gemeente
Den Helder

Gemeenteraad Den Helder
Postbus 36
1780 AA DEN HELDER

verzendgegevens	behandeld door	uw gegevens
datum : 29-08-2016	dhr. M. Versteeg	brief van :
kenmerk : AU16.06367	telefoon (0223) 67 8106	kenmerk :

onderwerp
Rekenkamerbrief onderzoek digitale velligheid

Geachte leden van de raad,

De opmars van de digitalisering heeft bij gemeenten geleid tot een sterk toegenomen hoeveelheid digitale gegevens en een toenemende uitwisseling van persoonsgegevens in het kader van de dienstverlening. Als gevolg hiervan wordt digitale informatiebeveiliging steeds belangrijker voor gemeenten, ook vanwege het toenemend aantal cyberaanvallen.

Binnen gemeenten is de laatste jaren dan ook steeds meer aandacht gekomen voor beveiliging van digitale systemen, netwerken en gegevens. Daarbij staan twee thema's centraal, namelijk bescherming tegen inbraak en bescherming van de privacy. Gemeenten moeten met betrekking tot het laatstgenoemde punt een goede balans zien te zoeken tussen een werkbare gegevensuitwisseling en een adequate bescherming van de privacy van burgers. Gegevens van burgers, bedrijven en instellingen moeten bij de overheid in goede handen zijn. Dat is de essentie van het vertrouwen dat men in de overheid moet kunnen stellen.

De ontwikkelingen op het gebied van informatieveiligheid vormden voor de Rekenkamercommissie Den Helder (RKC) aanleiding om onderzoek te doen naar de staat van de informatiebeveiliging van de gemeente Den Helder. Daarbij heeft de RKC de effectiviteit van de door de gemeente Den Helder genomen maatregelen ter bescherming van gevoelige informatie en gegevens van burgers in ogenschouw genomen.

Normaliter wordt u bij de start van een rekenkameronderzoek door de RKC in kennis gesteld van de onderzoeksopzet en planning van de werkzaamheden. Bij dit onderzoek is gekozen voor een andere werkwijze. Wij hebben aanvankelijk uitsluitend de burgemeester en de gemeentesecretaris op de hoogte gesteld van het onderzoek. Hiervoor is bewust gekozen, omdat de alertheid van de (ambtelijke) organisatie onderdeel uitmaakte van het onderzoek. Dit kan alleen functioneren wanneer het aantal betrokkenen vanuit de organisatie op voorhand zo beperkt mogelijk is.

In het regulier overleg tussen uw fractievoorzitters en de RKC, op 18 april 2016, zijn de fractievoorzitters in kennis gesteld van de uitvoering en de hoofdlijnen van het onderzoek. Daarbij is aangegeven dat de voltallige raad op een later moment via een rekenkamerbrief zou worden geïnformeerd. Door middel van voorliggende rekenkamerbrief informeren wij u over de uitkomsten van het onderzoek. Hierbij gaan wij achtereenvolgens in op:
- Inrichting en verloop van het onderzoek
- Uitkomsten van het onderzoek
- Reactie van het college

- Proces van deze rekenkamerbrief

Inrichting en verloop van het onderzoek
Op 18 december 2015 is aan het bureau Hoffmann, gespecialiseerd in bedrijfsrecherche, de opdracht verstrekt het onderzoek uit te voeren. Het onderzoek is voornamelijk in de maanden januari en februari 2016 uitgevoerd (voor wat betreft de dataverzameling). De werkzaamheden van het bureau bestonden onder meer uit:
- Testen van de informatiebeveiliging van de gemeente Den Helder vanaf het internet
- Testen van de informatiebeveiliging van de gemeente Den Helder vanaf het lokale netwerk
- Identificeren van het draadloos netwerk van de gemeente Den Helder en het testen van de beveiliging ervan
- Testen van de security awareness van medewerkers van de gemeente Den Helder.

Concreet is door twee ethische hackers vanuit het bureau een penetratietest uitgevoerd op de interne- en externe informatiesystemen van de gemeente Den Helder. Naast de penetratietest is ook een zogenaamde 'phishing actie' uitgevoerd. Hierbij is een e-mail verstuurd aan alle medewerkers van de gemeente Den Helder. In de e-mail werden de medewerkers naar een externe website 'gelokt', waar hen vervolgens werd gevraagd de gemeentelijke inloggegevens in te voeren in ruil voor een gratis presentje. Het doel van de phishing actie was het bevorderen van bewustzijn en alertheid op deze veel voorkomende vorm van cybercrime. Ten slotte is ook het wifi-netwerk van de gemeente getest.

Gedurende de tweede dag van het onderzoek werden de hackers opgemerkt door de systeembeheerder van de gemeente Den Helder. Hierop is adequaat actie ondernomen door de systeembeheerder. Ten aanzien van de phishing actie heeft het team ICT direct een bericht rondgestuurd in de organisatie, waarin melding werd gemaakt van phishing en hoe te handelen. Ook is op het intranet een waarschuwing geplaatst voor medewerkers en werden medewerkers verplicht tot het wijzigen van hun wachtwoord voor toegang tot het netwerk. Een dag na de phishing actie is de externe website waarnaar werd verwezen geblokkeerd.

Uitkomsten van het onderzoek
De uitkomsten van het onderzoek zijn door de onderzoekers opgenomen in een vertrouwelijke rapportage. In deze rapportage is beschreven welke constateringen de onderzoekers hebben gedaan en op welke wijze zij daartoe zijn gekomen. Vanzelfsprekend is de inhoud van een dergelijke rapportage gezien de risico's niet geschikt voor enige vorm van publicatie. Wij hebben de onderzoekers verzocht om hun bevindingen toe te lichten aan het college van burgemeester en wethouders en vanwege de technische aard van de materie met name ook aan de betrokken ambtenaren. Tijdens deze bijeenkomst op 13 april 2016 is afgesproken dat de organisatie beperkt de tijd zou krijgen om de noodzakelijke maatregelen te treffen. De rapportage zelf is hierna door betrokkenen van de RKC verwijderd van hun computers en overgedragen aan de professionals in de gemeentelijke organisatie.

Het college heeft vervolgens op 23 mei 2016 schriftelijk gereageerd op het onderzoeksrapport. Op 6 juni 2016 heeft een vervolgbijeenkomst plaatsgevonden met de wethouder Informatiebeveiliging en betrokken medewerkers. Tijdens deze bijeenkomst is de RKC op de hoogte gesteld van de opvolging die aan de uitkomsten van het onderzoek is gegeven. De ambtelijke organisatie kon aantonen dat de constateringen uit het onderzoek adequaat zijn opgepakt. Zaken die nog wel nadere uitwerking nodig hadden, vereisten veelal overleg met leveranciers van software. Het navolgende schema is aan ons verstrekt door het college en geeft op hoofdlijnen inzicht in het aantal issues en de reeds opgeloste issues.

Prioriteit	Aantal	Opgelost	(Nog) niet opgelost
Hoog	21	14	Onderdelen van de 7 resterende bevindingen zijn reeds opgelost. Het overige gedeelte van deze bevindingen wordt in samenwerking met leveranciers opgelost. In het gesprek van 6 juni lichten wij de planning toe.
Midden	11	10	**Onderdelen van 1 resterende bevinding** zijn **opgelost. Het overige gedeelte van deze bevinding** wordt in samenwerking met de leverancier opgelost.
Laag	8	7	De oplossing van 1 resterende bevinding is in beeld.
Totaal	40	31	9

Tabel: Bevindingen beveiligingsonderzoek **stand van** zaken 23 mei 2016

Uit het onderzoek komt resumerend naar voren dat de beveiliging van de (informatie)systemen van de gemeente Den Helder op orde lijkt te zijn voor aanvallen van buitenaf (via het internet). Ook de beveiliging van het gemeentelijk wifi-netwerk bleek op orde. De beveiliging van de (informatie)systemen voor aanvallen vanaf het gemeentelijk netwerk (van binnenuit) was op onderdelen voor verbetering vatbaar.

Het organisatiebewustzijn omtrent cybercrime kan worden versterkt. Naar aanleiding van de verstuurde phishingmail en het relatief grote aantal reacties daarop, blijkt dat er noodzaak is de alertheid van medewerkers op dit punt verder aan te scherpen. Begin 2015 is de gemeente Den Helder gestart met een bewustwordingscampagne. Het college geeft aan dat deze campagne in 2016 wordt gecontinueerd en geïntensiveerd.

Reactie van het college
Het college heeft laten weten content te zijn met het initiatief van het onderzoek en waardeert de concrete uitkomsten ervan. Naar aanleiding van het rapport geeft het college aan voornemens te zijn op eigen initiatief en op reguliere basis beveiligingsonderzoeken te laten uitvoeren door een extern bureau, om nu en in de toekomst toe te zien op de veiligheid van (informatie)systemen. Voorkomen is immers beter dan genezen.

Proces van deze rekenkamerbrief
Wij bevelen de gemeenteraad van Den Helder aan deze rekenkamerbrief te behandelen in de raadscommissie en het college te vragen regulier (minimaal jaarlijks) te rapporteren over de ondernomen acties en de stand van zaken in de gemeente Den Helder ten aanzien van digitale veiligheid.

Indien u vragen heeft over deze rekenkamerbrief, kunt u contact opnemen met de heer mr. K.A.J.E. Kirpensteijn via de secretaris van de rekenkamercommissie, de heer M. Versteeg.

Hoogachtend,
de voorzitter van de Rekenkamercommissie Den Helder

drs. R.J. Morée MBA