



Uitdagingen Chief Information Security Officer

Informatie veiligheid is een groeiend thema en wordt omvangrijker.

Elke organisatie wil een defensief beleid voeren daardoor zal de CISO een belangrijke rol binnen organisaties krijgen.

Context

De afgelopen paar jaar zijn gesloten ICT netwerken ontwikkeld tot internet communities. Dit betekent dat gebruikers kansen en mogelijkheden krijgen om in verschillende informatieomgevingen te werken. Deze kansen en mogelijkheden adresseren een aantal fundamentele vragen die samenhangen met de verdergaande digitalisering binnen de overheid en de vragen en dilemma's die uit deze niet te stoppen ontwikkeling voortvloeien. Vragen en dilemma's waar veel organisaties mee worstelen. In de managementreactie op het OneDrive rapport wordt hier meer inhoudelijk op ingegaan. In ieder geval is de conclusie dat informatieveiligheid een relatief nieuw en in belang groeiend thema is, waar ten tijde van het HEC-rapport nog geen rekening mee is gehouden.

Aanpak

- **Dataclassificatie.** Dit betekent implementeren, registreren en onderhouden van data en gegevens classificatie.
- **Cloudbeleid** formuleren. Dit betekent het opstellen van kaders voor het gebruik van Cloud toepassingen. Hierbij is dataclassificatie een belangrijk element.
- **Identitymanagement.** Dit is het implementeren, registreren en onderhouden van afspraken wie gemachtigd is om gegevens te benaderen en verwerken. Hierbij is privacy een belangrijk aspect.
- **Innovatie** vraagt aandacht voor data (classificatie). Ontwikkelingen als ketensamenwerking, social media communicatie vragen om het classificeren van data en informatie. "Wat mag wel en wat kan niet".
- **Awareness** bij de medewerkers. Doordat medewerkers met de e-werkplek werken en doordat we stimuleren om samen te werken is bewustzijn belangrijk. Dit betekent dat we medewerkers kaders en spelregels moeten meegeven in deze ontwikkeling. Dit betekent overigens ook dat medewerkers aangesproken worden op hun verantwoordelijkheid.