iBestuur

magazine

> Ancilla van de Leest: De overheid is niet te vertrouwen

> EPD in de herkansing

> GIBIT: gemeentelijke inkoopvoorwaarden

grip op privacy

Special over hoe de overheid onze gegevens kan beschermen.

Onafhankelijk kwartaalmagazine voor de iOverheid. Nummer 21, jaargang 7, januari 2017

… maar nog geen grip op beveiliging

Wie persoonsgegevens verwerkt moet ze goed beveiligen, zegt de wet. Maar bijvoorbeeld bij gemeenten maken de afhankelijkheid van leveranciers en het werken in ketens en over verschillende wetsdomeinen van de beveiliging een taaie klus.

Brenno de Winter

De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen. – Artikel 13 Wbp

In de Wet bescherming persoonsgegevens (Wbp) staat het zo simpel: wie persoonsgegevens verwerkt moet ervoor zorgdragen dat dit veilig genoeg gebeurt. De data moeten volgens de wetgever beschermd zijn tegen verlies, enige vorm van onrechtmatige verwerking en onnodige verzameling. De plicht tot beveiligen legt duidelijk neer wat het doel van beveiliging is.

Koudwatervrees

Voor het artikel spreken we negen 'chief information security officers' (CISO's), die geen van allen met naam of organisatie genoemd willen worden. Het onderwerp ligt politiek gevoelig en de angst om publiekelijk in problemen te komen is groot. Meerdere CISO's geven aan moeite te hebben met het goed in kaart krijgen welke risico's nu worden gelopen. Daarbij is er ook onzekerheid of alle geconstateerde risico's daadwerkelijk goed afgedekt zijn. In veel gevallen betwijfelen ze dat en is de vrees dat bij een incident niet aan de verwachting van het bestuur kan worden voldaan.

De Informatiebeveiligingsdienst (IBD), in 2012 opgericht door alle Nederlandse gemeenten, ondersteunt gemeenten in brede zin bij hun informatiebeveiliging en incidenten op dat vlak. Zij herkennen de vrees bij CISO's om open over beveiliging te praten. "Als je beveiliging heel goed doet vertel je er als je slim bent niet te veel over en als je het op punten niet op orde hebt ook niet", vertelt Nausikaä Efstratiades, hoofd van de IBD. "Voor veel mensen is het lastige materie of mensen denken dat het erg technisch is. Desalniettemin constateert de IBD dat gemeenten vooral open en transparant willen zijn over de wijze waarop zij met gegevens omgaan. Zij erkennen hun verantwoordelijkheid."

Ketenverantwoordelijkheid

Efstratiades wijst erop dat er bij gemeenten veel specifieke uitdagingen zijn, omdat er veel samenwerkingsketens zijn. "Denk alleen al aan bijvoorbeeld de jeugdketen, waarin gemeenten allerhande informatie uitwisselen met GGD, bureau Halt, Jeugdzorg, het OM en ga zo maar door", illustreert zij. "Dan is het niet voldoende om je eigen beveiliging op orde te hebben maar moet dat ook in samenhang met de ketenpartners worden geregeld." Het is in samenwerkingsverbanden niet altijd op het eerste gezicht en voor het gehele proces duidelijk wie welke rol heeft: is de gemeente bewerker of verantwoordelijke?

Voor beveiliging maakt dat laatste punt veel uit. De gegevensbewerker die verantwoordelijke is, blijft dat ook als een andere partij de gegevens verder bewerkt of een ICT-dienstverlener wordt ingeschakeld. Die verantwoordelijkheid wordt sinds

de invoering van de nieuwe wetgeving begin 2016 opeens in volle hevigheid gevoeld. Met alle worstelingen om zelf aan de verplichtingen te voldoen, is het goed toezicht uitoefenen op leveranciers voor de meeste security officers nog niet mogelijk.

Baselines

Als de problematiek wordt opgepakt dan wordt vaak aan leveranciers gevraagd om aan normen te voldoen. Populair zijn dan de Baseline Informatiebeveiliging Rijksdienst (BIR), de Baseline Informatiebeveiliging Gemeenten (BIG) of de ISO-27001/27002-normen. Maar het gebeurt ook wel dat de leverancier de leiding neemt in het beveiligen. Het bestuursorgaan heeft dan in het geheel geen regie over de situatie en voldoet dan niet aan de regelgeving. Dat probleem is wel bekend, maar niet snel op te lossen. Het zelf voldoen aan de BIR en de BIG en het slagen voor de DigiD-audits is al een zodanige aanslag op de capaciteit, dat extra taken het overvragen van de organisatie is.

Intern leunen veel organisaties op de BIG of de BIR. Voor specifieke problematieken wordt gebruik gemaakt van specifieke oplossingen. Daarbij komt een aantal methodieken van het Centrum voor Informatiebeveiliging en Privacybescherming voorbij onder de naam Grip op Privacy. Deze bieden een raamwerk om organisaties te helpen met het voldoen aan de Wbp. Ook het maken van risicoanalyses als basis voor beleidsvoorstellen komt regelmatig voorbij.

Deze benadering lijkt hoogdravend, maar in de praktijk gaat het ook gepaard met het regelen van vaak nog hele basale zaken. In veel organisaties is er veel achterstand met het up-to-date krijgen van software. Er is veel achterstallig onderhoud te verrichten met het uitfaseren van niet meer ondersteunde softwareversies, waarvoor projecten moeten worden gestart. Een populaire stap 'omdat deze makkelijk met het argument compliance is te verkopen'. En 'de kosten voor de reguliere ICT-afdeling komen niet op het beveiligingsbudget'.

Ook is bij diverse organisaties het maken van backups opnieuw onder de aandacht gekomen nu ransomware een groeiend probleem is. Wie daardoor wordt getroffen moet in ieder geval melding doen bij de Autoriteit Persoonsgegevens en dat trekt aandacht. Door te werken met goede reservekopieën is er een andere oplossing dan op de chantage in te gaan. De Autoriteit Persoonsgegevens is er klip en klaar over: een ransomware aanval is een datalek, backup of niet. "De verantwoordelijke kan er bij ransom- of cryptoware niet van uitgaan dat de inbreuk beperkt is gebleven tot het zichtbaar besmette bestand of systeem. De besmetting kan het hele systeem en alle gekoppelde bestanden raken", schrijft de organisatie zelf.

Bewustwording

Een andere belangrijke poot in het uitrollen van een beveiligingsstrategie is volgens de CISO's het inzetten op bewustwording. Die stap is belangrijk, omdat in de Wbp niet alleen over technische maatregelen wordt gesproken maar ook over organisatorische maatregelen. Een groot gedeelte van de beveiliging van persoonsgegevens leunt op het gedrag van medewerkers en het inzetten op goede procedures. Daarom gaat een deel van de energie op aan het goed voorlichten van mensen.

Daarbij is de drijvende kracht niet alleen de huidige Nederlandse wetgeving, maar ook de Algemene Verordening Gegevensbescherming. Als in 2018 daadwerkelijk aan die regelgeving moet worden voldaan moeten organisaties een grote slag hebben geslagen. Zo moet bijvoorbeeld bekend zijn welke gegevens worden verwerkt en moeten bestuursorganen dat ook kunnen oplepelen. Het zoeken naar inzicht in die gegevens brengt veel nieuwe risico's op de radar en voedt daarmee de beveiligingsplannen.

Andere beveiligingsdoelen

Bij het maken van beveiligingsplannen lopen de doelen van een bestuur niet synchroon met de wensen van de wetgever. Bij bijvoorbeeld gemeenten spelen naast het voorkomen dat persoonsgegevens bij de verkeerde mensen kunnen terechtkomen, verloren gaan of onrechtmatig worden verwerkt, ook andere problematieken een rol. Zo moet dienstverlening worden gewaarborgd en de nodige systemen daarvoor beschikbaar zijn, administraties correct zijn en de vertrouwelijkheid van bepaalde bestuurlijke documenten worden gewaarborgd. De nervositeit over kritische vragen in de raad is dan groot. De Wbp wedijvert dan ook met andere eisen, die politiek zijn en voor het gevoel van de CISO's net zo zwaar wegen.

De IBD ziet wel veel aandacht voor beveiliging, als het om de Wbp gaat. "Het is nu duidelijker dan ooit waar organisaties en dus ook gemeenten voor staan en aan moeten voldoen om de privacy te waarborgen. Zeker door de toename van informatiestromen binnen gemeenten, onder andere door de samenwerking in ketens, is de gemeente kwetsbaarder geworden. Informatiebeveiliging heeft prioriteit gekregen. Alhoewel, hier wat meer, daar wat minder", vertelt Efstratiades. In de ondersteuning werkt de organisatie dan ook aan een programma dat zich toespitst op de specifieke situatie voor gemeenten op de verschillende aspecten van privacy.

Angst voeden

Die angst voor het op de vingers worden getikt, wordt ook gevoed door de toezichthouder. Een goed voorbeeld is een onderzoek uit april 2016. Daarin concludeerde de Autoriteit Persoonsgegevens dat gemeenten onzorgvuldig met gegevens omgaan. Uit het onderzoek blijkt dat de gemeente bij het verwerken van gegevens voor voorzieningen in het sociaal domein de aanvrager ook toestemming voor verwerking vraagt – iets wat moeilijk is te weigeren. Maar volgens de AP kan dat niet, want die gemeenten hebben geen goed overzicht van de doelen, grondslagen en persoonsgegevens die zij verwerken binnen de rechtsgronden van de diverse verschillende wetten in het sociaal domein. Zij voldoen dus al snel niet aan de randvoorwaarden van de Wbp.

De wetenschap dat het haast onmogelijk is om onder de huidige omstandigheden volledig aan de Wbp te voldoen, maakt het praten over de beveiliging voor de CISO's ingewikkeld. "Niemand wil met zo'n boodschap in de media naar buiten treden", stelt Efstratiades en CISO's en de overigen bevestigen dat desgevraagd. "Het gevolg is dan niet moeilijk om te bedenken", licht er een toe. "Mijn aandacht is er vooral op gericht om zo snel mogelijk compliant te zijn en dat is niet automatisch hetzelfde als veilig zijn."

Dat laatste is ook een verhaal van mensen en middelen. Er wordt vooral erg operationeel gewerkt; zaken als bijvoorbeeld de communicatie op orde krijgen heeft op dit moment weinig prioriteit. De slag om budgetten wordt iets gemakkelijker nu de Cybersecurityraad adviseert om tien procent van het ICT-budget te steken in beveiliging en door de druk van de wetgever. Maar in de kern blijft bij beveiliging de focus liggen op achterstallig onderhoud verrichten, leunen op de kennis en kunde van de leverancier en het introduceren van normenkaders. En, zoals een CISO toevoegt: "hopen dat je ondertussen niet getroffen wordt door een datalek."

Ik probeer zo snel mogelijk compliant te zijn en dat is niet automatisch hetzelfde als veilig zijn