

Standpuntbepaling waterschappen Herkenbaarheid overheidswebsites en – emails

De toenmalige Directie Informatiesamenleving en Overheid (DIO) van het ministerie van BZK heeft in 2018/2019 een onderzoek laten uitvoeren naar de herkenbaarheid van overheidswebsites en e-mails. In dit online-onderzoek, waar in totaal 1.423 burgers aan hebben deelgenomen, is onderzocht in hoeverre respondenten in staat zijn om de authenticiteit van overheidswebsites en –emails te beoordelen.

Uit het onderzoek bleek dat 72% van de respondenten ervaring heeft met phishing emails of vervalste emails en websites. Vervalste websites werden niet herkend door 50% tot 60% van de respondenten (afhankelijk van het voorbeeld). Bij vervalste emails waren de resultaten wat gunstiger: deze werden door 10% tot 30% niet herkend. Met het herkennen van echte overheidswebsites en -emails was het niet beter gesteld. Slechts 30% tot 50% herkende de voorgelegde websites als echt. Ook hier werden emails vaker herkend als authentiek (48% tot 74%, afhankelijk van het voorbeeld).

De resultaten van dit onderzoek riepen vragen op over de herkenbaarheid en betrouwbaarheid van overheidswebsites en –emails die voor burgers niet makkelijk zijn te herkennen als authentiek. Vervalste websites zorgen voor een algemene afname van het vertrouwen in overheidscommunicatie. De overheid eist van inwoners en bedrijven dat zij hun zaken digitaal melden of hun informatie digitaal beschikbaar stellen. In feite “dwingen” zij burgers om online te gaan en dus moeten inwoners en bedrijven er vanuit kunnen gaan dat hun informatie bij overheden in goede handen is. Dit maakt dat de overheid een plicht heeft om op een betrouwbare manier met deze informatie om te gaan. Privacybescherming en informatieveiligheid zijn daarom cruciaal en succesbepalend voor de kwaliteit van de (digitale) dienstverlening én voor het algehele vertrouwen van de samenleving in de overheid.

Het BZK onderzoek liet duidelijk zien naar welke aspecten burgers kijken om echte van valse websites en emails te onderscheiden. Het blijkt dat burgers vooral kijken naar het type domeinnaam van emails en websites. Een mogelijke oplossing is dus om als overheid te gaan werken met geüniformeerde domeinnamen (extensies) om de authenticiteit te vergroten.

Deze oplossingsrichting is in de vorm van enkele stellingen besproken in het Digitaliseringsberaad¹ van de waterschappen d.d. 5 september 2019. De leden van het Digitaliseringsberaad herkenden de problematiek maar vroegen zich af in hoeverre de voorgestelde oplossing het probleem oplost. Perfect bestaat niet; het is een kwestie van tijd voordat criminelen de mazen in de wet weer hebben gevonden. Op de vraag of de waterschappen mee willen gaan doen met overheid.nl of gov.nl werd bevestigend geantwoord. De reputatie van de waterschappen wordt als zeer waardevol gezien. Dit geldt ook voor de belasting innende organisaties. Niemand is voorstander van waterschap.nl o.i.d. als extensie voor de websites en emailadressen van de waterschappen. Op de vraag of het dan overheid.nl of gov.nl moet worden, antwoordde het Digitaliseringsberaad dat gekozen moet worden voor de meest veilige optie.

Naar aanleiding van de bespreking in het Digitaliseringsberaad hebben enkele waterschappen een ambtelijke reactie naar de Unie van Waterschappen gestuurd en is het onderwerp in het i-Platform² van de waterschappen d.d. 17 september 2019 besproken. Net als in het Digitaliseringsberaad werd opgemerkt dat van een uniforme extensie van overheids-urls geen wonderen moet worden verwacht voor het voorkomen van phishing en fraude. Desondanks kunnen we het als overheid nog steeds introduceren. Verwacht werd dat de introductie van uniforme domeinnamen een flinke impact op de digitalisering zal hebben. Enkele voorbeelden:

¹ Aan het Digitaliseringsberaad nemen bestuurders, (secretaris-)directeuren, Chief Information Officers en Chief Digital Officers van alle 21 waterschappen deel, aangevuld met een afgevaardigde van de Unie van Waterschappen, Het Waterschapshuis, de STOWA en een extern deskundige. Het doel van het Digitaliseringsberaad is om van elkaar te leren, kennis en ervaringen te delen, inspiratie op te doen, de bestuurlijk-ambtelijke dialoog te faciliteren en de digitale transformatie bij waterschappen aan te jagen.

² Het i-Platform van Het Waterschapshuis is een platform van de i-managers van alle waterschappen



- Domeinnamen worden gebruikt in beveiligingscertificaten waarmee berichtenverkeer en websites zijn beveiligd. Domeinnamen vervangen betekent waarschijnlijk dat al deze certificaten vervangen moeten worden.
- Bij digitale koppelingen/informatieuitwisselingen en het aanroepen van webservices maken domeinnamen onderdeel uit van de aanroep (zeg maar de "adressering"). Denk bijvoorbeeld aan de aansluiting op het Omgevingsloket. Deze services en de apps en websites die er gebruik van maken moeten gecheckt en mogelijk aangepast worden.
- Ook e-mailadressen van (medewerkers van) waterschappen veranderen als de domeinnaam verandert.
- E-mailadressen zijn vaak tegelijk ook de gebruikersnaam bij het inloggen op de kantoor-omgeving, software die medewerkers gebruiken en op externe websites/platformen die medewerkers gebruiken. Het vraagt tijd om dit aan te passen.
- Overheidsorganisaties maken gebruik van cloud-diensten bij private partijen, ook t.b.v. dienstverlening en communicatie aan burgers. Dit gebeurt soms met domeinnamen die de private partij ter beschikking stelt (denk aan het platform iBabs waarmee ook publiek vergaderstukken zijn te raadplegen: <https://ris2.ibabs.eu/UvW> voor de Unie)
- Steeds meer overheidsorganisaties werken met linked data; wat is de impact hier op?

De impact van uniforme domeinnamen moet dus zeker niet onderschat worden en een gedegen impactanalyse mag dus zeker niet ontbreken.

Het bovenstaande geeft een eerste indicatie hoe de waterschappen tegen uniforme domeinnamen aankijken. Een echt besluit hierover kan uiteraard pas genomen worden als de impact en kosten helder zijn.