Rekenkamercommissie Vallei en Veluwerand

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

Gemeenteraad Bunnik
Postbus 5
3980 CA Bunnik

Barneveld, 21 november 2018

Ons kenmerk:	Zaaknummer 627168	**verzonden op:**	Per e-mail op 21 november 2018
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 Bunnik		

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. In de eerste helft van 2018 heeft de rekenkamercommissie daarom een onderzoek uitgevoerd naar diverse aspecten van de digitale veiligheid van de gemeente Bunnik. Hiertoe hebben wij de veiligheid van de ICT-systemen van de gemeente Bunnik 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 (ad interim) en de gemeentesecretaris hebben wij de rapportage op grond van artikel 10 van de WOB als niet-openbaar aangemerkt. De rapportage ligt ter inzage bij de griffie. Verderop in deze brief gaan wij nader in op de argumentatie hiervoor.

Wij adviseren de gemeenteraad om in te stemmen met alle aanbevelingen uit de rapportage en erop toe te zien dat het college de aanbevelingen uitvoert. Het college heeft in zijn bestuurlijke reactie op de rapportage van Hoffmann (zie bijlage bij deze brief) aangegeven de aanbevelingen over te nemen en om te zetten in maatregelen. De meest urgente maatregelen 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.

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 Bunnik niet anders, het richt zich op de informatiesystemen van de gemeente . Doel van het onderzoek was om te toetsen of de 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 test) als vanaf het lokale netwerk (interne test). In beide gevallen hebben de hackers geprobeerd op verschillende manieren bij de gemeente toegang te krijgen tot de systemen: zonder voorkennis van de infrastructuur en zonder gebruikersaccount (blackbox) en vervolgens ook met een valide - in rechten beperkt - gebruikersaccount (greybox). Ook is het bewustzijn van medewerkers getest door middel van

mail-phishing en voice-phishing. Bij de mail-phishing is een valse e-mail verstuurd naar de medewerkers met het doel om inloggegevens te achterhalen. 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. 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 gemeentesecretaris. De gemeentesecretaris en de externe beheerder 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 beleidsadviseur Informatie en de coördinator informatieveiligheid (CISO) van de gemeente Bunnik. 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 men meteen al aan de slag kon gaan met geconstateerde kwetsbaarheden. Naar aanleiding van de technische reactie zijn 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 (zie bijlage bij deze brief).

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 Bunnik. Wel hebben de onderzoekers diverse kwetsbaarheden gevonden. Zo waren er bijvoorbeeld systemen waarbij een beveiligingsupdate ontbrak. Uit het onderzoek bleek ook dat enkele medewerkers gevoelig waren voor zowel de voice-phishing als de mail-phishing. Dit komt overigens overeen met ervaringen die de onderzoekers hebben bij andere organisaties en gemeenten.

Tijdens de inlooptest is gebleken dat het mogelijk was om fysieke toegang te verkrijgen tot de beveiligde kantoorruimtes van de gemeente Bunnik. Ook 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 Bunnik 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 Bunnik een integraal pakket aan maatregelen op het gebied van mens, techniek en organisatie. Hierbij kan men denken aan maatregelen die bevorderen dat medewerkers alert zijn op het gebruik van mail-phisingmethoden en ook dat zij weten hoe daarop te reageren. Verder technische maatregelen om zaken af te dwingen, te monitoren en organisatorische maatregelen om de technische aanbevelingen op te volgen en uit te voeren. Voor een uitgebreider overzicht van conclusies en aanbevelingen verwijzen wij u naar de niet-openbare rapportage van Hoffmann.

Rapport Hoffmann niet-openbaar
Na een grondige afweging is de rekenkamercommissie van mening dat openbaarmaking van het rapport het belang van de gemeente Bunnik 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. De rekenkamercommissie adviseert de raad te besluiten geheimhouding op te leggen op de inhoud van de rapportage van Hoffmann en op hetgeen hierover in de vergadering wordt besproken, op basis van art. 25 lid 1 Gemeentewet. 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 gemeenteraad bepalen of een doorwerkingsonderzoek zinvol is en hoe een dergelijk onderzoek er dan uit zou moeten zien. Denkbaar is bijvoorbeeld dat de gemeente besluit om binnen twee jaar een herhaalonderzoek te doen. Een evaluatie van onze kant is dan minder zinvol.

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 Bunnik

Bijlagen:
- Rapportage van Hoffmann, Onderzoek informatiebeveiliging gemeente Bunnik, d.d. 03-07-2018 (NIET OPENBAAR)
- Bestuurlijke reactie college B&W Bunnik d.d. 19 sep 2018