Informatiebeveiliging bij de overheid

Geachte woordvoerders Digitale Zaken,

Op 12 september debatteert u over Informatiebeveiliging bij de overheid. Dit onderwerp is van groot belang voor gemeenten en heeft direct invloed op mogelijkheden van gemeenten voor de invoering van de EU-wet- en regelgeving en de relatie van gemeenten met hun leveranciers. Daarom brengen wij graag een aantal aandachtspunten onder uw aandacht voor effectieve invoering en uitvoering van die regelgeving in reactie op de volgende agendapunten:

- Uitvoering van de motie van de leden Rajkowski en Van Weerdenburg (26643-830) en motie van het lid Rajkowski c.s. (26643-874)
- Waarborgen t.b.v. privacy en informatiebeveiliging en aanbestedingsregels[1]

Gemeenten zien dat digitale sabotage (dus een aanval op onze vitale infrastructuur) desastreuze gevolgen kan hebben, zoals digitale en maatschappelijke ontwrichting. Wij onderschrijven het risico dat in de moties van de leden Rajkowski en Van Weerdenburg en van Rajkowski c.s. wordt benoemd. Het risico van de inzet van programmatuur of apparatuur van organisaties uit landen met een offensieve cyberagenda is bij gemeenten meermaals onder de aandacht gebracht, bijvoorbeeld in relatie tot het gebruik van apps of de inzet van cameratoezicht. Waar risicovolle toepassing bekend is en wanneer dit mogelijk is, faseren gemeenten die uit[2][3]. In de risicoafweging wegen gemeenten het risico af van de inzet van programmatuur of apparatuur van organisaties uit landen met een offensieve cyberagenda vanuit de principes voor de digitale samenleving[4]. In de principes voor de digitale samenleving leggen gemeenten de basis om technologie, veilig, inclusief en verantwoord in te zetten. De principes van informatiebeveiliging- en privacybescherming by-design zijn hierin opgenomen. Deze principes zijn verder uitgewerkt in de Gemeentelijke inkoopvoorwaarden bij IT-toolbox GIBIT[5] die gemeenten bij inkoop en aanbesteding toepassen.

Wij zien mogelijkheden om de inzet van risicovolle producten of diensten samen met de leveranciers aan de voorkant van het inkoop- en aanbestedingsproces verder te kunnen beperken. Hiertoe stellen de verschillende ministeries echter verschillende handreikingen en eisensets op. De staatssecretaris voor Digitalisering stelt de inkoopeisen cybersecurity overheid (ICO)[6] op. In de Baseline Informatiebeveiliging Overheid (BIO) is de toepassing van de ICO-eisenset opgenomen. Met het voornemen van de staatssecretaris voor Digitalisering om de BIO in de nieuwe Cyberbeveiligingswet te verankeren, wordt de toepassing van de ICO-eisenset verplicht.
De NCTV publiceerde onlangs de Toolbox veilig inkopen[7]. Met de uitwerking van de Cyber Resillience Act[8] stelt de minister van EZ, mede namens de EU, cybersecurityeisen aan de fabrikanten en leveranciers, voordat zij een product of dienst op de Europese markt mogen brengen.

---

[1] Waarborgen t.b.v. privacy en informatiebeveiliging en aanbestedingsregels
https://www.tweedekamer.nl/downloads/document?id=2024D00510
[2] https://www.l1nieuws.nl/nieuws/2564200/chinese-cameras-gemeenten-gooien-ze-in-de-prullenbak
[3] https://nos.nl/artikel/2533835-gemeente-amsterdam-verbiedt-telegram-op-werktelefoons
[4] https://vng.nl/sites/default/files/2022-12/Principes-voor-de-Digitale-Samenleving.pdf
[5] https://vng.nl/projecten/gibit
[6] https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cybersecurity/inkoopeisen-cybersecurity-overheid/
[7] https://www.nctv.nl/onderwerpen/economische-veiligheid/toolbox-veilig-inkopen
[8] https://www.rijksoverheid.nl/actueel/nieuws/2023/12/01/europees-akkoord-veiligheidseisen-en-standaarden-voor-alle-digitale-producten

Toolbox Veilig inkopen is een middel en géén doel

Wij onderschrijven het belang van eenduidigheid in de eisenset voor inkoopeisen cybersecurity voor de hele overheid. Op dit moment is er echter geen interbestuurlijke governance en proces ingericht voor het opstellen, bijstellen en vaststellen van één basisset aan ICO-inkoopeisen cybersecurity waar de hele overheid aan zou moeten voldoen. Ook is er geen samenhang in de aanpak met andere vakministers.

In de GIBIT zijn nu aanbevelingen uit de toolbox Veilig inkopen en een deel van de inkoopeisen cybersecurity vanuit de ICO-eisenset opgenomen. Gemeenten gebruiken de rijks-tool voor de ICO-inkoopeisen *niet*. De aan de ICO-eisen toegevoegde sets zijn de afgelopen jaren door rijksonderdelen aangedragen en opgenomen zonder interbestuurlijke besluitvorming. Wij zien nu dat er alleen aandacht is voor het toepassen van de tool, waarmee dit middel tot doel verheven is.

Gemeenten werken toe naar een risicogebaseerde aanpak en aandacht voor het contact met de leverancier in het gehele proces, ook gedurende de uitnutting van het contract zodat dreigingen en kwetsbaarheden tijdig en samen kunnen worden aangepakt. Hierbij herkennen ze de fasering en mogelijkheden tot waarborgen van privacy en informatiebeveiliging in aanbestedingsregels en proces, zoals in de brief van de staatssecretaris genoemd[9]. Het goede gesprek gedurende de hele periode van aanbesteding en looptijd van het contract blijft heel belangrijk. Dat goede gesprek is met sommige leveranciers niet altijd mogelijk. Ook kunnen er juridische- en handelsbezwaren zijn om producten of diensten uit bepaalde landen uit aanbestedingen te kunnen weren. Dan zijn de opgestelde principes leidend.

Voor de effectieve invoering en uitvoering van al die richtlijnen is het voor gemeenten randvoorwaardelijk dat de nationale wet- en regelgeving tijdig, gebundeld, geïntegreerd en integraal afgewogen wordt aangeboden vanuit de verschillende ministeries en voorzien wordt van realistische middelen voor de uitvoerbaarheid en prioritering in de tijd. Wij zien dat hier mogelijkheden liggen tot synergie, om eenduidige en samenhangende kaders te stellen aan de inzet van veilige hard- en software in Nederland. Organisaties en leveranciers en fabrikanten kunnen er in samenwerking voor zorgen dat in diensten en producten het risico op spionage uit landen met een offensieve cyberagenda tot een mimimum beperkt worden en dat de diensten voldoen aan de Europese en nationale inkoopeisen cybersecurity.

Wij vragen om:

- De eisen voor gemeenten als aanbestedingsplichtige diensten ten aanzien van producten of diensten uit landen met een offensieve cyberagenda in lijn te brengen met de overige eisen vanuit bijvoorbeeld de set aan inkoopeisen cybersecurity overheid (ICO), de toolbox veilig inkopen en de Cyber Resillience Act, zodat de verantwoordelijkheden gedeeld worden met leveranciers en producenten en er een eenduidige en samenhangende aanpak uitgewerkt kan worden voor het hele proces.
- interbestuurlijk een governance en proces in te richten voor het opstellen, bijstellen en vaststellen van een samenhangende basisset aan inkoopeisen cybersecurity waar de hele overheid aan moet voldoen.
- Een tool (of de toepassing van een tool) niet als primair doel te stellen, maar het als middel te zien.

[9] Waarborgen t.b.v. privacy en informatiebeveiliging en aanbestedingsregels
https://www.tweedekamer.nl/downloads/document?id=2024D00510