EMBARGO tot maandag 5 februari 2018, 12:00 uur

Rekenkamer ROTTERDAM

PERSBERICHT

Rotterdam, 2 februari 2018

beveiliging gevoelige gegevens sterk verbeterd

In april 2017 publiceerde de Rekenkamer Rotterdam het onderzoeksrapport 'In onveilige handen'. Uit dit rapport bleek dat gevoelige informatie bij de gemeente onvoldoende veilig was. Recente testen leren dat de gemeente haar informatiebeveiliging sindsdien heeft verbeterd. Het is de rekenkamer, in tegenstelling tot het vorige onderzoek, niet gelukt om toegang te krijgen tot gevoelige persoonsgegevens. Dit en meer concludeert de Rekenkamer Rotterdam in een brief aan de gemeenteraad.

De Rekenkamer Rotterdam heeft op 6 april 2017 het rapport 'In onveilige handen' gepubliceerd. In dit rapport constateerde de rekenkamer een tekortschietende beveiliging van digitale informatiesystemen, een falende beveiliging van kantoorlocaties en een tekort aan beveiligingsbewustzijn bij medewerkers. Tijdens de behandeling van het rapport door de gemeenteraad heeft de rekenkamer aangekondigd in 2017 de beveiliging opnieuw te testen, om vast te stellen of de gemeente haar beveiliging inmiddels heeft verbeterd. Een gespecialiseerd bureau heeft deze testen uitgevoerd in november en december 2017.

Op basis van de testen concludeert de rekenkamer dat de beveiliging inderdaad sterk is verbeterd. Anders dan tijdens het vorige onderzoek, is het niet gelukt om toegang te krijgen tot informatiesystemen met gevoelige (persoons)gegevens. Ook kwamen onderzoekers niet in een positie om identiteitsfraude te plegen, de fysieke veiligheid van politiek-bestuurlijke ambtsdragers aan te tasten of de openbare orde en publieke dienstverlening te verstoren.

Dat de resultaten van de testen positief uitpakken, is geen toeval. Naar aanleiding van het rekenkamerrapport is de gemeente namelijk een verbeterprogramma gestart. Onderdeel van dit programma was een campagne om de bewustwording van informatieveiligheid onder medewerkers te vergroten. Ook zijn technische maatregelen getroffen, zoals betere beveiliging tegen kwaadaardige software en netwerkpoortbeveiliging.

Tijdens de testen constateerde de rekenkamer dat deze maatregelen effectief waren. Zo bleken medewerkers nauwelijks gevoelig voor 'voice phishing', waarbij zij telefonisch worden verleid om wachtwoorden af te geven. Technische kwetsbaarheden, die naar voren kwamen in het vorige onderzoek, waren inmiddels verholpen. Hackpogingen van de onderzoekers werden door nieuwe beveiligingssoftware in een vroeg stadium ontdekt.

Op één terrein schoot de beveiliging nog wel te kort. Ondanks extra beveiligingsmedewerkers bleek het nog steeds mogelijk om zonder toestemming kantoorpanden binnen te dringen. Deze lacune in de beveiliging kan onder andere worden gedicht door het dragen van duidelijke zichtbare passen en beter toezicht. De rekenkamer doet verder de aanbeveling om, bij het dichten van technische kwetsbaarheden, voort te gaan op de ingeslagen weg Ook beveelt ze aan om door trainingen te blijven werken aan het beveiligingsbewustzijn van medewerkers.

Het college onderschrijft de conclusies van de rekenkamer en neemt alle aanbevelingen over. De rekenkamer zal de implementatie van de aanbevelingen de komende jaren nauwlettend blijven volgen.

Noot redactie:
De brief 'vervolgonderzoek informatiebeveiliging' is vanaf 5 februari 12.00 uur digitaal beschikbaar op www.rekenkamer.rotterdam.nl. Voor meer informatie kunt u contact opnemen via tel. 010-2672242.