EMBARGO tot woensdag 20 december 2017

Rekenkamer
LANSINGERLAND

PERSBERICHT **Lansingerland, 19 december 2017**

gevoelige gegevens niet veilig bij gemeente

Het belang van gemeenten om de informatiebeveiliging op orde te hebben en weerbaar te zijn tegen cybercrime is aanzienlijk toegenomen. Gemeenten hebben immers door de decentralisaties in het sociaal domein meer (bijzondere) persoonsgegevens in beheer. Uit onderzoek van de Rekenkamer Lansingerland blijkt dat (bijzondere) persoonsgegevens bij de gemeente Lansingerland onvoldoende in veilige handen zijn. De beveiliging van digitale informatiesystemen tegen aanvallen van binnenuit schiet tekort, de fysieke beveiliging van de kantoorlocatie faalt en er is een tekort aan 'social & security awareness' bij medewerkers Dit en meer schrijft de Rekenkamer Lansingerland in haar rapport 'Wat niet weet, maar wel deert. Onderzoek beveiliging van gevoelige informatie.'.

Gemeenten hebben als gevolg van de decentralisaties in het sociaal domein steeds meer (bijzondere) persoonsgegevens in beheer. Ook wordt steeds meer informatie digitaal opgeslagen en overgedragen en worden systemen en data steeds vaker aan elkaar gekoppeld. Het belang van gemeenten om de informatiebeveiliging op orde te hebben en weerbaar te zijn tegen dreigingen als cybercrime is als gevolg van deze ontwikkelingen aanzienlijk toegenomen.

Uit onderzoek van de rekenkamer blijkt dat gevoelige informatie, zoals (bijzondere) persoonsgegevens, over het algemeen onvoldoende in veilige handen is bij de gemeente Lansingerland. Digitale informatiesystemen zijn onvoldoende beveiligd voor aanvallen van binnenuit. Ook de beveiliging van drie applicaties, die vaak worden gebruikt in het sociaal domein, schiet tekort. De fysieke beveiliging van de kantoorlocatie faalt en is er te weinig 'social & security awareness' bij medewerkers. Beveiligingsmaatregelen volgen niet uit systematische en actuele risicoanalyses, hoewel het beleid van de gemeente deze analyses wel voorschrijft. De personele en financiële capaciteit voor informatieveiligheid wordt, in navolging van het gemeentelijke beleid, ingezet voor de implementatie van bepaalde beveiligingsnormen die slechts een basisniveau van beveiliging bieden. Voor 75 applicaties, waaronder de drie genoemde applicaties, geeft dit beveiligingsniveau echter onvoldoende bescherming tegen misbruik of verlies van data.

Door de tekortschietende informatiebeveiliging bestaan er reële risico's op identiteitsfraude, misbruik van publieke middelen en 'datalekken'. Hierdoor kan de effectiviteit van gemeentelijk beleid en het vertrouwen in de overheid onder druk komen te staan. De rekenkamer heeft onder meer aanbevolen om veiligheidsrisico's, in plaats van de beveiligingsnormen, centraal te stellen bij de inrichting van de informatiebeveiliging. Ook heeft de rekenkamer aanbevolen om alle in het onderzoek aangetoonde kwetsbaarheden in de beveiliging, te dichten.

Naar aanleiding van het rapport van de rekenkamer heeft het college aangegeven alle conclusies te onderschrijven en alle aanbevelingen van de rekenkamer over te nemen. Het college is voornemens om informatiebeveiliging risicogericht te organiseren en de concrete kwetsbaarheden die zijn aangetroffen in het onderzoek op korte termijn te verhelpen.

Noot redactie: 20 december 2017 is het rapport digitaal beschikbaar: www.rekenkamer.rotterdam.nl.
Informatie: Rekenkamer Lansingerland, tel. 010 - 267 22 42.