Q.C.N. Services B.V.
Kantoor Capelle aan den IJssel: Maindal 10 ; 2904 CS Capelle a/d IJssel ; Tel. 010 - 28.40.940 ; www.qcn.nl

Kleine handreikingen voor een FG en dingen om over na te denken

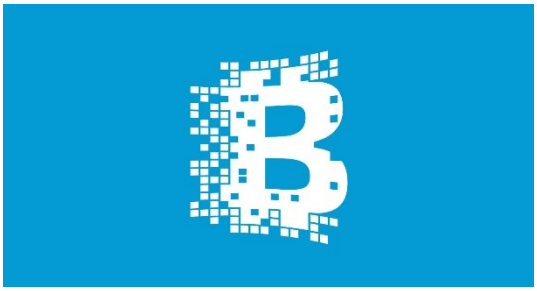
Hoe onafhankelijk dient een FG te zijn?

De FG dient in alle onafhankelijkheid zijn werkzaamheden te kunnen uitvoeren en ontvangt daarbij geen instructies vanuit de gemeente en verwerkers[1], Wel rapporteert de FG rechtstreeks aan het college van B&W over zijn werkzaamheden. Er is overleg mogelijk met de AP, maar er is geen meldingsplicht bij de AP voor onregelmatigheden. Er dient te worden voorkomen dat de FG in een spagaat terecht komt als de FG zich (teveel) met uitvoerende taken bezig houdt. De FG controleert dan in feite zijn eigen uitvoerende werkzaamheden. Deze situatie kan zich ook voordoen bij de adviserende rol van de FG. Een dergelijke spagaat zou de geloofwaardigheid en betrouwbaarheid van de functie en de functionaris niet ten goede komen.

De relatie blockchain / AVG

De AVG moest de diverse Europese privacywetgeving niet alleen harmoniseren maar bovenal moderniseren. Met als doel een versterkte bescherming van persoonsgegevens. Maar steeds meer bekruipt ons het gevoel dat deze nieuwe wet achter technologische ontwikkelingen zoals blockchain aanloopt en daardoor reeds bij invoering verouderd is.

Wie denkt aan blockchain ziet vaak een eindeloze reeks technische mogelijkheden om bestaande processen ingrijpend te wijzigen en te moderniseren. Denk bijvoorbeeld aan de bitcoin. Ook smart contracts zijn een veelbelovende toepassing binnen blockchain. Waarbij overigens de kanttekening moet worden gemaakt dat deze smart contracts juist niet ‘smart’ zijn. Het betreft doorgaans simpele rechttoe-rechtaan juridische afspraken. Voor meer ingewikkelde overeenkomsten is een volautomatische uitvoering in de praktijk niet haalbaar.



Whitepapers en andere studies naar blockchain schrijven vol enthousiasme over de nieuwe mogelijkheden, maar met betrekking tot privacybescherming wordt vaak aangegeven dat “hier nog meer onderzoek naar moet worden verricht”. Dat is eufemistisch taalgebruik voor een probleem dat vooralsnog niet is opgelost: veel blockchain-toepassingen staan op gespannen voet met de AVG.

Factoren bij een cloud keuze

In de eerste plaats is het voor overheden van cruciaal belang om te weten wie de leverancier is. Heeft hij banden met Amerikaanse bedrijven en/of overheden en valt hij daarmee onder de Patriot Act ? de Patriot Act zorgt er immers voor dat in dat geval de Amerikaanse overheid altijd bij uw data kan komen !

[1] Artikel 4 lid 7 en 8 van de AVG

Ervaring

Hoe lang is de cloudleverancier al actief in de industrie en wat is zijn expertise? Cloud computing is inmiddels meer dan tien jaar oud en cloudleveranciers van het eerste uur hebben een schat aan ervaring opgedaan. Let hierbij ook op de (wereldwijde) voetafdruk van een leverancier. Datasoevereiniteit is een prioriteit voor organisaties bij het kiezen van de juiste cloud. Een wereldwijde datacenter-footprint is hierbij essentieel. Zoek een cloudleverancier die de workload van klanten kan beheren en back-up- en DR-faciliteiten op de juiste plekken biedt.

Ruim aanbod

Welke diensten van de cloudleverancier versterken het productportfolio van de channelpartner? Er is veel vraag naar cloudbased backup en DR-oplossingen, en organisaties hebben er baat bij om samen te werken met cloudleveranciers die vooroplopen in dit gebied. Voor managed-serviceproviders is het een belangrijke overweging of een cloudleverancier in staat is om alle clouddiensten, zoals DRaaS, IaaS en backup, voor klanten te monitoren en te beheren. Het aanbod bestaat idealiter uit toepassingen die het beheer van betalingen, prestaties, beveiliging, compliance, testen en rapportage vereenvoudigen.

Beveiliging en compliance

Cloudbeveiliging en compliance zijn belangrijke prioriteiten in een cloudomgeving. Het is daarom essentieel te kiezen voor een cloudleverancier die zowel de compliance-eisen van het bedrijf als die van de klanten ondersteunt. Om bedrijven te helpen bij hun verdediging tegen cyberaanvallen moeten cloudleveranciers geavanceerde beveiligingsfeatures in hun platform geïntegreerd hebben. Kijk dus naar een leverancier die de veiligheid goed op orde heeft en (in principe) de ISO 27002 ondersteunt.

Responsible Disclosure

In de ICT-wereld bestaan meerdere praktijken om kwetsbaarheden in ICT bekend te maken. Voorbeelden hiervan zijn de zogeheten ‘full disclosure’, oftewel het volledig publiekelijk bekendmaken van een kwetsbaarheid en een verantwoorde wijze van responsible disclosure. Bij het volledig publiek maken van een kwetsbaarheid is deze nog steeds aanwezig en kan een veiligheidsrisico ontstaan. De praktijk van responsible disclosure heeft dan ook nadrukkelijk de voorkeur. Binnen de ICT-community is veel kennis en de wil om deze te delen met betrekking tot kwetsbaarheden in ICT alsmede de wijze waarop deze verholpen kunnen worden. De samenwerking met de ICT-community is daarmee van het grootste belang in het kader van het gezamenlijke streven naar cyber security.

Met het voeren van een beleid voor responsible disclosure wordt beoogd dat in gezamenlijkheid door melder en organisatie een bijdrage wordt geleverd aan het verminderen van kwetsbaarheden in informatiesystemen. Het werken met responsible disclosure laat echter de bestaande verantwoordelijk heden en verplichtingen onverlet. De verschillende actoren die betrokken zijn bij responsible isclosure hebben allemaal een eigen rol.

Responsible disclosure is primair een aangelegenheid die organisatie en melder aangaat en waartoe een organisatie een beleid kan vaststellen. Dit neemt echter niet weg dat het NCSC een rol heeft in het stimuleren van het voeren van een beleid van responsible disclosure. Tevens heeft het NCSC een rol in het uitdragen van kennis over kwetsbaarheden in ICT aan de overheid en de vitale sectoren. Het NCSC kan door organisaties worden betrokken bij het zo nodig over geconstateerde kwetsbaarheden
informeren van andere organisaties. Het NCSC zal, indien een melding direct bij het NCSC wordt gedaan, trachten de melder in contact te brengen met de betrokken organisatie.