



Informatieveiligheid Gemeente Lansingerland

14 februari 2018

Martin Buitelaar



Agenda

- Introductie
- Terugblik 2017
- Rekenkamer onderzoek
- Vooruitblik 2018
- Afsluiting

12 februari 2018



Informatiebeveiliging

Belangrijkste doel: beschermen persoonsgegevens

Dit vraagt om informatieveiligheid

Belangrijk, heeft continue aandacht

Extra aandacht vanwege Algemene Verordening
Gegevensbescherming

Informatiebeveiliging valt of staat met mensen

Mensen zijn de zwakste schakel
(maatregelen omzeilen)



Maar ... mensen kunnen ook de ontbrekende schakel zijn
(gaten opvangen / maatregelen versterken)



Bewustzijn: een gewaarschuwd mens telt voor twee!

Complexiteit

- +/- 300 applicaties, waarvan +/- 75 met persoonsgegevens
- Veel processen waarin persoonsgegevens gebruikt moeten worden om wettelijke taken uit te voeren
- 400 medewerkers
- Tientallen leveranciers, samenwerkingsverbanden, etc.
- BIG: 114 beheersmaatregelen / 303 maatregelen
- AVG: grote uitdaging voor ons én de rest van Europa

Stand van zaken implementatie BIG

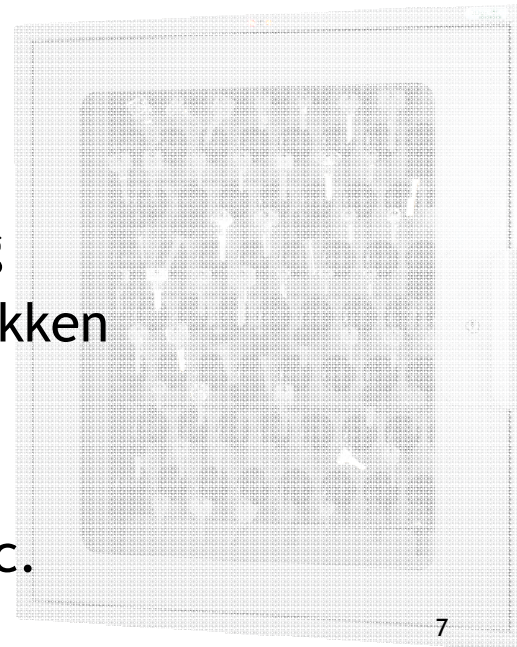
- BIG gap analyse: 174 van 303 maatregelen geïmplementeerd
- Risico inventarisatie en evaluatie: selectie 57 maatregelen
- Implementatie projectmatig opgepakt
- Benodigde procedures, etc. opgesteld en vastgesteld
- Sinds december focus op bewustwording, implementatie en borging.

12 februari 2018

Voorbeelden maatregelen implementatie BIG

- Controle autorisaties
- Wijzigingsbeheer
- In- en uit dienst en doorstroming
- Afhandelen incidenten en datalekken
- Bewustwording!
- Toegangsbeleid
- Procedures backup, antivirus, etc.

12 februari 2018



Aanbevelingen Rekenkamer

- Aanpak
 - Van compliance based naar risk based
- Bevindingen penetratietests en inlooptest
 - Bevindingen oppakken
 - Bewustwording!
 - Hertesten na max. 1 jaar.
- Voorkomen slordig omgaan met vertrouwelijke informatie
- Beveiliging applicaties



Risk based aanpak

- Diepgaande risico analyse sociaal domein
- Bepalen scope & planning overige domeinen
 - Op basis van dataclassificatie en uitkomsten privacy workshop sept. 2017
- Uitvoeren overige domeinen

Bewustwording

- Campagne
 - Er zijn in verleden meerdere campagnes gevoerd
 - Campagne “Bewust Informatie Gebruiken (BIG)” loopt sinds december
 - Aandacht voor punten uit rekenkamer rapport
 - Effectiviteit meten: door hertest
- Opnemen in introductie nieuwe medewerkers
 - Handout en presentatie tijdens introductieprogramma
- Training medewerkers via e-learning
- Bespreken in afdelings- en teamoverleggen
- Actief informatie delen @Work
- Introductieprogramma raad (bijv. <https://laatjeniethackmaken.nl/>)



Bevindingen penetratietests en inlooptest

- Externe pentest
 - één oplossing nog testen en activeren
 - rest opgelost
- Interne pentest:
 - één update en één wijziging nog uit te rollen door leverancier (eind feb)
 - een item complex; meenemen in TOPwerken
 - rest opgelost (al dan niet met alternatieve maatregelen)
- Inlooptest
 - Bewustwordingscampagne en hertest

Conclusie

- Veelomvattend en complex
- Vereist structureel aandacht
- Mensen en middelen randvoorwaardelijk
- Risico analyse geeft inzicht in te treffen maatregelen
- Planning

	2017				2018			2019	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	
Implementatie BIG									
Opstellen procedures, etc.		x	x	x					
Implementatie procedures, borging & aantoonbaarheid					x	x	x		
Updaten en vaststellen beleid							x	x	
Bepalen implementatieplan (2018-2019)							x	x	
Uitvoeren implementatieplan								x	x
Aandachtspunten rekenkamer onderzoek									
Onderzoek			x	x					
Risk based aanpak									
Diepgaande risicoanalyse sociaal domein						x			
Scope en planning overige domeinen						x			
Uitvoeren						x	x	x	x
Bevindingen externe en interne pentest en inlooptest									
Zaken als "incidenten" oplossen				x	x				
Complexe wijzigingen (impact bepalen, etc.)					x	x	x	x	x
Voorkomen slordig omgaan met vertrouwelijke info (volgt o.a. uit risico analyses)						x	x	x	x
Bewustwording									
Campagne (incl. bevindingen social engineering test)					x	x	x	x	
Introductie nieuwe medewerkers						x	x	x	
E-learning training medewerkers						x	x	x	
Bespreken in team- /afdelingsoverleggen					x	x	x	x	
Hertest (social engineering, interne + externe pentest)							x		
ENSIA									
Zelfevaluatie BRP, PUN			x						
Zelfevaluatie BIG (incl. DigiD, Suwinet, BAG, BGT)				x					
Collegeverklaring & IT-audit					x	x			
Uploaden assurance report en collegeverklaring						x			
Verantwoording richting raad (mei)						x			

Planning

Vragen?



12 februari 2018

14

