

Fractie SP
T.a.v. de heer M. Tonies

ICT
Raadhuislaan 2, Oss
Telefoon 14 0412
Fax [0412] 64 26 05
E-mail gemeente@oss.nl
www.oss.nl

Postbus 5
5340 BA Oss

Wilt u bij uw reactie de
datum van deze brief en
ons kenmerk vermelden?

Datum	Ons kenmerk	Behandeld door	Doorkiesnummer
17 juni 2016		Th. Koolen	9723
Onderwerp			
Artikel 41-vragen over proces rond veiligheid gemeentelijke en samenwerkende websites			

Geachte heer Tonies,

Op 8 mei 2016 heeft u het college een aantal vragen gesteld over het proces van de veiligheid van gemeentelijke en samenwerkende websites. Dit heeft u gedaan n.a.v. de beantwoording van eerdere vragen van 30 maart 2016.

Wij beantwoorden uw vragen als volgt:

1. Is het de portefeuillehouder, mevr W.J.L. Buijs-Glaudemans, opgevallen dat op een aantal van de eerder gestelde vragen geen antwoord is gegeven?

Antwoord:

Bij nadere bestudering van de antwoorden is gebleken dat er inderdaad onduidelijk antwoord is gegeven op de vraag naar welke externe websites waarop persoonsgegevens kunnen of moeten worden ingevuld de Osse website verwijst (vraag 7). Onze excuses daarvoor. Bij vraag 5 zal een uitgebreid antwoord hierop worden gegeven.

2. Wat is de mening van de portefeuillehouder, over de gebrekkige beantwoording van de eerder gestelde schriftelijke vragen?

Antwoord:

Informatiebeveiliging is een complex en breed terrein; het betreft zowel aspecten van houding en gedrag van medewerkers en burgers als zichtbare en onzichtbare technische zaken. Hierbij is het niet altijd mogelijk om in kort bestek aan al deze zaken recht te doen. Daardoor kan het zijn dat er onduidelijkheid is ontstaan. Daarnaast is het niet altijd opportuun om publiekelijk onze beveiligingsmaatregelen bekend te maken.

We realiseren ons dat informatiebeveiliging een belangrijk onderwerp is dat volop de aandacht heeft en maken graag van de gelegenheid gebruik u verder te informeren. Indien daar belangstelling voor is, kunnen wij in een podiumbijeenkomst of in gesprek verder ingaan op hoe de gemeente Oss omgaat met haar beveiliging van o.a. websites, de rol van de InformatieBeveiligingsDienst voor gemeenten (IBD) en de implementatie van de Baseline Informatieveiligheid Gemeenten (BIG).

3. Op vraag 3 is het antwoord dat U de kwaliteit van de in de pers genoemde onderzoeken niet kan waarborgen, maar dat U wel bekend bent met de genoemde problematiek. Bij deze de vraag: wat is de status van verschillende genoemde websites met betrekking tot het Drown-lek?

Antwoord:

Uit onze tests blijkt dat er bij de volgende websites geen sprake (meer) is van de Drown-problematiek:

www.oss.nl

webmail.oss.nl

loket.oss.nl

hulpwijzer.oss.nl

www.permitonline.nl

www.werkenbijdegemeenteoss.nl

Bij wion.oss.nl is de leverancier helaas nog niet zo ver dat een oplossing geïmplementeerd kan worden. Omdat deze site slechts openbare gegevens en geen persoonsgegevens bevat, is dit voor ons nu nog acceptabel. Overigens doen wij er alles aan om dit zo spoedig mogelijk op te laten lossen.

4. Op vraag 4 is het antwoord dat alle, en zeker de gevoelige, e-mail veilig verstuurd dient te worden. Is dat ook het geval?

Antwoord:

Het is belangrijk dat gevoelige informatie beveiligd verstuurd wordt. Echter, doordat hierbij een groot aantal partijen bij is betrokken, is het nog niet altijd mogelijk. Oss is daarbij op meerdere fronten actief.

Om beveiligde e-mail te versturen is het nodig dat zowel de versturende als de ontvangende partij dit technisch hebben geregeld. Dit is helaas nog lang niet overal het geval. Wij maken daarom voor algemene e-mail gebruik van Opportunistic TLS voor het beveiligd versturen en ontvangen. Hierbij "kijkt" onze mailserver of de ontvangende partij beveiligde e-mail kan ontvangen. Indien dat het geval is wordt de e-mail beveiligd verzonden (en ontvangen). Is de ontvangende partij niet in staat om beveiligde e-mail te ontvangen, dan wordt de e-mail gewoon verstuurd. Hierbij zijn wij dus altijd afhankelijk van de ontvangende partij. Uiteraard kunnen wij zowel beveiligd versturen als ontvangen.

Speciaal voor het zorgdomein zijn we bezig met de invoering van een specifiek systeem van beveiligde e-mail tussen de gemeente Oss en de gecontracteerde instellingen in de zorg. Hierbij wordt de e-mail altijd beveiligd verzonden en ontvangen. Op dit moment gebruiken we een tijdelijke werkwijze om veilige te e-mailen.

Op landelijk niveau is er een aantal initiatieven voor berichtenverkeer: de Collectieve OpdrachtRouteerVoorziening (CORV), de Berichtenbox van MijnOverheid en het Gemeentelijk GegevensKnooppunt (GGK) voor WMO en Jeugdwet. Oss maakt hier - uiteraard - gebruik van.

5. Op vraag 7 is naar onze mening geen bevredigend antwoord gegeven. Is de in het antwoord genoemde lijst in te zien of te krijgen, om alsnog deze vraag van een antwoord te voorzien?

Antwoord:

Op de website van de gemeente Oss verwijzen wij naar enkele honderden websites. De meeste van deze websites hebben een informatief karakter. Uiteraard kunt u deze lijst van ons krijgen.

Bij de beantwoording van deze vraag interpreteren wij het begrip "persoonlijke gegevens" als een combinatie van naam, adres, postcode, woonplaats en BSN.

Uitgaande van deze definitie gaat het voor wat betreft de verwijzing in het kader van de gemeentelijke dienstverlening op www.oss.nl om de volgende websites:

Belastingen	www.bs-ob.nl Hierop wordt ingelogd met DigiD
Huwelijken	oss.iburgerzaken.nl Hierop wordt ingelogd met DigiD
Vacatures	www.werkeninnoodoostbrabant.nl Communicatie via veilige verbinding
Digitaal loket	loket.oss.nl Hierop wordt ingelogd met DigiD
Afspraken	internetafspraken.oss.nl/internet_afspraken Communicatie via veilige verbinding

6. Eerder stelde U dat U met ons van mening bent dat een beveiligingswaarschuwing niet zou mogen verschijnen, tenzij in uitzonderlijke situaties. Bent U ook met ons van mening dat het uitblijven van een oplossing van zo'n zichtbaar probleem weinig vertrouwen schept met betrekking tot het veiligheidsbeleid van de gemeentelijke websites?

Antwoord:

De website oss.nl (zonder www) laat geen waarschuwing meer zien. Dat de site oss.nl niet onveilig was, was niet direct voor iedereen duidelijk. Vanwege lagere prioriteit is dit niet meteen opgepakt. Wij vinden het jammer als dit de indruk van onveiligheid zou hebben gewekt.

7. In het antwoord op vraag 11 stelt U dat het probleem wel opgelost wordt, dat is echter geen antwoord op de gestelde vraag. Ligt dit bijvoorbeeld aan de externe partij die dit probleem moet oplossen? Is er in de gemeentelijke organisatie geen aandacht voor dit soort zichtbare problemen?

Al met al de vraag: kunt U alsnog antwoord geven op waarom dit nog steeds niet gebeurd is?

Antwoord:

Zoals gezegd was de site niet onveilig. Abusievelijk is een certificaat gebruikt dat alleen geschikt was voor www.oss.nl en niet voor oss.nl (zonder www), waardoor bij oss.nl een melding werd gegeven. Aangezien er geen onveilige situatie was, had dit probleem een minder hoge prioriteit. Dat hierdoor wellicht onterecht het beeld is ontstaan dat de website onveilig zou zijn is iets wat wij betreuren.

8. Het POODLE-probleem draagt een minder hoog risico met zich mee, maar alsnog de vraag: is het normaal dat beveiligingsproblemen zo lang blijven bestaan?

Antwoord:

Indien naar aanleiding van tests en audits blijkt dat er mogelijke veiligheidsproblemen zijn, dan worden als eerste en direct de problemen met de hoogste prioriteit aangepakt. Indien er zaken spelen die een minder ernstig veiligheidsprobleem vormen, dan worden die - conform de BIG - ingepland en successievelijk afgewerkt.

Namens het College, de portefeuillehouder

A handwritten signature in black ink, appearing to read 'W.J.L. Buijs', with a horizontal line underneath.

Mevrouw drs. W.J.L. Buijs - Glaudemans