Auteurs: Pepijn van den Broek, partner bij ISR Nederland BV, Jean-Pierre van Eekelen, Corporate Business Continuity Officer ProRail, Gert Kogenhop, Operationeel Manager BCM Kader Group, Dick Hortensius, Senior-consultant managementsystemen, NEN Zorg, Consumenten en Maatschappij. Voor meer informatie over deze visie of het uitwisselen van ideeën erover neem contact op met de auteurs via pepijn.vandenbroek@isrnederland.nl.

Bescherming van vitale infrastructuur? Gebruik bestaande normen!

Bepaalde processen zijn zo essentieel voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting of grote economische schade leidt en een bedreiging vormt voor onze nationale veiligheid. Elektriciteit, toegang tot internet, drinkwater en betalingsverkeer zijn voorbeelden van deze vitale processen. Deze processen en hun infrastructuur vormen de Nederlandse vitale infrastructuur. Als vitale infrastructuur uitvalt, kan dat grote maatschappelijke gevolgen hebben.

De mogelijke grote maatschappelijke gevolgen zijn de reden voor overheid, bedrijfsleven, hulpverleningsdiensten en inlichtingendiensten om nauw samen te werken om de bescherming van zulke vitale producten, diensten en processen continu te verbeteren en te borgen. De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) heeft een coördinerende rol bij de bescherming van onze vitale infrastructuur en het opstellen van beleid en wetgeving die hierbij horen. Echter, in de Nederlandse beschermingsaanpak van vitale infrastructuur, die sinds circa het jaar 2000 (als gevolg van de millenniumproblematiek) bestaat, wordt nauwelijks het gebruik van normen gestimuleerd als het gaat om hoe als vitaal aangemerkte organisaties (de vitale aanbieders) zich dienen te beschermen tegen uitval. De overheid vindt de processen die deze organisaties uitvoeren en de infrastructuur die ze daarbij gebruiken essentieel voor ons maatschappelijk functioneren, maar stelt nauwelijks eisen aan hoe risico's op uitval van hun vitale diensten beheerst dienen te worden.
Wanneer je als organisatie als vitale aanbieder bent geïdentificeerd én de essentiële processen/diensten die je levert afhankelijk zijn van ICT en dataverkeer én je bent aangewezen als Aanbieder van een Essentiele Dienst (AED) of als een Andere Aangewezen Vitale Aanbieder (AAVA), dan dien je aan specifieke eisen voor informatiebeveiliging te voldoen die gelden vanuit de Wet beveiliging Netwerk- en informatiesystemen (Wbni). Maar meer eisen gericht op instandhouding van vitale dienstverlening zijn er eigenlijk nauwelijks, zelfs niet met het actief worden van de nieuwe Europese richtlijn Critical Entities Resilience (CER).

En dat is op zijn minst best vreemd te noemen, in een tijd waarin we steeds afhankelijker worden van (ICT-)infrastructuur en we meer en meer gericht zijn op het uitbannen van risico's en het voorkomen van grote crises. Om die reden pleiten wij voor een verbeterde aanpak van de bescherming van de vitale infrastructuur, niet zozeer door meer wet- en regelgeving, maar door veel meer gebruik te maken van beschikbare internationale normen en standaarden en daarmee een betere aansluiting te realiseren bij gangbare risico- en crisisbeheersingsmethodieken binnen vitale organisaties en tevens te zorgen voor een meer uniforme, Europese aanpak.

Er wordt al jaren gewerkt aan het normaliseren en standaardiseren van processen om stabiele processen en producten te kunnen garanderen en risico's op afwijkingen te verkleinen. Onder andere de Internationale Organisatie voor Standaardisatie (ISO) werd hier in 1947 voor opgericht. De normen die door ISO worden ontwikkeld kunnen door organisaties over de gehele wereld worden gebruikt en zorgen ervoor dat processen, diensten, producten en materialen geschikt zijn voor hun doel. Ook zorgt ISO ervoor dat deze vereisten in alle aangesloten landen (167 in totaal) overeenkomen, zodat er sprake is van internationale standaardisering.

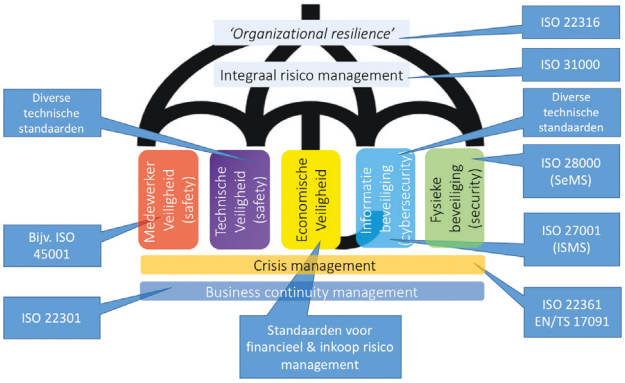
Een weerbare vitale infrastructuur door het gebruik van standaarden

Het doel van het Nederlandse programma Bescherming vitale infrastructuur onder regie van de NCTV is om de beveiliging en continuïteit van vitale processen en infrastructuur zo goed mogelijk te kunnen garanderen. Een stabiele vitale infrastructuur is dus eigenlijk niets minder dan het hebben van een stabiele en beheerste procesuitvoering met een focus op continuïteit. En dat is precies waar normen en standaarden bij kunnen helpen. Er zijn diverse standaarden gericht op risicobeheersing (ISO 31000), informatiebeveiliging/ cybersecurity (o.a. ISO 27001), crisisbeheersing (ISO 22361) en bedrijfscontinuïteit (ISO 22301) die door vitale aanbieders kunnen worden gebruikt om continuïteitsrisico's te mitigeren en effecten van verstoring sneller te verhelpen. Hiermee werken de vitale aanbieders aan risicobeheersing, weerbaarheid, continuïteit en veerkracht. In het Engels is daar een overkoepelende term voor, namelijk 'organizational resilience'.

'Organizational resilience: the ability of an organization to absorb and adapt in a changing environment'

(Bron: ISO 22316:2017 Security and resilience – Organizational resilience – Principles and attributes)

Organizational resilience gaat dus over de mate waarin een als vitale aanbieder aangemerkte organisatie in staat is zich 'te wapenen' tegen veranderingen en de risico's die daaruit kunnen ontstaan. Risico's die de bedrijfsvoering ernstig kunnen verstoren en dientengevolge de continuïteit van product- en dienstlevering kunnen bedreigen. Organizational resilience vormt als het ware de conceptuele paraplu waaronder alle aandachtsgebieden gericht op procesbeheersing en risicobeheersing zich bevinden. Ook voor organizational resilience is inmiddels een ISO-norm ontwikkeld, de standaard ISO 22316.



Figuur 1: model voor organizational resilience m.b.v. internationale standaarden – © ISR Nederland BV.

Dit model zou door vitale aanbieders, de verantwoordelijke ministeries en de toezichthouders als referentiekader gehanteerd kunnen worden om de organizational resilience van vitale aanbieders (en dus de weerbaarheid) aantoonbaar te verbeteren. Door vanuit beleid (de NCTV en de ministeries die beleidsverantwoordelijk zijn voor de aanbieders die vitale processen uitvoeren) het gebruik van standaarden meer te stimuleren en hier duidelijker op te sturen ontstaat een meer uniforme en toetsbare aanpak en risicobeheersing.

De vitale aanbieders kunnen deze internationaal geaccepteerde standaarden gebruiken om hun weerbaarheid te organiseren op een systematische en aantoonbare manier door gebruik te maken van de standaarden, de voorbeelden van beheersmaatregelen daarin en de lerende aanpak die erin is opgenomen. Daarnaast maakt het gebruik van standaarden het mogelijk voor vitale

‘Ter bevordering van de convergente uitvoering van deze richtlijn moedigen de lidstaten, waar nuttig en zonder het gebruik van een bepaald soort technologie op te leggen of te bevoorrechten, het gebruik aan van Europese en internationale normen en technische specificaties die relevant zijn voor de beveiligings- en weerbaarheidsmaatregelen die van toepassing zijn op kritieke entiteiten.’

(Artikel 16 CER-richtlijn).

aanbieders om eenvoudig en snel kennis van het toepassen van standaarden van de markt te betrekken. De toezichthouders hebben zeer waarschijnlijk ook baat bij meer gebruik van standaarden. Door een gestandaardiseerde aanpak neemt de toezichtlast waarschijnlijk af, omdat er duidelijker normen worden gehanteerd. Daarnaast is `metatoezicht’ mogelijk. Door als toezichthouder te kunnen vertrouwen op de gecertificeerde toepassing van de standaarden door de vitale aanbieders, kan efficiënter effectief toezicht plaatsvinden.
Een laatste voordeel van meer standaardisering is nog dat het eenvoudiger wordt om gestructureerd kennis op te bouwen over de beschermingsaanpak via regulier onderwijs en commercieel onderwijs. Met name omdat een aanpak via standaarden goed aansluit bij bestaande bedrijfskundige theorieën. Er zijn al tal van voorbeelden van succesvolle toepassing van normen in als vitaal aangemerkte sectoren, zoals NEN 7510 (gebaseerde op ISO 27001) voor informatiebeveiliging in de zorg en de NTA 8620 (gebaseerd op ISO 55001) voor assetmanagement bij netbeheerders. Deze normen geven praktische handvatten voor het voldoen aan algemene wettelijke zorgverplichtingen.

Ook op Europees niveau wordt het gebruik van standaarden voor de organisatie van meer weerbaarheid (resilience) gestimuleerd. De recent aangenomen nieuwe Europese richtlijn gericht op de verbetering van de weerbaarheid van kritieke/vitale sectoren, de Criticial Entities Directive (EU) 2022/2557 (hierna de CER-richtlijn) bevat ook een duidelijke eis richting de lidstaten om meer gebruik te maken van normen en standaarden.

De eisen uit de CER-richtlijn worden vanaf oktober 2024 van toepassing op alle Nederlandse vitale aanbieders. Op dit moment wordt door het ministerie van Justitie en Veiligheid de Nederlandse wet ontwikkeld die de Europese eisen verplicht zal stellen aan de Nederlandse vitale aanbieders. Daarom is volgens ons nú het moment om in de wet (of de toelichting daarop) de visie van organizational resilience te adopteren en het gebruik van standaarden als hulpmiddel voor de aantoonbare organisatie van weerbaarheid te stimuleren. Op deze manier kan gebruik worden gemaakt van normen die vaak in samenwerking met vertegenwoordigers uit vitale sectoren zijn ontwikkeld waardoor deze aanpak op draagvlak en praktische toepasbaarheid kunnen bogen en er geen nieuwe wielen hoeven te worden uitgevonden.

Referenties

(1) https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen
(2) https://eur-lex.europa.eu/eli/dir/2022/2557/oj