Rekenkamer Den Haag

RIS320818

Veilig op afstand

Onderzoek naar de digitale veiligheid van mobiel werken binnen de gemeente Den Haag

Voorwoord

Het gemeentebestuur neemt het afwegen van risico's voor de digitale veiligheid onvoldoende mee in beslissingen over ICT. Dat is in het kort de conclusie van ons onderzoek naar de digitale veiligheid van mobiel werken. De gemeente heeft de afgelopen jaren, net als veel andere organisaties, stevig ingezet op mobiel werken. Dit maakt dat medewerkers van de gemeente lang niet meer altijd op het kantoor werken, maar bijvoorbeeld ook thuis, in de trein of in een café. Binnen de gemeente geldt deze mogelijkheid voor alle personen die gebruik maken van de gemeentelijke ICT. Het gaat hierbij om ambtelijk medewerkers, maar ook bestuurders, raadsleden en externe medewerkers of opdrachtnemers van de gemeente.

De ontwikkeling van mobiel werken is niet zonder risico's. Zo kunnen laptops van medewerkers kwijtraken of gehackt worden, bijvoorbeeld als iemand een niet veilige wifi-verbinding gebruikt. In dit onderzoek hebben we gekeken in hoeverre de gemeente de beveiliging van de toegang tot gemeentelijke systemen en informatie vanaf mobiele werkplekken waarborgt. We hebben hiervoor een technisch onderzoek laten doen naar de beveiliging van de toegang tot gemeentelijke systemen en informatie vanaf mobiele werkplekken. Ook hebben we onderzocht in hoeverre de gemeentelijke organisatie de beveiliging van mobiel werken waarborgt. De uitkomsten van ons onderzoek zijn geen reden tot acute zorg, maar we vonden wel fundamentele aandachtspunten, bijvoorbeeld waar het gaat om een volledig en actueel overzicht van alle gebruikers en gebruikte apparaten bij mobiel werken.

Het college geeft in zijn reactie op ons onderzoek aan de aanbevelingen die wij doen over te nemen en hiermee al aan de slag te zijn. Dat is een goed teken. Wij hopen dat dit onderzoek een positieve bijdrage zal leveren aan de digitale veiligheid van mobiel werken.

H.A. (Manus) Twisk
voorzitter

VEILIG OP AFSTAND

De Rekenkamer Den Haag heeft onderzocht hoe goed de gemeente de toegang tot systemen en informatie vanaf mobiele werkplekken beveiligt. Mobiele werkplekken zijn locaties buiten de vaste kantooromgeving waar werkzaamheden kunnen worden uitgevoerd. De ontwikkeling naar meer mobiel werken brengt risico's met zich mee, waaronder het gebruik van onveilige wifi of privé apparaten.

Deze infographic vat het rapport kort samen.

LEES HET VOLLEDIGE RAPPORT OP ONZE WEBSITE!

rekenkamerdenhaag.nl

Hoofdconclusie

Het gemeentebestuur heeft in het ICT-beleid onvoldoende aandacht voor risico's, waardoor op verschillende niveaus kwetsbaarheden voor mobiel werken bestaan.

Deelconclusie 1

Het gemeentebestuur stuurt in het gevoerde beleid voor ICT onvoldoende op het analyseren en beheersen van risico's.

Onvoldoende afweging van risico's

Onvoldoende inzet op medewerkers-bewustzijn

Deelconclusie 2

De gemeentelijke ICT kent op verschillende niveaus kwetsbaarheden voor de informatiebeveiliging van mobiel werken.

Gebrek aan zicht en grip op het ICT-landschap

Niet alle beveiligings-mogelijkheden benut

Aanbevelingen

De rekenkamer doet aanbevelingen om het herkennen en meewegen van risico's als vast onderdeel mee te nemen in de beleidsontwikkeling en besluitvorming, en de grip op de beveiliging van mobiel werken te versterken.

Inhoudsopgave

1. Inleiding

De Rekenkamer Den Haag heeft onderzocht in hoeverre de gemeente de beveiliging van toegang tot gemeentelijke systemen en informatie vanaf mobiele werkplekken waarborgt. De term 'mobiele werkplekken' verwijst naar alle werkplekken waar werkzaamheden buiten de vaste werkomgeving van de gemeente kunnen worden uitgevoerd.[1] Door de flexibiliteit die mobiel werken biedt, is het voor medewerkers van de gemeente mogelijk om op elke plek en tijdstip hun werk te doen.[2] De ontwikkeling naar meer mobiel werken is niet zonder risico, bijvoorbeeld omdat hierbij ook gebruik gemaakt kan worden van privé apparaten om toegang te krijgen tot gemeentelijke systemen. Het onderzoek richt zich in brede zin op de beveiliging van de toegang tot gemeentelijke systemen en informatie bij het gebruik van mobiele werkplekken. Daarbij is onder meer gekeken naar het gemeentelijke beleid, de organisatie, de gebruikers van mobiele werkplekken, hardware, software en aanvullende voorzieningen.

De centrale onderzoeksvraag van dit onderzoek luidt:

> *In hoeverre waarborgt de gemeente de beveiliging van toegang tot gemeentelijke systemen en informatie vanaf mobiele werkplekken?*

Deze onderzoeksvraag hebben wij beantwoord aan de hand van de volgende deelvragen:

1. *In hoeverre neemt de gemeente de risico's van mobiel werken mee in de ontwikkeling van het informatiebeveiligingsbeleid?*
2. *In hoeverre waarborgt de gemeente medewerkersbewustzijn in het kader van mobiel werken?*
3. *In hoeverre heeft de gemeente overzicht over en grip op het ICT-landschap wat betreft faciliteiten voor mobiel werken?* [3]
4. *In hoeverre waarborgt de gemeente de beveiliging van toegang vanuit mobiele werkplekken met technische maatregelen?*

Een toelichting op de onderzoeksmethoden is opgenomen in bijlagen bijlage 1. De onderzoeksverantwoording is beschreven in bijlage 2.

---

[1] *Handreiking Telewerkbeleid*, Informatiebeveiligingsdienst voor gemeenten, juli 2019, p. 6.
[2] RIS313799, Collegebesluit, *Uitvoeringsdata 2023 digitalisering en dienstverlening,* College van Burgermeester en Wethouders, 29 november 2022.
[3] In dit rapport verwijst het begrip 'ICT-landschap' naar de digitale infrastructuur, de daaraan verbonden apparaten en applicaties die (binnen de gemeente) worden gebruikt en de gebruikers. Voor de volledige begrippenlijst, zie ook bijlage 4.

1.1 Waarom hebben wij dit onderzoek gedaan?

De gemeente Den Haag zet sterk in op meer mobiel werken.[4] De gemeente faciliteert de 'mobiele ambtenaar' door het mogelijk te maken dat medewerkers van de gemeente op elke plek en op elk tijdstip hun werk kunnen doen.[5] Deze ontwikkeling is ten eerste toe te schrijven aan de opkomst van de informatiesamenleving en de groeiende digitalisering binnen gemeenten. Ten tweede evolueert het werkconcept, waarbij steeds vaker tijd- en plaatsonafhankelijk wordt gewerkt.[6] De coronacrisis heeft deze ontwikkeling versneld.

Sinds maart 2019 heeft de gemeente de mogelijkheden voor mobiel werken sterk uitgebreid. De digitale toegang tot gemeentelijke systemen is daarmee verlegd van het voornamelijk werken op gemeentelijke werklocaties naar een werkplek die niet plaatsgebonden is.[7] Medewerkers van de gemeente gebruiken daarbij verschillende mobiele apparaten, zoals smartphones, tablets en laptops, voor het raadplegen of verwerken van gemeentelijke informatie.[8]

Deze ontwikkeling is niet zonder risico's. Het is van belang dat de gemeente de actuele risico's van mobiel werken identificeert en daarop beleid bepaalt met als doel deze risico's te beheersen.[9] Risico's zijn bijvoorbeeld dat mobiele apparaten besmet kunnen raken met malware en daarmee ook de gemeentelijke netwerken infecteren, gebruik maken van onveilige wifi, gestolen worden of zoekraken.[10] Daarnaast worden op de mobiele apparaten ook gegevens en informatie van de gemeente verwerkt en lokaal opgeslagen. Deze informatie is (deels) gevoelig. Gevoelige informatie kan gaan over burgers en bedrijven. Een goede beveiliging van deze informatie is nodig om hun belangen niet te schaden.

Binnen de gemeente is het toegestaan om privé apparaten te gebruiken voor werk.[11] Ook de inzet van deze privé apparaten brengt extra risico's met zich mee. Als er geen afspraken zijn

---

[4] Intern document *Werkplek visie Haagse Digitale Werkomgeving*, 23 februari 2023.
[5] RIS313799, Collegebesluit, *Uitvoeringsdata 2023 digitalisering en dienstverlening,* College van Burgermeester en Wethouders, 29 november 2022.
[6] *Handreiking Mobile Device Management*, Informatiebeveiligingsdienst voor gemeenten, december 2018, p. 6.
[7] Intern document *Werkplek visie Haagse Digitale Werkomgeving*, 23 februari 2023.
[8] *Handreiking Mobile Device Management*, Informatiebeveiligingsdienst voor gemeenten, december 2018, p. 6.
[9] *Handreiking Mobile Device Management*, Informatiebeveiligingsdienst voor gemeenten, december 2018, p. 6.
[10] *Handreiking Mobile Device Management*, Informatiebeveiligingsdienst voor gemeenten, december 2018, p. 6.
[11] Intern document *Regeling gebruik ICT middelen en gemeentelijke informatie 2014*, 7 oktober 2014, artikel 3.4; Dit geldt voor alle medewerkers met een gemeente Den Haag account. Daar vallen bijvoorbeeld ook raadsleden onder.

gemaakt over het gebruik van deze apparaten, heeft de gemeente hier weinig tot geen controle over.[12] Wanneer er bijvoorbeeld geen beveiligingsmaatregelen op privé apparaten worden afgedwongen, kunnen deze apparaten een eenvoudige opstap zijn voor hackers om toegang te krijgen tot systemen van de gemeente.[13] Zo worden op privé apparaten vaker websites bezocht en applicaties gedownload dan op een werklaptop. Het gebruiken van één apparaat voor zowel privé- als zakelijke doeleinden leidt daarmee tot een verhoogd risico, ten opzichte van het scheiden van werk en privé.[14]

1.2 Hoe is dit document opgebouwd?

In het volgende hoofdstuk lichten we onze hoofdconclusie toe. In de daaropvolgende hoofdstukken beschrijven we de deelconclusies en zetten we uiteen op welke bevindingen elke deelconclusie is gebaseerd. In de bijlagen bij dit rapport zijn ten slotte de onderzoeksverantwoording, een toelichting op het normenkader, een begrippenlijst en het overzicht van gebruikte bronnen opgenomen.

[12] *Bring Your Own Device (BYOD*), website Digital Trust Center, (datum onbekend), https://www.digitaltrustcenter.nl/informatie-advies/bring-your-own-device-byod, geraadpleegd op: 21 mei 2024.
[13] *Werk jij op je privélaptop? Wees dan extra alert*, website RTL nieuws, 18 april 2023, https://www.rtl.nl/economie/van-onze-partner/artikel/5378093/cyberupdate-persoonlijke-systemen-hacken?redirect=rtlnieuws, geraadpleegd op: 8 april 2024.
[14] *Werk jij op je privélaptop? Wees dan extra alert*, website RTL nieuws, 18 april 2023, https://www.rtl.nl/economie/van-onze-partner/artikel/5378093/cyberupdate-persoonlijke-systemen-hacken?redirect=rtlnieuws, geraadpleegd op: 8 april 2024.

2. Hoofdconclusie: Het gemeentebestuur heeft in het ICT-beleid onvoldoende aandacht voor risico's, waardoor op verschillende niveaus kwetsbaarheden voor mobiel werken bestaan.

Hoewel de gemeente een risico gebaseerde aanpak als uitgangspunt in het informatieveiligheidsbeleid heeft geformuleerd,[15] besteedt het gemeentebestuur onvoldoende aandacht aan het herkennen en meewegen van risico's in het gevoerde beleid en is de organisatie onvoldoende op deze werkwijze ingericht. Daarnaast zet het college onvoldoende in op het verminderen van de risico's bij de medewerkers. De aanpak om medewerkers bewust en medeverantwoordelijk te maken is vooralsnog vrijblijvend. De onvoldoende aandacht voor risico's brengt kwetsbaarheden met zich mee op het niveau van het beleid en de organisatie voor ICT, en de technische beveiliging van het mobiele werken.

Wij constateren verschillende kwetsbaarheden in de beveiliging van het mobiele werken. De eerste is dat de ambtelijke organisatie geen volledig zicht en grip heeft op alle onderdelen van het ICT-landschap en de gebruikers daarvan. Daardoor loopt de gemeente het risico dat zwakke plekken daarin niet zichtbaar zijn. En dat de gemeente niet tijdig en passend kan reageren op incidenten, omdat informatie niet beschikbaar of niet actueel is. Ten tweede hebben we enkele technische en beheersmatige kwetsbaarheden geconstateerd in de toegangsbeveiliging vanaf mobiele werkplekken. Ten slotte worden medewerkers onvoldoende getraind, waardoor het risico ontstaat dat zij niet de nodige kennis hebben om veilig te werken. Medewerkers zijn immers een belangrijke schakel bij het veilig omgaan met gemeentelijke systemen en informatie.

De hoofdconclusie is gebaseerd op de volgende deelconclusies:

1. Het gemeentebestuur stuurt in het gevoerde beleid voor ICT onvoldoende op het analyseren en beheersen van risico's.
2. De gemeentelijke ICT kent op verschillende niveaus kwetsbaarheden voor de beveiliging van mobiel werken.

De deelconclusies worden in de volgende paragrafen toegelicht.

---

[15] RIS304162, Collegebesluit, *Strategisch Beleidskader Informatieveiligheid 2019-2022*, College van Burgemeester en Wethouders, 18 december 2019.

3. Deelconclusie 1: Het gemeentebestuur stuurt in het gevoerde beleid voor ICT onvoldoende op het analyseren en beheersen van risico's

De gemeente heeft mogelijke risico's voor de beveiliging van de ICT niet structureel inzichtelijk. Daardoor bestaat het risico dat er bedreigingen zijn die onopgemerkt en onbeheerd blijven. Het college heeft namelijk niet gewaarborgd, dat risicoanalyses systematisch onderdeel zijn van het proces van beleidsontwikkeling en besluitvorming over ICT. Daarmee is in de organisatie niet geregeld hoe potentiële risico's worden gesignaleerd en hoe over de beheersing van deze risico's besluiten worden genomen.

Daarnaast constateren we dat het college op onderdelen te kort schiet bij het stimuleren van medewerkersbewustzijn, waardoor de gemeente het risico loopt dat medewerkers zich niet bewust zijn van veiligheidsrisico's of niet veilig werken.[16] Zo stelt het college trainingen voor medewerkers niet verplicht. Daarnaast maakt het college geen specifieke afspraken over mobiel werken om veilig gedrag onder medewerkers te bewerkstelligen.

We baseren de eerste deelconclusie op de volgende twee aspecten.

1. Er mist een formele afweging van de veiligheidsrisico's in het proces van besluitvorming.
2. De gemeente doet onvoldoende aan het bewust en medeverantwoordelijk maken van medewerkers.

Deze worden hierna afzonderlijk toegelicht aan de hand van de bevindingen uit dit onderzoek.

3.1 Er mist een formele afweging van de veiligheidsrisico's in het proces van besluitvorming.

Bevinding 1: er zijn geen (actuele) risicoanalyses gericht op de (informatie) beveiliging van mobiele werkplekken.

De rekenkamer constateert dat er geen (recente) risicoanalyses beschikbaar zijn met betrekking tot (de beveiliging van) mobiele werkplekken. Hiermee loopt de gemeente het risico dat zij geen overzicht heeft van mogelijke nieuwe risico's. Daarnaast zijn de

[16] *Handreiking Telewerkbeleid*, Informatiebeveiligingsdienst voor gemeenten, juli 2019, p. 12.

overwegingen die ten grondslag liggen aan besluiten met betrekking tot mobiel werken niet navolgbaar.

We hebben in het kader van dit onderzoek gevraagd naar de overwegingen die ten grondslag liggen aan besluiten ten aanzien van de geconstateerde opschaling van mobiele werkplekken en de beveiliging daarvan. Specifiek hebben we daarbij gevraagd naar risicoanalyses. We hebben van de ambtelijke organisatie geen onderbouwingen en/of risicoanalyses ontvangen van dit soort besluiten.

De ambtelijke organisatie kon onder meer de onderliggende overwegingen (kosten versus baten) met betrekking tot de keuze om privé apparaten voor zakelijk gebruik toe te staan, niet aanleveren. Datzelfde geldt voor een risicoanalyse die ten grondslag zou moeten liggen aan deze keuze.[17] In dit onderzoek is duidelijk geworden dat de gemeente geen beheersmaatregelen neemt of afdwingt op privé apparaten die worden gebruikt om toegang te krijgen tot gemeentelijke systemen en applicaties.[18] Ook voor mogelijke risico's voortkomend uit deze keuze kon de ambtelijke organisatie geen (expliciete) risicoanalyse overhandigen.[19] Het organisatieonderdeel van de gemeente dat verantwoordelijk is voor ICT-beheer geeft aan dat ze zelfstandig de keuze hebben gemaakt om geen beheersmaatregelen toe te passen op deze apparaten.[20] De ambtelijke organisatie gaf hierbij wel aan dat aan besluiten altijd risico-overwegingen ten grondslag liggen, zoals het wel of niet toelaten van privé apparaten. Tegelijk werd aangegeven dat het besluit om het gebruik van privé apparaten voor zakelijke doeleinden toe te staan lang geleden is genomen, namelijk vóór de opschaling van het mobiele werken als gevolg van de coronapandemie.[21]

Bevinding 2: er is geen formeel proces waarbij risicosignalen leiden tot voorstellen voor beleidsontwikkeling en besluitvorming.

De ambtelijke organisatie signaleert risico's met betrekking tot de beveiliging van de ICT, maar is er geen geformaliseerd proces waarbij risicosignalen leiden tot (voorstellen voor) beleidsontwikkeling en besluitvorming.[22] Het organisatieonderdeel dat risico's signaleert, heeft niet de formele mogelijkheid om deze te agenderen op een managementniveau met voldoende financieel en inhoudelijk mandaat.[23] Dit heeft als gevolg dat het beleid op

[17] E-mail ambtelijke organisatie.
[18] Zie Bevinding: het apparatenbeheer is niet voor alle onderdelen toereikend.
[19] *Rapport Pentest Den Haag*, Hoffmann, 23 november 2023.
[20] Interview ambtelijke organisatie.
[21] Interview ambtelijke organisatie.
[22] Interview ambtelijke organisatie.
[23] Interview ambtelijke organisatie.

onderdelen verouderd is en achterloopt op de ontwikkelingen in de uitvoering. Daarnaast leiden de geconstateerde risico's niet altijd tot aangepaste of nieuwe kaders voor de uitvoeringsorganisatie, of tot een formeel besluit om de (nieuwe) risico's te accepteren.[24] In het kader van dit onderzoek hebben we hiervan meerdere voorbeelden gevonden. In het kader van vertrouwelijkheid geeft de rekenkamer in dit rapport geen gedetailleerde beschrijving van deze voorbeelden.

Voor het centraler organiseren van onder andere het risicomanagement heeft de ambtelijke organisatie een inrichtingsvoorstel opgesteld.[25] Dit is een voorstel voor het oprichten van een apart team binnen het organisatieonderdeel dat verantwoordelijk is voor informatisering en automatisering. Dit team zou onder meer nieuwe ontwikkelingen signaleren en zorgdragen voor een 'soepele en zorgvuldige besluitvorming'.[26] Met dit inrichtingsvoorstel wil de ambtelijke organisatie tegemoetkomen aan het ontbreken van een formeel proces waarin risicosignalen worden vertaald naar voorstellen voor beleid.[27] Het is echter niet duidelijk in hoeverre het voorstel bijdraagt aan het door ons geconstateerde probleem dat voorstellen niet op het juiste managementniveau geagendeerd kunnen worden (zie hierboven). Het voorstel is op het moment van afronden van de uitvoeringsfase van dit onderzoek nog in concept.

Bevinding 3: het proces van delen van informatie over veiligheidsrisico's en het vertalen hiervan in mogelijke technische oplossingen om deze risico's te beheersen, is in de organisatie onvoldoende geborgd.

Binnen de gemeentelijke organisatie zijn verschillende organisatieonderdelen betrokken bij de beveiliging van mobiel werken. Uit de interviews met de ambtelijke organisatie bleek dat deze onderdelen geen regelmatig en formeel contact met elkaar onderhouden.[28] Dit beperkt de kennisuitwisseling tussen organisatieonderdelen die zich bezighouden met beleidsontwikkeling en risicosignalering, en organisatieonderdelen die actief zijn in de uitvoering. Hiermee ontbreekt een formele structuur voor het identificeren en beheersbaar maken van risico's tussen verschillende aspecten van de voor informatiebeveiliging verantwoordelijke teams binnen de ambtelijke organisatie. Een gevolg daarvan is dat de

[24] Interview ambtelijke organisatie.
[25] Intern document *Digitale Strategie & Informatiebeleid Inrichtingsvoorstel (draft)*, als ontvangen op 13 februari 2024.
[26] Intern document *Digitale Strategie & Informatiebeleid Inrichtingsvoorstel (draft)*, als ontvangen op 13 februari 2024.
[27] Intern document *Digitale Strategie & Informatiebeleid Inrichtingsvoorstel (draft)*, als ontvangen op 13 februari 2024.
[28] Interview ambtelijke organisatie.

Chief Information Security Officer (CISO) van de gemeente afhankelijk is van informele contacten om volledig zicht te krijgen op de technische mogelijkheid om risico's beheersbaar te maken.[29]

Bevinding 4: de gemeente heeft geen specifiek beleid voor de beveiliging van mobiele werkplekken.

De gemeente heeft aandacht voor de ontwikkelingen van mobiel werken. Ze investeert bijvoorbeeld in het opleveren van een mobiele werkplek die overal toegang geeft tot de gemeentelijke systemen en benodigde informatie.[30] Zo zijn er steeds meer applicaties toegankelijk gemaakt via het internet, zodat medewerkers op elke plek en op elk tijdstip kunnen werken.[31] Daarnaast zijn ook vanaf 2024 alle vaste werkplekken vervangen door een 'WOW'-plek (zie toelichting hieronder), waarbij gebruik gemaakt wordt van een laptop, die ook thuis of op andere locaties gebruikt kan worden.[32]

Het ontbreekt echter aan beleid voor de beveiliging van het mobiel werken.[33] Mobiel werken is bijvoorbeeld niet meegenomen in het strategisch beleidskader voor informatieveiligheid.[34] De *'Visie voor digitalisering en dienstverlening'* en de *'Agenda digitaal veilig Den Haag'* bieden ook geen kaders ten behoeve van (veilig) mobiel werken.[35]

Uit ons onderzoek blijkt daarnaast, dat het voor de IT-organisatie die verantwoordelijk is voor de uitvoering ontbreekt aan (beleids-) kaders voor beveiliging van de gemeentelijke ICT. Initiatieven voor de invoering van nieuwe technieken komen vaak vanuit deze uitvoeringsorganisatie zelf, zonder dat hiervoor richtinggevende kaders zijn opgesteld.[36]

---

[29] Interview ambtelijke organisatie.
[30] RIS305017, Raadsvoorstel, *Masterplan IT*, College van Burgemeester en Wethouders, 1 april 2020.
[31] RIS313799, Collegebesluit, *Uitvoeringsdata 2023 digitalisering en dienstverlening,* College van Burgermeester en Wethouders, 29 november 2022.
[32] *2.600 vaste computers worden vervangen door werkplekken voor laptops*, interne website Gemeente Den Haag, 18 januari 2024, https://denhaag.sharepoint.com/sites/DenHaagNieuws/SitePages/2.600-vaste-computers-worden-vervangen-door-werkplekken-voor-laptops.aspx, geraadpleegd op: 20 februari 2024.
[33] De rekenkamer constateert dit op een analyse van alle relevantie beleidsdocumenten met betrekking tot de ICT en de informatiebeveiliging van de gemeente. Zie voor een overzicht van geanalyseerde documenten de bronnenlijst bij dit onderzoek.
[34] RIS304162, Collegebesluit, *Strategisch Beleidskader Informatieveiligheid 2019-2022*, College van Burgemeester en Wethouders, 18 december 2019.
[35] RIS305093, Commissiebrief, Visie op digitalisering en dienstverlening 2020-2023, College van Burgemeester en Wethouders, 14 juli 2020.
[36] Interview ambtelijke organisatie.

De WOW-plek[37]

De WOW-plek (werk en ontmoeten werkplek) is de werkplek waarop je een laptop kan aansluiten. Hierdoor kan er met één apparaat op elke locatie worden gewerkt. De WOW-plek bestaat uit twee beeldschermen, een toetsenbord en een muis. De WOW-plek is een vervanging van de vaste werkplek met desktopcomputer op de gemeentelijke locaties.[38]

3.2 De gemeente doet onvoldoende aan het bewust en medeverantwoordelijk maken van medewerkers.

Bevinding 5: de gemeente besteedt in de (beleids-)kaders voor het gedrag van medewerkers geen specifieke aandacht aan mobiel werken.

De gemeente heeft geen regels ten aanzien van telewerken (mobiel) werken en maakt geen specifieke afspraken met medewerkers die op privé apparaten werken.[39]

De gemeente zet echter wel sterk in op een verschuiving naar mobieler werken. In de '*Werkplekvisie 2023*' geeft de gemeente bijvoorbeeld aan dat ze bezig is met het optimaal faciliteren van de mobiele ambtenaar.[40] Dit betekent onder andere dat er gezorgd wordt dat medewerkers makkelijk mobiel toegang kunnen hebben tot de informatie en systemen die ze nodig hebben om hun werk uit te voeren.[41] Daarnaast worden vanaf 2024 alle vaste werkplekken vervangen door de eerder beschreven 'WOW-plek', waarbij gewerkt wordt met een laptop, die zowel op kantoor als thuis of op andere locaties gebruikt kan worden.[42]

Desondanks heeft de gemeente in het personeelsreglement geen (gedrags-)regels opgenomen ten behoeve van mobiel werken. De gemeente heeft wel een handreiking voor hybride werken samengesteld, waarin ze vijf regels heeft opgenomen voor het veilig hybride

---

[37] Voor de volledige begrippenlijst, zie bijlage 4
[38] Gebruikershandleiding WOW!, interne website gemeente Den Haag, (datum onbekend), https://denhaag.sharepoint.com/sites/hetplein/SitePages/Gebruikershandleiding-WOW.aspx?web=1, geraadpleegd op 23 april 2024.
[39] Interview ambtelijke organisatie.
[40] Intern document *Werkplek visie Haagse Digitale Werkomgeving*, 23 februari 2023.
[41] Intern document *Werkplek visie Haagse Digitale Werkomgeving*, 23 februari 2023.
[42] *2.600 vaste computers worden vervangen door werkplekken voor laptops*, interne website Gemeente Den Haag, 18 januari 2024, https://denhaag.sharepoint.com/sites/DenHaagNieuws/SitePages/2.600-vaste-computers-worden-vervangen-door-werkplekken-voor-laptops.aspx, geraadpleegd op: 20 februari 2024.

werken.[43] De regels gaan bijvoorbeeld over het gebruiken van een beveiligd netwerk en het niet uitprinten van vertrouwelijke informatie. Ook hierin staan echter geen beveiligingseisen voor privé apparaten, zoals het beveiligen met een wachtwoord of pincode, het hebben van een virusscanner en anti-malware programma's.

Bevinding 6: de gemeente biedt (bewustzijns)trainingen aan, maar deze zijn vrijwillig en dus niet verplicht.

De gemeente biedt vrijblijvende trainingen voor onder andere informatiebeveiliging. Een analyse van de beschikbare trainingen door de rekenkamer laat zien, dat er een algemene training bestaat voor digitale vaardigheden, een training voor veilig omgaan met persoonsgegevens en een training voor mobiel werken. Deze laatste richt zich meer op mobiel werken in het algemeen dan informatieveiligheid. Uit een analyse van de rekenkamer blijkt ook dat de volgens de BIO verplichte I-bewustzijn training van de VNG (zie toelichting hieronder), niet door de gemeente wordt aangeboden.

De gemeente is van plan actiever trainingen aan te gaan bieden en deze (deels) verplicht te maken. Tijdens de looptijd van dit onderzoek is de commissiebrief '*Governance Digitale veiligheid'* gepubliceerd. Hierin zegt het college toe te werken aan een verplichte training om de medewerkers van de gemeente bewust te maken van de verantwoordelijkheden die zij hebben op het gebied van informatieveiligheid.[44]

Toelichting I-bewustzijnstraining VNG

De I-bewustzijn opleiding is een kosteloze online training ontworpen om de informatieveiligheid te bevorderen door het bewustzijn van medewerkers te verhogen.[45] De training wordt aangeboden door de VNG in samenwerking met het Ministerie van Binnenlandse Zaken en de Taskforce Bestuur en Informatieveiligheid Dienstverlening.[46] Volgens artikel 7.2.2.2 van de Baseline Informatiebeveiliging Overheid dienen alle

[43] Intern document *Handreiking Hybride werken, voor medewerkers en leidinggevenden*, April 2023, p. 7. Deze handreiking is niet bindend en wordt niet opgenomen in gedragsregels.
[44] RIS317224 Commissiebrief *Governance Digitale Veiligheid*, College van Burgemeester en Wethouders, 7 december 2023.
[45] *iBewustzijn Overheid Bewust en veilig omgaan met (digitale) informatie!,* website VNG, datum onbekend, https://www.vngconnect.nl/academie/Training/ibewustzijn-overheid-bewust-en-veilig-omgaan-met-digitale-informatie/edd25b97-95d3-4ce8-ac63-b26dccd91e4e geraadpleegd op: 28 maart 2024.
[46] *iBewustzijn Overheid Bewust en veilig omgaan met (digitale) informatie!,* website VNG, datum onbekend, https://www.vngconnect.nl/academie/Training/ibewustzijn-overheid-bewust-en-veilig-omgaan-met-digitale-informatie/edd25b97-95d3-4ce8-ac63-b26dccd91e4e geraadpleegd op: 28 maart 2024.

medewerkers die gebruikmaken van de informatiesystemen- en diensten binnen drie maanden na indiensttreding de training I-bewustzijn succesvol gevolgd te hebben.[47]

4. Deelconclusie 2: De gemeentelijke ICT kent op verschillende niveaus kwetsbaarheden voor de informatiebeveiliging van mobiel werken

Naast het onder deelconclusie 1 genoemde risico dat medewerkers onvoldoende bewust zijn van veiligheidsrisico's, zitten in de beveiliging van mobiel werken op twee niveaus kwetsbaarheden.

Allereerst constateren we dat het binnen de gemeentelijke organisatie ontbreekt aan zicht en grip op het gehele ICT-landschap. Hierdoor loopt de gemeente het risico dat relevante informatie niet beschikbaar is wanneer dat nodig is, bijvoorbeeld bij incidenten rond de beveiliging van ICT.[48] Zo heeft de organisatie geen centraal en actueel overzicht van applicaties, eigenaren van applicaties, gebruikers, apparaten en toegangsrechten. Hierdoor is niet altijd duidelijk wat de gevolgen zijn wanneer een applicatie of systeem bij een incident of onderhoud tijdelijk uitgeschakeld moet worden.

Ook benut het college niet alle beschikbare technische mogelijkheden om de toegang tot gemeentelijke applicaties en systemen te beveiligen. Hoewel uit ons onderzoek geen acute bedreigingen naar voren kwamen bij de beveiliging van mobiel werken, constateren we wel een aantal tekortkomingen die een risico opleveren. Zo heeft de gemeente de toegangsbeveiliging niet in alle gevallen eenduidig en afdoende gewaarborgd en is het beheer van mobiele apparaten niet voor alle onderdelen toereikend.

Wij baseren deze deelconclusie, in combinatie met het onder deelconclusie 1 benoemde risico met betrekking tot medewerkersbewustzijn, op de volgende twee aspecten.

1. De gemeentelijke organisatie heeft onvoldoende zicht en grip op het ICT-landschap
2. De gemeente maakt onvoldoende gebruik van bestaande technische mogelijkheden om de toegang tot gemeentelijke applicaties en systemen te beveiligen

Deze worden hierna afzonderlijk toegelicht aan de hand van de bevindingen uit dit onderzoek.

---

[47] *Baseline informatiebeveiliging overheid*, 2020, artikel 7.2.2.1.
[48] *Handreiking Samenhang Beheerprocessen en Informatiebeveiliging*, Informatiebeveiligingsdienst voor gemeenten, juni 2019, p. 12

4.1 De gemeentelijke organisatie heeft onvoldoende zicht en grip op het ICT-landschap.

Bevinding 7: de gemeente beschikt over een centraal overzicht van de gemeentelijke apparaten.

De gemeente heeft een centraal overzicht van welke laptops, telefoons en tablets er door de gemeente zijn uitgegeven aan medewerkers.[49] In dit overzicht kan de gemeente ook zien wie de eigenaar is, op welk systeem het apparaat draait en wanneer deze voor het laatst is gebruikt.

Bevinding 8: de gemeente heeft geen centraal overzicht van de privé apparaten die gebruikt worden voor zakelijke doeleinden.

Uit ons onderzoek werd duidelijk dat privé apparaten (computers, laptops, tablets) die zakelijk worden gebruikt, niet centraal worden geregistreerd.[50] Voor de privé apparaten heeft de gemeente wel de mogelijkheid om in te zien welke apparaten zijn ingelogd op de gemeentelijke systemen.[51] De ambtelijke organisatie gaf echter aan op dit moment geen gebruik van te maken van deze mogelijkheid.[52]

De rekenkamer heeft daarnaast een overzicht van de ambtelijke organisatie ontvangen met geregistreerde privé apparaten. Dit ging echter alleen om mobiele telefoons.

Bevinding 9: er is geen compleet en actueel overzicht van alle applicaties die de mobiel te benaderen zijn en de interne eigenaren hiervan.

Verschillende afdelingen houden applicaties op uiteenlopende manieren bij.[53] De gemeente gebruikt hiervoor een configuratiemanagement-database (CMDB, zie toelichting hieronder). Hierin houdt het gemeentelijke ICT-beheer applicaties bij die op de servers van de gemeente

[49] Intern document *All Apple devices*, als ontvangen op 13 november 2023; Intern document *All Android devices*, als ontvangen op 13 november 2023; Intern document *All Windows devices*, als ontvangen op 13 november 2023.
[50] Interview ambtelijke organisatie.
[51] In het overzicht zijn 206 mobiele telefoons opgenomen. Privé mobiele telefoons die door medewerkers van de rekenkamer worden gebruikt, staan niet in het overzicht.
[52] Interview ambtelijke organisatie.
[53] E-mail ambtelijke organisatie.

draaien.[54] Van de applicaties die niet op de servers van de gemeente draaien, is er geen sluitend overzicht. Dat betekent dat er geen compleet en actueel overzicht is van de applicaties die via het internet vanaf mobiele werkplekken te benaderen zijn (Software as a Service).[55]

Daarnaast is er binnen de gemeente geen actueel en compleet overzicht over de eigenaren van applicaties. Binnen de gemeente is de eigenaar de verantwoordelijke voor het feit dat een applicatie in gebruik is genomen of gebruikt wordt. De organisatie heeft geen centraal sluitend beeld van de eigenaren van applicaties (zowel intern als via het internet te benaderen).[56] De rekenkamer heeft tweemaal een overzicht gevraagd van belangrijkste applicaties met onder meer gegevens over eigenaarschap.[57] In eerste instantie ontvingen we een incompleet overzicht waarvan de informatie over eigenaren verouderd was.[58] Vervolgens leverde de ambtelijke organisatie een handmatig opgesteld overzicht aan bij de rekenkamer.[59] Dit overzicht is daarmee eenmalig en niet representatief voor wat de ambtelijke organisatie direct beschikbaar heeft.

Door het ontbreken van (complete) overzichten van applicaties en eigenaren van applicaties kan onder meer bij het aanpassen van systemen niet altijd worden ingeschat welke gevolgen deze aanpassingen hebben voor de functionaliteit van applicaties. Het is bijvoorbeeld niet altijd duidelijk wie benaderd moet worden met betrekking tot gewenste wijzigingen van een specifieke applicatie.[60]

Toelichting Configuratiemanagement Data Base (CMDB)
De CMDB is een database die alle relevante informatie bevat over de elementen die beheerd en gecontroleerd moeten worden (zoals hardware en software) in de IT-infrastructuur.[61] Het doel van een CMDB is om een georganiseerd en gestructureerd overzicht te bieden van de

[54] E-mail ambtelijke organisatie.
[55] E-mail ambtelijke organisatie.
[56] Interview ambtelijke organisatie.
[57] E-mail ambtelijke organisatie; Intern document *rekenkamer*, als ontvangen op 15 november 2023; Intern document *Applicaties voor rekenkamer*, ontvangen op 22 november 2023.
[58] Intern document *rekenkamer*, als ontvangen op 15 november 2023.
[59] E-mail ambtelijke organisatie; Intern document *Applicaties voor rekenkamer*, ontvangen op 22 november 2023.
[60] Interview ambtelijke organisatie.
[61] *Handreiking configuratiemanagement*, Informatiebeveiligingsdienst voor gemeenten, februari 2020, p. 8.

ICT-middelen van een organisatie, waardoor het gemakkelijker wordt om configuraties te beheren en bijvoorbeeld problemen op te lossen en wijzigingen door te voeren.[62]

Bevinding 10: er is geen compleet en actueel overzicht van toegangsrechten van gebruikers van applicaties.

Voor de meerderheid van applicaties maakt de gemeente gebruik van beveiligingsgroepen (zie toelichting hieronder) die door eigenaren van afzonderlijke applicaties worden aangemaakt.[63] Het bijhouden en beheren van toegangsrechten is hiermee decentraal belegd via de betrokken manager of applicatie eigenaar.[64] De ambtelijke organisatie gaf aan dat autorisatiebeheer daarmee 'op de achtergrond' loopt, namelijk voor elke applicatie afzonderlijk.[65] Er is hiermee geen eenduidige werkwijze voor het verlenen van toegangsrechten (oftewel autorisaties), waardoor er centraal geen werkbaar overzicht van de beveiligingsgroepen bestaat.[66]

Concreet heeft dit als gevolg dat het ICT-beheer geen zicht heeft op de autorisatiemodellen van alle applicaties.[67] Het beheer heeft geen inzage of controle over het autorisatiebeleid van elke applicatie. Daarbij is het ook niet mogelijk om regelmatig audits uit te voeren, omdat de autorisaties de verantwoordelijkheid zijn van de eigenaar van de applicatie. [68]

Daarnaast gebruikt de gemeente verschillende authenticatiemodellen en bestaat hier geen centraal overzicht van.[69] Hierdoor heeft de gemeente heeft geen volledig zicht op de authenticatiemodellen van alle applicaties in haar ICT-landschap.[70] Hierdoor kan de gemeente niet overzien of alle applicaties voldoen aan de normen van authenticatie en loopt zij het risico dat er mogelijk applicaties zijn die niet aan haar normen voldoen.

Toelichting beveiligingsgroepen
Wanneer iemand toegang krijgt tot een applicatie, dat wil zeggen wanneer iemand een autorisatie wordt toegekend, wordt diens account toegevoegd tot een beveiligingsgroep.

---

[62] *Handreiking configuratiemanagement*, Informatiebeveiligingsdienst voor gemeenten, februari 2020, p. 8.
[63] E-mail ambtelijke organisatie.
[64] Met beheer wordt het 'technisch beheren' van de beveiligingsgroepen bedoeld. Beheerders zijn niet altijd eigenaren en vice versa.
[65] Interview ambtelijke organisatie.
[66] Interview ambtelijke organisatie.
[67] Interview ambtelijke organisatie.
[68] Interview ambtelijke organisatie.
[69] In het kader van vertrouwelijkheid geeft de rekenkamer in dit rapport geen beschrijving over welke applicaties dit gaat.
[70] Interview ambtelijke organisatie.

Iedereen in één beveiligingsgroep heeft toegang tot een hieraan gekoppelde applicatie. In theorie is er met dit systeem een overzicht van alle verleende toegangsrechten voor alle applicaties. In de praktijk is dit overzicht echter niet eenvoudig en beheersbaar. Uit het overzicht van beveiligingsgroepen is bijvoorbeeld niet eenduidig te herleiden op welke applicaties de beveiligingsgroepen betrekking hebben. Als gevolg hiervan is het in de praktijk ook niet veilig om groepen te bewerken of te verwijderen. Hierdoor is het totaal aan beveiligingsgroepen opgelopen tot circa 60.000.[71]

4.2 De gemeente maakt onvoldoende gebruik van bestaande technische mogelijkheden om de toegang tot gemeentelijke applicaties en systemen te beveiligen

Bevinding 11: de beveiliging van mobiele werkplekken kent in de praktijk een beperkt aantal kwetsbaarheden.

Uit het praktijkonderzoek door een extern onderzoeksbureau kwamen verschillende bevindingen naar voren met betrekking tot de toegangsbeveiliging. [72] Dit bureau heeft de ernst van de gevonden kwetsbaarheden beoordeeld aan de hand van een CVSS-score (zie toelichting onderaan).

Voor het grootste deel heeft de gemeente de beveiliging van informatie technisch goed geregeld. Een groot deel van de bevindingen uit het rapport van het externe onderzoeksbureau is dan ook informatief. Deze bevindingen hebben geen directe gevolgen voor de kwetsbaarheid van de organisatie. Zes bevindingen vallen onder de classificatie ‘laag’. Dit betekent dat deze kwetsbaarheden een relatief klein effect hebben op de veiligheid van de systemen.[73] Drie bevindingen worden geclassificeerd als ‘gemiddeld’ en het praktijkonderzoek duidde op één bevinding met een hoge mate van ernst. [74] We hebben de ambtelijke organisatie geïnformeerd over de bevindingen van dit externe onderzoek en de daaraan verbonden risico’s. De bevindingen van het technisch onderzoek worden in dit feitenrapport niet in detail opgenomen gezien de gevoeligheid van de informatie.

[71] Interview ambtelijke organisatie.
[72] *Rapport Pentest Den Haag*, Hoffmann, 23 november 2023.
[73] *Rapport Pentest Den Haag*, Hoffmann, 23 november 2023, p. 14.
[74] *Rapport Pentest Den Haag*, Hoffmann, 23 november 2023.

De gemeente heeft in februari 2024 zelf ook een technisch onderzoek laten doen naar de beveiliging van laptops uitgegeven door de gemeente. Uit dit technisch onderzoek van de gemeente komen vijf bevindingen waarvan vier worden beoordeeld met een hoog risico. De bevindingen uit dit onderzoek kwamen grotendeels overeen met bevindingen in het externe onderzoek van de rekenkamer. De bevindingen zijn in het eigen onderzoek van de gemeente met een hoger ernst beoordeeld dan in het onderzoek van de rekenkamer, ondanks het gebruik van hetzelfde CVSS-classificatiesysteem.[75] De rekenkamer heeft niet kunnen achterhalen waar dit verschil in risicobeoordeling vandaan komt.

Toelichting CVSS-score

De 'Common Vulnerability Scoring System' (CVSS) is een scoringsmethode die gebruikt wordt als kwalitatieve maatstaf voor het aangeven van de ernst van een kwetsbaarheid. De CVSS-score is een weging van de ernst van een bevinding. Hierbij wordt gekeken naar de mate waarin een gevonden kwetsbaarheid benut kan worden door kwaadwillenden en naar de impact die het benutten van een kwetsbaarheid zou hebben.[76]

Bevinding 12: het apparatenbeheer is niet voor alle onderdelen toereikend.

Uit het praktijkonderzoek van de rekenkamer blijkt dat de gemeente momenteel geen volledig beheer heeft op alle apparaten. Het apparatenbeheer is op verschillende onderdelen ontoereikend. Voor het beheren van enkele onderdelen, mist het ook aan de nodige afspraken en regels.[77] Hierdoor loopt de gemeente het risico dat zij zwakke plekken in haar ICT-landschap niet overziet. In het kader van vertrouwelijkheid geeft de rekenkamer in dit rapport geen beschrijving over welke onderdelen dit gaat.

Bevinding 13: niet voor alle applicaties heeft de gemeente zeker gesteld dat er gebruik wordt gemaakt van multi-factor authenticatie.

In het externe praktijkonderzoek van de rekenkamer zijn er vier categorieën van applicaties geïdentificeerd. In drie van de vier categorieën wordt er direct via de applicatie of indirect via de Virtuele Desktop Infrastructuur (VDI)[78] gebruik gemaakt van multi-factor authenticatie (MFA, zie toelichting hieronder).[79] Indirect wil hier zeggen dat MFA gebruikt wordt om

[75] Het technisch onderzoek van de gemeente achterhaalt vijf bevindingen waarvan vier worden beoordeeld met een hoog risico.
[76] *Rapport Pentest Den Haag*, Hoffmann, 23 november 2023.
[77] Interview ambtelijke organisatie.
[78] De ICT-infrastuctuur waarmee je virtueel toegang kan krijgen tot het (besturings)systeem [van de gemeente]. Voor nadere toelichting, zie bijlage 4.
[79] *Rapport Pentest Den Haag*, Hoffmann, 23 november 2023.

toegang te krijgen tot de VDI-omgeving. Van daaruit is het niet nodig in de applicatie zelf opnieuw in te loggen. Van de vierde categorie is er geen sluitend beeld. Deze applicaties draaien buiten de servers van de gemeente en zijn niet centraal gekoppeld aan het systeem. Het is van een specifieke applicatie afhankelijk welke toegangsbeveiligingsbeleid van toepassing is.[80] De ambtelijke organisatie gaf aan dat er geen beeld is van het toegangsbeveiligingsbeleid van deze categorie van applicaties.[81]

Toelichting MFA

Multi-factor authenticatie (MFA) is een beveiligingsmethode die vereist dat gebruikers twee of meer verificatiefactoren verstrekken om toegang te krijgen tot een applicatie of account. MFA verhoogt de beveiliging door naast een gebruikersnaam of wachtwoord te vragen om een extra verificatie met bijvoorbeeld een applicatie.[82] Dit zorgt ervoor dat (potentiële) kwaadwillenden niet met alleen een gebruikersnaam en wachtwoord toegang hebben.[83] Volgens de BIO moet MFA van toepassing zijn wanneer er vanuit een 'onvertrouwde zone' toegang wordt verleend naar een 'vertrouwde zone'.[84]

Bevinding 14: gebruikerssessies worden niet eenduidig beheerd en vormen in sommige gevallen een beveiligingsrisico.

Er wordt geen onderscheid gemaakt tussen gemeentelijke en privé apparatuur wat betreft de duur van login sessies. Dit vormt in sommige gevallen een beveiligingsrisico. In het kader van de vertrouwelijkheid geeft de rekenkamer in dit rapport geen beschrijving over welke beveiligingsrisico's dit gaat. Er is geen eenduidig beeld van het tijdsblok waarvoor gebruikerssessies actief blijven. In het praktijkonderzoek van de rekenkamer zijn zowel laptops van de externe onderzoekers als van de staf van de rekenkamer gebruikt om de geldigheidsduur van gebruikerssessies te analyseren. Hieruit is gebleken dat de sessies beïnvloed worden door verschillende factoren zoals de browser en het apparaat.[85]

[80] *Rapport Pentest Den Haag*, Hoffmann, 23 november 2023.
[81] Interview ambtelijke organisatie.
[82] *What is: Multifactor Authentication*, website Microsoft, (datum onbekend), https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661, geraadpleegd op 28 maart 2024.
[83] Handreiking *2-Factor authenticatie (2FA) voor gemeenten,* Informatiebeveiligingsdienst voor gemeenten, oktober 2020, p.7.
[84] *Baseline informatiebeveiliging overheid,* 2020, artikel 9.4.2.1.
[85] *Rapport Pentest Den Haag*, Hoffmann, 23 november 2023.

5. Aanbevelingen

We formuleren op basis van de conclusies uit dit onderzoek vier aanbevelingen. Deze aanbevelingen hebben als doel het herkennen en meewegen van risico's als vast onderdeel mee te nemen in de beleidsontwikkeling en besluitvorming, en om de grip op de beveiliging van mobiel werken te versterken.

Aanbeveling 1: Draag het college op het ICT-beleid en de ICT-organisatie te herzien en daarbij:

a. de inventarisatie en analyse van mogelijke risico's voor de beveiliging van ICT integraal onderdeel te maken van de besluitvorming.

Het doel van deze aanbeveling is te waarborgen dat risicomanagement structureel onderdeel uitmaakt van het organiseren van de digitale veiligheid. Het college dient de inventarisatie en analyse van risico's integraal mee te nemen in het proces van beleidsontwikkeling en besluitvorming op het gebied van ICT. Dit betekent dat risico's geïdentificeerd, beoordeeld en beheerst moeten worden.[86] Hierdoor heeft de gemeente beter inzicht in mogelijke bedreigingen en zwakke plekken en kan de gemeente verantwoording afleggen over gemaakte keuzes.[87]

In ons onderzoek constateren we dat er geen risicoanalyses zijn gemaakt voor verschillende aspecten van mobiel werken en dat het college geen formeel proces heeft ingericht waarin risicosignalen leiden tot besluiten. Mede als gevolg hiervan kent de beveiliging van mobiel werken kwetsbaarheden op verschillende niveaus.

b. beleid voor mobiel werken en de beveiliging daarvan op te stellen en uit te dragen.

Het doel van deze aanbeveling is te waarborgen dat de gemeente voorbereid is op de risico's voor de veiligheid van mobiel werken en de mogelijkheid heeft om deze te beheren. Mobiel werken en mobiele apparaten kunnen namelijk risico's met zich meebrengen: de apparaten kunnen bijvoorbeeld gebruik maken van onveilige wifi of zoekraken (zie ook de aanleiding van dit onderzoek). Specifiek beleid voor mobiel werken helpt om ervoor te zorgen dat er

[86] *Baseline informatiebeveiliging overheid*, 2020, p. 9.
[87] *Baseline Informatieveiligheid Overheden*, 2020, p. 9.

veilig wordt omgegaan met mobiele apparaten en de gemeentelijke gegevens die erop kunnen staan.[88]

Uit ons onderzoek is gebleken dat het college geen beleid heeft bepaald waarin is vastgelegd hoe er wordt omgegaan met de risico's van mobiele apparatuur en mobiel werken. Mede als gevolg hiervan ontbreekt het voor de organisatie die verantwoordelijk is voor de uitvoering van ICT-beleid ook aan (beleids-)kaders.

c. informatie-uitwisseling over beveiligingsrisico's en mogelijke beheersmaatregelen binnen de organisatie te reguleren.

Het doel van deze aanbeveling is het waarborgen van informatie-uitwisseling tussen de verschillende afdelingen die betrokken zijn bij het beveiligen van de ICT binnen de gemeente en het beter positioneren van de Chief Information Security Officer (CISO) binnen die informatie-uitwisseling. Op deze manier kan de gemeente waarborgen dat relevante informatie met alle betrokken partijen via formele kanalen worden gedeeld.

Uit ons onderzoek is gebleken dat de kennisuitwisseling tussen de verschillende organisatieonderdelen die betrokken zijn bij (de beveiliging van) de ICT, geen formeel contact of contactmogelijkheid hebben. Hierdoor zijn betrokkenen, waaronder de CISO, afhankelijk van informele informatiedeling.

d. een compleet en centraal overzicht op te stellen van het gemeentelijk ICT-landschap en dit overzicht te beheren.

Het doel van deze aanbeveling is het waarborgen van het zicht en grip van de gemeente op het gehele ICT-landschap. Wanneer de gemeentelijke organisatie een compleet en actueel overzicht heeft, krijgt zij beter grip op mogelijke kwetsbaarheden en risico's in het ICT-landschap.[89] En kan de gemeentelijke organisatie doeltreffender ingrijpen, wanneer dat

---

[88] *Handreiking Mobile Device Management*, Informatiebeveiligingsdienst voor gemeenten, december 2018, p. 6

[89] *Bring Your Own Device (BYOD*), website Digital Trust Center, (datum onbekend), https://www.digitaltrustcenter.nl/informatie-advies/bring-your-own-device-byod, geraadpleegd op: 21 mei 2024.

nodig is.[90] Het is ook van belang dat het college borgt dat informatie in de overzichten actueel wordt gehouden.[91]

In ons onderzoek constateren we dat het overzicht van de gemeentelijke organisatie op het gehele ICT-landschap niet compleet is. Hierdoor loopt de organisatie het risico dat zij geen zicht heeft op alle (mogelijke) zwakke punten in het ICT-landschap en dat informatie niet beschikbaar is wanneer dat nodig is.

Aanbeveling 2: Draag het college op medewerkers van de gemeente bewust en medeverantwoordelijk te maken voor de veiligheid van mobiel werken

Het doel van deze aanbeveling is het waarborgen van de beveiliging van mobiel werken door het bewust en medeverantwoordelijk maken van medewerkers voor het informatiebeveiligingsbeleid. Medewerkers van de gemeente horen op de hoogte te zijn van de beveiligingsrisico's van de informatie en systemen waarmee ze werken en proactief stappen te ondernemen om deze risico's te verminderen.[92] De rekenkamer beveelt daarom aan gebruik te maken van diverse instrumenten, zoals verplichte trainingen en aanvullende afspraken om te waarborgen dat medewerkers beveiligingsbewust en veilig werken. Wanneer medewerkers niet bewust zijn van de regels, loopt de gemeente het risico op schade door (onbewust) handelen van medewerkers.[93] Middels de inzet van diverse instrumenten op het gebied van medewerkersbewustzijn kan het college de beveiliging van mobiel werken verbeteren.[94]

In ons onderzoek constateerden we dat de gemeente momenteel in beleidskaders voor het gedrag van medewerkers geen specifieke aandacht besteed aan mobiel werken en dat deelname aan de door de gemeente aangeboden trainingen vrijwillig is.

---

[90] Bedrijfsmiddelen-inventaris, website Nederlandse Overheid Referentie Architectuur, 22 november 2021, https://www.noraonline.nl/wiki/ISOR:Bedrijfsmiddelen_inventaris, geraadpleegd op: 6 mei 2024.
[91] *Eigenaarschap Huisvesting IV*, website Nederlandse Overheid Referentie Architectuur, 22 november 2021, https://www.noraonline.nl/wiki/ISOR:Eigenaarschap, geraadpleegd op: 19 september 2024.
[92] *Handreiking Telewerkbeleid*, Informatiebeveiligingsdienst voor gemeenten, juli 2019, p. 11 en 12.
[93] https://www.noraonline.nl/wiki/ISOR:Training_en_Awareness
[94] *Personeelsbeleid gemeente*, Informatiebeveiligingsdienst voor gemeenten, mei 2020.

Aanbeveling 3: Draag het college op bestaande technische mogelijkheden voor toegangsbeveiliging beter te benutten, om zo de door de rekenkamer geconstateerde risico's beter te beheersen

Het doel van deze aanbeveling is de door de rekenkamer geconstateerde risico's beter te beheersen.[95] Het praktijkonderzoek dat is uitgevoerd in opdracht van de rekenkamer constateerde enkele bevindingen met bijbehorende risico's. Hoewel het college momenteel een beveiliging realiseert die ervoor zorgt dat kwaadwillenden niet eenvoudig toegang verkrijgen tot gemeentelijke informatie, benut het college nog niet alle beschikbare technische mogelijkheden. We bevelen dan ook aan om ook de bedreigingen die het onderzoek van de rekenkamer heeft geïdentificeerd, aan te pakken.

Aanbeveling 4: Draag het college op binnen twee maanden nadat de raad een besluit heeft genomen over de aanbevelingen, te rapporteren over een plan van aanpak voor de opvolging van dit onderzoek

De rekenkamer beveelt aan dat het college een voorstelt doet over een plan van aanpak voor de opvolging van dit onderzoek, binnen een termijn van twee maanden.

[95] *Bedrijfsmiddelen-inventaris*, Nederlandse Overheid Referentie Architectuur (NORA), website NORA, 22 november 2021, https://www.noraonline.nl/wiki/ISOR:Bedrijfsmiddelen_inventaris, geraadpleegd op: 1 augustus 2024.

6. Reactie van het College van Burgemeester en Wethouders

Aan de voorzitter van de Rekenkamer Den Haag
De heer H.A. Twisk

Ons kenmerk
DBV/10822827

Contactpersoon

Dienst
Dienst Bedrijfsvoering

Afdeling
DBV DS&I

Telefoonnummer
14070

E-mailadres

Datum
26 november 2024

Onderwerp:
Bestuurlijke reactie rapport Rekenkamer Veilig op afstand

Geachte voorzitter,

Hartelijk dank voor uw zorgvuldige verkenning van de beveiliging van mobiel werken binnen onze gemeente. Wij waarderen uw grondige analyse en de aandacht die u heeft besteed aan dit belangrijke onderwerp.
De bevindingen in uw rapport zijn grotendeels herkenbaar. We zijn verheugd te kunnen melden dat we op verschillende fronten al bezig zijn om de geconstateerde aandachtspunten aan te pakken.
Wij nemen uw aanbevelingen ter harte en zullen deze zeker opvolgen. Hieronder geven we per aanbeveling aan hoe we dit concreet gaan aanpakken:

1. Risicoanalyses:
We gaan een structureel proces implementeren voor het uitvoeren van risicoanalyses bij ICT-gerelateerde besluitvorming. Dit omvat het opstellen van een formeel kader voor risicoanalyses en het integreren hiervan in onze besluitvormingsprocessen. Hiervoor is al een zogenoemd ISMS in gebruik genomen (Information Security Management System. Managementsysteem voor de beveiliging van informatie. Met dit systeem bewaakt men het proces van beveiliging).
We zullen zorgen dat de uitkomsten van deze analyses expliciet worden meegenomen in beleidsstukken en collegebesluiten.

2. Medewerkersbewustzijn:
Er komen trainingen beschikbaar voor alle medewerkers over informatiebeveiliging en veilig mobiel werken. Daarnaast organiseren we regelmatige bewustwordingscampagnes, zoals het huidige Digifit-programma, en stellen we specifieke richtlijnen op voor mobiel werken. We zetten ook een systeem op om de effectiviteit van deze maatregelen te monitoren.

3. ICT-landschap overzicht:
We zijn bezig met het verbeteren van onze inventarisatie en monitoring door een gedetailleerd overzicht op te stellen van alle apparaten en systemen binnen ons ICT-landschap. Dit wordt ondersteund door geautomatiseerde tools voor continue monitoring en updaten van deze informatie. We ontwikkelen ook procedures om dit overzicht actueel te houden.

4. Technische beveiliging:
We scherpen onze toegangscontroles aan door beveiligingsmaatregelen te implementeren voor privé-apparaten die toegang hebben tot gemeentelijke systemen. We onderzoeken ook hoe we de beveiliging van mobiele apparaten verder kunnen versterken.

Met het oog hierop zijn wij bezig om een integraal plan te ontwikkelen dat alle aspecten van onze digitale beveiliging omvat. Dit plan adresseert niet alleen de door u aangestipte punten, maar ook andere cruciale elementen van onze cybersecurity strategie.
We stellen het zeer op prijs u hierover vertrouwelijk bij te praten na de zomer van 2025. Tijdens deze sessie zullen we u graag informeren over onze holistische aanpak en de stappen die we nemen om de digitale veiligheid van onze gemeente te waarborgen.
Nogmaals dank voor uw waardevolle inzichten. We kijken ernaar uit om u op de hoogte te houden van onze vorderingen en om samen te werken aan een veiligere digitale omgeving voor onze gemeente.

Het college van burgemeester en wethouders,

De secretaris,	De burgemeester,
Ilma Merx	Jan van Zanen

7. Nawoord

Op 26 november 2024 heeft de Rekenkamer Den Haag de bestuurlijke reactie op de conclusies en aanbevelingen ontvangen van het College van Burgemeester en Wethouders (zie hoofdstuk 6). Het is een positief teken dat het college aangeeft onze aanbevelingen op te zullen volgen en al op verschillende fronten bezig is met het aanpakken van de door ons geconstateerde aandachtspunten. Het college geeft per aanbeveling aan hoe het dat concreet wil aanpakken. Wij constateren dat op enkele onderdelen nog niet geheel duidelijk is of het college daadwerkelijk alle punten uit onze aanbevelingen oppakt. Hieronder geven we per aanbeveling een weergave van de reactie van het college en het nawoord van de rekenkamer.

Aanbeveling 1: Draag het college op het ICT-beleid en de ICT-organisatie te herzien en daarbij:

a. de inventarisatie en analyse van mogelijke risico's voor de beveiliging van ICT integraal onderdeel te maken van de besluitvorming.

Reactie college:

Het college geeft aan een structureel proces te gaan implementeren voor het uitvoeren van risicoanalyses bij ICT-gerelateerde besluitvorming. Dit omvat het opstellen van een formeel kader voor risicoanalyses, het integreren van het kader in besluitvormingsprocessen en het expliciet meenemen van de uitkomsten van de risicoanalyses in beleidsstukken en collegebesluiten.

Nawoord rekenkamer:

De reactie van het college is in lijn met de aanbeveling van de rekenkamer.

b. beleid voor mobiel werken en de beveiliging daarvan op te stellen en uit te dragen.

Reactie college

Het college reageert niet expliciet op deze aanbeveling, maar geeft wel aan bezig te zijn een ‘integraal plan te ontwikkelen dat alle aspecten van onze digitale beveiliging omvat’.

Nawoord rekenkamer

Wij gaan ervan uit dat het college bij het uitwerken van dit integrale plan ook beleidskaders van mobiel werken en de beveiliging daarvan meeneemt.

c. informatie-uitwisseling over beveiligingsrisico's en mogelijke beheersmaatregelen binnen de organisatie te reguleren.

Reactie college

Het college geeft naar aanleiding van onze aanbeveling over risicoanalyses aan een structureel proces te gaan implementeren voor het uitvoeren van risicoanalyses (zie hierboven bij 1.a). Het college geeft daarbij ook aan dat het hiervoor al een managementsysteem voor de beveiliging van informatie (ISMS) in gebruik heeft genomen.

Nawoord rekenkamer

Het wordt uit de reactie van het college niet duidelijk of het genoemde managementsysteem zich ook richt op interne informatie-uitwisseling. Zoals wij in de toelichting op dit punt van onze aanbeveling aangeven, is het van belang een betere informatie-uitwisseling tussen verschillende afdelingen te formaliseren. Daarbij is het ook van belang de positie van de Chief Information Security Officer binnen die informatie-uitwisseling te verstevigen. Uit ons onderzoek kwam naar voren dat het delen van relevante informatie over risico's en beheersmaatregelen via informele kanalen gebeurt. Daarmee ontbreekt een waarborg dat relevante informatie wordt uitgewisseld.

d. een compleet en centraal overzicht op te stellen van het gemeentelijk ICT-landschap en dit overzicht te beheren.

Reactie college

Het college geeft aan bezig te zijn met het verbeteren van de inventarisatie en monitoring, door een gedetailleerd overzicht op te stellen van alle apparaten en systemen binnen het ICT-landschap van de gemeente. Het college zegt ook toe om procedures te ontwikkelen om het overzicht actueel te houden.

Nawoord rekenkamer

De reactie van het college is in lijn met de aanbeveling van de rekenkamer.

Aanbeveling 2: Draag het college op medewerkers van de gemeente bewust en medeverantwoordelijk te maken voor de veiligheid van mobiel werken

Reactie college

Het college zet verschillende instrumenten in om het medewerkersbewustzijn te bevorderen. Tevens zegt het college toe de effectiviteit van deze maatregelen te zullen monitoren.

Nawoord rekenkamer

Het college beschrijft in zijn reactie wat feitelijk al de praktijk is binnen de gemeentelijke organisatie en gaat niet in op onze voorstellen om zeker te stellen dat medewerkers daadwerkelijk trainingen volgen. We merken hierbij op dat volgens de Baseline

Informatiebeveiliging Overheden (BIO) het trainen van medewerkers een verplichting zou moeten zijn. Verder merken we op dat, waar het college spreek over ‘richtlijnen voor mobiel werken’, niet duidelijk wordt of het hierover ook bindende afspraken met medewerkers gaat maken. Als richtlijnen alleen eenzijdig vanuit het college worden gecommuniceerd, ontstaat nog niet de door ons bedoelde medeverantwoordelijkheid voor medewerkers. Een bindende afspraak zou bijvoorbeeld onderdeel kunnen uitmaken van het Haags Personeelsreglement.

Aanbeveling 3: Draag het college op bestaande technische mogelijkheden voor toegangsbeveiliging beter te benutten, om zo de door de rekenkamer geconstateerde risico's beter te beheersen

Reactie college

Het college geeft aan een integraal plan te ontwikkelen dat alle aspecten van de digitale beveiliging omvat. Specifiek noemt het college dat het de beveiligingsmaatregelen voor de toegang tot gemeentelijke systemen met privé apparaten gaat aanscherpen. En daarnaast te zullen onderzoeken hoe de beveiliging van mobiele apparaten versterkt kan worden.

Nawoord rekenkamer

Wij gaan ervan uit dat het college bij het opstellen en implementeren van het genoemde integrale plan alle door ons geconstateerde kwetsbaarheden zal aanpakken.

Aanbeveling 4: Draag het college op binnen twee maanden nadat de raad een besluit heeft genomen over de aanbevelingen, te rapporteren over een plan van aanpak voor de opvolging van dit onderzoek

Reactie college

Het college reageert niet op deze aanbeveling. Wel nodigt zij de rekenkamer uit voor een toelichting op het plan voor een integrale aanpak van de digitale beveiliging waarin ook onze aanbevelingen worden geadresseerd. Deze toelichting zou na de zomer van 2025 plaatsvinden.

Nawoord rekenkamer

De rekenkamer doet aanbevelingen aan de gemeenteraad met als doel het gevoerde beleid voor mobiel werken en de beveiliging daarvan te verbeteren. Bij ons onderzoek doen wij de raad een voorstel voor het vaststellen van onze aanbevelingen. Daarom geven wij in onze vierde aanbeveling ook aan dat het college de raad zou moeten informeren over een plan van aanpak. Ook stellen wij voor dit al na twee maanden te doen. We stellen deze korte termijn voor mede gezien het feit dat de ambtelijke organisatie al tijdens ons onderzoek is geïnformeerd over de door ons geconstateerde kwetsbaarheden in de beveiliging van mobiel werken. Voor de digitale veiligheid is het verder belangrijk dat oplossingen zo snel mogelijk doorgevoerd worden. Tot slot zijn wij, met inachtneming van onze rol als rekenkamer, graag bereid om met het college het gesprek te voeren over de opvolging van onze aanbevelingen.

Bijlage 1: Aanpak van het onderzoek

Met dit onderzoek oordeelt de Rekenkamer Den Haag over het beleid inzake de beveiliging van de toegang tot gemeentelijke systemen en de uitvoering daarvan. Het gaat daarbij over de beveiliging van de diverse mogelijkheden die de gemeente biedt om gemeentelijke informatiesystemen vanaf mobiele werkplekken te benaderen.

Afbakening

Waar we in dit onderzoek het begrip mobiel werken gebruiken, bedoelen we alle werkzaamheden die worden verricht vanuit een externe locatie en waarbij toegang wordt verkregen tot gemeentelijke systemen en/of informatie. Mobiel werken in dit onderzoek, omvat alle werkzaamheden die plaats-onafhankelijk uitgevoerd kunnen worden. Werkzaamheden die alleen op vaste, gemeentelijke locaties uitgevoerd kunnen worden, zijn niet meegenomen in dit onderzoek.

Onderzoeksmethodes

Voor dit onderzoek heeft de rekenkamer een documentenstudie gedaan, interviews met de ambtelijke organisatie gehouden en een technisch onderzoek laten doen door een extern bureau. In bijlage 2 lichten we elke methode toe.

Daarnaast gebruikt de rekenkamer een normenkader. De normen zijn gebaseerd op wet- en regelgeving. We hebben hierbij vooral gebruik gemaakt van de Baseline Informatiebeveiliging Overheid (BIO). Dit is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen. Hierbij hebben we informatie uit de handreikingen van de Informatiebeveiligingsdienst (IBD) voor gemeenten die bij onderdelen van de BIO horen ook meegenomen in het normenkader. Daarnaast zijn enkele algemene normen gebaseerd op het normenkader van het National Institute of Standards and Technology (NIST).

In het onderzoek doen we geen uitputtende toetsing op de naleving van de BIO, maar nemen wij alleen de normen mee die betrekking hebben tot de beveiliging van mobiele werkplekken. Het volledige normenkader hebben wij opgenomen in bijlage 3.

Bijlage 2: Onderzoeksverantwoording

In deze bijlage beschrijven we de onderzoeksmethoden en verantwoorden we de keuzes voor de thema's en deelvragen.

Onderzoeksmethoden

Om het onderzoek uit te voeren, hanteerde de rekenkamer de volgende onderzoeksmethoden:

1. Documentenstudie
2. Interviews
3. Technisch onderzoek

Hieronder zetten wij uiteen hoe wij de bovengenoemde methoden hebben uitgevoerd.

Documentenstudie

Voor dit onderzoek heeft de rekenkamer documenten uitgevraagd en vervolgens geanalyseerd. Het betreft de volgende type documenten:

1. Documenten uit het raadsinformatiesysteem inzake beleid, visies of plannen met betrekking tot de beveiliging van mobiele werkplekken.
2. Documenten met betrekking tot informatieveiligheid en mobiele werkplekken.
3. Documenten over de regels, regelingen en gedragscodes binnen de gemeente op het gebied van mobiel werken.
4. Overzichten van apparaten, gebruikers, eigenaren en applicaties van ICT-beheer.

Zie voor een volledig overzicht van gebruikte bronnen bijlage 5.

Interviews

Voor dit onderzoek heeft de rekenkamer interviews uitgevoerd met verschillende betrokkenen vanuit de ambtelijke organisatie. Het betreft semigestructureerd interviews. De interviews hadden het doel om meer informatie te verkrijgen over het beleid, de uitvoering en het proces rond de beveiliging van mobiele werkplekken.

Van de interviews heeft de rekenkamer verslagen gemaakt. De verslagen zijn vertrouwelijk en door de geïnterviewden gecontroleerd op feitelijke juistheid. De verslagen zijn vervolgens gebruikt als bron voor dit onderzoek.

Technisch onderzoek

De rekenkamer heeft aan een extern bureau de opdracht verstrekt om een (technisch)onderzoek te doen naar de beveiliging van mobiele werkplekken. Tijdens dit onderzoek is in de periode van 25 oktober tot 23 november 2023 de mate van beveiliging beoordeeld van:

- Een gemeente laptop

- Een privé laptop
- Een gemeente telefoon
- Een gemeente tablet

Daarnaast heeft het externe bureau gekeken naar de beveiliging van de interne netwerk-infrastructuur. Hierbij is onderzocht:

- Het gebruik van Single Sign On (SSO)
- Het gebruik van Multi-factor Authenticatie (MFA)
- De toegangsbeveiliging tot applicaties

Ten behoeve van het technisch onderzoek is een gebruikers-account van een reguliere medewerker van de gemeente Den Haag gemaakt. Dit account had geen speciale privileges. Voor het onderzoeken van een selectie van de applicaties binnen de gemeente, is er voor dit account wel aanvullend toegang aangevraagd tot enkele applicaties die niet tot de standaard werkomgeving behoren.

Van de resultaten van het technisch onderzoek heeft de rekenkamer een rapport ontvangen. Dit rapport bevat gedetailleerde (technische) beschrijvingen van de geconstateerde kwetsbaarheden en is daarom vertrouwelijk. Om die reden publiceert de rekenkamer het rapport niet. De ambtelijke organisatie is door de rekenkamer geïnformeerd over de uitkomsten van het technische onderzoek.

Het rapport van het technische onderzoek classificeert bevindingen op basis van het ‘Common Vulnerability Scoring System’ (CVSS). CVSS is een scoringsmethode die gebruikt wordt om als kwalitatieve maatstaf voor het aangeven van de ernst van een kwetsbaarheid (of te wel een bevinding). CVSS is geen maatstaf voor het aangeven van het risico, maar van de ‘weging’ van een bevinding. De classificering van bevindingen is voor de rekenkamer als uitgangspunt genomen voor de beoordeling van de beveiliging van mobiel werken.

De CVSS-score bestaat uit twee sub-scores: de mate waarop er misbruik van een kwetsbaarheid gemaakt kan worden (exploitability) en de impact van een kwetsbaarheid. Voor dit onderzoek is er voor elke bevinding een score gegeven van 0 tot 10 (zie tabel 1). Meer informatie over de CVSS-score en de bijbehorende sub-scores zijn te vinden op: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Tabel 1 Classificatie CVSS-score

Classificatie	Base score
Kritiek	9.0 – 10.0
Hoog	7.0 – 8.9
Gemiddeld	4.0 – 6.9
Laag	0.1 – 3.9
Informatief	0.0

Afstemming gemeente

De rekenkamer heeft voorafgaand aan en tijdens het technische onderzoek afgestemd met de gemeentelijke organisatie. Daarbij verleende de gemeente medewerking aan het onderzoek, voor zover dat voor de betreffende onderdelen noodzakelijk was. Zo heeft de ambtelijke organisatie een medewerker account aangemaakt en een overzicht van applicaties beschikbaar gesteld aan de rekenkamer. De bevindingen van het technische onderzoek bespraken we na afronding met de betrokkenen vanuit de ambtelijke organisatie.

Verantwoording keuze afwijkingen onderzoeksopzet

Dit rapport kent enkele afwijkingen ten opzichte van de eerder gepubliceerde onderzoeksopzet.[96] Het betreft de volgende wijzigingen:

1. De termen ‘thuiswerken’ en ‘thuiswerkplekken’ zijn vervangen door de termen ‘mobiel werken’ en ‘mobiele werkplekken’.
2. De structuur van de deelvragen is met inachtneming van het normenkader veranderd.

Wij lichten de wijzigingen hieronder nader toe.

‘Mobiele werkplekken’ in plaats van ‘thuiswerkplekken’

Oorspronkelijk werd in de onderzoeksvraag de term ‘thuiswerkplekken’ gebruikt. Omdat het inloggen op en gebruikmaken van de gemeentelijke ICT buiten gemeentelijke werkplekken niet beperkt is tot alleen thuiswerkplekken., hebben we gekozen voor ‘mobiele werkplekken’. Deze term omvat alle werkzaamheden die plaats onafhankelijk uitgevoerd kunnen worden.

De structuur van de beantwoording van de deelvragen is met inachtneming van het normenkader veranderd

Ten behoeve van het leesgemak en om de logica van het normenkader aan te houden, heeft de rekenkamer besloten de deelvragen anders in te delen. In de onderzoeksopzet was de hoofdvraag opgesplitst in twee deelvragen. De eerste deelvraag had betrekking op het technisch onderzoek dat is uitgevoerd door het externe bureau. Deze deelvraag is opgesplits in twee afzonderlijke deelvragen: deelvraag drie en vier. Deelvraag twee in de oorspronkelijke onderzoeksopzet was gericht op het achterliggende proces en beleid. Deze deelvraag is in dit rapport opgesplitst in de afzonderlijke deelvragen één en twee.

[96] RIS316694, Brief Bijlage, *Digitale beveiliging van thuiswerken bij de gemeente Den Haag – onderzoeksopzet*, Rekenkamer, 6 oktober 2023

Toetsing op de normen

Dit onderzoek doet geen uitputtende toetsing van de Baseline Informatiebeveiliging Overheid (BIO). Het normenkader van de BIO betreft informatiebeveiliging in het algemeen en valt daarmee buiten de scope van dit onderzoek. De rekenkamer heeft daarom enkel de normen meegenomen die relevant zijn voor mobiel werken (zie bijlage 3 voor een toelichting op het normenkader). De rekenkamer heeft deze normen vervolgens gegroepeerd in vier thema's. De thema's zijn de basis voor definitieve onderzoeksvragen:

1. In hoeverre neemt de gemeente de risico's van mobiel werken mee in de ontwikkeling van het informatiebeveiligingsbeleid?
2. In hoeverre waarborgt de gemeente medewerkersbewustzijn in het kader van mobiel werken?
3. In hoeverre heeft de gemeente grip op het ICT-landschap wat betreft faciliteiten voor mobiel werken?
4. In hoeverre waarborgt de gemeente de beveiliging van toegang vanuit mobiele werkplekken met technische maatregelen?

Van onderzoeksvragen naar conclusies

De onderzoeksvragen zoals die hierboven zijn weergegeven vormden de basis voor het onderzoek. De beantwoording van de onderzoeksvragen bestaat uit diverse bevindingen. Op basis van deze beantwoording en bevindingen, heeft de rekenkamer de conclusies voor dit onderzoek geformuleerd. Daarbij is een weging gemaakt van het belang van de verschillende uitkomsten en is gezocht naar voor het gemeentebestuur relevante samenhang tussen onderwerpen. Dit heeft ertoe geleid dat de bovenstaande volgorde van onderzoeksvragen niet één op één terug te vinden is in de bevindingen die ter onderbouwing van de deelconclusies zijn opgenomen. De beantwoording van deelvragen 1 en 2 vormt de onderbouwing van de eerste deelconclusie, terwijl de beantwoording van deelvragen 3 en 4 de onderbouwing vormt voor de tweede deelconclusie.

Bijlage 3: Beschrijving normenkader

Normen bij deelvraag 1: in hoeverre neemt de gemeente de risico's van mobiel werken mee in de ontwikkeling van het informatiebeveiligingsbeleid?

Norm: De gemeente neemt risico-gebaseerd maatregelen, voert risicoanalyses uit (ook met betrekking tot mobiel werken en privé apparatuur) en heeft hiermee de risico's van mobiel werken in beeld en neemt deze mee in het beleid ten aanzien van de beveiliging van mobiel werken.

Toelichting op de norm: Zowel de Baseline Informatiebeveiliging Overheden (BIO) als het kader van de National Institute of Standards and Technology (NIST) eisen dat informatiebeveiliging risico-gebaseerd opgesteld wordt. Dit betekent volgens de BIO dat er risicomanagement toegepast moet worden.[97] De BIO definieert risicomanagement als "het inzichtelijk en systematisch inventariseren, beoordelen en – door het treffen van maatregelen – beheersbaar maken van risico's en kansen, die het bereiken van de doelstellingen van de organisatie bedreigen dan wel bevorderen, op een zodanige wijze dat verantwoording kan worden afgelegd over de gemaakte keuzes".[98] De BIO geeft daarnaast aan dat de gemeente beleid en ondersteunende maatregelen moet vaststellen om [geconstateerde] risico's te beheren.[99] In de handreiking 'risicomanagement' van de IBD wordt benadrukt dat het belangrijk is dat risicoanalyses regelmatig herhaald worden.[100]

Daarnaast wordt bij het mobiel werken veelvuldig gebruik gemaakt van mobiele apparaten waar ook (gevoelige) informatie en data wordt verwerkt.[101] Het is daarom belangrijk om beleid te hebben waarin bepaald wordt hoe hiermee moet worden omgegaan, om de bijbehorende risico's te beheren.[102]

Het kader van de NIST eist in artikel ID.RM dat risicomanagement processen worden vastgesteld, beheerd en goedgekeurd door belanghebbenden binnen de organisatie.[103] Dit

---

[97] *Baseline informatiebeveiliging overheid*, 2020, p. 9.
[98] *Baseline informatiebeveiliging overheid*, 2020, p. 9.
[99] *Baseline Informatieveiligheid Overheden*, 2020, art. 6.2.1, p. 24.
[100] *Handreiking Risicomanagement door lijnmanagers*, Informatie Beveiligingsdienst voor gemeenten, mei 2020, p. 12.
[101] *Handreiking Mobile Device Management*, Informatiebeveiligingsdienst voor gemeenten, december 2018, p. 6.
[102] *Handreiking Mobile Device Management*, Informatiebeveiligingsdienst voor gemeenten, december 2018, p. 6.
[103] *NIST Cybersecurity Framework US National Institute of Standards and Technology*, 2018, artikel ID.RM.

betekent dat relevante risico's moeten worden geïdentificeerd, geëvalueerd en beheerd. Specifiek eist de NIST in artikel PM-9 dat er beleid ontwikkeld moeten worden om veiligheidsrisico's (voor de operatie en assets) te beheren.[104]

Normen bij deelvraag 2: in hoeverre waarborgt de gemeente medewerkersbewustzijn in het kader van mobiel werken?

Norm: De gemeente waarborgt medewerkersbewustzijn als het gaat om digitale veiligheid en mobiel werken, middels de inzet van regelgeving en (bewustzijns)trainingen.

Toelichting op de norm: Voor het opstellen van regels zijn er in de Baseline Informatiebeveiliging Overheid (BIO) verschillende normen te vinden. Allereerst wordt in paragraaf 7.1.2 gesteld dat de verantwoordelijkheden voor informatieveiligheid in de contractuele overeenkomst met medewerkers gemeld zijn.[105] Volgens paragraaf 8.1.3 van de BIO behoren regels voor aanvaardbaar gebruik van ICT-middelen die samenhangen met informatie en informatie verwerkende faciliteiten te worden vastgelegd en geïmplementeerd en daarop volgt in de sub-norm 8.1.3.1 dat medewerkers hier aantoonbaar op zijn gewezen.[106]

Naast deze algemene regels kent de BIO ook normen ten aanzien van mobiel werken. Volgens paragraaf 6.2.2 van de BIO dient er beleid en ondersteunende beveiligingsmaatregelen te worden geïmplementeerd ter beveiliging van informatie die vanaf mobiele werkpleklocaties wordt benaderd, verwerkt of opgeslagen.[107] Hierbij wordt verwezen naar de handreiking telewerkbeleid van de informatiebeveiligingsdienst (IBD).[108] Hierin staat dat er voor het werken op afstand en het gebruik van privémiddelen beleid met gedragsregels opgesteld moeten worden en dat er afspraken gemaakt moeten worden voor mobiel werken.[109] Onder andere betekent dit dat er bij het uitvoeren van werkzaamheden niet gewerkt mag worden met illegale software en dat er een plicht is voor de beveiliging van gemeentelijke informatie op een privé apparaat. De gemeente kan daarbij regels opstellen over maatregelen die genomen moeten worden om gemeentelijke informatie op een privé-apparaat te beschermen.[110] Specifiek geeft de handreiking een aantal punten die

---

[104] *NIST Cybersecurity Framework US National Institute of Standards and Technology*, 2018, artikel PM-9.
[105] *Baseline informatiebeveiliging overheid*, 2020, artikel 7.1.2.
[106] *Baseline informatiebeveiliging overheid*, 2020, artikel 8.1.3(.1).
[107] *Baseline informatiebeveiliging overheid*, 2020, artikel 6.2.2.
[108] *Handreiking Telewerkbeleid*, Informatiebeveiligingsdienst voor gemeenten, juli 2019.
[109] *Handreiking Telewerkbeleid*, Informatiebeveiligingsdienst voor gemeenten, juli 2019, p. 8, p.13.
[110] *Handreiking Telewerkbeleid*, Informatiebeveiligingsdienst voor gemeenten, juli 2019, p. 7.

opgenomen kunnen worden in gedragsregels of gebruiksvoorwaarden van het mobiel werken. De werknemer moet bijvoorbeeld zijn privé apparaat voorzien van een up-to-date virusscanner, personal firewall, anti-malware tool, screensaver beveiligd met een wachtwoord en up-to-date besturingssysteem en applicaties. Daarnaast kan de medewerker ook verboden worden om bedrijfsinformatie lokaal op te slaan.[111]

Over het aanbieden van opleidingen worden in de Baseline Informatiebeveiliging Overheid (BIO) ook normen opgenomen. Volgens paragraaf 7.2.2 uit de BIO behoren alle medewerkers passende bewustzijnsopleiding en -training en regelmatige bijscholing van beleidsregels te krijgen.[112] Hierbij wordt in de daarbij horende sub-norm 7.2.2.2 specifiek gesteld dat er bij indiensttreding het i-bewustzijn training van de VNG succesvol moet worden gevolgd.[113] In paragraaf 7.2.2.3 wordt ook gesteld dat er (door het management) regelmatig en actief gestimuleerd moet worden om trainingen op het gebied van informatiebeveiliging te volgen.[114] Hierbij wordt verwezen naar de handreiking 'personeelsbeleid gemeente' van de informatiebeveiligingsdienst (IBD).[115] Daarin staat dat alle gemeentelijke medewerkers, ingehuurde partijen en derden toereikende voorlichting en training behoren te krijgen om hun bewustzijn ten aanzien van informatiebeveiliging te vergroten en hun beveiligingsgedrag te verbeteren.[116]

Normen bij deelvraag 3: in hoeverre heeft de gemeente grip op het ICT-landschap wat betreft faciliteiten voor mobiel werken?

Norm: De gemeente heeft zicht op en controle over de ICT dat gebruikt wordt binnen de organisatie, waaronder de mobiele apparatuur die wordt gebruikt voor mobiel werken, de gebruikers van de gemeentelijke ICT en het gebruik van en toegang tot applicaties.

Toelichting op de norm: Zowel de Baseline Informatieveiligheid Overheid (BIO) als het internationaal erkend kader van het National Institute of Standards and Technology (NIST) benadrukken het belang van het identificeren en bijhouden van bedrijfsmiddelen in het waarborgen van cyber security. Het NIST benadrukt dat het belangrijk is om zicht te hebben

[111] *Handreiking Telewerkbeleid*, Informatiebeveiligingsdienst voor gemeenten, juli 2019, p.13.
[112] *Baseline informatiebeveiliging overheid*, 2020, artikel 7.2.2.1.
[113] *Baseline informatiebeveiliging overheid*, 2020, artikel 7.2.2.2.1.
[114] *Baseline informatiebeveiliging overheid*, 2020, artikel 7.2.2.3.
[115] *Handreiking Personeelsbeleid gemeente*, Informatiebeveiligingsdienst voor gemeenten, mei 2020.
[116] *Handreiking Personeelsbeleid gemeente*, Informatiebeveiligingsdienst voor gemeenten, mei 2020, p. 17.

in de apparaten en software binnen de organisatie, omdat dit vaak de toegangspunten zijn voor kwaadwillende actoren.[117]

Volgens artikel 8.1.1 van de BIO moeten alle bedrijfsmiddelen geïdentificeerd zijn, en bijgehouden worden in een inventaris.[118] In artikel 8.1.2 wordt benadrukt dat bedrijfsmiddelen die in het inventarisatieoverzicht staan een eigenaar hebben.[119]

In het artikel onder ID.AM-1 van het NIST framework worden soortgelijke eisen gesteld: alle fysieke apparaten en systemen binnen de organisatie moeten worden geïnventariseerd en beheerd.[120] Hierbij wordt onder artikel MOS-09 specifiek gesteld dat alle mobiele apparaten die worden gebruikt om bedrijfsgegevens op te slaan en te openen, moeten worden bijgehouden.[121]

Applicaties

Voor het overzicht van de applicaties wordt naast de algemene norm van de BIO 8.1.1 en 8.1.2 zoals hierboven genoemd in de Handreiking 'Beleid logische toegangsbeveiliging' van de informatie beveiligingsdienst (IBD) ook gesteld dat er een overzicht beschikbaar moet zijn van de informatiesystemen binnen de gemeente, verwerkt in het configuratiebeheersysteem (CMDB).[122] Ook binnen het kader van het NIST wordt ook in artikel ID-AM 2 vereist dat alle softwareplatforms en applicaties binnen de organisatie zorgvuldig worden geïnventariseerd.[123]

Gebruiker

Ook over gebruikersbeheer kent de Baseline Informatiebeveiliging Overheid (BIO) normen. In artikel 9.2.2.3 wordt gesteld dat er een actueel mandaatregister is, of dat er functieprofielen zijn waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van

---

[117] CSF 1.1 Quick Start Guide, website NIST, 23 januari 2023, https://www.nist.gov/cyberframework/getting-started/quick-start-guide#:~:text=Maintain%20hardware%20and%20software%20inventory,as%20simple%20as%20a%20spreadsheet, geraadpleegd op: 7 februari 2024.
[118] *Baseline Informatieveiligheid Overheden*, 2020, artikel 8.1.1.
[119] *Baseline Informatieveiligheid Overheden*, 2020, artikel 8.1.2.
[120] *NIST Cybersecurity Framework US National Institute of Standards and Technology*, 2018, artikel ID.AM-1.
[121] *NIST Cybersecurity Framework US National Institute of Standards and Technology*, 2018, artikel MOS-9.
[122] Handreiking *Beleid logische toegangsbeveiliging*, Informatiebeveiligingsdienst voor gemeenten, september 2021, p. 13.
[123] *NIST Cybersecurity Framework US National Institute of Standards and Technology*, 2018, artikel ID-AM 2.

toegangsrechten.[124] Volgens artikel 9.2.5 van de BIO moeten de toegangsrechten van gebruikers regelmatig beoordeeld worden.[125]

De BIO verwijst ook naar de normen van het Centrum Informatiebeveiliging en Privacybescherming (CIP) 'Grip op Secure Software Development (SSD)'. Hierin staan basisnormen die dienen als richtlijn voor ontwikkeling en onderhoud van veilige software.[126] Volgens artikel SSD-7/01.01 van de CIP moet er voor het beheersen van de autorisaties de toegangsrechten tot gegevens en functies in de applicatie op een gestructureerde manier georganiseerd zijn.[127] Dit kan door gebruik te maken van beveiligingsgroepen. Bij het gebruik van beveiligingsgroepen moeten deze zodanig zijn opgezet dat de groepen eenvoudig en beheersbaar te koppelen zijn met taken en organisatorische functies.[128] Artikel SSD-7.01.03 van de CIP stelt dat er ook een mogelijkheid moet zijn om toegangsrechten bijvoorbeeld veilig te blokkeren of verwijderen.[129]

Normen bij deelvraag 4: in hoeverre waarborgt de gemeente de beveiliging van toegang vanuit mobiele werkplekken met technische maatregelen?

Norm: De gemeente neemt technische maatregelen om de veiligheid van mobiel werken te waarborgen.

Toelichting op de norm: Ook voor de technische eisen kent de Baseline Informatiebeveiliging Overheid (BIO) normen. In artikel 9.1.2 van de BIO wordt gesteld dat gebruikers alleen toegang behoren te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.[130] Specifiek betekent dit volgens artikel 9.1.2.1 van de BIO dat alleen geauthentiseerde apparatuur toegang kan krijgen tot een vertrouwde zone.[131] Volgens artikel 9.1.2.2 behoren gebruikers met eigen of ongeauthenticeerde apparatuur (Bring Your Own Device) alleen toegang te krijgen tot een onvertrouwde zone.[132] Als vanuit

---

[124] *Baseline Informatieveiligheid Overheden*, 2020, artikel 9.2.2.3.
[125] *Baseline Informatieveiligheid Overheden*, 2020, artikel 9.2.5.
[126] *Grip op Secure Software Development Beveiligingseisen voor (web)applicaties*, Centrum Informatiebeveiliging en Privacybescherming, M. Koers & R. van der Veer, 20 juli 2020.
[127] *Grip op Secure Software Development*, Centrum Informatiebeveiliging en Privacybescherming, 2020, artikel SSD-7/01.01.
[128] *Grip op Secure Software Development*, Centrum Informatiebeveiliging en Privacybescherming, 2020, artikel SSD-7/01.01.
[129] *Grip op Secure Software Development*, Centrum Informatiebeveiliging en Privacybescherming, 2020, artikel SSD-7.01.03.
[130] *Baseline informatiebeveiliging overheid*, 2020, artikel 9.1.2.
[131] *Baseline informatiebeveiliging overheid*, 2020, artikel 9.1.2.1.
[132] *Baseline informatiebeveiliging overheid*, 2020, artikel 9.1.2.2.

een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, behoort dit volgens 9.4.2.1 van de BIO alleen op basis van minimaal two-factor authenticatie te gebeuren.[133]

Ook kent de BIO normen ten aanzien van beheersmaatregelen tegen malware. Volgens artikel 12.2.1 van de BIO behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd ter bescherming tegen malware.[134] Daarnaast moet volgens artikel 12.2.1.1 het downloaden van bestanden beheerst en beperkt zijn op basis van risico en need-of-use.[135] Volgens BIO 12.2.1.3 dienen de gebruikte anti-malwaresoftware en bijbehorende herstelsoftware actueel te zijn en te worden ondersteund door periodieke updates.[136]

Volgens artikel 6.2.1.1 van de BIO moet mobiele apparatuur zo worden ingericht dat informatie niet onbewust wordt opgeslagen.[137] Als vertrouwelijke informatie wel wordt opgeslagen moeten de gegevens versleuteld zijn. Daarnaast moet in dat geval 'wissen op afstand' mogelijk zijn.[138] Daarnaast stelt de BIO in artikel 6.2.1.2 dat er beheersmaatregelen genomen worden bij het inzetten van mobiele apparatuur.[139] Onder andere houdt het in dat er gebruikt wordt gemaakt van Mobile Device Management (MDM) of Mobile Application Management (MAM) oplossingen en dat het device deel uit maakt van patchmanagement en hardening.[140] Volgens de handreiking 'Mobile Device Management' van de IBD, waarnaar gerefereerd wordt in artikel 6.2.1 van de BIO, wordt expliciet beschreven dat de beveiligingsmaatregelen ook betrekking hebben op privé apparatuur die zakelijk gebruikt wordt.[141]

De BIO verwijst ook naar de normen van het Centrum Informatiebeveiliging en Privacybescherming (CIP) 'Grip op Secure Software Development (SSD): De Normen voor Mobile Apps'. Hierin staan basisnormen die dienen als richtlijn voor veilige mobiele apps.[142]

---

[133] *Baseline informatiebeveiliging overheid*, 2020, artikel 9.4.2.1.
[134] *Baseline informatiebeveiliging overheid*, 2020, artikel 12.2.1.
[135] *Baseline informatiebeveiliging overheid*, 2020, artikel 12.2.1.1.
[136] *Baseline informatiebeveiliging overheid*, 2020, artikel 12.2.1.3.
[137] *Baseline informatiebeveiliging overheid*, 2020, artikel 6.2.1.1.
[138] *Baseline informatiebeveiliging overheid*, 2020, artikel 6.2.1.1.
[139] *Baseline Informatieveiligheid Overheden*, 2020, artikel 6.2.1.2.
[140] *Baseline Informatieveiligheid Overheden*, 2020, artikel 6.2.1.2b; *Baseline Informatieveiligheid Overheden*, 2020, artikel 6.2.1.2c.
[141] *Handreiking Mobile Device Management*, Informatiebeveiligingsdienst voor gemeenten, 2018, p. 6.
[142] *Grip on Secure Software Development Security requirements for Mobile Apps*, Centrum Informatiebeveiliging en Privacybescherming, M. Koers, 25 februari 2016.

Volgens artikel SSDm-10 dat een app de gebruiker sessie automatisch beëindigt na een vooraf ingestelde periode van gebruikersinactiviteit.[143]

In artikel 12.6.2 van de BIO wordt gesteld dat er voor het installeren van software door gebruikers regels behoren te worden vastgesteld en geïmplementeerd.[144] In de bijbehorende sub-norm in artikel 12.6.2.1 wordt gesteld dat gebruikers op hun werkomgeving niets zelf kunnen installeren, anders dan wat via de ICT-leverancier wordt aangeboden of wordt toegestaan.[145]

Verder stelt de BIO in artikel 9.4.1.2 dat gebruikers alleen de informatie met specifiek belang kunnen inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.[146]

[143] *Grip on Secure Software Development Security requirements for Mobile Apps*, Centrum Informatiebeveiliging en Privacybescherming, M. Koers, 25 februari 2016.
[144] *Baseline informatiebeveiliging overheid*, 2020, artikel 12.6.2.
[145] *Baseline informatiebeveiliging overheid*, 2020, artikel 12.6.2.1.
[146] *Baseline informatiebeveiliging overheid*, 2020, artikel 9.4.1.2.

Bijlage 4: Begrippenlijst

Authenticatie	Het verifiëren dat de gebruiker daadwerkelijk is wie hij beweert te zijn, bijvoorbeeld door een wachtwoord en gebruikersnaam.
Autorisatie	Het toekennen van toegang, rechten of privileges (tot een applicatie).
Beheerdersrechten	Speciale toegangsrechten die een gebruiker heeft [op een apparaat] om systeemwijzigingen uit te voeren.
Configuratie Management Database (CMDB)	Een database die alle relevante informatie bevat over de elementen die beheerd en gecontroleerd moeten worden (zoals hardware en software) in de IT-infrastructuur.
CVSS-score	Common Vulnerability Scoring System' (CVSS) is een scoringsmethode die gebruikt wordt als kwalitatieve maatstaf voor het aangeven van de ernst van een kwetsbaarheid.
Gebruikers	Alle personen, werkzaam binnen de gemeentelijke organisatie die gebruik maken van de ICT-faciliteiten van de gemeente. Dit betreft zowel medewerkers van de ambtelijke organisatie, externen met een gemeente Den Haag account, als raadsleden.
Gebruikerssessies	De periode dat een gebruiker actief is en gebruik maakt van een applicatie of systeem.
Hardening	Het verkleinen van het aanvalsoppervlak door niet gebruikte functies in hardware en software uit te zetten of weg te halen en de rechten van andere functies waar mogelijk te beperken. Zo verkleint men ook het risico van aanvallen.[147]
I-bewustzijn opleiding	Een kosteloze e-learning programma ontworpen door de VNG om de

[147] *Cybersecurity Woordenboek 2021*, Cyberveilig Nederland, december 2021.

	informatieveiligheid te verhogen door het bewustzijn van medewerkers te verhogen.[148]
ICT-landschap	Het geheel aan ICT en de daaraan verbonden processen binnen de organisatie.
ICT-middelen	Alle elektronische informatie- en communicatieapparatuur en voorzieningen, inclusief alle bijbehorende hard- en software en bestanden.[149]
Malware	Schadelijke programma's.
Mobiele werkplekken	(Digitale) werkplekken die plaats-onafhankelijk zijn.
Mobile Device Management (MDM)	Het stelsel van maatregelen, procedures en ondersteunende producten die het mogelijk maken om mobiele apparaten veilig te kunnen gebruiken en te kunnen beheersen.[150]
Multi-factor authenticatie	Een beveiligingsmethode die vereist dat gebruikers twee of meer verificatiefactoren verstrekken om toegang te krijgen tot een applicatie of account.
Patches	Kleine programma's die aanpassingen maken om fouten op te lossen of verbeteringen aan te brengen. Zij helpen met het up-to-date houden van de applicaties.[151]
Patchmanagement	Het bijhouden van patches.
Risico	Een onzekere gebeurtenis in de toekomst die invloed kunnen hebben op jouw onderneming. [152]

[148] *iBewustzijn Overheid Bewust en veilig omgaan met (digitale) informatie!,* website VNG, datum onbekend, https://www.vngconnect.nl/academie/Training/ibewustzijn-overheid-bewust-en-veilig-omgaan-met-digitale-informatie/edd25b97-95d3-4ce8-ac63-b26dccd91e4e geraadpleegd op: 28 maart 2024.
[149] Intern document *Regeling gebruik ICT middelen en gemeentelijke informatie 2014*, 7 oktober 2014.
[150] *Handreiking Mobile Device Management,* Informatiebeveiligingsdienst voor gemeenten, december 2018.
[151] Handreiking *Samenhang Beheerprocessen en Informatiebeveiliging*, Informatiebeveiligingsdienst voor gemeenten, juni 2019.
[152] Stappenplan risicoanalyse, website digital trustcenter, (datum onbekend), https://www.digitaltrustcenter.nl/stappenplan-risicoanalyse, geraadpleegd op 23 april 2024.

Risicoanalyse	Een grondige beoordeling van het risico dat geïdentificeerd is.[153]
Risicomanagement	Het beheren van risico's om de [digitale] veiligheid te waarborgen door risico's te identificeren en gepaste maatgelen te treffen.
Toegangsrechten	Het recht om gebruik te maken van [een programma, applicatie, document].
Virtuele Desktop Infrastructuur (VDI)	Een ICT-infrastructuur waarmee je virtueel, toegang krijgt tot het (besturings)systeem van het bedrijf, in dit geval de gemeente. Hierdoor kan met vrijwel elk apparaat toegang worden verkregen tot het interne (beveiligde) netwerk.[154]
WOW-plek	Werk en ontmoeten werkplek waarop je een laptop kan aansluiten. De WOW-plek bestaat uit twee beeldschermen, een toetsenbord en een muis. De WOW-plek is een vervanging van de vaste werkplek met desktopcomputer.[155]

[153] Stappenplan risicoanalyse, website digital trustcenter, (datum onbekend), https://www.digitaltrustcenter.nl/stappenplan-risicoanalyse, geraadpleegd op 23 april 2024.
[154] *Wat is VDI (Virtual Desktop Infrastructure)?,* website Microsoft, (datum onbekend), https://azure.microsoft.com/nl-nl/resources/cloud-computing-dictionary/what-is-virtual-desktop-infrastructure-vdi/#infrastructure, geraadpleegd op: 8 mei 2024.
[155] Gebruikershandleiding WOW!, interne website gemeente Den Haag, (datum onbekend), https://denhaag.sharepoint.com/sites/hetplein/SitePages/Gebruikershandleiding-WOW.aspx?web=1, geraadpleegd op: 23 april 2024

Bijlage 5: Bronverwijzingen

Raadsinformatiesysteem Gemeente Den Haag

- RIS304162 Collegebesluit, *Strategisch Beleidskader Informatieveiligheid 2019-2022*, College van Burgemeester en Wethouders, 18 december 2019.
- RIS305017, Raadsvoorstel, Masterplan IT, College van Burgemeester en Wethouders, 1 april 2020.
- RIS305093, Commissiebrief, Visie op digitalisering en dienstverlening 2020-2023, College van Burgemeester en Wethouders, 14 juli 2020.
- RIS313799, Collegebesluit, Uitvoeringsdata 2023 digitalisering en dienstverlening, College van Burgermeester en Wethouders, 29 november 2022.
- RIS315739 Verslag, *Verslag van de Rekeningencommissie*, Rekeningencommissie, 31 Mei 2023.
- RIS317224 Commissiebrief *Governance Digitale Veiligheid*, College van Burgemeester en Wethouders, 7 december 2023.

Interne documenten Gemeente Den Haag

- Intern document *All Android BYOD,* als ontvangen op 27 februari 2024.
- Intern document *All Android devices*, als ontvangen op 13 november 2023.
- Intern document *All Apple BYOD,* als ontvangen op 27 februari 2024.
- Intern document *All Apple devices*, als ontvangen op 13 november 2023.
- Intern document *All Windows devices*, als ontvangen op 13 november 2023.
- Intern document *Applicaties voor rekenkamer*, als ontvangen op 22 november 2023.
- Intern document *rekenkamer*, als ontvangen op 15 november 2023.
- Intern document *Digitale Strategie & Informatiebeleid Inrichtingsvoorstel (draft),* als ontvangen op 13 februari 2024.
- Intern document *Handreiking Hybride werken, voor medewerkers en leidinggevenden*, versie April 2023.
- Intern document *New perspectives for Gemeente Den Haag,* 4 maart 2024.
- Intern document *Rekenkamer overzicht applicatie*, als ontvangen op 15 november 2023.
- Intern document *Regeling gebruik ICT middelen en gemeentelijke informatie 2014*, 7 oktober 2014.
- Intern document *Werkplek visie Haagse Digitale Werkomgeving*, 23 februari 2023.

Website

- *2.600 vaste computers worden vervangen door werkplekken voor laptops*, interne website Gemeente Den Haag, 18 januari 2024, https://denhaag.sharepoint.com/sites/DenHaagNieuws/SitePages/2.600-vaste-computers-worden-vervangen-door-werkplekken-voor-laptops.aspx, geraadpleegd op: 20 februari 2024.
- *Alles over thuiswerken*, interne website Gemeente Den Haag, 24 augustus 2021, https://denhaag.sharepoint.com/sites/werknet/portalen/ictdiv/Paginas/Alles-over-thuiswerken.aspx, geraadpleegd op: 15 februari 2024.
- *Baseline Informatiebeveiliging Overheid (BIO) & NEN-ISO/IEC 27001 en 27002*, website Communicatie Rijk, (datum onbekend), https://www.communicatierijk.nl/vakkennis/rijkswebsites/verplichte-richtlijnen/baseline-informatiebeveiliging-

rijksdienst#:~:text=CommunicatieRijk%20Start%20zoeken-,Baseline%20Informatiebeveiliging%20Overheid%20(BIO)%20%26%20NEN%2DISO%2FIEC,samengewerkt%20en%20gegevens%20worden%20uitgewisseld, geraadpleegd op: 8 april 2024.
- *Bedrijfsmiddelen-inventaris*, website Nederlandse Overheid Referentie Architectuur, 22 november 2021, https://www.noraonline.nl/wiki/ISOR:Bedrijfsmiddelen_inventaris, geraadpleegd op: 6 mei 2024.
- *Blader door de BIO en zoek de bijbehorende practices*, website BIO overheid, (datum onbekend), https://www.bio-overheid.nl/bio-practices/, geraadpleegd op: 24 juni 2024.
- *Bring Your Own Device (BYOD*), website Digital Trust Center, (datum onbekend), https://www.digitaltrustcenter.nl/informatie-advies/bring-your-own-device-byod, geraadpleegd op: 21 mei 2024.
- *CSF 1.1 Quick Start Guide*, website NIST, 23 januari 2023, https://www.nist.gov/cyberframework/getting-started/quick-start-guide#:~:text=Maintain%20hardware%20and%20software%20inventory,as%20simple%20as%20a%20spreadsheet, geraadpleegd op: 7 februari 2024.
- *Cybersecurity Woordenboek 2021*, Cyberveilig Nederland, december 2021, https://cyberveilignederland.nl/woordenboek, geraadpleegd op: 2 mei 2024.
- *Eigenaarschap Huisvesting IV*, website Nederlandse Overheid Referentie Architectuur, 22 november 2021, https://www.noraonline.nl/wiki/ISOR:Eigenaarschap, geraadpleegd op: 19 september 20024.
- *iBewustzijn Overheid Bewust en veilig omgaan met (digitale) informatie!,* website VNG, (datum onbekend), https://www.vngconnect.nl/academie/Training/ibewustzijn-overheid-bewust-en-veilig-omgaan-met-digitale-informatie/edd25b97-95d3-4ce8-ac63-b26dccd91e4e, geraadpleegd op 28 maart 2024.
- *Microsoft Intune beheert op beveiligde wijze identiteiten, apps en apparaten*, website Microsoft, 16 februari 2024, https://learn.microsoft.com/nl-nl/mem/intune/fundamentals/what-is-intune, geraadpleegd op: 7 maart 2024.
- *Wat is VDI (Virtual Desktop Infrastructure)?,* website Microsoft, (datum onbekend), https://azure.microsoft.com/nl-nl/resources/cloud-computing-dictionary/what-is-virtual-desktop-infrastructure-vdi/#infrastructure, geraadpleegd op: 8 mei 2024.
- *Werk jij op je privélaptop? Wees dan extra alert*, website RTL nieuws, 18 april 2023, https://www.rtlnieuws.nl/economie/van-onze-partner/artikel/5378093/cyberupdate-persoonlijke-systemen-hacken, geraadpleegd op 8 april 2024.
- *What is: Multifactor Authentication,* website Microsoft, (datum onbekend), https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661, geraadpleegd op: 28 maart 2024.

Wet- en Regelgeving

- *2: Inventory and Control of Software Assets*, website NIST, (datum onbekend), https://csf.tools/reference/critical-security-controls/version-8/csc-2/, geraadpleegd op: 27 februari 2024.

- *Baseline Informatieveiligheid Overheden*, 2020. Geraadpleegd op: https://www.bi-overheid.nl
- *Grip op Secure Software Development Beveiligingseisen voor (web)applicaties*, Centrum Informatiebeveiliging en Privacybescherming, M. Koers & R. van der Veer, 20 juli 2020. Geraadpleegd op: https://www.cip-overheid.nl/media/clkmwp3x/20200720-ssd-normen-v30.pdf
- *Grip on Secure Software Development Security requirements for Mobile Apps*, Centrum Informatiebeveiliging en Privacybescherming, M. Koers, 25 februari 2016. Geraadpleegd op: https://www.cip-overheid.nl/productcategorieen-en-workshops/producten?product=grip-op-ssd-de-normen-voor-mobiele-apps
- *Handreiking 2-Factor authenticatie (2FA) voor gemeenten,* Informatiebeveiligingsdienst voor gemeenten, 2020. Geraadpleegd op: https://www.informatiebeveiligingsdienst.nl/product/handreiking-2-factor-authenticatie-2fa-voor-gemeenten/
- Handreiking *Beleid logische toegangsbeveiliging*, Informatiebeveiligingsdienst voor gemeenten, 2021. Geraadpleegd op: https://www.informatiebeveiligingsdienst.nl/product/beleid-logische-toegangsbeveiliging-v1-0/
- *Handreiking configuratiemanagement*, Informatiebeveiligingsdienst voor gemeenten, 2020. Geraadpleegd op: https://www.informatiebeveiligingsdienst.nl/product/handreiking-configuratiemanagement/
- *Handreiking Mobile Device Management*, Informatiebeveiligingsdienst voor gemeenten, 2018. Geraadpleegd op: https://www.informatiebeveiligingsdienst.nl/product/mobile-device-management/
- *Handreiking Personeelsbeleid gemeente*, Informatiebeveiligingsdienst voor gemeenten, 2020. Geraadpleegd op: https://www.informatiebeveiligingsdienst.nl/product/personeelsbeleid/
- *Handreiking Risicomanagement voor lijnmanagers*, Informatie Beveiligingsdienst voor gemeenten, 2020. Geraadpleegd op: https://www.informatiebeveiligingsdienst.nl/product/handreiking-risicomanagement-door-lijnmanagers/
- *Handreiking Samenhang Beheerprocessen en Informatiebeveiliging*, Informatiebeveiligingsdienst voor gemeenten, 2019. Geraadpleegd op: https://www.informatiebeveiligingsdienst.nl/product/samenhang-beheerprocessen-en-informatiebeveiliging/
- *Handreiking Telewerkbeleid*, Informatiebeveiligingsdienst voor gemeenten, 2019. Geraadpleegd op: https://www.informatiebeveiligingsdienst.nl/product/telewerkbeleid/

- *NIST Cybersecurity Framework* US National Institute of Standards and Technology, 2018. Geraadpleegd op: https://www.nist.gov/cyberframework

Overige documenten

- *Rapport Pentest Den Haag*, Hoffmann, 23 november 2023.

Overige informatie

- E-mail ambtelijke organisatie, Dienst bedrijfsvoering (DBV), 12 februari 2024.
- E-mail ambtelijke organisatie, Dienst bedrijfsvoering (DBV), 22 februari 2024.
- E-mail ambtelijke organisatie, Dienst bedrijfsvoering (DBV), 17 januari 2024.

Interviews

- Interview gemeente Den Haag, 17 januari 2024.
- Interview gemeente Den Haag, 15 februari 2024.
- Interview gemeente Den Haag, 27 februari 2024.