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
6 januari 2021

Onderwerp
Doorwerking rekenkameronderzoek digitale veiligheid Leusden.

Bijlagen
-

Aan de raad van de gemeente Leusden
Postbus 150
3830 AD LEUSDEN

Geachte gemeenteraad,

Graag informeert de rekenkamercommissie Vallei en Veluwerand u over een doorwerkingsonderzoek. In 2016 hebben professionele hackers van Hoffmann Bedrijfsrecherche B.V. in opdracht van de rekenkamercommissie onderzoek uitgevoerd naar de digitale veiligheid in de gemeente Leusden. Uit het onderzoek kwam destijds een aantal technische kwetsbaarheden van de digitale systemen naar voren. Ook bleken medewerkers zich niet volledig bewust van de risico's van 'phishing'. In oktober 2016 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 Information Security Officer) van Leusden gevraagd naar de stand van zaken. Deze is zowel schriftelijk als mondeling toegelicht. Naar aanleiding daarvan heeft de rekenkamercommissie contact gehad met Hoffmann Bedrijfsrecherche B.V. 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 Bedrijfsrecherche B.V. is dat een onderzoek naar de digitale veiligheid door de rekenkamercommissie op dit moment geen meerwaarde heeft. Deze conclusie wordt hieronder nader toegelicht.

Opvolging aanbevelingen uit 2016

De gemeente Leusden heeft de aanbevelingen uit 2016, die met een hoog risico waren aangemerkt, destijds direct opgepakt. De overige aanbevelingen zijn in de loop van de tijd opgevolgd. Daarbij dient opgemerkt te worden dat de gemeente Leusden in 2017 anders is gaan werken, waardoor sommige aanbevelingen niet meer van toepassing waren. De ICT infrastructuur is in 2017 zodanig ingericht dat alle medewerkers op iedere plek binnen en buiten het Huis van Leusden en op een zelf gekozen tijdstip kunnen werken. De nieuwe inrichting is in 2017 getest. Deze test liet zien dat de beveiliging van de digitale systemen duidelijk was verbeterd ten opzichte van het jaar daarvoor ten tijde van het rekenkameronderzoek, zo blijkt uit het gemeentelijk jaarverslag van 2017.

Samenwerking binnen BNLP

Sinds 2017 werkt de gemeente Leusden op het gebied van de ICT samen met de gemeenten Bunschoten, Nijkerk en Putten binnen het samenwerkingsverband BNLP. De CISO werkgroep van BNLP pakt digitale veiligheid gezamenlijk op. Deze werkgroep bestaat uit vier gemeentelijke CISO's en één coördinerende CISO.

Digitale kwetsbaarheid testen

De gemeente Leusden laat jaarlijks een 'pentest' uitvoeren. In het rekenkameronderzoek in 2016 is een dergelijke test ook uitgevoerd. Deze testen tonen de digitale kwetsbaarheden van de gemeentelijke ICT infrastructuur. Risicovolle kwetsbaarheden, die uit de testen naar voren komen, worden opgelost. De test die in 2020 uitgevoerd zou worden, heeft de gemeente doorgeschoven naar 2021, door gewijzigde prioriteiten als gevolg van de Corona pandemie.

Naast de jaarlijkse pentesten legt het college jaarlijks verantwoording af over de status van informatiebeveiliging aan de gemeenteraad en de toezichthouders informatieveiligheid van de Rijksoverheid. Voor deze verantwoording wordt de ENSIA-systematiek gevolgd. ENSIA staat voor Eenduidige Normatiek Single Information Audit. De informatiebeveiliging wordt getoetst met behulp van zelfevaluaties die gebaseerd zijn op normen van de Nederlandse overheid (BIO: Baseline Informatiebeveiliging Overheid). De evaluaties hebben betrekking op de Basisregistratie Personen (BRP) en Reisdocumenten, Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (SUWI) richting de rijksoverheid (zie ook www.vngrealisatie.nl).

Ook sluit de gemeente Leusden, net als de andere BNLP gemeenten, zich aan bij initiatieven (perceel 1) van het landelijke VNG project GGI-Veilig (gemeentelijke gemeenschappelijk Infrastructuur). Via dit project kan de gemeente onder andere 'actieve netwerk monitoring' afnemen voor het bewaken van dataverkeer op het bedrijfsnetwerk. Ook kunnen beveiligingsexpertisediensten worden afgenomen evenals beveiligingsproducten voor de gemeentelijke ICT infrastructuur zoals pentesten, firewalls en anti DDOS (distributed denial of service aanvallen) (zie ook www.vngrealisatie.nl).

Bewustzijn medewerkers

Uit het rekenkameronderzoek van 2016 kwam naar voren dat het bewustzijn van de medewerkers de nodige aandacht verdiende. De gemeente Leusden heeft dit opgepakt door in de afgelopen jaren diverse activiteiten uit te voeren. In 2018 heeft binnen de samenwerking BLNP een phishing mail campagne plaatsgevonden onder alle medewerkers van de vier gemeenten. De uitkomsten hebben geleid tot het uitvoeren van een communicatieplan met als doel de medewerkers bewuster te maken van hun verantwoordelijkheid en gedrag. In 2019 is bij alle vier gemeenten een mystery-guest onderzoek uitgevoerd. Mede naar aanleiding van deze onderzoeken is de gemeente ervan doordrongen dat bewustwording een structureel onderdeel moet zijn van het informatieveiligheidsbeleid.

Veiligheid ten aanzien van thuiswerken

De gemeente Leusden heeft naar eigen zeggen bij de invoering van het huidige werkplekconcept veel aandacht besteed aan de digitale veiligheid met betrekking tot het werken op afstand. Mede omdat dit belangrijk was voor het realiseren van een passende werkomgeving binnen het Huis van Leusden. De gemeente werkt met Citrix: medewerkers kunnen alleen op de systemen van de gemeente werken binnen

een beveiligde omgeving. Bij Citrix wordt gebruikgemaakt van een versleutelde beveiligde ‘tunnel’, ongeacht of het gebruikte wifi-netwerk veilig is of niet. Verder gebruiken medewerkers ‘zero footprint’ laptops: dat betekent dat medewerkers zelf niets kunnen installeren op deze laptops. Ook kan er geen USB opslag apparatuur gebruikt worden op de laptops. De gemeente realiseert zich terdege dat de mens een zwakke schakel kan zijn. Daarom zijn er handreikingen en richtlijnen opgesteld voor medewerkers over veilig digitaal werken. Vanuit de CISO werkgroep van BNLP is er voortdurend aandacht om medewerkers te informeren en te stimuleren om zich te houden aan de regels voor het werken op afstand.

Tot slot

De rekenkamercommissie gaat er vanuit dat u met deze brief voldoende geïnformeerd bent over de huidige stand van zaken ten aanzien van de digitale veiligheid en hoe de aanbevelingen van het rekenkameronderzoek van destijds zijn opgevolgd. De rekenkamercommissie ziet op dit moment geen meerwaarde voor een rekenkameronderzoek op dit terrein, gelet op de diverse activiteiten die de gemeente Leusden (in samenwerking met BNLP) reeds uitvoert en de jaarlijkse pentesten die ze laat uitvoeren.

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 Leusden