ENSIA guidance DigiD–assessments

Joep Janssen
Werkgroep DigiD assessments

31 oktober 2017

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Agenda

- Het nieuwe DigiD normenkader 2.0
- De eerste inzichten
- ENSIA en DigiD

DigiD assurance

Richtlijn 3000	DigiD assessment
Opdrachtaanvaarding	Verantwoordelijke partij
Opdracht	Doel Verantwoordelijkheid opdrachtgever Verantwoordelijkheid auditor (RE)
Normenkader	20 NCSC ICT-Beveiligingsrichtlijnen voor Webapplicaties
Scope	Webapplicatie met DigiD en beheer. Niet achterliggende (zaak-)systeem
Diepgang	Opzet en bestaan, geen werking.
Aspecten	Integriteit, niet vertrouwelijkheid en beschikbaarheid. Geen efficiency.
Zekerheid derden (ICT leverancier)	Carve-out → Third Party Memorandum (TPM) Inclusive → Eigen onderzoek auditor
Beperkingen	Selectie van NCSC normen. Geen overall oordeel over de beveiliging van de DigiD-aansluiting, oordeel per norm.
Oordeelsvorming	Beheersingsmaatregelen zijn volgens de criteria in alle materiële opzichten effectief.
Criteria	- beheersingsmaatregelen zijn geïmplementeerd; - de risico's die de betrouwbaarheid van DigiD aantasten, werden onderkend; - interne beheersingsmaatregelen geven een redelijke mate van zekerheid dat die risico's het voldoen aan beveiligingsrichtlijnen niet verhinderen.
Rapportage	Beperking doelgroep

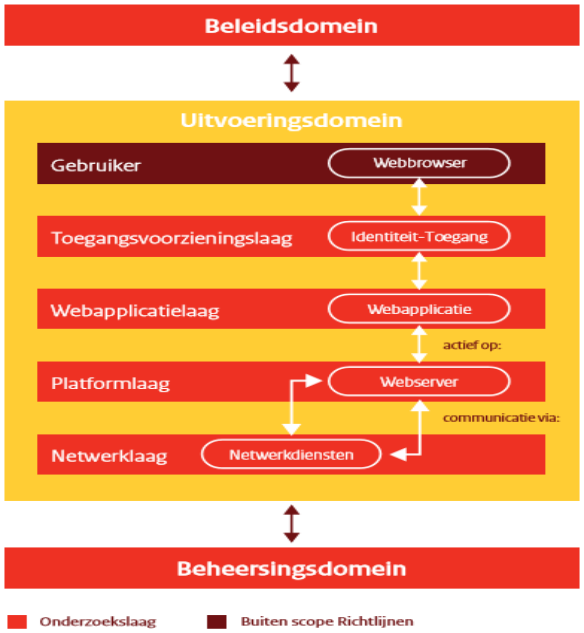
Overwegingen bij de nieuwe DigiD normen 2.0

- Aansluiten op de nieuwe beveiligingsrichtlijnen voor webapplicaties van het NCSC 2015
- Een geheel nieuwe indeling en nummering van nieuwe NCSC beveiligings-richtlijnen
- Focus op technische normen om zo de overlap met de ISO27001/2 en afgeleiden als BIG te verkleinen → DigiD normen staan naast de BIG normen
- Auditlast van de DigiD assessment verminderen.
- De focus op thema's als:
  - Normen met betrekking tot logging en monitoring (C)
  - Veilig programmeren normen (WA)
  - Normen met betrekking tot incident detectie (IDS) en opvolging (WA en C)

NOREA: Handreiking DigiD-assessments 2.0. 19 december 2017

De nieuwe DigiD normen 2.0

- De nieuwe normen zijn een selectie van de nieuwe ICT-beveiligings-richtlijnen van het NCSC.
- In totaal zijn voor DigiD 2.0 een 20-tal normen bepaald.



Domein	Aantal normen
Beleid (B)	1
Toegangsvoorziening (TV)	1
Webapplicaties (WA)	4
Platformen en webservices (PW)	4
Netwerken (NW)	4
Beheersing (control/monitoring) (C)	6

Nieuwe DigiD normen 2.0

Nummer	NCSC richtlijn
B.05 Houder	In een contract met een derde partij voor de uitbestede levering of beheer van een webapplicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld.
U/TV.01 Houder	De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.
U/WA.02 Houder	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.
U/WA.05 Houder	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.
U/PW.03	De webserver is ingericht volgens een configuratie-baseline.
U/PW.05	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen.
U/PW.07	Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar.

Nummer	NCSC richtlijn
U/NW.03	Het netwerk is gescheiden in fysieke en logische domeinen (zones), in het bijzonder is er een DMZ die tussen het interne netwerk en het internet gepositioneerd is.
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.
U/NW.06	Voor het configureren van netwerken is een hardeningsrichtlijn beschikbaar.
C.03	Vulnerability assesments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.
C.07	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.
C.08 Houder	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.

Penetratietesten

DigiD 2.0 bevat norm C.04: Penetratietesten:

- Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).

Als onderdeel van de assessment dient de auditor wel vast te stellen dat deze:

- periodiek (jaarlijks) worden uitgevoerd
- de juiste scope hebben gehad
- voldoende kwaliteit hebben → Procesmatige kwaliteitseisen bij DigiD penetratiestesten
- de organisatie evalueert de bevindingen op basis van eigen risicoanalyse en stelt een actieplan met prioriteitenstelling op.

Eerste inzichten

Algemeen

- Wel beperkt verbetermogelijkheden, geen wijzigingen voor 2017
- Nadere toelichting en tekstuele punten → eind november
- Begin 2018 verbeterpunten → Logius, NCSC, NOREA
- Geen verwijzing meer naar oude normen
- Toevoegen welke partij is verantwoordelijk voor welke normen

Specifiek

- Naast opzet en het bestaan ook werking beoordelen → over 2019?
- Reacties auditors betrekken bij verbeteringen → zenden aan NOREA t.a.v. DigiD assessments
- Security incident afhandeling door houder explicieter
- DNSSEC verantwoordelijkheid van registrant (leverancier of houder)
- BZK wil groepsaansluitingen beëindigen → alternatieve assessmentbenadering

Logius : DigiD assessment is voor alle aansluithouders gelijk

Geen verschil in beoordeling tussen gemeenten (388) en overige aansluithouders (plm. 400)

- 20 NCSC normen
- Oordeel per norm voldoet/voldoet niet
- TPM van serviceprovider
- Bij niet voldoen aan norm vraagt Logius verbeterplan
- Nieuwe aansluiting binnen 2 maanden assessmentrapport van RE
- Digitaal inleveren van rapportage (nieuw)
  - Gemeenten → ENSIA tool en beveiligde email
  - Overige aansluithouders→ digitaal portaal / beveiligde email

Gevolgen van ENSIA voor DigiD assessment

- Geen DigiD–assurancerapport van de onafhankelijke auditor
- Zelfevaluatie door gemeente is de basis voor de Collegeverklaring
- Van direct reporting naar assertion based (300D→3000A)
- Assurance rapport van auditor bij Collegeverklaring met aanvullende zekerheid
- Verantwoording College aan raad (horizontaal) en aan Logius (verticaal)
- Voor 31december zelfevaluatie; tussen 31december en 1 mei Collegeverklaring en assurance rapport
- TPM van leverancier eerder; 15 oktober
- Zelfevaluatie in ENSIA tool
- ENSIA tool levert bijlagen B en C per DigiD aansluiting
- KING Handreiking DigiD zelfevaluatie

Rapportage aan Logius

- ‘Bijlage B’: Object van onderzoek.
  - Algemene informatie over scope en functionaliteit van webomgeving. Geen technische details (e.g. IP nummers, netwerknummers). Naam en aansluitnummer van de DigiD aansluiting. Eigen beheer of uitbesteding: namen van Applicatie/Infra/SaaS leveranciers.
- ‘Bijlage C’:
  - Gegenereerd door ENSIA tool conform bijlage C standaard DigiD assurancerapport
  - Getoetste normen bij de gemeente (minimaal B.05, U/TV.01, U/WA.02, U/WA.05, C.08)
  - Normen getoetst door auditor van de leverancier
  - Getoetste aanvullende maatregelen gemeenten (‘user control considerations’)

Nr	Beschrijving van de norm	Getoetst bij leverancier	Referentie / rapportnummer	Aanvullende beheersmaatregelen gebruikersorganisatie	Getoetst bij gebruikers-organisatie	Referentie / rapportnummer

- Collegeverklaring ENSIA
- Assurancerapport ENSIA

Bedankt

Voor meer informatie kun je contact opnemen met:

Joep GM Janssen
06 51426705
joep.janssen@vka.nl

31 oktober 2017

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS