Bestuurlijk rapport

ZO STERK ALS DE ZWAKSTE SCHAKEL

EEN ONDERZOEK NAAR DE INFORMATIEVEILIGHEID BIJ DE GEMEENTE UTRECHT

REKEN KAMER UTRECHT

REKEN KAMER UTRECHT

ZO STERK ALS DE ZWAKSTE SCHAKEL

EEN ONDERZOEK NAAR DE INFORMATIEVEILIGHEID BIJ DE GEMEENTE UTRECHT

7 april 2021
Eindrapport

REKENKAMER UTRECHT

LEDEN

- Paul Venhoeven (voorzitter)
- Carolien de Boer
- Sjoerd Keulen

MEDEWERKERS ONDERZOEK

- Johan Snoei
- Pauline de Jong
- Naomi Meys

CONTACTGEGEVENS

030 - 286 1391
rekenkamer@utrecht.nl
utrecht.nl/rekenkamer
Postbus 16200, 3500 CE Utrecht

VOORWOORD

Informatieveiligheid is een onderwerp dat met de toenemende digitalisering steeds belangrijker wordt. Gemeenten verwerken grote hoeveelheden gegevens in een veelvoud aan systemen en programma's. Veel van deze gegevens betreffen (bijzondere) persoonsgegevens of andere belangrijke gegevens die goed beschermd moeten zijn. Zonder goede informatiebeveiliging liggen cybercriminaliteit, fraude, oplichting en ondermijning op de loer. En recente voorbeelden bij de GGD, de gemeente Hof van Twente en eerder de Rotterdamse haven en de Universiteit van Maastricht tonen aan dat een aanval door kwaadwillenden grote gevolgen kan hebben.

Voor informatiebeveiliging geldt het gezegde dat de keten zo sterk is als de zwakste schakel. Om te weten hoe het met de huidige informatiebeveiliging van de gemeente is gesteld, heeft de rekenkamer dit door bureau Hoffmann B.V. laten testen. Er kwam een aantal technische kwetsbaarheden naar voren. Daarnaast bleek dat het gedrag van medewerkers in relatie tot informatieveiligheid een belangrijk risico vormt. Ook bleken er eenvoudig te kraken wachtwoorden bij de gemeente in gebruik te zijn. Alle reden dus om informatieveiligheid de aandacht te geven die het verdient. Utrechtse inwoners en ondernemers moeten er immers op kunnen vertrouwen dat er bewust en veilig wordt omgegaan met informatie die de overheid van hen heeft. Daarnaast gaan de ontwikkelingen op het gebied van ICT en informatieveiligheid snel. Dat betekent dat de beveiliging van informatie continu aandacht behoeft. Steeds kunnen er nieuwe veiligheidsrisico's ontstaan die zo snel mogelijk moeten worden ontdekt en opgelost. Dit onderwerp vraagt dus blijvende aandacht van politiek, bestuur en organisatie. En het geeft ons reden om in de toekomst de (organisatie van) informatieveiligheid verder te onderzoeken.

In dit onderzoek hebben wij gesproken met medewerkers van de gemeente die betrokken zijn bij informatieveiligheid. Zij hebben ons informatie verstrekt over de stand van zaken op het gebied van informatieveiligheid. Wij danken de contactpersonen en geïnterviewden voor hun medewerking en inbreng.

Paul Venhoeven,
voorzitter

Gerth Molenaar,
secretaris

Utrecht, 7 april 2021

INHOUDSOPGAVE

DEEL I BESTUURLIJK RAPPORT

1 DOELSTELLING ONDERZOEK

Aanleiding

De Utrechtse gemeenteraad heeft het onderwerp informatieveiligheid verschillende keren als onderzoeksthema aangedragen bij de Rekenkamer Utrecht. Bij de raadsleden leven vragen over de visie en aanpak van de gemeente Utrecht en de bewustwording van de risico's binnen het gemeentelijk apparaat. Voor de rekenkamer aanleiding om met dit onderwerp aan de slag te gaan. In voorliggend rapport presenteren wij de resultaten van ons onderzoek.

Doel en centrale vraag

Het doel van het onderzoek is de gemeenteraad inzicht geven in de manier waarop de gemeente Utrecht invulling geeft aan de informatieveiligheid en te beoordelen of de informatieveiligheid voldoende is gewaarborgd. De centrale vraag van het onderzoek is:

> Is de informatieveiligheid bij de gemeente Utrecht voldoende gewaarborgd?

Toelichting werkwijze rekenkamer

Het onderzoek is uitgevoerd in de periode september – december 2020. We hebben de relevante beleidsdocumenten, documenten uit de begrotingscyclus en andere raadsinformatie over informatieveiligheid bestudeerd. Voor het inzicht in de risico's die zijn geïdentificeerd en de beheersmaatregelen hebben wij onder andere de risicorapportages van de gemeente ingezien. We hebben tien interviews gehouden met de medewerkers van de gemeente die nauw betrokken zijn bij informatieveiligheid. De testen of het mogelijk was om op een oneigenlijke manier toegang te krijgen tot informatie bij de gemeente zijn uitgevoerd door Hoffmann B.V. (hierna genoemd: het externe bureau). We beoordeelden in het onderzoek drie aspecten: (1) organisatie en proces, (2) mens en (3) techniek. Bij de beantwoording van de onderzoeksvragen en de beoordeling van de onderzochte aspecten van informatieveiligheid hebben wij een normenkader gehanteerd. In de inleiding van de verschillende hoofdstukken in de separaat aangeboden nota van bevindingen staan deze normen in een tabel met daarbij de beoordeling na afronding van het onderzoek. De nota van bevindingen is anders dan gebruikelijk als apart document op de website gepubliceerd, omdat de belangrijkste bevindingen ook terugkomen in de toelichting bij de verschillende conclusies en aanbevelingen in deze bestuurlijke nota.

2 CONCLUSIES EN AANBEVELINGEN

Op basis van de bevindingen zoals gepresenteerd in het onderzoeksrapport komt de rekenkamer tot een hoofdconclusie met vier deelconclusies. Bij deze deelconclusies formuleren we een of meer aanbevelingen en geven we een korte toelichting.

HOOFDCONCLUSIE

De gemeente Utrecht is voldoende beschermd tegen inbraken van buitenaf. Het lukte de extern onderzoekers namelijk niet om van buitenaf in te breken in de gemeentelijke systemen. Toch tonen interne testen op het gebied van techniek en menselijk handelen risico's aan die het beeld van de informatieveiligheid minder rooskleurig maken. Sommige technische kwetsbaarheden in software en hardware blijven jarenlang bestaan en medewerkers geven in phishing mails hun inloggegevens af. Ook zijn onbevoegde 'inlopers' eenvoudig gemeentelijke gebouwen binnengekomen en hebben zij daar geheime informatie kunnen bemachtigen zonder te zijn aangesproken door medewerkers.

Het beleid om de informatiebeveiliging te verbeteren is in opzet goed. Maar door een combinatie van een gebrek aan personeel, middelen en prioriteit loopt de uitvoering van het beleid achter op de oorspronkelijke planning. Risicogestuurd werken – het uitgangspunt van het beleid – wordt topdown ingevuld en is door het ontbreken van de benodigde risicoanalyses nog niet mogelijk. Daarnaast ontbreekt een centraal programma om medewerkers informatiebewust te maken.

De gemeente Utrecht heeft sinds 2018 al diverse maatregelen getroffen om de informatiebeveiliging te verbeteren. Zo is de governance versterkt, de bemensing uitgebreid en heeft de gemeenteraad in 2020 extra middelen beschikbaar gesteld voor gegevensbescherming. Ook zijn de risico's op het gebied van informatieveiligheid in kaart gebracht. Toch wijzen de testresultaten en de stand van het beleid uit dat er bij de gemeente verbetering noodzakelijk is. De recente voorbeelden van digitale aanvallen op publieke instellingen laten zien hoe kwetsbaar en afhankelijk de samenleving is van digitale middelen. Zeker nu thuiswerken de norm is en de overheid snel (digitaal) moet kunnen handelen. Om te kijken of verbeteracties voortvarend zijn uitgevoerd zal de rekenkamer de informatieveiligheid bij de gemeente Utrecht in de toekomst verder onderzoeken.

DEELCONCLUSIE 1: INFORMATIEVEILIGHEID VAN BUITENAF BETER DAN VAN BINNENUIT

Informatie van de gemeente Utrecht is technisch gezien beter beveiligd tegen aanvallen van buitenaf dan van binnenuit.

AANBEVELING 1:

Neem de benodigde maatregelen tegen de technische risico's die bekend zijn. Benut daarbij ook de uitkomsten van (interne en externe) pentesten van het rekenkameronderzoek.

Toelichting

Het is het externe bureau binnen de beschikbare tijd van twee dagen niet gelukt om van buitenaf (via het internet) binnen te dringen in de gemeentelijke systemen. Ook de Wifi-netwerken van de gemeente Utrecht hebben de penetratietesten doorstaan. Uit deze testen kwam wel een zestal kwetsbaarheden naar voren, waarvan één kritiek en één hoog risico. Kritiek was de constatering dat er niet meer ondersteunde software werd gebruikt en dat het mogelijk was om multifactor-authenticatie te registreren. Hierdoor is het in de huidige situatie mogelijk om veilige en niet veilige omgevingen te vermengen. De laatste kwetsbaarheid is al sinds 2018 bekend bij de gemeente, maar door het ontbreken van consensus over de oplossing ligt besluitvorming om dit aan te pakken stil. De consequentie is dat de betrouwbaarheid van informatie niet te garanderen is, omdat het eenvoudig mogelijk is om misbruik te maken van de toegang tot de informatie.

De interne penetratietesten – een aanval van binnenuit de gemeentelijke gebouwen – heeft binnen de beschikbare tijd van vier dagen 17 kwetsbaarheden aangetoond. Zes daarvan zijn direct gerelateerd aan de werkstations van de medewerkers. Deze werkstations (mini pc's) bevinden zich op alle werkplekken en het bleek mogelijk om ongeautoriseerd toegang te krijgen en live mee te kijken met medewerkers in de personeelsdossiers van de gemeente. Ook was het mogelijk om gebruikersnamen en wachtwoorden van deze medewerkers buit te maken. De gemeente Utrecht heeft deze kwetsbaarheid – ondanks de beschikbare beveilingsupdates die zijn uitgebracht – nog niet opgelost. De gemeente wijt dit aan een ongelukkige samenloop van interne omstandigheden, waaronder de uitval van medewerkers en een reorganisatie.

Andere kritieke risico's zijn het ontbreken van beveiligingsupdates, verouderde besturingssystemen, en serviceaccounts die niet goed beschermd zijn. Een hoog risico vormt het ontbreken van multifactor-authenticatie op bijvoorbeeld de webmail. Inmiddels is multifactor-authenticatie op de webmail doorgevoerd. Het bleek dat veel wachtwoorden bij de gemeente Utrecht zwak waren en gekraakt konden worden. Daarnaast worden wachtwoorden onveilig opgeslagen. Daarmee kwalificeren wij de interne situatie rondom informatieveiligheid als ernstig. Wel is het positief dat de gemeente Utrecht haar netwerk gesegmenteerd heeft, waardoor indringers niet direct het hele netwerk kunnen binnenkomen, zoals bij eerdere hacks van publieke instellingen wel is gebeurd.

De rekenkamer beveelt aan om de benodigde maatregelen met voorrang te nemen om de geconstateerde risico's te verhelpen. Vanwege de ernst van de aangetroffen kwetsbaarheden en de urgentie om deze aan te pakken, hebben wij de testresultaten al eerder, zonder vertraging ter beschikking gesteld aan de gemeente. Een deel van de kwetsbaarheden is inmiddels verholpen. Wij bevelen aan om ook voor de openstaande onderwerpen zo snel mogelijk de noodzakelijke maatregelen te treffen.

DEELCONCLUSIE 2: INFORMATIEBEWUSTZIJN EN FYSIEKE BEVEILIGING ZIJN ONVOLDOENDE EN CENTRAAL PROGRAMMA INFORMATIEBEWUSTZIJN ONTBREEKT

Uit de mail-phishing test blijkt dat een aanzienlijk deel van de medewerkers (16-19%) niet altijd bewust omgaat met informatieveiligheid. Ook lijken medewerkers niet altijd te weten hoe zij bij beveiligingsproblemen en -incidenten moeten handelen. Tijdens inlooptesten konden onderzoekers eenvoudig gemeentelijke gebouwen betreden en werden zij niet door medewerkers aangesproken op hun onbevoegde aanwezigheid. Er is geen centraal programma over informatiebewustzijn. Organisatieonderdelen besteden individueel en op hun eigen manier aandacht aan het onderwerp en er worden ad hoc acties uitgevoerd.

AANBEVELINGEN 2, 3 EN 4:

2. Investeer structureel in het bewustzijn van medewerkers over informatieveiligheid. Besteed daarbij ook aandacht aan tijdelijke en externe medewerkers.
3. Structureer en verhelder zoveel mogelijk de procedure voor het melden van beveiligingsproblemen en -incidenten. Maak deze breed bekend en benadruk (nogmaals) de urgentie ervan.
4. Verbeter de beveiliging van gemeentelijke gebouwen om de toegang voor onbevoegden te voorkomen.

Toelichting
Er is bij de gemeente geen centraal programma of plan voor informatiebewustzijn. Van 2015-2018 was er wel een centrale bewustwordingscampagne, maar deze is vanwege gebrek aan budget en het vertrek van de projectleider beëindigd. Sindsdien worden er ad hoc acties uitgevoerd, zoals de Dag van de Gegevensbescherming en een mail-phishing test in januari 2020. De organisatieonderdelen besteden op hun eigen manier aandacht aan informatiebewustzijn. Zo wordt de introductie op het onderwerp informatieveiligheid voorafgaand aan het dienstverband niet organisatiebreed, maar door sommige organisatieonderdelen afzonderlijk ingevuld. Ook is de introductie vaak alleen gericht op vaste en niet op tijdelijke of externe medewerkers. De gemeente heeft aangegeven te willen intensiveren op dit thema en bereidt sinds oktober 2020 een nieuw centraal bewustwordingsprogramma voor, waarvan de rekenkamer in december 2020 een eerste concept heeft ingezien. De implementatie ervan staat voor 2021 gepland.

De urgentie van een dergelijk bewustwordingsprogramma wordt duidelijk uit beveiligingstests die de rekenkamer in samenwerking met het externe bureau heeft laten uitvoeren. Bij de mail-phishing hebben 950 medewerkers (16%) gebruikersnaam en wachtwoord verstrekt, 121 gebruikers deden dit zelfs na de waarschuwing die door de gemeente is afgegeven na de eerste testdag. Dit percentage van 16% is vergelijkbaar met uitkomsten van dergelijke onderzoeken die het externe bureau heeft uitgevoerd bij andere gemeenten. Vaak heeft een kwaadwillende al aan één combinatie van gebruikersnaam en wachtwoord genoeg om zich toegang te verschaffen tot systemen van de gemeente. Uit een mail-phishing simulatie die de gemeente in januari 2020 zelf uitvoerde, bleek ook al dat een deel van de medewerkers niet alert is op pogingen van phishing. Ten slotte werd tijdens ons onderzoek door medewerkers van twee van de vier verspreide USB-sticks de inhoud geopend. Een kwaadwillende kan hiermee toegang krijgen tot de betrokken computer.

Het is van belang dat medewerkers melding doen van dergelijke incidenten. Hoe eerder iets gesignaleerd en gemeld wordt, hoe korter een kwaadwillende schade kan aanrichten en hoe sneller verdere stappen kunnen worden voorkomen. Bij de mail-phishing test van de rekenkamer werd slechts 477 keer officieel melding van phishing gedaan. Ook meer algemeen geldt dat het aantal meldingen van datalekken tussen 2019 en 2020 is afgenomen. Medewerkers lijken daarom niet altijd te weten wat zij moeten doen bij incidenten zoals mail-phishing en datalekken. De meldingsbereidheid ten opzichte van het totaalaantal beveiligingsincidenten is echter niet te achterhalen. Het is namelijk onduidelijk hoe vaak datalekken in de afgelopen jaren zijn voorgekomen.

De beveiliging van en sociale controle op het Stadskantoor en het Stadhuis kunnen niet voorkomen dat onbevoegden gemakkelijk en ongestoord binnen kunnen komen. Ondanks dat de gemeente aangeeft dat er een open cultuur heerst waarin medewerkers elkaar aanspreken, blijkt uit de voor de rekenkamer uitgevoerde inlooptesten (‘mystery guest bezoek’) dat de onderzoekers niet werden aangesproken op hun aanwezigheid. Zij konden ongestoord dossierkasten openen en informatie inzien. De onderzoekers hebben daarnaast een laptop van een medewerker mee kunnen nemen waarop een post-it met bijbehorend wachtwoord was bevestigd. Hierdoor kon eenvoudig toegang worden verkregen tot de laptop. De onderzoekers hebben daarmee bij deze testen zowel op papier als digitaal geheime informatie kunnen inzien.

Wij bevelen daarom aan om structureel te investeren in het informatiebewustzijn van medewerkers en daarin ook tijdelijke en externe medewerkers mee te nemen. Het is van groot belang dat medewerkers alert zijn op pogingen van onbevoegden om gevoelige informatie te bemachtigen, zowel digitaal als fysiek. Daarnaast bevelen wij aan om de procedure en bekendheid rondom het melden van beveiligingsproblemen en -incidenten te structureren, zodat medewerkers hier zo snel mogelijk melding van doen. Daarbij is van belang om de urgentie van het doen van meldingen bij incidenten (nogmaals) te benadrukken. Om te voorkomen dat beveiligingsproblemen door onbevoegden op locatie zich kunnen voordoen, bevelen wij aan om de fysieke beveiliging van in

ieder geval het Stadskantoor als het Stadhuis te verbeteren. Mogelijk is dit ook nodig voor de andere gemeentelijke gebouwen.

DEELCONCLUSIE 3: GEMEENTE KAN NOG NIET RISICOGESTUURD WERKEN, BEKENDE RISICO'S BLIJVEN ONNODIG LANG BESTAAN

De gemeente Utrecht heeft in juli 2019 het nieuwe *Beleid voor gegevensbescherming 2019-2022* vastgesteld. De gemeente hanteert hierbij het uitgangspunt van risicogestuurd werken. De roadmap (routekaart) die hiervoor is ontwikkeld is een goed instrument, maar deze wordt onvoldoende gevolgd. Daarvoor is momenteel te weinig personeel beschikbaar en krijgt het te weinig prioriteit. Hierdoor loopt de uitvoering vertraging op en kunnen verschillende bekende risico's jarenlang blijven bestaan. Voorbeelden van te lang bestaande risico's zijn het niet uitvoeren van cruciale software updates, kwetsbare werkstations op alle bureaus en het ontbreken van multifactor-authenticatie bij de webmail. Doordat een groot deel van de risicoanalyses zijn uitgevoerd kan de gemeente nog niet risicogestuurd werken.

AANBEVELINGEN 5 EN 6:

5. Versnel het uitvoeren van de maatregelen in de roadmap. Voor verdere maatregelen is het ook nodig om na te gaan of eerder getroffen maatregelen hebben gewerkt. Zet daarbij het extra geld voor gegevensbescherming en de uitbreiding van de DISO-capaciteit effectief in. Zorg ook binnen de organisatieonderdelen voor voldoende capaciteit.
6. Voer alle benodigde risicoanalyses uit om een totaalbeeld op te kunnen maken van de huidige stand van de risico's. Benut daarbij de inzet van de extra DISO-capaciteit.

Toelichting
Het uitgangspunt van het nieuwe *Beleid voor gegevensbescherming 2019-2022* is risicogestuurd werken. Om risicogestuurd te kunnen werken is het cruciaal om risicoanalyses en Data Protection Impact Assessments (DPIA's) uit te voeren. Het plan is om deze risicoanalyses op alle niveaus – strategisch, tactisch en operationeel – uit te voeren. De gemeente werkt sinds 2019 met een strategisch risico-overzicht. Maar van de benodigde 21 tactische risicoanalyses zijn er slechts 6 gereed. Op het gebied van privacy zijn ruim 150 DPIA's afgerond, maar de overige operationele risicoanalyses voor informatieveiligheid zijn – met uitzondering van 6 operationele risicoanalyses als pilot bij Stadsbedrijven – nog niet uitgevoerd. Omdat risicoanalyses en DPIA's cruciaal zijn om risicogestuurd te werken, is dit nog niet volledig mogelijk.

Voor de implementatie van het nieuwe beleid is een roadmap opgesteld. Hierin staan de onderwerpen waaraan de gemeente gaat werken en de mijlpalen die daarbij behaald moeten worden. De gemeente heeft al een aantal algemene maatregelen genomen, zoals het versterken van de governance waarbij een stuurgroep, vakgroep, regiegroep en taskforce zijn ingesteld die op verschillende niveaus de voortgang van risico's en maatregelen bewaken. Ook zijn er in 2020 extra

middelen beschikbaar gesteld waarmee onder andere de capaciteit voor Decentrale Informatie en Security Officers (DISO's) is uitgebreid en een projectleider bewustwording is aangesteld voor een initiële periode van zes maanden.

We constateren dat de uitvoering bij een aantal cruciale onderdelen achterloopt op de oorspronkelijke planning. Deze achterstand moet mede worden ingelopen door het extra personeel en de extra middelen die in 2020 beschikbaar zijn gesteld. Daarnaast is er urgentie en daadkracht nodig bij het management en de proceseigenaren, en is er ruimte vereist voor uitvoerende medewerkers om hier, naast hun reguliere werkzaamheden, aan te werken. Het valt op dat in de testen verschillende risico's zijn gevonden die al jaren bij de gemeente bekend waren, maar niet zijn verholpen. Daardoor heeft de gemeente al langere tijd onnodig risico gelopen. Een voorbeeld hiervan is de mogelijkheid om in te breken in de werkstations van medewerkers. Deze kwetsbaarheid is al sinds 2017 bekend, maar is eind 2020 nog altijd niet opgelost. Een tweede risico is het niet uitvoeren van beschikbare updates in kwetsbare software die in 2017 en 2018 in wereldwijde hackaanvallen zijn gebruikt. Sinds 2018 zijn de risico's op het gebied van informatieveiligheid in kaart gebracht en geprioriteerd. Van de in totaal 60 risico's die in 2020 in de ICT zijn geïdentificeerd, staan er januari 2021 nog 24 (40%) open.

Wij bevelen aan om de uitvoering van maatregelen in de roadmap fors te versnellen. Daarbij is ook van belang om na te gaan of eerder getroffen maatregelen hun werking hebben gehad. Wij bevelen aan om hierbij de extra middelen voor gegevensbescherming en de extra DISO-capaciteit effectief in te zetten. Hierbij is het belangrijk dat er binnen de organisatieonderdelen voor capaciteit wordt gezorgd, zodat medewerkers hier naast de reguliere werkzaamheden tijd aan kunnen besteden.

Verder beveelt de rekenkamer aan om de tactische risicoanalyses uit te voeren, en aansluitend de operationele risicoanalyses en daarbij de inzet van extra DISO-capaciteit te benutten. Alleen zo ontstaat het noodzakelijke totaalbeeld om risicogestuurd te kunnen werken.

DEELCONCLUSIE 4: BEPERKT ZICHT OP VEILIG THUISWERKEN

De gemeente weet niet van alle medewerkers in welke mate zij thuiswerken met veilige apparatuur. Slechts 15% van de laptops die de gemeente heeft verstrekt is voorzien van de juiste beveiligingsmaatregelen. De gemeente biedt een beveiligde virtuele werkomgeving aan, maar heeft geen zicht op de beveiliging van privé apparatuur en stelt geen eisen aan de beveiliging van WiFi-netwerken bij medewerkers thuis. Om het gemeentenetwerk niet te overbelasten, moeten vergadertools buiten de beveiligde werkomgeving gebruikt worden. Zo ontstaat het risico dat medewerkers toch buiten de werkomgeving blijven werken en mogelijk gevoelige informatie lokaal opslaan.

AANBEVELING 7:

Verbeter het toezicht op en de technische beveiligingsmaatregelen voor informatieveiligheid in de thuiswerksituatie.

Toelichting

Sinds het begin van de coronacrisis in maart 2020 werkt het merendeel van de medewerkers van de gemeente Utrecht thuis. De gemeente Utrecht weet niet van alle medewerkers of zij thuiswerken met veilige apparatuur. In februari 2021 waren in totaal bijna 2.500 laptops door de gemeente uitgegeven. Sinds november 2020 worden beveiligde laptops uitgeleverd die beschermd zijn tegen aanvallen op onveilige netwerken en bij diefstal en verlies. Het gaat hier om ongeveer 375 laptops (15%). De bijna 2.100 eerder verstrekte laptops zijn daarentegen niet allemaal voorzien van de juiste beveiligingsmaatregelen. Op een deel van deze laptops is sprake van achterstallig onderhoud: er ontbreekt harddiskencryptie en USB-poorten zijn nog toegankelijk. Daarnaast werken medewerkers die geen laptop van de gemeente in bruikleen hebben thuis waarschijnlijk op eigen apparatuur. De gemeente heeft geen zicht op de beveiliging van deze apparatuur, maar biedt medewerkers een beveiligde virtuele werkomgeving aan om zoveel mogelijk te voorkomen dat gegevens lokaal worden opgeslagen. Ook stelt de gemeente geen eisen aan de beveiliging van WiFi-netwerken bij mensen thuis.

Een ander risico op het gebied van thuiswerken ontstaat door het gebruik van vergadertools. De gemeente heeft maatregelen genomen om drie vergadertools (*Microsoft Teams, Zoom* en *GoToMeeting*) zo veilig mogelijk aan te bieden. Deze vergadertools moeten echter buiten de werkomgeving worden gebruikt, om te voorkomen dat het netwerk overbelast raakt. Het risico dat hierdoor ontstaat, is dat medewerkers vervolgens buiten de werkomgeving blijven werken en bijvoorbeeld toch vertrouwelijke informatie op eigen gegevensdragers opslaan.

Mede met het oog op de aanhoudende thuiswerksituatie rondom COVID-19 en de verwachting dat dit daarna deels structureel zal doorgaan, bevelen wij aan om zowel de technische beveiligingsmaatregelen voor informatieveiligheid in de thuiswerksituatie als het toezicht erop te verbeteren.

INDICATIEVE BENCHMARK

De gemeenteraad heeft gevraagd om de bevindingen over informatieveiligheid van de gemeente Utrecht te benchmarken met andere gemeenten. De afgelopen jaren hebben veel rekenkamers onderzoek gedaan naar de informatieveiligheid bij hun gemeente. De rekenkamer heeft daarom de onderzoeksresultaten, conclusies en aanbevelingen vergeleken met de uitkomsten in enkele andere gemeenten, te weten: Den Haag (2014), Dordrecht (2017), Rotterdam (2017), Lansingerland (2017) en Vlaardingen (2020).

Daarbij plaatsen wij vooraf wel enkele kanttekeningen. In de eerste plaats geldt dat iedere gemeente een andere technische en organisatorische ICT-inrichting kent. Systemen en

organisaties die getest en in kaart gebracht worden, verschillen daarom van elkaar. In de tweede plaats gaan de ontwikkelingen op het gebied van informatieveiligheid snel. De stand van de techniek en het moment van testen hebben daarmee een grote invloed op de resultaten. Ook de onderzoeksmethode maakt een belangrijk verschil. Dit maakt dat de vergelijking van de uitkomsten als indicatief moet worden beschouwd.

Wanneer we de uitkomsten in Utrecht op hoofdlijnen vergelijken met onderzoeken door andere gemeentelijk rekenkamer(commissie)s, dan zien we grotendeels dezelfde bevindingen en aanbevelingen:

- het binnendringen via de externe testen is minder succesvol is dan bij interne testen.
- bij vergelijkbare mail-phishing aanvallen laat een vergelijkbaar percentage medewerkers inloggegevens achter.
- medewerkers gebruiken zwakke wachtwoorden en spreken onbekende bezoekers niet aan.
- de fysieke beveiliging van gemeentelijke gebouwen schiet vaak tekort om de toegang van onbevoegden te voorkomen.
- gemeenten moeten aan de slag met het (verder) uitvoeren van risicoanalyses.

VERVOLGONDERZOEK

De uitkomsten van het onderzoek zijn voor ons aanleiding om de informatieveiligheid bij de gemeente Utrecht te blijven volgen. Over een jaar zullen wij weer kort onderzoek doen naar de stand van het beleid van informatiebeveiliging, de organisatie en het proces. Zo kunnen we vaststellen of de hernieuwde inzet van mensen en geld ertoe geleid heeft dat de gemeente inmiddels risicogestuurd kan werken en voldoende voortgang maakt met de roadmap. We zien dat de gemeente de testbevindingen voortvarend heeft opgepakt en ook al deels heeft geïmplementeerd. Wij hopen dat deze inzet blijvend is. Daarom zullen wij op een later moment nogmaals de penetratie- en social engineeringtesten gaan herhalen.

3 BESTUURLIJKE REACTIE COLLEGE VAN B&W

Wij danken u voor de uitvoering van het onderzoek ’Informatieveiligheid bij de Gemeente Utrecht’. U heeft hierin, op verzoek van de gemeenteraad, onderzocht op welke manier wij invulling geven aan de informatieveiligheid en u heeft beoordeeld of de informatieveiligheid voldoende is gewaarborgd.

Wij zijn u erkentelijk voor dit uitgebreide rapport op dit complexe onderwerp en zien in uw bevindingen een bevestiging van de koers die wij in 2018 hebben ingezet met ons beleid voor gegevensbescherming en het hierop gestoelde programma gegevensbescherming. Hierbij herkennen wij de door u geformuleerde aandachtspunten. In deze brief geven wij eerst een algemene reactie en zullen wij daarna ingaan op de specifieke aanbevelingen in het rapport.

Algemene reactie
Wij waarderen de grondigheid van uw rapport. Informatieveiligheid en privacy zijn een zeer actuele maatschappelijke uitdaging en verdienen serieuze aandacht. U doet waardevolle bevindingen en zinvolle aanbevelingen. Wij nemen alle aanbevelingen over, een aantal aanbevelingen zijn reeds in uitvoering.

Hoofdconclusie
Wij herkennen uw conclusie dat de gemeente voldoende is beschermd tegen inbraken van buitenaf, maar dat de gemeente intern op het gebied van techniek en menselijk handelen nog risico loopt. Wij onderschrijven ook uw conclusie dat ons beleid om de informatiebeveiliging te verbeteren in opzet goed is. Wij maken onze ambitie om een voorbeeldfunctie te zijn voor de regio nog niet voldoende waar en daarom streven we ernaar deze beveiliging verder te verbeteren.

Uw conclusie dat het ons ontbreekt aan personeel en middelen om de uitvoering van het beleid tijdig vorm te geven delen wij gedeeltelijk. Medio 2020 hebben wij dit zelf ook geconcludeerd en hebben wij financiële en personele middelen beschikbaar gesteld om de achterstand in te halen. Wij verwachten in de eerste helft van 2021 effect te zien van deze investering en de achterstand bij het uitvoeren van de analyses vanaf nu in te gaan lopen. Deze achterstanden verwachten we in het eerste kwartaal van 2022 te hebben weggewerkt.

U concludeert terecht dat risicogestuurd werken in bepaalde gevallen te weinig prioriteit krijgt. Dit vormt een drempel voor de verdere invoering van risicogestuurd werken. Wij gaan naar aanleiding van uw onderzoek hier meer ruimte voor creëren.

Uw conclusie dat het de gemeente ontbreekt aan een centraal programma om medewerkers informatiebewust te maken verdient naar onze mening enige nuancering. De financiering voor een structureel bewustwordingsprogramma is in september 2020 beschikbaar gesteld. Sinds oktober 2020 heeft de gemeente een projectleider bewustwording gegevensbescherming aangesteld die

momenteel onze plannen vormgeeft. De eerste contouren van deze plannen zijn met u gedeeld. Voor de zomer van 2021 starten we met de uitvoering van dit plan.

Deelconclusie 1. Informatie van de gemeente Utrecht is technisch gezien beter beveiligd tegen aanvallen van buitenaf dan van binnenuit.

AANBEVELING 1:

Neem de benodigde maatregelen tegen de technische risico's die bekend zijn. Benut daarbij ook de uitkomsten van (interne en externe) pentesten van het rekenkameronderzoek.

Aanbeveling 1 nemen wij over

Direct volgend op de pentest[1] zijn we gestart met het oplossen van de kritieke en hoge technische risico's die zijn gevonden. Op dit moment zijn de oorzaken van vijf risico's geheel weggenomen en is de beheersing van zes risico's in een vergevorderd stadium. De overige risico's kunnen wij pas oplossen bij de introductie van de nieuwe digitale werkomgeving. Voor deze risico's voeren wij in de tussentijd extra controles uit.

We hebben in 2020 een proces voor het beheren en bewaken van technische risico's geïmplementeerd. Wij hebben deze risico's in dat proces opgenomen.

Deelconclusie 2. Informatiebewustzijn en fysieke beveiliging zijn onvoldoende en centraal programma informatiebewustzijn ontbreekt.

AANBEVELINGEN 2, 3 EN 4:

2. Investeer structureel in het bewustzijn van medewerkers over informatieveiligheid. Besteed daarbij ook aandacht aan tijdelijke en externe medewerkers.
3. Structureer en verhelder zoveel mogelijk de procedure voor het melden van beveiligingsproblemen en -incidenten. Maak deze breed bekend en benadruk (nogmaals) de urgentie ervan.
4. Verbeter de beveiliging van gemeentelijke gebouwen om de toegang voor onbevoegden te voorkomen.

Aanbeveling 2 nemen wij over

Zoals wij hierboven reeds hebben benoemd, zijn wij een programma voor het verhogen van het informatieveiligheidsbewustzijn van onze interne en externe medewerkers gestart. Vanuit dit programma gaan wij alle medewerkers structureel ondersteunen bij het ontwikkelen van hun kennis over gegevensbescherming. Hierbij maken wij onderscheid tussen algemene kennis en kennis die specifiek voor bepaalde functies of afdelingen nodig is. Daarnaast gaan wij aandacht

[1] De genoemde pentest of penetratietest betreft een tweetal technische testen die uitgevoerd zijn tijdens het onderzoek. Een test om vanaf het internet toegang te krijgen tot ons netwerk en een test om vanaf het stadskantoor toegang te krijgen tot ons netwerk.

besteden aan de vaardigheden die medewerkers nodig hebben om op basis van deze kennis daadwerkelijk veilig met informatie te werken.

De structurele inbedding van dit programma is nog niet geregeld. In het programma gegevensbescherming nemen wij op dat wij in de tweede helft van 2021 een plan zullen uitwerken om bewustwording op informatieveiligheid structureel een plaats te geven binnen onze organisatie en zullen de raad hierover informeren.

Aanbeveling 3 nemen wij over
Wij beschikken over een gestructureerde procedure voor het melden van datalekken en beveiligings- incidenten. Onze incidentregistratie toont aan dat medewerkers en burgers hier ook gebruik van maken. Wij gaan deze procedure en het belang hiervan opnieuw onder de aandacht brengen en zullen dit periodiek blijven doen. In het structurele plan voor bewustwording op informatieveiligheid nemen wij deze periodieke herhaling op.

Aanbeveling 4 nemen wij over
Ons huidige beleid voor fysieke beveiliging gaat uit van een zoneringsaanpak. Voor toegang tot zones waar een hoog risico op onbevoegde toegang tot gevoelige informatie is hanteren wij een hoger beveiligingsniveau. Wij zullen het huidige beleid voor fysieke beveiliging en de uitvoering daarvan evalueren in het licht van uw bevindingen. Indien nodig laten wij het beleid daarna aanscherpen en/of medewerkers beter instrueren in het volgen hiervan. Wij zullen de raad hierover in de tweede helft van dit jaar informeren.

Dit laat onverlet dat medewerkers zich te allen tijde aan de beveiligingsinstructies moeten houden, wat bij uw testen niet het geval was. We gaan het belang van een goede beveiliging met medewerkers bespreken en de instructies toelichten. Daarnaast gaan we medewerkers beter in staat stellen verbeteringen aan te dragen door ze actiever te betrekken bij het beveiligingsproces.

Hierbij willen wij u opmerkzaam maken op het volgende:

1. Ons stadskantoor en stadhuis zijn ontworpen als open ruimtes om elkaar te ontmoeten en persoonlijk contact te stimuleren. Bij het opvolgen van deze aanbeveling moeten we dus een balans zoeken tussen onze wens tot openheid en onze noodzaak tot veiligheid. Het bepalen van een goede balans is geen eenmalige actie, maar een continu proces.

2. Het stadhuis is het huis van de raad en de raad dient hier dus zelf afwegingen in te maken. Gesprekken hierover zijn op het moment van dit schrijven in volle gang.

Deelconclusie 3: Gemeente kan nog niet risicogestuurd werken, bekende risico's blijven onnodig lang bestaan.

AANBEVELINGEN 5 EN 6:

5. Versnel het uitvoeren van de maatregelen in de roadmap. Voor verdere maatregelen is het ook nodig om na te gaan of eerder getroffen maatregelen hebben gewerkt. Zet daarbij het extra geld voor gegevensbescherming en de uitbreiding van de DISO-capaciteit effectief in. Zorg ook binnen de organisatieonderdelen voor voldoende capaciteit.
6. Voer alle benodigde risicoanalyses uit om een totaalbeeld op te kunnen maken van de huidige stand van de risico's. Benut daarbij de inzet van de extra DISO-capaciteit.

Aanbeveling 5 is reeds in uitvoering

In de loop van 2020 hebben wij financiële en personele middelen beschikbaar gesteld om de uitvoering van de roadmap gegevensbescherming te versnellen. Voorbeelden hiervan zijn informatieveiligheidsbewustzijn, risicogestuurd werken en ICT-beveiliging. Hoewel deze versnelling niet het directe gevolg is van uw rapport, zien we hierin wel een bevestiging dat we de juiste keuzes maken.

De extra DISO-capaciteit wordt ingezet bij alle organisatieonderdelen ter ondersteuning van hun huidige bezetting. Doordat de nieuwe DISO's meerdere organisatieonderdelen ondersteunen op het uitvoeren van de roadmap halen we achterstanden in. Daarnaast verbeteren we de kwaliteit doordat er meer uitwisseling is tussen organisatieonderdelen en DISO's van elkaar kunnen leren.

Aanbeveling 6 nemen wij over

Een juist en volledig inzicht in de risico's op het gebied van gegevensbescherming is essentieel om de risico's te beheersen. Wij zorgen ervoor dat alle resterende risicoanalyses worden uitgevoerd, zodat wij een totaalbeeld krijgen van onze huidige risico's op het gebied van informatieveiligheid.

Een belangrijk punt hierbij is het beter inrichten van de sturing op het risicomanagementproces. In de roadmap gegevensbescherming is een actie opgenomen om gegevensbescherming in de planning- en controlcyclus op te nemen. Daarnaast bieden wij dit jaar voor het eerst het jaarverslag informatieveiligheid aan de raad aan. Zo willen wij de raad beter in staat stellen om te sturen op risicomanagement.

Deelconclusie 4. Beperkt zicht op veilig thuiswerken.

AANBEVELING 7:

Verbeter het toezicht op en de technische beveiligingsmaatregelen voor informatieveiligheid in de thuiswerksituatie.

Aanbeveling 7 nemen wij over
Het verbeteren van het toezicht op en de technische beveiligingsmaatregelen voor informatieveiligheid in de thuiswerksituatie is ingewikkeld. De nieuwe werkplek die wij voornemens zijn uit te rollen bevat de mogelijkheden om alle apparatuur goed te beveiligen.

Als een medewerker thuis gebruikt maakt van privé-apparatuur, zoals een eigen printer of computer, kunnen wij in beperktere mate maatregelen treffen. Wij stellen waar mogelijk beveiligde software beschikbaar en stellen richtlijnen op voor veilig thuiswerken. Technische maatregelen kunnen we in dergelijke situaties echter niet (volledig) afdwingen.

In deze brief zijn wij ingegaan op uw algehele conclusie en een viertal deelconclusies van uw onderzoek naar informatieveiligheid binnen de gemeente. Wij hopen u hiermee voldoende inzicht te bieden in onze vervolgstappen op basis van uw grondige onderzoek.

Met vriendelijke groet,
Burgemeester en wethouders van Utrecht,

25 maart 2021

4 NAWOORD REKENKAMER

Rekenkamer Utrecht dankt het college voor de uitgebreide en gestructureerde reactie op het rapport.

Wij zien dat het college grotendeels instemt met onze conclusies en onze aanbevelingen overneemt. Wij willen hierbij benadrukken om met urgentie uitvoering te geven aan onze aanbevelingen. In dat licht begrijpen wij de nuancering die het college plaatst bij de inmiddels gedane investeringen in middelen en personeel en bij het tijdens het onderzoek afwezige bewustwordingsprogramma voor het personeel. Wij hopen dat deze investeringen vanaf 2021 resultaten op zullen leveren. Vanwege het grote belang van het onderwerp zullen wij de resultaten van deze investeringen en de vorderingen op het gebied van informatiebeveiliging op een later moment nagaan.

Wij zien de behandeling van het rapport en de verdere uitwerking in het plan van aanpak met belangstelling tegemoet

REKENKAMER UTRECHT

wil bijdragen aan het verbeteren van het gemeentelijke bestuur en het versterken van de controlerende rol van de gemeenteraad.

Dat doet de Rekenkamer via het doen van onafhankelijk onderzoek naar de doeltreffendheid en doelmatigheid van het gevoerde beleid en bestuur.

Voor de inwoners van de gemeente Utrecht wil de Rekenkamer zichtbaar maken hoe publiek geld wordt besteed en wat er terecht komt van de voornemens van de gemeente.