RAADSINFORMATIEBRIEF met beantwoording artikel 42 vragen

Van
college van burgemeester en wethouders

Vergadering van
9 mei 2023

Kenmerk
Z/23/059230 / D/23/104448

Portefeuillehouder
Mariëtte Pennarts-Pouw

Portefeuille
Welzijn/WMO/integrale toegang Woerden Wijzer

Opsteller
Heiningen, José van

Onderwerp
Beantwoording vragen Splinter Schriftelijke vragen - Datalek Sociale Kracht

Beantwoording van de vragen

1. **Hoe is het mogelijk dat er sinds 5 april jongstleden een bericht op de gemeentelijke website staat, maar de gemeenteraad niet proactief geïnformeerd is door het college waardoor veel raadsleden het bericht pas op 7 april uit het Algemeen Dagblad hebben vernomen?**
   In het geval van een datalek heeft het informeren van de (mogelijk) direct getroffenen prioriteit.

2. **Klopt het dat het onderzoeksbureau Dimensus voor het onderzoek Sociale Kracht gebruik heeft gemaakt van Nebu software?**
   Dat klopt.

3. **Wanneer is het datalek door Dimensus gemeld aan de gemeente?**
   Op maandag 27 maart 2023, 17:34 uur, is een medewerker van de gemeentelijke organisatie per e-mail geïnformeerd over het datalek.

4. **Is het datalek door de gemeente na de melding door Dimensus binnen 72 uur gemeld bij de Autoriteit Persoonsgegevens?**
   Binnen 72 uur na de mededeling door Dimensus heeft de gemeente zelf melding gemaakt van het datalek bij de Autoriteit Persoonsgegevens (AP) en de Informatiebeveiligingsdienst (IBD).

5. **Is de gemeente bekend met het feit dat het datalek bij Nebu al op 10 maart jl. heeft plaatsgevonden en pas na 31 uur ontdekt werd?**
   Dit is bekend.

6. **Is de gemeente bekend met het feit dat het datalek pas weken na 10 maart gemeld is door Nebu?**
   Dit is bekend.

7. **Weet de gemeente wanneer Dimensus zelf door Nebu geïnformeerd is over de cyberaanval en het resulterende datalek?**
   Ja. In de melding aan de gemeente schrijft Dimensus dat zij op 23 maart 2023, 21:13 uur, zijn geïnformeerd door Nebu/Enghouse Systems.

8. **Op basis waarvan stelt de gemeente dat internetcriminelen ongeveer drie kwartier tot een uur toegang hebben gehad tot gegevens bij Nebu gezien de vorige vraag?**

De gemeente baseert dit op de berichtgeving rondom het kort geding tussen Nebu en Blaauw op 5 april en het directe contact tussen Dimensus en de gemeente Woerden.

Dit feit wordt nogmaals bevestigd in de interne incidentrapportage van Nebu.

9. **Op basis van welke experts baseert de gemeente het oordeel dat in beperkte tijd nooit veel gegevens gelekt kunnen zijn?**

Op basis van informatie gedeeld door Dimensus en interne beraadslaging met gemeentelijke specialisten op het gebied van informatiebeveiliging en privacy.

Uit de incidentrapportage van Nebu, gedeeld met de gemeente door Dimensus blijkt dat er mogelijk 4 – 5% van de totaal aanwezige data op de Nebu-servers is ontvreemd.

10. **Op basis van welke argumenten stelt de gemeente te denken dat de inwoners geen groot risico lopen gezien het feit dat niet bekend is welke gegevens gelekt zijn?**

Onder 'groot risico' verstaan wij de kans op identiteitsfraude, phishing, spam, financiële of emotionele schade. Over het algemeen maken internetcriminelen voor deze doeleinden gebruik van andere persoonlijke gegevens (bijvoorbeeld e-mailadressen en BSN-nummers) dan de gegevens die door Dimensus voor de Monitor Sociale Kracht zijn gebruikt.

Op basis van de huidige kennis is het niet aannemelijk dat kwaadwillenden de door ons beschikbaar gestelde gegevens van Woerdense inwoners gebruiken voor identiteitsfraude en dergelijke.

11. **Is er contact geweest met Dimensus om na te gaan welke gegevens zij naar aanleiding van het onderzoek Sociale Kracht in de Nebu omgeving heeft ingevoerd?**

Ja.

12. **Zo ja, wie is binnen de gemeente de contactpersoon aangaande dit datalek?**

De Informatiemanager Sociaal Domein a.i. is de gemeentelijke contactpersoon naar en voor Dimensus. De informatiemanager staat in nauw contact met de CISO (Chief Information Security Officer)en Functionaris Gegevensbescherming van de gemeente Woerden. Zij onderhouden het contact met andere partijen zoals de Informatiebeveiligingsdienst.

13. **Zijn de inwoners die mee hebben gedaan aan het onderzoek Sociale Kracht al via een brief geïnformeerd door de gemeente?**
Zo nee, op welke termijn gebeurt dit alsnog?

De inwoners die hebben meegedaan aan het onderzoek zijn nog niet per brief geïnformeerd. De gemeente heeft de wettelijke verplichting om slachtoffers van een datalek te informeren.

Zodra bekend is dat er daadwerkelijk persoonsgegevens zijn gestolen met betrekking tot de Monitor Sociale Kracht zullen de gedupeerden worden geïnformeerd.

14. **Is er door de gemeente contact opgenomen met andere gemeenten, zoals Den Haag, die (mogelijk) ook geraakt zijn door dit datalek?**

Wij hebben contact met omliggende gemeenten. Daarnaast hebben wij de Informatiebeveiligingsdienst ingelicht. Zij hebben andere gemeenten geïnformeerd.

Wij hebben zelf geen contact gehad met de gemeente Den Haag.

15. **Is de gemeente van plan of bereid om naar aanleiding van dit datalek preventief een onderzoek te laten uitvoeren naar zowel de eigen informatiebeveiliging en privacybescherming en als die van de leveranciers van de gemeente?**

Nee.

De gemeente doet al veel om de eigen informatiebeveiliging en privacybescherming te onderzoeken en te beschermen (zie hieronder en het antwoord op vraag 16).

Voor uitgebreidere onderzoeken bij leveranciers van de gemeente zijn onvoldoende middelen beschikbaar. Wel maken we met hen duidelijk afspraken over databeveiliging (zie het antwoord op vraag 16).

Eigen informatiebeveiliging

De gemeente voert elk jaar periodiek onderzoek uit naar de eigen informatiebescherming. In de eerste plaats wordt elk jaar een zelfevaluatie naar de Baseline

Informatiebeveiliging Overheid (BIO) uitgevoerd. Verder voert een externe auditor jaarlijks onderzoek uit naar risicomanagement, interne beheersing van de algemene ICT
beheersmaatregelen (ISAE3402 type II). De auditcommissie is op 22 februari 2022 geïnformeerd over de resultaten ten aanzien van het jaar 2021.
Dit jaar laten we aanvullend een onderzoek naar het risico van onze vier belangrijkste applicaties (application controls). De resultaten van de ISAE3402 2022 en
de application controls worden in het najaar gepresenteerd aan de auditcommissie.
De gemeente laat verder elk jaar ethische hackers kijken of ze kunnen binnendringen in onze systemen (penetratietest).
Daarnaast hebben we software die voortdurend alle verdachte netwerkactiviteiten monitort en een externe partij die hier indien nodig voor kan waarschuwen
en in actie kan komen.
Leveranciers van de gemeente
Met de huidige middelen is het onmogelijk om alle leveranciers van de gemeente en al hun leveranciers voortdurend te monitoren.
Wel is de gemeente al begonnen met een onderzoek naar de enquête. Dit onderzoek moet duidelijkheid geven over of wij bij de inkoop van dit soort enquêtes verdere
verbeteringen kunnen aanbrengen om dergelijke situaties te voorkomen.

16. **Welke maatregelen heeft de gemeente reeds geïmplementeerd als het gaat om het beschermen van de (persoons)gegevens van inwoners die door de gemeente beheerd worden?**

De gemeente stelt voorwaarden aan haar softwareleveranciers, dataverwerkers en subverwerkers over databeveiliging. Deze voorwaarden zijn gebaseerd op
ons informatieveiligheidsbeleid, gebaseerd op de BIO (Baseline Informatiebeveiliging Overheid). De BIO bestaat uit enkele honderden maatregelen die op basis van
risicomanagement worden beoordeeld. We zijn voortdurend bezig om te kijken welke maatregelen we gezien de beperkte middelen en tijd het meest effectief kunnen nemen.
Deze maatregelen vinden zowel op technisch als organisatorisch vlak plaats, op alle verschillende niveaus en bij organisaties waar onze gegevens zich bevinden.
We zijn altijd bereid dit in een besloten sessie verder toe te lichten.

Bijlagen
