Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

30 821 Nationale Veiligheid

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 203

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 22 december 2023

Tijdens het Commissiedebat Online veiligheid en cybersecurity op 29 juni jl. heb ik toegezegd uw Kamer uiterlijk volgend jaar bij de update van de Aanpak vitaal te informeren over terugvalopties en de opbrengsten van de weerbaarheidsanalyses, conform de motie van de leden Rajkowski (VVD) en Van Raan (PvdD) over het in kaart brengen in hoeverre terugvalopties nodig zijn voor het versterken van de digitale weerbaarheid (Kamerstuk 26 643 nr. 1053). Met deze brief informeer ik uw Kamer, mede namens het kabinet, over de invulling van de toezegging en de motie.

De weerbaarheidsanalyse binnen de Aanpak vitaal

De vitale infrastructuur bestaat uit processen en diensten die essentieel zijn voor de Nederlandse samenleving, zoals bijvoorbeeld elektriciteit, toegang tot internet en drinkwater. Uitval, verstoring of manipulatie van deze processen en diensten kan grote gevolgen hebben voor het functioneren van de Nederlandse economie en maatschappij en kan zelfs een bedreiging vormen voor de nationale veiligheid. De Aanpak vitaal is erop gericht om verstoring van vitale processen te voorkomen en de weerbaarheid aanhoudend te verhogen. Voor de zomer informeerde ik uw Kamer over de Aanpak vitaal.[1] In de cyclus vitaal, die onderdeel is van de Aanpak vitaal, identificeren vakdepartementen welke processen en aanbieders vitaal zijn en welke dreigingen en risico's binnen die vitale processen bestaan. Tevens worden maatregelen genomen om de weerbaarheid te verhogen. De cyclus vitaal bestaat uit vier stappen:

1. Vitaalbeoordeling: bepalen wat een vitaal proces is (bijvoorbeeld drinkwatervoorziening of giraal betalingsverkeer) en welke bedrijven en organisaties vitale aanbieders zijn.
2. Weerbaarheidsanalyse: analyse van de belangrijkste dreigingen en risico's en hoe weerbaar deze processen zijn.
3. Actieprogramma: op basis van de weerbaarheidsanalyses worden acties geformuleerd om de weerbaarheid te versterken.

[1] *Kamerstukken II* 2022/23, 30 821, nr. 182.

kst-30821-203
ISSN 0921 - 7371
's-Gravenhage 2023

4. Toetsen van de effectiviteit en het waar nodig bijstellen van deze maatregelen.

Het verantwoordelijke vakdepartement voert deze cyclus uit voor ieder vitaal proces in samenwerking met de betrokken vitale aanbieders. Zo doet het Ministerie van Economische Zaken en Klimaat dit voor internettoegang en dataverkeer en het Ministerie van Volksgezondheid, Welzijn en Sport voor de zorg. Dit gebeurt minimaal elke vier jaar voor ieder vitaal proces of vaker als dat nodig is. De uitvoering van de cyclus vitaal is daarnaast ook relevant voor de implementatie van de *Critical Entities Resilience directive* (CER-richtlijn) en *Network and Information Security directive* (NIS2-richtlijn), waar het kabinet op dit moment aan werkt. [2] De cyclus vitaal speelt een belangrijke rol in de vertaling van deze richtlijnen naar de Nederlandse werkelijkheid, bijvoorbeeld omdat de analyses behulpzaam zijn om inzicht te krijgen in de risico's waar organisaties die onder de richtlijnen vallen zich tegen dienen te beveiligen. Het kabinet streeft er naar de cyclus vitaal uiterlijk in Q1 2026 opnieuw te hebben doorlopen voor de sectoren uit deze richtlijnen.

Binnen de cyclus vitaal is daarnaast voortdurend aandacht voor het verhogen van de fysieke en digitale weerbaarheid van vitale processen. Zo worden er soms versnelde analyses of *quickscans* uitgevoerd bij een actualiteit of dreiging. Denk bijvoorbeeld aan Covid-19, de Russische inval in Oekraïne, de explosies bij Nordstream 1 en 2 of een ontwikkeling in technologie. Op deze manier is er, naast de looptijd van de cyclus vitaal, ook regelmatige informatie-uitwisseling tussen overheden en vitale aanbieders over belangen, dreigingen, weerbaarheid en maatregelen om deze risico's te mitigeren.

Inhoud van een weerbaarheidsanalyse en actieprogramma

In de weerbaarheidsanalyses worden relevante dreigingen voor het vitale proces in kaart gebracht, mede op basis van inzichten uit de Rijksbrede Risicoanalyse.[3] Dit kunnen bijvoorbeeld zijn:
- Klimaat- en natuurrampen
- Zware ongevallen
- Cyberdreigingen zoals digitale sabotage of spionage
- Ongewenste strategische afhankelijkheden
- Afhankelijkheden van andere vitale processen

Vervolgens wordt gekeken naar de fysieke, digitale en economische weerbaarheid hiertegen, maar ook naar ketenafhankelijkheid en crisisbeheersing. De volgende onderwerpen komen hier o.a. aan bod:
- Beleid, wet- en regelgeving
- Risicomanagement
- *Business continuity management*
- Samenwerking binnen de sector
- Incidenten

In een actieprogramma worden (aanvullende) maatregelen en acties opgesteld. Die acties kunnen zowel sectoraal als sectoroverstijgend zijn. Voorbeelden zijn:
- Inbouwen van redundantie
- Aanleggen van voorraden

[2] Voor een korte toelichting op de richtlijnen, zie *Kamerstukken II* 2022/23, 30 821, nr. 182.
[3] Analistennetwerk Nationale Veiligheid, *Rijksbrede Risicoanalyse Nationale Veiligheid*, 2022. Kamerstukken II 2022/23, 30 821, nr. 165.

– Realiseren van een alternatieve werkwijze (binnen het vitale proces en/of bij afnemers van een digitale dienst)
– Realiseren van aanvullende wet- of regelgeving

Alternatieve werkwijzen

De motie van de leden Rajkowski en Van Raan vraagt om in de weerbaarheidsanalyses in kaart te brengen in hoeverre terugvalopties nodig zijn voor het versterken van de weerbaarheid van vitale processen. Onze samenleving is sterk gedigitaliseerd. Digitale processen, systemen en netwerken zijn complex en steeds meer met elkaar verweven.[4] Hierdoor neemt de kans op grootschalige uitval van bijvoorbeeld vitale processen toe. Het is belangrijk om de continuïteit van vitale processen te blijven waarborgen en om maatschappelijke ontwrichting te voorkomen. Hier wordt op gestuurd in de Aanpak vitaal.

Het formuleren van risicomitigerende en weerbaarheidsverhogende maatregelen is onderdeel van de cyclus vitaal. Het realiseren van een alternatieve werkwijze, zoals een digitale of analoge terugvaloptie, is een weerbaarheidsverhogende maatregel. In de cyclus vitaal worden alle mogelijke maatregelen in het Actieprogramma in samenhang bezien. Echter, in veel gevallen is het realiseren van een analoge terugvaloptie geen reële mogelijkheid vanwege verregaande digitalisering of buitenproportionele kosten. Dan wordt gekeken naar andere mitigerende maatregelen.

Uiteindelijk is iedere organisatie, vitaal en niet-vitaal, zelf verantwoordelijk voor de continuïteit van hun dienstverlening en het nemen van maatregelen om risico's te mitigeren. Het nemen van maatregelen is voor iedere organisatie maatwerk en afweging vindt onder andere plaats op basis van risicobeoordelingen, wettelijke kaders, het belang van de geleverde dienst, haalbaarheid en proportionaliteit. Door de implementatie van de CER-richtlijn en NIS2-richtlijn in Nederlandse wet- en regelgeving krijgen veel vitale aanbieders te maken met wettelijke verplichtingen en toezicht. Beide richtlijnen bevatten bijvoorbeeld een zorgplicht die entiteiten verplicht om passende en evenredige technische, operationele en organisatorische maatregelen te nemen om hun dienstverlening zoveel mogelijk te beschermen tegen fysieke risico's en risico's voor de beveiliging van de netwerk- en informatiesystemen. Op basis van de NIS1-richtlijn en de implementatie daarvan in de Wet beveiliging netwerk- en informatiesystemen kent een deel van de vitale aanbieders al soortgelijke verplichtingen en wordt daarop reeds toezicht gehouden.[5] [6]

Voortgang op de Aanpak vitaal

Als coördinerend bewindspersoon voor de bescherming van de vitale infrastructuur, wil ik uw Kamer jaarlijks informeren over de voortgang van de Aanpak vitaal. Deze jaarlijkse update gaat onder andere in op ontwikkelingen binnen de vitale infrastructuur, de cyclus vitaal, de wettelijke verplichtingen die volgen uit de CER-richtlijn en NIS2-richtlijn en maatregelen die vanuit de Europese Unie worden genomen.

---

[4] NCTV, *Cybersecuritybeeld Nederland 2023*, Kamerstukken II 2022/23, 26 643, nr. 1045.

[5] De sectoren die onder de huidige NIS1-richtlijn vallen zijn: energie, digitale infrastructuur, digitale dienstverleners, bankwezen, infrastructuur voor de financiële markt, gezondheidszorg, vervoer en drinkwater. Onder de NIS2-richtlijn worden deze sectoren uitgebreid met: beheerders van ICT-diensten, overheidsdiensten, ruimtevaart, post- en koeriersdiensten, afvalstoffenbeheer, chemische stoffen, levensmiddelen, vervaardiging, digitale aanbieders en onderzoek.

[6] *Kamerstukken II* 2020/21, 22 112, nr. 3053.

Daarnaast zal ik, conform de toezegging, waar mogelijk ingaan op de opbrengsten van de weerbaarheidsanalyses, bijvoorbeeld door relevante risico's en trends binnen vitale processen te beschrijven.[7] Ik informeer uw Kamer uiterlijk eind 2024 met een update van de Aanpak vitaal.

De Minister van Justitie en Veiligheid,
D. Yeşilgöz-Zegerius

[7] De inhoud van de weerbaarheidsanalyses zijn niet openbaar. Een analyse kan bedrijfsgevoelige informatie bevatten of (operationele) informatie die de veiligheid van de staat kan schaden. Bijvoorbeeld omdat er bepaalde kwetsbaarheden en risico's binnen vitale processen worden blootgelegd.