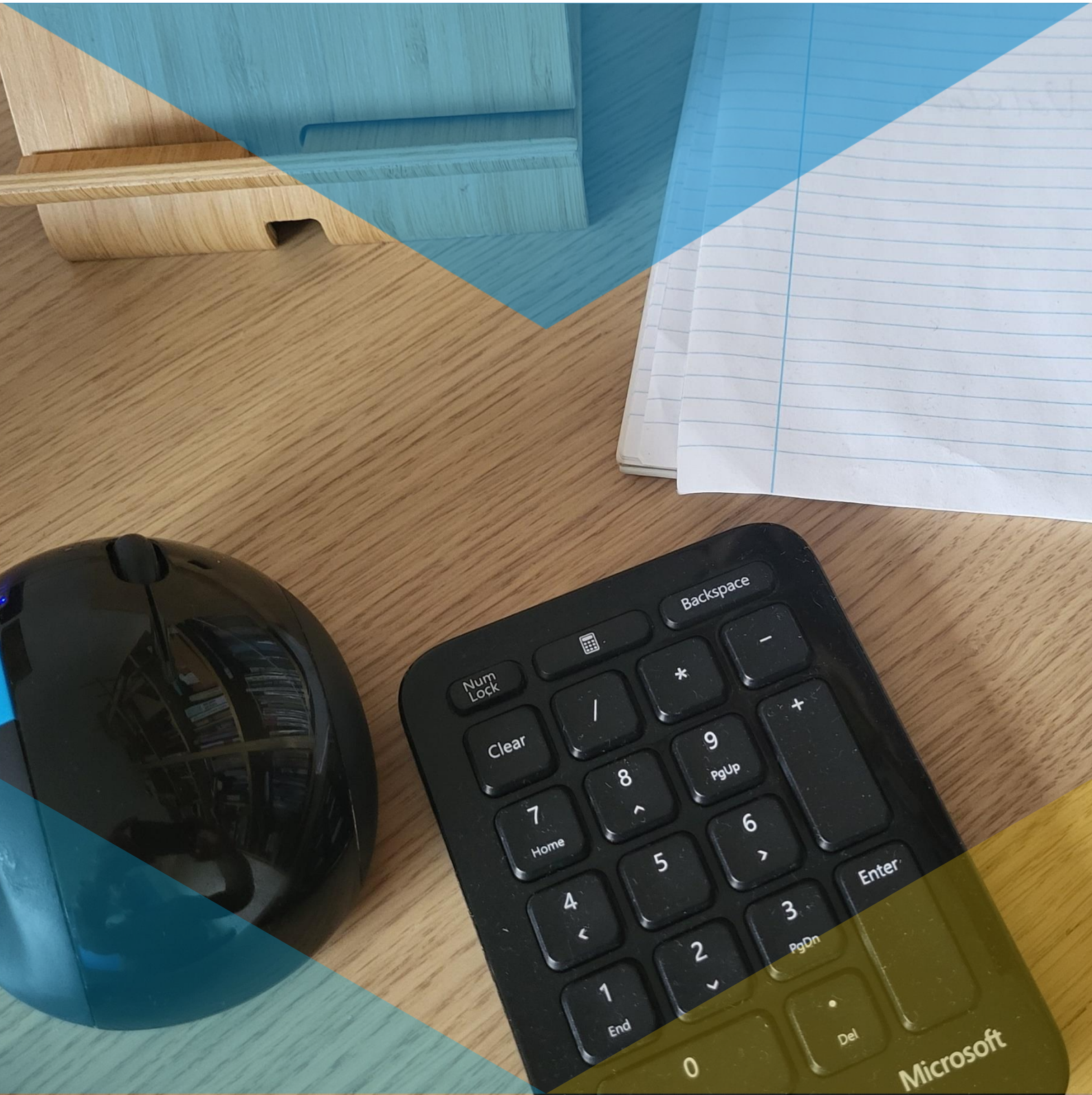
Rekenkamer
Den Haag

Veilig thuiswerken

Digitale beveiliging van thuiswerken bij de gemeente Den Haag - onderzoeksopzet
oktober 2023 *RIS316694*



1. Inhoudsopgave

2. Inleiding en leeswijzer

Sinds het begin van de Coronacrisis heeft de gemeente Den Haag de mogelijkheden om thuis te werken sterk uitgebreid. De toegang tot gemeentelijke systemen is daarmee verlegd van voornamelijk vanaf werkplekken op gemeentelijke werklocaties naar toegang via internet vanaf werkplekken binnen of buiten gemeentelijke werklocaties. De gemeente beheert veel informatie, waarvan een deel gevoelig is. Gevoelige informatie kan gaan over mensen en over bedrijven. Een goede beveiliging van deze informatie is nodig om de belangen van individuen en bedrijven niet te schaden. Dit onderzoek richt zich op de vraag in hoeverre de sterke toename van thuiswerken heeft geleid tot kwetsbaarheden in de beveiliging van de gemeentelijke informatie en communicatie technologie.

3. Centrale onderzoeksvraag. In hoeverre waarborgt de gemeente de beveiliging van toegang tot gemeentelijke systemen en informatie vanuit thuiswerkplekken?

Dit korte onderzoek heeft als doel een oordeel te geven over de uitvoering en het beleid ten aanzien van de beveiliging van de toegang tot gemeentelijke systemen via thuiswerkfaciliteiten. Het gaat daarbij over de beveiliging van de diverse mogelijkheden die de gemeente biedt om gemeentelijke informatiesystemen te benaderen, zoals via Citrix, Sharepoint of vanaf lokaal (thuis) geïnstalleerde applicaties (OneDrive, Microsoft Teams, Microsoft Word etc.) en via internet benaderbare systemen (Werknet, TopDesk, P-digitaal, Oracle EBS, etc.).

De verwachting is dat dit onderzoek eventuele kwetsbaarheden in de beveiliging van thuiswerkplekken blootlegt. Daarnaast is het mogelijk dat er in de kaderstelling en aansturing van het beveiligingsbeleid zaken zijn die verbeterd kunnen worden. De uitkomst van dit onderzoek kan dan ook zijn dat de gemeente zowel in het beleid als in de aansturing en uitvoering van informatiebeveiliging verbeteringen door kan voeren.

Kwetsbaarheden worden in dit onderzoek omschreven als mogelijkheden om ongeoorloofd toegang te krijgen tot gemeentelijke informatie en systemen.

Het onderzoek beperkt zich nadrukkelijk tot de beveiliging(en) van de verschillende vormen van toegang tot informatie en systemen via thuiswerkfaciliteiten.

Op basis van de centrale onderzoeksvraag worden de volgende deelvragen gesteld:

Deelvraag 1. In hoeverre waarborgt de gemeente in de praktijk de beveiliging van toegang tot gemeentelijke systemen vanaf thuiswerkplekken?

Deze deelvraag valt uiteen in de volgende onderzoeksvragen:

- Op welke wijze kunnen niet legitieme gebruikers toegang krijgen tot (gegevens op) laptops van de gemeente en privé computers (evt. ook telefoons)?
- Op welke wijze kunnen niet legitieme gebruikers toegang krijgen tot gemeentelijke systemen met behulp van laptops van de gemeente en privé-computers?
- Op welke wijze kunnen legitieme gebruikers van de gemeente beveiligingsmaatregelen voor thuiswerken omzeilen of uitschakelen op laptops van de gemeente en privé-computers?
- In hoeverre zijn systemen van de gemeente voor toegang beveiligd met meer factor authenticatie?
- In hoeverre wordt niet legitiem gebruik opgemerkt door de gemeente Den Haag en welke opvolging wordt gegeven aan opgemerkt niet legitiem gebruik?

Deelvraag 2. In hoeverre waarborgt de gemeente in het beleid en de uitvoering daarvan de beveiliging van toegang tot gemeentelijke systemen vanaf thuiswerkplekken?

Deze deelvraag valt uiteen in de volgende onderzoeksvragen:

- In hoeverre voldoet de gemeente aan de daaraan te stellen vereisten voor de beveiliging van de toegang van systemen en informatie vanuit thuiswerkplekken?
- In hoeverre zijn oorzaken van feitelijke kwetsbaarheden in de toegang tot systemen en informatie vanuit thuiswerkplekken gelegen in het beleid en de uitvoering daarvan?

4. Hierom doen wij dit onderzoek

Thuiswerken is sinds de Coronacrisis sterk uitgebreid

Kort na het begin van de Coronacrisis, in maart 2020, heeft de gemeente Den Haag in zeer korte tijd een sterke uitbreiding doorgevoerd van het aantal thuiswerkmogelijkheden. Er kunnen sindsdien veel meer mensen vanuit huis werken en er zijn meer faciliteiten beschikbaar. Ook is de gemeente sinds begin 2020 in één stap overgegaan naar het werken vanuit een clouddienst voor de reguliere digitale kantooromgeving (Microsoft Sharepoint). De sterke uitbreidingen van mogelijkheden en functies die via internet beschikbaar zijn leidt tot de vraag of de beveiliging van deze mogelijkheden en functies gelijk op is gegaan. Of heeft dit mogelijk tot kwetsbaarheden geleid in de gemeentelijke informatisering.

Den Haag beheert veel informatie, waaronder gevoelige informatie

Den Haag heeft veel informatie, waaronder informatie over inwoners van de stad en gegevens over bijvoorbeeld beveiliging en infrastructuur in de stad. Informatie kan gevoelig zijn wanneer personen, organisaties of de samenleving geschaad kunnen worden door het ongeoorloofde gebruik ervan. De beveiliging van deze informatie is dan ook van belang. Het onderwerp is daarnaast relevant vanwege de al genoemde sterke toename van de mogelijkheden om toegang te krijgen tot gemeentelijke systemen via het internet. Dat wil

zeggen vanaf andere plekken dan reguliere werkplekken in het stadhuis. Met deze toename van mogelijkheden is ook het aantal te beveiligen toegangen sterk toegenomen.

5. Zo pakken we dit onderzoek aan

Onderzoek naar praktijk en beleid

In dit korte onderzoek wordt vanuit de praktijk onderzocht welke kwetsbaarheden er zijn bij het thuiswerken binnen de Gemeente Den Haag en wat mogelijke oorzaken zijn van (aangetroffen) kwetsbaarheden. Het onderzoek richt zich in eerste instantie op het zoeken naar kwetsbaarheden. Hierbij wordt gekeken naar de toegang tot gemeentelijke systemen, naar de monitoring en opvolging van niet-legitieme activiteiten tijdens het onderzoek en naar de beveiliging via multifactor authenticatie in de toegang tot diverse systemen (zie bijlage Systemen voor thuiswerken voor een opsomming van een aantal van deze systemen). Voor dit deel van het onderzoek wordt een opdracht verstrekt aan een ter zake deskundig externe onderzoeksbureau (zie de bijlage Opdrachtomschrijving praktijkonderzoek voor een nadere omschrijving van dit onderdeel van het onderzoek)

Daarnaast voeren wij een onderzoek uit naar mogelijke achterliggende oorzaken van kwetsbaarheden in de toegang vanaf thuiswerkplekken. Daarbij wordt ook onderzocht in hoeverre de Gemeente zich houdt aan geldende wet- en regelgeving en/of de afspraken die zij heeft gemaakt.

Ten behoeve van het (extern uitgevoerde) onderzoek naar feitelijke kwetsbaarheden zal nauw overleg worden gevoerd met de gemeentelijke organisatie verantwoordelijk voor ICT en de beveiliging daarvan. Aandachtspunten daarbij zijn in ieder geval de vrijwaring door de gemeente voor dit onderzoek, mogelijk risico's en risico scenario's en beheersmaatregelen van benoemde risico's.

De rapporten van de rekenkamer zijn openbaar

De uitkomsten van het praktijkonderzoek en het onderzoek naar achterliggende oorzaken in beleid en uitvoering worden opgenomen in een feitenrapport.[1] Dit rapport legt de rekenkamer voor aan de ambtelijke organisatie voor een controle op onjuistheden en vertrouwelijke informatie. Op basis van het feitenrapport zal de rekenkamer een bestuurlijk rapport opstellen. Dit rapport wordt voorafgaand aan publicatie voorgelegd aan het college van burgemeester en wethouders voor een bestuurlijke reactie.[2]

---

[1] *Omdat het feitenrapport op grond van art. 185 eerste en zesde lid van de gemeentewet openbaar is en geen vertrouwelijke informatie mag bevatten, zal feitelijke informatie over kwetsbaarheden hierin niet worden opgenomen. Wanneer nodig zal de rekenkamer gebruik maken van de mogelijkheid om de gemeenteraad en/of het college aanvullend aan het openbare rapport vertrouwelijk te informeren over uitkomsten van het onderzoek (art. 185, derde lid, gemeentwet).*

[2] *Zie voor meer informatie het onderzoeksprotocol van de rekenkamer (https://www.rekenkamerdenhaag.nl/wp-content/uploads/2023/05/Onderzoeksprotocol-gemeente-2023-05-19.pdf)*

We beoordelen het beleid en de uitvoering aan de hand van normen

Voor dit onderzoek houdt de rekenkamer een normenkader aan. Aan de hand van het normenkader worden beleid en uitvoering van de gemeente beoordeeld. Het normenkader is gebaseerd op verschillende bronnen. Hierbij kijkt de Rekenkamer allereerst naar het basisnormenkader voor informatiebeveiliging binnen de overheid. Dit is de Baseline Informatiebeveiliging Overheid (BIO). De gemeente dient zich te houden aan de BIO.

Daarnaast zullen we ook kijken naar andere afspraken, plannen en ambities die de gemeente heeft gemaakt rondom digitale veiligheid met thuiswerken. Deze zullen voortkomen uit bestuurlijke documenten.

Afbakening beperkt zich tot thuiswerken

Het onderzoek beperkt zich tot:

- Thuiswerken vanaf een computer, zowel een door de gemeente beschikbaar gestelde laptop als een privé computer met Windows OS. Eventueel ondersteunende apparaten voor het verkrijgen van toegang vallen hier ook onder (bijvoorbeeld mobiele telefoon met MFA app)
- Optioneel worden ook andere apparaten en andere OS (dan windows) betrokken bij het onderzoek.
- Standaard kantoor applicaties (dus niet de specifieke toepassingen die alleen beschikbaar zijn voor bepaalde diensten of afdelingen van de gemeente, bijvoorbeeld SUWINET).

Het onderzoek zal zich in ieder geval niet richten op:

- Kwetsbaarheden in de ICT-beveiliging binnen systemen (bijvoorbeeld mogelijkheden om toegangsrechten op te schalen, kwetsbaarheden in de kantoorwerkomgeving, printers etc.)
- Kwetsbaarheden in de website of WIFI-netwerken van de gemeente.
- Andere vormen van toegang dan via een computer met Windows OS (Gemeente Den Haag/Privé).

Geplande datum van publicatie is maart 2024

Voor dit korte onderzoek gaan we uit van de volgende planning:

Onderzoeksplan	Sept/okt 2023
Uitvoeren praktijkonderzoek	Oktober 2023
B**eleidsonderzoek**	Oktober/november2023
Opstellen onderzoeksrapport	November 2023

Feitelijk wederhoor+ twee weken verwerking reactie en gesprek ambtelijke organisatie	December 2023
Bestuurlijk wederhoor	Februari 2024
Publicatie	Maart 2024

6. Bijlagen

6.1 Welke wet- en regelgeving is van toepassing?

De gemeente moet voldoen aan het Baseline Informatiebeveiliging Overheden (BIO). Dit besluit richt zich op alle vormen van informatie en de beveiliging daarvan. Daarnaast is de gemeente verplicht zorgvuldig om te gaan met persoonsgegevens van inwoners en medewerkers van de gemeente. Hiervoor is de Europese Algemene Verordening Gegevensbescherming (AVG) en de Nederlandse uitwerking daarvan in de Uitvoeringswet AVG het wettelijk kader.

6.2 Hoe is de gemeentelijke beleidsuitvoering georganiseerd?

De dienst bedrijfsvoering is verantwoordelijk voor de gemeentelijke ICT en voor de beveiliging daarvan. Daarnaast zijn medewerkers van de dienst belast met de taken van de Concern Information Officer (CIO, de algemeen directeur DBV) en de Central Information Security Officer (CISO). De directie Informatisering & Automatisering is binnen DBV verantwoordelijk voor de uitvoering van de gemeentelijke ICT en voor de beveiliging daarvan.

6.3 Opdrachtomschrijving praktijkonderzoek

Uitgaande van de onderzoeksopzet ‘Digitale Veiligheid Thuiswerken’ wil de rekenkamer het volgende onderzoek laten uitvoeren door een externe partij.

Het onderzoek volgt drie sporen:

1. Windowslaptop voor thuiswerken van de gemeente Den Haag
2. Privé Windows computer/-laptop
3. Overige devices (telefoons, tablets) en operating systems (Apple, Android, Linux).

Beide computers (onder 1 en 2) zijn volledig geconfigureerd voor (standaard) thuiswerken bij de gemeente Den Haag en zijn ook actief in gebruik.[3] Dat wil zeggen dat er standaard

[3] *Voor de privé computer wordt dit gedaan door een medewerker van de rekenkamer. De gemeente heeft dus geen invloed (vooraf) op deze computer.*

kantoorapplicaties zijn geïnstalleerd of benaderbaar zijn. Daarnaast is via de verschillende toegangsmogelijkheden al ingelogd (geweest). Eventuele sessioncookies, gebruikersnamen en wachtwoorden zijn dus mogelijk al opgeslagen. Op beide laptops zijn in ieder geval geïnstalleerd:

- Govroam (standaard Wifi toegang voor medewerkers op locaties van de gemeente)
- Microsoft office applicaties
- Microsoft Teams
- Citrix / DVI toegang

Ten behoeve van dit onderzoek wordt een user-account van een reguliere medewerker aangemaakt.[4]

Het onderzoek richt zich op de volgende doelstellingen:

Toegang

- Het proberen toegang te krijgen tot beide laptops
- Toegang als zodanig
- Bereiken, kopiëren, bewerken van informatie op de laptop (toegangsinformatie en/of Gemeente Den Haag bestanden)
- Het proberen via beide laptops toegang te krijgen tot de gemeentelijke systemen (zie de bijlage voor een overzicht van systemen die voor thuiswerken beschikbaar zijn).
- Het als legitieme gebruiker omzeilen van beveiligingsmaatregelen (scope is beperkt tot toegang krijgen. Het gaat dus bijvoorbeeld om het omzeilen van MFA waar dat in eerste instantie wel gevraagd wordt of het verlengen van session cookies. Het gaat niet om bijvoorbeeld het zich toe-eigenen van hogere rechten binnen de systemen van de gemeente).

Monitoring

- Testen van de monitoring door de gemeente:
- Herkenning van pogingen om toegangsbeveiliging te omzeilen
- Herkenning van kwaadwillende software (o.a. draaien van Kali zou herkend worden door de gemeente).

[4] *Nader te bepalen: niveau toegang voor betreffend account. Een medewerker heeft minder mogelijkheden dan een manager. In overleg met opdrachtnemer niveau bepalen.*

MFA scan

- Het inventariseren van MFA vereisten voor systemen van de gemeente Den Haag

6.4 Systemen thuiswerken

De onderstaande systemen zijn in ieder geval benaderbaar via internet en vragen in de praktijk niet altijd (of langere tijd niet) om een verificatie bij toegang. De lijst is opgesteld op basis van eigen ervaringen van de rekenkamer en is niet uitputtend.

1. Outlook
2. Microsoft Office suite (Word, Excel, Powerpoint)
3. OneDrive
4. SharePoint
5. Werknet
6. Microsoft Teams
7. VDI (Citrix)
8. P-digitaal, van alle medewerkers:
    a. Ziekmeldingen
    b. Persoonsgegevens van de medewerkers, waaronder inschaling en privé contactgegevens
    c. Personeelsdossier: aanstellingsbesluiten, contractwijzigingen, ambtseed, VOG, etc.
    d. Loonstrookjes, jaaropgaaf
    e. Afspraken, voortgang en beoordelingen functioneringsgesprekken
    f. Nevenwerkzaamheden
    g. Opleidingen
    h. Oracle autoriseren facturen, declaraties, personeelsbesluiten en verlof.
9. XpertSuite (verzuimdossiers van alle medewerkers)
10. TopDesk, waaronder het voor anderen aanvragen van:
    i. Toegang tot netwerkmappen
    j. Nieuwe gastaccounts
    k. Nieuwe applicaties
    l. Telefoons
    m. Doorgeven van storingen
11. Planon (Reserveringen vergaderzalen en catering)
12. Lightning Force (systeem voor selectie van kandidaten voor vacatures)