Onderwerp: Bijpraten gemeenteraad informatiebeveiliging en privacy

Datum: 16-03-2017

Aanleiding:
U hebt verzocht te worden bijgepraat over de onderwerpen privacy en informatiebeveiliging. Hieronder leest u op welke wijze de gemeente Doetinchem hiermee omgaat. In de presentatie van 16 maart zal dit worden toegelicht en is er ruimte voor vragen.

Noodzaak van informatiebeveiliging
Informatie is een bedrijfsmiddel, dat net als andere belangrijke bedrijfsmiddelen waarde heeft voor de organisatie. Betrouwbare informatie is van essentieel belang voor een kwalitatief hoogwaardige èn efficiënte dienstverlening, en een belangrijke basisvoorwaarde voor een succesvolle samenwerking met externe partners. Burgers en bedrijven verwachten ook dat er zorgvuldig wordt omgegaan met privacygevoelige informatie. De gemeente heeft een belangrijke verantwoordelijkheid op dit gebied.

ICT biedt ongekende mogelijkheden waardoor de communicatie tussen burgers, bedrijven en (gemeentelijke) overheid steeds vaker digitaal verloopt. Medewerkers werken thuis en op mobiele (privé) apparaten. Landelijke ontwikkelingen zoals decentralisaties, ketensamenwerking en veranderende wet- en regelgeving hebben grote invloed op de informatievoorziening van de gemeente. Dit vraagt voortdurende aandacht voor (nieuwe) kwetsbaarheden in de informatie uitwisseling. Steeds weer gaat het om de afweging tussen goede dienstverlening, effectieve bedrijfsvoering en privacy van inwoners.

Het beleidskader
Om dit te regelen, is er informatiebeleid en informatiebeveiligingsbeleid waarin de belangrijkste uitgangspunten staan. Eén van die uitgangspunten is digitaal werken. Dit voorkomt dat papier op plekken ligt waar het toegankelijk is voor onbevoegden. Naast een clean desk policy (geen vertrouwelijke informatie achterlaten op een onbemand bureau) kennen wij ook een clear screen policy (beeldscherm vergrendelen als je de werkplek verlaat).
In de Wet bescherming persoonsgegevens (Wbp) staat wat er wel en niet mag met persoonsgegevens. Onlangs hebben wij, naar aanleiding van de nieuwe taken in het sociaal domein, aanvullend privacybeleid opgesteld. Dit is gemeentebreed beleid, maar voor de taken van het Buurtplein en het Zorgplein is er een verbijzondering opgesteld gezien het belang van privacy bij de uitvoering van deze taken. Dit privacybeleid ligt op dit moment voor bij de raad.
Ons informatiebeveiligingsbeleid is gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). De BIG kent een strategisch deel waarin de organisatie van en de verantwoording over informatiebeveiliging binnen de gemeente centraal staan. Daarnaast is er een tactisch deel met richtlijnen rondom technische en (vooral) organisatorische beveiligingsmaatregelen. Het invoeren hiervan betreft een meerjarenplan en vraagt om continue aanpassing.

Wie heeft welke verantwoordelijkheid?

Het informatiebeveiligingsbeleid en privacybeleid wordt vastgesteld door het college en ter kennisname gestuurd naar de raad.
Het informatiebeveiligingsplan bevat de prioritering van de concreet te nemen maatregelen, deze wordt vastgesteld door directie. De afdelingshoofden zijn - als integraal manager - verantwoordelijk voor de informatieveiligheid van de werkprocessen van de afdeling.
Om de samenhang te bewaken, te ondersteunen en te kunnen monitoren zijn de volgende ondersteunende rollen benoemd:

strategisch: *security officer* (afdelingshoofd Services)
tactisch: *beveiligingscoördinator* en *privacycoördinator* (gepositioneerd binnen Team IM)
operationeel: *beveiligingsbeheerder* (alle functioneel applicatiebeheerders)

Horizontale en verticale verantwoording:
De verantwoording over informatieveiligheid aan de gemeenteraad vindt plaats via de P&C-cyclus: in een bijlage bij de jaarrekening. Naast de (horizontale) verantwoording vanuit de BIG is er ook de verticale verantwoording vanuit verschillende taakvelden, te weten:

- Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (de SUWI-wet),
- Wet Basisregistratie Personen (BRP),
- Wet Paspoortuitvoeringsregeling (PUN)
- Wet Basisregistratie Adressen en Gebouwen (BAG)
- Digitale persoonsidentificatie (DigiD)

Op dit moment kent elke sector (ministerie) zijn eigen verantwoordingsmethodiek die niet parallel loopt met de P&C cyclus. Bij grote afwijkingen rapporteren wij tussentijds aan de raad.

Om deze verantwoordingsystematiek zo effectief en efficiënt mogelijk in te richten, is er een landelijk project gestart, genaamd ENSIA (Eenduidige Normatiek Single Information Audit). Hierin wordt één zelfevaluatie-tool ontwikkeld die op één moment een rapportage vraagt. De verwachting is dat dit in 2018 wordt ingevoerd. Dit heeft tot doel het verantwoordings-proces over informatieveiligheid bij gemeenten verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus. Hierdoor heeft het gemeentebestuur meer overzicht over de stand van zaken van de informatieveiligheid en kan hier ook beter op sturen.

Specifieke aandachtspunten informatiebeveiliging:

Meldingen vanuit de IBD
De gemeente Doetinchem is aangesloten bij de Informatiebeveiligingsdienst voor gemeenten (IBD). Technologie verandert snel en daarmee dus ook de bedreigingen en de maatregelen die nodig zijn om risico's te beperken. De IBD deelt dagelijks kennis (mede afkomstig van het Nationaal Cyber Security Center (NCSC)) waardoor we snel op de hoogte zijn van bedreigingen. Bij acute dreigingen worden de aangewezen contactpersonen binnen de gemeente direct geïnformeerd.

Privacywetgeving
De belangrijkste regels voor de omgang met persoonsgegevens in Nederland zijn vastgelegd in de Wet bescherming persoonsgegevens (Wbp). De Autoriteit Persoonsgegevens (AP, voorheen College Bescherming Persoonsgegevens (CBP)) houdt toezicht op de naleving van deze wet.

De gemeente is verplicht de verwerking van bepaalde persoonsgegevens te melden bij de AP. De AP heeft op haar website een openbaar register van alle organisaties die persoonsgegevens verwerken. Zo kunnen mensen zien wie welke persoonsgegevens van hen gebruikt en met welk doel. De gemeente Doetinchem houdt daarom een privacyregister bij van alle werkprocessen waarin persoonsgegevens worden verwerkt. Dit is de verantwoordelijkheid van de privacycoördinator.
De privacycoördinator ondersteunt ook bij het melden van datalekken. De meldplicht datalekken is ingegaan op 1 januari 2016. Deze meldplicht houdt in dat organisaties direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben en soms ook aan de mensen van wie de persoonsgegevens zijn gelekt. Niet (tijdig) melden kan aanzienlijke boetes tot gevolg hebben.
Op 25 mei 2016 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden. Binnen 2 jaar moeten gemeenten aan deze eisen voldoen. De VNG heeft bij minister Plasterk inmiddels aandacht gevraagd voor de financiële gevolgen die de nieuwe Europese regelgeving de komende jaren zal gaan hebben voor gemeenten. De Europese privacy-verordening is strenger dan de huidige wetgeving. Een van de stappen die wij zullen moeten zetten, is het aanstellen van een Functionaris voor de Gegevensbescherming (FG). De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de privacywetgeving. Naar verwachting zullen wij dit regionaal oppakken.

Bewustwording medewerkers
Informatiebeveiliging is vooral een kwestie van gedrag en cultuur. Uit onderzoek blijkt dat de meeste beveiligingsincidenten worden veroorzaakt door gedrag van medewerkers en niet door problemen met de techniek. Bewustzijn is daarom de belangrijkste beveiligingsmaatregel!
Om dit bewustzijn te versterken, wordt er jaarlijks een kennistoets informatiebeveiliging onder de medewerkers uitgevoerd zodat zij weten hoe om te gaan met informatie. Ook besteden wij in de werkoverleggen aandacht aan deze onderwerpen. Daarnaast is er een aparte pagina op intranet met alle belangrijke informatie over beveiliging. Deze activiteiten worden alleen voor de gemeentelijke organisatie uitgevoerd.

Informatieveiligheid en samenwerkingsverbanden
In toenemende mate werken we samen met partners in diverse ketens, gemeentelijke samenwerkingsverbanden of door middel van het uitbesteden van taken. Waar het wettelijke verplichtingen betreft verstrekken wij persoonsgegevens. De gemeente blijft te allen tijde eindverantwoordelijk voor de bescherming van deze persoonsgegevens. Daarom vragen we aan élke (grote en kleine) partij die namens de gemeente Doetinchem persoonsgegevens verwerkt, een zogenaamde Bewerkersovereenkomst te ondertekenen. Dit is een bijlage bij het samenwerkingscontract waarin de partner aangeeft *alle passende technische en organisatorische maatregelen te nemen om de (persoons)gegevens te beveiligingen en beveiligd te houden tegen verlies of tegen enige vorm van onzorgvuldig, ondeskundig of ongeoorloofd gebruik*.
In het sociaal domein gelden deels andere regels. Het is niet noodzakelijk met iedere zorgverlener een bewerkersovereenkomst te sluiten. Dit wordt geregeld via het VECOZO.
Leveranciers van webapplicaties moeten voldoen aan de NCSC-normen. Dit zijn (met name technische) normen waaraan de applicatie minimaal moet voldoen.
Onze verbonden partijen kunnen informatieveiligheid en privacy òf zelf regelen, òf deze diensten bij de gemeente Doetinchem afnemen. Gezien de complexiteit van deze onderwerpen werken wij ook als gemeente binnen de regio nauw met elkaar samen.