DE MENS ALS ZWAKSTE SCHAKEL

EEN OPVOLGINGSONDERZOEK NAAR DE INFORMATIEVEILIGHEID VAN DE GEMEENTE UTRECHT

REKEN KAMER UTRECHT

DE MENS ALS ZWAKSTE SCHAKEL

EEN OPVOLGINGSONDERZOEK NAAR DE INFORMATIEVEILIGHEID VAN DE GEMEENTE UTRECHT

12 december 2024
Eindrapport

REKENKAMER UTRECHT

LEDEN

- Paul Venhoeven (voorzitter)
- Sjoerd Keulen
- Nanda ‘t Lam

MEDEWERKERS ONDERZOEK

- Johan Snoei
- Vince van Houten

CONTACTGEGEVENS

rekenkamer@utrecht.nl
www.utrecht.nl/bestuur-en-organisatie/rekenkamer
Postbus 16200, 3500 CE Utrecht

INHOUD

Deel I Bestuurlijk rapport 6

Onderzoek: Is de informatieveiligheid voldoende gewaarborgd? 6

Conclusie: Informatieveiligheid is verbeterd, maar blijft door menselijk handelen kwetsbaar 8

Deelconclusie 1: Aanbevelingen uit rekenkameronderzoek 2021 grotendeels opgevolgd 9

Deelconclusie 2: Technische risico's uit 2021 beheerst, bij huidige testen geen kritieke risico's aangetroffen 9

Deelconclusie 3: Informatiebewustzijn onder medewerkers nog altijd onvoldoende 9

Deelconclusie 4: Onvoldoende centrale sturing op organisatie en processen 10

Aanbevelingen 11

Aanbeveling 1: Beheers resterende technische risico's en kwetsbaarheden zo spoedig mogelijk 11

Aanbeveling 2: Voer verdere maatregelen uit om de fysieke beveiliging van gebouwen en het informatiebewustzijn van medewerkers te vergroten 11

Aanbeveling 3: Zet binnen de hele organisatie op de lange termijn in op een cultuurverandering 11

Aanbeveling 4: Zorg voor meer centrale aansturing van het informatieveiligheidsbeleid 12

Bestuurlijke reactie college van B&W 12

Nawoord rekenkamer 16

Deel II Nota van bevindingen 18

1 Inleiding: Opvolging en actualiteit 18

2 Context: Centraal beleid wordt decentraal uitgevoerd 22

2.1 Risicogebaseerd werken uitgangspunt bij uitvoering 22

2.2 Opnieuw extra financiële middelen vrijgemaakt voor gegevensbescherming 27

2.3 Organisatieonderdelen zelf verantwoordelijk voor omgaan met en leren van incidenten 29

2.4 Langs managementsysteem voor gegevensbescherming moet verantwoording worden afgelegd 30

3 Organisatie en proces: Wijzigingen vragen om verdere verbetering 32
3.1 Op strategisch niveau ontbreekt een centraal sturingsmechanisme 33
3.2 Op tactisch en operationeel niveau geven organisatieonderdelen hun eigen invulling aan beleid 36

4 Mens: Maatregelen in opzet goed, in de praktijk nog te vrijblijvend 43
4.1 Bewustwordingsplan vastgesteld, uitvoering maatregelen nog te vrijblijvend 44
4.2 Medewerkers kwetsbaar voor externe aanvallen 48

5 Techniek: Informatie beter beveiligd tegen digitale inbraken 53
5.1 Digitale inbraken door technische maatregelen niet meer mogelijk 54
5.2 Thuiswerkplekken technisch goed beveiligd, gedrag op afstand niet controleerbaar 61
5.3 Wisselende ervaringen met de fysieke beveiliging van gemeentelijke gebouwen 63

6 Opvolging: Grotendeels op orde 66
6.1 Meeste maatregelen uitgevoerd, na sterk vertraagde uitvoering 67
6.2 Rekenkamerrapport droeg bij aan urgentie van informatieveiligheid 68
6.3 Gemeenteraad goed door college geïnformeerd over opvolging raadsbesluit 70

BIJLAGE 1 Afkortingen 72
BIJLAGE 2 Onderzoeksverantwoording 74

DEEL I BESTUURLIJK RAPPORT

ONDERZOEK: IS DE INFORMATIEVEILIGHEID VOLDOENDE GEWAARBORGD?

Aanleiding
Gemeenten verwerken steeds grotere hoeveelheden informatie. De laatste decennia gebeurt dat in allerlei gedigitaliseerde en geautomatiseerde systemen en programma's. De verwerkte informatie bevat vaak (bijzondere) persoonsgegevens, zogeheten 'kroonjuwelen', die goed beschermd moeten zijn. De informatieveiligheid moet daarom op alle aspecten – in organisatie en proces, bij medewerkers en in de techniek – voldoende geborgd zijn. In 2021 voerde Rekenkamer Utrecht onderzoek uit naar de manier waarop de gemeente Utrecht invulling gaf aan die drie aspecten van informatieveiligheid. De uitkomsten daarvan gaven de rekenkamer aanleiding om het onderwerp te blijven volgen. We gaven in ons bestuurlijk rapport ook aan op een later moment een opvolgingsonderzoek uit te zullen voeren.

Doel en centrale vraag
Het doel van dit onderzoek is om de Utrechtse gemeenteraad inzicht te geven in de mate waarin de besluiten naar aanleiding van het rekenkamerrapport "*Zo sterk als de zwakste schakel*" zijn opgevolgd. Daarnaast besteden we aandacht aan aanvullende onderwerpen die in het onderzoek uit 2021 onderbelicht zijn gebleven. Het gaat onder meer om de managementinformatie, de afhandeling van incidenten, het gebruik van de gemeentelijke telefoons en de maatregelen om het thuiswerken te beveiligen.

De centrale vraag van het onderzoek is:

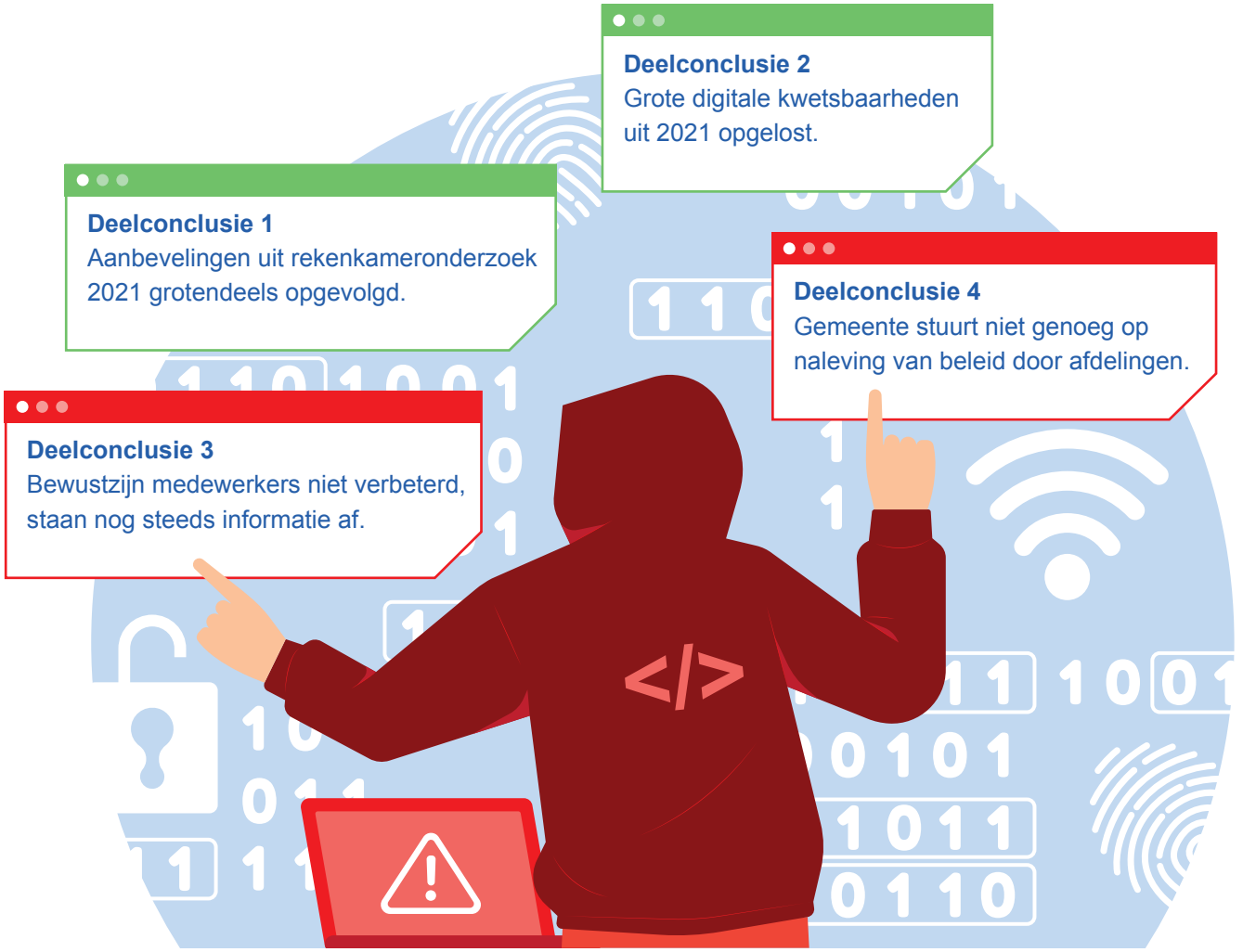
In hoeverre heeft de gemeente Utrecht uitvoering gegeven aan de aanbevelingen van het rekenkameronderzoek uit 2021 en is de informatieveiligheid nu voldoende gewaarborgd?

Werkwijze
Het onderzoek is uitgevoerd in de periode februari 2024 tot en met juli 2024. Naast de documentstudie en analyse van beschikbare data hebben wij interviews gehouden met medewerkers van Informatie- en Procesmanagement (IPM) en andere medewerkers binnen de gemeentelijke organisatie die een verantwoordelijkheid dragen voor informatieveiligheid. Wij bedanken de betrokken medewerkers hartelijk voor hun bijdrage aan het onderzoek. We hebben daarnaast NFIR B.V. opdracht verleend voor het uitvoeren van testen om oneigenlijk toegang te krijgen tot digitale en fysieke informatie bij de gemeente. Een uitgebreide toelichting op de onderzoeksmethode is opgenomen in bijlage 1.

REKENKAMER UTRECHT

De informatieveiligheid is verbeterd, maar blijft door menselijk handelen kwetsbaar

In 2021 zag de rekenkamer dat de informatieveiligheid bij de gemeente Utrecht niet op orde was. De rekenkamer heeft daarom nu opnieuw onderzoek gedaan. Daaruit blijkt dat de digitale beveiliging van informatie is verbeterd, maar dat het menselijk handelen nog steeds kwetsbaar is.



Aanbevelingen om de informatieveiligheid te verbeteren

1. Los de resterende digitale kwetsbaarheden snel op.
2. Verbeter de beveiliging van gebouwen verder en vergroot het bewustzijn van medewerkers.
3. Zet in op een cultuurverandering zodat medewerkers verantwoordelijkheid nemen en actief onbekenden aanspreken.
4. Zorg voor betere naleving van beleid door meer centraal te sturen.

CONCLUSIE: INFORMATIEVEILIGHEID IS VERBETERD, MAAR BLIJFT DOOR MENSELIJK HANDELEN KWETSBAAR

Met ons onderzoek uit 2021 concludeerden we dat informatie binnen de gemeente Utrecht niet altijd goed beschermd was. We zagen met name op het gebied van de techniek en het menselijk handelen kritieke kwetsbaarheden.

Op basis van de bevindingen van dit opvolgingsonderzoek komen we nu tot de volgende hoofdconclusie met vier deelconclusies. Wij formuleren hierbij ook vier aanbevelingen.

Hoofdconclusie

Met de technische kant van informatieveiligheid is de gemeente Utrecht de afgelopen jaren goed aan de slag gegaan. Zo zijn maatregelen genomen om de technische risico's en kwetsbaarheden aan te pakken. De zeer kwetsbare werkstations van de medewerkers zijn vervangen. De afgelopen jaren zijn er ook meer analyses uitgevoerd om risico's te identificeren. Daarnaast is de technische beveiliging bij het thuiswerken verbeterd door laptops en telefoons te verstrekken die door de gemeente worden beheerd.

Organisatieonderdelen zijn zelf verantwoordelijk voor het identificeren en beheersen van de verschillende risico's rond informatieveiligheid. Hierin zijn achterstanden ontstaan. Risico's blijven mede daardoor lang bestaan. Zo is er op systemen nog verouderde software aanwezig die niet langer onderhouden wordt. Software wordt daardoor kwetsbaar en kan door hackers worden uitgebuit. Vanuit de directie is hier te weinig op toegezien en gehandhaafd.

Er is wel geïnvesteerd in de fysieke beveiliging van de gemeentelijke gebouwen en in het bewustzijn van de medewerkers, maar deze maatregelen schieten nog tekort. Het medewerkersgedeelte van het Stadskantoor blijkt op dit moment nog eenvoudig door onbevoegden te betreden en nog te weinig medewerkers gaan veilig met informatie om.

Het menselijk handelen is de afgelopen jaren niet aantoonbaar verbeterd. De mens blijkt daarmee de zwakste schakel bij de informatieveiligheid, waardoor deze nog niet volledig is gewaarborgd. Aangekondigde maatregelen om het bewustzijn van medewerkers te vergroten zijn niet of te vrijblijvend doorgevoerd. Medewerkers staan tijdens phishing-acties nog steeds gevoelige informatie zoals inloggegevens af. En medewerkers spreken onbevoegden die gemeentelijke gebouwen weten te betreden niet aan, waardoor deze langere tijd binnen kunnen verblijven.

DEELCONCLUSIE 1: AANBEVELINGEN UIT REKENKAMERONDERZOEK 2021 GROTENDEELS OPGEVOLGD

In 2021 zijn de zeven aanbevelingen van de rekenkamer unaniem overgenomen door de gemeenteraad. De gemeente was tijdens de behandeling van het rapport al gestart met het treffen van technische maatregelen om de geïdentificeerde kwetsbaarheden te beheersen. Die maatregelen zijn de afgelopen jaren verder doorgezet. De uitvoering van deze maatregelen heeft wel lang geduurd. Dit komt door een gebrek aan capaciteit, onvoldoende daadkracht, de organisatiecultuur en de grote financiële investeringen die voor een aantal maatregelen nodig waren. De gemeenteraad is in de afgelopen jaren wel goed over de voortgang geïnformeerd.

DEELCONCLUSIE 2: TECHNISCHE RISICO'S UIT 2021 BEHEERST, BIJ HUIDIGE TESTEN GEEN KRITIEKE RISICO'S AANGETROFFEN

Vrijwel alle technische risico's die in 2021 nog openstonden zijn opgelost. Er zijn daarmee geen kritieke risico's meer aanwezig. Uit de nieuwe penetratietesten van dit onderzoek bleek wel dat er nog altijd verouderde software aanwezig is. Dit krijgt te weinig aandacht, terwijl het wel tot kwetsbaarheden leidt. De laptops en telefoons die door de gemeente worden beheerd en uitgegeven blijken technisch goed beveiligd. Door de invoering van multi-factor authenticatie is de informatieveiligheid bij het thuis- en op afstand werken van medewerkers sterk verbeterd.

Dit geldt niet voor de fysieke beveiliging van het Stadskantoor. Onderzoeksbureau NFIR heeft in opdracht van de rekenkamer getracht zonder bevoegdheid het Stadskantoor en Stadhuis te betreden. Insluipers konden tijdens deze inlooptesten vrijwel altijd het Stadskantoor binnenkomen. De fysieke beveiliging van het Stadhuis is door de grote inspanningen sinds 2021 sterk verbeterd. Indringen was daardoor lastig, maar niet onmogelijk doordat medewerkers nog altijd onoplettend waren.

DEELCONCLUSIE 3: INFORMATIEBEWUSTZIJN ONDER MEDEWERKERS NOG ALTIJD ONVOLDOENDE

Nog te weinig medewerkers gaan bewust om met informatie. Er zijn veel maatregelen genomen om dit te verbeteren, maar dit levert nog te weinig resultaten op omdat de uitvoering vrijblijvend is. Zo is deelname aan de e-learning – één van de belangrijkste maatregelen op dit aspect – te laag en zijn er aanzienlijke verschillen tussen organisatieonderdelen. Raads-, commissie- en fractieleden worden zelfs helemaal niet voor de e-learning uitgenodigd. Dat geldt ook voor de leden van de rekenkamer. De e-learning biedt daarnaast inhoudelijk te weinig maatwerk waardoor de aanpak niet altijd aansluit op de behoeften van de verschillende organisatieonderdelen. Daardoor is het gedrag van medewerkers onvoldoende veranderd.

Onderzoeksbureau NFIR heeft namens de rekenkamer testen uitgevoerd om het informatieveiligheidsbewustzijn van medewerkers te bepalen. Medewerkers trappen nog steeds in de USB-dropping en staan hun inloggegevens af tijdens de *voice phishingtest*. Ook de organisatiecultuur is onveranderd. Medewerkers spreken elkaar te weinig aan op ongewenst gedrag en onbekenden worden niet op hun aanwezigheid aangesproken.

DEELCONCLUSIE 4: ONVOLDOENDE CENTRALE STURING OP ORGANISATIE EN PROCESSEN

Het thema informatieveiligheid is gedecentraliseerd naar de verschillende organisatieonderdelen. We zien daardoor een strategisch risico ontstaan: op dit moment ontbreekt het op sleutelposities aan overzicht, slagkracht en mandaat om met informatieveiligheid aan de slag te gaan. De voortgang van maatregelen duurt daardoor lang en hangt te veel af van de bereidwilligheid van leidinggevenden en de individuele medewerkers. Naleving wordt niet 'van bovenaf' afgedwongen. Dat leidt ertoe dat de gemeente niet altijd *in control* is, bijvoorbeeld als het gaat om het leveranciers- en contractmanagement. Hierdoor kan verouderde software op de IT-systemen aanwezig blijven die niet meer door de leverancier wordt ondersteund (*end-of-life*). Dit maakt systemen onnodig kwetsbaar.

In 2021 stond de gemeente Utrecht nog aan het begin van het risicogebaseerd werken. Met deze methode zouden geïdentificeerde risico's moeten worden geclassificeerd (hoe groot is het risico?), afgewogen en vervolgens wel of niet worden beheerst (teruggebracht naar een acceptabel niveau). In de praktijk zien we dat er inmiddels meer risicoanalyses worden uitgevoerd om risico's te identificeren, maar blijven achterstanden bestaan. Op tactisch niveau worden risico's geïdentificeerd die op een heel organisatieonderdeel van toepassing zijn. Wij constateren dat voor een meerderheid van de geïdentificeerde tactische risico's geen beheersmaatregelen worden genomen. Deze risico's staan ook vaak al (te) lang open. En het wordt onvoldoende duidelijk of er een risicogebaseerde afweging ten grondslag ligt aan de tactische risico's die wél zijn beheerst. We kunnen door een gebrek aan informatie ook niet vaststellen hoe het er met het beheersen van de geïdentificeerde operationele risico's voor staat. Dit zijn risico's die van toepassing zijn op één proces of applicatie binnen een organisatieonderdeel.

Organisatieonderdelen worden bij het verbeteren van de informatieveiligheid ondersteund door gemeentelijke medewerkers van informatie- en procesmanagement. Deze ondersteuning wordt niet risicogebaseerd verdeeld. Dat leidt ertoe dat organisatieonderdelen die met cruciale systemen werken – zoals de basisregistratie personen of privacygevoelige informatie zoals uitkeringsinformatie – niet per definitie meer ondersteuningsinzet krijgen. Organisatieonderdelen leren daarnaast op hun eigen manier van beveiligingsincidenten,

maar leren door een gebrek aan kennisuitwisseling en een centraal registratiesysteem niet van elkaar.

AANBEVELINGEN

Op basis van de hiervoor toegelichte hoofdconclusie en de vier deelconclusies doen we vier aanbevelingen verdeeld over de drie aspecten techniek (aanbeveling 1), mens (2 en 3) en organisatie (4). Omdat de mens de zwakste schakel is bij informatieveiligheid hebben we voor dit aspect twee aanbevelingen geformuleerd: één voor de korte en één voor de lange termijn.

AANBEVELING 1: BEHEERS RESTERENDE TECHNISCHE RISICO'S EN KWETSBAARHEDEN ZO SPOEDIG MOGELIJK

Kijk daarbij met voorrang naar de kwetsbaarheden met de hoogste risico's, zoals de verouderde software die bij herhaling is aangetroffen.

AANBEVELING 2: VOER VERDERE MAATREGELEN UIT OM DE FYSIEKE BEVEILIGING VAN GEBOUWEN EN HET INFORMATIE-BEWUSTZIJN VAN MEDEWERKERS TE VERGROTEN

Geef bij het verbeteren van de fysieke beveiliging voorrang aan de gebouwen met een publieksfunctie en waar met gevoelige informatie wordt gewerkt. Het gaat dan met name om het Stadskantoor en het Stadhuis.

Handhaaf het minimale niveau voor de e-learning om op de korte termijn het informatiebewustzijn onder medewerkers te vergroten, ook voor de leden van gemeenteraad en personen die hen ondersteunen. En voer de maatregelen uit het programma informatiebewustzijn consequent uit. Herhaal maatregelen die de bewustwording vergroten. Vooral het uitvoeren van phishing- en penetratietesten zijn een must om het bewustzijn blijvend te vergroten en de enige echte test om de robuustheid van de informatiebeveiliging te meten.

AANBEVELING 3: ZET BINNEN DE HELE ORGANISATIE OP DE LANGE TERMIJN IN OP EEN CULTUURVERANDERING

Rondom het menselijk handelen op informatieveiligheid moet de organisatie van een cultuur van toezien en afwachten naar een cultuur van actief aanspreken en verantwoordelijkheid nemen. Die verandering moet breder worden ingezet dan alleen met de huidige focus op nieuwe medewerkers via het introductieprogramma.

AANBEVELING 4: ZORG VOOR MEER CENTRALE AANSTURING VAN HET INFORMATIEVEILIGHEIDSBELEID

Dwing naleving en uitvoering van beleid met centrale sturing af, waarbij ook ruimte is voor maatwerk per organisatieonderdeel. Verbeter het risicogebaseerd werken door ondersteuningscapaciteit op basis van risico's en gebruik van cruciale systemen aan de organisatieonderdelen toe te wijzen. Richt de registratie- en managementinformatiesystemen uniform in, zodat gemeentebreed inzicht bestaat in de ontwikkelingen en incidenten, en zodat daarmee effectiever geleerd en verbeterd kan worden.

BESTUURLIJKE REACTIE COLLEGE VAN B&W

Wij danken u voor het toesturen van uw rapport *De mens als zwakste schakel - Een opvolgingsonderzoek naar de Informatieveiligheid van de gemeente Utrecht*. U heeft onderzocht in hoeverre wij de aanbevelingen uit het vorige rekenkameronderzoek hebben opgevolgd en of de informatieveiligheid voldoende geborgd is. We spreken onze waardering uit voor uw grondige analyse. Uw rapport geeft ons waardevolle inzichten die we kunnen gebruiken in de doorlopende verbetering van informatieveiligheid.

Conclusie
In een steeds verder digitaliserende stad als Utrecht is informatieveiligheid niet alleen een technische noodzaak, maar een fundamenteel onderdeel van onze maatschappelijke verantwoordelijkheid. Het is als onderdeel van het geheel van gegevensbescherming essentieel voor het vertrouwen van onze burgers, het beschermen van hun rechten en vrijheden, en het realiseren van onze missie voor een gezond stedelijk leven voor iedereen.

Het doet ons daarom deugd dat u oordeelt dat de technische beveiliging en de fysieke beveiliging van het Stadhuis sterk verbeterd zijn. We onderschrijven deze conclusie. We hebben in de afgelopen jaren geïnvesteerd in het oplossen en structureel beheersen van de grootste technische risico's. Dit is een complexe opgave die inzet van vele professionals vraagt. Uw onderzoek en conclusies laten zien dat deze inzet zijn vruchten afwerpt.

Tegelijk laat uw onderzoek zien dat er nog steeds kwetsbaarheden zijn. Uw onderzoek bevestigt dat informatieveiligheid blijvende aandacht nodig heeft. Het laat zien dat hier met name sprake van is bij het bewustzijn onder medewerkers, de fysieke beveiliging van het Stadskantoor en de centrale aansturing van informatieveiligheid. We herkennen het beeld dat u schetst en de conclusies die u daarover trekt.

Hieronder gaan wij in op de aanbevelingen die u doet. De huidige financiële situatie van de gemeente kan hierbij niet onbenoemd blijven. Er is geen extra geld beschikbaar om aanbevelingen uitgebreid aan te pakken. Sterker nog, er moeten nog besparingen worden

gerealiseerd en er zal moeten worden geprioriteerd. De opvolging van de aanbevelingen moet dan ook in dat licht worden bezien. We zetten bestaande middelen optimaal in om de aanbevelingen te realiseren, maar doen dit risicogestuurd. Dat wil zeggen dat we de grotere risico's sneller adresseren dan de lagere risico's. We doen daarbij doorlopend de afweging van de kosten van maatregelen versus de te verwachten afname van risico's. Dit kan ook betekenen dat we soms bewust besluiten om risico's (nog) niet te adresseren maar ze expliciet te accepteren.

Aanbevelingen

Aanbeveling 1: Beheers resterende technische risico's en kwetsbaarheden zo spoedig mogelijk.

*Aanbeveling 1 nemen wij over***.**

We hebben een vast intern proces voor het identificeren, beheren en bewaken van technische kwetsbaarheden. Wij hebben deze kwetsbaarheden in dat proces opgenomen. De opvolging van technische risico's en kwetsbaarheden wordt geprioriteerd aan de hand van het corresponderende risiconiveau. We hanteren hierbij een richttijd van één tot twee maanden voor kwetsbaarheden in de categorie Hoog, zes maanden voor de categorie Midden en een best effort inzet op de categorie Laag. Ons proces voor het beheersen van technische kwetsbaarheden wordt op dit moment uitgebreid zodat we beter in staat zijn om ook door externe partijen gemelde technische kwetsbaarheden op te volgen.

De bevindingen die in uw rapport ter informatie zijn opgenomen beoordelen we om vast te stellen of er sprake is van een risico voor de gemeente en volgen we op waar nodig.

Aanbeveling 2: Voer verdere maatregelen uit om de fysieke beveiliging van gebouwen en het informatie-bewustzijn van medewerkers te vergroten.

Aanbeveling 2 nemen wij over, hier is al progressie op geboekt.

Ten aanzien van *fysieke beveiliging* hebben we na uw vorig onderzoek de beveiliging van het stadhuis en het stadskantoor geëvalueerd via een dreiging- en risicoassessment. Op basis hiervan zijn aanvullende maatregelen genomen, vanuit risico perspectief eerst op het stadhuis en later op het stadskantoor. Voor het stadskantoor wordt een deel van de maatregelen op dit moment nog uitgevoerd. Onveranderd ten opzichte van uw vorig onderzoek is dat ons stadskantoor en stadhuis zijn ontworpen met een open karakter om elkaar te ontmoeten en persoonlijk contact te stimuleren. Bij de door de concerndirectie (stadskantoor) en het presidium (stadhuis) besloten maatregelen is een balans gezocht tussen de wens tot openheid en de noodzaak tot veiligheid.

De genomen maatregelen van het stadhuis worden in het licht van uw bevindingen geëvalueerd en de geplande maatregelen van het stadskantoor worden reeds uitgevoerd. Na implementatie van de maatregelen op het stadskantoor en eventueel stadhuis wordt risico gebaseerd gekeken naar de andere locaties zoals wijkbureaus en JGZ locaties. Het evalueren van de genomen maatregelen door een periodieke dreiging- en risicoassessment en het toetsen van de effectiviteit van de maatregelen door periodieke inlooptesten maken we structureel onderdeel van onze aanpak.

We onderschrijven het belang van *informatiebewustzijn*. Naast informatieveiligheid besteden we hier aandacht aan in het Programma Informatie op Orde. Dit programma draagt onder andere via een eigen e-learning bij aan het informatiebewustzijn. Onder de Regeling Risicovolle Projecten wordt de raad over de voortgang van dit programma geïnformeerd. We zetten bovendien extra in op informatiebewustzijn met de nieuwe functie Adviseur Bewustwording en Adoptie binnen het domein Informatie- en Procesmanagement (IPM). Daarmee krijgt bewustwording in de volle (IPM-) breedte meer aandacht. Ten aanzien van het bewustzijnsprogramma hebben we ook al een aantal aanvullende stappen gezet. E-learning hebben we verplicht gesteld voor alle medewerkers. Het management krijgt voortgangsrapportages en stuurt actief op het verhogen van de deelname. Dezelfde e-learning wordt inmiddels aangeboden aan de leden van de gemeenteraad en de personen die hen ondersteunen, waaronder de Rekenkamer. Ook hebben we sinds de afronding van uw onderzoek een phishing test met voorlichtingscampagne uitgevoerd.

Het bestaande bewustwordingsplan zal worden hernieuwd waarbij nadrukkelijk aandacht besteed zal worden aan het inzetten van instrumenten zoals *phishing*tests en mystery guests. Deze instrumenten dienen dan zowel voor bewustwording van medewerkers als voor het meten van het effect van de activiteiten rondom informatiebewustzijn.

We merken hierbij op dat maatregelen ten aanzien van informatiebewustzijn proportioneel genomen zullen worden. Dat wil zeggen dat we ook hier blijvend onze maatregelen afwegen ten opzichte van andere belangen zoals de kosten en de benodigde tijdsinvestering van medewerkers.

Aanbeveling 3: Zet binnen de hele organisatie in op de lange termijn in op een cultuurverandering.

Aanbeveling 3 nemen we over.

In de afgelopen jaren hebben we geïnvesteerd in het informatiebewustzijn. Houding en gedrag zijn verankerd in de doelen van ons bewustwordingsprogramma informatieveiligheid. Een van de doelstellingen van ons programma is het realiseren van voorbeeldgedrag door het management en het door het management aanspreken van medewerkers op het naleven van interne regels en afspraken. Zo heeft het management een uitdragende en sturende rol

bij de (inmiddels verplichte) e-learning. Dit voorbeeldgedrag vanuit het management zien we als de cruciaal om een cultuur te creëren van aanspreken en verantwoordelijkheid nemen. In de hernieuwing van plan voor informatiebewustzijn maken we dit het centrale speerpunt.

Deze rol van het management is in lijn met de Cyberbeveiligingswet die in 2025 wordt verwacht als invulling van de Europese NIS2 richtlijn. Het doel van de Cyberbeveiligingswet is onder andere om binnen essentiële entiteiten zoals de gemeente Utrecht een cyberweerbaarheidscultuur neer te zetten Het management krijgt een expliciete rol in het goedkeuren van en toezien op maatregelen behorend bij cyber-risico's. Ze moet zich scholen zodat ze aantoonbaar beschikt over de hiervoor benodigde kennis en vaardigheden. De implementatie van deze wet zal vanaf de tweede helft van 2025 bijdragen aan de realisatie van uw aanbeveling.

Tegelijk is de cultuur rondom informatieveiligheid niet los te zien van de bredere organisatiecultuur. Die organisatiecultuur is onderdeel van de organisatieontwikkeling die vanuit de concerndirectie is ingezet door de introductie van Duidelijk, Resultaatgericht en Aanspreekbaar (DRA) als basiselementen van onze nieuwe cultuur. In deze organisatieontwikkeling nemen we informatieveiligheid mee. We gaan de duidelijkheid vergroten zodat iedereen weet wat ons beleid is, we gaan concrete resultaatgerichte afspraken maken daarover en gaan mensen daarop aanspreken.

Aanbeveling 4: Zorg voor meer centrale aansturing van het informatieveiligheidsbeleid.

Aanbeveling 4 nemen wij over.

We onderschrijven het belang van duidelijke aansturing van het informatieveiligheidsbeleid. We hebben voor de aansturing van gegevensbescherming, waar informatieveiligheid onder valt, een managementsysteem. Dit bevat een cyclisch Plan, Do, Act, Check (PDCA-)proces voor centrale aansturing van het beleid met als vertrekpunt (strategisch) risicomanagement. Dit proces is essentieel in het concern breed maken en effectueren van keuzes, waaronder het afdwingen van beleid wanneer nodig. Dit afdwingen van het beleid gaan we verbeteren. De noodzaak voor centrale aansturing is in lijn met de Cyberbeveiligingswet en de eerder benoemde organisatieontwikkeling (DRA).

Bij het verbeteren van onze centrale sturing op het informatieveiligheidsbeleid verbeteren we ook de monitoring van de naleving en uitvoering van dit beleid zodat we betere sturingsinformatie hebben. Dit is een randvoorwaarde om mogelijke strategische risico's tijdig te identificeren en te kunnen beheersen. Bijvoorbeeld om te signaleren dat geplande beheersing van (tactische) risico's middels maatregelen achterblijft; dat onderdelen van de organisatie afwijken van beleid; of dat het geheel van risico's onze risicobereidheid overstijgt. Het zorgt er bovendien voor dat we een hogere mate van zekerheid hebben over de actuele

stand van zaken wanneer we verantwoording afleggen over informatiebeveiliging in de ENSIA-cyclus.
Als onderdeel van het verbeteren van centrale aansturing gaan we ook de inzet van beschikbare capaciteit omvormen naar een meer risico-gestuurde inzet van capaciteit. Dit zorgt ervoor dat we onze inzet richten op de grootste risico's en belangrijkste gemeentelijke processen.

Tot slot
Wij danken u voor uw herhaalde aandacht voor het onderwerp. Wij herkennen uw aanbevelingen en betrekken die in de verdere verbetering van informatieveiligheid.

Hoogachtend,
Burgemeester en wethouders van Utrecht,

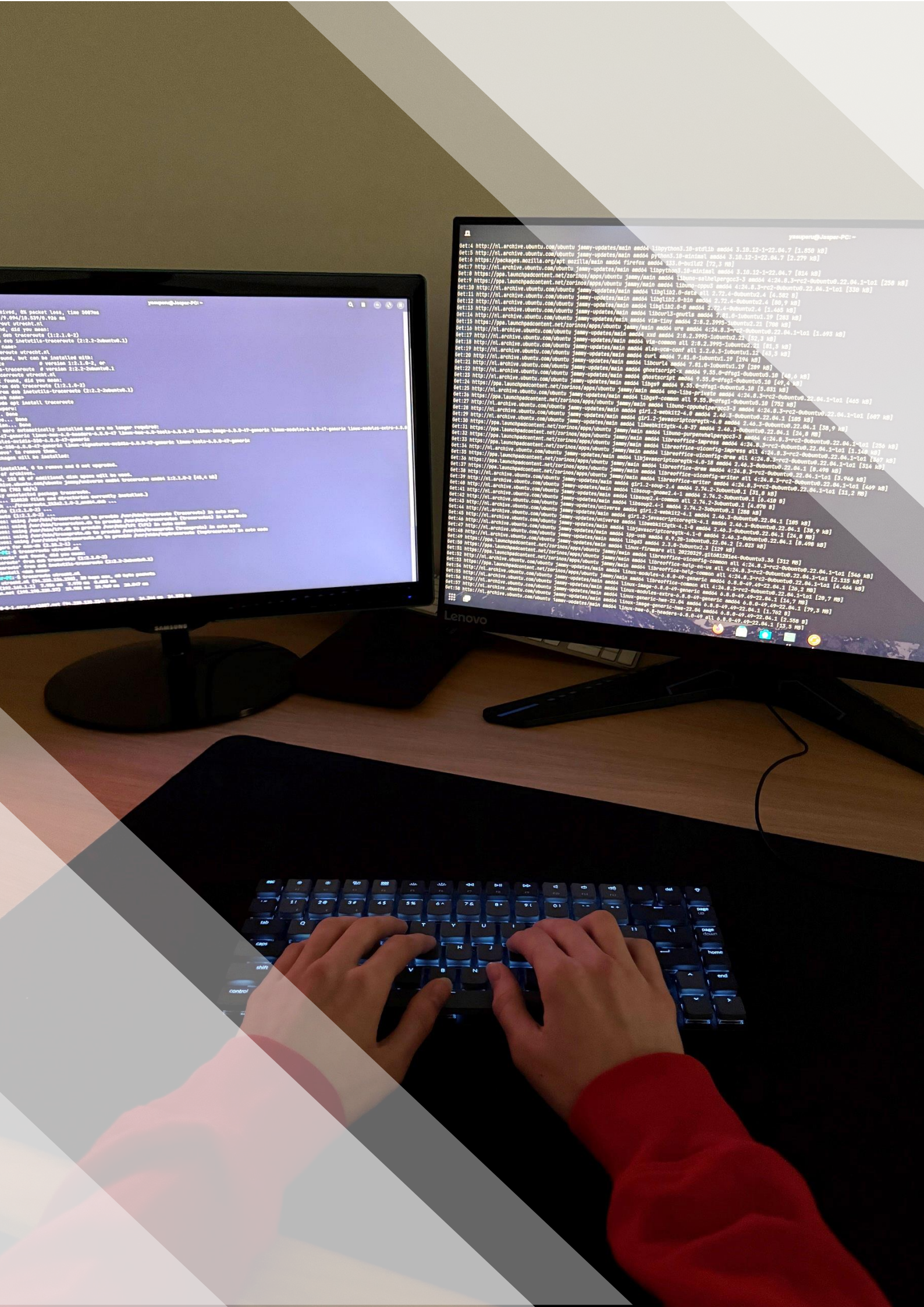
4 december 2024

NAWOORD REKENKAMER

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

Wij zien dat het college onze conclusies herkent en onderschrijft en al onze aanbevelingen overneemt. Wij onderstrepen het belang om blijvend aandacht te besteden aan de informatieveiligheid. Ook in tijden van bezuinigingen.

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



DEEL II NOTA VAN BEVINDINGEN

1 INLEIDING: OPVOLGING EN ACTUALITEIT

1.1 AANLEIDING

Gemeenten verwerken steeds grotere hoeveelheden informatie. De laatste decennia gebeurt dat in allerlei gedigitaliseerde en geautomatiseerde systemen en programma's. De verwerkte informatie bevat vaak (bijzondere) persoonsgegevens die goed beschermd moeten zijn. De informatieveiligheid moet daarom op alle aspecten – in organisatie en proces, bij de medewerkers en in de techniek – voldoende geborgd zijn. In 2021 voerde Rekenkamer Utrecht onderzoek uit naar de manier waarop de gemeente Utrecht invulling gaf aan de drie aspecten van informatieveiligheid. De uitkomsten gaven ons aanleiding om het onderwerp te blijven volgen. We gaven in ons bestuurlijk rapport daarom aan op een later moment (na ongeveer een jaar) een opvolgingsonderzoek uit te gaan voeren. In september 2022 heeft concernaudit een follow-up audit uitgevoerd naar de stand van zaken van de uitvoering van het raadsbesluit. Mede op basis daarvan besloot de rekenkamer om het aangekondigde opvolgingsonderzoek uit te stellen. Uiteindelijk heeft de rekenkamer in de periode februari tot en met juli 2024 onderzoek gedaan naar de opvolging van aanbevelingen uit 2021 en de actuele stand van zaken van de informatieveiligheid.

1.2 DOEL EN ONDERZOEKSVRAGEN

Het doel van dit onderzoek is om de Utrechtse gemeenteraad inzicht te geven in de mate waarin de besluiten naar aanleiding van het rekenkamerrapport "*Zo sterk als de zwakste schakel*" zijn opgevolgd. Daarnaast besteden we aandacht aan aanvullende onderwerpen die in het onderzoek uit 2021 onderbelicht waren gebleven. Het gaat onder meer om de managementinformatie, de afhandeling van incidenten, het gebruik van de gemeentelijke telefoons en de maatregelen om het thuiswerken te beveiligen.

De centrale vraag van het onderzoek luidt:

In hoeverre heeft de gemeente Utrecht uitvoering gegeven aan de aanbevelingen van het rekenkameronderzoek uit 2021 en is de informatieveiligheid nu voldoende gewaarborgd?

Deze centrale vraag werken we uit aan de hand van vier onderzoeksvragen:

1) Organisatie en proces:
    a. In hoeverre zijn de aanbevelingen over het onderdeel organisatie en proces door de gemeente Utrecht opgevolgd?
    b. Aanvullend: In hoeverre zijn de afhandeling van incidenten en meldingen, de managementinformatie en het incidentenmanagementproces adequaat?
2) Mens:
    a. In hoeverre zijn de aanbevelingen over het onderdeel mens door de gemeente Utrecht opgevolgd?
3) Techniek:
    a. In hoeverre zijn de aanbevelingen over het onderdeel techniek door de gemeente Utrecht opgevolgd?
    b. Aanvullend: in hoeverre is bij het gebruik van gemeentelijke telefoons en bij het thuiswerken de informatieveiligheid technisch beveiligd?
4) Welke (verdere) maatregelen zijn mogelijk om de informatieveiligheid te optimaliseren?

Bij de beantwoording van de onderzoeksvragen hebben wij een normenkader gehanteerd. De gehanteerde normen sluiten aan bij de normen uit het rekenkameronderzoek uit 2021 naar dit onderwerp. Aan het begin van de hoofdstukken zijn per onderzoeksvraag de bijbehorende normen en criteria met daarbij een beoordeling naar de mate waarin eraan wordt voldaan (rood, oranje, groen, grijs) opgenomen. Een rood vlak betekent dat er niet aan de norm voldaan wordt. Oranje wijst erop dat er deels aan de norm wordt voldaan en groen wil zeggen dat er (grotendeels) aan de norm voldaan is. Met grijs wordt aangegeven dat de realisatie ten opzichte van de norm niet door de rekenkamer te beoordelen is.

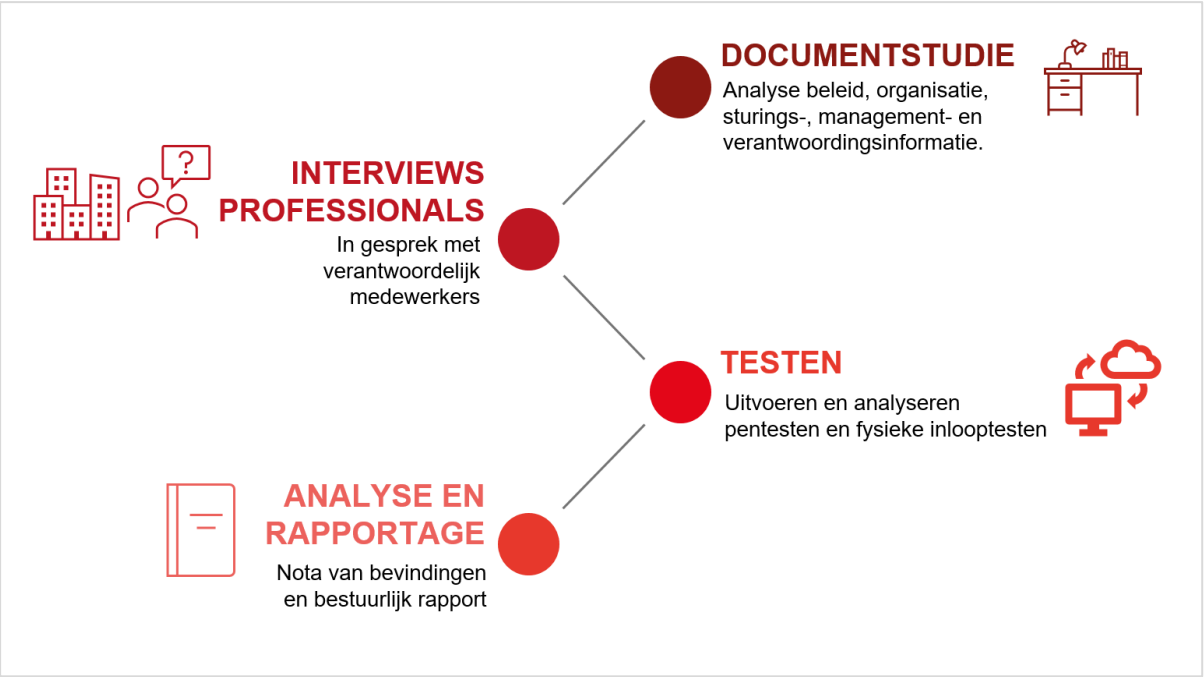
1.3 WERKWIJZE EN AFBAKENING

Werkwijze

Het onderzoek voerden wij uit aan de hand van onderstaande vier stappen. De werkwijze in het onderzoek lichten wij nader toe in bijlage 1.

Bij de analyse van de doorwerking hanteren wij het analyseschema zoals wij dat hebben ontworpen voor een breder opvolgingsonderzoek[1] van de rekenkamer uit 2020. In dit schema worden verschillende fasen van doorwerking benoemd die gerelateerd zijn aan het proces van onderzoek, de raadsbehandeling en de opvolging van het raadsbesluit. Het gaat dan om het agenderen en bespreken, besluiten, implementeren, effectueren en publiek verantwoorden.

[1] Rekenkamer Utrecht (2020). *Opvolgingsonderzoek rekenkamerrapporten 2014-2018. Inzicht in de doorwerking van rekenkameronderzoek en de opvolging van raadsbesluiten*.



Afbakening

Wij hebben verschillende keuzes gemaakt om het onderzoek af te bakenen. Deze beschrijven we hieronder puntsgewijs:

- Met dit onderzoek kijken we naar de drie eerdergenoemde onderdelen: organisatie en proces, mens en techniek. Daarbij besteden we per onderdeel specifiek aandacht aan aanvullende onderwerpen die onder andere bij de raadsbehandeling in 2021 zijn benoemd.
- De focus van ons onderzoek ligt op de periode vanaf de uitvoering van het eerdere onderzoek (in het najaar van 2020) tot op heden.
- We voeren geen aanvullende risicoanalyses en audits uit, maar maken gebruik van de informatie die er op dit onderdeel al is en welke maatregelen de gemeente naar aanleiding van de analyses heeft genomen.
- Er zal geen vergelijking plaatsvinden met andere gemeenten. Het onderzoeksterrein is continu in beweging en ook de inrichting van de organisatie en systemen verschilt sterk. Bij het onderzoek in het najaar van 2020 bleek al dat de situatie bij andere gemeenten te afwijkend was om een goede inhoudelijke benchmark te kunnen opstellen.
- We zullen de doorwerking van het rekenkamerrapport uit 2021 beoordelen. Deze beoordeling is gericht op de onderdelen implementeren, effectueren en (publiek) verantwoorden. Bij ‘implementeren’ gaat het om de vraag of de aanbevelingen door het college van Burgemeester en Wethouders (B&W) en de ambtelijke organisatie zijn doorgevoerd in de organisatie, het beleid en/of de uitvoering. Effectueren gaat om het effect op het gevoerde beleid en op het realiseren van de beoogde maatschappelijke effecten van dit beleid. Het publiek verantwoorden heeft betrekking op de verantwoording van het college aan de gemeenteraad over de uitvoering van het raadsbesluit.

1.4 LEESWIJZER

Om inzicht te krijgen in de belangrijkste bevindingen van het onderzoek volstaat het kennisnemen van de inleiding op de verschillende hoofdstukken en de ingevulde delen van het normenkader. Voor een nadere toelichting op deze bevindingen verwijzen we naar de uitwerking in de onderliggende paragrafen.

In hoofdstuk 2 beschrijven we hoe de gemeente Utrecht in de organisatie en processen aandacht besteedt aan informatieveiligheid. In hoofdstuk 3 beoordelen we in hoeverre de gemeente Utrecht hierbij risicogebaseerd werkt. In hoofdstuk 4 gaan we in op de manier waarop bewustwording een plaats krijgt in beleid en organisatie en hoe de medewerkers van de gemeente hier in de praktijk mee omgaan. In hoofdstuk 5 presenteren we op hoofdlijnen de uitkomsten van testen die wij door een extern bureau (NFIR B.V.) hebben laten uitvoeren op de technische aspecten van de informatiebeveiliging. De onderliggende rapportages worden in verband met de risico's en kwetsbaarheden niet openbaar gemaakt, maar zijn wel gedeeld met de gemeentelijke organisatie. De gemeente heeft inmiddels op de geconstateerde kwetsbaarheden waar nodig actie ondernomen om deze te beheersen. Ten slotte bespreken we in hoofdstuk 6 in welke mate de gemeente Utrecht opvolging heeft gegeven aan de aanbevelingen uit het rekenkameronderzoek uit 2021.

2 CONTEXT: CENTRAAL BELEID WORDT DECENTRAAL UITGEVOERD

Het beleid voor informatieveiligheid wordt centraal vastgesteld en moet op decentraal niveau – door de organisatieonderdelen – worden uitgevoerd. Risicogebaseerd werken vormt daarbij het uitgangspunt. Via een managementsysteem moet daarover verantwoording worden afgelegd. Organisatieonderdelen zijn ook zelf verantwoordelijk voor de manier waarop zij omgaan met het leren van beveiligingsincidenten.

In dit hoofdstuk beschrijven we hoe informatieveiligheid is georganiseerd binnen de gemeente Utrecht. Dit hoofdstuk bevat daarom geen normenkader, bevindingen of beoordeling. In hoofdstuk 3 beoordelen we de mate waarin de gemeente Utrecht erin slaagt om risicogebaseerd te werken.

2.1 RISICOGEBASEERD WERKEN UITGANGSPUNT BIJ UITVOERING

Om de informatieveiligheid te borgen moeten informatieveiligheidsrisico's eerst worden geïdentificeerd en geclassificeerd (hoe groot is het risico?) en vervolgens worden teruggebracht naar een acceptabel niveau (beheersing). Tijdens het rekenkameronderzoek uit 2021 constateerden we dat er voor informatieveiligheid beperkte capaciteit beschikbaar was binnen de gemeente Utrecht. Er werd daarom gekozen om aan de hand van het 'risicogebaseerd werken' te bepalen welke risico's wel en niet werden beheerst. Dat betekent dat risico's werden afgewogen op basis van zakelijke overwegingen (kosten versus baten) of externe verplichtingen (wet- en regelgeving, contracten).[2] Sommige risico's werden daarmee direct aangepakt. Maar het gebeurde ook dat de gemeente op een aantal risico's geen maatregelen nam en deze risico's bewust accepteerde.

In het rekenkameronderzoek uit 2021 concludeerden we dat de gemeente Utrecht nog onvoldoende invulling gaf aan het risicogebaseerd werken. Om risicogebaseerd te kunnen werken is het namelijk noodzakelijk dat de gemeente de risico's in beeld heeft. Destijds waren echter nog niet alle benodigde risicoanalyses uitgevoerd om een volledig overzicht van de risico's te hebben. Het was daardoor niet mogelijk om te onderbouwen welke risico's wel en niet beheerst moesten worden. Daarnaast bleek de uitvoering van het beleid op cruciale onderdelen achter te lopen. Met extra geld en mensen moest deze achterstand in de achterliggende jaren worden ingelopen. Het risicogebaseerd werken vormt nog steeds een belangrijk fundament voor de uitvoering van het beleid voor informatieveiligheid.

[2] Gemeente Utrecht (2019). *Beleid voor gegevensbescherming 2019-2022*.

Centraal beleid moet decentraal worden uitgevoerd

De gemeente Utrecht hanteert een geïntegreerde aanpak van privacy en informatieveiligheid onder de noemer 'gegevensbescherming'. Gegevensbescherming kent een centrale strategie die decentraal wordt aangestuurd en uitgevoerd. Op strategisch niveau wordt het beleidskader vastgesteld, dat door de gemeente Utrecht in 2023 is herzien. Dit beleidskader vormt de basis voor het treffen van passende organisatorische, procedurele en technische maatregelen om gegevens te beschermen. Daarin wordt gesteld dat "(…) *de speerpunten om de governance te verstevigen en risicogebaseerd werken meer centraal te zetten inmiddels in de praktijk zijn gebracht.*"[3] Aanvullend wordt gesteld dat "(…) *alleen risicogebaseerd werken niet voldoende is om tijdig te voldoen aan alle wet- en regelgeving en bijbehorende internationale en nationale normenkaders.*"[4] Een voorbeeld van zo'n normenkader is de Baseline Informatiebeveiliging Overheid (BIO, zie box 2.1). Om aan de wet- en regelgeving en normenkaders te voldoen heeft de gemeente Utrecht de afgelopen jaren vijf strategische standaarden voor gegevensbescherming[5] ontwikkeld. Deze standaarden vormen de nadere uitwerking van het strategisch beleidskader.

Box 2.1 Nieuwe wetgeving stelt meer eisen aan gegevensbescherming

Gemeenten zijn verplicht om actueel beleid voor gegevensbescherming te hebben. De Baseline Informatiebeveiliging Overheid (BIO) vormt het basisnormenkader voor informatiebeveiliging binnen alle Nederlandse overheidslagen en is sinds januari 2020 van kracht. De BIO beschrijft uitgangspunten waar beleid aan moet voldoen en wat daar in de interne organisatie voor moet worden georganiseerd. Voldoen aan de BIO is niet verplicht. Al streeft de gemeente Utrecht hier wel naar.

Op dit moment wordt gewerkt aan de BIO2.0, die eind 2024 van kracht gaat zijn.[6] Ook wordt de 'Network and Information Security directive' (NIS2-richtlijn) vertaald naar Nederlandse wetgeving. Dit is door de Europese Unie vastgesteld. Met de NIS2-richtlijn moet de cyberbeveiliging en weerbaarheid van essentiële diensten in EU-lidstaten worden verbeterd.[7] Dit leidt tot meer wetgeving van een verplicht karakter, waar ook de gemeente Utrecht aan zal moeten voldoen.

Aan het strategische beleid en de standaarden voor gegevensbescherming moet decentraal op tactisch en operationeel niveau uitvoering worden gegeven. Dat betekent dat elk organisatieonderdeel zelf verantwoordelijk is voor het risicogebaseerd implementeren en uitvoeren van het centrale beleid. De strategische standaarden worden door de organisatieonderdelen niet in één keer doorgevoerd. Dat moet namelijk aan de hand van '*life cycle management'* gebeuren. Dit betekent dat delen van de strategische standaarden gelijktijdig worden ingevoerd met het doorvoeren van reguliere maatregelen zoals de implementatie van nieuwe applicaties en procesveranderingen. Hierdoor wordt een volledige implementatie van de BIO pas gerealiseerd wanneer het volledige applicatielandschap van

[3] Gemeente Utrecht (2023). *Gegevensbescherming in Utrecht: verantwoord en transparant. Intern strategisch beleidskader voor gegevensbescherming van Utrecht*, p. 5.
[4] Gemeente Utrecht (2023). *Gegevensbescherming in Utrecht: verantwoord en transparant. Intern strategisch beleidskader voor gegevensbescherming van Utrecht*, p. 9.
[5] Deze hebben betrekking op: 1) Business Continuity Management; 2) Cryptografie; 3) Identificatie, Authenticatie en Autorisatie; 4) Logging en Monitoring; en 5) Naleving Gegevensbescherming Management System.
[6] Zie: Baseline Informatiebeveiliging Overheid Cybersecurity - Digitale Overheid
[7] Zie: NIS2-richtlijn - Digitale Overheid

de gemeente Utrecht is vernieuwd. Dat zal naar verwachting vijf tot zeven jaar – tot 2030 – duren.[8]

Op strategisch, tactisch en operationeel niveau wordt aan informatieveiligheid gewerkt

In ons vorige onderzoek concludeerden we dat met het instellen van een stuurgroep, vakgroep, regiegroep en taskforce de interne governance was verstevigd. Omdat we de interne organisatie en governance daaromheen destijds beperkt hebben onderzocht, is daar in dit onderzoek extra aandacht aan besteed. We bespreken de interne organisatiestructuur (zie figuur 2.2) aan de hand van drie niveaus waarop aan informatieveiligheid wordt gewerkt (strategisch, tactisch, operationeel).

<u>Strategisch</u>

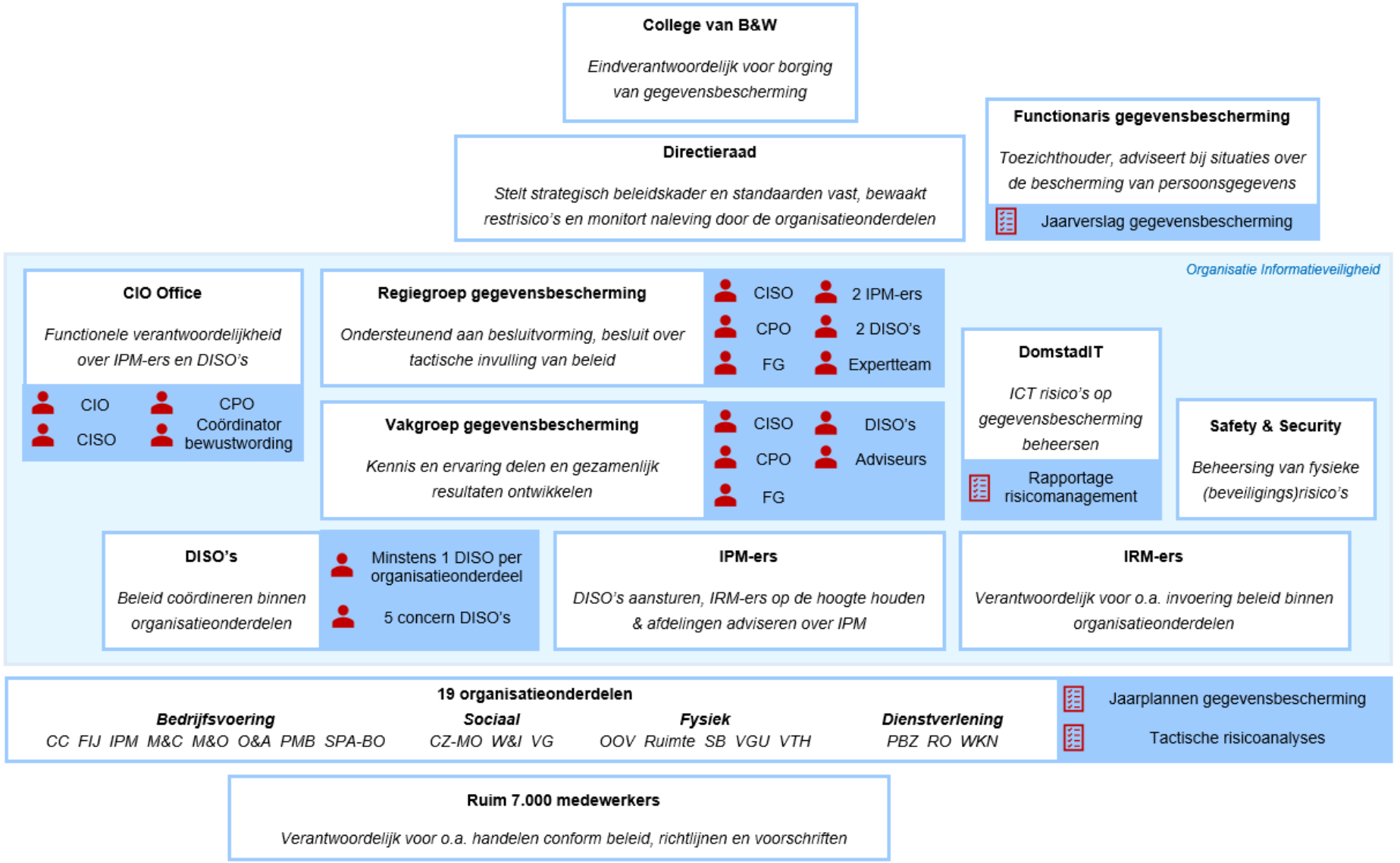
Op strategisch niveau worden besluiten over informatieveiligheid voorgelegd aan het **managementteam** van de **Chief Information Officer**[9] (MT CIO). Het MT CIO is altijd de eerste schakel in de besluitvormingsketen voor gegevensbeschermingsbeleid. Aan het MT CIO neemt onder andere een vertegenwoordiging van **Informatie- en Procesmanagers**[10] (IPM-ers) deel. Omdat IPM-ers betrokken zijn bij de uitvoering van beleid binnen de organisatieonderdelen is daarmee in opzet centraal zicht op wat er decentraal gebeurt. De **regiegroep gegevensbescherming** zorgt voorafgaand aan de besluitvorming voor vakinhoudelijke afstemming tussen de strategische, tactische en operationele lagen van gegevensbescherming. De **Chief Privacy Officer**[11] (CPO) en **Chief Information Security Officer**[12] (CISO) stemmen nieuwe en gewijzigde beleidsvoorstellen met de regiegroep af voordat het ter besluitvorming wordt aangeboden.[13]

Uiteindelijk stel de **Directieraad** het strategische beleidskader en de standaarden voor gegevensbescherming met gemeentebrede impact vast. Daarnaast zou de Directieraad ook de naleving van het beleid en de standaarden voor gegevensbescherming door de organisatieonderdelen op tactisch en operationeel niveau moeten monitoren. De **Integraal Resultaatverantwoordelijk Managers**[14] (IRM-ers) zijn verantwoordelijk voor de invoering van het beleid binnen de organisatieonderdelen. De Directieraad spreekt de IRM-ers (indien nodig) op naleving aan en legt over het gevoerde beleid verantwoording af aan het **college van B&W** (eindverantwoordelijk voor de borging van gegevensbescherming binnen de gemeente Utrecht).

---

[8] Gemeente Utrecht (2023). *Gegevensbescherming in Utrecht: verantwoord en transparant. Intern strategisch beleidskader voor gegevensbescherming van Utrecht*.
[9] De CIO is beleidsmatig verantwoordelijk voor alle aspecten van informatie- en procesmanagement, waaronder gegevensbescherming.
[10] Een IPM-er coördineert de uitvoering van het beleid voor gegevensbescherming binnen een organisatieonderdeel.
[11] De CPO bereidt samen met de CISO het beleid voor gegevensbescherming voor.
[12] De CISO regisseert informatiebeveiliging op concernniveau.
[13] Gemeente Utrecht (2023). *Gegevensbescherming in Utrecht: verantwoord en transparant. Intern strategisch beleidskader voor gegevensbescherming van Utrecht*.
[14] De IRM-er is de directeur van een organisatieonderdeel.

Figuur 2.2 Overzicht van de interne organisatie en verantwoordelijkheden bij gegevensbescherming



Naast het vaststellen van beleid worden op strategisch niveau ook risico's in kaart gebracht die impact hebben op de gehele gemeentelijke organisatie. Onder het programma Gegevensbescherming dat tot de zomer van 2023 actief was lag het eigenaarschap van de strategische risico's bij de **stuurgroep gegevensbescherming**. De stuurgroep bracht prioritering aan in de gevonden strategische risico's en stuurde op de voortgang van maatregelen om de risico's te beheersen. Met de stopzetting van het programma is ook de stuurgroep opgeheven. Een deel van de verantwoordelijkheden van de stuurgroep is overgeheveld aan de Directieraad. Dat geldt bijvoorbeeld voor het monitoren van de strategische risico's, die in juli 2023 voor het laatst van een update zijn voorzien.[15]

Tactisch

Tactische risico's vormen een bedreiging voor een specifiek organisatieonderdeel. De managementteams van de individuele organisatieonderdelen zijn verantwoordelijk voor het uitvoeren van tactische risicoanalyses om risico's te identificeren en de IRM-ers zijn (als risicodrager) eindverantwoordelijk voor de beheersing van de risico's. Bij het implementeren van beleid en het uitvoeren van risicoanalyses wordt ieder organisatieonderdeel ondersteund door een eigen IPM-er en **Decentrale Information Security en Privacy Officer**[16] (DISO).

Op tactisch niveau zijn er twee centrale onderdelen binnen informatie- en procesmanagement: **DomstadIT** en **Safety & Security** (S&S). DomstadIT is verantwoordelijk voor het leveren van ICT-middelen en de beveiliging daarvan. S&S is verantwoordelijk voor de beheersing van fysieke (beveiligings)risico's.

Operationeel

Operationele risico's vormen een bedreiging voor een specifiek proces, systeem of applicatie dat binnen een organisatieonderdeel wordt gebruikt. Op operationeel niveau is daarom een belangrijke rol toebedeeld aan de **systeem- en proceseigenaren** om daar actuele risicoanalyses op uit te voeren. De IRM-er van het organisatieonderdeel is – naast de tactische risico's – ook eindverantwoordelijk voor het beheersen van de operationele risico's.

Periodiek nemen alle inhoudelijke actoren (waaronder de DISO's en **Functionaris voor Gegevensbescherming**[17]) op operationeel niveau deel aan de **Vakgroep Gegevensbescherming**. Deze wordt georganiseerd door de CISO en CPO om opgedane kennis en ervaringen te delen.

[15] Gemeente Utrecht (4 juli 2023). Interne memo *Herijking en overdracht strategische risico's gegevensbescherming*.
[16] DISO's bewaken de naleving van het beleid voor gegevensbescherming binnen de organisatieonderdelen en rapporteren hierover periodiek aan de IPM-ers, IRM-ers, CISO en CPO. DISO's bieden ook ondersteuning aan organisatieonderdelen bij het uitvoeren en implementeren van het beleid.
[17] De FG is toezichthouder en adviseert bij aangelegenheden die verband houden met de bescherming van persoonsgegevens en/of politiegegevens, waaronder DPIA's.

2.2 OPNIEUW EXTRA FINANCIËLE MIDDELEN VRIJGEMAAKT VOOR GEGEVENSBESCHERMING

De uitgaven aan gegevensbescherming of het specifieke onderdeel informatieveiligheid daarbinnen zijn niet één-op-één terug te vinden in de begroting en de jaarrekening. Het onderwerp valt in de categorie *overhead* onder IPM. Specifieke incidentele en structurele uitgaven worden wel zichtbaar gemaakt. Zo stemde de gemeenteraad in 2020 in met € 3,4 miljoen extra budget voor gegevensbescherming verdeeld over drie jaar om de uitvoering van het programma Gegevensbescherming te versnellen (zie tabel 2.3). De raad stemde ook in met € 0,6 miljoen extra structureel budget om de vijf 'vliegende' (flexibel inzetbare) DISO's mee aan te stellen. Omdat het programma Gegevensbescherming in 2023 is gestopt, liep ook deze incidentele financiering af.

Tabel 2.3 Incidentele financiële middelen programma Gegevensbescherming over drie jaar verdeeld (x 1.000)

	2020	2021	2022	2023	2024
Gegevensbescherming	€ 1.000	€ 1.500	€ 900	€ 0	€ 0

Bron: Gemeente Utrecht (2020). *Eerste Bestuursrapportage.*

In 2021 werd 'het nieuwe werken 3.0' geïntroduceerd, gericht op het structureel faciliteren van flexibel en plaats onafhankelijk werken. De voorspelling was dat na de coronapandemie een groot deel van de gemeentelijke medewerkers hybride zou blijven werken. Dat vroeg om aanpassingen aan zowel het Stadskantoor als de IT (zoals het uitgeven van beheerde laptops). De gemeenteraad heeft daarvoor in 2021 structureel geld vrijgemaakt. In 2022 gaf het college aan dat daarmee de eerste knelpunten waren opgepakt, maar dat "(…) *voor de realisatie van plaats onafhankelijk werken voor een grotere groep medewerkers aanvullende investeringen nodig zijn.*"[18] Deze investeringen hadden betrekking op vier aspecten, waaronder mobiele apparaten voor medewerkers zonder werkplek en toekomstbestendige thuiswerkfaciliteiten. De gemeenteraad stemde in met het vrijmaken van extra financiële middelen om ook de aanvullende investeringen te realiseren. De kosten hiervoor zijn niet nader gespecificeerd. De vrijgemaakte jaarlijkse bedragen verschillen over de verschillende jaren van elkaar (zie tabel 2.4).

[18] Gemeente Utrecht (2022). *Voorjaarsnota en Eerste Bestuursrapportage 2022*, p. 37.

Tabel 2.4 Vrijgemaakte middelen voor realisatie van ‘het nieuwe werken 3.0’ verschillen per jaar (x 1.000)

	2021	2022	2023	2024	2025	2026
Het nieuwe werken 3.0	€ 1.050	€ 1.506	€ 2.463	€ 2.133	€ 1.738	€ 1.761

Bron: Gemeente Utrecht (2021). *Voorjaarsnota en Eerste Bestuursrapportage 2021.* En: Gemeente Utrecht (2022). *Voorjaarsnota en Eerste Bestuursrapportage 2022*.

In juni 2022 is het bewustwordingsprogramma gegevensbescherming van start gegaan. Dit structurele programma is erop gericht om de kennis over privacy en informatiebeveiliging van medewerkers te verbeteren en om hun houding en gedrag met betrekking tot privacy en informatiebeveiliging te verbeteren.[19] Om de activiteiten daartoe uit te kunnen voeren is vanaf 2023 structureel € 130.000 beschikbaar gesteld (zie de tabel 2.5 en 2.6). Dat bedrag is als volgt opgebouwd:

Tabel 2.5 Helft structureel budget bewustwordingsprogramma gegevensbescherming voor inzet fulltime medewerker op bewustwording

Activiteit	Kosten
Beleidsadviseur bewustwording (1 fte)	€ 70.000
Kosten hosting en aanpassingen e-learning	€ 20.000
Incidentele bijeenkomsten	€ 10.000
Interventies (bijvoorbeeld phishing testen, externe sprekers)	€ 15.000
Campagnemateriaal	€ 5.000
Onvoorziene uitgaven	€ 10.000
Totaal	**€ 130.000**

Bron: Gemeente Utrecht (2022). Plan *Bewustwording en communicatie gegevensbescherming.*

In de Voorjaarsnota van 2024 geeft het college aan dat vanaf 17 oktober 2024 de Europese NIS2-richtlijn (zie box 2.1 in paragraaf 2.1) van kracht wordt. Dat leidt voor de gemeente Utrecht tot aanscherpingen in de uitvoering van onder andere wet- en regelgeving, zoals de BIO en de Algemene verordening gegevensbescherming (AVG). Ondanks de huidige financiële situatie wil en moet de gemeente daaraan voldoen. Dit zorgt structureel voor extra kosten van € 0,965 miljoen per jaar (zie tabel 2.6).[20]

[19] Gemeente Utrecht (2022). *Bewustwording en communicatie gegevensbescherming*.
[20] Gemeente Utrecht (2024). *Voorjaarsnota en Eerste Bestuursrapportage 2024*.

Tabel 2.6 Toegekende extra financiële middelen voor gegevensbescherming structureel (bedragen x 1.000)

	2023	2024	2025	2026	2027	2028
Informatiebeveiliging	€ 0	€ 440	€ 965	€ 965	€ 965	€ 965
Bewustwordingsprogramma	€ 130	€ 130	€ 130	€ 130	€ 130	€ 130

Bronnen: Gemeente Utrecht (2024). *Voorjaarsnota en Eerste Bestuursrapportage 2024*. En: Gemeente Utrecht (2022). *Programmabegroting 2023*.

2.3 ORGANISATIEONDERDELEN ZELF VERANTWOORDELIJK VOOR OMGAAN MET EN LEREN VAN INCIDENTEN

Beveiligingsincidenten (zoals datalekken) vormen een belangrijke graadmeter voor hoe het ervoor staat met gegevensbescherming. De gemeente geeft aan dat "(…) *een goede analyse van de oorzaak van incidenten kan voorkomen dat hetzelfde incident nog eens plaatsvindt.*"[21] Gebeurtenissen rondom de gemeentelijke processen en diensten zouden beter gemonitord moeten worden om een beter overzicht te krijgen van de zwakke plekken die tot een beveiligingsincident kunnen leiden[22]: "*Nieuwe informatie correleren met informatie uit onze bestaande digitale processen leidt tot een verbeterd datagedreven overzicht.*"[23]

De wijze waarop verantwoordelijkheden bij incidenten zijn toebedeeld, is helder beschreven in het strategisch beleidskader. Zo moeten individuele medewerkers beveiligingsproblemen of -incidenten signaleren en melden. De DISO stelt eerst vast of er sprake is van een datalek, en vervolgens of de Autoriteit Persoonsgegevens moet worden ingelicht.[24] Samen met de verantwoordelijk lijnmanager, opdrachtgever of proceseigenaar handelt de DISO het incident vervolgens tijdig en volgens richtlijnen af. De IRM-er van het organisatieonderdeel waarin het incident heeft plaatsgevonden is eindverantwoordelijk voor de tijdige en juiste afhandeling van alle incidenten binnen het organisatieonderdeel.

Aan organisatieonderdelen wordt na het afhandelen van een incident door de DISO teruggekoppeld wat er in de toekomst anders kan om incidenten te voorkomen.[25] Het benutten van deze informatie en de manier waarop van incidenten wordt geleerd is aan de verschillende organisatieonderdelen zelf.[26]

[21] Gemeente Utrecht (2023). *Gegevensbescherming in Utrecht: verantwoord en transparant. Intern strategisch beleidskader voor gegevensbescherming van Utrecht*, p. 12.
[22] Gemeente Utrecht (2023). *Gegevensbescherming in Utrecht: verantwoord en transparant. Intern strategisch beleidskader voor gegevensbescherming van Utrecht*.
[23] Gemeente Utrecht (2023). *Gegevensbescherming in Utrecht: verantwoord en transparant. Intern strategisch beleidskader voor gegevensbescherming van Utrecht*, p. 12.
[24] Rekenkamer Utrecht (2024). *Interview gemeente*.
[25] Rekenkamer Utrecht (2024). *Interview gemeente*.
[26] Rekenkamer Utrecht (2024). *Interview gemeente*.

DomstadIT houdt – als centraal onderdeel binnen informatie- en procesmanagement – een eigen registratiesysteem bij voor de ICT-incidenten waar zij op acteren. Alle incidenten komen (uiteindelijk) binnen bij het Serviceplein en het Serviceportaal. Sinds een aantal maanden worden twee registratiesystemen van elkaar gescheiden:

1. Systeem voor het 'standaard' incidentenproces: het gaat hier met name om verstoringen in de dienstverlening, zoals problemen met inloggen.
2. Systeem voor security gerelateerde incidenten: dat helpt bij het behouden van het overzicht over alle lopende securityincidenten. Het systeem wordt (o.a.) gebruikt om te leren en verbeteren van incidenten. Wanneer een securityincident een hoge impact dreigt te hebben (calamiteit) kan een apart proces worden opgestart (opschaling naar o.a. de CISO en procesmanager) om de impact te mitigeren. Dit proces wordt altijd met een (evaluatie)rapportage afgesloten.

2.4 LANGS MANAGEMENTSYSTEEM VOOR GEGEVENSBESCHERMING MOET VERANTWOORDING WORDEN AFGELEGD

Veel betrokkenen geven aan dat het gegevensbeschermingsmanagementsysteem (GBMS) wordt gebruikt om over het functioneren van de informatiebeveiliging te rapporteren aan het management (zowel van operationeel naar tactisch niveau, als van tactisch naar strategisch niveau).[27] Het GBMS is de Utrechtse variant op een Information Security Management Systeem (ISMS) en de laatste versie is na een ontwikkelperiode van meer dan twee jaar in maart 2024 vastgesteld en in gebruik genomen. In het begeleidende beleidsdocument wordt aangegeven dat "(…) *we met het GBMS geen informatiesysteem bedoelen, maar een werkwijze om de bescherming van gegevens continu te verbeteren op basis van risicomanagement.*"[28] Het GBMS is daarmee vooral een aanvulling op de Utrechtse aanpak voor risicomanagement, zoals onder meer beschreven in het strategisch beleidskader.

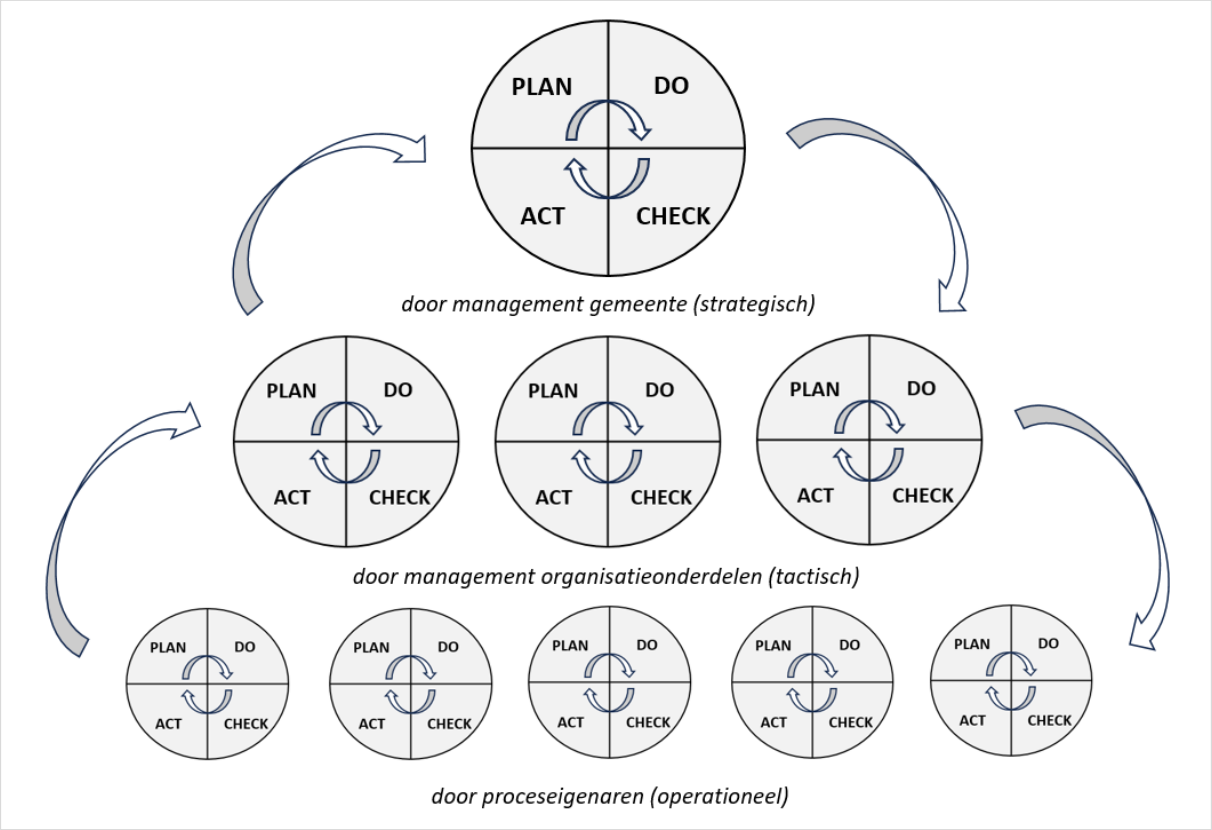
Daarvoor onderscheidt het GBMS Plan-Do-Check-Act-cycli (PDCA) op drie niveaus:

1. Strategisch: door het management van de gemeente, de Directieraad.
2. Tactisch: door het management van een organisatieonderdeel.
3. Operationeel: door het management van een proces, de proceseigenaren.

Het is de bedoeling dat de PDCA-cycli op de drie niveaus met elkaar in verbinding staan doordat eigenaren hun eigen PDCA-cyclus afstemmen op die van andere eigenaren (zie figuur 2.7). Dat moet onder andere gebeuren door aan te sluiten op de bestaande planning- & controlcyclus van de gemeente.

[27] Rekenkamer Utrecht (2024). *Interviews gemeente*.
[28] Gemeente Utrecht (2024). *Gegevensbescherming Managementsysteem*, p. 4.

Figuur 2.7 De PDCA-cycli op de verschillende niveaus moeten horizontaal en verticaal op elkaar zijn afgestemd



Bron: Rekenkamer Utrecht (2024) o.b.v. Gemeente Utrecht (2024). *Gegevensbescherming Managementsysteem*.

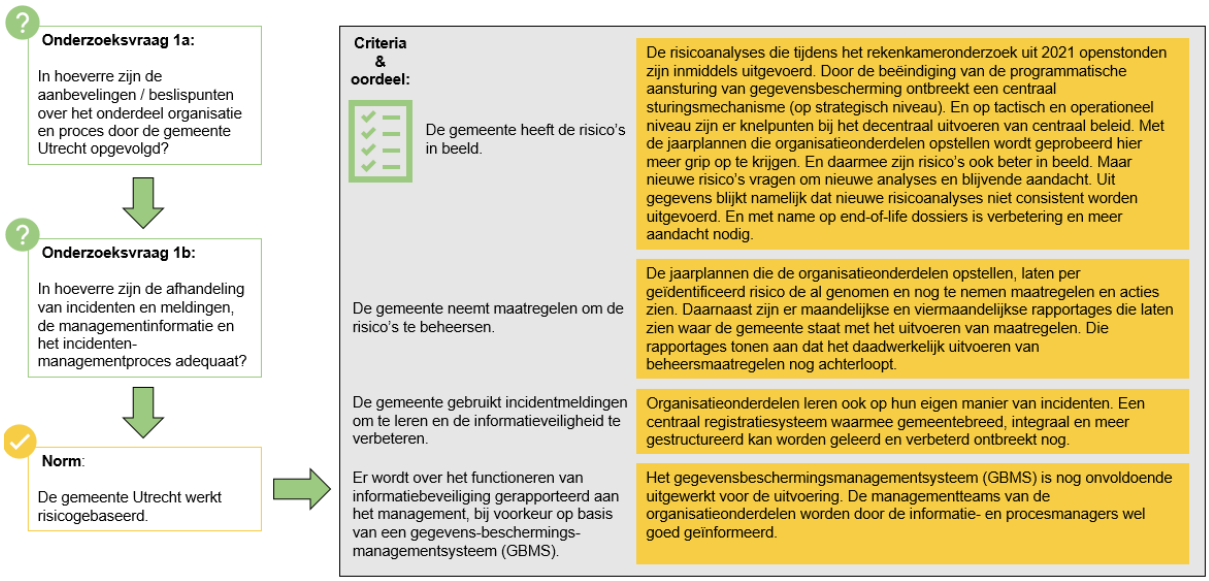
3 ORGANISATIE EN PROCES: WIJZIGINGEN VRAGEN OM VERDERE VERBETERING

Er wordt in vergelijking met 2021 meer risicogebaseerd gewerkt, al zijn daar ook zeker nog verbeterpunten in. Op strategisch niveau ontbreekt namelijk door de beëindiging van de programmatische aansturing van gegevensbescherming een centraal sturingsmechanisme. Naleving van beleid door organisatieonderdelen wordt onvoldoende afgedwongen. Door een gebrek aan sturing geven organisatieonderdelen op tactisch en operationeel niveau een eigen invulling aan de manier waarop zij het beleid uitvoeren. Risicoanalyses zijn daardoor niet altijd actueel en risico's worden niet of niet tijdig beheerst. En ook van beveiligingsincidenten wordt op dit moment niet gemeentebreed geleerd en verbeterd. Het gegevensbeschermingsmanagementsysteem (GBMS) is nog onvoldoende uitgewerkt voor de uitvoering. De managementteams van de organisatieonderdelen worden door de informatie- en procesmanagers wel goed geïnformeerd.

In dit hoofdstuk beoordelen we hoe de gemeente Utrecht informatieveiligheid heeft georganiseerd en hoe zich dat heeft ontwikkeld sinds ons vorige onderzoek. We beantwoorden daarmee onderzoeksvragen 1a en 1b.

De uitvoering, afgezet tegen de bijbehorende norm, leidt in figuur 3.1 tot onze beoordeling en bevindingen. Hierin leggen we ook direct de relatie tussen de onderzoeksvragen, de norm en bijbehorende criteria.

Figuur 3.1 Norm, criteria en beoordeling "Organisatie en proces"



Toelichting op het normenkader
Aan de hand van het risicogebaseerd werken worden risico's geprioriteerd. Het is daarom noodzakelijk dat de gemeente Utrecht de risico's in beeld heeft. En dat vervolgens de juiste maatregelen worden genomen om die risico's te beheersen. Voor goede monitoring en aansturing is het belangrijk dat het management wordt geïnformeerd over de voortgang daarvan. Verder moet de gemeente incidenten rondom informatieveiligheid (zoals security incidenten en datalekken) benutten om structureel van te leren en verbeteren.

3.1 OP STRATEGISCH NIVEAU ONTBREEKT EEN CENTRAAL STURINGSMECHANISME

De programmatische aansturing van gegevensbescherming is in de zomer van 2023 beëindigd. Wij constateren dat mede daardoor nu een centraal sturingsmechanisme op strategisch niveau ontbreekt. Op strategisch niveau kunnen organisatieonderdelen niet door informatie- en procesmanagement worden gedwongen om met informatieveiligheid aan de slag te gaan. De Directieraad kan dat wel, maar doet dat in de praktijk onvoldoende. En doordat het gegevensbeschermingsmanagementsysteem (GBMS) onvoldoende is uitgewerkt is te beperkt informatie beschikbaar om strategische besluiten te nemen.

Organisatieonderdelen beter vertegenwoordigd in regiegroep gegevensbescherming
De regiegroep gegevensbescherming speelt een belangrijke rol bij besluitvorming over gegevensbescherming (zie ook paragraaf 2.1). De samenstelling van de regiegroep is sinds het vorige rekenkameronderzoek enigszins gewijzigd. De gemeente Utrecht is namelijk steeds meer in domeinen gaan werken. De organisatieonderdelen zijn toebedeeld aan één van de vier domeinen (fysiek, sociaal, bedrijfsvoering of dienstverlening). Per domein nemen één IPM-er of één DISO deel aan de regiegroep. Zij brengen advies uit namens alle organisatieonderdelen binnen hun domein. Daarmee zijn alle organisatieonderdelen in de regiegroep vertegenwoordigd. Dat is een positieve ontwikkeling omdat voorheen slechts een aantal organisatieonderdelen vertegenwoordigd waren.[29]

Door de beëindiging van de programmatische aansturing ontbreekt een centraal sturingsmechanisme
In paragraaf 2.1 legden we uit dat het tijdelijke programma Gegevensbescherming, ingericht om de realisatie van gemeentelijke ambities te versnellen, in de zomer van 2023 is beëindigd. Daarmee is ook de stuurgroep gegevensbescherming – voorheen verantwoordelijk voor het monitoren en beheersen van strategische risico's – in de zomer van 2023 is opgeheven. Een deel van de verantwoordelijkheden van de stuurgroep is overgeheveld aan de Directieraad. Echter zijn niet alle verantwoordelijkheden overgenomen. Daardoor ontbreekt zonder de stuurgroep een centraal sturingsmechanisme op strategisch

[29] Rekenkamer Utrecht (2024). *Interview gemeente.*

niveau.[30] In diezelfde periode viel ook de CISO (als één van de strategen op dit onderwerp) uit en waren er personele wisselingen in de CIO- en Concerndirecteursfunctie.[31] Die ontwikkelingen samen leidden tot urgentieverlies en zorgen ervoor dat het implementeren van strategische maatregelen vaak langer duurt dan voorheen.[32] In december 2023 wordt in een intern document aangegeven: "(…) *strategische risico's hebben op papier een eigenaar, maar deze behandelt het risico niet proactief*."[33] De risico's zijn sinds juli 2023 ook niet opnieuw herijkt. Er is dus nog winst te behalen in het strategisch risicomanagement. De gemeente Utrecht heeft in december 2023 aangegeven haar strategisch risicomanagement te herzien.[34]

Door gebrek aan informatie kunnen niet altijd strategische besluiten worden genomen
Informatieveiligheid moet met de opheffing van de stuurgroep breed, en meer decentraal in de organisatie inbedden.[35] Organisatieonderdelen zijn zelf verantwoordelijk voor het identificeren, classificeren, beheersen en monitoren van tactische en operationele risico's. En voor het doorvoeren van centraal beleid. De Directieraad heeft de mogelijkheid om een IRM-er van een organisatieonderdeel – de operationele en tactische risicodrager – indien nodig op naleving aan te spreken.

IRM-ers leggen halfjaarlijks verantwoording af aan de themadirecteur bedrijfsvoering (lid van de Directieraad). Dat gebeurt nogal vrijblijvend: "*Dat moeten we niet groter maken dan het is. Er komen in dat gesprek misschien wel twintig onderwerpen voorbij in één uur.*"[36] Al wordt dat door betrokkenen niet per se als een probleem gezien: "*De aandacht en sturing moet primair vanuit het eigen managementteam komen in afstemming met de CIO.*"[37] IRM-ers worden in de gesprekken met de themadirecteur gewezen op onderdelen die niet goed gaan, bijvoorbeeld als er te weinig risicoanalyses zijn uitgevoerd. Dat gebeurt constructief: er wordt in die gevallen gevraagd of de IRM-ers extra IPM-ondersteuning nodig hebben om de achterstand in te lopen.[38]

De volledige Directieraad wordt met de bedrijfsvoeringrapportage tweemaal per jaar geïnformeerd over de stand van zaken van gegevensbescherming. In die rapportage komen tien thema's aan bod, waaronder gegevensbescherming (waar informatieveiligheid een onderdeel van uitmaakt). De informatie die over informatieveiligheid wordt gedeeld is summier, en maakt slechts een klein onderdeel uit van de bespreking. Het is daardoor niet altijd mogelijk om strategische besluiten te nemen op basis van de beschikbare informatie. Er leeft bij de Directieraad daarom de behoefte om meer uitgebreide informatie te ontvangen

[30] Rekenkamer Utrecht (2024). *Interview gemeente.*
[31] Rekenkamer Utrecht (2024). *Interview gemeente.*
[32] Rekenkamer Utrecht (2024). *Interview gemeente.*
[33] Gemeente Utrecht (2023). *Herinrichting strategisch risicomanagement*.
[34] Gemeente Utrecht (2023). *Herinrichting strategisch risicomanagement*.
[35] Rekenkamer Utrecht (2024). *Interview gemeente.*
[36] Rekenkamer Utrecht (2024). *Interview gemeente.*
[37] Rekenkamer Utrecht (2024). *Interview gemeente.*
[38] Rekenkamer Utrecht (2024). *Interview gemeente.*

over de stand van zaken van informatieveiligheid.[39] Het gaat dan met name om wat de belangrijkste risico's zijn, hoe de organisatie (breed) daarmee omgaat en welke beheersmaatregelen worden genomen om de risico's naar een acceptabel niveau te brengen.

Of er voldoende wordt geleerd van beveiligingsincidenten zoals datalekken is niet vast te stellen. Volgens betrokkenen leren de CISO en CPO goed van de incidenten die plaatsvinden.[40] Maar op het strategische niveau van de Directieraad is er behoefte aan meer voortgangsrapportages over datalekken. Zo is voor de Directieraad nu niet altijd duidelijk wat voor incidenten er hebben plaatsgevonden, hoeveel en wat de impact daarvan is geweest.[41]

Naleving en uitvoering van centraal beleid wordt onvoldoende afgedwongen
De CISO wordt periodiek door de IPM-er van een organisatieonderdeel op de hoogte gehouden van de voortgang op de uitvoering van het centrale beleid binnen dat organisatieonderdeel. Op het moment dat organisatieonderdelen het beleid niet naleven kunnen de CPO en de CISO dat niet afdwingen. De CISO-functie is in de gemeente Utrecht zodanig gepositioneerd dat deze geen mandaat heeft om 'hard' te sturen op naleving van beleid voor gegevensbescherming door IRM-ers. Er kan wel worden geëscaleerd naar de CIO, maar ook die kan uitvoering en naleving niet afdwingen bij zijn of haar mededirecteuren. Binnen informatie- en procesmanagement wordt geprobeerd om hier meer grip op te krijgen, onder andere door het vaststellen van jaarplannen gegevensbescherming en informatiebeheer. De Directieraad heeft wel de mogelijkheid om naleving door IRM-ers af te dwingen, maar doet dat in de praktijk onvoldoende.

Kwaliteit jaarplannen toegenomen, moeten ook zorgen voor voldoende capaciteit
In de jaarplannen gegevensbescherming en informatiebeheer geven organisatieonderdelen (o.a.) aan hoe de belangrijkste thema's en risico's rondom gegevensbescherming worden aangepakt. Sinds 2022 gebeurt dat op een risicogebaseerde manier. De jaarplannen laten de geïdentificeerde risico's zien en op welk niveau die zich bevinden (strategisch – tactisch – operationeel). Door eerdere jaarplannen van hetzelfde organisatieonderdeel te vergelijken worden de nieuw geïdentificeerde risico's zichtbaar. In de jaarplannen wordt (langs centrale richtlijnen) ook beschreven wie binnen het organisatieonderdeel verantwoordelijk is voor het uitvoeren van de verschillende risicoanalyses.

De CIO is gedurende 2023 gestart met het geven van een formele terugkoppeling op de conceptjaarplannen voor 2024. De organisatieonderdelen moeten de adviezen van de CIO doorvoeren voordat de plannen formeel vastgesteld mogen worden. De jaarplannen worden daardoor kwalitatief beter en van een hoger volwassenheidsniveau.[42] En de plannen bieden meer structuur. Daarmee is een stijgende lijn zichtbaar van de eerste risicogebaseerde

[39] Rekenkamer Utrecht (2024). *Interview gemeente.*
[40] Rekenkamer Utrecht (2024). *Interview gemeente*
[41] Rekenkamer Utrecht (2024). *Interview gemeente*.
[42] Rekenkamer Utrecht (2024). *Interview gemeente*.

jaarplannen in 2022, naar volledige plannen in 2023 die soms nog lastig en te laat werden vastgesteld, naar kwalitatief goede plannen in 2024 die ook op kortere termijn zijn vastgesteld door de managementteams van de organisatieonderdelen.

IRM-ers moeten intern voldoende capaciteit vrijmaken om het jaarplan uit te kunnen voeren. Vanaf de jaarplannen voor 2024 moet worden gezorgd dat IRM-ers dat ook doen. Maar omdat dit een recente ontwikkeling is, is nog onzeker of dit ook in de praktijk zal werken.[43] Zo wordt in een jaarplan 2024 voor de belangrijkste geïdentificeerde risico's aangegeven welke maatregelen al zijn genomen en nog genomen moeten worden, met bijbehorend capaciteitsbeslag. Die capaciteit moet van tevoren al door de IRM-er worden vrijgemaakt. De organisatieonderdelen zouden daarmee tijdig capaciteit in moeten ramen om met risicobeheersing aan de slag te gaan.

3.2 OP TACTISCH EN OPERATIONEEL NIVEAU GEVEN ORGANISATIEONDERDELEN HUN EIGEN INVULLING AAN BELEID

Het uitvoeren van het strategische beleid voor gegevensbescherming is op decentraal niveau belegd. Op tactisch en operationeel niveau geven organisatieonderdelen op een eigen manier invulling aan de uitvoering. Risicoanalyses zijn daardoor niet altijd actueel en sommige risico's worden niet of niet tijdig beheerst. En van beveiligingsincidenten wordt niet gemeentebreed geleerd en verbeterd.

Ondersteuning niet risicogebaseerd verdeeld

Zoals aangegeven in paragraaf 2.1 wordt ieder organisatieonderdeel ondersteund bij het uitvoeren van centraal beleid en het identificeren en beheersen van risico's door één IPM-er en minstens één DISO. Maar niet ieder organisatieonderdeel heeft evenveel ondersteuning nodig. Dat leidt ertoe dat ondersteuningscapaciteit niet wordt vrijgemaakt op basis van de ondersteuningsbehoefte en/of daar waar de grootste risico's voor de organisatie liggen. Met vijf 'vliegende' (flexibel inzetbare) DISO's wordt geprobeerd om meer flexibel op de ondersteuningsbehoefte in te spelen. Maar er bestaat een bredere behoefte om hier meer domeingericht op te sturen, zodat de ondersteuningscapaciteit nog beter kan worden afgestemd op de plekken die op basis van een bredere risicoafweging de meeste aandacht verdienen.[44] Denk bijvoorbeeld aan de organisatieonderdelen die regelmatig met persoonsgegevens of andere privacygevoelige informatie (zogeheten kroonjuwelen) werken. Zij krijgen op dit moment niet per definitie meer ondersteuning dan de organisatieonderdelen die weinig of niet met dat type informatie aan de slag zijn.

[43] Rekenkamer Utrecht (2024). *Interview gemeente.*
[44] Rekenkamer Utrecht (2024). *Interviews gemeente*.

Eerdere risicoanalyses inmiddels uitgevoerd, achterstanden blijven bestaan

De risicoanalyses die tijdens het vorige onderzoek nog openstonden – en waardoor het risicogebaseerd maken van afwegingen niet mogelijk was – zijn inmiddels uitgevoerd.[45] Maar de ontwikkelingen staan niet stil. Processen en applicaties zijn continu aan verandering onderhevig, waardoor het monitoren van (nieuwe) risico's voortdurend nodig blijft.[46] De afgelopen jaren is er daarom mede op ingezet om een "(…) *risicomanagementproces voor gegevensbescherming op te bouwen.*"[47] Wij constateren dat de gemeente Utrecht hier de afgelopen jaren grote stappen in heeft gezet.

Tien van de twaalf organisatieonderdelen hebben op dit moment processen op orde om tactische en operationele risico's te identificeren, classificeren en monitoren.[48] Ieder managementteam moet vervolgens een jaarlijkse risicosessie organiseren om de risico's op tactisch niveau voor het eigen organisatieonderdeel vast te stellen. Negen van de twaalf organisatieonderdelen slagen erin om zo'n risicosessie een structureel onderdeel van de managementcyclus te maken.[49] De risico's die op basis van de risicosessie worden geïdentificeerd vormen de basis voor de eerdergenoemde risicogebaseerde jaarplannen gegevensbescherming en informatiebeheer die de organisatieonderdelen sinds 2022 opstellen.

Betrokkenen geven aan dat het uitvoeren van risicoanalyses binnen de meeste organisatieonderdelen meer gestructureerd plaatsvindt en beter is belegd in de Plan-Do-Check-Act-cyclus (PDCA).[50] En er is volgens hen een stijgende lijn waarneembaar in het aantal risicoanalyses dat door de organisatieonderdelen wordt uitgevoerd op zowel tactisch als operationeel niveau.[51] Binnen de organisatieonderdelen heerst daarmee het gevoel dat de meeste risico's in beeld zijn.[52]

Ook wij zien dat de organisatie inmiddels verder is met het uitvoeren van de risicoanalyses dan tijdens het rekenkameronderzoek uit 2021. Maar wij constateren ook dat niet alle organisatieonderdelen de afgelopen vier tertalen[53] een actuele tactische risicoanalyse hebben uitgevoerd (zie tabel 3.2). Ook niet alle benodigde operationele risicoanalyses worden structureel uitgevoerd (met name de ORA's en PRA's). Deze trend is al langer zichtbaar. Zo wordt begin 2023 gezegd: "*De trend toont een vertraging van het totaal aantal uitgevoerde operationele analyses (BIA / ORA / PRA / DPIA) per tertaal.* (…) *Dit vinden we een zorgelijke ontwikkeling.*"[54] Een betrokkene geeft aan dat de gemeentelijke organisatie

[45] Gemeente Utrecht (10 oktober 2023). Raadsbrief *Update Rekenkameronderzoek 'Zo sterk als de zwakste schakel'*.
[46] Rekenkamer Utrecht (2024). *Interviews gemeente*.
[47] Gemeente Utrecht (2023). *Gegevensbescherming in Utrecht: verantwoord en transparant. Intern strategisch beleidskader voor gegevensbescherming van Utrecht*, p. 9.
[48] Gemeente Utrecht (januari 2024). *Brede rapportage bedrijfsvoering.*
[49] Gemeente Utrecht (januari 2024). *Brede rapportage bedrijfsvoering.*
[50] Rekenkamer Utrecht (2024). *Interview gemeente*.
[51] Rekenkamer Utrecht (2024). *Interviews gemeente*.
[52] Rekenkamer Utrecht (2024). *Interviews gemeente*.
[53] Een tertaal beslaat een periode van vier maanden.
[54] Gemeente Utrecht (2023). *Monitor gegevensbescherming T3 2022.*

geen goede verklaring heeft voor deze ontwikkeling.[55] De trend is wel besproken in het MT CIO. Een belangrijke nuancering bij de trend is dat de gemeente Utrecht geen doel heeft gesteld voor het absolute of relatieve aantal risicoanalyses die minimaal uitgevoerd moeten worden. Wij constateren daarom dat blijvende aandacht nodig is om risicoanalyses uit te voeren.

Tabel 3.2 Meer risicoanalyses uitgevoerd, maar nog niet allemaal gereed en actueel

Tactisch	**2023 T1**	**2023 T2**	**2023 T3**	**2024 T1**
Aantal organisatieonderdelen dat het afgelopen jaar een tactische risicoanalyse heeft uitgevoerd	8/19	8/19	9/19	13/18
Operationeel	**2023 T1**	**2023 T2**	**2023 T3**	**2024 T1**
Totaal aantal noodzakelijke Bedrijfs Impact Analyses (BIA's) die binnen de organisatieonderdelen uitgevoerd moeten worden	244	281	349	360
➢ Aantal BIA´s daadwerkelijk uitgevoerd, gereed en actueel	212 (87%)	256 (91%)	208 (60%)	227 (63%)
Totaal aantal noodzakelijke Operationele Risico Analyses (ORA's) die binnen de organisatieonderdelen uitgevoerd moeten worden	118	114	103	108
➢ Aantal ORA´s daadwerkelijk uitgevoerd, gereed en actueel	40 (34%)	28 (25%)	31 (30%)	24 (22%)
Totaal aantal noodzakelijke Privacy Risico Analyses (PRA's) die binnen de organisatieonderdelen uitgevoerd moeten worden	142	146	195	321
➢ Aantal PRA´s daadwerkelijk uitgevoerd, gereed en actueel	131 (92%)	140 (96%)	140 (72%)	93 (29%)
Totaal aantal noodzakelijke Data Protectie Impact Analyses (DPIA's) die binnen de organisatieonderdelen uitgevoerd moeten worden	105	124	128	82
➢ Aantal DPIA´s daadwerkelijk uitgevoerd, gereed en actueel	75 (71%)	94 (76%)	114 (89%)	82 (100%)

Bronnen: Rekenkamer Utrecht (2024) o.b.v. *Monitor gegevensbescherming* van de gemeente Utrecht 2023 T3 en 2024 T1.

Voor meerderheid tactische risico's nog geen beheersmaatregelen genomen

Risico's moeten niet alleen worden geïdentificeerd, maar vervolgens ook worden geclassificeerd en beheerst. Wij constateren dat de gemeente Utrecht nu verder is met het nemen van beheersmaatregelen dan tijdens het rekenkameronderzoek uit 2021. Tegelijkertijd zien we ook dat voor een meerderheid van de geïdentificeerde tactische risico's nog geen maatregelen zijn getroffen. Veel risico's staan ook al lang open. Wanneer maatregelen wel zijn getroffen dan heeft dat vaak (te) lang geduurd.

Individuele managers en/of proceseigenaren moeten met het doorvoeren van beheersmaatregelen aan de slag. Maar het risicogebaseerd werken is bij zowel IRM-ers als

[55] Rekenkamer Utrecht (2024). *Aanvullende vragen aan de gemeente*.

bij managers en proceseigenaren "(…) *nog geen onderdeel van de genen geworden.*"[56] En: "*Medewerkers en leidinggevenden zijn ontzettend druk. Aandacht voor gegevensbescherming komt daar nog bovenop. Het is best een uitdaging om medewerkers daarop in beweging te krijgen.*"[57] IRM-ers zouden daarom nog te vaak de verantwoordelijkheid voor informatieveiligheid verschuiven naar de CISO en hun DISO.[58]

Op basis van tabel 3.3 constateren wij dat voor meerdere tertalen een meerderheid van de geïdentificeerde tactische risico's niet is opgepakt / beheerst. Een groot deel staat ook al langer dan 12 maanden open. En een groot deel van de risico's die zijn opgelost blijken niet binnen de afgesproken tijdspanne te zijn opgelost. Dit wordt door een aantal betrokkenen ook herkend. Zij zijn van mening dat meer maatregelen nodig zijn[59] en dat het oppakken en mitigeren van risico's vaak nog te lang duurt.[60] Wij kunnen niet constateren of er een risicogebaseerde afweging ten grondslag ligt aan de risico's die wel zijn opgepakt. Ter illustratie vormt DomstadIT een goed voorbeeld van hoe het risicogebaseerd werken en sneller beheersen van ICT-risico's kan worden uitgevoerd (zie box 3.4).

Tabel 3.3 Meerderheid van tactische risico's nog niet opgepakt

Tactisch	**2023 T1**	**2023 T2**	**2023 T3**	**2024 T1**
Aantal organisatieonderdelen dat het afgelopen jaar een tactische risicoanalyse heeft uitgevoerd	8/19	8/19	9/19	13/18
Totaal aantal geïdentificeerde tactische risico's*	168	131	203	183
➢ Aantal openstaande risico's	109	96	143	141
➢ Waarvan over tijd	23	23	35	41
➢ Waarvan open >12 maanden	65	65	123	98
➢ Aantal opgeloste risico's	36	31	59	46
➢ Waarvan tijdig opgelost	9	4	32	13
➢ Waarvan niet tijdig opgelost	27	27	27	33

Bron: Rekenkamer Utrecht (2024) o.b.v. *Monitor gegevensbescherming* van de gemeente Utrecht.

***** De tabel bevat een aantal optelfouten. Dit ligt aan de brondata die aan de tabel ten grondslag ligt. Het invullen van de brondata is handwerk, cijfers worden vaak uit een andere administratie onttrokken, cijfers van organisatieonderdelen worden niet in detail gecontroleerd dan wel overlegd en niet alle DISO's hanteren dezelfde nauwkeurigheid en/of hebben dezelfde mate van begrip van wat moet worden ingevuld. Deze tabel wordt dan ook vooral door het MT CIO gebruikt om de grote lijnen te bespreken.[61]

[56] Rekenkamer Utrecht (2024). *Interview gemeente.*
[57] Rekenkamer Utrecht (2024). *Interview gemeente.*
[58] Rekenkamer Utrecht (2024). *Interview gemeente.*
[59] Rekenkamer Utrecht (2024). *Interviews gemeente*.
[60] Rekenkamer Utrecht (2024). *Interviews gemeente*.
[61] Rekenkamer Utrecht (2024). *Aanvullende vragen aan de gemeente*.

Box 3.4 Hoe DomstadIT stuurt op het sneller beheersen van risico's

Zoals aangegeven in paragraaf 2.1 is DomstadIT een centraal onderdeel binnen informatie- en procesmanagement en is (o.a.) verantwoordelijk voor het leveren van ICT-middelen en de beveiliging daarvan. DomstadIT spreekt haar risico-eigenaren tegenwoordig vaker aan op het sneller oppakken van geïdentificeerde ICT-risico's. Ook heeft DomstadIT eind 2023 een handboek voor risicomanagement ontwikkeld om haar risicomanagers te helpen bij het identificeren, beoordelen, beheersen en monitoren van risico's.[62] DomstadIT brengt ook iedere maand een risicomanagement-rapportage uit waarin wordt aangegeven hoeveel risico's er zijn geïdentificeerd, afgehandeld, geaccepteerd of nog open staan. Deze rapportage wordt (o.a.) met de risico-eigenaren besproken.[63]

Deze ontwikkelingen dragen eraan bij dat risico's sneller worden opgepakt dan voorheen.[64] In die zin is DomstadIT een goed voorbeeld van hoe aan het risicogebaseerd werken invulling gegeven kan worden. Wat ons betreft verdient deze ontwikkeling bredere navolging binnen de gemeentelijke organisatie.

Genomen maatregelen op operationele risico's onbekend

In tabel 3.2 lieten we zien dat de organisatieonderdelen aan de hand van risicoanalyses operationele risico's identificeren. Er zijn geen data beschikbaar over voor hoeveel van die risico's beheersmaatregelen zijn genomen. Het is dus onbekend of maatregelen daadwerkelijk zijn genomen, en zo ja of dit risicogebaseerd heeft plaatsgevonden.

Organisatie met name op contract- en leveranciersmanagement niet in control

Met name het inzicht in de '*end of life*' dossiers vraagt om aandacht. Er is sprake van *end of life* wanneer de fabrikant aangeeft het (software)product niet meer te ondersteunen en onderhouden. Daardoor wordt het product (na verloop van tijd) kwetsbaar. De organisatie heeft niet scherp welke producten *end of life* zijn of dreigen te worden. Het contract- en leveranciersmanagement is decentraal (op operationeel niveau) bij individuele managers en/of systeemeigenaren belegd. Dat vereist dat deze medewerkers dit ook als hun eigen taak zien, daar verantwoordelijkheid in nemen en op sturen. Dat gebeurt volgens betrokkenen nog te weinig.[65] De gemeente Utrecht is daardoor niet in control. Dat leidt ertoe dat de verantwoordelijke medewerkers niet altijd goede afspraken maken met leveranciers, in de gaten houden dat aan afspraken wordt voldaan, dat software wordt geüpdatet of dat tijdig wordt aanbesteed wanneer contracten aflopen.[66] Er is daardoor beperkt zicht op oude – maar nog steeds actief zijnde – software. Dit leidt niet alleen tot kwetsbaarheden, maar ook tot de onmogelijkheid om het *life cycle management* uit te voeren om aan de Baseline Informatiebeveiliging Overheid[67] te voldoen. Er wordt daarom gewerkt aan het samenstellen

[62] Gemeente Utrecht (2024). *Handboek Risicomanagement Gegevensbescherming*.
[63] Rekenkamer Utrecht (2024). *Interview gemeente.*
[64] Rekenkamer Utrecht (2024). *Interview gemeente.*
[65] Rekenkamer Utrecht (2024). *Interview gemeente.*
[66] Rekenkamer Utrecht (2024). *Interview gemeente.*
[67] De BIO is het basisnormenkader voor informatiebeveiliging binnen alle Nederlandse overheidslagen. Zie verder hoofdstuk 2 (en met name box 2.1).

van een overzicht met alle *end of life* contracten en dossiers om te bepalen wat de doorlooptijden zijn en de mogelijke issues die daarbij komen kijken.[68]

Organisatieonderdelen leren op eigen manier van incidenten

Het afhandelen van beveiligingsincidenten verloopt volgens betrokkenen goed, maar duurt soms nog langer dan nodig. Dat komt met name doordat medewerkers elkaar niet altijd zelfstandig weten te vinden.[69] Het vervolgens leren en verbeteren van incidenten is aan de organisatieonderdelen zelf. IRM-ers gaan daar dan ook op hun eigen manier mee om. Zo geeft één IRM-er aan ernstige incidenten te bespreken met het managementteam, waarna de managers dat vervolgens vaak op hun eigen manier bespreekbaar maken in hun teams.[70]

De monitor gegevensbescherming bevat per vier maanden gegevens over het aantal incidenten dat per organisatieonderdeel heeft plaatsgevonden. De monitor bevat geen gegevens over de manier waarop de incidenten zijn opgepakt. Op basis van de beschikbare gegevens wordt geprobeerd trends zichtbaar te maken. In de viermaandelijks gesprekken tussen IPM-er en het managementteam wordt over strategieën gesproken om die trends te beheersen.[71] Hier is geen vast proces voor. IPM-ers hebben daarnaast geen zicht op de manieren waarop incidenten bij andere organisatieonderdelen worden opgepakt.[72] Daarmee wordt onvoldoende van elkaar geleerd.

We gaven in paragraaf 2.3 aan dat DomstadIT een eigen registratiesysteem voor security-incidenten bijhoudt. Incidenten werden bij DomstadIT altijd al goed opgepakt, maar het aanspreken van elkaar en het goed evalueren van incidenten ontbrak soms.[73] De afgelopen jaren is ingezet op verbetering daarvan. Onder andere het registratiesysteem wordt daarvoor gebruikt. Incidenten hebben echter niet altijd uitsluitend betrekking op DomstadIT, maar vaak ook op één of meerdere processen van een organisatieonderdeel. De managementteams van de organisatieonderdelen hebben geen zicht op het registratiesysteem van DomstadIT. Betrokkenen opperen een meer centraal en inzichtelijk registratiesysteem te hanteren, zodat beter kan worden geanalyseerd waar incidenten het vaakst plaatsvinden.[74] En zodat gemeentebreed en meer integraal van incidenten kan worden geleerd en verbeterd. Zo heeft de coördinator bewustwording gegevensbescherming op dit moment geen zicht op de oorzaken van incidenten. Bewustwordingscampagnes en -activiteiten kunnen nu dus niet vanuit een centraal punt worden afgestemd op de incidenten die decentraal plaatsvinden.[75]

[68] Rekenkamer Utrecht (2024). *Interview gemeente.*
[69] Rekenkamer Utrecht (2024). *Interview gemeente.*
[70] Rekenkamer Utrecht (2024). *Interview gemeente*.
[71] Rekenkamer Utrecht (2024). *Interview gemeente*.
[72] Rekenkamer Utrecht (2024). *Interview gemeente*.
[73] Rekenkamer Utrecht (2024). *Interview gemeente.*
[74] Rekenkamer Utrecht (2024). *Interview gemeente*.
[75] Rekenkamer Utrecht (2024). *Interview gemeente*.

Gegevensbeschermingsmanagementsysteem (GBMS) nog onvoldoende uitgewerkt voor de uitvoering, management organisatieonderdelen desondanks wel goed geïnformeerd

In paragraaf 2.4 legden we uit dat het GBMS wordt gebruikt om verantwoording af te leggen aan het management. Het GBMS onderscheidt daarvoor PDCA-cycli op drie niveaus (strategisch, tactisch, operationeel). Deze cycli moeten met elkaar in verbinding staan doordat eigenaren hun eigen PDCA-cyclus afstemmen op die van andere eigenaren. Onder andere door aan te sluiten op de bestaande planning- & controlcyclus van de gemeente. Maar hoe en hoe vaak precies afgestemd moet worden tussen de niveaus, wordt niet gespecificeerd. Het wordt ook niet duidelijk hoe de eigenaren op hetzelfde niveau met elkaar afstemmen (bijvoorbeeld de verschillende organisatieonderdelen op het tactische niveau, die allen een eigen PDCA-cyclus hanteren). Het GBMS mist daarmee nog de concrete controleslag op en tussen de verschillende niveaus. Ook niet alle medewerkers maken op dit moment gebruik van het GBMS.[76] Wij constateren dat het GBMS in opzet goed is, maar nog onvoldoende is uitgewerkt om er in de praktijk (integraal) uitvoering aan te kunnen geven.

Het afleggen van verantwoording op tactisch en operationeel niveau gebeurt viermaandelijks. De IPM-ers rapporteren periodiek aan het managementteam van hun eigen organisatieonderdeel over de voortgang op de uitvoering van het jaarplan. Dat gebeurt aan de hand van een rapportage over recordmanagement, privacy en informatieveiligheid. Deze rapportage wordt ook periodiek met de IPM-er besproken. De CISO of CPO is daar ook bij aanwezig. Er wordt met name gesproken over de voortgang op de acties en (beheers)maatregelen die zijn uitgevoerd op de eerder geïdentificeerde risico's. Op die manier blijft het management van het organisatieonderdeel goed betrokken bij en geïnformeerd over de uitvoering.[77]

[76] Rekenkamer Utrecht (2024). *Interview gemeente*.
[77] Rekenkamer Utrecht (2024). *Interview gemeente*.

4 MENS: MAATREGELEN IN OPZET GOED, IN DE PRAKTIJK NOG TE VRIJBLIJVEND

In 2022 heeft de gemeente het bewustwordingsplan voor veilig digitaal werken vastgesteld. De maatregelen daarin zijn goed, maar de uitvoering ervan is vrijblijvend. Zo heeft een klein deel van de medewerkers de e-learning afgerond en maken niet alle organisatieonderdelen gebruik van ambassadeurs als verbinding tussen de uitvoerende medewerkers en de professionals op het gebied van informatieveiligheid (DISO's en IPM-ers). Er zijn de afgelopen jaren door de gemeente geen phishing testen uitgevoerd. Uit onze testen blijkt dat medewerkers inloggegevens afstaan tijdens *voice phishing* en achtergelaten USB-sticks gebruiken. Niet alle medewerkers die met deze testen te maken hebben gehad, hebben hier melding van gemaakt. En niet alle gemeentelijke medewerkers spreken onbevoegden aan, waardoor zij lang ongestoord kunnen verblijven op medewerkersgedeelten van het Stadskantoor en Stadhuis.[78]

In dit hoofdstuk beschrijven we de manier waarop bewustwording een plaats krijgt in beleid en organisatie en hoe de medewerkers van de gemeente hier in de praktijk mee omgaan. Daarbij gaan we ook in op hoe dit zich sinds het onderzoek uit 2021 heeft ontwikkeld. We beantwoorden hiermee onderzoeksvraag 2.

De uitvoering, afgezet tegen de bijbehorende norm, leidt in figuur 4.1 tot onze beoordeling en bevindingen. Hierin leggen we ook direct de relatie tussen de onderzoeksvraag, de normen en bijbehorende criteria.

Figuur 4.1 Normen, criteria en beoordeling "Mens"

[78] De uitkomsten van een recente audit van concernaudit bevestigt onze bevindingen ten aanzien van de beperkte deelname aan de e-learning, het ontbreken van phishing testen en het gedrag van medewerkers (Concernaudit (8 augustus 2024). *Rapport Cyberweerbaarheid*).

Toelichting op het normenkader

Breed wordt onderkend dat het gedrag van mensen het belangrijkste aspect in de informatiebeveiliging is. Uit onderzoek komt naar voren dat hier vaak de grootste risico's en kwetsbaarheden optreden. Daarom is het van groot belang dat de gemeente Utrecht een concreet plan heeft om medewerkers bewust te maken van een goede manier van omgaan met (persoonlijke) informatie. En daarnaast moet ook uit de dagelijkse praktijk blijken dat medewerkers dit bewustzijn en het bijpassende gedrag ook in de uitvoering van de werkzaamheden laten zien.

4.1 BEWUSTWORDINGSPLAN VASTGESTELD, UITVOERING MAATREGELEN NOG TE VRIJBLIJVEND

Vanuit de Baseline Informatiebeveiliging Overheid BIO[79] is voorgeschreven dat alle medewerkers van de organisatie en – voor zover relevant – contractanten een passende bewustzijnsopleiding en -training krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover dat relevant is voor hun functie. Ten tijde van het rekenkameronderzoek in 2021 ontbrak een centraal programma informatiebewustzijn. De organisatieonderdelen besteedden destijds individueel en op hun eigen manier aandacht aan het onderwerp en voerden ad hoc acties uit. De rekenkamer deed daarom de aanbeveling om structureel te gaan investeren in het bewustzijn van medewerkers over informatieveiligheid. En daarbij ook aandacht te gaan besteden aan tijdelijke en externe medewerkers, omdat de introductie op het onderwerp informatiebewustzijn vaak alleen gericht was op vaste en niet ook op tijdelijke of externe medewerkers.

In oktober 2020 is het opstellen van het programma "*Bewustwording Gegevensbescherming*" opgestart.[80] Dit programma diende als strategisch document dat vervolgens werd uitgewerkt in het "*Actieplan bewustwording gegevensbescherming*". Als vervolg op het actieplan is op 21 juni 2022 het plan "*Bewustwording en communicatie gegevensbescherming. Hoe we bewust gedrag kunnen stimuleren door transparant te communiceren*" vastgesteld. In dit plan wordt op basis van kennis uit de gedragswetenschap ermee rekening gehouden dat van alle

[79] De BIO is het basisnormenkader voor informatiebeveiliging binnen alle Nederlandse overheidslagen. Zie verder hoofdstuk 2 (en met name box 2.1).
[80] Gemeente Utrecht (9 juli 2021). Raadsbrief *Plan van aanpak bij het rekenkameronderzoek*.

beslissingen die mensen op een dag nemen, zij er 95% tot 99% onbewust nemen. Het programma richt zich er dan ook op om medewerkers onbewust bekwaam te maken.[81] In het plan worden de doelen, doelgroepen, communicatiekanalen en -middelen, en de organisatie en financiën beschreven. In de gemeentelijke organisatie is veel waardering voor het plan: betrokkenen vinden het duidelijk geschreven met een heldere opdracht en dat het plan handvatten biedt om er uitvoering aan te kunnen geven.[82] Wij zien dat met name de aangekondigde maatregelen in het plan in opzet goed zijn, maar dat de uitvoering daarvan nog te vrijblijvend is.

Het plan (dat centraal is opgesteld en vastgesteld) bevat ook verantwoordelijkheden voor de "decentrale organisatie". Naast de inzet van het CIO Office wordt namelijk inzet gevraagd van de organisatieonderdelen. Leidinggevenden worden geacht hun medewerkers jaarlijks minimaal vier uur tijd beschikbaar te stellen zodat zij de e-learning kunnen volgen en kunnen deelnemen aan één of twee bewustwordingsactiviteiten. Ook een aanvullende introductie voor nieuwe medewerkers, aandacht en scholing voor specifieke kennis die nodig is voor de aard van de werkzaamheden, en de inzet van ambassadeurs zijn activiteiten die aan de organisatieonderdelen worden gelaten. In de praktijk wordt zichtbaar dat organisatieonderdelen hier dan ook op heel verschillende manieren invulling aan geven. Daardoor verschilt aandacht voor en intensiteit van bewustwordingsactiviteiten per organisatieonderdeel.

Deelname aan de e-learning blijft achter bij de doelstelling, ook andere maatregelen laten soms lang op zich wachten, phishing-testen ontbreken zelfs volledig

Betrokkenen merken ook op dat er sinds het centrale plan "*steviger wordt geacteerd"* op bewustwording.[83] De belangrijkste maatregelen en acties in de afgelopen jaren maken ook zichtbaar dat er sinds het vorige onderzoek veel in gang is gezet. In tabel 4.2 laten we zien wanneer de maatregelen in de gemeentelijke organisatie zijn geïmplementeerd. De donkergroene velden geven aan dat deze maatregel in dat jaar volledig is ingevoerd, de lichtgroene velden betekenen dat dit ten dele het geval was. Met name de algemene, informerende maatregelen zijn relatief snel en 'volledig' genomen. Uit het overzicht komt echter ook naar voren dat verschillende van de voorgenomen maatregelen nog open staan (witte velden)**.** Met name het uitblijven van **jaarlijkse interventies** zoals phishing-simulaties valt hierbij op, omdat wel onderkend wordt dat dergelijke regelmatige en terugkerende acties nodig zijn om het bewustzijn vast te houden. Het college geeft daarnaast ook aan de adoptie en het effect van maatregelen op bewustwording nauwlettend te willen monitoren. Op dit moment is er in de gemeentelijke organisatie nog altijd de wens om structureel interventies zoals phishing-simulaties in te zetten.[84]

[81] Gemeente Utrecht (21 juni 2022). Plan *Bewustwording en communicatie gegevensbescherming. Hoe we bewust gedrag kunnen stimuleren door transparante te communiceren.*
[82] Rekenkamer Utrecht (2024). *Interviews gemeente.*
[83] Rekenkamer Utrecht (2024). *Interview gemeente.*
[84] Gemeente Utrecht (9 juli 2021). Raadsbrief *Plan van aanpak bij het rekenkameronderzoek*; Rekenkamer Utrecht (2024). *Interview gemeente.*

Tabel 4.2 Maatregelen hebben in de uitvoering een vrijblijvend karakter en een deel staat nog open

	2021	2022	2023	2024
Informerend:				
Berichten op Intranet				
Informatieboekje veilig werken				
Website over gegevensbescherming				
Campagnes (m.n. Stadskantoor)				
Bewustwording:				
Welkomstmail nieuwe medewerkers				
Gegevensbescherming onderdeel onboardingsprogramma				
Trainingen voor nieuwe en bestaande leidinggevenden				
Beschikbaar stellen verdiepende opleidingen en trainingen				
Vaststellen gebruikersprotocol				
Inzetten ambassadeurs gegevensbescherming				
E-learning voor alle medewerkers				
Jaarlijks organiseren minstens 2 interventies (phishing, pubquiz, etc.)				

Bron: Rekenkamer Utrecht (2024) o.b.v. Plan *Bewustwording en communicatie gegevensbescherming;* Interviews gemeente (2024).

Bij andere maatregelen op de bewustwording constateren wij dat de implementatie lang op zich heeft laten wachten. Zo was de verwachting in juli 2021 dat het **gebruikersprotocol** in het derde kwartaal van dat jaar zou worden vastgesteld, maar was dit uiteindelijk pas in februari 2024. En de specifieke aandacht voor informatieveiligheid bij de **onboarding** van nieuwe medewerkers is centraal geregeld maar pas vanaf 2023 in de praktijk gebracht.[85] Vanaf april 2021 werd volstaan met schriftelijke informatie in een **welkomstmail** aan alle nieuwe – dus ook de tijdelijke en externe – medewerkers waarin werd verteld welke soorten informatie er zijn en hoe hiermee moet worden omgegaan. Ook werden er voor leidinggevenden en specifieke functies **verdiepende trainingen en opleidingen** aangeboden, waar decentraal binnen de organisatieonderdelen ook vaak verschillend invulling aan wordt gegeven. Ook het inzetten van **ambassadeurs** als vooruitgeschoven posten is in 2021 gestart met verschillende pilots. Bij vier organisatieonderdelen – Volksgezondheid, Maatschappelijke Ontwikkeling, een deel van Wijken en een deel van Vergunningen, Toezicht en Handhaving – is deze aanpak formeel gebruik geworden. Bij

[85] Gemeente Utrecht (30 maart 2023). *Veilig werken onboarding.*

andere organisatieonderdelen is dit nog "*in ontwikkeling*".[86] Voor betrokkenen bij deze organisatieonderdelen blijken de ambassadeurs daarmee (vrijwel) niet zichtbaar.[87]

De **e-learning voor alle medewerkers** wordt gezien als kern van de aanpak op bewustwording. In juli 2021 is de aanbesteding gedaan om te komen tot een geschikte applicatie. Vervolgens is de e-learning vanaf 2022 gefaseerd geïmplementeerd in de gemeentelijke organisatie. Op dit moment is de e-learning bij 13 van de 18 organisatieonderdelen uitgerold. Bij de overige vijf organisatieonderdelen is dit 'deels' gedaan.[88] Binnen de e-learning wordt inmiddels een breed palet aan cursussen aangeboden, maar het gebruik wordt niet afgedwongen. Wel zouden er al in de loop van 2022 maatregelen worden genomen als gedurende het jaar zou blijken dat het gebruik van deze tools achterblijft.[89] Het oorspronkelijke doel daarbij was dat alle medewerkers minimaal het niveau zilver in de e-learning zouden gaan behalen. De aangekondigde maatregelen om achterstanden in te lopen zijn niet uitgevoerd. In 2023 is wel het algemene afrondingspercentage waarnaar gestreefd wordt bijgesteld naar 80% van alle medewerkers medio 2024. Wij constateren echter dat het gebruik van de e-learning al enkele jaren niet voldoet aan deze doelstellingen (zie tabel 4.3). De gemeenteraad is hierover in oktober 2023 ook geïnformeerd. Op dat moment had "*ongeveer 10% van de ongeveer 7.000 medewerkers het gewenste niveau (level zilver) behaald*."[90] Uit de cijfers van het eerste tertaal van 2024 blijkt dat ruim 79% van de medewerkers niet op het minimale niveau zilver is.

Tabel 4.3 Deelname aan de e-learning blijft achter bij de doelstellingen

		2023 - 1	2023 - 2	2024 - 1
Niet gestart	Aantal	5.814	5.276	4.653
	Percentage	84,5%	71,3%	64,4%
Beginner	Aantal	267	401	470
	Percentage	3,9%	5,4%	6,5%
Brons	Aantal	386	614	593
	Percentage	5,6%	8,3%	8,2%
Zilver	Aantal	416	413	484
	Percentage	6,0%	5,6%	6,7%
Goud	Aantal	-	692	383
	Percentage	0,0%	9,4%	5,3%

[86] Gemeente Utrecht (9 juli 2021). Raadsbrief *Plan van aanpak bij het rekenkameronderzoek*; Gemeente Utrecht (10 oktober 2023). Raadsbrief *Update Rekenkameronderzoek 'Zo sterk als de zwakste schakel"*.
[87] Rekenkamer Utrecht (2024). *Interview gemeente.*
[88] Gemeente Utrecht (april 2024). *Monitor gegevensbescherming 1e tertaal 2024, concernoverzicht.*
[89] Gemeente Utrecht (9 juli 2021). Raadsbrief *Plan van aanpak bij het rekenkameronderzoek*.
[90] Gemeente Utrecht (10 oktober 2023). Raadsbrief *Update Rekenkameronderzoek 'Zo sterk als de zwakste schakel'.*

Diamant	Aantal	-	-	640
	Percentage	-	-	8,9%
Totaal	**Aantal**	**6.883**	**7.396**	**7.223**
	Percentage	**100,0%**	**100,0%**	**100,0%**

Bron: Rekenkamer Utrecht (2024) o.b.v. de *dashboards deelname e-learning concern.*

Betrokkenen zien dat er verschillende belemmeringen zijn om de e-learning te volgen. Zo vinden zij de huidige opzet te breed, te weinig flexibel, niet passend bij alle functies die er zijn en voor delen van de organisatieonderdelen te moeilijk.[91] Er zijn ook grote verschillen zichtbaar in de deelnamecijfers per organisatieonderdeel. De organisatieonderdelen Werk en Inkomen, Publiekszaken en Maatschappelijke Ontwikkeling kennen in vergelijking een hogere deelname, maar nog altijd heeft daar respectievelijk bijna 55%, ruim 31% en ruim 26% van alle medewerkers het gewenste niveau (op basis van de meest recente cijfers).

De e-learning is bij raads-, commissie- en fractieleden niet onder de aandacht gebracht. Dit geldt ook voor de leden van de rekenkamer. Uit de verdiepende analyse van concernaudit blijkt dat de deelname van het college en de 20 hoogste ambtenaren (“20Beraad”) ondermaats is. Slecht 1 persoon in het college en 6 van de 20 hoogste ambtenaren hebben minstens niveau zilver behaald.[92] Daarnaast wordt door betrokkenen ook opgemerkt dat het eenmalige karakter maakt dat de e-learning de bewustwording niet langdurig vergroot.[93]

De discussie over te nemen maatregelen om het gebruik van de e-learning te vergroten loopt op dit moment nog. Inmiddels heeft de centrale ondernemingsraad toestemming gegeven om deelname aan de e-learning verplicht te stellen.[94] Daarnaast wordt ook nagedacht over het aanbrengen van meer flexibiliteit en maatwerk.[95] De regiegroep heeft medio 2024 de e-learning ook geëvalueerd met het oog op een komende nieuwe aanbesteding.[96] Voor de langere termijn – vanaf 2025 – wordt nagedacht over een digitale ‘*license to operate*’: een breder toelatingsbewijs voor startende medewerkers voordat zij van de gemeentelijke ICT gebruik kunnen maken.[97]

4.2 MEDEWERKERS KWETSBAAR VOOR EXTERNE AANVALLEN

Uit ons rekenkameronderzoek van 2021 bleek dat een aanzienlijk deel van de medewerkers niet altijd bewust omging met informatie. Bij de beveiligingstesten die we destijds uit lieten voeren stond 16% van de medewerkers gebruikersnaam en wachtwoord af. Een deel

[91] Rekenkamer Utrecht (2024). *Interviews gemeente.*
[92] Concernaudit (8 augustus 2024). *Rapport Cyberweerbaarheid.*
[93] Rekenkamer Utrecht (2024). *Interview gemeente.*
[94] Rekenkamer Utrecht (2024). *Interview gemeente*.
[95] Rekenkamer Utrecht (2024). *Interview gemeente.*
[96] Rekenkamer Utrecht (2024). *Interview gemeente.*
[97] Rekenkamer Utrecht (2024). *Interviews gemeente.*

daarvan deed dat ook nadat de gemeente na de eerste testdag een waarschuwing had uitgegeven. Ook de beveiliging en sociale controle bleek op het Stadskantoor en Stadhuis niet voldoende om te voorkomen dat onbevoegden gemakkelijk en ongestoord binnen konden komen en blijven.

Medewerkers nog altijd onvoldoende bewust van de waarde van informatie

Door de e-learning, de algemene berichtgeving en aandacht voor het onderwerp op Intranet en via campagnes op de kantoorlocaties hoopt de gemeente dat de bewustwording voor informatiebeveiliging van haar medewerkers is toegenomen. In de praktijk wordt ook hier gewezen op de verschillen tussen de organisatieonderdelen.[98] Betrokkenen vragen zich ook af of aandacht vragen voor het onderwerp ook wel daadwerkelijk bewustwording verhogend is.[99] Anderen onderkennen namelijk dat in bredere zin kennis en vaardigheden nog vaak tegenvallen en dat er ook wel naïef gedrag zichtbaar blijft. Bijvoorbeeld als het gaat om gedrag op de werkplekken – zoals het niet locken van het beeldscherm als men de werkplek verlaat – en bij ontmoetingsplekken als de koffieautomaat waar gevoelige informatie weliswaar onderling maar in de openbaarheid wordt gedeeld.[100]

Ook de uitkomsten van de *mystery guest* bezoeken die we uit hebben laten voeren onderschrijven het voorgaande. Tijdens deze bezoeken waren diverse computers op het Stadskantoor niet vergrendeld. En op de bureaus lagen diverse documenten, mappen en notitieblokken. Zelfs bij de netwerkbeheerders zijn er notitieblokken aangetroffen waarvan één post-it met doorgestreepte wachtwoorden. Gesprekken van medewerkers bleken voor de *mystery guest* op het Stadskantoor af te luisteren in de kantine en op de werkplekken. Zo was het mogelijk om mee te luisteren bij de presentatie '*onboarding devices*' voor nieuwe medewerkers in de kantine en bij een telefoongesprek over maatregelen tegen de op dat moment gaande zijnde *voice phishing*test. In het Stadhuis is een oude laptop van de gemeente Utrecht aangetroffen met daarop een sticker 'inloggen Welkom123'. Het was niet mogelijk om deze laptop aan te zetten, want de batterij van de laptop was leeg en de bijbehorende adapter was niet aanwezig.[101]

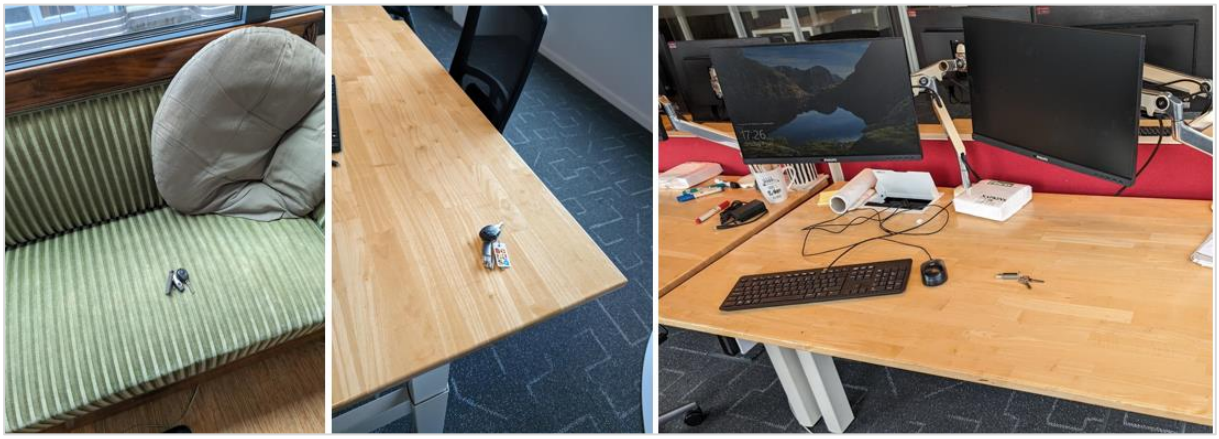
Onvoldoende bewust van de risico's van het gebruiken van achtergelaten USB-sticks

Net als in 2020 heeft de rekenkamer in 2024 een USB-dropping laten uitvoeren. Een kwaadwillende kan met een USB-stick namelijk oneigenlijk toegang krijgen tot de computer van de gebruiker. Medewerkers van de gemeente blijken nog altijd onvoldoende op de hoogte te zijn van de gevaren van USB-dropping. Bij de *mystery guest* bezoeken op het Stadskantoor en op het Stadhuis zijn tussen 3 en 5 juni vijf USB-sticks op verschillende plekken achtergelaten (zie figuur 4.4).

[98] Rekenkamer Utrecht (2024). *Interviews gemeente*.
[99] Rekenkamer Utrecht (2024). *Interview gemeente*.
[100] Rekenkamer Utrecht (2024). *Interviews gemeente*.
[101] Rekenkamer Utrecht (18 juli 2024) o.b.v. NFIR. *Rapportage Social Engineering: Mystery Guest, Voice Phishing, USB dropping.*

Op 4 en 6 juni zijn de bestanden op twee USB-sticks onveilig geopend. Dit is een vergelijkbare uitkomst met het rekenkameronderzoek uit 2021 toen twee van de vier achtergelaten USB-sticks werden geopend. Drie USB-sticks zijn door medewerkers ingeleverd bij het Serviceplein. Eén USB-stick is gevonden op de 18e verdieping (waar ook de IPM-afdeling is gehuisvest). Door de USB-stick te analyseren stelde DomstadIT op 12 juni vast dat deze malware bevatte. Diezelfde dag is Safety & Security (S&S) hiervan op de hoogte gesteld. Op basis daarvan heeft S&S haar beveiligers en centralisten verzocht om scherp te zijn op eventueel rondslingerende USB-sticks of andere afwijkende materialen. Specifiek ook bij de surveillance en brand- en sluitrondes die dagelijks worden gelopen. Er zijn verder geen USB-sticks meer aangetroffen, waardoor één USB-stick nog altijd niet is gevonden of ingeleverd. Het gebruiken van USB-sticks is in de extern toegankelijke (virtuele) werkomgeving van de gemeente overigens geblokkeerd, maar dat geldt niet voor het gebruik van USB-sticks op de beheerde laptop omdat volgens betrokken nog verder uitgezocht moet worden wat de impact daarvan zou zijn op de dagelijkse werkzaamheden van medewerkers.[102]

Figuur 4.4 USB-sticks zijn achtergelaten op verschillende plekken op het Stadskantoor en Stadhuis



Bron: Rekenkamer Utrecht (2024) o.b.v. NFIR (2024).

Medewerkers met voice phishing over te halen om inloggegevens af te staan

Medewerkers van de gemeente blijken ook te verleiden te zijn om hun inloggegevens achter te laten tijdens *voice phishing*. Ook wanneer er anoniem wordt gebeld. In totaal zijn zeven medewerkers van de gemeente Utrecht door het externe bureau via de telefoon benaderd via 19 belpogingen. Van de zeven medewerkers hebben vier medewerkers een website geopend en daar hun inloggegevens ingevoerd op een nep ICT Servicedesk pagina. Medewerkers blijken niet altijd de ware identiteit van de beller te controleren. En het is voor kwaadwillenden eenvoudig om op basis van openbare informatie de persoonsgegevens van een medewerker van de gemeente te benutten. Medewerkers van de gemeente blijken zich

[102] Rekenkamer Utrecht (2024). *Interview gemeente*.

niet bewust van de gevaren van *voice phishing*.[103] Het is niet mogelijk om een ontwikkeling of trend af te leiden met eerdere phishingacties, omdat de acties uit 2020 anders van opzet waren (*mail phishing*) en er in de afgelopen jaren door de gemeente geen phishingtesten zijn uitgevoerd.

Betrokkenen ervaren een open cultuur, maar elkaar aanspreken op ongewenst gedrag, het melden van incidenten en aanspreken van onbekend bezoek gebeurt nog onvoldoende

Net als ten tijde van ons onderzoek in het najaar van 2020 ervaren betrokkenen een open cultuur bij de gemeente Utrecht. Een open en veilige cultuur is belangrijk om medewerkers zich vrij te laten voelen om incidenten en risico's te melden en maatregelen voor te stellen. Het omgaan met informatiebeveiligingsincidenten is inmiddels een vast onderdeel van het bewustwordingsprogramma. Medewerkers worden gestimuleerd om incidenten te melden en bij de afhandeling richt men zich erop om van de ervaring te leren en melders er niet op af te rekenen. Betrokkenen benadrukken dat daar blijvende aandacht voor moet zijn, omdat er nog altijd schaamte rond het melden van incidenten bestaat.[104]

Er zijn twee routes voor de meldingen: formeel via Serviceplein en informeel via de IPM-er en/of de DISO van het organisatieonderdeel. Omdat beide routes regelmatig worden gebruikt, is het algemene beeld dat medewerkers incidenten in principe wel durven te melden.[105] Het aantal gemelde incidenten is echter al langere tijd min of meer stabiel. Uit de meest recente monitoren gegevensbescherming blijkt dat het per tertaal om circa 40 tot 45 meldingen van securityincidenten gaat. En ook het aantal meldingen van datalekken is min of meer stabiel tussen de 40 en 50 per tertaal.[106] Jaarlijks komt het aantal meldingen daarmee per categorie op circa 150.

Het elkaar aanspreken op ongewenst gedrag komt in de beleving van betrokkenen maar mondjesmaat voor.[107] Betrokken merken dat de cultuur bij de gemeentelijke organisatie nog vaak te "*lief, naïef en behulpzaam*" of "*te slap*" is.[108] Dit wordt ook zichtbaar bij de bezoeken van de *mystery guest*. Op verschillende momenten is deze door medewerkers van de gemeentelijke organisatie aangesproken, maar medewerkers begeleiden ongewenste bezoekers niet naar buiten het beveiligd gebied.[109] Meldingen van de USB-dropping lieten over het algemeen langer op zich wachten. Over de *voice phishing* werd beter gemeld (maar niet door iedereen). Zo werden op maandag 3 juni de eerste inloggegevens van twee medewerkers bemachtigd. Die dag kwam één melding over de *voice phishing* binnen bij het Serviceplein. Op donderdag 6 juni werden de inloggegevens van nog twee medewerkers

[103] Rekenkamer Utrecht (18 juli 2024) o.b.v. NFIR. *Rapportage Social Engineering: Mystery Guest, Voice Phishing, USB dropping.*
[104] Rekenkamer Utrecht (2024). *Interview gemeente.*
[105] Rekenkamer Utrecht (2024). *Interviews gemeente.*
[106] Gemeente Utrecht (april 2024). *Monitor gegevensbescherming 1e tertaal 2024, concernoverzicht.*
[107] Rekenkamer Utrecht (2024). *Interviews gemeente.*
[108] Rekenkamer Utrecht (2024). *Interview gemeente*.
[109] Rekenkamer Utrecht (18 juli 2024) o.b.v. NFIR. *Rapportage Social Engineering: Mystery Guest, Voice Phishing, USB dropping.*

bemachtigd, waarna nog eens vijf medewerkers melding deden. Er is door DomstadIT snel gehandeld en meteen besloten om dit als een security incident aan te merken. Diezelfde dag werd nog een waarschuwing over een actieve *voice phishing* aanval verstuurd naar alle gemeentelijke medewerkers.

Medewerkers accepteren niet altijd dat zij op hun houding, gedrag of functioneren worden aangesproken. Het is voor leidinggevenden daarom lastig om daarop te sturen.[110] Om dingen te kunnen veranderen in houding en gedrag bij incidenten achten betrokkenen dan ook een cultuurverandering nodig. "*Mensen mogen kritisch zijn op zichzelf en collega's, zodat iedereen leert van situaties.* (…) *Dit stukje reflectiviteit en leren is mogelijk nog niet goed georganiseerd.*"[111] Hierbij is het besef aanwezig dat cultuurverandering tijd nodig heeft. Daarom wordt ook hier *life cycle management* ingezet, waarbij de verandering begint bij de nieuwe medewerkers. Hen wordt (tijdens de onboarding) met name onder de aandacht gebracht dat zij zelf een verantwoordelijkheid dragen bij gegevensbescherming. In een periode van ongeveer zeven jaar (bij natuurlijk verloop) zou dan een cultuurverandering breder moeten zijn doorgevoerd.[112]

[110] Rekenkamer Utrecht (2024). *Interview gemeente.*
[111] Rekenkamer Utrecht (2024). *Interview gemeente*.
[112] Rekenkamer Utrecht (2024). *Interviews gemeente.*

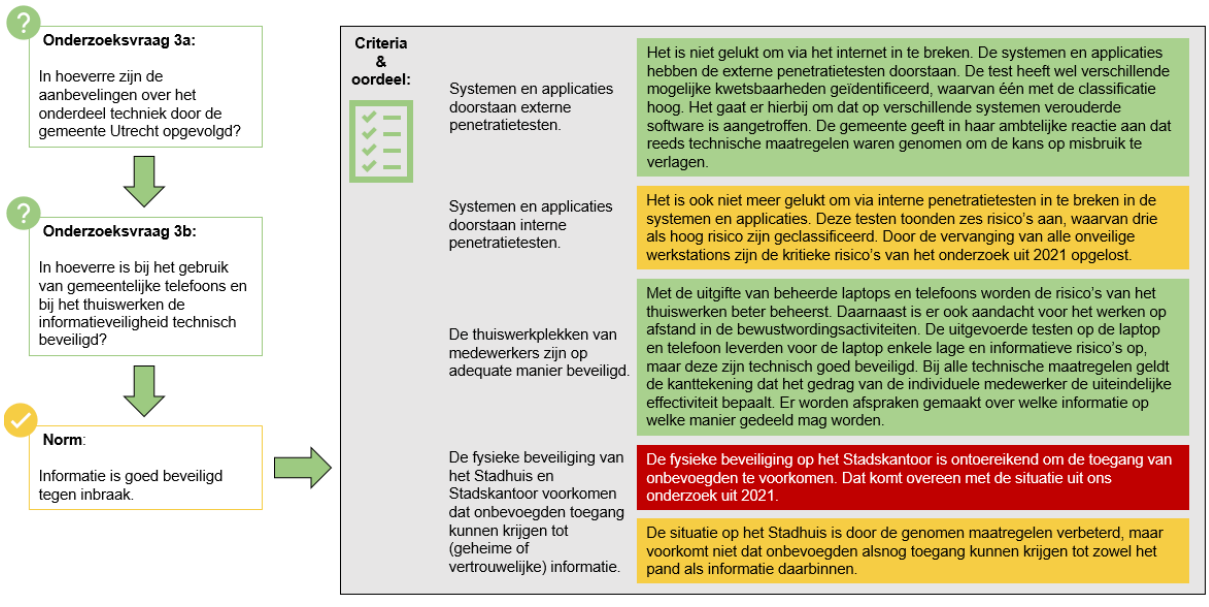
5 TECHNIEK: INFORMATIE BETER BEVEILIGD TEGEN DIGITALE INBRAKEN

Gemeentelijke systemen zijn beter beveiligd tegen digitale inbraken dan in 2021. Doordat technische maatregelen zijn doorgevoerd doorstaan systemen en applicaties zowel externe als interne penetratietesten. Deze testen identificeren nog wel een aantal 'hoge' risico's die aangepakt moeten worden. Thuiswerkplekken zijn inmiddels goed beveiligd dankzij het doorvoeren van (technische) maatregelen. Dit geldt ook voor de door de gemeente beheerde laptops en telefoons. Maar het gedrag van medewerkers is op afstand niet controleerbaar. Ook in de thuiswerksituatie is dus een belangrijke rol weggelegd voor bewustwording bij medewerkers over het veilig en verstandig omgaan met informatieveiligheid. De fysieke beveiliging op het Stadskantoor is nog steeds ontoereikend. Op het Stadhuis zijn beveiligingsmaatregelen doorgevoerd, maar ook daar blijft het mogelijk om als onbevoegde toegang te krijgen tot het beveiligd gebied en informatie in te zien.

In dit hoofdstuk beschrijven we de uitkomsten van de verschillende testen die het externe bureau heeft uitgevoerd op de technische en fysieke beveiliging. Daarbij wordt ook in kaart gebracht hoe er opvolging is gegeven aan de aanbevelingen op dit aspect uit het vorige onderzoek. Hiermee beantwoorden we de onderzoeksvragen 3a en 3b.

De uitvoering, afgezet tegen de bijbehorende norm, leidt in figuur 5.1 tot onze beoordeling en bevindingen. Hierin leggen we ook direct de relatie tussen de onderzoeksvraag, de norm en bijbehorende criteria.

Figuur 5.1 Norm, criteria en beoordeling "Techniek"



Toelichting op het normenkader

Om de informatie tegen toegang en misbruik voor onbevoegden te beschermen is een goede technische beveiliging van systemen en applicaties nodig. Daarnaast werken veel medewerkers van de gemeente Utrecht deels thuis of op andere locaties. Het is daarom nodig dat de gemeente ook maatregelen treft om dit werken op afstand veilig te laten verlopen. En een adequate fysieke beveiliging moet voorkomen dat externen toegang hebben tot de afgesloten delen van de gemeentelijke gebouwen en daar geheime of vertrouwelijke informatie kunnen inzien of ontvreemden.

5.1 DIGITALE INBRAKEN DOOR TECHNISCHE MAATREGELEN NIET MEER MOGELIJK

Zowel voor ons onderzoek in het najaar van 2020 als tijdens dit opvolgingsonderzoek is de technische beveiliging van de systemen en applicaties van de gemeente Utrecht door een gespecialiseerd bureau onderzocht.[113] Hiervoor zijn verschillende zogeheten penetratietesten uitgevoerd. Bij externe penetratietesten gaat het om digitale aanvallen van buitenaf, bij interne penetratietesten om digitale aanvallen vanaf werklocaties van de gemeente. De testen zijn uitgevoerd volgens internationale standaarden voor het ontdekken en classificeren van kwetsbaarheden.[114]

De kwetsbaarheden die dit keer gevonden zijn, lichten we onder de uitkomsttabellen nader toe. Daarbij geven we ook advies over hoe deze kwetsbaarheden te beheersen. De kwetsbaarheden uit 2021 zijn nader toegelicht in het onderzoeksrapport van destijds, maar zijn nu ook in de tabellen van een oordeel voorzien over de mate van opvolging (in de kolom “Huidige status”). Deze opvolging is op verschillende momenten gemeten: in 2022 heeft concernaudit een follow-up audit gedaan bij de opzet van de opvolging van onze bevindingen uit 2021[115] en de gemeente Utrecht heeft accountantsorganisatie BDO in 2024 opdracht gegeven om een hertest uit te voeren op de interne en externe infrastructuur.[116] Op deze hertest heeft de rekenkamer in het kader van dit opvolgingsonderzoek een review laten uitvoeren.[117]

Systemen en applicaties doorstaan de externe penetratietesten

Het is net als in het najaar van 2020 niet gelukt om via het internet binnen te dringen in de gemeentelijke systemen en applicaties. Een groot deel van de kwetsbaarheden van 2021 zijn inmiddels (bijna) opgelost en ook het niveau van de gevonden kwetsbaarheden is nu

[113] NFIR (18 juli 2024). *Rapportage pentest. Externe en Interne Infrastructuur (Timeboxed)*
[114] De volgende standaarden zijn van toepassing op deze opdracht:
- Penetration Testing Execution Standard (PTES): standaard ten behoeve van infrastructuur penetratietesten.
- Common Vulnerability Scoring System (CVSS): standaard die wordt gebruikt om de ernst van de kwetsbaarheden te classificeren.

[115] Concernaudit (16 september 2022). *Rapport Follow-up audit opvolging bevindingen Rekenkamer – Definitief*.
[116] BDO (25 march 2024). Pentest report. *New perspectives for gemeente Utrecht*.
[117] NFIR (25 juni 2024). *Hertest rapportage: RKC en VDI/Laptop.*

lager (zie tabel 5.2). De externe penetratietest voor het opvolgingsonderzoek heeft wel verschillende risico's geïdentificeerd, waarvan één met de classificatie hoog: op verschillende systemen is verouderde software aangetroffen.

Tabel 5.2 Externe penetratietesten maken een positieve ontwikkeling zichtbaar

Kwetsbaarheid 2021	Risico-classificatie	Huidige status	Kwetsbaarheid 2024	Risico-classificatie
Niet meer ondersteunde software aanwezig	Kritiek	Opgelost	Verouderde software aangetroffen	Hoog
Registreren van multifactor-authenticatie mogelijk	Hoog	Opgelost	Onveilige (SSL/TLS) configuratie	Gemiddeld
Ontbreken van security headers	Gemiddeld	Deels opgelost	Onveilige (SSL) certificaten	Gemiddeld
Niet-ondersteunde versie scripttaal gedetecteerd	Gemiddeld	Opgelost	Security Headers	Laag
Verouderde Javascript-bibliotheek aangetroffen	Gemiddeld	Opgelost	Wachtwoordbeleid onvoldoende	Laag
Gegevens onnodig benaderbaar voor alle medewerkers	Gemiddeld	Opgelost	Enumeratie vacatureteksten leidt tot inzicht in de infrastructuur	Informatief
Password Spraying niet mogelijk	Informatief	n.v.t.	Metadata inzichtelijk	Informatief
			Gelekte wachtwoorden gevonden	Informatief
			Achterhaalde telefoonnummers leiden tot succesvolle voice-phishing	Informatief
			Beheerpagina – Extern beschikbaar	Informatief
			Openbare informatie over de Wi-Fi netwerken	Informatief

Bronnen: Hoffmann B.V., 2021; NFIR, 2024.

Verouderde software aangetroffen (hoog)

De hoogste kwetsbaarheid vormt de verouderde software die bij de testen is aangetroffen. Omdat verouderde software mogelijke kwetsbaarheden bevat en/of geen beveiligingsupdates meer ontvangt, kan dit niet langer als veilig worden beschouwd. Dit kan

op langere termijn tot problemen leiden, omdat deze (toenemende) kwetsbaarheden door kwaadwillenden uitgebuit kunnen gaan worden. Ook in het onderzoek in het najaar van 2020 vormde ‘niet meer ondersteunde software’ een risico (destijds geclassificeerd als kritiek). Ondanks dat BDO in januari 2024 vaststelde dat deze kwetsbaarheid uit 2021 was opgelost, blijkt er bij de externe penetratietest van NFIR in juni 2024 toch weer verouderde software aanwezig te zijn. In principe geldt dat de constatering van vandaag, morgen al achterhaald kan zijn. Dit benadrukt het belang van goed leveranciers- en contractmanagement en het continu blijven monitoren van de End-of-Life datum van een (nieuw) product. De gemeente geeft in haar ambtelijke reactie aan dat op dit punt reeds technische maatregelen waren genomen om de kans op misbruik te verlagen.

Onveilige configuratie (gemiddeld)
Verschillende protocollen zijn kwetsbaar voor aanvallen die het versleutelde verkeer tussen de server en computer aftappen en ontsleutelen. Deze protocollen zijn soms al jarenlang end-of-life en worden daarom niet meer ondersteund door de meest gebruikte browsers. Een kwaadwillende kan een aanval uitvoeren en zo het onderlinge dataverkeer ontsleutelen, waardoor alle informatie die wordt verstuurd inzichtelijk wordt. Het advies is daarom om de onveilige instellingen niet meer te ondersteunen.

Onveilige certificaten (gemiddeld)
Het externe bureau heeft verschillende certificaten aangetroffen die onveilig zijn. Dit kan meerdere oorzaken hebben: het certificaat is verlopen en dus ongeldig, het certificaat is niet uitgegeven door een erkende certificaatautoriteit, of een certificaat is ‘self-signed’ en wordt daarom ook niet ondersteund door een certificaatautoriteit. De gemeente Utrecht loopt hiermee het risico dat een kwaadwillende het verkeer naar een applicatie onderschept. Het advies is om geldige en veilige certificaten te gebruiken zodat gebruikers de applicatie kunnen bezoeken over een beveiligde verbinding (HTTPS).

Security headers (laag)
Security headers helpen bezoekers van de gemeentelijke websites om hun browser weerbaar te maken tegen kwetsbaarheden. Bij 7 van de 39 websites die in het opvolgingsonderzoek zijn onderzocht, zijn niet alle aanbevolen security headers ingesteld. Het niet instellen van security headers kan resulteren in de succesvolle uitbuiting van applicatie specifieke kwetsbaarheden en bekend onveilig gedrag van browsers. Daarom wordt geadviseerd om de security headers restricties in te stellen volgens de aanbevolen *best practice*.

Wachtwoordbeleid externe website onvoldoende (laag)
Het gebruikte wachtwoordbeleid op één specifieke gemeentelijke website kan geen veilige wachtwoorden garanderen. Hierdoor kunnen gebruikers van deze website onveilige wachtwoorden aanmaken en gebruiken. De wachtwoordlengte voldoet niet aan het gestelde advies van het Nationaal Cyber Security Centrum (NCSC). Daardoor ontstaat de

mogelijkheid dat een account zonder toestemming van de gebruiker wordt overgenomen. De eindgebruiker is daarmee de controle over het account kwijt. Daarom wordt geadviseerd om een nieuw wachtwoordbeleid in te voeren, zoals voorgeschreven door het NCSC.

Naast deze vijf belangrijkste risico's zijn zes risico's geïdentificeerd in de categorie 'informatief':

- Enumeratie vacatureteksten: in openbare vacatureteksten staat informatie over de digitale infrastructuur en diensten van de gemeente Utrecht. Kwaadwillenden kunnen deze informatie gebruiken voor gerichte aanvallen op specifieke systemen. Geadviseerd wordt daarom om deze informatie niet meer in vacatureteksten te delen.
- Metadata inzichtelijk: metadata zijn gegevens die andere gegevens beschrijven zoals de software waarmee een bestand is gemaakt, de opsteller van een document en bijvoorbeeld e-mailadressen. Deze informatie kan een kwaadwillende gebruiken voor gerichte *social engineering* en/of *password spraying* aanvallen. Geadviseerd wordt om de metadata voor publicatie van de bestanden te verwijderen.
- Gelekte wachtwoorden: door gebruik te maken van een database uit 2012 zijn in totaal 115 gelekte wachtwoorden gevonden. Een kwaadwillende kan deze met andere datalekken mogelijk gebruiken om een account over te nemen. Maatregelen hiertegen vallen onder het advies van nieuw wachtwoordbeleid.
- Achterhaalde telefoonnummers: met behulp van *Google Dorks* was het mogelijk om telefoonnummers van medewerkers te achterhalen. Deze informatie kan een kwaadwillende gebruiken voor een gerichte *social engineering* aanval. Maatregelen hiertegen sluiten aan bij het verwijderen van metadata voor publicatie van bestanden.
- Beheerpagina – Extern beschikbaar: een beheerportaal van een gemeentelijke website blijkt extern toegankelijk. Met de juiste inloggegevens kan een kwaadwillende hier extern toegang toe krijgen. Geadviseerd wordt alleen IP-adressen toegang te verlenen die daadwerkelijk toegang tot dit portaal nodig hebben.
- Openbare informatie Wi-Fi netwerken: het blijkt mogelijk om informatie te achterhalen over de Wi-Fi netwerken waarmee een kwaadwillende een aanval kan plaatsen. Daarmee kan vervolgens geprobeerd worden zwakke punten of kwetsbaarheden in de netwerkbeveiliging te identificeren en uit te buiten door ongeautoriseerde toegang. Geadviseerd wordt om hier certificaten en segmentatie voor te gebruiken.

Systemen en applicaties doorstaan nu ook de interne penetratietesten

Het is – in tegenstelling tot de uitkomsten van het najaar 2020 – nu niet meer gelukt om via interne penetratietesten in te breken in de gemeentelijke systemen en applicaties. Deze testen toonden destijds zes risico's aan, waarvan drie met een hoog risico. De gemeente had de risico's die voortkwamen uit het onderzoek destijds al in twee categorieën opgedeeld[118]:

1. Risico's die als zelfstandig konden worden opgepakt en opgelost, en;
2. Risico's die verbonden zijn aan de inrichting van de werkplekken.

[118] Gemeente Utrecht (9 juli 2021). Raadsbrief *Plan van aanpak bij het rekenkameronderzoek*.

Door de vervanging van alle onveilige werkstations op de werkplekken zijn de kritieke risico's de afgelopen jaren opgelost. Het blijkt nog wel mogelijk om Powershell te openen ondanks dat dit geblokkeerd is. De kwetsbaarheid van het ontbreken van netwerkauthenticatie blijkt wel volledig te zijn opgelost, maar leidt tot nieuwe (meer beperkte) risico's. De overige kwetsbaarheden uit 2021 zijn inmiddels wel opgelost (zie tabel 5.3).

Tabel 5.3 Interne kwetsbaarheden met de vervanging van de werkstations grotendeels opgelost

Kwetsbaarheid 2021	Risico-classificatie	Huidige status	Kwetsbaarheid 2024	Risico-classificatie
Werkstations onveilig	Kritiek	Opgelost	Evil-twin aanval mogelijk	Hoog
Ontbrekende beveiligingsupdates niet toegepast	Kritiek	Opgelost	Verouderde software aangetroffen	Hoog
Verouderde besturingssystemen aanwezig	Kritiek	Opgelost	Onveilige configuratie	Gemiddeld
Administratieaccounts onvoldoende beschermd	Kritiek	Opgelost	Netwerktoegang zonder authenticatie	Gemiddeld
Ontbreken multifactor-authenticatie	Hoog	Opgelost	Onveilige Remote Desktop configuratie	Laag
Zwakke wachtwoorden en beheer onvoldoende veilig	Hoog	Deels opgelost	LLMNR[119] Spoofing mogelijk	Informatief
Ontbreken netwerk-authenticatie	Hoog	Opgelost		
Systemen kwetsbaar voor spoofing	Hoog	Opgelost		
Ontbreken harddisk encryptie	Gemiddeld	Opgelost		

Bronnen: Hoffmann B.V., 2021; NFIR, 2024

Evil-twin aanval mogelijk (hoog)

Tijdens het onderzoek is informatie achterhaald over de gebruikte Wi-Fi netwerken. Deze informatie is gebruikt voor het uitvoeren van een Evil-twin aanval.[120] Via deze aanval zijn wachtwoorden van medewerkers onderschept. Tijdens deze penetratietest is het echter niet

[119] LLMNR: *Link-Local Multicast Name Resolution.*

[120] Een Evil-twin is een kwaadaardig draadloos toegangspunt dat zich voordoet als een legitiem Wi-Fi toegangspunt, zodat een aanvaller persoonlijke of bedrijfsinformatie kan verzamelen zonder medeweten van de eindgebruiker, zoals de inloggegevens van het netwerk.

gelukt om het versleutelde wachtwoord te kraken naar een leesbaar wachtwoord. Geadviseerd wordt om gebruik te maken van certificaten voor het authentiseren op Wi-Fi netwerken.

Verouderde software aangetroffen (hoog)
Net als bij de externe penetratietesten is ook bij de interne penetratietesten op verschillende systemen verouderde software aangetroffen. Deze software heeft kwetsbaarheden en/of heeft beveiligingsupdates nodig en kan in zijn huidige vorm niet langer als veilig worden beschouwd. Door de kwetsbaarheden uit te buiten zou een kwaadwillende het systeem over kunnen nemen. Geadviseerd wordt om ook deze software te updaten naar de nieuwste versie of een nieuwe versie te installeren.

Onveilige configuratie (gemiddeld)
Bij de interne testen bleken ook verschillende protocollen kwetsbaar te zijn voor aanvallen die het versleutelde verkeer tussen de server en computer aftappen en ontsleutelen. Ook deze protocollen zijn soms al jarenlang end-of-life en worden daarom niet meer ondersteund door de meeste browsers. Een kwaadwillende kan een aanval uitvoeren en zo het onderlinge dataverkeer ontsleutelen. Dit maakt alle informatie die wordt verstuurd inzichtelijk. Ook hier is het advies om de onveilige instellingen niet meer te ondersteunen.

Netwerktoegang zonder authenticatie (gemiddeld)
Bij het tot stand brengen van een verbinding met een netwerkkabel wordt toegang verkregen tot internet zonder enige vorm van authenticatie. Er wordt toegang verleend tot een omgeving die gescheiden is van het interne bedrijfsnetwerk. Hierdoor zouden kwaadwillenden en medewerkers met een eigen laptop aan dit gescheiden deel van het netwerk kunnen worden gekoppeld. Als er sprake is van fysieke toegang tot de gemeentelijke gebouwen – hier gaan we paragraaf 4.2 nader op in – dan kan een kwaadwillende toegang krijgen tot dit gescheiden netwerk en dit als basis gebruiken om interne kwetsbaarheden in het netwerk op te sporen. De gemeente loopt dan ook het risico dat eigen IT-middelen zonder medeweten van de DomstadIT worden ingeschakeld. En toegang tot het gescheiden netwerk kan wel worden gebruikt om Shadow-IT op toe te passen en om interne scans naar kwetsbaarheden in de systemen op uit te voeren. Geadviseerd wordt om onbekende apparaten niet toe te laten op het netwerk.

Onveilige Remote Desktop configuratie (laag)
De host heeft een onveilige configuratie. De gemeente geeft in haar ambtelijke reactie aan dat het hier om een verouderde test werkplek gaat. Daarmee is het voor een kwaadwillende mogelijk om een aanval uit te voeren en mogelijk de sessie van de gebruiker over te nemen. Daarnaast kan de versleuteling van de verbinding niet worden gegarandeerd. Geadviseerd wordt om alleen andere vormen van authenticatie toe te passen.

LLMNR Spoofing mogelijk (informatief)
Het is mogelijk om het *Link-Local Multicast Name Resolution* (LLMNR) te spoofen. Spoofing is het vervalsen van kenmerken met als doel om tijdelijk een valse identiteit aan te nemen. Om dit te bereiken luistert de aanvaller naar LLMNR-verzoeken en vervalst wachtwoorden om verkeer naar zijn machine te leiden. De verkregen *hashes* (in dit geval niet van de gemeente) kunnen mogelijk worden gekraakt en daarmee kan een kwaadwillende wachtwoorden van gebruikers verkrijgen. Geadviseerd wordt om te onderzoeken of het LLMNR-protocol noodzakelijk is binnen het netwerk. Het protocol kan mogelijk ook worden uitgeschakeld waardoor deze kwetsbaarheid wordt opgelost.

Voor wat betreft de aanpak van de technische risico's wordt door betrokkenen met name verwezen naar de kennis van de CISO en de ICT'ers bij DomstadIT omdat zij daar zelf geen volledig zicht op hebben.[121] De CISO en DomstadIT geven aan dat er de afgelopen jaren veel stappen zijn gezet om de technische beveiliging te verbeteren. Zij constateren dat daarmee inmiddels de buitenste schil op orde is. Nu worden de mogelijkheden verkend om niet alleen de gebruikte apparatuur te beveiligen, maar ook de gebruikte gegevens, bestanden en de data daarin. Als bestanden beveiligd worden, kunnen alleen gemachtigden deze openen. Dan wordt het ook voor medewerkers die uit dienst zijn niet langer mogelijk om dat daarna nog te doen (wanneer zij bijvoorbeeld werkbestanden naar een privémailadres hebben gestuurd).[122] En er is sprake van spanningsvelden. "*Vanuit informatiebeheer is het bijvoorbeeld belangrijk om gegevens lang te bewaren zodat ook op lange termijn de organisatie zichzelf kan verantwoorden. Maar sommige maatregelen op veiligheid vragen juist om het tegenovergestelde. Hoe ga je daarmee om? En wie maakt uiteindelijk de keuze als de CPO en CISO het op een onderwerp met elkaar oneens zijn?*"[123] Deze vragen zijn nog onbeantwoord.

DomstadIT neemt jaarlijks penetratietesten af op de werkplekken en maakt daarnaast ook gebruik van externe kennis op het gebied van informatieveiligheid. Zij willen (potentiële) kwetsbaarheden zoveel mogelijk proactief aanpakken om de veiligheid van de gemeentelijke systemen te waarborgen.[124] Volgens betrokkenen gaat dat steeds beter.[125] DomstadIT verhelpt namelijk in toenemende mate problemen. Maar in de gevallen waarbij organisatieonderdelen betrokken moeten worden bij het oplossen van problemen gaat dat nog een stuk langzamer. Het is niet duidelijk wat er moet gebeuren wanneer kwetsbaarheden daardoor te lang open blijven staan. Er is binnen de gemeente geen stok achter de deur om het gebruik van kwetsbare software te verbieden, of om applicatie- of proceseigenaren te dwingen de kwetsbaarheden te verhelpen. [126]

[121] Rekenkamer Utrecht (2024). *Interviews gemeente.*
[122] Rekenkamer Utrecht (2024). *Interviews gemeente.*
[123] Rekenkamer Utrecht (2024). *Interview gemeente.*
[124] Gemeente Utrecht (25 april 2024). Intern memo. *Toelichting Retest op de VDI, fat client en laptop.*
[125] Rekenkamer Utrecht (2024). *Interview gemeente*.
[126] Rekenkamer Utrecht (2024). *Interview gemeente*.

5.2 THUISWERKPLEKKEN TECHNISCH GOED BEVEILIGD, GEDRAG OP AFSTAND NIET CONTROLEERBAAR

Bij het beveiligen van de thuiswerkplekken is sprake van een spanningsveld. Het college verwoordt dit al in het plan van aanpak: "*Omdat thuiswerken per definitie betrekking heeft op de privésfeer van de werknemer is de mate waarin we controle uit kunnen en willen oefenen beperkt.*"[127] Medewerkers hebben daardoor een belangrijke verantwoordelijkheid in het veilig en bewust omgaan met informatieveiligheid in de thuiswerksituatie. Betrokkenen geven aan dat niet met zekerheid kan worden gesteld dat alle medewerkers thuis (of op een andere locatie) op een goed beveiligde WiFi-verbinding werken.[128] Het werken buiten de gemeentelijke apparaten om wordt zoveel mogelijk gebruiksonvriendelijk gemaakt.[129] Daardoor spelen discussies tussen gebruiksgemak en beheersmaatregelen voor informatieveiligheid vaak op. Er zijn de afgelopen jaren twee maatregelen genomen die het veilig thuis werken hebben bevorderd:

1. Het uitgeven van beheerde laptops en telefoons en het gebruik van een virtual desktop (via Azure). Hiermee wordt zoveel mogelijk voorkomen dat medewerkers op privéapparatuur en in een digitale privéomgeving werken en houdt de gemeente de controle over de (beveiliging van) data. Medewerkers die toch liever op een privételefoon werken kunnen gebruikmaken van een beveiligde virtuele omgeving op hun eigen telefoon.[130] Ook de digitale samenwerkingsomgeving en het gebruik van vergadertools wordt met 'Werken 3.0' beter georganiseerd. Informatie blijft op deze manier niet op onbeheerde plekken achter.
2. Aandacht voor veilig thuiswerken in de bewustwordingsactiviteiten. In het nieuwe protocol voor het gebruik van automatiseringsmiddelen wordt in afzonderlijke paragrafen ingegaan op het 'werken op afstand' en het gebruiken van automatiseringsmiddelen en het werken in het buitenland.[131]

DomstadIT draagt zorg voor de technische maatregelen die nodig zijn, maar er wordt bewust geen software geïnstalleerd die controleert of en hoe de medewerkers aan het werk zijn.[132]

Door de gemeente beheerde laptop en telefoon technisch goed beveiligd

Het externe bureau heeft ook een door de gemeente beheerde laptop en telefoon getest. Dit leverde voor de laptop enkele lage en informatieve risico's op (zie tabel 5.4).

[127] Gemeente Utrecht ((9 juli 2021). Raadsbrief *Plan van aanpak bij het rekenkameronderzoek*.
[128] Rekenkamer Utrecht (2024). *Interviews gemeente*.
[129] Rekenkamer Utrecht (2024). *Interview gemeente*.
[130] Gemeente Utrecht (11 januari 2022). Raadsbrief *Actiepunten rekenkameronderzoek*.
[131] Gemeente Utrecht (28 februari 2024). *Protocol automatiseringsmiddelen.* Met name de pagina's 8 en 9.
[132] Gemeente Utrecht (10 oktober 2023). Raadsbrief *Update Rekenkameronderzoek 'Zo sterk als de zwakste schakel'*.

Tabel 5.4 Enkele lage en informatieve risico's bij de laptop en telefoon

Kwetsbaarheid	Risicoclassificatie
WiFi-wachtwoorden opgeslagen op laptop	Laag
Toegang tot Command Prompt en PowerShell	Informatief
USB-sticks worden niet overal geblokkeerd	Informatief
Proxy configuratie staat op 'detecteer automatisch'	Informatief

Bron: NFIR, 2024

Wi-Fi wachtwoorden opgeslagen op laptop (laag)
Er zijn meerdere draadloze netwerken opgeslagen op de laptop. Met de profielnaam en het wachtwoord is het mogelijk in te loggen op de gevonden Wi-Fi netwerken. Geadviseerd wordt om netwerken die niet meer gebruikt worden uit het geheugen te halen.

Toegang tot Command Prompt en PowerShell (informatief)
Gebruikers van de gemeentelijke laptops hebben toegang tot Command Prompt (CMD) en PowerShell waarmee een kwaadwillende commando's kan uitvoeren. Daarmee kan worden geprobeerd om verdere toegang tot het systeem te krijgen. Geadviseerd wordt om deze tools te blokkeren voor de standaardgebruikers.

USB-sticks worden niet geblokkeerd (informatief)
Het gebruik van USB-sticks wordt toegestaan op de door de gemeente beheerde laptop. Ook andere verwijderde opslag *devices* worden hier niet geblokkeerd. USB-sticks kunnen op verschillende manieren door kwaadwillenden misbruikt worden. Geadviseerd wordt om de functies 'lezen' en 'schrijven' uit te schakelen, waardoor wel gebruik kan worden gemaakt van toetsenborden, muizen en *docking stations* maar niet meer van USB-sticks en andere opslagapparatuur.

Proxy configuratie staat op 'detecteer automatisch' (informatief)
Windows zoekt en gebruikt een netwerk proxy op het moment dat deze gedetecteerd wordt. Een kwaadwillende kan hiermee een aanval opzetten die bijvoorbeeld kan leiden tot het vergiftigen van websitepagina's. Ook kunnen phishing en malware pagina's worden getoond. Geadviseerd wordt om de 'detecteer automatisch' instelling uit te schakelen.

De aangeleverde telefoon leverde geen veiligheidsrisico's op, en is dus technisch goed beveiligd.[133] We zien ook dat de gemeente Utrecht veel aandacht heeft besteed aan het beveiligen van de laptops en telefoons. Maar ook bij de werktelefoon speelt het veilig en bewust omgaan met informatieveiligheid een rol: "*Veel collega's hebben apps van cyber offensieve landen en commerciële bedrijven op hun telefoon die – ondanks dat veel mensen*

[133] NFIR (18 juli 2024). *Rapportage pentest. Externe en Interne Infrastructuur (Timeboxed)*.

zich daar niet van bewust zijn – potentieel stiekem meeluisteren."[134] Inmiddels zijn medewerkers er over geïnformeerd dat zij een aantal apps moeten verwijderen van hun werktelefoon. Dat levert soms weerstand op onder medewerkers en raads- en commissieleden.[135]

De goede (technische) beveiliging neemt niet weg dat het werken op afstand risico's met zich mee blijft brengen, omdat het gedrag van de medewerkers de uiteindelijke effectiviteit van de technische maatregelen bepaalt. Betrokkenen zijn zich hier ook van bewust en willen met name goed gedrag bevorderen en stimuleren. Zo wordt er ook nagedacht en afspraken gemaakt over het gebruik van verschillende apps, waarbij het vooral van belang is dat medewerkers weten welke informatie ze op welke manier mogen delen. Verder vraagt met name de toenemende behoefte om in het buitenland te mogen werken nog om een verdere uitwerking.[136]

5.3 WISSELENDE ERVARINGEN MET DE FYSIEKE BEVEILIGING VAN GEMEENTELIJKE GEBOUWEN

Fysieke beveiliging op het Stadskantoor vrijwel ongewijzigd en daarmee ontoereikend om de toegang van onbevoegden te voorkomen, situatie Stadhuis verbeterd
Het is een *mystery guest* gelukt om op vijf verschillende dagen het Stadskantoor te betreden, zonder gebruik te hoeven maken van een toegangspas of de vrijwaring die door de gemeente Utrecht was afgegeven. Ook toen er meer beveiliging aanwezig was ten behoeve van het stembureau voor de Europese verkiezingen, was het mogelijk om het medewerkersdeel te betreden. Een andere *mystery guest* is door een medewerker (geen beveiliger) aangesproken bij het meelopen door de toegangspoorten en is de toegang ontzegd. Ook bij een tweede poging werd hij bij de toegangspoorten aangesproken, ditmaal wel door een beveiliger. Het lukte de tweede *mystery guest* die dag niet om het Stadskantoor binnen te komen.

Bij het Stadhuis is het een *mystery guest* één keer gelukt om het gebouw te betreden zonder gebruik te hoeven maken van een toegangspas of de vrijwaring. Ook toen hier meer beveiliging aanwezig was ten behoeve van het stembureau voor de Europese verkiezingen. Maar een andere poging op het Stadhuis van beide *mystery guests* slaagde niet. In het algemeen blijkt wel dat de beveiligers op het Stadskantoor en Stadhuis niet goed toezicht houden op de toegangspoorten. Betrokkenen geven aan dat er een driejarig programma wordt opgestart om het beveiligingsteam (verder) op te leiden om afwijkend gedrag te herkennen en incidenten te voorkomen. Dat programma zal gefaseerd worden opgebouwd, zodat de beveiligers worden meegenomen in een leercurve. De uiteindelijke trainingsvorm

[134] Rekenkamer Utrecht (2024). *Interview gemeente*.
[135] Rekenkamer Utrecht (2024). *Interview gemeente*.
[136] Gemeente Utrecht (2024). *Interviews gemeente.*

zal uit *red teaming*[137] bestaan waarbij aan het einde van dit programma een breed, integraal scenario wordt doorlopen. Zo kan er zo realistisch mogelijk worden gesimuleerd.[138]

Het bleek ook mogelijk om na sluitingstijd van het publiekstoegankelijke deel van het Stadskantoor in het kantoorgedeelte voor medewerkers diverse opbergkasten open te maken. Deze kasten waren niet afgesloten. In deze kasten bevond zich onder andere een telefoon, een harde schijf en diverse documenten. In theorie was het mogelijk om diverse fysieke hardware items op het Stadskantoor, zoals een laptop of telefoon, te stelen.[139] Dit viel echter buiten scope van de opdracht van de rekenkamer.

Spanningsveld tussen wens tot openheid en de noodzaak van fysieke beveiliging heeft geleid tot nieuwe keuzes

Zowel in de bestuurlijke reactie op de aanbevelingen van het onderzoek van 2021 als in het plan van aanpak wijst het college op het spanningsveld tussen de wens tot openheid en de noodzaak van (informatie)beveiliging.[140] Met een dreiging- en risicoassessment (DRA) is voor het Stadskantoor en het Stadhuis de fysieke beveiliging en de uitvoering daarvan geëvalueerd. Bij het Stadhuis heeft dit geleid tot een aantal concrete maatregelen: de toegangscontrole is aangepast door het gebruik van tourniquets tussen de verschillende zones, is er een bezoekers- en leveranciersbeleid en is er meer aandacht voor veiligheidsbewustwording. Bij het Stadskantoor worden verdere maatregelen gelijktijdig met het 'Werken 3.0' ingevoerd en wordt onderzoek gedaan naar zowel het beleid voor toegangspassen als verdere maatregelen uit de DRA die niet samen met 'Werken 3.0' kunnen worden gerealiseerd.[141] Het gaat om een maatregelenpakket waarmee de Directieraad inmiddels heeft ingestemd.

De Directieraad wil ook graag het open karakter van het Stadhuis en het Stadskantoor behouden. Dat heeft geleid tot het concept van 'open waar het kan, gesloten waar het moet'. Dat betekent dat de beveiligde schil wel wordt versterkt, maar niet dusdanig dat iedere kwaadwillende kan worden tegengehouden. Dat is een geaccepteerd risico waar weliswaar aanvullende maatregelen aan zijn verbonden. Plekken waar intern met gevoelige informatie wordt gewerkt worden aanvullend beschermd door bronmaatregelen, bijvoorbeeld in de vorm van een extra compartimentering (extra ruimte met aanvullend toegangsbeheer en een paslezer in combinatie met een selectieve groep medewerkers met toegang).[142]

Daarnaast zijn de ongeveer 35 beveiligers en centralisten die op het Stadskantoor en Stadhuis werkzaam zijn sinds februari 2023 intern in dienst genomen. Zij werden voorheen

[137] Bij *red teaming* wordt met een realistische (cyber)aanval getest in hoeverre de gemeentelijke organisatie de aanval detecteert en in staat is hier op een goede manier op te reageren.
[138] Rekenkamer Utrecht (2024). *Interview gemeente.*
[139] Rekenkamer Utrecht (18 juli 2024) o.b.v. NFIR. *Rapportage Social Engineering: Mystery Guest, Voice Phishing, USB dropping.*
[140] Gemeente Utrecht (9 juli 2021). Raadsbrief *Plan van aanpak bij het rekenkameronderzoek*.
[141] Gemeente Utrecht (10 oktober 2023). Raadsbrief *Update Rekenkameronderzoek 'Zo sterk als de zwakste schakel'.*
[142] Rekenkamer Utrecht (2024). *Interview gemeente.*

ingehuurd bij een externe partij. Daardoor kan volgens betrokkenen meer op de kwaliteit van de dienstverlening worden gestuurd, waarbij ook informatieveiligheid een integraal onderdeel van het werk vormt.[143]

[143] Rekenkamer Utrecht (2024). *Interview gemeente.*

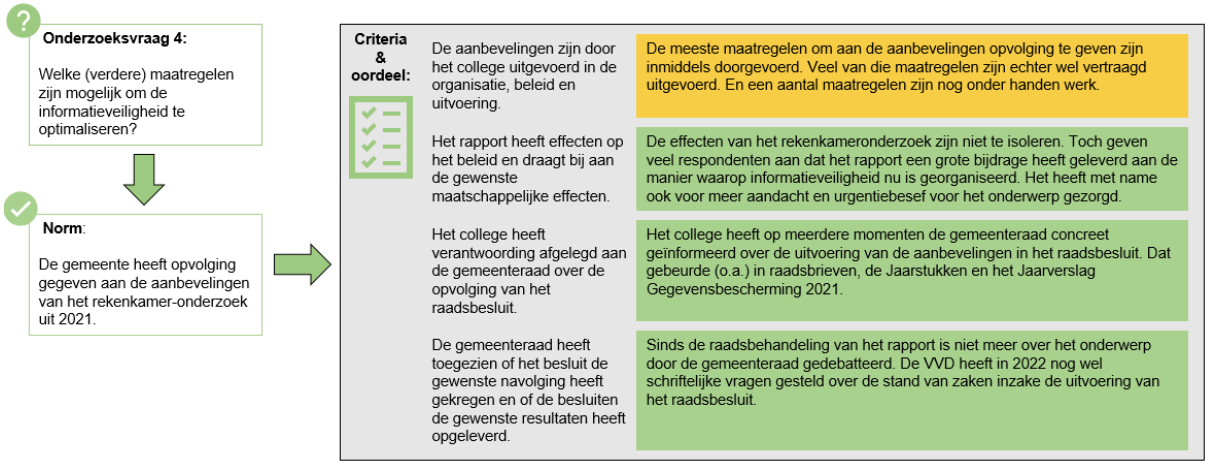
6 OPVOLGING: GROTENDEELS OP ORDE

De beslispunten uit het raadsvoorstel zijn grotendeels uitgevoerd omdat het merendeel van de maatregelen daaruit zijn doorgevoerd. Veel van die maatregelen zijn echter wel vertraagd uitgevoerd. Het college heeft de gemeenteraad de afgelopen jaren goed geïnformeerd over de uitvoering van de aanbevelingen. Het rekenkamerrapport heeft (indirect) de gewenste effecten gehad. Met name doordat er meer aandacht is voor het onderwerp informatieveiligheid en het urgentiebesef om aan de slag te gaan is toegenomen.

In dit hoofdstuk beschrijven we de mate waarin de gemeente opvolging heeft gegeven aan de aanbevelingen van het rekenkameronderzoek uit 2021, hoe zij daarover verantwoording heeft afgelegd aan de gemeenteraad en of de raad op de uitvoering heeft toegezien. Ook beschrijven we of het rapport daadwerkelijk heeft bijgedragen aan beter beleid.

De uitvoering, afgezet tegen de bijbehorende norm, leidt in figuur 6.1 tot onze bevindingen. Hierin leggen we ook direct de relatie tussen de onderzoeksvraag, de norm en bijbehorende criteria.

Figuur 6.1 Norm, criteria en beoordeling "Opvolging"



Toelichting op het normenkader

Om aan de aanbevelingen van het rekenkameronderzoek uit 2021 opvolging te geven moet de gemeente deze hebben doorgevoerd in de organisatie, het beleid en de uitvoering. En het college moet daarover verantwoording afleggen aan de gemeenteraad, zodat de raad erop kan toezien of de aanbeveling juist wordt uitgevoerd en de gewenste effecten heeft. Het is namelijk belangrijk dat het rapport en met name de aanbevelingen van de rekenkamer daadwerkelijk bijdragen aan beter beleid, uitvoering in de praktijk en gewenste maatschappelijke effecten.

6.1 MEESTE MAATREGELEN UITGEVOERD, NA STERK VERTRAAGDE UITVOERING

Op 3 juni 2021 stemde de gemeenteraad unaniem voor het raadsvoorstel met daarin de aanbevelingen uit het rekenkameronderzoek. Een aantal weken later ontving de gemeenteraad op 9 juli 2021 een plan van aanpak waarin het college uiteenzette hoe zij het raadsbesluit over de aanbevelingen wilde uitvoeren.[144] Over dat plan van aanpak oordeelden wij positief, met name omdat de aanbevelingen waren voorzien van concrete maatregelen per onderdeel. We zagen ook dat "(…) *er sinds de uitvoering van ons onderzoek op veel terreinen stappen zijn gezet en voor de korte termijn worden aangekondigd.*"[145] Sinds de vaststelling van het raadsbesluit zijn er ook volgens betrokkenen veel stappen gezet.[146]

Wij zien dat een groot deel van de aangekondigde maatregelen zijn doorgevoerd. Maar de uitvoering heeft wel vaak langer op zich laten wachten dan dat in eerste instantie was aangekondigd. Zo concludeerde concernaudit op basis van een follow-up audit dat in september 2022 70% van de bevindingen nog onderhanden werk was.[147] Verklaringen daarvoor zijn een gebrek aan capaciteit, onvoldoende daadkracht, de cultuur van de organisatie en de grote financiële investeringen die voor een aantal maatregelen nodig zijn. Een voorbeeld van een vertraagde maatregel is het uitvoeren van een penetratietest om te verifiëren dat alle technische kwetsbaarheden daadwerkelijk waren weggenomen (zie box 6.2). Andere vertraagde maatregelen zijn inmiddels nog steeds onder handen werk (zie box 6.3).

Box 6.2 Twee maatregelen die vertraagd zijn doorgevoerd

In oktober 2022 werd aangegeven dat de penetratietest zou worden uitgevoerd na de implementatie van het 'Werken 3.0' in Q4 2022.[148] Een maand eerder ondersteunde ook concernaudit in haar auditrapport het belang van het uitvoeren van de penetratietest. Het heeft echter nog tot april 2024 geduurd voordat de bevindingen uit eerdere testen waren opgevolgd en de validerende eind-penetratietest daadwerkelijk werd uitgevoerd.

Een ander voorbeeld van een maatregel die vertraagd is uitgevoerd, is het vervangen van computers op het Stadskantoor. In het plan van aanpak werd aangegeven dat dit uiterlijk in Q4 2021 zou gebeuren. Een jaar later zou dit uiterlijk in Q4 van 2022 zijn. In een raadsbrief uit oktober 2023 werd aangegeven dat de maatregel inmiddels was uitgevoerd. Wanneer precies werd niet nader gespecificeerd.

[144] Gemeente Utrecht (9 juli 2021). Raadsbrief *Plan van Aanpak bij het rekenkameronderzoek 'Zo sterk als de zwakste schakel'*.
[145] Rekenkamer Utrecht (2 september 2021). Rekenkamerbrief *Plan van aanpak rekenkameronderzoek informatieveiligheid*, p.1.
[146] Rekenkamer Utrecht (2024). *Interview gemeente*.
[147] Concernaudit (16 september 2022). *Rapport Follow-up audit opvolging bevindingen Rekenkamer – Definitief*.
[148] Gemeente Utrecht (2022). *Jaarverslag gegevensbescherming 2021*.

Box 6.3 Sommige vertraagde maatregelen zijn nog steeds onderhanden werk

Over het uitvoeren van *phishing* testen wordt in het plan van aanpak aangegeven dat "(…) *het noodzakelijk is om periodiek te oefenen hoe we moeten omgaan met dit soort situaties.*"[149] In oktober 2023 blijkt uit een raadsbrief dat er sinds het rekenkameronderzoek echter geen *phishing* simulaties meer hebben plaatsgevonden. Er is prioriteit gegeven aan de opzet van de e-learning, zodat medewerkers weten waar zij op moeten letten. *Phishing* simulaties zullen na akkoord in september 2024 in gang worden gezet.[150]

Ook het doorvoeren van fysieke beveiligingsmaatregelen voor het Stadskantoor zijn nog onder handen werk. Naar verwachting zou in Q1 2022 een analyse zijn uitgevoerd om te bepalen welke extra maatregelen genomen moesten worden.[151] De analyse om te bepalen welke maatregelen genomen moesten worden is in maart 2022 opgeleverd. Het daaropvolgende adviesrapport is in september 2022 afgerond.[152] In februari 2023 is akkoord gegeven op het doorvoeren van de gestelde maatregelen die uit de analyse naar voren kwamen. De maatregelen zullen – naar verwachting – in december 2024 deels zijn doorgevoerd.[153] De resterende maatregelen zullen in het tweede kwartaal van 2025 of in het programma Werken 3.0 (lopend in de periode 2024 – 2026) worden geïmplementeerd.

Andere voorbeelden van onderhanden werk maatregelen zijn het opstellen van een gebruikersprotocol voor het veilig werken met informatie en systemen en het invoeren van gegevensbeschermingsambassadeurs. Deze zijn eerder toegelicht in paragraaf 4.1.

6.2 REKENKAMERRAPPORT DROEG BIJ AAN URGENTIE VAN INFORMATIEVEILIGHEID

Het is belangrijk dat het rekenkamerrapport uit 2021 heeft bijgedragen aan beter beleid en de uitvoering daarvan. Betrokkenen geven veelal aan dat er vanuit meerdere perspectieven aan de gegevensbeschermingsopgave is en wordt gewerkt. Het rekenkamerrapport vormt één van die perspectieven.[154] Ontwikkelingen die de afgelopen jaren hebben plaatsgevonden zijn daardoor niet één-op-één toe te schrijven aan het rekenkamerrapport. Het rapport heeft met name indirecte invloed gehad, maar wordt ook als belangrijke verklaring genoemd voor de manier waarop de opgave nu is ingericht.[155] Omdat de gemeente Utrecht goede stappen heeft gezet in het risicogebaseerd werken en gegevens nu beter worden beschermd constateren wij dat het rapport (al dan niet indirect) de gewenste effecten heeft gehad op informatieveiligheid bij de gemeente Utrecht.

[149] Gemeente Utrecht (9 juli 2021). Raadsbrief *Plan van Aanpak bij het rekenkameronderzoek 'Zo sterk als de zwakste schakel'*, p. 5.
[150] Gemeente Utrecht (10 oktober 2023). Raadsbrief *Update Rekenkameronderzoek 'Zo sterk als de zwakste schakel'*.
[151] Gemeente Utrecht (10 oktober 2023). Raadsbrief *Update Rekenkameronderzoek 'Zo sterk als de zwakste schakel'*.
[152] Concernaudit (16 september 2022). *Rapport Follow-up audit opvolging bevindingen Rekenkamer – Definitief*.
[153] Gemeente Utrecht (10 oktober 2023). Raadsbrief *Update Rekenkameronderzoek 'Zo sterk als de zwakste schakel'*.
[154] Rekenkamer Utrecht (2024). *Interview gemeente*.
[155] Rekenkamer Utrecht (2024). *Interview gemeente*.

Betrokkenen benoemen dat het rekenkamerrapport heeft geholpen bij acceptatie van en het creëren van draagvlak voor het onderwerp.[156] Met name bij de directeuren. Zij hebben vaak beperkte kennis van het informatiebeveiliging en de techniek daarachter, waardoor zij niet altijd goed de gevolgen en risico's van het gevoerde beleid kunnen inschatten.[157] Mede dankzij het rapport kon bij hen het bewustzijn worden gecreëerd dat verandering noodzakelijk was. Dat werd door hen goed opgepakt.[158] Het onderwerp heeft meer urgentie en staat beter op de agenda dan voorheen.[159] En intern wordt door de managementteams "(…) *dankbaar gebruikgemaakt van het rapport*"[160] om de adviezen daaruit goed op te volgen.

Het rekenkamerrapport werd ook als signaal gezien voor onderdelen die echt beter moesten, zoals bewustwording. Ten tijde van het vorige rekenkameronderzoek stond bewustwording nog in de kinderschoenen.[161] "*Dat was voorheen geen speerpunt, maar uit het onderzoek kwam naar voren dat daar echt wat aan moest gebeuren. Dat hebben we serieus opgepakt.*"[162] Er is nu dan ook meer aandacht voor (het vergroten van) het bewustzijn van informatieveiligheid bij medewerkers dan voorheen.[163] Al zien we wel dat hier in de praktijk nog beter op ingezet en gestuurd moet worden (zie hoofdstuk 4).

Op de technische kant was de invloed van het rapport er ook, maar minder sterk. Betrokkenen geven aan dat de organisatie zich er vaak al van bewust was dat de technische beveiliging niet helemaal op orde was.[164] Geïnterviewden menen dat kwetsbaarheden waarschijnlijk ook zonder het rapport opgepakt zouden zijn, maar vertelden dat het rapport wel hielp om het belang daarvan extra onder de aandacht te brengen.[165] In ons vorige onderzoek constateerden wij echter dat veel kwetsbaarheden die al jarenlang bekend waren, maar alsmaar niet werden opgepakt.[166] De extra aandacht heeft er volgens betrokkenen toe geleid dat de veiligheid van buitenaf en systemen nu beter is geregeld en dat meer optimalisatie heeft plaatsgevonden. Dat is onder meer terug te zien aan het gebruik van goed beveiligde gemeentelijke laptops, het doorvoeren van fysieke beveiligingsmaatregelen, het hanteren van een beter wachtwoordbeleid en het invoeren van tweestapsverificatie voor het inloggen op de gemeentelijke systemen.[167] Het rapport heeft ook de noodzakelijkheid van

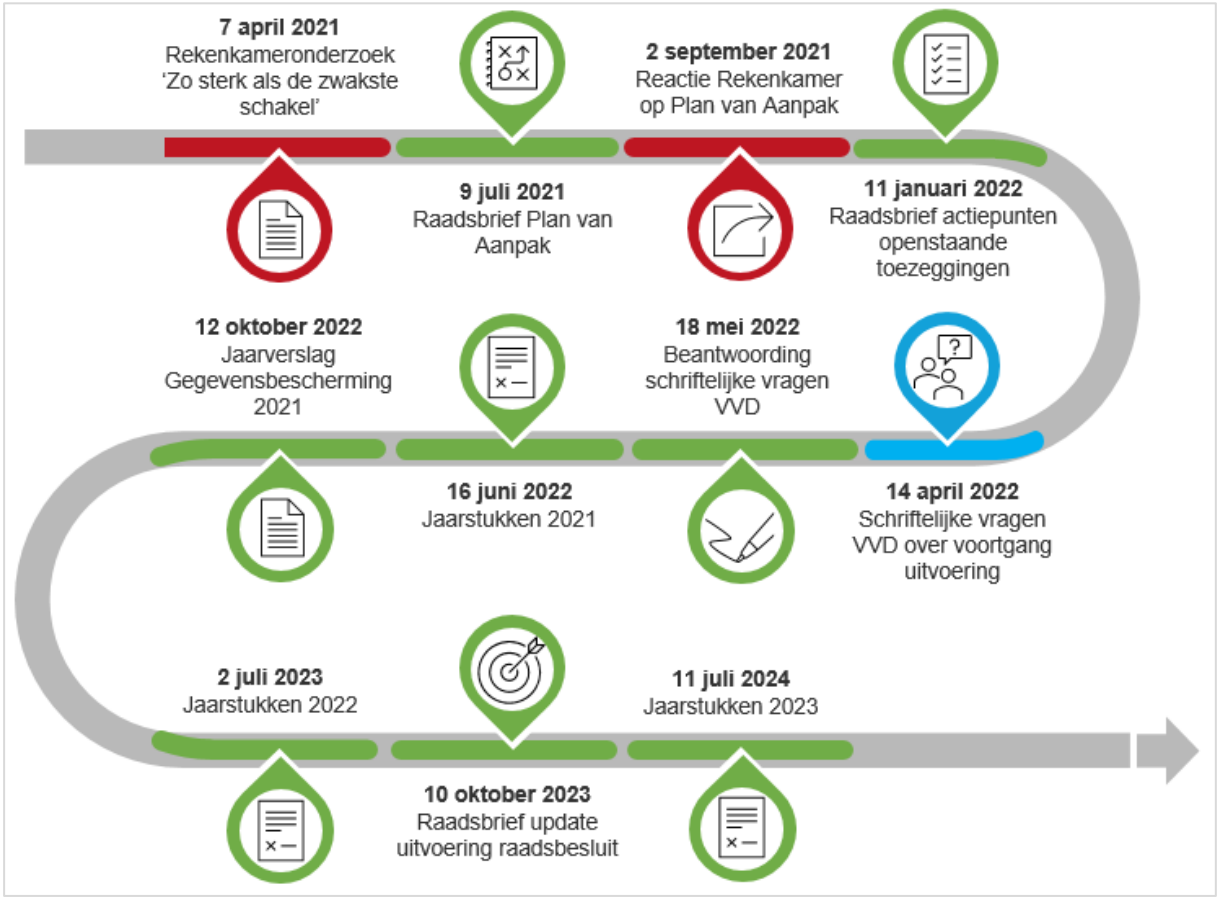
[156] Rekenkamer Utrecht (2024). *Interviews gemeente*.
[157] Rekenkamer Utrecht (2024). *Interview gemeente*.
[158] Rekenkamer Utrecht (2024). *Interview gemeente.*
[159] Rekenkamer Utrecht (2024). *Interview gemeente*.
[160] Rekenkamer Utrecht (2024). *Interview gemeente*.
[161] Rekenkamer Utrecht (2024). *Interview gemeente.*
[162] Rekenkamer Utrecht (2024). *Interview gemeente.*
[163] Rekenkamer Utrecht (2024). *Interviews gemeente*.
[164] Rekenkamer Utrecht (2024). *Interviews gemeente.*
[165] Rekenkamer Utrecht (2024). *Interview gemeente*.
[166] Rekenkamer Utrecht (2021). *Zo sterk als de zwakste schakel. Een onderzoek naar de informatieveiligheid bij de gemeente Utrecht.*
[167] Rekenkamer Utrecht (2024). *Interviews gemeente*.

het uitvoeren van voldoende technische (risico)analyses onder de aandacht gebracht. Daar is de afgelopen jaren veel werk van gemaakt.[168]

6.3 GEMEENTERAAD GOED DOOR COLLEGE GEÏNFORMEERD OVER OPVOLGING RAADSBESLUIT

Wij constateren dat het college de gemeenteraad goed heeft geïnformeerd over de voortgang op het uitvoeren van het raadsbesluit (zie figuur 6.4). Tijdens de behandeling van het rekenkamerrapport deed de wethouder een aantal toezeggingen aan de gemeenteraad. Twee van die toezeggingen kwamen niet in het gemeentelijke plan van aanpak terug. In de rekenkamerbrief van september 2021 waarin wij onze visie op het plan van aanpak gaven wezen wij daarop. Het college heeft daarop in januari 2022 in een raadsbrief aangegeven in welke mate zij aan de gedane toezeggingen invulling zou gaan geven.

Figuur 6.4 De gemeenteraad is door het college de afgelopen jaren goed geïnformeerd over de opvolging van de aanbevelingen



Bron: Rekenkamer Utrecht (2024) op basis van de documenten die in de figuur worden genoemd.

[168] Rekenkamer Utrecht (2024). *Interviews gemeente*.

Vervolgens heeft het college in juni 2022 in de Jaarstukken 2021 de gemeenteraad per aanbeveling beknopt geïnformeerd over de planning en stand van zaken van de uitvoering. Daarna is in oktober 2022 het Jaarverslag Gegevensbescherming 2021 gepubliceerd, waarin de gemeentelijke organisatie verantwoording aflegde aan de gemeenteraad over de ontwikkelingen in 2021 op het gebied van gegevensbescherming.[169] Het jaarverslag bevat per aanbeveling concrete informatie over de reeds uitgevoerde en nog te nemen acties. Dit verslag zou ieder jaar worden gedeeld met de gemeenteraad. Maar sinds het jaarverslag over 2021 is dat niet meer gebeurd.

Daarna is de gemeenteraad aan de hand van de Jaarstukken 2022 opnieuw over de stand van zaken per aanbeveling geïnformeerd in juli 2023. In een uitgebreide raadsbrief uit oktober 2023 is vervolgens een update gegeven over de mate waarin het raadsbesluit op dat moment was opgevolgd. De meest recente informatie met betrekking tot de stand van zaken is terug te vinden in de Jaarstukken 2023 uit juli 2024.

Sinds de raadsbehandeling van het rekenkamerrapport is door de gemeenteraad niet meer over het onderwerp gedebatteerd. In april 2022 heeft de VVD-fractie nog wel schriftelijke vragen aan het college gesteld over het gebruik van ethische hackers. Daarin wordt het college onder andere gevraagd naar de voortgang op de acties die zijn en worden ondernomen naar aanleiding van het rekenkamerrapport. Maar er worden ook vragen gesteld die breder betrekking hebben op het onderwerp informatieveiligheid. De vragen zijn in mei 2022 door het college beantwoord.

[169] Gemeente Utrecht (2022). *Jaarverslag Gegevensbescherming 2021*, p. 3.

BIJLAGE 1 AFKORTINGEN

Afkorting	Betekenis
AVG	Algemene Verordening Gegevensbescherming
BIA	Business Impact Analyse
BIO	Baseline Informatiebeveiliging Overheid
BSN	Bedrijfsvoerings- en Strategienetwerk
B&W	Burgemeester en wethouders
CC	Concerncontrol
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPO	Chief Privacy Officer
CZ	Culturele Zaken
DISO	Decentrale Informatie en Security Officer
DPIA	Data Protection Impact Assessment
DRA	Dreiging- en Risicoassessment
FG	Functionaris Gegevensbescherming
FIJ	Financiën, Inkoop en Juridische Zaken
GBMS	Gegevensbeschermingsmanagementsysteem
HR	Human Resources
HRM	Human Resource Management
IB	Interne bedrijven
IBD	Informatiebeveiligingsdienst
ICT	Informatie- en communicatietechnologie
IPM	Informatie- en procesmanagement / Informatie- en procesmanager
IRM	Integraal Resultaatverantwoordelijk Manager
ISMS	Information Security Management System
IT	Informatietechnologie
LLMNR	Link-Local Multicast Name Resolution
MCN	Marketing- en Communicatienetwerk
MG	Mystery guest
MO	Maatschappelijke Ontwikkeling

M&O	Mens en Organisatie
NCSC	Nationaal Cyber Security Centrum
NIS2	Network and Information Security Directive
ORA	Operationele risicoanalyse
O&A	Onderzoek en Advies
PBZ	Publiekszaken
PDCA	Plan-Do-Check-Act
PMB	Projectmanagementbureau
PRA	Privacy risicoassessment
RO	Raadsorganen
SB	Stadsbedrijven
SPA-BO	Strategie & Public Affairs en Bestuursondersteuning
S&S	Safety & Security
TRA	Tactische risicoanalyse
VGU	Vastgoedorganisatie Utrecht
VG	Volksgezondheid
VLG	Veiligheid
VNG	Vereniging van Nederlandse Gemeenten
VTH	Vergunningen, Toezicht en Handhaving
WenI	Werk en Inkomen

BIJLAGE 2 ONDERZOEKSVERANTWOORDING

WERKWIJZE

De rekenkamer heeft de volgende onderzoeksactiviteiten uitgevoerd:

- Documentstudie: We hebben de relevante beleidsdocumenten, documenten uit de begrotingscyclus en andere raadsinformatie over informatieveiligheid bestudeerd. Hiermee hebben we in kaart gebracht welk beleid de gemeente Utrecht voert. Voor het inzicht in de risico's die zijn geïdentificeerd en de genomen beheersmaatregelen hebben wij onder andere de gegevensbescherming- en risicorapportages van de gemeente ingezien.
- Interviews: In de maanden april tot en met juli 2024 zijn interviews gehouden met de medewerkers van de gemeente die nauw betrokken zijn bij informatieveiligheid. In deze gesprekken lag de nadruk op hoe informatieveiligheid zich de afgelopen jaren op drie aspecten heeft ontwikkeld: organisatie, mens en techniek. Wij zijn in de gesprekken ook nader ingegaan op hoe het eerdere rekenkamerrapport heeft bijgedragen aan deze ontwikkelingen en hoe met incidenten (zoals datalekken) wordt omgegaan.
- Testen: De rekenkamer heeft NFIR B.V. opdracht verleend voor het uitvoeren van testen op het oneigenlijk toegang krijgen tot informatie bij de gemeente. Er zijn drie soorten testen uitgevoerd:
    1. Social engineering test: Dit onderdeel bestaat uit een *voice phishing* test (het telefonisch benaderen van gemeentelijke medewerkers om inloggegevens te bemachtigen), het verspreiden van USB-sticks die bij gebruik malware zouden kunnen installeren (baiting) en inlooptesten op het Stadskantoor en Stadhuis om ongeautoriseerd toegang te krijgen tot een kantoorruimte. De *voice phishing* verving in dit onderzoek de *mail-phishing* uit het vorige rekenkameronderzoek. Daarnaast is een laptop van de gemeente aan een analyse onderworpen om na te gaan of deze voldoende beschermd is tegen aanvallen in onveilige netwerken en tegen diefstal en verlies.
    2. Penetratietesten (pen-testen): Dit onderdeel is zowel intern als extern uitgevoerd. Er is zowel vanaf een gemeentelijke locatie als via het internet geprobeerd om oneigenlijk toegang te krijgen tot informatie.

       De risico's worden aan de hand van de formule *waarschijnlijkheid x impact* van een niveau voorzien die de ernst van de kwetsbaarheid zichtbaar maakt. Figuur A laat zien dat er vijf niveaus zijn: informatief, laag, gemiddeld, hoog en kritiek.

Figuur A Indeling risiconiveaus op vijf niveaus

Impact	**Waarschijnlijkheid**		
	Laag	**Gemiddeld**	**Hoog**
Laag	Informatief	Laag	Gemiddeld
Gemiddeld	Laag	Gemiddeld	Hoog
Hoog	Gemiddeld	Hoog	Kritiek

Een kritiek risico heeft een hoge waarschijnlijkheid dat deze door een kwaadwillende wordt uitgebuit en een hoge impact (schade) voor de gemeentelijke organisatie.

3. Review: De gemeente heeft in 2024 accountantsorganisatie BDO de opdracht gegeven om een hertest uit te voeren op de interne en externe infrastructuur. Op deze hertest heeft de rekenkamer in het kader van dit opvolgingsonderzoek een review laten uitvoeren.

- Analyse en rapportage: Het onderzoeksmateriaal uit de voorgaande stappen is in samenhang geanalyseerd en in verband gebracht met de vooraf vastgestelde normen. De normenbeoordelingen zijn vervolgens vastgelegd in de conceptnota van bevindingen en aan de ambtelijke organisatie voorgelegd voor feitelijk wederhoor. Na de verwerking van de ambtelijke reactie hebben we een bestuurlijk rapport opgesteld met conclusies en aanbevelingen. Het geheel is daarna voorgelegd aan het college van burgemeester en wethouders voor bestuurlijk wederhoor. Na het ontvangen van de bestuurlijke reactie hebben we het definitieve rapport opgemaakt met een nawoord van de rekenkamer.

GERAADPLEEGDE PERSONEN

Gemeente Utrecht:

- Directeur Bedrijfsvoering
- Directeur Informatie en Procesmanagement (IPM) / hoofd CIO office
- Plaatsvervangend hoofd CIO office
- Integraal Resultaatverantwoordelijk Managers (3)
- Informatie en Procesmanagers (IPM’ers; 2)
- Chief Information and Security Officer (CISO)
- Chief Privacy Officer (CPO)
- Decentrale Information and Security Officer (DISO)
- Coördinator bewustwording
- Hoofd DomstadIT

- Plaatsvervangend hoofd DomstadIT
- Teamleider DomstadIT
- Teamleider Safety & Security
- Adviseur Safety & Security

GERAADPLEEGDE DOCUMENTEN

Gemeentelijke documenten over informatieveiligheid:

- Gemeente Utrecht (1 juli 2019). *Beleid voor gegevensbescherming gemeente Utrecht 2019-2022 "Bescherming van het digitale DNA van de stad"*.
- Gemeente Utrecht (9 juli 2021). Raadsbrief *Plan van Aanpak bij het rekenkameronderzoek 'Zo sterk als de zwakste schakel'*.
- Gemeente Utrecht (11 januari 2022). Raadsbrief *Actiepunten rekenkameronderzoek*.
- Gemeente Utrecht (7 oktober 2022). Raadsbrief *Beveiligingsmedewerkers gemeente Utrecht*.
- Gemeente Utrecht (12 oktober 2022). *Jaarverslag Gegevensbescherming 2021*.
- Gemeente Utrecht (16 augustus 2023). *Gegevensbescherming in Utrecht: verantwoord en transparant. Intern strategisch beleidskader voor gegevensbescherming van Utrecht*.
- Gemeente Utrecht (10 oktober 2023). Raadsbrief *Update Rekenkameronderzoek 'Zo sterk als de zwakste schakel'*.

Gemeentelijke planning en controldocumenten:

- Gemeente Utrecht (16 juli 2020). *Eerste Bestuursrapportage 2020*.
- Gemeente Utrecht (8 juli 2021). *Voorjaarsnota 2021 en Eerste Bestuursrapportage 2021*.
- Gemeente Utrecht (16 juni 2022). *Jaarstukken 2021*.
- Gemeente Utrecht (7 juli 2022). *Voorjaarsnota 2022 en Eerste Bestuursrapportage 2022*.
- Gemeente Utrecht (10 november 2022). *Programmabegroting 2023*.
- Gemeente Utrecht (2 juli 2023). *Jaarstukken 2022*.
- Gemeente Utrecht (11 juli 2024). *Jaarstukken 2023*.
- Gemeente Utrecht (11 juli 2024). *Voorjaarsnota en Eerste Bestuursrapportage 2024*.

Interne gemeentelijke documenten:

- Monitor gegevensbescherming van de gemeente Utrecht, met gegevens over de perioden 2022 tertaal 3 t/m 2024 tertaal 1.
- Verslagen van tertaalgesprekken met OOV, PBZ, VTH en BSN.
- Maandelijkse rapportage gegevensbescherming van DomstadIT, versies januari 2024 t/m juni 2024.
- Jaarplannen Gegevensbescherming en Informatiebeheer 2024 van OOV, PBZ, VTH en BSN.

- Gemeente Utrecht (21 juni 2022). *Bewustwording en communicatie gegevensbescherming. Hoe we bewust gedrag kunnen stimuleren door transparant te communiceren*.
- Concernaudit (16 september 2022). *Rapport Follow-up audit opvolging bevindingen Rekenkamer – Definitief*.
- Concernaudit (8 augustus 2024). *Rapport Cyberweerbaarheid*.
- Gemeente Utrecht (6 januari 2023). *Dashboard deelname e-learning concern*.
- Gemeente Utrecht (30 maart 2023). *Veilig werken onboarding*.
- Gemeente Utrecht (6 juni 2023). *Strategische standaard voor Business Continuity Management*.
- Gemeente Utrecht (6 juni 2023). *Strategische standaard voor Cryptografie*.
- Gemeente Utrecht (6 juni 2023). *Strategische standaard voor Identificatie, Authenticatie en Autorisatie*.
- Gemeente Utrecht (6 juni 2023). *Strategische standaard voor Logging en Monitoring*.
- Gemeente Utrecht (6 juni 2023). *Strategische standaard voor naleving GBMS*.
- Gemeente Utrecht (4 juli 2023). Interne memo *Herijking en overdracht strategische risico's gegevensbescherming*.
- Gemeente Utrecht (4 juli 2023). Rapportage *Herijking en overdracht strategische risico's gegevensbescherming*.
- Gemeente Utrecht (13 september 2023). *Architectuurboard gemeente Utrecht*.
- Gemeente Utrecht (4 december 2023). *Herinrichting strategisch risicomanagement*.
- Gemeente Utrecht (7 december 2023). *Dashboard deelname e-learning concern*.
- Gemeente Utrecht (januari 2024). *Brede rapportage bedrijfsvoering*.
- Gemeente Utrecht (22 januari 2024). *Handboek Risicomanagement Gegevensbescherming*.
- Gemeente Utrecht (28 februari 2024). *Protocol Automatiseringsmiddelen 2024*.
- Gemeente Utrecht (19 maart 2024). *Gegevensbescherming Managemensysteem*.
- BDO (25 maart 2024). *Pentest report. New perspectives for gemeente Utrecht*.
- BDO (23 april 2024). *Pentest report – Retest VDI, Fat client and Laptop Gemeente Utrecht*.
- Gemeente Utrecht (25 april 2024). Interne memo. *Toelichting Retest op de VDI, fat client en laptop*.
- Gemeente Utrecht (30 april 2024). *Dashboard deelname e-learning concern*.

Schriftelijke vragen, moties en amendementen:

- VVD Utrecht (14 april 2022). SV 2022 nr. 78 *Inzet ethische hackers bij gemeente Utrecht.*

Andere bronnen:

- Rekenkamer Utrecht (23 juni 2020). *Opvolgingsonderzoek rekenkamerrapporten 2014-2018. Inzicht in de doorwerking van rekenkameronderzoek en de opvolging van raadsbesluiten*.

- Rekenkamer Utrecht (7 april 2021). *Zo sterk als de zwakste schakel. Een onderzoek naar de informatieveiligheid bij de gemeente Utrecht*.
- Rekenkamer Utrecht (2 september 2021). Rekenkamerbrief *Plan van aanpak rekenkameronderzoek informatieveiligheid*.
- NFIR (18 juli 2024). *Hertest rapportage: RKC en VDI/laptop*.
- NFIR (18 juli 2024). *Rapportage pentest. Extern en Interne Infrastructuur (Timeboxed)*.
- NFIR (18 juli 2024). *Social Engineering: Mystery Guest, Voice Phishing, USB dropping*.

Websites:
- Digitale Overheid (18 januari 2022). *Baseline Informatiebeveiliging Overheid*. Geraadpleegd via: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cybersecurity/bio-en-ensia/baseline-informatiebeveiliging-overheid/
- Digitale Overheid (28 mei 2024). *NIS2-richtlijn*. Geraadpleegd via: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nis2-richtlijn/

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.