06 maart 2019, 07:30 (CET)

Één op de drie zorg- en onderwijswebsites niet goed beveiligd

Een op de drie websites van publieke organisaties is nog altijd niet goed beveiligd. Gevoelige informatie zoals burgerservicenummers of zelfs medische en psychologische klachten kan zo op straat belanden. Dat blijkt uit onderzoek van Open State Foundation.

Open State onderzoekt sinds 2016 websites van publieke organisaties met Pulse, een eigen tool die periodiek controleert of websites HTTPS (https://) ondersteunen. Ook laat de tool zien hoe sterk de implementatie van HTTPS is. Dat HTTPS op gevoelige websites niet geïmplementeerd is kunnen we bijvoorbeeld zien op de website van Kinderpsychologen Naarden-Bussum waar niet-beveiligd gevraagd wordt naar het BSN-nummer van een kind en op NetZwanger.nl, een verloskundigenpraktijk in Noord-Holland. Bekijk de volledige lijst met websites via Pulse.

HTTPS is heel belangrijk omdat het zorgt voor een veilige en niet-manipuleerbare internetverbinding tussen websites en haar bezoekers. Als er geen HTTPS-verbinding is, maar 'slechts' HTTP kunnen mensen met kwade wil makkelijk de data aflezen en misbruiken. Daarom gaat bijvoorbeeld ook het online bankverkeer alleen via het veilige HTTPS. Vanaf 2019 is het verplicht voor alle overheidswebsites om gebruik te maken van HTTPS.

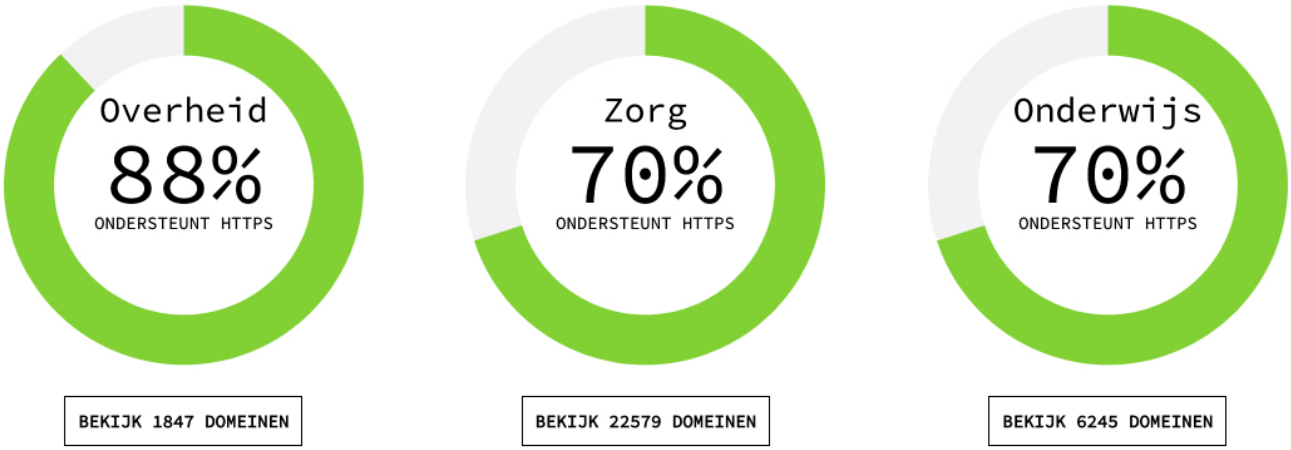
Hoe weet je of een website veilig is?

Wanneer je gebruik maakt van een online (contact)formulier controleer dan ook goed of je wel gebruik maakt van een veilige verbinding. Dit kun je gemakkelijk zien door het slotje en 'https://' aan het begin van de url in je adresbalk. Wanneer er geen slotje is, is het verstandig om geen belangrijke gegevens te delen zoals adres, bankgegevens of medische gegevens. HTTPS afdwingen op je eigen website kan zeer eenvoudig en kosteloos via aanbieders zoals Let's Encrypt.

Nieuwe Pulse Scan

Open State Foundation onderzocht meer dan 30.000 domeinen in relevante sectoren, zorg, onderwijs en overheid. Dit doen we door het gedrag van vier “endpoints” van elk domein: http://, http://www, https://, en https://www te analyseren. Data van deze endpoints wordt gebruikt om het totale gedrag van het domein te bepalen. Voor deze analyse wordt gebruikt gemaakt van open source tools en de SSL LabsAPI.

Concreet zijn de resultaten van de laatste scan van eind februari als volgt:



Resultaten vorige scans: Overheid (72% op 24-12-2017), Zorg (39% op 07-08-2017) en Onderwijs (32% op 01-12-2017)

Let op het afdwingen van HTTPS

Voor de duidelijkheid: ‘ondersteunt HTTPS’ betekent dat je gebruik kan maken van HTTPS, niet dat de website het afdwingt. Zo kun je op websites die HTTPS ondersteunen maar niet afdwingen nog steeds onbeveiligd informatie doorsturen, als je niet zelf eerst HTTPS intypt. Slechts 61% van de zorgdomeinen dwingt HTTPS echt af, en is het dus altijd veilig om informatie te delen.

Meer weten over Pulse? Bekijk dan pulse.openstate.eu, en bekijk de volledige data van alle scans op data.openstate.eu.

Tom Kunzler
tom@openstate.eu
06 237 59 257
Adjunct-directeur
Teaumas

OVER OPEN STATE FOUNDATION

Open State Foundation bevordert digitale transparantie door het ontsluiten van open data en de ontwikkeling van innovatieve en creatieve toepassingen te stimuleren.

Open State Foundation promotes digital transparency by unlocking open data and stimulates the development of innovative and creative applications.