Rekenkamer
ROTTERDAM

Meent 94
t 010 • 267 22 42

Postbus 70012
3000 KP Rotterdam

info@rekenkamer.rotterdam.nl
www.rekenkamer.rotterdam.nl

Gemeente Rotterdam
d.t.k.v. de Griffie
Gemeenteraad
Coolsingel 40
3011 AD ROTTERDAM

datum
8 mei 2017

ons kenmerk
R.O.17.071/PH/RW/EL

betreft
nawoord nagekomen reactie college informatiebeveiliging

Geacht raadslid,

Op 12 april 2017 ontving u van het college een aanvullende bestuurlijke reactie op het op 6 april jl. door de Rekenkamer Rotterdam gepubliceerde rapport over de informatiebeveiliging ('In onveilige handen'). Omdat deze reactie is verschenen na publicatie van het rapport, hebben we deze vanzelfsprekend niet (zoals gebruikelijk) in het rapport van een nawoord kunnen voorzien. Via deze weg ontvangt u alsnog dit nawoord.

Het stemt de rekenkamer tot tevredenheid dat het college de conclusies en aanbevelingen van de rekenkamer grotendeels overneemt. Het onderkent daarmee dat er problemen zijn met de informatiebeveiliging en de daaraan verbonden risico's. Aan de andere kant wordt naar het oordeel van de rekenkamer de ernst van de uitkomsten nog wel te veel gerelativeerd. Zo benadrukt het college dat de kwetsbaarheden in de informatiebeveiliging vooral intern en niet extern liggen. Dat is inderdaad uit het rekenkameronderzoek gebleken, maar louter op basis van de vaststelling dat het de onderzoekers niet is gelukt binnen enkele dagen van buitenaf (via het internet) in de gemeentelijke informatiesystemen binnen te dringen. Dat betekent níet dat de Rotterdamse systemen tegen externe inbreuken volledig veilig zijn. Een vasthoudende hacker neemt wellicht langer de tijd. r.O.Bovendien kan via 'social engineering' (zoals het sturen van phishing mails) alsnog van buitenaf in de Rotterdamse systemen gekomen worden. Juist op dit laatste punt is de gemeente kwetsbaar, zo blijkt uit het onderzoek. Kortom, ook de beveiliging voor bedreigingen van buitenaf behoeft blijvende aandacht.

Een tweede voorbeeld van de onterechte relativering betreft het feit dat de door de rekenkamer ingehuurde hackers (of: pentesters) zijn gelokaliseerd en betrapt. Dit is correct, maar met de door de pentesters gehanteerde technieken was die kans normaal gesproken ook vrij groot. Met de gekozen methode werd geprobeerd zoveel mogelijk kwetsbaarheden bloot te leggen. Dat laat veel sporen na, waardoor hackpogingen gemakkelijker worden gedetecteerd. Een werkelijk kwaadwillende hacker zal voor een methode kiezen die zo weinig mogelijk sporen nalaat. Verder hadden de pentesters op het moment van de onderbreking al cruciale informatie verzameld om op een later moment (en op een andere locatie) verder te gaan.

Rekenkamer
ROTTERDAM

Ten derde benoemt het college diverse maatregelen die de afgelopen jaren zijn genomen, zoals het vrij maken van extra geld en een formatie-uitbreiding. Het college vermeldt daar niet bij dat de extra toegekende middelen en formatie aanzienlijk minder waren dan vanuit het ambtelijk apparaat nodig werd geacht. Los hiervan hebben deze extra middelen klaarblijkelijk niet geleid tot een goede informatieveiligheid.

Evenzo blijkt uit het rekenkameronderzoek dat voor zover er maatregelen zijn genomen om de reeds in 2015 bekende tekortkomingen aan te pakken, deze in ieder geval niet effectief zijn gebleken. Dat 16 van de 21 door een extern bureau vastgestelde bevindingen zijn opgelost, zoals het college nu meldt, is op zich zelf een groot aantal. Maar dat laat onverlet dat door de rekenkamer vastgestelde kwetsbaarheden ook reeds in 2015 bekend waren. De informatieveiligheid is dus ondanks alle eventueel genomen maatregelen in de tussentijd niet voldoende verbeterd.

Ten slotte bevat de reactie van het college diverse voornemens en plannen om de informatiebeveiliging te verbeteren. Zo komt er een apart investeringsprogramma. Dat is een goede zaak, maar de rekenkamer had eigenlijk verwacht dat – gelet op de ernst van de bevindingen en de conclusies van de rekenkamer – het college óók had aangegeven de beveiligingslekken meteen of anders op de kortst mogelijke termijn te zijn gaan dichten. In plaats daarvan worden vooral nieuwe plannen en maatregelen in het vooruitzicht gesteld en heeft het college in een brief aan de raad van 23 maart aangegeven nog zeker zestig dagen nodig te hebben; terwijl de kwetsbaarheden uit de test van de rekenkamer al op 26 oktober 2016 aan de gemeente zijn gemeld. Hieruit spreekt niet de urgentie die volgt uit de conclusies in het rekenkamerrapport. De zorgen van de rekenkamer over de veiligheid van de gegevens die de Rotterdamse burgers aan de gemeente heeft toevertrouwd, zijn nog niet weggenomen.

Met vriendelijke groet,

Drs. P. Hofstra RO CIA
directeur