Volwassenheidsniveau 4, de route naar groei

Sectoraal hebben we de ambitie om de procesvolwassenheid voor informatieveiligheid en privacy op niveau 4 te brengen. Over dat niveau 4 is de afgelopen jaren veel gediscussieerd. Wat houdt “niveau 4” nu precies in? Een werkgroep met vertegenwoordiging uit CIW en CPW heeft zich eind vorig jaar gebogen over nadere uitwerking van dit volwassenheidsniveau. Deze uitwerking is eind 2022 gepresenteerd in de CBCF en daar omarmd als leidend voor onze sector.

In dit artikel wordt deze uitwerking verder toegelicht.

Waarom een ambitie voor volwassenheid?

In de verschillende onderliggende modellen voor procesvolwassenheid (CMMI, CIP) is een duidelijke rode draad te onderkennen. Een volwassen organisatie werkt risicogestuurd, beoordeelt haar eigen effectiviteit en stuurt bij waar nodig. Een volwassen organisatie is zich bewust van haar omgeving en stemt de privacy- en securitymaatregelen af op de doelen en de verwachtingen uit de omgeving. Hierdoor kan de organisatie haar middelen doelmatig inzetten.

Aan de hand van het door de werkgroep ontwikkelde model wordt hierna verder toegelicht hoe de organisatie hier invulling aan kan geven.

Startpunt voor de organisatie zijn altijd de doelen van de organisatie en de eisen die de omgeving aan haar stelt. Deze rechtvaardigen het bestaansrecht van de organisatie en geven richting aan de identificatie van de cruciale assets, data en andere kroonjuwelen.

De kroonjuwelen staan voor de essentiële objecten, gegevens en andere zaken die randvoorwaardelijk zijn voor de organisatie om de doelen te bereiken en te voldoen aan de verwachtingen van de omgeving. Door deze scherp in beeld te hebben, kan de organisatie haar

risicoanalyse en de maatregelen richten op de meest essentiële zaken. Zo worden hoofdzaken van bijzaken onderscheiden.

De organisatie heeft een beeld van de dreigingen in haar omgeving, die potentieel van invloed zijn op de doelen en de kroonjuwelen. Middels een risicoanalyse bepaalt de organisatie de kans dat een dreiging werkelijkheid wordt en de impact die dat heeft op de organisatie. In de risicoanalyse bepaalt de organisatie welke maatregelen prioriteit moeten krijgen om de risico's tot acceptabele proporties terug te brengen. Wat in deze context acceptabel is, is vastgelegd in de risicobereidheid van de organisatie. Niet alle risico's kunnen worden weggenomen, een zekere mate van risico moet geaccepteerd worden.

Let op, het gaat hierbij om het prioriteren van maatregelen. Welke maatregelen dat zijn ligt vast in onderliggende normen, zoals de BIO, de IEC 62443 en de AVG. Hulpmiddelen in de vorm van richtlijnen (CSIR, CIP Privacy Baseline) geven richting aan de implementatie. Uitgangspunt is dat de organisatie alle maatregelen uit de normen implementeert. Alleen als de risicoanalyse uitwijst dat een maatregel onnodig is, kan deze achterwege worden gelaten. De organisatie verantwoordt deze keuzes in de Verklaring van toepasselijkheid.

Bovengenoemde stappen, de bovenste cirkel van het volwassenheidmodel, vormt eigenlijk de uitwerking van de PLAN-fase uit de klassieke PDCA-cyclus. Op basis van de voorgaande stappen weet de organisatie welke maatregelen prioriteit moeten krijgen. Voor deze geprioriteerde maatregelen richt de organisatie de PDCA-cyclus in. Andere, niet-geprioriteerde maatregelen worden ook geïmplementeerd maar hiervoor richt de organisatie geen pdca-cyclus in.

DO: De organisatie implementeert de maatregelen en draagt zorg voor actief beheer van deze maatregelen. Een maatregel heeft een eigenaar die verantwoordelijk is voor het effectief functioneren ervan.

CHECK: De organisatie onderzoekt met regelmaat de effectiviteit van de maatregelen. Bijvoorbeeld door testen, oefeningen en audits beoordeelt de organisatie het functioneren van de maatregelen, in absolute zin en ten opzichte van vergelijkbare organisaties. Kritieke performance indicatoren (KPI's) zijn hierbij een nuttig hulpmiddel. Deze onderzoeken leveren input voor verdere verbetering van de effectiviteit.

ACT: Aan de hand van de onderzoeken implementeert de organisatie de verbeteringen die zijn onderkend in audits, testen en oefeningen.

Indicatoren voor een volwassen organisatie

Volwassenheidsniveau 4 vertaalt zich in een aantal concrete indicatoren. Deze criteria zijn toetsbaar en kunnen een leidraad vormen bij een audit op volwassenheid.

De organisatie:

- heeft inzichtelijk wat haar doelen zijn en de eisen die de omgeving aan haar stelt
- heeft bepaald welke kroonjuwelen essentieel zijn voor het bereiken van de doelen (objectclassificatie, dataclassificatie, processclassificatie, gevoeligheid van persoonsgegevens)
- heeft een actueel dreigingsbeeld dat als input wordt gebruikt voor de risicoanalyse
- heeft haar risicobereidheid vastgesteld
- heeft middels een risicoanalyse de kans en impact van de risico's vastgesteld, maatregelen geprioriteerd en de restrisico's geaccepteerd

- Heeft in beginsel alle maatregelen uit de relevante baselines (BIO, AVG, IEC62443) geïmplementeerd:
    - Verantwoording van keuzes (comply-or-explain) gebaseerd op de risicoanalyse, vastgelegd in de Verklaring van toepasselijkheid
- Bepaalt voor de geprioriteerde maatregelen periodiek de effectiviteit, ondermeer aan de hand van (sectorale) kpi's
- Vergelijkt de eigen performance op deze maatregelen met de prestaties van de andere waterschappen en eventueel vergelijkbare organisaties
- Beoordeelt derden (w.o. leveranciers, partners, samenwerkingsverbanden) op de effectiviteit van maatregelen, voor zover maatregelen door derden worden uitgevoerd
- Verbetert voortdurend de effectiviteit van de maatregelen om de PDCA-cyclus te sluiten
- De organisatie doorloopt aantoonbaar en periodiek alle bovengenoemde stappen (werking)

Daarnaast vertaalt het volwassenheidsniveau zich in handelen door de verschillende rollen in de organisatie.

De bestuurder:

- Is zich bewust van het dreigingsbeeld en de potentiële impact op de maatschappelijke opgave van de organisatie, borgt de beschikbaarheid van de benodigde middelen, overtuigt zich van de effectiviteit en geeft een in-controlverklaring af

De directie:

- Toont eigenaarschap van de risico's en de verklaring van toepasselijkheid, ziet toe op het behalen van het beoogde volwassenheidsniveau

Het lijnmanagement:

- Toont eigenaarschap van de maatregelen en ziet toe op uitvoering, meet de effectiviteit en stuurt bij waar nodig

De operatie:

- Voert maatregelen uit, draagt actief bij aan het verbeteren van de effectiviteit en is alert op veiligheids- en privacy-issues

De ISO's, OSO's, privacy officers:

- Adviseren, faciliteren, voeren ondersteunende ib- en privacytaken uit, maar zijn nadrukkelijk geen eigenaar van maatregelen

De FG, CISO:

- Is onafhankelijk, zonder operationele betrokkenheid of verantwoordelijkheid
- Adviseert over de juiste toepassing van de baselines en organisatie-inrichting
- Helpt de organisatie bij het maken van afgewogen strategische keuzes
- Controleert de werking van de risicoanalyse en de pdca-cyclus en adviseert over verbeteringen
- Heeft een directe lijn naar de bestuurder

Concerncontrol:

- Neemt de thema's mee in de integrale planning- en controlcyclus van de organisatie
- Benoemt de thema's in audits en onderzoeken

Een volwassen organisatie kenmerkt zich verder door een bestuur dat het maatschappelijk belang van de thema's onderkent en vertaalt naar een opdracht voor de organisatie. Een directie die het belang van informatieveiligheid en privacy in houding en gedrag stimuleert. Management dat in-control is op deze thema's en stuurt op kwaliteitsmeting en verbetering. Op de thema's competente medewerkers in de processen. Een IB- en privacy-organisatie die als facilitator op deze thema's fungeert en een onafhankelijk gepositioneerde en acterende FG en CISO. Informatieveiligheid en privacybescherming zijn onderdeel van de cultuur en de werking van de organisatie.

De uitwerking van volwassenheid is hierboven vertaald naar de thema's informatieveiligheid en privacy. Het volwassenheidsmodel is echter breed toepasbaar als kader voor kwaliteitsdenken. Het helpt als dit kwaliteitsdenken niet enkel op deze thema's wordt toegepast. Werk aan organisatiebreed kwaliteitsmanagement dat het proces van risicomanagement en de PDCA-cyclus ondersteunt.