REKENKAMERCOMMISSIE
VALLEI & VELUWERAND

p/a Gemeente Barneveld
Postbus 63
3770 AB Barneveld
www.rkvalleienveluwerand.nl

Inlichtingen
Ingrid M.T. Spoor
T 06 20 47 57 14
E i.spoor@barneveld.nl

Datum
15 maart 2021

Onderwerp
Doorwerking rekenkameronderzoek digitale veiligheid Barneveld.

Bijlagen
-

Aan de raad van de gemeente Barneveld
Postbus 63
3770 AB BARNEVELD

Geachte gemeenteraad,

Graag informeert de rekenkamercommissie Vallei en Veluwerand u over een doorwerkingsonderzoek. In 2016 hebben professionele ethische hackers van Hoffmann Bedrijfsrecherche B.V. in opdracht van de rekenkamercommissie Vallei en Veluwerand onderzoek uitgevoerd naar de digitale veiligheid in de gemeente Barneveld. Uit het onderzoek kwam destijds een aantal kwetsbaarheden naar voren op het gebied van de bewustwording van medewerkers, het wachtwoordbeleid, de segmentatie van het netwerk en protocollen voor inloggen. In februari 2017 hebben wij u hierover geïnformeerd en aanbevelingen gedaan.

De rekenkamercommissie kijkt zo'n drie tot vier jaar na afronding van een onderzoek in hoeverre de aanbevelingen zijn opgevolgd. Dat is het zogenoemde doorwerkingsonderzoek. Zo zijn we ook bij dit onderzoek nagegaan hoe de opvolging heeft plaatsgevonden. Daarvoor hebben we de CISO (Chief Informatie Security Officer) van Barneveld gevraagd naar de stand van zaken. Daarnaast heeft de rekenkamercommissie contact gehad met het bureau Hoffmann met de vraag of een herhaalonderzoek meerwaarde heeft waarbij het accent zou moeten liggen op de digitale veiligheid bij thuiswerken. De conclusie uit de gesprekken met de CISO en Hoffmann is dat een rekenkameronderzoek naar de digitale veiligheid op dit moment geen meerwaarde heeft. De gemeente onderneemt namelijk zelf stappen om de digitale veiligheid te testen. Deze conclusie lichten we hieronder nader toe. Ook worden hieronder de conclusies voor wat betreft de opvolging van de aanbevelingen uit het onderzoek toegelicht.

Opvolging aanbevelingen

Algemeen

Na het onderzoek in 2016 is de gemeente Barneveld aan de slag gegaan met de aanbevelingen. De gemeente heeft de aanbevelingen omgezet in maatregelen en de meest urgente maatregelen zijn direct uitgevoerd. De gemeente heeft aangegeven dat de overige maatregelen in de loop van 2017/2018 zijn geïmplementeerd.

Bewustwording medewerkers

Om medewerkers bewust te maken van de digitale risico's organiseert de gemeente voor nieuwe medewerkers een workshop "informatieveiligheid en privacy". Medewerkers die al langer in dienst zijn

kunnen ook deelnemen aan deze workshop. Daarnaast organiseert de gemeente incidenteel acties om het bewustzijn van medewerkers te vergroten, bijvoorbeeld door het versturen van 'phishing mails' (valse mails die verstuurd worden om van een nietsvermoedende gebruiker inlognaam en wachtwoorden te stelen). Ook staan er periodiek berichten voor medewerkers op intranet om de digitale veiligheid en risico's onder de aandacht te brengen.

Wachtwoordbeleid
De rekenkamercommissie adviseerde in 2016 om het wijzigen van standaardwachtwoorden bij het in gebruik nemen van nieuwe systemen en applicaties op te nemen in het beleid. Het wachtwoordbeleid is inmiddels aangescherpt volgens de gemeente. De gemeente heeft aangegeven dat bij het merendeel van de applicaties een wachtwoordinstructie is opgelegd en geen standaardwachtwoorden meer gebruikt kunnen worden.

Segmentatie van het netwerk
In 2017 heeft de gemeente Netwerk Access Control (NAC) geïmplementeerd. Dit is een methode waarbij de beveiliging van het eigen netwerk wordt versterkt. Dit gebeurt door het beperken van de toegang tot het digitale netwerk. Alleen apparaten die voldoen aan een bepaald veiligheidsbeleid krijgen toegang. Er wordt voorkomen dat 'vreemde' en onveilige apparaten toegang kunnen krijgen tot het netwerk.

Protocollen op gebied van inloggen
Het beleid van de gemeente is inmiddels dat onderlinge communicatie tussen servers via beveiligde verbindingen gebeurt. Ook interne websites zijn alleen via een veilige 'https' te bezoeken. In 2016 bleken bepaalde netwerkschijven toegankelijk voor gebruikers die daar beroepshalve geen gebruik van hoeven te maken. Inmiddels zijn de schijven alleen toegankelijk voor geautoriseerde gebruikers. Bovendien kunnen slechts één of twee contactpersonen/beheerders per afdeling autorisaties toekennen.

Voor het tijdelijk delen van gegevens wordt gebruik gemaakt van een lokale schijf. Dit is een schijflocatie waar alleen tijdelijke bestanden kunnen worden geplaatst, omdat ze periodiek automatisch worden gewist. Deze schijflocatie is niet geschikt voor het plaatsen van vertrouwelijke bestanden of bestanden met persoonsgegevens. Binnen de gemeentelijke organisatie wordt hier regelmatig aandacht voor gevraagd zodat medewerkers er zich bewust van worden.

Jaarlijkse pentest
Na het digitale veiligheidsonderzoek in 2016 had de gemeente Barneveld het voornemen om jaarlijks een pentest te laten uitvoeren. Een penetratietest of pentest (binnendringingstest) is een toets van een of meer computersystemen op kwetsbaarheden, waarbij deze kwetsbaarheden ook werkelijk gebruikt worden om in de digitale systemen in te breken.

In 2017 heeft deze test niet plaatsgevonden, omdat de gemeente in dat jaar nog bezig was met het implementeren van de aanbevelingen uit het onderzoek van 2016. Begin 2018 is een pentest uitgevoerd. In 2019 is de test uitgesteld vanwege de overgang naar een nieuw datacenter. In 2020 is opdracht gegeven voor het uitvoeren van een pentest in 2021. Deze is inmiddels uitgevoerd. De acties die hieruit naar voren zijn gekomen worden opgepakt.

Veiligheid ten aanzien van thuiswerken

Medewerkers hebben vanuit huis toegang tot de gemeentelijke systemen via VDI (Virtual Desktop Infrastructure). Hierdoor werkt de medewerker feitelijk niet op zijn of haar eigen lokale computer. Daardoor kunnen geen gegevens en bestanden vanuit de VDI omgeving op de lokale computer gekopieerd of geplaatst worden. Om toegang te krijgen tot het systeem wordt gebruik gemaakt van een 'twee-factor authentication'. Na het invoeren van een inlognaam en een wachtwoord ontvangt de medewerker in een app een bericht dat goedgekeurd moet worden, waarna toegang tot het systeem verkregen wordt.

De gemeente Barneveld maakt voor het thuiswerken gebruik van de software van CITRIX. Begin 2020 bleek de veiligheid van de CITRIX systemen niet op orde. Veel gemeenten kwamen daardoor in de problemen. De fout zat in twee diensten van CITRIX, die de gemeente Barneveld niet afneemt. Daardoor heeft de gemeente Barneveld geen problemen gehad.

Tot slot

De rekenkamercommissie realiseert zich dat incidenten zich kunnen voordoen en dat de gemeente Barneveld niet alles volledig in de hand heeft. Honderd procent veiligheid bestaat niet, omdat nu eenmaal niet alle risico's in beeld zijn, maar ook omdat dit in de praktijk onwerkbaar en onbetaalbaar zou zijn. Het is echter wel 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.

De rekenkamercommissie gaat ervan uit dat u met deze brief voldoende geïnformeerd bent over de huidige stand van zaken ten aanzien van de digitale veiligheid. Indien u behoefte heeft aan meer informatie over dit onderwerp dan adviseren wij u nadrukkelijk om daar naar te vragen. De CISO van de gemeente heeft aangegeven dat hij te allen tijde bereid is om in een besloten vergadering van de auditcommissie één en ander toe te lichten.

Met vriendelijke groet,

De heer drs. J. van Zomeren
Voorzitter rekenkamercommissie

Mevrouw ir. I.M.T. Spoor
Secretaris/onderzoeker rekenkamercommissie

c.c. College van burgemeester en wethouders van de gemeente Barneveld