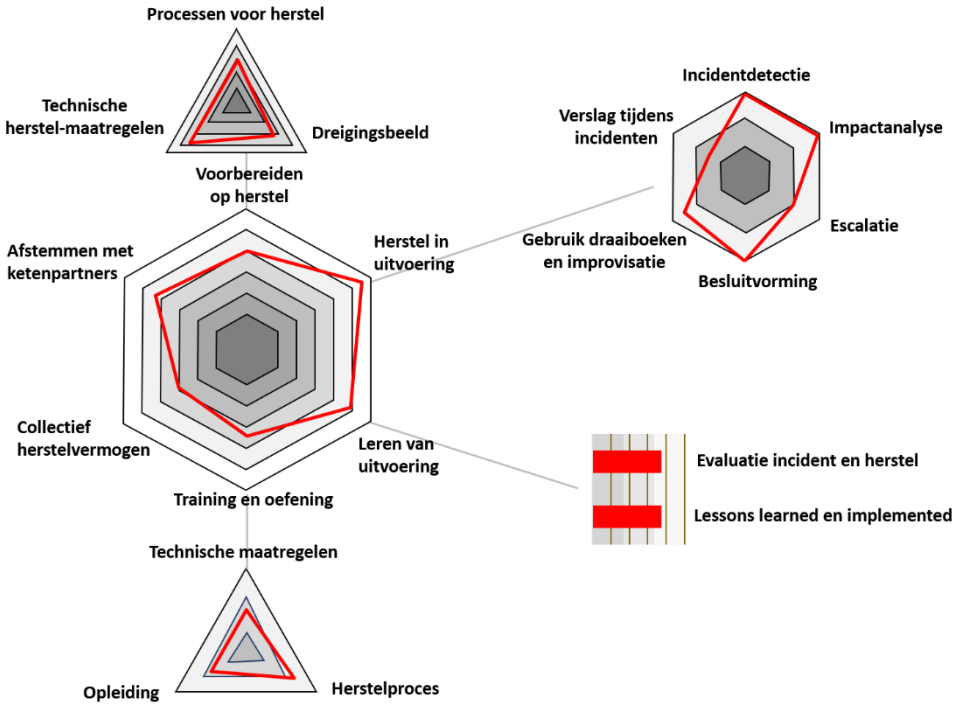
Bovendien wordt de awareness bij het management ook beïnvloed door recente (grote) incidenten bij eigen of vergelijkbare organisaties. De ransomware aanval op Universiteit Maastricht leidde tot vragen bij het management van diverse organisaties: “kan dit ook bij ons gebeuren?”

Alle geïnterviewde partijen bereiden zich voor op herstel door training en oefening. Het herstelproces wordt vooral geoefend door middel van het uitvoeren van herstel op (nep-)incidenten. Daarnaast wordt er getraind op de communicatie tussen stakeholders (bijvoorbeeld d.m.v. table-top exercises), en wordt het herstel van technische componenten (regelmatig) getest. De genoemde redenen om te oefenen, trainen en testen zijn het verbeteren van de inrichting van herstelvermogen, maar ook compliance en wetgeving.

Ook blijkt er uit de interviews dat een aantal belangrijke aspecten van herstelvermogen verbeterd kunnen worden. Deze worden hieronder in meer detail besproken.

5.1.1 Ruimte voor verbetering

In onderstaande spindiagram zijn de belangrijkste aspecten, zoals behandeld in dit rapport, weergegeven. Ook geven de scores van deze (deel)aspecten aan in hoeverre er ruimte voor verbetering mogelijk lijkt te zijn.



Figuur 12: Kwalitatieve beoordeling van alle (deel)aspecten van herstelvermogen

Ondanks dat voor veel aspecten van herstelvermogen geldt dat de inrichting adequaat lijkt te zijn ingeregeld, wordt in het bovenstaande spindiagram in één oog opslag duidelijk voor welke aspecten van herstelvermogen er relatief de meeste ruimte voor verbetering lijkt te zijn. Dit betekent natuurlijk niet dat de punten die op dit moment goed zijn ingericht, nu op pauze gezet kunnen worden. In de volgende alinea's worden de aspecten met meeste ruimte voor verbetering (nogmaals) kort toegelicht.

Bij het voorbereiden op herstel is het belangrijk dat incidentscenario's worden bepaald en periodiek worden bijgesteld. Uit de interviews blijkt echter dat de meeste organisaties deze scenario's pas herzien en bijstellen wanneer 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 incident-gedreven aanpak is een gebrek aan toegewezen tijd en middelen om deze activiteit periodiek uit te voeren.

Op het gebied van training en oefening biedt vooral het beproeven van de inrichting van technische maatregelen ruimte voor verbetering. Namelijk, eenvoudige technische maatregelen worden wel degelijk geoefend, soms ook on-the-job, maar er is terughoudendheid om risicovolle technische oefeningen uit te voeren, vanwege de lastig te voorspellen impact op de bedrijfsuitvoering. De mogelijkheid om complexere technische herstelvoorzieningen te testen is daardoor beperkt.

Op het gebied van collectief herstelvermogen zijn geen praktische voorbeelden naar voren gekomen in de interviews. Vooral bij de vitale infrastructuur organisaties wordt hier al wel over nagedacht, bijvoorbeeld over de inrichting van gezamenlijke IT-voorzieningen voor

sectorpartners in geval van calamiteiten. Dit levert dan wel weer juridische complicaties op, zoals onduidelijkheid over aansprakelijkheid.

5.1.2 Conclusies met mogelijke vervolgstappen voor het NCSC

Hieronder worden de conclusies besproken die relevant zijn voor het NCSC om vervolgstappen op te ondernemen. Suggesties voor mogelijke vervolgstappen worden niet bij alle conclusies besproken, omdat daar onvoldoende informatie is opgehaald om een weloverwegen advies over te geven.

Informatiedeling over incidenten, dreigingsbeelden en herstelvermogen wordt op prijs gesteld en vaak al in enige vorm gedaan tussen gelijkgestemde organisaties. Ook het NCSC wordt daarbij regelmatig genoemd.

Aandacht voor het periodiek bijstellen van incidentscenario's is belangrijk omdat uit de interviews is gebleken dat de meeste organisaties incidentscenario's pas herzien en bijstellen wanneer er een (grootschalig) incident plaatsvindt in de eigen organisatie of daarbuiten.

Een aantal organisaties maakt afspraken rondom herstelvermogen voor processen binnen een keten. Risico- en dreigingsprofielen opgesteld door organisaties zijn divers / weinig uniform, wat keten-risico-denken lastig maakt. Aan de andere kant is er ook een zekere huiver om de ketenpartners een spreekwoordelijk kijkje in de keuken te geven.

Daarnaast kan het oefenen van realistische grootschalige incidenten het herstelvermogen van organisaties mogelijkerwijs verbeteren. Namelijk, eenvoudige technische maatregelen worden wel degelijk geoefend, soms ook on-the-job, maar er is terughoudendheid om risicovolle technische oefeningen uit te voeren, vanwege de lastig te voorspellen impact op de bedrijfsuitvoering. De mogelijkheid om complexere technische herstelvoorzieningen te testen is daardoor beperkt.

Ook het concretiseren van collectief herstelvermogen kan bijdragen aan de verbetering van herstelvermogen. In de interviews zijn wel voorbeelden naar voren gekomen van informatiedeling, maar geen praktische voorbeelden genoemd van gezamenlijk optrekken richting herstel. Vooral bij de vitale infrastructuur organisaties wordt hier al wel over nagedacht, bijvoorbeeld over de inrichting van gezamenlijke IT-voorzieningen voor sectorpartners in geval van calamiteiten. Dit levert dan wel weer juridische complicaties op, zoals onduidelijkheid over aansprakelijkheid.

Bovendien bieden sommige conclusies handelingsperspectief voor het NCSC. Namelijk, beïnvloeding van de awareness en commitment bij het management van organisaties kan leiden tot de verbetering van herstelvermogen. De volgende twee conclusies zijn hiervoor relevant:

- nieuws is een belangrijke drijfveer voor het herzien van de eigen inrichting van herstelvermogen; en
- wet- en regelgeving is een belangrijke drijfveer voor het inrichten of verbeteren van herstelvermogen.

Nieuws blijkt een belangrijke drijfveer voor het herzien van de eigen inrichting van herstelvermogen. Niet alleen recente incidenten bij de eigen organisatie leiden tot bewustwording, maar ook incidenten bij andere organisaties die via de media binnenkomen

kunnen inzichten creëren. Dergelijke incidenten beïnvloeden de perceptie over de kans op een incident. Deze perceptie is door NCSC beïnvloedbaar, bijvoorbeeld door bepaalde incidenten specifiek uit te lichten via gepubliceerde dreigingsbeeld en/of via de media.

Wettelijke regelgeving is door een aantal organisaties genoemd als belangrijke drijfveer voor het inrichten van herstel maatregelen. Voor het NCSC biedt dit handelingsperspectief om herstelvermogen te beïnvloeden in gereguleerde sectoren via toezichthouders.

5.2 Ambities voor vervolgonderzoek

In dit hoofdstuk worden de ambities voor vervolgonderzoek besproken en beargumenteerd.

De bevindingen en conclusies in dit rapport zijn grotendeels gebaseerd op een negental interviews. Ondanks dat dit in een verkennende fase van dit onderzoek heel veel nuttige informatie heeft opgeleverd, kan de kleine omvang van deze steekproef als beperking worden beschouwd. Om deze mogelijke tekortkoming te adresseren zal in vervolgonderzoek de steekproef worden vergroot, met als voorstel om de informatie op te halen in de vorm van een self-assessment.

De onderverdeling van herstelvermogen in (deel)aspecten en kwalitatieve beoordeling van deze aspecten, zoals weergeven in het spindiagram in Figuur 12, biedt een goede voedingsbodem voor het ontwerpen van een self-assessment. Namelijk, leent het kwalitatieve beoordelingssysteem onderliggend aan deze spindiagram een goede basis om verder uit te werken specifiek voor een self-assessment. Het verder uitwerken van een self-assessment is daarom één van de taken die in het vervolg van dit onderzoek worden opgepakt. Het idee is dat organisaties zichzelf kunnen beoordelen op de belangrijkste aspecten van herstelvermogen zoals geïdentificeerd in dit onderzoek.

Een self-assessment kan veel leerzame inzichten opleveren voor organisaties. Bijvoorbeeld is het interessant als organisaties zichzelf kunnen meten met andere, idealiter soortgelijke, organisaties (zoals sector partners). Daarnaast is het interessant om in dit self-assessment een adviserende component op te nemen, zodat partijen die zichzelf minder adequaat scoren op een (deel)aspect van herstelvermogen, ook handvatten toegereikt krijgen over hoe dit verbeterd zou kunnen worden. Deze adviezen/handvatten kunnen zowel gebaseerd zijn op tips en adviezen van andere organisaties, als op documentatie (standaarden, best-practice guides, etc.).

In 2020 is er gefocust op de inrichting van herstelvermogen specifiek voor IT-infrastructuren. In het vervolg van dit onderzoek zal ook gekeken worden naar hoe herstelvermogen wordt opgepakt voor OT-infrastructuren. Voor het NCSC is dit relevant omdat veel vitale infrastructuur organisaties OT-infrastructuren beheren. Het vermoeden is wel dat de OT-infrastructuren van verschillende organisaties over het algemeen in mindere mate uniform zullen zijn dan de IT-infrastructuren bij verschillende organisaties. Daarnaast wordt verwacht dat Cyber Security een onderbelicht thema is binnen herstelvermogen voor OT-infrastructuren. Het is daarom interessant om inzicht te krijgen in hoeverre organisaties hierbij innovatievere herstelvermogen activiteiten uitvoeren, bijvoorbeeld op basis van het vakgebied digitale weerbaarheid.

6 Appendix 1 – Verantwoording van visualisaties

In hoofdstuk 4 Bevindingen en hoofdstuk 5 Conclusies en vervolgonderzoek is gebruikt gemaakt van visualisaties om de relatieve stand van zaken van de (deel)aspecten van herstelvermogen intuïtief in kaart te brengen. In deze appendix wordt uitgelegd welke conclusies de grondslag zijn geweest voor deze relatieve beoordeling van de (deel)aspecten.

Hoofdaspect	**Deelaspect**	**Kwalitatieve beoordeling van stand van zaken**	**Conclusies o.b.v. alle interviews (positief, negatief of neutraal beoordeeld)**
Voorbereiden op herstel	Dreigingsbeeld en risico-inschatting	2/4	+ Vrijwel alle organisaties houden rekening met een breed assortiment van types dreigingen + Scenario-schetsen [vormen] het middel om de juiste herstelmaatregelen en processen in te richten - Lastig om [..] de juiste scenario's af te stemmen - Meeste organisaties [herzien] hun scenario's pas wanneer er een (grootschalig) incident plaatsvindt
	Technische herstelmaatregelen	2/3	+ [Er is] goed [] nagedacht over de te treffen technische maatregelen +/- Ingericht op [slechts] het verhelpen van enkelvoudige verstoringen +/- Lastig om de juiste maatregelen te treffen [i.v.m.] moeite om de relevante scenario's te schetsen
	Processen voor herstel	2/3	+ Meeste organisaties [werken met] [..] standaard [herstel] draaiboeken - Per organisatie verschillen de herstelplannen wel + Alle organisaties [hebben] ook processen voor escalatie en [crisisbestrijding]

Herstel-in-uitvoering	Incidentdetectie	2/2	+ Bij alle organisaties blijken er passende mechanismen aanwezig te zijn om incidenten in kaart te brengen + “Bij de meeste organisaties lijkt de incidentmelding terecht te komen bij de juiste persoon”
	Impactanalyse	3/3	+ Bij vrijwel alle organisaties blijken er passende mechanismen aanwezig te zijn om de impact (scope en effect) van een incident te bepalen en op waarde te schatten *+ De impact is bij de meeste organisaties gescoord volgens een standaardlijst (gerelateerd aan ITIL impact scores).* *+ De organisaties hanteren de uitkomst van de impactanalyse consistent over alle herstelfasen heen, vanaf bij het bekend worden van het incident tot aan de implementatie van uit een incident geleerde lessen.*
	Escalatie	2/3	+/- Bij sommige organisaties zijn van tevoren de verschillende escalatiestappen omschreven (geen standaard) +/- Eén organisatie heeft een expliciete escalatiedesk (een “+” voor deze organisatie, maar een “-“ voor de overige + De meeste organisaties geven dat in de beslissing om te escaleren ook de incidentscope en effect meegenomen worden.
	Besluitvorming	2/2	+ Klein, technisch incident [wordt] door de technici opgelost. [..] is het incident groter [..] dan worden beslissingen bij bijna alle organisaties door hoger management genomen. + Verschillende organisaties geven aan een gestandaardiseerde besluitvorming methode te gebruiken, waarbij de BOB(OC) methode (Beeldvorming, Oordeelsvorming, Besluitvorming, Opdracht, Controle) vaak genoemd worden.
	Gebruik draaiboeken en improvisatie	2,5/3	+/- Bijna alle geïnterviewde organisaties geven aan dat er gebruik wordt gemaakt van vooraf opgestelde herstelplannen. Eén organisatie geeft aan dat herstelplannen niet of nauwelijks toereikend zijn.

			+ [Als] een draaiboek onvoldoende toereikend is [i.v.m. een onvoorzien incident], geven alle organisaties aan dat er ruimte is voor improvisatie +/- Ook geven partijen aan dat het herstel van kleine technische incidenten geautomatiseerd mogelijk is. Dit voorkomt dan 'ongecontroleerde IT-aanpassingen'.
	Verslaglegging tijdens incidenten	1/2	+/- De meeste partijen geven aan dat er procedures zijn voor verslaglegging of logging, van zowel incident, besluitvorming, als herstelhandelingen. +/- Wat niet duidelijk bleek uit de interviews, is de kwaliteit van de logging
Leren van uitvoering	Evaluatie incident en herstel	3/4	+ Alle geïnterviewde organisaties geven aan dat zij incidentevaluaties uitvoeren + door sommige [..] organisaties wordt bij de uitvoering van de evaluatie wel eens een externe organisatie betrokken + "In de meeste incidentevaluaties is [..] IT een vaststaand onderdeel. [..] veel organisaties [besteden] ook aandacht aan evaluatie van de crisis management procedure en de communicatie tijdens het proces." - Ongeveer de helft van de organisaties geven aan dat evaluaties niet altijd gedaan worden als gevolg van een combinatie van prioriteitstelling en beperkte bemensing.
	Lessons learned en lessons implemented	1.5/2	+ [..] inzichten uit de incidentevaluaties worden [..] gerapporteerd aan relevante betrokkenen binnen de organisatie. +/- Bij het implementeren van geïdentificeerde verbeteringen [worden] kosten / baten afwegingen worden gemaakt

Training en opleiding	Opleiding	1/2	+ In geen enkel interview is aangegeven dat er onvoldoende kennis of resources beschikbaar waren, [noch] onvoldoende aandacht is geweest voor opleiding of training - Slechts twee organisaties geven aan dat zij een [..] training & opleiding programma aanbieden aan hun medewerkers
	Technische maatregelen testen	1/2	+ Alle partijen voeren testen uit met technische maatregelen tegen IT uitval - Alle partijen [zijn] terughoudendheid om meer risicovolle oefeningen uit te voeren
	Herstelproces beproeven	2/3	+ Meeste organisaties geven aan dat er geoefend wordt op crisis- en herstelmanagement + [Er wordt] geoefend op bekendheid met crisis procedures, rol- en taakverdeling en communicatie [..] [en via] diverse [..] oefenvormen - Enkele organisaties geven aan dat niet elke oefening [..] succesvol is
Afstemming met ketenpartners		2/3	+ eisen rondom herstelvermogen [..] worden vastgelegd in de SLA met hun IT-leverancier [en] andere delen van de organisatie [..] als 'ketenpartner' + er [wordt] ook geoefend [..] op crisis management en herstel met klanten en/of met leveranciers. - [bij] oefeningen met leveranciers betreft het niet de grote IT of cloud dienstverleners
Collectief herstelvermogen		2/4	+ Onder kennisinstellingen blijkt [..] SURF een positieve rol te spelen ten aanzien van informatiedeling - verschillende belangen van organisaties in de keten [..] [kunnen] een belemmering vormen voor het delen van [..] de toedracht van een crisis + [] organisaties die vallen onder vitale infrastructuur, [noemen] dat er afspraken worden gemaakt met toezichthouders [over collectief herstel], en denken deze organisaties zelf na over gebruik van gezamenlijke IT-voorzieningen voor sectorpartners [] - "[Voor] collectief herstel wordt ruimte voor verbetering gezien, maar ook [..] juridische complicaties"

Tabel 1: Verantwoording van kwalitatieve beoordeling van (deel)aspecten.