

AANBEVELINGEN

De Onderzoeksraad komt tot de volgende aanbevelingen.

Aan de minister van Binnenlandse Zaken en Koninkrijksrelaties

1. Zorg dat bestuurders van alle overheidsorganisaties hun verantwoordelijkheid nemen voor het beheersen van digitale veiligheid.

Daartoe moet u een programma ontwikkelen dat bestuurders van overheidsorganisaties doordringt van het belang van digitale veiligheid, en hen voorziet van voldoende inzicht en vaardigheden om hen in staat te stellen actief sturing te geven aan de beheersing van digitale veiligheid in hun organisatie.

Ook moet u overheidsorganisaties verplichten om zich te verantwoorden over de wijze waarop zij digitale veiligheid waarborgen. Veranker daartoe een duidelijk omschreven openbare verantwoordingsplicht op het gebied van digitale veiligheid in de planning & controlcyclus van overheidsorganisaties, en laat bestuurders van overheidsorganisaties jaarlijks een 'in control statement' voor digitale veiligheid afgeven.

Aan de minister van Binnenlandse Zaken en Koninkrijksrelaties; aan de minister van Veiligheid en Justitie

2. Schep voorwaarden zodat overheidsorganisaties hun digitale veiligheid systematisch beheersen.

Hiertoe moet u ervoor zorgen dat alle overheidsorganisaties de open standaarden NEN-ISO/IEC 27001 en 27002 naleven, die gezamenlijk een kader voor systematische digitale veiligheidszorg bieden. Stel daarvoor een plan op waarin concrete doelen, maatregelen en een tijdsplan worden benoemd. Wijs bovendien een organisatie aan die overheidsorganisaties kan begeleiden bij het tot stand brengen van adequate digitale veiligheidszorg.

Als onderdeel van een dergelijke systematische aanpak moet vanuit gemeenten, veiligheidsregio's en het Rijk aandacht bestaan voor het voorbereid zijn op, en het herstellen van schade als gevolg van, digitale incidenten. Burgers en bedrijven wier gegevens door een digitaal veiligheidsincident zijn getroffen, moeten kunnen volstaan met dit één keer te melden waarna adequate maatregelen moeten worden getroffen door alle betrokken overheidsorganisaties.

Aan de minister van Binnenlandse Zaken en Koninkrijksrelaties; aan de minister van Economische Zaken, Landbouw en Innovatie

3. Realiseer een veiliger uitgifte en gebruik van digitale certificaten.

Pas hiervoor de rol van OPTA en Logius zodanig aan, dat sprake is van werkelijk toezicht op en handhaving van de feitelijke naleving door certificaatdienstverleners van de vigerende regelgeving ten aanzien van gekwalificeerde en PKI-overheid-certificaten.

Bevorder daarnaast een cultuuromslag bij alle partijen die bij certificaatdienstverlening betrokken zijn, in het bijzonder ten aanzien van het melden en leren van incidenten. Maak daarbij gebruik van ervaringen met veilig melden uit andere sectoren.

Bestuursorganen aan wie een aanbeveling is gericht dienen een standpunt ten aanzien van de opvolging van deze aanbeveling binnen een half jaar na verschijning van deze rapportage aan de betrokken minister kenbaar te maken. Niet-bestuursorganen of personen aan wie een aanbeveling is gericht dienen hun standpunt ten aanzien van de opvolging van de aanbeveling binnen een jaar kenbaar te maken aan de betrokken minister. Een afschrift van deze reactie dient gelijktijdig aan de voorzitter van de Onderzoeksraad voor Veiligheid en de minister van Veiligheid en Justitie verstuurd te worden.