

Statenfractie PVV
t.a.v. de heer A. van Hattem
Postbus 90151
5200 MC 'S-HERTOGENBOSCH

Brabantlaan 1
Postbus 90151
5200 MC 's-Hertogenbosch
Telefoon (073) 681 28 12
Fax (073) 614 11 15
info@brabant.nl
www.brabant.nl
Bank ING 67.45.60.043



Onderwerp

Beantwoording vragen ex artikel 3.2 van het Reglement van Orde betreffende schriftelijke vragen ex art. 3.2 RvO inzake beveiliging provinciale website.

Geachte heer Van Hattem,

Bij brief van 13 oktober 2011, ingekomen op 14 oktober 2011, heeft u namens de PVV-fractie ingevolge artikel 3.2 van het Reglement van Orde voor Provinciale Staten meerdere vragen gesteld, te weten:

Geacht college,

Naar aanleiding van een bericht op Brabant Vandaag over een beveiligingsprobleem van de site van de provincie Noord-Brabant komt onze fractie tot de volgende vragen:

1. Bent u bekend met het bericht op Brabant Vandaag?¹
2. Welke stappen heeft u ondernomen om de beveiligingsproblemen aan te pakken?
3. In het artikel op Brabant Vandaag is het volgende te lezen:
“De beveiligingsproblemen zijn voor de provincie aanleiding binnenkort haar ICT-beleid nog eens goed onder de loep te nemen.”
Bent u bereid om niet ‘binnenkort’ maar onmiddellijk het ICT-beleid goed onder de loep te nemen? Zo nee, waarom niet?
4. Is er extra controle uitgevoerd op privacygevoelige onderdelen van de provinciale webruimte, zoals het intranet? Zo nee, waarom niet?
5. Zijn privacygevoelige of vertrouwelijke gegevens in databases, zoals mailboxen, getroffen door hack-acties? Heeft er extra controle

¹ <http://www.brabantvandaag.nl/nieuws/algemeen/2011-10-13/na-gemeenten-ook-site-provincie-noord-brabant-lek>

Datum

25 oktober 2011

Ons kenmerk

2822465

Uw kenmerk

schriftelijke vragen ex art.
3.2 RvO inzake
beveiliging provinciale
website

Contactpersoon

O.P. Vollinga

Directie

Middelen

Telefoon

(073) 681 25 35

Fax

(073) 681 28 44

Bijlage(n)

-

E-mail

OVollinga@brabant.nl

Het provinciehuis is vanaf het centraal station bereikbaar met stadsbus, lijn 61 en 64, halte Provinciehuis, met de treintaxi en met de OV-fiets.

plaatsgevonden of deze voldoende beschermd zijn? Zo nee, waarom niet?

6. Bent u voornemens om met regelmaat de nodige uitgebreide veiligheidscontroles uit te voeren op de provinciale websites? Zo nee, waarom niet?
7. Bij de recente beantwoording van de vragen van de PVV-fractie inzake Diginotar gaf u aan dat extra maatregelen niet nodig waren en dat Brabantse burgers er op kunnen vertrouwen dat de provinciale websites veilig zijn. Deelt u onze mening dat dit vertrouwen veel te lichtvaardig is ingeschat en er onvoldoende zorgvuldigheid is betracht rond de veiligheid van provinciale websites? Zo nee, waarom niet?
8. Hoe beziet u deze beveiligingsproblematiek in het licht van de ontwikkelingen op het gebied van papierloos werken en volledige elektronische dossiervorming? Welke beveiligingsrisico's brengt dit met zich mee en welke beveiligingsmaatregelen worden hiervoor genomen?

Datum

25 oktober 2011

Ons kenmerk

2822465

Namens de PVV Noord-Brabant,

Alexander van Hattem
Lid Provinciale Staten

Wij beantwoorden deze vragen als volgt.

1. *Bent u bekend met het bericht op Brabant Vandaag?*

Ja, wij zijn bekend met de berichtgeving op Brabant Vandaag.

2. *Welke stappen heeft u ondernomen om de beveiligingsproblemen aan te pakken?*

Naar aanleiding van onder meer de berichtgeving met betrekking tot de problemen met Diginotar zijn wij extra alert op dit soort situatie. De geconstateerde situatie is direct verholpen.

3. *In het artikel op Brabant Vandaag is het volgende te lezen: "De beveiligingsproblemen zijn voor de provincie aanleiding binnenkort haar ICT-beleid nog eens goed onder de loep te nemen." Bent u bereid om niet 'binnenkort' maar onmiddellijk het ICT-beleid goed onder de loep te nemen? Zo nee, waarom niet?*

Ja, wij hebben het ICT-beleid en meer specifiek de beveiliging direct onder de loep genomen en blijven dat ook doen.

4. *Is er extra controle uitgevoerd op privacygevoelige onderdelen van de provinciale webruimte, zoals het intranet? Zo nee, waarom niet?*

Ja, alle provinciale webruimtes zijn en worden gecontroleerd aan de hand van de richtlijnen van govcert.nl

5. *Zijn privacygevoelige of vertrouwelijke gegevens in databases, zoals mailboxen, getroffen door hack-acties? Heeft er extra controle plaatsgevonden of deze voldoende beschermd zijn? Zo nee, waarom niet?*

Voor zover wij kunnen constateren zijn er geen privacygevoelige of vertrouwelijke gegevens getroffen. Mailboxen die zijn geopend met een juiste user-id / password combinatie zien wij als regulier gebruik. Het is aan de gebruiker van de mailbox deze informatie voor zich te houden en geen standaard wachtwoorden te gebruiken.

Er is een extra controle uitgevoerd.

6. *Bent u voornemens om met regelmaat de nodige uitgebreide veiligheidscontroles uit te voeren op de provinciale websites? Zo nee, waarom niet?*

Ja wij zijn voornemens om met regelmaat uitgebreide veiligheidscontroles uit te (laten) voeren.

7. *Bij de recente beantwoording van de vragen van de PVV-fractie inzake Diginotar gaf u aan dat extra maatregelen niet nodig waren en dat Brabantse burgers er op kunnen vertrouwen dat de provinciale websites veilig zijn. Deelt u onze mening dat dit vertrouwen veel te lichtvaardig is ingeschat en er onvoldoende zorgvuldigheid is betracht rond de veiligheid van provinciale websites? Zo nee, waarom niet?*

Wij delen deze mening niet. In de situatie die zich heeft voorgedaan is het uiterlijk van de provinciale site in één specifieke sessie tijdelijk aangepast door een externe afbeelding in te voegen in het resultaat van een zoekactie op de zoekpagina. Er is geen beveiligde informatie naar buiten gebracht, geen informatie in de site veranderd en geen verbinding met achterliggende systemen gemaakt.

Datum

25 oktober 2011

Ons kenmerk

2822465

8. *Hoe bezielt u deze beveiligingsproblematiek in het licht van de ontwikkelingen op het gebied van papierloos werken en volledige elektronische dossiervorming? Welke beveiligingsrisico's brengt dit met zich mee en welke beveiligingsmaatregelen worden hiervoor genomen?*

Datum

25 oktober 2011

Ons kenmerk

2822465

Informatiebeveiliging is het afwegen van risico's en het nemen van tegenmaatregelen om te komen tot acceptabele situaties. Het volledig veilig maken van dossiers kan alleen door deze niet beschikbaar te stellen. Het op enigerlei wijze beschikbaar maken van dossiers brengt veiligheidsrisico's met zich mee. Het is niet alleen de techniek maar ook de menselijke factor die de zwakste schakel bepaalt. Wij kunnen als voorbeeld onze wachtwoord policy op de email toegang zo sterk maken dat deze 99% veilig is maar voorkomen daarmee niet dat email wordt doorgestuurd naar voor ons niet beheerbare omgevingen zoals Gmail. Ons streven is om de techniek zo veilig mogelijk te maken en om in aanvulling daarop de instructies van de gebruikers zo doeltreffend mogelijk te maken.

Gedeputeerde Staten van Noord-Brabant,

Voorzitter,

Secretaris,