NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Handreiking ICT-beveiligingsassessments DigiD door RE's

Inhoud

1. Inleiding
2. Formele aspecten van de opdracht
3. Scope en beoordeling van de maatregelen

   Bijlage 1: Tabel/toelichting bij beveiligingsrichtlijnen met aandachtspunten (versie 2015)

   Bijlage 2: Procesmatige kwaliteitsaspecten bij de DigiD pentest (2015)

   Bijlage 3: Modelrapport (Rapportage-Template, versie 2015)

1. Inleiding

Organisaties die gebruik maken van DigiD, moeten jaarlijks hun ICT-beveiliging toetsen op basis van een ICT-beveiligingsassessment onder verantwoordelijkheid van een Register EDP-Auditor (RE), ingeschreven in het register van de NOREA.

De Minister van BZK 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. In een brief van de Minister van 9 juli 2014 is vastgesteld dat de aangesloten organisaties het eerstvolgende assessmentrapport moeten inleveren bij Logius vóór 1 mei 2015. Voor nieuwe aansluitingen moet er na 2 maanden na ingebruikname een assessment worden ingeleverd.

Bij de uitvoering van ICT-beveiligingsassessments moet de "Norm ICT-beveiligingsassessments DigiD", gedateerd 21 februari 2012 worden gehanteerd. 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. De norm is vastgesteld door het ministerie van BZK in overleg met Logius, de auditdienst rijk en het NCSC.

In overleg met Logius is door NOREA een rapportageformat opgesteld dat gebruikt moet worden door de RE's, die deze opdrachten uitvoeren en daarover rapporteren aan het management van de DigiD-gebruikende organisaties en aan Logius.

In deze handreiking zijn ten behoeve van de RE's enkele aanbevelingen en suggesties voor de uitvoering van deze opdrachten opgenomen, die ook zijn bedoeld om bij te dragen aan een éénduidige en consistente interpretatie van de norm.

2. Formele aspecten van de opdracht

De opdrachten inzake de DigiD-beveiligingsassessments worden door RE's uitgevoerd in het kader van het Raamwerk voor Assurance-opdrachten en (dus) overeenkomstig Richtlijn 3000 'Assurance-opdrachten' en/of Richtlijn 3402 'Assurance-rapporten betreffende interne beheersingsmaatregelen bij een serviceorganisatie'. Voor beide varianten is het Modelrapport bruikbaar. Daarnaast gelden tevens de Richtlijnen voor opdrachtaanvaarding en rapportage, zoals die van toepassing zijn voor alle professionele diensten die door RE's worden uitgevoerd.

De werkzaamheden in het kader van deze opdrachten richten zich op het geven van oordelen per beveiligingsrichtlijn van de 'Norm ICT-beveiligingsassessments DigiD' van Logius, over de opzet en het bestaan van de maatregelen gericht op de ICT beveiliging van de webomgeving van DigiD aansluiting. Het feit dat de 'Norm ICT-beveiligingsassessments DigiD' is een selectie is van beveiligingsrichtlijnen uit de "ICT-beveiligingsrichtlijnen voor webapplicaties" van Nationaal Cyber Security Centrum (NCSC) impliceert derhalve dat de auditor niet in staat is om een overall oordeel te verschaffen omtrent de beveiliging van de betreffende DigiD-aansluiting. Dit is expliciet in de tekst van het Modelrapport opgenomen.

Het rapport wordt uitsluitend verstrekt ten behoeve van de betreffende organisatie en Logius aangezien anderen, die niet op de hoogte zijn van de precieze scope, aard en doel van de werkzaamheden, de resultaten onjuist kunnen interpreteren.

3. Scope en beoordeling van de maatregelen

DigiD ICT-beveiligingsassessment wordt uitgevoerd op de webomgeving van DigiD-aansluiting van de gebruikmakende organisatie conform de meest recente versie (2.1) van de "Handleiding uitvoering ICT-beveiligingsassessment" van Logius (te vinden op de Logius-website). De opdracht omvat het onderzoeken van de opzet en het bestaan van maatregelen en procedures gericht op de ICT beveiliging van de webomgeving van betreffende DigiD aansluiting. De opdracht omvat geen werkzaamheden met betrekking tot de werking van interne beheersmaatregelen van DigiD-aansluiting.

Een aandachtspunt vormt de verantwoordelijkheid van de auditor van de organisatie ten aanzien van de TPM van een leverancier die door een andere auditor is opgesteld. In het algemeen geldt dat er twee opties zijn:
a. De inclusive-methode methode waarbij de IT-auditor van de organisatie verantwoordelijkheid neemt voor het werk van de andere IT-auditor i.c. de IT-auditor van de leverancier. In deze situatie moet de IT-auditor van de organisatie de werkzaamheden van de IT-auditor van de leverancier reviewen.
b. De carve out-methode waarbij de IT-auditor van de organisatie geen conclusies overneemt uit het rapport van de IT-auditor van de leverancier. De IT-auditor van de

gemeente verwijst slechts naar het rapport van de IT-auditor van de leverancier. De IT-auditor van de organisatie moet wel vaststellen dat zijn eigen werkzaamheden plus de werkzaamheden van de IT-auditor van de leverancier de juiste en volledige scope afdekken. Daar is geen review van de werkzaamheden van de IT-auditor van de leverancier voor nodig.

Omdat bij de DigiD-assessments sprake is van de carve-out methode geldt optie b en is er geen review nodig. Er zal verder wel moeten worden vastgesteld dat het rapport is getekend door een RE en conform de NOREA template is opgesteld.

Bijlage 1: Tabel/toelichting bij beveiligingsrichtlijnen met aandachtspunten (versie 2015)

Het doel van deze tabel is de IT-auditor een handreiking te verstrekken ten aanzien van het toepassingsgebied, de scope en testaanpak, alsmede een nadere toelichting voor het uitvoeren van een DigiD ICT-beveiligingsassessment op basis van de Logius-norm. Het is de verantwoordelijkheid van de individuele auditor voldoende werkzaamheden te verrichten om per norm een oordeel te verstrekken met een redelijke mate van zekerheid.

Bijlage 2: Procesmatige kwaliteitsaspecten bij de DigiD pentest (versie 2015)

Als aanvulling op de richtlijnen inzake de pentesten (B-08/B3-15) zijn procesmatige kwaliteitsaspecten benoemd die voor auditors houvast kunnen bieden bij hun oordeelsvorming

Bijlage 3: Modelrapport (versie 2015)

Ten behoeve van de rapportage door de onafhankelijke IT-auditor, is een template als Word bestand beschikbaar. Optioneel zijn daarin paragrafen opgenomen die het rapport eveneens bruikbaar maakt in het geval gebruik wordt gemaakt van (een) service-organisatie(s). Ten behoeve van de beoordeling wordt per beveiligingsrichtlijn vermeld of wel of niet is voldaan. In Bijlage A worden de testresultaten beschreven en in Bijlage B wordt een typering en omschrijving gegeven van het object van onderzoek. Deze bijlagen zijn met name bedoeld om de opdrachtgever (uitvoeriger) te informeren, terwijl het eigenlijke rapport en bijlage C bedoeld zijn om Logius te informeren over de conclusies en de volledigheid van de scope, wanneer daartoe ook bevindingen en/of conclusies uit TPM-rapporten van leveranciers zijn gebruikt.