Onderwerp Beantwoording vragen ex art. 36 RvO van Student & Stad over Cyberveiligheid gemeente Groningen
ter informatie

De leden van de raad van de gemeente Groningen
te
GRONINGEN

Telefoon	14 050	Bijlage(n)	1	Ons kenmerk	375612-2023
Datum	13-12-2023	Uw brief van		Uw kenmerk	-

Geachte lezer,

Hierbij doen wij u toekomen ons antwoord op de door mevrouw M. Goodijk van Student & Stad gestelde vragen ex art. 36 RvO over Cyberveiligheid gemeente Groningen. De brief van de vragensteller treft u als bijlage aan.

Wij onderschrijven dat informatie één van de voornaamste bedrijfsmiddelen is van de gemeente Groningen. Het verlies van informatie, de uitval van ICT, of het door onbevoegden kennisnemen of (bewust) manipuleren van informatie, kan ernstige gevolgen hebben voor de bedrijfsvoering en de dienstverlening aan inwoners en bedrijven. Het kan direct of indirect leiden tot maatschappelijke en/of financiële schade voor de gemeente Groningen en de partijen waarvoor de gemeente Groningen de ICT-dienstverlening verzorgt zoals de RIGG, stichting WIJ, het Noordelijk Belastingkantoor (NBK) en de GGD Groningen.

Het registreren en het tijdig opvolgen van alle typen incidenten is derhalve een wezenlijk onderdeel van de ICT-beheersing binnen de gemeente Groningen.

Beantwoording van de vragen:

1. *Heeft de gemeente Groningen een CVD-procedure?*

   Ja, gemeente Groningen heeft een Responsible Disclosure procedure (is een synoniem voor Coordinated Vulnerability Disclosure of CVD-procedure).

2. *Is de meldingsprocedure duidelijk en toegankelijk gemaakt op de gemeentewebsite? Zo ja, waar is deze te vinden?*

Ja, zie https://gemeente.groningen.nl/proclaimer#section-974.

3. *Hoeveel beveiligingslekken zijn er per maand bij de gemeente Groningen?*

Gemeente Groningen publiceert jaarlijkse het aantal informatiebeveiligingsincidenten die als mogelijk datalek kunnen worden geclassificeerd in de paragraaf bedrijfsvoering van haar jaarrekening, zie https://gemeente.groningen.nl/file/jaarrekening-2022.
In 2023 zijn 211 beveiligingsincidenten als mogelijk datalek onderzocht. Gemiddeld derhalve 18 beveiligingsincidenten per maand.

4. *Binnen welke termijn wordt er gemiddeld door de gemeente Groningen gereageerd op een melding? Is dit snel genoeg?*

Alle incidenten binnen de gemeente Groningen worden na registratie zo snel als mogelijk opgevolgd.
De categorie beveiligingsincidenten volgt dit reguliere incidentbeheerproces.
Niet alle datalekken hoeven te worden gemeld, maar de datalekken die gemeente Groningen meldt dienen binnen de wettelijke termijn van 72 uur door de Functionaris Gegevensbescherming te worden (aan)gemeld bij de Autoriteit Persoonsgegevens.
Binnen het incidentbeheerproces gelden dienstverleningsafspraken met onze ICT-leveranciers voor de volgende niveaus:

Prio	Prio label	Reactie-tijd	Feedback-tijd	Oplos-tijd*	Change confirmatie tijd
1	Kritiek	< 15 klokmin.	< ½ klokuur	< 4 klokuren	Volgende E-CAB
2	Hoog	< 1 klokuur	< 1 klokuur	< 8 klokuren	Volgende CAB
3	Middel	Volgende werkdag	n.v.t.	< 2 werkdagen	Volgende CAB +1
4	Laag	< 2 werkdagen	n.v.t.	< 5 werkdagen	In afstemming

In 2023 zijn deze dienstverleningsafspraken gemiddeld genomen conform de geldende KPI's gehaald:

Prioriteit	**Gemiddeld verstreken zakelijke duur / oplostijd *incidenten***
1 - Kritiek	3 Uur 46 Minuten 12 Seconden
2 - Hoog	3 Uur 47 Minuten 3 Seconden
3 - Matig	16 Uur 47 Minuten 16 Seconden
4 - Laag	6 Uur 45 Minuten 59 Seconden

In 2023 zijn de dienstverleningsafspraken specifiek voor de categorie beveiligingsincidenten niet altijd gehaald:

Prioriteit	**Gemiddeld verstreken zakelijke duur / oplostijd *beveiligingsincidenten***
1 - Kritiek	*11 Uur 55 Minuten 46 Seconden*
2 - Hoog	*12 Uur 33 Minuten 41 Seconden*
3 - Matig	8 Uur 35 Minuten 22 Seconden
4 - Laag	14 Uur 59 Minuten 37 Seconden

De oplostijden liggen daarbij overigens voor *alle* beveiligingsincidenten gemiddeld wel binnen de wettelijke termijn van 72 uur waarin een beveiligingsincident/datalek (alleen) gemeld dient te worden bij de Autoriteit Persoonsgegevens.

Wettelijk derhalve snel genoeg, maar conform contractuele afspraken niet altijd. Zoals we in onze brieven over de ICT-outsourcing ook hebben aangegeven, sturen we op nakoming van de contractuele verplichtingen.

5. *Hoeveel van de gemelde beveiligingslekken wordt opgelost? Is dit voldoende?*

   In principe allemaal. De doorlooptijd is soms langer dan gewenst (zie hiervoor). Meestal kunnen incidenten wel direct worden opgelost, maar heel soms zijn diepgaande analyses en/of grote wijzigingen nodig die meer oplostijd voor de incidenten vergen.

6. *Wordt er een terugkoppeling gegeven aan de melder? Zo nee, waarom niet?*

   Ja, iedere melder (intern of extern) van een (mogelijk) incident krijgt standaard de terugkoppeling binnen het reguliere incidentbeheerproces.

7. *Is het mogelijk om anoniem een melding te maken van een beveiligingslek? Zo nee, waarom niet?*

   Ja, zie ENSIA[1]-verantwoordingsvraag 7.2.1.1: *Is iedereen in staat om anoniem en veilig beveiligingsissues te kunnen melden?* Alle typen incidenten (inclusief de melding van datalekken) verlopen via het reguliere incidentbeheerproces. Telefonisch kan men anoniem een incident melden en laten registreren door de ICT-servicedesk in ServiceNow. Indien de melding echt heel gevoelig is, kan altijd (telefonisch of per e-mail) direct contact worden opgenomen met het Informatiebeveiligingsteam, de Chief Information Security Officer of de Functionaris Gegevensbescherming. Uiteraard heeft gemeente Groningen ook (algemene, interne en externe) vertrouwenspersonen die zouden kunnen worden benaderd.

8. *Wat gebeurt er momenteel nog meer om beveiligingslekken te voorkomen? Is dit voldoende?*

   Beveiligingslekken/datalekken kunnen nooit helemaal worden voorkomen, maar met de juiste aandacht voor de bewustwording van informatieveiligheid en privacy kan het aantal en de impact ervan wel worden beperkt. De gemeente Groningen besteedt hier intern veel aandacht aan onder de medewerkers.
   Zie de jaarlijkse ENSIA-verantwoording aan de gemeenteraad en ministeries voor alle activiteiten: https://gemeenteraad.groningen.nl/Documenten/ENSIA-2022-Verantwoording-Informatiebeveiliging.pdf.

9. *Is het college bekend met de nieuwe NIS2-richtlijn?*

   Wij zijn als gemeente Groningen aangehaakt in het landelijke beleidsoverleg ENSIA en het uitvoeringsoverleg ENSIA. De gemeente Groningen volgt daarmee mede de ontwikkelingen omtrent NIS2 vanuit het ministerie van Binnenlandse

[1] Gemeenten verantwoorden zich over informatiebeveiliging en informatiekwaliteit middels ENSIA. Dat staat voor *Eenduidige Normatiek Single Information Audit* (https://ensia.nl/wat-is-ensia/).

Zaken en Koninkrijksrelaties op de voet. Zodra is uitgekristalliseerd wat NIS2 voor de Nederlandse gemeenten precies gaat betekenen qua diepgang en ENSIA-verantwoordingsmethodiek zal de gemeente Groningen hieraan concreet invulling gaan geven.
Zie het recentste bericht van afgelopen week (d.d. 23 november 2023): https://www.informatiebeveiligingsdienst.nl/nieuws/gemeenten-essentieel-onder-nis-2/.

10. *Wordt er al op de komst van deze nieuwe richtlijn en nationale wetgeving voorbereid? Zo nee, waarom niet? Zo ja, hoe?*

    De verwachting is dat de komst van NIS2 met name de diepgang van de Baseline Informatiebeveiliging Overheid (BIO versie 2.0) en daarmee de ENSIA-verantwoordingsmethodiek gaat wijzigen met de toetsing van de *werking* van de huidig geldende informatiebeveiligingsmaatregelen.
    Vooralsnog gelden de huidige jaarlijkse ENSIA-vragenlijsten, op basis van BIO versie 1.0, voor de verantwoording van de status van informatiebeveiliging richting de gemeenteraad en de ministeries.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,
burgemeester en wethouders van Groningen,

burgemeester,	secretaris,
Koen Schuiling	Christien Bronda

Deze brief is elektronisch aangemaakt en daarom niet ondertekend.