Rekenkamercommissie Vallei en Veluwerand

P/a Gemeente Barneveld
Postbus 63
3770 AB Barneveld
Tel: 14 0342

Gemeenteraad Zeewolde
Postbus 1
3890 AA Zeewolde

Barneveld, 6 maart 2019

Ons kenmerk:		**verzonden op:**	Per e-mail op 7 maart 2019
Behandelend ambtenaar:	Ingrid Spoor		
Doorkiesnummer:	0342-495830	**e-mailadres:**	i.spoor@barneveld.nl
Uw brief van:		**met kenmerk:**	
Bijlage(n):	2		
Onderwerp:	Rekenkameronderzoek digitale veiligheid Zeewolde		

Geachte gemeenteraad,

Gemeenten beschikken over veel vertrouwelijke gegevens van onder andere burgers en bedrijven. Met de toenemende digitalisering van de samenleving en de koppeling van informatie, wordt digitale veiligheid voor gemeenten steeds belangrijker. Medio 2018 heeft de rekenkamercommissie daarom in overleg met de auditcommissie van de raad een onderzoek uitgevoerd naar diverse aspecten van de digitale veiligheid van de gemeente Zeewolde. Hiertoe hebben wij de veiligheid van de ICT-systemen van de gemeente Zeewolde getest met behulp van professionele hackers van het bureau Hoffmann Bedrijfsrecherche BV.

Naar aanleiding van het onderzoek heeft Hoffmann in samenwerking met de rekenkamercommissie een rapportage opgesteld, met conclusies en aanbevelingen. Deze rapportage heeft de rekenkamercommissie overgenomen. In overleg met de griffier en de gemeentesecretaris hebben wij op de rapportage en de bestuurlijke reactie en de behandeling daarvan geheimhouding opgelegd, op grond van artikel 6 lid 2 van onze verordening[1]. Verderop in deze brief gaan wij nader in op de argumentatie hiervoor.

Wij adviseren de gemeenteraad om in te stemmen met alle in de rapportage genoemde aanbevelingen en erop toe te zien dat het college de aanbevelingen uitvoert. Het college heeft in zijn bestuurlijke reactie op de rapportage van Hoffmann aangegeven de aanbevelingen op één na over te nemen. De meest urgente aanbevelingen zijn direct uitgevoerd door het college. De rekenkamercommissie is verheugd dat het onderzoek op deze wijze direct bijdraagt aan het verbeteren van de digitale veiligheid. Met betrekking tot de aanbeveling die het college niet overneemt, heeft het college aangegeven dat zij een alternatieve werkwijze hanteert, die zich heeft bewezen. Van de onderzoekers van Hoffmann hebben wij echter begrepen dat deze werkwijze het risico niet volledig wegneemt. Daarom adviseren wij het college de gemaakte keuze te heroverwegen.

Het onderzoek
Bij een onderzoek op het terrein van digitale veiligheid gaat het in de regel om een vrij technisch onderzoek. Dat is in dit onderzoek bij de gemeente Zeewolde niet anders, het richt zich op de informatiesystemen van de gemeente. Doel van het onderzoek was om te toetsen of de

[1] *Verordening gemeenschappelijke Rekenkamercommissie Vallei en Veluwerand, 2014*

informatiesystemen van de gemeente voldoende beveiligd zijn tegen het risico van hacken. Hackers van Hoffmann Bedrijfsrecherche hebben de informatiebeveiliging zowel getest vanaf het internet (externe penetratietest) als vanuit het gemeentehuis (interne penetratietest).
Ook is het bewustzijn van medewerkers, bestuurders en raadsleden getest door middel van spear-phishing, voice-phishing en USB-keydrop. Bij de spear-phishing is een e-mail met malware[2] verstuurd aan een specifieke groep waarbij men verzocht wordt om op een link te klikken waardoor de hackers toegang krijgen tot de systemen van de gemeente. Bij de voice-phishing hebben de hackers telefonisch geprobeerd om gevoelige informatie van de medewerkers of de organisatie te bemachtigen, zoals een gebruikersnaam en wachtwoord. Bij de USB-keydrop is een USB stick met malware[1] binnen de gemeente achtergelaten met de bedoeling dat deze door medewerkers in een pc gedaan wordt en dat hierdoor door de hackers op afstand toegang wordt verkregen tot de systemen. Ook is een fysieke inlooptest gedaan. Hierbij heeft een medewerker van Hoffmann geprobeerd om zonder toestemming binnen te komen bij de gemeentelijke werkplekken.

Toestemming voor onderzoek
Omdat het bij dit onderzoek ging om een poging tot “digitale inbraak” en om eventuele schade tijdens het onderzoek te kunnen beperken, hebben wij vooraf overleg gehad met de gemeente. De gemeentesecretaris, de directeur van Meerinzicht[3] en de externe beheerders van de website hebben vooraf toestemming gegeven voor de uitvoering van het onderzoek. Voor en tijdens het onderzoek hebben wij daarnaast nauw contact onderhouden met de afdelingsmanager Informatisering en Automatisering van Meerinzicht. Wij hebben betrokkenen nadrukkelijk gevraagd om geen ruchtbaarheid te geven aan het onderzoek. In het belang van het onderzoek was het noodzakelijk dat zo min mogelijk mensen op de hoogte zouden zijn. Dit is goed nageleefd.

Rapportage van Hoffmann Bedrijfsrecherche BV
De rapportage is opgesteld door het externe Bureau Hoffmann in opdracht van, en in samenwerking met, de rekenkamercommissie. Conform het onderzoeksprotocol is deze rapportage aan de gemeentelijke organisatie voorgelegd voor technische reactie met de vraag om aan te geven of er feitelijke onjuistheden in de rapportage staan. In afwijking van onze gebruikelijke werkwijze stonden in de rapportage ook al conclusies en aanbevelingen. De reden hiervoor is dat de rekenkamercommissie het van belang vond deze al te delen met de ambtelijke organisatie, zodat deze meteen al aan de slag kon gaan met geconstateerde kwetsbaarheden. Naar aanleiding van de technische reactie is nog een aantal correcties aangebracht in de rapportage. Daarna is de rapportage van Hoffmann definitief gemaakt en is deze aan het college aangeboden voor een bestuurlijke reactie. Op de bestuurlijke reactie is evenals op de rapportage en de behandeling daarvan, door de rekenkamercommissie geheimhouding opgelegd.

Conclusies
Binnen de beschikbare tijd voor dit onderzoek is het de onderzoekers (hackers) niet gelukt vanaf het internet zonder voorkennis ongeautoriseerde toegang te verkrijgen tot de systemen van de gemeente Zeewolde. Ook is het de hackers niet gelukt om binnen het interne netwerk ongeautoriseerd toegang te verkrijgen. Wel hebben de onderzoekers na het inloggen met een aangeleverd gebruikersaccount een aantal kwetsbaarheden gevonden. In de rapportage zijn deze nader omschreven en zijn aanbevelingen gedaan om de kwetsbaarheden op te lossen. Uit het onderzoek bleek dat een medewerker gevoelig was

[2] *Malware is software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot computersystemen. Het woord is een samentrekking van het Engelse malicious software (kwaadaardige software).*
[3] *Binnen het samenwerkingsverband Meerinzicht werkt de gemeente Zeewolde o.a. op het gebied van ICT samen met de gemeente Ermelo en Harderwijk.*

voor de voice-phishing, waardoor een geldige logincombinatie achterhaald werd die misbruikt kon worden. De gestuurde spear-phishing e-mails zijn in de spam mailbox van de gemeente terecht gekomen en hebben de medewerkers, bestuurders en raadsleden niet bereikt. Van de achtergelaten USB sticks is er één in een computer gestopt, maar door technische maatregelen werd deze gelijk gedetecteerd en werd de malware niet uitgevoerd.

Tijdens de inlooptest is gebleken dat het mogelijk was om fysieke toegang te verkrijgen tot niet-openbare werkplekken en toegang te krijgen tot dossiers en poststukken. Dit komt overeen met de ervaring van Hoffmann bij andere gemeenten. In de praktijk lukt het vrijwel altijd om tijdens een fysieke inlooptest binnen te komen.

Het rekenkameronderzoek was gericht op het vinden van zwakke plekken en verbeterpunten in de beveiliging. Zoals altijd bij dergelijk onderzoek zijn er ook bij de gemeente Zeewolde kwetsbaarheden en zwakke plekken gevonden. Per kwetsbaarbaarheid hebben wij een aanbeveling ter verbetering geformuleerd. Graag wijzen wij u erop dat 100% veiligheid niet bestaat, aangezien dit in de praktijk onwerkbaar en onbetaalbaar zou zijn, maar ook omdat nu eenmaal niet alle risico's in beeld zijn. Het is van belang dat de gemeente adequate maatregelen neemt om de grootste risico's te beperken en ervoor te zorgen dat men bewuste keuzes maakt in de mate van veiligheid versus werkbaarheid en financiën.

Aanbevelingen
Op basis van het onderzoek adviseert de rekenkamercommissie de gemeente Zeewolde diverse maatregelen op het gebied van mens en techniek, waarbij de ene maatregel belangrijker is dan de ander. Hierbij kan men denken aan maatregelen die bevorderen dat medewerkers alert zijn op het gebruik van phishingmethoden en ook dat zij weten hoe daarop te reageren. Verder worden ook technische maatregelen aanbevolen om bijvoorbeeld toegang tot systemen te beperken en risico's te minimaliseren. Voor een uitgebreider overzicht van conclusies en aanbevelingen verwijzen wij u naar de geheime rapportage van Hoffmann.

Rapport Hoffmann geheim
Na een grondige afweging is de rekenkamercommissie van mening dat openbaarmaking van het rapport het belang van de gemeente Zeewolde kan schaden. Het rapport bevat gedetailleerde informatie over de architectuur van de ICT-systemen. Het is uit veiligheidsoverwegingen zeer ongewenst dat deze gegevens bij een grotere groep bekend worden. Bovendien zouden bepaalde details uit het rapport kwaadwillenden op een idee kunnen brengen. Dit geldt ook voor de bestuurlijke reactie van het college. De rekenkamercommissie legt daarom geheimhouding op omtrent de inhoud van de rapportage van Hoffmann, de bestuurlijke reactie van het college en op hetgeen hierover in de vergadering wordt besproken, op basis van art. 6 lid 2 van de Verordening[4]. De motivering hiervoor is gelegen in art.10 lid 2 sub b Wet openbaarheid van bestuur.

Tot slot
Gebruikelijk is dat de rekenkamercommissie zo'n twee tot drie jaar na het afronden van een rekenkameronderzoek een zogenaamd doorwerkingsonderzoek doet. Tijdens zo'n doorwerkingsonderzoek kijkt de rekenkamercommissie wat er is gebeurd met de aanbevelingen die de gemeenteraad heeft overgenomen. Tegen die tijd zullen wij na overleg met (een afvaardiging vanuit) de

[4] *Verordening gemeenschappelijke Rekenkamercommissie Vallei en Veluwerand, 2014*

gemeenteraad bepalen of een doorwerkingsonderzoek zinvol is en hoe een dergelijk onderzoek er dan uit zou moeten zien.

Graag willen wij de ambtelijke organisatie bedanken voor de goede medewerking voorafgaand, tijdens en na afronding van het feitenonderzoek.

Met vriendelijke groet,

De heer drs. J. van Zomeren
Voorzitter rekenkamercommissie
Vallei en Veluwerand

Mevrouw ir. I.M.T. Spoor
Secretaris/onderzoeker rekenkamercommissie
Vallei en Veluwerand

cc: College van burgemeester en wethouders van de gemeente Zeewolde

Bijlagen:
- Rapportage van Hoffmann, Onderzoek informatiebeveiliging gemeente Zeewolde, d.d. 07-03-2019 (GEHEIM)
- Bestuurlijke reactie college B&W Zeewolde d.d. 23 -01-2019 (GEHEIM)