Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 749

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 18 maart 2021

Langs deze weg informeer ik uw Kamer over verschillende trajecten die betrekking hebben op het thema informatieveiligheid bij de overheid. Ik blik terug op de in 16 oktober 2018[1] aangekondigde maatregelen die overheidsbreed zijn getroffen om de informatieveiligheid bij de overheid te verhogen. Deze maatregelen zijn onderdeel van een interbestuurlijke actie-agenda informatieveiligheid, een belangrijk onderdeel van de agenda NL DIGIbeter. Deze voortgangsbrief doet verslag van wat er in de periode 2018–2020 is ondernomen om de digitale weerbaarheid bij de publieke sector te verhogen en biedt een vooruitblik op de activiteiten die vanaf dit jaar plaatsvinden. Over de voortgang bij de Rijksdienst heb ik uw Kamer op 5 februari jl. geïnformeerd.[2]

De interbestuurlijke actie-agenda was gericht op het op orde brengen en houden van de informatieveiligheid van overheidsorganisaties en het bevorderen van overheidsbrede samenwerking. Ook het bieden van een veilige digitale dienstverlening aan burgers en ondernemers en het treffen van maatregelen om uitval/stilstand tegen te gaan waren onderdeel van de actie-agenda.

De in oktober 2018 aan uw Kamer aangekondigde maatregelen zijn gerealiseerd, met uitzondering van een tweetal wetgevingstrajecten. Het eerste wetgevingstraject gaat over opname van de categorie digitale overheid als vitale infrastructuur, onderdeel van de Wet beveiliging netwerk- en informatiesystemen (Wbni). Naar verwachting zal de herziening van het bijhorend besluit van deze wet in de eerste helft van dit jaar in werking treden. En het tweede wetgevingstraject gaat over het verplichten van de open informatieveiligheidsstandaard HTTPS. Na inwerkingtreding van de aanstaande Wet Digitale Overheid, die momenteel bij de Eerste Kamer ter behandeling ligt, wordt de

[1] Kamerstuk 26 643, nr. 574.
[2] Kamerstuk 26 643, nr. 739.

kst-26643-749
ISSN 0921 - 7371
's-Gravenhage 2021

mogelijkheid geboden om de open standaard HTTPS bij algemene maatregel van bestuur (AMvB) te verplichten.

Overheidsorganisaties zijn zelf verantwoordelijk voor de wijze waarop het informatieveiligheidsbeleid in hun organisatie gestalte krijgt. Mijn taak als Staatssecretaris is kaderstellend, voorts ondersteunend, en waar nodig aanjagend naar alle overheidslagen. Met onze medeoverheden streven we vooral naar uniformiteit van de aanpak binnen de overheidslaag zelf en zorgen we voor optimale afstemming tussen de overheidslagen. Hiermee kunnen we echt werken als één overheid. En dat is waar ik mij sterk voor maak.

Langs de volgende thema's zal ik uw Kamer informeren:
1. Kaders en standaarden
2. Oefenen en crisisbeheersing
3. Vitaal en versleuteling
4. Pilots met informatieveiligheid
5. Verankering in wet- en regelgeving

1. Kaders en afspraken

Baseline Informatiebeveiliging Overheid (BIO)

Sinds eind 2018 geldt de BIO, waarin de normen voor informatiebeveiliging zijn vastgelegd waaraan alle overheden zich moeten houden.[3] Binnen de overheidslagen Rijk, provincies, gemeenten en waterschappen is in samenwerking met het Centrum voor Informatiebeveiliging en Privacybescherming (CIP) een groot aantal biogerelateerde hulpmiddelen en producten ontwikkeld, verzameld en ontsloten via het bioportaal www.bio-overheid.nl. Op dit portaal zijn onder andere webinars en handreikingen te vinden. Overheidsorganisaties worden hiermee praktisch geholpen en ook geïnspireerd op het gebied van informatieveiligheid.
Door de COVID-19-pandemie zijn specifiek voor de overheden ontwikkelde BIO ondersteuningsprogramma's in hoog tempo overgeschakeld naar digitale werkvormen. Hierdoor is het bereik van deze programma's vergroot.

Veilig inkopen bij de overheid

De overheid kan met haar inkoopbeleid de vraag naar digitaal veilige ICT-producten en diensten stimuleren door informatieveiligheids-eisen op te nemen in het inkoopbeleid. In het kader van deze actielijn is een online instrument met de naam «Inkoopeisen Cybersecurity Overheid» (ICO) ontwikkeld. Dit instrument is sinds maart vorig jaar online beschikbaar als prototype.[4] Een expertgroep met vertegenwoordigers vanuit het Rijk, provincies, gemeenten en waterschappen heeft bijgedragen aan het formuleren van informatieveiligheids- eisen voor verschillende inkoopcategorieën, zoals clouddiensten en serverplatformen.[5] Om een breed beeld te krijgen van de praktische uitwerking van het instrument worden pilots binnen alle overheidslagen uitgevoerd. Deze worden in het eerste kwartaal van 2021 afgerond. Binnen de verschillende overheidslagen worden ook andere hulpmiddelen ontwikkeld waarmee veilige ICT-inkoop

[3] Stcrt. 2019, nr. 26526.
[4] De ICO-wizard is te vinden op https://www.bio-overheid.nl/ico-wizard/
[5] De onderkende inkoopsegmenten zijn: Applicatieontwikkeling algemeen, Clouddiensten, Communicatievoorzieningen, DiGiD applicaties, Huisvesting IV, Maatwerk of maatwerkpakket, Middleware, Mobiele Applicaties, Serverplatform, Softwarepakketten en Toegangsbeveiliging.

kan worden gestimuleerd. Overheidsbreed wordt eraan gewerkt deze hulpmiddelen op elkaar aan te laten sluiten.

Eenduidige Normatiek Single Information Audit (ENSIA)

ENSIA heeft tot doel te komen tot een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid bij gemeenten, gebaseerd op de BIO.[6] De verantwoordingssystematieken van zeven stelsels zijn in ENSIA samengevoegd en geharmoniseerd.[7] Op die manier is één verantwoordingsproces gerealiseerd. ENSIA vormt de basis voor de verantwoording van het college aan de gemeenteraad. Begin 2020 is de werking van het ENSIA-stelsel geëvalueerd.[8] Belangrijkste conclusie is dat de implementatie van ENSIA de bewustwording over het thema informatieveiligheid bij gemeenten heeft vergroot, maar dat er ook behoefte is om het stelsel effectiever en efficiënter te kunnen toepassen. De aanbevelingen uit het evaluatierapport worden momenteel ter hand genomen. In dit kader wordt gewerkt aan een nieuw ondersteuningsinstrument van ENSIA, om verbeteringen te kunnen doorvoeren.

Verhogen adoptie informatieveiligheidsstandaarden

Burgers en ondernemers moeten erop kunnen vertrouwen dat gegevensuitwisseling met de overheid veilig verloopt. Om dit te kunnen waarborgen, dienen overheden onder andere diverse open standaarden zoals informatieveiligheidsstandaarden te implementeren. De adoptie van deze informatieveiligheidsstandaarden wordt halfjaarlijks gemeten. Halverwege 2020 zijn achterblijvende overheidsorganisaties aangeschreven door het Forum Standaardisatie met adviezen ter verbetering.[9] De toepassing van de overige open standaarden van de «pas-toe-of-leg-uit» lijst van het Forum Standaardisatie wordt jaarlijks gemeten. De meest recente versie van deze Monitor Open standaarden 2020 wordt uw Kamer hierbij aangeboden.[10] Het beeld is dat het gebruik van de verplichte open standaarden verder toeneemt.

PKIoverheid

Begin juli 2020 werd een wereldwijd probleem met digitale certificaten geconstateerd, waaronder met PKIoverheid-certificaten. Daarover is uw Kamer geïnformeerd op 7 oktober 2020.[11] Deze certificaten worden gebruikt voor veilige dienstverlening en gegevensuitwisseling tussen burgers en bedrijven met de overheid, zowel voor websites als voor communicatie tussen machines. Na analyse van het probleem bleek voor de oplossing van dit incident het vervangen van een specifieke set certificaten noodzakelijk. Er is een vervangingsplan voor de betreffende certificaten opgesteld en de vervanging is najaar 2020 in gang gezet. De

---

[6] De ENSIA verantwoording is met ingang van het verantwoordingsjaar 2020 gebaseerd op de BIO in plaats van de Baseline Informatieveiligheid Nederlandse Gemeenten (BIG).

[7] Het betreft de Basisregistratie Personen (BRP) en wet- en regelgeving Reisdocumenten (PUN / PNIK), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet).

[8] Zie voor het onderzoek https://www.rijksoverheid.nl/documenten/rapporten/2020/05/28/evaluatie-en-versterking-ensia-stelsel

[9] De meting van de informatieveiligheidsstandaarden van september 2020 is te vinden op https://www.digitaleoverheid.nl/nieuws/beveiliging-internetdomeinen-overheid-vereist-voortdurende-aandacht/

[10] De monitor Open Standaarden, inclusief de informatieveiligheidsstandaarden, van september 2020 is te vinden op https://www.forumstandaardisatie.nl/publicaties/overige-publicaties

[11] Kamerstukken 26 643 en 31 490, nr. 713

certificaathouders hebben vervolgens in januari 2021 de certificaten ingetrokken, wat goed is verlopen. Naast deze oplossing voor de korte termijn wordt ook gekeken hoe de robuustheid en flexibiliteit van het PKIoverheid-stelsel versterkt kan worden op lange termijn. Bij de analyse wordt ook eerder onderzoek uit 2019 naar de toepassing van PKIoverheid-certificaten betrokken.[12]

Veilige overheidswebsites

Om de beveiliging van overheidswebsites verder te bevorderen, wordt gewerkt aan het verplicht stellen van de open informatieveiligheidsstandaard HTTPS (het kenmerkende slotje in de adresbalk van de internetbrowser) en de complementaire HSTS-standaard (deze ondersteunt HTTPS en zorgt ervoor dat een webbrowser, na het eerste contact over HTTPS, bij vervolgbezoek de website altijd direct over HTTPS opvraagt) voor het beveiligen van de verbinding met overheidswebsites en webapplicaties. Deze standaarden dragen gezamenlijk bij aan het vertrouwelijk houden van de gegevensuitwisseling met overheidswebsites en -webapplicaties. De concept Wet Digitale Overheid, die momenteel bij de Eerste Kamer ter behandeling ligt, biedt de mogelijkheid om deze open standaarden bij algemene maatregel van bestuur (AMvB) te verplichten.

Herkenbaarheid van overheidswebsites en e-mail

Een veilige en betrouwbare overheid moet ook goed herkenbaar zijn voor burgers en ondernemers. Uit onderzoek naar de herkenbaarheid van en vertrouwen in websites en e-mails van de overheid,[13] is gebleken dat burgers en ondernemers moeite hebben de digitale overheid te herkennen. In hetzelfde onderzoek hebben burgers en ondernemers positief gereageerd op het idee van één domeinnaam-extensie, zoals in veel landen binnen en buiten de EU is ingevoerd.[14] Evenals op het idee om alle communicatie via één overheidsdienstenportal zoals mijn.overheid.nl te laten verlopen. Recent onderzoek naar het oordeel van burgers en ondernemers over overheidsdienstverlening bevestigt de behoefte aan realisatie van één landelijke website waarop informatie en transacties bijeen worden gebracht.[15]

Het herkenbaarheidsprobleem van de digitale overheid wordt mede veroorzaakt door een wildgroei aan internetdomeinen van de overheid.[16] De problematiek rondom de beheersing van internetdomeinen raakt aan verschillende disciplines zoals communicatie, informatiebeveiliging, informatiehuishouding en ICT-beheer. Voor het Rijk wordt door CIO Rijk een start gemaakt met plan van aanpak voor de verbetering van de beheersing van internetdomeinen, zodat beter gestuurd kan worden op het voldoen aan verplichte kaders en richtlijnen op het gebied van veiligheid en digitale toegankelijkheid. https://www.digitaleoverheid.nl/

---

[12] Zie voor het onderzoek https://www.rijksoverheid.nl/documenten/rapporten/2019/03/13/pki-overheid---onderzoek-naar-mogelijkheden-om-gebruik-te-vergroten-bijvoorbeeld-via-verplichtstelling

[13] Zie voor het onderzoek https://www.rijksoverheid.nl/documenten/rapporten/2019/01/31/herkenbaarheid-van-en-vertrouwen-in-websites-en-e-mails-van-de-overheid

[14] Zie voor het onderzoek https://www.rijksoverheid.nl/documenten/rapporten/2019/11/27/buitenlandonderzoek-domeinnaambeleid

[15] Zie voor het onderzoek Eindrapport onderzoek overheidsdienstverlening 2020 | Rapport | Rijksoverheid.nl

[16] Zie voor publicatie hierover op de website van het Bureau Forum Standaardisatie https://www.forumstandaardisatie.nl/nieuws/beveiliging-internetdomeinen-overheid-vereist-voortdurende-aandacht

nieuws/beveiliging-internetdomeinen-overheid-vereist-voortdurende-aandacht/

Overheidsbreed wordt de komende jaren gewerkt aan verankering van afspraken op het gebied van domeinnaambeleid via bijvoorbeeld de BIO en het Forum Standaardisatie. De eerder verrichte onderzoeken ter verbetering van de herkenbaarheid en betrouwbaarheid van overheidswebsites en e-mails, worden betrokken bij de verankering van afspraken op het gebied van domeinnaambeleid.[17]

2. Oefenen en crisisbeheersing

i-Bewustzijn Overheid

Sinds 2019 vindt jaarlijks de Overheidsbrede Cyberoefening[18] plaats. In deze Overheidsbrede Cyberoefening wordt aan de hand van een gesimuleerde hackaanval bij de systemen van een overheid geoefend met het goed afhandelen van een cyberincident. Naast de Overheidsbrede Cyberoefening wordt er ook steeds meer door de medeoverheden zelf op kleinere schaal geoefend. Zo heeft het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) subsidie ter beschikking gesteld voor de ontwikkeling van een drietal cyberoefenpakketten voor gemeenten[19] en provincies[20] (ontwikkeld door het Instituut voor Veiligheids-, en Crisismanagement) en zijn ook de waterschappen bezig om het thema oefenen invulling te geven.

De aanpak van de komende jaren zal zich richten op een interbestuurlijk oefen- en testprogramma, in aansluiting op het nationale oefen- en testprogramma binnen de Nederlandse Cybersecurity Agenda (NCSA) van de Minister van Justitie en Veiligheid. In het programma van het Ministerie van BZK zullen drie thema's centraal staan: kennis delen, testen[21] en oefenen[22]. Het bevorderen van overheidsbrede samenwerking en kennisdeling vormt hierbij steeds het uitgangspunt. Voor alle activiteiten geldt dat het programma vooral wil aansluiten bij wat er al is. Dit vanuit de gedachte dat er al heel veel kennis, kunde en materiaal beschikbaar is en verder ontwikkeld wordt bij de overheid.

Verder is in maart van dit jaar is een oefening met de G4 en de IBD[23] voorzien. De oefening richt zich primair op de interactie tussen lokale en nationale actoren in een cybercrisis en heeft als doel kennis op te doen over hoe wordt samengewerkt binnen de bestaande kaders, zoals het Nationaal Crisisplan Digitaal en de Handreiking cybergevolgbestrijding van de G4. De geleerde lessen van deze oefening worden ingebracht in de door de NCTV tweejaarlijks georganiseerde nationale cyberoefening

---

[17] Zie voor het onderzoek https://www.rijksoverheid.nl/documenten/rapporten/2020/07/08/een-herkenbare-en-betrouwbare-digitale-overheid

[18] Informatie over de Overheidsbrede Cyberoefening is te vinden op https://www.weerbaredigitaleoverheid.nl/

[19] De gemeentelijke cyberoefenpakketten zijn reeds gereed en te vinden op de website van de IBD: https://www.informatiebeveiligingsdienst.nl/project/cyberoefenpakket-vng-oefenscenarios-digitale-incidenten/

[20] Voor de provincies vindt oplevering van de cyberoefenpakketten dit jaar plaats.

[21] Testen is een «toetsing van de kwaliteit van zaken». Een test vindt veelal plaats op het daadwerkelijke digitale systeem, of in een testomgeving van dat systeem. Een test voorziet een meetbaar resultaat in de kwaliteit van beveiliging en geeft real-time inzicht in kwetsbaarheden.

[22] Een oefening is gebaseerd op een scenario en ziet toe op het bekwaam maken door herhaling. Door het oefenen van een incident is men beter in staat om tijdens daadwerkelijke incidenten adequaat te handelen.

[23] IBD is de Informatiebeveiligingsdienst van de Nederlandse gemeenten.

Isidoor. Aan Isidoor 2021 nemen meerdere onderdelen binnen de overheid deel om met elkaar te oefenen met het Nationaal Crisisplan Digitaal. Op die manier werken we concreet samen aan een éénduidige invulling van oefenen met digitale crises bij de overheid.

Redteaming

Een red team-oefening is een effectieve manier om de feitelijke informatieveiligheid van een organisatie te testen. Ethische hackers voeren bij een red team-oefening een realistische aanval uit die alle onderdelen van de deelnemende organisatie op de proef stelt op het gebied van organisatie, techniek en gedrag. Om bekendheid te geven aan dit type oefening heeft het Ministerie van BZK in 2019 een tweetal red team-oefeningen gefinancierd bij een provincie en waterschap en zijn de ervaringen en leerpunten met andere overheden gedeeld. Op deze manier wil ik aanjagend zijn richting alle overheden. Inmiddels is het beeld dat steeds meer overheden deze vorm van testen toepassen in hun eigen organisatie, wat ten goede komt aan het verhogen van de digitale veiligheid.

Incident response capaciteit

Om medeoverheden te ondersteunen met het interbestuurlijk beeld van de incident response capaciteit heeft het Ministerie van BZK in 2019 een verkenning uitgevoerd bij de bestuurslagen provincies, gemeenten en waterschappen. In het bijzonder is gekeken naar de monitoring- en detectiecapaciteiten van systemen en netwerken. De computercrisisteams (CSIRTS)[24] van de medeoverheden spelen een belangrijke rol om overheidsorganisaties te ondersteunen bij het voorkomen en verhelpen van digitale incidenten. De opbrengsten zijn overgedragen aan de bestuurslagen die de uitkomsten benutten om de incident response capaciteit van hun eigen bestuurslaag te versterken, daar waar dat nodig is gebleken uit de verkenning.

Digitale ontwrichting bij medeoverheden

In de kabinetsreactie op het WRR-rapport «Voorbereiden op digitale ontwrichting» van 20 maart 2020,[25] is aangegeven dat het Ministerie van BZK in overleg zal gaan met gemeenten, veiligheidsregio's, waterschappen en provincies. Doelstelling is te onderzoeken of de bestaande kaders en afspraken die er bestaan voldoende zijn of dat er aanvullende afspraken nodig zijn. In een brief van 3 februari 2021 van de Minister van Justitie en Veiligheid,[26] is aangegeven dat ik separaat in zal gaan op de uitkomsten van de uitgevoerde interbestuurlijke verkenning.[27] Dat doe ik via deze brief.

Uit de verkenning blijkt dat bij al deze overheidslagen tal van initiatieven worden ontplooid die in lijn zijn met de aanbevelingen vanuit het WRR-rapport om de digitale weerbaarheid van overheden te verhogen. Zo hebben de gemeenten een plan van aanpak voor hun sector opgesteld, te

---

[24] Het Nationaal Cybersecurity Centrum (NCSC) is het CSIRT voor het Rijk en vitale organisaties. Provincies verkennen, met subsidie beschikbaar gesteld door mijn ministerie, momenteel de inrichting van een CSIRT-functie voor het provinciaal domein. De waterschappen hebben sinds april 2017 samen met Rijkswaterstaat een CERT. Watermanagement en de gemeenten hebben sinds 2013 een eigen CERT, de Informatiebeveiligingsdienst (IBD).

[25] Kamerstukken 26 643 en 30 821, nr. 673.

[26] Kamerstuk 26 643, nr. 738.

[27] Zie voor het onderzoek https://www.rijksoverheid.nl/documenten/rapporten/2021/01/31/quick-scan-voorbereiding-op-digitale-ontwrichting

weten de gemeentelijke *Agenda Digitale Veiligheid 2020–2024*.[28] Ook is er een gemeentelijke handreiking voor cybergevolgbestrijding.[29] De veiligheidsregio's hebben de uitvoering van hun *Bestuurlijk routeboek digitale ontwrichting* opgestart.[30] Het Ministerie van Infrastructuur en Waterstaat heeft ter opvolging van het Bestuursakkoord Water een uitvoeringsprogramma *Versterken Cyberweerbaarheid in de Watersector* geïnitieerd, waarbij intensief wordt samengewerkt met waterschappen, gemeenten en provincies.[31] Provincies besteden vanuit de *Interprovinciale Digitale Agenda 2019–2023* aandacht aan samenwerking rondom digitale incidenten.[32] Met al deze bestuurlijke initiatieven boeken de medeoverheden vooruitgang met zowel het verhogen van de cyberweerbaarheid als met het beter voorbereid zijn op digitale ontwrichting. Voor dat laatste zal een optimale aansluiting worden gezocht op het reeds bestaande Nationaal Crisisplan Digitaal. Dat biedt snel inzicht en overzicht in mogelijke gevolgen en maatregelen, rollen, taken en bevoegdheden op nationaal niveau ten tijde van een digitale crisis.

Bovenvermelde initiatieven zijn waardevol en blijven, net als andere in deze brief genoemde stappen, belangrijk om voort te zetten. Deze huidige stappen zijn echter vooral gericht op de eigen bestuurslaag, met ieder hun eigen prioriteiten en accenten. Omdat digitale dreigingen zich niet aan deze organisatorische grenzen houden, is het ook nodig te werken aan de verdere verbetering van interbestuurlijke samenwerking en het borgen van samenhang tussen de bestaande initiatieven. Vanuit het Ministerie van BZK worden, in afstemming met het Ministerie van Justitie en Veiligheid en de medeoverheden, in de eerste helft van 2021 alle interbestuurlijke verbeteracties verzameld en uitgewerkt tot een verbeterplan. De maatregelen die worden getroffen naar aanleiding van de aan uw Kamer aangeboden evaluatie van de Wet veiligheidsregio's[33] van 4 december 2020 worden hierbij betrokken.

3. Vitaal en versleuteling

Vitale digitale overheid

Een aantal voorzieningen van de digitale overheid is als vitaal aangewezen. Deze voorzieningen zijn daarnaast aangewezen als Aanbieders van Essentiële Diensten (AED). Deze aanwijzing zal worden bevestigd in de herziening van het Besluit beveiliging netwerk- en informatiesystemen (Bbni) van de Minister van Justitie en Veiligheid. De Minister van Justitie en Veiligheid heeft de voorgenomen herziening van dit besluit, dat voortvloeit uit de Wet beveiliging netwerk- en informatiesystemen (Wbni), voorgelegd aan de Raad van State; over het onderdeel Digitale Overheid had de Raad geen opmerkingen. De wijziging zal naar verwachting in de eerste helft van dit jaar in werking treden.

Verder heeft het Ministerie van BZK een verkenning laten uitvoeren naar mogelijke vitale digitale overheidsvoorzieningen (producten en diensten) bij departementen, ZBO's, agentschappen, marktpartijen waarmee veel wordt samengewerkt en de decentrale bestuurslagen. Gebleken is dat er voorzieningen en informatieprocessen zijn waarvan uitval niet tot landelijke ontwrichting leidt, maar op lokaal en regionaal niveau wel. En

---

[28] Agenda Digitale Veiligheid 2020–2024, *een veilige (digitale) gemeente*, VNG
[29] Handreiking Cybergevolg-bestrijding (CGB) G4-gemeenten, Berenschot
[30] Bestuurlijk routeboek digitale ontwrichting, Veiligheidsberaad
[31] Versterken Cyberweerbaarheid in de Watersector 2019–2022, Ministerie van Infrastructuur en Waterstaat
[32] Interprovinciale Digitale Agenda 2019–2023, *regie op digitale transformatie,* Regiegroep digitale transformatie
[33] Kamerstuk 29 517, nr. 198.

uit de verkenning is naar voren gekomen dat er overheidsbreed behoefte bestaat aan een generiek kader voor vitale digitale overheidsvoorzieningen. Zodoende zal het Ministerie van BZK in 2021, in het kader van de overheidsbrede aanpak vitale infrastructuur, een algemeen kader voor de digitale overheid opstellen. Het Ministerie van BZK heeft in 2019 laten onderzoeken[34] welke best practices er op dit vlak in OESO landen voorhanden zijn. Dit onderzoek zal worden betrokken bij deze en andere vervolgstappen.

Versleuteling basisregistraties

Naar aanleiding van opname in het Regeerakkoord[35] dat gegevens van burgers in basisadministraties en andere privacygevoelige informatie altijd versleuteld worden opgeslagen, heb ik uw Kamer geïnformeerd op 21 oktober 2020.[36] In dat kader heeft onderzoek plaatsgevonden naar versleuteling van de Basisregistratie Personen (BRP).[37] Voor de BRP is onderzocht of de huidige veiligheidsmaatregelen voldoende bescherming bieden tegen mogelijke beveiligingsrisico's. Uit het onderzoek blijkt dat versleuteling op dit moment niet de meest passende maatregel is. Er is door het nemen van andere maatregelen meer winst te behalen bij het verbeteren van de bescherming van privacygevoelige informatie in de basisregistraties. Niet uitgesloten is dat door voortschrijdend inzicht gegevens in de toekomst wel (extra) worden versleuteld.

4. Pilots met informatieveiligheid

Integrale beveiligingsaanpak

Zoals aan uw Kamer aangekondigd op 2 juli 2020,[38] werkt het Ministerie van BZK samen met het Ministerie van Justitie en Veiligheid, relevante netwerkpartners waaronder de VNG en een aantal gemeenten aan de pilot «integrale beveiligingsaanpak». In deze aanpak worden zowel fysieke als digitale beveiliging aan elkaar verbonden. Tot de zomer van 2021 maken gemeenten, onder externe begeleiding en van elkaar lerend, voortgang op het gebied van integrale beveiliging. De opgedane kennis en ervaring maakt gemeenten beter weerbaar tegen ondermijnende invloeden en andere dreigingen. De opgedane en ontwikkelde kennis, informatie en ervaringen worden online gedeeld. Op deze manier kunnen ook andere gemeenten op een laagdrempelige en toegankelijke manier de informatie vinden die zij nodig hebben om hun integrale beveiligingsaanpak op te zetten of verder te brengen.

City Deal Lokale Weerbaarheid Cybercrime

Cybercrime is de laatste decennia een serieuze bedreiging geworden. En door de huidige COVID-19-pandemie en het thuiswerken is cybercrime ook toegenomen. Daarom hebben acht gemeenten, drie ministeries waaronder het Ministerie van BZK, zeven regionale veiligheidsorganisaties en vier kennisinstellingen in de City Deal Lokale Weerbaarheid Cybercrime op 28 oktober 2020 met elkaar afgesproken om burgers en

---

[34] Zie voor het onderzoek https://www.rijksoverheid.nl/documenten/rapporten/2020/02/19/onderzoek-vitale-infrastructuur-in-de-digitale-overheid

[35] Bijlage bij Kamerstuk 34 700, nr. 34

[36] Kamerstuk 27 859, nr. 148.

[37] Zie voor het onderzoek https://www.rijksoverheid.nl/ministeries/ministerie-van-binnenlandse-zaken-en-koninkrijksrelaties/documenten/rapporten/2020/10/18/rapport-noordbeek-doorlichting-veiligheid-basisregistratie-personen-brp

[38] Kamerstuk 28 844 nr. 218.

bedrijven weerbaarder te maken tegen cybercrime.[39] Zij zijn samen aan de slag om de «cyberweerbaarheid» te verhogen onder inwoners en bedrijven. Dit wordt gedaan in 18 lokale experimenten met inzet van onder andere digitale wijkambassadeurs, cyberbuddies en een lokale helpdesk bemand door IT-studenten. Een aantal experimenten die raken aan informatieveiligheid zijn onder andere het «barrièremodel ransomware». In dit experiment wordt er samen met ondernemers en maatschappelijke instellingen (als scholen en universiteiten) uit de regio Oost-Brabant een barrièremodel ontwikkeld om gijzelsoftware oftewel ransomware tegen te gaan. Ook moet duidelijk zijn wat men moet doen als een organisatie getroffen is. Het experiment «hackshield» is een cybersecurity game voor kinderen tussen de 8 en 12 jaar. Op een speelse manier leren kinderen zich wapenen tegen digitale gevaren. Kinderen worden dan «Junior Cyber Agent» en worden gestimuleerd het geleerde ook over te brengen op hun (groot)ouders. En het experiment «story-telling cybercrime» heeft als doel het bewustzijn rondom het onderwerp cybercrime bij ouderen en laaggeletterden te vergroten. De aanpak is gebaseerd op verhalen van slachtoffers. Daarmee is het te vertellen verhaal authentiek, aansprekend en realistisch. Verschillende verhalenvertellers worden in de regio Oost-Brabant opgeleid om de kwetsbare doelgroepen voor te lichten over de risico's en cybercrime. Het eindproduct zal onder andere ingezet worden bij bijeenkomsten met senioren, in verzorgingshuizen, sociale diensten, taallessen en alfabetiseringscursussen.

5. Verankering in wet- en regelgeving

Voorbereiding wettelijke grondslag BIO

Door het Ministerie van BZK is onderzocht op welke wijze informatieveiligheid een plaats moet krijgen in een volgende tranche van de aanstaande Wet Digitale Overheid. De noodzaak daarvoor is uit onderzoek[40] duidelijk naar voren gekomen: veel specifieke informatieprocessen van de overheid kennen informatieveiligheidswet- en regelgeving die onderling vergelijkbare algemene informatieveiligheidseisen stellen, die min of meer overeenkomen met de BIO. Voor een aantal van deze processen is verticaal interbestuurlijk toezicht op de naleving van deze regels opgezet. Vooral bij de medeoverheden komen deze regels in de uitvoering weer samen waardoor zij zich geconfronteerd zien met een grote hoeveelheid gelijksoortige toezicht- en verantwoordingsprocessen. In de paragraaf onder «ENSIA» heb ik uitgewerkt welke inspanningen er worden verricht om de lastendruk bij gemeenten hiervan te verminderen.

Om de lastendruk bij overheden te verminderen en de BIO als juridisch uitgangspunt te hanteren voor informatieveiligheid, zal het Ministerie van BZK de wettelijke grondslag voor de BIO gaan voorbereiden voor de volgende tranche van de Wet Digitale Overheid. Daarvoor zal draagvlak moeten bestaan bij de bestuurslagen Rijk, provincies, gemeenten en waterschappen. Tevens wordt hierbij bezien of sturing en verantwoording[41] voor de vitale digitale overheid een aparte plaats in wetgeving nodig heeft. Ik verwijs hiervoor ook naar het onderzoek dat ik in de paragraaf over de vitale digitale overheid in deze brief reeds noemde.

---

[39] Stcrt. 2020, nr. 68369.

[40] Zie voor het onderzoek https://www.rijksoverheid.nl/documenten/rapporten/2020/03/15/onderzoek-wetgevingskader-informatieveiligheid

[41] Zie ook het onderzoek: https://www.rijksoverheid.nl/documenten/rapporten/2019/02/28/onderzoek-toezicht-en-verantwoording-informatieveiligheid-overheid

Conclusie en vooruitblik

Onder mijn coördinatie zijn de afgelopen jaren belangrijke stappen gezet voor het verhogen van de digitale weerbaarheid via de interbestuurlijke actie-agenda informatieveiligheid, onderdeel van de agenda NL DIGIbeter. Dit heeft onder andere geleid tot de vaststelling en toepassing van de BIO sinds 2019, informatieveiligheidscriteria voor veilig inkopen, stijgende adoptiegraden van de informatieveiligheidsstandaarden en de versterking van de kennisdeling met en samenwerking tussen overheidsorganisaties (via ondermeer de overheidsbrede cyberoefening en de aanpak in het kader van crisisbeheersing).

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 de gemeenten Hof van Twente, Lochem en de universiteit van Maastricht laten zien dat de afhankelijkheid van onze digitale dienstverleningsprocessen en systemen ons ook kwetsbaar maakt. Technologie en de bijbehorende bedreigingen lijken zich sneller te ontwikkelen dan dat organisaties adequate beheersmaatregelen kunnen inrichten. Hierbij is het besef gekomen dat men meer en meer moet accepteren dat cyberincidenten niet altijd te voorkomen zijn, maar dat men beter in staat moet zijn deze incidenten te detecteren en beter moet kunnen ingrijpen om de gevolgen te beperken.

Daarom is in mijn beleid steeds meer inzet gepleegd op het oefenen met cybersecurity-incidenten bij de systemen van overheden en op crisisbeheersing in samenwerking met mijn collega, de Minister van J&V, vanuit zijn coördinerende verantwoordelijkheid voor crisisbeheersing. Bij de uitvoering van deze trajecten ben ik, samen met de medeoverheden, steeds kritisch blijven kijken of we het goede doen, en wat er beter kan en moet. We zijn als samenleving afhankelijk van digitale middelen en zien tegelijkertijd een permanente digitale dreiging die de komende jaren zal blijven groeien. Stilzitten is om die reden geen optie; als overheid moeten we onszelf scherp houden en onze inzet blijven aanscherpen op basis van voortschrijdend inzicht.
De verrichte onderzoeken, die zijn opgesomd in de bijlage bij deze brief, helpen hierbij. Tegelijkertijd leveren deze onderzoeken ook aandachtspunten op voor de toekomst, die worden betrokken bij de doorontwikkeling van informatieveiligheid bij de overheid. Concluderend kan ik stellen dat de interbestuurlijke actie-agenda informatieveiligheid conform de aan uw Kamer aangeboden planning is uitgevoerd en dat er aanvullende activiteiten zijn ontplooid. Zoals hierboven aangegeven hebben die aanvullende activiteiten zich gefocust op het oefenen.

Informatieveiligheid is een gezamenlijke verantwoordelijkheid van de gehele publieke sector. Permanente aandacht blijft nodig voor de risico's die verdergaande technologische en maatschappelijke ontwikkelingen brengen. Voor de overheid betekent dat vooral: een krachtige regierol, inspelen op de ontwikkelingen, overheidsbreed samenwerken en voorwaarden scheppen. Burgers, ondernemers en andere organisaties moeten blijvend kunnen vertrouwen op de overheid, ook in het digitale tijdperk.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
R.W. Knops

Bijlage 1:

Overzicht uitgevoerde onderzoeken informatieveiligheid (januari 2019–januari 2021)

• «Herkenbaarheid van en vertrouwen in websites en e-mails van de overheid» (Kantar Public, januari 2019)
Een onderzoek naar de herkenning van echte en vervalste websites en e-mails van de overheid.
Gepubliceerd op: https://www.rijksoverheid.nl/documenten/rapporten/2019/01/31/herkenbaarheid-van-en-vertrouwen-in-websites-en-e-mails-van-de-overheid

• «Onderzoek toezicht en verantwoording informatieveiligheid overheid» (Verdonck, Klooster & Associates, februari 2019)
Een onderzoek naar de wijze waarop BZK vanuit haar stelselverantwoordelijkheid voor informatieveiligheid in het openbaar bestuur de verantwoording over en het toezicht op informatieveiligheid kan organiseren en welke instrumenten daarvoor ingezet kunnen worden.
Gepubliceerd op: https://www.rijksoverheid.nl/documenten/rapporten/2019/02/28/onderzoek-toezicht-en-verantwoording-informatieveiligheid-overheid

• «PKIoverheid» (Innovalor, maart 2019)
Een onderzoek naar het gebruik van PKIoverheid- certificaten inclusief een analyse van mogelijkheden om het gebruik te vergroten, bijvoorbeeld door verplichten.
Gepubliceerd op: https://www.rijksoverheid.nl/documenten/rapporten/2019/03/13/pki-overheid---onderzoek-naar-mogelijkheden-om-gebruik-te-vergroten-bijvoorbeeld-via-verplichtstelling

• «Buitenlandonderzoek domeinnaambeleid» (PBLQ, november 2019)
Een onderzoek naar de ervaringen met domeinnaambeleid bij buitenlandse overheden.
Gepubliceerd op: https://www.rijksoverheid.nl/documenten/rapporten/2019/11/27/buitenlandonderzoek-domeinnaambeleid

• «Onderzoek vitale infrastructuur in de digitale wereld» (Verdonck, Klooster & Associates, februari 2020)
Een onderzoek in het kader van de verkenning van de Wet Digitale Overheid, 2e tranche, naar de manier waarop buitenlandse overheden sturing geven en toezicht uitoefenen op vitale infrastructuren in de digitale overheid.
Gepubliceerd op: https://www.rijksoverheid.nl/documenten/rapporten/2020/02/19/onderzoek-vitale-infrastructuur-in-de-digitale-overheid

• «Onderzoek wetgevingskader informatieveiligheid» (Verdonck, Klooster & Associates/Berenschot, maart 2020)
Een onderzoek naar de (algemene) informatieveiligheidsregels die voor Nederlandse overheidsorganisaties gelden. Denk hierbij aan regels voor de inhoudelijke eisen aan informatieveiligheid, en regels voor toezicht, handhaving, verantwoording en governance.
Gepubliceerd op: https://www.rijksoverheid.nl/ministeries/ministerie-van-binnenlandse-zaken-en-koninkrijksrelaties/documenten/rapporten/2020/03/15/onderzoek-wetgevingskader-informatieveiligheid

• «Evaluatie en versterking ENSIA stelsel» (I-interim Rijk, mei 2020)
Een onderzoek om inzicht te krijgen in de manier waarop het verantwoordingsstelsel ENSIA (Eenduidige Normatiek Single Information Audit) functioneert en te komen tot verbetering en versterking van het stelsel.
Gepubliceerd op: https://www.rijksoverheid.nl/documenten/rapporten/2020/05/28/evaluatie-en-versterking-ensia-stelsel

• «Een herkenbare en betrouwbare digitale overheid» (Ecorys, juli 2020)
Een quickscan verkenning naar oplossingsrichtingen en maatschappelijke effecten om te komen tot verbetering van de herkenbaarheid en betrouwbaarheid van overheidswebsites en e-mails.
Gepubliceerd op: https://www.rijksoverheid.nl/documenten/rapporten/2020/07/08/een-herkenbare-en-betrouwbare-digitale-overheid

• «Quick scan voorbereiding op digitale ontwrichting» (BZK/DGOO, januari 2021)
Een quick scan naar de bestuurlijke verbeterprogramma's rondom digitale weerbaarheid. De quick scan is verricht bij gemeenten, waterschappen, provincies en veiligheidsregio's.
Gepubliceerd op:
https://www.rijksoverheid.nl/documenten/rapporten/2021/01/31/quick-scan-voorbereiding-op-digitale-ontwrichting