Nr. RV19.0013 (2019)

Beantwoording van de schriftelijke vragen, gesteld door de fractie GroenLinks betreffende Cybersecurity

Aan de fractie GroenLinks
i.a.a. de leden van de Gemeenteraad

Op 29 januari 2019 heeft u onder verwijzing naar artikel 36 van het reglement van orde voor de vergaderingen van de raad, de navolgende vragen gesteld over Cybersecurity, het antwoord vindt u onder de vraag:

1. Hoe is de controle op de cybersecurity van gemeentelijke systemen (zowel intern als die waar ook burgers gebruik van kunnen maken) georganiseerd?

De cybersecurity van gemeentelijke systemen in Den Helder voor zowel intern gebruik als gebruik door burgers, en de controle daarop, is afhankelijk van het classificatieniveau van de systemen georganiseerd. Grofweg kan worden gesteld dat systemen die lager geclassificeerde gegevens bevatten een lager beschermingsniveau en toezichtregime hebben dan systemen die hoger geclassificeerde gegevens bevatten.

Bijvoorbeeld: het grootschalige uitwisselen van persoonsgegevens vindt alleen plaats binnen besloten overheidsnetwerken. Deze netwerken worden door de instanties die deze netwerken beschikbaar stellen gemonitord. Voorbeelden hiervan zijn het landelijke netwerk Basis Registratie Personen van de Rijksdienst voor Identiteitsgegevens (RvIG) en het landelijk netwerk voor Werk en Inkomen gegevens van het Bureau Ketensamenwerking Werk en Inkomen (BKWI).

Systemen waarvan burgers gebruik kunnen maken zijn via de gemeentelijke website toegankelijk. Wanneer het om geclassificeerde gegevens gaat dan zijn landelijk voorgeschreven beveiligingsmaatregelen van toepassing. Een voorbeeld hiervan is het gebruik van DigiD.

Naast de technische inrichting van ICT-systemen en controle is security ook een kwestie van goed gebruik van systemen, software die up to date is en gedrag van medewerkers dat gericht is op het voorkomen van datalekken. Binnen de gemeentelijke organisatie ligt hier grote focus.

2. Wie is verantwoordelijk voor de cybersecurity?

Op het niveau van het dagelijkse gebruik van systemen, gegevens en de uitwisseling van deze gegevens is het lijnmanagement verantwoordelijk. Het betreft hier een integrale verantwoordelijkheid voor het creëren, opslaan, verwerken en distribueren van gegevens.

Op stafniveau zijn enkele toezichthoudende en coördinerende rollen ingericht. Het gaat hier om de rollen Functionaris Gegevensbescherming (FG) en Concern Information Security Officer (Ciso).

Het IT team is in technische zin verantwoordelijk voor de aanleg en beveiliging van het gemeentelijke netwerk en de koppelingen met ketenpartners.

Eindverantwoordelijk op ambtelijk niveau is de gemeentesecretaris.

Het college van B&W is op bestuurlijk niveau verantwoordelijk. Het college verantwoord zich jaarlijks middels de Enkelvoudige Normatiek Single Information Audit (ENSIA) aan de gemeenteraad. De verantwoording is onderdeel van de jaarrekening.

3. Hoe is de cybersecurity tussen de gemeente en private partijen (PPS) geborgd?

Cybersecurity is in opzet middels contracten, dienstenovereenkomsten, convenanten, en dergelijke, geregeld. De gemeente koopt in principe in conform richtlijnen van instituties als de Vereniging Nederlandse Gemeenten (VNG) en de Informatie Beveiliging Dienst (IBD). Uitzondering hierop zijn partijen die enkel conform eigen leveringscondities aanbieden zoals telecomproviders.

4. Worden er ook penetratietesten uitgevoerd (= bedrijf opdracht geven om ethisch te hacken om te controleren of er beveiligingsgaten gedicht moeten worden)?

Ja, dit gebeurd. De resultaten van ethische hacks zijn vertrouwelijk omdat mogelijke zwakheden in het beveiligingssysteem niet openbaar mogen worden gemaakt.

5. Wat wordt gedaan aan bevordering van digitale awareness bij de medewerkers?

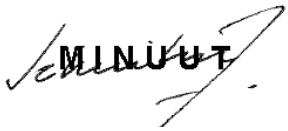
De medewerkers voor wie dat van toepassing is worden bij aanvang van de werkzaamheden uitgelegd hoe de werkprocessen verlopen, dat het gebruik van systemen gemonitord kan worden, en dat er informatieveiligheid- en privacyregels van toepassing kunnen zijn.

De opgedane kennis wordt up tot date gehouden middels bijscholing. Deze bijscholing wordt veelal aangeboden in de vorm van externe nieuwsbrieven, kwaliteitsbrochures en (interne) communicatiecampagnes. Intern worden er actualiteitencolleges georganiseerd en worden laagdrempelige campagnes via bijvoorbeeld intranet gepubliceerd. In specifieke domeinen of voor specifieke vraagstukken worden (inhouse) trainingen gevolgd.

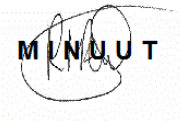
Wij vertrouwen erop u met vorenstaande voldoende te hebben geïnformeerd.

Den Helder, 5 maart 2019

Burgemeester en Wethouders van Den Helder,



burgemeester
Koen Schuiling



secretaris
Robert Reus