Aan: het college van Burgemeester en Wethouders van de gemeente Groningen

Betreft: Schriftelijke vragen ex art. 36 RvO omtrent cyberveiligheid gemeente Groningen

Groningen, 21 november 2023

Geacht college,

Digitale veiligheid is een ontzettend belangrijk onderwerp dat ook binnen gemeentes veel aandacht vereist. Elke gemeente bezit immers over hele kostbare persoonsgegevens en systemen. Om deze goed te kunnen blijven beveiligen, is het van belang dat er melding gemaakt kan worden van een lek zodra deze ontdekt wordt.

Vorige maand riep de Informatie Beveiliging Dienst (IBD) gemeenten op om hun Coordinated Vulnerability Disclosure (CVD) procedure nog eens goed onder de loep te nemen. Recent onderzoek van de Universiteit Twente toont aan dat meer dan de helft van de onderzochte gemeenten nog geen duidelijke CVD procedure hanteert.[1]

Een CVD procedure is een procedrue voor het melden van beveiliginsproblemen en -lekken. Het hebben van een dergelijke procedure is verplicht. Echter, uit onderzoek blijkt dat gemeenten vaak niet snel of adequaat genoeg op meldingen over beveiligingslekken reageren. Ook is er vaak geen terugkoppeling aan de melder.

Het is van belang dat de drempels voor melders — vaak ethische hackers — verlaagd worden om zo onze gegevens en systemen goed te kunnen blijven beveiligen. Daarom stelt de fractie van Student & Stad de volgende vragen:

1. Heeft de gemeente Groningen een CVD-procedure?
2. Is de meldingsprocedure duidelijk en toegankelijk gemaakt op de gemeentewebsite? Zo ja, waar is deze te vinden?
3. Hoeveel beveiligingslekken zijn er per maand bij de gemeente Groningen?
4. Binnen welke termijn wordt er gemiddeld door de gemeente Groningen gereageerd op een melding? Is dit snel genoeg?
5. Hoeveel van de gemelde beveiligingslekken wordt opgelost? Is dit voldoende?
6. Wordt er een terugkoppeling gegeven aan de melder? Zo nee, waarom niet?
7. Is het mogelijk om anoniem een melding te maken van een beveiligingslek? Zo nee, waarom niet?
8. Wat gebeurt er momenteel nog meer om beveiligingslekken te voorkomen? Is dit voldoende?

Daarnaast komt er nog meer nieuwe (Europese) wet- en regelgeving aan op het gebied van informatieveiligheid. Een daar van is de NIS2-richtlijn betreffende maatregelen voor een hoog gemeenschappelijk niveuw van cijberbeveiliging van de Europese Unie. Alle Europese lidstaten hebben tot en met eind 2024 om deze richtlijn te integreren in nationale wetgeving. Vanaf dat moment is het voor zowel publieke als private organisaties vereist om zowel een zorgplicht als een meldingsplicht te hebben van cyberbeveiligingsrisico's en -incidenten.

[1] https://ibestuur.nl/artikel/ibd-roept-gemeenten-op-eigen-cvd-procedure-te-bekijken/

De Rijksoverheid adviseert organisaties om niet af te wachten totdat de wet- en regelgeving volledig duidelijk is, aangezien de cyberbeveiligingsrisico's er nu ook al zijn. Het is van belang om goed voorbereid te zijn op de komst van de nieuwe wetgeving, door bijvoorbeeld een risicoanalyse uit te voeren.[2]

9. Is het college bekend met de nieuwe NIS2-richtlijn?
10. Wordt er al op de komst van deze nieuwe richtlijn en nationale wetgeving voorbereid? Zo nee, waarom niet? Zo ja, hoe?

Met vriendelijke groet,

Mirte Goodijk — Student & Stad

[2] https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie