Rekenkamer
ROTTERDAM

Meent 94
t 010 • 267 22 42

Postbus 70012
3000 KP Rotterdam

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

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

datum
5 oktober 2016

ons kenmerk
RR/16.078/PH/RW/CS

pagina
1 van 2

betreft
onderzoek informatiebeveiliging

Geacht raadslid,

Momenteel is de rekenkamer, mede op uw verzoek, een onderzoek aan het verrichten naar de informatiebeveiliging in de gemeente Rotterdam. De opzet van dit onderzoek heb ik u op 9 mei 2016 doen toekomen. Eén van de daarin opgenomen onderdelen is een test of het mogelijk is oneigenlijke toegang tot Rotterdamse informatiesystemen te krijgen. Via deze brief wil ik u aanvullend aan de opzet informeren over de wijze waarop de rekenkamer dit gaat aanpakken.

Als eerste zal de rekenkamer een zogeheten penetratietest (laten) uitvoeren. Die bestaat uit drie componenten. Er wordt geprobeerd om van buitenaf ongeoorloofd de Rotterdamse systemen binnen te dringen ("white hat hacking"). Daarnaast zal worden getest of het mogelijk is om van binnenuit oneigenlijke toegang tot bepaalde informatie te krijgen. In dat geval wordt met een speciaal voor deze test aangemaakt regulier gebruikersaccount geprobeerd bepaalde systemen binnen te dringen, terwijl het betreffende account daarvoor geen rechten heeft. Deze zogeheten "grey hat hacking" wordt toegepast op enkele "kroonjuwelen", dat wil zeggen informatiesystemen met veel gevoelige (persoons)gegevens, zoals de informatiesystemen in het sociaal domein. Een derde element van de penetratietest is te beoordelen of het mogelijk is oneigenlijke toegang tot specifieke e-mail- en agendagegevens te krijgen. Overigens is anderhalf jaar geleden ook, in opdracht van de gemeente zelf, een penetratietest uitgevoerd. De rekenkamer zal bij haar test de toenmalige uitkomsten betrekken, onder meer door te kijken of de destijds gesignaleerde tekortkomingen inmiddels afdoende zijn verholpen.

De uitkomsten van een penetratietest geven een beeld van de mate waarin er technisch-fysieke risico's op oneigenlijke toegang en gebruik van informatiesystemen bestaan. In het kader van informatiebeveiliging is het beheersen van de menselijke risico's minstens even belangrijk. Immers, er kunnen allerlei fysieke en procedurele beheersingsmaatregelen zijn genomen, maar de gebruikers moeten wel op adequate wijze hiermee omgaan. Om dit aspect te onderzoeken, wordt een "social engineering test" uitgevoerd. Deze test bestaat vooralsnog uit de volgende componenten:

1. Versturen van phishing e-mails, waarbij medewerkers van de gemeente Rotterdam een algemene e-mail ontvangen met een link waarbij gevraagd wordt

erop te klikken. Daarna wordt verzocht om hun gebruikersnaam en wachtwoord in te voeren.
2. Versturen van een spear-phishing mail naar een groep medewerkers waarbij een bijlage met malware (kwaadaardige software) is gevoegd. Na klikken hierop verkrijgen de onderzoekers toegang tot de werkplek van de medewerker.
3. Uitvoeren van een USB-drop, waarbij met malware besmette USB sticks worden verspreid en duidelijk wordt of nieuwsgierigheid het wint van veiligheidsbewustzijn (en of computers kunnen worden geïnfecteerd).
4. Uitvoeren van voice-phishing waarbij via de telefoon om vertrouwelijke gegevens wordt gevraagd uit de kroonjuwelen die extra aandacht hebben in het onderzoek.
5. Uitvoeren van een inlooptest waarbij één of meerdere mystery guests proberen locaties te betreden waartoe zij eigenlijk geen toegang (behoren te) hebben.

Voor de uitvoering van deze testen maakt de rekenkamer gebruik van een gespecialiseerd bedrijf dat niet eerder voor de gemeente Rotterdam opdrachten heeft vervuld. De uitvoering gebeurt in nauw en doorlopend overleg met het concern. Daarbij zal er voor worden gewaakt dat met de penetratietest kritische bedrijfsprocessen worden verstoord. Indien er urgente en grote beveiligingsrisico's worden aangetroffen, wordt dit meteen met de voor informatiebeveiliging verantwoordelijke afdeling gedeeld. In het geval van de social engineering test zullen afspraken worden gemaakt ten aanzien van de bescherming van de betreffende ambtenaren. Mocht bijvoorbeeld blijken dat medewerkers onbedoeld oneigenlijke toegang verschaffen, dan wordt alleen vastgelegd dat dit gebeurt en niet door wie. Voorafgaand aan beide testen zullen er vrijwaringsovereenkomsten tussen de gemeente Rotterdam, de Rekenkamer Rotterdam en het uitvoerend bureau worden afgesloten.

De uitvoering van de testen vindt in oktober en november 2016 plaats. De uitkomsten zullen onderdeel uitmaken van de uiteindelijke rapportage, waarvan de publicatie is gepland in februari 2017.

Ik hoop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

Drs. P. Hofstra RO CIA
Directeur

c.c. College van B en W, de heer A.L.H. Visser
c.c. De heer P.F.M. Raets, gemeentesecretaris