Rapportage doelmatigheid fysieke toegang en beveiliging

(onderzoek conform art. 213a Gemeentewet)



Steller: [redacted]

Afdeling: Stadscontrol

Datum: November 2025

Inhoud

1. Inleiding 3
   1.1 Aanleiding onderwerp 3
   1.2 Doel onderzoek 3
   1.3 Leeswijzer 3
2. Aanpak & onderzoeksmethode 4
3. Samenvatting bevindingen 5
4. Belangrijkste bevindingen fysieke toegang en beveiliging 7
5. Toetsing aan BIO-normen 9
6. Reflecties en aanbevelingen 12
7. Kosten bestaande en nieuwe maatregelen 17
8. Conclusie 18

1. Inleiding

1.1 Aanleiding onderwerp

Met de gemeenteraad is afgesproken dat jaarlijks een doelmatigheidsonderzoek (conform art. 213.a Gemeentewet) wordt uitgevoerd. Doelmatigheid gaat over de mate waarin een maximale hoeveelheid producten en prestaties is gerealiseerd met een minimale hoeveelheid middelen of een hogere kwaliteit wordt bereikt met een gelijkblijvende hoeveelheid aan middelen.

Dit jaar richten we ons op de doelmatigheid van ons beleid rondom fysieke toegang en beveiliging van onze gemeente als belangrijke maatregelen voor informatiebeveiliging en het beschermen van (persoons)gegevens. In de Baseline Informatiebeveiliging Overheid (BIO[1]) staat opgenomen op welke wijze fysieke beveiliging vormgegeven en geïmplementeerd moet worden.

Het doel van fysieke beveiliging is meerledig. Fysieke beveiligingsmaatregelen zoals onze toegangspoortjes, afgesloten ruimtes of deuren met kaartlezers zorgen ervoor dat alleen geautoriseerd personeel toegang heeft tot gevoelige informatie, hardware en/of IT-systemen. Door middel van beveiligingssystemen zoals alarmsystemen, bewakingscamera's en beveiligingspersoneel wordt daarnaast het risico op fysieke inbraak en diefstal verminderd.

Ondanks deze maatregelen kunnen zich veiligheidsincidenten voordoen waarbij onbevoegden toch toegang krijgen tot de kantoorgebouwen. Een eerder bezoek van een mystery guest (2022) en de recente incidenten waarbij dezelfde inwoner drie keer de beveiligde zones van een van de gebouwen is binnengedrongen, laten zien dat de huidige technische maatregelen niet alle risico's kunnen voorkomen. Het gedrag en de alertheid van medewerkers vormen dan ook een even belangrijke factor bij het voorkomen van deze risico's. Dit onderzoek richt zich daarom zowel op de 'harde' technische maatregelen als op het gedrag en de naleving door medewerkers.

1.2 Doel onderzoek

Het doel van dit onderzoek is de **doelmatigheid** van het gemeentelijk beleid voor fysieke toegang en beveiliging te evalueren. Hierbij richten we ons op de vraag: In hoeverre worden de gewenste prestaties en maatschappelijke effecten op het gebied van fysieke toegang en beveiliging - als belangrijk onderdeel van informatiebeveiliging - effectief gerealiseerd met een optimale inzet van middelen?

Hoewel er geen afzonderlijke doelstellingen voor fysieke toegang en beveiliging formeel zijn vastgesteld, sluiten de ambities aan bij de bredere maatschappelijke doelstellingen voor informatiebeveiliging. Het strategisch informatiebeveiligingsbeleid 2022 stelt onder meer dat "een betrouwbare informatievoorziening noodzakelijk is voor het goed functioneren van de gemeente en de basis vormt voor het beschermen van de identiteit en democratische rechten van burgers en bedrijven. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn." Daarnaast is vastgelegd: "Door het treffen van technische en organisatorische maatregelen willen we onze informatie beschermen en de kwaliteit waarborgen. We willen ons volwassenheidsniveau als gemeente verhogen en tegelijkertijd voldoen aan wet- en regelgeving."

De resultaten van dit onderzoek ondersteunen een hernieuwde risicoafweging en bieden input voor mogelijke aanscherping van de fysieke beveiligingsmaatregelen.

1.3 Leeswijzer

Dit rapport is als volgt opgebouwd:

- *§2 – Aanpak en onderzoeksmethode:* toelichting op de werkwijze en de gebruikte onderzoeksmethoden.
- *§3 – Samenvatting bevindingen:* een beknopt overzicht van de belangrijkste uitkomsten.
- *§4 – Belangrijkste bevindingen fysieke toegang en beveiliging:* presentatie van de kernpunten in de vorm van een korte SWOT-analyse.

[1] Baseline Informatiebeveiliging Overheid - het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen

- *§5 – Toetsing aan BIO-normen:* overzicht van de relevante BIO-normen en de mate waarin onze gemeente hieraan voldoet.
- *§6 – Reflectie en aanbevelingen:* interpretatie van de bevindingen en concrete verbeterpunten.
- *§7 – Kosten van bestaande en nieuwe maatregelen:* inzicht in de kosten van bestaande én mogelijke nieuwe maatregelen.
- *§8 – Conclusie:* afsluitende samenvatting en totaal oordeel.

2. Aanpak & onderzoeksmethode

We hebben ons tijdens dit onderzoek gefocust op de locaties Mariënburg, Stadhuis en het Regionaal Archief Nijmegen (RAN). Het gaat dan met name om de beveiligde zones van deze gebouwen, waar over het algemeen met gevoelige informatie wordt gewerkt. Een beveiligde zone wil zeggen dat toegang uitsluitend kan worden verkregen met een medewerker- of bezoekerspas. Hiervoor onderzochten we de periode vanaf de invoering van de poortjes in het Stadhuis en de Mariënburg (1 oktober 2021) tot heden.

De centrale onderzoeksvraag was:

In hoeverre dragen onze inspanningen rondom fysieke beveiligingsmaatregelen effectief en kostenefficiënt bij aan onze doelstellingen op het gebied van informatiebeveiliging?

De deelvragen:

1) Welke ambitie hebben we op het vlak van fysieke beveiliging?
2) Welke maatregelen treffen we op het gebied van fysieke beveiliging?
3) Wat zijn de jaarlijkse kosten van deze maatregelen?
4) Zijn er aanvullende maatregelen nodig om de ambitie te halen? En tegen welke extra kosten of inspanningen?
5) In hoeverre worden de maatregelen nageleefd door de medewerkers?
6) Welke bijdrage leveren deze maatregelen aan het behalen van onze doelstellingen om te voldoen aan de BIO?
7) Zijn er ook alternatieve maatregelen die een vergelijkbaar effect hebben?
8) Welke (aanvullende) interventies zijn nodig om de efficiëntie verder te vergroten?

Onderzoeksmethode

We hebben een analyse uitgevoerd van bestaande beleidsdocumenten, protocollen, procedures en eerdere onderzoeken en aanbevelingen met betrekking tot fysieke toegang en beveiliging. Daarnaast hebben we interviews gevoerd en de fysieke beveiligingsmaatregelen geïnventariseerd die op dat moment in gebruik waren. Met steekproefsgewijze waarnemingen bij de receptie van het Stadhuis en in de Stadswinkel hebben we een beeld gevormd van de naleving en uitvoering van de beveiligingsmaatregelen binnen de organisatie. Tot slot hebben we ons huidige beveiligingsniveau vergeleken met dat van drie vergelijkbare G40 - gemeenten en met normen en handreikingen binnen de sector (BIO/BIO2/IBD).

Presentatie van de uitkomsten

Bij de presentatie van de uitkomsten zijn enkele constateringen bewust in algemene termen beschreven, om het risico op misbruik van interne kwetsbaarheden te beperken. De gedetailleerde constateringen zijn opgenomen in een ambtelijke uitwerking en onder de aandacht gebracht bij de betreffende afdelingen.

3. Samenvatting bevindingen

In dit onderzoek stond de vraag centraal in hoeverre onze inspanningen op het gebied van fysieke beveiligingsmaatregelen effectief en kostenefficiënt bijdragen aan de gemeentelijke doelstellingen voor informatiebeveiliging.

Wij concluderen dat het beleid en de maatregelen voor fysieke toegang en beveiliging in de kern doelmatig zijn. Met redelijke middelen wordt een solide basisniveau bereikt dat vergelijkbaar is met dat van drie andere G40-gemeenten die we in het kader van dit onderzoek gesproken hebben. Niet alle kosten konden volledig inzichtelijk worden gemaakt vanwege de verwevenheid met andere uitgaven. Hetzelfde zien we bij de drie andere gemeenten, waardoor een directe kostenvergelijking niet mogelijk was. Toch achten wij de getroffen maatregelen over het geheel genomen efficiënt.

Met enkele kleinere interventies en maatregelen kan de doelmatigheid verder worden vergroot. Met meer ingrijpende aanpassingen is naar verwachting zelfs een substantiële verbetering van de effectiviteit mogelijk.

Hieronder lichten wij per deelvraag de belangrijkste bevindingen en conclusies uit dit onderzoek toe.

1) Welke ambitie hebben we op het vlak van fysieke beveiliging?

Gemeente Nijmegen heeft de ambitie om minimaal te voldoen aan de geldende normen in de BIO[2]. Daarin staat beschreven aan welke controls gemeenten moeten voldoen.

2) Welke maatregelen treffen we op het gebied van fysieke beveiliging?

Zowel het Stadhuis als de Mariënburg kennen verschillende beveiligingszones. Bij beide kantoorgebouwen is toegang via poortjes alleen mogelijk met een toegangspas. Voor bezoekers geldt een bezoekersprocedure met aanmeldplicht. Ook voor leveranciers en monteurs zijn specifieke afspraken gemaakt. Naast de poortjes is bij de trappenhuizen en liften een paslezer geplaatst. Voor een aantal afdelingen zijn risicogericht extra maatregelen getroffen en afspraken gemaakt. Denk aan afgesloten deuren met paslezers en beperkte toegang voor andere medewerkers. Elke avond worden de gebouwen gecontroleerd door de beveiliging en buiten de kantooruren wordt het alarm ingeschakeld.

3) Wat zijn de jaarlijkse kosten van deze maatregelen?

Het onderhoud van het toegangssysteem i-Protect kost jaarlijks ongeveer €15.000 en de aanschaf van nieuwe toegangspassen circa €8.000. Deze bedragen geven slechts een indicatie van de kosten omdat deze verweven zijn met andere maatregelen zoals gebouwbeheer, brandveiligheid en ICT-beveiliging. Een afzonderlijk kostenoverzicht is daardoor niet zonder grote inspanning te realiseren. Ter illustratie: Heyday maakt jaarlijks circa €16.600 aan onderhoudskosten voor hardware (deurcontrollers, lezers) en voert namens de gemeente Nijmegen het regie- en technisch beheer uit van de vastgoedportefeuille. Deze kosten komen ten laste van het gemeentelijk onderhoudsbudget.

4) Zijn er aanvullende maatregelen nodig om de ambitie te halen? En tegen welke extra kosten of inspanningen?

Om minimaal te voldoen aan de BIO, dient een sleutelplan opgesteld te worden en de registratie van fysieke sleutels te worden verbeterd. Daarnaast kunnen aanvullende interventies en maatregelen de fysieke toegangsbeveiliging verder versterken. Een aantal maatregelen kan tegen minimale extra kosten worden gerealiseerd (zie deelvraag 8). Twee voorgestelde maatregelen vergen echter een aanzienlijke eenmalige investering: de overstap naar DESFire (ca. €125.000) en de volledige uitrol van role-based access (kosten nog onbekend).

5) In hoeverre worden de maatregelen nageleefd door de medewerkers?

Hoewel de naleving van de toegangsafspraken sinds de introductie van de poortjes verbeterd is, doen zich nog dagelijks incidenten voor. De naleving van de basisafspraken rondom fysieke toegang is wisselend. Overtredingen

[2] Op het moment van dit onderzoek betreft dit BIO versie 1.04.

betreffen met name het (on)juiste gebruik van de poortjes door medewerkers en bezoekers. Daarnaast worden bezoekers niet altijd conform procedure aangemeld of terug begeleid naar de uitgang. Binnen de afdelingen met aanvullende maatregelen is de naleving over het algemeen op orde.

6) Welke bijdrage leveren deze maatregelen aan het behalen van onze doelstellingen om te voldoen aan de BIO?

De getroffen maatregelen dragen in hoge mate bij aan het realiseren van onze doelstelling en ambitie om te voldoen aan de BIO. Enkele aanvullende interventies en maatregelen kunnen dit verder verbeteren.

7) Zijn er ook alternatieve maatregelen die een vergelijkbaar effect hebben?

Uit dit onderzoek kwamen geen alternatieve goedkopere maatregelen waarmee een vergelijkbaar beveiligingsniveau bereikt kan worden. Aanvullende maatregelen die op termijn ons beveiligingsniveau verbeteren, vragen om een extra investering. Denk aan het volledig implementeren van role-based access en automatische deactivering van rechten bij functiewijzigingen. Daarnaast zijn de huidige Mifare-chips in de toegangspassen verouderd en kwetsbaar. De toegangspassen kunnen daardoor makkelijk gekopieerd worden door kwaadwillenden. De overstap naar DESFire of een app-gebaseerd toegangssysteem verlaagt op termijn structureel het risico op misbruik.

8) Welke (aanvullende) interventies zijn nodig om de efficiëntie verder te vergroten?

De effectiviteit van de poortjes kan relatief eenvoudig worden verbeterd, door een anti-pass-back functie te activeren. Hierdoor kan hetzelfde pasje niet twee keer worden gebruikt om toegang te verkrijgen. Ook het gebruiksvriendelijker maken van de bezoekersregistratie in Planon door de migratie naar de Cloud vergroot naar verwachting de naleving. Buiten de openingstijden van de kantoorgebouwen zouden de toegangspassen geblokkeerd kunnen worden om onnodige kosten vanwege de activering van het alarm te voorkomen. Een goede onboarding en regelmatige communicatie over huisregels kunnen de effectiviteit van bestaande maatregelen vergroten, zonder noemenswaardige extra kosten.

4. Belangrijkste bevindingen fysieke toegang en beveiliging

Hieronder volgt een SWOT-overzicht met de belangrijkste bevindingen uit het onderzoek. De bevindingen zijn ingedeeld in de vier kwadranten ‘Sterktes’, ‘Zwaktes’, ‘Kansen’ en ‘Bedreigingen’. Een toelichting op deze begrippen staat onder de analyse.

SWOT Fysieke toegang en beveiliging



Toelichting begrippen

Als inkleuring van die begrippen de volgende leidraad:

- Sterk: beschrijving van wat je ziet, ervaart, hoort wat als sterk/positief beschouwd kan worden. Voor sturing vanuit het management betekent dit: draag zorg voor behoud van deze waarden.
- Zwak: idem maar dan zwak/negatief. Voor sturing vanuit het management betekent dit: zorg ervoor dat deze acties en handelingen stoppen.

[3] Eenduidige Normatiek Single Information Audit - is een gestandaardiseerde verantwoordingsmethode voor gemeenten op het gebied van informatiebeveiliging.

- Kans: beschrijving van een beweging, richting, koers of trend die als positief of kansrijk ervaren kan worden. Dat hoeft dus niet feitelijk zo te zijn. Het gaat er hier om dat je dit soort bewegingen, signalen of “kansen” ziet en wilt duiden. Voor sturing vanuit het management betekent dit: zet méér energie (inzet mensen en het geven van prioriteit) op deze kansen.
- Bedreiging: idem maar dan als negatief en bedreigend. Voor sturing vanuit het management betekent dit: bespreek regelmatig deze bedreigingen en onderneem acties daartegen.

5. Toetsing aan BIO-normen

Gemeente Nijmegen streeft ernaar om minimaal te voldoen aan de geldende normen uit de Baseline Informatiebeveiliging Overheid (BIO[4]). De BIO beschrijft de eisen en maatregelen waaraan overheidsorganisaties moeten voldoen op het vlak van informatiebeveiliging.

In de BIO zijn de ISO-controls[5] (beheersmaatregelen) opgenomen die relevant zijn voor de overheid. Waar nodig zijn deze uitgewerkt in verplichte overheidsmaatregelen (zie BIO versie 1.04, p. 14). Hoofdstuk 11 van de BIO richt zich op 'fysieke beveiliging en beveiliging van de omgeving'. Het gaat hier onder meer om fysieke beveiligingszones, fysiek toegangsbeleid, beveiligen van kantoren, ruimten en faciliteiten, bescherming tegen bedreigingen van buitenaf, werken in beveiligde gebieden en tenslotte laad- en losruimten.

Om te bepalen in hoeverre de gemeente voldoet aan haar ambitie op het gebied van fysieke toegang en beveiliging, is in onderstaande tabel weergegeven in welke mate aan de betreffende BIO-normen wordt voldaan.

11.1.1 Fysieke beveiligingszone	
ISO-control	Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten.
Verplichte overheidsmaatregel	Er wordt voor het inrichten van beveiligde zones gebruik gemaakt van standaarden.
Voldoet aan BIO norm?	Ja. De dienstgebouwen zijn voorzien van zonering. In sommige gevallen zijn aanvullende maatregelen getroffen binnen specifieke afdelingen, zoals bij Publiekszaken en Handhaving en Toezicht. Deze ruimten zijn afgesloten en alleen toegankelijk met een toegangspas.
11.1.2 Fysieke toegangsbeveiliging	
ISO-control	Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.
Verplichte overheidsmaatregel	In geval van concrete beveiligingsrisico's worden waarschuwingen, conform onderlinge afspraken, verzonden aan de relevante collega's binnen het beveiligingsdomein van de overheid.
Voldoet aan BIO norm?	Ja grotendeels. Diverse ruimten zijn alleen toegankelijk met de juiste autorisaties. De ruimten worden beveiligd middels scanapparatuur bij de ingangen. De autorisaties worden zo veel mogelijk afgegeven op rollen en daarmee samenhangende bevoegdheden. Er is een bezoekersregeling: deze krijgen een pasje en dienen opgehaald en teruggebracht te worden door degene die hen ontvangt. De receptie verstrekt de toegangspassen. Voor leveranciers en onderhoudspersoneel gelden aparte afspraken: zij krijgen óf een vaste pas op basis van werkzaamheden en bevoegdheden of een dagpas, na aanmelding bij de receptie. Zowel de bezoekersregeling als de regeling voor leveranciers en onderhoudspersoneel is niet waterdicht. Dit heeft met name te maken met houding en gedrag van de mensen die hier gebruik van maken. Het komt voor dat meerdere mensen op één pas naar binnen gaan. En niet altijd worden bezoekers teruggebracht. Ophalen gaat doorgaans goed, maar terugbrengen is vaak een handeling te veel.
11.1.3 Kantoren, ruimten en faciliteiten beveiligen	

[4] Op het moment van dit onderzoek betreft dit BIO versie 1.04.
[5] Dit zijn beheersmaatregelen die voortkomen uit de ISO 27002.

ISO-control	Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.
Verplichte overheidsmaatregel	Sleutelbeheer is ingericht op basis van een sleutelplan.
Voldoet aan BIO norm?	Nee. Sleutels voor de dienstpanden zijn in beheer bij Facilitaire Zaken, maar er is geen sleutelplan. Sleutels zijn alleen in gebruik binnen de gebouwen, nadat er toegang is verkregen met een toegangspas. Fysieke beveiliging steunt op het afsluiten van ruimten, die alleen betreden kunnen worden met een pas. Een sleutel is dan niet noodzakelijk en soms ook niet bruikbaar. Slechts enkele ruimtes kunnen alleen door een sleutel betreden worden.
11.1.4 Beschermen tegen bedreigingen van buitenaf	
ISO-control	Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.
Verplichte overheidsmaatregel 1	De organisatie heeft geïnventariseerd welke papieren archieven en apparatuur bedrijfskritisch zijn. Tegen bedreigingen van buitenaf zijn beveiligingsmaatregelen genomen op basis van een expliciete risicoafweging.
Voldoet aan BIO norm?	Ja grotendeels. Deze hangt samen met de zonering. Apparatuur staat in de ruimten waar medewerkers komen (PC's, kasten, kopieerapparaten, koffie en thee voorzieningen). Bijzondere apparatuur (ICT-gerelateerd zoals patchkasten en datacentra) en fysieke archieven staan in afgesloten ruimten die alleen met een geautoriseerde pas toegankelijk zijn.
Verplichte overheidsmaatregel 2	Bij huisvesting van IT-apparatuur wordt rekening gehouden met de kans op gevolgen van rampen veroorzaakt door de natuur en menselijk handelen.
Voldoet aan BIO norm?	Ja grotendeels. Voor de (beide) datacentra is hiermee rekening gehouden. De verantwoordelijkheid hiervoor ligt bij IRvN. Voor de overige IT-apparatuur geldt de normale beveiliging zoals deze ook in de kantoorruimten geldt. Het toegangsbeleid tot deze ICT-gerelateerde ruimte is niet duidelijk. Voor IRvN is niet duidelijk wie toegang heeft en verkrijgt en op basis van welke criteria, terwijl hun apparatuur wel in de ruimten staat. De afspraken tussen Facilitaire Zaken en IRvN dienen op dit aspect opnieuw vastgesteld te worden.
11.1.5 Werken in beveiligde gebieden	
ISO-control	Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.
Verplichte overheidsmaatregel	Niet specifiek uitgewerkt in verplichte overheidsmaatregel.
Voldoet aan BIO norm?	Ja. Er is een fysiek beveiligingsbeleid en een bezoekersprocedure opgesteld op het moment dat de toegangspoortjes werden geïntroduceerd (oktober 2021). Deze zijn nog steeds actueel. De vraag is of deze inmiddels een update nodig hebben. De benoemde maatregelen lijken nog steeds afdoende.
11.1.6 Laad- en loslocatie	
ISO-control	Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatie verwerkende faciliteiten om onbevoegde toegang te vermijden.
Verplichte overheidsmaatregel	Niet specifiek uitgewerkt in verplichte overheidsmaatregel.

Voldoet aan BIO norm?	Ja. Deze plekken zijn beveiligd met een toegangspas met specifieke autorisatie. Dat betekent dat niet elke medewerker hiertoe toegang heeft. Deze toegang wordt ook gebruikt door medewerkers van Handhaving en Toezicht. Tot op heden heeft dit niet tot knelpunten of veiligheidsrisico's geleid.

6. Reflecties en aanbevelingen

In dit hoofdstuk presenteren we de reflecties en aanbevelingen. Deze belichten wij langs drie hoofdthema's die als natuurlijke rode draad uit de gevoerde gesprekken naar voren zijn gekomen.

- Beleid & governance
- Maatregelen en risico's in de praktijk
- Naleving, gedrag & gedrag

Reflecties beleid & governance

- De afdeling Facilitaire Zaken is primair verantwoordelijk voor het opstellen en actualiseren van beleid voor fysieke toegang en beveiliging. De CISO houdt toezicht op de implementatie van de fysieke beveiligingsmaatregelen en adviseert over noodzakelijke aanpassingen. Het functioneel beheer van het toegangssysteem i-Protect is belegd bij iRvN. Team Privacy heeft momenteel geen expliciete rol bij het opstellen en herzien van het beleid.
- Het fysieke toegangsbeleid dateert uit de introductie van de poortjes (medio 2021) en is 2022 aangevuld met beleid voor medewerkers van leveranciers. Een structurele herziening heeft sindsdien niet meer plaatsgevonden.
- Het huidige beleid kent een aantal belangrijke elementen die vergelijkbaar zijn met dat van drie andere geïnterviewde G40 - gemeenten en is in de basis op orde.:
    - Zonering van ruimten.
    - Afgesloten ruimten die alleen met geautoriseerde toegangspassen toegankelijk zijn.
    - Gebruik van toegangspoortjes en bijbehorende toegangspassen die op afstand gedeactiveerd kunnen worden.
    - Een bezoekersregeling met afspraken over de uitgifte en inname van bezoekerspasjes.
    - Afspraken over het verstrekken van toegangspassen aan leveranciers.
- Sinds de introductie van de poortjes in 2021 hebben zowel het Stadhuis als de Mariënburg twee beveiligingsschillen: toegangspoortjes én paslezers bij tussendeuren en in de liften. Dit heeft het probleem van de toegang van onbevoegden tot de kantoorgebouwen grotendeels opgelost. Hoewel het risico op onbevoegd toegang nooit helemaal voorkomen kan worden, ervaren medewerkers merkbare verbeteringen. De geconstateerde problemen hangen nu vooral samen met het juiste gebruik van de poortjes en de toegangspassen door medewerkers en bezoekers. Zie hoofdstuk *Naleving, gedrag en cultuur*.
- Voor het Regionaal Archief Nijmegen (RAN) is gezien het semipublieke karakter van het gebouw bewust de keuze gemaakt om geen poortjes te plaatsen. De archiefbewaarplaats is binnen het gebouw een extra beveiligde ruimte met beperkte toegang voor een aantal medewerkers.
- Specifiek risico-gebaseerd beleid voor organisatieonderdelen met bijzondere risico's (zoals Publiekszaken en Toezicht & Handhaving/Meldkamer) wordt in overleg en samenwerking met deze afdelingen vormgegeven. Extra maatregelen zoals afgesloten ruimtes beperken de risico's van onbevoegd toegang en het lekken van gevoelige (persoons)gegevens aanzienlijk en verdienen continuering.

Aanbevelingen

- Evalueer of het fysieke toegangsbeleid nog aansluit bij actuele ontwikkelingen en risico's en actualiseer waar nodig. Een volledig nieuw beleidsdocument lijkt niet noodzakelijk.
- Betrek Team Privacy expliciet bij toekomstige herzieningen van het beleid, zodat specifieke privacy risico's voldoende aandacht krijgen.

- Onderzoek of de fysieke beveiliging van andere “open” afdelingen zoals de Sociale Recherche verbeterd kan worden met laagdrempelige (fysieke) voorzieningen en werkafspraken. Denk aan privacy schermen voor laptops, geluidsbarrières en werkafspraken over flexplekken.

Reflectie maatregelen en risico’s in de praktijk

De concrete kwetsbaarheden en risico’s zijn intern gedeeld met de afdeling Facilitaire Zaken, die op basis hiervan aanvullende maatregelen kan treffen.

- Er wordt doorgaans expliciet afgewogen of externen een bezoekerspas of een vaste toegangspas ontvangen. Dit wordt beoordeeld op basis van de aard en frequentie van de werkzaamheden. Een deel valt onder het beheer van Facilitaire Zaken, en een ander deel onder Vastgoed, Sport & Accommodaties (VSA). De informatie-uitwisseling tussen de twee afdelingen is niet altijd volledig of tijdig. Hierdoor ontstaat een kwetsbaarheid in het proces rondom het verstrekken en beheren van bezoekerspassen aan externen.
- Enkele toegangspunten tot de kantoorgebouwen staan in bepaalde situaties langer open dan noodzakelijk. Dit kan ertoe leiden dat onbevoegden ongewenst verder het gebouw in kunnen komen, of dat vertrouwelijke informatie tijdelijk onbeheerd blijft.
- Binnen enkele afdelingen zijn doorgangen en toegangspunten aangetroffen die niet altijd consequent gesloten zijn. Hierdoor bestaat het risico dat onbevoegden zich in beveiligde zones begeven of zicht hebben op vertrouwelijke documenten. De betrokken afdelingen treffen maatregelen om dit risico te verkleinen. Onder andere via werkafspraken over het verwijderen van vertrouwelijke informatie en door te zorgen voor continue aanwezigheid van medewerkers.
- Er is geen sleutelplan aanwezig bij Facilitaire Zaken, waardoor men onvoldoende inzicht heeft in het gebruik van sleutels binnen het gebouw en de daarmee verbonden risico’s. Naar verwachting zijn de risico’s hiervan wel beperkt aangezien het om sleutels voor intern gebruik gaat.
- De afspraken tussen Facilitaire Zaken en iRvN over beheer en verantwoordelijkheid van de MER- en SER[6]-ruimten zijn niet schriftelijk vastgelegd en geformaliseerd. Dit zorgt voor onduidelijkheid over wie beveiligingsmaatregelen bepaalt, wie toegang verleent en wie verantwoordelijk is voor cameratoezicht in en rondom deze ruimten.
- Afspraken over de taken en verantwoordelijkheden rondom het functioneel applicatiebeheer van het toegangssysteem i-Protect zijn niet geformaliseerd tussen iRvN en Facilitaire Zaken. Het functionele beheer wordt momenteel informeel uitgevoerd door een medewerker van iRvN, die begin 2026 met pensioen gaat. Hiermee ontstaat onduidelijkheid bij betrokkenen over de borging en continuïteit in de toekomst. Momenteel wordt dit door iRvN belegd bij externe inhuur. Dit is echter geen duurzame oplossing voor de lange termijn.
- Alle readers op deuren en poortjes zijn recent vervangen en geschikt gemaakt voor nieuwe technologie. De huidige Mifare-chips[7] in de toegangspassen zijn echter verouderd en kwetsbaar. Een overstap naar DESFire[8] met geavanceerdere beveiliging is volgens betrokkenen wenselijk.
- Externe bezoekers krijgen toegangspassen waarmee zij de poortjes kunnen passeren. De ontvangende medewerker meldt de bezoeker normaliter aan. Gebeurt dit niet, dan probeert de receptie de juiste medewerker te bereiken. Als laatste redmiddel kan de receptie zelf de bezoeker aanmelden. Het systeem is in principe sluitend: bezoekers komen niet binnen zonder pas en aanmelding. Bij grote groepen worden echter regelmatig uitzonderingen gemaakt, waardoor zij zonder bezoekerspas toegang krijgen en het overzicht ontbreekt van wie zich binnen de beveiligde zone bevindt.

[6] Main Equipment Room (MER) en Satellite Equipment Room (SER)

[7] MIFARE is een type contactloze smartcardtechnologie dat wordt gebruikt voor toegangscontrole en identificatie

[8] DESFire is een geavanceerde variant van MIFARE-technologie die extra beveiliging biedt

- Er is een duidelijke procedure voor het intrekken van toegangsrechten bij het vertrek van medewerkers en bij het beëindigen van werkzaamheden van externen en leveranciers. Dit proces verloopt over het algemeen goed. Bij interne functiewijzigingen ontstaan echter knelpunten. Bestaande toegangsrechten blijven regelmatig (te lang) actief. Dit speelt met name bij medewerkers die vanuit hun functie of rol aanvullende rechten hebben, zoals BHV'ers of medewerkers met toegang tot specifieke ruimten. Hierdoor bestaat het risico dat medewerkers onbevoegd toegang behouden tot afdelingen met een verhoogd beveiligingsniveau.
- De kantoorgebouwen zijn in de avond, nacht en in het weekend extra beveiligd met een alarm. Bij een alarmmelding wordt een beveiligingsbedrijf ingeschakeld. Er zijn situaties geweest waarin het alarm onterecht afging doordat medewerkers per ongeluk buiten openingstijden het gebouw of beveiligde zones hebben betreden. Dit veroorzaakt onnodige kosten en roept twee vragen op: zijn medewerkers voldoende op de hoogte van de openingstijden, en waarom beschikken medewerkers over toegang buiten de openingstijden?

Aanbevelingen

- Evalueer en verduidelijk de afspraken tussen VSA en Facilitaire Zaken over het verstrekken en beheren van toegangsrechten van externen, zodat dit efficiënt en veilig verloopt.
- Maak bewust een risicoafweging van de hierboven genoemde kwetsbare locaties binnen de kantoorgebouwen en bepaal of aanvullende maatregelen noodzakelijk zijn.
- Stel een sleutelplan op en beoordeel welke fysieke sleutels nog noodzakelijk zijn. Registreer alle uitgegeven sleutels en koppel deze aan een uitleenregistratie en periodieke inventarisatie. Beperk het gebruik van fysieke sleutels zoveel mogelijk.
- Leg de afspraken over toegangsbeheer, cameratoezicht en verantwoordelijkheden voor MER- en SER-ruimten formeel vast tussen Facilitaire Zaken en iRvN. Bepaal en documenteer wie beveiligingsmaatregelen vaststelt en uitvoert, wie toegang verleent en hoe incidenten worden geregistreerd en geëvalueerd.
- Formaliseer de afspraken tussen Facilitaire Zaken en iRvN over het functionele applicatiebeheer van het toegangssysteem i-Protect en zorg voor een duurzame, formele borging hiervan binnen iRvN.
- Overweeg een versnelde overstap van Mifare naar DESFire of een vergelijkbare, goed beveiligde technologie (bijvoorbeeld toegang via app) om toekomstbestendig te worden. Onderzoek hiervoor kosten en baten van beschikbare opties.
- Blijf investeren in de verdere implementatie van role-based access, waarbij rechten en autorisaties aan functies en rollen zijn gekoppeld. Dit verkleint het risico op te ruime toegangsrechten bij interne functiewijzigingen.
- Onderzoek de mogelijkheid om de toegangsrechten van medewerkers te beperken tot de officiële openingstijden, zodat zij het gebouw of extra beveiligde zones buiten deze tijden niet kunnen betreden en incidenten door onbekendheid met de toegangsregels worden voorkomen.

Reflectie naleving, gedrag & cultuur

- Hoewel de naleving van de toegangsafspraken sinds de introductie van de poortjes volgens betrokkenen is verbeterd, doen zich nog dagelijks incidenten voor. Uit zowel gesprekken als steekproeven blijkt dat de naleving van de basisafspraken rondom fysieke toegang wisselend is. Dit betreft met name het (on)juiste gebruik van de poortjes door medewerkers en bezoekers. De volgende incidenten komen regelmatig (wekelijks tot dagelijks) voor:
    - Tailgaten: achter iemand meelopen zonder eigen pas of gebruikmaken van het pasje van een collega. Dit komt dagelijks bij medewerkers voor. Recent heeft een inwoner op deze wijze driemaal onbevoegd toegang verkregen tot de beveiligde zone van een kantoorgebouw. Dit incident heeft bij sommige medewerkers geleid tot een gevoel van onveiligheid. Hoewel er op dit

moment geen vergelijkbare veiligheidsincidenten bekend zijn, blijft dit een reëel risico. Dat incidenten niet bekend zijn, betekent immers niet dat ze niet voorkomen. In het verleden zijn niet alle incidenten zorgvuldig geregistreerd. Daarnaast laat een eerder mystery guest onderzoek uit 2022 zien dat onbevoegden niet of nauwelijks worden herkend en aangesproken.

    - Bezoekers niet (correct) aanmelden en hen toch toegang geven met een eigen pas. Soms worden bezoekers, ook als ze wel correct zijn aangemeld, direct opgehaald door de medewerker zonder een bezoekerspas te ontvangen. Dit komt dagelijks voor.
    - Bezoekers niet terug begeleiden naar de balie, waardoor het risico ontstaat dat zij ongeleid door het gebouw dwalen.
    - Doordat bezoekers niet naar de balie worden teruggebracht, leveren zij hun toegangspas geregeld niet in. In zulke gevallen wordt het pasje doorgaans direct geblokkeerd. Dit komt minimaal maandelijks voor.
- Genoemde oorzaken voor deze overtredingen zijn onder andere:
    - Onbekendheid met de (huis)regels, met name bij nieuwe medewerkers.
    - Bewuste overtreding van de regels, bijvoorbeeld omdat men het belang ervan niet inziet.
    - Onvoldoende besef van de risico's die het eigen gedrag met zich meebrengt.
    - De procedure voor het aanmelden, ophalen en terugbrengen van bezoekers wordt als omslachtig ervaren. Met name het aanmelden via Planon in Citrix wordt niet als gebruiksvriendelijk gezien.
    - Het niet zichtbaar dragen van toegangspassen en het ontbreken van een visueel onderscheid tussen vaste toegangspassen en bezoekerspassen.
- Medewerkers van de receptie spreken zowel medewerkers als bezoekers regelmatig aan op ongewenst gedrag. Dit leidt soms tot geïrriteerde of lacherige reacties, met name van medewerkers. Ook krijgen receptiemedewerkers soms instructies hoe om te gaan met (specifieke) personen met onbegrepen gedrag. Wanneer dit niet werkt, wordt van de receptie (impliciet) verwacht dat zij het zelf oplost. Deze factoren dragen regelmatig bij aan een gevoel van kwetsbaarheid. Er bestaan wel afspraken over het inschakelen van hulp bij hevige incidenten. De receptie kan dan hulp van handhavers of de beveiliging van de Mariënburg inschakelen.
- Medewerkers spreken elkaar of onbekenden vaak niet aan op de genoemde overtredingen. Dit wordt mede veroorzaakt door het feit dat toegangspassen voor medewerkers en bezoekers er hetzelfde uitzien en vaak niet zichtbaar worden gedragen, waardoor het lastig is om elkaar hierop te corrigeren. Het verplicht zichtbaar dragen van de toegangspassen is eerder besproken als mogelijke maatregel, maar is destijds niet doorgevoerd. De maatregel roept weerstand op en zou niet aansluiten bij de organisatiecultuur.
- Binnen de afdelingen met aanvullende beveiligingsmaatregelen (Publiekszaken en Toezicht & Handhaving) wordt het belang van naleving van de toegangsafspraken over het algemeen goed begrepen. Medewerkers zijn redelijk bekend met de afspraken, al blijft extra aandacht met name voor nieuwe medewerkers nodig. Incidenteel worden afspraken niet nageleefd, maar op beide afdelingen is sprake van een cultuur waarin collega's elkaar hierop aanspreken. Medewerkers zijn zich bovendien bewust van de risico's die het werken met gevoelige persoonsgegevens met zich meebrengt. Bij Toezicht & Handhaving bestaat wel behoefte aan duidelijke/expliciete afspraken over wie verantwoordelijk is voor het bewaken van de toegangsregels.
- Een van de achterdeuren wordt regelmatig gebruikt door handhaving en incidenteel om bijvoorbeeld politiecollega's zonder pas toegang te verlenen, waardoor geen volledig zicht op de instroom bestaat. Het is onduidelijk in hoeverre hier concrete afspraken over zijn.

Aanbevelingen

- We ondersteunen de plannen om Planon te migreren naar de cloud waardoor het registreren van bezoekers ook buiten Citrix mogelijk wordt. Deze quick win stimuleert naar verwachting een betere

naleving van het bezoekersprotocol. Op termijn zou een gebruikersvriendelijk bezoekersregistratiesysteem wenselijk zijn.

- Onderzoek de mogelijkheden en kosten van een anti-passback-functie[9], zodat niemand twee keer met dezelfde pas kan binnenkomen of een bezoeker met de eigen pas kan doorlaten.
- Heroverweeg de vervanging van de huidige toegangspassen en -druppels door varianten met een zichtbaar onderscheid tussen vaste passen en bezoekerspassen. Combineer dit vervangingstraject met de gewenste overgang van Mifare naar DESFire-chiptechnologie. Zorg hierbij voor aanvullende gedragsafspraken, waarbij het zichtbaar dragen van toegangspassen actief wordt gestimuleerd.
- Blijf continu communiceren richting medewerkers om kennis en acceptatie te borgen en het juiste gedrag te stimuleren. Introduceer de huisregels al bij onboarding en herhaal regelmatig het belang van de afgesproken maatregelen, in het bijzonder de bezoekersprocedure en ieders rol daarin.
- Maak een expliciete risico-inschatting van het toelaten van politiecollega's zonder registratie en bezoekerspas. Maak waar nodig nieuwe afspraken.

[9] Een functionaliteit die voorkomt dat een toegangspas kan worden doorgegeven aan een andere persoon.

7. Kosten bestaande en nieuwe maatregelen

Bestaande maatregelen

- Het is jaarlijkse budget voor onderhoud van fysieke toegang en beveiliging bestaat uit twee delen:
    - Onderhoud van het toegangssysteem i-protect - € 15.000, - per jaar.
    - Aanschaf nieuwe toegangspassen - € 8.000, - per jaar.

  Deze posten geven slechts een indicatie van de directe jaarlijkse kosten en vormen geen volledig financieel beeld. De kosten voor fysieke toegang en beveiliging zijn structureel verweven met andere integrale (beveiligings)maatregelen, zoals gebouwbeheer, brandveiligheid en algemene ICT-beveiliging. Een betrouwbaar afzonderlijk kostenoverzicht is daarom niet zonder onevenredige inspanning te realiseren.

  Ter illustratie: Heyday maakt jaarlijks directe onderhoudskosten voor de hardware (waaronder deurcontrollers en lezers) ter hoogte van circa €16.600. Het bedrijf voert namens de gemeente Nijmegen het regie- en technisch beheer uit van de vastgoedportefeuille. Deze onderhoudskosten komen ten laste van het onderhoudsbudget dat door de gemeente Nijmegen beschikbaar is gesteld.
- Met de twee belangrijkste kostenposten - onderhoud en aanschaf - bereiken we een beveiligingsniveau dat in de basis op orde is. Daarmee kunnen spreken van een doelmatige besteding van middelen met inachtneming van bovengenoemde kanttekening.
- Een vergelijking van de kosten met drie andere G40-gemeenten blijkt lastig. Kosten verschillen namelijk per gemeente door lokale omstandigheden, bestaande contractafspraken en het al dan niet integreren van fysieke toegang in bredere beveiligings- of facilitaire pakketten.

Mogelijk toekomstige maatregelen

- De overstap naar toekomstbestendige toegangspassen of Mobile Access brengt minimaal volgende eenmalige kosten met zich mee:
    - Vervanging van alle 5.000 passen[10] door het veiligere type DESFire EV3: ca. € 125.000.
    - Vervanging van de Orbit deur-controllers voor toegang via Mobile Access: ca. €90.000. Kosten voor eventuele aanpassing van oude bekabeling zijn hierin niet opgenomen. Uit ervaring blijkt dat de uiteindelijke kosten vaak hoger uitvallen. Een voordeel van Mobile Access is dat de jaarlijkse kosten voor nieuwe toegangspassen vervallen.
    - Bij vervanging van de passen door het type DESFire kunnen de jaarlijkse onderhoudskosten veranderen. Deze zijn nog niet in beeld gebracht.
- De kosten van andere maatregelen, zoals het inrichten van een anti-passbackfunctie, de migratie van Planon naar de cloud (reeds gestart) en het beperken van toegangsrechten buiten de openingstijden, zijn niet in kaart gebracht. Naar verwachting liggen deze kosten aanzienlijk lager, terwijl deze maatregelen de effectiviteit en doelmatigheid van het beleid verder kunnen vergroten.
- De volledige uitrol van role-based-access brengt naar verwachting hogere kosten met zich mee. Deze maatregel dient echter meerdere doelen, waardoor de kosten niet volledig zijn toe te rekenen aan fysieke toegang en beveiliging. Ook deze maatregel zal op termijn naar verwachting de effectiviteit en doelmatigheid van het beleid verbeteren.
- Andere aanbevelingen betreffen interventies en maatregelen die met weinig inspanning en geringe extra kosten de doelmatigheid van het beleid verder kunnen verbeteren. Denk aan een goede onboarding, regelmatige communicatie, elkaar aanspreken op gedrag en het maken van duidelijke afspraken intern en met partners.

[10] Dit is inclusief passen voor onder andere ODRN, externe partners en leveranciers.

8. Conclusie

Het beleid voor fysieke toegang en beveiliging is in de kern doelmatig. Met redelijke middelen wordt een goed basisniveau van fysieke toegang beveiliging bereikt dat vergelijkbaar is met dat van drie andere G40 - gemeenten. De belangrijkste voorzieningen en maatregelen, zoals poortjes, paslezers, bezoekersregistratie en alarm, functioneren naar behoren. Ook het intrekken van toegangsrechten bij uitdiensttreding of het beëindigen van werkzaamheden verloopt efficiënt. Aanvullende maatregelen binnen afdelingen worden risico-gebaseerd getroffen. Met de huidige inrichting voldoen wij grotendeels aan onze eigen ambitie om minimaal te voldoen aan de BIO-norm.

Tegelijkertijd blijkt uit de bevindingen dat met relatief beperkte inspanningen en enkele quick wins een hoger beveiligingsniveau kan worden bereikt. Dagelijkse incidenten zoals tailgaten, onvolledige bezoekersregistratie en het niet terugbegeleiden van bezoekers leiden tot risico's en extra werk voor de receptie. Een recent incident waarbij een inwoner driemaal onbevoegd toegang kreeg tot de beveiligde zone van een kantoorgebouw, laat zien dat we ondanks de huidige maatregelen kwetsbaar blijven. Hoewel er op dit moment geen vergelijkbare incidenten zijn gemeld, blijft dit een reëel risico. Dat incidenten niet bekend zijn, betekent niet dat ze niet voorkomen. Zo zijn in het verleden niet alle incidenten geregistreerd. Ook het mystery-guest onderzoek uit 2022 laat zien dat onbevoegden nauwelijks worden herkend of aangesproken.

De effectiviteit van de poortjes hangt dus sterk af van het gedrag van medewerkers. Het gebruik van duidelijk onderscheidende toegangspassen voor medewerkers en bezoekers, en het zichtbaar dragen ervan, kan dit risico verkleinen. Daarnaast kan de werking van de poortjes eenvoudig worden verbeterd door de anti-pass-backfunctie te activeren, waardoor een pas niet meerdere keren kan worden gebruikt. Het gebruiksvriendelijker maken van de bezoekersregistratie in Planon door de migratie naar de Cloud, vergroot bovendien naar verwachting de naleving van de bezoekersprocedure. Ook het feit dat medewerkers buiten openingstijden toegang kunnen krijgen, kan leiden tot onnodige kosten door een onterecht alarm en inzet van beveiliging. Een goede onboarding en regelmatige communicatie over huisregels kunnen de effectiviteit van bestaande maatregelen tegen minimale extra kosten versterken.

Verder kan de doelmatigheid worden verbeterd met een aantal gerichte grotere aanpassingen. Het volledig implementeren van role-based access en automatische deactivering van rechten bij functiewijzigingen zou handmatig beheer (en fouten) verminderen en het beveiligingsniveau verder verhogen. De overstap naar DESFire of een app-gebaseerd toegangssysteem vraagt een grotere investering, maar verlaagt op termijn structureel het risico op misbruik. Indien voor een app-gebaseerd toegangssysteem wordt gekozen, verlaagt dit op termijn bovendien de kosten van fysieke pasuitgifte.