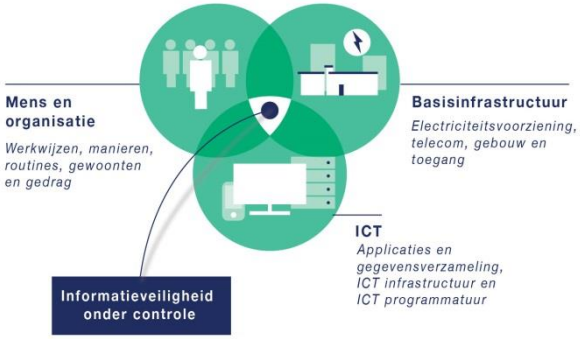
Informatieveiligheid

Provincie Utrecht

Provincies zijn voor de uitvoering van hun taken steeds meer afhankelijk van informatiesystemen en informatiestromen. De veiligheid van informatie neemt dan ook een steeds belangrijker positie in. Informatieveiligheid houdt in dat informatie alleen door de juiste personen is te zien en te gebruiken. Ook dient informatie volledig, juist, actueel en op het juiste moment toegankelijk te zijn. Om informatieveiligheid te waarborgen, kunnen maatregelen worden genomen op de aandachtsgebieden Mens & Organisatie, ICT en basisinfrastructuur (zie afbeelding). Door deze maatregelen kunnen organisaties risico's voor informatieveiligheid tot een acceptabel niveau terugbrengen.



Met de ondertekening van het Convenant Interprovinciale Regulering Informatieveiligheid eind 2014 hebben de provincies kenbaar gemaakt de informatieveiligheid verder te willen optimaliseren en professionaliseren. De Randstedelijke Rekenkamer heeft onderzocht hoe de provincies zijn gevorderd met de borging van de informatieveiligheid.

Vraagstelling

Heeft de provincie Utrecht de informatieveiligheid voldoende geborgd?

De centrale onderzoeksvraag is beantwoord aan de hand van de volgende vier deelvragen:

1. Heeft de provincie de sturing op en de verantwoordelijkheid voor informatieveiligheid goed verankerd?
2. Is het informatieveiligheidsbeleid in opzet, uitvoering én in resultaat adequaat?
3. Heeft de provincie voldoende aandacht voor bewustwording op het gebied van informatieveiligheid?
4. Heeft de provincie het afleggen van verantwoording over en het houden van toezicht op informatieveiligheid goed geregeld?

Conclusies

Tot eind 2015 is er ondanks verschillende kritische signalen te weinig gestuurd op de realisatie van acties om de informatieveiligheid te verbeteren. Het gaat dan onder meer om een goede verdeling van verantwoordelijkheden en het vergroten van het bewustzijn voor informatieveiligheid. Hierdoor is weinig tot geen voortgang geboekt bij zaken die belangrijk zijn voor informatieveiligheid, zoals de uitvoering van risicoanalyses. Sinds eind 2015 is de provincie actiever in de verbetering van informatieveiligheid. De eerste stappen bij de invulling van rollen en verantwoordelijkheden zijn gezet. Er komt ook nieuw informatieveiligheidsbeleid, waaraan voor het eerst ook een plan van aanpak wordt gekoppeld.

De hoofdconclusie is gebaseerd op de volgende vier deelconclusies:

1. Tot eind 2015 is er te weinig gestuurd op informatieveiligheid. Op verschillende zaken die belangrijk zijn voor de verbetering van de informatieveiligheid, is weinig tot geen voortgang geboekt. Zo was de verdeling van verantwoordelijkheden voor informatieveiligheid lange tijd alleen op papier goed uitgewerkt. Vanaf eind 2015 heeft de provincie de eerste stappen gezet om meer sturing te geven op informatieveiligheid. Er is een begin gemaakt met de toedeling van verantwoordelijkheden. Verder zijn de vaststelling van nieuw informatieveiligheidsbeleid en een bijbehorend plan van aanpak voorzien in juni 2016.
2. Het in 2015 opgestelde informatieveiligheidsbeleid van de provincie voldoet in opzet aan de eisen. Dit beleid wordt echter niet uitgevoerd, omdat de provincie van plan is om in juni 2016 een geactualiseerde versie van het informatieveiligheidsbeleid, met daaraan gekoppeld een plan van aanpak, vast te stellen. Het is niet goed te beoordelen of de provincie de benodigde informatieveiligheidsmaatregelen uitvoert, want een systeem dat hier inzicht in moet geven, is nog niet goed geïmplementeerd. Om te beoordelen of de informatie van de provincie voldoende beschermd is, is een test uitgevoerd. Daarbij is een aantal kwetsbaarheden met een hoog, maar niet direct kritiek risico ontdekt. Ook is geconstateerd dat de provincie onvoldoende monitort of er indicaties zijn voor ongeoorloofde toegang tot provinciale systemen. Op basis van de test kan overigens geen algemene uitspraak worden gedaan.
3. De provincie heeft tot eind 2015 nog onvoldoende aandacht gehad voor de bewustwording van het belang van informatieveiligheid; er is slechts een beperkt aantal acties ondernomen om dit bewustzijn te vergroten. De provincie heeft wel in 2015 een mystery guest-onderzoek laten uitvoeren om het bewustzijn van informatieveiligheid te meten. Uit dit onderzoek en uit verschillende andere onderzoeken blijkt dat het bewustzijn van informatieveiligheid in de organisatie nog duidelijk verbeterd kan worden. Het vergroten van het bewustzijn in de provinciale organisatie van het belang van informatieveiligheid is een speerpunt van het plan van aanpak, dat in juni 2016 vastgesteld moet worden.
4. De provincie had het houden van toezicht op informatieveiligheid tot medio 2015 nog niet voldoende geregeld. Er zijn diverse onafhankelijke onderzoeken uitgevoerd naar de stand van zaken van informatieveiligheid. Echter, slechts de onderzoeken vanaf medio 2015 leidden tot vervolgacties. Het afleggen van verantwoording over informatieveiligheid in de provincie is nog niet voldoende geregeld. Informatieveiligheid maakt nog geen deel uit van de P&C-cyclus. Er is wel een jaarlijkse zelfevaluatie over informatieveiligheid uitgevoerd, maar die wordt niet gebruikt voor verantwoording of sturing.

Aanbevelingen

1. Vraag GS om te bewaken dat het plan van aanpak informatieveiligheid goed en voortvarend wordt uitgevoerd.
2. Spreek met GS af hoe u wordt geïnformeerd over de voortgang en resultaten bij het verbeteren van de informatieveiligheid.

Meer informatie

Dit onderzoek heeft geresulteerd in het rapport Informatieveiligheid en vindt u op onze website www.randstedelijke-rekenkamer.nl. Voor meer informatie kunt u zich wenden tot Ans Hoenderdos, info@randstedelijke-rekenkamer.nl tel. 020 58 18 585.