Rijksoverheid ontbeert digitaal sourcingsbeleid

Victor de Pous (22 januari 2020)

Voormalig PvdA-kamerlid Oosenburg pleitte vorig jaar als voorzitter van de Stichting Open Source & Overheid voor een parlementaire enquête over de ICT-aanbestedingen van het Rijk. ‘Bij aanbestedingen van ICT-projecten zijn het vrijwel altijd oplossingen uit de hoek van de closed source software, die er met de buit vandoor gaan.’ De belegen emotionele ‘open’ versus ‘gesloten’ discussie, die nooit zwart-wit was maar wel zo werd gevoerd, heeft inmiddels verder aan complexiteit gewonnen.
Ondertussen is de veelal strategische waarde van dit ontwikkel- en leveringsmodel *voor leveranciers* buiten kijf komen te staan. Niet voor niets betaalde Microsoft 7,5 miljard dollar voor het ontwikkelaarsplatform GitHub en telde IBM maar liefst 33,4 miljard dollar uit voor RedHat, het enige open-sourcebedrijf ter wereld van serieuze omvang, dat behalve onderhoudsabonnementen en tools voor *entreprise* Linux, ook de hybride cloudmarkt bedient. Daarvan profiteren ook gebruikers, onder meer door een snellere time-to-markt van nieuwe software en diensten.

Waar overheidsorganisaties in Nederland meer behoefte aan hebben dan een aanbestedingsenquête (dus verhoren onder ede), is gedegen digitaal sourcingsbeleid. Heldere uitgangspunten voor aanschaf, inclusief ontwikkeling, van digitale producten en diensten *en voor hun leveranciers*, inclusief de context. Een voorbeeld. Mag de digitale beveiliging van onze staatsgeheimen worden uitbesteed aan het door de Engelsen destijds (op 25 november 2015) onverwachts overgenomen Fox-IT? En zo ja, onder welke voorwaarden voor technologie en leverancier? Antwoord: er is geen beleid dus in beginsel is alles mogelijk.

Terug naar de specifieke casus. Het probleem met open source software is dat alles wat je in het concrete geval zegt, waar kan zijn maar zelden algemene geldigheid kent. Onze onderbouwde stelling van 15 jaar geleden staat nog onverkort, terwijl er nieuwe argumenten bij zijn gekomen. Neem het eclatante succes van cloud computing. Zo heeft een gebruikersorganisatie die open source software *als dienst* van een derde afneemt in de praktijk weinig aan het vaak gehoorde voordeel dat vendor lock-in ontbreekt. *Third-party clouddiensten vergroten juist de afhankelijkheid van leveranciers ten principale* en daarbij doet dat een afwijkend licentieregime van de achterliggende programmatuur weinig aan af.

Daarnaast toont Android aan dat openbaarheid en vrije beschikbaarheid van de basiscode *en* de aanwezigheid van een grote gemeenschap van internationale ontwikkelaars niet per definitie voor betere digitale veiligheid zorgen. De wereld telt meer dan twee miljard Android-telefoons, met talloze security bugs, maar de helft ontvangt geen veiligheids-update. *Zegge en schrijve een miljard onveilige open source-smartphones worden dagelijks gebruikt*; wellicht mede door medewerkers van Nederlandse overheidsorganisaties ten behoeve van hun werk.

Dat laat onverlet dat de inzet van open source-softwareproducten ook de Staat majeure voordelen kan bieden, bijvoorbeeld door applicaties eenmaal te (laten) ontwikkelen en vervolgens breed onder overheidsorganisaties te verspreiden. (Let op: discriminatie mag niet, waardoor de toepassingsprogrammatuur ter zake aan een ieder *moet* worden aangeboden.) Deze opties voor efficiënt automatiseren vragen echter om transparant, geavanceerd en tevens gedifferentieerd sourcingsbeleid, dat getoetst kan worden door onder meer het parlement.

Hetzelfde kunnen we stellen ten aanzien van in beginsel alle overheidsautomatisering. De inzet van het Amerikaanse softwareproduct Microsoft Office ProPlus bleek na een gegevensbeschermingseffectbeoordeling (*data protection impact assessment*), zoals omschreven in de Algemene verordening gegevensbescherming (AVG), door een derde partij in 2018 een ‘hoog’ privacyrisico voor de 300.000 ambtenaren met hun rijkswerkplek op te leveren. De oplossing werd gevonden in een ‘verbeterplan’ en een termijn van vier maanden. De anti-virusprogrammatuur van de Russische leverancier Kaspersky moest echter op basis van een inbreukvermoeden dan wel op nimmer openbaar gemaakte informatie op last van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), eerder dat jaar, bij de rijksoverheid worden ‘uitgefaseerd’. Dit zijn geheel verschillende maatregelen, die op basis van ‘Rijkssourcingsbeleid’ voldoende verklaard en getoetst zouden kunnen worden.

Tel daarbij op dat geopolitiek een steeds gewichtiger factor behelst. Dat onderkent ook hetzelfde NCTV in zijn Cybersecuritybeeld Nederland 2019. Er moet aandacht komen voor de notoire afhankelijkheid van ICT dat ons, zelfs maatschappij-breed, kwetsbaar maakt. Opvallend en lovenswaardig is zijn bredere blik, die verder gaat dan spionage en criminaliteit. Nederland is (ook) ‘afhankelijk van een beperkt aantal aanbieders en landen, dit maakt ons kwetsbaar voor hun (veranderende) intenties’, daarbij wijzend naar de VS en China. Wij stellen na 75 jaar commerciële electronic data processing dat ICT menens wordt. Eén gevolg van deze conclusie is dat de Rijksoverheid niet langer onder integraal digitaal sourcingsbeleid uitkomt.

Mr. V.A. de Pous is analist en adviseur digitaal recht.