Auteur: Maurice Derogee is werkzaam als ISO bij Servicepunt71. Maurice is bereikbaar via m.derogee@servicepunt71.nl.

Due diligence en Due care

Vanuit het rijk zijn er vele handreikingen, richtlijnen en kaders waarnaar wij ons kunnen richten, of die wij wettelijk moeten volgen. Zo zijn deze handreikingen en kaders voor de lokale overheid gebaseerd op de code voor informatiebeveiliging (NEN/ISO 27001 en 27002 de maatregelen), en worden de BIO genoemd. BIO staat voor Baseline Informatieveiligheid Overheid. Deze handreikingen (best practises) worden aangeleverd door de IBD (Informatiebeveiligingsdienst) als onderdeel van de VNG (Vereniging Nederlandse Gemeenten).

Met BIO kunnen we per onderwerp (organisatie, personeel, gebouwen, systemen) in kaart brengen wat er al is of wat er nog verbeterd of gestart moet worden om zo een goede beveiligingsorganisatie op te zetten. Er is door het kabinet veel gesproken over vermindering van de regeldruk maar hiervan is eigenlijk weinig terechtgekomen. In 1980 waren er nog 1100 wetten, anno 2020 zijn er 2500 wetten en circa 140.000 wetsartikelen. Hierbij opgeteld dan nog de AMvB's (Algemene Maatregel van Bestuur) per gemeente. Als we dan de impact hiervan op het bedrijfsleven bekijken in de zin van 'wat kost het het bedrijfsleven om aan al de relevante wetten en regels te kunnen voldoen', dan komen we uit op een bedrag van 9,5 miljard. De kosten voor de overheid om aan deze regels te voldoen zijn dan ook fors.
Dit houdt mij en mijn collega's flink aan de slag om alles volgens het boekje te willen doen. Hier worden wij door jaarlijkse audits en zelfevaluaties (de ENSIA ofwel Eenduidige Normatiek Single Information Audit) op getoetst. De ENSIA is specifiek voor bepaalde onderwerpen zoals SUWI, DigiD, BAG, BRO, BGT, Informatiebeveiliging en wordt gerapporteerd naar de toezichthouders Rijk.

Informatiebeveiliging niet sexy

Deze beknopte inleiding in de gemeentewereld leidt tot mijn vraagstelling. Is een gemeentelijke organisatie of samenwerkingsverband wel echt in staat dit zelf te organiseren op de juiste wijze? Ik doel hierbij niet op deskundigheid, want die is er. Al merk ik zelf dat dit beeld niet erg leeft buiten de gemeenten, of zelfs het rijk. Je merkt zelfs vaak verbazing als je in een gesprek met een externe partij blijk geeft van inhoudelijke en gedegen vakkennis. "Waar ligt dit dan aan?", vraag ik mij af. Deels kan ik het wel verklaren. Een gemeente is een politiek gedreven organisatie en hier liggen de doelen toch anders dan bij een onderneming in de commerciële wereld. Informatiebeveiliging is nu eenmaal geen sexy onderwerp, en wordt eerder als belemmering gezien dan een kwaliteitsverhogende discipline. De BIO is gebaseerd op een risico analyse die kwalitatief is. Ofwel het is deels te bepalen door het soort gegevens dat in bijvoorbeeld een informatiesysteem wordt gebruikt, ofwel het is deels te bepalen op het gevoel van de eigenaar van deze gegevens. Het is dus lastig aan te geven wat de kosten en baten zullen zijn van een mitigerende maatregel. Ook schrijven al de richtlijnen, wetten en regels niets over het verplicht hebben van een budget voor de beveiliging van de gegevens ofwel een informatiebeveiligingsbudget.

Een software-ontwikkelaar zal dit commercieel gezien op een kwantitatieve manier aanpakken. Hierbij worden wel alle kostenaspecten meegenomen en is er inzicht in de totale kosten van een te nemen maatregel. Dat kan vervolgens afgezet worden tegen het risico en de kosten als dit risico zich daadwerkelijk voordoet, dus ook wat dit jaarlijks zou betekenen (de JSV ofwel Jaarlijkse Schade Verwachting). Dan kun je dus de vraag 'wat levert het ons op' van de algemeen directeur beantwoorden.
Wat ik vooral zie, is dat de lokale overheid hard werkt aan de digitalisering en veel moderne technieken en diensten omarmt. In de coronatijd blijkt dit wel. De gemeenten draaien door op afstand en weten al hun dienstverlening feitelijk prima voort te zetten. Eigenlijk net zo goed als het bedrijfsleven dit doet in de dienstverlening. Hier kom ik dus weer terug op het beeld over de gemeenten en de vraag of zij dit allemaal zelf wel kunnen.

Paarse krokodil

Veelal zie je dat er bij de grotere gemeenten een goede organisatie is opgebouwd voor informatiebeveiliging en privacy. Maar ook daar hoor ik dezelfde geluiden over maatregelen en bijbehorende kosten. Uitbesteden wordt dan ook vaak gekozen. Op zich niet vreemd, want zoals eerder beschreven, hebben mensen een gefixeerd beeld van de overheid en ook hierdoor is het lastig gespecialiseerd personeel in voldoende mate te werven. En als je het geluk hebt dit wel voor elkaar te krijgen dan is het een kunst ze ook te houden. We kennen allemaal wel het reclamefilmpje van de paarse krokodil dat helaas ook wel slaat op de snelheid waarmee de zaken lopen binnen een gemeente. Dus huren veel gemeentes personeel in, maar daar komen vanuit de maatschappij weer negatieve reacties op: te veel kosten aan inhuur. Immers als je alles zelf wilt organiseren als gemeente, dan heb je heel specialistische mensen nodig die bijvoorbeeld: de netwerkbeveiliging op orde brengen, de firewalls beheren (24x7x365!), web- en e-mailsecurity op orde brengen, architectuur beheren en bewaken, een SOC/SIEM-service leveren, Incident Response Teams. Dit is dus nauwelijks als geheel te organiseren zonder bepaalde zaken uit te besteden aan specialistische partijen. En dit gaat uiteindelijk op voor ICT als geheel. Vanuit de overheid is er dan ook een aanbesteding gedaan voor een gezamenlijke dienstverlening op het gebied van onder andere informatiebeveiliging, ofwel GGI (Gezamenlijke Gemeentelijke Infrastructuur). Effectief gezien dus: schaalvoordeel halen en goedkoper je maatregelen realiseren bij diezelfde marktpartijen, als waar je als

individuele gemeente op was uitgekomen, en op een manier die dan ook hetzelfde is als bij de andere deelnemers.
Maar net als het niet verplicht hebben van een beveiligingsbudget, is ook hier geen verplichting om daaraan mee te doen. Vaak zie je dan toch een situatie ontstaan waarbij er zaken bij diverse partijen zijn belegd en dat deze partijen, om als geheel effectief te zijn, goed moeten samenwerken en ook goed moeten worden aangestuurd.

Due diligence en Due care

Er zijn twee soorten aanbieders. De ene is gespecialiseerd in dienstverlening aan de overheidswereld en weet goed hoe de processen daar werken. De ander biedt generieke diensten en specialismen die binnen elke bedrijfsomgeving kunnen worden ingezet. Deze aanbieders voeren uit wat er wordt gevraagd (binnen de kaders van de afspraken) en je zult dan dus zelf goed moeten weten of wat je vraagt wel het juiste is. Een regie-organisatie kan dan niet zonder mensen met technische kennis op de uitbestede specialismen. Je mag alleen al vanwege de verantwoordelijkheden, die je toegewezen zijn, niet blind vertrouwen op externe partijen.

De overheidsbezuinigingen – en dan met name aangaande de ICT – betekenen vaak echter bezuiniging op menskracht. Dan houd je als gemeente uiteindelijk al snel enkel jouw CISO en misschien jouw ISO(`s) over en hopelijk jouw Privacy Officer naast de verplichte FG. Je bent dan vooral bezig met het managen van contracten en het invullen van je maatregelen met informatie die de externe partijen jou moeten aanleveren. En hoe controleer je of alles echt gaat, zoals beweerd?

Je bent als (gemeentelijke!) organisatie verplicht om gedegen onderzoek te verrichten en op een goede manier zorg te dragen voor de (persoons)gegevens die je onder je hebt. Je kunt hierbij verantwoordelijkheid niet delegeren. Due diligence en Due care. Dus als je het beheer van een informatiesysteem en de betrokken gegevens uitbesteedt, zul je gedegen onderzoek moeten doen of de beoogde partij voldoende maatregelen heeft genomen en haar organisatie op orde heeft, die passen bij het beveiligingsniveau van de betrokken gegevens. De opdrachtnemer zal dan moeten zorgen dat het benodigde niveau geleverd wordt en op peil blijft. Gaat het mis, dan zal er door bijvoorbeeld de Autoriteit Persoonsgegevens (AP) worden gekeken naar deze omgeving en die zal dus toetsen of er voldoende is gedaan om te voorkomen dat het mis zou kunnen gaan. Is dit niet in orde dan zal dit bepalend zijn voor de hoogte van een opgelegde boete.

Slachtoffer betaalt zelf

Hier ontstaat dan gelijk het probleem (althans, zoals ik het zie). Stel dat er een claim wordt gelegd bij de leverancier van de dienst omdat deze volgens de gemeente oorzaak is geweest van het incident en de opgelegde boete. Dit zal uiteindelijk een rechter worden voorgelegd. Stel verder dat blijkt dat het incident is veroorzaakt omdat de gemeente heeft geëist van de leverancier dat het wachtwoord voor het aanmelden eraf moest omdat dit veel te lastig werd gevonden. En dat de leverancier hierop meerdere malen heeft aangegeven dat dit onverstandig was, maar uiteindelijk onder druk toch heeft ingestemd en dat dat uiteindelijk de oorzaak bleek van het incident. Dan zal de leverancier een deel van de boete moeten gaan betalen vanwege het feit dat ze dit hadden moeten weigeren, ongeacht de gevolgen. De gemeente zal zelf nog steeds het grootste deel voor haar rekening krijgen vanwege de verantwoordelijkheid, maar ook vanwege … het gebrek aan kennis?

De externe partij had niet mogen zwichten en betaalt daar de prijs voor. De gemeente betaalt eigenlijk niets, immers zij werken met gemeenschapsgeld. Dus feitelijk betaalt de ingezetene van de betrokken gemeente. Dus het slachtoffer (de burger wiens gegevens zijn gelekt) betaalt zelf en zal mogelijk nog meer betalen in persoon doordat zijn of haar identiteit wordt misbruikt door een crimineel die de gegevens online ontdekte. De zogenoemde afgeleide schade.

Zou dit dan voldoende grond zijn om een gemeente wettelijk te verplichten de zaken intern volledig en in praktijk bewezen op orde te hebben en zelfs als voorbeeld te dienen? Immers een gemeente heeft een schat aan gegevens en informatie onder zich. En uiteraard kost het de gemeente haar reputatie zodra het goed misgaat. Maar dan nog zal een burger niet kunnen beslissen om zijn paspoort of rijbewijs bij een andere gemeente te halen (omdat die van zijn of haar woonplaats niet te vertrouwen is). En de boetes dan? Een commercieel bedrijf kan het de kop kosten. Een gemeente feitelijk dus niet. Het zal politiek niet lekker worden ontvangen en er zullen mensen vertrekken. Ook zal er onderzoek worden gedaan en verbeteringen worden voorgesteld of zelfs bevolen. Maar uiteindelijk draait alles door. Rechtsongelijkheid zou je zo denken. En feitelijk ervaar ik dat ook zo.

De gemeenten moeten bezuinigen op het ambtelijk apparaat

Zou je dus moeten concluderen dat een gemeente anders wordt benaderd vanwege een lager kennisniveau in vergelijking tot een commercieel bedrijf? Of omdat het nu eenmaal een ambtelijk en politiek apparaat betreft waar alles nog gaat op een manier die al jaren zo is? Dit naast alle moderne ambities die de overheid heeft met bijbehorende wettelijke verplichtingen en de forse verantwoordelijkheden. Het doet je afvragen of het niet tijd wordt voor een modernere organisatiestructuur. Als ware het een commercieel bedrijf. De Wet Normalisatie Ambtelijk Personeel (WNRA) is er al een begin voor.

Gemeente als commercieel dienstverlener

Het politieke element zal blijven. Dit is nu eenmaal het kenmerk. Maar politiek zorgt ook voor tegenstrijdige belangen. Zoals in dit artikel beschreven moeten de gemeenten bezuinigen op het ambtelijk apparaat. Zo ontstond in 1992 discussie rond het aantal ambtenaren. Het rijk zou het met 7.000 ambtenaren minder moeten doen. Per 1 januari 1997 moesten de werktijden worden aangepast en werd de werkweek van 40 uur naar 36 uur teruggebracht. Net als de beloofde vermindering van de regeldruk is ook hier tot op de dag van vandaag nog steeds discussie over.
De regio waarin ik werkzaam ben is hier uiteraard ook mee bezig geweest. Zo is ook het Servicepunt71 op 1 januari 2012 ontstaan als dienstverlener voor de deelnemers en eigenaren (de betreffende regiogemeenten). De deelnemers hebben hun personeelsbestand ingekrompen en deze mensen zijn samengekomen in het Servicepunt. Op zich beschouwd leidde dit tot een tweeledig effect. De gemeenten hebben het aantal ambtenaren teruggebracht en met het Servicepunt71 hebben de kleinere gemeenten in het samenwerkingsverband tevens ineens meer specialismen tot hun beschikking en dus ook continuïteit in hun dienstverlening gekregen. Zo ontstond dus een gespecialiseerde lokale overheid dienstverlener.
Maar ook hier was er al sprake van uitbesteding van netwerkdiensten door een tekort aan interne specialisten. Anno nu heeft dit door verdere bezuinigingen - en moeite om gespecialiseerd technisch personeel te werven - geleid tot volledige uitbesteding van de ICT-dienstverlening op de Servicedesk na. Servicepunt71 werd dus een regievoerende organisatie.

Hoe wordt dit een moderne organisatie die enerzijds politiek gedreven moet zijn (en is) en anderzijds functioneert als een commerciële dienstverlener? Is dit een haalbaar scenario gezien de specifieke taken die een gemeente uitvoert met specifiek voor de gemeente gebouwde informatiesystemen door gespecialiseerde dienstverleners?
Net voor de deadline van dit artikel publiceerde de Rijksoverheid een notitie over de *Digitale overheid in het post-coronatijdperk*, getiteld: *Dichterbij door digitalisering* (1). Over actualiteit gesproken, ik ga mij er in verdiepen en kom wellicht daar later op terug.

Referentie

(1) Dichterbij door digitalisering:
www.rijksoverheid.nl/documenten/rapporten/2020/08/20/dichterbij-door-digitalisering