DNSSEC en DKIM bij de overheid

College en Forum Standaardisatie werken aan het op een hoger plan brengen van standaardisatie en interoperabiliteit binnen de Nederlandse overheid. Kortgeleden erkende het College de door het Forum voorgestelde standaarden DNSSEC en DKIM, die daarmee op de 'pas toe of leg uit'-lijst van standaarden zijn gekomen. Waarom juist deze standaarden en hoe verloopt de selectieprocedure? Bart Knubben, adviseur bij Bureau Forum Standaardisatie en Nico Westpalm van Hoorn, voorzitter van Forum Standaardisatie, geven tekst en uitleg.

College en Forum Standaardisatie zijn in 2006 door het kabinet ingesteld. Zij bevorderen interoperabiliteit van de Nederlandse overheid. Open standaarden zijn hierbij van essentieel belang. ''Standaardisatie van gegevensuitwisseling biedt veel economische voordelen. Het werkt echter pas als organisaties hun koppelvlakken op eenzelfde manier inrichten en dat gaat helaas niet vanzelf. College en Forum faciliteren dit proces binnen de overheid. '', aldus Nico Westpalm van Hoorn, voorzitter van het Forum Standaardisatie en tot voorkort CIO bij Havenbedrijf Rotterdam.

PAS TOE OF LEG UIT

Forum Standaardisatie is een adviesorgaan van ongeveer 15 deskundigen op bestuurlijk niveau uit overheid, bedrijfsleven en wetenschap. Het Forum rapporteert aan het College Standaardisatie, dat bestaat uit diverse hoge ambtelijke vertegenwoordigers van ministeries, provincies, gemeentes en waterschappen. Het College beoordeelt de adviezen van het Forum. Wordt een advies akkoord bevonden, dan komt de standaard op de zogenaamde 'pas toe of leg uit' -lijst te staan. Het College heeft als hoofdtaak het beheren en doen toepassen van de op de lijst geplaatste standaarden.

Het kabinet stelt open standaarden als norm. Voor de (semi-)publieke sector geldt sinds 2009 het 'pas toe of leg uit'-regime. Overheden zijn verplicht om bij de aanschaf van ICT-systemen te kiezen voor de relevante standaarden van de 'pas toe of leg uit'-lijst. Het 'pas toe of leg uit'-regime is voor de Rijksoverheid vastgelegd in een Rijksinstructie en in de Rijksbegrotingsvoorschriften. Voor gemeenten, provincies en waterschappen is de verplichting vastgelegd in bestuursakkoorden en in de begrotingsvoorschriften voor gemeentes en provincies.
''Overheidsinstellingen verplichten zich de standaarden op de lijst te gebruiken. De uitleg waarom een standaard nog niet wordt toegepast moet in het jaarverslag worden opgenomen, daar wordt op gelet. Niet toepassen is geen optie, maar er is geen bovenbaas die harde straffen uitdeelt, het is een zelfopgelegd commitment.'' Westpalm van Hoorn typeert de relatie tussen Forum en College als 'deskundigen zonder macht die rapporteren aan de macht zonder deskundigheid'. Een goedwerkend concept, vindt hij.

STANDAARDEN AANMELDEN

Het speelveld van standaarden is breed. De scope van het Forum beperkt zich tot standaarden die tussen organisaties gebruikt kunnen worden. ''Je ziet daarin verschillende lagen,'' zegt Bart Knubben, adviseur bij het ondersteunende bureau van het Forum Standaardisatie. ''Er zijn standaarden op het gebied van organisatorische afstemming en samenwerking, er zijn standaarden die zich richten op semantiek, en er zijn technische standaarden. De onlangs op de lijst geplaatste standaarden DNSSEC en DKIM zitten typisch in de laatste categorie. Daarbij zijn het ook nog technische standaards van het type beveiliging. Interoperabiliteit is niet alleen het kunnen uitwisselen van gegevens op zich. Het betekent ook dat je de kwaliteit borgt, dat je het betekenisvol doet, dat je het veilig doet.''
De focus van College en Forum Standaardisatie ligt op open standaarden. 'Open'

heeft betrekking op het standaardisatieproces en is één van de toetsingscriteria voor opname op de lijsten. Het gaat daarbij om laagdrempelige beschikbaarheid van documentatie, een liberale licentie inzake intellectuele eigendomsrechten (bijv. octrooien), inspraakmogelijkheden, en onafhankelijkheid en duurzaamheid van de standaardisatie-organisatie. ''Open standaarden sluiten niemand uit en zijn dus van en voor iedereen. Het is als het ware infrastructuur. Iedere marktpartij kan een open standaard inbouwen in haar software. Het gaat erom dat marktpartijen concurreren óp de standaard en niet óm de standaard'', zo licht Westpalm van Hoorn toe.

Het Forum opereert vooral vraaggestuurd. Het is geen orgaan dat zelf standaarden ontwikkelt. De aanmeldingen voor standaarden komen vanuit de markt; het is aan het Forum om te beoordelen of de aanmelding ontvankelijk is en toegevoegde waarde heeft.
Knubben: ''Na de aanmelding doorloopt een aspirant-standaard een proces. We zoeken afstemming met het netwerk van deskundigen door het erbij te betrekken en te bevragen: is het verstandig om als overheid op deze standaard in te zetten? Onze experts komen samen en geven een oordeel over de aspirant-standaard. De basis voor het oordeel vormen de toetsingscriteria: openheid, toegevoegde waarde, draagvlak en nut van opname. Sommige experts zouden persoonlijk belang kunnen hebben bij de invoer van een bepaalde standaard. We zijn daar zeer alert op en zorgen voor een evenwichtige samenstelling van de expertgroep.'' Het rapport van deze groep wordt publiekelijk gemaakt op internet, waar iedereen een maand lang commentaar kan leveren, en vragen stellen. Op basis daarvan brengt het Forum advies uit aan het College dat uiteindelijk besluit.
''Wordt een standaard niet geaccepteerd, dan ligt de oorzaak regelmatig in het feit dat het beheer rond de standaard niet goed geregeld is,'' zegt Westpalm van Hoorn. ''We onderzoeken altijd of er een organisatie is die het beheer voor zijn rekening neemt. We willen de zekerheid hebben dat de overheid duurzame keuzes maakt. Het is belangrijk dat bij een volgende versie van de standaard de gebruikersinbreng en de openheid geregeld zijn.''
Het hele proces van indiening tot op de lijst zetten neemt iets meer dan een half jaar in beslag. Het College vergadert dan ook twee keer per jaar, in mei en november.

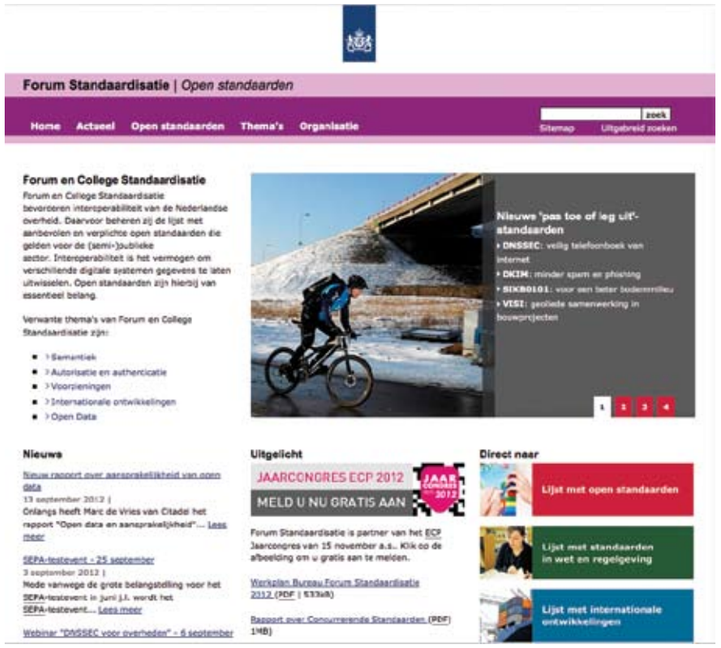
INCIDENTEN

Security is zeker voor de overheid van groot belang. Incidenten worden direct breed uitgemeten in de media. ''De overheid is erg gevoelig voor negatieve publiciteit rond security. Voor veel overheden is het echter relatief nieuwe materie. Banken zijn al langer doelwit en lijken meer bedreven in het bestrijden van cybercriminaliteit,'' meent Westpalm van Hoorn. ''Het is in die sector een gegeven, dat er duizenden criminelen zijn die zich de hele dag bezighouden met het kraken van banksystemen. Het is een permanent gevecht tussen de experts bij de banken en hackers die proberen binnen te komen om geld te bemachtigen. Bij de banken leeft men daarmee. Bij de overheid is het besef ook sterk gegroeid. De overheid organiseert zich daarom steeds beter om incidenten te voorkomen. Het kiezen voor beveiligingsstandaarden zoals DNSSEC en DKIM hoort daarbij.''
Knubben voegt daar aan toe: ''Bij banken valt natuurlijk vooral geld te halen. Bij een overheid is dat in bepaalde gevallen ook zo, maar bij een overheid kan het ook om persoonlijke, politiek relevante of beursgevoelige informatie gaan. Het afgelopen jaar zou de e-mail van Van Rompuy zijn gehackt door lieden die direct toegang tot zijn mailbox kregen. Op dat moment werden er nogal wat beslissingen genomen over de Euro-zone. Als je van tevoren weet wat die beslissingen behelzen, is dat voorkennis en dus beursgevoelige informatie. Het was even in het nieuws, maar kreeg eigenlijk veel te weinig aandacht.''

Nico Westpalm van Hoorn is sinds 2007 voorzitter van het Forum Standaardisatie. Daarvoor was hij jarenlang CIO bij het Havenbedrijf Rotterdam en hij noemt zichzelf IT-generalist. In de logistieke wereld speelt standaardisatie een grote rol, wat de opstap naar zijn functie bij het Forum vormde.

Website: www.forumstandaardisatie.nl
Twitter: twitter.com/openstandaarden

Meer informatie over de beveiligingsstandaarden
DNSSEC: www.forumstandaardisatie.nl/dnssec
DKIM: www.forumstandaardisatie.nl/dkim



DNSSEC

Kort geleden maakte het College Standaardisatie bekend dat de security-standaarden DNSSEC en DKIM op de 'past toe of leg uit'-lijst van de overheid zijn geplaatst.
DNSSEC werd vorig jaar bij het Forum Standaardisatie aangemeld door SIDN, de beheerder van het nl-domein. DNSSEC zet als het ware een digitale handtekening als authenticatie van het IP-adres dat is gekoppeld aan een URL.
''DNS is als het ware het telefoonboek van het internet. DNS koppelt namen aan nummers. Meer specifiek, domeinnamen aan IP-adressen. DNS is zo oud als internet zelf, ontworpen in een tijd dat internet-security nog lang niet aan de orde was. De mensen die het internet gebruikten, kenden elkaar bij wijze van spreken allemaal persoonlijk. Er werd niet gesjoemeld, er werd niet gehackt, gekraakt en gephisht,'' schetst Knubben de situatie van toen. ''Na de extreme groei die internet heeft doorgemaakt kun je constateren dat het basissysteem kwetsbaar is, gevoelig voor manipulatie. DNS is een zwakke plek geworden.''
Op het moment dat DNS-verkeer gemanipuleerd kan worden impliceert dat dat een eindgebruiker niet meer de garantie heeft dat hij in zijn browser informatie ziet die van het juiste IP-adres afkomstig is. ''Zelfs een SSL-certificaat van bijvoorbeeld PKIoverheid dekt dat niet af,'' aldus Knubben. ''Die biedt alleen garantie dat er een versleutelde verbinding met het gevraagde domein is gemaakt . Maar het dekt niet af of een gebruiker met het juiste achterliggende IP-adres verbonden is. DNSSEC checkt dat laatste stuk wél. DNSSEC werkt dus aanvullend aan SSL.''

SIDN

SIDN wendde zich voor hulp tot het Forum Standaardisatie om massa en push te krijgen voor DNSSEC, vooral ook binnen de overheid. ''SIDN heeft het moment van introductie van DNSSEC slim gekozen,'' vindt Knubben. ''Er is al een aantal landen dat ervaring heeft opgedaan met DNSSEC zoals Zweden, Tsjechië, Brazilië en de VS. SIDN heeft hiervan geleerd. Ze heeft er niet voor gekozen om frontrunner te zijn, maar koos een goeddoordachte aanpak. Dat hebben ze zo goed gedaan, dat het nu een behoorlijke vlucht neemt. In Nederland zijn ongeveer 5 miljoen domeinnamen geregistreerd. Sinds de introductie van de geautomatiseerde versie van DNSSEC in mei 2012 zijn er meer dan 1 miljoen domeinen gesigneerd. Dat is best een rappe introductie. Nederland zou nu al de grootste DNSSEC-gebruiker ter wereld zijn. Zo'n nieuwe standaard moet massa maken en dat is gebeurd.''
SIDN meldde DNSSEC in november 2011 aan, waarna de expertgroep ernaar keek. Punt van kritiek was dat SIDN de software voor DNSSEC-ondertekening handmatig had ingeregeld om er ervaring mee op te doen. De expertgroep stelde dat dat geautomatiseerd moest worden om grote hoeveelheden aan te kunnen. Dat besefte SIDN zich terdege en zorgde voor een geautomatiseerd proces, waarna DNSSEC in mei 2012 op de 'pas toe of leg uit' -lijst van de overheid werd geplaatst.
Knubben over wat overheden nu kunnen doen: ''Via de website van SIDN kan je eenvoudig controleren of je domeinnaam is ondertekend met DNSSEC. Als dat nog niet het geval is, dan kan je aan je domeinnaambeheerder vragen wanneer deze de standaard zal gaan ondersteunen. Als dit te lang duurt dan kan je eventueel overstappen naar een andere aanbieder.''
Voor Rijksoverheden is het eenvoudig om voor hun domeinnamen DNSSEC in te regelen. Zij zijn namelijk al verplicht om domeinnamen onder te brengen bij Dienst Publiek en Communicatie (DPC) van het ministerie van Algemene Zaken (AZ). DPC biedt ondersteuning voor DNSSEC.

DOMAINKEYS IDENTIFIED MAIL – DKIM

Ook e-mailverkeer is een van de oudste onderdelen van het internet en draagt eigenlijk geen enkele vorm van beveiliging in zich. ''Als ontvanger kun je niet vaststellen of de e-mail echt is verstuurd door de partij die hem verzonden lijkt te hebben. En daar wordt misbruik van gemaakt door spammers en phishers, die het afzendadres spoofen, en vervangen door een ander. Ook de (domein-)namen van overheden, zoals het KLPD, de Belastingdienst en DigiD, zijn als vermeende afzenders misbruikt,'' legt Knubben uit. ''DKIM lost dat probleem op door via de DNS te controleren of wellicht een andere domeinnaam is ingevuld. Foute mailtjes kunnen dus worden gefilterd, waardoor de hoeveelheid spam en de hoeveelheid phishing-gevaar afnemen. Steeds meer banken maar ook organisaties zoals Wehkamp en Markplaats gebruiken de standaard voor het verzenden van e-mail. Grote e-maildiensten zoals Gmail en Yahoo! ondersteunen de standaard zowel voor het verzenden als het ontvangen van e-mail. Daarnaast zijn er verschillende Nederlandse providers, zoals XS4ALL en Ziggo, die bij het ontvangen van e-mail DKIM-validatie toepassen.''
Knubben wijst erop dat er steeds meer e-mails verstuurd worden vanuit systemen zonder tussenkomst van mensen. ''Dat maakt het moeilijker de legitimiteit van de mail vast te stellen. De persoonlijke relatie ontbreekt dan namelijk. En het aantal systeemmailtjes neemt de komende jaren alleen maar toe.''

Bart Knubben is werkzaam als adviseur voor het Bureau Forum Standaardisatie, dat is ondergebracht bij Logius. Het Forum adviseert het College Standaardisatie. Zij bevorderen standaardisatie en interoperabiliteit binnen de Nederlandse overheid. Het Bureau Forum Standaardisatie ondersteunt beide instellingen bij hun werkzaamheden. Knubben houdt zich vooral bezig met adoptie van de open standaarden die op de 'pas toe of leg uit'-lijst staan - waaronder de DKIM en DNSSEC.