Bijlage ICT-afhankelijkheid

25 april 2017, FSFE Nederland

In deze bijlage vindt u vier uitgewerkte thema's omtrent de ICT-afhankelijkheid bij gemeenten met bijhorende voorbeeldvraag.

1. Interoperabiliteit via Open Standaarden

Een belangrijke stap naar onafhankelijkheid is het gebruik van 'open standaarden'. Open standaarden zijn vrij verkrijgbare specificatiedocumenten voor gegevensuitwisseling tussen ICT-systemen. De openheid van de standaarden zorgt ervoor dat iedereen de standaard kan gebruiken. (meer informatie via Forum Standaardisatie)

Sinds 2002 is het gebruik van open standaarden verplicht voor gemeentelijke systemen. Alleen met gegronde reden mag hiervan afgeweken worden, het zogenaamde 'pas toe of leg uit' beleid.

In de praktijk betekent dit dat het verspreiden van een Docx (Microsoft Word formaat) niet is toegestaan, en daarvoor in de plaats moet worden gekozen voor Odt of Pdf. Forum Standaardisatie houdt lijsten bij van goedgekeurde standaarden, die ook regelmatig een update krijgen. De gemeente moet op elk moment een overzicht kunnen tonen van de gevallen waarin geen open standaarden gebruikt zijn, dit mag tenslotte niet zonder een degelijke onderbouwing.

Voorbeeldvraag

Gemeenten moeten verplicht open standaarden gebruiken, tenzij er een gegronde reden is om daarvan af te wijken. Past onze gemeente momenteel overal open standaarden toe? Zo nee, welke delen van de ICT-infrastructuur gebruiken nog geen open standaarden, welke software is hierbij betrokken, en welke leveranciers zijn hiervoor verantwoordelijk?

2. Toezicht op de ontwikkeling van onmisbare software

De adoptie van open standaarden gaat in Nederland te traag, en het zal dan ook nog jaren duren voordat de huidige afhankelijkheid significant is afgebouwd. In de tussentijd zijn we voor kritieke infrastructuur afhankelijk van een handjevol producten van een handjevol partijen. Juist die afhankelijkheid maakt het des te belangrijker dat de gemeente op haar strepen gaat staan bij de inkoop van softwareproducten, om los te komen van de machtspositie van de grote softwareleveranciers.

Voorbeeldvraag

Constaterende dat ook onze gemeente voor haar ICT afhankelijk is van een handjevol leveranciers, moet de gemeente een vinger aan de pols houden over de naleving van gemaakte afspraken. Denk hierbij aan de omgang met persoonsgegevens, het gebruik van bepaalde open standaarden en het hanteren van een hoog beveiligingsniveau. Hoe ziet de gemeente hierop toe?

3. Bescherming persoonsgegevens van burgers

De Amerikaanse Stored Communications Act geeft de Amerikaanse overheid het recht om gegevens op te vragen van bedrijven met een Amerikaanse oorsprong. Maar de jurisprudentie over die wet is nog niet sluitend. In 2016 hoefde Microsoft Amerika geen persoonsgegevens over te dragen beheerd door Microsoft Ierland (blogpost jurist Arnout Engelfriet). Maar in 2017 moest Google Amerika wel e-mails overdragen die buiten Amerika waren opgeslagen (blogpost jurist Arnout Engelfriet). Persoonsgegevens zijn in Amerika minder goed beschermd dan in Europa, en daarom is deze Amerikaanse inmenging zorgelijk.

Met twee maatregelen kan het risico worden verkleind op een rechtmatige overdracht van Nederlandse persoonsgegevens naar de Amerikaanse overheid. Door geen zaken te doen met softwarebedrijven met een Amerikaanse oorsprong wordt inmenging van de Amerikaanse overheid voorkomen. Bij een softwareleverancier met Amerikaanse oorsprong moet ervoor worden gezorgd dat deze partij zo min mogelijk in aanraking komt met persoonsgegevens.

Voorbeeldvraag

De Amerikaanse oorsprong van softwareleveranciers als Microsoft staat op gespannen voet met de taak van de overheid om de privacy van Nederlandse burgers te garanderen volgens Europese maatstaven. Zijn er alternatieven overwogen voor de huidige softwareleveranciers die een Amerikaanse oorsprong hebben, en hoe wordt op dit moment voorkomen dat software van Amerikaanse bedrijven in aanraking komt met persoonsgegevens?

4. Een monocultuur aan software speelt hackers in de hand

Een ander aspect van de huidige situatie is het verhoogde risico op een succesvolle cyberaanval. De monocultuur van software in gebruik bij de overheid is namelijk een interessant doelwit om kwetsbaarheden voor te vinden. Op het moment dat zo'n kwetsbaarheid wordt ontdekt, wordt in een mum van tijd een mogelijkheid ontwikkeld om de kwetsbaarheid te gebruiken voor een cyberaanval. Een meer divers gebruik van software zou dit risico verlagen, omdat dan een meer gerichte aanpak nodig is. Meer achtergrond hierover is te lezen in een wetenschappelijk paper dat in 2010 werd gepubliceerd vanuit de overheid.

Voorbeeldvraag

De gemeente doet mee aan de monocultuur van softwareproducten en heeft daarmee een verhoogd risico op een succesvolle cyberaanval. Welke maatregelen zijn genomen om dit risico af te dekken, en is uitwijken naar andere softwareproducten hierin meegenomen als mogelijke maatregel?