'Informatieveiligheid is echt een onder-de-motorkap-onderwerp'

Sinds anderhalf jaar werkt de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID) om informatieveiligheid hoger op de agenda te zetten bij overheidsbestuurders. Een van de gemeenten waar dat goed is gelukt, is de gemeente Utrecht. Een tweegesprek tussen Louke Vissers, directeur Publiekszaken bij de gemeente Utrecht en Harro Spanninga, accountmanager gemeenten bij de Taskforce BID.

Pieter Verbeek, journalist

Harro Spanninga en Louke Vissers zijn het met elkaar eens: 'Informatiebeveiliging heeft een cruciale rol binnen de gemeentelijke informatiehuishouding'

Utrecht staat de komende tijd voor een aantal uitdagingen op het gebied van informatieveiligheid. Niet alleen krijgt ze er nieuwe taken bij door de decentralisatie, waarbij weer meer persoonsgegevens worden gekoppeld, ook staat ze voor een grote verhuizing. Alle afdelingen gaan eind dit jaar naar het nieuwe stadhuis, inclusief alle gevoelige data. Gelukkig zijn steeds meer afdelingen zich bewust van het belang van de veiligheid van al die data.

Met elkaar verbonden

Dat bewustzijn gaat niet overal even makkelijk. 'Informatieveiligheid wordt vaak vergeten wanneer de dienstverlening wordt verbeterd. Steeds meer registraties zijn echter met elkaar verbonden. Als er ergens een lek is, is alles daardoor kwetsbaar', vertelt Spanninga. Hoe kwetsbaar informatie kan zijn, bleek uit de DigiNotar-affaire in 2011. Dit bedrijf verzorgde de PKI-overheidcertificaten voor grote delen van de Nederlandse overheid, waaronder die van DigiD, maar werd zelf gehackt. Reden genoeg voor het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties om voor een periode van twee jaar de Taskforce BID op te richten op advies van de Onderzoeksraad voor Veiligheid. Informatieveiligheid moest bovenaan de bestuurlijke agenda komen.

Baseline

Utrecht heeft de aanbevelingen van de Taskforce BID en de VNG Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' overgenomen, waaronder het invoeren van de Baseline Informatiebeveiliging Nederlandse Gemeenten, de zogeheten BIG, een set regels en gedragscomponenten waarmee overheidsafdelingen hun informatieveiligheid op orde kunnen krijgen. Deze BIG is ontwikkeld door de Informatiebeveiligingsdienst voor gemeenten (BID), een initiatief van de VNG en KING. Daarnaast is er binnen de gemeente Utrecht een *Chief Information Security Officer* aangesteld, legt Vissers uit. 'Zijn taak is te zorgen voor meer bewustwording over veiligheid onder de medewerkers. Hier bij Burgerzaken werken we al heel lang met de registratie van personen en zit het dan ook tussen onze oren. Nu moeten we ervoor zorgen dat ook andere afdelingen goed omgaan met deze gegevens. Het wordt goed gestimuleerd vanaf topniveau, met dank aan de Taskforce BID. Het is niet makkelijk. Informatieveiligheid is echt een onder-de-motorkap-onderwerp. Maar wel eentje dat geld en aandacht behoeft.'

Spanninga herkent dat. 'Informatieveiligheid is zoiets als de riolering', stelt hij. 'Je merkt er niets van totdat het fout gaat en er problemen ontstaan. Dat is meteen de kern van het probleem waarom het zo weinig aandacht krijgt. Het is niet direct zichtbaar.'

Afhankelijk van de ICT-afdeling

Maar wat voor risico's lopen gemeenten eigenlijk precies? Door de snelle digitalisering worden overheden al snel afhankelijk van de afdeling ICT. 'Zo loopt de continuïteit van je dienstverlening gevaar. Straks kun je niks meer als er iets fout is', meent Spanninga.

Een concreet voorbeeld daarvan is het Dorifel-virus, dat in 2012 zeker dertig overheidsinstellingen platlegde. De schade liep in de tonnen. Spanninga: 'Als je systemen plat liggen, kun je niets meer. Stel je voor dat het gebeurt juist wanneer uitkeringen moeten worden overgemaakt. Dat kan enorme maatschappelijke gevolgen hebben. Bij elk ICT-incident van de overheid halveert het vertrouwen van de burger.'

En dat vertrouwen is al niet zo hoog. Een enquête van de Nationale ombudsman laat zien dat zeker een derde van de Nederlanders vindt dat de overheid onvoldoende veilig omgaat met hun gegevens.

Cybercrime en identiteitsfraude

Spanninga geeft aan dat steeds meer overheden de dupe worden van identiteitsfraude en cybercrime. 'In Oost-Europese landen zijn gewoon hele callcenters actief om onze DigiD-inloggegevens hier los te peuteren. De kwetsbaarheid van onze GBA-gegevens is groot. Als je die in handen krijgt, zijn de mogelijkheden enorm wat je daar allemaal mee kunt doen. Daarom is dit onderwerp zo belangrijk. Vroeger toen de gegevens niet digitaal waren, was de schade ook niet zo groot. Nu is er ook zoveel meer te halen.'

De eerder genoemde BIG is overigens niet wettelijk verplicht om in te voeren voor overheden. Maar alle gemeenten willen ermee aan de slag. Daarvoor hebben ze eind vorig jaar de VNG *Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente'* aangenomen. Daarmee hebben ze verklaard dat informatieveiligheid een deel moet worden van het


Foto: Katja Schade


Foto: Katja Schade

Spanninga (rechts) tegen Vissers (links): 'De gemeente Utrecht is een echte voortrekker als het om informatieveiligheid gaat'

collegeprogramma en standaard moet worden meegenomen in de planning- en controlecyclus binnen de gemeente.

Gedragscomponenten

Utrecht gaat daar na de gemeenteraadsverkiezingen mee aan de slag. De baseline is nu ingevoerd, en met succes. 'Juist de gedragscomponenten hierin vind ik belangrijk', stelt Vissers. 'Het gaat niet alleen om het bewustzijn over veiligheid en privacy van onze medewerkers maar ook van de tijdelijke krachten, bijvoorbeeld uitzendkrachten.' Door het houden van audits en steekproeven toetst Utrecht de baseline. Vissers: 'We toetsen dan of medewerkers op een juiste manier met gegevens omgaan en volgens de juiste werkwijze. Verder kijken we of de personele kanten deugen, wie precies welke autorisaties hebben.'
Vissers is blij met de baseline. 'Mooi dat de Informatiebeveiligingsdienst voor gemeenten (IBD) zich daarmee bezighoudt', zegt ze tegen Spanninga. 'Omdat informatieveiligheid geen sexy onderwerp is, kon het vaak in de dagelijkse praktijk een sluitpost worden. Dankzij de baseline is men zich er meer bewust van geworden. Het moet echt tussen de oren komen. Met de baseline hoef je niet opnieuw het wiel uit te vinden. Dat is zeker een voordeel: kennisdelen via de Taskforce.' Naast het hanteren van de baseline organiseert Vissers ook integriteitbijeenkomsten om haar medewerkers bewust te maken van informatieveiligheid.

Voortrekkersrol

'Is Publiekszaken een voorbeeld voor andere afdelingen?', vraagt Spanninga. Vissers is daarvan overtuigd. 'Persoonsregistratie, paspoorten, burgerlijke stand, het is al zo'n oud beroep. Daardoor leeft het besef van veiligheid bij ons, het zit bij ons echt in de genen.' De uitdaging is om dat dus bij anderen ook te bereiken. Zeker met de decentralisaties die komen gaan. 'Als gemeentemedewerkers meer gesprekken gaan voeren aan de keukentafel, willen wij niet hebben dat ze zonder autorisatie met een laptop aan die tafel zitten met de gevoelige persoonsgegevens', zegt Vissers. 'Dit soort vraagstukken zijn niet vanzelfsprekend, je moet het gesprek erover aangaan. Ik zie ons daarbij vooral als bron van kennis en ervaring. Ga vooral met ons in gesprek.'
'Hebben jullie daar een actief beleid voor?', wil Spanninga weten. Vissers wijst op de informatiemanager van Publiekszaken. 'Hij werkt al 25 jaar in dit veld. Mijn opdracht aan hem is om informatieveiligheid gemeentebreed te agenderen. Ik vind dat heel belangrijk. We staan nog relatief aan het begin en moeten zien hoe het verder afloopt. We hebben net de baseline ingevoerd, en zijn klaar om informatieveiligheid voortaan mee te nemen in de planning en controlesystemen en stresstesten.'
'Wat dat betreft zijn jullie een echte voortrekker', antwoordt Spanninga. 'Het zou mooi zijn die kennis met andere gemeenten te delen.'
Vissers: 'Je moet echt aan de bel trekken, zorgen dat je gehoord wordt. Je moet niet als Calimero aan tafel zitten. Vaak wordt gezien dat het gedoe om privacy alleen maar remmend werkt. Maar ja, je persoonsgegevens zijn van jou, en dan wil je niet dat iemand anders ermee aan de haal gaat.'
Daar is Spanninga het helemaal mee eens. 'Als ze uitlekken leidt dat tot echte schade. Niet alleen voor de overheid, maar vooral voor mensen. Het gaat namelijk om mensenlevens die er de dupe van zijn.'

Het onderwerp informatieveiligheid is blijvend in ontwikkeling, benadrukt Spanninga. 'De technologie verandert maar door, de ontwikkelingen gaan idioot hard, sneller dan we bij kunnen houden. Je moet continu verbeteren. Hoe richt je je processen in zodat ze bij de tijd blijven? Het komend jaar moeten we de eerste resultaten zien van de slag in de bewustwording in de overheidslagen. Dit verdient serieus de aandacht.'

TASKFORCE
Bestuur & Informatieveiligheid Dienstverlening

De Taskforce Bestuur en Informatieveiligheid Dienstverlening (BID) is op 13 februari 2013 door minister Plasterk (BZK) voor een periode van twee jaar in het leven geroepen. Het doel van de Taskforce BID is om het onderwerp informatieveiligheid hoog op de agenda te krijgen bij bestuurders en topmanagement van alle overheidslagen. Zowel qua bewustwording als sturing. Dit vanuit het perspectief van Verplichtende Zelfregulering per overheidslaag.
Op zoek naar opleidingen, concrete instrumenten en kennis over informatieveiligheid? Lees meer op onze Pleio-site Informatieveiligheid en deel hier ook uw eigen kennis.

https://informatieveiligheid.pleio.nl/
www.taskforcebid.nl