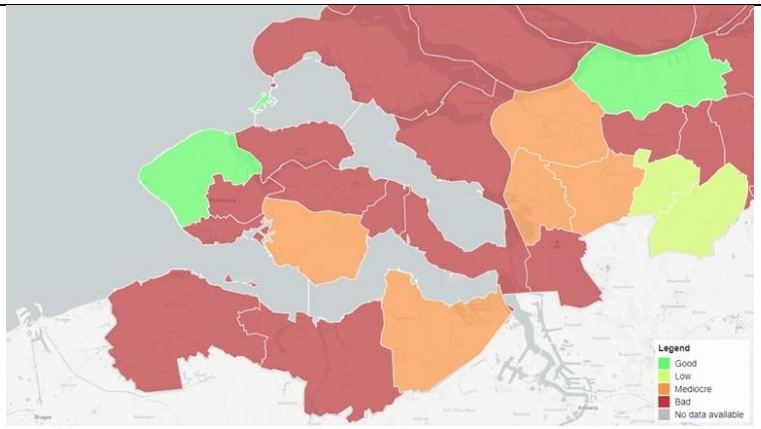
Schriftelijke vraag

(art. 27 RvO commissie)

Per onderwerp afzonderlijk formulier gebruiken
Indienen via het e-mailadres griffie@tholen.nl

Nummer *(in te vullen door griffie)*	19.0017
Datum ontvangst raadsgriffie *(in te vullen door griffie)*	28 augustus 2019
Datum	28 augustus 2019
Vraag wordt gesteld aan	College B&W
Naam vragensteller	Jacques Dekkers en Jan Heshof, fractie PvdA/GL
Verzocht wordt de volgende vraag (vragen) te beantwoorden	1. Heeft het college kennisgenomen van de berichtgeving d.d. 25 augustus j.l. inzake de beveiliging van gemeentelijke websites door Omroep Zeeland? 2. Kunt u aangeven welke (privacy) risico's onze inwoners lopen? 3. Hoe kan het zijn dat onze gemeente, ondanks de nodige investeringen in ICT, tot een dermate slechte score komt in vergelijking met andere gemeenten? (Plaats 293) 4. Bent u het met de suggestie van Elger Jonker eens dat het vooral een gebrek aan kennis betreft? 5. Wat kan onze gemeente leren van bv de gemeente Veere waar de beveiliging wel op orde is? 6. Welke matregelen en op welke termijn gaat het college nemen om de beveiliging op orde te brengen?
Toelichting *(indien nodig)*	zondag 25 augustus 2019, 12:54 **Veere heeft online-beveiliging op orde, bij andere gemeenten kan het beter** De gemeente Veere is de enige Zeeuwse gemeente die wat de digitale beveiliging van de eigen websites betreft de zaken op orde heeft. Op de Faalkaart, dat is een website waarop te zien is hoe het gesteld is met de digitale beveiliging van gemeentelijke websites en online-diensten, is Veere de enige groen gekleurde gemeente van onze provincie.



Veere is de enige groene Zeeuwse gemeente op de Faalkaart (foto: Faalkaart)

Veere was bovendien afgelopen week landelijk gezien bijna de veiligste gemeente. Bijna, omdat gemeente De Fryske Marren nog beter scoorde en daarom bovenaan het lijstje staat. Veere staat op de nummer twee.
Veere is landelijk de nummer twee van gemeenten die de digitale beveiliging op orde hebben.. (foto: Faalkaart)
De rest van Zeeland scoort belabberd. Borsele en Hulst krijgen nog een 'middelmatig', maar de andere Zeeuwse gemeenten scoren volgens de website ronduit 'slecht'. Dit Zeeuwse beeld past in het landelijke plaatje. Alle provincies zijn op de kaart grotendeels rood gekleurd, met slechts hier en daar een groen vlekje, zoals Veere.

'Het ontbreekt aan kennis'

De Faalkaart is in 2016 opgezet door Elger Jonker, die daarmee wil laten zien dat het er bij veel gemeenten nog ontbreekt aan kennis over ict. De site zoekt doorlopend alle domeinnamen van gemeenten en controleert meerdere onderdelen, zoals of het beveiligingscertificaat van de site klopt.
Op basis daarvan krijgen alle gemeenten een waarde toegekend, waarvan de resultaten op basisbeveiliging.nl in de vorm van een kaart getoond worden. De gemeente Amsterdam voert landelijk gezien de lijst aan van gemeenten met de meeste beveiligingsrisico's op de eigen websites.

Kanttekening

Daarbij plaatst de maker van de website zelf ook een kanttekening: er wordt automatisch gekeken naar alle domeinnamen van de gemeente en als daar één tussen zit met in zijn ogen verkeerde instellingen telt dat al als een fout. Dat gebeurt ook als het gaat om een domeinnaam van de gemeente die niet in gebruik is of die alleen voor de eigen medewerkers gebruikt wordt, zoals het intranet van de gemeente Veere.

Elger Jonker van de Faalkaart over beveiliging websites

	Het is dus niet per se zo dat een inwoner van een gemeente die op de faalkaart rood uitslaat gevaar loop als die de website van die gemeente bezoekt. Toch staan tussen de Zeeuwse sitenamen die volgens de faalkaart de beveiliging niet op orde hebben ook veel websites die wél voor bewoners toegankelijk zijn, zoals afvalkalender.borsele.nl of bijvoorbeeld middelburg.nl. **Gevoelige informatie** Maar ook bij de sites die niet voor de inwoners bedoeld zijn, is het volgens Jonker belangrijk om dit probleem aan de kaart te stellen. "Sommige van die domeinnamen worden gebruikt voor heel specifieke diensten en als daar de beveiliging niet klopt, kunnen gevoelige data op straat komen te liggen en dat is nóg veel ernstiger", aldus Jonker. Zo staat ook een webmailadres van de gemeente Middelburg tussen de internetadressen die volgens de faalkaart niet goed beveiligd zijn. Jonker hoopt dat zijn kaart en de berichtgeving daarover gemeenten aanspoort om actie te ondernemen en verbeteringen door te voeren. Zoals de gemeente Veere.

Antwoord van college/ burgemeester indien schriftelijk antwoord wordt gegeven *(in te vullen door afdeling)*	1. Het college heeft kennisgenomen van de berichtgeving van Omroep Zeeland inzake de beveiliging van gemeentelijke websites door Omroep Zeeland. 2. Onze inwoners lopen geen (privacy) risico's. De kwetsbaarheden zijn gevonden op twee servers die niet ingezet worden voor dienstverlening aan of gebruik door inwoners. a. De eerste server, ftp.tholen.nl (File Transport Protocol (FTP), wordt gebruikt om openbare documentatie te ontsluiten voor overleggen ten behoeve van vergaderingen waarbij een iPad wordt gebruikt. Er is daarom geen sprake van een privacy risico voor inwoners. b. De tweede server, autodiscover.tholen.nl, wordt gebruikt om automatisch gebruikersprofielen van (geautoriseerde) email-gebruikers te configureren. Er worden aan deze gebruikers geen persoonsgegevens teruggekoppeld. Er is daarom geen sprake van een privacy risico voor inwoners. De bevindingen van basisbeveiliging.nl hebben betrekking op deze twee servers, niet op de gemeentelijke website. Deze website voldoet aan alle eisen.

	3. Metingen van beveiligingsstandaarden op websites van gemeenten door de website basisbeveiliging.nl, bieden zonder context onvoldoende beeld van het algemene beveiligingsniveau. Het beeld dat we als gemeente slecht scoren heeft daarom enige nuance nodig. Zie ook de beantwoording van vraag 2. Basisbeveiliging.nl publiceert een 'Top Fail' lijst. Bij de nummer 1 van die lijst zijn de meeste kwetsbaarheden gevonden. Positie 293 betekent in dit geval dat Tholen bij de top 100 hoort van gemeenten die de beveiliging het best hebben georganiseerd. Feit is dat de genoemde punten opgelost moeten worden en structureel gemonitord moeten worden. De betreffende kwetsbaarheden waren bekend en tevens opgenomen in de planning om te worden verholpen. Een kwalitatieve vergelijking alleen op basis van financiële investeringen is echter moeilijk te maken. Iedere gemeente geeft geld uit om de informatieveiligheid te kunnen blijven garanderen. Op basis van een risicoafweging wordt bepaald of een beveiligingsmaatregel moet worden toegepast. Zo hoort bij een formulier waarop inwoners gegevens doorgeven aan de gemeente een ander beveiligingsregime dan op een informatieve website met de openingstijden van de dierentuin. De roodgekleurde kaarten zijn daarom niet altijd een indicatie van een slecht ingerichte beveiliging. Maar ook groen is geen garantie op een goed ingerichte beveiliging. Informatiebeveiliging gaat altijd om een samenhangend pakket van niet alleen technische -, maar ook organisatorische maatregelen. Het is waar dat de digitale infrastructuur per definitie kwetsbaar is. Daarom werkt de gemeente Tholen volgens de norm van de Baseline Informatiebeveiliging Gemeenten / Overheid (BIG/BIO) doorlopend aan informatiebeveiliging. Alle gemeenten leggen hierover ieder jaar via ENSIA (zie www.ensia.nl) verantwoording af aan de eigen gemeenteraad en het rijk. 4. De onderzochte kwetsbaarheden zeggen niet direct iets over het kennisniveau. Zoals in vraag 3 is aangegeven, wordt op basis van een risicoafweging bepaald of en wanneer een beveiligingsmaatregel wordt toegepast. De implementaties worden gerealiseerd door middel van een zo efficiënt (financieel en organisatorisch) mogelijke planning. Soms zijn oplossingen afhankelijk van andere componenten waardoor het niet altijd mogelijk of gewenst is de implementatie direct te starten. 5. Iedere gemeente werkt volgens de norm van de Baseline Informatiebeveiliging Gemeenten / Overheid (BIG/BIO) en wordt bepaald of en wanneer een beveiligingsmaatregel wordt toegepast. Alle gemeenten leggen hierover ieder jaar via ENSIA verantwoording af aan de eigen gemeenteraad en het rijk. Door de gehanteerde Plan Do Check Act (PDCA) cyclus is bijsturing periodiek mogelijk. Uitwisseling van kennis en ervaring met andere gemeenten is altijd gewenst en er zijn diverse collegiale contacten met andere gemeenten voor het uitwisselen van kennis en ervaring, waarbij het leren van elkaar zeker aandacht heeft. 6. De betreffende kwetsbare omgevingen worden aangepast en/of vervangen door veiligere oplossingen. Dit houdt concreet in dat de FTP-server binnen enkele weken zal worden vervangen en daarna niet meer op basisbeveiliging te zien zal zijn. Daarnaast gebeurt de configuratie van de Autodiscover-server ook grotendeels in die periode.

Datum beantwoording *(in te vullen door afdeling)*	28 augustus 2019

Ingeleverd bij de griffie *(in te vullen door griffie)*	3 september 2019