Impactanalyse
Wet digitale overheid

De impact van de Wet digitale overheid (Wdo) op overheidsorganisaties en hun informatievoorziening

Auteur: Remco Overvelde

November 2024

archixl

Inleiding

De Wet digitale overheid[1] is een kaderwet die sinds **1 juli 2023** (gedeeltelijk) van kracht is. De wet wordt gefaseerd ingevoerd. De wet regelt dat **veilig** en **betrouwbaar** inloggen bij de (semi-)overheid voor **Nederlandse burgers** en **bedrijven** mogelijk is. Het is een **kaderwet** die de algemene principes, verantwoordelijkheden en procedures hiervoor benoemt. De wet zorgt ervoor dat belangrijke waarden en zekerheden voor burgers en bedrijven altijd geborgd zijn. Details van deze wet zijn in Algemene Maatregelen van Bestuur (**AMvB's**) en Ministeriële Regelingen (**MR's**) verder uitgewerkt.

In deze impactanalyse onderzoeken we wat de impact van de Wdo is op de **informatievoorziening** van (semi-)overheidsorganisaties in de Nederlandse publieke sector. De analyse is gedaan op basis van eerder uitgevoerde impactanalyses en andere gevonden artikelen. Het document is opgedeeld in vier hoofdstukken:

1. De **inhoud** van de Wdo
2. **Toelichting** van de Wdo
3. **Samenhang** met andere verordeningen, wetten en kaders
4. Analyse van de **impact** van de Wdo op de informatievoorzieningen van (semi)overheidsorganisaties

1. Inhoud Wdo (artikelen)

In deze sectie zullen de hoofdstukken en bijbehorende artikelen worden besproken. De artikelen aangeduid met een * zijn nog niet in werking getreden (per 21-02-2024).

Hoofdstuk 1 - Algemeen

Artikel 1: Definities

Enkele belangrijke definities uit dit artikel.

attribuut:	uniek kenmerk of gegeven van een natuurlijke persoon, onderneming of rechtspersoon;
authenticatie:	elektronisch proces voor de verificatie en bevestiging van de identiteit van een natuurlijke persoon, onderneming of rechtspersoon;
eIDAS-verordening[1]:	Verordening (EU) 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.
erkende dienst:	middelenuitgever, authenticatiedienst, ontsluitende dienst of machtigingsdienst die is erkend op grond van artikel 9 of 11 van deze wet.
ontsluitende dienst:	partij die het elektronisch verkeer tussen een bestuursorgaan of aangewezen organisatie en erkende authenticatiediensten, middelenuitgevers en machtigingsdiensten routeert teneinde toegang tot elektronische dienstverlening te faciliteren;

Artikel 2: Reikwijdte

Dit artikel bevat bepalingen over de reikwijdte van deze wet. Voor de toepassing van deze wet worden rechterlijke instanties gelijkgesteld met bestuursorganen en aangewezen organisaties.

Hoofdstuk 2 - Algemene regels

Artikel 3: Standaarden

Standaarden voor digitaal verkeer kunnen verplicht gesteld worden bij AMvB, mits verplichtingsproces en beschikbaarheid ervan aan de eisen voldoen.

De AMvB bepaalt: (a) het functioneel toepassingsgebied, (b) de organen waar dit voor geldt en (c) de ingangsdatum.

Op 11 mei 2023 is besloten in een AMvB dat de volgende standaarden verplicht worden gesteld voor publiek toegankelijke websites en webapplicaties van bestuursorganen: HTTPS en HSTS . Deze standaarden moeten worden geconfigureerd overeenkomstig de instellingen die de status voldoende of goed krijgen in de TLS-richtlijnen. Een bezoeker van de website/webapplicatie moet doorverwezen worden naar de HTTPS-versie op de bezochte domeinnaam.

[1] eIDAS, https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32014R0910

Hoofdstuk 3 - De generieke digitale infrastructuur

Artikel 4: Informatieveiligheid*

Organen voldoen aan regels (gesteld door AMvB) over de toegang tot digitale diensten op verschillende betrouwbaarheidsniveaus. De organen overleggen periodiek een verklaring van een auditor dat zij hieraan voldoen.

Artikel 5: Verantwoordelijkheid voor het beheer

Minister van BZK draagt zorg voor de generieke digitale infrastructuur en de voorzieningen.

Hoofdstuk 4 - Toegang tot elektronische dienstverlening

Artikel 6: Betrouwbaarheidsniveaus

Bestuursorganen moeten zelf aangeven welke betrouwbaarheidsniveaus nodig zijn voor hun diensten, en machtiging daarbij. We kennen de betrouwbaarheidsniveaus laag, substantieel en hoog. Er is ruimte om tijdelijk voor substantieel of hoog toch een niveau lager te kunnen laten authenticeren, waarbij niveau laag wel 'two-factor' moet zijn.

Artikel 7: Acceptatie*

Bestuursorganen mogen uitsluitend de toegelaten identificatiemiddelen accepteren.

Artikel 8: Gebruik in publieke domein

Het gebruik van het publiek identificatiemiddel voor toegang tot bestuursorganen wordt beperkt.

Artikel 9: Toelaten van identificatiemiddelen en diensten*

De minister van BZK kan:
(a) identificatiemiddelen toelaten (mits die voldoen aan eisen van werking, beveiliging en betrouwbaarheid);
(b) een publieke middelenuitgever en authenticatiedienst erkennen*
(c) een ontsluitende dienst erkennen*

*Mits deze voldoet aan bij AMvB nader te stellen voorwaarden en regels (leveringsplicht, dekkingsgraad, tarieven, uitgifte en beëindiging).

Artikel 10: Regels ten aanzien van gebruik

De gebruiker van een identificatiemiddel moet diefstal, verlies en misbruik van dit middel voorkomen. Gebruikers zijn burgers en bedrijven.

Artikel 11*

De richtlijnen voor het erkennen van een middelenuitgever, authenticatiedienst, ontsluitende dienst of machtigingsdienst. De aard van de criteria die een rol spelen worden hierin uitgelegd.

Artikel 12*

Attributen (gegevens) kunnen worden betrokken bij de digitale identificatie voor bedrijven of rechtspersonen. De minister moet hiervoor aanwijzingen doen en publiceren in de Staatscourant.

Artikel 13*

Dit artikel bevat bepalingen over de rechten en plichten voor erkende diensten, met de optie tot nadere regels bij AMvB, tot bindende aanwijzing door de minister, of geven van een ontheffing.

Artikel 14*

Dit artikel regelt de intrekking van de erkenning, beëindiging of overdracht ervan.

Artikel 15*

Dit artikel beschrijft bijzondere situaties voor het niet hoeven accepteren van identificatiemiddelen voor bedrijven of organisaties als KvK-nr of RSIN voor dienstverlening op substantieel/hoog niveau niet nodig zijn.

Hoofdstuk 5 - Bescherming van persoonsgegevens

Artikel 16: Bescherming persoonsgegevens

De verwerking van persoonsgegevens is toegestaan voor de goede uitvoering van deze wet, inclusief verwerking van het BSN.

Hoofdstuk 6 - Naleving

Artikel 17: Toezicht en handhaving

De minister wijst ambtenaren aan voor het naleven van art 3, 6, 7, 8 en 15 van bestuursorganen. De Rijksinspectie Digitale Infrastructuur (RDI) is aangewezen als toezichthouder op authenticatie- en machtigingsdiensten. Zij houdt toezicht op de naleving van de eisen die in de Wdo en onderliggende regelgeving aan deze partijen stellen. Publieke dienstverleners moeten voldoen aan de gestelde eisen over informatieveiligheid. Op de naleving van deze regels ziet Logius toe.

Artikel 18: Bijzondere bevoegdheden

De minister kan de toegang tot elektronische dienstverlening van een bestuursorgaan onderbreken, bij ernstige verstoringen, incidenten, misbruik of niet-naleving.

Artikel 19: Informatieverstrekking

Bestuursorganen en houders van een erkenning moeten incidenten melden. De minister heeft een informatieplicht voor het melden over inbreuken op veilige en betrouwbare digitale toegang.

Hoofdstuk 7 - Financiële bepalingen

Artikel 20: Leges voor verstrekking publiek identificatiemiddel

De kosten die het Rijk maakt voor een publiek identificatiemiddel worden doorbelast aan de verkrijger van het middel. Bij ministeriële regeling wordt per publiek middel het tarief en wijze van betaling vastgesteld.

Artikel 21: Doorberekening kosten*

Kosten voor uitvoering van art 5 en 9 worden doorbelast aan bestuursorganen en aangewezen organisaties.

Artikel 22: Doorberekening aanvraag erkenning en toezicht op naleving erkenningseisen*

Voor erkenningen en het toezicht daarop kan de minister een heffing opleggen, wordt geregeld bij AMvB.

Hoofdstuk 8 - Overgangs- en slotbepalingen

Artikel 23: Evaluatie

De wet moet geëvalueerd worden binnen 5 jaar na inwerkingtreding.

Artikel 24: Overgangsrecht bedrijfs- en organisatiemiddel*

Dit artikel bevat het overgangsrecht voor organisatie en bedrijfsmiddelen.

Artikel 25: Parlementaire betrokkenheid bij gedelegeerde regelgeving

Beide kamers der Staten-Generaal moeten worden betrokken bij voordrachten van AMvB en bij de daadwerkelijke vaststelling van AMvB.

Artikel 26: Innovatie

Bij AMvB kan er worden afgeweken van deze wet als innovatie de authenticatie doeltreffender en veiliger kan maken. Een experiment wordt dan ingesteld met een duur van ten hoogste vier jaar.

Artikel 27: Wijziging Wegenverkeerswet 1994

Aanpassing van de wegenverkeerswet, omdat de kosten voor het publiek ID-middel op het rijbewijs in de leges daarvoor kunnen worden doorbelast.

Artikel 28: Omhangen

Na de inwerkingtreding van deze wet berust het
(a) “Besluit verwerking persoonsgegevens generieke digitale infrastructuur op artikel 16, vierde lid, van deze wet”;
(b) “het Tijdelijk besluit digitale toegankelijkheid overheid op artikel 3, tweede en derde lid, van deze wet.”

Artikel 29: Inwerkingtreding

Artikel 3 en 20 treden in werking een dag na de datum van uitgifte van de Staatscourant waarin zij wordt geplaatst. Op 1 juli 2023 is de Wdo (gedeeltelijk) in werking getreden.

Artikel 30: Citeertitel

“Wet digitale overheid”

2. Toelichting Wdo

In deze sectie zullen we de Wdo verder toelichten. Wat houdt de Wdo in, wie zijn er betrokken bij de Wdo, waarom is de Wdo er, op welke wijze wordt de Wdo ingezet, wanneer wordt de Wdo ingezet en met welke middelen wordt de Wdo ingezet. Daarbij wordt de samenhang met andere verordeningen, wetten en kaders toegelicht.

Wat houdt de Wdo in?

De Wet digitale overheid is een eerste tranche van regelgeving ten behoeve van de verdere digitalisering van de overheid op verschillende niveaus. Het is een zogeheten kaderwet: de wet regelt algemene principes, verantwoordelijkheden en procedures, maar bevat geen gedetailleerde regels. De details worden uitgewerkt in AMvB's en MR's. De wet bevat, volgens de Memorie van Toelichting, urgente onderwerpen van regelgeving voor de digitale overheid, te weten:

- De bevoegdheid om bepaalde (open) **standaarden** te verplichten in het elektronisch verkeer van de overheid;
- Het stellen van regels over **informatieveiligheid** en het verwerken van persoonsgegevens;
- De **verantwoordelijkheid** voor het beheer van de Generieke Digitale Infrastructuur (GDI) en de voorzieningen;
- Regels voor de **digitale toegang** tot publieke dienstverlening voor burgers en bedrijven.

Het besluit digitale toegankelijkheid overheid is ook onderdeel van de Wdo[2]. Vanaf 1 april 2024 worden websites en applicaties met een minimale status voor digitale toegankelijkheid als ontoegankelijk aangemerkt.

Wie is er betrokken bij de Wdo?

De **minister van BZK** is verantwoordelijk voor het beheer van de GDI. **Logius** is de uitvoerende organisatie onder aansturing van het ministerie van BZK.

De wet stelt regels voor **bestuursorganen** en '**aangewezen organisaties'** die publieke digitale diensten aanbieden. De bestuursorganen zijn bijvoorbeeld de staat, provincies, waterschappen, gemeenten, maar ook uitvoeringsorganisaties, zoals Belastingdienst, DUO en het UWV. De aangewezen organisaties zijn vooralsnog zorgaanbieders, zorgverzekeraars, pensioenuitvoerders en instellingen in het hoger onderwijs.

De wet stelt ook regels voor private partijen (erkende diensten), zoals de middelenuitgever, authenticatiedienst, ontsluitende dienst of machtigingsdienst. De private partijen moeten voldoen aan regels en voorwaarden om toegelaten te worden tot het stelsel als 'erkende dienst'.

Waar geldt de Wdo?

De Wdo heeft alleen betrekking op de Nederlandse publieke digitale dienstverlening. Het heeft invloed op **Nederlandse burgers** met een BSN en **Nederlandse bedrijven**.

Waarom bestaat de Wdo?

De Wdo is gebaseerd op het regeerakkoord Rutte III. De Wdo legt de basis voor een verdere digitalisering van de Nederlandse overheid[3]. Daarbij regelt het dat burgers en bedrijven **veilig** en

betrouwbaar kunnen inloggen bij de (semi-)overheid. Daarmee wordt bedoeld dat burgers elektronische identificatiemiddelen krijgen met een 'hoog' of 'substantieel' betrouwbaarheidsniveau. De betrouwbaarheidsniveaus zijn gebaseerd op die in de Europese verordening eIDAS. Private inlogmiddelen en inlogmiddelen uit andere Europese lidstaten worden ook toegelaten.

Op welke wijze wordt de Wdo ingezet?

De minister van BZK is verantwoordelijk voor de technische ontwikkeling en het beheer van de **GDI**, zoals DigiD, een machtigingsvoorziening en een routeringsvoorziening waarmee publieke dienstverleners via één punt aansluiten op de verschillende inlogmiddelen. Een deel van de technische ontwikkeling vindt plaats op de vrije markt. De private voorzieningen (bijv. inlogmiddelen of ontsluitende diensten) kunnen worden toegelaten als 'erkende dienst' door de minister van BZK.

De verschillende betrouwbaarheidsniveaus zijn geregeld in de **Regeling betrouwbaarheidsniveaus**[4]. Hierin staan regels voor het bepalen van het betrouwbaarheidsniveau van authenticatie en machtiging voor een elektronische dienst en de communicatie hierover naar gebruikers. Bestuursorganen kunnen kiezen voor de routeringsvoorziening of voor een andere 'ontsluitende dienst'.

Wanneer treedt de Wdo in werking?

De Wdo wordt per **1 juli 2023** gefaseerd ingevoerd. Niet alle artikelen treden al in werking, omdat er nog onduidelijkheden zijn over de uitvoering hiervan. Verdere details van de uitwerking van de wet zullen in **AMvB's** en **MR's** worden opgenomen.

Met welke middelen?

De financiële bepalingen zijn opgenomen in artikel 20, 21 en 22.

De kosten die gemaakt worden voor een publiek middel worden doorbelast aan de gebruiker. De private middelen zullen hun kosten ook doorberekenen aan de gebruiker

De kosten voor de ontwikkeling en het beheer van de GDI en het toelaten van middelen en diensten worden doorberekend aan de publieke dienstverleners.

Aan het erkennen van middelen en diensten en het toezicht erop hangen ook kosten. Dit zijn vastgestelde tarieven voor de aanvrager.

3. Samenhang Wdo met andere wetten

De Wet digitale overheid hangt samen met een aantal andere Europese verordeningen en nationale wetten en kaders. In dit hoofdstuk zullen we deze wetten behandelen.

eIDAS-verordening

In de eIDAS staan afspraken over de **onderlinge digitale infrastructuur** van lidstaten en verschillende betrouwbaarheidsniveaus. eIDAS staat voor “Electronic Identitites And Trust Services”. Een onderdeel van de verordening is het grensoverschrijdend gebruik van **Europees erkende inlogmiddelen**. Maar in de eIDAS zijn ook de mogelijke **betrouwbaarheidsniveaus** voor inlogmiddelen vastgelegd. De betrouwbaarheidsniveaus zijn ‘laag’, ‘substantieel’ en ‘hoog’. Deze niveaus worden ook in de Wdo toegepast. De eIDAS verplicht organisaties om een inlogmiddel te hanteren dat past bij het betrouwbaarheidsniveau van de dienst. Nederlandse (semi-)overheidsorganisaties moeten sinds *29 september 2018* Europees erkende inlogmiddelen accepteren.

eIDAS2-verordening

De herziene eIDAS-verordening ziet erop om de **tekortkomingen** van de oorspronkelijke eIDAS op te lossen. De nieuwe verordening introduceert een Europese **portemonnee** (**wallet**) waarmee burgers gebruik kunnen maken van digitale diensten. De wallet kan gebruikt worden als een identificatiemiddel en kan als volgt worden ingezet:

- De wallet kan toegang geven tot een persoonlijke bankrekening;
- Het indienen van een belastingaangifte kan geschieden m.b.v. de wallet;
- De inschrijving tot een onderwijsinstelling kan worden voltooid met de inzet van de wallet.

De verordening is echter nog niet klaar en technische aspecten moeten nog verder worden uitgewerkt. Het is dus *niet duidelijk* wanneer de vernieuwde versie van de eIDAS in werking treedt.

Wet Modernisering Elektronisch Bestuurlijk Verkeer (WMEBV)

De WMEBV zal naar verwachting op *1 januari 2026* in werking treden. De WMEBV regelt dat burgers en bedrijven het recht krijgen om **officiële berichten**, zoals aanvragen voor vergunningen en bezwaarschriften, elektronisch aan het bestuursorgaan te zenden op een door het bestuursorgaan bepaalde wijze. Voor de implementatie van de wet is een handreiking opgesteld om bestuursorganen te ondersteunen en mogelijke vragen rond de werkingssfeer te beantwoorden[5].

Algemene Verordening Gegevensbescherming (AVG)

Vanuit de AVG is er een wettelijke grondslag nodig voor het gebruik maken van het BSN en sommige andere gegeven. De Wdo biedt deze wettelijke grondslag, ook aan private partijen die gegevens nodig hebben als erkende dienst.

Algemene wet bestuursrecht (Awb)

De Awb vereist dat elektronisch verkeer tussen burger en bestuursorgaan ‘voldoende betrouwbaar en vertrouwelijk’ verloopt en dat eenieder zich moet kunnen laten bijstaan of vertegenwoordigen.

Wegenverkeerswet

Door de Wdo is een aanpassing aan de wegenverkeerswet nodig. Op rijbewijzen is vanaf 2018 een publiek identificatiemiddel geplaatst.

Paspoortwet

Per 4 januari 2021 is er in de identiteitskaart een applet ingebouwd waarmee je kan inloggen via DigiD betrouwbaarheidsniveaus ‘substantieel’ en ‘hoog’.

Baseline Informatiebeveiliging Overheid (BIO)

Vanaf 1 januari 2020 is de BIO van kracht, een gezamenlijk normenkader voor informatiebeveiliging voor de gehele overheid, gebaseerd op de ISO27001/2. Vanuit de BIO worden eisen gesteld aan de inrichting van de toegang van gebruikers tot informatie en informatie verwerkende faciliteiten. De eisen rondom informatiebeveiliging zullen gebaseerd zijn op de BIO.

4. Impact op organisaties en hun informatievoorzieningen

In dit hoofdstuk zullen we de impact van de Wet digitale overheid analyseren op basis van analyses die al gemaakt zijn door andere partijen [3][6]. De impactanalyses kijken naar verschillende soorten organisaties, zoals gemeenten, provincies, waterschappen, uitvoeringsorganisaties(zoals de Belastingdienst, DUO en RWS), maar ook naar organisaties in de zorg en het onderwijs. Als bepaalde informatie specifiek voor een soort organisatie is, zal dat expliciet worden vermeld. We zullen de impact toelichten aan de hand van verschillende aspecten van de Wdo.

4.1. Informatiebeveiliging van toegang tot elektronische dienstverlening

Organisaties zijn door de Wdo wettelijk verplicht om maatregelen te nemen op het gebied van informatiebeveiliging van de toegang tot hun elektronische dienstverlening. Toezicht hierop vindt plaats middels een self-assessment en een verklaring van een onafhankelijke auditor, waarmee verantwoording wordt afgelegd aan de minister van BZK. Als organisaties zich niet houden aan de regels, kan toegang tot de elektronische dienstverlening worden onderbroken (artikel 18). Gedetailleerde regels zijn toegelicht in de Regeling dienstverleners informatieveiligheidsaudits [7].

Artikel 4 gaat over de informatieveiligheid van de toegang van de elektronische dienstverlening. Artikel 16 gaat over het verwerken van persoonsgegevens, zoals het BSN. Artikel 21 van het Besluit verwerking persoonsgegevens generieke digitale infrastructuur [8] bepaalt dat organisaties geacht worden te voldoen aan de gestelde eisen over informatiebeveiliging. Het bepaalt bijvoorbeeld dat organisaties zich aan artikel 16 tot en met 19 van het besluit moeten houden als zij ISO/NEN 27001 en 27002 toepassen voor de toegang tot elektronische dienstverlening. De artikelen in dit besluit brengen diverse verplichtingen met zich mee met betrekking tot informatieveiligheidsbeleid, organisatie en beheer, personele en fysieke beveiliging en ICT-voorzieningen en informatiesystemen. Er zal dus veel werk nodig zijn om het informatieveiligheidsbeleid uit te voeren in een organisatie.

Verantwoording informatiebeveiliging

Organisaties leggen nu verantwoording af via de ENSIA-methodiek, waarin de BIO-normen zijn verwerkt. De extra lastendruk zal voor organisaties liggen in het verantwoording afleggen op het gebied van informatiebeveiliging voor meerdere inlogmiddelen. Verder moeten de informatiebeveiligingsmaatregelen meegenomen worden in de “Plan Do Check Act”-cyclus en moet er een ISMS worden ingericht voor informatiebeveiliging.

Logging

Het gewijzigde Besluit verwerking persoonsgegevens generieke digitale infrastructuur bepaalt dat overheidsorganisaties logbestanden moeten bijhouden over het gebruik van ICT voorzieningen voor toegang tot elektronische dienstverlening en deze regelmatig bijhouden. Logbestanden betreffen de uitgevoerde authenticaties, de daarbij gebruikte identificatiemiddelen, de tijdstippen waarop is ingelogd en uitgelogd, de systeemtechnische gegevens, waaronder het IP-adres en, indien van toepassing, machtigingsgegevens. De logbestanden worden maximaal 5 jaar bewaard [8].

Organisaties moeten hiervoor wellicht technische aanpassingen doen aan hun logging systemen, dit vergt veelal een grote inspanning. De opslag en het beheer van log-gegevens en de beveiliging ervan moet worden ingericht.

4.2 Digitale diensten moeten worden ingeschaald naar betrouwbaarheidsniveaus

In artikel 6 en in de regeling betrouwbaarheidsniveaus authenticatie elektronische dienstverlening [4] is deze bepaling opgenomen. Hierin zijn regels opgenomen voor het bepalen van het betrouwbaarheidsniveau van authenticatie en machtiging voor een elektronische dienst en de communicatie hierover naar de burger.

Inschaling van dienstverlening

Organisaties zijn verplicht hun digitale diensten in te schalen op betrouwbaarheidsniveau. Op dit moment wordt alle gemeentelijke online dienstverlening nog op betrouwbaarheidsniveau 'laag' aangeboden. De Wdo hanteert de drie Europese eIDAS-betrouwbaarheidsniveaus 'Laag', 'Substantieel' en 'Hoog'. Het eIDAS-betrouwbaarheidsniveau 'Laag' gaat uit van tenminste een tweefactor authenticatie. Het inschalen van digitale diensten zal veel werk opleveren voor organisaties. Het Ministerie van BZK en de RVO hebben een regelhulp betrouwbaarheidsniveaus[2] ontwikkeld om organisaties te helpen met deze inschaling. VNG realisatie heeft een overzicht van betrouwbaarheidsniveaus voor de gemeentelijke dienstverlening gemaakt om gemeenten te ondersteunen[9].

In de zorg moeten digitale diensten voldoen aan betrouwbaarheidsniveau 'substantieel' of 'hoog'. Als er sprake is van toegang tot medische persoonsgegevens geldt het betrouwbaarheidsniveau 'hoog'. Forum Standaardisatie heeft in 2016 een handreiking geschreven om overheidsorganisaties te ondersteunen bij het kiezen van een betrouwbaarheidsniveau voor een digitale dienst.[3] Eind november 2024 zal er een nieuwe versie van deze handreiking gepubliceerd worden

De grootste impact gaat zitten in het herzien van de digitale dienstverlening. Er moet per dienst nagegaan worden welke gegevens verwerkt worden en of voor deze dienst authenticatie noodzakelijk of wenselijk is. Daarbij moet gekeken worden welk betrouwbaarheidsniveau van authenticatie van toepassing is voor welke dienst (bij machtiging is een naastgelegen lager betrouwbaarheidsniveau toegestaan, mits inachtneming van risico-verlagende maatregelen).

Communicatie

Daarbij moeten organisaties de communicatie met inwoners en organisaties op orde hebben over de verplichte betrouwbaarheidsniveaus van inlogmiddelen. Het wordt wellicht lastiger voor inwoners om in te loggen bij digitale diensten, waardoor organisaties meer ondersteuning moeten bieden op locatie. Organisaties zullen hoogstwaarschijnlijk geen extra ondersteuning nodig hebben bij het gebruik van een inlogmiddel met een hoger betrouwbaarheidsniveau.

Randvoorwaarde: Informatiehuishouding op orde

Een belangrijke randvoorwaarde voor het inschalen van de digitale diensten naar betrouwbaarheidsniveau is dat de informatiehuishouding op orde is. Het moet inzichtelijk zijn welke digitale diensten er zijn en wie verantwoordelijk is voor die diensten. Daarbij is het bij het inschalen van digitale diensten nodig om nog eens te kijken naar dataminimalisatie.

---

[2] Regelhulp Betrouwbaarheidsniveaus, https://regelhulpenvoorbedrijven.nl/betrouwbaarheidsniveaus/

[3] Handreiking Betrouwbaarheidsniveaus, https://www.forumstandaardisatie.nl/onderwerpen/veilig-internet/betrouwbaarheidsniveaus

4.3. Acceptatieplicht toegelaten inlogmiddelen

Organisaties worden verplicht om alle publieke en alle erkende (private) inlogmiddelen te accepteren. Momenteel zijn de meeste organisaties aangesloten op DigiD en eHerkenning. Dat wordt straks dus anders als meerdere publieke en erkende inlogmiddelen op de markt zijn.

Organisaties kunnen gebruikmaken van een routeringsvoorziening, waarbij alle erkende inlogmiddelen zijn aangesloten. Een dergelijke oplossing is de belangrijkste randvoorwaarde voor organisaties om te kunnen voldoen aan de acceptatieplicht. De routeringsvoorzieningen zijn nog in ontwikkeling, waarbij de TVS al gebruikt wordt binnen de Rijksoverheid en de zorgsector.
Met de TVS kunnen organisaties in de zorg zich nu al in één keer Wdo-proof inrichten.

Organisaties kunnen er ook voor kiezen om een leverancier te contracteren die onder verantwoordelijkheid van de organisatie zelf een routeringsvoorziening aanbiedt. Echter, er is voor veel organisaties nog te veel onduidelijk over of en hoe ze willen aansluiten bij een dergelijke routeringsvoorziening.

Op dit moment is een inlogmiddel vaak onderdeel van een informatiesysteem waar een dienst op berust. In de toekomst zou een inlogmiddel gebruikt kunnen worden voor meerdere diensten, die wellicht op meerdere informatiesystemen berusten. Organisaties zijn afhankelijk van de aanpassingen die leveranciers moeten maken om de toegelaten inlogmiddelen toe te laten tot hun informatiesystemen.

Provincies en waterschappen stellen dat hoe meer inlogmiddelen moeten worden geaccepteerd hoe meer maatregelen nodig zijn om voldoende mate van beveiliging van dienstverlening te kunnen blijven realiseren. Het vergt veel werk om alle erkende inlogmiddelen te accepteren.

4.4. Verplichte standaarden

Organisaties zijn per 1 juli 2023 verplicht om hun publiek toegankelijke websites en webapplicaties te voorzien van de volgende standaarden: HTTPS en HSTS. Dit is bepaald in het besluit Beveiligde verbinding met overheidswebsites en -webapplicaties [10].

De HTTPS en HSTS standaarden moeten worden geconfigureerd overeenkomstig met instellingen die de status voldoende of goed krijgen in de TLS-richtlijnen. Een bezoeker van de website/webapplicatie moet doorverwezen worden naar de HTTPS-versie op de bezochte domeinnaam.

Vanuit meerdere organisaties lijken er weinig belemmeringen te zijn om te voldoen aan de verplichte standaarden HTTPS en HSTS. Een belangrijke uitdaging is om het overzicht te houden van publiek toegankelijke websites. De meeste organisaties hebben een dergelijk overzicht op orde.

Gebruikte bronnen

[1] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, *Wet digitale overheid*. Accessed: Feb. 16, 2024. [Online]. Available: https://wetten.overheid.nl/BWBR0048156/2023-07-01

[2] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, *Tijdelijk besluit digitale toegankelijkheid overheid*. Accessed: Feb. 16, 2024. [Online]. Available: https://wetten.overheid.nl/BWBR0040936/2018-07-01

[3] VNG Realisatie, "Impactanalyse Wet digitale overheid: 1e analyse op de onderdelen informatiebeveiliging, acceptatieplicht en betrouwbaarheidsniveaus." [Online]. Available: https://vng.nl/sites/default/files/2021-06/20210419-rapportage-impactanalyse-wet-digitale-overheid-.pdf

[4] Ministerie van Binnenlandse Zaken en koninkrijksrelaties, *Regeling betrouwbaarheidsniveaus authenticatie elektronische dienstverlening*. Accessed: Feb. 21, 2024. [Online]. Available: https://wetten.overheid.nl/BWBR0048168/2023-07-01

[5] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, "Handreiking implementatie Wet modernisering elektronisch bestuurlijk verkeer," webpagina. Accessed: Feb. 21, 2024. [Online]. Available: https://www.digitaleoverheid.nl/document/eindconcept-voorlopige-handreiking-implementatie-wet-modernisering-elektronisch-bestuurlijk-verkeer-11-april-2017/

[6] Berenschot, "Uitvoeringstoets Wdo | Eindrapport." [Online]. Available: https://uvw.bestuurlijkeinformatie.nl/Document/View/5573fac9-08c2-488d-bda9-5182aa9b9390

[7] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, *Regeling dienstverleners informatieveiligheidsaudits Wdo*. [Online]. Available: https://www.internetconsultatie.nl/informatieveiligheidsaudits/document/11203

[8] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, *Besluit van 30 oktober 2023, houdende wijziging van het Besluit verwerking persoonsgegevens generieke digitale infrastructuur in verband met het stellen van de kaders voor informatieveiligheid en persoonsgegevensverwerking*. Ministerie van Justitie en Veiligheid, 2023. Accessed: Mar. 08, 2024. [Online]. Available: https://zoek.officielebekendmakingen.nl/stb-2023-390.html

[9] VNG Realisatie, "Betrouwbaarheidsniveaus online dienstverlening." Accessed: Feb. 21, 2024. [Online]. Available: https://vng.nl/artikelen/betrouwbaarheidsniveaus-online-dienstverlening

[10] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, *Besluit van 11 mei 2023, houdende aanwijzing van de open informatieveiligheidsstandaarden HTTPS en HSTS voor websites en webapplicaties van bestuursorganen (Besluit beveiligde verbinding met overheidswebsites en -webapplicaties)*. Ministerie van Justitie en Veiligheid. Accessed: Feb. 21, 2024. [Online]. Available: https://zoek.officielebekendmakingen.nl/stb-2023-179.html