Onderzoeksrapport

ZO STERK ALS DE ZWAKSTE SCHAKEL

EEN ONDERZOEK NAAR DE INFORMATIEVEILIGHEID BIJ DE GEMEENTE UTRECHT

REKEN KAMER UTRECHT

ZO STERK ALS DE ZWAKSTE SCHAKEL

EEN ONDERZOEK NAAR DE INFORMATIEVEILIGHEID BIJ DE GEMEENTE UTRECHT

7 april 2021
Eindrapport

REKENKAMER UTRECHT

LEDEN

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

MEDEWERKERS ONDERZOEK

- Johan Snoei
- Pauline de Jong
- Naomi Meys

CONTACTGEGEVENS

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

INHOUDSOPGAVE

DEEL II ONDERZOEKSRAPPORT

1 INLEIDING

1.1 AANLEIDING

Informatieveiligheid is een onderwerp dat met de toenemende digitalisering steeds belangrijker wordt. Gemeenten verwerken grote hoeveelheden gegevens in een veelvoud aan systemen en programma's. Veel van deze gegevens betreffen (bijzondere) persoonsgegevens of andere belangrijke gegevens die goed beschermd moeten zijn. Het gaat dan bijvoorbeeld om persoonsgegevens in de Basisregistratie Personen (BRP) en in het sociaal domein waarbij bijzondere persoonsgegevens worden geadministreerd, maar ook gegevens over bijvoorbeeld financiën, ruimtelijke projecten en de veiligheid in de stad. Zonder goede informatiebeveiliging liggen cybercriminaliteit, fraude, oplichting en ondermijning op de loer.

De gemeenteraad heeft het onderwerp informatieveiligheid verschillende keren als onderzoeksthema aangedragen bij de Rekenkamer Utrecht. In de bijeenkomst van de rekenkamer met de gemeenteraad in november 2019 bleek dat er bij de raadsleden vragen leven rondom informatieveiligheid, maar ook over de visie en aanpak van de gemeente Utrecht en de bewustwording van de risico's binnen het gemeentelijk apparaat. Daarbij was de vraag wat de gemeente Utrecht doet ten opzichte van de Rijksoverheid en andere grote steden. Voor de rekenkamer gaf dit voldoende aanleiding om met dit onderwerp aan de slag te gaan. In voorliggend onderzoeksrapport rapporteren wij onze bevindingen.

1.2. DOEL EN ONDERZOEKSVRAGEN

Het doel van de rekenkamer met dit onderzoek is om de gemeenteraad inzicht te geven in de manier waarop de gemeente Utrecht invulling geeft aan de informatieveiligheid en te beoordelen of de informatieveiligheid voldoende is gewaarborgd. We kijken daarbij naar drie aspecten: (1) organisatie en proces, (2) mens en (3) techniek.

De centrale vraag van het onderzoek is:

> Is de informatieveiligheid bij de gemeente Utrecht voldoende gewaarborgd?

Deze centrale vraag is uitgewerkt in de volgende onderzoeksvragen:

1. (Organisatie/proces:) Wat doet de gemeente Utrecht op het gebied van informatieveiligheid?
   a. Welk beleid voert de gemeente op informatieveiligheid?

b. Welke risico's en maatregelen heeft de gemeente benoemd?
c. In hoeverre zijn de maatregelen geïmplementeerd?

2. (Mens:) Op welke manier zet de gemeente in op het bewust omgaan met informatie? Hoe gaan de medewerkers van de gemeente in de praktijk om met informatieveiligheid?

3. (Techniek:) Zijn gegevens bij de gemeente voldoende beschermd tegen de toegang door onbevoegden? Zo niet, wat zijn daarvan de gevolgen voor burgers en ondernemers? Wat zijn de risico's en kwetsbaarheden?

Bij de beantwoording van de onderzoeksvragen 1, 2 en 3 hebben wij een normenkader gehanteerd. Per hoofdstuk zijn de normen die aan de orde komen in de inleiding vermeld met daarbij een beoordeling naar de mate waarin eraan wordt voldaan (rood, oranje of groen) en een verwijzing naar de bevinding(en) waarop dit oordeel is gebaseerd.

1.3 WERKWIJZE EN AFBAKENING ONDERZOEK

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 wij in kaart gebracht welk beleid de gemeente Utrecht voert. Voor het inzicht in de risico's die zijn geïdentificeerd en de beheersmaatregelen hebben wij onder andere de risicorapportages van de gemeente ingezien. De uitkomsten van beveiligingstesten, zelfassessments en audits van de gemeente zijn met name gebruikt ter voorbereiding op de testen die de rekenkamer door een extern bureau heeft laten uitvoeren. Voor het overzicht van de kerndocumenten waarop de bevindingen van de rekenkamer zijn gebaseerd, verwijzen wij naar bijlage 2.
- Interviews: In de maanden oktober tot en met december 2020 zijn interviews gehouden met de medewerkers van de gemeente die nauw betrokken zijn bij informatieveiligheid. Bij deze gesprekken gingen wij in op het gevoerde beleid en de processen, een globaal inzicht in de menskracht en het geld dat hiervoor beschikbaar is, de manier waarop bewustwording onder medewerkers onderdeel van beleid en uitvoering uitmaakt, en de mogelijke maatregelen die zij zien voor verdere optimalisatie van de informatieveiligheid. Voor een overzicht van de personen die wij gesproken hebben, verwijzen wij naar bijlage 2.
- Testen: De rekenkamer heeft Hoffmann B.V. (hierna genoemd: het externe bureau) opdracht verleend voor het uitvoeren van testen op het oneigenlijk toegang krijgen tot informatie bij de gemeente. Er zijn twee soorten testen uitgevoerd:

    - Social engineering test: Dit onderdeel bestaat uit een mail-phishing test (verzoek per e-mail om informatie te delen), het verspreiden van USB-sticks die bij gebruik malware zouden kunnen installeren (baiting), en inlooptesten op het Stadskantoor en het Stadhuis om ongeautoriseerd toegang te krijgen tot een kantoorruimte. 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.
    - Penetratietesten (pen-testen): Dit onderdeel is zowel intern als extern uitgevoerd. Er is zowel vanaf een gemeentelijke locatie (werkruimte) als via internet geprobeerd oneigenlijk toegang te krijgen tot informatie.
- Analyse en rapportage: Het onderzoeksmateriaal uit de voorgaande stappen is in samenhang geanalyseerd en opgenomen in voorliggend rapport.

In het onderzoeksplan was ook een enquête onder medewerkers voorzien om na te gaan hoe zij informatieveiligheid in de praktijk ervaren en hoe zij hier zelf invulling aan geven om dit voldoende te kunnen waarborgen. Bij de verkenning van de uitvoeringsmogelijkheden bleek dat een combinatie met verschillende andere enquêtes binnen de gemeentelijke organisatie niet tijdig gerealiseerd kon worden. Dit heeft ons ertoe gebracht af te zien van een enquête en om op dit punt de documentstudie, de interviews met medewerkers, en de uitkomsten van de social engineering test van het externe bureau als basis te nemen voor de beoordeling van dit onderdeel.

Afbakening

We hebben verschillende keuzes gemaakt om het onderzoek duidelijk af te kunnen bakenen. Deze noemen we hieronder puntsgewijs:

- Onderdelen: Het onderzoek richt zich op informatieveiligheid. We hebben gekozen voor de focus op de onderdelen organisatie/proces, mens en techniek, waarbij de nadruk ligt op mens en techniek. Wat de gemeente doet als het onverhoopt toch misgaat – bijvoorbeeld bij een datalek, hackaanval of storing – hebben we niet meegenomen.
- Organisatie en proces: Bij het onderdeel organisatie/proces kijken we met name naar wat er wordt gedaan op het gebied van informatieveiligheid. Het gaat erom een beeld te geven op hoofdlijnen. We hebben gebruik gemaakt van de risicoanalyses en audits die al aanwezig waren en van de maatregelen die de gemeente naar aanleiding daarvan heeft genomen. Hierbij zijn ook de activiteiten die de gemeente onderneemt rondom de BIO (Baseline Informatiebeveiliging overheid) en ISO (Internationale Organisatie voor Standaardisatie) in de analyse meegenomen. Deze activiteiten hebben een plaats gekregen in de roadmap implementatie gegevensbescherming.
- Mens: Bij het onderdeel mens bekijken we de inzet van de gemeente om de medewerkers bewust te laten omgaan met informatie. We hebben in kaart gebracht welke campagnes er zijn geweest en wanneer, hoe medewerkers worden geïnstrueerd en opgeleid om op een goede manier met informatie om te gaan, en hoe gezorgd wordt

voor een veilige werkomgeving. We bekeken op hoofdlijnen de inhoud van de activiteiten, maar hebben deze niet op detailniveau en ook niet onderwijskundig beoordeeld.

- Techniek: Een beschrijving van de uitgevoerde testen is beschreven bij de werkwijze van het onderzoek. Nadere toelichting volgt in hoofdstuk 4.

1.4 LEESWIJZER

Om inzicht te krijgen in de belangrijkste bevindingen van het onderzoek volstaat de eerste paragraaf van de verschillende hoofdstukken. Voor een nadere toelichting op deze bevindingen kan kennisgenomen worden van de uitwerking in de tweede paragrafen.

In hoofdstuk 2 beschrijven we wat de gemeente Utrecht doet op het gebied van informatieveiligheid (vraag 1). In hoofdstuk 3 gaan we in op de manier waarop de gemeente Utrecht inzet op het bewust omgaan met informatie en hoe de medewerkers van de gemeente daar in de praktijk mee omgaan (vraag 2). In hoofdstuk 4 presenteren we de resultaten van verschillende externe en interne penetratietesten die zijn uitgevoerd om vast te kunnen stellen of gegevens bij de gemeente voldoende beschermd zijn (vraag 3).

Het geheel heeft twee bijlagen: de lijst met gebruikte afkortingen (1) en de lijst met geraadpleegde personen en documenten (2). De rapporten met de (technische) informatie over de testen die door het externe bureau zijn uitgevoerd zijn separaat ter beschikking gesteld aan de gemeente Utrecht.

2 ORGANISATIE EN PROCES: HOE DE GEMEENTE UTRECHT INFORMATIE-VEILIGHEID INHOUD GEEFT

In dit hoofdstuk beschrijven we wat de gemeente Utrecht doet op het gebied van informatieveiligheid. Daarmee beantwoorden we de eerste onderzoeksvraag: Wat doet de gemeente Utrecht op het gebied van informatieveiligheid? (a) Welk beleid voert de gemeente op informatieveiligheid? (b) Welke risico's en maatregelen heeft de gemeente benoemd? (c) In hoeverre zijn de maatregelen geïmplementeerd?

In paragraaf 2.1 geven we de belangrijkste bevindingen weer. Deze bevindingen lichten we toe in paragraaf 2.2. Aan de hand van de bevindingen beoordelen we in tabel 2.1 de bijbehorende norm.

Tabel 2.1 Normen en criteria thema 'organisatie en proces'

Norm	Criteria	Beoordeling
De gemeente werkt risicogestuurd.	De gemeente heeft de risico's in beeld.	Zie bevinding 1 van § 2.1
	De gemeente neemt maatregelen om de risico's te laten afnemen.	Zie bevinding 2 van § 2.1

2.1 BELANGRIJKSTE BEVINDINGEN

1. De gemeente Utrecht heeft in 2019 het nieuwe Beleid voor gegevensbescherming 2019-2022 vastgesteld. Het uitgangspunt van dit beleid is risicogestuurd werken. Aan het risicogestuurd werken wordt echter nog onvoldoende invulling gegeven. De gemeente werkt sinds 2019 met een strategisch risico-overzicht. Maar van de benodigde 21 tactische risicoanalyses zijn er slechts 6 gereed. In het kader van de privacy zijn ruim 150 DPIA's afgerond, maar de overige operationele risicoanalyses voor informatieveiligheid zijn – met uitzondering van 6 operationele risicoanalyses als pilot bij Stadsbedrijven – nog niet uitgevoerd. Omdat risicoanalyses en Data Protection Impact Assessments (DPIA's) cruciaal zijn om risicogestuurd te werken, is dit nog niet volledig mogelijk.

2. Bij de implementatie van het nieuwe beleid voor de gegevensbescherming heeft de gemeente Utrecht ook een roadmap opgesteld die jaarlijks wordt herijkt en geactualiseerd. Deze bevat onderwerpen waarmee de gemeente aan de slag gaat en de mijlpalen die daarbij behaald moeten worden. De uitvoering van het

informatiebeveiligingsbeleid loopt op cruciale onderdelen achter op de oorspronkelijke planning. Met extra geld en mensen moet de achterstand worden ingelopen, maar daarvoor zijn ook daadkracht en urgentie bij het management en de proceseigenaren, en de ruimte die van uitvoerende medewerkers vereist is naast hun reguliere werkzaamheden. De gemeente heeft verschillende algemene maatregelen genomen om de risico's te laten afnemen. Zo is de governance sinds 2018 verstevigd. Er zijn een stuurgroep, vakgroep, regiegroep en taskforce ingesteld die op verschillende niveaus de voortgang van risico's en maatregelen moeten bewaken. Met extra middelen is sinds eind 2020 de capaciteit voor Decentrale Informatie en Security Officers (DISO's) uitgebreid en is voor een initiële periode van zes maanden een projectleider bewustwording aangesteld. Ook zijn sinds 2018 de risico's op het gebied van informatieveiligheid in kaart gebracht en geprioriteerd. Van de in totaal 60 risico's die in 2020 in de ICT zijn geïdentificeerd, staan er januari 2021 nog 24 (40%) open.

2.2 TOELICHTING OP DE BEVINDINGEN

2.2.1 BELEID EN RISICOGESTUURD WERKEN

De gemeente Utrecht heeft in 2019 het nieuwe Beleid voor gegevensbescherming 2019-2022 vastgesteld. Het uitgangspunt van dit beleid is risicogestuurd werken.

Gemeenten zijn wettelijk verplicht om een actueel beleid voor gegevensbescherming te hebben (zie tekstkader). In 2019 heeft de gemeente Utrecht het *Beleid voor gegevensbescherming 2019-2022* vastgesteld. De missie van de gemeente voor gegevensbescherming staat in het beleid als volgt beschreven: "*Wij zorgen ervoor dat burgers en ondernemers gegevens aan de gemeente toe durven te vertrouwen omdat de gemeente deze gegevens aantoonbaar goed beschermt. Burgers en ondernemers weten hoe deze bescherming is ingericht, over welke gegevens wij beschikken en wat wij ermee doen*." (p.3)

Baseline Informatiebeveiliging Overheid

Sinds 1 januari 2020 is voor alle Nederlandse overheden de *Baseline Informatiebeveiliging Overheid* (BIO) van kracht. De BIO verving de verschillende baselines informatieveiligheid voor de gemeenten, het Rijk, waterschappen en de provincies voor één gezamenlijk normenkader voor informatieveiligheid. In de BIO staan onder meer beschreven waar het beleid aan moet voldoen en wat georganiseerd moet zijn in de interne organisatie. Deze verplichting komt, naast de BIO, voort uit de *Algemene Verordening Gegevensbescherming* (AVG) en het landelijk verantwoordingsstelsel over informatiebeveiliging.

Een belangrijke wijziging in het nieuwe beleid is dat er meer risicogestuurd gewerkt moet gaan worden om zo de belangrijkste risicogebieden eerst aan te kunnen pakken.[1] De gemeente Utrecht heeft voor het risicogestuurd werken gekozen, omdat er veel ontwikkelingen zijn op het gebied van digitalisering en er maar een bepaalde capaciteit voor informatieveiligheid beschikbaar is. Er moeten daarom keuzes gemaakt worden in de processen die eerst opgepakt worden en welke nog even kunnen wachten.[2] Op basis van de risico's worden ook keuzes gemaakt voor de inzet van mensen (capaciteit), bijvoorbeeld als het gaat om de Decentrale Informatie en Security Officers (DISO's). Er is nu, in tegenstelling tot het verleden, schaarsere DISO-capaciteit beschikbaar op processen die minder risicovol zijn.

De gemeente Utrecht hanteert dertien basisprincipes voor het veilig omgaan met gegevens die zijn vastgelegd in het *Beleid voor gegevensbescherming 2019-2022*. Als het gaat om het treffen van maatregelen is principe 11 van belang: "*Maatregelen moeten kwalitatief en kwantitatief in balans zijn met de te beschermen waarden. Er moeten zakelijke argumenten zijn om beveiligingsmaatregelen te treffen, en omgekeerd, als er geen argumenten zijn, mogen er geen maatregelen getroffen worden. Utrecht gebruikt risicoanalyses als methode om onderzoek te doen naar de noodzaak van maatregelen.*" (p. 8)

Aan het risicogestuurd werken wordt top down invulling gegeven. De gemeente werkt sinds 2019 met een strategisch risico-overzicht. Maar van de benodigde 21 tactische risicoanalyses zijn er slechts 6 gereed. In het kader van de privacy zijn ruim 150 DPIA's afgerond, maar de overige operationele risicoanalyses voor informatieveiligheid zijn – met uitzondering van 6 operationele risicoanalyses als pilot bij Stadsbedrijven – nog niet uitgevoerd. Omdat risicoanalyses en Data Protection Impact Assessments (DPIA's) cruciaal zijn om risicogestuurd te werken, is dit nog niet volledig mogelijk.

Sinds 2018 heeft de gemeente Utrecht een strategisch risico-overzicht. Op basis hiervan worden de inspanningen op het gebied van gegevensbescherming aangestuurd. De risico- en beheersingsmatrix bevat op 1 december 2020 zes hoge (bruto) risico's:

- Access & Identity management: het risico dat onbevoegden toegang krijgen tot applicaties met gevoelige informatie,
- Derdepartij risico's: het risico dat de bescherming en beveiliging van gegevens die door derde partijen worden verwerkt niet is geborgd,
- Awareness: het risico dat medewerkers zich onvoldoende bewust zijn van het belang van gegevensbescherming waardoor zij onbedoeld datalekken of beveiligingsincidenten creëren,
- Veilige gegevensuitwisseling: het risico dat de vertrouwelijkheid van gevoelige gegevens gedurende uitwisseling met andere partijen wordt geschonden,

[1] Gemeente Utrecht (5 juli 2019). Raadsbrief *Beleid voor gegevensbescherming 2019 – 2022*.
[2] Rekenkamer Utrecht. *Interview gemeente Utrecht.*

- Beveiligingslek zaaksysteem: medewerkers met toegang tot het zaaksysteem kunnen contactmomenten inzien die in voorkomende gevallen vertrouwelijke informatie en bijlagen kunnen bevatten,
- Security Domstad-IT: overzicht van beveiligingsissues en bijbehorende risico's in de ICT.

Per onderwerp zijn een risicoeigenaar, een strategie en beheersmaatregel(en) opgenomen, en wordt vervolgens een beoordeling gegeven van het risico dat na de maatregelen blijft bestaan (netto risico/ restrisico). Van de zes hoge risico's geldt dat in drie gevallen ook het restrisico hoog blijft.

De rekenkamer constateert dat ten tijde van het onderzoek een groot deel van de risicoanalyses, privacy risicoassessments en Data Protection Impact Assessments (DPIA's) nog moet worden uitgevoerd (zie tabel 2.2). Van de 21 organisatieonderdelen hebben slechts 6 organisatieonderdelen de tactische risicoanalyse afgerond. Op het gebied van privacybescherming zijn 112 DPIA's uitgevoerd, waarbij de gemeente aangeeft dat hiermee gestart is gezien het belang van privacy binnen de gemeente. Op het gebied van operationele risicoanalyses informatiebeveiliging geldt dat er als pilot zes analyses zijn uitgevoerd bij Stadsbedrijven. De overige operationele risicoanalyses zijn nog niet beschikbaar.

Tabel 2.2 Stand van zaken tactische risicoanalyses (TRA'S), privacy risicoassessments (PRA's), data protection impact assessments (DPIA's) en operationele risicoanalyses (ORA's)

Norm	**TRA's** R Nee , O Gepland, G Ja	**PRA's** R < 75% , O < 90%, G >90%	**DPIA's** R < 75% , O < 90%, G >90%	**ORA's** R Nee , O Gepland, G Ja
Aantal	15	7	2	-
Aantal	0	3	3	-
Aantal	6	11	6	-
Nader te bepalen	-	-	10	21
Totaal	**21**	**21**	**21**	**21**

Bron: Gemeente Utrecht (december 2020). *Programmadashboard 2021* bewerking rekenkamer

Het management is verantwoordelijk voor het identificeren van de hoogste risico's, het prioriteren ervan en het treffen van maatregelen om de risico's terug te brengen. In het beleid voor gegevensbescherming meldt de gemeente Utrecht dat maatregelen risicogebaseerd worden genomen op basis van zakelijke overwegingen (kosten versus baten) of omdat er externe verplichtingen zijn (wet- en regelgeving, contracten). Een aantal risico's wordt

bewust geaccepteerd en daarvoor worden geen maatregelen genomen.[3] Operationele risicoanalyses zijn dus noodzakelijk om maatregelen te maken en daarmee cruciaal om risicogestuurd te kunnen werken. Wegens het gebrek aan tactische en operationele risicoanalyses is dit dus nog niet volledig mogelijk.

2.2.2. MAATREGELEN OM RISICO'S TE VERMINDEREN

Bij de implementatie van het nieuwe beleid voor gegevensbescherming heeft de gemeente Utrecht een roadmap opgesteld die jaarlijks wordt herijkt en geactualiseerd. Deze bevat onderwerpen waarmee de gemeente aan de slag gaat en de mijlpalen die daarbij behaald moeten worden.

Voor de implementatie van het beleid voor de gegevensbescherming is een roadmap opgesteld. In de roadmap zijn de onderwerpen opgenomen waar de gemeente Utrecht in de jaren 2019-2022 mee aan de slag gaat. Daarbij zijn per kwartaal mijlpalen gedefinieerd. De roadmap wordt vastgesteld in het directeurenoverleg en is daarmee bindend voor de interne organisatie. Tabel 2.3 geeft inzicht in de onderwerpen die in de roadmap zijn opgenomen. Wij hebben deze onderwerpen verdeeld over de terreinen organisatie/proces, mens en techniek. De onderstreepte onderwerpen zijn toegevoegd na de herijking van de roadmap in november 2020. De schuingedrukte onderwerpen zijn bij de herijking uit de roadmap gehaald. Voor sommige onderwerpen geldt dat zij onder meerdere categorieën vallen, deze zijn onderin de tabel opgenomen. Onder de tabel lichten wij kort de huidige stand van zaken toe.

Tabel 2.3 Onderwerpen in de roadmap naar categorie

Organisatie en proces		**Mens**	**Techniek**
Gegevensbeschermings-plan	Afspraken derde partijen	Kennis en vaardigheden – specifiek	Logging
Eigenaarschap	Resilience strategie en governance	Kennis en vaardigheden – generiek	Security Architectuur Generiek
Classificatie	Verwerving en onderhoud	*Updaten personeelsbeleid*	Security Architectuur Techniek (Capabilities)
Risicoanalyse	Beheer van cryptosleutels en certificaten	*Naleving*	(netwerk) Communicatie
DPIA's	Statement of Applicability	Bewustwording	
Risicomanagement	Beveiligingsplan		

[3] Gemeente Utrecht (1 juli 2019). Beleid voor gegevensbescherming Gemeente Utrecht 2019-2022, *"Bescherming van het digitale DNA van de stad".*

Security incident management	Directie beoordeling		
Security monitoring en rapportage	Gegevens classificatie		
Gegevensbeschermings-audits	Documentatiebeheer		
Standaarden voor gegevensbescherming	Bedrijfsvoering - eisen aan de support delivery services		
Inzageverzoeken	Security Architectuur Processen		
Strategisch beleid voor gegevensbescherming	Naleving (wetgeving)		
Inrichten Crisismanagement	Gemeenteverordening (privacy)		
IB in ICT beheerprocedures	Cryptografie		
Borging interne organisatie			
Onderwerpen die vallen onder meerdere categorieën			
Fysieke beveiliging (organisatie en proces, techniek)			
Business Continuity Management, inclusief Disaster recovery management en BCM standaard (organisatie en proces, mens, techniek)			
Ondersteunende middelen (organisatie en proces, mens, techniek)			
Identity & Access Management, Identificatie, authenticatie, authorisatie (organisatie en proces, mens, techniek)			
Ontwikkelingen DomstadIT (organisatie en proces, mens, techniek)			

Bron: Rekenkamer Utrecht op basis van Roadmap implementatie gegevensbescherming 2019-2022

De uitvoering van het informatiebeveiligingsbeleid loopt op cruciale onderdelen achter op de oorspronkelijke planning. Met extra geld en mensen moet de achterstand worden ingelopen, maar daarvoor zijn ook daadkracht en urgentie bij de proceseigenaren en de inzet van uitvoerende medewerkers vereist.

Organisatie en proces

In de roadmap is een veelheid aan onderwerpen opgenomen als het gaat om de organisatie en het proces rondom gegevensbescherming. Ieder organisatieonderdeel vertaalt de onderwerpen uit de roadmap naar doelen en acties voor het eigen onderdeel in het *gegevensbeschermingsplan*. We constateren dat deze plannen – met uitzondering van de Utrechtse Vastgoed Organisatie – in 2020 voor alle organisatieonderdelen zijn op- en vastgesteld. De achterstand op de uitvoering van de maatregelen die we zagen bij het uitvoeren van de *risicoanalyses* en *DPIA's* zien we ook bij andere onderwerpen terug. De

doelstelling voor 2020 was bijvoorbeeld dat het *eigenaarschap* up-to-date zou zijn, maar dat is niet gehaald.[4] Hetzelfde geldt voor het onderwerp *classificatie,* waar de doelstelling van een up-to-date Business Impact Analyse (BIA) en verwerkingenregister in 2020 nog niet zijn gerealiseerd. Deze stap wordt naar verwachting in het eerste kwartaal van 2021 afgerond.[5]

Mens

Er zijn vier onderwerpen in de roadmap opgenomen om invulling te geven aan de ontwikkeling van kennis en vaardigheden van de medewerkers. Bij het onderwerp *kennis en vaardigheden specifiek* gaat het om de DISO's, bij *generiek* om alle medewerkers van de gemeente Utrecht. In de roadmap uit 2019 was hierbij alleen het organiseren van een DISO-opleiding opgenomen, verdere doelstellingen ontbraken. De gemeente geeft hierbij aan dat het om een bewuste keuze ging omdat er beperkt budget beschikbaar was. Dit was voor de stuurgroep aanleiding om in 2020 additioneel budget voor gegevensbescherming beschikbaar te stellen, waaronder € 200.000 voor "Bewustwording en opleiding gegevensbescherming gemeentelijke organisatie"[6] Voor het *updaten van het personeelsbeleid* was de doelstelling om in het 2e kwartaal van 2019 de vereisten gegevensbescherming voor het personeel uit te werken en die in 2020 en 2021 door HRM door te laten voeren. Wij constateren dat ook hier vertraging is opgelopen. De planning is nu dat de strategische standaard gegevensbescherming binnen HR in 2021 wordt geïmplementeerd. Verder is er een gebruikersprotocol in ontwikkeling en is er in oktober 2020 een (tijdelijke) projectleider awareness aangesteld die een bewustwordingsprogramma voor de medewerkers ontwikkelt. Wij gaan hier in hoofdstuk 3 (Mens) dieper op in.

Techniek

Volgens geïnterviewden geeft de roadmap houvast en een koers als het gaat om de maatregelen die nodig zijn. Men is het er ook over eens dat dit de juiste maatregelen zijn voor de gemeente Utrecht.[7] Tegelijkertijd wordt de opgelopen achterstand in de uitvoering ook breed onderkend. Vooral het gebrek aan capaciteit is daarbij benoemd als belangrijkste oorzaak voor de opgelopen vertraging.[8] Daarnaast wijzen verschillende geïnterviewden ook op het gebrek aan urgentie en daadkracht[9], en de keuze om eerst aan de slag te gaan met het privacydeel van het beleid voor de gegevensbescherming.[10]

De monitoring van de resultaten vindt op verschillende niveaus binnen de organisatie plaats. DomstadIT hanteert naast de roadmap ook een jaarplan voor de technische maatregelen die nodig zijn. DomstadIT rapporteert de ICT-risico's op gegevensbescherming aan de

[4] Zie ook Rekenkamer Utrecht. *Interviews gemeente Utrecht.*
[5] Rekenkamer Utrecht. *Interview gemeente Utrecht.*
[6] Gemeente Utrecht (3 februari 2020). *Memo intensivering gegevensbescherming*
[7] Rekenkamer Utrecht. *Interviews gemeente Utrecht*
[8] Rekenkamer Utrecht. *Interviews gemeente Utrecht*; Gemeente Utrecht (5 maart 2020). *Informatiebeheer- en beveiligingsplan 2020*. Werk en Inkomen.
[9] Rekenkamer Utrecht. *Interview gemeente Utrecht.*
[10] Rekenkamer Utrecht. *Interview gemeente Utrecht*.

stuurgroep gegevensbescherming en kopieert een aantal stakeholders, waaronder de CISO (Chief Information Security Officer) van de gemeente Utrecht, hierop in. De stuurgroep gegevensbescherming bedient zich van het strategisch risico-overzicht (risicolog). Het programma gegevensbescherming rapporteert maandelijks aan de stuurgroep over de voortgang via het programmadashboard. De organisatieonderdelen zijn via hun DISO's zelf verantwoordelijk voor het invullen van het dashboard waarin de voortgang van onder andere de verschillende (risico)analyses per organisatieonderdeel wordt bijgehouden. Het programmadashboard wordt regelmatig besproken in de vakgroep gegevensbescherming. De themadirecteur bedrijfsvoering is voorzitter van de stuurgroep gegevensbescherming. In de voortgangsgesprekken die op managementniveau halfjaarlijks worden gevoerd wordt intern verantwoording afgelegd door de IRM-ers aan de themadirecteur. De gemeente Utrecht laat zelf ook periodiek technische penetratietests uitvoeren om de kwaliteit van de beveiliging te testen. Dit betreft bijvoorbeeld de jaarlijkse wettelijk verplichte testen omtrent DigiD. Daarnaast worden bij belangrijke externe ontwikkelingen ad hoc testen uitgevoerd. Dit betreft bijvoorbeeld beveiligingsincidenten bij andere gemeenten.

Bij de herijking van de roadmap in december 2020 zijn 18 nieuwe onderwerpen aan de roadmap toegevoegd. Bij een deel van deze onderwerpen gaat het om een verfijning of specificering van de onderwerpen die eerst op hoofdlijnen waren opgenomen. De roadmap is gebaseerd op alle onderwerpen die de gemeente vanuit de BIO standaarden en de ISO27001 (op termijn) moeten uitvoeren. Naast het inhalen van de achterstand op de andere onderwerpen is daarmee een groot aantal andere maatregelen nog uit te voeren. Bij de nieuwe onderwerpen wordt eerst gestart met het opstellen van een standaard (onder andere *identificatie*, *authenticatie*, *autorisatie*, bij *logging* en bij *cryptografie*) die vervolgens moet worden vastgesteld en in de tweede helft van 2021 voorzien van maatregelen.

De gemeente heeft verschillende algemene maatregelen genomen om de risico's te laten afnemen. Zo is de governance sinds 2018 verstevigd. Er zijn een stuurgroep, vakgroep, regiegroep en taskforce ingesteld die op verschillende niveaus de voortgang van risico's en maatregelen moeten bewaken.

De gemeente Utrecht heeft verschillende algemene maatregelen genomen om de risico's rondom informatieveiligheid te laten afnemen. De eerste maatregel is het verstevigen van de governance. Zo is er in 2018 een programmamanager gegevensbescherming aangesteld. De gemeente Utrecht heeft de verantwoordelijkheid voor gegevensbescherming op verschillende niveaus in de organisatie belegd, deze zijn uitvoerig beschreven in het *Beleid voor gegevensbescherming 2019-2022*.[11] Het college van B&W is eindverantwoordelijk voor de borging van gegevensbescherming binnen de gemeente Utrecht. De stuurgroep gegevensbescherming – onder voorzitterschap van de themadirecteur – legt verantwoording af over het gevoerde beleid aan het college, en de integraal resultaat managers (IRM'ers) zijn verantwoordelijk voor de invoering van het beleid binnen de organisatieonderdelen. Een

[11] Gemeente Utrecht (5 juli 2019). *Beleid voor gegevensbescherming 2019 – 2022*

centrale rol is op operationeel niveau binnen de verschillende organisatieonderdelen toebedeeld aan de systeem- en proceseigenaren. Ook zijn er Decentrale Informatie en Security Officers (DISO's) aangesteld om medewerkers te adviseren, helpen en te monitoren.

Figuur 2.4 geeft een overzicht van de interne organisatie omtrent gegevensbescherming. Hier is de versteviging van de governance onder andere terug te zien in dat ieder organisatieonderdeel ten minste één DISO ter beschikking heeft die wordt aangestuurd door de informatie- en procesmanager. Deze DISO's vormen samen een vakgroep, waarin de grootste risico's op een lager niveau gesignaleerd worden en waar daar gezamenlijk oplossingen voor worden bedacht. De DISO-capaciteit is uitgebreid met een pool van vijf DISO's die niet verbonden zijn met een organisatieonderdeel, maar risicogestuurd worden ingezet. De CIO-office heeft de functionele verantwoordelijkheid over IPM-ers (Informatie- en Procesmanagers) en DISO's. De stuurgroep brengt prioritering aan in de gevonden risico's en stuurt op de voortgang van maatregelen om de risico's te doen afnemen. Deze risico's worden door de stuurgroep bijgehouden in het strategisch risico-overzicht. Tussen de organisatieonderdelen en stuurgroep in zit de regiegroep. Deze adviseert de stuurgroep, stemt af tussen de verschillende niveaus en zorgt ervoor dat voorstellen van de stuurgroep voldoende draagvlak hebben bij de organisatieonderdelen. Het hoofd van het CIO-office – de CIO (Chief Information Officer) – bespreekt samen met de voorzitter van de stuurgroep, de CISO en het college de bestuurlijke risico's, welke uiteindelijk worden vertaald naar de gemeenteraad.

Figuur 2.4 Overzicht interne organisatie omtrent gegevensbescherming

Met extra middelen is sinds eind 2020 de capaciteit voor Decentrale Informatie en Security Officers (DISO's) uitgebreid en is er voor zes maanden een projectleider bewustwording aangesteld.

De tweede algemene maatregel is het uitbreiden van het budget voor informatieveiligheid. De uitgaven aan het specifieke onderwerp informatieveiligheid of gegevensbescherming zijn niet een-op-een terug te vinden in de begroting en jaarrekening. Het onderwerp valt in de categorie overhead onder Informatie- en procesmanagement (IPM). Daarnaast zijn er uitgaven in de decentrale overhead, zoals voor de decentrale information security officers (DISO's) per organisatieonderdeel en de projecten die zij uitvoeren. Bij de *Eerste bestuursrapportage* heeft de gemeenteraad ingestemd met € 3,4 miljoen extra budget voor gegevensbescherming, verdeeld over 3 jaar om het reeds geplande programma te versnellen en € 0,6 miljoen structureel om extra DISO's aan te trekken (zie tabel 2.5).

Tabel 2.5 Toegekende extra middelen voor gegevensbescherming (bedragen in € 1.000)

	2020	2021	2022	2023	2024
Gegevensbescherming	1.000	1.500	900	0	0
Gegevensbescherming: DISO's	150	600	600	600	600

Bron: Gemeente Utrecht (19 juni 2020). *Eerste Bestuursrapportage.*

Ook zijn sinds 2018 de risico's op het gebied van informatieveiligheid in kaart gebracht en geprioriteerd. Van de in totaal 60 risico's die in 2020 in de ICT zijn geïdentificeerd, staan er januari 2021 nog 24 (40%) open.

Als derde algemene maatregel heeft de gemeente het proces van scanning en patching meer inhoud willen geven. DomstadIT levert de diensten aan de verschillende organisatieonderdelen als het gaat om de technische maatregelen. De verschillende onderwerpen en bijbehorende maatregelen zijn nader uitgewerkt in de rapportage gegevensbescherming. Uit de rapportage van november 2020 blijkt dat op dat moment ruim driekwart (76%) van de geïdentificeerde risico's nog openstaat. Voor 12% van de risico's geldt dat zij gemitigeerd (verminderd) zijn, de overige 12% wordt (tijdelijk) geaccepteerd. Wanneer de risicorapportages over een langere periode worden geanalyseerd, dan constateren wij dat er in totaal in 2020 60 risico's in de ICT in kaart zijn gebracht. Begin 2021 staan er nog 24 (40%) open, waarvan bij 9 risico's geldt dat het risico door de eigenaar wordt geaccepteerd. Geïnterviewden geven aan dat het een positieve ontwikkeling is dat veel technische risico's nu in beeld zijn. De gemeente Utrecht heeft zich de afgelopen 1,5 jaar ontwikkeld van "*we varen blind naar we varen transparant*".[12] De komende jaren moeten de verschillende risico's verder worden gemitigeerd, al blijven zich ook steeds nieuwe risico's voordoen waardoor de risico's nooit 100% gemitigeerd zullen zijn. Ten aanzien van de techniek wijzen geïnterviewden ook op de inzet en de stappen die gezet zijn op het gebied

[12] Rekenkamer Utrecht. *Interviews gemeente Utrecht.*

van crisismanagement (wat te doen als er zaken misgaan?).[13] Omdat dit buiten de scope van dit onderzoek valt, laten we dit verder buiten beschouwing. Op de stand van zaken van de techniek gaan we in hoofdstuk 4 dieper in aan de hand van de testen die door het externe bureau zijn uitgevoerd.

[13] Rekenkamer Utrecht. *Interview gemeente Utrecht.*

3 MENS: HOE MEDEWERKERS IN DE PRAKTIJK OMGAAN MET INFORMATIEVEILIGHEID

In dit hoofdstuk beschrijven we op welke manier de gemeente inzet op het bewust omgaan met informatie (informatiebewustzijn) en hoe medewerkers in de praktijk omgaan met informatieveiligheid. Daarmee wordt de tweede onderzoeksvraag beantwoord: Op welke manier zet de gemeente in op het bewust omgaan met informatie? Hoe gaan de medewerkers van de gemeente in de praktijk om met informatieveiligheid?

In paragraaf 3.1 geven we de belangrijkste bevindingen weer. Deze bevindingen lichten we toe in paragraaf 3.2. Aan de hand van de bevindingen beoordelen we in tabel 3.1 de bijbehorende normen.

Tabel 3.1 Normen en criteria thema 'mens'

Norm	Criteria	Beoordeling
Medewerkers gaan in de praktijk bewust met informatie/gegevens om.	Medewerkers weten wat ze wel en niet mogen/moeten doen met informatie/gegevens en herkennen incidenten, dit is te relateren aan de leerdoelen van de instructies/opleiding.	Zie bevinding 1 en 2 van § 3.1
De gemeente zorgt voor het informatiebewustzijn van medewerkers.	Er is een plan/programma voor medewerkers over informatiebewustzijn, dat medewerkers in staat stelt om op een bewuste manier om te gaan met informatie.	Zie bevinding 3 van § 3.1

3.1 BELANGRIJKSTE BEVINDINGEN

1. Een groot deel van de medewerkers gaat niet altijd bewust om met informatieveiligheid. Dit werd zichtbaar uit de phishing test die de rekenkamer heeft laten uitvoeren, waarbij 950 medewerkers (16%) gebruikersnaam en wachtwoord hebben verstrekt. Dit is vergelijkbaar met de uitkomsten van dergelijke onderzoeken bij andere gemeenten. In januari 2020 was een groot deel van de medewerkers ook al niet alert op een poging van phishing. Van twee van de verspreide USB-sticks werd door medewerkers de inhoud geopend. Een kwaadwillende kan hiermee toegang krijgen tot de betrokken computer. Ook bleek dat de fysieke beveiliging van en sociale controle op het Stadskantoor en Stadhuis de toegang van onbevoegden niet konden voorkomen. Op deze locaties was sommige geheime informatie niet veilig opgeborgen.

2. Medewerkers lijken niet altijd te weten wat zij moeten doen bij beveiligingsincidenten. Zo blijkt uit de phishing actie van november 2020 dat 950 medewerkers hun gegevens achterlieten, maar er slechts 477 keer officieel melding van phishing werd gedaan. Ook is het aantal gemelde datalekken tussen 2019 en 2020 afgenomen. De meldingsbereidheid is niet te achterhalen, omdat niet duidelijk is hoe vaak een datalek daadwerkelijk is voorgekomen. Er is volgens geïnterviewden binnen de gemeente Utrecht wel sprake van een open cultuur. De gemeente wijst verschillende plekken aan om meldingen te doen.

3. Tijdens het onderzoek is er geen centraal plan/programma voor medewerkers over informatiebewustzijn. Er worden ad hoc acties uitgevoerd en organisatieonderdelen besteden op hun eigen manier aandacht aan het bewust omgaan met (gevoelige) informatie. Een eerdere bewustwordingscampagne is in 2018 gestopt vanwege gebrek aan budget en het vertrek van de projectleider. De gemeente wil intensiveren op dit gebied en bereidt sinds eind 2020 een nieuw bewustwordingsprogramma voor dat in 2021 uitgevoerd moet worden.

3.2 TOELICHTING OP DE BEVINDINGEN

3.2.1 INFORMATIEBEWUSTZIJN IN DE PRAKTIJK

Een groot deel van de medewerkers gaat niet altijd bewust om met informatieveiligheid. Dit werd zichtbaar uit de phishing test die de rekenkamer heeft laten uitvoeren, waarbij 950 medewerkers (16%) gebruikersnaam en wachtwoord hebben verstrekt. Dit is vergelijkbaar met de uitkomsten van dergelijke onderzoeken bij andere gemeenten.

Voor de informatieveiligheid van de gemeente is het van belang dat medewerkers in de praktijk bewust met informatie en gegevens omgaan. Ook is het van belang dat zij alert zijn op pogingen van kwaadwillenden om toegang te krijgen tot vertrouwelijke informatie. Uit verschillende social engineering testen – mail-phishing en mystery guest bezoeken – die de gemeente en de rekenkamer hebben laten uitvoeren, blijkt echter dat een groot deel van de medewerkers niet altijd bewust omgaat met informatie en de risico’s die zich hierbij manifesteren. Wij hebben in november 2020 door het externe bureau een mail-phishing actie laten uitvoeren. Phishing is een vorm van cybercriminaliteit waarmee criminelen persoonlijke gegevens proberen te verkrijgen of malware op de computer proberen te installeren. Het vormt een van de grootste risico’s voor informatieveilig werken. De resultaten van deze actie zijn te vinden in onderstaande tabel 3.1.

Tabel 3.1 Resultaten mail-phishing actie november 2020

Aantal e-mails verstuurd	Aantal personen link geopend	Aantal personen gegevens achtergelaten	Aantal minuten tot eerste melding
5.769	1.100 (19%)	950 (16%)	9

In de e-mail werd door de servicedesk verzocht om mobiele apparaten te registreren. De eerste mail werd om 10.36 uur verzonden, de eerste melding bij de servicedesk volgde negen minuten later. Om 16.30 uur, toen de teller van medewerkers die hadden ingelogd op 808 unieke gebruikers stond, lag het aantal meldingen op 438. De phishing link is ook daarna nog een aantal dagen beschikbaar gebleven. Ondanks een waarschuwing in een e-mail aan alle medewerkers door de gemeente omstreeks 18.00 uur op de eerste dag bleken nog altijd nieuwe gebruikersnamen en wachtwoorden doorgegeven te worden. Uiteindelijk zijn na een week 950 unieke gebruikers (16%) op het verzoek ingegaan door hun gebruikersnaam en wachtwoord in te vullen, 121 gebruikers deden dit na de waarschuwing. Dit percentage is vergelijkbaar met uitkomsten van dergelijke onderzoeken bij andere gemeenten. De gemeente Utrecht zou graag zien dat de VNG/IBD een benchmark voor alle Nederlandse gemeenten opzet om als gemeenten van elkaar te kunnen leren op dit gebied. En daarbij geldt dat één gebruikersnaam en wachtwoord veelal voor een kwaadwillende al genoeg is om de digitale infrastructuur van een organisatie binnen te dringen.

In januari 2020 was een groot deel van de medewerkers ook al niet alert op een poging van phishing.

Dat een groot deel van medewerkers van de gemeente Utrecht niet alert is op pogingen van phishing, was al bekend. In januari 2020 heeft de gemeente Utrecht namelijk ook een mail-phishing simulatie laten uitvoeren.[14] Maar liefst 3.418 medewerkers (80%) klikten op de link in deze phishing mail. Het bedrijf dat de actie uitvoerde concludeerde naar aanleiding van de actie dat medewerkers nog niet goed op de hoogte zijn van phishing inlogpagina's.[15] De resultaten van de actie uit januari zijn te vinden in onderstaande tabel 3.2.

Tabel 3.2 Resultaten mail-phishing actie januari 2020

Aantal e-mails verstuurd	Aantal personen link geopend	Aantal personen gegevens achtergelaten	Aantal minuten tot eerste melding
4.277	3.418 (80%)	38 (1%)[16]	9

[14] LBVD (17 februari 2020). *Rapportage Phishlink-simulatie*. Gemeente Utrecht.

[15] Uit deze phishing-actie zijn zeven algemene en drie technische aanbevelingen gekomen, waaronder "Continueer phishing e-mail-simulaties om medewerkers te blijven testen" (aanbeveling 2) en "Deel de resultaten van de phishing-actie met de medewerkers. Vertel hen wat zij zelf kunnen doen tegen een phishing-aanval en deel de beveiligingstips" (aanbeveling 3).

[16] Omdat de gemeente het verstrekken van gegevens vroegtijdig heeft geblokkeerd maar wel het aantal personen dat de link opende heeft doorgeteld, ligt dit percentage erg laag.

Net als bij de actie in november werd bij deze simulatie een e-mail verzonden naar medewerkers van de gemeente Utrecht met daarin een link, waarna medewerkers werd gevraagd om in te loggen. Een verschil tussen de twee acties was dat in januari de mogelijkheid om gegevens achter te laten snel werd geblokkeerd door een medewerker van de gemeente Utrecht. Daardoor hebben in deze simulatie slechts 38 mensen hun gegevens kunnen achterlaten. Wel vormen zij 53% van het aantal klikkers (71) dat het onderzoeksbureau heeft geregistreerd tot aan de blokkade. In onze test van november 2020 is deze mogelijkheid niet afgesloten waardoor 950 personen hun inloggegevens konden achterlaten. Door deze interventie zijn de twee acties zijn dus niet volledig vergelijkbaar.

Doordat men sinds de coronacrisis veel minder vaak fysiek met elkaar werkt, is er waarschijnlijk minder sociale controle onder collega's. Mogelijk kan dit van invloed zijn geweest op de resultaten van de mail-phishing test van november 2020.

Van twee van de vier verspreide USB-sticks werd door medewerkers de inhoud geopend. Een kwaadwillende kan hiermee toegang krijgen tot de betrokken computer. Ook bleek dat de fysieke beveiliging van en sociale controle op het Stadskantoor en Stadhuis de toegang van onbevoegden niet konden voorkomen. Op deze locaties was sommige geheime informatie niet veilig opgeborgen.

Het externe bureau heeft naast de mail-phishing actie ook twee pogingen ondernomen om gebouwen van de gemeente Utrecht – het Stadskantoor en het Stadhuis – te betreden en daar (gevoelige) informatie te verzamelen. Het bureau heeft daar USB-sticks verspreid, om te testen of medewerkers de inhoud van de USB-sticks zouden bekijken. Op de USB-sticks stond een verstopte afbeelding die verbinding kon maken met de webserver van de onderzoekers van het externe bureau. Bij de inlooptesten zijn vier USB-sticks achtergelaten. Van twee USB-sticks zijn daadwerkelijk bestanden geopend. Een kwaadwillende kan zo toegang tot een computer van het slachtoffer krijgen.

In beide pogingen zijn de 'mystery guests' erin geslaagd om het gebouw te betreden. Op het Stadskantoor hebben de onderzoekers een dag-pas aangevraagd en ontvangen om door de beveiligingspoorten te komen. De onderzoekers zijn niet aangesproken op hun aanwezigheid en hebben (vertrouwelijke) informatie kunnen inzien. Zo hebben ze dossierkasten kunnen openen en informatie kunnen inzien. De onderzoekers hebben daarnaast een laptop van een medewerker mee kunnen nemen waarop een post-it met bijbehorend wachtwoord was bevestigd. Hierdoor kon eenvoudig toegang worden verkregen tot de laptop.

Op het Stadhuis zijn de onderzoekers binnengekomen door achter een medewerker aan te lopen die de toegangsdeur opende. Tijdens deze poging heeft de onderzoeker een hele dag in een kantoorruimte op het Stadhuis gewerkt, waarvan gedeeltelijk samen met een medewerker van de gemeente Utrecht. De onderzoeker heeft onder andere vanachter een computer van een van de medewerkers gewerkt toen diegene zijn/haar computer niet afgeschermd achterliet.

3.2.2 CULTUUR EN MELDINGEN

Uit het gedrag van medewerkers blijkt dat zij onvoldoende weten wat te doen bij incidenten. Zo blijkt uit de phishing actie van november 2020 dat 950 medewerkers hun gegevens achterlieten, maar er slechts 477 keer officieel melding van werd gedaan.

In het huidige *Beleid voor Gegevensbescherming 2019-2022* is de verantwoordelijkheid van medewerkers opgenomen dat zij beveiligingsproblemen of -incidenten signaleren en melden. Uit de mail-phishing actie (november 2020) blijkt echter dat 950 medewerkers hun gebruikersnaam en wachtwoord hebben achtergelaten, maar phishing slechts 477 keer centraal werd gemeld. In totaal zijn er als gevolg van de mail-phishing actie 136 bellers geregistreerd in het Serviceportaal en heeft de Servicedesk 341 e-mails ontvangen.

Ook is het aantal gemelde datalekken tussen 2019 en 2020 afgenomen. De meldingsbereidheid is niet te achterhalen, omdat niet duidelijk is hoe vaak een datalek daadwerkelijk is voorgekomen.

Uit cijfers van de functionaris gegevensbescherming – op basis van de vastgelegde meldingen in het zaaksysteem - blijkt het aantal meldingen van datalekken in de jaren 2019 en 2020 min of meer gelijk te zijn (zie tabel 3.3). Meldingen hebben bijvoorbeeld betrekking op verkeerd verstuurde e-mails of brieven. Het aantal unieke melders ligt in 2020 vooralsnog lager dan het jaar daarvoor. De meldingsbereidheid ten opzichte van het totaalaantal incidenten is echter niet te achterhalen. Het is namelijk niet duidelijk hoe vaak bijvoorbeeld een datalek in de afgelopen jaren daadwerkelijk is voorgekomen. Volgens de gemeente is het, conform de definitie van de autoriteit persoonsgegevens (AP), ook niet mogelijk om het werkelijke aantal datalekken te kennen.

Tabel 3.3 Datalekmeldingen 2019 en 2020 (tot 27 november)

	2019	***2020 (tot 27-11)***	**Totaal 2019 en 2020 (tot 27-11)**
Aantal meldingen	140	*110*	250
Aantal unieke melders	54	*32*	72
Aantal meldingen top 10 melders	72	*69*	132
Aandeel meldingen van top 10 melders	51%	*63%*	53%

Bron: Gemeente Utrecht (27 november 2020). *Datalekmeldingen 2019 en 2020.*

Het aandeel van de top 10 personen met de meeste meldingen ligt in 2020 voorlopig hoger dan in 2019. In de praktijk worden meldingen relatief vaak gedaan door DISO's en Informatie- en procesmanagers (IPM-ers). Ook worden datalekmeldingen vastgelegd in een

register dat openbaar beschikbaar moet zijn.[17] Dit register is echter wegens gebrek aan middelen en capaciteit slechts tot eind 2018 geactualiseerd. De capaciteit is uitgebreid en de gemeente verwacht in Q1/Q2 van 2021 het register te kunnen aanvullen.[18]

Er is volgens geïnterviewden binnen de gemeente Utrecht wel sprake van een open cultuur.

In het *Beleid voor gegevensbescherming 2019-2022* onderschrijft de gemeente de tien bestuurlijke principes voor informatiebeveiliging[19] van de VNG. Het eerste principe beschrijft dat bestuurders een veilige cultuur bevorderen, waarin men zich vrij voelt om risico's te melden en maatregelen voor te stellen. Het belang van een open cultuur wordt ook benoemd in het *Dreigingsbeeld Informatiebeveiliging 2021-2022* van de Informatiebeveiligingsdienst (IBD).[20] Geïnterviewden geven aan dat er binnen de gemeente Utrecht sprake is van een open cultuur om incidenten en datalekken te melden en elkaar aan te spreken op de naleving van het beleid.[21] Medewerkers worden gestimuleerd meldingen te doen van datalekken en incidenten, weten de weg en krijgen niet 'op hun kop' als zij een melding doen. Binnen de gemeente heerst het beeld dat mensen elkaar aanspreken en open zijn.

De gemeente wijst verschillende plekken aan om meldingen te doen.

De rekenkamer is in het beleid en de communicatie van de gemeente Utrecht nagegaan op welke plek medewerkers beveiligingsproblemen en -incidenten dienen te melden. Er komen verschillende plekken naar voren. Er worden zowel de functionaris voor de gegevensbescherming[22] en de servicedesk[23], als leidinggevenden en DISO's van een organisatieonderdeel[24] genoemd. Volgens geïnterviewden van de gemeente dienen medewerkers via een webformulier melding te doen, maar er geldt bij de gemeente ook een 'no-wrong-door policy': waar men ook meldt, het is altijd goed dát men meldt. De rekenkamer heeft niet kunnen constateren of gegevens dan elders zijn doorgegeven. In haar ambtelijke reactie ligt de gemeente toe dat zij medewerkers meerdere kanalen biedt voor het melden van incidenten, met als reden het hen zo makkelijk mogelijk te maken en melden te stimuleren. Een aantal geïnterviewden antwoordt positief op de vraag of beveiligingsproblemen en -incidenten door medewerkers op de juiste plek worden gemeld.[25] Een enkele geïnterviewde geeft aan mensen soms te wijzen op het feit dat meldingen ook centraal bij de servicedesk kunnen worden gedaan.[26]

---

[17] Zie https://www.utrecht.nl/bestuur-en-organisatie/privacy/privacymelding/

[18] Rekenkamer Utrecht. *Interview Gemeente Utrecht.*

[19] VNG (januari 2019). Baseline *De 10 bestuurlijke principes voor informatiebeveiliging.* Behorende bij de Baseline Informatiebeveiliging Overheid (BIO).

[20] Hierin staat dat medewerkers zich veilig moeten voelen om onveilige situaties, incidenten of ongelukken te melden, en van incidenten moeten kunnen leren.

[21] Rekenkamer Utrecht. *Interviews gemeente Utrecht.*

[22] Gemeente Utrecht. *Privacyverordening gemeente Utrecht.*

[23] Gemeente Utrecht (2019). *Beleid accounts, authenticatiemiddelen en wachtwoorden Gemeente Utrecht*.

[24] Gemeente Utrecht Intranetpagina 'Datalekken'.

[25] Rekenkamer Utrecht. *Interviews gemeente Utrecht.*

[26] Rekenkamer Utrecht. *Interview gemeente Utrecht.*

3.2.3 PROGRAMMA INFORMATIEBEWUSTZIJN

Tijdens het onderzoek is er geen centraal plan/programma voor medewerkers omtrent informatiebewustzijn.

Uit onderzoek van de VNG blijkt dat bijna de helft van alle incidenten afkomstig is uit onbewust handelen van medewerkers.[27] Daarom is het van belang dat de gemeente voldoende aandacht besteedt aan informatiebewustzijn onder medewerkers. Daarnaast is de gemeente wettelijk verplicht om medewerkers bepaalde informatie te verschaffen over veilig informatiegebruik.[28] Ten tijde van het onderzoek is er binnen de gemeente Utrecht geen centraal plan of programma voor medewerkers omtrent informatiebewustzijn. Ook wordt de introductie op het onderwerp informatieveiligheid voorafgaand aan indiensttreding nog niet organisatie-breed opgepikt. Medewerkers ontvangen bij indiensttreding niet standaard informatie/instructies over veilig omgaan met informatie en gegevens. Dit soort instructies wordt daarnaast ook niet voor alle medewerkers tijdens het dienstverband periodiek herhaald. Wel bestaan er richtlijnen omtrent informatieveiligheid bij uitdiensttreding. Het lijnmanagement is verantwoordelijk voor "*het direct wijzigen of blokkeren van toegangsrechten op informatiesystemen wanneer een medewerker van functie wisselt of uit dienst gaat*" (p. 14).[29]

Informatiebewustzijn blijkt geen vast onderdeel te zijn van medewerkersgesprekken. Ook worden er organisatie-breed geen opleidingen aangeboden omtrent informatieveiligheid en/of -bewustzijn. Medewerkers kunnen de landelijke training 'i-bewustzijn' volgen, maar onbekend is hoeveel medewerkers van de gemeente Utrecht dit doen of hebben gedaan.

Er worden ad hoc acties uitgevoerd en organisatieonderdelen besteden op hun eigen manier aandacht aan het bewust omgaan met (gevoelige) informatie.

Er is een aantal acties omtrent informatiebewustzijn meer ad hoc uitgevoerd. De acties die organisatie-breed zijn uitgevoerd betreffen bijvoorbeeld een mail-phishing test en twee drukbezochte dagen in het kader van privacy en informatieveiligheid.

Naast deze acties trof de rekenkamer een *Gebruikersprotocol Bewust Informatiegebruik* (2018)[30] aan en nog enkele beleidsstukken en richtlijnen op specifieke thema's, zoals het gebruik van mobiele apparaten[31] en wachtwoorden en accounts[32]. Met uitzondering van publicatie op het intranet, worden deze documenten niet structureel en actief gedeeld met

---

[27] Gemeente Utrecht (1 juli 2019). Beleid voor gegevensbescherming Gemeente Utrecht 2019-2022, *"Bescherming van het digitale DNA van de stad".*

[28] Rekenkamer Utrecht. Interview gemeente Utrecht.

[29] Gemeente Utrecht (1 juli 2019). Beleid voor gegevensbescherming Gemeente Utrecht 2019-2022, *"Bescherming van het digitale DNA van de stad".*

[30] In haar ambtelijke reactie geeft de gemeente aan dat het gebruikersprotocol wordt opgesteld, om een begrijpelijke vertaling voor medewerkers te maken.

[31] Gemeente Utrecht (z.j.). *Enterprise Mobility Management beleid gemeente Utrecht*

[32] Gemeente Utrecht (3 september 2019). *Beleid accounts, authenticatiemiddelen en wachtwoorden Gemeente Utrecht.*

medewerkers. Ook zijn er de centrale bewustwording, in de vorm van de totale communicatie over IT, en berichten op intranet.[33] Op het intranet zijn daarnaast verschillende pagina's te vinden omtrent veilig omgaan met informatie. Deze bevatten richtlijnen voor informatieveiligheid en antwoorden op veel gestelde vragen. Ook is er een speciale pagina omtrent 'thuiswerken in coronatijd'. Deze pagina bevat informatie over o.a. veilig thuiswerken en digitale thuiswerk- en vergadertools. Over het gebruik van vergadertools zijn inmiddels ook regels vastgesteld door de directieraad.[34] Er is vanuit de gemeente een algemeen protocol omtrent thuiswerken, maar dat is zeer verouderd. Een nieuw protocol is in concept beschikbaar en wordt door de Regiegroep gegevensbescherming verder uitgewerkt. Vanuit de coördinatie Integriteit is er in 2020 een nieuwe gedragscode ontwikkeld voor medewerkers. Informatiebeveiliging is hiervan een onderdeel. De gedragscode is echter alleen van invloed op medewerkers van de gemeente Utrecht, niet op ingehuurde, externe medewerkers. Dat geldt ook voor de introductiedag voor nieuwe medewerkers.

Daarnaast gebeuren er allerlei dingen op dit thema bij de organisatieonderdelen, zoals incidenten die onderling met medewerkers worden afgehandeld.[35] Ook is de uitvoer van introductie op het onderwerp bij indiensttreding toebedeeld aan de afzonderlijke organisatieonderdelen.[36] Sommige organisatieonderdelen geven nieuwe medewerkers standaard instructies, maar niet alle organisatieonderdelen doen dit.[37] Zo wordt er voor het gebruik van SUWINET training geboden, is er een vakopleiding voor DISO's en wordt er voor andere applicaties bij Werk en Inkomen extra ondersteuning geboden. Bij bepaalde organisatieonderdelen wordt tijdens het dienstverband de kennis van medewerkers bijgespijkerd en zijn specifieke thuiswerkafspraken gemaakt met medewerkers.[38] Ten slotte wordt bij een enkel organisatieonderdeel periodiek aandacht aan informatiebewustzijn besteed in dag- en weekstarts, het werkoverleg en af en toe in individuele gesprekken.[39]

Aandacht voor informatiebewustzijn wordt door de afzonderlijke organisatieonderdelen dus wisselend ingevuld. Dit heeft ten dele te maken met het feit dat het ene organisatieonderdeel meer of op een andere manier met gevoelige informatie te maken heeft dan het andere.

Een eerdere bewustwordingscampagne is in 2018 gestopt vanwege gebrek aan budget en het vertrek van de projectleider.

Het ontbreken van een centraal programma/plan omtrent informatiebewustzijn, heeft onder andere te maken met de beëindiging van een vorige bewustwordingscampagne uit 2015. Dit

[33] Rekenkamer Utrecht. *Interview gemeente Utrecht*.
[34] Rekenkamer Utrecht. *Interview gemeente Utrecht.*
[35] Rekenkamer Utrecht. *Interview gemeente Utrecht.*
[36] Rekenkamer Utrecht. *Interview gemeente Utrecht.*
[37] Rekenkamer Utrecht. *Interview gemeente Utrecht.*
[38] Rekenkamer Utrecht. *Interview gemeente Utrecht.*
[39] Rekenkamer Utrecht. *Interview gemeente Utrecht.*

betrof de campagne over *Bewust Informatie Gebruiken* (BIG)[40], welke vanwege een gebrek aan structurele middelen/budget en het vertrek van de vorige projectleider, in 2018 is gestopt. Volgens de rekenkamer beoordeelt de functionaris gegevensbescherming terecht dat de gemeente in 2018/2019 slechts deels voldeed aan de norm dat er voldoende aandacht is voor bewustwording en gedragsverandering. Er is in 2019 vanuit de stuurgroep voorgesteld om de bewustwordingscampagne met beperkte middelen voort te zetten. Dit heeft geleid tot twee opdrachten. De eerste was het organiseren van de dag van de gegevensbescherming. In de tweede opdracht zou een gereedschapskist voor gegevensbescherming voor leidinggevenden worden gemaakt en uitgerold in de organisatie.[41] Deze opdracht is in gang gezet, maar niet goed verlopen, waardoor het eindproduct onbruikbaar was. Later is dit niet meer opgepakt.[42]

De gemeente wil intensiveren op dit gebied en bereidt sinds eind 2020 een nieuw bewustwordingsprogramma voor dat in 2021 uitgevoerd moet worden.

Er is voorgesteld om te intensiveren op bewustzijn (awareness) en de gemeenteraad heeft bij de *Eerste Bestuursrapportage 2020* middelen beschikbaar gesteld om het onderwerp structureel aandacht te geven en planmatig te benaderen. Er is voor een initiële periode van zes maanden een projectleider awareness aangesteld die een plan/bewustwordingsprogramma gaat ontwikkelen.[43] Dit plan is inmiddels gepresenteerd aan de stuurgroep gegevensbescherming en wordt in 2021 geïmplementeerd.

Bewustwordingsprogramma 2021

In het nieuwe bewustwordingsprogramma is als insteek gekozen voor het verloop van een dienstverband (voorafgaand, tijdens, bij wijziging en bij beëindiging).[44] Inhoudelijk staat voor dit programma een aantal zaken op de planning, zoals: een standaard informatiepakket voor nieuwe medewerkers, specifieke informatie voor bepaalde organisatieonderdelen, nul- en effectmetingen, workshops, e-learning, lezingen, werken met testimonials en ambassadeurs. Ook zal thuiswerken een plek krijgen in het nieuwe bewustwordingsprogramma.[45]

De gemeente ontwikkelt ook een strategische standaard voor gegevensbescherming binnen HR. Deze wordt momenteel afgestemd met de HR-organisatie en in 2021 geïmplementeerd. Het bevat de standaard diensten die de HR-functie aan organisatieonderdelen levert op het gebied van gegevensbescherming. Ook hierin wordt het verloop van een dienstverband gehanteerd als indeling. Volgens deze standaard zullen

[40] Gemeente Utrecht (mei 2019). *Gegevensbescherming in Utrecht.* Jaarverslag van de Functionaris Gegevensbescherming Gemeente Utrecht, 2018.
[41] Gemeente Utrecht (19 december 2019). Raadsbrief *Evaluatie jaarverslag functionaris gegevensbescherming*.
[42] Rekenkamer Utrecht. *Interview gemeente Utrecht.*
[43] Rekenkamer Utrecht. *Interviews gemeente Utrecht.*
[44] Rekenkamer Utrecht. *Interview gemeente Utrecht.*
[45] Rekenkamer Utrecht. *Interview gemeente Utrecht.*

in de toekomst tijdens het dienstverband instructies over omgaan met gegevens periodiek worden herhaald, aangepast aan actuele risico’s en dreigingen. Ook staat erin vermeld dat het veilig en integer omgaan met gegevens door HR zal worden geïntegreerd in de ontwikkel- en beoordelingscyclus.

4 TECHNIEK: HOE DE GEMEENTE INFORMATIE TECHNISCH BEVEILIGT

In dit hoofdstuk beschrijven we de resultaten van de verschillende testen die het externe bureau heeft uitgevoerd op de technische beveiliging. Daarmee beantwoorden we de derde onderzoeksvraag: zijn de gegevens bij de gemeente Utrecht voldoende beschermd tegen de toegang door onbevoegden? En zo niet, wat zijn de risico's en kwetsbaarheden en wat zijn daarvan de gevolgen voor burgers en ondernemers?

In paragraaf 4.1 geven we de belangrijkste bevindingen weer. Deze bevindingen lichten we toe in paragraaf 4.2. Aan de hand van de bevindingen beoordelen we in tabel 4.1 de bijbehorende norm.

Tabel 4.1 Normen en criteria thema 'techniek'

Norm	Criteria	Beoordeling
Informatie/gegevens zijn goed beschermd tegen inbraak van buitenaf.	Systemen/applicaties doorstaan pentesten.	Zie bevinding 1, 2 en 3 (onderwerp Wifi-netwerken) van § 4.1
	Medewerkers hebben een thuiswerkplek met adequate beveiliging.	Zie bevinding 3 van § 4.1

4.1 BELANGRIJKSTE BEVINDINGEN

1. Het is via het internet met externe penetratietesten niet gelukt om binnen te dringen in de gemeentelijke systemen. Deze tests toonden wel zes risico's en kwetsbaarheden aan. Het feit dat er software aanwezig is die niet meer ondersteund wordt, is gekwalificeerd als kritiek risico. De mogelijkheid om als medewerker zelf een apparaat of telefoonnummer te registreren voor multifactor-authenticatie (inloggen in meerdere stappen) is een hoog risico. Bij een langdurigere aanval zouden de kwetsbaarheden door indringers misschien uitgebuit kunnen worden.

2. De interne penetratietesten hebben 17 risico's en kwetsbaarheden aangetoond. Een deel van deze risico's was al jaren bij de gemeente bekend. Hiermee loopt de gemeente Utrecht al langere tijd onnodig risico. Zo blijkt het mogelijk om digitaal in te breken in de werkstations van medewerkers. Deze kwetsbaarheid is ondanks de beschikbare beveiligingsupdates nog niet opgelost.

3. De Wifi-netwerken van de gemeente Utrecht hebben de penetratietesten doorstaan. De gemeente Utrecht weet niet van alle medewerkers of zij thuiswerken met veilige

apparatuur. De gemeente heeft bijna 2.500 laptops verstrekt, die worden vanwege de coronacrisis nu veel gebruikt om thuis te werken. Circa 375 laptops (15%) zijn goed beschermd tegen aanvallen in onveilige netwerken en bij diefstal en verlies. De circa 2.100 eerder verstrekte laptops zijn niet allemaal voorzien van de juiste beveiligingsmaatregelen. Medewerkers die geen laptop van de gemeente hebben geleend, werken waarschijnlijk op eigen apparatuur bij het thuiswerken. De gemeente heeft geen zicht op de beveiliging van deze apparatuur, maar biedt medewerkers een virtuele werkomgeving aan om zoveel mogelijk te voorkomen dat gegevens lokaal worden opgeslagen.

4.2 TOELICHTING OP DE BEVINDINGEN

4.2.1 RESULTATEN EXTERNE PENETRATIETESTEN

Het is via het internet met externe penetratietesten niet gelukt om binnen te dringen in de gemeentelijke systemen. Deze tests toonden wel zes risico's en kwetsbaarheden aan. Het feit dat er software aanwezig is die niet meer ondersteund wordt, is gekwalificeerd als kritiek risico. De mogelijkheid om als medewerker zelf een apparaat of telefoonnummer te registreren voor multifactor-authenticatie (inloggen in meerdere stappen) is een hoog risico.

Om de bescherming van gegevens tegen toegang voor onbevoegden te garanderen, is het van belang dat via internet (extern) geen toegang kan worden verschaft tot de systemen van de gemeente Utrecht. Om te onderzoeken of dit wel of niet mogelijk is, heeft het externe bureau externe penetratietesten uitgevoerd. Bij het uitvoeren van de externe testen is de blackbox-methode toegepast. Dit betekent dat de onderzoekers de testen uitvoeren zonder voorkennis over de systemen en applicaties die in gebruik zijn. Deze methode staat dicht bij de werkwijze van een kwaadwillende hacker. Het externe bureau heeft daarmee eerst de systemen moeten ontdekken waarbij de onderzoekers gestart zijn met een geautomatiseerde scan.

De systemen van de gemeente bleken vanaf het internet in de periode van het onderzoek redelijk goed beveiligd. Voor het uitvoeren van de externe penetratietesten waren twee dagen beschikbaar. Het is in die tijd niet gelukt om toegang te krijgen tot de systemen van de gemeente Utrecht. Er zijn wel zes kwetsbaarheden aan het licht gekomen. Deze kwetsbaarheden zijn omwille van de risico's op het uitvallen van de systemen niet geëxploiteerd.

De risico's worden aan de hand van de formule *waarschijnlijkheid x impact* van een niveau voorzien. Figuur 4.2 laat zien dat er vijf niveaus zijn: informatief, laag, gemiddeld, hoog en kritiek.

Figuur 4.2 Indeling risiconiveaus

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

Een kritiek risico heeft zowel een hoge waarschijnlijkheid dat deze door een kwaadwillende wordt uitgebuit als een hoge impact (schade) voor de organisatie. De niet meer ondersteunde software die nog aanwezig is, valt in deze categorie. Het feit dat Password Spraying niet mogelijk is, leidt ertoe dat deze in de categorie informatief is ingedeeld. De maatregelen die op dit punt door de gemeente Utrecht zijn getroffen volstaan op dit moment en dienen gehandhaafd en met regelmaat geëvalueerd te worden. Wij werken deze kwetsbaarheid daarom niet verder uit. Op de andere kwetsbaarheden geven wij een nadere toelichting. De kwetsbaarheden die gevonden zijn, staan in tabel 4.3 en worden onder de tabel toegelicht.

Tabel 4.3 Bevindingen externe penetratietesten

Kwetsbaarheid	Risico
Niet meer ondersteunde software aanwezig	Kritiek
Registreren van multifactor-authenticatie mogelijk	Hoog
Ontbreken van security headers	Gemiddeld
Niet-ondersteunde versie scripttaal gedetecteerd	Gemiddeld
Verouderde Javascript-bibliotheek aangetroffen	Gemiddeld
Gegevens onnodig benaderbaar voor alle medewerkers	Gemiddeld
Password Spraying niet mogelijk	Informatief

Bron: Rapportage Hoffmann B.V., 2021

Niet meer ondersteunde software aanwezig (kritiek)
Softwaresystemen die niet meer worden ondersteund ontvangen geen beveiligingsupdates meer. Hierdoor worden nieuwe en bestaande kwetsbaarheden niet meer verholpen. Deze softwaresystemen moeten vervangen worden door sofwaresystemen die wel door leveranciers worden ondersteund. Het externe bureau heeft bij de externe penetratietest software aangetroffen die mogelijk end-of-life is en daarmee mogelijk kwetsbaarheden bevat. In de rapportage gegevensbescherming van november 2020 zien we dat op dit punt – “patchstatus beheerde hard en software” – al in oktober 2018 een projectvoorstel is

ingediend. In 2019 heeft dit proces enige tijd stilgelegen, vanaf 2020 zijn hier scans aan toegevoegd om de kwetsbaarheden in beeld te brengen en is vervolgens uitvoering gegeven aan maatregelen. Eind 2020 is dit naar het oordeel van DomstadIT vrijwel afgerond (status 97%).

Registreren multifactor-authenticatie mogelijk (hoog)
Door deze kwetsbaarheid was het mogelijk om in te loggen op de digitale werkplekomgeving van Utrecht. Tweefactor-authenticatie is het minimale beveiligingsniveau. Wanneer het registreren van een eigen apparaat of telefoonnummer mogelijk is, kunnen kwaadwillenden als zij een gebruikersnaam en wachtwoord hebben bemachtigd ook eigen apparaten koppelen. Daarmee is het in de huidige situatie mogelijk om veilige en niet veilige omgevingen te vermengen. Ook deze kwetsbaarheid was bekend bij de gemeente. De consequentie is dat de betrouwbaarheid van informatie niet is te garanderen, omdat het eenvoudig mogelijk is om misbruik te maken van de toegang tot de informatie.

Ontbreken van security headers (gemiddeld)
Security headers helpen bezoekers van een website om hun browser weerbaar te maken tegen kwetsbaarheden. Op de website van de gemeente Utrecht ontbreken enkele headers. Deze websites zijn daarmee vatbaar voor mogelijke aanvallen van buitenaf. Deze kwetsbaarheid vinden wij niet terug in de rapportages van de gemeente Utrecht.

Niet-ondersteunde versie scripttaal gedetecteerd (gemiddeld)
Het externe bureau heeft een versie van scripttaal aangetroffen die niet langer wordt ondersteund. Daarmee worden geen beveiligingsupdates meer vrijgegeven door de leverancier. Het gevolg is dat er waarschijnlijk beveiligingsproblemen bestaan.

Verouderde Javascript-bibliotheek aangetroffen (gemiddeld)
Er is een verouderde bibliotheek op de gemeentelijke website aangetroffen die kwetsbaarheden bevat. Kwaadwillenden kunnen deze in de toekomst mogelijk misbruiken door er malware aan toe te voegen.

Gegevens onnodig benaderbaar voor alle medewerkers (gemiddeld)
Het bleek tijdens de externe testen mogelijk om gegevens te benaderen die voor alle reguliere medewerkers beschikbaar zijn, maar niet nodig. Deze gegevens zijn bruikbaar voor kwaadwillenden om in de toekomst doelgerichte aanvallen uit te voeren.

Bij een langduriger aanval zouden de kwetsbaarheden door indringers misschien uitgebuit kunnen worden.

In de beschikbare onderzoekstijd is het weliswaar niet gelukt om van buitenaf in te breken op de websites van de gemeente, maar kwaadwillenden zouden bij een langere periode de gevonden kwetsbaarheden misschien uit kunnen buiten. Als het lukt om de systemen binnen te dringen, kunnen gegevens worden misbruikt. Inwoners en ondernemers lopen daarmee

het risico dat (bijzondere) persoonsgegevens in handen komen van derden die daar geen inzage in mogen hebben.

4.2.2 RESULTATEN INTERNE PENETRATIETESTEN

De interne penetratietesten hebben 17 risico's en kwetsbaarheden aangetoond. Een deel van deze risico's was al jaren bij de gemeente bekend. Hiermee loopt de gemeente Utrecht al langere tijd onnodig risico. Zo blijkt het mogelijk om digitaal in te breken in de werkstations van medewerkers. Deze kwetsbaarheid is ondanks de beschikbare beveiligingsupdates nog niet opgelost.

Om te onderzoeken of er vanuit het netwerk van de gemeente Utrecht (intern) onbevoegd toegang kan worden verschaft tot gegevens, heeft het externe bureau interne penetratietesten uitgevoerd. In tegenstelling tot bij de externe pentesten, is het externe bureau er bij de interne pentesten wel in geslaagd om zonder voorkennis deels ongeautoriseerd toegang te krijgen tot de systemen van de gemeente. Er zijn in totaal 17 kwetsbaarheden geconstateerd. Omdat kwetsbaarheden in sommige gevallen nauw op elkaar aansluiten, zijn deze geclusterd opgenomen in tabel 4.4. Vier clusters vallen in de categorie kritiek en vier vallen in de hoog risico categorie. Daarnaast is er een risico geconstateerd in de categorie gemiddeld. Hierna lichten we de kwetsbaarheden nader toe.

Tabel 4.4 Bevindingen interne penetratietesten

Kwetsbaarheid	Risico
Werkstations onveilig	Kritiek
Ontbrekende beveiligingsupdates niet toegepast	Kritiek
Verouderde besturingssystemen aanwezig	Kritiek
Serviceaccounts onvoldoende beschermd	Kritiek
Ontbreken multifactor-authenticatie	Hoog
Zwakke wachtwoorden en beheer onvoldoende veilig	Hoog
Ontbreken netwerk-authenticatie	Hoog
Systemen kwetsbaar voor spoofing	Hoog
Ontbreken harddisk encryptie	Gemiddeld

Bron: Rapportage Hoffmann B.V., 2021

Werkstations onveilig (kritiek)

Het externe bureau heeft van de gemeente Utrecht de resultaten van eerder uitgevoerde kwetsbaarhedenscans ontvangen. Daaruit kwam een al langer bekende kwetsbaarheid uit 2017 naar voren. In die periode is deze kwetsbaarheid actief misbruikt om andere grote

organisaties mee in de problemen te brengen door de bestanden te versleutelen (ransomware). Het externe bureau heeft van deze kwetsbaarheid gebruik kunnen maken om ongeautoriseerd toegang te krijgen tot enkele werkstations. De gemeente Utrecht was al langer bekend met deze kwetsbaarheid, maar heeft deze – ondanks de beschikbare beveilingsupdates die zijn uitgebracht – niet opgelost. De gemeente geeft als reden dat door een ongelukkige samenloop van omstandigheden deze kwetsbaarheid niet is aangepakt.[46]. Vervolgens zijn verschillende andere kwetsbaarheden in het systeem geconstateerd die kwaadwillenden uiteindelijk toegang zouden kunnen geven tot de accounts.

Het gevolg van het binnendringen van de werkstations is dat het voor kwaadwillenden mogelijk is om live mee te kijken en screenshots te maken van de desktop van medewerkers van de gemeente die zijn ingelogd. Zo kon het externe bureau bijvoorbeeld meelezen met een HR-medewerker in de personeelsdossiers van de gemeente. Daarnaast was het mogelijk om medewerkers te forceren om af te sluiten en opnieuw aan te melden. Daarmee zijn de gebruikersnamen en (versleutelde waarden van) wachtwoorden van deze medewerkers buitgemaakt.

Het bleek vervolgens ook mogelijk om in de werkomgeving met scripttaal verder te werken. Zo kan er bij de gemeente Utrecht via Internet Explorer een tekstbestand op worden geslagen op het bureaublad. Hiermee kunnen beheertaken op de werkstations worden uitgevoerd. Met behulp van de scripttaal is het vervolgens ook mogelijk om zogeheten tickets van serviceaccounts op te vragen. Medewerkers hebben daar bij de gemeente Utrecht geen speciale privileges voor nodig. Er kan vervolgens offline geprobeerd worden om de tickets te kraken. En als dat lukt hebben kwaadwillenden het wachtwoord van de serviceaccounts die niet aan een persoon maar aan een systeem(service) gekoppeld zijn.

Ontbrekende beveiligingsupdates niet toegepast (kritiek)
Op een aantal systemen bleken geen beveiligingsupdates toegepast die wel beschikbaar zijn. Er zijn verouderde applicaties aangetroffen die bekende kwetsbaarheden bevatten. Voor een aantal van deze kwetsbaarheden is ook een code gepubliceerd waarmee deze kunnen worden uitgebuit. Ontbrekende beveiligingsupdates kunnen in veel gevallen leiden tot ongeautoriseerde toegang tot systemen en gegevens.

Verouderde besturingssystemen aanwezig (kritiek)
Er zijn besturingssystemen aangetroffen die end-of-life zijn. Dit houdt in dat het systeem niet meer ondersteund wordt door de leverancier en dat er geen beveiligingsupdates meer voor worden uitgebracht. De gemeente Utrecht heeft bij de leverancier de ondersteuning verlengd (extended support) waarmee nog wel beveiligingsupdates beschikbaar worden gesteld. Maar het externe bureau wijst erop dat kwaadwillenden anticiperen op verouderde besturingssystemen door via kwetsbaarheden in de digitale infrastructuur binnen (proberen) te dringen.

[46] Rekenkamer Utrecht. *Interview gemeente Utrecht.*

Serviceaccounts onvoldoende beschermd (kritiek)
Het externe bureau is erin geslaagd de inloggegevens voor serviceaccounts te achterhalen, zie 'Zwakke wachtwoorden en beheer onvoldoende veilig'. Met deze serviceaccounts is toegang gekregen tot enkele systemen en zijn er versleutelde wachtwoorden achterhaald van zogeheten admin accounts. Hiermee is toegang verkregen tot een beperkt gedeelte van het netwerk.

Ontbreken multifactor-authenticatie (hoog)
Omdat er geen multifactor-authenticatie wordt afgedwongen is het intern zeer eenvoudig om met achterhaalde gebruikersnamen en wachtwoorden in te loggen. Zo kan ingelogd worden op de webmail en de werkomgeving van medewerkers. Met name voor systemen die benaderbaar zijn via het internet is het belangrijk om multifactor-authenticatie toe te passen. De gemeente was al langer op de hoogte van deze kwetsbaarheid bij de webmail, maar kon dit technisch niet oplossen. De infrastructuur was daarvoor niet up-to-date genoeg. In februari 2021 is de tweefactor-authenticatie op de webmail doorgevoerd.[47]

Zwakke wachtwoorden en beheer onvoldoende veilig (hoog)
Het bleek dat veel wachtwoorden bij de gemeente Utrecht zwak waren en gekraakt konden worden door het externe bureau. Van de 137 versleutelde waarden van de wachtwoorden (hashes) is het bij 49 gelukt om deze te kraken (36%).
In het ambtelijk wederhoor merkt de gemeente hierbij op dat er tegen de 10.000 accounts (users, services, applicaties, etc.) zijn. Er is daarnaast een password spraying[48] aanval uitgevoerd, waarbij met voor de hand liggende wachtwoorden geprobeerd wordt in te loggen op serviceaccounts. Hiermee is het daadwerkelijk gelukt een wachtwoord te raden, omdat dit wachtwoord ook zwak bleek.

In het beheer van de wachtwoorden zijn kwetsbaarheden aangetroffen. Zo zijn er wachtwoorden gevonden in een gedeelde (netwerk)map. Ook in een veelgebruikt softwareprogramma zijn (initiële) wachtwoorden in leesbare tekst aangetroffen. Er is niet gecontroleerd of deze wachtwoorden ergens anders gebruikt konden worden, maar het wordt afgeraden om wachtwoorden op te slaan in leesbare bestanden.

Ontbreken netwerk-authenticatie (hoog)
Netwerk-authenticatie zorgt ervoor dat een gebruiker pas toegang krijgt tot het gemeentelijke netwerk nadat de gebruiker is ingelogd. Dit ontbreekt op een aantal specifieke beheerwerkplekken. Hierdoor kon via een fysieke toegang tot een netwerkpoort een IP-adres verkregen worden. Het externe bureau heeft op deze manier ongeautoriseerde apparatuur met het netwerk kunnen verbinden. Kwaadwillenden kunnen met de fysieke toegang tot het netwerk verkenningen en aanvallen uitvoeren.

[47] Rekenkamer Utrecht. *Interview gemeente Utrecht.*
[48] Een techniek waarbij een aanvaller veelgebruikte wachtwoorden probeert om op een account in te loggen.

Systemen kwetsbaar voor spoofing (hoog)
Het bleek eenvoudig om door middel van spoofing (een andere identiteit aannemen) de gebruikersnaam en het wachtwoord van een medewerker te verkrijgen. Het systeem van het externe bureau werd gekoppeld aan de medewerker die vervolgens de vraag kreeg om zich te authentiseren. Door dit vervolgens te kraken kon de onderzoeker geldige inloggegevens bemachtigen.

Ontbreken van harddiskencryptie (gemiddeld)
De harde schijf van het werkstation van de gemeente Utrecht bleek niet versleuteld. Doordat het systeem toegankelijk is als opgestart wordt vanaf een USB-stick, zijn via die weg versleutelde wachtwoorden en gebruikersnamen te achterhalen. Het wachtwoord dat daarvoor nodig is was eerder in de testen al buitgemaakt. Bij het grote werkstation is geen wachtwoord ingesteld.

Door de gevonden kwetsbaarheden langer uit te buiten kunnen kwaadwillenden de digitale infrastructuur van de gemeente Utrecht verder binnendringen. En door een langere periode mee te kijken met medewerkers kan veel gevoelige informatie worden buitgemaakt. De gegevens van inwoners en ondernemers zijn daarmee onvoldoende beschermd tegen misbruik door derden. Het misbruiken van (bijzondere) persoonsgegevens kan in de persoonlijke levenssfeer grote gevolgen hebben.

4.2.3 RESULTATEN TESTEN WIFI-NETWERKEN EN LAPTOP

De Wifi-netwerken van de gemeente Utrecht hebben de penetratietesten doorstaan.

Het externe bureau heeft een penetratietest uitgevoerd op het WiFi-netwerk van de gemeente Utrecht. Het is de onderzoekers niet gelukt om gebruikersnamen en wachtwoorden op te vangen. Daarnaast is een draadloos netwerk onderzocht waarbij het ook niet is gelukt om het wachtwoord te achterhalen. Daarmee concludeert het externe bureau dat de gemeente Utrecht de beveiliging op dit onderdeel goed op orde heeft.

De gemeente Utrecht weet niet van alle medewerkers of zij thuiswerken met veilige apparatuur. De gemeente heeft bijna 2.500 laptops verstrekt, die worden vanwege de coronacrisis nu veel gebruikt om thuis te werken. Circa 375 laptops (15%) zijn goed beschermd tegen aanvallen in onveilige netwerken en bij diefstal en verlies. De circa 2.100 eerder verstrekte laptops zijn niet allemaal voorzien van de juiste beveiligingsmaatregelen.

Sinds het begin van de coronacrisis zijn de meeste medewerkers van de gemeente Utrecht thuis gaan werken, onder andere met laptops die door de gemeente zijn verstrekt. In februari 2021 waren in totaal bijna 2.500 laptops door de gemeente uitgegeven. Sinds november

2020 worden deze alleen nog beheerd en beveiligd uitgeleverd en nieuwe laptops zijn daarmee beschermd tegen aanvallen in onveilige netwerken en bij diefstal en verlies. Het gaat dan om circa 375 laptops. De rekenkamer heeft een laptop die onlangs aan een van de medewerkers was verstrekt laten onderzoeken door het externe bureau. Daaruit bleek dat het mogelijk is om de laptop vanaf een USB-stick op te starten (laag risico). De harde schijf is voorzien van harddisk encryptie, waarmee de informatie versleuteld is en de inhoud niet bekeken kan worden.

De bijna 2.100 eerder verstrekte laptops zijn, in tegenstelling tot de nieuwe laptops, niet allemaal voorzien van de juiste beveiligingsmaatregelen. Op een deel van deze laptops is sprake van achterstallig onderhoud: er ontbreekt harddiskencryptie en USB-poorten zijn nog toegankelijk.

Medewerkers die geen laptop van de gemeente hebben geleend, werken waarschijnlijk op eigen apparatuur bij het thuiswerken. De gemeente heeft geen zicht op de beveiliging van deze apparatuur, maar biedt medewerkers een virtuele werkomgeving aan om zoveel mogelijk te voorkomen dat gegevens lokaal worden opgeslagen.

Gezien het aantal uitgegeven laptops kan er van uit worden gegaan dat er ook veel medewerkers werken op privé apparatuur. Hiervan is de status van de beveiliging voor de gemeente onbekend. De gemeente hanteert een bring-your-own-device beleid en heeft daarmee minder controle op hoe medewerkers met privé devices omgaan. Dit risico wil de gemeente mitigeren door medewerkers een virtuele werkomgeving aan te bieden. Dit moet zoveel mogelijk voorkomen dat gegevens lokaal worden opgeslagen. Ook zijn er geen eisen gesteld aan de beveiliging van wifi-netwerken bij mensen thuis.

Om in het begin van de coronacrisis de bedrijfscontinuïteit niet te veel te dwarsbomen, heeft de gemeente een aantal veiligheidsrisico's omtrent vergadertools geaccepteerd. Inmiddels zijn er maatregelen genomen om drie vergadertools (*Microsoft Teams*, *Zoom* en *GoToMeeting*) zo veilig mogelijk aan te bieden.[49] Echter, om het netwerk niet te overbelasten, moeten deze vergadertools vooral buiten de werkomgeving worden gebruikt. Hierdoor bestaat het risico dat medewerkers toch buiten de beveiligde werkomgeving blijven werken. Op eigen telefoons en tablets kunnen medewerkers alleen gebruik maken van gemeentelijke informatie als zij de IT beveiligingssoftware van de gemeente accepteren.

[49] Rekenkamer Utrecht. *Interview gemeente Utrecht.*

BIJLAGE 1 AFKORTINGEN

Afkorting	Betekenis
AVG	Algemene Verordening Gegevensbescherming
BCM	Business Continuity Management
BIA	Business Impact Analyse
BIG	Bewust Informatie Gebruiken
BIO	Baseline Informatiebeveiliging Overheid
BSN	Bedrijfsvoerings- en Strategienetwerk
B&W	Burgemeester en wethouders
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
FG	Functionaris Gegevensbescherming
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
IT	Informatietechnologie
MO	Maatschappelijke Ontwikkeling
OOR	Ontwikkelorganisatie Ruimte
ORA	Operationele risicoanalyse
PBZ	Publiekszaken
PRA	Privacy risicoassessment
RO	Raadsorganen
SB	Stadsbedrijven
TRA	Tactische risicoanalyse

UVO	Utrechtse Vastgoed Organisatie
VG	Volksgezondheid
VLG	Veiligheid
VNG	Vereniging van Nederlandse Gemeenten
VTH	Vergunningen, Toezicht en Handhaving
W&I	Werk en Inkomen

BIJLAGE 2 ONDERZOEKSVERANTWOORDING

GERAADPLEEGDE PERSONEN

Gemeente Utrecht, ambtelijke organisatie:

- Leden Stuurgroep Gegevensbescherming
- Leden Regiegroep Gegevensbescherming
- Bedrijfsvoerings- en Strategienetwerk
- IRM Werk en Inkomen
- IRM Utrechtse Vastgoed Organisatie
- Clustermanager Veiligheid
- IPM Publiekszaken
- IPM Veiligheid
- DomstadIT

GERAADPLEEGDE DOCUMENTEN

Gemeentelijke documenten (chronologisch):

- Gemeente Utrecht (september 2014). Strategisch Informatiebeveiligingsbeleid Gemeente Utrecht 2014 – 2018 *"Betrouwbaar en Vertrouwd"*.
- Gemeente Utrecht (september 2014). Tactische Richtlijnen Informatiebeveiliging Gemeente Utrecht *"Betrouwbaar en Vertrouwd".*
- Gemeente Utrecht (14 oktober 2014). Raadsbrief *Concern Informatiebeveiligingsbeleid*. Kenmerk 14.500285.
- Gemeente Utrecht (20 september 2018). *Privacyverordening gemeente Utrecht.*
- Gemeente Utrecht (mei 2019). *Gegevensbescherming in Utrecht*. Jaarverslag van de Functionaris voor Gegevensbescherming Gemeente Utrecht, 2018.
- Gemeente Utrecht (1 juli 2019). Beleid voor gegevensbescherming Gemeente Utrecht 2019 – 2022 *"Bescherming van het digitale DNA van de stad"*.
- Gemeente Utrecht (5 juli 2019). Raadsbrief *Beleid voor gegevensbescherming 2019 – 2022.*
- Gemeente Utrecht (3 september 2019). *Beleid accounts, authenticatiemiddelen en wachtwoorden Gemeente Utrecht.*
- Gemeente Utrecht (19 december 2019). Raadsbrief *Evaluatie jaarverslag functionaris gegevensbescherming.*
- Gemeente Utrecht (z.j.). *Enterprise Mobility Management beleid Gemeente Utrecht.*

Interne documenten Gemeente Utrecht (chronologisch):

- Gemeente Utrecht (24 mei 2018). Gebruikersprotocol Bewust informatie gebruik.
- Gemeente Utrecht (23 mei 2019). GBMS Gemeente Utrecht – Managementsysteem voor gegevensbescherming, *"Bescherming van het digitale DNA van de stad".*
- Gemeente Utrecht (30 januari 2020). Plan Informatiebeheer & Gegevensbescherming 2020 Veiligheid.
- LBVD (17 februari 2020). *Rapportage Phishlink-simulatie.* Gemeente Utrecht.

- Gemeente Utrecht (27 juli 2020). *Aandacht voor integriteit.* Jaarverslag 2019.
- Gemeente Utrecht (19 juni 2020). *Eerste Bestuursrapportage*.
- Gemeente Utrecht (15 september 2020). *Strategische standaard gegevensbescherming – HR-functie*.
- Gemeente Utrecht (november 2020). *Rapportage Gegevensbescherming* november 2020.
- Gemeente Utrecht (24 november 2020). Presentatie '*Strategie bewustwording t.a.v. privacy & gegevensbescherming*'.
- Gemeente Utrecht (27 november 2020). *Datalekmeldingen 2019 en 2020.*
- Gemeente Utrecht (december 2020). *Programma Dasboard 2021*.
- Gemeente Utrecht (1 december 2020). *Risico en Beheersing Matrix – Strategische risico's gegevensbescherming.*
- Gemeente Utrecht (z.j.). *Betrouwbaar werken voor Utrecht. Gedragscode voor iedereen die werkt bij de gemeente Utrecht*.
- Gemeente Utrecht (z.j.). *Informatiebeheer- en beveiligingsplan 2020 Werk en Inkomen*.
- Gemeente Utrecht (z.j.). *Roadmap implementatie gegevensbescherming 2020-2021*.
- Gemeente Utrecht (z.j.). *Roadmap Implementatie gegevensbescherming 2019-2021*.

Andere bronnen:

- Algemene Verordening Gegevensbescherming (AVG)
- Baseline Informatiebeveiliging Overheid (BIO)
- VNG (januari 2019). Baseline *De 10 bestuurlijke principes voor informatiebeveiliging*. Behorende bij de Baseline Informatiebeveiliging Overheid (BIO).

Websites:

- https://www.utrecht.nl/bestuur-en-organisatie/privacy/privacymelding/

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.