Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

1641

Vragen van het lid **Leijten** (SP) aan de Staatssecretaris en Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Justitie en Veiligheid over *digitale veiligheid* (ingezonden 14 december 2021).

Antwoord van Staatssecretaris **Van Huffelen** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 10 februari 2022). Zie ook Aanhangsel Handelingen, vergaderjaar 2021–2022, nr. 1266.

Vraag 1
Kunt u een stand van zaken geven over de ontwikkeling van een Europese digitale identiteit en de Nederlandse inzet daaromtrent?[1]

Antwoord 1
De Europese Commissie heeft op 3 juni 2021 een wetsvoorstel ingediend voor een «raamwerk voor een Europese Digitale Identiteit», dat de huidige eIDAS-verordening herziet. De Commissie deed ook een aanbeveling voor een met de lidstaten te ontwikkelen «Toolbox».[2]
De Minister van Buitenlandse Zaken informeerde Uw Kamer op 9 juli 2021 over de positie van het kabinet in dit dossier in het BNC-fiche.[3] De kern van dit fiche is dat het voorstel van de Commissie inhoudelijk aansluit op het Nederlandse beleid voor elektronische identificatie en uitwisseling van gegevens. Het Nederlandse beleid heeft tot doel dat alle ingezetenen en bedrijven in Nederland en in andere Europese landen op een veilige, betrouwbare, toegankelijke en gebruiksvriendelijke manier digitaal transacties kunnen verrichten in het publieke en in het private domein. Een verdere toelichting op het Europese digitale identiteit raamwerk is eerder gegeven in de Kamerbrief voortgangsrapportage domein toegang.[4]

Vraag 2
Kunt u een stand van zaken geven over de ontwikkeling van Nederlandse digitale identiteiten, zoals de eID?

---

[1] Follow the Money, 11 december 2021, «Wetenschappers waarschuwen voor een nieuwe digitale identiteit» (https://www.ftm.nl/artikelen/internationale-digid-lobby?share=U5Q42y8vm97o0s58p6UytCooht8mvxjioBVRLWkpCJ6IY5KXTH9ZRTx0z2p6euw%3D)
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0281&qid=1625048320890&from=NL
[3] Kamerstuk 22 112, nr. 3161
[4] Kamerstuk 22 643 nr. 788

ah-tk-20212022-1641
ISSN 0921 - 7398
's-Gravenhage 2022

Antwoord 2
Op 12 oktober 2021 is uw Kamer uitgebreid geïnformeerd over de voortgang op het domein digitale toegang.[5] In deze brief wordt uitgebreid ingegaan op het gehele domein van de digitale toegang waar zowel de doorontwikkeling van DigiD, het publieke inlogmiddel voor burgers, als eHerkenning, het private stelsel van inlogmiddelen voor bedrijven) onder valt. Het domein Toegang heeft in de kern twee doelen. Allereerst (persoonlijke) toegang verlenen tot een goede, efficiënte digitale dienstverlening voor burgers en bedrijven. En ten tweede de betrouwbaarheid van de private en publieke inlogmiddelen garanderen, zodat persoonsgegevens zo goed mogelijk beschermd zijn.
In de genoemde brief over het domein toegang zijn eveneens de ontwikkelingen op het domein digitale identiteit meegenomen. Voor een visie op dit domein verwijs ik naar de visiebrief digitale identiteit die in februari 2021 naar uw Kamer is gestuurd.[6] Hierin wordt uitgebreid ingegaan op de taken en verantwoordelijkheden die de overheid invult met betrekking tot de digitale identiteit en de digitale infrastructuur.

Vraag 3
Kunt u helder uiteenzetten in welke mate en hoe de data die gekoppeld is aan een eID decentraal wordt opgeslagen en in welke mate en hoe dit centraal wordt opgeslagen? Zo nee, waarom niet?

Antwoord 3
Bij de inrichting van het eID-stelsel worden om in te loggen bij overheden geen andere attributen (persoonsgegevens) verwerkt dan het burgerservicenummer; dat wil zeggen niet op andere plekken dan waar dit nu reeds plaatsvindt. Bij de implementatie van eID is overigens een centrale, maar ook een decentrale opzet, of een combinatie van beide mogelijk. In alle situaties is de kern dat er een adequate privacybescherming wordt gerealiseerd. Daarbij dienen alle beginselen uit de AVG worden meegenomen.

Vraag 4
Begrijpt u de kritiek van experts, die aangeven dat hoewel mensen eigenaar *lijken* te zijn van hun eigen data, maar dat dit principe ondermijnd wordt door verdienmodellen van verschillende deelnemers en aanbieders van digitale identiteiten? Zo nee, waarom niet? Zo ja, wat zijn de waarborgen waardoor deze prikkels worden weggenomen?

Antwoord 4
Ik deel de achterliggende zorg. Ik ben het met de experts eens dat persoonsgegevens van burgers geen handelswaar zijn en dat verdienmodellen van aanbieders daarop ook niet gebaseerd mogen zijn. Ik ben van mening dat daarvoor ook afdoende waarborgen getroffen zijn en worden. Zowel in de revisie van de bestaande eIDAS verordening tot vorming van een Europees digitale identiteit raamwerk, als in de voorstellen voor de Wet Digitale Overheid, is opgenomen dat gebruiks- en gebruikersgegevens en eventuele andere categorieën persoonsgegevens niet gebruikt mogen worden voor andere doeleinden dan de veilige uitgifte van inlogmiddelen en het inloggen met deze middelen.[7] De data van mensen dienen dus niet het verdienmodel van een aanbieder van een digitaal identiteitsmiddel, omdat dit onder de voorgestelde wetgeving niet wordt toegestaan.

Vraag 5
Waarom is er bij de ontwikkeling van de eID/SSI (Self-Sovereign Identity) gekozen voor blockchaintechnologie? Begrijpt u de kritiek van wetenschappers dat dit kwetsbaar en kostbaar is, onder andere omdat data, ook als deze niet juist is, niet verwijderd kan worden? Kunt u uw antwoord toelichten?

---

[5] Kamerstuk 22 643, nr. 788
[6] Kamerstuk 22 643, nr. 743
[7] Zie EU voorstel «amending Regulation (EU) No 910/2014». Artikel 6a-7.

Antwoord 5
Het artikel waaraan u refereert beschrijft één experiment en geen breed maatschappelijk geïmplementeerde toepassing. De genoemde pilot wordt momenteel niet aan burgers aangeboden. Het Nederlandse eID voor burgers is DigiD. Hierbij wordt de door u genoemde technologie niet gebruikt.
De mate waarin distributed ledger technologie (blockchain) in de toekomstige Europese en Nederlandse digitale identiteit infrastructuur gebruikt wordt staat nog niet vast. Ik kijk hier zeer kritisch naar, niet alleen vanuit het oogpunt van privacy, maar ook vanuit duurzaamheid. Het maatschappelijke doel staat in het Nederlandse beleid voorop, niet de ondersteunende technologie. De overheid blijft graag in open dialoog en onderzoekt diverse technologische initiatieven die kunnen bijdragen aan een betrouwbare digitale identiteit infrastructuur, zeker waar het gaat om het borgen van de autonomie en privacy van Nederlandse burgers. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties tracht hierbij zo min mogelijk voorbarige conclusies te trekken, maar probeert te leren door te experimenteren.

Vraag 6
Kunt u ingaan op de zorgen over hoe de gekozen techniek mensen ernstig kan benadelen, omdat zij aan een systeem vastzitten en daar alleen afstand van kunnen nemen met grote persoonlijke consequenties? Hoe denkt u dit te voorkomen?

Antwoord 6
Ik ben bekend met deze technologie en de kritiek hierop. We onderzoeken, bijvoorbeeld in het kader van het European Blockchain Partnership, diverse mogelijkheden om distributed ledgers (blockchains) te gebruiken zonder daarop persoonsgegevens op te slaan. Dit heeft mijn voorkeur. Zoals in het antwoord op de vorige vraag is aangegeven, staat de mate waarin distributed ledger technologie (blockchain) in de toekomstige Europese en Nederlandse digitale identiteit infrastructuur gebruikt wordt, nog niet vast. Het maatschappelijke doel staat in het Nederlandse beleid voorop, niet de ondersteunende technologie.

Vraag 7
Hoeveel lobbycontacten zijn er geweest tussen de overheid en het platform ID2020? Kunt u een overzicht verstrekken?

Antwoord 7
In het opstellen van de Nederlandse lijn in het werken aan het Europese digitale identiteit raamwerk zijn geen contacten geweest met medewerkers van het platform ID2020.

Vraag 8
Kunt u ingaan op de zorgen van wetenschappers dat de coronapandemie door bedrijven en politici wordt gebruikt of misbruikt om een digitale identiteitskaart(ID) in te voeren? Kunt u uw antwoord toelichten?

Antwoord 8
De Nederlandse digitale identiteitskaart bestaat op dit moment niet. De wet op de identificatieplicht laat dit niet toe. Voor een visie op dit domein verwijs ik naar de visiebrief digitale identiteit die in februari 2021 naar uw Kamer is gestuurd.[8]

Vraag 9
In hoeverre vindt u het ethisch verantwoord dat bedrijven of beleidsmakers een gezondheidscrisis gebruiken om een digitale identiteit aan te prijzen, waardoor zij meer winst kunnen maken of meer invloed kunnen vergaren door dataverzameling?

[8] Kamerstuk 22 643, nr. 743

Antwoord 9
Er is door de overheid geen gezondheidscrisis gebruikt om meer winst te maken of invloed te vergaren door datavergaring. De verdere doorontwikkeling van onze digitale identiteit infrastructuur zal altijd een maatschappelijk vraagstuk zijn dat weloverwogen stappen vergt. In de visiebrief digitale identiteit (feb 2021) heb ik nadrukkelijk stil gestaan bij de diverse publieke waarden die hierbij meespelen.[9] Denk hierbij aan publieke waarden als de cyberveiligheid van ons land, de autonomie van de burger, de privacy van de burger, economische kansen en vermindering van administratieve lasten voor de burger. De kern is dat ik wil bouwen aan vertrouwen in de digitale wereld door een betrouwbare digitale identiteit infrastructuur in te richten. Winst van private partijen zal hierbij geen doel zijn. Invloed vergaren door middel van dataverzameling bij het gebruik van digitale identiteitsmiddelen is voor zowel overheden als private partijen volgens de voorgestelde wetgeving niet toegestaan. Zie het antwoord op vraag 4.

Vraag 10
Op welke manier zijn de ethische aspecten meegewogen in het beleid rond de Europese en Nederlandse digitale identiteit? Kunt u uw antwoord toelichten?

Antwoord 10
De verdere doorontwikkeling van onze digitale identiteit infrastructuur zal altijd een maatschappelijk vraagstuk zijn dat weloverwogen en ethisch verantwoorde stappen vergt. In de visiebrief digitale identiteit (feb 2021) is nadrukkelijk stil gestaan bij de diverse publieke waarden die hierbij meespelen. Denk hierbij aan publieke waarden als de cyberveiligheid van ons land, de autonomie van de burger, de privacy van de burger, economische kansen en vermindering van administratieve lasten voor de burger. Ook worden in deze brief enkele uitgangspunten voor de toekomstige digitale identiteit infrastructuur aangegeven.[10] Om een gedragen en betrouwbare inrichting van de Nederlandse en Europese digitale identiteit infrastructuur te bewerkstelligen zal ik hierover in de toekomst met uw Kamer en met diverse maatschappelijke experts, waaronder ethici, in gesprek gaan.

Vraag 11
Kunt u reflecteren op de wenselijkheid van de invloed van onder andere Microsoft, maar ook andere multinationals of big techbedrijven, in de oproep aan overheden tot het ontwikkelen van een zogenoemde coronapas? Zo nee, waarom niet?

Antwoord 11
De inrichting van het «raamwerk voor een Europese Digitale Identiteit», dat de huidige eIDAS-verordening herziet, wordt onafhankelijk van het eerder ontwikkelde EU digitale Corona Certificaat ontwikkeld. Voor de ontwikkeling van de onder vraag 1 genoemde toolbox zal ook de kennis en ervaring vanuit het bedrijfsleven betrokken worden. Dit doen we op een open wijze met een gelijk speelveld voor de betrokken partijen.

Vraag 12
In hoeverre vindt u het afhankelijk worden van een digitale identiteit wenselijk als er tegelijkertijd nog altijd grote beveiligingsrisico's zijn voor mensen als het gaat om het gijzelen van data en persoonsgegevens?[11]

Antwoord 12
Op het terrein van informatieveiligheid binnen en buiten de overheid is veel werk te doen. Het kabinet zet zich permanent in voor het vergroten van de digitale veiligheid in de samenleving; ik verwijs naar de Kamerbrief met de Beleidsreactie Cybersecuritybeeld Nederland 2021 (CSBN2021) en de

[9] Kamerstuk 22 643, nr. 743
[10] Kamerstuk 22 643, nr. 743
[11] NOS, 11 december 2021, «Cyberwaakhond waarschuwt voor gevaarlijk beveiligingslek» (https://nos.nl/nieuwsuur/artikel/2409121-cyberwaakhond-waarschuwt-voor-gevaarlijk-beveiligingslek)

voortgangsrapportage Nederlandse Cybersecurity Agenda (NCSA).[12] De digitale dreiging is immers groeiende en alle overheden en organisaties wereldwijd kampen met dit vraagstuk. Het is een brede maatschappelijke opgave voor publieke en private partijen. Digitale veiligheid is dan ook een essentiële randvoorwaarde voor het slagen van de digitale transitie. Daarom dient deze veiligheid in de basis geborgd te worden zodat dit geen beletsel vormt voor de toekomstbestendigheid van de Europese en Nederlandse digitale identiteit infrastructuur.

Vraag 13
Kunt u aangeven wat u onderneemt om deze kwetsbaarheid, en het oplossen van die kwetsbaarheden, zo veel mogelijk onder de aandacht te brengen van (overheids)instellingen en bedrijven?

Antwoord 13
Vanuit de driehoek BZK, JenV en EZK wordt nauw samengewerkt om de digitale weerbaarheid in de publieke en private sectoren in Nederland te verhogen. Een goed voorbeeld hiervan is de recente aanpak van Apache Log4j kwetsbaarheid waarbij binnen de rijksoverheid, onder operationele coördinatie door het NCSC, organisaties vanuit de eigen rollen en taken nauw hebben samengewerkt. Een speciaal georganiseerd online-webinar, georganiseerd door het Digital Trust Center (DTC), NCSC en CSIRT-DSP, werd door 4000 IT- en cyberspecialisten bezocht waardoor kennis snel gedeeld kon worden met partijen die aan de knoppen zitten. Uw Kamer is hier op 17 december jl. over geïnformeerd.[13]

Vraag 14
Kunt u aangeven hoe bedrijven en (overheids)instellingen en getroffen burgers worden ondersteund bij eventuele schade van dit veiligheidslek?

Antwoord 14
Leveranciers van software zijn allereerst verantwoordelijk om bij kwetsbaarheden actie te nemen en zo te zorgen dat hun producten veilig zijn. Door de stichting Apache zijn in deze casus ook updates beschikbaar gesteld om de kwetsbaarheden te dichten.[14] Bedrijven en organisaties in Nederland zijn primair zelf verantwoordelijk voor de beveiliging van hun IT en dienen de patch, waar dat kan, dan ook zo snel mogelijk uit te voeren.
Het NCSC heeft daarnaast krachtens de Wet beveiliging netwerk- en informatiesystemen (Wbni) tot taak om vitale aanbieders en Rijksoverheidsorganisaties in het geval van dreigingen of incidenten met betrekking tot hun netwerk- en informatiesystemen, zowel desgevraagd als proactief, te informeren, adviseren en overige bijstand te verlenen. Digitale dienstverleners (clouddiensten, online marktplaatsen, zoekmachines) die onder de Wbni vallen kunnen desgewenst bijstand verkrijgen van het nationale Cyber Security Incident Response Team voor digitale dienstverleners (CSIRT-DSP).[15] Het DTC ondersteunt het MKB hierin met algemene en specifieke dreigingsinformatie, advies, handelingsperspectieven en tools. Ook stimuleert het sectorale en regionale samenwerkingsverbanden van bedrijven die tot doel hebben de cyberweerbaarheid van hun deelnemers te verhogen.
Het is aan alle partijen om zich goed voor te bereiden op eventuele compromittering van hun netwerk- en informatiesystemen, zoals dat ook bij inbraak en diefstal het geval is in de analoge situaties. Wanneer onverhoopt burgers slachtoffer worden van een dergelijk incident, dan zal per geval bekeken moeten worden of er partijen aansprakelijk gesteld kunnen worden. Wanneer burgers of instellingen als gevolg van een dergelijk incident te maken krijgen met cybercrime, dan kunnen zij hiervan aangifte doen bij de politie.

---

[12] Kamerstuk 26 643, nr. 767
[13] Kamerstuk 26 643, nr. 814
[14] Zie onder andere: https://www.ncsc.nl/onderwerpen/log4j
[15] https://www.csirtdsp.nl/

Vraag 15
Vindt u het wenselijk dat zoveel bedrijven en instellingen afhankelijk zijn van het veiligheidsbeleid van één bedrijf? Zo nee, wat is hiervoor volgens u een oplossing?

Antwoord 15
Als een (digitale) toepassing door heel veel bedrijven en instellingen wordt gebruikt dan zal de economische of maatschappelijke schade bij incidenten veelal groter zijn dan wanneer er weinig gebruikers zijn. Organisaties zijn zelf primair verantwoordelijk voor hun eigen digitale weerbaarheid en het bepalen van welke producten of diensten ze daartoe afnemen. Voor verschillende organisaties geldt wel dat ze wel onder meer op grond van de Wbni een zorgplicht hebben en dus passende en evenredige beveiligingsmaatregelen moeten treffen. Ook vindt er toezicht op de naleving hiervan plaats.[16] Daarnaast is het kabinet in dit verband positief over het commissievoorstel voor de herziening van de NIB-richtlijn. Dat voorstel bevat onder andere bepalingen over het inrichten van een proces voor gecoördineerde risicoanalyses voor kritieke ICT-systemen, -producten of diensten. Ook regelt het voorstel dat de entiteiten die zullen vallen onder de herziene NIB-richtlijn adequate beveiligingsmaatregelen moeten treffen, waarbij ook rekening moet worden gehouden met de beveiliging van hun toeleveringsketens. Zie ook het antwoord op vraag 16.

Vraag 16
Kunt u aangeven of er een melding moet worden gedaan van digitale aanvallen en beveiligingslekken waardoor er preventief kan worden opgetreden om verdere onveiligheden op te lossen? Kunt u uw antwoord toelichten?

Antwoord 16
Het doel van het kabinetsbeleid ten aanzien van digitale aanvallen en beveiligingslekken is om slachtoffers en schade te voorkomen, het aanvalsproces te verstoren en daders op te sporen. Voor verschillende organisaties geldt er onder meer krachtens de Wbni reeds een meldplicht van incidenten met aanzienlijke gevolgen voor de dienstverlening. Op dit moment wordt er in de EU onderhandeld over de herziening van de NIB-richtlijn, die in Nederland is geïmplementeerd via de Wbni. Met de herziening van de NIB-richtlijn zal het aantal sectoren en organisaties die onder de herziene richtlijn komen te vallen en dus onder meer moeten voldoen aan een meldplicht van incidenten met aanzienlijke gevolgen voor de dienstverlening behoorlijk worden uitgebreid. Tevens stimuleert het NCSC het inrichten van een beleid voor Coordinated Vulnerability Disclosure (CVD), waarbij gebruikers melding kunnen maken van kwetsbaarheden bij de eigenaars of producenten van software en systemen. Het NCSC kan bemiddelen indien een leverancier of eigenaar niet of niet goed reageert op een dergelijke melding.
Daarnaast staan het NCSC, het CSIRT voor digitale diensten en het DTC met elkaar in contact om zo veel als mogelijk te adviseren over welke beveiligingsmaatregelen organisaties kunnen nemen en zij waarschuwen bij geconstateerde kwetsbaarheden hun onderscheidenlijke doelgroepen om onder meer het bewustzijn te vergroten. Ook bieden ze hulpmiddelen voor het treffen van maatregelen aan ter verhoging van de cyberweerbaarheid.

[16] Zie voor overzicht toezichthoudende diensten: https://www.nctv.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen/wie-doet-wat/bevoegde-autoriteiten