Rekenkamer Den Haag

Voorstel van de Rekenkamer Den Haag inzake het rekenkameronderzoek 'Veilig op afstand' naar de digitale veiligheid van mobiel werken

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 buiten de vaste werkomgeving van de gemeente waar werkzaamheden 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]

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.

Aanleiding voor dit onderzoek was dat de gemeente Den Haag sterk inzet op het uitbreiden van mobiel werken.[3] Deze ontwikkeling is niet zonder risico's. Het is daarom 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.[4] 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.[5] 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.

---

[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] Intern document *Werkplek visie Haagse Digitale Werkomgeving*, 23 februari 2023.
[4] *Handreiking Mobile Device Management*, Informatiebeveiligingsdienst voor gemeenten, december 2018, p. 6.
[5] *Handreiking Mobile Device Management*, Informatiebeveiligingsdienst voor gemeenten, december 2018, p. 6.

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,[6] 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:

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

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

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.[7] 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.

Deelconclusie 2: De gemeentelijke ICT kent op verschillende niveaus kwetsbaarheden voor de beveiliging 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.[8] 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.

3. Aanbevelingen, reactie college en nawoord rekenkamer

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

[7] *Handreiking Telewerkbeleid*, Informatiebeveiligingsdienst voor gemeenten, juli 2019, p. 12.
[8] *Handreiking Samenhang Beheerprocessen en Informatiebeveiliging*, Informatiebeveiligingsdienst voor gemeenten, juni 2019, p. 12

versterken. De aanbevelingen zijn in het dictum van het concept raadsbesluit opgenomen (zie hierna).

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. 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 volgen de aanbevelingen naar aanleiding van ons onderzoek. Per aanbeveling geven we tevens een toelichting en een beschrijving van het doel daarvan. Ook geven we een weergave van de reactie van het college en een nawoord naar aanleiding van die reactie. De volledige reactie van het college op ons onderzoek is opgenomen in het rapport 'Veilig op afstand'.

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.[9] Hierdoor heeft de gemeente beter inzicht in mogelijke bedreigingen en zwakke plekken en kan de gemeente verantwoording afleggen over gemaakte keuzes.[10]

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.

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

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

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.

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 veilig wordt omgegaan met mobiele apparaten en de gemeentelijke gegevens die erop kunnen staan.[11]

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.

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.

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

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

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.

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.

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.[12] En kan de gemeentelijke organisatie doeltreffender ingrijpen, wanneer dat nodig is.[13] Het is ook van belang dat het college borgt dat informatie in de overzichten actueel wordt gehouden.[14]

---

[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] Bedrijfsmiddelen-inventaris, website Nederlandse Overheid Referentie Architectuur, 22 november 2021, https://www.noraonline.nl/wiki/ISOR:Bedrijfsmiddelen_inventaris, geraadpleegd op: 6 mei 2024.
[14] *Eigenaarschap Huisvesting IV*, website Nederlandse Overheid Referentie Architectuur, 22 november 2021, https://www.noraonline.nl/wiki/ISOR:Eigenaarschap, geraadpleegd op: 19 september 2024.

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.

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

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.[15] 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.[16] Middels de inzet van diverse instrumenten op het gebied van medewerkersbewustzijn kan het college de beveiliging van mobiel werken verbeteren.[17]

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.

[15] *Handreiking Telewerkbeleid*, Informatiebeveiligingsdienst voor gemeenten, juli 2019, p. 11 en 12.
[16] https://www.noraonline.nl/wiki/ISOR:Training_en_Awareness
[17] *Personeelsbeleid gemeente*, Informatiebeveiligingsdienst voor gemeenten, mei 2020.

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

Het doel van deze aanbeveling is de door de rekenkamer geconstateerde risico's beter te beheersen.[18] 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.

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.

[18] *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.

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

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.

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.

Raadsbesluit 'Veilig op afstand', rekenkameronderzoek naar de digitale veiligheid van mobiel werken

Gezien het vorenstaande stelt de rekenkamer de raad voor het volgende besluit te nemen:

De raad van de gemeente Den Haag,

Gelet op artikel 185, tweede lid Gemeentewet en de aanbevelingen van de Rekenkamer Den Haag uit het rapport ‘Veilig op afstand’.

Besluit het college het volgende op te dragen:

I: 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 hiervan 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. Hierdoor heeft de gemeente beter inzicht in mogelijke bedreigingen en zwakke plekken en kan de gemeente verantwoording afleggen over gemaakte keuzes.

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

Het doel hiervan 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 veilig wordt omgegaan met mobiele apparaten en de gemeentelijke gegevens die erop kunnen staan.

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

Het doel hiervan 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.

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

Het doel hiervan 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. En kan de gemeentelijke organisatie doeltreffender ingrijpen, wanneer dat nodig is. Het is ook van belang dat het college borgt dat informatie in de overzichten actueel wordt gehouden.

II: Medewerkers van de gemeente bewust en medeverantwoordelijk te maken voor de veiligheid van mobiel werken

Het doel hiervan 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. 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. Middels de inzet van diverse instrumenten op het gebied van medewerkersbewustzijn kan het college de beveiliging van mobiel werken verbeteren.

III: Bestaande technische mogelijkheden voor toegangsbeveiliging beter te benutten, om zo de door de rekenkamer geconstateerde risico's beter te beheersen

Het doel hiervan is de door de rekenkamer geconstateerde risico's beter te beheersen. 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.

IV: 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

Aldus besloten in de openbare raadsvergadering van DATUM

De griffier De voorzitter