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 februari 2018

ons kenmerk
RR/18.005/PH/RW/EL

pagina
1 van 6

betreft
vervolgonderzoek informatiebeveiliging

Geacht raadslid,

De Rekenkamer Rotterdam heeft op 6 april 2017 het rapport 'In onveilige handen' gepubliceerd. In dit rapport werd geconcludeerd dat gevoelige informatie bij de gemeente onvoldoende in veilige handen was. De rekenkamer constateerde een tekortschietende beveiliging van digitale informatiesystemen voor aanvallen van binnenuit, een falende fysieke beveiliging van meerdere kantoorlocaties en een tekort aan benodigde 'social & security awareness' bij medewerkers. Deze kwetsbaarheden kwamen naar voren in een zogeheten penetratietest en social engineering test, uitgevoerd door een gespecialiseerd bureau. Veel van de geconstateerde kwetsbaarheden waren reeds 1,5 jaar bekend bij de gemeente.

In zijn reactie op het rapport heeft het college aangegeven dat er in het kader van de opvolging van de aanbevelingen een verbeterprogramma zal worden opgesteld. De rekenkamer heeft in haar nawoord aangekondigd de uitvoering van dit programma de komende jaren nauwlettend volgen. Tijdens de behandeling van het rapport door de Commissie Veiligheid, Organisatie en Financiën op 18 mei 2017 heeft de rekenkamer tevens aangekondigd dat in dit kader in 2017 opnieuw een penetratietest en social engineering test wordt uitgevoerd. Door middel van deze testen wil de rekenkamer vaststellen in hoeverre de gemeente haar beveiliging inmiddels heeft verbeterd. De raad moet er immers vanuit kunnen gaan dat de tekortkomingen dit keer wél voortvarend worden opgepakt. In onze brief van dinsdag 28 november jl. is het voornemen om deze testen opnieuw uit te voeren herbevestigd.

Na overleg met de gemeente heeft het gespecialiseerde bureau, in opdracht van de rekenkamer, eind november/begin december opnieuw een aantal testen verricht. Op 11 december 2017 ontving de rekenkamer de rapportage met de resultaten. Deze rapportage is inmiddels gedeeld met de gemeentelijke organisatie. De vertrouwelijke rapportage maakt, net als bij het onderzoek dat ten grondslag lag aan het rapport 'In onveilige handen', geen onderdeel uit van deze openbare brief van de rekenkamer. In de voorliggende brief wordt in algemene zin een indruk gegeven van de aard van de bevindingen, het daarbij behorende risico en de mogelijke consequenties.

Achtereenvolgens zal in deze brief worden ingegaan op de resultaten van de verschillende testen. Vervolgens zal worden samengevat welk beeld deze testen bieden van de staat van de informatiebeveiliging van de gemeente en de opvolging van de aanbevelingen uit het rapport 'In onveilige handen'. Afgesloten wordt met enkele nieuwe aanbevelingen aan het college.

resultaten social engineering test
De social engineering test, waarbij wordt gepoogd via medewerkers toegang te krijgen tot vertrouwelijke gegevens, bestond dit maal uit twee onderdelen: het versturen van e-mails (spear phishing) en het telefonisch benaderen van medewerkers (voice phishing). Voice phishing was een nieuw element ten opzichte van de testen die eind 2016 zijn uitgevoerd.

Via e-mail phishing bleek het niet mogelijk toegang tot inloggegevens of systemen van medewerkers te verkrijgen. E-mails met een kwaadaardige bijlage werden tegengehouden en niet afgeleverd bij de medewerkers. Van een e-mail die wel de beveiliging passeerde, bleek de bijlage door beveiligingsinstellingen niet te kunnen worden geopend door de ontvanger. De onderzoekers stuurden ook een e-mail met een link naar een gefingeerde website van de gemeente. Medewerkers van de gemeenten bezochten weliswaar deze website, maar lieten geen login-gegevens achter. Bovendien werden de betreffende e-mail gedetecteerd door de gemeente, waarna het gespecialiseerde bureau op de hoogte werd gebracht.

Ook de pogingen om via de telefoon contact te leggen met medewerkers mislukten. Het bleek niet mogelijk inlog-gegevens te verkrijgen waarmee het gemeentelijke netwerk kon worden binnengedrongen. Weliswaar werd door één medewerker de combinatie van wachtwoord en gebruikersnaam verstrekt, maar bij het inloggen stuitten de onderzoekers op een extra verificatie-stap. Deze stap moet worden doorlopen wanneer wordt ingelogd buiten de gemeentelijke kantoorpanden. Doordat de onderzoekers niet beschikten over gegevens voor deze laatste verificatiestap kregen zij geen toegang tot het gemeentelijke netwerk.

resultaten inlooptest
Tijdens de inlooptest probeerden onderzoekers ongeautoriseerd toegang te krijgen tot (werk)ruimtes in twee gemeentelijke kantoorpanden. Het was de bedoeling dat de onderzoekers, bij een geslaagde poging, vervolgens zouden proberen om het gemeentelijke ICT-netwerk binnen te dringen. Met de gemeente was afgesproken dat de test zou worden beëindigd als de onderzoekers werden gedetecteerd of aangesproken. Hiermee is een realistische situatie nagebootst waarin een hacker, zonder hulp van binnenuit, poogt zich toegang te verschaffen tot informatiesystemen met gevoelige gegevens.

Bij één van de onderzochte gemeentelijke panden was bij de toegangspoortjes continu een extra beveiligingsmedewerker aanwezig. Door deze maatregel – waarvan een zekere preventieve werking uitging – bleek het moeilijker om ongeautoriseerd toegang te krijgen tot het pand vergeleken met de inlooptesten die de rekenkamer eerder liet uitvoeren. Desalniettemin slaagden de onderzoekers er – na de nodige moeite – bij beide panden wel in om zich toegang te verschaffen. Bij een van deze panden kregen de onderzoekers toegang tot documenten en dossiers op bureaus van medewerkers. De infiltranten werden niet door medewerkers van de gemeente aangesproken.

Tijdens de inlooptest zijn hacking tools geïnstalleerd op werkstations. Door beveiligingsmaatregelen van de gemeente lukte het echter niet om via deze tools toegang te verkrijgen tot het interne netwerk.

resultaten interne penetratietest
Bij de interne penetratietest is geprobeerd om vanuit de gemeentelijke kantoorpanden oneigenlijke toegang te verkrijgen tot gevoelige (persoons)gegevens van de gemeente. Hiermee is de situatie nagebootst waarbij een medewerker van de gemeente en/of een infiltrant van binnenuit, probeert de gemeentelijke informatieomgeving binnen te dringen. Dit is op twee manieren gedaan: “black box”, dat wil zeggen, zonder enige voorkennis en “grey box”, waarbij gebruik wordt gemaakt van aangeleverde inloggegevens.

Uit de “black box” penetratietest bleek dat in het vorige rekenkameronderzoek geconstateerde kwetsbaarheden, waarmee relatief eenvoudig toegang tot het gemeentelijke netwerk kon worden verkregen, inmiddels gedeeltelijk zijn verholpen. Kwaadwillenden hebben thans minder mogelijkheden om schade toe te brengen. Niet volledig weggewerkt zijn de kwetsbaarheden ten aanzien van netwerktoegang en verouderde software. Deze kwetsbaarheden stelden de onderzoekers in staat om toegang te krijgen tot een individueel werkstation, een specifiek informatiesysteem (zonder persoonsgegevens) en een map met persoonsgegevens, waaronder identiteitsbewijzen van medewerkers en boetes.

Een hacker met relatief veel tijd tot zijn beschikking zou gebruik kunnen maken van deze kwetsbaarheden om toegang te verkrijgen tot meer gemeentelijke informatiesystemen met (gevoelige) persoonsgegevens. De onderzoekers kregen echter geen kans om de kwetsbaarheden op deze manier te misbruiken en in een positie te komen om schade aan te brengen, omdat de hackpoging tamelijk snel door de gemeentelijke organisatie werd opgemerkt. Ook in de vorige penetratietest die in opdracht van de rekenkamer was uitgevoerd, werden de onderzoekers op een gegeven moment ontdekt. Dit was echter in een veel later stadium van de hack en bij een specifieke applicatie. De testers waren toen al zo ver gevorderd dat zij schade konden aanbrengen of daar – na de onderbreking – elders mee door konden gaan. De ontdekking in de hertest was veel sneller, terwijl bovendien deze penetratiepogingen op een veel “geruislozere” manier plaatsvonden.

In de “grey box” variant van de test, dus met een door de gemeentelijke organisatie aangeleverd account, mislukten de pogingen om in de systemen binnen te dringen (behoudens enkele soortgelijke kwetsbaarheden als hiervoor) en misbruik te plegen.

resultaten wifi-test
Een nieuw onderdeel vormde een zogeheten ‘wifi-test’, waarbij wordt geprobeerd om via het draadloze netwerk het interne ICT-netwerk binnen te dringen. De onderzoekers detecteerden tijdens deze test geen kwetsbaarheden in de beveiliging van het wifi-netwerk. Het is dan ook niet gelukt om via het wifi-netwerk toegang te verkrijgen tot het gemeentelijke ICT-netwerk.

totaalbeeld penetratietesten
De resultaten van de social engineering test, de inlooptest, de interne penetratietest en de wifi-test geven een positief beeld. De rekenkamer constateert dat de effectiviteit van de beveiliging sinds eind 2016 merkbaar is verbeterd. Anders dan tijdens de testen die de rekenkamer eind 2016 heeft laten uitvoeren, is het immers niet gelukt om tijdens de test toegang te krijgen tot meerdere informatiesystemen

met gevoelige (persoons)gegevens en in een positie te komen om bijvoorbeeld identiteitsfraude te plegen, de fysieke veiligheid van politiek-bestuurlijke ambtsdragers aan te tasten, de openbare orde en publieke dienstverlening te verstoren of publieke middelen te misbruiken.

duiding resultaten penetratietesten
Dat de resultaten van de testen positief uitpakken, is geen toeval. Al tijdens de testen bleek dat de gemeente sinds 2016 technische en organisatorische maatregelen heeft getroffen om de beveiliging te verbeteren. De testresultaten wijzen er op dat deze maatregelen de gewenste werking hebben gehad.

Zo stuitten de onderzoekers tijdens de testen op nieuwe beveiligingsmaatregelen, die de gemeente heeft getroffen sinds eind 2016. Deze maatregelen voorkwamen dat de onderzoekers tijdens de penetratietesten wederom eenvoudig toegang kregen tot informatiesystemen met gevoelige (persoons)gegevens. De rekenkamer ontving na het afronden van de testen een overzicht van de getroffen beveiligingsmaatregelen sinds 2016. Maatregelen die in dit overzicht zijn genoemd werden daadwerkelijk door de onderzoekers aangetroffen. Het ging hierbij bijvoorbeeld om netwerkpoortbeveiliging en maatregelen tegen malware. Deze technische beveiligingsmaatregelen verkleinen het restrisico dat wordt veroorzaakt doordat de fysieke beveiliging nog niet op orde is.

Verder bleek uit de inlooptest en de social engineering test dat medewerkers slechts in beperkte mate gevoelig bleken voor spear phishing e-mails of telefonisch voice phishing. Het is aannemelijk dat het hogere beveiligingsbewustzijn samenhangt met het gemeentelijke ‘awareness’ programma, dat is gestart in 2017. Met name de resultaten van de voice phishing test lijken te wijzen op een bovengemiddeld beveiligingsbewustzijn bij medewerkers. Zo motiveerde een medewerker van de gemeente, die zonder succes door onderzoekers werd benaderd bij de voice phishing test, haar handelen door te verwijzen naar dit programma. Anderzijds bleek tijdens de inlooptest dat indringers zich nog steeds vrij kunnen bewegen op kantoorlocaties, zonder aangesproken te worden. Op dit onderdeel schiet het beveiligingsbewustzijn dus nog te kort.

Wanneer de getroffen beveiligingsmaatregelen worden geconfronteerd met de testresultaten, valt verder op dat met name op het terrein van fysieke beveiliging de meeste maatregelen nog ‘onderhanden werk’ zijn. Dat juist op dat terrein de beveiliging nog niet op orde is, is dus niet verrassend. Voorlopige maatregelen, zoals de inzet van extra beveiligingsmedewerkers, een signaleringssysteem ter preventie van ‘meelopen’ en communicatie gericht op awareness ten aanzien van dit fenomeen, blijken nog onvoldoende om indringers daadwerkelijk tegen te houden.

(opvolging) aanbevelingen
Al met al is in belangrijke mate opvolging gegeven aan de aanbevelingen 5 tot en met 10 uit het rekenkamerrapport ‘In onveilige handen’. Niettemin zijn er enkele – relatief gemakkelijk te verhelpen – kwetsbaarheden gevonden. Daarmee blijft een zogeheten restrisico op oneigenlijke inbreuken in de informatiesystemen bestaan.

De beoordeling van de voortgang van de implementatie van aanbevelingen 1 tot en met 4 van de rekenkamer, die betrekking hebben op (centrale sturing op) de uitvoering van het informatiebeveiligingsbeleid, maakte geen onderdeel uit van dit vervolgonderzoek, noch de oordeelsvorming. Dat geldt ook voor aanbeveling om de beveiliging van een aantal kritische applicaties te verbeteren. De implementatie van

deze aanbevelingen is onderdeel van een meerjarig verbeterprogramma dat pas in 2020 volledig zal zijn afgerond. Het is op dit moment te vroeg om de opvolging van deze aanbevelingen volledig te kunnen beoordelen. De rekenkamer zal deze beoordeling in een later stadium verrichten.

Op basis van deze hertest doet de rekenkamer de volgende (nieuwe) aanbevelingen:

1. Ga ten aanzien van het dichten van de concrete kwetsbaarheden die bleken uit de huidige en voorgaande testen voort op de ingeslagen weg.

Door verbetering van het beveiligingsbewustzijn wordt het risico gereduceerd dat hackers de resterende kwetsbaarheden voor aanvallen van binnenuit weten te benutten. Dat geldt ook voor risico's door nieuwe zwakheden, die dagelijks ontstaan door de voortschrijdende technologie en de inventiviteit van hackers.

2. Blijf werken aan het onderhoud van het beveiligingsbewustzijn, door voorlichting en training van medewerkers. Besteed hierbij in het bijzonder aandacht aan het aanspreken van onbekenden op kantoorlocaties.
3. Verbeter de fysieke beveiliging, aangezien op dit terrein de getroffen maatregelen nog onvoldoende effectief waren. Gedacht kan worden aan de reeds geplande maatregel (Q1 2018) om het dragen van duidelijk zichtbare passen, met daarop de naam leesbaar en met foto, verplicht te stellen voor iedereen in de gemeentelijke gebouwen. Tevens kan gedacht worden aan de inzet van een host in de ontvangstzone, die ook toezicht houdt op het gedrag van bezoekers rond de beveiligingspoortjes.
4. Beoordeel na één jaar, door middel van pentesten en inlooptesten, of de getroffen maatregelen effectief zijn gebleken.
5. Draag zorg voor de borging van informatiebeveiliging conform het beleid, ook na 2020, als het meerjarig verbeterprogramma is afgerond.

De rekenkamer zal de implementatie van de aanbevelingen de komende jaren nauwlettend blijven volgen. Hiertoe zullen de voortgangsrapportages van het verbeterprogramma en de resultaten van hernieuwde pentesten en inlooptesten doorlopend worden gemonitord.

reactie college

Hartelijk dank voor het toezenden van de bevindingen uit het vervolgonderzoek Informatiebeveiliging dat de Rekenkamer de afgelopen periode heeft uitgevoerd. In deze brief geven wij u onze reactie op uw bevindingen en de aanbevelingen die u doet.

De publicatie van het vorige rekenkamerrapport in april 2017 over de stand van zaken rond informatiebeveiliging heeft veel aandacht gehad. Het college is daarom verheugd om te lezen dat in vervolgonderzoek van de rekenkamer het volgende wordt geconcludeerd: "De rekenkamer constateert dat de effectiviteit van de beveiliging sinds eind 2016 merkbaar is verbeterd. Anders dan tijdens de testen die de rekenkamer eind 2016 heeft laten uitvoeren, is het immers niet gelukt om tijdens de test toegang te krijgen tot meerdere informatiesystemen met gevoelige (persoons)gegevens en in een positie te komen om bijvoorbeeld identiteitsfraude te plegen, de fysieke veiligheid van politiek-bestuurlijke ambtsdragers aan te tasten, de openbare orde en publieke dienstverlening te verstoren of publieke middelen te misbruiken."

Het college herkent de conclusie van de rekenkamer dat er veel werk is verzet op het gebied van informatiebeveiliging, met de gewenste uitwerking op de veiligheid als gevolg. De organisatie heeft hier grote stappen in weten te zetten. Tegelijkertijd blijft het zaak dat eenieder (ambtenaren, college en raadsleden) alert blijft op digitale dreigingen.

Het programma dat naar aanleiding van het rekenkamerrapport is opgestart, is nog in volle gang en zal verder gaan met het treffen van effectieve verbeteringen voor wat betreft beveiligingsmaatregelen op het gebied van awareness en fysieke en technische beveiliging.
Dit is een continue en dynamische aanpak die, indien nodig, wordt aangepast aan eventuele nieuwe of veranderende bedreigingen.

In uw brief doet u een aantal (nieuwe) aanbevelingen. Deze worden door ons onderschreven en, waar dat nog niet het geval is, onderdeel gemaakt van ons meerjarig programma Rekenkamer informatiebeveiliging en het bijbehorende maatregelenpakket.

nawoord rekenkamer
De rekenkamer stelt vast dat het college alle conclusies en aanbevelingen onderschrijft. Het college stelt daarbij terecht dat informatiebeveiliging continue aandacht behoeft. De rekenkamer zal daarom, zoals ook in deze brief reeds is aangegeven, de uitvoering van het meerjarige programma de komende jaren blijven volgen.

Met vriendelijke groet,

Drs. P. Hofstra RO CIA
directeur

EMBARGO tot 5 februari 2018, 12:00 uurcc

cc
college B en W