Concept Jaarrapportage informatiebeveiliging 2023

Gemeente Zaanstad

www.zaanstad.nl

ZNSTD

Inhoudsopgave

1 Samenvatting

In dit jaarverslag beschrijft de CISO[1] van Zaanstad de stand van zaken rond informatiebeveiliging.

Zaanstad meet zichzelf ieder jaar aan de hand van de Baseline informatiebeveiliging overheid (BIO) Ook verantwoordt Zaanstad zich aan de toezichthouders. Voor de BIO scoort Zaanstad over het algemeen voldoende. Over de verantwoording aan de toezichthouders voldoet Zaanstad aan de eisen die de toezichthouders stellen.

Zaanstad wil de lat echter ieder jaar hoger leggen om bij te blijven aan de uitdagingen die de toename in afhankelijkheid ons stelt. Zo is er in 2023 veel geïnvesteerd in de informatiebeveiliging. Dit mede onder invloed van een toename aan cyberdreigingen en vooruitlopend op nieuwe wetgeving rond digitalisering en informatieveiligheid.
De opbrengst valt vooralsnog echter tegen. Daarvoor zijn verschillende oorzaken:

Zaanstad heeft in 2023 geïnvesteerd in de techniek. Zo is er geïnvesteerd in, cyberretainer voor ondersteuning bij aanvallen, ransomeware protectie, antivirus, firewalls, IDS, SIEM, (zie hoofdstuk 3) Hierdoor is er meer inzicht verkregen in de kwetsbaarheden en mogelijke aanvallen. Maar techniek alleen is niet voldoende.

In 2023 heeft Zaanstad daarom ook een onderzoek gedaan naar het beveiligingsbewustzijn van medewerkers. Ook zijn er korte elearnings aangeboden. Het beveiligingsbewustzijn van medewerkers is momenteel relatief laag. Uit een als test gestuurde phishing mail blijkt dat Zaanstad niet altijd adequaat reageert op een phishing mail. De scores van Zaanstad waren minder goed dan bij andere gemeenten. De organisatie maakt nu plannen hoe dit in 2024 verbeterd kan worden.

Een mogelijke verklaring voor het lage beveiligingsbewustzijn is de werkdruk. Als de werkdruk toeneemt, is de neiging om te concentreren op de primaire taken. Ondersteunende processen waar de primaire taken op draaien dreigen dan minder aandacht te krijgen.

Een ander punt waar Zaanstad niet goed scoort is bedrijfscontinuïteit. Het lijkt erop dat dit te informeel is geregeld. Binnen de organisatie weet men elkaar goed te vinden als er een cybercrisis dreigt, maar formeel is er nog weinig vastgelegd Hiermee is het onduidelijk welke processen als eerste moeten worden opgestart bij systeemuitval of andere calamiteiten. Het opstellen van bedrijfscontinuïteitsplannen en het regelmatig testen hiervan is noodzakelijk eventuele uitval zo kort mogelijk te houden.

Al met al is er een lichte verbetering van de informatiebeveiliging in 2023. Wel moet er in 2024 geïnvesteerd worden in bewustwording en bedrijfscontinuïteit. Zaanstad wordt steeds afhankelijker van digitalisering, hackers worden steeds slimmer en de eisen die toezichthouders aan gemeenten stellen worden steeds strenger.

[1] Chief information security officer

2 Inleiding

Om te kijken in hoeverre Zaanstad de basis op orde heeft houdt de CISO ieder jaar een zelfevaluatie waarin diverse organisatieonderdelen zichzelf beoordelen in hoeverre ze voldoen aan de basisbeveiligingseisen volgens de Baseline Informatiebeveiliging Overheid (BIO).
Uit de BIO-score blijkt dat Zaanstad de basis op orde heeft, maar dat er wel wat verbeterpunten zijn.

In dit jaarverslag staan eerst een aantal onderwerpen die rond informatiebeveiliging in 2023 speelden. Dit zijn onderwerpen die speciale aandacht kregen, of die in de BIO niet voorkomen.
Daarna gaat het jaarverslag in op de BIO scores die uit de zelfevaluatie bleken.

Behalve verantwoording aan de gemeenteraad legt Zaanstad ook verantwoording af aan toezichthouders over diverse stelsels. Zo vereisen de toezichthouders van DigiD (Logius namens het ministerie van Binnenlandse zaken) en Suwinet (BKWI namens het ministerie van Sociale Zaken & Werkgelegenheid) een IT-auditrapport. De uitkomsten hiervan staan in Hoofdstuk 6.
In hoofdstuk 7 staat een korte uitleg dat de toetsen op informatiebeveiliging helaas geen garantie geven, vanwege restrisico's en onvoorziene risico's.
In hoofdstuk 8 zijn de belangrijkste aanbevelingen voor de volledigheid nog een keer opgesomd.

3 IT-security investeringen voor cyberweerbaarheid

Door de scanningtools die Zaanstad in 2022 heeft aangeschaft zijn in 2023 meer kwetsbaarheden gevonden die konden worden opgelost, of waarvan de schadelijke gevolgen konden worden beperkt. Potentiële kwetsbaarheden die gemeld werden door de Informatiebeveiligingsdienst konden meteen worden gecheckt. Zo heeft de IT-organisatie in 2023 al een aantal keer tijdig actie kunnen nemen.

Verder is in 2023 geïnvesteerd o.a. in nieuwe firewalls met betere bescherming en ransomeware protectie: voor detecteren, blokkeren en onschadelijk maken van gijzelsoftware.

Dit boven op de IDS die al eerder inzicht geeft in ongewenst dataverkeer, antivirus scan in de VDI en VMware en de SIEM (security Incident management system)

Deze diverse tools en software houden het dataverkeer in de gaten, sporen kwetsbaarheden en kwaadaardige software (ransomeware) op, om deze vervolgens te blokkeren en verwijderen.

4 Cybersecurity bij IOT-bruggen/ sluizen en rioolgemalen

In het jaarverslag Informatiebeveiliging over 2022 stond dat eerder opgestelde verbeterplannen nog niet waren afgerond. Dat is nog steeds zo. Hierdoor is het nog niet mogelijk geweest om te starten met de verbetercyclus, zodat Zaanstad nog niet continue meet en verbetert.

In de zomer van 2023 heeft Siemens een update uitgebracht met betrekking tot kwetsbaarheden in de sturingsapparatuur (voor brugbediening, pompsystemen e.d.). Destijds concludeerde Zaanstad dat deze apparaten dermate geïsoleerd stonden dat deze kwetsbaarheden geen directe bedreiging vormen. Alle bruggen die groot onderhoud hadden in 2023 hebben de update gehad. Er zijn nog twee bruggen die staan ingepland voor het groot onderhoud. De laatste brug staat gepland in Q4 2024/Q1 2025. Dit is aanvaardbaar omdat het risico beperkt is.

Om de huidige staat van weerbaarheid vast te stellen komt er een onderzoek door een externe organisatie. Deze opdracht omvat niet alleen het vaststellen van de weerbaarheid, maar ook het bepalen van de benodigde kennis en waar deze moet worden geborgd.

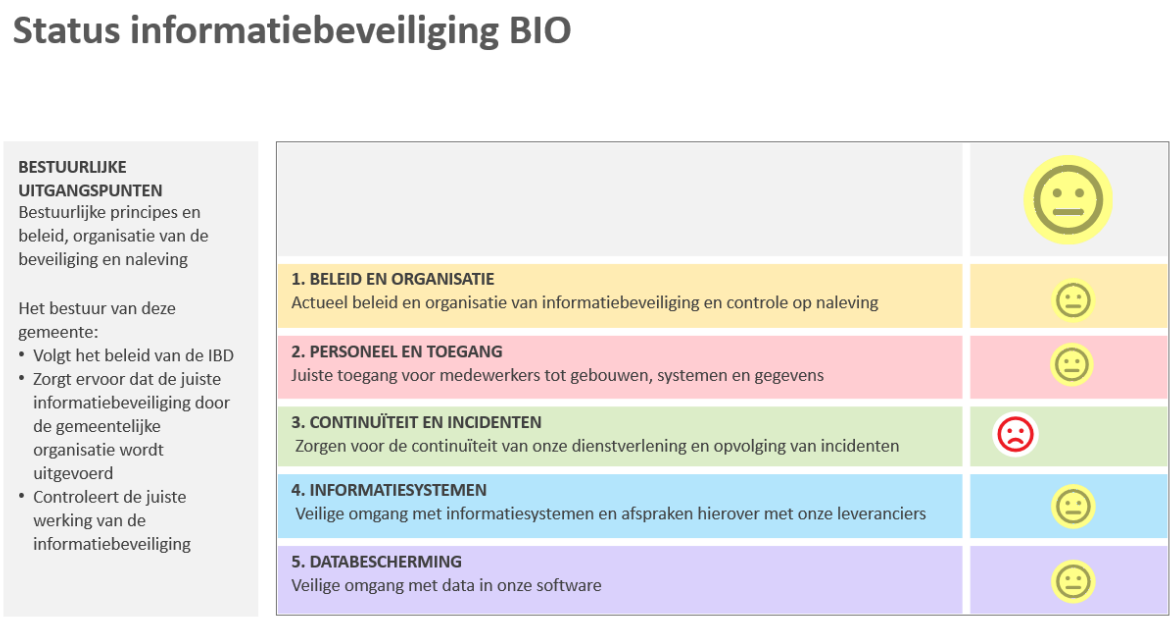
Momenteel wordt een opdracht uitgezet in de markt, gevolgd door de uitvoering van het onderzoek.

Het is noodzakelijk om cybersecurity in de buitenruimte (brugbediening, riolering en verkeerslichtinstallatie) net zo serieus te nemen als bij ICT/kantoorautomatisering. Momenteel is op dit gebied de gehele keten van ondersteunende en technische afdelingen (die verantwoordelijk voor de werking van bruggen, sluizen en rioolgemalen) onvoldoende goed georganiseerd om de hedendaagse uitdagingen het hoofd te bieden. Uit het onderzoek moet blijken hoe de verantwoordelijkheden het beste kunnen worden belegd.

5 Baseline Informatiebeveiliging Overheid (BIO)

In dit hoofdstuk staat waar Zaanstad staat ten opzichte van de Baseline informatiebeveiliging overheid (BIO). In paragraaf 5.1 staat het overall beeld en een samenvatting. Vervolgens worden in paragraaf 5.2 t/m 5.6 ingegaan in de onderliggende hoofdstukken uit de BIO. Daar waar nodig staan er vanaf 5.2 aanbevelingen waarop de organisatie kan verbeteren.

5.1 Algemene score



De scores van 2023 komen redelijk overeen met het jaar ervoor. Op de meeste onderdelen scoort Zaanstad voldoende. Er zijn veel acties ingezet, maar daar zijn in 2023 nog niet de vruchten van geplukt.

Zaanstad scoort in 2023 lager dan 2022 op het onderdeel personeel en toegang. Dit kwam voornamelijk door het onderdeel bewustwording en managementcommitment op bewustwordingsacties. Uit extern onderzoek blijkt dat Zaanstad slechter scoort dan andere gemeenten. Inmiddels is dit besproken in de organisatie.

Het onderdeel Continuïteit en Incidenten blijft een aandachtspunt. In 2023 is geïnvesteerd in een cyberretainer. Dat wil zeggen dat als Zaanstad wordt gehackt, er forensisch consultants van een extern bureau kunnen worden ingehuurd. Hiervoor heeft dit bureau een onderzoek gedaan. Hieruit kwamen een aantal (voornamelijk technische) aanbevelingen die momenteel worden doorgevoerd. Maar het grootste probleem blijft het ontbreken van bedrijfscontinuïteitsplannen. Bedrijfsonderdelen zijn druk met hun gewone werkzaamheden, en zien het maken van bedrijfscontinuïteitsplannen als een IT-aangelegenheid. De prioritering moet echter door de bedrijfsonderdelen zelf worden aangegeven.

Net als vorig jaar zijn er veel zaken wel geregeld, maar niet uitgeschreven in procedures. Dit maakt het aantoonbaar maken van waar Zaanstad staat lastiger. Ook geeft het risico's als de kennis alleen

in de hoofden van een aantal experts zit. Als die de organisatie verlaten dreigt Zaanstad de kennis te verliezen. Het formaliseren en uitschrijven van procedures borgt de kennis in de organisatie. Dit is ook belangrijk voor het voorbereiden op toekomstige wetgeving rond informatiebeveiliging.

5.2 Beleid en organisatie

Het informatiebeveiligingsbeleid is geldig t/m eind 2023. Dit betekent dat er in 2024 een nieuw beleid moet komen, maar dat voor 2023 Zaanstad een geldig beleid heeft.
Bij naleving scoort Zaanstad een voldoende en geen goed. Dit komt vooral door het ontbreken van een Information securitymanagement system (ISMS). Hierin kan Zaanstad, bijhouden waar Zaanstad staat.
Het gaat hier niet zozeer om een systeem maar om de methodiek van bijhouden wat de stand is, met name ten opzichte van de BIO.

Aanbeveling:
Begin met een ISMS-methodiek in te voeren. Een ISMS ondersteunt het management risicogerichte keuzes te maken ten aanzien van informatiebeveiliging. Op die manier kan de directie en het bestuur van Zaanstad beter sturen op risicogerichte verbeteringen. Hiermee is Zaanstad voorbereid op nieuwe wetgeving die dit verplicht stelt.

Wel is Zaanstad begonnen met een aantal interne audits uit de zelfevaluatie te houden. Het beleggen van de opvolging van de aanbevelingen is nog niet altijd gerealiseerd omdat tot op heden een duidelijke procesbeschrijving ontbreekt van de risico evaluatie.

Aanbeveling
Leg de aanbevelingen uit de interne audits vast en beleg deze bij een verantwoordelijke. Geef opvolging aan of deze aanbeveling is opgepakt.

5.3 Personeel en toegang

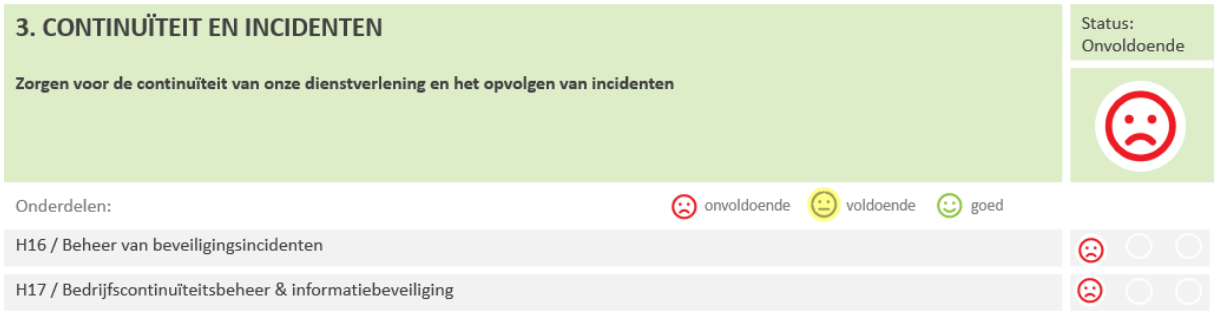
In 2023 heeft een extern bureau een onderzoek gehouden naar het beveiligingsbewustzijn van het personeel van Zaanstad. Ook zijn er korte e-learnings uitgerold en is er een phishing actie gehouden. Uit het onderzoek en uit de phishing actie bleek Zaanstad slechter te scoren dan andere gemeenten. Bij de phishing actie klikte helaas veel medewerkers op de link en deelden ook te veel medewerkers vrijwillig gevoelige gegevens.

Aanbeveling:
Zorg dat bewustwordingsprogramma's continue aandacht krijgen op alle niveaus in de organisatie. Betrek de leidinggevenden en benadruk het belang van de e-learnings en de lessen die hieruit volgen.

Bij (logische) toegangsbeveiliging zijn er wel zaken verbeterd, maar nog onvoldoende. Zaanstad werkt met een systeem waarbij medewerkers toegang krijgen op basis van een procesrol. Deze rol is gekoppeld aan de werkzaamheden.
Nog niet alle systemen zijn gekoppeld aan deze methodiek. Ook werkt deze methodiek alleen als leidinggevenden ook actief controleren of de rollen nog kloppen.
Bovendien is er een probleem met medewerkers die bij Zaanstad in een andere rol terecht komen (de doorstromers). De leidinggevende moet dan actief de oude rollen innemen, iets dat niet altijd goed gebeurt.

Aanbeveling:
Benadruk het belang bij leidinggevenden van de controles van de rollen, vooral bij doorstromers.

5.4 Continuïteit en incidenten



In 2023 heeft Zaanstad geïnvesteerd in een cyberretainer: er is een extern bedrijf ingehuurd dat ons bijstaat als er cyberincidenten zijn.
Het bedrijf dat Zaanstad kan bellen als er spraken is van een cyberaanval, heeft een onderzoek gedaan zodat dit bedrijf de sterktes en zwakheden van Zaanstad bekend zijn.
Zaanstad kreeg het advies om meer te trainen op het gebied van cyberincidenten.

Uit het externe onderzoek bleek dat de gemeente in staat is om op te reageren op cyber incidenten. Dit betrof echter met name op de technische scans.
De BIO kijkt meer of Zaanstad in opzet ook de juiste procedures hebben beschreven, en formeel hebben vastgelegd. Dit is nog niet overal het geval. Bij incidenten weten medewerkers elkaar te vinden. Het risico is echter dat als deze medewerkers met kennis de organisatie verlaten, dat nieuwe medewerkers deze kennis niet hebben.

Bedrijfscontinuïteit is van cruciaal belang voor het voortbestaan van een gemeente. Het is de verantwoordelijkheid van de directie om de visie, strategieën en middelen vast te stellen die nodig zijn om operationele verstoringen te minimaliseren en te beheren. Daarnaast is ook de betrokkenheid van de proceseigenaren essentieel, aangezien zij de operationele kennis en expertise hebben om de bedrijfsprocessen effectief te beheren en te waarborgen dat de bedrijfsdoelstellingen worden behaald, zelfs in onvoorziene omstandigheden.

Het externe onderzoeksbureau adviseert Zaanstad ook om bedrijfscontinuïteitsplannen te maken. Aangezien het lijnmanagement weet welke activiteiten niet stil kunnen liggen, is het belangrijk dat zij dit plan maken. Hiervoor is waarschijnlijk ondersteuning nodig.

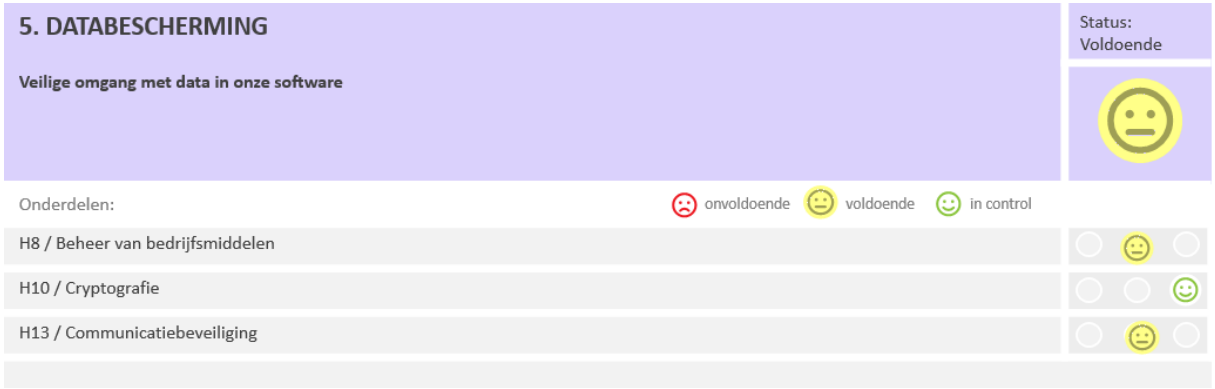
Het risico van het niet hebben van bedrijfscontinuïteitsplannen en het niet jaarlijks testen van deze plannen is dat Zaanstad niet goed acteert als er straks verstoringen zijn en Zaanstad opnieuw wil opstarten.

Aanbeveling
Zorg dat er een begin wordt gemaakt met bedrijfscontinuïteitsplannen. Kies hiervoor eerst twee of die bedrijfsonderdelen die hiermee beginnen.

5.5 Informatiesystemen

In 2023 heeft Zaanstad voortgang geboekt op het gebied van leveranciersmanagement. Met de meeste leveranciers zijn contracten afgesloten, inclusief verwerkersovereenkomsten. Daarin staan de verantwoordelijkheden beschreven.
Er wordt nog niet altijd verantwoordingsrapportages opgevraagd. Alleen als er een DigiD koppeling is kan een auditrapport worden afgedwongen.

5.6 Databescherming



In 2023 zijn er grote slagen gemaakt in de overgang naar M365. Als deze volledig is afgerond kunnen documenten (met vaak zeer vertrouwelijke persoonsgegevens) beter worden beveiligd.

De uitrol van M365 is begin 2024 compleet.

Eind 2023 heeft Zaanstad haar internetbeveiliging verbeterd. Zaanstad haalt nu een score van 100% op de site internet.nl[2]. Zaanstad heeft dus aantoonbaar alle aanbevolen beveiligingsprotocollen goed ingesteld.

[2]Het testtool internet.nl is een initiatief van het platform internetstandaarden. Het doel van het platform is om gezamenlijk het gebruik van moderne internetstandaarden verder te vergroten om daarmee het internet voor iedereen toegankelijker, veiliger en betrouwbaarder te maken. Het platform is een samenwerkingsverband van partijen uit de Internetgemeenschap en de Nederlandse overheid.

6 Collegeverklaring ENSIA inzake informatiebeveiliging DigiD en Suwinet

Jaarlijks leggen gemeenten verantwoording af aan de toezichthouders over de informatiebeveiliging van Suwinet en DigiD aansluitingen. Dit loopt via de ENSIA (Eenduidige Normatiek Single Information Audit) systematiek.
Het college van B&W verklaart per DigiD aansluiting of aan het normenkader wordt voldaan en waar er eventuele afwijkingen zijn. Hetzelfde geldt voor Suwinet. B&W tekent deze verklaring en een externe IT-auditor controleert de getrouwheid van de verklaring.

In 2023 voldeed Zaanstad aan alle normen rond informatiebeveiliging van Suwinet en aan alle normen rond informatiebeveiliging van DigiD.

Uit de BIO evaluatie blijkt dat Zaanstad voldoende punten haalt bij de Burgerzaken voor de basisregistratie personen (BRP) en reisdocumenten.

De ENSIA-vragenlijsten voor Belastingen zijn meer gericht op de juistheid van de gegevens. Hierbij scoort Zaanstad voldoende punten voor de basisregistratie adressen en gebouwen (BAG), basisregistratie grootschalige topografie (BGT) en de basisregistratie ondergrond (BRO).

7 Nota bene

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 Zaanstad neemt zal er een balans moeten worden gevonden tussen de werkbaarheid voor de organisatie en het risico dat Zaanstad loopt.
Dit is een grote uitdaging in de jaren waarbij Zaanstad kampt met een budgettekort.

8 Opsomming aanbevelingen

In de vorige hoofstukken staan regelmatig aanbevelingen die de organisatie kan oppakken. Hier staan ze nog een keer opgesomd. Met deze bevindingen maken we een start met de continue verbetercyclus.

Beleid en organisatie
Begin met een ISMS-methodiek in te voeren. Een ISMS ondersteunt het management risicogerichte keuzes te maken ten aanzien van informatiebeveiliging. Op die manier kan de directie en het bestuur van Zaanstad beter sturen op risicogerichte verbeteringen. Hiermee is Zaanstad voorbereid op nieuwe wetgeving die dit verplicht stelt.

Leg de aanbevelingen uit de interne audits vast en beleg deze bij een verantwoordelijke. Geef opvolging aan of deze aanbeveling is opgepakt.

Personeel en toegang
Zorg dat bewustwordingsprogramma's continue aandacht krijgen op alle niveaus in de organisatie. Betrek de leidinggevenden en benadruk het belang van de e-learnings en de lessen die hieruit volgen.

Benadruk het belang bij leidinggevenden van de controles van de rollen, vooral bij doorstromers.

Continuïteit en incidenten
Zorg dat er een begin wordt gemaakt met bedrijfscontinuïteitsplannen. Kies hiervoor eerst twee of die bedrijfsonderdelen die hiermee beginnen.