



Blijf Stellingwarfs
dhr. I. Kehe

Gemeentehuis
Griffioenpark 1, Wolvega
Postadres
Postbus 60, 8470 AB Wolvega
Telefoon
140561
Fax
(0561) 61 36 06
Internet
www.weststellingwerf.nl
E-mail
info@weststellingwerf.nl

Wolvega, 20 juni 2022

Referentienummer: 0098156723
Documentnummer: 0098425397

Behandeld door S. Stuver,

Onderwerp: Vragen artikel 31 - ICT-beveiliging van Blijf Stellingwarfs

Geachte heer Kehe,

Op 31 mei jl. ontvingen wij een aantal schriftelijk vragen van u over de ICT-beveiliging van de gemeente Weststellingwerf. Een onderwerp dat de laatste tijd helaas steeds vaker in het nieuws is vanwege de enorme toename van beveiligingsincidenten. De gevolgen hiervan zijn steeds groter en naast de schending van privacy kunnen ze in sommige gevallen leiden tot ontwrichting van de samenleving.

Ook wij als college zijn ons ervan bewust dat wij als gegevensverwerkende organisatie risico's lopen voor de gegevens van onze burgers en organisatie en hebben de afgelopen jaren hier de nodige maatregelen voor getroffen. In een memo aan de raad van 4 november 2021, naar aanleiding van een schrijven van de VNG gericht aan de burgemeesters over informatiebeveiliging, hebben wij de raad geïnformeerd over de maatregelen die wij de afgelopen jaren hebben getroffen en blijven treffen om risico's tot een minimum te beperken.

Graag reageren wij middels deze brief op de door u schriftelijk gestelde vragen:

Uw schrijven:

Op 1 april werden de gemeenten Buren en Neder-Betuwe getroffen door een grote digitale hack. Honderdduizenden digitale bestanden (130GB) waren gestolen tijdens een ransomwareaanval begin welke worden aangeboden op het Dark web. De gemeente Buren meldde dat het gaat om o.a. 'gevoelige persoonsgegevens en vertrouwelijke informatie'. Criminelen claimen op het Dark web dat ze '5TB' aan gegevens hebben buitgemaakt. De hackers hebben naar eigen zeggen 'financiële informatie, contracten en gegevens van gemeentemedewerkers' buitgemaakt.

Vraag:

Is de gemeente Weststellingwerf bekend met dit voorval?

Antwoord:

Het college is op de hoogte van deze en eerdere voorvallen. Als gemeentelijke organisatie zijn wij aangesloten bij de IBD (Informatiebeveiligingsdienst voor gemeenten) die nauw samenwerkt met het NCSC (Nationaal Cyber Security Centrum) en wij zijn intern zo georganiseerd dat we snel kunnen

reageren op bedreigingen die worden gesignaleerd. Via deze platformen wordt eveneens de kennis gedeeld over actuele aanvallen en te treffen maatregelen.

Vraag:

Zo ja; welke ICT-maatregelen zijn er genomen om een dergelijke digitale dreiging tegen te kunnen gaan? En kunt u de veiligheid van de digitale gegevens van de Gemeente Weststellingwerf, haar medewerkers en haar inwoners (blijven) waarborgen?

Antwoord:

Naast de organisatorische maatregelen hebben wij technische maatregelen getroffen om onze ICT-infrastructuur tegen dreigingen van zowel buitenaf als binnenuit te weren. Bij deze maatregelen moet u denken aan firewalls, netwerk segmentering, policy rules, behaviour scanning en antivirus software. De grootste dreiging zit hem echter in menselijk handelen. Vanuit onze informatiebeveiliging kennen wij een continu bewustwordingsprogramma en worden onze medewerkers regelmatig getraind door middel van microlearnings en spam-trainingen. Daarnaast maken wij periodiek gebruik van ethical hacking om de door ons getroffen maatregelen te testen en worden wij jaarlijks geaudit op de maatregelen die wij op het gebied van informatiebeveiliging hebben getroffen (DigiD-audit en de BIO (Baseline Informatiebeveiliging Overheid)).

Vraag:

*Zo nee, is de gemeente Weststellingwerf ervan overtuigd dat dit onze gemeente niet kan overkomen?
En hoe kunt u dit maatstaven?*

Antwoord:

In 2015 is de OWO-samenwerking al eens een ransomware-aanval overkomen. De vraag is ook niet of dit ooit weer zal gaan gebeuren maar eerder wanneer. Wij doen het maximale om de gegevens van en over onze inwoners zo goed mogelijk te beschermen, maar kunnen niet garanderen dat wij niet zullen worden getroffen door een digitale aanval. Door onze maatregelen en procedures goed in te regelen verwachten wij in een dergelijk geval adequaat te kunnen reageren en te trachten de schade zo beperkt mogelijk te houden.

Vraag:

*Zijn we ons ervan bewust dat onze gemeente website een DANE-configuratiefout heeft ? *1
Zo nee, is de gemeente zich bewust dat hiermee alle gegevens van burgers openbaar zijn ?*

Antwoord:

De getroffen beveiligingsmaatregelen voor de gemeentelijke website scoort 100% conform de landelijk gestelde eisen. Wij zijn ons er van bewust dat voor het onderdeel DANE een waarschuwing wordt afgegeven. Het niveau van deze maatregel is echter optioneel. De inspanning die zowel eenmalig als structureel moet worden gedaan om dit te onderhouden weegt niet op tegen het risico dat wij hier mee lopen. Dit is de reden waarom wij deze optie niet hebben doorgevoerd.

Vraag:

*Zijn we ons ervan bewust dat onze gemeente webserver www.weststellingwerf.nl geen Content-Security-Policy (CSP) actief heeft? *2 Zo nee, elke login via DigiD is hiermee onveilig. Beseft men dit?*

Antwoord:

Uw veronderstelling is onjuist. Er is een CSP actief op het domein www.weststellingwerf.nl. Onze website wordt als SAAS-oplossing gehost door een externe partij. Deze wordt jaarlijks door een accountant onderworpen aan een audit en hierover dient een TPM (Third Party Melding) aan onze organisatie te worden overhandigd ten teken dat de beheers- en beveiligingsmaatregelen die zij hebben getroffen aan de landelijke voorschriften voldoet. Ons domein scoort 100% als het gaat om getroffen maatregelen (zie www.internet.nl).

Deze CSP kan echter wel strikter worden ingeregeld, echter gaat het in dat geval ten koste van de functionaliteit voor onze inwoners. Dit is de reden waarom hij op het huidige niveau is ingesteld.

Zodra een burger naar mijn.weststellingwerf.nl wordt doorverwezen, het digitale loket dat achter DigiD hangt, gelden er nog strengere eisen waar onze leverancier, zoals in de TPM gemeld, aan voldoet. Uw veronderstelling dat inloggen via DigiD hierdoor niet veilig is, is onjuist. DigiD wordt verplicht voor alle overheidsinstanties beheerd door Logius en voldoet aan de hoogste veiligheidseisen.

Vraag:

*Zo zijn er nog meer veiligheidsproblemen die simpel te herkennen en op te lossen zijn.
Wanneer gaat de gemeente hier maatregelen tegen nemen?*

Antwoord:

Onze organisatie maakt gebruik van gereedschappen die continue bedreigingen op onze ICT-infrastructuur detecteert. Deze worden voorzien van een classificatie High, Medium of Low risk. In de kadernota van 2023 en eerdere aanvragen is formatie aangevraagd voor uitbereiding voor ICT. Eén van de redenen daartoe is cybersecurity. De huidige inrichting van ons personeelsbestand op ICT dateert van begin van de OWO-samenwerking (2015). De enorme toename in onder andere beveiligingsproblematiek noodzaakt ons op dit moment alleen de High geclassificeerde bedreigingen op te pakken. Daarnaast drukt de VNG (Vereniging Nederlandse Gemeenten) ons op het hart om te blijven investeren in mensen en middelen om de gegevens van onze burgers zo goed mogelijk te blijven beschermen. Dit is ook de reden waarom wij hebben besloten vanaf de zomer van 2022 te gaan inhuren op deze functies. Daarnaast hebben wij vanaf 2023 een structurele invulling voor deze functies opgenomen.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,

Burgemeester en wethouders van Weststellingwerf,
de secretaris, de burgemeester,

