FS-20140617.03B1

Forum Standaardisatie

Wilhelmina v Pruisenweg 52
2595 AN Den Haag
Postbus 96810
2509 EJ Den Haag
www.forumstandaardisatie.nl

notitie

FORUM STANDAARDISATIE

Bijlagen:	geen		
Aan:	Forum Standaardisatie		
Van:	Stuurgroep open standaarden		
Datum:	5 juni 2014	**Versie**	1.0
Betreft:	Samenhang beveiligingsstandaarden en opname TLS op de 'pas toe of leg uit'-lijst		

Gevraagd besluit

Forum Standaardisatie wordt gevraagd in te stemmen met:

a. De constatering dat de organisatorische beveiligingsstandaarden (ISO27001 en 27002) en de technische beveiligingsstandaarden (DNSSEC, DKIM, SAML en Digikoppeling) op de 'pas toe of leg uit'-lijst complementair zijn en elkaar versterken;
b. Op basis van de in deze notitie geschetste samenhang van standaarden in te stemmen met het Forum-advies voor opname van TLS versie 1.2 op de 'pas toe of leg uit'-lijst. Daarbij wordt geadviseerd om ook eerdere versies van TLS (versie 1.1 en 1.0) ten behoeve van de interoperabiliteit toe te passen;
c. Het uitgangspunt dat als een overheidsorganisatie een sectorale Baseline Informatiebeveiliging eist, dat betekent dat deze handelt in lijn met de 'pas toe of leg uit'-status voor NEN-ISO27001/2, mits hier geen bezwaren tegen naar voren komen in lopend onderzoek;
d. Het uitvoeren van een nader onderzoek om de samenhang tussen beveiligingsstandaarden (op de lijst en daarbuiten) nog meer inzichtelijk te maken en 'witte vlekken' te identificeren (mede in het kader van 'sterker sturen op de lijst').

Toelichting

Inleiding
Forum en College Standaardisatie houden zich ten behoeve betrouwbare gegevensuitwisseling binnen de gehele (semi-)publieke sector ook bezig met

standaardisatie van informatiebeveiliging. Dit sluit ook aan op het instellingsbesluit waarin staat dat wordt gestreefd naar "veilige en betrouwbare uitwisseling en (her)gebruik van gegevens tussen overheidsorganisaties en bedrijven". Zo is een aantal informatiebeveiligingsstandaarden opgenomen op de 'pas toe of leg uit'-lijst. Daarnaast heeft het Forum onder andere een handreiking 'Handreiking Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten' ontwikkeld en is op verzoek van NCSC vanuit standaardisatieperspectief gereageerd op hun nieuwe concept-versie van de 'ICT-beveiligingsrichtlijnen voor webapplicaties'.

Tijdens de Forumvergadering van 15 april 2014 is gesproken over het opnemen van TLS op de 'pas toe of leg uit'-lijst. Tijdens het overleg kwam naar voren dat er inhoudelijk geen bezwaar is om de standaard op de lijst te plaatsen. Daarnaast werd herbevestigd dat het Forum en College een rol hebben met betrekking tot beveiligingsstandaarden, zoals ook terugkomt in het Instellingsbesluit.

Wel bracht BZK/DGOBR de volgende vragen naar voren.

1. Hoe hangt TLS samen met de andere beveiligingsstandaarden op de 'pas toe of leg uit'-lijst?
2. Hoe verhoudt de sturing op de adoptie van de Baselines Informatiebeveiliging zich tot de sturing op adoptie van standaarden met een 'pas toe of leg uit'-status, zoals TLS?

Het Forum besloot eerst in te gaan op bovenstaande vragen, voordat TLS op de 'pas toe of leg uit'- lijst wordt opgenomen. Deze notitie geeft hieraan invulling.

Samenhang tussen beveiligingsstandaarden op de 'pas toe of leg uit'-lijst

Standaarden zijn cruciaal voor informatiebeveiliging. Er is alleen niet één bepaalde IB-standaard die alle beveiligingsrisico's afdekt. Het gaat om een samenspel van meerdere standaarden. Op dit moment staat een vijftal standaarden die betrekking hebben op informatiebeveiliging op de 'pas toe of leg uit'-lijst, namelijk:

1. NEN-ISO27001/27002: beschrijft hoe informatiebeveiliging procesmatig in te richten. De baselines informatiebeveiliging (BIR/BIG/BIWA/IBI) zijn op deze standaarden gebaseerd;
2. DNSSEC: zorgt dat domeinnamen betrouwbaar worden vertaald naar ip-adressen;
3. DKIM: voorkomt misbruik van het afzendadres/domein en beschermt daarmee tegen phishing-mails;
4. SAML: beschrijft identiteitsattributen, uitwisselprotocollen en transport t.b.v. authenticatie;
5. Digikoppeling: zorgt voor beveiligd berichtenverkeer.

Aanvullend hierop staan er ook verschillende standaarden voor informatiebeveiliging op de gangbare lijst (AES, IPSec, SHA2, HTTPS, SSH2, X509).

TLS

De kandidaat 'pas toe of leg uit'-standaard TLS is complementair aan bovengenoemde standaarden. TLS zorgt voor versleuteling van het gegevenstransport met behulp van certificaten. De standaard doet zijn werk bijvoorbeeld als een gebruiker "https://" in zijn browser ziet. Alle moderne browsers ondersteunen de standaard. TLS speelt eveneens een rol bij het

uitwisselen van SAML-berichten en ook Digikoppeling bouwt voort op TLS. De voorganger van TLS is SSL dat door experts niet meer als veilig wordt beschouwd. Voor ieder van de genoemde standaarden geldt dat qua adoptie nog terrein te winnen valt. Tegelijkertijd is duidelijk dat de adoptie binnen het Rijk maar ook binnen andere overheidssectoren de afgelopen jaren duidelijk is toegenomen en nog steeds toeneemt.

NEN-ISO
Het karakter van NEN-ISO 27001/2 is organisatorische/procesmatig van aard, en bevat geboden als:

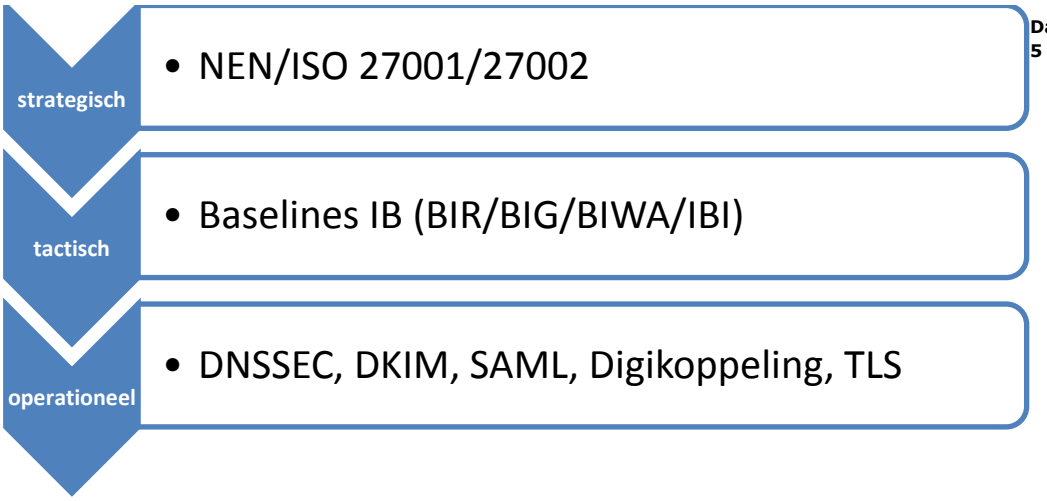
- Zorg voor authenticatie en autorisatie van medewerkers;
- Bescherming van gegevens en privacy dienen overeenkomstig te zijn met wet en regelgeving;
- Registraties behoren te worden beschermd tegen verlies, vernietiging en vervalsing;
- Een beheerkader moet worden vastgesteld om de implementatie van informatiebeveiliging in de organisatie te initiëren en te beheersen.

De andere standaarden van de 'pas toe of leg uit'-lijst zijn meer technisch ofwel operationeel van aard. Ze zorgen met name voor vertrouwelijkheid en integriteit van uitgewisselde informatie en waarborgen daarbij de interoperabiliteit en leveranciersonafhankelijkheid.

De NEN-ISO normen (en de daarop gebaseerde Baselines Informatiebeveiliging) geven niet aan welke concrete maatregelen een organisatie moet treffen. De technische standaarden hebben wél het karakter van concrete maatregel. SAML helpt bijvoorbeeld bij de veilige authenticatie en autorisatie van gebruikers. De technische standaarden geven daarmee invulling aan bepaalde aspecten, waarvan de NEN-ISO-standaarden voorschrijven dat deze moeten worden geadresseerd.

Beide typen standaarden- organisatorisch/ procesmatig enerzijds en technisch/ operationeel anderzijds- vullen elkaar dus aan en versterken elkaar. Een aanvaardbaar niveau van beveiliging kan pas worden bereikt als er overheidsbreed zowel organisatorische als technische als informatiebeveiligingsstandaarden worden gebruikt. Vandaar dat het Forum en College er voor hebben gekozen om zowel de procedurele NEN-ISO-standaarden als een (beperkt) aantal technische beveiligingsstandaarden voor te schrijven.

Relatie met de Baselines Informatiebeveiliging
De sectorale Baselines Informatiebeveiliging, die op de NEN-ISO-standaarden zijn gebaseerd, zijn eveneens organisatorische/procesmatig van aard. Deze geven voor overheden tactische invulling aan de meer abstracte, strategische normen, maar schrijven nog geen technische/operationele standaarden voor.



Het is van meerwaarde als de stimulering van de adoptie van beveiligingsstandaarden in lijn is met de beleidsimpulsen rondom BIR, BIG, IBI en BIWA. Een goede stap hierin is om duidelijk te maken dat met de adoptie van de Baselines, overheidsorganisaties óók voldoen aan de 'pas toe of leg uit' verplichting van ISO 27001/2.

Op dit moment wordt getoetst wat de impact is van de nieuwe 2013-versie van NEN-ISO 27001/2 voor de overheid. Daarbij wordt ook getoetst of de baselines voldoen aan ISO27001/2 en of dit zonder meer gelijkgeschakeld kan worden op de 'pas toe of leg uit'-lijst. In de jaarlijkse monitor open standaardbeleid zal de beschikbare adoptie-informatie m.b.t. baselines ook al mee worden genomen in de rapportage.

Nader onderzoek naar samenhang
Bij de opname van nieuwe standaarden op de 'pas toe of leg uit'-lijst wordt altijd gekeken naar de relatie tot bestaande standaarden op de lijst. Dit kan echter onvoldoende zijn omdat hierdoor geen zicht is op welke standaarden mogelijk nog meer relevant zijn, de zogenoemde 'witte vlekken'. Bovendien is de samenhang nog niet altijd duidelijk voor een gebruiker van de 'pas toe of leg uit'-lijst. Dit is ook naar voren gekomen in het Forum. In het najaar start het Forum daarom met een onderzoek om de samenhang tussen beveiligingsstandaarden beter inzichtelijk te maken en 'witte vlekken' te identificeren .