notitie

Test veilige toepassing TLS (beveiligde verbindingen)

FORUM STANDAARDISATIE 28 oktober 2014
Agendapunt 05. Open standaarden, adoptie
Stuk 05B. Test veilige toepassing TLS

Van:	Stuurgroep open standaarden
Aan :	Forum Standaardisatie

Doel: ter discussie

Het Forum Standaardisatie wordt gevraagd om op basis van de testresultaten te discussiëren aan de hand de volgende vragen:
1. Hoe kunt u in uw eigen organisatie of bij uw eigen achterban de veilige toepassing van TLS bevorderen?
2. Welke mogelijkheden ziet u voor de verspreiding en het gebruik van de aanstaande NCSC-handreiking?

Aanleiding en achtergrond

In de collegevergadering van 4 september is TLS versie 1.2 t/m 1.0 opgenomen op de 'pas toe of leg uit'-lijst. TLS is de standaard die zorgt voor het opzetten van een met certificaten beveiligde verbinding (bijv. https://...). In het Forumadvies over de opname van TLS op de 'past toe of leg'-lijst komt naar voren dat voor een goede beveiliging het van belang is om TLS 1.2 (de nieuwste versie) te ondersteunen en daarnaast te zorgen voor veilige TLS-instellingen. Onveilige TLS-instellingen biedt kwaadwillenden de mogelijkheid om 'af te luisteren'. Om meer inzicht te geven in de adoptie van de standaard is in bijgevoegde overzicht voor een aantal webportalen weergegeven op welke manier ze TLS ondersteunen.

Betrokkenen en proces

De test is door BFS uitgevoerd op 16 september 2014 met de testtool van SSLlabs (https://www.ssllabs.com/ssltest/). Er is een aantal voorzieningen geselecteerd die binnen het domein van de verschillende Forum-leden vallen. Ook is gekeken naar een aantal bekende consumentenportalen. Aanvullend op de vraag of er gebruik wordt gemaakt van TLS, is met de tool gemeten of de standaard op een veilige wijze is ingesteld.

Consequenties en vervolgstappen

Uit de test blijkt dat in een aantal gevallen TLS 1.2 geactiveerd is, maar dat aanvullende actie nodig is om de standaard zo te configureren dat deze daadwerkelijk maximaal veilig is ingesteld. Naar aanleiding van de toetsingsprocedure en het collegebesluit wordt dan ook door het NCSC een handreiking opgesteld hoe met het gebruik en de configuratie van TLS om te gaan.

Resultaten uitgevoerde test
De scoringsmeetlat loopt van A (zeer goed) tot F (slecht). Voor de veiligheid van de configuratie is alleen een A te scoren als gebruik wordt gemaakt van TLS-versie 1.2.

Voorziening	TLS1.2 ondersteund	TLS 1.1 ondersteund	TLS 1.0 ondersteund	Score veiligheid configuratie
Berichtenbox	Nee	Nee	Ja	C
DigiD	Ja	Nee	Ja	A-
Subsidieportaal	Nee	Nee	Ja	B
Mijn DUO	Nee	Nee	Ja	B
Studielink	Nee	Nee	Ja	B
EloVOG	Ja	Ja	Ja	A-
Omgevingsloket	Ja	Ja	Ja	A-
RDW loket	Nee	Nee	Ja	F
Mijn UWV	Nee	Ja	Ja	F
Ondernemersportaal Belastingdienst	Ja	Ja	Ja	A-
Mijn Toeslagen	Ja	Ja	Ja	A-
Mijn Loket Gemeente- en waterschapsbelastingen	Nee	Nee	Ja	B
Overheid.nl	Ja	Ja	Ja	A-
VNG	Ja	Ja	Ja	F
Dienstenportaal Almelo	Ja	Nee	Ja	A-
Dienstenportaal provincie Utrecht	Nee	Nee	Ja	B
MijnOverheid	Ja	Ja	Ja	A+
SURFnet	Ja	Ja	Ja	A
Rabobank Internetbankieren	Ja	Ja	Ja	A-
ABN Amro Internetbankieren	Ja	Ja	Ja	A-
ING Internetbankieren	Ja	Nee	Ja	A-
BOL.com	Ja	Ja	Ja	A-
Marktplaats	Ja	Ja	Ja	A-
Thuisbezorgd	Ja	Ja	Ja	F
Vliegtickets.nl	Ja	Nee	Ja	B
Zalando	Ja	Ja	Ja	A-

Conclusie
Bovenstaande overzicht geeft aan dat de portalen voldoende interoperabel zijn, daar ze allemaal TLS versie 1.0 ondersteunen. Maar we kunnen ook concluderen dat met betrekking tot veilige configuratie en het ondersteunen van versie 1.2 er nog wel het nodige valt te verbeteren. Ook zien we dat de overheid bij het ondersteunen van versie 1.2 enigszins achterloopt op het bedrijfsleven.

Handreiking NCSC
Op dit moment wordt op advies van Forum/College door het NCSC een handreiking ontwikkeld hoe om te gaan met het gebruik van TLS. De verwachting is dat deze handreiking eind oktober is afgerond. Deze moet overheden en andere partijen helpen bij de veilige configuratie van TLS. Het is van belang dat ook het Forum zich inspant om deze handreiking breed onder de aandacht te brengen.

Zeer recent is er overigens een kwetsbaarheid bekend geworden in SSL versie 3, dat de voorganger is van TLS. Het NCSC adviseert om SSL versie 3 op servers en clients uit te schakelen waar mogelijk.[1]

[1] *Zie: https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/beveiligingsadviezen/NCSC-2014-0641+1.00+Kwetsbaarheid+in+SSL+3.0+ontdekt.html*