Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

26 643 Informatie- en communicatietechnologie (ICT)

30 821 Nationale Veiligheid

Nr. 1044

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 29 juni 2023

Bij het Commissiedebat Informatiebeveiliging bij de overheid op 5 april jl.[1] heeft het lid Leijten gevraagd naar de toepasbaarheid van bestaande criteria voor vitale digitale processen. Daarop heb ik toegezegd dat ik het onderzoek dat is uitgevoerd naar extra eisen en toezicht voor vitale digitale processen van de overheid, in juni met uw Kamer zal delen. Met deze brief ontvangt u het rapport *Gegevens, documenten en registraties van Nationaal Belang*[2] (hierna Het Rapport) en geef ik invulling aan deze toezegging.

Op dit moment wordt er gewerkt aan een versterkte aanpak voor de bescherming van de vitale infrastructuur door de Minister van Justitie en Veiligheid (JenV), die coördinerend Minister is voor de bescherming van de vitale infrastructuur en cybersecurity. Hierover is de Kamer op 30 mei jl. geïnformeerd.[3] De versterkte aanpak voor de bescherming van de vitale infrastructuur raakt ook mijn verantwoordelijkheid voor digitalisering, omdat uitval van onder meer «digitale overheidsprocessen» de dienstverlening aan onze burgers kan verstoren.

In mijn Kamerbrief *Generiek kader voor vitale digitale processen van de overheid* van 29 september 2022[4] heb ik aangegeven dat een apart kader voor vitale processen binnen de overheid niet zinvol is, omdat het om een betrekkelijk gering aantal processen gaat. Wel zie ik nut en noodzaak in van een zorgvuldig risico-afwegingsproces in de keuze van de te treffen maatregelen, daar waar het gaat om processen en/of systemen die bij (langdurige) onbeschikbaarheid een maatschappij-ontwrichtend effect kunnen hebben. Overheidsprocessen en/of -systemen met een potentieel ontwrichtend effect bij (langdurige) onbeschikbaarheid, kunnen ook

[1] Kamerstuk 26 643, nr. 1016.
[2] Zie bijlage.
[3] Kamerstuk 30 821, nr. 182.
[4] Kamerstuk 26 643, nr. 917.

kst-26643-1044
ISSN 0921 - 7371
's-Gravenhage 2023

organisatie-overstijgend zijn, doordat we in ketens met diverse partijen verbonden zijn.

Het Rapport geeft richting aan wat een zorgvuldig risico-afwegingsproces is en geeft de keuze wat de te treffen maatregelen zouden kunnen zijn voor processen en/of systemen die bij (langdurige) onbeschikbaarheid een potentieel ontwrichtend effect kunnen hebben (in het Rapport genoemd: nationale belangen) en hoe centraal toezicht er uit zou kunnen zien.

Op dit moment wordt ook onder coördinatie van de Minister van JenV gewerkt aan de implementatie van de herziene Netwerk- en Informatiebeveiligingsrichtlijn (NIS2-richtlijn) in wetgeving. Voor de sector overheid betekent deze wetgeving een kans om een versnelling te realiseren om informatieveiligheid voor de publieke sector wettelijk te verankeren. Ik heb dat tijdens het Commissiedebat op 5 april met u gedeeld.

De herziene Netwerk- en Informatiebeveiligingsrichtlijn (NIS2-richtlijn)[5] schrijft voor dat entiteiten op basis van proportionaliteit de maatregelen treffen om risico's voor hun netwerk- en informatiesystemen te beperken. Het onderscheid tussen de beveiliging van zogenoemde «nationale» belangen en reguliere belangen past bij het uitgangspunt van proportionaliteit. Deze eisen worden als onderdeel van NIS2 tevens wettelijk verankerd.

Ik ben verder voornemens om Rijk/ZBO's, provincies, waterschappen en gemeenten te betrekken bij de aanstaande actualisatie van de Baseline Informatiebeveiliging Overheid (BIO).[6] De BIO geldt sinds eind 2018 als het basisnormenkader voor informatiebeveiliging waaraan alle overheden zich moeten houden en zichzelf ook aan hebben gecommitteerd. De geactualiseerde versie van de BIO is voorzien in 2024 van kracht te worden, eveneens het jaar waarin de NIS2-richtlijn van kracht wordt voor de Nederlandse context. Daarmee geef ik richting en invulling aan de NIS2-richtlijn ten aanzien van het proportionaliteitsbeginsel voor de te treffen beveiligingsmaatregelen bij de overheid. Tevens sluit ik met de actualisatie van de BIO aan bij (inter)nationale ontwikkelingen en geef ik toezicht nader vorm voor de sector overheid.

De afhankelijkheid van digitale processen is groot en is door de COVID-19-pandemie nog verder toegenomen. Incidenten zoals de problematiek rondom de software van het bedrijf Citrix in januari 2020 en de ransomware bij diverse overheden laten zien dat de afhankelijkheid van onze digitale dienstverleningsprocessen en systemen ons ook kwetsbaar maakt. Technologie en bijbehorende bedreigingen lijken zich sneller te ontwikkelen dan dat organisaties adequate beheersmaatregelen kunnen inrichten. Om die reden zet ik sterk in op kaderstelling en toezicht, zoals de in deze brief uitgewerkte aanpak.

Permanente aandacht voor adequate beheersmaatregelen blijft nodig voor de risico's die verdergaande technologische en maatschappelijke ontwikkelingen brengen.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
A.C. van Huffelen

---

[5] Op dit moment wordt onder coördinatie van de Minister van JenV gewerkt aan de implementatie van de herziene NIS2-richtlijn.

[6] Stcrt. 2019, nr. 26526.