ISO publiceert richtlijnen voor crisismanagement

Onlangs is ISO 22361 'Crisismanagement (CM) - Richtlijnen' gepubliceerd. Deze ISO-norm is uitstekend te combineren met ISO 22301 Business Continuity Management en ISO 31000 Risicomanagement, waardoor organisaties geholpen worden zich optimaal voor te bereiden op disruptieve gebeurtenissen die grote impact hebben op de organisatie en haar omgeving.

Door Dick Hortensius, NEN en Gert Kogenhop, Kader group

Crises lijken tegenwoordig aan de orde van de dag te zijn. Maatschappelijke crises, zoals de crisis in de opvang van asielzoekers, de stikstof-, corona- en klimaatcrisis. Maar ook op het niveau van een organisatie: een crisis als de stroom uitvalt in een ziekenhuis of een bedrijf dat plat komt te liggen vanwege een ransomware-aanval. In zo'n situatie is het zaak snel te handelen om onherstelbare schade voor de organisatie, voor de mensen die daar werken, voor de klanten en andere belanghebbenden te voorkomen. Een combinatie van het managen van de crisissituatie (CM) en de zorgen voor de continuïteit van levering van de producten en diensten (BCM). En ondanks dat elke crisissituatie unieke kenmerken heeft, geldt bij het managen van een crisis toch dat een goede voorbereiding het halve werk is. Daarvoor geeft ISO 22361 praktische handvatten.

Wat is een crisis?

In ISO 22361 wordt een crisis omschreven als *'een abnormale of **uitzonderlijke** gebeurtenis of situatie die een **bedreiging** vormt voor een organisatie of gemeenschap en die een strategische, **adaptieve en tijdige** respons vereist om ervoor te zorgen dat **vitaliteit en integriteit** ervan in stand blijven'*.

In deze omschrijving zijn een paar belangrijke woorden vet aangegeven. Het gaat om bijzondere en in het algemeen weinig voorkomende situaties, maar die wel een ernstige bedreiging voor de organisatie vormen. Daarom is het belangrijk tijdig (snel) te reageren om, soms in extreme gevallen, het voortbestaan van de organisatie te waarborgen. Omdat elke crisissituatie anders is en onvoorspelbaar kan verlopen is een flexibele en telkens aan de omstandigheden aan te passen respons nodig. Crisismanagement is dan ook niet iets wat een organisatie tot in de puntjes kan voorbereiden. ISO 22361 spreekt daarom van het ontwikkelen van een vermogen (*capability*) om crises te managen, te beheren en beheersen.

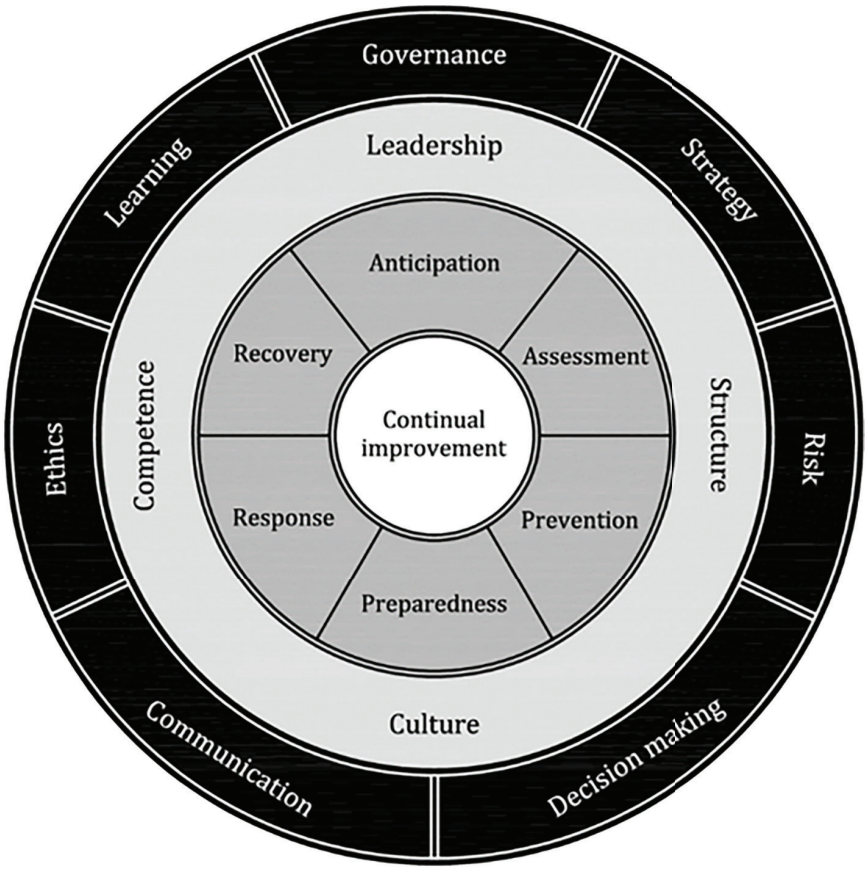
Ondanks dat elke crisissituatie unieke kenmerken heeft, geldt bij het managen van een crisis toch dat een goede voorbereiding het halve werk is. Daarvoor geeft ISO 22361 praktische handvatten.

Principes voor crisismanagement

ISO 22361 benoemt een aantal uitgangspunten voor crisismanagement. De belangrijkste daarvan zijn:

- **Governance**: effectieve besturing en leiderschap op alle niveaus in de organisatie met duidelijke toebedeling van rollen, verantwoordelijkheden en de definiëring van de daarvoor benodigde competenties;
- **Risicomanagement**: situationeel en risicobewustzijn op basis van actieve monitoring van interne en externe omgevingsfactoren en beoordeling van potentiële kwetsbaarheden;
- **Besluitvorming**: gebaseerd op goede informatie, situationeel bewustzijn en inzicht in de eisen en verwachtingen van belanghebbenden;
- **Communicatie**: het geven van accurate, geloofwaardige en tijdige informatie aan interne en externe belanghebbenden;
- **Leren**: het vergroten van het vermogen om crises te managen door training en oefening en leren van (ook andermans) ervaringen.

Het ontwikkelen van een goed vermogen voor crisismanagement omvat twee hoofdcomponenten: het opzetten van een *raamwerk voor risicomanagement* en het inrichten van een *risicomanagementproces*. Het raamwerk moet ervoor zorgen dat crisismanagement onderdeel gaat uitmaken van de belangrijke activiteiten en functies van de organisatie: topmanagement en leiderschap, structuur (rollen, verantwoordelijkheden, bevoegdheden, procedures, faciliteiten), cultuur (waaronder



Principes, raamwerk en proces voor crisismanagement volgens ISO 22361.

risicobewustzijn) en competentieontwikkeling op alle niveaus in de organisatie. Het risicomanagementproces omvat alle stappen/fasen die moeten worden doorlopen om vroegtijdig een crisissituatie op te merken en die effectief te managen. Denk in dit geval aan *anticiperen*: voortdurend scannen en monitoren van de omgeving om '*early warning*' signalen van een mogelijke crisis op te vangen. *Beoordelen*: inzicht in en beoordeling van mogelijke risico's binnen en buiten de organisatie die tot een crisis kunnen leiden. Zeker ook *preventie en mitigatie*: voorzorgsmaatregelen treffen die de kans op een crisis verkleinen en interventiemaatregelen om te voorkomen dat een (klein) incident zich verder ontwikkelt tot een grote crisis. Vanzelfsprekend ook optimale *voorbereiding* in de vorm van het opstellen van een crisismanagementplan en inrichten van een crisismanagementteam en *response*, reageren op de crisis en acties nemen die passen bij de dynamiek en complexiteit van de crisis zoals die zich daadwerkelijk voordoet en zich verder ontrolt. Voorts *herstel*, de terugkeer naar de 'oude' situatie of een aangepast 'nieuwe normaal' en uiteindelijk *verbeteren en leren*. Onder het bekende motto '*never waste a good crisis*' lessen trekken uit wat zich heeft voorgedaan en zo het vermogen verbeteren om op een volgende crisis te reageren.

Op de belangrijkste componenten en succesfactoren van crisismanagement wordt in ISO 22361 in enkele verdiepende hoofdstukken uitgebreid ingegaan om deze de juiste waarde en aandacht te geven. Uitermate belangrijk is crisisleiderschap. Wat zijn de belangrijkste vaardigheden en kenmerken van een 'goede leider' in crisissituaties en hoe kun je die ontwikkelen? Wat zijn de rollen en verantwoordelijkheden tijdens de crisissituatie en hoe vul je die in de praktijk in? Er moeten besluiten worden genomen, soms onder enorme druk. Hoe zorg je voor een zo goed mogelijke informatiebasis voor beslissingen? Welke perspectieven en percepties zijn belangrijk om mee te wegen? Hoe ga je om met tijdsdruk, stress, het betrekken van belanghebbenden en de benodigde wendbaarheid en flexibiliteit? Eén van de belangrijkste componenten – en waar het ook vaak mis gaat weten we inmiddels uit ervaring – is de crisiscommunicatie. Veel zaken zijn voor te bereiden (standaardteksten, sjablonen, rollen, (sociale) media-overzichten, communicatiekanalen), maar elke crisis zal een specifieke strategie, aanpak en doelgroep hebben en dus is een goed voorbereid communicatieteam essentieel. Zonder regelmatige aandacht in de vorm van training, oefening en evaluatie wordt een onnodig risico genomen. Zorg er dus voor dat de benodigde competenties worden ontwikkeld, bepaalde scenario's daadwerkelijk worden geoefend en de ervaringen daarbij goed geëvalueerd en verwerkt worden in crisismanagementplannen. En natuurlijk een uitgebreide evaluatie van de aanpak van een crisis die zich daadwerkelijk voordeed.

Als je terugdenkt aan de aanpak van de Coronacrisis in de afgelopen jaren, kost het waarschijnlijk weinig moeite om het belang van bovenstaande punten te onderkennen, te zien welke invulling en inkleuring er toen aan is gegeven en wat daar (achteraf bezien) wel en minder effectief was.

De NEN-normcommissie

De ontwikkeling van ISO 22361 is actief gevolgd en beïnvloed door de NEN-normcommissie 'Business continuity management en crisismanagement'. Enkele leden van de normcommissie hebben deelgenomen aan de vele vergaderingen van de ISO-werkgroep die de teksten voorbereidde en daarop ingebrachte commentaren verwerkte. Momenteel werkt de commissie aan de Nederlandse vertaling van ISO 22361 die in de loop van 2023 zal worden gepubliceerd.

Voor meer informatie over ISO 22361 en deelname aan deze normcommissie kunt u contact opnemen met Dick Hortensius, consultant managementsystemen bij NEN, telefoon 015 269 01 15, e-mail: mm@nen.nl of met Gert Kogenhop, voorzitter van de normcommissie, telefoon 06 53101821, e-mail: g.kogenhop@kader.nl

Hoe richt je een effectieve cybercrisis-organisatie in?

Organisaties getroffen door cyberaanvallen zoals ransomware zijn niet meer uit het nieuws weg te denken. Bedrijven en overheden zijn genoodzaakt om grote investeringen te doen om hun informatie en continuïteit te beschermen. Een belangrijk aspect hiervan is het revalueren van de huidige crisis- en calamiteitenorganisatie. Is de traditionele calamiteitenorganisatie wel bestand tegen een onzichtbare dreiging?

Door Erik Veldhuis, Expert IT Crisismanagement IND

Effectief cybercrisis-management begint met een passende crisisdefinitie, gebaseerd op de kritische processen binnen de organisatie. Wanneer is een incident in het cyberdomein voor de organisatie een crisis? Een heldere crisisdefinitie schetst kaders en geeft richting bij het bepalen van de potentiële impact van een incident. Een pragmatisch classificatiemodel kan uitkomst bieden bij het identificeren en classificeren van incidenten. Een overzichtelijke methode is om binnen cyber onderscheid te maken tussen vier impactgebieden, namelijk: dataprivacy, informatiebeveiliging (security), uitval van intern beheerde systemen en uitval van systemen bij leveranciers. Door het opstellen van classificaties per impactgebied binnen cybersecurity wordt er met een integrale blik gekeken naar de impact op de kerntaken van de organisatie. De classificaties dienen dan ook als ideaal startpunt voor het inrichten van efficiënte crisisorganisatie. Want wat moet u doen als u helder hebt wat voor uw organisatie een cybercrisis is?

Scenariodenken

De volgende stap is het inrichten van de (cyber) crisisorganisatie om te bepalen wie, wat maar ook wanneer actie ondernomen moet worden. Een pragmatische maar effectieve aanpak is om met de impactgebieden in het achterhoofd scenariodenken toe te passen en daarbij de volgende punten helder en concreet vast te leggen:

- een helder onderscheid tussen wat geldt als een cyberincident en als cybercrisis;
- duidelijke rollen en verantwoordelijkheden binnen zowel het escalatieproces als tijdens de crisis response;
- per impactgebied een opzet crisismanagementteam en ondersteunend(e) team(s);
- een overzicht met zowel interne als externe samenwerkingspartners en belanghebbenden – denk bijvoorbeeld aan een incident response samenwerkingspartij;
- duidelijke richtlijnen voor afschalen.

Vermijd hierbij complexe en overcomplete crisismanagementplannen, omdat die vrijwel altijd in een lade belanden. De ervaring leert dat een bondig maar compleet plan het meest effectief is voor crisisteams en ondersteunende teams die niet met regelmaat betrokken zijn binnen het crisismanagementproces. Zorg ervoor dat de initiële stappen ten tijde van een cybercrisis in één duidelijk overzicht staan en voeg per impactgebied een Quick Reference kaart toe. Een Quick Reference kaart kan refereren naar het crisisteam en bijbehorende rollen of personen per situatie; zo kan men snel handelen wanneer dit nodig is.

De mensen maken het verschil

De basis is op orde, en dan? Hoe goed er ook is nagedacht over de inrichting van een crisisstructuur en mogelijke cybercrisis scenario's; de mensen maken het verschil. Een combinatie van opleiden, trainen en oefenen is van het grootste belang bij de voorbereiding op een crisissituatie. Essentieel hierin is het element ervarend leren door het organiseren van tabletop oefeningen of crisis simulaties.