Informatiebeveiliging gemeenten

Terreinverkenning in 4 stappen

FAMO Congres:

Bedrijfsvoering in het sociaal domein!

Vlaardingen, 7 september 2016

Pieter Schraverus | Sr. Manager Cyber Security
Helmer Berkhoff | Sr. Manager Cyber Security
BDO Advisory

FAMO Federatie ...jouw netwerk!

BDO

Mogen wij ons voorstellen?

- Pieter Schraverus en Helmer Berkhoff

- *BDO branchegroep publieke sector*
- Een team van specialisten van en uit de publieke sector
- Informatiebeveiliging en privacy deskundigheid in heel NL

- Adviseurs en IT-auditors in hetzelfde team dus een integrale aanpak
- Experts in IB-trajecten: van risicoanalyses tot en met certificeringstrajecten

- Onze aanpak: pragmatisch en persoonlijk
- Informatisering is mensenwerk

Onderzoek: Informatiebeveiliging binnen gemeenten

- Tweede rapport van BDO over informatiebeveiliging
  - Vorig jaar Zorginstellingen, nu Gemeenten
- 75% geeft aan minstens 1 IB-incident te hebben gehad
- Overeenkomst Zorginstellingen en Gemeenten:
  - ICT redelijk op orde, medewerkers onvoldoende bekend met materie
- Verschillen Zorginstellingen en Gemeenten:
  - 75% Gemeenten heeft een Security Officer (beduidend meer dan in de Zorg)
    - **Echter: meer dan de helft heeft niet de juiste opleiding/achtergrond!**

'Slechts naar de letter voldoen aan wet- en regelgeving is niet voldoende'

Terreinverkenning in 4 stappen

1. Strengere regelgeving per 1-1-2016
   - Wet Bescherming Persoonsgegevens, Wet meldplicht Datalekken en een nog veel strengere regelgeving op komst: Europese Privacyverordening

2. Geen sturing van bovenaf
   - Geen regie vanuit Rijksoverheid

3. Datastroom groeit explosief
   - De transities in het sociaal domein hebben de privacygevoelige datastroom fors vergroot

4. ‘Smart city’ is de toekomst
   - Internet of Things

1. Strengere regelgeving per 1-1-2016

Bij de gemeente Utrecht lagen de gegevens van minimaal 5000 en maximaal 140.000 mensen op straat.
Foto: foto Peter Schoonen

Gemeente Utrecht kampte met groot datalek

Persoonsgegevens lagen op straat

Gisteren, 09:48 John Maes

UTRECHT - De persoonsgegevens van duizenden Utrechters zijn eerder dit jaar onbeschermd geweest door een zogeheten datalek bij de gemeente Utrecht.

In totaal stonden 316 pagina's met namen en bijbehorende burgerservicenummers op intranet. Het gaat om minimaal 5000 en maximaal 140.000 personen.

Dat blijkt uit stukken die zijn opgevraagd door De Telegraaf met een beroep op de Wet Openbaarheid Bestuur. De personen om wie het gaat zijn niet door de gemeente Utrecht in kennis gesteld.

Omdat de gegevens op het intranet stonden, zou het onwaarschijnlijk zijn dat de blootgestelde informatie werd ingezien en/of misbruikt. Bij de gemeente werken echter een kleine 4000 mensen.

Mogelijk misbruik van de persoonsgegevens was volgens de gemeente niet aantoonbaar maar valt tegelijkertijd ook niet uit te sluiten. Niet duidelijk is hoelang de gegevens in te zien waren.

Kwaadwillenden kunnen identiteitsfraude plegen met de combinatie BSN en naam, adres en woonplaats. De (im-) materiële schade valt dan niet te overzien.

3.400 DATALEKKEN GEMELD NA INVOERING MELDPLICHT

Koos Tervooren
Gisteren, 16:56

Foto: ANP

▶ **LUISTER** Wilbert Tomesen over datalekken

In 2016 zijn er tot nu toe 3.400 datalekken gemeld aan de Autoriteit Persoonsgegevens. Sinds 1 januari dit jaar is er een meldplicht voor bedrijven en organisaties.

Wilbert Tomesen, vicevoorzitter van de Autoriteit Persoonsgegevens vindt het aantal meldingen niet hoog. In Nederland zijn er volgens de vicevoorzitter in Nederland 135.000 instanties die omgaan met persoonsgegevens en potentieel door een lek kunnen worden getroffen. 'Dan is 3.400 weinig'

De meldplicht is er zodat 'bedrijven er vooral open over zijn', zegt Tomesen.

Utrecht

Bij de gemeente Utrecht waren er onlangs dagenlang gevoelige persoonsgegevens in te zien door medewerkers van de gemeente.

In de intranet-omgeving van de gemeente kregen medewerkers toegang tot een beveiligd gedeelte, waar ze normaal niet kunnen komen. Daar staan 316 pagina's met namen en bijbehorende BSN-nummers vermeld.

De Telegraaf heeft het lek in Utrecht via een Wob-verzoek moeten opvragen. Het lek werd dus niet door de gemeente zelf naar buiten gebracht. Tomesen wil niet zeggen of hij de gemeente Utrecht daarom een boete gaat opleggen. Wel kan hij zeggen dat er dit jaar nog geen enkele boete is opgelegd.

Van hoeveel personen de gegevens te zien waren, weet de gemeente Utrecht niet. *De Telegraaf* meldt dat het om 4.000 tot 140.000 mensen gaat. Het datalek is inmiddels gemeld bij de Autoriteit Persoonsgegevens.

1. Strengere regelgeving per 1-1-2016

Wat speelt er?

- Wet Bescherming Persoonsgegevens: Strengere regelgeving per 1-1-2016 (Wet meldplicht datalekken)
- Nog veel strengere regelgeving op komst (Europese Privacy verordening)

1. Strengere regelgeving per 1-1-2016

Wat zien wij?

- Gemeenten hebben data nodig om de rechtmatigheid van hun zorginkoop aan te kunnen tonen
- Gemeenten dienen een privacy commissie te benoemen ter beoordeling van data-incidenten
- Gemeenten en zorginstellingen moeten bewerkingsovereenkomsten met elkaar aangaan m.b.t. hun onderlinge datastroom

2. GEEN STURING ‘VAN BOVENAF’

2. GEEN STURING ‘VAN BOVENAF’

Wat speelt er?

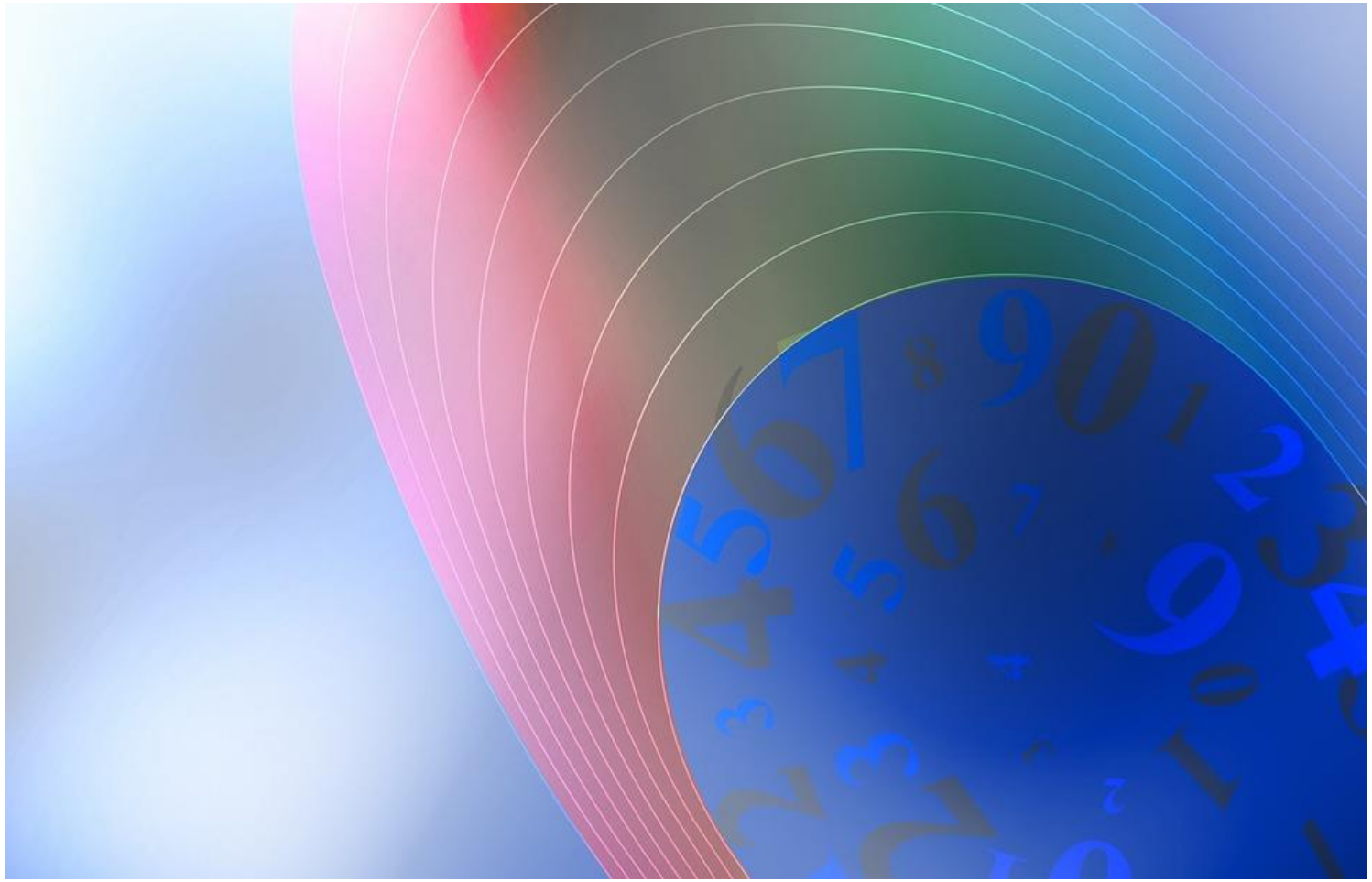
- Geen standaarden, geen protocollen
- AP: ‘Er is te weinig sturing vanuit Den Haag’
- De menselijke kant van de beveiliging

2. GEEN STURING ‘VAN BOVENAF’

Wat zien wij?

- Slechts 20% van de deelnemende gemeenten is gecertificeerd volgens ISO 27001
- ISO-certificering werkt om te voldoen aan BIG (BIG blijft achter)
- De helft van de benoemde Security Officers heeft geen achtergrond in informatiebeveiliging
- Een goede Security Officer met volledige steun van de organisatietop is van vitaal belang

3. DATASTROOM GROEIT EXPLOSIEF…



3. DATASTROOM GROEIT EXPLOSIEF…

Wat speelt er?

- Transities in het sociaal domein hebben de privacygevoelige datastroom fors vergroot
  - Wonen / Zorg / Gemeente
- AP: Gemeenten onvoldoende bekend met persoonsgegevens en regelgeving
- Vertrouwen vanuit burgers staat onder druk

3. DATASTROOM GROEIT EXPLOSIEF…

Wat zien wij?

- Gemeenten hebben data nodig om de rechtmatigheid van hun zorginkoop aan te kunnen tonen
- Menig gemeente vraagt veel te veel data op om controle te kunnen verzekeren, met alle privacy-issues van dien
- Gemeenten en zorginstellingen moeten bewerkingsovereenkomsten met elkaar aangaan m.b.t. hun onderlinge datastroom
- Door ‘datasamenwerking’ uit te breiden naar woningcorporaties, kunnen gemeenten regie voeren op een hoger niveau

4. …EN GROEIT STRAKS NOG VEEL SNELLER!

4. …EN GROEIT STRAKS NOG VEEL SNELLER!

Wat speelt er?

- Inspirerend toekomstbeeld: Internet of Things
  - Stedelijk beheer
  - Toezicht (veiligheid)
  - Verlichting
  - Et cetera

- Toename mogelijke data safety issues

- Klaar voor de toekomst?
  - Privacy by design
  - Competenties van medewerkers

4. …EN GROEIT STRAKS NOG VEEL SNELLER!

Wat zien wij?

- Mensen zijn cruciaal bij de beveiliging van gegevens
- Op het gebied van screening, gedragscodes en awareness hebben gemeenten een achterstand op het bedrijfsleven
- Slechts 40% van de onderzochte gemeenten heeft intern een awareness programma uitgerold
    - Awareness moet bij gemeenten bovenaan de agenda komen

Vragen?

Interesse in het rapport?

Laat uw e-mailadres achter op de intekenlijst.

Contactgegevens:

Pieter.Schraverus@BDO.nl

Helmer.Berkhoff@BDO.nl