Q&A raadsfracties n.a.v. mogelijk datalek

Van: Marc Roza (CISO)
Aan: Else Ruizeveld (gemeentesecretaris Eemnes), Roland van Benthem (pfh. (informatie)veiligheid Eemnes)
C.c.: Garmt Kolhorn (pfh. ICT Directieraad)
Datum: 12 december 2016
****

Q&A fractie Dorpsbelang

1) Is er een melding gedaan bij de Autoriteit Persoonsgegevens?

Ja, de gemeentesecretaris heeft voor het college van Eemnes op donderdag 1 december, binnen de 72-uurs termijn na melding vanuit de leverancier die hier voor staat, de melding van een mogelijk datalek aan de Autoriteit Persoonsgegevens gedaan.

2) Zijn de betrokkenen geïnformeerd, of is dat in dit geval niet nodig?

Op advies van de Informatiebeveiligingsdienst voor gemeenten (IBD) en in lijn met de acties van de andere getroffen gemeenten in Nederland zijn alleen via een algemene kennisgeving de inwoners, c.q. eigenaren en gebruikers van onroerende goederen van de gemeente Eemnes op de hoogte gesteld en geïnformeerd over de mogelijke gevolgen en zelf te nemen maatregelen. Het advies van de IBD wordt hierin gevolgd, omdat het niet bekend is of er data van eigenaren/gebruikers van onroerende zaken op de gestolen laptop stonden. Wanneer er eventueel data op stonden, is het niet bekend of die data te herleiden zijn naar welke betrokkenen precies. Het is een mogelijkheid, die helaas niet uit te sluiten valt.

3) Wat voor afspraken waren er gemaakt met de externe partij omtrent beveiliging van de gegevens?

De BEL Combinatie heeft sinds november 2015 een contract voor het uitvoeren van taxaties en het vullen van databestanden m.b.t. waardering van onroerende zaken, nodig voor o.a. het opleggen van ozb-aanslagen door de gemeente.

Het contract voldoet aan de Algemene Inkoopvoorwaarden van de BEL Combinatie, alleen stonden daar toen nog geen specifieke eisen in m.b.t. de informatieveiligheid.

4) Uit persbericht kwam naar voren dat het om een bedrijf ging voor waardebepaling van woningen. Waarom worden er dan BSN gegevens verstrekt ?

Het gaat om een bedrijf dat een aantal taken in opdracht van de gemeente uitvoert voor de waardebepaling van zowel woningen als niet-woningen. Daarbij is het uiteindelijk ook van belang dat deze waarden gekoppeld worden aan personen (via BSN-nummers) en bedrijven (via RSIN-nummers). Hiervoor wordt een standaard “gegevensbestand” gegenereerd. Over een paar weken is deze koppeling geheel geautomatiseerd (hetgeen al gepland was) en worden er geen losse bestanden meer onderling verstuurd.

5) Hoe regelt de BEL organisatie met externe partijen de ketenaansprakelijkheid. en specifiek in dit geval. M.a.w. zijn wij als gemeente verantwoordelijk ?

De gemeente is wettelijk gezien de 'verantwoordelijke' voor deze gegevensuitwisseling. De BEL Combinatie heeft als gemeenschappelijke regeling van drie gemeenten een verantwoordelijkheid voor een juiste verwerking van die data bij hun dienstverlening aan de inwoners van de 3 BEL-gemeenten.

6) Kan de gemeente een boete krijgen van de Autoriteit Persoonsgegevens en zo ja hoe groot kan die boete zijn?

In theorie kan de gemeente een boete krijgen. Op dit moment heeft nog geen enkele gemeente een boete gekregen van de Autoriteit Persoonsgegevens. Dit wil niet zeggen dat dit niet mogelijk is. De IBD geeft aan dat er mogelijk wel een onderzoek door de Autoriteit Persoonsgegevens kan volgen, maar dat het dan van belang is dat gemeenten hun datalek tijdig hebben gemeld (is gebeurd) en leren van dit incident door het vervolgens nemen van repressieve, corrigerende en preventieve maatregelen. Daar zijn wij nu druk mee bezig.

Ondanks het feit dat de Autoriteit Persoonsgegevens tot nu toe geen gemeente heeft beboet, geeft de IBD aan dat bij zo'n boete op € 10.000 per incident gerekend moet worden.

7) Hebben de medewerkers van de BEL organisatie privacy gevoelige gegevens op hun laptop/notebook/ipads?

Het beleid is dat medewerkers van de BEL Combinatie hun werk verrichten binnen het beveiligde netwerk van de BEL Combinatie. Zij kunnen dit ook vanuit een willekeurige werkplek (zoals thuis) benaderen, maar hiervoor is dan een 2-wegs authenticatie nodig om in te loggen, d.w.z. een gebruikersnaam en wachtwoord, alsmede een code die per SMS die naar de telefoon van de betreffende medewerker wordt gezonden.

Daarnaast hebben alle ambtenaren van de BEL Combinatie een ambtseed afgelegd, waarin onder andere staat aangegeven dat er vertrouwelijk met informatie zal worden omgegaan. En externe inhuurkrachten ondertekenen op hun eerste werkdag een geheimhoudingsverklaring met soortgelijke inhoud.

8) Zijn de gegevens van de laptops/notebooks/ipads versleuteld van de medewerkers van de BEL organisatie, zodat bij verlies/diefstal de data niet direct op staat ligt?

Medewerkers die werkzaamheden voor de BEL Organisatie uitvoeren worden geïnstrueerd geen data op hun laptops of iPads/iPhones op te slaan. Hiervoor kunnen zij op eenvoudige wijze van een willekeurige werkplek in een beveiligde omgeving inloggen. We zullen n.a.v. dit incident de controle op de uitvoering van dit beleid gaan intensiveren. Dit is één van de preventieve maatregelen volgend uit dit incident.

De BEL Combinatie is nu met een pilot bezig waarin getest wordt met mobiele apparatuur waarop geen enkele data meer kan worden opgeslagen. Daarmee worden ook situaties voorkomen waarin een medewerker zich niet aan het protocol houdt.

9) Uit persbericht kwam naar voren dat er software beschikbaar is om privacy gevoelige bestanden veilig uit te wisselen. Betekent dat vanaf heden alle privacy gevoelige bestanden via deze software gaan (en dus niet via mail, USB-stick etc)? Zijn hier ook audits op?

Een van de maatregelen die al in uitvoering was om het dataverkeer naar buiten toe veiliger te maken is het delen van informatie via de beveiligde samenwerkingsomgeving met Alfresco Share, dus niet meer via Dropbox, WeTransfer, usb-sticks of per mail.

Daarnaast zal voor de volgende aanslagenronde de koppeling tussen de OZB-belastingsoftware en de WOZ-waarderingssoftware geheel geautomatiseerd via beveiligde datalijnen plaatsvinden. Ook dit is nieuw en zal het dataverkeer een stuk veiliger maken.

De BEL Combinatie heeft een kwaliteitsteam dat audits en zelfevaluaties uitvoert. De BEL Combinatie is daarnaast bezig met bewustwordingstrainingen, zodat awareness ontstaat over het veilig opslaan en bewerken van data.