Aan	Nationaal Beraad via Regieraad Interconnectiviteit
Van	Forum Standaardisatie

Forum Standaardisatie
Bureau Forum Standaardisatie

Contactpersoon
Ludwig Oberendorff
[redacted]

Datum
29 april 2015

Kenmerk
2015-0000255139

notitie

Afspraken standaardisatie

Gevraagd besluit

Het Nationaal Beraad wordt gevraagd om akkoord te gaan met:

1. voorgestelde resultaatsafspraken over adoptie van informatieveiligheid-standaarden (tegen vervalsingen van overheidswebsites en -email); en
2. herbevestiging en verlenging van de bestaande overheidsbrede 'pas-toe-of-leg-uit' -afspraak tot eind 2017

Aanleiding algemeen

Er zijn verschillende aanleidingen voor het maken van aanvullende afspraken in het Nationaal Beraad over de adoptie van open standaarden:

- de resultaten van de monitor open standaarden 2014: voor het derde jaar op rij blijkt dat in 60% van de ICT-aanbestedingen van de overheid onterecht om geen enkele relevante open standaard van de 'pas-toe-of-leg-uit'-lijst wordt gevraagd;
- de bevindingen van de commissie Elias: "overheid zie daadwerkelijk toe op de toepassing van het 'pas-toe-of-leg-uit'-beleid rond open standaarden (aanbeveling 9)";
- signalen van leveranciers: "we bieden ICT aan mét open standaarden, maar de overheid vraagt er niet om";
- de onlangs Kamerbreed gesteunde motie Oosenbrug/Gesthuizen over Open Standaarden, die door de regering is overgenomen: "verzoekt de regering ervoor te zorgen dat voor eind 2015 bij alle aanbestedingen correct wordt omgegaan met de relevante open standaarden" (zie bijlage);
- meer in het bijzonder druk op het vertrouwen van burgers en bedrijven in de werking van de e-overheid door fraude en *phishing (zie bijlage voor voorbeelden).*

In het Digiprogramma staat ondermeer daarom:

- "worden (…) bindende adoptie afspraken met betrekking tot overheidsbrede standaarden gemaakt" (p.27); en
- "(…) De Regieraad Interconnectiviteit stimuleert beleidsontwikkeling voor toezicht op, en juiste implementatie van standaarden en (verplicht) gebruik van voorzieningen. In een later stadium ziet de Regieraad ook toe op de daadwerkelijke uitvoering van het ontwikkelde beleid." (p.28).

Ad. 1 Resultaatsafspraken informatieveiligheid-standaarden

Waarom?
Om de doelstellingen van Digitaal 2017 te verwezenlijken is het ondermeer noodzakelijk ervoor te zorgen dat burgers en bedrijven vertrouwen hebben en houden in de Digitale overheid.
Om dat te laten welslagen is nodig dat de informatieveiligheid op orde is. Burgers en bedrijven moeten er op kunnen rekenen dat een website of e-mail daadwerkelijk van de overheid is, voordat ze erop inloggen en betaal- en/of persoonsgegevens prijs geven. Het gebeurt nu nog te vaak dat mensen in *Phishing*-mails en nepsites trappen. Dat kan onder andere worden tegengegaan door het gebruik van standaarden[1] die de echtheid van overheidswebsites en overheidsmail zichtbaar maken.

Het is cruciaal dat deze standaarden door ***alle*** overheidsorganisaties worden toegepast. Want net als bij echtheidskenmerken van papiergeld (het watermerk) is het zinloos indien het echtheidskenmerk is opgenomen bij 60% van de echte bankbiljetten. Je hebt er pas echt wat aan, als je ervan uit kunt gaan dat in elk écht bankbiljet een watermerk zit. Dat geldt ook voor de echtheidskenmerken van websites. Banken begrijpen dat, en daarom hebben ook al hun websites dezelfde echtheidskenmerken (o.a. 'het slotje' zie www.veiligbankieren.nl). Dit beginsel van eenduidigheid geldt ook voor de overheid: ook een overheidswebsite moet je telkens op eenzelfde manier als echt kunnen herkennen.

Daarom is het voorstel om conform het Digiprogramma rondom de volgende set informatieveiligheid-standaarden onderstaande aanvullende resultaatafspraken te maken.

Welke resultaatsafspraken informatieveiligheid?
Voorgestelde resultaatsafspraken:

i. beveiligde overheids-websiteverbindingen (TLS, in de vorm van https):
resultaatsafspraak: TLS wordt toegepast bij alle overheidswebsites waarbij burgers en of bedrijven gegevens moet invoeren, of waarbij gegevens vooringevuld zijn;

ii. beveiliging overheids-domeinnamen (DNSSEC):
resultaatsafspraak: DNSSEC wordt gebruikt voor elke domeinnaam waarmee een overheidsorganisatie met burgers en/of bedrijven communiceert;

iii. beveiliging overheids-email (DMARC, SPF en DKIM: anti-phishing en anti-imitatie):
resultaatafspraak: deze 'e-mail' standaarden worden toegepast voor alle overheidsdomeinnamen of deze nu wel of niet gebruik maken van mail.

Er wordt een gefaseerde aanpak voorgesteld, waarbij de adoptie van deze standaarden stapsgewijs doorgroeit naar 100%:

Planning	K3 2015	K4 2015	K1 2016	K2 2016	K3 2016	K4 2016
GDI Voorzieningen						
Organisaties uit het Nationaal Beraad						
Overige overheidsorganisaties						

Hergebruik implementatie-kennis
Daarnaast zal ondersteuning van de implementatie plaatsvinden door kennis

[1] TLS, DNSSEC en DKIM/SPF/DMARC.

daarover herbruikbaar te maken. Zo zal de Belastingdienst haar ervaringen met de implementatie van DKIM met andere uitvoerders delen. Momenteel wordt gezocht naar de juiste vorm (bijvoorbeeld *best practices, workshops of handreiking*), zodat het kennisaanbod goed aansluit op de vraag. Voor een eerste beeld kunnen organisaties op www.internet.nl zelf al checken hoe de websites/e-mail van hun organisatie ervoor staan (op ondermeer bovenstaande standaarden).

Toelichting per standaard:

i. Beveiligde overheids-websiteverbindingen - *TLS*: TLS is een standaard voor beveiligde internetverbindingen. In de browser is de standaard zichtbaar als het slotje bij een webadres dat start met https. De standaard zorgt ervoor dat de verbinding niet kan worden afgeluisterd of informatie kan worden gemanipuleerd. Bovendien zorgt TLS ervoor dat een gebruiker de echtheid van een website kan verifiëren.

De resultaatafspraak is dat:

1. TLS in ieder geval moet worden toegepast voor die overheidswebsites waarbij burgers en of bedrijven gegevens moet invoeren (zoals in een contactformulier) of waarbij gegevens voor ingevuld zijn. Voor puur informatieve websites geldt deze resultaatafspraak niet, hoewel het gebruik van TLS dan ook bijdraagt aan betrouwbare communicatie tussen overheid en burger/bedrijfsleven.
2. Bij de implementatie van TLS de 'ICT-beveiligingsrichtlijnen voor TLS' van NCSC worden gevolgd.

Implementatie inspanning
Implementatie van TLS kost doorgaans niet veel tijd (maximaal een paar uur) en betreft het instellen van een (PKIoverheid-)-certificaat voor uw website. Dit dient te worden afgestemd met de webhoster.

Implementatie voorbeelden
Verschillende organisaties hebben TLS al conform de TLS-richtlijnen van NCSC toegepast, zoals DigiD, Ondernemersplein en Logius. Deze organisaties hebben de implementatie van TLS niet alleen gekozen vanwege de veiligheid, maar ook omdat Google goed beveiligde websites hoger rangschikt.

ii. Beveiliging overheids-domeinnamen - *DNSSEC*: DNSSEC zorgt ervoor dat een domeinnaam op een veilige manier vertaald wordt naar een IP-adres. Hierdoor wordt voorkomen dat je wordt omgeleid naar een valse webpagina of dat je e-mail wordt afgeleverd bij een valse mailserver.

Het gebruik van de standaard is verplicht voor elke domeinnaam waarmee een overheid met burgers en/of bedrijven communiceert.

Implementatie inspanning
Implementatie van deze standaard is niet ingewikkeld. Veel moderne software biedt hiervoor ondersteuning. Bovendien is er veel ervaring binnen en buiten de overheid. Het toepassen van de standaard dient te worden afgestemd met de beheerder van het DNS-systeem. Domeinnamen van het Rijk moeten reeds worden ondergebracht bij Dienst Publiek en Communicatie van het Ministerie

van Algemene Zaken. Zij biedt als aanvullend kosteloze dienst ook DNS-beheer inclusief ondersteuning van DNSSEC.

Implementatie voorbeelden
Meer dan 40% van alle nl-domeinen is ondertekend met DNSSEC waaronder ook websites van verschillende overheden zoals de gemeente Den Haag, het Kadaster en overheid.nl.

iii. Beveiliging overheids-email - *DMARC/SPF/DKIM*: DMARC, SPF en DKIM zijn standaarden die spoofing (imitatie) en phising via e-mail tegengaan. Een ontvanger van mail kan hiermee geautomatiseerd controleren of de afzender (een mailadres) en de verzender (een computersysteem) van een mail inderdaad kloppen, en dat de inhoud onderweg niet is veranderd. Daardoor zal een mail van een kwaadwillende, die het beschermde e-mailadres misbruikt, de beoogde ontvanger niet bereiken.

De resultaatafspraak is dat de standaarden toegepast worden voor alle overheidsdomeinnamen of deze nu wel of niet gebruik maken van mail. Ook domeinnamen (het adres wat achter de @ staat) die niet gebuikt worden voor mail kunnen misbruikt worden door kwaadwillenden.

Implementatie inspanning
Implementatie van de standaarden is relatief eenvoudig, met name als er geen mail wordt gestuurd vanaf een domeinnaam is het een kwestie van aanvinken van de juist instellingen. In het derde kwartaal 2015 zal het NCSC een 'ICT-beveiligingsrichtlijn mail' publiceren waarin staat hoe de standaarden te implementeren.

Implementatie voorbeelden
Verschillende organisaties hebben de standaarden al geïmplementeerd zoals de Belastingdienst, de Ministeries van Binnenlandse Zaken en Veiligheid en Justitie en de gemeente Heerlen.

Ad. 2 Herbevestiging en verlenging van bestaande overheidsbrede 'pas toe of leg uit' -afspraak tot eind 2017

'Pas-toe-of-leg-uit' betekent dat overheden bij aanschaf van ICT moeten kiezen voor de relevante open standaarden van de zogeheten 'pas-toe-of-leg-uit'-lijst. Afwijken mag alleen bij zwaarwegende reden en hierover moet via het jaarverslag worden verantwoord. Voor het Rijk is het 'pas-toe-of-leg-uit'-principe voor onbepaalde tijd vastgelegd in een Rijksinstructie.[2] De 'pas-toe-of-leg-uit'-afspraak voor decentrale overheden komt terug in resultaatverplichting 20 van i-NUP en in bestuursakkoorden.[3]

Hoewel iNUP per 31-12-2014 is afgelopen, bestaat formeel nog tot eind 2015 een bestuurlijke basis voor overheidsbrede 'pas-toe-of-leg-uit' voor open standaarden[4],

[2] 'Instructie rijksdienst bij aanschaf ICT-diensten of ICT-producten', https://zoek.officielebekendmakingen.nl/stcrt-2008-837.html
[3] 'Pas toe of leg uit'-regime, https://www.forumstandaardisatie.nl/open-standaarden/voor-overheden/pas-toe-of-leg-uit-regime/
[4] Namelijk via het Bestuursakkoord 2011-2015 (zie: https://zoek.officielebekendmakingen.nl/kst-32749-1.html).

waardoor de rijksinstructie ook geldt voor Gemeenten, Provincies en Waterschappen. Het ligt evenwel voor de hand om – mede gelet op de motie Oosenbrug/Gesthuizen[5] - deze afspraak op dit moment te herbevestigen en daarmee te verlengen tot eind 2017:
"Gemeenten, Provincies, Rijk en Waterschappen maken gebruik van de open standaarden zoals vastgesteld door het National Beraad en werken hierbij volgens het principe 'pas-toe-of-leg-uit'[6]".

Daarin staat: "Standaarden die zijn vastgesteld door het College standaardisatie dienen door alle overheidsorganen te worden toegepast volgens het principe 'pas-toe-of-leg-uit' waarom niet'."

[5] Voor een beeld hoe de motie zich verhoudt tot de hier voorgestelde afspraken wordt u verwezen naar de tabel in de bijlage.

[6] Zoals vastgelegd in de eerdergenoemde Rijksinstructie.

Bijlage: voorbeelden van afnemend vertrouwen als gevolg van phishing

- htt-ps://www.waarschuwingsdienst.nl/Risicos/Actuele+dreigingen/Softwarelekken/WD-2014-007+Waarschuwing+phishing-e-mail+uit+naam+van+het+Centraal+Justitieel+Incassobureau+CJIB+in+omloop.html

- htt-ps://www.waarschuwingsdienst.nl/Risicos/Actuele+dreigingen/Virussen+en+wormen/WD-2013-014+Sterke+toename+in+nep+incasso+e-mails.html

- htt-ps://www.waarschuwingsdienst.nl/Risicos/Actuele+dreigingen/Virussen+en+wormen/WD-2013-020+Sterke+toename+in+spam+e-mail+die+van+de+Politie+lijkt+te+zijn.html

- http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/standaard_functies/prive/contact/andere_onderwerpen/phishing

- http://www.fraudehelpdesk.nl/nieuwsbericht/digid_tijdelijk_onbereikbaar_door_vereiste_verificatie

Datum
29 april 2015

Kenmerk
2015-0000255139

Bijlage: motie Oosenbrug/Gesthuizen

Tweede Kamer der Staten-Generaal

Vergaderjaar 2014–2015

33 326 Parlementair onderzoek ICT-projecten bij de overheid

Nr. 21 GEWIJZIGDE MOTIE VAN DE LEDEN OOSENBRUG EN GESTHUIZEN TER VERVANGING VAN DIE GEDRUKT ONDER NR. 19

Voorgesteld 14 april 2015

De Kamer, gehoord de beraadslaging,

constaterende dat de motie-Vendrik al in 2002 opriep tot voldoen aan open standaarden in 2006 en ambitieuze doelstellingen voor gebruik van opensourcesoftware;

constaterende dat uit de Monitor Open Standaardenbeleid 2014 van het ICTU blijkt dat bij aanbestedingen slechts een beperkt deel van de relevante open standaarden gevraagd wordt en dat er geen sprake is van een «pas toe of leg uit»-principe;

constaterende dat er geen ambitieuze doelstellingen zijn voor het gebruik van opensourcesoftware; van mening dat hierdoor de afhankelijkheid van een beperkt aantal grote softwareleveranciers te sterk is en dat dit kan leiden tot te hoge maatschappelijke kosten voor software;

verzoekt de regering,

ervoor te zorgen dat voor eind 2015 bij alle aanbestedingen correct omgegaan wordt met de relevante open standaarden;

verzoekt de regering voorts om, te onderzoeken hoe de overheid door exitstrategieën minder afhankelijk kan worden van ICT-aanbieders en hiervan verslag uit te brengen aan de Tweede Kamer;

verzoekt de regering verder om, in elke aanbesteding van een nieuw ICT-project het bestek zodanig op te stellen dat opensourcetoepassingen een gelijke kans maken en bij de keus voor een closedsourcetoepassing deze toe te lichten,

en gaat over tot de orde van de dag.

Oosenbrug Gesthuizen

Tweede Kamer, vergaderjaar 2014–2015, 33 326, nr. 21 2

Bijlage: verhouding tussen resultaatafspraken, verlenging overheidsbrede 'pas-toe-of-leg-uit'-afspraak en motie

Datum
29 april 2015

Kenmerk
2015-0000255139

	Resultaatsafspraken adoptie inf.veil.stand. **(voorstel 1 uit deze notitie)**	**Verlenging overheids brede 'pas-toe-leg-uit'** **(voorstel 2 uit deze notitie)**	**Motie Oosenbrug/ Gesthuizen t.a.v. open standaarden**
aard afspraak	resultaat	proces	proces
wanneer	stapsgewijs 2015 en 2016	tot en met 2017	voor eind 2015
aangrijp punt	gebruik	aanbestedingen	aanbestedingen
welk deel ptolu lijst	aantal informatie veiligheid standaarden ptolu	hele ptolu lijst	hele ptolu lijst
gremium	Nat.Beraad 18-5 toezicht: regie raad interconnectiviteit	Nat.Beraad 18-5	PM toezicht: audit dienst rijk en PM