Gemeente Amsterdam

Auditrapport

Informatiebeveiliging omtrent het proces scannen fysieke post

Fysieke beveiliging, logische beveiliging, procesinrichting en samenwerking in één pand

Referentie: IA/verzoek 2021-09/JP/PW/IeK

Opdrachtgever: directie Belastingen

Auteur: Interne Audit [redacted]

Proceseigenaar: directies Belastingen, ICT, Facilitair en IV-eenheid D&I

4 januari 2022 - Definitief

1 Inleiding

Interne audit geeft uitvoering aan een auditjaarplan, dat wordt vastgesteld door het GMT. Daarnaast voeren wij ook audits op verzoek uit. Deze audit is uitgevoerd op verzoek van directie Belastingen.

Aanleiding voor het verzoek is het incident van 6 april 2021 waarbij een groot datalek is ontstaan als gevolg van de diefstal van een harde schijf uit de scan-pc.

Na constatering van de diefstal is een onderzoek door politie en bureau integriteit uitgevoerd, zijn de wethouder en de raad geïnformeerd en zijn maatregelen getroffen om herhaling te voorkomen.

Het verzoek van Belastingen is om de getroffen maatregelen in de informatiebeveiliging rondom het proces scannen van poststukken voor directie Belastingen in de nieuwe situatie te beoordelen. Dit is een ketenproces waarbij de directies Belastingen, Facilitair, ICT en de IV-eenheid van cluster Dienstverlening en Informatie betrokken zijn.

Doelstelling en centrale vraag

Dit onderzoek richt zich op het beoordelen van de opzet en het vaststellen van het bestaan van de beheersingsmaatregelen t.b.v. de informatiebeveiliging bij het scanproces van de postkamer van directie Belastingen. Waar mogelijk (opzet/bestaan voldoet) en relevant (gezien de relatief korte periode sinds de verbetermaatregelen) hebben wij ook de effectieve werking van de beheersingsmaatregelen getoetst.

In overleg met de auditee is de centrale vraag geformuleerd:
Zijn de digitale en fysieke gegevens van Belastingen die worden verwerkt in het scanproces in de nieuwe situatie goed beschermd?

De nieuwe situatie betreft hier de situatie na verhuizing van de locatie aan de Herikerbergweg naar de locatie aan het Anton de Komplein.

Scope

De audit richt zich op de volgende onderwerpen:

A. Fysieke beveiliging van het pand, Anton de Komplein 150
B. Informatiebeveiliging IV en hardware in het pand Anton de Komplein 150 (logisch en fysiek)
C. Proces van scannen inkomende poststukken Belastingen
D. Samenspel van verantwoordelijkheden in één pand (ketensamenwerking)

In bijlage 1 is een gedetailleerd overzicht van onderzoeksvragen opgenomen, gegroepeerd per onderzoeksonderwerp en voorzien van auditresultaat.

Niet in Scope

Buiten de scope van deze audit vallen de processen ten behoeve van informatiebeveiliging voor andere processen, andere hardware met harde schijven en de informatiebeveiliging in andere gemeentelijk panden. Ook de communicatie omtrent het incident van het datalek als gevolg van een gestolen harde schijf van april 2021 en de wenselijkheid van behoud van een fysieke poststroom vallen buiten de scope van onze audit.

Toetsingskader

- De BIO (Baseline Informatiebeveiliging Overheid;
- Gemeentelijk informatiebeveiligingsbeleid
- Vastgestelde risicoanalyses (URA/DRA) en privacy impact analyse (DPIA)
- AVG

In hoofdstuk 2 hebben wij de samenvatting en conclusies opgenomen. In hoofdstuk 3 zijn onze uitgevoerde werkzaamheden en bevindingen opgenomen. In de bijlagen hebben wij deze bevindingen nader uitgewerkt. Wij adviseren u om de risico`s en beheersmaatregelen op te nemen in Naris.

Wij bedanken de medewerkers die bij dit onderzoek betrokken zijn geweest voor de open en constructieve samenwerking bij het verrichten van onze werkzaamheden. Tot het verstrekken van nadere toelichting zijn wij uiteraard bereid.

2 Samenvatting en conclusies

De audit over de informatiebeveiliging van het proces scannen fysieke post van directie Belastingen is uitgevoerd op verzoek van directie Belastingen. Ook de directies Facilitair, ICT en de IV-eenheid van cluster Dienstverlening en Informatie zijn in de audit betrokken.

De audit richt zich op de centrale vraag:
Zijn de digitale en fysieke gegevens van Belastingen die worden verwerkt in het scanproces in de nieuwe situatie goed beschermd?

Conclusie
Op basis van de door ons uitgevoerde auditwerkzaamheden concluderen wij dat de digitale en fysieke gegevens verwerkt in het scanproces in de nieuwe situatie nog niet voldoende zijn beschermd.

Het is nog steeds mogelijk dat het risico van een datalek zich voordoet. Wij constateren wel dat de informatiebeveiliging sterk is verbeterd t.o.v. de oude situatie, waarbij het lastiger is gemaakt om toegang tot de gegevens te krijgen en met name de omvang van een potentieel datalek (impact) fors is verkleind. De belangrijkste verbeteringen zijn het dagelijks verwijderen van de gescande stukken van de scan-pc en de forse beperking in de toegang tot de postkamer.

Per deelonderwerp is onze conclusie:

Nr.	Onderwerp	Conclusie
A.	Fysieke beveiliging gebouw (Anton de Komplein 150)	
B.	Informatiebeveiliging IV en Hardware in pand	
C.	Proces van scannen inkomende poststukken Belastingen	
D.	Samenspel van verantwoordelijkheden in één pand	

Gezien de extra gevoelige informatie van gegevens mag verhoogde bescherming worden verwacht. Uit onze bevindingen blijken een aantal aandachtspunten waardoor nog risico op herhaling van een datalek bestaat. De belangrijkste betreffen:

- Meer medewerkers dan noodzakelijk hadden toegang tot de G-schijf. De niet noodzakelijke rechten zijn n.a.v. deze audit direct ingetrokken (B).
- Schoning van de harde schijven vindt niet op juiste wijze plaats, waardoor het mogelijk blijft deze data te herstellen (C).
- Wachtwoorden zijn eenvoudig te achterhalen (B).
- Fysieke toegang tot zone-2 delen van het pand is mogelijk voor onbevoegden als gevolg van enkele slecht ingeregelde passcanners (A).
- Aanwezigheid van een maand aan ontvangen fysieke post in een standaard kantoorkast binnen de zone 2-beveiligde postkamer (C).
- De beveiliging van de papierbakken voldoet niet altijd aan de gestelde eisen en de gesloten papierbakken worden gestald in een minder beveiligde ruimte (A).
- Het ontbreken van procesbeschrijvingen met duidelijkheid over taken, bevoegdheden en verantwoordelijkheden voor stedelijke processen (A-D).

Wij hebben in dit rapport meerdere bevindingen opgenomen, die betrekking hebben op verschillende partijen. Niet alle bevindingen hoeven te worden opgevolgd door directie Belasting. Wel moet er een goede combinatie van toereikende maatregelen bij de verschillende partijen worden gerealiseerd. Daarbij zijn partijen afhankelijk van elkaar. Maatregelen dichterbij de postkamer zijn het meest effectief voor de beveiliging van de postkamer. In ogenschouw moet worden genomen dat de postkamer niet de enige plek is waar informatie voldoende beveiligd dient te zijn. Wij bevelen aan dat betrokken partijen met elkaar in gesprek gaan om tot een goede combinatie te komen.

Ten slotte melden wij u dat het definitieve auditrapport wordt toegestuurd aan de concerncontroller, de manager Control, de betrokken controllers, de procescontroller en ACAM. Wanneer ACAM erom verzoekt, verstrekken wij hen ook toegang tot ons dossier. De conclusies en belangrijkste bevindingen worden opgenomen in onze voortgangsrapportage die aan het GMT worden toegestuurd.

3 Werkzaamheden en bevindingen

Werkzaamheden

In de uitvoering van het onderzoek maken wij gebruik van de onderzoekstechnieken interviews, documentinspectie en waarneming ter plaatse. Door toepassing van deze onderzoekstechnieken wordt vastgesteld of de inrichting (opzet) van de beheersingsmaatregelen in overeenstemming zijn met de BIO en het gemeentelijk informatiebeveiligingsbeleid. Ook wordt het bestaan en, waar mogelijk en relevant, de goede werking van de beheersingsmaatregelen vastgesteld. De werking is getoetst voor de periode 1 juli 2021 tot en met 30 november 2021 en met behulp van gegevensgerichte toetsingswerkzaamheden. Waar wij bevindingen constateren ten aanzien van de opzet en/of het bestaan zal de werking niet worden getoetst.

Opvolging van de bevindingen kunnen na deze audit door de verantwoordelijke directie worden uitgevoerd, waarna in een separate follow-up audit opzet, bestaan en werking van het proces (opnieuw) kunnen worden vastgesteld.

Bevindingen

Onderstaand hebben we onze bevindingen kort vermeld en voorzien van een conclusie in stoplichtvorm. De bevindingen zijn (met overeenkomstige nummering) nader uitgewerkt in bijlage 2.

1. Fysieke beveiliging pand	**Beoordeling**
1a. Onvolledige realisatie van de adviezen gegeven door de beveiligingsadviseurs De adviseurs beveiliging en veiligheid hebben in het initiële advies in juni 2021 10 adviezen gegeven waarvan bij de afronding van de audit, vijf maanden later, één niet is gerealiseerd en vier gedeeltelijk zijn gerealiseerd. De overige vijf adviezen zijn volledig gerealiseerd. Aandacht is nodig voor realisatie van: - Het versterken van de bewustwording bij de medewerkers. - Betere inregeling van de toegang voor de lift in de centrale hal. - Verbetering beveiliging van fysieke documenten met o.a. een betere kwaliteit papierbakken ter beveiliging van te vernietigen documenten in het proces voor afvoer van de te vernietigen documenten en alsnog levering van een betere kwaliteit kast in de postkamer.	
1b. Randvoorwaarden voor goede fysieke beveiliging deels gerealiseerd Er zijn vier randvoorwaarden onderkend. Voor drie van de vier randvoorwaarden is verdere aandacht noodzakelijk. Dit betreffen: - goed ingericht stedelijk sleutelbeheer voorzien van sleutelplan. - uitvoering van periodieke toetsing van de autorisaties voor betreding van zone 2-ruimten. - tijdig betrekken van adviseurs beveiliging en veiligheid bij wijzigingen in het pand.	
Akkoord bevonden zijn: • Het systeem van beveiligingscamera's is in opzet aanwezig en functioneert. In het pand zijn camera's alleen aanwezig bij de stadsloketten, niet in de andere delen van het pand. Wel zijn beveiligingscamera's rondom het gebouw geplaatst. • De toegangsbeveiliging tot de postkamer is in opzet goed ingericht en functioneert in overeenstemming met de opzet. • Gecertificeerd beveiligingspersoneel wordt ingehuurd via een stedelijk contract. • Het beveiligingssysteem kent een 'achtervang'-functie waarbij langdurig uitgeschakeld zijn van één of meer beveiligingselementen ook leidt tot een melding in de meldkamer. • Stedelijk toegangsbeleid is ingericht. Hiermee is voldaan aan de 4e geïdentificeerde randvoorwaarde. • Pasaanvragen voor zone 2-ruimten moeten procedureel door de ruimteverantwoordelijke worden goedgekeurd. Dit is onderdeel van het stedelijk proces voor toegangsverlening. • Logging van scannen van passen wordt zes maanden bewaard.	

2. Informatiebeveiliging IV en Hardware in pand	Beoordeling
2a. Onvoldoende onderbouwing besluit plaatsing scan-pc buiten ADW Een risicoanalyse van de plaatsing van de scan-pc's buiten ADW voorzien van te treffen beheersmaatregelen was achteraf niet beschikbaar. Het risicoprofiel wordt beïnvloed door gebruik van een pc met interne harde schijf + werken anders dan via de kantoorstandaarden (= via ADW). De scan-pc is evenals de ADW-werkstations voorzien van onbeveiligde usb-poorten.	
2b. Beveiliging scan-pc - Logische toegangsbeveiliging De wachtwoorden gebruikt in het scanproces zijn eenvoudig te achterhalen. Het wachtwoord voor inlog in de scan-pc is opgenomen in de procesdocumentatie. Het wachtwoord voor inlog in FileZilla, de software voor verzenden van de gescande documenten naar Centric, is zonder beveiliging in een tekstbestand aanwezig op de scan-pc. Gebruik van een wachtwoordmanager beveiligd met een wachtwoord en/of biometrische toegang zou hier passend zijn.	
Akkoord bevonden zijn: • De scan-pc's beschikken niet over internettoegang. • De gebruikers hebben in opzet niet de mogelijkheid om software op de pc te installeren • De scan-pc's zijn voorzien van virusscanner en malwareprotectie welke op afstand door Centric wordt onderhouden. • De software voor scannen en verzenden van de gescande documenten naar de SaaS-oplossing Key2Belastingen wordt eveneens op afstand door Centric onderhouden. • De beveiliging van de harde schijven van de scan-pc's is voorzien van Bitlocker. • De communicatie met Centric is in opzet en bestaan voldoende beveiligd.	

3. Proces van scannen inkomende poststukken Belastingen	Beoordeling
3a. Archiveren en vernietiging van fysieke poststukken Het vernietigingsproces voor fysieke poststukken bevat zwakheden zoals het gebruik van wisselende kwaliteit papiercontainers waarbij het veelal na sluiting van de papierbak nog mogelijk is documenten uit de bak te halen en het stallen van afgesloten volle papierbakken in een zone 1 ruimte in afwachting van de ophaaldienst. Het risico wordt vergroot doordat documenten niet worden versnipperd voor plaatsing in de papiercontainer.	
3b. Schonen digitale opslaglocaties Belastingen heeft gekozen voor een werkwijze waarbij een kopie van de gescande bestanden dagelijks op de G-schijf worden geplaatst. Er is geen proces ingericht voor schoning van de bestanden op de G-schijf. Wel is belastingen inmiddels gestart met het ontwikkelen van een informatiebeheerplan. Ook is geconstateerd dat meer medewerkers zijn geautoriseerd voor deze G-schijf dan noodzakelijk in de huidige procesuitvoering. Deze autorisaties zijn n.a.v. de audit alsnog ingetrokken. Wel worden de bestanden na verzending dagelijks verwijderd van de scan-pc's en van de externe harde schijf, die gebruikt wordt voor transport naar de G-schijf binnen de postkamer. Dit betreft eenvoudige verwijdering waarbij data achteraf door een IT-specialist alsnog (deels) kan worden hersteld. Tijdens het locatiebezoek bleek de prullenbak op de pc nog niet opgenomen te zijn in het schoningsproces. Schonen van de prullenbak is n.a.v. de audit alsnog toegevoegd.	
Akkoord bevonden zijn: • Tijdige vernietiging van ontvangen fysieke post is geborgd. De post wordt na scannen voorzien van een label met de datum van vernietiging en op volgorde van datum van vernietiging in de kast van de postkamer opgeslagen. Een logboek van ontvangst en vernietiging is aanwezig en wordt bijgehouden.	

• Ontvangen fysieke post wordt dagelijks gesorteerd en vervolgens gescand. De gescande documenten zijn voorzien van een benaming op basis waarvan de documenten na ontvangst door Centric in de juiste werkvoorraad geplaatst kunnen worden. • De gescande documenten worden na verzending dagelijks van de scan-pc's verwijderd.	

4. Samenspel van verantwoordelijkheden in één pand	Beoordeling
4a. Samenwerking Belastingen – Facilitair Bureau: Inrichting Procesdocumentatie met duidelijkheid over taken, verantwoordelijkheden en bevoegdheden is beperkt beschikbaar via Mavim en intranet. Deze ontwikkeling is ook beïnvloed door de reorganisatie bij Facilitair Bureau als gevolg van toevoeging van taken (1-1-2021) en wijziging in organisatiestructuur (1-9-2021).	
4b. Samenwerking Belastingen – Facilitair Bureau: Ervaringen Een aandachtspunt in de samenwerking is versterking van de uitvoering. Dit betreft bijvoorbeeld informatielevering, maar ook tijdige realisatie van door betrokken partijen noodzakelijk geachte beveiligingsmaatregelen.	
4c. Samenwerking Belastingen – IV – ICT: Inrichting De samenwerking is vormgegeven in stedelijke generieke processen waarvoor instructie is vermeld op intranet. Procesbeschrijvingen als zodanig zijn niet beschikbaar via de gemeentelijke tool Mavim.	
4d. Samenwerking Belastingen – IV – ICT: Ervaringen In de samenwerking met externe leveranciers is een sterke afhankelijkheid van sleutelpersonen geconstateerd voor tijdige beantwoording van vragen. De samenwerking met ICT betreft een beperkt aantal onderwerpen, m.n. ADW en de balie-app.	
Akkoord bevonden zijn: • Instructies voor aanvragen bij Facilitair Bureau respectievelijk IV zijn op intranet vermeld en kunnen via de self service desk (SSD) worden ingediend. • Belastingen en IV hebben regelmatig contact en overleg, zowel formeel als informeel. • De samenwerking met leveranciers is vormgegeven via contractafspraken. • Medewerkers zijn enthousiast en betrokken bij hun werkzaamheden.	

Analyse

Ondanks alle getroffen maatregelen voor beveiliging van de postkamer en het minimaliseren van gegevens aanwezig in de postkamer resteert nog altijd een risico op het verlies van data, een nieuw datalek. De impact van het lek is beperkt tot:

- 1 maand aan fysiek aanwezige data in de postkamer.
- Onbekende hoeveelheid data in de papierbakken voor een beperkte periode.
- Data van onbekende omvang die eventueel vanaf de beveiligde interne harde schijf van de scan-pc's en de onbeveiligde externe harde schijf (door een IT-expert) kan worden teruggehaald.
- De aanwezigheid van een back-up van gescande poststukken op de G-schijf, waarvoor (nog) geen schoningsbeleid is ingericht en uitgevoerd.

De impact is hiermee beperkt ten opzichte van de oude situatie. Het risico is echter nog niet volledig gemitigeerd en kan verder worden beperkt.

Een (mogelijke) oorzaak van bovenstaande bevindingen is onvoldoende samenwerking tussen partijen. Er zijn geen beleidsstukken en procesbeschrijvingen beschikbaar waaruit ondubbelzinnig blijkt wie verantwoordelijk is voor welke taken en over bijbehorende bevoegdheden beschikt voor uitvoering van de taken. Beveiligingsmaatregelen bij de verschillende partijen zijn niet voldoende op elkaar afgestemd. Wanneer de ene partij iets laat of doet, heeft dat gevolgen voor een andere partij. Een regiehouder voor het geheel ontbreekt.

Een andere (mogelijke) oorzaak betreft het bewustzijn en gedrag. Een aantal bevindingen, zoals de enkelvoudige schoning van de interne harde schijf en het niet legen van de digitale prullenbak, leiden tot de vraag in welke mate voldoende aandacht is voor de beveiliging van informatie. De indruk ontstaat dat iedereen in zijn eigen cocon werkt en dat de grotere opdracht niet wordt gezien. Integrale afstemming met alle betrokken partijen lijkt te weinig plaats te vinden.

Aanbevelingen

Te bespreken mogelijkheden tot verdere beperking van het risico zijn:

- Het stoppen met het maken van een back-up van de gescande poststukken op de G-schijf. Dit betekent ook het sturen op de correcte ontvangst en verwerking van de gescande poststukken door Centric middels goed leveranciersmanagement waarbij specifiek aandacht wordt besteedt aan goed functioneren van de scanstraat en verwerking van de gescande documenten.
- Verbeteren van het bewustzijn en gedrag door het aanbieden van periodieke trainingen op het gebied van informatiebeveiliging.
- Versterken van de samenwerking tussen lijndirectie, locatieteam en specialisten (Facilitair Bureau-Beveiliging, IV, ICT) ter borging van de volledigheid van de identificatie van beveiligingsrisico's en optimalisatie van te nemen maatregelen. Bij iedere bijzondere situatie zou sprake moeten zijn van een gedocumenteerde risicoanalyse met informatie van *alle* betrokkenen en een gedocumenteerde gedegen afweging van mogelijke beheersingsmaatregelen en eventueel periodiek uit te voeren toetsen op het blijvend correct functioneren van deze beheersingsmaatregelen.
- Versterken van de samenwerking tussen lijndirectie, locatieteam en specialisten voor uitvoering van de monitoring van de naleving van gemaakte afspraken.
- Realisatie van een goede mix van aanvullende beveiligingsmaatregelen t.a.v. :
    - Periodieke diepgaande schoning van de scan-pc's met bijvoorbeeld een wekelijks script of als onderdeel van de afsluitroutine van de scan-pc's.
    - Sluitend samenstel van maatregelen omtrent bewaren en vernietigen van ontvangen fysieke poststukken. Dit betreft het geheel vanaf de levering door Pantar tot en met de afvoer van de gesloten volle papierbakken door de contractpartij verantwoordelijk voor transport van te vernietigen documenten.

In bijlage 1 is een volledig overzicht opgenomen van alle door ons getoetste interne beheersmaatregelen met onze conclusies over de opzet, het bestaan en de effectieve werking van de getoetste beheersingsmaatregelen.

Bijlage 1: Overzicht van gecontroleerde beheersmaatregelen

Legenda	
✓	Opzet, Bestaan en/of Effectieve Werking is vastgesteld
O	Opzet, Bestaan en/of Effectieve Werking is gedeeltelijk vastgesteld
✘	Opzet, Bestaan en/of Effectieve Werking is niet vastgesteld
—	Opzet, Bestaan en/of Effectieve Werking is niet getoetst
	Een oordeel is wegens de aard van de vraag niet vermeld. Beantwoording van de vraag is gerealiseerd via subvragen of de aard van de beheersingsmaatregel maakt uitsluitend vaststellen van bestaan op enig moment mogelijk wegens het ontbreken van historie in de vastlegging.

Nr.	Onderwerp	Nr.	Toetsingsvragen	Opzet	Bestaan	Werking	Toelichting
A.	Algemeen	1.	Onderzoek in hoeverre de inrichting van de fysieke- en informatiebeveiliging in opzet, bestaan en werking voldoen aan de voor het te onderzoeken object van onderzoek				
B.	**Fysieke beveiliging gebouw**	2.	Is er een actuele en volledige risico- en dreigingsanalyse van het pand en de processen en werkt deze in voldoende mate?	O	O		Bevinding 1a
		3.	Voldoet het sleutelplan in opzet, bestaan en werking aan de daarvoor gelden voorschriften en kwaliteitseisen?	✘	—		Bevinding 1b
		4.	Hoe ziet het besluitvormingsproces eruit in opzet, bestaan en werking voor investeringen in de fysieke beveiliging van een gebouw?	O	—		Bevinding 1b
		5.	Hoe ziet de opzet, bestaan en werking eruit van het systeem van beveiligingscamera's in en rond een gebouw?	✓	✓		

Nr.	Onderwerp	Nr.	Toetsingsvragen	Opzet	Bestaan	Werking	Toelichting
C.	**Informatiebeveiliging IV en Hardware in gebouw**	6.	Is er een risicoanalyse voor het plaatsen van een scan-pc buiten de beveiligde Amsterdamse werkomgeving? --> Van het waarom van deze hardware-oplossing?	✘	—		Bevinding 2a
		7.	Zijn er beheersmaatregelen in opzet, bestaan en werking voor de beveiliging van de scanpc buiten de beveiligde Amsterdamse werkomgeving?				
		7a.	Logische toegangsbeveiliging	✘	—		Bevinding 2b
		7b.	Hardening	✓	✓		
		7c.	Back-up & recovery	✓	—		
		7d.	Beveiliging van de communicatie	✓	✓		
		7e.	Malwarebescherming	✓	✓		
D.	**Proces van scannen inkomende poststukken Belastingen**	8.	Is er een procesbeschrijving in opzet, bestaan en werking voor het scannen van inkomende poststukken (bij Belastingen)?	✓	✓	✓	
		9.	Is er een procesbeschrijving in opzet, bestaan en werking voor het archiveren en vernietigen van (inkomende) fysieke poststukken?	✓	O	O	Bevinding 3a.
		10.	Zijn er afspraken over het opslaan van gescande poststukken en over de periodieke schoning van de digitale opslagplaats?	O	✘		Bevinding 3b.
E.	**Samenspel van verantwoordelijkheden in één pand**	11.	Hoe werkt het samenspel van verantwoordelijkheden tussen verschillende organisatieonderdelen (in dit geval FB, ICT, IVE en Belastingen)?	O	O		Bevinding 4.
		12.	Zijn Taken, Bevoegdheden en Verantwoordelijkheden vastgelegd en gecommuniceerd?	O	O		Bevinding 4.
		13.	Wie heeft de lead bij een integraal incident, wie beslist, wie communiceert?	✓	✓		

Bijlage 2: Gedetailleerde bevindingen en aanbevelingen

1. Deelonderwerp fysieke beveiliging pand

Achtergrond

In BIO-hoofdstuk 11 is aangegeven dat een beveiligingsbeleid op basis van geïdentificeerde risico's dient te zijn ontworpen en geïmplementeerd. In de beveiligingsbranche is het gebruikelijk om daarvoor per locatie (fysiek pand) een risico- en dreigingsanalyse op te stellen en daarin adviezen op te nemen over te nemen beveiligingsmaatregelen. Onderdelen van het beveiligingsbeleid betreffen het inrichten van toegangsbeveiliging, het inrichten van sleutelbeheer en het realiseren van bewustwording (BIO-hoofdstuk 7).

In het gemeentelijk beveiligingsbeleid is vastgelegd dat de risico- en dreigingsanalyse wordt opgesteld door beveiligingsspecialisten van directie Facilitair Bureau. Implementatie van de gegeven adviezen is de verantwoordelijkheid van de locatiemanager (tot 1-9-2021 de huismeester met diens teamleider). Voor goede en tijdige realisatie van beveiligingsmaatregelen is tijdig betrekken van beveiligingsspecialisten bij wijzigingen in en aan het pand een noodzakelijke voorwaarde.

De locatie Anton de Komplein bestaat uit een complex geheel van gangen voorzien van toegangsdeuren en liften. Het pand bevat meerdere bewoners en als gevolg daarvan ook beveiliging voorzien van meerdere zoneringen. Belastingen is gehuisvest in een zone 2. Deze zone is rechtstreeks per lift toegankelijk, via gangen vanuit een ander deel van het pand en via deuren vanuit trappenhuizen. De postkamer van Belastingen bevindt zich in het deel van het pand toegewezen aan Belastingen en is afzonderlijk voorzien van een zone 2 toegangsbeveiliging (zone 2 binnen zone 2).

Er is een risico- en dreigingsanalyse vanuit de fysieke beveiliging opgesteld in 2016 voor het gehele pand. In juni 2021 heeft een actualisatie gericht op de verhuizing van Belastingen naar de 3^{e} en 4^{e} verdieping plaatsgevonden. In augustus 2021 is een inspectie op nakoming van de adviezen uit juni 2021 uitgevoerd.

Facilitair Bureau heeft in 2021 twee grote wijzigingen doorgemaakt. Per 1 januari 2021 zijn taken gerelateerd aan pandgebruik door Gemeentelijk Vastgoed overgedragen aan Facilitair Bureau. En per 1-9-2021 is een reorganisatie doorgevoerd. Vanaf deze datum valt beveiliging ook onder de verantwoordelijkheid van de locatiemanagers van Facilitair Bureau. De locatiemanagers kunnen advies vragen aan de beveiligingsadviseurs in de afdeling services. Als gevolg van de reorganisatie is de verantwoordelijkheid voor beveiliging hiermee in twee afdelingen verdeeld. De verantwoordelijkheid voor de dagelijkse uitvoering en realisatie van gegevens beveiligingsadviezen is belegd bij de uitvoerende twee afdelingen met de locatieteams. De verantwoordelijkheid voor beleidsmatige activiteiten is belegt in de afdeling services.

1a. Onvolledige realisatie van de adviezen gegeven door de beveiligingsadviseurs

Bevindingen

In juni 2021 zijn door de adviseurs beveiliging en veiligheid 10 adviezen gegeven. Dit betreft adviezen waarvoor de verantwoordelijkheid voor uitvoering deels bij Belastingen legt en deels bij Facilitair Beheer. Aan de hand van vervolgrapportages (uit augustus), documentatie en een locatiebezoek op 8 november is vastgesteld in welke mate de maatregelen zijn gerealiseerd. Ten tijde van de afronding van de audit resteren nog de volgende punten:

- Liftautorisaties zijn nog altijd problematisch. Door eigen waarneming van de auditors is geconstateerd dat het mogelijk is om met de lift in de centrale hal begane grond met een pas voor zone 1 de 3e verdieping te bereiken. Ook is het mogelijk om deze lift zonder pas te betreden.
- De deuren zijn voorzien van sterke deurdrangers. Tijdens een inspectie is echter geconstateerd dat één van de deuren slecht sloot.
- De loopdeuren naar de platte daken op de verdiepingen dienen minimaal voorzien te zijn van een deurcontactsensor aangesloten op het inbraakdetectiesysteem van het pand. Tijdens een inspectie is geconstateerd dat dit voor één van de deuren nog niet is gerealiseerd.
- Geadviseerd is de opslagtermijn van de gescande post te beperken tot 1 maand en op te slaan in een zone 2 ruimte. Dit advies is gerealiseerd. Echter de post wordt nog wel in een standaard kantoorkast opgeslagen. Een betere kast is besteld, maar nog niet ontvangen.
- Geadviseerd is om het personeel te trainen in de naleving van de beveiligingsmaatregelen, met name het tegengaan van "meelopers" in liften, traphuizen en bij klapdeuren. Door Belastingen is besloten tot instructie aan de medewerkers postkamer om niemand toe te laten in de postkamer. Hiermee is gekozen voor een andere, strengere, invulling van het advies specifiek voor de postkamer.

De postkamer is gerealiseerd als een zone 2 in een zone 2 en beschikt uitsluitend over een deur naar een reguliere gang binnen het zone 2 domein van Belastingen. Deze deur is voorzien van een goed functionerende paslezer.

1b. Randvoorwaarden voor goede fysieke beveiliging deels gerealiseerd

Bevindingen

Er zijn verschillende randvoorwaarden waaraan voldaan moet worden voor goed ingerichte en uitgevoerde fysieke beveiliging. Randvoorwaarden relevant voor de beveiliging van de postkamer van Belastingen betreffen:

1. Inrichting van stedelijk toegangsbeleid
2. Inrichting van stedelijk sleutelbeheer voorzien van een sleutelplan

3. Tijdig betrekken van de adviseurs beveiliging en veiligheid bij geplande wijzigingen in het pand zoals verhuizingen en verbouwingen. Tijdig betekent op een moment dat voldoende tijd en praktische mogelijkheden aanwezig zijn om gedegen advies te geven én de adviezen te realiseren voorafgaand aan ingebruikname van de locatie of het deel van de locatie waarvoor de adviezen benodigd zijn. Uiteraard hoort ook budget beschikbaar te zijn voor realisatie van de adviezen.
4. Uitvoering van periodieke toetsing van de geautoriseerden voor zone 2 ruimten, in ieder geval voor de toegang tot de postkamer.

T.a.v. randvoorwaarde 1: Geconstateerd is dat het stedelijk toegangsbeleid via Mavim beschikbaar is. Hiermee is voldaan aan de randvoorwaarde dat stedelijk toegangsbeleid ingericht dient te zijn.

T.a.v. randvoorwaarde 2: Ondanks herhaaldelijk verzoek is het niet mogelijk gebleken om het sleutelbeheer te leveren. Ook het sleutelplan voor de locatie Anton de Komplein 150 bleek niet beschikbaar. Hiermee is niet voldaan aan de randvoorwaarde dat stedelijk sleutelbeheer voorzien van sleutelplan ingericht dient te zijn.

T.a.v. randvoorwaarde 3: Belastingen is per 1 juni 2021 verhuisd naar de nieuwe locatie aan de Anton de Komplein 150. De eerste beveiligingsadviezen dateren van juni 2021 en zijn daarna gerealiseerd. Ten tijde van de afronding van de audit waren een deel van de adviezen nog altijd niet gerealiseerd (zie ook bevinding 1a.). Door de adviseurs beveiliging en veiligheid is aangegeven dat tijdens de inspectie t.b.v. de verhuizing van Belastingen ook is geconstateerd dat verbouwingen gaande waren in het pand waar zij niet bij betrokken waren. Hiermee is niet voldaan aan de randvoorwaarde dat de adviseurs beveiliging en veiligheid tijdig betrokken dienen te worden bij wijzigingen.

T.a.v. randvoorwaarde 4: door facilitair vind op dit moment geen uitvoering van de periodieke toetsing van de juistheid van geautoriseerden voor zone 2-ruimten plaats wegens het vele thuiswerken als gevolg van de landelijke beperkingen wegens het Covid-19 virus. Hiermee is niet voldaan aan de vierde randvoorwaarde.

2. Informatiebeveiliging IV en Hardware in pand

Achtergrond

In de BIO zijn de vereisten opgenomen voor de informatiebeveiliging IV en hardware. Dit betreft o.a. H8 beheer van bedrijfsmiddelen, H9 Toegangsbeveiliging, maar ook de hoofdstukken 12 Beveiliging bedrijfsvoering en 13 Communicatiebeveiliging. De BIO-vereisten zijn mede vormgegeven in het gemeentelijk informatiebeveiligingsbeleid met onderliggende documentatie.

	Het gemeentelijk beleid is dat alle IT-toepassingen en hardware binnen ADW worden geplaatst. Indien het technisch niet mogelijk is om de IT-toepassing binnen ADW te laten functioneren kan directie ICT op basis van een risicoanalyse alsnog toestemming verlenen en worden aanvullende beveiligingsmaatregelen getroffen. Alle inkopen van IT-toepassingen, waaronder ook de scanstraat bij Belastingen, vinden plaats via de leadbuyer ICT. De scanstraat bij Belastingen is aangeschaft als onderdeel van de SaaS-oplossing Key2Belastingen met bijbehorende applicaties en koppelingen. Onderdeel van de aanschaf betrof de hardware welke door leverancier Centric is geleverd voorzien van de benodigde installaties voor uitvoering van de scantaken. De aanbesteding van de SaaS-oplossing Key2Belastingen met bijbehorende applicaties en koppelingen is begeleidt door de lead-buyer ICT. Medewerkers van directie ICT, evenals van de IV-eenheid, zijn als projectmedewerkers betrokken geweest bij de implementatie van deze SaaS-oplossing, waar de scanstraat een onderdeel van is. De postkamer is enkele jaren geleden van IV-DIV overgegaan naar Belastingen. De scanstraat bevindt zich fysiek op een locatie van gemeente Amsterdam en is via een ethernetkabel aangesloten op een netwerkpoort. Op basis van MAC-adres en IP zijn connecties gelegd van/naar Centric servers.

2a. Onvoldoende onderbouwing besluit plaatsing scanpc buiten ADW

Bevinding	Ten tijde van de audit was het niet (meer) mogelijk voor betrokkenen om een vastlegging te leveren van de risicoafweging en het besluit tot verlenen van toestemming om de scanstraat buiten de ADW-omgeving te plaatsen. In deze risicoafweging was informatie verwacht over de geïdentificeerde risico's en getroffen mitigerende beveiligingsmaatregelen wegens gebruik van dezelfde infrastructurele poorten als voor toegang tot ADW. Directie ICT is samen met leverancier Motiv betrokken geweest bij de installatie en activering van de scanstraat met de on-line-verbinding naar het datacentrum van Centric. Dit als onderdeel van het VIB-project. De besluitvorming omtrent het plaatsen van de scan-pc buiten ADW heeft in project VIB plaatsgevonden. Bij de verhuizing is geen nieuwe risicoanalyse opgesteld. Risicoanalyses zijn wel opgesteld voor de SaaS-oplossing van Key2Belastingen met bijbehorende applicaties en koppelingen. Dit betreffen en verkorte en een uitgebreide risicoanalyse en een privacy-risicoanalyse. De analyses zijn initieel opgesteld bij de start van de vervanging van Neotax in 2015 en aangescherpt bij actuele ontwikkelingen zoals de implementatie van Key2Woz en de integratie van gemeente Weesp. De scan-pc's worden echter niet genoemd in deze risicoanalyses.

	Belangrijke verschillen tussen de scan-pc's en ADW-werkstations betreffen de aanwezigheid van een rechtstreekse verbinding met Centric en de aanwezigheid van een interne harde schijf waar informatie opgeslagen kan worden. De scan-pc's beschikken over standaard windows-functionaliteit, maar zonder algemene internet-toegang. Tijdens de audit is vastgesteld dat de beveiliging van de interne harde schijven in opzet en bestaan toereikend zijn. Ook is vastgesteld dat de beveiliging van de communicatie met Centric in opzet en bestaan toereikend is. Overigens is ook geconstateerd dat de usb-poorten van de scan-pc's evenals van de gemeentelijke ADW-stations zonder (wachtwoord)beveiliging bruikbaar zijn voor de medewerkers.

2b. Beveiliging scanpc – logische toegangsbeveiliging

Bevinding	De scanpc's zijn voorzien van beveiligde toegang bestaande uit een gebruikersnaam en wachtwoord. Het gebruikersaccount bestemd voor de postkamermedewerker is één account welke door beide postkamermedewerkers gezamenlijk wordt gebruikt. Het wachtwoord is opgenomen in de procesdocumentatie van het scanproces. Periodieke wijziging van het wachtwoord wordt niet technisch of procedureel afgedwongen. De gebruikersnaam is gelijk voor beide postmedewerkers, niet vermeld in de procesdocumentatie maar aanklikbaar bij inloggen. Het generieke account kan op beide scan-pc's gelijktijdig worden gebruikt. Hiermee wordt niet voldaan aan de vereisten opgenomen in het gemeentelijk informatiebeveiligingsbeleid en de BIO ten aanzien van unieke identificeerbaarheid en geheimhouding. Voor toegang tot de software (Kofax) benodigd voor scannen van de post is geen extra inlog noodzakelijk. Hiermee wordt gebruik gemaakt van single sign on voor de scanfunctionaliteit. Voor toegang tot de verzendfunctionaliteit (Filezilla) is gebruik van een ander wachtwoord noodzakelijk. Het wachtwoord is opgenomen in een tekstbestand welke op de scanpc's zelf is opgeslagen. Het tekstbestand is niet voorzien van verdere toegangsbeveiliging (logisch, biometrisch). De bescherming van het wachtwoord voor Filezilla is hiermee beperkt tot de beveiliging van de scan-pc met eenvoudige inlogprocedure. De PC zelf is geplaatst in een zeer beperkt toegankelijke zone 2-locatie. De postkamermedewerkers evenals medewerkers van IV en ICT beschikken niet over de mogelijkheid van remote access tot de scanpc's.

3. Proces van scannen inkomende poststukken Belastingen

3a. Archiveren en vernietiging van fysieke poststukken

Achtergrond

Het proces scannen van inkomende poststukken bij directie Belastingen verloopt als volgt:

- Pantar bezorgt de post. Pantar haalt daarvoor bij de receptie een pasje, loopt via de afgesproken route door het pand, levert de post af bij de postkamer, loopt terug en levert de pas weer in bij de receptie.
- De medewerker van de postkamer opent de post en sorteert de post voor het scannen van de documenten
- De gescande poststukken worden voorzien van de datum van geplande vernietiging en in de kast gelegd.
- Op de geplande datum van vernietiging worden de poststukken uit de kast gehaald en in de papiercontainer gegooid.

Proces van afvoer van te vernietigen poststukken

- Zodra de papiercontainer vol is wordt deze afgesloten
- De medewerker postkamer belt facilitair voor afvoer van de volle papiercontainer en vervanging met een lege papiercontainer
- De volle papiercontainers worden geplaatst in de opslagruimte (beveiligd met zone 1)
- Op de afgesproken dag worden de volle papiercontainers in de vrachtwagen geplaatst van de externe partij ingehuurd voor vernietiging van gemeentelijke documenten. Lege papiercontainers worden aan de locatie geleverd.

Bevinding

B1. Voor het afvoeren van de vernietigen documenten wordt gebruik gemaakt van papierbakken welke door Facilitair Bureau ter beschikking worden gesteld. De bakken staan geopend in de beveiligde postkamer van Belastingen. De documenten worden rechtstreeks in de papierbak gegooid op de datum van vernietiging.

B2. Volle papierbakken worden gesloten. Hierbij valt het deksel in het slot. De gemeente maakt gebruik van verschillende modellen papierbakken. Sommige bakken hebben een gat in het deksel voor het deponeren van te verwijderen documenten in de bakken', een onbeveiligde 'brievenbus'. Andere bakken hebben een beveiligde 'brievenbus'. Weer andere bakken hebben een deksel dat helemaal dicht is. De postkamer maakt gebruik van alle varianten. Het risico op een datalek doordat iemand documenten uit de afgesloten papierbak haalt wordt vergroot doordat de documenten niet worden versnipperd.

	B3. Volle gesloten papierbakken worden in een zone 1 ruimte geplaats in afwachting van ophalen door de gemeentelijke contractpartij voor vernietiging van vertrouwelijke documenten.

3b. Schoning digitale opslaglocaties

Achtergrond	Het proces scannen van inkomende poststukken bij directie Belastingen verloopt als volgt: • Pantar bezorgt de post. Pantar haalt daarvoor bij de receptie een pasje, loopt via de afgesproken route door het pand, levert de post af bij de postkamer, loopt terug en levert de pas weer in bij de receptie. • De medewerker van de postkamer opent de post en sorteert de post • De medewerker van de postkamer logt in op de scan-pc en scant de post in de afgesproken groepen. Iedere batch krijgt een eigen naam welke overeenkomt met de afgesproken aanduidingen ter identificatie en routering van werkvoorraden. • De medewerker logt vervolgens in op Filezilla en verzend de gescande batches naar Centric voor plaatsing in de juiste werkvoorraden in het medewerkersportaal. • De medewerker zet een kopie van de gescande post op een draagbare gegevensdrager en wist vervolgens de gegevens van de scan-pc. • De medewerker verplaatst de kopie van de gescande post met de draagbare gegevensdrager naar de G-schijf op het ADW-werkstation • De medewerker wist de gegevens op de draagbare gegevensdrager. • De poststukken worden voorzien van de datum van geplande vernietiging en in de kast gelegd. • Op de geplande datum van vernietiging worden de poststukken uit de kast gehaald en in de papiercontainer gegooid.
Bevinding	In het proces van scannen van ontvangen fysieke poststukken is sprake van handelingen waarbij opslag en transport van gegevens binnen de postkamer plaatsvindt. Als gevolg van de wens om een back-up van de gescande post op de G-schijf te bewaren wordt gebruik gemaakt van een onbeveiligd transportmedium, een externe harde schijf welke niet betrokken was bij het incident van april 2021. Zowel de harde schijf van de scan-pc als de externe harde schijf worden met de delete-functionaliteit leeg gemaakt na verzending en verplaatsing van de gescande poststukken. Als gevolg van het verwijderen van bestanden van de scan-pc met behulp van de delete-knop worden bestanden in de prullenbak op de scan-pc geplaatst en daarmee niet volledig verwijderd. Naar aanleiding van de audit is het leeg maken van de prullenbak op de scan-pc's toegevoegd aan de procedure. De keuze voor het bewaren van de gescande post op de G-schijf heeft tot gevolg dat vertrouwelijke gegevens op een andere locatie dan

de beveiligde SaaS-oplossing wordt bewaard. Voor de G-schijf zijn geen afspraken voor opschoning aangetroffen. Wel wordt de inrichting van een proces voor schoning in het informatiebeheerplan. Realisatie is gepland in 2022. Ook is de toegang tot de G-schijf getoetst. Geconstateerd is dat meer personen bevoegd zijn tot de G-schijf dan betrokken bij het proces. Naar aanleiding van de bevinding is door de teammanager een verzoek ingediend tot intrekken van de overbodige autorisaties. Deze is opgevolgd door de IVDesk.

4. Samenspel van verantwoordelijkheden in één pand

Achtergrond

In de onderzoeksvragen voor de scope van de audit zijn de volgende vragen gesteld t.a.v. het onderwerp samenspel van verantwoordelijkheden in één pand:
1. Hoe werkt het samenspel van verantwoordelijkheden tussen verschillende organisatieonderdelen (in dit geval FB, ICT, IVE en Belastingen)?
2. Zijn Taken, Bevoegdheden en Verantwoordelijkheden vastgelegd en gecommuniceerd?
3. Wie heeft de lead bij een integraal incident, wie beslist, wie communiceert?

In ons onderzoek hebben we daarvoor de beschikbare procesdocumentatie in Mavim en op intranet geanalyseerd. Ook hebben we de gesprekspartners gevraagd naar hun ervaringen omtrent samenwerking bij de uitvoering van hun operationele taken.

Een belangrijk aandachtspunt is dat bij Facilitair Bureau in 2021 grote wijzigingen in haar takenpakket en in haar organisatiestructuur zijn doorgevoerd. Per 1 januari 2021 zijn taken door directie Gemeentelijk Vastgoed overgedragen aan Facilitair Bureau. Dit betreffen taken gerelateerd aan het gebruik van het gebouw en de daarin aanwezige werkplekken. Per 1 september 2021 is vervolgens een reorganisatie doorgevoerd binnen Facilitair Bureau waarbij alle operationele taken in locatieteams zijn samengevoegd en regietaken in gespecialiseerde productafdelingen (afdeling services, afdeling huisvesting). Doelstellingen van de reorganisatie zijn minder schakels, eenvoudige structuur, meer aandacht voor uitvoering (met directe sturing), duidelijk eigenaarschap, fijne samenwerking en een mooie balans in de organisatie (strategie-tactisch-operationeel).

Op een eerder moment (2019) is een reorganisatie geweest waarbij de postkamer van IV-DIV is overgedragen aan Belastingen. Hierbij zijn mensen en hardware overgedragen.

De derde deelvraag is geïnterpreteerd als betrekking hebbend op het incident van april 2021. Dit is het enige ons bekende incident waar

	alle vier partijen daadwerkelijk bij betrokken zijn. De inrichting en het bestaan van stedelijke processen is meegenomen bij de beantwoording van de vragen 1 en 2.

4a. Samenwerking Belastingen - Facilitair Bureau: Inrichting

Bevindingen	De documentatie van de stedelijke processen voor facilitaire taken, waaronder de beveiliging van de locaties, is in ontwikkeling. 1. In Mavim zijn inmiddels schema's beschikbaar van een aantal processen zoals toegangsbeheer. Andere processen zoals sleutelbeheer zijn nog in ontwikkeling. 2. Op intranet is eveneens informatie opgenomen over de stedelijke afspraken voor verrichting van facilitaire taken. Medewerkers kunnen daar informatie vinden over welke taken facilitair verricht en ook staat daar vermeld op welke wijze een facilitair verzoek kenbaar gemaakt kan worden bij Facilitair Bureau. Voor veel typen verzoeken wordt gebruik gemaakt van de self service desk. Voor een aantal taken is aanvullend ook nog een mailadres beschikbaar op intranet voor rechtstreeks contact. 3. In de aanwezige documentatie ontbreekt informatie over termijnen voor uitvoering en levering. Ook ontbreekt informatie over terugkoppeling aan de aanvrager over de uitvoering van de ingediende verzoeken. 4. In het toegangsbeleid is de verantwoordelijkheid voor de beveiliging belegd bij de lijnorganisatie, d.w.z. de gebruikers van de locatie. Het toegangsbeleid is onderdeel van het gehele beveiligingsbeleid en regelt o.a. het pasjestoegang. Opvallend is de vermelding in het toegangsbeleid dat het mogelijk is om blanco passen aan te vragen, ook voor zone 2-ruimten, wel gemaximaliseerd op vijf stuks. Bij blanco passen is het gebruik niet herleidbaar naar natuurlijke personen. Blanco passen voor zone 2-ruimten zijn verkrijgbaar na goedkeuring door de ruimteverantwoordelijke. 5. Onderdeel van het normenkader (BIO H7) is de werkgeversverplichting om zorg te dragen voor bevordering van gedrag dat een positieve invloed op de informatiebeveiliging heeft. Door Belastingen en Facilitair is aangegeven dat zij daar ieder op hun eigen wijze invulling aangeven. Belastingen bespreekt casussen in werkoverleggen. Facilitair noemde de training bij de introductie van 1Stad1Pas waarbij ze o.a. hebben geleerd om mensen aan te spreken bij twijfel of de persoon zich wel op een locatie bevindt waar deze toegang toe heeft. Beiden gaven aan niet bekend te zijn met verdere centraal georganiseerde trainingen voor het onderwerp I-bewustzijn.

4b. Samenwerking Belastingen - Facilitair Bureau: Ervaringen

Bevinding	Vanuit gesprekken is informatie ontvangen over de ervaringen die de gesprekspartners hebben met ketensamenwerking. Ook maken we gebruik van onze eigen ervaringen in het verkrijgen van informatie gedurende de audit. Uiteraard is het goed om te beseffen dat het

soort informatieverzoeken voor een audit in enige mate kan afwijken van de dagelijkse verzoeken vanuit de lijn.

Tijdens de audit is geconstateerd dat:

1. De beleving van de adviseurs beveiliging en veiligheid is dat het realiseren van aanbevelingen ter versterking van de locatiebeveiliging soms moeizaam verloopt. Dit wordt geweten aan o.a. moeizaam verkrijgen van budget.
2. De beleving van de adviseurs beveiliging en veiligheid wordt versterkt door de constatering in de audit dat een deel van de adviezen gegeven in juni 2021 bij hertoetsing in augustus niet waren gerealiseerd en ook bij onze locatiebezoeken enkele van deze punten geconstateerd konden worden (vb vermelding lift centrale hal, sterkere kast postkamer in rapportage van augustus welke ook naar de contactpersonen bij de lijndirectie was gemaild).
3. Ten aanzien van de omgang met frequente bezoekers van dienstverlenende contractpartijen is sprake van botsende en strijdige afspraken en regels. Een gemeentelijke huisregel is dat bezoekers, en daar vallen medewerkers van gemeentelijke contractpartijen feitelijk ook onder, niet onbegeleid door het pand mogen. Voor de medewerker van contractpartij Pantar is door Belastingen met de accounthouder bij Pantar afgesproken dat deze via een vooraf afgesproken route en met een dagelijks op te halen pas zelfstandig naar de postkamer komt.
4. Wegens het vele thuiswerken heeft Facilitair Bureau de periodieke controle op de juistheid van de verstrekte passen, voor onbepaalde tijd uitgesteld.
5. Bij het verkrijgen van informatie voor uitvoering van een lijncontrole op de verstrekking en inname van toegangspassen bleek het zeer moeilijk om de juiste contactpersoon te verkrijgen waarna vervolgens nog lang op documentatie gewacht moest worden. In week 49 was de benodigde informatie nog niet ontvangen.
6. Belastingen heeft gekozen voor een eigen invulling voor het onderwerp bewustwording. Gekozen is voor stringente toegangsbeperking voor de postkamer. In de hele directie vindt daarnaast gespreksvoering n.a.v. incidenten plaats.

4c. Samenwerking Belastingen - IV - ICT: Inrichting

Bevinding

Vanuit gesprekken is informatie ontvangen over de ervaringen die de gesprekspartners hebben met ketensamenwerking. Ook maken we gebruik van onze eigen ervaringen in het verkrijgen van informatie gedurende de audit. Uiteraard is het goed om te beseffen dat het soort informatieverzoeken voor een audit in enige mate kan afwijken van de dagelijkse verzoeken vanuit de lijn.

Tijdens de audit is geconstateerd dat:

1. Er stedelijk beleid is ingericht voor informatiebeveiliging
2. Er geen procesbeschrijvingen beschikbaar zijn in Mavim voor IV Dienstverlening en Informatie
3. Ook voor ICT zijn geen procesbeschrijvingen beschikbaar in Mavim, wel is een overzichtspagina opgenomen.
4. De werkwijzen van ICT en IV, inclusief onderlinge samenwerking, is uitgebreid op intranet weergegeven. Hieruit blijkt dat wel

	processen zijn ingericht en gehanteerd. 5. De samenwerking met leveranciers (IV – Centric + ICT – Motiv) is vormgegeven via contractafspraken voorzien van bijlagen zoals DAP, SLA etc. Voor de procesinrichting van ICT en IV is relevant dat in 2022 de reorganisatie I-domein gerealiseerd zal worden hetgeen ook weer invloed heeft op de benodigde procesdocumentatie.

4d. Samenwerking Belastingen - IV – ICT: Ervaringen

Bevinding	Vanuit gesprekken is informatie ontvangen over de ervaringen die de gesprekspartners hebben met ketensamenwerking. Ook maken we gebruik van onze eigen ervaringen in het verkrijgen van informatie gedurende de audit. Uiteraard is het goed om te beseffen dat het soort informatieverzoeken voor een audit in enige mate kan afwijken van de dagelijkse verzoeken vanuit de lijn. Tijdens de audit is benoemd: 1. In het scanproces wordt door Belastingen gebruik gemaakt van een onbeveiligde externe harddrive voor het overzetten van data van de scan-pc's naar de G-schijf op het ADW-werkstation. De externe harddrive is meegekomen bij de overdracht van de postkamer naar Belastingen vanuit IV-DIV enkele jaren geleden. 2. Tijdens gesprekken is aangegeven dat de betrokkenheid van directie ICT klein is bij Belastingen als gevolg van het gebruik van de SaaS-oplossing voor uitvoering van het primaire Belastingproces. Het benodigde contact richt zich op ADW en op kleinere toepassingen zoals de Balie-app. Indien toch contact nodig is wordt het contact ervaren als moeizamer dan in het verleden. Er wordt daarbij wel gebruikt gemaakt van de huidige standaardprocessen voor contact tussen IV en ICT. Indien beantwoording van de vragen langer duurt, wordt incidenteel nog wel buiten het proces om rechtstreeks met een leverancier zoals Motiv gebeld. 3. Uit eigen waarneming is tijdens de audit vastgesteld dat voor de levering van informatie sprake is van afhankelijkheid van enkele sleutelpersonen. Afwezigheid wegens vakantie (IV) en ziekte (Centric) heeft bijvoorbeeld tot een vertraging van ca. 2-3 weken in oplevering van informatie benodigd voor vaststelling van het bestaan van beveiligingsmaatregelen geleidt.

Bijlage 3: Gezamenlijke managementreactie

Hieronder is de gezamenlijke managementreactie van de directies Belastingen, Facilitair Bureau, ICT en de IV-eenheid opgenomen.

De directies Belastingen, Facilitair Bureau, ICT en de IV-E/Dienstverlening & Informatie kunnen zich vinden in de bevindingen en aanbevelingen in het auditrapport Informatiebeveiliging omtrent het proces scannen fysieke post. De audit is in opdracht van de directie Belastingen uitgevoerd door DMC/Interne Audit. De aanleiding was een incident met een ontvreemde harde schijf uit een scanpc bij Belastingen medio april 2021, uit het vorige pand van Belastingen aan de Herikerbergweg.

Op 23 december 2021 zijn de auditresultaten door Interne Audit aan de directies gepresenteerd, waarbij de belangrijkste bevindingen en aanbevelingen met de directies zijn besproken. De directies zijn content met de integrale aanpak van de audit, waarin het belang van samenwerken en communicatie is aangetoond.

De directies onderschrijven de conclusie dat de digitale en fysieke gegevens verwerkt in het scanproces, nog niet voldoende zijn beschermd. Het risico van een datalek is nog niet uitgesloten. Geconstateerd is dat de informatiebeveiliging wel sterk is verbeterd t.o.v. de oude situatie aan de Herikerbergweg. Het is lastiger gemaakt om toegang tot de gegevens te krijgen. Daarbij is met name de omvang van een potentieel datalek (impact) aanzienlijk beperkt. De belangrijkste verbeteringen zijn het dagelijks verwijderen van de gescande stukken van de scan-pc en de forse beperking in de toegang tot de postkamer. Gezien de extra gevoelige informatie van gegevens, mag verhoogde bescherming worden verwacht. Uit de bevindingen blijken een aantal aandachtspunten waardoor nog risico op herhaling van een datalek bestaat. De directies onderschrijven deze risico's en nemen de opgenomen aanbevelingen over.

De directies hebben afgesproken dat een werkgroepje, samengesteld uit medewerkers van de vier ketenpartners en de ISO, aan de slag gaat met het concretiseren en uitvoeren van de opgenomen aanbevelingen. Een eerste bijeenkomst daarvoor wordt in januari gepland. Het initiatief daartoe zal door de directie Belastingen worden genomen. Medio april/mei volgt een tweede afstemming op directieniveau waarbij in ieder geval wordt gesproken over de voortgang van de uitvoering en over de wijze waarop de samenwerking en communicatie in de keten kan worden versterkt.

Mede namens de directies Facilitair Bureau, ICT en de IV-E/Dienstverlening en Informatie,

[redacted]

[redacted]

[redacted]