B en W Adviesnota

Gemeente Venray

Onderwerp	RIB voortgang aanbevelingen rekenkamercommissie onderzoek informatiebeveiliging en privacy		
Zaaknummer		**Teammanager**	Ruud Steegh
B & W datum	26 oktober 2020	**Afdeling/Team**	Bedrijfsvoering/Informatie en Automatisering
Naam steller	Jeroen Frencken	**Portefeuillehouder**	Jan Jenneskens
Openbaarheid	Deze adviesnota is openbaar		
Bevoegd orgaan	B & W		
Ter kennisname	Aanbieden via de Griffie aan Raad		

ADVIES

1. Instemmen met bijgevoegde raadsinformatiebrief en deze toezenden aan de gemeenteraad.

B en W Adviesnota

Gemeente Venray

Samenvatting
= Samenvatting van nota (1 minuut nota). Hier vermeld je de aanleiding/oorzaak.

Beoogd resultaat

Argumenten

Risico's

Kanttekeningen

Communicatie

Financiële gevolgen

Personele/organisatorische gevolgen

Juridische gevolgen

Rechtmatigheid

Fatale termijnen

Vervolgtraject besluitvorming

Evaluatie

Bijlagen

Naslagwerk

Gemeente Venray

Informatie en Automatisering
Raadhuisstraat 1
Postbus 500, 5800 AM Venray
Telefoon (0478) 52 33 33
Telefax (0478) 52 32 22
E-mail gemeente@venray.nl
Internet www.venray.nl
KvK-nummer 14132389

IBAN NL20 BNGH 028 5028 383 (belastingen)
IBAN NL11 BNGH 028 5008 757 (algemeen)
BIC BNGHNL2G

Leden van de gemeenteraad van Venray

Datum	19 oktober 2020	Behandeld door	Jeroen Frencken
Ons kenmerk		Datum uw brief	
Pagina	1 van 3	Uw kenmerk	

Onderwerp Voortgang aanbevelingen rekenkamercommissie onderzoek informatiebeveiliging en privacy

Beste leden van de Raad,

Met deze raadsinformatiebrief informeren wij u over de voortgang van onze informatiebeveiliging en privacy, waaronder de bevindingen uit het rekenkameronderzoek.

De rekenkamercommissie concludeerde op basis van dat onderzoek dat de veiligheid van de systemen, waar de gemeente Venray toen gebruik van maakte, onvoldoende was. Daarnaast concludeerde de rekenkamercommissie dat er sprake was van een ontkoppeling tussen beleid en uitvoering op het gebied van informatieveiligheid en privacybescherming.

Het is inmiddels anderhalf jaar geleden dat het onderzoek heeft plaatsgevonden. Een tijd waarin we conform het ICT-vervangingstraject de automatiseringshardware hebben vervangen en up-to-date gebracht en waarmee een veilige basis is gelegd voor de gemeentelijke systemen. De belangrijkste bevinding uit het onderzoeksrapport, dat "de veiligheid van de systemen waar de gemeente Venray gebruik van maakt ten tijde van het onderzoek onvoldoende was" is hiermee verholpen.

Informatiebeleidsplan
Ook is in 2019 het informatiebeleidsplan (IBP) vastgesteld, waarin twee sporen zijn opgenomen die invulling geven aan de overige aanbevelingen uit het rapport.
In spoor 1 van het IBP, 'De basis op orde' werken we verder aan het op orde brengen en effectief inzetten van onze systemen, processen en informatievoorziening. Dit betreft de processen rondom fysieke beveiliging, gebruikersbeheer en patchmanagement (de manier waarop we omgaan met software-updates van leveranciers) die er voor zorgen dat onze huidige veilige ICT-omgeving, ook veilig blijft. Hierbij maken we gebruik van de Informatiebeveiligingsdienst van de VNG. Zij informeren ons over mogelijke nieuwe dreigingen, zodat we de benodigde updates en patches tijdig kunnen installeren en maatregelen kunnen treffen.

Informatiebeveiliging is een proces van continue aandacht voor risico's en bedreigingen en werkt het beste in een organisatie die leert van ervaringen en op basis hiervan verbeteringen doorvoert.

Dit wordt meegenomen in spoor 2 van het IBP, 'Doorontwikkeling organisatie'. Hier ligt de focus op het digitaal bewust en vaardig maken van onze medewerkers. Met de komst van COVID-19 en het verplichte thuiswerken, is deze noodzaak in een stroomversnelling geraakt. Onderdeel van deze doorontwikkeling is een e-learning informatieveiligheid, waarin we medewerkers steeds meer bewust maken van de risico's die we lopen en de maatregelen die daarbij horen. Inmiddels heeft meer dan 80% van onze medewerkers deze e-learning met succes doorlopen

Informatiebeveiligingsbeleid
Recent is vernieuwd beleid opgesteld dat is afgestemd op en aansluit bij de uitvoering. Dit beleid is gebaseerd op de nieuwe Baseline Informatiebeveiliging Overheid (BIO). Deze baseline is verplicht voor alle overheidsorganisaties. Met de komst van de BIO verschuift de nadruk van beleid op basis van normen en maatregelen naar een op risicogebaseerde implementatiestrategie van beveiligingsmaatregelen, vastgelegd in een jaarplan. Informatiebeveiliging is een continu verbeterproces. Het managementsysteem 'Plan, do, check en act' zorgt er voor dat het bestuur beter 'in control' raakt. Dit wordt onder andere gerealiseerd door de rapportagecyclus in te richten volgens ENSIA (Eenduidige Normatiek Single Information Audit). Wij zullen u via de jaarrekening informeren over de resultaten van de ENSIA verantwoording.

Informatiebeveiligingstest
De afgesproken informatiebeveiligingstest zal jaarlijks in het laatste kwartaal plaatsvinden. Het onderwerp van dit onderzoek wordt ieder jaar opnieuw bepaald. Voor 2020 zal het onderzoek zich niet richten op de techniek, maar op houding en gedrag van medewerkers.

Tot die keuze zijn we gekomen doordat het verplicht thuiswerken vanwege COVID-19 nieuwe informatiebeveiligingsrisico's met zich mee brengt. Zoals het afvoeren van privacygevoelige informatie en het voeren van vertrouwelijke telefoongesprekken. Ook is er een toename aan meldingen van aan COVID-19 gerelateerde phishingmails en valse e-mails. Door te onderzoeken of medewerkers de opgedane kennis uit de e-learning ook in de praktijk kunnen brengen, kunnen we vaststellen of deze effectief is geweest. De uitkomsten worden meegenomen in de jaarplannen.

Door afronding van het ICT-vervangingstraject en de daaropvolgende netwerkscan, waaruit is gebleken dat de kwetsbaarheden uit het rapport niet meer optraden, is er een veilige basis gelegd voor de gemeentelijke systemen. Hierdoor is een technische informatiebeveiligingstest voor nu minder urgent. Wel wordt voor begin volgend jaar een nieuwe netwerkscan ingepland.

Gemeente Venray

Dit is de laatste RIB naar aanleiding van het rekenkameronderzoek. Wij zullen de raad regulier informeren over informatieveiligheid via de eerder genoemde jaarlijkse ENSIA-rapportage. Ook is Informatiebeveiliging en Privacy onderdeel van de reguliere rapportage conform het voorstel in het Informatiebeleidsplan (IBP).

Hoogachtend,

Het college van burgemeester en wethouders,

, burgemeester , secretaris