Rekenkamercommissie Vallei en Veluwerand

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

Gemeenteraad Barneveld
Postbus 63
3770 AB Barneveld

Barneveld, 8 februari 2017

Ons kenmerk:	1035655	**verzonden op:**	8 februari 2017
Behandelend ambtenaar:	B. Meijboom		
Doorkiesnummer:	0342 - 495 384	**e-mailadres:**	b.meijboom@barneveld.nl
Uw brief van:		**met kenmerk:**	
Bijlage(n):	niet-openbare rapportage van Hoffmann		
Onderwerp:	rekenkameronderzoek digitale veiligheid Barneveld		

Beste leden van de gemeenteraad,

Gemeenten beschikken over veel vertrouwelijke gegevens van 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 2016 heeft de rekenkamercommissie daarom een onderzoek uitgevoerd naar diverse aspecten van de digitale veiligheid van de gemeente Barneveld. Hiertoe hebben wij de veiligheid van de ICT-systemen van de gemeente Barneveld getest met behulp van professionele hackers van het bureau Hoffmann Bedrijfsrecherche BV.

Naar aanleiding van het onderzoek heeft Hoffmann op verzoek van de rekenkamercommissie en in nauwe samenwerking met de rekenkamercommissie een uitgebreide rapportage opgesteld, met conclusies en aanbevelingen. Deze rapportage heeft de rekenkamercommissie overgenomen. In nauw overleg met de griffier en de gemeentesecretaris hebben wij de rapportage op grond van artikel 10 van de WOB als niet-openbaar aangemerkt. De rapportage is vergrendeld met een wachtwoord, dat bij de griffier op te vragen is. Verderop in deze brief gaan wij nader in op de argumentatie hiervoor.

Wij adviseren de gemeenteraad om akkoord te gaan met alle aanbevelingen uit de rapportage en erop toe te zien dat het college de aanbevelingen uitvoert. Het college heeft in haar bestuurlijke reactie op de rapportage van Hoffmann aangegeven alle aanbevelingen over te willen nemen. Verderop in deze brief gaan wij hier nader op in.

Het onderzoek
Het gaat om een vrij technisch onderzoek, gericht op de informatiesystemen van de gemeente Barneveld. Doel van het onderzoek was om te toetsen of de informatiesystemen van de gemeente Barneveld 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 binnen te komen zonder voorkennis van de infrastructuur en zonder gebruikersaccount (blackbox), en vervolgens ook met een valide - in rechten beperkt - gebruikersaccount (greybox). Ook is het bewustzijn, besef (awareness) van medewerkers getest d.m.v. een phishing-mail en een USB test met malware (geïnfecteerde bestanden). Tot slot is het draadloze netwerk getest.

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 een beperkte afvaardiging vanuit het team Informatie en Automatisering (I&A) van de gemeente Barneveld. Wij hebben de gemeentesecretaris en een contactpersoon van het team I&A 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 van het onderzoek. Men heeft dit goed nageleefd.

Rapportage van Hoffmann Bedrijfsrecherche BV
De rapportage is opgesteld door het externe Bureau Hoffmann - in opdracht van - en in nauwe 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 essentieel 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. Verderop in deze brief gaan we in op de bestuurlijke reactie.

Conclusies
Naar aanleiding van het onderzoek concludeert de rekenkamercommissie dat de gemeente Barneveld de informatieveiligheid vergeleken met andere gemeenten in Nederland redelijk op orde heeft. Zo is het de onderzoekers niet gelukt om - binnen de gestelde tijd van het onderzoek - via de externe penetratietest vertrouwelijke gegevens te bemachtigen. Ook reageerde men procedureel adequaat op de phishing-actie en is malware op de USB-sticks niet geactiveerd op een computer met internettoegang. Daarnaast is de afscherming van het Wifi-netwerk op orde.

Uiteraard zijn er tijdens het onderzoek zwakke plekken en verbeterpunten in de beveiliging gevonden, aangezien het rekenkameronderzoek hier voornamelijk op gericht was. Hierbij zijn diverse kwetsbaarheden naar voren gekomen, bijvoorbeeld op het gebied van de awareness van medewerkers, het wachtwoordbeleid, de segmentatie van het netwerk en protocollen op het gebied van inloggen. Naar aanleiding van het onderzoek kunnen wij dan ook stellen dat het netwerk van de gemeente Barneveld - ondanks diverse (goede) technische genomen beveiligingsmaatregelen - kwetsbaar is voor aanvallen door kwaadwillenden van buitenaf. De gemeente voldoet dan ook niet aan enkele normen die gesteld worden in de Baseline Informatiebeveiliging Gemeenten (BIG), zoals het wachtwoordbeleid.

Graag wijzen wij u er nogmaals op 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. Wel zijn wij van mening dat de gemeente zou moeten voldoen aan de normen van de BIG. 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
Om tot een volwassen informatiebeveiligingsbeleid te komen bij de gemeente Barneveld adviseert de rekenkamercommissie op basis van het onderzoek een integraal pakket aan maatregelen op het gebied van mens, techniek en organisatie. Hierbij kan men denken aan het creëren van veilig gedrag bij de medewerkers, technische maatregelen om zaken af te dwingen, beperken of te monitoren en organisatorische maatregelen om zaken te borgen, begeleiden en uit te voeren. Voor een uitgebreider overzicht van conclusies en aanbevelingen verwijzen wij u naar de niet-openbare rapportage van Hoffmann.

Bestuurlijke reactie van het college
Wij hebben het college van burgemeester en wethouders gevraagd een reactie te geven op de conclusies en aanbevelingen van de rapportage van Hoffmann. De bestuurlijke reactie luidt als volgt:

"*Het College van Burgemeester en Wethouders van de gemeente Barneveld vindt het rapport van Hoffman in de huidige vorm zeer waardevol voor Informatie en Automatisering. De aanbevelingen uit het rapport worden overgenomen en waar mogelijk omgezet in maatregelen. Ze zijn grotendeels technisch van aard.*
Naar aanleiding van de bevindingen en de aanbevelingen van het onderzoek is een gedetailleerde actielijst opgesteld, inclusief tijdpad en budgetten. De meest urgente maatregelen zijn direct ingevoerd. Over de voortgang van de maatregelen doet Informatie en Automatisering periodiek verslag aan de directie. De actielijst dient ook als leidraad voor de afweging van mogelijke maatregelen. Maatregelen dienen altijd te worden bezien in relatie tot het risico (kans en impact) dat ze ondervangen, de daarvoor benodigde kosten en de impact op de performance van het systeem en de werkbaarheid voor de gebruiker.
Wat betreft awareness zijn er directe raakvlakken met de huidige ambtelijke werkgroepen ten aanzien van de privacywetgeving en de fysieke toegang tot de kantoorlocaties. De laatste raakt ook de bevindingen met betrekking tot de fysieke toegang tot het netwerk. Met de deelname van de informatiebeveiliger (CISO in het kader van BIG, Chief Information Security Officer) aan deze werkgroepen wordt de gecombineerde aanpak van de awareness geborgd.
Het rapport van Hoffmann gaat zeer gedetailleerd in op de gevonden kwetsbaarheden / aandachtspunten die voor verbetering vatbaar zijn, maar classificeert sec op het betreffende onderdeel (niet in samenhang). Een beoordeling/duiding van de informatiebeveiliging in samenhang met bestaande beveiligingsmaatregelen, aard en toepassing van de betrokken systemen ontbreekt."

Nawoord rekenkamercommissie n.a.v. bestuurlijke reactie
De rekenkamercommissie is content te vernemen dat het college van burgemeester en wethouders het rapport van Hoffmann waardevol vindt voor Informatie en Automatisering. Graag wijzen wij erop dat de werking van het onderzoek natuurlijk breder is dan alleen I&A. Awareness gaat over de hele gemeentelijke organisatie. Ook is het goed om te vernemen dat de meest urgente maatregelen direct ingevoerd zijn en dat het college van plan is de aanbevelingen over te nemen en dat er een gedetailleerde actielijst is opgesteld, inclusief tijdpad en budgetten.

De rekenkamercommissie is het eens met de opmerking van het college dat het rapport van Hoffmann vooral ingaat op de gevonden kwetsbaarheden die voor verbetering vatbaar zijn. Graag wijzen wij erop dat de aard van dergelijk onderzoek (penetratietesten) nu eenmaal gericht is op het zoeken naar kwetsbaarheden en het zoeken naar de zwakste schakel in de beveiliging. Hierbij is niet primair gekeken

naar zaken die wel goed geregeld waren. Het rekenkameronderzoek was een beperkt onderzoek naar mogelijkheden om te hacken (en het is niet met alle mogelijke middelen uitgevoerd).

Het college geeft in haar bestuurlijke reactie ook aan dat een beoordeling van de informatiebeveiliging in samenhang met bestaande beveiligingsmaatregelen, aard en toepassing van de betrokken systemen in het rapport van Hoffmann ontbreekt. De rekenkamercommissie wijst erop dat dit klopt, omdat dit buiten de scope van het onderzoek viel. Als men de complete informatiebeveiliging wil laten onderzoeken, dan zal gekeken moeten worden naar de elementen mens, techniek en organisatie (en in hun samenhang). Het huidige onderzoek heeft zich enkel gericht op de techniek. Zaken als bijvoorbeeld de structuur en processen zijn hierbij niet onderzocht.

Rapport Hoffmann niet-openbaar
Na een grondige afweging is de rekenkamercommissie van mening dat openbaarmaking van het rapport het belang van de gemeente Barneveld 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. Op grond van artikel 10 van de WOB hebben wij de rapportage daarom als niet-openbaar aangemerkt.

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.P.P. van Dort
Voorzitter rekenkamercommissie
Vallei en Veluwerand

Mevrouw drs. B. Meijboom
Secretaris/onderzoeker rekenkamercommissie
Vallei en Veluwerand

cc: College van burgemeester en wethouders van de gemeente Barneveld