Technische vragen buiten de Politieke Avond
Termijn voor beantwoording is 1 week

Onderwerp	**Digitale veiligheid van de gemeente Wageningen**
Partij	Partij voor de Dieren
Datum vragen	
Datum antwoorden	04-05-2026

23 april 2026 werd er bekend gemaakt dat er door een cyberaanval op een server in de gemeente Epe er gegevens buit zijn gemaakt van vrijwel alle inwoners, 32.000 mensen.[1] Waarbij er ook van meer dan duizend mensen een kopie van hun identiteitsbewijs is buitgemaakt. Op dezelfde dag als de bekendmaking van dit nieuws lag het systeem van onze eigen gemeente de gehele ochtend ook plat. Hierdoor was de op- en afhaal van documenten gesloten en kwamen mensen, die niet afgebeld konden worden, opdagen om verteld te worden dat ze een andere keer terug moesten komen. Door deze gebeurtenissen hebben wij enkele vragen.

Overkoepelende reactie vooraf
De gemeente neemt informatieveiligheid van de Wageningse ICT serieus. De verbeteringen op het gebied van informatieveiligheid is daarom onderdeel van het programma Digitale Organisatie. De raad wordt periodiek bijgepraat over alle ontwikkelingen rondom de Digitale Organisatie met een collegepresentatie. Gezien de gevoeligheid van sommige informatie is deze bijeenkomst besloten. Tijdens deze collegepresentatie kunnen we u meer informatie verstrekken dan via deze (openbare) beantwoording. In de hierna volgende beantwoording treft u daarom antwoorden op hoofdlijnen aan. Tijdens de volgende collegepresentatie Digitale Organisatie, op 7 september, kunnen we u in meer detail uitleg geven over maatregelen die de gemeente treft rondom informatieveiligheid/cyberdreigingen.

Vraag 1
Ziet de gemeente het risico dat er een cyberaanval, zoals bij de gemeente Epe, kan gebeuren bij haar eigen servers?
Zo ja, welke maatregelen gaat zij nemen?
Zo nee, waarom niet?

Antwoord
De gemeente Wageningen erkent dit als een risico. Geen enkele organisatie is volledig immuun voor cyberaanvallen, en dit geldt ook voor de gemeente Wageningen.

Om dit risico te beheersen, maken we gebruik van een risicogebaseerde aanpak. Dat betekent dat maatregelen worden geprioriteerd op basis van de kans op een incident en de potentiële impact ervan op de bedrijfsvoering en de dienstverlening aan onze inwoners en ondernemers. Beveiligingsmaatregelen worden afgestemd op de specifieke dreigingen en kwetsbaarheden die voor onze organisatie relevant zijn, in lijn met de overheidsbrede standaard voor informatieveiligheid, de Baseline Informatiebeveiliging

[1] Persoonsgegevens van vrijwel alle inwoners Epe gestolen bij cyberaanval

Overheid (afgekort: BIO). Deze maatregelen variëren van technische tot organisatorische aard, maar hebben ook oog voor bewustwording en menselijk gedrag. In het kader van informatieveiligheid kunnen we enkel op hoofdlijnen informatie geven over de maatregelen, gezien de openbaarheid van deze beantwoording.

We hebben – op hoofdlijnen – de volgende maatregelen genomen.

- Ketenbewustzijn
  We zijn ons bewust van de afhankelijkheden binnen de digitale keten. We maken afspraken met leveranciers en ketensamenwerkingspartners over informatiebeveiliging en risicobeheersing.
- Technische en organisatorische maatregelen, waaronder een monitoringsvoorziening voor cyberrisico's.
- Wageningen maakt gebruik van monitoringvoorziening inclusief een organisatie die continue onze systemen en netwerk in de gaten houden op verdachte activiteiten Digitale weerbaarheid van medewerkers
  Medewerkers worden getraind om phishing, social engineering en andere vormen van digitale misleiding te herkennen en te melden. Menselijk gedrag is immers een van de belangrijkste factoren waardoor informatiebeveiligingsincidenten ontstaan.

Aanvullend willen we benadrukken dat de gemeente voortdurend bezig blijft met nieuwe maatregelen treffen. Dit omdat de aard van de dreigingen voortdurend verandert, maar ook de (o.a. technische) mogelijkheden om ons daartegen te beschermen. In de eerder genoemde collegepresentatie Digitale Organisatie praten wij u hierover bij.

Vraag 2
Heeft de gemeente een adequaat plan mocht deze situatie, zoals in Epe, gebeuren in Wageningen?
Zo ja, wat is het plan?
Zo nee, waarom niet?

Antwoord
Ja, de gemeente Wageningen beschikt over een samenhangend stelsel van plannen en beleid om adequaat te kunnen reageren op een ernstig cyberincident.

De gemeente beschikt over een procedure voor datalekken en informatieveiligheidsincidenten. Bij een ernstig datalek zoals die in Epe plaatsvond, informeren we allereerst zowel de Autoriteit Persoonsgegevens als betrokkenen die getroffen worden door een datalek. Voor het goed oppakken van een cyberincident als deze heeft de gemeente een crisisstructuur, beleid en een werkwijze. Bij een ernstig cyberincident wordt opgeschaald naar een crisisteam dat de besluitvorming coördineert, de communicatie naar betrokkenen verzorgt en de samenwerking met externe partijen zoals de Informatiebeveiligingsdienst (IBD) van de VNG en het Nationaal Cyber Security Centrum (NCSC) organiseert.

De gemeente is ook proactief bezig met zowel het voorkomen als het voorbereiden op een cyberincident:

- Zo oefent de gemeente ook dit soort situaties met functionarissen, management en bestuurlijk portefeuillehouders. De geleerde lessen uit deze oefeningen worden ook weer gebruikt om beleid, plannen en werkwijze te verbeteren;

- Tot slot vindt er elk half jaar een risico-inventarisatie plaats van cyberdreigingen. Daarbij kijken we onder andere naar actuele cyberdreigingen en welke maatregelen de gemeente hier kan en moet nemen.

Vraag 3
Heeft de gemeente contact met andere gemeentes/organisaties over digitale veiligheid om te leren van de situaties die zich hebben voorgedaan bij andere gemeentes/organisaties?
Zo ja, wordt hier vaak waardevolle informatie verkregen om de digitale veiligheid van de gemeente te verbeteren?
Zo nee, waarom heeft de gemeente geen contact met andere gemeentes/organisaties om te leren van hun situaties?

Antwoord
Ja, de gemeente Wageningen neemt actief deel aan verschillende samenwerkingsverbanden op het gebied van informatiebeveiliging. Kennisdeling met andere gemeenten en gespecialiseerde organisaties is belangrijk, omdat dreigingen voortdurend evolueren en leren van elkaars ervaringen de weerbaarheid van alle deelnemers vergroot.

De gemeente neemt deel aan en organiseert een regionaal overleg waarin CISO's (chief information security officers) van omliggende gemeenten bijeenkomen. In dit overleg wordt informatie over actuele dreigingen en incidenten bij andere gemeenten met elkaar gedeeld.

Als lid van de Vereniging van Nederlandse Gemeenten (VNG) maakt de gemeente gebruik van de diensten van de Informatiebeveiligingsdienst (IBD). De IBD voorziet gemeenten van dreigingsinformatie, beveiligingsadviezen, handreikingen en ondersteuning bij incidenten. Informatie over incidenten bij andere gemeenten, zoals in Epe, wordt via dit kanaal gedeeld en geanalyseerd.

De leverancier van onze monitoringsvoorziening (voor verdachte activiteiten binnen het Wagenings ICT-netwerk) deelt actief dreigingsinformatie en analyses op basis van wat zij waarnemen binnen hun bredere klantenkring. Dit vergroot het situationeel bewustzijn van de gemeente en versnelt het ontdekken van nieuwe aanvalsmethoden.

Vraag 4
Is er een verband tussen de cyberaanval op een server van de gemeente Epe en de storing in het systeem van onze eigen gemeente?
Zo ja, wat is het verband?
Zo nee, is het al bekend hoe de storing in het systeem van Wageningen is ontstaan?

Antwoord
Er is geen verband tussen de cyberaanval op de gemeente Epe en de storing die zich in Wageningen heeft voorgedaan. Het betreft twee volledig van elkaar losstaande situaties met een geheel verschillende oorzaak en systeem.

Bij de gemeente Epe was sprake van een cyberaanval, waarbij kwaadwillende hackers informatie van het netwerk van de gemeente hebben gestolen.

De storing in Wageningen was het gevolg van een technische storing. De storing trof specifiek de fysieke computers. Dit hangt samen met het feit dat de balie afhankelijk is van fysieke werkstations die direct gekoppeld zijn aan randapparatuur, zoals printers, scanners en vingerafdrukapparatuur voor het verwerken van documenten en identiteitsbewijzen. Uitwijken naar alternatieve apparatuur was daardoor niet meer mogelijk.

Vraag 5
Heeft de gemeente geprobeerd om inwoners te laten weten dat er, desbetreffende ochtend een storing was in hun systeem?
Zo ja, op welke wijze?
Zo nee, waarom niet?

Antwoord
Inwoners die op die ochtend het Stadhuis bezochten, werden bij de aanmeldzuil direct geïnformeerd over de storing. Bezoekers met een afspraak werden geadviseerd op een later moment terug te komen. Dit was de enige actieve communicatie die op dat moment mogelijk was.

De afspraakgegevens van inwoners waren beschikbaar, maar op het moment van de storing was de kennis om deze gegevens te raadplegen niet direct voorhanden. Hierdoor kon de gemeente inwoners met een afspraak niet tijdig telefonisch informeren over de storing en hen adviseren op een later moment terug te komen. Hoe de gemeente voortaan wel snel kan beschikken over deze afspraakgegevens wordt meegenomen binnen het werkoverleg van publieke dienstverlening.

Zodra de storing was verholpen, zijn inwoners van wie de afspraak die ochtend geen doorgang kon vinden, nog diezelfde dag geholpen. We hebben er daarmee voor gezorgd dat de vertraging voor betrokken inwoners zo beperkt mogelijk bleef en zij niet op een andere dag hoefden terug te komen.