Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Handleiding uitvoering ICT-beveiligingsassessment

Versie 2.2

Datum : 19 december 2016
Status : Definitief

Colofon

Projectnaam : DigiD
Versienummer : 2.0
Contactpersoon : Servicecentrum Logius
Postbus 96810
2509 JE 's-Gravenhage
servicecentrum@logius.nl

Documentbeheer

Datum	Versie	Auteur	Opmerkingen
22 februari 2012	1.0	Logius	
30 november 2012	2.0	Logius	Wijziging NOREA Richtlijn
01 januari 2013	2.1	Logius	Wijziging Hoofdstuk 5
19 december 2016	2.2	Logius	Hyperlink aangepast

Inhoud

Inleiding

Op 11 oktober 2011 heeft de Minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) per brief (kenmerk 2011-2000454268) de Tweede Kamer geïnformeerd over de aanpak van de geconstateerde beveiligingslekken bij een aantal gemeentelijke websites. De feitelijke uitvoering van het beleid heeft de Minister opgedragen aan Logius.

In vervolg op deze brief, is de Minister op 2 februari 2012 in een brief aan de Tweede Kamer (kenmerk 2012-0000057362) nader ingegaan op de inzet van een aantal specifieke maatregelen, zoals deze is aangekondigd in de brief van 11 oktober 2011[1].

De Minister heeft in de brief van 2 februari 2012 aangegeven dat is gekozen voor een gefaseerde aanpak. De grootgebruikers van DigiD moeten voor het eind van 2012 een ICT-beveiligingsassessment hebben laten uitvoeren. De overige organisaties moeten het assessment voor eind 2013 hebben laten uitvoeren. Door deze gefaseerde aanpak zal voor de grootgebruikers vanaf 2012 en de overige organisaties vanaf 2013 sprake zijn van een jaarlijkse herhaling van het ICT-beveiligingsassessment.

Bij de uitvoering van ICT-beveiligingsassessments moet de "Norm ICT-beveiligingsassessments DigiD", gedateerd 21 februari 2012 worden gehanteerd[2]. Deze norm, die beschikbaar is op de website van Logius, is een selectie van richtlijnen uit het document "ICT-beveiligingsrichtlijnen voor webapplicaties" van het Nationaal Cyber Security Centrum (NCSC), die in samenspraak met een aantal publieke en private partijen is opgesteld. De actuele versie van de ICT-beveiligingsrichtlijnen is beschikbaar op de website van het NCSC[3]. De norm is vastgesteld door het ministerie van BZK in overleg met Logius, de auditdienst rijk en het NCSC.

De ICT-beveiligingsassessments moeten worden uitgevoerd onder verantwoordelijkheid van een Register EDP-auditor. De Minister staat toe dat organisaties die zelf een Register EDP-auditor in dienst hebben, de ICT-beveiligingsassessments onder verantwoordelijkheid van de interne Register EDP-auditor kunnen laten uitvoeren.

Een ICT-beveiligingsassessment heeft tot doel de verantwoordelijke voor de webomgeving en Logius inzicht te geven in de mate van beveiliging van de webomgeving. Dit brengt met zich mee dat organisaties die DigiD gebruiken, de uitkomsten van de ICT-beveiligingsassessments aan Logius ter beschikking stellen.

In aanvulling op de brief van 2 februari 2012 hebben het ministerie van BZK en Logius in samenspraak met NOREA (de beroepsgroep van de auditors) een vooraf gedefinieerd rapportageformat opgesteld. Met dit format is de toepassing van een uniforme rapportering bereikt waardoor

[1] *http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2012/02/03/kamerbrief-over-ict-beveiligingsassessments-bij-digid-gebruikende-organisaties/kamerbrief-over-ict-beveiligingsassessments-bij-digid-gebruikende-organisaties.pdf*

[2] *https://www.logius.nl/fileadmin/logius/ns/diensten/digid/assessments/120221_norm_ict-beveiligingsassessments_digid.pdf*

[3] *https://www.ncsc.nl/actueel/nieuwsberichten/ict--beveiligingsrichtlijnen.html*

waarborgen zijn gecreëerd voor de inzichtelijkheid en de reikwijdte van de rapportage voor alle betrokkenen.

1 Doel van deze handleiding

Deze handleiding heeft als doel om de Register EDP-auditor een handvat aan te reiken voor de wijze waarop hij invulling dient te geven aan het ICT-beveiligingsassessment.

2 Overleg

Om actief in te kunnen spelen op ontwikkelingen die zich in de uitvoeringspraktijk zullen voordoen, zal Logius periodiek overleg voeren met de direct betrokken partijen. De uitkomsten van dit overleg, kunnen, waar aan de orde en noodzakelijk, mogelijk leiden tot een herijking van de ICT-beveiligingsrichtlijnen voor webapplicaties van het NCSC en/of het ICT-beveiligingsassessment van het ministerie van BZK en Logius.

Eventuele vakinhoudelijke specifieke auditvragen over het ICT-beveiligingsassessment kunnen primair worden gericht aan NOREA.

3 Begrippen en definities

In deze handleiding wordt verstaan onder:

Opdrachtgever	:	degene die de opdracht tot het uitvoeren van een ICT-beveiligingsassessment verstrekt. Meestal zal dit in de praktijk de "verantwoordelijke" zijn. Het kan echter zijn dat een andere partij die daartoe bevoegd is, de opdrachtgever is.
Verantwoordelijke	:	de natuurlijke persoon, rechtspersoon of ieder ander die verantwoordelijk is voor de webomgeving die in het kader van een ICT-beveiligingsassessment wordt beoordeeld.
ICT-beveiligingsassessment	:	de werkzaamheden die in de vorm van een vastgesteld normenkader worden uitgevoerd, met als doel de gebruikers van het rapport in staat te stellen zichzelf een oordeel te vormen over de werkzaamheden en de bevindingen die de Register EDP-auditor in zijn rapport heeft weergegeven.
Webomgeving	:	de in het kader van een ICT-beveiligingsassessment te beoordelen webomgeving betreft de internet-facing webpagina's, systeemkoppelingen[4] en infrastructuur die met DigiD of DigiD 'eenmalig inloggen' gekoppeld zijn en betrekking hebben op het DigiD of het DigiD 'eenmalig inloggen' proces'.[5]
Register EDP-auditor	:	de Register EDP-auditor die de verantwoordelijkheid draagt voor de uitvoering van een ICT-beveiligingsassessment.
Normenkader	:	het toetsingskader dat wordt gebruikt voor het toetsen van een object van onderzoek, in dit geval de webomgeving zoals eerder is gedefinieerd. In het geval van een ICT-beveiligingsassessment moet de "Norm ICT-beveiligingsassessments DigiD", gedateerd 21 februari 2012 als norm worden gehanteerd. Deze norm is vastgesteld door het ministerie van BZK in overleg met Logius, de auditdienst rijk en het NCSC.

[4] *Hier wordt met name de s2s koppeling (authenticatieverzoek en uitwisselen RID en verificatieverzoek van webdienst) mee bedoeld.*

[5] *Deze afgebakende scope is een afweging tussen enerzijds het beperken van de scope van het onderzoek waardoor het uitvoerbaar blijft voor alle partijen en anderzijds het risico (blijven) lopen dat DigiD bij een afnemer alsnog kwetsbaar is via een lekke andere applicatie, die niet bij het DigiD proces is betrokken.*

4 Invulling van een ICT-beveiligingsassessment

Een ICT-beveiligingsassessment focust op het stelsel van maatregelen en procedures gericht op de beveiliging van een webomgeving. Het stelsel omvat zowel geautomatiseerde als niet geautomatiseerde maatregelen en procedures.

Het is mogelijk dat een organisatie (verantwoordelijke) die DigiD gebruikt een deel (van het beheer of de verwerking van) de webomgeving heeft uitbesteed aan een derde partij. In dit geval moet de verantwoordelijke waarborgen dat het ICT-beveiligingsassessment mede de uitbestede diensten omvat. Dit is mogelijk als de verantwoordelijke met deze derde partij afspraken heeft gemaakt, of maakt, over medewerking aan een ICT-beveiligingsassessment in de vorm van het recht om bij deze organisatie de noodzakelijke onderzoekswerkzaamheden uit te laten voeren door de verantwoordelijke Register EDP-auditor, dan wel door het beschikbaar stellen door deze derde organisatie van een assurance-rapport[6], dat de verantwoordelijke Register EDP-auditor de benodigde informatie verschaft over de kwaliteit van de dienstverlening en de interne beheersing van deze derde organisatie.

In de brief van 2 februari 2012 heeft de Minister aangegeven dat zij ervan uitgaat dat vertegenwoordigers van de organisaties die DigiD gebruiken per direct een samenwerkingstraject starten met een vertegenwoordiging van de auditors en ICT-leveranciers, met als doel om een efficiënte uitvoering van de ICT-beveiligingsassessments te bewerkstellingen.

Een ICT-beveiligingsassessment wordt uitgevoerd in de vorm van een opdracht tot het onderzoeken van de opzet en het bestaan van maatregelen en procedures die zijn gericht op de ICT beveiliging van de webomgeving van de DigiD aansluiting. Er worden geen werkzaamheden uitgevoerd die zijn gericht op de werking van interne beheersingsmaatregelen van de DigiD aansluiting.
De feitelijke bevindingen worden per norm aangegeven, waaruit blijkt of de webomgeving aan de gestelde norm wordt voldaan. Indien niet aan de norm wordt voldaan, dan dient kort en duidelijk de reden daarvoor worden benoemd.

De opdracht heeft als doel de lezer de informatie te verschaffen op basis waarvan de lezer een oordeel moet kunnen vormen over de werkzaamheden en de bevindingen die de Register EDP-auditor in het rapport heeft weergegeven.

[6] *NOREA Richtlijn Assurance-opdrachten door IT-auditors*

5 Opdrachtaanvaarding

Bij de aanvaarding van een opdracht tot het verrichten van auditwerkzaamheden dient de Register EDP-auditor na te gaan of hij beschikt over de vereiste deskundigheid. Hierbij dient hij rekening te houden met de specifieke problematiek die samenhangt met het gebruik van DigiD.

Indien een Register EDP-auditor niet zelf in voldoende mate beschikt over de vereiste kennis, dan kan hij gebruikmaken van deskundigen uit de eigen organisatie of van derden, met de aantekening dat de desbetreffende Register EDP-auditor in alle gevallen eindverantwoordelijk blijft voor de uitvoering van de opdracht.

Indien de Register EDP-auditor werkzaam is als interne auditor bij de organisatie waarvan de webomgeving moet worden beoordeeld, dan gaat hij bij de aanvaarding van de opdracht na of hij in voldoende mate onafhankelijk is van de verantwoordelijke.

Indien de Register EDP-auditor als interne auditor werkzaam is bij de organisatie van de verantwoordelijke en de eindverantwoordelijkheid draagt voor de opdracht, dan dient hij dit te vermelden in zijn rapport.

De Register EDP-auditor dient de opdrachtvoorwaarden vast te leggen in een schriftelijke opdrachtbevestiging overeenkomstig NOREA Richtlijn 'Opdrachtaanvaarding'. Aanvullend dient in de bevestiging ook te worden opgenomen:

- Een verwijzing naar de Logius "Handleiding uitvoeren ICT-beveiligingsassessment" waarin de overeengekomen auditwerkzaamheden zijn vastgelegd;
- Het feit dat de opdracht tot het verrichten van overeengekomen auditwerkzaamheden betrekking heeft op het beoordelen of de webomgeving voldoet aan de normen zoals vastgelegd in de "Norm ICT-beveiligingsassessments DigiD" gedateerd 21 februari 2012;
- Het feit dat de opdracht zich richt op het uitvoeren van een ICT-beveiligingsassessment DigiD waarin per afzonderlijke norm wordt vermeld of aan de norm is voldaan. Indien niet aan de norm wordt voldaan, dan dient kort en duidelijk de reden daarvoor worden benoemd;
- De rapportage uitsluitend bestemd is voor de opdrachtgever die, zoals aangegeven is in de brief van de Minister gedateerd 2 februari 2012, de opdrachtgever moet verstrekken aan Logius. Eventuele onderliggende deelrapportages, subbevindingen, managementletters, methodische verantwoordingen en dergelijke verstrekt de auditor primair ten behoeve van de opdrachtgever in wiens opdracht het onderzoek plaatsvindt. Wel dient te worden vermeld dat op verzoek van Logius de onderliggende bescheiden en dossiers aan Logius ter inzage worden verstrekt.

6 Het normenkader

De Register EDP-auditor dient bij zijn beoordeling de normen te hanteren die zijn opgesteld door het ministerie van BZK in overleg met Logius, de auditdienst rijk en het NCSC. In het normenkader is aangegeven aan welke eisen het stelsel van maatregelen en procedures in opzet en bestaan minimaal moet voldoen.

7 Aanpak en uitvoering van de werkzaamheden

De Register EDP-auditor dient bij de aanpak en de uitvoering van de werkzaamheden rekening te houden met de NOREA richtlijn 3000, "Richtlijn Assurance -opdrachten door IT-auditors'. Dit vereist dat de auditor voldoet aan de voor hem geldende ethische voorschriften en dat hij zijn werkzaamheden zodanig plant en uitvoert dat een redelijke mate van zekerheid wordt verkregen over de vraag of per norm de interne beheersingsmaatregelen, in alle van materieel belang zijnde aspecten, op afdoende wijze qua opzet en bestaan zijn ingeregeld.

8 Rapportering en vertrouwelijkheid

Om de bruikbaarheid en vergelijkbaarheid van de uitkomsten van ICT-beveiligingsassessments in de vorm van een opdracht tot het verrichten van overeengekomen specifieke werkzaamheden te waarborgen, dient de Register EDP-auditor voor zijn rapportage verplicht gebruik te maken van de in bijlage 1 opgenomen modelrapportage.

Deze rapportage is uitsluitend bestemd voor de opdrachtgever die, zoals aangegeven is in de brief van de Minister gedateerd 2 februari 2012, de de opdrachtgever moet verstrekken aan Logius.

Indien opdrachtgever een pleitbaar standpunt kan innemen dat er daadwerkelijk een gerechtvaardigd belang is dat opdrachtgever de rapportage als vertrouwelijk moet classificeren, dan zal Logius de ontvangen vertrouwelijke rapportage een vergelijkbare rubricering meegeven ingevolge het Besluit Voorschrift informatiebeveiliging rijksdienst bijzondere informatie.
Het is bij een eventueel Wob-verzoek echter aan de rechter om te bepalen of de aangebrachte vorm van classificering (en de daarmee door Logius vergelijkbare vorm van rubricering) in rechte stand kan worden gehouden. Logius heeft daar geen enkel invloed op.

9 Dossiervorming

De dossiervorming van de uitgevoerde werkzaamheden dient plaats te vinden in overeenstemming met de aanwijzingen zoals deze zijn opgenomen Richtlijn ‘Documentatie’.