



notitie

Reactie van Forum Standaardisatie inzake de Baseline Informatiebeveiliging Overheid

Forum Standaardisatie
Wilhelmina v Pruisenweg 52
2595AN Den Haag
www.forumstandaardisatie.nl

Contactpersoon
Nico Westpalm van Hoorn
Voorzitter
Forum Standaardisatie
T 070-8887776

Datum
6 augustus 2018

Geachte heer Wesseling,

Met dit schrijven reageer ik namens het Forum Standaardisatie op de door uw werkgroep opgestelde Baseline Informatiebeveiliging Overheid (BIO).

Het Forum Standaardisatie onderschrijft al langer het belang van heldere kaders en richtlijnen voor informatiebeveiliging. Al in 2008 plaatste het Forum de ISO 27001 en ISO27002 standaarden op de 'pas toe of leg uit'-lijst.

Mede hierdoor en door het feit dat deze standaarden de basis vormden van de verschillende overheidsbaselines, is de toepassing hiervan bij overheidsorganisaties de afgelopen jaren fors toegenomen¹.

Daarnaast adviseerde het Forum in 2016, om te werken aan een geharmoniseerd normenkader voor informatiebeveiliging dat overheidsbreed verplicht is en voldoende diepgang kent. Feitelijk één overheidsbreed basisniveau voor informatiebeveiliging in de vorm van een Baseline Informatiebeveiliging Overheid².

Forum Standaardisatie vindt het dan ook een positieve ontwikkeling dat met de BIO de verschillende baselines voor informatiebeveiliging zijn gestandaardiseerd tot één baseline voor de gehele overheid. Dit zorgt voor meer duidelijkheid en een betere toepassing. Bovendien zal naar onze verwachting het gebruik van één baseline bijdragen aan betere uitvoerbare verantwoording en audits. Kortom, de BIO draagt bij aan een betere informatiebeveiliging van de overheid als geheel.

Naast het resultaat vindt het Forum het positief dat bij de totstandkoming van deze BIO de gehele overheid actief betrokken is. Nu de BIO (bijna) is opgeleverd zou het Forum graag zien dat deze aanpak, gestoeld op brede betrokkenheid en draagvlak, wordt bestendigd in de beheerfase van de baseline.

¹<https://www.forumstandaardisatie.nl/file/monitor-open-standaarden-2017>

²https://www.forumstandaardisatie.nl/sites/bfs/files/proceedings/FS%20161019.4A%20Onderzoek%20Samenhang%20in%20ICT-beveiligingsstandaarden_0.pdf

Datum
6 augustus 2018

Met alleen het publiceren van de baseline is de adoptie ervan nog niet geborgd. Op adoptie dient actief te worden ingezet en de voortgang dient te worden gemonitord. Het Beheer- en OntwikkelModel voor Open Standaarden (BOMOS)³ biedt hiervoor een aantal maatregelen zoals: governance, opleiding, helpdesk, validatie & certificatie, community, benchmarking, documentatie, promotie en publicatie.

Aanvullend is het Forum van mening dat met de BIO een goede invulling wordt gegeven aan een geharmonieerd normenkader op tactisch niveau. De diepgang en waarde hiervan dienen verder te worden verhoogd door (op uitvoerend niveau) richtlijnen per inhoudelijke taakgebied (bijv. voor website, e-mail, netwerken etc.) vast te stellen en daarin ook technische standaarden te positioneren.

De governance (zoals vaststellingsprocedure) voor de BIO en de status van de BIO, inclusief de onderliggende operationele richtlijnen, dienen, wat Forum Standaardisatie betreft, op wettelijk niveau verankerd te zijn.

In dat licht zou het goed zijn als u meer duidelijkheid kunt geven over de wijze waarop de komende jaren invulling zal worden gegeven aan het beheer van de baseline en aanpalende stimuleringsmaatregelen.

Tot slot zou het Forum Standaardisatie ook graag een statusupdate ontvangen over de verwerking van de adviezen die u tijdens de consultatieperiode van Bureau FS ontving.

Hopende u hiermee een bruikbare reactie te hebben gegeven, zien wij uit naar uw reactie. Bij voorbaat dank.

Namens het Forum Standaardisatie,

Met vriendelijke groet,

Nico Westpalm van Hoorn
Voorzitter Forum Standaardisatie

³ Beheer- en OntwikkelModel voor Open Standaarden (BOMOS):

<https://www.forumstandaardisatie.nl/thema/ontwikkelen-en-beheren-van-open-standaarden>