Rekenkamercommissie Vallei en Veluwerand

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

Gemeenteraad Nijkerk
Postbus 1000
3860 BA NIJKERK

Barneveld, 25 september 2017

Ons kenmerk: 1057198
Behandelend ambtenaar: B. Meijboom
Doorkiesnummer: 0342 - 495 384
Uw brief van:
Bijlage(n): geheime rapportage van Hoffmann
Onderwerp: rekenkameronderzoek digitale veiligheid Nijkerk

verzonden op: 25 SEP 2017
e-mailadres: b.meijboom@barneveld.nl
met kenmerk:

Geachte 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 periode van november 2016 t/m februari 2017 heeft de rekenkamercommissie daarom een onderzoek uitgevoerd naar diverse aspecten van de digitale veiligheid van de gemeente Nijkerk. Hiertoe hebben wij de veiligheid van de ICT-systemen van de gemeente Nijkerk getest met behulp van professionele hackers van bureau Hoffmann Bedrijfsrecherche BV, afdeling Cybersecurity. Op verzoek van de gemeente is als onderdeel van het rekenkameronderzoek ook gekeken wat de gemeente Nijkerk zelf al doet aan bewustzijn van de medewerkers op het gebied van digitale veiligheid. Hiertoe heeft de rekenkamercommissie een interview gehouden met de manager van de afdeling Facilitaire Dienstverlening en de Coördinator Automatisering van de gemeente Nijkerk.

Naar aanleiding van het onderzoek heeft Hoffmann in opdracht van en onder de verantwoordelijkheid van de rekenkamercommissie een uitgebreide rapportage opgesteld, met conclusies en aanbevelingen. Na 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 ligt voor raadsleden onder geheimhouding ter inzage bij de griffie.

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 onder andere aangegeven de kwetsbaarheden die tijdens het onderzoek geconstateerd zijn zo snel mogelijk weg te zullen nemen. Verderop in deze brief gaan wij hier nader op in.

Het onderzoek
Het gaat om een technisch onderzoek, gericht op de informatiesystemen van de gemeente Nijkerk. Doel van het onderzoek was om te toetsen of de informatiesystemen van de gemeente Nijkerk voldoende beveiligd zijn tegen het risico van hacken. Hackers van Hoffmann Cybersecurity hebben de informatiebeveiliging zowel getest vanaf het internet (***externe penetratietest***) als vanaf het lokale netwerk ***(interne penetratietest***). Ook is het bewustzijn, besef (awareness) van medewerkers getest door middel van een phishing-mail. Tot slot is het draadloze netwerk getest.

Zowel bij de interne als de externe test hebben de hackers eerst geprobeerd binnen te komen zonder voorkennis van de infrastructuur en zonder gebruikersaccount (blackbox), en vervolgens ook met een valide - in rechten beperkt - gebruikersaccount (greybox).

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 manager van de afdeling Facilitaire Dienstverlening en de Coördinator Automatisering van de gemeente Nijkerk. Wij hebben hen gevraagd 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 Cybersecurity
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 een technische reactie met de vraag aan te geven of er feitelijke onjuistheden in de rapportage staan. In afwijking van onze gebruikelijke werkwijze stonden in deze 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.

Samenvatting bevindingen
Externe onderzoek (externe penetratietest)
Het externe onderzoek is uitgevoerd vanaf het internet en richtte zich onder andere op websites. Hierbij is het scenario gevolgd waarbij een kwaadwillende vanuit zijn eigen huis, of bijvoorbeeld vanuit een internetcafé, de systemen van de gemeente Nijkerk aanvalt. De rekenkamercommissie concludeert dat het de onderzoekers niet gelukt is om - binnen de gestelde tijd van het onderzoek - via de externe penetratietest vertrouwelijke gegevens te bemachtigen. Er is slechts één kwetsbaarheid aangetroffen, dus de mogelijkheid tot misbruik door kwaadwillenden is zeer beperkt gebleken.

Intern onderzoek (interne penetratietest)
De interne test is uitgevoerd op locatie bij de gemeente Nijkerk. Daarbij is gekeken naar de mogelijkheden die een kwaadwillende heeft, als hij eenmaal fysieke toegang heeft tot het gebouw, bijvoorbeeld door zijn laptop aan te sluiten op het netwerk. In eerder uitgevoerde onderzoeken bij andere organisaties, waaronder gemeenten, is aangetoond dat de medewerkers van Hoffmann eenvoudig binnen konden komen in gebouwen. Uit een vergelijkbaar onderzoek dat de gemeente Nijkerk in 2015 zelf heeft laten uitvoeren (mystery guest onderzoek) bleek dat het ook in Nijkerk mogelijk was om binnen te komen. De rekenkamercommissie heeft daarom besloten geen fysieke inlooptest te laten uitvoeren.

Tijdens het onderzoek van de rekenkamercommissie bleek dat het interne netwerk van de gemeente Nijkerk eenvoudig toegankelijk was voor iedereen die fysieke toegang heeft tot het pand. Hierbij merkt de rekenkamercommissie op dat men in Nijkerk niet zo maar binnenkomt, aangezien men eerst voorbij een balie moet en vervolgens ook nog een badge nodig heeft om verder binnen te komen. Eenmaal aangesloten op het interne netwerk, bleek dat er eenvoudig vertrouwelijke informatie te achterhalen was. Er zijn meerdere kritieke kwetsbaarheden aangetroffen. Dit komt overeen met de situatie die Hoffmann bij veel andere gemeenten aantreft. Nijkerk scoort op dit punt dan ook gemiddeld.

Bij de interne test wijst de rekenkamercommissie erop dat de hackers van Hoffmann snel betrapt werden door de servicedesk van de gemeente Nijkerk. Systeembeheer zorgde er vervolgens voor dat de hackers afgesloten werden van het netwerk. De hackers konden hun werk vervolgens pas weer voortzetten nadat zij hiervoor toestemming gekregen hadden.

Phishing-actie
Voor de phishing-actie is een e-mail gestuurd naar alle medewerkers met als onderwerp "*Winterse attentie voor medewerkers Gemeente Nijkerk*". De mail is gestuurd naar 292 medewerkers van de gemeente. Hiervan heeft 8% op de link in de mail gedrukt en 21 medewerkers hebben hun login-gegevens achtergelaten op de website. Om digitaal in te breken op de systemen van de gemeente Nijkerk heeft een kwaadwillende overigens voldoende aan de logingegevens van één medewerker. Tijdens het interview wijzen de ambtelijke respondenten erop dat de gemeente Nijkerk sinds 2013 structureel diverse acties inzet gericht op het vergroten van de awareness van medewerkers[1]. Uit het onderzoek blijkt ook dat de reactie en de afhandeling van het incident door de afdeling Servicedesk en Communicatie correct en professioneel was. Hierdoor werden de mogelijkheden om misbruik te maken van de verkregen login(s) snel geblokkeerd.

Conclusie
Naar aanleiding van het onderzoek concludeert de rekenkamercommissie dat het netwerk van de gemeente Nijkerk - ondanks diverse (goede) technische genomen beveiligingsmaatregelen - kwetsbaar is voor aanvallen van buitenaf (met name via de medewerkers). Als we Nijkerk vergelijken met andere gemeenten in Nederland kunnen we concluderen dat Nijkerk de digitale veiligheid op de onderzochte onderdelen redelijk op orde heeft. Uiteraard zijn er tijdens het onderzoek zwakke plekken en verbeterpunten in de beveiliging gevonden, aangezien het onderzoek hier voornamelijk op gericht was.

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. Wel 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 Nijkerk 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 en organisatorische maatregelen om zaken uit te voeren en te borgen. Voor een uitgebreider overzicht van conclusies en aanbevelingen verwijzen wij u naar de geheime 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. In de bestuurlijke reactie wijst het college er onder andere op dat het onderzoek van de rekenkamercommissie de gemeente in staat stelt de al ingezette

[1] Zo is in 2015 een mystery guest onderzoek gedaan, waarbij een mysterie guest geprobeerd heeft om binnen te komen in het gemeentehuis. In 2016 heeft de gemeente een enquête naar bewustwording laten uitvoeren onder alle medewerkers, met vragen betreffende bewustwording. Ook vindt er actieve voorlichting en informatie plaats gericht op medewerkers, bijvoorbeeld door het bezoeken van werkoverleggen, maar ook via intranet.

ontwikkelingen op dit vlak beter te sturen en het stelsel aan maatregelen verder te verbeteren. In de bestuurlijke reactie geeft het college aan de resultaten van het onderzoek te willen gebruiken om:

- *"geconstateerde kwetsbaarheden zo snel als mogelijk weg te nemen;*
- *het onderzoek aan te grijpen om de bewustwording bij medewerkers te verbeteren, als onderdeel van de structurele aanpak hiervoor (o.a. In de samenwerking op het gebied van de bedrijfsvoering tussen Bunschoten, Leusden, Nijkerk en Putten);*
- *het stelsel van maatregelen dat de risico's voor onze informatieveiligheid beheersbaar houdt verder te verbeteren;*
- *de al lopende en geplande ontwikkelingen op dit vlak met de uitkomsten van het rapport waar mogelijk beter te prioriteren."*

In de bestuurlijke rectie geeft het college ook aan dat diverse kwetsbaarheden inmiddels verholpen zijn, sommige daarvan al lopende het onderzoek. Aan alle andere geconstateerde technische kwetsbaarheden wordt gewerkt. De laatste kwetsbaarheden zullen naar verwachting vóór 2018 weggenomen zijn.

Rapport Hoffmann niet-openbaar
Na een grondige afweging is de rekenkamercommissie van mening dat openbaarmaking van het rapport het belang van de gemeente Nijkerk kan schaden. Het rapport bevat gedetailleerde informatie over de architectuur van de ICT-systemen. Het is uit veiligheidsoverwegingen 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 omtrent de inhoud van de rapportage van Hoffmann, 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 van) de gemeenteraad bepalen ofeen 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.

IA

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

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

cc: College van burgemeester en wethouders van de gemeente Nijkerk