

Berghem, 30 maart



Betreft: artikel 41 vragen over veiligheid gemeentelijke en samenwerkende websites

Geacht college van B&W,

Naar aanleiding van het artikel "Beveiliging tientallen gemeentesites lek: persoonsgegevens niet veilig"¹ op de website van RTL Nieuws, waarin journalisten gemeentelijke websites hebben getest, en het artikel "SSL en TLS verbinding verzuipt dankzij Drown-lek"^{2,3} op Webwereld.nl, alsmede eigen ervaringen, stuur ik U de volgende vragen.

Allereerst deze algemene vragen:

1. Bent U net als de SP van mening dat zodra er persoonsgegevens of andere persoonlijke gegevens elektronisch uitgewisseld worden dat dit, in ieder geval vanuit de gemeente, veilig (naar redelijkheid) dient te gebeuren?
2. Bent U van mening dat de websites van organisaties waar de gemeente Oss (nauw) mee samenwerkt ook veilig (naar redelijkheid) dienen te zijn met betrekking tot de elektronische uitwisseling van gegevens?
3. Bent U bekend met bovengenoemde artikelen? Zo ja, heeft U contact opgenomen om te informeren of Oss op de lijst van veilige of onveilige websites staat? Zo nee, waarom niet?
4. Wat is Uw mening over de mogelijke inzet van beveiligde e-mail in plaats van "plain text e-mail" vanuit de gemeente Oss richting haar burgers?
5. Wie is er verantwoordelijk voor de veiligheid en controle van de veiligheid van de gemeentelijke websites, is dat de eigen automatiseringsafdeling of een externe partij?

De volgende vragen over de website van de gemeente Oss.

6. Op oss.nl zijn volgens ons onderzoek de volgende subdomeinen actief: www, webmail, wion, loket en hulpwijzer. Welk van deze of andere actieve subdomeinen hebben volgens U een beveiligde verbinding nodig vanwege gegevensuitwisseling?
7. Naar welke externe websites (behalve permitonline.nl en werkenbijdegemeenteoss.nl) waar persoonlijke gegevens ingevuld kunnen of moeten worden verwijst de Osse website nog meer?
8. Is de onbeveiligde website wion.oss.nl, waarop men kan inloggen, nog actief in gebruik? Zo ja, waarom heeft deze geen beveiligde verbinding, zo nee, waarom is deze nog bereikbaar?

De gebruiker krijgt een beveiligswaarschuwing (zie bijgevoegde schermafbeelding) wanneer oss.nl (dus zonder "www") wordt bezocht. In deze waarschuwing staat dat er bij het bezoeken van de website op deze manier, informatie gestolen kan worden. Dit probleem *is reeds in 2009* gemeld via e-mail⁴, en opnieuw op 8 januari door mij en journalist Paul Driessen.⁵ Volgens de terugkoppeling via het gemeentelijk Twitter account, zou dit in februari opgelost worden.⁶ Op het moment van schrijven verschijnt nog steeds de beveiligswaarschuwing.

9. Bent U met ons van mening dat bij het bezoeken van de gemeentelijke website geen beveiligswaarschuwing mag verschijnen, tenzij in uitzonderlijke situaties zoals net ontdekte problemen waarop nog geen actie is ondernomen?

1 <http://www.rtlnieuws.nl/nieuws/binnenland/beveiliging-tientallen-gemeentesites-lek-persoonsgegevens-niet-veilig>

2 <https://drownattack.com/#question-answer>

3 <http://webwereld.nl/security/92463-ssl-en-tls-verbinding-verzuipt-dankzij-drown-lek>

4 Het betreft een e-mail van mij op 5 augustus 2009 aan Arike Jongman (a.jongman@oss.nl)

5 <https://twitter.com/MartijnTonies/status/685473174495051776>

6 <https://twitter.com/gemeenteoss/status/687263465912844288>

10. Bent U met ons van mening dat elke duidelijke mondelinge of schriftelijke melding (al dan niet via een elektronisch kanaal zoals Twitter) over beveiligingsproblemen richting ambtenaren serieus genomen en in behandeling genomen dient te worden? Zo nee, waarom niet?
11. Bovenstaand probleem is op meerdere manieren eenvoudig op te lossen, waarom is dit nog steeds niet gebeurd?

De volgende vragen hebben betrekking op de veiligheids-status van gemeentelijke websites of websites waarmee Oss samenwerkt.

12. Volgens ons onderzoek is de beveiligde verbinding naar www.oss.nl niet up-to-date en gebruikt of ondersteunt het onveilige SSL 3 protocol. Zonder www is er een "onveilig certificaat" waarschuwing, zoals eerder beschreven. Vindt U dit een probleem? Zo ja, wat gaat U daar aan doen? Zo nee, waarom niet?
13. Wie naar Home > Inwoners > Parkeren > Uw parkeerkaart⁷ op de Osse website gaat, wordt doorverwezen naar een externe website bij permitonline.nl⁸. Wie beheert deze website, gezien het gemeentelijke logo en contactgegevens bovenaan de pagina? Volgens ons onderzoek is de beveiliging van deze website niet up-to-date en kwetsbaar voor minimaal één probleem, de zogenaamde POODLE-aanval, bekend sinds oktober 2014⁹. Vindt U dit een probleem? Zo ja, wat gaat U daar aan doen? Zo nee, waarom niet?
14. Op de website werkenbijdegemeenteoss.nl kunnen persoonlijke gegevens ingevuld worden (zie bijvoorbeeld het formulier voor een stageplek¹⁰, inclusief uploaden CV/brief met daarin persoonlijke gegevens en persoonsgegevens). Deze website heeft geen beveiligde verbinding. Vindt U dit een probleem? Zo ja, wat gaat U daar aan doen? Zo nee, waarom niet?

Bij voorbaat dank voor de spoedige beantwoording van deze vragen.

Met vriendelijke groet,

Martijn Tonies,
namens de Socialistische Partij Oss

⁷ <https://www.oss.nl/gemeente/inwoners/parkeren-2/uw-parkeerkaart-1.htm>

⁸ <https://ossepas.permitonline.nl/gsmpark-www/login.html>

⁹ <https://www.us-cert.gov/ncas/alerts/TA14-290A>

¹⁰ <http://www.werkenbijdegemeenteoss.nl/stageplek.html>

Bijlage:

schermafdruk oss.nl (zonder www)

