DEPARTEMENT
KANSELARIJ &
BUITENLANDSE ZAKEN

Vlaamse overheid
Beroepsinstantie inzake openbaarheid van bestuur
en hergebruik van overheidsinformatie
Afdeling openbaarheid van bestuur
Havenlaan 88, bus 20
1000 BRUSSEL
T : 02 553 57 25
Mail: openbaarheid@vlaanderen.be

Dossiernummer: OVB/2023/094

DE BEROEPSINSTANTIE - Afdeling openbaarheid van bestuur

Bevoegdheid beroepsinstantie

Bestuursdecreet van 7 december 2018, titel II, hoofdstuk 3, afdeling 6.

Besluit van de Vlaamse Regering van 19 juli 2007 tot oprichting van de beroepsinstantie inzake openbaarheid van bestuur en hergebruik van overheidsinformatie.

Voorafgaande procedure

Op 28 februari 2023 diende [redacted] (hierna vermeld als: verzoeker), een verzoek in bij de stad Antwerpen en het Autonoom Gemeentebedrijf Digipolis Antwerpen tot het verkrijgen van een afschrift van de volgende documenten:

1. Het forensisch technisch rapport dat is opgesteld als onderdeel van het onderzoek naar de cyberaanval, inclusief een "Root Cause Analysis" en beschrijving van de volgende elementen:

- Het algemene scenario
- De wijze waarop de aanvaller initieel toegang kreeg tot het systeem
- De laterale bewegingen en de wijze waarop de aanvaller deze uitvoerde
- Hoe de aanvaller zijn privileges heeft geëscaleerd naar een hoger niveau
- Hoe de aanvaller een persistente toegang heeft gekregen tot het systeem
- Hoe de ransomware werd verspreid
- Wat de payload was van de aanval (enkel encryptie of encryptie en exfiltratie van data)
- De geobserveerde technieken en procedures
- Een lijst van indicatoren (IOC's)
- Technische bewijsstukken
- De gebruikte methodiek
- De gebruikte software
- Een algemene tijdlijn

2. Het technisch rapport over hoe de stad Antwerpen haar infrastructuur heeft opgeschoond en terug online heeft gebracht.

3. Informatie over de wijze waarop de derde partij die betrokken was bij de incident response process is gekozen en welke criteria hiervoor zijn gehanteerd, inclusief:
- Welke partij is voor welk doel aangetrokken
- De basis waarop deze werden geselecteerd
- Wat was de respectievelijke kost van deze partijen
4. Inzicht in de rol van Digipolis in dit verhaal, met name of Digipolis de ICT-provider voor de stad Antwerpen is en op welke manier het betrokken is geweest bij het incident.
5. De communicatie tussen de stad Antwerpen en het Cyber Security Center Belgium (CCB) met betrekking tot de aanval.

Bij mailbericht d.d. 17 maart 2023 werd voormeld openbaarheidsverzoek gedeeltelijk afgewezen door een gezamenlijk besluit van de stad Antwerpen en AG Digipolis Antwerpen.

Met een mail d.d. 7 april 2023 heeft verzoeker beroep ingesteld tegen de voormelde gedeeltelijke weigeringsbeslissing van de stad Antwerpen en AG Digipolis Antwerpen. Het beroepschrift werd op 7 april 2023 geregistreerd door de beroepsinstantie.

Ontvankelijkheid van het beroep

Het oorspronkelijk openbaarheidsverzoek van verzoeker dateert van 28 februari 2023.

De gedeeltelijke weigeringsbeslissing van de stad Antwerpen en AG Digipolis Antwerpen dateert van 17 maart 2023. Via een afzonderlijke mail d.d. 31 maart 2023 werd verzoeker op de hoogte gesteld van de beroepsmogelijkheid en -modaliteiten, zoals voorgeschreven in artikel II.43, §1, derde lid van het Bestuursdecreet.

Het beroep van verzoeker werd ingediend bij mailbericht d.d. 7 april 2023 en is bijgevolg tijdig ingesteld.
Het ingediende beroep is bijgevolg **ontvankelijk**.

Gegrondheid van het beroep

Overeenkomstig artikel II.31, eerste lid Bestuursdecreet heeft het recht op passieve openbaarheid betrekking op bestuursdocumenten. Op grond van deze bepaling is elke instantie in principe verplicht aan eenieder die erom verzoekt inzage te geven in, uitleg te verschaffen over of een afschrift te bezorgen van de gewenste bestuursdocumenten.

De openbaarmaking kan slechts geweigerd worden mits toepassing wordt gemaakt van één of meerdere uitzonderingen, zoals gestipuleerd in de artikelen II.33 tot en met II.39 van voormeld decreet.

1. De beslissing van de stad Antwerpen en AG Digipolis Antwerpen

Met hun besluit d.d. 17 maart 2023 hebben de stad Antwerpen en AG Digipolis Antwerpen het openbaarheidsverzoek ingewilligd voor wat betreft het derde onderdeel van het openbaarheidsverzoek (informatie over de wijze waarop de derde partij die betrokken was bij het incident werd gekozen en welke criteria hiervoor zijn gehanteerd).

Wat betreft het vierde onderdeel van het openbaarheidsverzoek (de rol van Digipolis in dit verhaal, met name of Digipolis de ICT-provider voor de stad Antwerpen is en op welke manier het betrokken is geweest bij het incident) werd in de beslissing aangegeven dat daaromtrent geen afzonderlijke documenten werden

opgemaakt. De rol en het takenpakket van Digipolis Antwerpen wordt immers heel uitvoering beschreven op de website: https://www.digipolisantwerpen.be/

Voorst werd het openbaarheidsverzoek afgewezen voor het eerste, tweede en vijfde onderdeel van het openbaarheidsverzoek en daarvoor werd verwezen naar de volgende uitzonderingsgronden:

- Artikel II.34, 2° Bestuursdecreet: Het forensisch technisch rapport en bijlagen bevat mogelijk, maar niet zeker, persoonlijke gegevens van andere personen. Het is disproportioneel om alle personen wiens gegevens mogelijk maar niet zeker in de betreffende bestuursdocumenten zijn opgenomen te identificeren en om instemming te verzoeken met inzage door de aanvrager in deze bestuursdocumenten.
- Artikel II.34, 3° Bestuursdecreet: Het forensisch technisch rapport en bijlagen, het technisch rapport en bijlagen en de opgevraagde communicatie betreffen documenten die instrumenteel zijn in het kader van de besluitvorming van AG Digipolis Antwerpen en stad Antwerpen aangaande de cyberveiligheid en de digitale strategie van stad Antwerpen. Deze documenten zijn onlosmakelijk verweven met de door de diverse organen genomen beslissingen. Deze documenten kunnen niet openbaar gemaakt worden zonder het geheim van beraadslaging te schenden.
- Artikel II.35, 1° Bestuursdecreet: het belang van de openbaarheid weegt niet op tegen de bescherming van een economisch, financieel of commercieel belang van de stad Antwerpen.
- Artikel II.35, 3° Bestuursdecreet: De cyberaanval waarvan stad Antwerpen het voorwerp is geweest, was van een ongeziene schaal, en heeft een ongekende impact gehad op de IT-infrastructuur van de stad Antwerpen. De snelheid waarmee het herstelplan is opgesteld en uitgevoerd wordt, heeft geleid en leidt tot innovatieve inzichten, strategieën, samenwerkingsvormen en methodologieën die een onmiskenbaar economische waarde hebben voor alle betrokken stadsdiensten, alsook voor alle interne en externe partijen betrokken bij de opzet van de nieuwe IT-infrastructuur en het nieuwe IT-netwerk. Veel van de opgestelde documentatie zijn de neerslag van creatieve, originele denkprocessen die om deze reden beschermd zijn door het auteursrecht.
- Artikel II.35, 5° Bestuursdecreet: het belang van de openbaarheid weegt niet op tegen de bescherming van het vertrouwelijke karakter van de handelingen van een overheidsinstantie als die vertrouwelijkheid noodzakelijk is voor de politieke besluitvorming: De digitale strategie van stad Antwerpen voor de toekomst, en de acute en actuele nood tot een versnelde uitvoering ervan, heeft een belangrijke financiële impact en een groot operationeel belang voor de stad Antwerpen en de Antwerpenaar. De objectieve politieke besluitvorming in dit kader moet maximaal beschermd worden.
- Artikel II.35, 6° Bestuursdecreet: het belang van de openbaarheid weegt niet op tegen de openbare orde en de veiligheid. Het forensisch technisch rapport en bijlagen, het technisch rapport en bijlagen en de opgevraagde communicatie bevatten informatie over sterktes en kwetsbaarheden van de IT-infrastructuur en het IT-netwerk van stad Antwerpen die experten hebben geobserveerd, over waarom de cyberaanval de gevolgen heeft kunnen hebben die deze had, alsook aanbevelingen om zich te beschermen tegen een toekomstige cyberaanval. Deze documenten bevatten gevoelige informatie over het cyberveiligheidsbeleid van stad Antwerpen en de operationalisering ervan. De openbare veiligheid staat eraan in de weg dat deze informatie openbaar wordt gemaakt.

2. Inhoud van het beroepschrift

Verzoeker geeft in zijn beroepschrift aan dat hij geen beroep instelt wat betreft het derde en vierde onderdeel van zijn openbaarheidsverzoek. Het beroep is dus beperkt tot het eerste, tweede en vijfde onderdeel van het oorspronkelijk openbaarheidsverzoek en hij motiveert zijn beroep als volgt:

" Het forensisch technisch rapport

Beginnende bij het meest pertinente voorbeeld van punt 1, het forensisch technisch rapport. Als uitzonderingsgrond haalt men het volgende aan:

1. Mogelijke maar niet zekere aanwezigheid van persoonsgegevens
2. Het geheim van de beraadslagingen
3. Bescherming van het economisch belang
4. Bescherming van commerciele en industriele informatie
5. Het auteursrecht
6. Bescherming van:

a. Administratieve handhaving
b. Een lopende audit
c. Politieke besluitvorming

7. Bescherming van de openbare orde

Mochten al de bovenstaande zaken tegelijk waar zijn dan dient dit rapport de stempel vertrouwelijk of geheim te dragen volgens de criteria beschreven in de wet van 11 december 1998 (https://etaamb.openjustice.be/nl/wet-van-11-december-1998_n1999007004.html). Ik neem dan ook aan dat dit niet het geval is, mocht het wel zo zijn zal ik mijn aanvraag zal aanpassen naar een tot inzage ter plaatse en de juiste veiligheidsmachtiging voorleggen. Beroepshalve ben ikzelf forensisch analist en schrijf ik regelmatig forensische rapporten als derde partij voor een slachtoffer van een cyber aanval. Sta mij toe uit te leggen wat er in zo een rapport wel en niet in staat:

I. Een forensisch technisch rapport bevat normaal weinig tot geen persoonsgegevens. Het is zeker mogelijk dat een account dat misbruikt werd opgenomen is in het rapport maar dit kan op zeer eenvoudige manieren geredigeerd worden zodat de link tussen de accountnaam en de persoon volledig verdwijnt. Ik aanvaard het argument dat er persoonsgegevens in kunnen staan, maar de kleine moeite die het kost om deze uit het rapport te halen (als ze er al in staan) mag volgens mij geen reden zijn om het principe van openbaarheid van bestuur uit te hollen.

II. Een forensisch rapport gaat over hoe een aanvaller binnen is gedrongen in een systeem, wat hij daar gedaan heeft en welke sporen hij/zij heeft achtergelaten. Dit gaat in geen geval over iets waarbij de stadsdiensten betrokken zijn geweest, daar de aanval gebeurde voor dat er iemand ook maar op de hoogte was van wat er speelde. De volgende argumenten zijn desgevallend niet van toepassing op dit rapport:

a. Geheim van beraadslaging
b. Bescherming van de administratieve handhaving
c. Bescherming politieke besluitvorming

III. We zijn ondertussen een 5 maanden na de aanval, enige kwetsbaarheid dit blootgelegd werd door dit rapport zal ondertussen verholpen zijn. In het hoogst opmerkelijke geval dat dit niet zo zou zijn aanvaard ik een redelijke aanpassing van de termijnen waarin de documenten overgemaakt dienen te worden. Met dat de kwetsbaarheden verholpen zijn in het systeem vervalt het argument van bescherming van de openbare orde.

IV. Als de stad antwerpen bij een derde partij een forensische analyse vraagt en bekomt is de stad Antwerpen ook gewoon eigenaar van alle rechten op dat rapport daar de stad voor dit rapport een, hopelijk billijke, vergoeding heeft betaald aan de derde partij. Het argument van de auteursrechten op het forensische rapport die de handelingen van de aanvaller beschrijft is dus ontegensprekelijk op lucht gebaseerd.

V. Daar het rapport in kwestie de handelingen en technieken van een aanvaller / crimineel beschrijft en niet van de stad zijn de argumenten van bescherming van het economisch belang en bescherming van commerciële en industriële informatie zonder onderwerp. Het tegenovergestelde is trouwens waar. Alle commerciële en private entiteiten hebben een belang bij het openbaar maken van juist deze informatie daar dat hun toe laat zichzelf ervan te vergewissen dat ze goed beschermd zijn ten opzichte van de technieken, procedures en tactieken van de aanvaller.

VI. Rest er nog het punt van de bescherming van een lopende audit. Eens een forensisch rapport over hoe de aanval heeft plaats gevonden, wat de aanvaller deed en welke technieken hij gebruikte is afgerond is dit een vast gegeven voor de lopende onderzoeken. Het publiek maken hiervan kan slechts als effect hebben dat er mogelijk iemand anders met kennis van zaken mogelijke fouten uit het rapport kan halen, of aanvullende inzichten kan geven (peer review). Dit kan de lopende onderzoeken enkel voordelig uitkomen.

Het punt i.v.m. de opschoning van het netwerk

Ik aanvaard dat men deze niet wil openbaar maken zolang de audit over de effectiviteit (niet efficiëntie) van de genomen maatregelen nog niet is afgerond onder de noemer van bescherming van de administratieve handhaving alsook bescherming van een lopende audit. Wat ik niet wil aanvaarden is het argument van het auteursrecht (zelfde redenering als bij het forensisch technisch rapport) noch deze van: bescherming van het economisch belang, commerciële en industriële informatie. Ook hier hebben de belastingbetalers er alle baat bij dat deze informatie publiek gemaakt word teneinde zichzelf beter te kunnen wapenen tegen mogelijke nieuwe aanvallen op hun infrastructuur. Teneinde woninginbraken te doen afnemen doet de stad toch ook campagnes om de burgers te informeren, waarom zouden ze niet hetzelfde principe hanteren voor het digitale equivalent? Ook hier zijn we bezig over technische zaken en safeguards, het argument van bescherming van politieke besluitvorming houdt dus wederom geen steek. Bottom line: ik aanvaard uitstel tot implementatie van de technische middelen en het afronden van de audit over de effectiviteit maar vraag uitdrukkelijk van daarna de gehanteerde methodiek en systemen te openbaren.

De communicatie met het CCB

Ik betreur ten stelligste dat het argument van politiek beraad/besluitvorming hiervoor aangewend wordt voor de openbaarheid van bestuur te herleiden naar een schijnvoorstelling. Ik herinner er aan dat wetten dienen om de burger te beschermen t.o.v. de overheid en niet de overheid te beschermen voor de burger.

Conclusie

Ik kan mij niet van de indruk ontdoen dat de stadsdiensten zich in dit geval getracht hebben om en zo nauw mogelijke invulling te geven aan de openbaarheid van bestuur in plaats van de voor en nadelen tegen elkaar af te wegen en een eerlijke analyse te maken a charge en a decharge. Daar een poging tot bemiddeling of verduidelijking afgewezen werd door de stadsdiensten, vraag ik aan het Vlaamse niveau om hier als beroepsorgaan op te treden en uitdrukkelijk het punt 1 (punt 3.1 in het antwoord van de stad) toch gegrond en ontvankelijk te verklaren alsook punt 2 (3.2 in het antwoord) in overweging te nemen en met een zeker uitstel ook te doen openbaren daar vele burgers een voordeel kunnen halen uit de openbaring ervan. “

3. Standpunt van de beroepsinstantie

De beroepsinstantie heeft contact opgenomen met de stad Antwerpen en het AG Digipolis Antwerpen, waarbij om nadere toelichting werd gevraagd aangaande de door verzoeker opgevraagde documenten.

Vanuit de stad Antwerpen en het AG Digipolis Antwerpen werd uitvoerig toelichting gegeven aan de beroepsinstantie op 12 april 2023, 26 april 2023, 28 april 2023 en 3 mei 2023. Tevens werden de opgevraagde documenten aan de beroepsinstantie bezorgd, zodat deze kennis kon nemen van de inhoud ervan.

Uit de ingewonnen informatie is gebleken dat er, voor wat betreft het eerste onderdeel van het openbaarheidsverzoek, drie rapporten/analyses in aanmerking komen die het voorwerp uitmaken voor dit onderdeel:

- Finaal onderzoeksrapport van 26 december 2022 door Orange Cyberdefense (externe partner die werd aangezocht door Digipolis om digitale forensische audit uit te voeren)
- Incident report d.d. 13 februari 2023 door CERT (federale Cyber Emergency Response Team, de operationele dienst van het Centrum voor Cybersecurity België - CCB)
- Interne analyse door Digipolis Antwerpen d.d. 11 december 2022 met betrekking tot de cyberaanval

Voor wat betreft het tweede onderdeel, stelt de beroepsinstantie samen met de stad Antwerpen en Digipolis Antwerpen vast dat er geen "technisch rapport" an sich bestaat over hoe de stad Antwerpen haar infrastructuur heeft opgeschoond en terug online heeft gebracht of gaat brengen. Wel bestaan er in dat verband vijf presentaties (PowerPoint) die intern werden opgesteld binnen de stad Antwerpen en Digipolis Antwerpen en dienden voor interne overlegvergaderingen met informatici, cyberbeveiliging of bestuursorganen. Het gaat daarbij om de volgende documenten, die naar de mening van de beroepsinstantie het voorwerp uitmaken van het tweede onderdeel van het openbaarheidsverzoek:

- Overzicht van 16 december 2025 van de vastgestelde feiten van de cyberaanval en de ondernomen acties
- Overzicht op 18 december 2022 met dringende aandachtspunten en prioriteitenlijst
- Overzicht van stand van zaken op 3 januari 2023 en plannen voor de heropbouw naar nieuwe beveiligde omgeving
- Overzicht van stand van zaken op 25 januari 2023 en plannen voor de heropbouw naar nieuwe beveiligde omgeving
- Overzicht op 21 februari 2023: stand van zaken en plan van aanpak

Voor wat betreft het vijfde onderdeel van het openbaarheidsverzoek, de communicatie tussen de stad Antwerpen en het CCB (Centrum voor Cybersecurity België), kon de beroepsinstantie vaststellen dat er heel wat mailverkeer heeft plaatsgevonden tussen enerzijds de stad Antwerpen en Digipolis Antwerpen en anderzijds het CCB, dit naar aanleiding van het cyberincident binnen de stad Antwerpen en in voorbereiding van de opmaak van het Incident report d.d. 13 februari 2023 door CERT (federale Cyber Emergency Response Team), de operationele dienst van het Centrum voor Cybersecurity België.

Voor de duidelijkheid geeft de beroepsinstantie in het kort de context weer van de feiten waarbinnen dit openbaarheidsverzoek dient gekaderd te worden (zoals meegedeeld vanuit de stad Antwerpen): begin december 2022 vond er een grote cyberaanval plaats binnen de administratieve diensten van de stad Antwerpen. Naar aanleiding daarvan is er een grootschalige crisisorganisatie op poten gezet binnen de stad Antwerpen en het AG Digipolis Antwerpen, de IT-partner van de stad Antwerpen, waarbij ook externe partners werden betrokken. Er diende te worden achterhaald wat de exacte oorzaak van de cyberaanval was, hoe die technisch kon worden gerealiseerd, wat de onmiddellijke impact was op de interne werking van de stadsdiensten, welke eventuele schade er werd geleden, hoe zo snel mogelijk de meest kritieke toepassingen terug online aan het werk konden worden gekregen, nagaan hoe dergelijke cyberaanvallen in de toekomst kunnen worden vermeden door het opstarten van een nieuwe beveiligde cyberomgeving. Daarvoor werden en worden maximaal alle beschikbare middelen ingezet binnen de stad Antwerpen. Procesmatig, structureel en financieel betreft het hier één van de grootst opgezette processen binnen de stad Antwerpen, een proces die een planmatige aanpak heeft met een zeer lange doorlooptijd.

De beroepsinstantie stelt vast, na kennisname van alle doorgezonden documenten vanuit de stad Antwerpen en het AG Digipolis Antwerpen, dat de openbaarmaking van de documenten zoals door verzoeker gevraagd in het eerste, tweede en vijfde onderdeel van zijn openbaarheidsverzoek (voorwerp van de huidige beroepsprocedure) en zoals die hiervoor werden aangeduid door de beroepsinstantie, terecht werd geweigerd door de stad Antwerpen en het AG Digipolis en de beroepsinstantie verwijst daarbij naar de toepassing van de hierna vermelde uitzonderingsgronden:

Uitzonderingsgronden die van toepassing zijn op alle gevraagde documenten

De beroepsinstantie verwijst in hoofdorde naar de toepassing van *artikel II.39, tweede lid van het Bestuursdecreet*, waarin is bepaald dat de in het Bestuursdecreet bepaalde uitzonderingen gelden, onverminderd de andere bij de wet, het decreet of ordonnantie bepaalde uitzonderingen op de gronden die te maken hebben met de uitoefening van de bevoegdheden van de federale overheid, de gemeenschap of het gewest. In casu verwijst de beroepsinstantie naar de toepassing van *artikel 6, §1, 5° van de federale wet van 11 april 1994 inzake de openbaarheid van bestuur*.

De voormelde wetsbepaling uit de federale openbaarheidswet voorziet dat een verzoek om openbaarmaking wordt afgewezen als het belang van de openbaarheid niet opweegt tegen de bescherming van de opsporing of vervolging van strafbare feiten.

Uit de door de beroepsinstantie ingewonnen informatie blijkt dat er momenteel een gerechtelijk strafonderzoek lopende is om de daders van de voormelde cyberaanval binnen de stadsdiensten van de stad Antwerpen te ontmaskeren en nadien te vervolgen. Er werd enerzijds een PV opgesteld door de Politie te Antwerpen op 7 december 2022, na een klacht vanwege de CEO van Digipolis Antwerpen, en anderzijds is er ook een gerechtelijk onderzoek opgestart door de Federal Computer Crime Unit, een onderdeel van de Belgische Federale Gerechtelijke Politie die bevoegd is om computercriminaliteit te onderzoeken. In casu gaat het dus om een gerechtelijk onderzoek in verband met mogelijke strafbare feiten met betrekking tot internetcriminaliteit, ICT-misdrijven en afpersing.

Het is immers zo dat de bescherming van het opsporingsonderzoek een exclusieve federale bevoegdheid (geregeld in het Wetboek van Strafvordering) is en betrekking heeft op het geheel van handelingen die ertoe strekken de misdrijven, hun daders en de bewijzen ervan op te sporen en de gegevens te verzamelen die dienstig zijn voor de uitoefening van de strafvordering.

Onder voormelde federale uitzonderingsgrond vallen ook die bestuursdocumenten die niet uitsluitend werden opgesteld ten behoeve van de strafvordering, maar die eventueel wel in een strafrechtelijk onderzoek kunnen gebruikt worden. In dat geval dient er een belangenafweging te gebeuren tegenover het belang van de openbaarheid van de opgevraagde documenten.

De beroepsinstantie moet in casu vaststellen dat er momenteel een strafrechtelijk onderzoek loopt vanuit het Parket te Antwerpen, dit in het kader van een gerechtelijk onderzoek naar internetcriminaliteit, ICT-misdrijven en afpersing door onbekenden bij de stadsdiensten van de stad Antwerpen.

De beroepsinstantie is, verwijzende naar het feit dat er momenteel een gerechtelijk onderzoek hangende is naar strafrechtelijke feiten, zoals hiervoor aangegeven, daarom de mening toegedaan dat de openbaarmaking van de opgevraagde documenten aan verzoeker, onmogelijk kan toegestaan worden. Er loopt immers nog volop een strafonderzoek momenteel, waarvan de door verzoeker opgevraagde documenten deel uitmaken: de forensische en technische rapporten i.v.m. cyberaanval en de communicatie tussen stad Antwerpen en CCB. Al deze informatie werd vanuit Digipolis Antwerpen ook al bezorgd aan de bevoegde Parketdiensten.

Daarnaast is er in dit verband ook nog een onderzoek lopende bij de Gegevensbeschermingsautoriteit en de Vlaamse Toezichtscommissie.

De beroepsinstantie concludeert daarom dat de door verzoeker opgevraagde documenten m.b.t. de cyberaanval binnen de stadsdiensten van de stad Antwerpen aan de openbaarmaking moeten worden onttrokken, omdat het belang van de openbaarmaking van die documenten in casu niet opweegt tegen het

belang van de bescherming van de opsporing en de mogelijke vervolging van strafbare feiten, zoals voorzien in artikel 6, §1, 5° van de federale wet van 11 april 1994 inzake de openbaarheid van bestuur. Het is van het allergrootste belang dat dergelijk gerechtelijk onderzoek in alle sereniteit kan worden gevoerd, met respect voor het vermoeden van onschuld van de betrokken partijen en hun rechten op verdediging in een hangend strafrechtelijk onderzoek. De openbaarmaking van de opgevraagde documenten kan dus niet worden toegestaan.

Als bijkomende uitzonderingsgrond verwijst de beroepsinstantie ook naar *artikel II.35, 1° van het Bestuursdecreet*, dat stipuleert dat een aanvraag om openbaarmaking dient afgewezen te worden indien het belang van de openbaarheid niet opweegt tegen de bescherming van het economisch, financieel of commercieel belang van een overheidsinstantie. Deze bepaling heeft tot doel de economische, financiële en commerciële belangen van instanties te beschermen tegen het risico van speculatieve daden die voorkennis van informatie kan meebrengen.

Artikel II.35, 1° van het Bestuursdecreet vertoont een relatief karakter zodat het aan de beroepsinstantie toekomt te oordelen of het belang van de ingeroepen uitzonderingsgrond in casu al dan niet opweegt tegen het belang van de openbaarmaking van het gevraagde.

De stad Antwerpen en Digipolis Antwerpen reiken in hun toelichting aan de beroepsinstantie voldoende valabele argumenten aan om de openbaarmaking van de door verzoeker gevraagde documenten (zoals hoger opgesomd door de beroepsinstantie) te weigeren, omdat de stad Antwerpen zelf een enorme financiële en/of economische schade zou ondervinden bij de openbaarmaking van de opgevraagde documenten.

De beroepsinstantie kon immers zelf vaststellen dat alle opgevraagde documenten betrekking hebben op een beschrijving in detail van de cyberaanval die heeft plaatsgevonden binnen de administratie van de stad Antwerpen, de concrete schade die er werd geleden, de manier waarop de meest kritieke toepassingen terug online aan het werk konden worden gekregen, de genomen maatregelen om tegen te gaan dat dergelijke cyberaanvallen in de toekomst nogmaals zouden kunnen plaatsvinden en een beschrijving in detail van een nieuwe beveiligde cyberomgeving voor de stadsdiensten.

Al deze documenten bevatten gedetailleerde informatie aangaande mogelijke kwetsbaarheden in de informaticasystemen binnen de administratie van de stad Antwerpen, werkpunten ter verbetering van de beveiliging, te ondernemen investeringen en aan te pakken gevoeligheden inzake het informatieveiligheidsbeleid van de stad.

De beroepsinstantie is daarom ook van oordeel dat een eventuele kennisname van de informatie die voorkomt in de voormelde documenten met vermelding van gebreken en tekortkomingen inzake informatiebeveiliging, suggesties voor een betere cyberomgeving, door personen met mogelijks minder goede bedoelingen, de stad Antwerpen ontegensprekelijk zou kunnen bloot stellen aan een verhoogd risico inzake criminele activiteiten zoals phishing, hacking, installen van malware, virussen, spyware of ransomware, …. . Dit kan leiden tot verlies of onbeschikbaarheid van bedrijfsgevoelige data, financiële en/of commerciële schade, blootstelling aan afpersing, …. Doordat heel wat issues rond informatiebeveiliging in detail besproken worden in de opgevraagde documenten, zou de openbaarmaking ervan buitenstaanders (en mogelijke cybercriminelen) uiteraard heel wat informatie verschaffen over de kwetsbaarheden van de IT-systemen van de stad Antwerpen en de wijze waarop die uitgebuit kunnen worden. Het spreekt voor zich dat dit dient vermeden te worden, zoniet dreigt de stad Antwerpen mogelijks ernstige financiële en economische schade te lijden als de voormelde gevoelige informatie openbaar zou gemaakt worden.

De beroepsinstantie is om voormelde redenen dan ook overtuigd van het feit dat de opgevraagde documenten van economisch en financieel belang zijn voor de stad Antwerpen en daarom dienen afgeschermd te worden, meer specifiek om hen te beschermen tegen mogelijke cybercriminaliteit en de bijhorende financiële en economische schade die daardoor wordt veroorzaakt, in toepassing van artikel II.35, 1° van het Bestuursdecreet. De belangenafweging waartoe dit artikel, zoals elke relatieve uitzonderingsgrond, verplicht, leidt niet tot een oordeel in het voordeel van de verzoeker. De openbaarmaking ten koste van het beschermde belang mag enkel maar worden bevolen als daarmee het algemeen belang gediend wordt. De beroepsinstantie ziet geen argumenten om te besluiten dat dit hier het geval is. De betrokken te beschermen belangen van de stad Antwerpen wegen in casu zwaarder door dan het algemeen belang van de openbaarheid. Dit laatste belang dient, om in aanmerking te komen om te primeren op het belang van de financiële en economische belangen van de stad Antwerpen, het belang van de gemeenschap te betreffen: de openbare orde, de veiligheid van de bevolking, grote maatschappelijke issues, globale bescherming van het leefmilieu enzovoort. De beroepsinstantie is van oordeel dat dergelijke issues in dit concrete dossier niet aanwezig zijn. Integendeel zelfs, zoals hierna verder nog zal worden besproken, de openbare veiligheid vereist juist dat de informatie die voorkomt in de opgevraagde documenten moet worden afgeschermd. De individuele belangen van verzoekers doen aan het voorgaande geen afbreuk.

De beroepsinstantie wijst in bijkomende orde ook nog naar de toepassing van de uitzonderingsgrond die is voorzien in *artikel II.35, 6° van het Bestuursdecreet* om de openbaarmaking van de opgevraagde documenten te weigeren. Dit artikel bepaalt dat de overheidsinstanties, vermeld in artikel II.28, §1, een aanvraag tot openbaarmaking moeten afwijzen, indien ze van oordeel zijn dat het belang van de openbaarheid niet opweegt tegen de bescherming van de openbare orde en de veiligheid. Er moet telkens en in concreto geoordeeld worden of deze weigeringsgrond al dan niet van toepassing is.

De beroepsinstantie stelt in concreto vast dat alle door verzoeker opgevraagde documenten inderdaad heel wat gevoelige informatie bevat inzake de sterktes en kwetsbaarheden van de IT-infrastructuur en het IT-netwerk van de stad Antwerpen. De opgevraagde informatie heeft immers betrekking op de analyse van de cyberaanval, hoe deze is kunnen gebeuren, hoe deze werd aangepakt en hoe de stad Antwerpen haar systemen in de toekomst beter kan beveiligen. Dergelijke informatie zou zeer nuttig zijn voor hackers die in de toekomst nog eens een aanval op de IT-systemen van de stad Antwerpen willen organiseren. Met name de kennis over hoe de stad Antwerpen haar systemen heeft verbeterd, zou misbruikt kunnen worden om opnieuw een aanval op de IT-systemen van de stad Antwerpen (of andere overheden) te organiseren.

Een belangrijk aspect van de cyberveiligheid is immers dat derden er om te beginnen al geen of toch zo weinig mogelijk zicht op hebben hoe de beveiliging van de ICT-systemen is opgevat. Het vrijgeven van de informatie die voorkomt in de opgevraagde forensische rapporten, interne analyses of communicatie tussen de stad Antwerpen zou aldus een gevaar voor de openbare orde en veiligheid vormen, doordat cybercriminelen mogelijks langs die weg heel wat informatie kunnen verkrijgen over de kwetsbaarheden van de IT-systemen van de stad Antwerpen en de wijze waarop die uitgebuit of aangevallen kunnen worden.

De beroepsinstantie is van oordeel dat de openbaarmaking van deze gevoelige gegevens in de opgevraagde documenten de openbare orde en de veiligheid wel degelijk in het gedrang brengen. Het algemeen belang dat gediend is met de openbaarmaking van de opgevraagde documenten weegt niet zwaarder door dan het te beschermen belang, met name de openbare orde en veiligheid. De beroepsinstantie verwijst hiervoor naar de belangenafweging, zoals hiervoor uiteengezet.

Ook de uitzonderingsgrond van *artikel II. 33,3° Bestuursdecreet* is in casu van toepassing voor de door verzoeker opgevraagde documenten. Op basis van de voormelde uitzondering op het

openbaarheidsprincipe, mogen overheidsinstanties een aanvraag tot openbaarmaking van bestuursdocumenten afwijzen wanneer deze betrekking heeft op interne communicatie, tenzij het belang van de openbaarheid zou primeren:
“Tenzij het belang van de openbaarheid primeert, mogen de overheidsinstanties, vermeld in artikel II.28, § 1, een aanvraag afwijzen:
(…) 3° als de aanvraag betrekking heeft op interne communicatie.”

De Memorie van Toelichting bij artikel II.33, 3° van het Bestuursdecreet (Parl.St. Vl.Parl. 2020-21, nr. 780/1, 90-93) verduidelijkt dat deze uitzondering betrekking heeft op de interne uitwisseling van berichten, communicatie en mailwisseling tussen kabinetten en administratie, en administratie en kabinetten onderling. Daarenboven wordt in de parlementaire voorbereiding ook gesteld dat “Ook informatie die een overheidsinstantie van een externe bron heeft ontvangen, kan intern zijn “mits zij vóór de ontvangst ervan door deze instantie niet beschikbaar was of had moeten worden gesteld aan het publiek en zij niet buiten de muren van die instantie terechtkomt nadat zij deze informatie heeft ontvangen”. arrest HvJ EU 20 januari 2021, randnummer 43 – C-619/19)”

Bovendien zijn er bij toepassing van deze uitzonderingsgrond geen beperkingen wat de inhoud van “communicatie” betreft: het kan zowel gaan om persoonlijke beleidsopvattingen als feitelijke informatie of loutere data, zolang die informatie kadert in de voorbereiding van een beslissing of in het zoeken naar een oplossing van een specifiek probleem.

Het doel van deze uitzondering wordt als volgt beschreven in de Memorie van Toelichting:
“Een effectieve besluitvorming door de overheid veronderstelt dat voorstellen, ideeën of opvattingen over inhoudelijke, procesmatige, organisatorische of politieke aangelegenheden vrij kunnen uitgewisseld worden tussen personeelsleden van de overheid, en dat die uitwisseling ook schriftelijk kan zonder dat die voorstellen, ideeën of opvattingen op verzoek publiek moeten gemaakt worden. Een te rigide openbaarheidsregeling op dit punt heeft het ongewenste effect dat binnen de overheid niet meer vrijelijk van gedachten kan gewisseld worden over een dossier, beleidsproces, advies of ontwerpregelgeving. (…) Een zeker mate van ‘beleidsintimiteit’ en vertrouwelijkheid is noodzakelijk om te komen tot een effectieve besluitvorming. (…)
“Interne mededelingen bereiden een administratieve beslissing voor; een administratie moet de verschillende argumenten voor of tegen een beslissing over een specifiek probleem schriftelijk kunnen vastleggen, zonder dat deze interne beraadslagingen openbaar worden gemaakt. Het essentiële element is immers de administratieve beslissing en de eventuele rechtvaardiging daarvan, niet de manier waarop die beslissing tot stand is gekomen.””

De doelstelling van deze uitzonderingsgrond is om overheidsinstanties het recht te bieden hun interne raadplegingen en beraadslagingen en voorbereidingen te beschermen als dat noodzakelijk is om hun taken uit te voeren. Het begrip “intern” houdt in dat het gaat om informatie die niet buiten de muren van de overheidsinstantie terechtkomt, in het bijzonder wanneer zij niet is bekendgemaakt aan een derde of niet beschikbaar is gesteld aan het publiek.

Na onderzoek door de beroepsinstantie, kan, volgens het oordeel van de beroepsinstantie, voor wat betreft de door verzoeker opgevraagde documenten (forensische en technische rapporten i.v.m. cyberaanval en de communicatie tussen stad Antwerpen en CCB), inderdaad beroep worden gedaan op de uitzonderingsgrond zoals vermeld in artikel II.33, 3° Bestuursdecreet. De beroepsinstantie wenst hierbij te verwijzen naar de hierna aangehaalde overwegingen uit het arrest van het Europees Hof van Justitie d.d. 20 januari 2021 (ivm de interpretatie van het begrip “interne mededelingen”), waarnaar ook uitdrukkelijk wordt verwezen in de memorie van toelichting bij de voormelde bepaling in het Bestuursdecreet:

"Wat in de tweede plaats het woord „intern" betreft, volgt uit artikel 3, lid 1, van richtlijn 2003/4 van 28 januari 2003 inzake de toegang van het publiek tot milieu-informatie dat de overheidsinstanties beschikken over de milieu-informatie waartoe deze richtlijn beoogt toegang te verlenen. Overeenkomstig artikel 2, punt 3, van die richtlijn is dat het geval voor informatie die in het bezit is van een instantie en die zij heeft opgesteld of ontvangen. Met andere woorden, overheidsinstanties die in het bezit zijn van milieu-informatie, kunnen daarover beschikken, deze verwerken en intern analyseren en beslissen over de bekendmaking daarvan.
Hieruit volgt dat niet alle milieu-informatie waarover een overheidsinstantie beschikt noodzakelijkerwijs „intern" is. Dit is alleen het geval voor informatie die niet buiten de muren van een overheidsinstantie terechtkomt, in het bijzonder wanneer zij niet is bekendgemaakt aan een derde of niet beschikbaar is gesteld aan het publiek.
Indien een overheidsinstantie beschikt over milieu-informatie die zij van een externe bron heeft ontvangen, kan deze informatie ook „intern" zijn, mits zij vóór de ontvangst ervan door deze instantie niet beschikbaar was of had moeten worden gesteld aan het publiek en zij niet buiten de muren van die instantie terechtkomt nadat zij deze informatie heeft ontvangen.

Deze uitlegging van het woord „intern" wordt geschraagd door het doel dat wordt nagestreefd met de voor interne mededelingen gemaakte uitzondering op het recht van toegang tot milieu-informatie. In dit verband volgt uit de toelichting op artikel 4 van het op 29 juni 2000 ingediende voorstel van de Commissie voor een richtlijn van het Europees Parlement en de Raad inzake de toegang van het publiek tot milieu-informatie [COM(2000) 402 def. – 2000/0169(COD) (PB 2000, C 337 E, blz. 156)] dat de uitzondering op grond waarvan de toegang tot interne mededelingen kan worden geweigerd, net als de uitzondering voor nog onvoltooid materiaal of onvoltooide documenten, is bedoeld om tegemoet te komen aan de behoefte van de overheidsinstanties om te beschikken over een beschermde ruimte om intern te beraadslagen."

In casu gaat het om interne gevoelige informatie die kadert in de voorbereiding van beleidsbeslissingen die worden genomen rond maatregelen om toekomstige cyberaanvallen binnen de stad Antwerpen onmogelijk te maken.

De beroepsinstantie is van mening dat er in casu geen openbaar belang, zoals geduid in de parlementaire voorbereiding, gemoeid is met de openbaarmaking van de betrokken documenten (forensische en technische rapporten i.v.m. cyberaanval en de communicatie tussen stad Antwerpen en CCB). De memorie van toelichting stelt immers m.b.t. de belangenafweging het volgende: "De uitzonderingen worden alleen ingeroepen als het belang van de openbaarheid niet primeert. Daarmee wordt bedoeld: een met de openbaarmaking gediend openbaar belang. Deze bepaling betekent dus niet dat de private belangen van de aanvrager moeten afgewogen worden tegenover de belangen die met de uitzonderingen beschermd worden. Het gaat om het belang van de gemeenschap: de openbare orde, de veiligheid van de bevolking, grote maatschappelijke issues, globale bescherming van het leefmilieu enzovoort.." (Parl.St. Vl.Parl. 2017-18, 1656/1, 56). In voorliggend geval primeert het te beschermen belang boven het toch wel private belang van de beroeper.

Bijkomende uitzonderingsgrond voor het finaal onderzoeksrapport van 26 december 2022 door Orange Cyberdefense

De beroepsinstantie stelt vast dat hier gaat om een technisch onderzoeksrapport van een externe partner, Orange Cyberdefense, de deskundige cybersecurity afdeling van de Orange Group.

De beroepsinstantie is de mening toegedaan dat ook de uitzonderingsgrond van *artikel II.35, 3° Bestuursdecreet* van toepassing is op dit finaal onderzoeksrapport van 26 december 2022, opgesteld door Orange Cyberdefense.

Voormeld decreetartikel voorziet dat een bestuursinstantie een verzoek om openbaarheid dient af te wijzen als ze van oordeel is dat het belang van de openbaarheid niet opweegt tegen de bescherming van het vertrouwelijk karakter van commerciële en industriële informatie, wanneer deze informatie beschermd wordt om een gelegitimeerd economisch belang te vrijwaren, tenzij degene van wie de informatie afkomstig is met de openbaarheid instemt.

De uitzonderingsgrond in artikel II.35, 3° van het Bestuursdecreet beoogt de bescherming van de vertrouwelijke, aan een overheidsinstantie meegedeelde, commerciële en industriële gegevens, die als "ondernemingsgegevens" beschouwd kunnen worden, met inbegrip van handelsgeheimen. Als handelsgeheim wordt aanzien informatie die niet technisch van aard is, maar een commerciële waarde vertegenwoordigt zoals boekhoudkundige gegevens, lijsten van cliënteel en leveranciers, winstcijfers, omzet, stocks, enz. Er moet sprake zijn van een te vrijwaren economisch gelegitimeerd belang dat de overheidsinstantie tracht te beschermen en dat zwaarder doorweegt dan het belang van de openbaarmaking. Dit is volgens de Beroepsinstantie voorhanden wanneer er – ten gevolge van de openbaarmaking – een concurrentieel nadeel zou ontstaan in hoofde van de betrokken onderneming. Bovendien kan er rekening worden gehouden met de hoedanigheid van de verzoeker om het legitiem economisch belang correct te beoordelen.

Het forensisch onderzoeksrapport van Orange Cyberdefense bevat ontegensprekelijk commercieel waardevolle informatie, zoals de manier waarop er op de cyberaanval gereageerd is geweest, hoe de stad Antwerpen haar systemen terug operationeel heeft gekregen of zal krijgen in de toekomst en hoe de stad Antwerpen haar systeem in de toekomst beter zal beveiligen tegen mogelijke cyberaanvallen. Deze informatie kan zeer commercieel waardevol zijn voor concurrenten in de IT-sector, zoals in casu de aanvrager, om inzicht te krijgen in de manier waarop Orange Cyberdefense, een commerciële speler op de markt van cybersecurity, de stad Antwerpen heeft bijgestaan bij de aanval en welke strategieën zij hierbij hebben gehanteerd.

Het legitiem economisch belang van Orange Cyberdefense weegt daarenboven zwaarder door dan het algemeen belang van de openbaarheid. De aanvrager heeft bovendien al zelf aangegeven dat hij een technisch expert in cybersecurity is en zijn diensten commercieel aanbiedt. In casu gaat het hier om knowhow, eigen aan de betrokken firma. De vertrouwelijkheid van deze informatie moet beschermd worden om een gelegitimeerd economisch belang van de betrokken bedrijven in kwestie te vrijwaren, namelijk vermijden dat de commerciële knowhow van het betrokken bedrijf op het vlak van beveiliging van informaticasystemen en cybersecurity in handen zou kunnen komen van concurrerende bedrijven. De gegevens over de manier waarop Orange Cyberdefense met deze aanval is omgegaan, zou de aanvrager dan ook een aanzienlijk commercieel voordeel kunnen bieden voor toekomstige opdrachten.

De beroepsinstantie is in casu van oordeel dat de belangenafweging waartoe de artikel II.35, 3° van het Bestuursdecreet, zoals elke relatieve uitzonderingsgrond verplicht, niet tot een oordeel in het voordeel van verzoeker leidt. Er is geen openbaar belang, zoals geduid in de parlementaire voorbereiding bij het Bestuursdecreet, gemoeid met de openbaarmaking van de in casu opgevraagde documenten. De memorie van toelichting stelt immers m.b.t. de belangenafweging het volgende: "De uitzonderingen worden alleen ingeroepen als het belang van de openbaarheid niet primeert. Daarmee wordt bedoeld: een met de openbaarmaking gediend openbaar belang. Deze bepaling betekent dus niet dat de private belangen van de aanvrager moeten afgewogen worden tegenover de belangen die met de uitzonderingen beschermd worden. Het gaat om het belang van de gemeenschap: de openbare orde, de veiligheid van de bevolking, grote maatschappelijke issues, globale bescherming van het leefmilieu enzovoort …" (Parl.St. Vl.Parl. 2017-18, 1656/1, 56). In voorliggend geval dient de bescherming van de vertrouwelijke commerciële informatie van de

betrokken firma geacht te worden te primeren boven het algemeen belang dat met de openbaarmaking zou gediend zijn.

Artikel II.50 §1 Bestuursdecreet bepaalt dat als de aanvraag tot openbaarmaking wordt afgewezen op grond van artikel II.35, 3°, de beroepsinstantie contact opneemt met de betrokkene en vraagt of de aanvrager toestemming krijgt om alsnog toegang te krijgen tot de persoonsgegevens in het gevraagde bestuursdocument, als die toestemming nog niet is gevraagd door de betrokken overheidsinstantie. Uit het onderzoek door de beroepsinstantie is evenwel gebleken dat de betrokken firma heeft aangegeven dat ze niet wenste dat hun vertrouwelijke commerciële en industriële informatie openbaar zou worden gemaakt.

Bijkomende uitzonderingsgrond voor het Incident report d.d. 13 februari 2023, opgesteld door CERT en de communicatie tussen de stad Antwerpen en CCB

De beroepsinstantie is de mening toegedaan dat voor dit onderzoeksrapport van 13 februari 2023, opgesteld door CERT, alsook voor de opgevraagde communicatie tussen de stad Antwerpen en CCB (Centrum voor Cybersecurity België) ook *artikel II.39, tweede lid van het Bestuursdecreet* van toepassing is, waarin is bepaald dat de in het Bestuursdecreet bepaalde uitzonderingen gelden, onverminderd de andere bij de wet, het decreet of ordonnantie bepaalde uitzonderingen op de gronden die te maken hebben met de uitoefening van de bevoegdheden van de federale overheid, de gemeenschap of het gewest. In casu verwijst de beroepsinstantie naar de toepassing van *artikel 6, §2, 2° van de federale wet van 11 april 1994 inzake de openbaarheid van bestuur*.

Conform artikel 6, §2, 2° van de wet van 11 april 1994 betreffende de openbaarheid van bestuur wijst een federale of niet-federale administratieve overheid de vraag om inzage, uitleg of mededeling in afschrift van een bestuursdocument, die met toepassing van deze wet is gedaan, af wanneer de openbaarmaking van het bestuursdocument afbreuk doet aan een bij wet ingestelde geheimhoudingsverplichting.

De beroepsinstantie verwijst in dat verband naar de toepassing van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, artikel 20 van het koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen en artikel 9 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.

De CERT (het federale Cyber Emergency Response Team) is de operationele dienst van het Centrum voor Cybersecurity België (CCB) en heeft als opdracht het online opsporen, observeren en analyseren van veiligheidsproblemen en de verschillende doelgroepen hierover informeren. Het CERT en dus ook het CCB werden meteen op de hoogte gesteld van de grote cyberaanval die plaatsvond bij de stadsdiensten van de stad Antwerpen, aangezien het CCB is aangeduid als het nationale CSIRT (Computer Security Incident Response Teams), in de zin van de artikelen 60 tot 62 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.

Dit alles verklaart dat de rapporten van het CERT en de communicatie tussen de stad Antwerpen en de CCB vallen onder de toepassing van artikel 20 van het koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen: "*De documenten waarvan de overheid van oorsprong de verspreiding wil beperken tot de personen die bevoegd zijn om er kennis van te nemen, zonder aan deze beperking de juridische gevolgen te verbinden voorzien door de wet, worden gemerkt met de vermelding « Beperkte verspreiding »*.

Artikel 9, §2 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid stipuleert: "*De personeelsleden van de aanbieder van essentiële diensten, de digitale dienstverlener, of hun onderaannemers, zijn gebonden aan het beroepsgeheim wat de informatie over de uitvoering van deze wet betreft.*
Personen die uit hoofde van hun staat of beroep kennis dragen van geheimen die hun zijn toevertrouwd, mogen deze geheimen bekendmaken voor de uitvoering van deze wet." Deze wettelijke geheimhoudingsplicht is van toepassing op de CCB en het CERT in het bijzonder, die werd aangeduid als nationale CSIRT.

De beroepsinstantie kon zelf vaststellen dat bij het onderzoeksrapport van de CERT d.d. 13 februari 2023 heel uitdrukkelijk wordt verwezen naar de toepassing van voormeld artikel 20 van het KB van 24 maart 2000, met de vermelding "beperkte verspreiding". Deze vermelding houdt in dat de verspreiding van het document (het forensisch onderzoeksrapport in casu) beperkt is tot de personen die bevoegd zijn om er kennis van te nemen, zonder dat een classificatie (in de zin van de wet van 11 december 1998) relevant daarvoor is. In concreto betekent dit dus dat enkel bepaalde personen er toegang toe hebben, namelijk de houders van een veiligheidsmachtiging van minstens hetzelfde classificatieniveau als dat van de geclassificeerde informatie én voor zover ze de gegevens nodig hebben voor het uitvoeren van hun opdrachten. In casu zijn enkel de diensten van het CCB, de stad Antwerpen en Digipolis Antwerpen en de gerechtelijke instanties gerechtigd om kennis te nemen van dergelijke informatie met betrekking tot de cyberaanval bij de stadsdiensten van Antwerpen.

Het spreekt voor zich dat huidig verzoeker in dit beroepsdossier niet behoort tot de bevoegde personen in dit dossier in verband met de cyberaanval in Antwerpen, zodat de openbaarmaking van het onderzoeksrapport van 13 februari 2023, opgesteld door CERT, alsook de opgevraagde communicatie tussen de stad Antwerpen en CCB, moet geweigerd worden op basis van voormeld artikel 20 van voormeld KB van 24 maart 2000 en artikel 9 van voormelde wet van 7 april 2019, in combinatie met artikel 6, §2, 2° van de wet van 11 april 1994 betreffende de openbaarheid van bestuur. Door de openbaarmaking zou er immers afbreuk worden gedaan aan de wettelijke geheimhoudingsplicht, zoals voorgeschreven in artikel 20 van het KB van 24 maart 2000 en artikel 9 van de wet van 7 april 2019.

Het ingestelde beroep wordt om voormelde redenen (verwijzing naar alle hiervoor vermelde uitzonderingsgronden) dan ook als **ongegrond** beschouwd.

Na beraadslaging,

BESLUIT:

Het beroepschrift van [redacted] d.d. 7 april 2023 tegen de gedeeltelijke weigeringsbeslissing van de stad Antwerpen en AG Digipolis Antwerpen d.d. 17 maart 2023 wordt als ontvankelijk doch ongegrond beschouwd.

Brussel, 5 mei 2023

Voor de beroepsinstantie,
afdeling openbaarheid van bestuur,

Bruno ASSCHERICKX
Voorzitter