Rekenkamercommissie Vallei en Veluwerand

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

Gemeenteraad Leusden
Postbus 150
3830 AD LEUSDEN

Barneveld, 27 oktober 2016

Ons kenmerk:	1026275	**verzonden op:**	27 oktober 2016
Behandelend ambtenaar:	B. Meijboom		
Doorkiesnummer:	0342 - 495 384	**e-mailadres:**	b.meijboom@barneveld.nl
Uw brief van:		**met kenmerk:**	
Bijlage(n):	geheime rapportage van Hoffmann		
Onderwerp:	rekenkameronderzoek digitale veiligheid Leusden		

Geachte leden van de gemeenteraad,

In de eerste helft van 2016 heeft de rekenkamercommissie een onderzoek uitgevoerd naar diverse aspecten van de digitale veiligheid van de gemeente Leusden. Hiertoe hebben wij de veiligheid van de ICT-systemen van de gemeente Leusden getest met behulp van professionele hackers van het bureau Hoffmann Bedrijfsrecherche BV. Naar aanleiding van het onderzoek heeft Hoffmann in nauwe samenwerking met de rekenkamercommissie een uitgebreide rapportage opgesteld, met conclusies en aanbevelingen. De rapportage van Hoffmann hebben wij als beveiligde, vertrouwelijke rapportage aangeboden aan de griffier met het advies de raad voor te stellen de geheimhouding op te leggen. Verderop in deze brief gaan wij hier nader op in.

Wij adviseren de gemeenteraad om akkoord te gaan met alle aanbevelingen uit de rapportage van Hoffmann en het college op te dragen hiermee aan de slag te gaan. Het college heeft in haar bestuurlijke reactie aangegeven dat er naar aanleiding van het rekenkameronderzoek direct al een aantal maatregelen ingevoerd is. Ook heeft het college aangeven alle aanbevelingen uit de rapportage van Hoffmann 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 Leusden. Doel van het onderzoek was om te toetsen of de informatiesystemen van de gemeente Leusden 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), maar ook met een valide - in rechten beperkt - gebruikersaccount (greybox). Ook is het bewustzijn, besef (awareness) van medewerkers getest d.m.v. een phishing-mail. Tot slot is het draadloze netwerk getest.

Toestemming voor onderzoek
Omdat het bij dit onderzoek ging om een poging tot “digitale inbraak” 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 ICT afdeling van de gemeente Leusden. Wij hebben de gemeentesecretaris en een contactpersoon van de afdeling ICT nadrukkelijk gevraagd om geen ruchtbaarheid te geven aan het onderzoek. In het belang van het onderzoek was het van belang dat zo min mogelijk mensen op de hoogte zouden zijn van het onderzoek.

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 in het eerste halfjaar voorgelegd aan de gemeentelijke organisatie 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. De gemeentelijke organisatie heeft aangegeven dat de rapportage van Hoffmann technisch correct is, er zijn geen feitelijke onjuistheden gevonden. Daarna is de rapportage van Hoffmann definitief gemaakt. Verderop in deze brief gaan we in op de bestuurlijke reactie.

Conclusies
Naar aanleiding van het onderzoek concludeert de rekenkamercommissie dat de gemeente Leusden de informatieveiligheid vergeleken met andere gemeenten in Nederland redelijk op orde heeft. Wel kunnen wij stellen dat, ondanks diverse (goede) technische genomen beveiligingsmaatregelen, het netwerk van de gemeente Leusden kwetsbaar is voor aanvallen van buitenaf. De gemeente voldoet dan ook niet aan enkele normen die gesteld worden in de Baseline Informatiebeveiliging Gemeenten (BIG)[1], zoals het wachtwoordbeleid.

Uit het onderzoek komen onder andere de volgende kwetsbaarheden naar voren:
- De gemeente werkt met eenvoudige wachtwoorden voor medewerkers. Dit kan te maken hebben met het ontbreken van bewustzijn bij de medewerkers en het ontbreken van een gedegen wachtwoordbeleid.
- De gemeente hanteert eenvoudige gebruikersnamen (drie karakters). De resultaten van de phishing-actie laten verder zien dat de gemiddelde medewerker van de gemeente Leusden niet alert genoeg is op het herkennen van phishing. Ruim 30% van de medewerkers heeft zijn/haar logingegevens afgegeven op een website die buiten het domein van de gemeente Leusden ligt.
- Er zijn printers aangetroffen met standaard wachtwoorden en gebruikersnamen. Hierdoor was het voor onbevoegden mogelijk om inloggegevens te achterhalen die toegang geven tot kritieke systemen.
- Het interne netwerk is onvoldoende gesegmenteerd, waardoor elke medewerker of kwaadwillende op het interne netwerk bij alle systemen kan komen.
- De gemeente maakt gebruik van onversleutelde inlogprotocollen (intern en extern). Het risico hiervan is dat kwaadwillenden eenvoudig logingegevens kunnen onderscheppen, omdat deze gegevens onversleuteld over het internet worden verstuurd.

Graag willen wij u erop wijzen 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 dat men bewuste keuzes maakt in de mate van veiligheid versus werkbaarheid en financiën.

[1] *De BIG is ontwikkeld door de Informatiebeveiligingsdienst voor gemeenten (IBD), in samenwerking met de Vereniging Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING). De BIG is een set van beveiligingsmaatregelen (normen) die een goed basis-beveiligingsniveau voor gemeenten neerlegt. Alle gemeenten hebben toegezegd om voor eind januari 2017 te voldoen aan de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).*

Aanbevelingen
Om tot een volwassen informatiebeveiligingsbeleid te komen bij de gemeente Leusden adviseert de rekenkamercommissie in nauw overleg met bureau Hoffmann een integraal pakket aan maatregelen: een combinatie van maatregelen in de segmenten 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 gedetailleerde 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. Het college heeft naar aanleiding hiervan aangegeven dat men door het uitvoeren van het onderzoek inzicht gekregen heeft op een aantal risicovolle plekken in de ICT omgeving van de gemeente Leusden. Het college wil alle aanbevelingen naar aanleiding van de rapportage overnemen. Acute veiligheidsrisico's heeft het college direct nadat deze geconstateerd waren al laten repareren.

Het college heeft er ook op gewezen dat een dergelijke test van de ICT-systemen een momentopname is. Bij volgende tests zullen er weer nieuwe risico's worden geduid, omdat kwaadwillenden steeds modernere en verfijndere technieken tot hun beschikking hebben. Daarom vindt het college het jaarlijks laten uitvoeren van een penetratietest essentieel.

Een uitgebreidere bestuurlijke reactie van het college kunt u lezen in een apart memo van het college aan de gemeenteraad. Dit memo gaat zowel in op het onderzoek van de rekenkamercommissie als op het verslag van de VNG visitatiecommissie Informatieveiligheid.

Rapport van Hoffmann geheim
Na een grondige afweging is rekenkamercommissie van mening dat openbaarmaking van het rapport het belang van de gemeente Leusden 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. Na afstemming met de ambtelijke organisatie, het college van burgemeester en wethouders en de griffier adviseert de rekenkamercommissie de raad dan ook te besluiten geheimhouding op te leggen omtrent de inhoud van de rapportage van Hoffmann, op basis van art. 25 lid 1 Gemeentewet. De motivering hiervoor is de economische of financiële belangen van de gemeente, op grond van art.10 lid 2 sub b Wet openbaarheid van bestuur.

Tot slot / nawoord rekenkamercommissie
De rekenkamercommissie is blij te horen dat het college van burgemeester en wethouders meteen actie ondernomen heeft om geconstateerde acute veiligheidsrisico's op te pakken. Ook zijn wij blij dat het college alle aanbevelingen van de rekenkamercommissie en Hoffmann Bedrijfsrecherche over wil nemen. Wij zijn het verder eens met het college dat het goed zou zijn om een dergelijke penetratietest met enige regelmaat te laten uitvoeren.

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. Als het college jaarlijks een test laat doen, zijn de aanbevelingen van de rekenkamercommissie na twee tot drie jaar achterhaald.

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 Leusden