Jaarrapportage informatiebeveiliging 2022

Gemeente Zaanstad

www.zaanstad.nl

ZNSTD

Inhoudsopgave

1 Samenvatting

In dit jaarverslag legt het college van B&W van de gemeente Zaanstad verantwoording af over het gevoerde informatiebeveiligingsbeleid in 2022. Het geeft ook inzicht in de stand van zaken op de verschillende informatiebeveiligingsonderdelen.

De uitdaging zit tussen het vinden van balans tussen enerzijds het formaliseren van beleid en maatregelen en anderzijds te doen waar onze kracht zit. We steunen nu veel op de kennis van collega's en nemen we maatregelen die te vaak incident gestuurd zijn. (Dit kan zowel door incidenten bij onze eigen gemeente of cyberaanvallen of kwetsbaarheden die de pers halen).

Een ander belangrijk punt is dat informatiebeveiliging nog vaak wordt gezien wordt als een IT-zaak. Bijna al onze werkprocessen zijn afhankelijk van IT-infrastructuur en applicaties. IT mensen kunnen echter niet bepalen hoe belangrijk bepaalde bedrijfsprocessen zijn. Daarom ligt de verantwoordelijkheid voor informatiebeveiliging in de lijn. In de praktijk lijkt de lijn het toch vaak lastig te vinden om beslissingen te nemen over de eisen de aan IT-middelen gesteld moeten worden.

Wij verantwoorden ons grotendeels aan de hand van de Baseline Informatiebeveiliging Overheid (BIO). Vorige jaren besteedden wij veel aandacht aan de verplichte audits. Deze audits waren op deelgebieden. De sanctie op het niet voldoen aan de norm is afsluiting van de systemen zoals DigiD. Om continuïteit van de dienstverlening te borgen zijn in geval van dreigende afsluiting op kortetermijnmaatregelen nodig. Op 31 december 2022 voldeden we voor DigiD aan één norm niet. Dit is inmiddels opgelost.

Het vergde veel aandacht en capaciteit. Alle capaciteit die naar de verplichte audits gaat, konden wij niet stoppen in het controleren van de andere zelfevaluatielijsten. De BIO zegt iets over informatiebeveiliging over het geheel. Uit de BIO blijkt dat Zaanstad over het algemeen de basis voldoende op orde heeft.
In 2022 hebben we dit jaar wat meer tijd genomen om de zelfevaluatie in te vullen en zijn we meer bewijsstukken gaan zoeken of onze aannames klopte. Dit heeft geleid dat we op sommige gebieden iets slechter scoorden.

2 Inleiding

Om onze taken goed uit te kunnen voeren hebben wij veel gegevens nodig. Deze gegevens gaan vaak over onze inwoners en zijn vaak zeer vertrouwelijk.
Veel gemeentelijke processen kunnen niet plaatsvinden als onze gegevens, notities etc. niet beschikbaar zijn omdat een systeem niet werkt (door fouten in het netwerk, programmatuur, door hacks e.d.). De balies van burgerzaken kunnen niet functioneren, uitkeringen worden niet op tijd gestort. Ook onze democratische en bestuurlijke processen kunnen niet goed lopen. Zonder raadsinformatie kunnen we niet het normale besluitvormingsproces uitvoeren.
Als de gegevens gemanipuleerd of verminkt zijn, maken wij mogelijk verkeerde beslissingen.

De VNG en informatiebeveiligingsdienst hebben naar aanleiding van beveiligingsincidenten in de afgelopen jaren bij gemeenten op aangedrongen om de basis op orde te brengen. Maar zelfs met een goede basis is er geen garantie dat er geen cyberaanval plaatsvindt. Daarom moeten we ook hierop voorbereid zijn.
Daarom investeren wij al jaren in het verbeteren van onze informatiebeveiligingsmaatregelen. In cybersecurity moet de lat continue verhoogd worden. Beveiligingsmaatregelen die dit jaar voldoen, doen dat volgend jaar misschien niet meer. Het is soms net een race tegen de klok om up-to-date te blijven met beveiligingsmaatregelen.

Om te kijken in hoeverre wij de basis op orde hebben meten we ieder jaar of we voldoen aan de basisbeveiligingseisen volgens de Baseline Informatiebeveiliging Overheid (BIO).
Uit de BIO-score blijkt dat wij over het algemeen de basis voldoende op orde hebben.

In dit jaarverslag bekijken we eerst een aantal onderwerpen die rond informatiebeveiliging in 2022 speelden. Dit zijn onderwerpen die speciale aandacht kregen, of die in de BIO niet voorkomen.

Behalve verantwoording aan de gemeenteraad leggen wij ook verantwoording af aan toezichthouders over diverse stelsels. Hierbij vereisen de toezichthouders van DigiD en Suwinet een IT-auditrapport. De uitkomsten hiervan staan in Hoofdstuk 6.

3 IT-security investeringen voor cyberweerbaarheid

In 2022 hebben we extra geïnvesteerd in scanningtools. Hiermee scannen we wekelijks onze systemen op hun actuele basisbeveiliging en kwetsbaarheden. Regelmatig worden er nieuwe kwetsbaarheden ontdekt in IT-infrastructuur en in programmatuur. Een voorbeeld hiervan is de log4j kwetsbaarheid die wereldwijd eind 2021 bekend werd.
Door de kwetsbaarheden te scannen kunnen we maatregelen nemen om de kwetsbaarheden op te lossen. Zo houden we zowel de software als ons netwerk steeds up-to-date en passen het aan de nieuwste beveiligingseisen aan.

Verder hebben wij geïnvesteerd in tools die ons dataverkeer monitoren op actuele bedreigingen. Dit heet de Intrusion Detection Systems (IDS). IDS helpt ons sneller te ontdekken of er dreigingen van buitenaf komen, zoals van wereldwijde hosting providers. Ook kunnen we kwaadaardige software (malware) op ons netwerk beter en sneller ontdekken.
Het sneller ontdekken zorgt dat we aanvallen kunnen tegenhouden of eerder opsporen zodat we sneller acties kunnen uitzetten.

Verder willen wij beter voorbereid zijn als we toch zijn geraakt door een cyberaanval. We hebben daarvoor een aanbesteding uitgezet voor een partij die ons gaat ondersteunen met expertise en advies in werkelijke cyber crisissituaties, een zogenaamde cyber retainer/ incident response partij. Uit de aanbesteding kwam het bedrijf BDO naar voren. In 2023 houden we een initieel assessment met BDO en beginnen we de samenwerking op dit gebied.

4 Cybersecurity bij IOT-bruggen/ sluizen en rioolgemalen

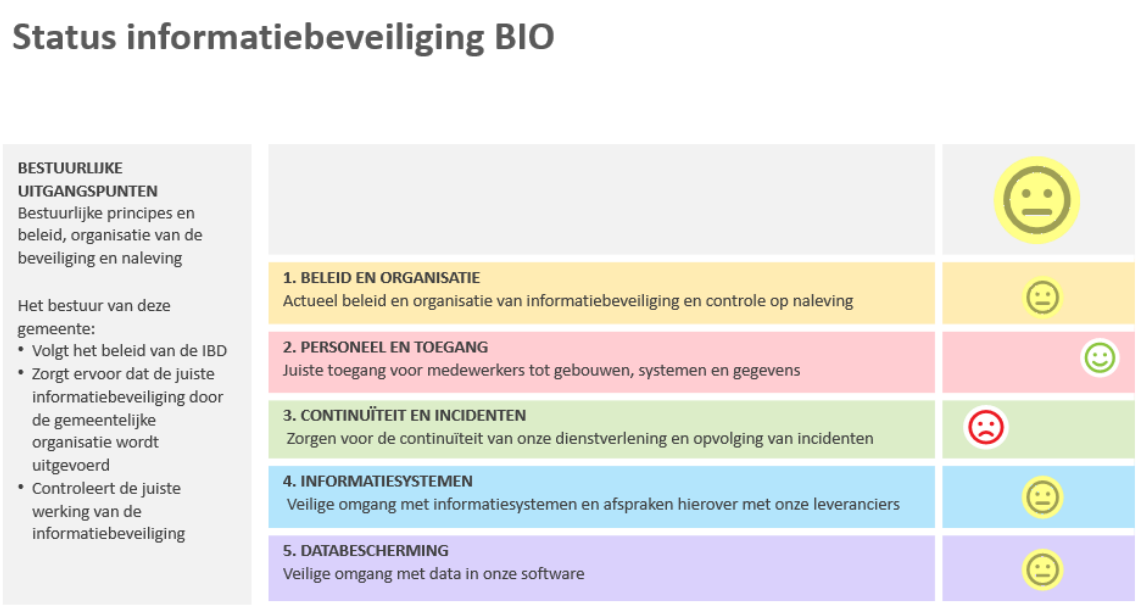
Door de beperkte capaciteit hebben de laatste loodjes van eerder opgestelde verbeterplannen (n.a.v. eerdere onderzoeken) niet de aandacht gekregen die ze zouden moeten hebben. Met name aan de menskant is er een gebrek aan capaciteit om zaken als bewustwording adequaat te kunnen uitvoeren. In 2023 zetten we een verbetercyclus (PDCA) op, zodat we bijhouden welke maatregelen nog moeten worden uitgezet en hoeveel capaciteit hiervoor nodig is.
Wel zijn er wederom hardware wijzigingen aangebracht om de toegang en beveiliging van het gesloten bedieningsnetwerk veiliger te maken.
Ook wordt er meer aandacht besteed aan de gebruikte camerasystemen n.a.v. de discussie over het gebruik van camera's van Chinese fabrikanten. Bij de brugbediening worden voornamelijk camera's van het merk Bosch gebruikt hoewel er ook nog een viertal camera's van een Chinese fabrikant wordt gebruikt. Deze zijn echter volledig afgesloten van toegang tot het Internet wat een eventueel risico op ongeautoriseerde toegang of data-exfiltratie uitsluit. De camera's zullen op termijn worden vervangen (waarschijnlijk eind 2023).

In 2022 zijn er wereldwijd kwetsbaarheden ontdekt in Siemens sturingsapparatuur (voor brugbediening, pompsystemen e.d.). Deze bevinden zich ook binnen Zaanstad maar deze apparaten zijn dermate geïsoleerd dat deze kwetsbaarheden geen directe bedreiging vormen. Ze staan op de nominatie om vervangen te worden en er is geen acuut risico. Daarom is het acceptabel om ze geïsoleerd in werking te houden. Onze leverancier houdt hierbij contact met Siemens wanneer er updates beschikbaar komen.

Om de cyberveiligheid in de openbare ruimte voor o.a. IOT-bedieningssystemen te kunnen waarborgen is het van belang dat er structureel aandacht voor komt. De CISO en informatiebeveiligers zullen in 2023 met de afdelingen bespreken wat dit betekent.
Gelet op de dreigingen die van buitenaf komen, de aanstaande wetgeving op dit gebied en de toenemende digitalisering in de buitenruimte is het noodzakelijk om cybersecurity daar net zo serieus te nemen als bij ICT/kantoorautomatisering. Momenteel doet een aantal medewerkers het 'erbij' omdat zij het belangrijk vinden (medewerkers van brugbediening, riolering en verkeerslichtinstallatie). Een structurelere aanpak is echter noodzakelijk.

5 Baseline Informatiebeveiliging Overheid (BIO)

5.1 Algemene score



Gemiddeld scoort Zaanstad volgens de BIO-classificatie op de hoofdonderdelen voldoende. We hebben basismaatregelen genomen en we bekijken deze ook regelmatig kritisch. Ondanks dat we een voldoende scoren, hebben we nog niet alle BIO-maatregelen volledig geïmplementeerd. Volgens de BIO moeten gemeente (en andere overheidsonderdelen) hun werkzaamheden en procedures vastleggen in beleid en richtlijnen. Alleen door het vastleggen borgen we de kennis en gaan we gestructureerder werken. Het blijkt dat we - net als vorig jaar – te weinig hebben vastgelegd. Daardoor steunen we nog te veel op kennis van ervaren medewerkers. Ondanks personeelsverloop zijn we in staat geweest om de systemen te laten draaien en de kennis over te dragen. Als we de stap nemen om procedures uit te schrijven zijn we minder afhankelijk van de kennis van ervaren medewerkers.

Uit het overzicht blijkt dat we onvoldoende scoren op continuïteit en incidenten. Dit ondanks dat we hier in 2022 de eerste stappen voor hebben gemaakt. Dit komt ten eerste doordat acties die we in 2022 hebben ingezet nog doorlopen in 2023. Maar ook omdat de lat steeds hoger komt te liggen. Het wereldwijde dreigingsbeeld wordt steeds ernstiger: hackers worden steeds slimmer en wij worden steeds afhankelijker van IT-middelen. In 2023 gaan we extra aandacht vragen om beter in te spelen op crisissituaties. Ook testen we onze bedrijfscontinuïteitsplannen en maken die waar ze nog ontbreken. Hierdoor zijn we beter voorbereid als we toch geraakt worden.

5.2 Beleid en organisatie

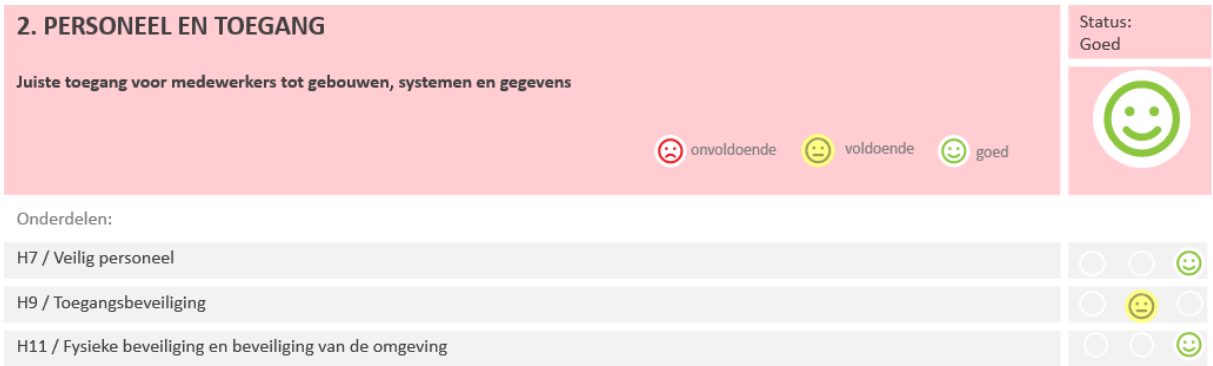
We voldoen aan (bijna) alle maatregelen die de BIO voorschrijft rond informatiebeveiliging. We hebben een Visie informatiebeveiliging en privacy met onderliggende beleidstukken over informatiebeveiliging en privacy. Deze stukken zijn geldig tot eind 2023.

De visie en beleidsstukken zijn abstract. Het informatiebeveiligingsbeleid geeft in de praktijk te weinig aanknopingspunten voor verder uitgewerkte richtlijnen. In een volgende versie van het informatiebeveiligingsbeleid willen we betere aanknopingspunten geven voor verdere uitwerking voor operationele richtlijnen. Een nieuwe visie en beleid staan eind 2023 ingepland.

We scoren voldoende voor organiseren van informatiebeveiliging. We kunnen hier nog verbeteren door meer te formaliseren. We moeten bijvoorbeeld beter vastleggen wie welke contacten heeft met welke instanties rond informatiebeveiliging. Hierdoor worden we minder kwetsbaar als medewerkers de organisatie verlaten.

In het hoofdstuk naleving scoren we minder goed op de gebieden van een duidelijke rapportagecyclus en een verbetercyclus. Hier willen we in 2023 een begin mee maken. Hiermee krijgen we een duidelijk beeld welke veranderingen we als eerst aan gaan pakken.

5.3 Personeel en toegang



In 2022 ging er een nieuwe gedragscode in. Alle medewerkers hebben deze thuisgestuurd gekregen. De gedragscode geeft invulling en uitleg aan de ambtseed. De gedragscode verwijst ook naar de geheimhouding van informatie.

In 2022 hebben we een eerste interne audit gehouden naar autorisatiebeheer. Hierbij bleek dat bedrijfsonderdelen niet altijd de periodieke controles houden of alle autorisaties nog kloppen.

Voor fysieke toegangsbeveiliging voldoen we aan alle maatregelen. We zien wel steeds meer gemeentelijke processen zich afspelen in openbare ruimtes, of ruimtes die met anderen worden gedeeld. In 2023 gaan we verder uitwerken welke informatiebeveiligingseisen we stellen aan de kantoorruimtes. Ook daar moeten we onze informatie veilig opbergen, zoals fysieke dossiers en open laptops.

5.4 Continuïteit en incidenten

Op het subonderdeel bedrijfscontinuïteit en informatiebeveiliging scoren we een onvoldoende.

In 2022 heeft de directie en een aantal managers een cybersecurity crisisgame gespeeld onder leiding van cyberexpert Brenno de Winter. Tijdens de cybercrisisgame ging het niet zozeer om de IT-activiteiten, maar om de gehele organisatie te laten ‘voelen’ dat cybersecurity de gehele organisatie aangaat. De rol van business leidinggevenden is hierin belangrijk. Hierin ligt een rol voor de directie en het business management.

De training was in maart 2022. Hier waren directieleden, (vertegenwoordigers van) het management en bestuurders aanwezig.

We hebben een eerste opzet van een actieplan dat de directie kan toepassen in het geval van een grote cybercrisis. Er is een eerste aanzet gemaakt voor een verdere uitwerking van de crisisorganisatie.

Behalve het opzetten van een crisisorganisatie is het ook belangrijk dat we bedrijfscontinuïteitsplannen hebben. Bedrijfscontinuïteitsplannen gaan in werking nadat de eerste tekenen van de crisis voorbij zijn. Hoe starten we de bedrijfsprocessen dan op? Welke processen moeten het eerst opgestart worden? Hebben we alternatieven voor de IT-systemen? Dit is iets wat de organisatie zelf moet bepalen en niet door de IT-afdeling gedaan kan worden. De ervaring leert dat bedrijfsonderdelen hierbij hulp en capaciteit nodig hebben.

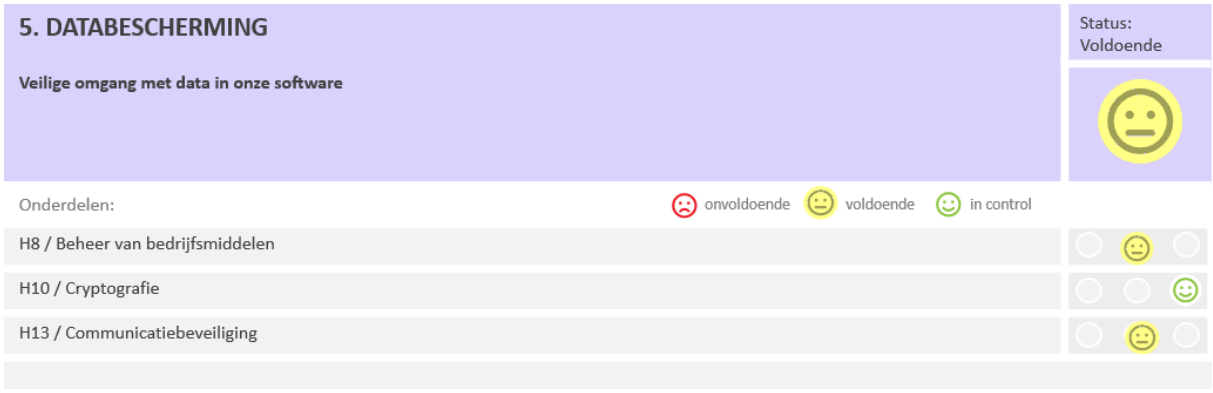
5.5 Informatiesystemen

Beveiliging van de bedrijfsvoering: we scoren nog geen goed omdat het ontbreekt aan het formaliseren en controleren (testen) van bestaande procedures. Zo hebben we veel maatregelen om onze back up bestanden te maken van onze netwerkschijven. We hebben echter niet vastgelegd hoeveel dataverlies we accepteren. Ook hebben we te weinig formele testen om te garanderen dat er geen virussen en malware op de back-ups staan. Hierdoor lopen we een risico dat als we te laat ontdekken dat we geraakt zijn dat we niet terug kunnen gaan naar oudere bestanden.

Leveranciersrelaties: we scoren hier nog onvoldoende op. Veel van onze data draait niet op onze eigen netwerkschijven maar staat bij leveranciers die ook de applicatie leveren.

We leggen wel in contracten vast dat we verantwoordingsinformatie willen, maar vragen deze alleen op voor auditverplichting. Een eerste stap hierin is dat we een 2023 een lijst met 5 kritische applicaties bepalen en hier rapportages voor opvragen (TPM of andere verklaring) en deze beoordelen.

5.6 Databescherming



We hebben diverse maatregelen om onze data te beschermen. We versleutelen belangrijke berichten en we beschermen zo ons netwerk. Volgens de BIO-normen moeten we echter een aantal van onze procedures uitschrijven. Hierdoor worden ze overdraagbaar aan andere medewerkers en maken we onze maatregelen aantoonbaar.

Dit gaat voornamelijk over informatie in applicaties en databases. Als het gaat om documenten op onze netwerkschijven zien we dat er veel zeer vertrouwelijke informatie staat. Hierover is niet altijd nagedacht of deze voldoende is afgeschermd.
Momenteel loopt er een project om documenten van de netwerkschijf over te zetten in een Microsoft 365 omgeving. Hierin gaan we documenten waarin zeer vertrouwelijke persoonsgegevens staan beveiligen.

6 Collegeverklaring ENSIA inzake informatiebeveiliging DigiD en Suwinet

Jaarlijks leggen wij verantwoording af aan de toezichthouders over de informatiebeveiliging van Suwinet en onze DigiD aansluitingen. Dit doen we via de ENSIA (Eenduidige Normatiek Single Information Audit) systematiek.
Wij verklaren per DigiD aansluiting of wij aan het normenkader voldoen en waar er eventuele afwijkingen zijn. Dit doen wij ook voor Suwinet. B&W tekent deze verklaring en een externe IT-auditor controleert de getrouwheid van de verklaring.

In 2022 voldeden we aan alle normen rond informatiebeveiliging van Suwinet en aan de meeste normen rond informatiebeveiliging van DigiD.

DigiD Burgerzaken: voldoet aan het normenkader.

DigiD Parkeren: voldoet aan het normenkader

DigiD Mijn Inkomen: voldoet aan het normenkader

DigiD Webformulieren: uit een pentest bleek nog één knelpunt. Hierdoor voldoen we niet volledig aan het DigiD normenkader voor deze aansluiting. Dit knelpunt is inmiddels al opgelost, maar wij moeten aan de toezichthouder de stand van 31-12-2022 doorgeven.

Suwinet: voldoet aan het normenkader.

7 Relatie met privacy

Een goede privacybescherming kan niet zonder informatiebeveiliging. De overlap is groot maar toch zijn er aparte aandachtspunten. Privacybescherming richt zich voornamelijk op de vertrouwelijkheid van *persoons*gegevens en is meer juridisch gericht. Informatiebeveiliging heeft meestal een technische en procedurele focus. Het richt zich op de beschikbaarheid, integriteit en vertrouwelijkheid van alle gegevens.

8 Meerjaren perspectief

In dit jaarverslag staat een terugblik op wat er in het jaar 2022 op informatiebeveiligingsgebied is gebeurd.

Een aantal acties hebben we in 2022 in gang gezet, maar lopen nog door in de komende jaren. Er komt nog een plan van aanpak over welke acties we de komende tijd uitzetten. Dit plan zal in de concerndirectie worden besproken. De concerndirectie houdt ook toezicht op de uitvoering van het plan.

Hieronder staat een opsomming van punten waarin we in het plan aandacht aan besteden. Dit plan is niet uitputtend. Waarschijnlijk is dit ook nog niet allemaal in één keer haalbaar en moeten we dit plan over meerdere jaren gefaseerd uitvoeren. Maar vooruitlopend op het plan is hier een doorkijk naar verbeterpunten.

Basis (blijvend) op orde:

- Eind 2023 moet er een nieuwe visie over privacy en informatiebeveiliging zijn. Hieronder komt een strategisch beleid (ook eind 2023).
- We zorgen voor een betere aansluiting tussen strategisch beleid en tactische en operationele richtlijnen.
- We organiseren een betere verbetercyclus. Onderdeel hiervan is de rapportagecyclus, waarin we de BIO-maatregelen als uitgangspunt nemen. We kijken risicogericht naar welke ontbrekende maatregelen we het eerst aanpakken.
- Ook houden we interne audits (op deelgebieden) om te toetsen of we de maatregelen daadwerkelijk hebben ingericht.
- We willen continue aandacht voor bewustwording. We komen met een plan voor een aanbesteding van een ‘nano-learning’; korte cyclus van informatiebeveiligingsvraagstukken.

Voorbereiden op crisis

- Uitwerking van de cyber crisis retainer
- Bewustwording van de business onderdelen van hun rol
- Plan maken hoe we omgaan met bedrijfscontinuïteit: hoe gaan we na een crisis weer de boel opstarten?

9 Restrisico

Het is belangrijk om te beseffen dat er geen garantie is dat Zaanstad gevrijwaard zal blijven van cybercriminaliteit. Het nemen van maatregelen kost investeringen in geld en in capaciteit.
Ook kunnen bepaalde beveiligingsmaatregelen het werk weer minder efficiënt maken.
Bij alle maatregelen die we nemen zullen we een balans moeten vinden tussen de werkbaarheid voor de organisatie en het risico dat we lopen.