Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

DGOO/DIO
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Turfmarkt 147
Den Haag
Postbus 20011
2500 EA Den Haag
www.rijksoverheid.nl
www.facebook.com/minbzk
www.twitter.com/minbzk

Kenmerk
2018-0000814840

Uw kenmerk

Datum 16 oktober 2018

Betreft Verhogen informatieveiligheid bij de overheid

Als onderdeel van de Agenda Digitale Overheid 'NL DIGIbeter'[1] stuur ik uw Kamer de toegezegde nadere uitwerking van maatregelen om de informatieveiligheid bij de overheid te verhogen.

De overheid heeft een bijzondere verantwoordelijkheid ten aanzien van de bescherming van persoonsgegevens en de te treffen beveiligingsmaatregelen. Voor deze bescherming is het van belang dat overheden permanent zorgdragen voor de integriteit van hun systemen en processen en dat de online communicatie met burgers en ondernemers op een veilige manier verloopt. Ook dient de overheid, als publiek orgaan, als launching customer het goede voorbeeld te geven. Voor de overheid betekent dat vooral: een krachtige regierol, meebewegen met de ontwikkelingen, overheidsbreed samenwerken en voorwaarden scheppen.

Dat het zaak is dat de overheid meebeweegt en zelf initiatieven ontplooit om mee te kunnen met de ontwikkelingen op het gebied van digitalisering heb ik uitgewerkt in de recente overheidsbrede agenda 'NL DIGIbeter'. Uitvoering van deze agenda vraagt om blijvende aandacht voor de risico's die verdergaande technologische en maatschappelijke ontwikkelingen brengen. Om hieraan tegemoet te komen is overheidsbreed een actie-agenda opgesteld.

Bij de uitwerking van de actie-agenda wordt er op kennis en expertise samengewerkt, waarbij het basisprincipe is en blijft dat afzonderlijke overheidsorganisaties zelf verantwoordelijk zijn en blijven voor hun informatieveiligheid. Zodoende stuurt de Minister van BZK uw Kamer binnenkort een brief over de versterking van de centrale sturing op ondermeer informatiebeveiliging bij de Rijksdienst en de sectorspecifieke maatregelen die zij hierop treft. Mijn rol is overheidsbrede samenwerking te stimuleren en daar waar het kan en nodig is randvoorwaardelijke kaders op te stellen.

Focus actie-agenda
De overheid heeft een grote verantwoordelijkheid ten aanzien van de beveiliging van gegevens die burgers en ondernemers aan haar toevertrouwen en de ICT – systemen waarmee zij werkt. Het op orde hebben en houden van het eigen informatieveiligheidsbeleid is dan ook randvoorwaardelijk voor de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens en systemen.

[1] Vergaderjaar 2017-2018, Kamerstuk 26643 nr.549

Zodoende focust een aantal maatregelen zich op het op orde brengen en houden van de informatieveiligheid van overheidsorganisaties en het bevorderen van overheidsbrede samenwerking. Het gaat er ondermeer om dat overheidsorganisaties richtlijnen betekenis geven in hun eigen ICT-bedrijfsvoering, hierover verantwoording afleggen en zichzelf blijven trainen.

Verder neemt het belang van informatieveiligheid aanzienlijk toe in de digitale communicatie van overheden met burgers en ondernemers. Voor het vergroten van de digitale veiligheid is het essentieel dat overheidsorganisaties moderne veiligheidsstandaarden in hun ICT hanteren. De standaarden gaan misbruik van afzenderschap (d.w.z. spoofing en phishing) tegen en zorgen ervoor dat de communicatie van overheden met burgers en ondernemers niet zo maar afgeluisterd of gemanipuleerd kan worden. Om die reden focust een aantal maatregelen zich op het bieden van een veilige digitale dienstverlening aan burgers en ondernemers, maar ook op maatregelen die ervoor zorgen dat belangrijke voorzieningen van de digitale overheid in voldoende mate zijn opgewassen tegen uitval/stilstand.

Overheidsbrede maatregelen

Baseline informatiebeveiliging overheid (BIO)
Momenteel stellen overheden hun informatieveiligheidsbeleid vast aan de hand van een basisnormenkader, ook wel de baseline informatiebeveiliging genoemd. Het Rijk hanteert de Baseline Informatiebeveiliging Rijksdienst (BIR), de provincies de Interprovinciale Baseline Informatiebeveiliging (IBI), de waterschappen de Baseline Informatiebeveiliging Waterschappen (BIWA) en de gemeenten de Baseline Informatiebeveiliging Gemeenten (BIG). De aanstaande Baseline Informatiebeveiliging Overheid (BIO) bundelt de huidige afzonderlijke baselines per overheidslaag (Rijk, provincies, waterschappen en gemeenten) en kan worden beschouwd als de 'kapstok' waaraan de elementen van informatiebeveiliging per overheidslaag opgehangen kunnen worden.[2] De ontwikkeling van de BIO betreft een doorontwikkeling van de sectorspecifieke baselines en biedt een uniforme basis om te zorgen dat de beveiliging van informatie(systemen) bij alle bedrijfsonderdelen van de overheid bevorderd wordt. De BIO wordt dit jaar nog vastgesteld en alle overheidslagen starten hierna met de implementatie. Hiervoor is het van belang dat bestuurders, ambtelijke top, middenmanagement, (ICT-)professionals en stakeholders op adequate wijze invulling geven aan de gestelde eisen en principes uit de BIO. Om de verschillende doelgroepen hierin zo goed mogelijk te faciliteren is voorzien in een interbestuurlijk ondersteuningsprogramma, waarbij het de bedoeling is dat overheden per 2021 zelf voorzien in die ondersteuning voor de eigen organisatie. Verkend wordt of de systematiek van de BIO in een Algemene Maatregel van Bestuur (AmvB), horende bij de aanstaande Wet Digitale Overheid, kan worden opgenomen.

Digitale veiligheid van hard- en software (DVHS)
In de Roadmap DVHS[3] van de staatssecretaris van EZK wordt een samenhangende aanpak geboden om als Nederland voorop te lopen bij het bevorderen van de digitale veiligheid van hard- en software. De Roadmap DVHS geeft mede invulling aan de Nederlandse Cyber Security Agenda.[4] De overheid

[2] Uiteraard met inachtneming van de contextuele verschillen per overheidslaag.
[3] Vergaderjaar 2017-2018, Kamerstuk 26643 nr.535
[4] Vergaderjaar 2017-2019, Kamerstuk 26643, nr. 536

kan de digitale veiligheid van de gehele productontwikkelingscyclus bevorderen. Door criteria hierover in het inkoopbeleid op te nemen moeten aanbieders van de overheid voldoen aan deze eisen. De overheid kan met haar inkoopbeleid de vraagzijde van digitaal veilige producten stuwen. Zij is namelijk een belangrijke gebruiker. Hierdoor ontstaat een prikkel voor aanbieders om digitaal veilige producten op de markt te brengen. Ook geeft de overheid hiermee het goede voorbeeld: kijk naar de digitale veiligheid van hard- en software voordat je dit koopt. Zodoende wordt onderzocht welke aanvullende maatregelen voor de digitale veiligheid van hard- en software bij inkoop binnen de overheid nodig en gewenst zijn.

Eenduidige Normatiek Single Information Audit (ENSIA)
Voor het gemeentelijke domein is een methode opgezet om de administratieve lasten op informatieveiligheid terug te brengen en tegelijkertijd de gemeentelijke bestuurlijke verantwoording te verstevigen. Zodoende richt dit traject zich op een eenduidige normatiek van diverse centrale regelingen[5] en focust het zich op een eenmalige uitvraag aan gemeenten. Door de bestuurlijke verantwoording (horizontale verantwoording) plaats te laten vinden in de gemeentelijke planning- en controlcyclus, wordt het gemeentebestuur versterkt in zijn rol meer zicht te krijgen op de informatieveiligheid in zijn gemeente; dit stelt het bestuur in staat beter te sturen en verantwoording af te leggen aan de gemeenteraad. Deze methodiek met de naam ENSIA wordt sinds 2017 bij alle gemeenten geïmplementeerd. ENSIA wordt nog doorontwikkeld en op sommige terreinen inmiddels ook door waterschappen gebruikt. De bestuurslagen - provincies en waterschappen - worden actief geïnformeerd over ENSIA, zodat deze methodiek (na optimalisaties) wellicht eveneens kan worden ingezet bij die overheidslagen.[6]

i-Bewustzijn Overheid
Aan de basis van informatieveiligheid moet de wil bestaan om veilig te handelen. Daarvoor is het noodzakelijk dat bestuurders, managers en medewerkers zich bewust zijn van de digitale dreigingen, de eigen rol en consequenties/risico's van het eigen handelen en de daarmee samenhangende (bedrijfs)risico's. Om die reden is voorzien in een overheidsbrede i-bewustzijnaanpak om bestuurders, managers en medewerkers blijvend te doen beseffen hoe belangrijk informatieveiligheid is en hun alertheid, kennis en vaardigheden op dit vlak te vergroten. De aanpak richt zich op een actueel en breed toepasbaar aanbod van documenten, leer- en communicatiemiddelen, campagnemateriaal en praktijkvoorbeelden en stimuleert hiermee samenwerking tussen de verschillende overheden. Overheden en Alert Online[7], veiliginternetten.nl[8] en het Digital Trust Centre[9] gaan samenwerken om kennis en aanpak te delen.

[5] Momenteel zijn dat de regelingen Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet).
[6] Waterschappen hebben een soortgelijke methodiek opgezet voor de Basisregistratie Grootschalige Topografie (BGT) en de Basisregistratie Ondergrond (BRO).
[7] Alert Online is een initiatief dat overheid, bedrijfsleven, onderwijs, wetenschap en consumenten in Nederland faciliteert en stimuleert samen te werken aan cybersecurity én hen meer cyber secure te laten handelen. Het zwaartepunt van Alert Online is in oktober: dé European Cybersecurity Month.
[8] Veiliginternetten.nl is een gezamenlijk initiatief van het ministerie van Economische Zaken en Klimaat, het ministerie van Justitie en Veiligheid / Nationaal Cyber Security Centrum, ECP | Platform voor de InformatieSamenleving en het bedrijfsleven.
[9] Het Digital Trust Center, van het ministerie van Economische Zaken en Klimaat, stimuleert en faciliteert ondernemers om zelfstandig of in samenwerkingsverband aan de slag te gaan met het verbeteren van hun online veiligheid.

Incident response capaciteit
Cybersecurity-incidenten zijn lastig te voorspellen en te voorkomen en dergelijke incidenten los je vaak niet alleen op. Juist omdat online veiligheid geen zaak is van één partij, is het van belang dat overheid en bedrijfsleven permanent slim samenwerken om van Nederland de meest open en veilige online samenleving te maken. In de Nederlandse Cyber Security Agenda van de minister van J&V is het belang van een landelijk dekkend stelsel van cybersecurity samenwerkingsverbanden genoemd, gericht op het versterken van de slagkracht van publieke en private partijen. Zo is er voor elke overheidslaag een Computer Emergency Response Team (CERT) dat overheidsorganisaties ondersteunt bij ICT-incidenten. Het Nationaal Cybersecurity Centrum (NCSC) is het CERT voor het Rijk en vitale organisaties. Provincies hebben de CERT-functie op dit moment individueel geregeld en verkennen de mogelijkheid van aansluiting bij een overheidsbrede CERT. De waterschappen hebben sinds april 2017 samen met Rijkswaterstaat een CERT Watermanagement en de gemeenten hebben sinds 2013 een eigen CERT, de Informatiebeveiligingsdienst (IBD). Ik hecht aan het belang van een landelijk dekkend stelsel en stimuleer de overheidsbrede samenwerking op dit terrein. Daarom wordt er de komende jaren een impuls gegeven aan het overheidsbreed oefenen met incidenten. Het permanent oefenen is van groot belang voor het overheidsbrede samenspel met relevante private partijen. Op die manier kan er al aan de voorkant beter op elkaar worden ingespeeld.

Vitale digitale overheid
Sommige processen zijn zo vitaal voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid. Deze processen tezamen vormen de Nederlandse vitale infrastructuur. Bij de herijking vitale infrastructuur uit 2015[10] is de categorie "digitale overheid" opgenomen als vitale infrastructuur. Dat betekent dat voor aangewezen vitale aanbieders binnen de sector digitale overheid een zogenoemde meldplicht gaat gelden. De meldplicht komt voort uit de Wet beveiliging netwerk- en informatiesystemen (Wbni), van de minister van Justitie en Veiligheid. Deze meldplicht gaat, naar verwachting, van kracht per medio 2019. Een melding leidt tot meer prioriteit en inzet van het NCSC. Vanwege mijn verantwoordelijkheid voor de digitale overheid voor burgers en ondernemers worden enkele vitale voorzieningen waarvoor ik een verantwoordelijkheid heb, vitaal verklaard. Dat zijn voorzieningen die van groot belang zijn voor de reilen en zeilen van de digitale overheid. Om een verscherpte aandacht van kwaadwillenden te voorkomen, worden deze vitale voorzieningen niet expliciet genoemd in deze brief.

Versleuteling basisregistraties
In het Regeerakkoord is opgenomen dat gegevens van burgers in basisadministraties en andere privacygevoelige informatie altijd versleuteld worden opgeslagen. Zodoende wordt gestart met een onderzoek naar de wijze waarop de huidige veiligheidsmaatregelen afdoende bescherming bieden tegen mogelijke beveiligingsrisico's. Uitgangspunt daarbij is het beschermen van privacygevoelige informatie. Hieruit kan volgen dat registraties en/of onderdelen van registratiesystemen die nu niet versleuteld zijn dat voortaan wel moeten worden.

[10] Vergaderjaar 2014-2015, Kamerstuk 30821 nr. 23

Verhogen adoptie informatieveiligheidsstandaarden
Burgers en ondernemers moeten erop kunnen vertrouwen dat gegevensuitwisseling met de overheid veilig verloopt. Om dit te kunnen waarborgen, dienen overheden diverse informatieveiligheidsstandaarden te implementeren.[11] Recente phishing-incidenten waarin overheidse-mail en websites werden nagemaakt[12], onderstrepen het belang van overheidsbrede adoptie van deze standaarden. Echter, de implementatie van de informatieveiligheidsstandaarden loopt nog achter.[13] Inmiddels ligt de implementatiegraad van informatieveiligheidsstandaarden op 87%, begin 2018 lag dit nog op 80%. Dit laat zien dat er sprake is van een stijging. Overheden hebben implementatieafspraken met elkaar gemaakt. Die afspraken hebben betrekking op het moment waarop de standaarden binnen de overheid zijn geïmplementeerd. Volgend jaar zal worden bezien in hoeverre de implementatieafspraken zijn behaald en of meer harde verplichtingen opportuun zijn om de veiligheid van digitale communicatie met de overheid, via web en e-mail[14] te bevorderen. Een eventuele verplichting zal volgen uit de (ontwerp) Wet Digitale Overheid.

Ondersteunend daaraan is het uitvoeren van frequente metingen op de implementatie van informatieveiligheidsstandaarden van groot belang. Eerder is er door het Platform Internet Standaarden een meetinstrument ontwikkeld, te vinden op www.internet.nl. Met behulp van een financiële impuls wordt deze tool beschikbaar gemaakt voor bulkmetingen, zodat geautoriseerde partijen grote aantallen domeinnamen in één keer kunnen testen. Hierdoor kan een vinger aan de pols worden gehouden ten aanzien van de voortgang van de eerder genoemde implementatieafspraken.

Veilige overheidswebsites
Om de beveiliging van overheidswebsites verder te bevorderen, wordt de open informatieveiligheidsstandaard HTTPS verplicht, zoals eerder aan uw Kamer toegezegd in 2017. Deze standaard (die te herkennen is aan het kenmerkende slotje in de adresbalk van de internetbrowser) zorgt ervoor dat de verbinding en gegevensuitwisseling tussen de bezoeker en de overheidswebsite zijn versleuteld, waardoor het voor kwaadwillenden onmogelijk is deze gegevens te onderscheppen. Bovendien kan de bezoeker dankzij HTTPS controleren of hij/zij direct met de website die hoort bij de gebruikte domeinnaam, contact heeft en niet met een vervalste website (spoofing). De Wet Digitale Overheid, die naar verwachting in 2019 van kracht zal worden, biedt de mogelijkheid open standaarden aan te wijzen voor een verplichting bij AmvB. De AMvB voor HTTPS is naar verwachting per medio 2019 van kracht.

Herkenbaarheid van overheidswebsites en e-mail
Burgers en ondernemers moeten overheidswebsites kunnen onderscheiden van andere websites. Om die reden komt er een onderzoek onder burgers en ondernemers naar de wenselijkheid te komen tot één domeinnaam-extensie voor alle e-mailadressen en websites van de Nederlandse overheid.[15] Uit dit onderzoek

[11] Voor alle organisaties binnen de publieke sector geldt een '*pas-toe-of-leg-uit*' verplichting voor open standaarden. Ook voor enkele informatiebeveiligingsstandaarden geldt die afspraak.
[12] Zie ook https://nos.nl/artikel/2237977-waarschuwing-voor-geraffineerde-phishingmails-van-nepoverheid.html
[13] Vergaderjaar 2017-2018, kamerstuk 26643, nr 530
[14] Daarnaast komen in het overleg Betrouwbare Overheidsmail mailbeheerders van de overheid sinds 2016 regelmatig samen om kennis en ervaringen te delen over moderne e-mailbeveiligingsstandaarden (DMARC+DKIM+SPF en STARTTLS+DNSSEC+DANE).
[15] Naar het voorbeeld van het Verenigd Koninkrijk (*.gov.uk), Duitsland (*.bund.de), Frankrijk (gouv.fr) en de Europese Unie (*.europa.eu).

zal moeten blijken wat het voor ontvangers van e-mail en bezoekers van websites lastig maakt om te bepalen of een verzender daadwerkelijk namens de overheid e-mailt, en of een website echt van de overheid is. Aanbevelingen die uit dit onderzoek naar voren komen kunnen bijdragen aan de bestrijding van het toenemende fenomeen van (spear)phishing.[16]

Verankering in wet- en regelgeving
Zoals eerder gesteld, geldt voor informatieveiligheid het basisprincipe dat afzonderlijke overheidsorganisaties zelf verantwoordelijk zijn en blijven voor hun informatieveiligheid. Vanwege het groeiend belang voor een veilige digitale overheid wordt eveneens gewerkt aan wetgeving waarin (minimum)eisen ten aanzien van informatieveiligheid worden vastgelegd. Een wettelijke basis waaraan de informatieveiligheid binnen de overheid moet voldoen, is ondersteunend aan het verder borgen en verhogen van veilige overheidsdienstverlening. Het doel hiervan is dat burgers en ondernemers erop moeten kunnen vertrouwen dat de gegevens die zij met de overheid uitwisselen, veilig zijn. Dit geldt ook voor de gegevensuitwisseling tussen overheden onderling. Op dit moment wordt regelgeving voorbereid over informatieveiligheid bij de toegang tot digitale overheidsdienstverlening (eID), alsmede over verplichte toepassing van de (technische) standaard HTTPS. Tevens wordt onderzoek gedaan naar het gebruik van algoritmen door overheden en komt er een kabinetsvisie ten aanzien van open source. Bezien wordt of en hoe meer generiek informatieveiligheidsbeleid een plaats moet krijgen in een volgende tranche van de aanstaande Wet Digitale Overheid.

Tot slot
Het naar een hoger plan tillen van informatieveiligheid binnen overheidsorganisaties blijft de komende jaren één van mijn speerpunten. Het functioneren van de overheid is in sterke mate afhankelijk van een goede sturing op en gebruik van digitale voorzieningen en infrastructuur. Het goed regelen van informatieveiligheid is hier onlosmakelijk mee verbonden. Dit binnen de overheid samen doen, zodat kennis, producten en oplossingen voor informatieveiligheid over en weer kunnen worden gedeeld, helpt het effect te vergroten en beperkt tevens de kosten. De komende tijd zal het accent ook worden gelegd op het delen van de overheidsbrede expertise, daar er sprake is van een groeiend tekort aan cybersecurity experts. Transparantie over de aanpak binnen de overheid helpt organisaties elkaar te vertrouwen. Burgers, ondernemers en andere organisaties moeten kunnen blijven vertrouwen op de overheid, ook in het digitale tijdperk. Overheidsorganisaties zijn zelf verantwoordelijk voor de wijze waarop het informatieveiligheidsbeleid in hun organisatie gestalte krijgt. Mijn taak als staatssecretaris zie ik als kaderstellend, voorts ondersteunend, en waar nodig aanjagend naar alle overheidslagen.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

drs. R.W. Knops

[16] Tweede Kamer, vergaderjaar 2017-2018, Kamerstuk 26643 nr. 540 - Cybersecuritybeeld Nederland 2018 -

DGOO/DIO
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Datum

Kenmerk
2018-0000814840

Bijlage: Overzicht maatregelen verhogen informatieveiligheid

Thema	Maatregel	Begin	Eind
BIO	Vaststellen Baseline Informatiebeveiliging Overheid (BIO)		Q4 2018
	Overheden ondersteunen met de implementatie van de BIO	Q4 2018	Q4 2020
DVHS	Onderzoek welke aanvullende maatregelen bij inkoop ter bevordering van de digitale veiligheid van hard- en software (DVHS) nodig en gewenst zijn	Q4 2018	Q4 2019
ENSIA	Implementatie en doorontwikkeling Eenduidige Normatiek Single Information Audit (ENSIA) bij gemeenten	Q4 2018	Q4 2020
i-Bewustzijn overheid	Alertheid, kennis en vaardigheden van bestuurders, managers en medewerkers vergroten door middel van een overheidsbrede campagne	Q2 2019	Q4 2020
Incident response capaciteit	Organiseren van overheidsbrede crisissimulatie-oefening	Q3 2019	Q3 2020
Vitale digitale overheid	Opnemen categorie digitale overheid als vitale infrastructuur, onderdeel van de Wet beveiliging netwerk- en informatiesystemen (Wbni)		Q3 2019
Versleuteling basisregistratie	Onderzoek naar de wijze waarop huidige veiligheidsmaatregelen afdoende bescherming bieden tegen mogelijke beveiligingsrisico's	Q3 2018	Q3 2019
Informatie-veiligheids-standaarden	Onderzoek naar de stand van zaken implementatie van informatieveiligheidsstandaarden	Q3 2018	Q2 2019
	Onderzoek of meer harde verplichtingen opportuun zijn op het gebied van de implementatie van informatieveiligheidsstandaarden	Q2 2019	Q1 2020
	Beschikbaar stellen meet-tool voor bulkmetingen t.a.v. de implementatie van informatieveiligheidsstandaarden	Q3 2018	Q2 2019
Veilige overheidsweb-sites	Verplichten open informatieveiligheidsstandaard HTTPS		Q2 2019
Herkenbaarheid van websites en e-mail	Onderzoek onder ondernemers en burgers naar wenselijkheid om te komen tot één domeinnaam -extensie voor de overheid	Q3 2018	Q2 2019
Verankering in wet- en regelgeving	Onderzoek of en hoe meer generiek informatieveiligheidsbeleid een plaats krijgt in de volgende tranche van de Wet Digitale Overheid	Q3 2018	Q2 2020