



Handreiking weerbaarheid: 'Ondernemen is vooruitdenken'

Praktische handvatten voor ondernemers, bedrijven en
brancheorganisaties om hun weerbaarheid te versterken

V N O N C W

MKB
Nederland

Inhoudsopgave

| | |
|--|----|
| Inleiding | 5 |
| Leeswijzer | 8 |
| De basis: Wat zijn de kroonjuwelen van jouw bedrijf? | 12 |
| STAP 1. Vooruitdenken; hoe bescherm ik mijn kroonjuwelen? | 14 |
| STAP 2. Voorkomen is beter dan genezen; voorzorgsmaatregelen nemen | 24 |
| STAP 3. Bereid je voor; werk de belangrijkste voorbereiding uit, test en oefen waar mogelijk | 30 |
| STAP 4. Reageer beheerst en alert; weet wat je te doen staat | 36 |
| STAP 5. Herstel en doorontwikkeling | 41 |
| Afsluiting | 44 |
| Literatuurlijst van geraadpleegde bronnen | 45 |
| Bijlage 1 – Voorstelbare scenario's | 48 |
| Bijlage 2 - Test jouw weerbaarheid | 52 |
| Colofon | 54 |

Inleiding

'Jouw bedrijf is alles voor je, en dan opeens werkt niets meer. Plotseling valt het internet uit, zit je in het donker, de betaalautomaat doet het niet meer, leveranciers zijn onbereikbaar en klanten staan voor een gesloten (digitale) deur.' Je denkt: 'Wat gebeurt er nu? Wat moet ik doen? Hoe lang kan mijn bedrijf dit volhouden? Hoe bereik ik mijn familie, klanten en leveranciers?' Op dit soort situaties wil je zo goed mogelijk zijn voorbereid. Deze handreiking helpt je daarbij.



De internationale veiligheid is de afgelopen jaren snel verslechterd. De Nationaal Coördinator Terrorismebestrijding en Veiligheid stelt in de Denk vooruit-campagne: 'Het is niet de vraag óf we te maken krijgen met grote verstoringen in de samenleving, maar wanneer.'¹ Zowel burgers als bedrijven moeten weerbaar zijn en zich voorbereiden op noodscenario's. De overheid heeft voor bedrijven de volgende drie scenario's centraal gesteld:

- Uitval van internet en telefonie (72 uur of langer),
- Uitval van elektriciteit (72 uur of langer), en
- Een situatie waarbij Nederland betrokken raakt bij een militair conflict.

Weerbaarheid is het vermogen van een organisatie zich voor te bereiden op verstoringen, de gevolgen ervan te beperken en effectief ('veerkrachtig') te reageren en herstellen. Deze handreiking helpt jouw bedrijf én jezelf weerbaarder te maken.

Daarnaast speel je als ondernemer ook een belangrijke rol bij het weerbaarder maken van de samenleving. Misschien voorzie je in primaire levensbehoeften, lever je diensten aan vitale processen, enzovoort. Kortom: jouw voorbereiding beschermt niet alleen jouw eigen onderneming, jezelf en jouw personeel, maar ondersteunt ook klanten, leveranciers en de samenleving. Door nu te handelen, kun je

¹ [Over de campagne | Denk vooruit](https://www.denkvooruit.nl/service/over-de-campagne) (https://www.denkvooruit.nl/service/over-de-campagne)

snel reageren op verstoringen en makkelijker inspelen op veranderende behoeften.

Deze handreiking is bedoeld voor ondernemers, bedrijven² én hun brancheorganisaties. In het document staat een aanpak met praktische voorbeeldmaatregelen om bedrijven weerbaarder te maken. Niets is verplicht. We geven vooral voorbeelden en inspiratie. Brancheorganisaties kunnen de voorbeeldmaatregelen waar wenselijk verder toesnijden op hun eigen branche of sector.

Door de handreiking stap voor stap te volgen, kun je kritische vragen stellen en beantwoorden

over jouw productie- en leveringsketens en de continuïteit van de bedrijfsvoering. Dit helpt je bij het stellen van prioriteiten en het nemen van maatregelen die passen bij jouw situatie. Daarmee versterk je ook de weerbaarheid van jouw bedrijf tegen andere gevaren en dreigingen.

De handreiking is opgesteld door VNO-NCW en MKB-Nederland, in afstemming met het ministerie van Economische Zaken. Deze partijen werken samen aan de weerbaarheid van het brede Nederlandse bedrijfsleven tegen de drie genoemde noodscenario's.

² Bedrijven die onderdeel uitmaken van de vitale infrastructuur zijn gebonden aan wettelijke eisen die (soms veel) verder gaan dan deze handreiking. Deze eisen staan in sectorale wetgeving maar ook in de wetsvoorstellen Wet weerbaarheid kritieke entiteiten en Cyberbeveiligingswet, zie: NIS2- en CER-richtlijnen | Nationaal Coördinator Terrorisbestrijding en Veiligheid. (<https://www.nctv.nl/onderwerpen/c/cer--en-nis2-richtlijnen>)

Leeswijzer

In deze handreiking starten we met twee kernvragen.

1. Welke activiteiten zijn echt cruciaal voor jouw bedrijf?
2. Wat is het minimale bedrijfsproces dat noodzakelijk is voor het voortbestaan?

De antwoorden op deze vragen laten zien welke onderdelen van jouw organisatie onmisbaar zijn voor het voortbestaan. Deze onderdelen noemen we de *kroonjuwelen* van jouw organisatie. Vervolgens worden vijf stappen uitgewerkt die vergelijkbaar zijn met de schakels van de veiligheidsketen:³

³ De veiligheidsketen organiseert crisisbeheersing en rampenbestrijding in vijf stappen: proactie, preventie, preparatie, repressie en nazorg. Deze vijf stappen zijn voor deze handreiking aangepast naar: vooruitdenken, voorkomen, voorbereiden, reageren en herstellen & doorontwikkelen.

STAP 1.

‘Vooruitdenken; hoe bescherm ik mijn kroonjuwelen?’

Je krijgt praktische handvatten voor hoe je jouw kroonjuwelen (beter) kunt beschermen (‘beveiligingsprincipes’) en welke acties daarbij horen.



STAP 2.

‘Voorkomen is beter dan genezen; voorzorgsmaatregelen nemen’.

Je ziet welke extra voorzorgsmaatregelen mogelijk zijn om jouw kroonjuwelen (beter) te beschermen, en stelt hierbij duidelijke prioriteiten.



STAP 3.

'Bereid je voor; werk de belangrijkste voorbereiding uit, test en oefen'.

Je stelt een praktisch nood- en herstelplan op: een 'handboek voor in nood'. Door regelmatig te testen en te oefenen, verbeter je de voorbereiding continu.



STAP 4.

'Reageer beheerst en alert; weet wat je te doen staat'.

Als het misgaat, treed je effectief en doelgericht op. Je past toe wat je hebt voorbereid en improviseert waar nodig, met het handboek voor in nood als houvast.



STAP 5. 'Herstel en doorontwikkeling'

Na een incident herstel je gestructureerd en planmatig. Je brengt de ervaringen in kaart en gebruikt deze om jouw organisatie nog sterker en veerkrachtiger te maken voor de toekomst.



Elke stap beschrijft een korte aanpak met acties, voorbeeldmaatregelen en verwijzingen naar extra informatie. De voorbeeldmaatregelen zijn door veel soorten ondernemingen direct te gebruiken.

Daarnaast zijn twee bijlagen toegevoegd. De eerste bijlage bevat een uitwerking van de drie scenario's die centraal staan voor bedrijven.⁴ De tweede bijlage bevat een korte casus met vragen. Deze casus kan worden gebruikt om de voorbereiding te toetsen en waar nodig nog extra maatregelen te nemen of voorbereidingen te treffen.

⁴ De nationale crisisstructuur, aanpak, besluiten, maatregelen en communicatie die horen bij het weer herstellen van uitgevallen internet-, telecom- en/of energievoorzieningen zijn geen onderwerp in deze handreiking. Daar bestaan landelijke crisisplannen voor die te vinden zijn op [Landelijke Crisisplannen | Nationaal Coördinator Terrorismebestrijding en Veiligheid](https://www.nctv.nl/onderwerpen/l/landelijke-crisisplannen). (<https://www.nctv.nl/onderwerpen/l/landelijke-crisisplannen>)

De basis: Wat zijn de kroonjuwelen van jouw bedrijf?

Om te weten wat en wie je nodig hebt als het misgaat, is het belangrijk te weten wát je precies moet beschermen. Hiervoor stel je de kroonjuwelen van jouw bedrijf vast. Kroonjuwelen zijn die mensen, processen, middelen en producten binnen je bedrijf die absolute prioriteit hebben voor de continuïteit (ononderbroken voortgang) van de bedrijfsvoering. Het zijn de belangrijkste onderdelen die je optimaal wilt beschermen.⁵

Om deze kroonjuwelen vast te stellen, kun je kijken naar de volgende vier onderdelen van jouw bedrijfsvoering:

1. **Personeel en organisatie:** Jijzelf als ondernemer, directie, medewerkers en onderlinge samenwerking.
2. **Ketens en klanten:** Jouw (belangrijkste) klanten, leveranciers en partners die afnemen of leveren.
3. **Producten en diensten:** Jouw unieke formule, assortiment, (kennis)product en/of dienstverlening.
4. **Ondersteunende processen en hulpmiddelen:** Inkoop, logistiek, administratie/financiën, ICT, gebouwen, voorraden, betaalmiddelen en transportmiddelen.

⁵ [Hoe breng ik mijn te beschermen belangen in kaart? | Wat kun je zelf doen? | Nationaal Cyber Security Centrum. \(https://www.ncsc.nl/risicomanagement/hoe-breng-ik-mijn-te-beschermen-belangen-kaart\)](https://www.ncsc.nl/risicomanagement/hoe-breng-ik-mijn-te-beschermen-belangen-kaart)

Vier onderdelen die kroonjuwelen herbergen



De twee kernvragen die je hier kunt stellen:

1. Welke activiteiten zijn echt cruciaal voor jouw bedrijf?
2. Wat is het minimale bedrijfsproces dat noodzakelijk is voor het voortbestaan?

Een vuistregel om jouw kroonjuwelen te bepalen, is: Als het wegvallen van een onderdeel van jouw bedrijf ervoor zorgt dat het bedrijf (bijna) stilvalt, dan is het een kroonjuweel.

Analyseer wat voor jouw bedrijf van wezenlijk belang is en werk dit samen met personeel en relevante partners uit in een overzicht. Evalueer regelmatig of dit overzicht nog actueel is.

STAP 1.

Vooruitdenken; hoe bescherm ik mijn kroonjuwelen?



In deze stap geven we praktische handvatten voor hoe je jouw kroonjuwelen (beter) kunt beschermen (genaamd 'beveiligingsprincipes') en welke acties daarbij horen. Gebruik hierbij de drie noodscenario's uit de inleiding als uitgangspunt.

De beveiligingsprincipes en acties zijn geordend rond de vier onderdelen van de bedrijfsvoering (zie hiervoor, bladzijde 13).

Beveiligingsprincipes Personeel en organisatie

- **Veiligheid:** Hoe borg ik de veiligheid van mijn personeel en hun families?

- **Continuïteit en beschikbaarheid:** Welke medewerkers hebben een cruciale functie of positie binnen het bedrijf en hoe moeilijk zijn zij te vervangen?
- **Bereikbaarheid:** Welke bereikbaarheidsafspraken heb ik als er geen communicatie meer mogelijk is?

Ketens en klanten

- **Continuïteit en beschikbaarheid:** Van wie ben ik als ondernemer sterk afhankelijk? Denk aan de samenwerking met leveranciers, dienstverleners en klanten. Maar ook: werkt mijn bedrijf samen met, of lever ik aan, bedrijven in een vitale sector?⁶

⁶ [Overzicht Vitale Processen | Nationaal Coördinator Terrorismebestrijding en Veiligheid.](https://www.nctv.nl/onderwerpen/v/vitale-infrastructuur/overzicht-vitale-processen)
(<https://www.nctv.nl/onderwerpen/v/vitale-infrastructuur/overzicht-vitale-processen>)

- **Bereikbaarheid:** Hoe bereik ik mijn leveranciers en klanten, en hoe bereiken zij mij?
- **Financiële schade:** Ken ik de financiële risico's voor mijn bedrijf voldoende en weet ik waarvoor ik (niet) verzekerd ben?
- **Reputatie:** Hoe voorkom ik (onnodige) reputatieschade?

Producten en diensten

- **Continuïteit en beschikbaarheid:** Hoe krijg ik mijn producten en diensten nog (tijdig) geproduceerd?
- **(Uit)leverbaarheid:** Hoe transporteer ik mijn goederen nog en wat doe ik als dat (tijdelijk) niet meer kan?
- **Beschikbaarheid nutsvoorzieningen:** Werk ik door als belangrijke nutsvoorzieningen uitvallen, en zo ja, hoe?
- **Bescherming:** Hoe bescherm ik mijn

producten, data en intellectueel eigendom onder crisismomstandigheden of als bepaalde beveiligingsvoorzieningen niet meer beschikbaar zijn?

Ondersteunende processen en hulpmiddelen

- **Continuïteit en beschikbaarheid:** Welke geautomatiseerde processen zoals inkoop, administratie (bijvoorbeeld facturering of salarisbetalingen) of IT-gedreven transacties vallen stil of lopen vast bij uitval van energie en/of internet/telefonie gedurende 72 uur of langer? En vanaf wanneer bedreigt dit de continuïteit van mijn bedrijf?
- **Betrouwbaarheid:** Hoe borg ik de kwaliteit van mijn productie, als (IT-)processen, transacties en nutsvoorzieningen niet meer betrouwbaar en/of beschikbaar zijn?

Mogelijke acties

Voorgaande vragen zijn voor jou een hulpmiddel om prioriteiten te stellen en na te gaan hoe de geïdentificeerde kroonjuwelen (beter) beschermd kunnen worden. Hieronder staan acties die je hierbij kunnen helpen. De volgorde geeft een indicatie van prioriteit, maar dit kan per bedrijf verschillen.

Personeel en organisatie

Veiligheid:

- Soms is het veilig en beheerst stilleggen van het bedrijf, beter of zelfs noodzakelijk: Stel duidelijk vast wanneer het niet veilig (of onmogelijk) is om (door) te werken, naar het bedrijf te komen of wanneer de veiligheid voor thuis en naasten voorgaat. Zorg ervoor dat personeel in dat geval veilig thuis kan komen.

- Zorg voor aanvullende veiligheidsmaatregelen voor doorwerken onder verstoorde omstandigheden.

Continuïteit en beschikbaarheid:

- Organiseer dat je voor uitval van personeel op cruciale functies of posities, vervangers kunt inhuren en/of hebt opgeleid.
- Houd er rekening mee dat er medewerkers op cruciale functies of posities kunnen zijn die nevenwerkzaamheden (zoals reservist) verrichten, mantelzorgtaken vervullen of oproepbaar zijn voor de dienstplicht (in Nederland of een ander land) waardoor ze in noodsituaties langere tijd afwezig kunnen zijn.

- Als de aanwezigheid op het bedrijf of op de vestiging essentieel en verantwoord is, zorg dan zo nodig voor alternatief transport om personeel op te halen en thuis te brengen.
- Denk na of je bij een langdurige crisis het personeel op een andere wijze kunt inzetten.
- Zoek de afstemming met collega-bedrijven of vraag advies bij jouw brancheorganisatie hoe zij met langdurige uitval of afwezigheid van personeel omgaan.

Bereikbaarheid:

- Stel samen met personeel bereikbaarheidsafspraken op.
- Zorg dat iedereen de afspraken kent. Licht ze regelmatig toe, zodat de afspraken (automatisch) in gang gezet worden als er (tijdelijk) geen communicatie mogelijk is.

Ketens en klanten

Continuïteit en beschikbaarheid:

- Ga in gesprek met bedrijven in vitale sectoren (zie voetnoot 6) waarmee je samenwerkt als klant. Bespreek welke extra afspraken nodig en mogelijk zijn om de continuïteit van jouw leveringen of producten te waarborgen. Bepaal hoe lang je nog kunt doorgaan met je bestaande voorraad, wanneer de belangrijkste leveranciers niet kunnen (of willen) leveren.
- Maak afspraken met je belangrijkste (toe) leveranciers over hoe je eventuele problemen door afhankelijkheid kunt opvangen. Bijvoorbeeld:
 - o Hoe je de afhankelijkheid van fysieke levering van onderdelen of producten kunt verkleinen.

- o Hoe je toch kunt doorwerken en blijven leveren, ook als leveranciers of klanten geografisch zeer verspreid zitten.
- Overweeg extra voorraad van cruciale grondstoffen en/of onderdelen aan te houden.
- Zoek de afstemming met die bedrijven met wie je al samenwerkt of een netwerk vormt en van wie je wellicht heel gericht kunt leren over bedrijfscontinuïteit, iets kunt delen of iets kunt overnemen.
 - o Denk daarbij ook aan bevriende ondernemers buiten de eigen branche.
 - o Aarzel niet om als klein bedrijf naar de wat grotere ondernemingen te stappen ('groot helpt klein').

Bereikbaarheid:

- Neem ook in leveringsvoorwaarden, contracten en projectplannen op wie onder verstoorde omstandigheden op welke wijze bereikt kan worden.

Financiële schade:

- Ga na of je de leveringsvoorwaarden, contracten en serviceovereenkomsten op bijzondere omstandigheden (overmacht) kunt aanpassen.
- Verzeker waar mogelijk aanvullende risico's of verzwaar de huidige dekking.
- Zet extra geld opzij en overleg met je bank wat mogelijk is.
- Ga na of er specifieke fiscale regelingen mogelijk zijn, bijvoorbeeld betalingsuitstel. Overleg met jouw accountant.

Reputatie:

- Wees open en duidelijk als afspraken, aangegane verplichtingen en/of leveringen in gevaar (kunnen) komen en zoek samen met klanten, leveranciers enzovoort naar oplossingen.
- Bedenk vooraf hoe je omgaat met klachten, ingebrekestellingen en communicatie om reputatieschade te beperken. Zorg bijvoorbeeld voor een goede jurist en/of communicatiespecialist in jouw netwerk die jou hierbij kan bijstaan.

Producten en diensten

Continuïteit en beschikbaarheid:

- Denk na over hoe jouw bedrijf open, actief en rendabel kan blijven als zich een langdurige crisissituatie voordoet. Bijvoorbeeld een situatie waarin Nederland betrokken

raakt bij een militair conflict en bijstand moet verlenen aan de NAVO.

(Uit)leverbaarheid:

- Denk na over alternatieve transportvoorzieningen of een andere wijze van uit- of afleveren van goederen. Kijk bijvoorbeeld of verkoop aan huis, afhalen, zelf brengen of een centrale leveringsplaats tijdelijk mogelijk zijn.

Beschikbaarheid nutsvoorzieningen:

- Ga na of en waar je de afhankelijkheid van nuts- en belangrijke technische voorzieningen (bijvoorbeeld IT) voor jouw productie en levering kunt verkleinen.
 - o Zijn er alternatieve manieren om door te werken, bijvoorbeeld handmatige bediening?

- o Controleer de afspraken over beheer en onderhoud, zowel intern als extern, en leg (waar nodig) aanvullende waarborgen vast.

Bescherming:

- Zorg zo nodig voor aanvullende (handmatige) fysieke beveiliging of bewaking.
- Jouw unieke diensten of producten kunnen onder normale omstandigheden maar zeker in tijden van hybride⁷ en/of militaire dreiging kwetsbaar zijn voor spionage, diefstal of sabotage. Maak het personeel hier alert op. Inventariseer de grootste risico's en neem maatregelen om je hiertegen te beschermen.⁸

Ondersteunende processen en hulpmiddelen

Continuïteit en beschikbaarheid:

- Verklein de afhankelijkheid van geautomatiseerde ondersteunende processen. Bijvoorbeeld: Zorg dat je handmatig facturen kunt uitschrijven of boekingen kunt doen.
- Verbeter de beveiliging. Bijvoorbeeld: Ga na of de gebouwbeveiliging en -toegang zodanig is opgezet dat veilige (hand)bediening mogelijk is.
- Maak jouw energievoorziening minder afhankelijk van één type brandstof. Bijvoorbeeld: Thuisaccu's en noodstroomaggregaten helpen je langere tijd te blijven produceren bij uitval van energie.

⁷ Een conflictvoering tussen staten met geïntegreerd gebruik van middelen en actoren, met als doel bepaalde strategische doelstellingen te bereiken, zie: [Een duiding van het fenomeen 'hybride dreiging'](https://www.nctv.nl/documenten/2019/04/18/duiding-fenomeen-hybride-dreiging) | Nationaal Coördinator Terrorismebestrijding en Veiligheid. (<https://www.nctv.nl/documenten/2019/04/18/duiding-fenomeen-hybride-dreiging>)

⁸ Stap 2 | Ken de risico's | Maak je bedrijf weerbaar. (<https://www.maakjebedrijfweerbaar.nl/ken-de-risicos>)

- Kijk of je een goede balans tussen brandstof en elektrisch materieel kunt aanhouden.
- Als je met andere ondernemers en bedrijven in een straat, verzamelgebouw of bedrijven-terrein zit, ga na waarmee jullie elkaar kunnen helpen tijdens een crisis. Bijvoorbeeld: Kijk waar gezamenlijke aanschaf en gebruik voordelen biedt, zoals van noodstroomaggregaten, thuisaccu's of extra andersoortige communicatiemiddelen (bijvoorbeeld portofoons of zelfs radio-zendapparatuur⁹).

Betrouwbaarheid:

- Zoek uit wat wettelijk mogelijk en toegestaan is op het gebied van bijvoorbeeld ARBO en brandveiligheid als je extra technische (energie)voorzieningen installeert of extra brandstof opslaat. Neem hierbij eventueel contact op met de toezichthouder(s) om (on)mogelijkheden of knelpunten te bespreken.
- Ga na waar geautomatiseerde procedures en systemen normaal gesproken de kwaliteit van producten of services bewaken. Ontwikkel daarvoor aanvullende handmatige procedures zodat je - wanneer nodig - extra handmatige en gerichte kwaliteitscontroles en -inspecties kunt uitvoeren.

⁹ Voor het bezit en gebruik van zendapparatuur zijn diploma's vereist, zie: [radiozendamateur worden | rijksinspectie digitale infrastructuur \(rdi\)](https://www.rdi.nl/onderwerpen/vergunningen-en-registraties/radiozendamateurs/opleiding-en-examens). (<https://www.rdi.nl/onderwerpen/vergunningen-en-registraties/radiozendamateurs/opleiding-en-examens>)

Tot slot

Denk ook na over welke bijdrage jouw onderneming kan leveren aan de samenleving en/of vitale sectoren tijdens een (langdurige) crisissituatie. Crisissituaties kunnen namelijk leiden tot verstoringen in ketens en tot veranderingen in de vraag naar producten en diensten.

Ondernemingen die hier flexibel en verantwoord op inspelen, kunnen klanten blijven bedienen en helpen maatschappelijke processen te continueren.

Stel jezelf hierbij ook de volgende vragen:
Welke rol kan jouw onderneming vervullen wanneer bestaande leveranciers uitvallen?
In hoeverre kun je tijdelijk opschalen om klanten of ketenpartners te ondersteunen?

Nu je beter in beeld hebt waar extra bescherming nodig is en welke opties daarvoor mogelijk zijn, is het tijd voor de volgende stap: Het gericht nemen van extra voorzorgsmaatregelen om jouw kroonjuwelen (beter) te beschermen.

STAP 2.

Voorkomen is beter dan genezen; voorzorgsmaatregelen nemen



Nu is het tijd voor (nog) meer actie! Maak jouw kroonjuwelen weerbaar(der), zodat je bij een verstoring of in tijden van een crisis zo lang mogelijk en veilig kunt blijven draaien. Welke extra maatregelen of middelen heb je hiervoor nodig?

De volgende figuur geeft per onderdeel van de bedrijfsvoering voorbeeldmaatregelen die je kunt nemen om jouw kroonjuwelen beter te beschermen.¹⁰ De vorige stap heeft je al richting gegeven. Deze stap helpt je passende voorzorgsmaatregelen te kiezen en in te richten.

¹⁰ NCSC - De bellijst, simpel maar effectief. (<https://www.ncsc.nl/preventieve-beveiligingsmaatregelen/de-bellijst-simpel-maar-effectief>)

Personeel en organisatie

- Bereikbaarheids- en communicatieafspraken
- Vervangingsregelingen
- Papieren adreslijsten
- Veilige (extra beveiligde) werklocaties
- Afgesproken verzamelplaats(en) /noodlocatie(s)
- Alternatieve vervoersmiddelen zoals bedrijfs-(bak)fietsen
- Alternatieve (extra) communicatiemiddelen; zoals 2e telefoon met simkaart van andere provider, satellietcommunicatie, etc.
- BHV (EHBO) trainingen
- Noodpakket(ten) op locatie
- Slaapplaatsen, sanitair- en keukenvoorzieningen voor essentiële medewerkers
- Persoonlijke beschermingsmiddelen
-

Ketens en klanten

- Specifieke afspraken met de vitale sectoren
- Geselecteerde alternatieve of extra leveranciers
- Papieren adressenlijst(en) van klanten en leveranciers
- Externe bereikbaarheids- en communicatieafspraken
- Extra (buffer) voorraden / alternatieve voorraadlocaties
- Alternatieve (af)leveringswijze(n)
- Aangescherpte leveringsvoorwaarden en contracten
- Aanvullende verzekering of –dekking
-

Ondersteunende processen en hulpmiddelen

- Papieren uitdraai belangrijkste administratie / bedrijfsgegevens
- Papieren factuur- en kwitantie blocnotes
- Back-up(s) (off-line systemen)
- Papieren catalogi, boekingen, bestellijsten, prijslijsten, etc.
- Procedures voor handmatige kwaliteitscontroles
- Handmatig bedienbare gebouw (toegang) beveiliging (veilig afsluitbaar)
- Alternatieve betaalmiddelen of (extra) contant geld
- Thuiswerkplek(ken)
- Noodaggregaat (+ voorraad dieselolie), thuisaccu's, powerbanks
- Alternatieve communicatiemiddelen (portofoons, zendapparatuur)
- Extra brandstof in veilige opslag
- Solar- of petroleumlampen, kaarsen
-

Producten en diensten

- Aangepaste producten of dienstverlening bij langdurige crisis
- Alternatieve transportvoorzieningen
- Alternatieve (handmatige) werkwijzen
- Alternatieve openingstijden / thuisverkoop
- Hulpmiddelen voor communicatie op locatie zoals papieren berichten/borden
- Extra (IT en fysieke) beveiligingsmaatregelen
-

Aandachtspunten

- **Noodpakket:** Zorg voor noodpakket(ten) thuis én op kantoor.¹¹ Met een radio op batterijen blijf je tijdens een noodsituatie op de hoogte van het nieuws en de adviezen van de overheid. Denk ook aan faciliteiten en hulpmiddelen waarmee je veilig en verantwoord langere tijd op het bedrijf kunt verblijven.
- **Sanitatie:** Houd er rekening mee dat bij langdurige energie-uitval wc's niet meer gebruikt kunnen worden doordat de riole-ring of rioolwaterzuivering uitvalt. Denk waar nodig na over alternatieven.¹²
- **Alternatieve betaalmiddelen:** Denk hierbij na over het gebruik van contant geld, QR-betalingen of offline pin.¹³
- **Back-ups (kopieën van opgeslagen data):** Zorg voor kwalitatief goede back-ups.¹⁴
- **Cyberhygiëne:** Breng met de vijf basisprincipes voor digitale weerbaarheid de cyberhygiëne van jouw bedrijf op orde en test deze.¹⁵
Er gebeuren nog altijd veel incidenten doordat bedrijven hun cyberhygiëne niet op orde hebben.
- **Algemeen:** Wees je ervan bewust dat elke nieuwe voorziening of alternatieve werk-

¹¹ Stel je noodpakket samen | Denk vooruit. (<https://www.denkvooruit.nl/bereid-je-voor/stel-je-noodpakket-samen>)

¹² Voorbereiden voor 72 uur | Denk vooruit. (<https://www.denkvooruit.nl/vraag-en-antwoord-2/voorbereiden>)

¹³ Adviezen MOB Denk vooruit, ook voor betalen en Terugvalopties pinnen - PIN.NL (<https://www.pin.nl/ondernemer/storingen/terugvalopties/>)

¹⁴ NCSC - Maak in 3 stappen een goede back-up. (<https://www.ncsc.nl/back-up/maak-3-stappen-een-goede-back-up>)

¹⁵ NCSC - De 5 basisprincipes van veilig digitaal ondernemen. (<https://www.ncsc.nl/basisprincipes/overzicht>)

wijze zowel legaal, veilig als beveiligd moet zijn. Houd het daarom in eerste instantie eenvoudig en overzichtelijk en raadpleeg zo nodig deskundigen, de branchevereniging, collega-ondernemers of een toezichthouder. Bijvoorbeeld: Denk goed na over de (brand) veiligheid en bereikbaarheid, (nood)verlichting in ruimtes en nooduitgangen bij stroomuitval, maar ook over het risico van het op voorraad hebben van extra contant geld zoals diefstal of overvallen.

De volgende stap is ervoor zorgen dat je als bedrijf ook echt voorbereid bent en blijft.

STAP 3.

Bereid je voor; werk de belangrijkste voorbereiding uit, test en oefen waar mogelijk



‘Wat je zelden doet, doe je zelden goed’.
Niemand weet of, wanneer of hoe lang een verstoring of crisis zich zal voordoen. De extra maatregelen, gemaakte afspraken en afwijkende werkwijzen voor noodsituaties zijn misschien lange tijd niet nodig. Dat kan geruststellend zijn, maar het betekent ook dat je ze misschien niet goed kunt toepassen wanneer het wél nodig is.

Daarom is het verstandig alle hulpmiddelen, alternatieve werkwijzen, noodvoorzieningen en afspraken vast te leggen in een plan, voorzien van duidelijke voorschriften en instructies. Zo ontstaat een praktisch **handboek voor in nood**. Wijs binnen het bedrijf een verantwoordelijke aan voor het handboek. Hij of zij moet ervoor zorgen dat het handboek regelmatig wordt bijgewerkt en actueel blijft.

¹⁶ Bereid je voor | Denk vooruit. (<https://www.denkvooruit.nl/bereid-je-voor>)

Wat kan er in het handboek voor in nood staan?
Denk aan de volgende onderwerpen:

1. **(Crisis)besluitvormingslijnen.** Beschrijf wie in een noodsituatie de leiding heeft, wie mag beslissen en wie waarover gaat.
2. **Afspraken met het personeel en het thuisfront.** Geef informatie aan je personeel over wat ze vooraf met het thuisfront kunnen regelen om voorbereid te zijn op een noodsituatie. Denk bijvoorbeeld aan een noodpakket.¹⁶
3. **(Nood)communicatieplan.** Leg vast waar en hoe je elkaar kunt bereiken als normale communicatie uitvalt (denk aan afspraken over fysieke ontmoetingsplaatsen). Dit geldt voor het thuisfront, personeel, klanten en leveranciers.

4. **Afspraken met leveranciers en dienstverleners.** Beschrijf hoe de samenwerking doorgaat tijdens een crisis. En dat er mogelijk een afschaling van bedrijfsactiviteiten tot het niveau van puur noodzakelijk plaatsvindt.
5. **Alternatieve betaal- en distributiemethoden.** Zorg dat duidelijk is welke opties beschikbaar zijn als de gebruikelijke betaal- en/of distributiemethoden niet meer werken.
6. **Belangrijkste principes van (alternatieve) werkwijzen en herstel.** Beschrijf hoe belangrijke processen of voorzieningen tijdens een verstoring kunnen blijven functioneren of zo snel mogelijk hersteld

kunnen worden als ze uitvallen. Werk dit uit in een herstelplan of checklist.¹⁷

Uit ervaringen blijkt dat een handboek tijdens een crisis vaak niet gebruikt wordt. Daarom is het verstandig aan de hand van het handboek een korte checklist te maken en te verspreiden (bijvoorbeeld in zakformaat, op een plastic kaartje). Dit helpt je vooral in de eerste hectische uren van een crisis, om stap voor stap te bepalen welke acties je moet voorbereiden of uitvoeren, in welke volgorde en wanneer.

¹⁷ Tip: Als je sterk afhankelijk bent van IT of veel IT-systemen beheert of hebt uitbesteed, is het verstandig om een apart Bedrijfscontinuïteitsplan (BCP) op te stellen. Zie bijvoorbeeld: [Bedrijfscontinuïteitsplan: blijf overeind na een ramp | KVK](https://www.kvk.nl/veilig-zakendoen/goed-voorbereid-op-een-calamiteit/) (<https://www.kvk.nl/veilig-zakendoen/goed-voorbereid-op-een-calamiteit/>)

Aandachtspunten

- Zorg dat iedereen het handboek kent (en weet te vinden). Leg een papieren uitdraai op meerdere plaatsen (op kantoor en thuis).
- Test technische (terugval)voorzieningen waaronder stroom- en energievoorzieningen, IT- en back-up systemen regelmatig. Wat niet werkt, moet zo snel mogelijk worden opgelost of anders worden ingericht.
- Verspreid de checklist voor de eerste respons (in een handzaam formaat) aan alle betrokkenen.
- Oefen regelmatig met dit handboek en de checklist, zodat jij, jouw medewerkers en samenwerkingspartners weten wat er van hen wordt verwacht in een noodsituatie.
- Oefenen van (realistische) scenario's hoort erbij. Als leidinggevende geef je het goede voorbeeld door hier zichtbaar structureel aandacht aan te besteden en het belang ervan te benadrukken. Dit zorgt ervoor dat teams gemotiveerd blijven en beter voorbereid zijn.
- Oefenen hoeft niet ingewikkeld te zijn. Start eenvoudig met een oefening op papier, dat maakt al het verschil. Later kun je uitbreiden naar een praktijkoefening.
- Gericht trainen, en oefenen onder druk helpen om de mentale weerbaarheid van individueel personeel en teams te vergroten.
- Evalueer en verbeter. Werk het handboek (en checklist(s)) regelmatig bij, bijvoorbeeld na een oefening.

Onderstaande figuur geeft de acties en aandachtspunten voor deze stap nog een keer kort weer:



De volgende stap beschrijft de specifieke uitdagingen die zich kunnen voordoen wanneer een (langdurige) verstoring of crisissituatie jouw bedrijf treft. Het legt uit hoe je op dat moment kunt reageren en hoe je omgaat met de focus en improvisatie die dan nodig zijn.

STAP 4.

Reageer beheerst en alert; weet wat je te doen staat



'En dan gebeurt het: onverwacht, ongelegen en ook anders dan iedereen had voorzien'. Dan moet je er staan, doen wat is voorbereid en improviseren waar nodig. Het in de vorige stap beschreven handboek voor in nood is nu de terugvalbasis. Maar houd er rekening mee dat stress en onzekerheid onder deze omstandigheden het handelen en samenwerken kunnen beïnvloeden.

Veel hangt af van jouw informatiepositie en die van anderen: 'Heb je nog toegang tot informatie over de dreiging of verstoring? Kun je nog communiceren? Of ga je meteen alternatieve communicatiemiddelen inzetten?' Daarom is het verstandig meteen de checklist te gebruiken die voor de eerste uren (eerste dag) ontwikkeld is.

In de eerste plaats gaat het daarbij uiteraard om de veiligheid van jezelf, het personeel, bezoekers of klanten op locatie, en het thuisfront. En ook om het veiligstellen van communicatie en locaties. Daarna volgt de continuïteit van de bedrijfsvoering, leveringen en alternatieve werkwijzen en noodmaatregelen. Bij minder ernstige situaties kan de prioriteit (vooral) bij de continuïteit van de bedrijfsvoering liggen.

De volgende tabel bevat een voorbeeld voor de opbouw en de inhoud van een (respons) checklist:

(Eigen) veiligheid
(personeel, bezoekers,
familie)



- Heb ik toegang tot (voldoende) noodmiddelen (de noodpakketten) met als eerste drinkwater?
- Heb ik mijn medicijnen, EHBO, verbanddoos, etc.?
- Functioneert de (nood)verlichting, ventilatie?
- Kan ik hulpverleningsdiensten bereiken (evt. fysiek)?

(Nood)communicatie



- Is mijn personeel en familie bereikbaar?
- Welke van de gemaakte afspraken geldt nu en zijn uitvoerbaar?
- Welke communicatiemiddelen werken (nu nog)?
- Zijn alternatieve communicatiemiddelen beschikbaar en werken ze?

Informatie (positie)



- Waar krijg ik informatie over de dreiging/ situatie?
- Heb ik de middelen (radio, fysiek contact) daartoe tot mijn beschikking?
- Wat zeggen de autoriteiten? Wat is de aard van de (dreigende) gebeurtenissen?
- Wie heb ik (nog meer) nodig?

Locatie(s)



- Is/zijn mijn locatie(s) veilig (genoeg) voor de dreiging?
- Is een veilig verblijf op locatie(s) (verwarming, frisse lucht, (nood)verlichting, alarmeren) nog geborgd?
- Wat zijn veilige en betrouwbare vervoersalternatieven?

Bedrijfsvoering (alternatieve werkwijze en noodmaatregelen)



- Hoe stel ik de kritische processen, goederen en voorraad veilig?
- Is (papier) cruciale informatie beschikbaar, evenals waardepapieren en betaalmiddelen (contant geld)?

Aandachtspunten

- In de eerste (vaak hectische) uren voorkom je chaos (en soms ook paniek) door terug te vallen op de afspraken die je hebt gemaakt met personeel en het thuisfront.
- Help elkaar. Binnen het bedrijf, maar ook met naburige bedrijven en in de ketens en netwerken waarin je normaal werkt.
- Toon leiderschap. Laat zien dat je er bent voor jouw bedrijf en het personeel. Dit is waar de voorbereiding voor bedoeld was. Maak steeds duidelijk wanneer doorwerken (nog) kan of stoppen moet.
- Overweeg ook om bijvoorbeeld de bedrijfslocatie(s) open te stellen om anderen op te vangen of te helpen.

Op basis van de voorzorgsmaatregelen, voorbereiding en improvisatie, reageer en handel je tijdens de crisis zo slagvaardig mogelijk. Zodra de omstandigheden verbeteren en essentiële voorzieningen (deels) hersteld zijn, begin je stapsgewijs met de terugkeer naar de normale bedrijfsvoering. Daarbij helpt de laatste stap.

STAP 5. Herstel en doorontwikkeling



‘Aan het einde van elke tunnel gloort er licht’. Zodra er zicht is op (gedeeltelijk) herstel van uitgevallen voorzieningen, is het tijd het bedrijf stapsgewijs weer te openen en op te starten. Ook daarvoor is het wenselijk een vooraf opgesteld herstelplan (onderdeel van het handboek voor in nood) of checklist te gebruiken. Je kunt bij het herstel twee fasen onderscheiden:

1. ‘Back to business’

Het bedrijf draait weer gedeeltelijk. De belangrijkste productie, levering en communicatie werken weer, terwijl sommige processen nog anders of beperkt verlopen. Gebruik het herstelplan en/of een checklist die bijvoorbeeld de volgende onderdelen bevatten:

- Controleer hoe het gaat met personeel, hun directe omgeving, leveranciers en klanten. Bespreek verwachtingen en geef aan waar nog verstoringen of andere werkafspraken gelden.
- Stel prioriteiten. Welke processen kunnen als eerste (veilig) opstarten en welke communicatie hoort daarbij?
- Bepaal welke extra (kwaliteits)controles en handmatige procedures hierbij nodig zijn.

2. 'Back to normal'

De situatie herstelt geleidelijk volledig. Informeer het personeel over het herstel, bewaak het welzijn van personeel, en regel waar nodig extra ondersteuning. Dit is ook het moment om eventuele schade vast te stellen en te claimen bij verzekeringen of schadefondsen.

Wacht niet te lang en ga met je personeel en anderen met wie je hebt samengewerkt om tafel zitten en kijk terug:

- Bespreek wat goed ging en wat beter kan.
- Verwerk de geleerde lessen in jouw handboek voor in nood.
- Sta stil bij de inzet en betrokkenheid van medewerkers.

Ten slotte: Het is belangrijk aandacht te hebben en houden voor medewerkers die nog extra (mentale) ondersteuning nodig hebben bij het herstel.

Afsluiting

Door deze handreiking stap voor stap door te nemen en in de praktijk toe te passen, ben je beter voorbereid op moeilijke omstandigheden en kun je sneller en effectiever handelen.

We kunnen ons voorstellen dat je bij het lezen en toepassen behoefte hebt aan meer ondersteuning. Neem dan contact op met jouw branchevereniging.

Voor vragen of opmerkingen over de handreiking zelf, kun je contact opnemen met VNO-NCW en MKB-Nederland.

Contact

VNO-NCW en MKB-Nederland

Sabine Gielens

gielens@vnoncw-mkb.nl

Literatuurlijst van geraadpleegde bronnen

- Federation of Finnish Entrepreneurs. (2025). SME Preparedness Guide. FFE.
- Kamer van Koophandel. Bedrijfscontinuïteitsplan: blijf overeind na een ramp. <https://www.kvk.nl/veilig-zakendoen/goed-voorbereid-op-een-calamiteit/>
- Kamerstuk 5937426, blz. 7. (6 december 2024). <https://www.nctv.nl/documenten/2024/12/06/kamerbrief-weerbaarheid-tegen-militaire-en-hybride-dreigingen>
- Maatschappelijk Overleg Betalingsverkeer. (20 mei 2025). Denk vooruit, ook voor betalen. <https://www.dnb.nl/media/vctdy4f/advies-mob-denk-vooruit-ook-voor-betalen.pdf>
- Ministerie van Economische Zaken. Maak je bedrijf weerbaar. Ken de risico's. <https://www.maakjebedrijfweerbaar.nl/ken-de-ricos>
- Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Over denk vooruit. <https://www.denkvooruit.nl/service/over-de-campagne>
- NCTV. Landelijke Crisisplannen. <https://www.nctv.nl/onderwerpen/l/landelijke-crisisplannen>.
- NCTV. NIS2- en CER-richtlijnen. <https://www.nctv.nl/onderwerpen/c/cer--en-nis2-richtlijnen>
- NCTV. Overzicht vitale processen. <https://www.nctv.nl/onderwerpen/v/vitale-infrastructuur/overzicht-vitale-processen>

- NCTV. Een duiding van het fenomeen hybride dreiging. <https://www.nctv.nl/documenten/2019/04/18/duiding-fenomeen-hybride-dreiging>
- NCTV. (2025). Bereid je voor op een noodsituatie. <https://www.denkvooruit.nl/informatieboekje>; <https://www.denkvooruit.nl/bereid-je-voor/stel-je-noodpakket-samen>; <https://www.denkvooruit.nl/vraag-en-antwoord-2/voorbereiden>
- NCTV. (22 juli 2025). Gesprekstool maatschappelijke weerbaarheid (light versie). <https://www.nctv.nl/documenten/2025/07/22/gesprekstool-maatschappelijke-weerbaarheid-light-versie>
- Nationaal Cyber Security Centrum (NCSC). Hoe breng ik mijn te beschermen belangen in kaart. <https://www.ncsc.nl/risicomangement/hoe-breng-ik-mijn-te-beschermen-belangen-kaart>
- NCSC. De bellijst, simpel maar effectief. <https://www.ncsc.nl/preventieve-beveiligingsmaatregelen/de-bellijst-simpel-maar-effectief>
- NCSC. Maak in 3 stappen een goede back-up. <https://www.ncsc.nl/back-up/maak-3-stappen-een-goede-back-up>
- NCSC. De 5 basisprincipes van veilig digitaal ondernemen. <https://www.ncsc.nl/basisprincipes/overzicht>
- Nederlands Instituut Bedrijfshulpverlening. (2025). Whitepaper Weerbaarheid. NIBHV. <https://www.nibhv.nl/hulpmiddel/whitepaper-weerbaarheid/>

- Rijksinspectie Digitale Infrastructuur. Radiozendamateurler worden. <https://www.rdi.nl/onderwerpen/vergunningen-en-registraties/radiozendamateurs/opleiding-en-examens>
- Swedish Civil Defence and Resilience Agency. (januari 2026). Preparedness for businesses – In case of crisis or war.
- Verslagen van Weerbaarheidstafels georganiseerd door VNO-NCW, MKB-Nederland, ministerie van Economische Zaken en Rijksdienst voor Ondernemend Nederland. (2025).

Bijlage 1 – Voorstelbare scenario's¹⁸

Uitval van internet en telefonie

In verschillende landen in Europa zijn teams actief die namens een statelijke actor digitale infrastructuur aan het saboteren zijn. Doelwitten zijn strategische locaties, zoals glasvezelkabels bij datacenters, internetknooppunten en telecomaانبieders. In Nederland wordt door een dergelijk team een landelijke mobiele telecomaانبieder getroffen.

De uitval heeft onmiddellijk grote gevolgen op het dagelijks leven. Mobiele netwerken, en het vaste netwerk vallen in delen van het land stil, waardoor bellen en internetgebruik niet mogelijk is. Doordat steeds meer apparaten verbonden zijn met internet ('Internet of Things'), zoals verlichting, zonnepanelen en de thermostaat, zullen deze ook niet beschikbaar zijn. Het toonbankbetalingsverkeer raakt verstoord, waardoor men niet meer kan afrekenen in onder andere supermarkten en apotheken. Contant geld opnemen is niet meer mogelijk door de verstoring van pinautomaten.

¹⁸ De drie scenario's zijn in februari 2025 opgesteld door de ministeries van Economische Zaken (EZ) en Klimaat en Groene Groei (KGG), in afstemming met de sectoren telecom en elektriciteit, en afgeleid van het overkoepelende scenario uit de Kamerbrief van 6 december 2024. (<https://www.nctv.nl/documenten/2024/12/06/kamerbrief-weerbaarheid-tegen-militaire-en-hybride-dreigingen>) De parameters zijn in overleg met VNO-NCW en MKB-Nederland overeengekomen en zijn in lijn met de aanpak van diverse Europese landen. De scenario's zijn t.b.v. deze handreiking in januari 2026 door de ministeries van EZ en KGG geactualiseerd.

Ook de handel met het buitenland wordt geraakt. Reizigers kunnen de weg op, maar dit zal ook belemmerd worden omdat Rijkswaterstaat geen digitaal zicht meer heeft op de weg, en het treinverkeer is regionaal belemmerd door uitval van interne netwerken. De telecomaanbieder geeft aan dat het onduidelijk is hoe lang het zal duren voordat de telefonie- en datavoorziening weer is hersteld. Herstelwerkzaamheden worden bemoeilijkt doordat monteurs ook geen toegang tot interne digitale systemen hebben die noodzakelijk zijn voor onderhoudswerkzaamheden.

In dit scenario gaan we ervan uit dat het 72 uur duurt om het grootste deel van de netwerk- en telecomvoorzieningen in het getroffen gebied weer op gang te brengen met behulp van noodoplossingen en provisorische oplossingen.

Uitval van elektriciteit

In een regio van Nederland valt de stroom uit, waardoor de 2 miljoen klanten van een netbeheerder zonder stroom komen te zitten. Al snel wordt duidelijk dat het om een aanval van een statelijke actor gaat. Bij de aanslag zijn op meerdere plekken verdeelstations kapot gemaakt. De netbeheerders werken aan herstel. Het is onduidelijk hoe lang het zal duren voor de elektriciteitsvoorziening weer is hersteld.

De uitval heeft onmiddellijk grote gevolgen op het dagelijks leven. Elektrische apparaten met een accu, zoals mobiele telefoons en laptops, maar ook medische thuisapparatuur en elektrische auto's kunnen enkele uren functioneren, maar vallen vervolgens ook uit. De telecommunicatie valt binnen enkele uren ook grotendeels

uit. Het toonbankbetalingsverkeer raakt verstoord, waardoor men niet meer kan afrekenen in onder andere supermarkten en apotheken.

Ook contant geld opnemen is niet meer mogelijk door de uitval van pinautomaten. Het treinverkeer valt uit, wat voor grote drukte op de stations zorgt. Het verkeer op wegen loopt vast vanwege het uitvallen van matrixborden, verkeerslichten en op afstand bestuurbare infrastructuur als bruggen. Schiphol ligt buiten het gebied waar de stroom is uitgevallen, maar raakt wel ontregeld door het vastlopen van snelwegen en treinen.

Ongeveer een dag na de uitval vallen meer nutsvoorzieningen uit. De verwarming doet het niet meer en bij woningen boven de tweede verdieping komt er geen water meer uit de

kraan. Er ontstaan problemen met de noodstroomvoorzieningen bij vitale objecten, omdat brandstofvoorraden niet overal aanwezig zijn.

Het duurt 72 uur om het grootste deel van de stroomvoorziening in het getroffen gebied weer op gang te brengen met behulp van noodoplossingen, hulp uit het buitenland en provisorische oplossingen.

Nederland betrokken bij een militair conflict

Nederland raakt betrokken bij een militair conflict in Oost-Europa en zal moeten voldoen aan haar bondgenootschappelijke verplichtingen onder de NAVO. Het betreft een langdurige situatie met daarin de volgende gebeurtenissen:

- Doorvoer van grote hoeveelheden militair materiaal en personeel zorgt ervoor dat transport van andere goederen wordt verstoord.
 - Door dreiging ten aanzien van zeehavens en transportverbindingen worden handel en economie breed en langdurig verstoord.
 - Europese landen aan de oostgrens hebben een mobilisatie afgekondigd waar veel arbeidsmigranten gehoor aan geven.
- Defensie heeft beperkt capaciteit om zich te richten op haar derde hoofdtaak: ondersteuning van de civiele maatschappij bij rampen of crisis, of voor de beveiliging van objecten.
 - Er is sprake van een vluchtelingstroom naar Nederland.
 - Ziekenhuizen liggen vol, gewonde militairen en vluchtelingen belasten het Nederlands zorgsysteem maximaal.

Bijlage 2 - Test jouw weerbaarheid

Stel je voor:

Het is maandagochtend, jouw winkel of bedrijf is open. Plotseling valt de stroom uit.

Geen licht, het wordt snel kouder, geen pinbetalingen, geen e-mail, geen contact met personeel of thuis. Je weet niet of het drie uur of drie dagen zal duren. De klok tikt.

Denk dan aan de volgende vragen:

- Wat doe je als eerste?
- Waar dreigt nu een acuut gevaar?
- Welke processen in het bedrijf liggen direct of snel stil?
- Welke schade is onomkeerbaar of (te) groot?
- Welke afspraken heb je met personeel, klanten en leveranciers om voorlopig door te kunnen?
- Wie informeer je als eerste en op welke manier?
- Wat heb je geregeld om onverwachte tegenslagen op te vangen?
- Hoe zorg je dat je zo snel mogelijk weer operationeel bent?

Gebruik hierbij het handboek voor in nood en de checklist(s). Zijn jouw personeel, jijzelf en jouw belangrijkste ketenpartners voorbereid om hiermee om te gaan en te handelen? Zo niet, wat hebben jullie (aanvullend) nodig om beter voorbereid te zijn?

Behoeftte om meer van dit soort tests uit te voeren?

Varieer in de bovenstaande casus bijvoorbeeld de dag, het tijdstip of de afwezigheid van jezelf als eerste verantwoordelijke. Of gebruik één van de andere scenario's.¹⁹

¹⁹ [Gesprekstool Maatschappelijke Weerbaarheid \(light versie\) | Nationaal Coördinator Terrorismebestrijding en Veiligheid \(https://www.nctv.nl/documenten/2025/07/22/gesprekstool-maatschappelijke-weerbaarheid-light-versie\)](https://www.nctv.nl/documenten/2025/07/22/gesprekstool-maatschappelijke-weerbaarheid-light-versie)

Colofon

Projectleider:

Sabine Gielens, VNO-NCW en MKB-Nederland

Auteur:

Laurens van der Sluys Veer, International Safety Research Nederland

Illustraties:

Willemijn ten Wolde, Tante Willem

Vormgeving:

Anoeska Kruithof, VNO-NCW en MKB-Nederland

Druk:

Drukkerij Vegron BV, Den Haag

© VNO-NCW en MKB-Nederland, januari 2026

Coverfoto: Erik van 't Woud/ANP

2500086

VNO-NCW

MKB
Nederland

