Informatiebeveiliging en privacy
Gemeente De Ronde Venen

Rapport

Rekenkamercommissie De Ronde Venen

- Definitieve versie -

Augustus 2022

Auteur: drs. Etienne Lemmens,

Prae Advies en onderzoek

Inhoudsopgave

Afbeelding titelpagina: Jan Alexander via Pixabay.

Samenvatting, conclusies en aanbevelingen

Rekenkameronderzoek

Vanaf december 2021 tot en met mei 2022 heeft de Rekenkamercommissie De Ronde Venen een onderzoek uitgevoerd naar het informatiebeveiligingsbeleid van de gemeente. De hoofdvraag luidt: *"Heeft de gemeente De Ronde Venen haar informatiebeveiliging op orde?"*

Aanpak

Vanwege de vele raakvlakken met het beleid hoe de gemeente De Ronde Venen omgaat met persoonsgegevens is ook (de uitvoering van) het privacybeleid meegenomen in dit onderzoek. Voor het onderzoek zijn beleidsdocumenten en rapportages op informatiebeveiliging en privacy bestudeerd. Daarnaast zijn in opdracht van de rekenkamercommissie enkele testen uitgevoerd op de systemen en is een phishingmail uitgezet onder de medewerkers van de gemeente. Daarnaast zijn interviews gehouden met een aantal sleutelpersonen op het gebied van informatiebeveiliging en privacy en van afdelingen die veel met uitvoering van het beleid te maken hebben.

In het onderzoek is aandacht geschonken aan de drie belangrijkste factoren die informatiebeveiliging bepalen: organisatie (beleid) – techniek (systemen) – mens (risicobewustzijn).

Hieronder volgt de beantwoording van de onderzoeksvragen, gevolgd door conclusies en aanbevelingen.

Beantwoording onderzoeksvragen

In deze samenvatting beantwoorden we de vier onderzoeksvragen:

1. Beschikt de gemeente De Ronde Venen over een adequaat informatiebeveiligingsbeleid?
2. Hoe wordt het beleid uitgevoerd en hoe wordt de uitvoering gemonitord?
3. In hoeverre zijn gegevens bij de gemeente beschermd tegen de toegang door onbevoegden?
4. Hoe wordt de gemeenteraad betrokken bij het informatiebeveiligingsbeleid?

Onderzoeksvraag 1 Beschikt de gemeente over een adequaat informatiebeveiligingsbeleid?

Informatiebeveiligingsbeleid

Het strategisch informatiebeveiligingsbeleid, vastgesteld in 2018, liep tot en met 2021. Deze was nog gebaseerd op de Baseline Informatiebeveiliging Gemeenten (BIG), dat vanaf 2020 vervangen is door de Baseline Informatiebeveiliging Overheid (BIO), het basisnormenkader voor informatiebeveiliging. Gemeld wordt dat er een nieuw beleid geformuleerd is, gebaseerd op de BIO, maar dat is vanwege de organisatieverandering nog niet vastgesteld. In het informatiebeveiligingsbeleid worden onder andere de ambitie beschreven en de verantwoordelijkheden op informatie-

beveiliging belegd. De ambitie van de gemeente is in control te zijn op het beveiligen van (persoons)informatie die de gemeente verwerkt. Het privacybeleid, dat samenhang kent met het informatiebeveiligingsbeleid en in 2018 is vastgesteld, wordt ook geactualiseerd. Jaarlijks wordt op basis van een GAP[1]- en risicoanalyse een uitvoeringsplan met activiteiten op informatiebeveiliging en privacy opgesteld.

Protocollen en richtlijnen

Onderdeel van het informatiebeveiligingsbeleid zijn protocollen en richtlijnen op de verschillende deelgebieden, zoals wachtwoordenbeleid en back-up en herstelbeleid. De meeste protocollen en richtlijnen zoals voorgeschreven door de BIO zijn aanwezig, maar op onderdelen missen nog protocollen. De gemeente is bezig met een procedure voor logging en is van plan aan de slag te gaan met een integraal bedrijfscontinuïteitsplan.

Aandacht

De aandacht voor informatiebeveiliging en privacy bij directie en college is volgens de respondenten aanwezig. Investeringen worden, mits goed onderbouwd, over het algemeen goedgekeurd. Verbetering van de positie van informatiebeveiliging en privacy kan plaatsvinden door het vroegtijdig in beleidsprocessen betrekken van de aspecten en functionarissen op informatiebeveiliging en privacy.

Onderzoeksvraag 2 Hoe wordt het beleid uitgevoerd en hoe wordt de uitvoering gemonitord?

Hierbij gaan we achtereenvolgens in op de functies op informatiebeveiliging en privacy en hun positionering, de overleggen en rapportages die hierin plaatsvinden, de (activiteiten op) bewustwording bij de medewerkers, leveranciers- en applicatiemanagement, de monitoring op de uitvoering van het beleid, het proces van verlenen van autorisaties tot applicaties en gegevens en tot slot handhaving.

Functies

De functies op informatiebeveiliging en privacy zijn ingevuld, zoals op strategisch niveau de Chief Information Security Officer (CISO) voor 0,8 fte en de Functionaris Gegevensbescherming (FG) voor 0,4 fte. Deze functionarissen worden naast hun strategische taken ook op tactisch en operationeel niveau ingezet. Op privacy is op tactisch gebied 1 fte voor de Privacyofficer (PO). Op tactisch en operationeel vlak is 0,5 fte privacy adviseur voor informatiebeveiliging en privacy en een netwerkbeheerder vanuit team I&A die daarnaast de taak van Technical Information Security Officer (TISO) heeft. Twee teams hebben nog apart een security officer. De teams hebben daarnaast ambassadeurs als eerstelijns aanspreekpunt.

De CISO en FG zijn bij de afdeling Control gepositioneerd en kunnen zelfstandig op strategisch niveau handelen. De PO is bij Juridische Zaken

[1] Met een GAP analyse wordt de bestaande situatie vergeleken met de gewenste situatie, namelijk voldoen aan de eisen van de BIO.

ondergebracht. De eisen aan deze en andere functies op informatisering en automatisering worden steeds zwaarder en het is voor kleine en middelgrote gemeenten lastig (extra) capaciteit uit de markt te halen.

Overleggen

Er zijn verschillende overleggen op informatiebeveiliging en privacy waar in wisselende samenstellingen CISO, FG en PO bij aansluiten. Overleggen zijn er tussen CISO en portefeuillehouder elk kwartaal, vaak informeel tussen CISO en team I&A en CISO en FG vaak met directielid en teamleider Control. Tweewekelijks breed overleg tussen gemeentesecretaris en teamleider I&A. Maandelijks is er het Privacy Informatieveiligheid Team (PIT) op strategisch niveau en meer operationeel het Privacyambassadeursoverleg (PIV). Recent is het tweemaandelijks adviseursoverleg. Naar aanleiding van de organisatieontwikkeling zal mogelijk de overlegstructuur op informatiebeveiliging en privacy opnieuw worden ingevuld.

Rapportages

Voor de verticale en horizontale verantwoording, richting respectievelijk landelijke toezichthouders en de gemeenteraad, stelt het college jaarlijks de verplichte Eenduidige Normatiek Single Information Audit (ENSIA) op. Daarin zijn externe en zelf-audits op belangrijke applicaties en databestanden opgenomen. Voorts stellen de CISO en FG jaarlijks een gecombineerd jaarrapport met betrekking tot informatiebeveiliging en privacy, en halfjaarlijks een voortgangsrapportage over de te nemen maatregelen. De gemeentesecretaris en portefeuillehouder krijgen updates over geconstateerde datalekken.

Bewustwording

Het aantal meldingen van datalekken neemt toe, wat een teken is dat het bewustzijn bij medewerkers op de risico's en incidenten toeneemt. In de interviews wordt ook gemeld dat medewerkers meer en meer zelf met oplossingen die in lijn liggen met de regelgeving conform BIO en AVG. Bewustwording vergt continue aandacht, omdat de risico's toenemen en de kennis snel wegebt. De gemeente organiseert ludieke activiteiten en biedt de medewerkers niet-verplichte trainingen aan. Het volwassenheidsniveau van de organisatie op informatiebeveiliging is in dit onderzoek niet gemeten, maar wordt op basis van waarnemingen tijdens het onderzoek geschat op een gemiddeld niveau tussen 2 (herhaalbaar) en 3 (gedefinieerd) op de schaal die Nederlandse Organisatie van Register EDP-Auditors (NOREA) hanteert.[2] Dat heeft tot gevolg dat de functionarissen op informatiebeveiliging en privacy, de CISO, FG en PO, ook nog veel op tactisch en operationeel niveau actief zijn.

Leveranciers- en applicatiemanagement

De algemene borging van leveranciers- en applicatiemanagement ligt bij contractmanagement. De privacyadviseurs in de teams hebben de opdracht het verwerkingsregister bij te werken en actueel te houden.

---

[2] De beroepsorganisatie van IT-auditors in Nederland (de Nederlandse Organisatie van Register EDP-Auditors, NOREA) hanteert een 5 puntenschaal om het volwassenheidsniveau van een organisatie op informatiebeveiliging te meten. Deze index is als bijlage 5 opgenomen.

Daaronder vallen ook de verwerkingsovereenkomsten die onder de contracten met betrekking tot verwerking van persoonsgegevens liggen. Ontwikkelingen hierop worden in het privacyambassadeursoverleg besproken.

Monitoring

De gemeente voert in het kader van ENSIA (zelf) audits uit en rapporteert daarover aan de landelijke toezichthouders en de gemeenteraad. Voorts zijn er de jaarrapportages en sinds kort de halfjaarlijkse voortgangs-rapportages. Instrumenten om de operationele monitoring uit te voeren zoals een zogenoemd SIEM/SOC en de logging op de applicaties. Door het mislukken van een landelijke aanbesteding van SIEM/SOC kan de gemeente zich gaan oriënteren op het zelf invullen van een dergelijke voorziening. Dat is nog niet gebeurd. Logging, het vastleggen van metadata, wordt op de meeste systemen uitgevoerd. Op Suwinet geschiedt de logging door de security officer die specifiek daarop zit. Er worden stappen gezet om de logging van de andere systemen systematisch te controleren.

Beveiligingsincidenten en datalekken worden bijgehouden en door de privacy ambassadeurs geanalyseerd. Verbetermaatregelen naar aanleiding van deze analyse worden aan de betreffende teamleider gerapporteerd.

(Pre-)Dpia's

Analyse van de risico's in verband met de verwerking van persoons-gegevens gebeurt door middel van data protection impact assessments (dpia). Er zijn circa 75 verwerkingsprocessen aangewezen als hoog risicovol. Daarop kan een oriënterende pre-dpia of uiteindelijk een volledig dpia gehouden worden. Er zijn nog slechts vijf dpia's en 16 pre-dpia's uitgevoerd. Met een beroep op de AVG kunnen inwoners om inzage in of vernietiging van door de gemeente geregistreerde persoonsgegevens verzoeken. In de periode 2020-2021 zijn 7 van dit soort verzoeken gedaan en deze zijn naar tevredenheid afgehandeld.

Autorisaties

Het autorisatieproces geeft aan hoe bepaald wordt wie toegang krijgt tot systemen, applicaties en gegevens. De toegangsrechten moeten gestoeld zijn op rollen en functies die medewerkers hebben, zodat voorkomen wordt dat medewerkers bij gegevens kunnen komen die zij niet mogen verwerken of inzien. Er zijn geen vaste toetsmomenten in het beleid opgenomen om te bezien of de autorisaties nog actueel zijn. De gemeente is van plan hiervoor een Identity- en Access Management (IAM) op te zetten. Met betrekking tot thuiswerken tijdens de coronapandemie is de toegang volgens de respon-denten goed geregeld. De toegang tot de digitale werkplek is via een 2 factor authenticatie (2FA) beveiligd.

Handhaving

In het kader van dit onderzoek is nader ingezoomd op de aspecten van informatiebeveiliging en privacy bij handhaving. Vanaf 2019 is in aanvulling op de AVG de Wet politiegegevens (Wpg) van kracht. Die wet regelt hoe Boa's om moeten gaan met informatie uit politiesystemen. Om onder andere te verbaliseren hebben zij niet zomaar toegang tot politiegegevens.

De Boa's gebruiken speciale beveiligde applicaties, zoals Citycontrol, om gegevens op te vragen of te delen met derden. Overige communicatie door en met de politie verloopt via de reguliere mail, die niet speciaal beveiligd is.

De gemeente heeft in 2021 een zelfaudit op de Wpg uitgevoerd en daaruit kwamen verbeteractiviteiten voort. De bedoeling is dat eind 2022 de uitvoering van de Wpg door een externe partij wordt geaudit.

Onderzoeksvraag 3 In hoeverre zijn gegevens bij de gemeente beschermd tegen de toegang door onbevoegden?

Technische bescherming

Technisch heeft de gemeente een aantal maatregelen genomen die de systemen beschermen tegen kwaadwillenden die binnen willen dringen, zoals firewalls, virusscanners, Network Access Control enz. En er zijn of er worden maatregelen genomen om de schade te beperken om als een kwaadwillende binnen is gedrongen, zoals logging en SIEM/SOC.

Eenmaal technisch iets geregeld hebben betekent niet dat de gemeente achterover kan leunen. Kwaadwillenden worden steeds vernuftiger in hun manieren om binnen te dringen. Er moet continu getest worden of de afweermechanismen voldoen aan de steeds hogere eisen. Dat gebeurt met behulp van ethische hackers die zogenoemde penetratietesten, of pen-testen, uitvoeren. De gemeente De Ronde Venen laat jaarlijks pentesten uitvoeren om de hardheid van de systemen te testen en om het risico-bewustzijn van medewerkers te testen. Daarnaast test de gemeente de uitwijk, om te bezien hoe snel na een storing of ramp de dienstverlening van de gemeente weer opgestart kan worden.

Pentesten

In het kader van het rekenkameronderzoek zijn aanvullende pentesten uitgevoerd door ethische hackers. Uitgevoerd zijn een externe en interne netwerk pentest, een Active directory audit, een phishing mail aanval en een inlooptest door een mystery guest. Vooraf is afgesproken dat de gemeente meteen op de hoogte gesteld zou worden als door de hackers een kritiek risico zou worden aangetroffen. Dat bleek niet nodig te zijn.

De testen leverden laag tot gemiddelde risico's op, geen kritieke risico's. Vanwege de kwetsbaarheden waar kwaadwillenden mogelijk gebruik van maken zijn de resultaten van deze testen vertrouwelijk gedeeld met de gemeentesecretaris. De gemeente kan dan aan de slag met de verbeter- en aandachtspunten uit de testen. Deze verbeterpunten hadden onder andere te maken met fysieke toegangsdrempels, het niet consequent toepassen van het wachtwoordenbeleid en risicobewustzijn van de medewerkers. Dat laatste is en blijft een continu aandachtspunt.

Onderzoeksvraag 4 Hoe wordt de gemeenteraad betrokken bij het informatiebeveiligingsbeleid?

Summier geïnformeerd

De raad heeft in het informatiebeveiligingsbeleid van de gemeente geen specifieke rol toebedeeld gekregen. Informatiebeveiliging wordt vooral opgevat als bedrijfsvoering, wat inhoudt dat in een kaderstellende rol met betrekking tot het informatiebeveiligingsbeleid niet wordt voorzien. In het kader van governance is in het informatiebeveiligingsbeleid wel opgenomen dat verantwoording aan de raad afgelegd moet worden.

P&C-cyclus, accountant

De raad wordt, conform de BIO, een keer per jaar over informatiebeveiliging en privacy geïnformeerd in het kader van de P&C-cyclus. Dat gebeurt summier en op hoofdlijnen over activiteiten en de resultaten van de audits in verband met ENSIA. Incidenteel komt informatiebeveiliging en privacy op de agenda van de raad, bij incidenten of een dreiging. De accountant gaat de laatste jaren meer in op aspecten van informatiebeveiliging en privacy, met name in relatie tot de financiële rechtmatigheid van de administratieve organisatie. Informatiebeveiliging en privacy zijn redelijk technische onderwerpen voor raadsleden, waarover zij weinig vragen stellen.

Niet ieder raadslid maakt gebruik van de beveiligde mailomgeving van de gemeente. De informatiebeveiliging van de raad zelf en de bewustwording daarop kan nog verder gebracht worden om hierop ‘in control’ te komen.

Conclusies

Algemeen

De onderstaande conclusies worden getrokken op basis van de bevindingen uit de interviews, deskresearch en pentesten uitgevoerd in het kader van het rekenkameronderzoek. De ontwikkelingen en de bedreigingen in de ICT-wereld zijn en blijven turbulent. De conclusies en aanbevelingen worden tegen de achtergrond gedaan dat de gemeentelijke dienstverlening plaatsvindt in dat continu veranderende IT-landschap en blijvend aandacht en investeringen zal vergen. De gemeente De Ronde Venen onderneemt de stappen om te voldoen aan de eisen die aan de uitvoering van informatiebeveiligings- en privacybeleid gesteld mogen worden. De in dit rapport gepresenteerde bevindingen geven aanleiding tot een positieve hoofdconclusie, zij het dat er binnen deze dynamiek door de gemeente ook nog stappen gezet moeten worden.

Hoofdconclusie	**De gemeente De Ronde Venen voldoet op hoofdlijnen aan de eisen zodat de informatiebeveiliging en privacy redelijk geborgd is maar blijvende inzet en aandacht is nodig om volledig in control te komen. Op alle niveaus kan het bewustzijn voor de risico’s die de gemeente loopt als informatie onvoldoende beveiligd is, verbeterd worden.**

Deelconclusies

Deze hoofdconclusie leidt tot de volgende deelconclusies:

1. Het informatiebeveiligings- en privacybeleid, samen in het informatie-veiligheidsbeleid, is actueel [3];
2. Op onderdelen moeten procedures en protocollen nog aangevuld worden;
3. Bewustwording van medewerkers krijgt aandacht, en blijft een punt van continue aandacht;
4. De formatie op informatieveiligheid is goed gepositioneerd en op niveau als deze functionarissen zich op hun strategische taken kunnen richten;
5. Informatiebeveiliging en privacy kunnen effectiever zijn als deze aspecten en de functionarissen daarop eerder worden betrokken in het beleids-proces;
6. Op basis van waarnemingen tijdens het onderzoek kan gesteld worden dat het gemiddelde taakvolwassenheidsniveau van de gemeentelijke organisatie op informatieveiligheidverhoogd kan worden;
7. De technische kant van informatieveiligheid kent, voor zover de scope van dit rekenkameronderzoek ging, geen kritieke risico's. Maar kan op punten nog verbeterd worden, zoals blijkt uit de pentesten in het kader van het rekenkameronderzoek;
8. De raad wordt te summier geïnformeerd over en te weinig betrokken bij informatieveiligheid, gelet op het belang van informatiebeveiliging voor de gemeentelijke dienstverlening;
9. De informatieveiligheid en risicobewustzijn van de raad vergt aandacht.

Aansporingen en aanbevelingen

De gemeente De Ronde Venen zet de nodige stappen om op informatie-beveiliging en privacy compliant te zijn. Omdat het beleidsveld zich snel ontwikkelt, brengt de rekenkamercommissie een onderscheid aan tussen aansporingen en aanbevelingen. Aansporingen om verder en versterkt in te zetten op activiteiten die al worden ondernomen en aanbevelingen op nieuw op te pakken activiteiten.

Aansporingen

De rekenkamercommissie wil het college aansporen op het ingeslagen pad verder te gaan door:

1. *Continu inzetten op bewustwording van medewerkers;*
2. *De ontbrekende protocollen en richtlijnen in het kader van informatie-veiligheidsbeleid op te stellen en aspecten op informatiebeveiliging en privacy eerder betrekken in beleidsprocessen;*
3. *(Pre-)Data protection impact assessments uitvoeren op geselecteerde verwerkingsprocessen;*
4. *Vormgeven van het autorisatieproces met behulp van het Identity en Access Management (IAM);*
5. *Vormgeven van de monitoring op de systemen door onder andere aanschaf van een SIEM/SOC;*

[3] Ervan uitgaande dat het informatiebeveiligingsbeleid 2022-2024 op korte termijn door het college wordt vastgesteld en in lijn is met de organisatieontwikkeling.

6. *Periodiek diverse (pen)testen en audits uitvoeren op de techniek (systemen), de organisatie (beleid) en de mens (risicobewustzijn) en ga aan de slag met de verbeterpunten uit de pentesten die in het kader van dit rekenkamer-onderzoek zijn uitgevoerd;*

Aanbevelingen

De conclusies leiden tot de volgende aanbevelingen op nieuw op te pakken activiteiten:

1. *Formuleer een ambitie om het gemiddelde volwasssenheidsniveau van de medewerkers van de gemeente te verhogen;*
2. *Betrek de raad meer bij het formuleren van ambities op informatieveiligheid en informeer de raad op de voortgang op deze ambities;*

Deze aanbevelingen worden hieronder nader uitgewerkt:

Aan college en raad

- Ga samen het gesprek aan om de huidige rapportages in het kader van de P&C-cyclus aan de raad in te vullen, zodat de raad voor zijn controlerende rol zicht krijgt op opzet, bestaan en werking van de maatregelen op informatiebeveiliging en privacy;

Aan de raad

- Geef het college de opdracht om:
    - aan de raad te rapporteren hoe de aansporingen zoals hierboven geformuleerd worden uitgevoerd;
    - een 0-meting uit te voeren op de volwassenheid van de medewerkers op basis van de NOREA-index en op basis daarvan een passend ambitieniveau te stellen;
    - in overleg met de griffie de informatieveiligheid van de raad zelf vorm te geven;
- Neem als raad meer dan nu het geval is de kaderstellende en controlerende rol op informatieveiligheid op en pak zelf de regie hierop:
    - Vul eventuele kennislacunes op door te scholen op het stellen van kritische vragen op informatiebeveiliging en privacy[4], of huur indien nodig externe expertise in voor een second opinion of pentesten;
    - Geef de accountant de opdracht consequent en systematisch onderzoek te doen en te rapporteren op aspecten op informatiebeveiliging.

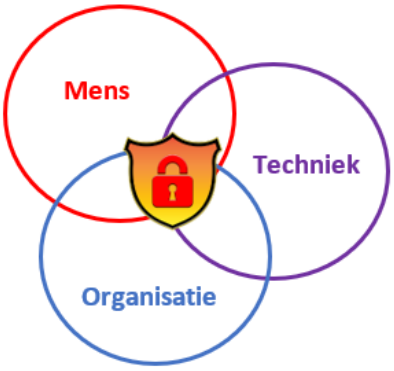
[4] Voorbeelden van vragen over informatiebeveiliging en privacy:
- Hoe recent is een GAP- en risicoanalyse op informatiebeveiliging uitgevoerd? Welke risico's accepteert de gemeente, op basis van welke afwegingen en onder welke voorwaarden?
- Zijn pentesten uitgevoerd? Zo ja, welke pentesten? Zijn de verbeterpunten in een plan van aanpak opgenomen?
- Hoeveel datalekken zijn gemeld bij de AP? Zijn de verbetermaatregelen daarop gerealiseerd?
- In hoeverre zijn de (pre)dpia's op de gegevensbewerkingsprocessen uitgevoerd? Zijn de verbeterpunten die daaruit naar voren komen opgepakt?
- Worden de aspecten informatiebeveiliging en privacy in de collegebesluiten meegenomen? Zo ja, op welke wijze?

1 Inleiding

Aanleiding

Onder andere door de toegenomen taken in het sociaal domein beheren en verwerken gemeenten meer en meer persoonlijke en gevoelige data. Gemeenten zijn daarbij kwetsbaar gebleken, zoals blijkt uit de datalekken die bij de Autoriteit Persoonsgegevens (AP) zijn gemeld, zware incidenten bij andere gemeenten en recente onderzoeken van verschillende rekenkamers. Wat gebeurt er bijvoorbeeld als die informatie op straat komt te liggen? Of als de digitale dienstverlening aan burgers niet meer mogelijk is? Naast financiële, juridische en technische gevolgen kunnen deze crises de privacy van burgers en het imago van de gemeente aantasten.

De Rekenkamercommissie De Ronde Venen wil de gemeenteraad inzicht geven in de stand van zaken op het gebied van informatiebeveiliging en privacy in de gemeente. Ten aanzien van informatiebeveiliging spelen drie aspecten een cruciale en op elkaar ingrijpende rol: mens – techniek – organisatie. De rekenkamercommissie adresseert deze drie aspecten in dit rapport.



Leeswijzer

Eerst worden in hoofdstuk 2 de doelstelling, onderzoeksvragen en de onderzoeksaanpak gepresenteerd. In hoofdstuk 3 gaan we in op het informatiebeveiligings- en privacybeleid van de gemeente. De uitvoering en monitoring van het beleid komen in hoofdstuk 4 aan bod. De bescherming van gegevens wordt in hoofdstuk 5 geadresseerd, inclusief de pentesten die in het kader van het rekenkameronderzoek zijn uitgevoerd. In hoofdstuk 6 komt de betrokkenheid van de raad op informatiebeveiliging en privacy aan bod.

In bijlage 1 zijn de geraadpleegde documenten opgenomen en de geïnterviewde functionarissen. In bijlage 2 is een verklarende woordenlijst opgenomen van termen en afkortingen die in het ICT-jargon worden gebruikt. In bijlage 3 zijn de normen, zoals gehanteerd in dit onderzoek, opgenomen en gerangschikt naar de onderzoeksvragen. In bijlage 4 worden de resultaten van de phishing test gepresenteerd, die in het kader van het rekenkameronderzoek is uitgevoerd. In bijlage 5 is de volwassenheidsindex van NOREA opgenomen.

2 Doelstelling, onderzoeksvragen en aanpak

2.1 Centrale onderzoeksvraag

De Rekenkamercommissie De Ronde Venen wil de volgende hoofdvraag beantwoorden:

"Heeft de gemeente De Ronde Venen haar informatiebeveiliging op orde?"

Daarbij gaat het om de veiligheid van gegevens en het beschermingsniveau van het gemeentelijke netwerk. Het doel dat de rekenkamercommissie nastreeft is, op hoofdlijnen en waar nodig, te bevorderen dat de door de gemeente beheerde informatie in veilige handen is en de bewustwording voor dit onderwerp te vergroten.

2.2 Onderzoeksvragen

De centrale onderzoeksvraag en doelstelling worden uitgewerkt aan de hand van de onderzoeksvragen zoals opgenomen in onderstaande tabel 1.

Tabel 1. Onderzoeksvragen

5.	**Beschikt de gemeente De Ronde Venen over een adequaat informatie-beveiligingsbeleid?**
6.	**Hoe wordt het beleid uitgevoerd en hoe wordt de uitvoering gemonitord?**
7.	**In hoeverre zijn gegevens bij de gemeente beschermd tegen de toegang door onbevoegden?**
8.	**Hoe wordt de gemeenteraad betrokken bij het informatiebeveiligings-beleid?**

Voor de normen bij deze onderzoeksvragen verwijzen we naar bijlage 3.

2.3 Onderzoeksaanpak

Het onderzoek bestaat uit drie verschillende onderdelen, nl. deskresearch, interviews en pentesten.

Deskresearch

Met betrekking tot beleid en de protocollen is deskresearch gepleegd. Een overzicht van de geraadpleegde documenten is in bijlage 1 opgenomen.

Interviews

Met acht bestuurlijke en ambtelijke sleutelfiguren is een interview afgenomen. Een lijst met geïnterviewde functionarissen is ook in bijlage 1 opgenomen.

Pentesten

Een ander onderdeel om de uitvoering te onderzoeken bestond uit pentesten. Pentesten, voluit penetratietesten, worden uitgevoerd door ethisch hackers en geven inzicht in het beveiligingsrisico van de organisatie. De pentesten zijn grotendeels gericht op de technische kant van informatie-beveiliging, en ook deels op de naleving van beleid en procedures. Deze zijn uitgevoerd door ethische hackers van Awaretrain en IP4Sure.

Besloten is in het kader van het rekenkameronderzoek een externe en interne netwerk pentest, Active Directory-audit, wifi-netwerkpentest, phishing test en een inlooptest met behulp van een mystery guest uit te voeren. Voor een uitleg van de testen en de testresultaten zie §5.2.

Hoor en wederhoor

Op 11 juli 2022 is de nota van bevindingen voor de feitencheck in het kader van de ambtelijke hoor en wederhoor aangeboden aan de gemeentesecretaris. De nota van bevindingen is daarna aangevuld met conclusies en aanbevelingen en op 1 september 2022 voor een bestuurlijke reactie voorgelegd aan het college van B&W. Daarna is het rapport met een nawoord van de rekenkamercommissie op 10 november 2022 aangeboden aan de gemeenteraad.

3 Beleid van de gemeente

Onderzoeksvraag 1

In dit hoofdstuk geven we antwoord op de eerste onderzoeksvraag: "Beschikt de gemeente De Ronde Venen over een adequaat informatiebeveiligingsbeleid?"

Informatiebeveiligingsbeleid

Het strategisch informatiebeveiligingsbeleid is 4-12-2018 vastgesteld door het college van B&W en loopt tot en met 2021. Een nieuw beleid voor de periode na 2021 was op moment van onderzoek nog niet vastgesteld door directie en college van B&W, mede vanwege de gemeenteraadsverkiezingen. Begin 2022 is veel aandacht van de functionarissen op informatiebeveiliging en privacy uitgegaan naar de rapportages, zoals de Eenduidige Normatiek Single Information Audit (ENSIA, zie ook §4.3) en de interne jaarrapportages. Daardoor kon het 'oude' college de rapportages nog vaststellen.

In het strategisch beleid is de ambitie van de gemeente met betrekking tot informatiebeveiliging neergelegd. De gemeente De Ronde Venen heeft de ambitie om in control te zijn op het beveiligen van (persoons)informatie waarmee binnen de gemeente wordt gewerkt en waarvoor de gemeente verantwoordelijk is. Het beleid is gebaseerd op de Baseline Informatiebeveiliging Gemeenten (BIG), maar loopt ook al vooruit op de Baseline Informatiebeveiliging Overheid (BIO) die vanaf 2019 de BIG vervangt. De BIO is meer risicogestuurd dan de BIG en bevat minder voorgeschreven maatregelen.

Verantwoordelijkheden

De verantwoordelijkheden van alle doelgroepen, in- en extern, worden in het gemeentelijk beleid belegd. Van het college van B&W, directie en lijnmanagement tot de auditors, leveranciers en ketenpartners. De gemeenteraad is opgenomen bij de governance, zonder specifieke rol. Behalve dat verantwoording afgelegd dient te worden aan de raad in het kader van de governance.

Het nieuwe en nog niet vastgestelde strategisch informatiebeveiligingsbeleid van de gemeente De Ronde Venen houdt rekening met de Agenda Digitale Veiligheid 2020-2024 van de VNG. In die agenda zijn op de vier thema's Awareness, Governance, Risicogericht handelen en Eén overheid/samen organiseren in totaal 10 bestuurlijke actielijnen opgenomen.[5] De gemeente is momenteel in een proces van

[5] De 10 bestuurlijke actielijnen op de vier thema's uit de Agenda Digitale Veiligheid 2020-2024 zijn:
Awareness: 1. Bewustzijn vergroten; 2. Weerbare organisatie; 3. Digitale brandoefening;
Governance: 4. Decentrale verantwoording waar kan, centraal toezicht waar moet; 5. OOV bevoegdheden en rollen voor de lokale bestuurders;
Risicogericht handelen: 6. Lokale vitale processen bepalen vanuit maatschappelijke taken; 7. Krachtige partner in de keten; 8. Risicomanagement geeft focus;
Eén overheid/samen organiseren: 9. Informatiebeveiligingsdienst gemeenten verbreden en versterken; 10. Eén overheid.

organisatieverandering en het is volgens respondenten nog onduidelijk hoe de teams en functies er precies uit gaan zien. Na de zomer van 2022 zal de organisatieverandering een start krijgen en zullen betrokken functies (zoals CISO, FG, Privacy Officer wellicht een andere plaats in de organisatiestructuur krijgen.[6]

Jaarplan

Op basis van een GAP- en risicoanalyse wordt jaarlijks een uitvoeringsplan opgesteld. Voor de GAP-analyse maakt de gemeente gebruik van een zogenoemde Governance-Risk-Compliance-tool (GRC). Daarin wordt de stand van zaken met betrekking tot informatiebeveiliging gekoppeld aan de normen in de BIO. Inzichtelijk wordt in hoeverre de gemeente compliant is, waar de risico's aanwezig zijn en welke activiteiten ondernomen moeten worden. Dat vormt meteen de basis voor de beleidscyclus Plan-Do-Check-Act (PDCA).

Vanaf 2021 werkt de gemeente met een gezamenlijk jaarplan voor informatiebeveiliging en privacy. De resultaten uit de GAP-analyse zijn in eerste instantie besproken met de privacy ambassadeurs in de teams (voor de functies op informatiebeveiliging en privacy zie §4.1). In november 2021 hebben de CISO en privacy adviseurs de activiteiten voor het jaarplan 2022 met de teamleiders besproken. Maart 2022 is het jaarplan vastgesteld door directie. Er staat onder andere de monitoring in, een aantal activiteiten op bewustwording, data protection impact assessments (dpia's), en risicoanalyses op informatiebeveiliging.

Privacybeleid

Er is een in april 2018 vastgesteld Privacybeleid, gebaseerd op de AVG, met een bijbehorend privacyreglement. De gemeente is bezig met een actualisatie van het privacybeleid, naar aanleiding van de toetsing van de hiervoor genoemde Governance-Risk-Compliance-tool (GRC). Ten tijde van het onderzoek was het nieuwe beleid in concept opgesteld. Op een organisatieonderdeel is een domeinspecifiek beleid opgesteld, namelijk een privacyprotocol voor Integrale Veiligheid. Dat is een handboek waarin medewerkers wordt uitgelegd hoe men moet omgaan met de AVG, verwerkingen, het verwerkingsregister, de procedure met betrekking tot datalekken enz.

Wpg

Voor organisaties waar Boa's werken geldt naast de AVG aanvullend ook de Wet politiegegevens (Wpg). Deze wet kent specifiekere regels dan de AVG, onder andere hoe gemeentelijke Boa's met politiegegevens moeten omgaan. De Wpg is sinds 2019 ingevoerd. Het is de bedoeling dat de regelingen op de Wpg als addendum bij het nieuw te formuleren privacybeleid worden opgenomen. Voor een nadere uitleg van de Wpg zie §4.8.

---

[6] Uit de ambtelijke hoor en wederhoor blijkt dat de CISO en FG gepositioneerd worden in Team Concerncontrol, onder directe aansturing van de CFO als directielid. De Privacy Officer wordt in Team Financiën, inkoop en juridische zaken gepositioneerd, onder aansturing van de teammanager.

Samenwerking

Veel kleinere en middelgrotere gemeenten werken samen op ICT, ondergebracht bij een gemeenschappelijke regeling of bij een gemeente die als gastheer op ICT en eventueel andere PIOFACH-terreinen fungeert. De gemeente De Ronde Venen heeft de automatisering zelfstandig ingericht. In de eigen organisatie, met een eigen infrastructuur waarbij onderdelen door externe partners worden beheerd. Er was in het verleden sprake van om met andere gemeenten te participeren in Duo+ [7], maar daar heeft de gemeente De Ronde Venen uiteindelijk niet voor gekozen.

Protocollen

In het kader van informatieveiligheid (informatiebeveiliging en privacy) schrijft de Informatie Beveiligingsdienst (IBD) voor dat er aanvullende protocollen zijn die richtlijnen bevatten voor de verschillende deelgebieden. Op de onderstaande punten zijn protocollen/richtlijnen aanwezig in gemeente De Ronde Venen die voldoen aan de eisen van de IBD:

- Afvoer ICT-middelen
- Back-up en herstelbeleid
- Beheer applicaties
- Beleid dataclassificatie
- Beleid logische toegangsbeveiliging
- Beleid mobiele gegevensdragers
- Beleid uitwisseling informatie
- Clear desk en -screen en -ruimte
- Encryptiebeleid
- Fysiek toegangsbeleid
- Incident- en datalekmanagement
- Ingescande handtekening
- Melding kwetsbaarheden
- Procedure patchmanagement
- Thuiswerken
- Uitwijkplan veiligheidsplan
- Wachtwoordgebruik en Identity Access Management (IAM)
- Websitebeveiliging

Wat mist?

De gemeente is bezig met de procedure voor de logging van gegevens op de verschillende applicaties. Op een aantal systemen wordt het dataverkeer al gelogd (zie ook §4.6). Zo ook op Suwinet en het zaaksysteem met de DigiD-aansluiting wordt gelogd, omdat dat landelijk verplicht is gesteld. Dat wordt gecontroleerd door landelijke toezichthouders in het kader van ENSIA (zie ook §4.3). Zo is op delen van het systeem, zoals het financiële systeem, logging aanwezig. De nieuw op te stellen procedure is ervoor om de loggings bijeen te brengen zodat ze systematisch gecontroleerd kunnen worden.

[7] DUO+ is de uitvoeringsorganisatie op bedrijfsvoering van Ouder-Amstel, Diemen en Uithoorn. De uitvoering van de Basisregistratie Grootschalige Topografie (BGT) is door De Ronde Venen ondergebracht bij Duo+.

Continuïteitsbeleid

Een integraal bedrijfscontinuïteitsplan, waarbij informatiebeveiliging een integraal onderdeel is van het bedrijfscontinuïteitsbeheer, is er nog niet. Op onderdelen zijn er wel al continuïteitsplannen aanwezig, zoals bijvoorbeeld een uitwijkplan. De bedoeling is op korte termijn met het nieuw college en de directie de noodzaak van een integraal plan vast te stellen en eventueel de middelen daarvoor vrij te maken. Daarna kunnen CISO, PO, team I&A, team Integrale Veiligheid en andere teams aan de slag om het integrale plan op te stellen. In interviews wordt aangegeven dat bij de teams I&A en Integrale veiligheid het bewustzijn hierop aanwezig is. Deze teams nemen, samen met de CISO en PO het voortouw, maar uiteindelijk moet het plan door alle geledingen en medewerkers gedragen worden.

Draagvlak

Respondenten geven aan dat het college van B&W open staat voor aangelegenheden op informatiebeveiliging en gegevensbescherming. Het is geen top prioriteit. Zo worden de CISO en PO niet altijd vooraan in beleids-processen meegenomen en is er bijvoorbeeld in de collegevoorstellen geen kopje ‘informatiebeveiliging en privacy’ opgenomen. Daardoor is het niet zeker dat de punten op informatiebeveiliging en privacy op voorhand mee worden genomen in de overwegingen bij beleidsvoorstellen.

Respondenten geven wel aan dat er draagvlak is voor de noodzakelijke investeringen.[8] De meeste, zo niet alle aanvragen zijn tot nu toe goedgekeurd naar aanleiding van gesprekken met management en bestuur (college van B&W en de raad.) Op de hoeveelheid gemeentelijke beleidsterreinen zijn er makkelijk andere investeringsprioriteiten denkbaar. Het college geeft aan de raad dat het werkveld gezien de dreigingen en risico’s nooit af is en dat niets doen geen optie is. Er is voor 2022 een budget van €70.000 vastgesteld, verdeeld over privacy adviseurs, CISO en FG. Dat is door deze functionarissen te besteden aan (bewustzijn bevorderende) activiteiten op informatiebeveiliging en privacy (zie ook §4.4).

8 De intentie is er bij het in 2022 nieuw aangetreden college om informatiebeveiliging en privacy serieus te nemen. In het Coalitieakkoord 2022-2026, dat gereed kwam tijdens de afronding van het onderzoek is onder hoofdstuk Handhaving Openbare Orde en Veiligheid opgenomen: “Wij geven prioriteit aan een digitaal weerbare gemeente. We zetten ons in om te voorkomen dat inwoners en bedrijven slachtoffer worden van cybercrime en gedigitaliseerde criminaliteit. Ook zorgen we ervoor dat de informatiebeveiliging van de gemeente op orde is en dat we goed voorbereid zijn op cybercrisis en online aangejaagde ordeverstoringen.” En onder het hoofdstuk Bedrijfsvoering, Dienstverlening en ICT staat: “We gaan zorgvuldig met gegevens van inwoners om. We houden hun gegevens veilig. We investeren in de ICT om dit op een kwalitatief goede manier mogelijk te houden. De organisatie moet op dit gebied up to date en veilig zijn en blijven.”

4 Uitvoering en monitoring van het beleid

Onderzoeksvraag 2

In dit hoofdstuk geven we antwoord onderzoeksvraag 2: Hoe wordt het beleid uitgevoerd en hoe wordt de uitvoering gemonitord?

Hieronder gaan we in op verschillende aspecten van de uitvoering en de monitoring daarvan. Daarbij worden achtereenvolgens behandeld: de functies op informatiebeveiliging en privacy, overleggen, rapportages op informatiebeveiliging en privacy, bewustwording, leveranciers- en applicatiemanagement, monitoring, autorisatieproces en handhaving.

4.1 Functies

Functies/taken

Alle functies op informatiebeveiliging en privacy zijn ingevuld. Met 0,8 fte voor de Chief Information Security Officer (CISO), 0,4 fte (18 uur) voor de Functionaris gegevensbescherming (FG) en in totaal 1 fte voor PO. Tijdelijk is er ruimte voor 0,5 fte voor een privacy adviseur. Ondanks de naam privacy adviseur heeft deze functie ook taken op informatiebeveiliging. Daarnaast is er ondersteuning vanuit het team I&A, waarbij een netwerkbeheerder de taak Technical Information Security Officer (TISO) heeft, en een waarnemer voor de CISO als deze uitvalt. Ten slotte zijn er sinds 2018 privacy ambassadeurs in de teams aanwezig. Dat zijn medewerkers die een training op informatiebeveiliging en privacy hebben gevolgd en aanspreekpunt zijn voor de CISO, FG en privacy adviseurs enerzijds en medewerkers uit de teams anderzijds.

Voorts zijn op twee applicaties specifieke functies ingericht voor security officers. Dat is op SUWI en BRP/reisdocumenten. Deze functies zijn op tactisch en operationeel gebied actief met betrekking tot de informatiebeveiliging op deze applicaties.

Positionering

De CISO en FG zijn adviserend en controlerend op strategisch niveau werkzaam en sinds 2020 bij de afdeling Control gepositioneerd. De privacy officers zijn bij Juridische Zaken gepositioneerd, terwijl de privacy ambassadeurs in de diverse teams aanwezig zijn.[9] De FG en CISO hebben mandaat om onafhankelijk ten opzichte van het management op strategisch niveau te kunnen opereren. Zij kunnen indien nodig meteen met de gemeentesecretaris schakelen.

Tevens zijn de FG en CISO ook nog op operationeel vlak met bewustwording bezig (zie ook §4.4). Zoals bij de vraagbaak waar jaarlijks 100-120 vragen binnenkomen die snel beantwoord moeten worden.

Capaciteit

De functies op ICT, informatiebeveiliging en privacy zijn ingevuld. De eisen die aan de functies worden gesteld worden door de ontwikkelingen op

[9] Zie voetnoot 2.

veiligheidsgebied steeds hoger. Zoals het installeren van patches (aanvullende programma onderdelen) en de updates (nieuwe software versies). In de interviews wordt aangegeven dat het voor een kleinere gemeentelijke organisatie een uitdaging is voldoende capaciteit, kennis en kunde te blijven regelen. En een aantrekkelijk functiegebouw te kunnen aanbieden in een hoog competitieve arbeidsmarkt.

4.2 Overleggen

Voor de reguliere bespreking van zaken op informatiebeveiliging en privacy zit de CISO een keer per kwartaal met de bestuurlijk portefeuillehouder om de tafel. Regelmatig schuift de CISO bij team I&A aan voor informeel overleg en uitwisseling van kennis. De CISO en FG hebben een lijn met de direct leidinggevende van de afdeling Control, die directielid is. Met de gemeentesecretaris is ook contact, onregelmatiger en als de noodzaak daartoe aanwezig is. Verder heeft de gemeentesecretaris met de teamleider I&A tweewekelijks een overleg, dat breder gaat dan alleen informatiebeveiliging. In de organisatie zijn diverse overlegstructuren opgezet om de lijnen tussen de verschillende functies zo kort mogelijk te houden.

PIT

Maandelijks is het overleg in het Privacy Informatieveiligheid Team (PIT-), waarin zaken op informatiebeveiliging op strategisch niveau worden besproken en uitgewisseld tussen systeembeheerders en management. Onder andere het jaarplan informatiebeveiliging en de ENSIA audits (zie §4.3). De CISO, teamleider I&A en andere teamleiders nemen deel aan het PIT. De FG is bij dit overleg in de rol van toehoorder.

PIV

Sinds medio 2018 is er elke maand het Privacyambassadeursoverleg (PIV). Dit overleg is met name operationeel. De CISO, FG, privacy officers en privacy ambassadeurs nemen hieraan deel. De eerst genoemde functionarissen bespreken de ontwikkelingen op het gebied van informatiebeveiliging en privacy. De privacy ambassadeurs hebben een haal- en brengfunctie richting de eigen teams. Zij vormen de link om de ontwikkelingen naar de teams te vertalen en tegelijk eventuele vraagstukken en ontwikkelingen vanuit de teams in het Privacyteam te brengen. Acties die de teams moeten ondernemen worden daar besproken.

Adviseursoverleg

Recent is gestart met een tweemaandelijks adviseursoverleg met functionarissen op informatieveiligheid, privacy en informatievoorziening. Daarmee kunnen de CISO, FG en de privacy adviseurs vroeg bij ontwikkelingen vanuit I&A betrokken worden.

De gemeente is momenteel bezig met een organisatiewijziging, waarmee de behoefte aan overleggen om elkaar op de hoogte te houden van ontwikkelingen en vraagstukken op informatiebeveiliging en privacy mogelijk anders zullen worden ingevuld.

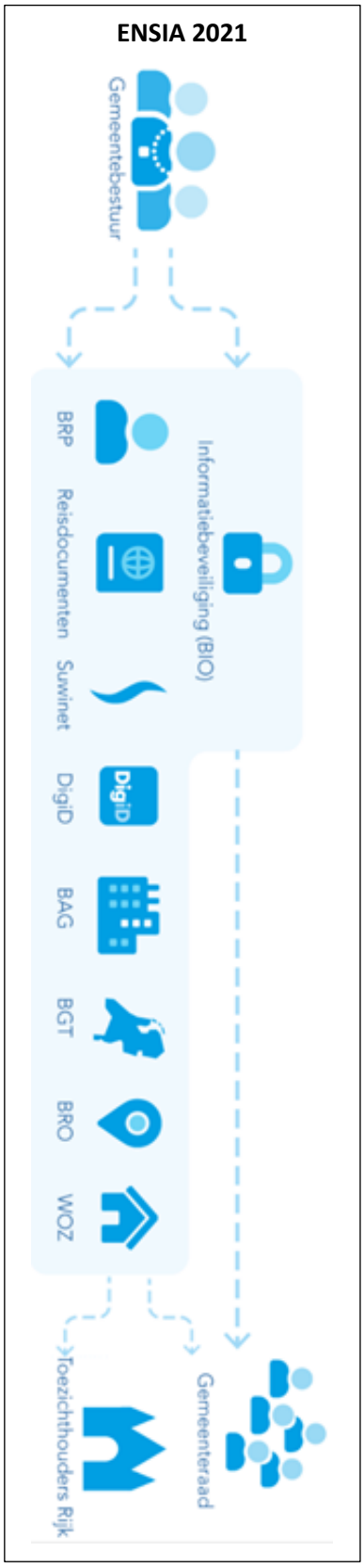
Externe overleggen

Extern hebben de CISO en FG in regionaal verband via de VNG en IBD overleggen als bron voor informatie, intervisie en inspiratie. Daarnaast is er ad-hoc contact met andere (omliggende) gemeentelijke CISO's en FG'en. De CISO komt vanwege samenwerkingsverbanden ook met CISO's uit Noord-Holland en Groene Hart bijeen, en met een aantal CISO's in een overleg bij de IBD.

4.3 Rapportages

ENSIA

Over informatiebeveiliging worden verschillende rapportages opgesteld. De jaarlijkse ENSIA-rapportage maakt een belangrijk onderdeel uit van de P&C-cyclus. Hierin staat de verticale verantwoording (landelijke toezicht-houders) en de horizontale verant-woording (gemeenteraad) centraal. Op de verschillende applicaties waar de gemeente mee werkt worden door de lijn (zelf)audits uitgevoerd. Daarvoor wordt gebruik gemaakt van een Information Security Management System (ISMS). De zelfevaluaties worden gecheckt door de CISO, die de ENSIA-coördinator is. Deze levert de rapportage op aan de directie en de portefeuillehouder. De applicaties Suwinet en DigiD worden door externe auditoren uitgevoerd en door de landelijke toezichthouders gecontroleerd. Uit de audits voor de ENSIA komen verbetermaatregelen op informatie-beveiliging en gegevensbeheer die in een plan van aanpak worden opgenomen.



Assuranceverklaring

Het college van B&W rapporteert de uitkomst van de ENSIA-audits ook naar de raad toe, in een paragraaf in de jaarrapportage (zie ook hoofdstuk 6). Volgens de interviews voldoen DigID en Suwinet over 2021 aan de gestelde normen en kwalificeert een externe auditor het assurance rapport over de collegeverklaring als juist.

Jaarrapport

De FG stelt dat sinds de AVG in 2018 het jaarrapport over de activiteiten op privacy opgesteld wordt. Vanaf 2021 stellen FG

en CISO een gecombineerde voortgangsrapportage op over informatiebeveiliging en privacy. Dat is in 2022 door de directie vastgesteld en vanwege de verkiezingen opgenomen in het overdrachtsdocument voor het nieuwe college. Normaal gesproken gaat het jaarrapport naar de directie en vervolgens wordt het met een informatienota aangeboden aan het college. De verbeterpunten uit de rapportage worden opgepakt.

Voortgangsrapportages

Halfjaarlijks stellen de CISO, PO en de FG voortgangsrapportage op met betrekking tot de activiteiten in de jaarplannen. Dat is een dashboard met de voortgang op de actiepunten. De FG is van plan jaarlijks voor een afdeling een beleidsaudit te starten. Te beginnen bij afdelingen waar de risico's met betrekking tot de verwerking van persoonsgegevens groot zijn, zoals het sociaal domein en integrale veiligheid. Voor informatiebeveiliging is er het Information Security Management System (ISMS) om de activiteiten te beleggen en over te rapporteren, voor de AVG en Wpg is een zogenoemd Data Protection Management System (DPMS) aanwezig.

Datalekken

De gemeentesecretaris en verantwoordelijk portefeuillehouder krijgen regelmatig updates van de gemelde datalekken. Over 2020 zijn 17 datalekken geregistreerd, waarvan 6 aan de Autoriteit Persoonsgegevens (AP) gemeld zijn. In 2021 zijn 27 incidenten als datalek gemeld waarvan 5 aan de AP zijn doorgegeven. Het merendeel van de datalekken komen door het delen van bestanden met persoonsgegevens via de mail of door verkeerd adresseren via de mail. Dat is overeenkomstig het beeld dat de AP in de jaarverslagen schetst over de datalekken in het algemeen.

4.4 Bewustwording

Wat gaat goed?

De meeste respondenten geven aan dat de uitvoering van het informatie-beveiligings- en privacybeleid goed gaat en dat het bewustzijn van de medewerkers op de risico's en incidenten toeneemt. Geconstateerd wordt dat een verkeerd gemaild bestand met persoonsgegevens als datalek wordt gemeld en dat was tot voor kort minder het geval. De boodschap is "je bent een held als je het meldt." Ook wordt geconstateerd dat medewerkers in toenemende mate zelf met oplossingen komen die in lijn met de BIO of AVG zijn. De vraag tegenwoordig is meer "klopt het als ik het zo aanpak" in plaats van "wat moet ik doen?" Tegelijkertijd geven de respondenten aan dat bewustwording continu aandacht vraagt. De veiligheidsrisico's nemen toe, onder andere omdat kwaadwillenden slimmere manieren bedenken om informatie of inloggegevens te ontfutselen of in de systemen te komen.

Trainingen?

De gemeente onderneemt veel activiteiten om de bewustwording bij medewerkers structureel te stimuleren. Zo biedt de gemeente trainingen aan via de E-learning omgeving. Hoewel de deelname aan de trainingen niet verplicht is, wordt deze wel gemonitord in afdelingsverband. Met de teamleiders is afgesproken dat aandacht in teamverband aan de deelname aan deze activiteiten wordt besteed.

Specifieke aandacht

Voor medewerkers die betrokkenen zijn bij de applicatie Suwinet is het volgen van E-learning wel verplicht. Dat wordt vanuit landelijke regelgeving in het kader van ENSIA-verantwoording afgedwongen. Bij DigID, ook een applicatie die in de ENSIA-verantwoording wordt meegenomen, is dat niet het geval. Vanuit de gemeente wordt deelname wel gestimuleerd.

In 2020 hebben de afdelingshoofden en teamleiders van de Afdeling Dienstverlening, Sociaal Domein en Inrichting, Beheer en Openbare Ruimte (IBOR) een training op informatiemanagement gevolgd. De hoofden van de andere afdelingen hebben deze in 2021 aangeboden gekregen.

Ludieke activiteiten

Ook wordt geprobeerd via luchtige en competitieve acties bewustzijn te stimuleren. Zo krijgen de medewerkers elke maandag via de mail een vraag voorgelegd over informatiebeveiliging en gegevensbescherming van 'Sir Askalot'. En er is een PIV-week met verschillende ludieke activiteiten op informatiebeveiliging en privacy, zoals een pub-quiz en een escaperoom. Deze week is door corona niet doorgegaan in 2020 en '21. Voor 2022 staat de week in de planning.

Ambassadeurs

Respondenten geven aan dat medewerkers de functionarissen op informatiebeveiliging en privacy makkelijk weten te vinden met vragen. Op ad hoc basis of op verzoek komen privacy adviseurs langs bij de teamoverleggen. Ook geven ze aan dat de privacy ambassadeurs in de teams drempelverlagend werken voor medewerkers om vragen te stellen. De boodschap landt makkelijker als die van directe collega's komt. Als vragen zo opgelost kunnen worden ontlast dat ook de privacy adviseurs, FG en CISO.

Volwassenheid

NOREA (de beroepsorganisatie voor IT-auditors) heeft een volwassenheids-index op informatiebeveiliging opgesteld (zie bijlage 5). Deze geeft aan in hoeverre de proceseigenaren binnen een organisatie activiteiten op informatiebeveiliging beheersen en planmatig uitvoeren. Een meting van de volwassenheid is niet door of namens de gemeente uitgevoerd en heeft ook niet plaatsgevonden in het kader van dit rekenkameronderzoek. Toch is het nuttig in dit kader kennis te nemen van het volwassenheidsmodel van NOREA.

De gemeentelijke organisatie is breed en kent veel diverse processen waarin informatiebeveiliging en privacy een wisselende rol van belang spelen. Het volwassenheidsniveau kan dan ook per team en proces verschillen. Zo worden in het kader van ENSIA strenge eisen gesteld aan de procedures rond Suwinet en DigiD. De medewerkers die daarmee te maken hebben zullen op taakvolwassenheid hoger scoren dan medewerkers van andere teams. Daarbij gaat het met name om het consistent en gestructureerd uitvoeren en aantoonbaar vastleggen van beheersingsmaatregelen, zodat deze administratief getoetst kan worden.

Gelet op hetgeen in de interviews is aangegeven en de accountant constateerde in de managementletter (zie hoofdstuk 6) met betrekking tot het vastleggen van (controle)activiteiten is de inschatting dat het gemiddelde volwassenheidsniveau van de gemeentelijke organisatie tussen niveau 2 (herhaalbaar) en 3 (gedefinieerd) zal liggen.

4.5 Leveranciers- en applicatiemanagement

Verwerkingsregister

In het verwerkingsregister houdt de gemeente bij in welke processen persoonsgegevens door en/of namens de gemeenten worden verwerkt. Daarbij heeft de gemeente ook in beeld welke externe partijen daarbij betrokken zijn. Key2control wordt als applicatie gebruikt om het verwerkingsregister en de verwerkingsovereenkomsten onder de contracten actueel te houden. Het verwerkingsregister wordt periodiek bijgewerkt door de privacy adviseurs en wanneer daartoe aanleiding is vanwege veranderende wet- en regelgeving, verandering in proces, etc. Medewerkers worden bevraagd of er verwerkingen zijn die nog niet in het verwerkingsregister zijn opgenomen.

De dienstverlening van een gemeente is breed en dat betekent dat er een veelvoud aan processen en applicaties aanwezig zijn, met veel leveranciers. Er is een brede mix van systemen, met eigen rekencentrum, applicaties en systemen in de cloud. In het PIV-overleg worden ontwikkelingen, aanbestedingen en contracten besproken in relatie tot eisen op het gebied van informatiebeveiliging en privacy. De algemene borging van leveranciersmanagement ligt buiten het gebied van informatiebeveiliging en privacy, en wordt meer beschouwd als onderdeel van contractmanagement.

Patches en updates

Met de toegenomen risico's en de snelle ontwikkelingen in informatiebeveiliging neemt de druk toe om de applicaties up to date en veilig te houden. Daartoe brengen softwareleveranciers updates (nieuwe versies) en patches (aanvullende programmaonderdelen) uit. Dat levert werkdruk op bij de afdelingen die de updates en patches moeten testen en installeren. Zo brachten grote en gerenommeerde leveranciers bij het softwarelek in verband met Log4J [10] snel hun patches uit die dan ook snel geïmplementeerd konden worden. Bij de kleinere ontwikkelaars duurde dat langer voordat ze met een patch kwamen.

[10] Log4J, of Apache Log4J, is een stuk software dat veel in webapplicaties en andere systemen wordt gebruikt. OP 12 december 2021 gaf het Nationaal Cyber Security Centrum (NCSC) de waarschuwing af dat Log4J kwetsbaar was. Op 17 september actualiseerde de NCSC de waarschuwing dat er aanvullend nog een ernstige kwetsbaarheid in Log4J was aangetroffen. Om dat te repareren brengen softwareontwikkelaars patches uit.

4.6 Monitoring

In control

De respondenten geven aan dat het lastig is te zeggen dat de gemeente in control is op informatiebeveiliging en privacy. Onduidelijk zijn de dreigingen, zoals de al voor februari 2022 toegenomen aandacht van Russische groepen hackers voor westerse overheidssites. Binnen de kaders van wat geweten kan worden, en de risico's die in beeld zijn, vinden respondenten dat de gemeente in control is. Op de verbeterpunten uit de audits en de risico's die niet geaccepteerd worden, worden activiteiten in de jaarplannen opgenomen. De CISO en FG kunnen zaken oppakken die zij nodig achten en op noodsituaties reageren, onafhankelijk van de lijn.

Log4J

Zo kon snel gehandeld worden op de dreiging van Log4J. De gemeente-secretaris van De Ronde Venen was de eerste gemeentesecretaris die met de coördinerend gemeentesecretaris in de veiligheidsregio hierover contact opnam. Het is evenwel geen garantie dat de gemeente niets zou kunnen overkomen. Het is zaak de drempels om binnen te komen zo hoog mogelijk te hebben en als kwaadwillenden eenmaal binnengedrongen zijn dat snel te detecteren en de eventuele schade zoveel mogelijk te beperken. Daartoe zijn middelen voorhanden, zoals een Security Information & Event Management/Security Operations Center (SIEM/SOC) [11]en logging.

SIEM/SOC

Een manier om vroegtijdig verdacht verkeer op de servers en de systemen te detecteren is een zogenoemde Security Information & Event Management (SIEM) en Security Operations Center (SOC). De gemeente participeerde in het kader van GGI-Veilig [12], een portfolio van producten op informatiebeveiliging van de VNG, in een gezamenlijke aanbesteding voor een SIEM/SOC oplossing. In die aanbesteding zijn problemen ontstaan en de gemeente kan niet naar een andere leverancier overstappen.[13] Momenteel waarschuwt een intern monitoringsysteem voor verdacht netwerkverkeer. Maar vanwege de allround detectie wordt een SIEM/SOC gemist door de medewerkers.

Logging

Zoals eerder aangegeven is de gemeente bezig de loggings, die op de meeste systemen aanwezig is, samen te brengen, zodat deze beter gecheckt en geëvalueerd kunnen worden. Vanwege de ENSIA-normen moeten de logs van Suwinet regelmatig gecheckt worden. Dat gebeurt door de security officer die specifiek op Suwinet zit. De netwerkbeheerders van team I&A checken de firewall die het ongeautoriseerde verkeer van buiten naar binnen moet tegenhouden.

---

11 SIEM/SOC is software die het dataverkeer op de systemen monitort en verdachte netwerkactiviteiten kan detecteren.

12 GGI-Veilig is een project van de VNG dat gemeenten ondersteunt bij hun digitale weerbaarheid. GGI-Veilig biedt een gezamenlijk inkoopplatform voor diensten en producten voor informatiebeveiliging, zoals firewalls en een SIEM/SOC. Deze voldoen dan uiteraard aan de eisen van de BIO.

13 Inmiddels heeft de VNG de aanbesteding ontbonden en kan de gemeente een oriëntatie starten hoe nu verder om een dergelijke voorziening te realiseren.

Incidenten

Beveiligingsincidenten, waaronder datalekken, worden bijgehouden in Key2control. Daarin zijn ook het verwerkingsregister en de verwerkingsovereenkomsten opgenomen. De privacy adviseurs analyseren de meldingen van incidenten en rapporteren deze aan de FG. Mogelijke verbetermaatregelen worden gerapporteerd aan de betreffende teamleider(s) die verantwoordelijk zijn voor de uitvoering.

DPIA's

Om de risico's op verwerking van gegevens door en/of namens de gemeente in beeld te krijgen worden data protection impact assessments (dpia) uitgevoerd. Om de kritieke verwerkingsprocessen in beeld te krijgen zijn door de privacy adviseurs en teamleiders alle processen doorgenomen. In totaal zijn in het verwerkingsregister 150 verwerkingsprocessen opgenomen, waarvan ongeveer de helft is aangewezen als hoog risico. Een dpia uitvoeren is intensief, vandaar dat het selecteren van de processen waarop een dpia uitgevoerd moet worden, gebeurt met behulp van een pre-dpia. Doel van een pre-dpia is te bepalen of een volledige dpia op basis van onderkende risico's noodzakelijk is. Sinds 2018 zijn vijf dpia's uitgevoerd en 16 pre-dpia's. In het jaarrapport over 2021 is de uitvoering van dpia's hoog op de agenda gezet.

Verzoeken om inzage en vernietiging van gegevens

Over 2020 zijn met een beroep op de AVG 2 verzoeken geweest om inzage of vernietiging van door of namens de gemeente verwerkte persoonsgegevens. Over 2021 waren dat in totaal 5 verzoeken, 3 keer om inzage en 2 keer om vernietiging van gegevens. Volgens het jaarrapport Gegevensbescherming en Informatieveiligheid 2021 zijn deze naar tevredenheid van de verzoeker afgerond of waren nog in behandeling op moment van rapportage.

4.7 Autorisatieproces

Autorisaties

Autorisatie houdt in het bepalen of een medewerker rechten heeft om toegang te krijgen tot applicaties of gegevens. In het kader van gegevens-bescherming is dat een kritiek proces, met name bij de in-, door- en uitstroom van personeel. In het algemeen gaat het bij de instroom van een medeweker meestal wel goed, want deze moet toegang krijgen tot gegevens en applicaties om het werk te kunnen uitvoeren. Bij door- en uitstroom kan het bijwerken of afsluiten van autorisaties vertraging oplopen. De gemeente De Ronde Venen heeft via de applicatie Youforce een geautomatiseerd proces dat rechten aan personen toekent. De team-leider start het proces bij indiensttreding en bij door- en uitstroom worden de oude autorisaties opgeruimd. Er is geen regelmatige toets door de teamleiders of de beheerders op de autorisaties, zo blijkt uit de interviews. Uit een van de interviews blijkt dat, met een relatief kleine en op in-, door- en uitstroom stabiele organisatie, leidinggevenden goed zelf bij te houden is of de autorisaties overeenkomen met de functies van de medewerkers. Vaste toetsmomenten per jaar worden dan niet nodig geacht.

Identity and Access-management (IAM)

Autorisaties maken onderdeel uit van het zogenoemde Identity- en Access Management (IAM). Op basis van een autorisatiematrix, verbonden met de rollen en functies in het functiegebouw, kan de toegang tot gegevens en applicaties toegekend worden. De gemeente is van plan het autorisatieproces op die manier in te richten.

Corona en thuiswerken

Thuiswerken was technisch al mogelijk, maar door Corona heeft dat een grote vlucht genomen. Respondenten geven aan dat dat goed geregeld is. Een risico dat gemeld wordt is dat het wachtwoordenbeleid gebruiksvriendelijk is ingesteld. Wachtwoorden hoeven maar eens per half jaar vervangen te worden, mits ze aan de complexiteitseisen voldoen. Dat is een gecalculeerd risico dat de gemeente neemt en voldoet aan de eisen van de BIO. Toegang tot de digitale werkplek verloopt via 2FA via de mobiele telefoon. Als extern wordt gewerkt, zonder beveiligd draadloos netwerk, wordt aangeraden om via 4G in te loggen. Uit de interviews blijkt dat medewerkers soms toch via openbare onbeveiligde netwerken op de gemeentelijke systemen komen. Hierbij wordt opgemerkt dat de verbinding altijd versleuteld en dus beveiligd wordt opgebouwd. In geval van “afluisteren” is dan alleen versleutelde data beschikbaar.

4.8 Handhaving

Met het team Integrale Veiligheid is in een gesprek nader ingezoomd op de aspecten informatiebeveiliging en privacy bij handhavingstaken.

Wet politiegegevens (Wpg)

De Wet politiegegevens (Wpg) is vanaf 2019 voor de gemeenten met Boa’s in werking getreden. Die wet regelt vanuit het kader van de politiewet en

Wpg

Een gemeente moet volgens de Wet politiegegevens (Wpg) aan een aantal vereisten voldoen bij de verwerking van gegevens. Die moet plaatsvinden in afzonderlijke systemen en door aangewezen medewerkers. De reden voor deze strenge eisen ligt in de aard van de bevoegdheden. Hiermee kan diep op de privacy van burgers worden ingegrepen en dit vraagt om strenge regels om de privacy van burgers te beschermen.

Voor de verwerking van politiegegevens stelt de Wpg net als de AVG een aantal algemene criteria. Dit betreft criteria over noodzakelijkheid, rechtmatigheid, juistheid, proportionaliteit, subsidiariteit en volledigheid. Daarnaast moet de verwerkingsverantwoordelijke gemeente een aantal technische en organisatorische maatregelen nemen:

1. Inspanningsverplichting verwerkingsverantwoordelijke
2. Beveiliging
3. Gegevensbeschermingseffectbeoordeling (GEB)/dpia
4. Rechten betrokken burgers
5. Registerplicht
6. Meldplicht datalekken
7. Documentatieplicht
8. Voorwaarden ICT-systeem

	de AVG hoe de gemeente om moet gaan met informatie uit de systemen waar de Boa's toegang toe hebben (zie kader).
Audits	Op de Wpg is eind 2021 een interne audit of 0-meting uitgevoerd. Op basis van deze audit is een verbeterplan opgesteld met activiteiten die zo snel als mogelijk moeten zijn gerealiseerd. Eind van 2022 is een nieuwe audit gepland die uitgevoerd gaat worden door een externe partij.
Rapportages	De toezichthouders maken rapportages op in word-documenten die op een beveiligd deel van het systeem worden opgeslagen. Daar kunnen alleen de Boa’s en het afdelingshoofd bij, waar tot voor kort ook nog andere medewerkers van het team bij konden. Er is een applicatie in ontwikkeling waarin alle meldingen en rapportages beveiligd kunnen worden geregistreerd.
Processen verbaal	Boa’s mogen niet zomaar gevoelige politiegegevens verwerken. Zij gebruiken daarvoor de applicatie CityControl van Sigmax. Dat is een systeem om online te verbaliseren, een beveiligde omgeving waarmee politiegegevens verwerkt mogen worden. Daarin kan onder andere bij een foutparkeerder op basis van het kenteken de gegevens van de kenteken-houder ingezien worden. Citycontrol heeft een eigen check op het verwerken van politiegegevens. De boetemeldingen van de Boa’s worden via e-herkenning naar het CJIB-portaal geüpload. Met de politie zelf worden gegevens voornamelijk gedeeld via de mail. Dat gebeurt niet standaard via een beveiligde mailapplicatie en het is niet uit te sluiten dat hiermee ook persoonsgegevens gedeeld worden. In acties, zoals de verzegeling van (drugs)panden, verloopt de communicatie tussen Boa’s en politie via beveiligde portofoons.
Meld Misdaad Anoniem	Een van de medewerkers is contactpersoon voor Meld Misdaad Anoniem (MMA). Deze kan, samen met het teamhoofd, de meldingen lezen, maar niet verder verwerken. Wel kunnen ze gedeeld worden met het Regionaal Informatie- en Expertise Centrum (RIEC), bijvoorbeeld in het kader van de registratie van ondermijning en georganiseerde criminaliteit. Deze uitwisseling van gegevens gebeurt beveiligd.
Wet Bibob	De Wet Bibob is een bestuursrechtelijk instrument dat gebruikt wordt om misbruik van vergunningen (preventief) te voorkomen. Aanvragen en adviezen worden geregistreerd door de gemeente. Deze kan in het kader van de Wet Bibob justitiële gegevens bekijken en opvragen bij Justis, het portaal van het Ministerie van J&V. De meldingen staan op een beveiligd deel van het systeem, waar enkele geautoriseerden bij kunnen komen.
Agressieprotocol	De gemeente hanteert een intern agressieprotocol. Daarin is geregeld dat de gemeente persoonsgegevens bijhoudt van degene die agressief gedrag vertoont richting een ambtenaar. Ook wordt de melding van een zedendelinquent bijgehouden in het beveiligde deel van het systeem.

5 Gegevensbescherming

Onderzoeksvraag 3

Onderzoeksvraag 3 wordt in dit hoofdstuk beantwoord: In hoeverre zijn gegevens bij de gemeente beschermd tegen de toegang door onbevoegden?

5.1 Beschermingsmaatregelen

Zoals eerder aangegeven bestaat informatiebeveiliging uit drie dimensies: organisatie-techniek-mens. Alle drie zijn belangrijk om de beschikbaarheid, integriteit en vertrouwelijkheid (biv) van de door of namens de gemeente verwerkte gegevens te garanderen. Daartoe dient de gemeente op de drie dimensies maatregelen te treffen, te onderhouden en te controleren. Beleid is goeddeels in hoofdstuk 4 aan bod gekomen, techniek en mens grotendeels in hoofdstuk 5. In dit hoofdstuk gaan we na hoe de gemeente daadwerkelijk ervoor zorgt dat de gegevens technisch beveiligd worden, maar ook hoe de menselijke factor hierop acteert.

Maatregelen

Gemeenten nemen verschillende technische maatregelen om ervoor te zorgen dat kwaadwillenden niet gemakkelijk toegang kunnen krijgen tot de systemen en de gegevens. En als ze onverhoopt toegang hebben gekregen dat snel te kunnen detecteren en schade zoveel mogelijk te kunnen beperken. Dat betekent dat gemeenten onder andere:

- de buitenste schil van de systemen/netwerken van de gemeente moeten beveiligen met onder andere firewalls;
- de toegang tot de netwerken en systemen moeten kunnen beheren via een netwerktoegangsbeheer (Network Acces Control, NAC);
- de (mobiele) apparaten van de medewerkers beveiligen;
- via de autorisaties de toegang tot applicaties en gegevens moeten kunnen beveiligen en controleren.

Testen

Op de meeste van deze terreinen heeft de gemeente beleid geformuleerd, technische maatregelen genomen en bewustwording gestimuleerd (zie ook hoofdstuk 3). Om de werking van deze inspanningen daadwerkelijk te checken voert de gemeente testen uit, of laat deze door externen uitvoeren. Jaarlijks worden pentesten (kort voor penetratietesten) uitgevoerd op de hardheid van de systemen, meerdere phishingmails uitgezet om bewustwording te testen en uitwijktesten om te bezien of de dienstverlening van de gemeente na een storing binnen bepaalde tijd weer opgestart kan worden.

5.2 Pentesten

Inleiding

Zoals aangegeven zijn in het kader van het rekenkameronderzoek pentesten uitgevoerd, door ethische hackers. Uitgevoerd zijn een externe en interne netwerk pentest, een Active directory audit, een phishing mail

aanval en een inlooptest door een mystery guest (zie hierna voor de resultaten). Bij de hoor en wederhoor zijn de resultaten van de pentesten vertrouwelijk gedeeld met de gemeentesecretaris.

Voor de testen worden doelen gesteld die de ethische hackers trachten te bereiken, zoals het kunnen bereiken van de serverruimte tijdens het bezoek van de mystery guest. Afgesproken dat zij de mogelijkheid aantonen dat bijvoorbeeld de gemeentelijke dienstverlening kan worden verstoord, maar dat zij dat zoveel als mogelijk proberen te vermijden. De impact van de risico's die met de testen kunnen worden aangetoond worden ingeschaald op onderstaande classificatieschaal

Risicoclassificatie	Toelichting
Kritisch (9-10)	Extreem hoge kans dat beveiligingsmaatregelen niet voldoende zijn of omzeild kunnen worden en dat hierdoor de kwetsbaarheid misbruikt kan worden met als gevolg catastrofale financiële verliezen.
Hoog (7.0-8.9)	Hoge kans dat beveiligingsmaatregelen niet voldoende zijn of omzeild kunnen worden en dat hierdoor de kwetsbaarheid misbruikt kan worden met als gevolg enorme financiële verliezen.
Gemiddeld (4.0-6.9)	Aannemelijke kans dat beveiligingsmaatregelen niet voldoende zijn of omzeild kunnen worden en dat hierdoor de kwetsbaarheid misbruikt kan worden met als gevolg financiële verliezen.
Laag (0.1-3.9)	Mogelijke kans dat beveiligingsmaatregelen niet voldoende zijn of omzeild kunnen worden en dat hierdoor de kwetsbaarheid misbruikt kan worden met als gevolg gelimiteerde financiële verliezen.
Best Practice	Deze bevinding omvat geen direct aanvalsscenario met negatieve gevolgen. Echter duidt een bevinding met deze classificatie wel aan dat er een beveiligingsmaatregel niet voldoet aan security best practices. Het ontbreken van deze beveiligingsmaatregel kan het uitvoeren van andere aanvallen vergemakkelijken.

Voor de testen is afgesproken dat kritieke risico's meteen gemeld zouden worden, zodat de gemeente direct maatregelen zou kunnen treffen. Dat is niet aan de orde geweest. Hieronder gaan we nader in op de bij de pentesten gesignaleerde risico's, waarbij de rekenkamercommissie ervoor waakt bevindingen te delen waar kwaadwillenden profijt van zouden kunnen hebben.

Externe netwerk pentest

Deze test is uitgevoerd in januari 2022. Door een ethisch hacker is de beveiliging van het externe netwerk getest, waarbij de kwetsbaarheden in kaart zijn gebracht en getracht is deze te exploiteren. Daarmee wordt de effectiviteit geverifieerd van de beveiligingsmaatregelen om kwaadwillenden buiten het netwerk te houden.

Vooraf wordt de scope (het doel) van de test bepaald. Doelen zijn onder andere te proberen ongeautoriseerd toegang te krijgen tot servers en accounts, lezen en schrijven van gegevens of de dienstverlening te verstoren. Geen van de doelen is behaald, waardoor het risico als laag wordt ingeschat. Wel zijn een beperkt aantal verbeterpunten gevonden. Deze zijn in de vertrouwelijke rapportage van de pentest opgenomen.

Interne netwerk pentest

Deze test is uitgevoerd in maart 2022, en betreft de test van de beveiliging van het interne netwerk. Ook hierbij worden de kwetsbaarheden in kaart

gebracht, maar dan van binnen het netwerk. Daarmee wordt de effectiviteit geverifieerd van de beveiligingsmaatregelen om de schade zoveel mogelijk te beperken die kwaadwillenden kunnen aanrichten als ze eenmaal in het netwerk zijn doorgedrongen.

Ook hier wordt het doel van de test vooraf bepaald. Doelen zijn min of meer dezelfde als bij de externe netwerk pentest. Hierbij is een van de gestelde doelen behaald, namelijk dat via het Wifi-netwerk onder andere een gebruikersnaam is achterhaald. Daardoor zou het mogelijk zijn dat een wachtwoord achterhaald kan worden. Dat is verder niet getest.[14] Het risico dat de gemeente loopt op gemiddeld ingeschat. In totaal zijn 5 verbeterpunten uit deze test naar voren gekomen die in de vertrouwelijke rapportage van de pentest zijn opgenomen.

AD audit

Een active directory (AD) staat beheerders toe om het beleid met betrekking tot rechten van medewerkers en instellingen in het netwerk van een organisatie te beheren. De AD van de gebruikersaccounts van de medewerkers van de gemeente zijn in de test meegenomen die op 12 januari 2022 is uitgevoerd. De AD-audit checkt op zwakke en gekraakte wachtwoorden. Zwakke wachtwoorden worden gecheckt op complexiteits-graad en wachtwoorden worden vergeleken met een lijst op internet met wachtwoorden die in relatie gebracht kunnen worden met de gemeente.

Tijdens de test zijn 1.424 gebruikersaccounts gescand op kwetsbaarheden. Van deze zijn 462 accounts (ca 32%) aangetroffen met een wachtwoord dat een jaar oud of nog ouder is en van 39 accounts verlopen de wachtwoorden nooit.[15] Twee zwakke en 31 niet unieke wachtwoorden zijn aangetroffen (ca 2%). In totaal zijn 5 accounts aangetroffen met een zwakke of kwetsbare beveiliging. Via een internetsearch zijn 64 wachtwoorden in combinatie met gebruikersnamen aangetroffen, die mogelijk nog in gebruik zijn. Dat is niet verder gecheckt.

Ingezoomd is op 43 accounts van beheerders, daar deze meer rechten hebben dan andere accounts. Hierop zijn een aantal kwetsbaarheden aangetroffen.

---

[14] Uit de ambtelijk reactie blijkt dat de gemeente met een pilot bezig is om via certificaten aan te melden. Hiermee wordt afgedwongen dat het apparaat waarmee ingelogd wordt te vertrouwen is. Daarmee zou het aanmelden met naam en wachtwoord komen te vervallen.

[15] Uit de ambtelijke reactie blijkt dat een aantal van de 462 accounts waarvan het wachtwoord 1 jaar of ouder is; 346 accounts van computers zijn, 10 gebruikersaccounts op ‘disabled’ stonden en inmiddels verwijderd zijn; 15 gebruikersaccounts nooit inloggen.
91 accounts staan op ‘never expires’ (wachtwoord verloopt nooit) omdat 28 nooit ingelogd zijn geweest; en van de 38 die wel ingelogd zijn geweest zijn 29 systeem accounts en 9 van raadsleden. Die laatste zijn inmiddels aangepast.
Van 25 accounts die wel op ‘expires’ staan ingesteld zijn er 14 nog nooit ingelogd, 8 oud medewerkers die inmiddels verwijderd zijn en drie nieuwe medewerkers die nog niet waren ingelogd.

De met de AD audit gevonden kwetsbaarheden lijken voornamelijk voort te komen uit het niet consequent toepassen van het wachtwoordbeleid. De kwetsbaarheden en mogelijke verbetermaatregelen zijn in de vertrouwelijke rapportage opgenomen.[16]

Phishingmail

Kwaadwillenden proberen vaak via e-mails mensen naar een valse website te lokken, om inlog- of andere gegevens buit te maken. Ook kunnen daarmee ransomware of virussen geïnstalleerd worden, of datalekken ontstaan. Om de alertheid en bewustzijn van medewerkers van de gemeente De Ronde Venen op dat soort e-mails te testen is op 25 januari 2022 een phishing mail uitgezet. De e-mail is verstuurd vanaf een extern mailadres en bevatte een uitnodiging voor een werkoverleg. Als een medewerker op een van de links klikte kwam deze op een landingspagina waarop gemeld werd dat dit onderdeel was van een test in opdracht van de rekenkamercommissie. En werd uitleg gegeven over phishing mails en hoe deze te herkennen. Het resultaat van de phishingmail aanval is in bijlage 4 opgenomen.

De medewerkers van de gemeente De Ronde Venen bleken iets meer dan gemiddeld vatbaar voor een phishingaanval. Dit was een standaard phishing mail, die vaker is uitgezet bij vergelijkbare organisaties zodat de scores vergeleken kunnen worden. Iets meer dan een derde van de medewerkers, 36,1% van de 504 uitgezette e-mails, heeft op een van de links in de mail geklikt. Het gemiddelde is ca. 35%. Positief is dat een deel van de medewerkers die niet op een van de links van de phishing mail heeft geklikt dat via de reguliere weg bij de CISO en privacy officer heeft gemeld.

Mystery guest

In landelijke richtlijnen is opgenomen dat er toegangsbeveiliging aanwezig is op de werk-, server- en technische ruimten. Dit geldt ook voor de ruimtes waar reisdocumenten zich bevinden en waar persoonsgegevens worden verwerkt. Op 2 maart 2022 is in het kader van het rekenkameronderzoek een inlooptest met behulp van een mystery guest uitgevoerd. Getracht is ongeautoriseerd toegang te krijgen de serverruimte, toegang te krijgen tot verdiepingen en ruimtes die gesloten zijn voor onbevoegden en ongestoord werkzaamheden op een (eigen/onbewaakt) computersysteem uit te voeren.

Het doel dat vooraf beoordeeld is als een risico met kritieke impact, te weten toegang tot de serverruimte, is niet behaald. De overige doelen, met een hoge en medium impact wel. De beveiligingsdrempels konden relatief gemakkelijk genomen worden en de mystery guests zijn door niemand aangesproken. Daardoor konden zij zich toegang verschaffen tot beveiligde ruimtes. Er is geen toegang verkregen tot een ICT gerelateerde ruimte maar

[16] Uit de ambtelijke reactie blijkt dat er op een aantal bevindingen maatregelen zijn genomen. En is gemeld dat voor de netwerkaccounts geen zwakke wachtwoorden worden toegelaten. Voor de systeemwachtwoorden gelden zware complexiteitseisen.

de ruimte waarin onder andere de verwarmingsapparatuur staat. De onderzoekers waren in de gelegenheid zich toegang te verschaffen tot computersystemen om een (fysieke) aanval te starten, die in enkele gevallen onbeheerd en niet vergrendeld waren. De onderzoekers waren in staat zonder aangesproken of gestopt te worden het gemeentehuis te verlaten via de hoofdingang.

Op basis van de inlooptest wordt bevonden dat de gemeente serieus bezig is met fysieke beveiliging daar drempels voor toegang door onbevoegden zijn opgeworpen, tegelijkertijd zijn er naar aanleiding van de test enkele verbeterpunten geconstateerd op de fysieke beveiliging en risicobewustzijn van medewerkers.

Deze zijn opgenomen in het rapport dat vertrouwelijk is overhandigd.

6 Betrokkenheid gemeenteraad

Onderzoeksvraag 4

In dit hoofdstuk geven we antwoord op vraag 4: Hoe wordt de gemeenteraad betrokken bij het informatiebeveiligingsbeleid?

Budgetrecht raad

De raad heeft vanuit de gemeentewet het recht het budget voor de uitvoering van gemeentelijke taken vast te stellen. Dat geldt uiteraard ook voor informatiebeveiliging en privacy. Informatiebeveiliging wordt over het algemeen gezien als onderdeel van de gemeentelijke bedrijfsvoering, wat onder de beslissingsbevoegdheid van het college valt. Budget(wijzigingen) daarop moet evenwel door de raad worden vastgesteld. Het college heeft aan de raad aangegeven dat digitalisering en beveiliging van de gemeentelijke dienstverlening een blijvende en in de toekomst stijgende kostenpost zal vormen. In tijden van schaarste en in concurrentie met onderwerpen als het sociaal domein, wordt in het algemeen investeren in bedrijfsvoering politiek lastig ervaren. Uitgaven moeten goed beargumenteerd worden. De directie is bezig met een meerjarenplan met betrekking tot informatievoorziening en digitalisering. Onder andere informatiebeveiliging en privacy maken daar een vast onderdeel van uit.

Lastig onderwerp

Voor raadsleden in het algemeen zijn informatiebeveiliging en privacy lastige onderwerpen. Informatiebeveiliging is een redelijk technisch onderwerp, wat niet meteen in het voorfront van de aandacht ligt. Een deel van raad heeft affiniteit op het terrein, maar een deel ook niet. Een deel van de respondenten ziet de raad incidenteel vragen stellen over informatiebeveiliging en privacy. Zo blijkt onder andere uit de beantwoording van technische vragen over de Kadernota's 2020 en 2022.[17] Vanuit het ambtelijk apparaat zijn met raadsleden sessies geweest over ICT en beveiliging. Daarin zijn volgens de respondenten weinig vragen gesteld over informatiebeveiliging.

De politieke gevoeligheid van informatiebeveiliging wordt in de interviews erkend. Zeker als de dienstverlening aan burgers in gevaar komt en persoonsgegevens van burgers door hackers gegijzeld worden of op het dark web worden aangeboden, zoals in recente voorbeelden van de gemeenten Hof van Twente en Buren. Uit een enkel interview komt echter het beeld naar voren dat informatiebeveiliging toch uiteindelijk onder bedrijfsvoering valt en de politieke dimensie beperkt moet blijven tot het college die daar uitvoering aan geeft.

Beleid

In de BIO is opgenomen dat de raad minimaal 1x per jaar in het kader van de P&C-cyclus geïnformeerd wordt over informatieveiligheid en privacy.

[17] In 2019 zijn door twee fracties technische vragen gesteld over informatieveiligheid en privacy naar aanleiding van de Kadernota 2020. In 2021 is naar aanleiding van de Kadernota 2022 door een fractie een technische vraag gesteld over informatieveiligheid. In 2021 zijn min of meer aanpalend door een fractie vragen gesteld over datagestuurd werken, zoals het werken met algoritmen naar aanleiding van de toeslagenaffaire.

Zoals in veel gemeenten wordt daarbij in De Ronde Venen gebruik gemaakt van de paragraaf bedrijfsvoering in de jaarstukken van de gemeente. In de Programmarekening 2020 wordt op hoofdlijnen ingegaan op activiteiten op informatiebeveiliging en privacy. Gemeld wordt onder andere dat tijdelijke formatie is ingezet op informatiebeveiliging en privacy, de gemeente deelneemt aan de landelijke aanbesteding GGI-Veilig, dpia's worden uitgevoerd, een Network Access Control (NAC) is geïmplementeerd en dat de audits in het kader van ENSIA succesvol zijn afgerond.

Meldingen

Het college rapporteert jaarlijks ENSIA ook naar de raad toe in de jaarrapportage. Incidenteel komt informatiebeveiliging en privacy op de agenda van de raad. Met name bij incidenten, als de raad via een raadsinformatiebrief wordt geïnformeerd, zoals met de kwetsbaarheid in verband met Log4J.

Accountant

De accountant geeft in opdracht van de raad een oordeel over de rechtmatigheid van de financiën van de gemeente. Accountants gaan de laatste jaren ook in op ICT en informatieveiligheid in relatie tot de financiële rechtmatigheid. Zo maakte de accountant in de managementletter 2020 opmerkingen over autorisatiebeheer en wijzigingsbeheer in relatie tot de applicaties op financiën en het sociale domein. Vanuit het college is aangegeven aan de slag te gaan met de adviezen van de accountant met betrekking tot beter en zichtbaar vastleggen van procesactiviteiten.

Informatiebeveiliging raad

De raadsleden hebben Ipads van de gemeente gekregen en krijgen in de nieuwe raadsperiode laptops. De raadsleden hebben wel een mailadres van de gemeente gekregen, maar een enkeling gebruikt deze. Dat zagen we terug in de phishingmail die is uitgezet in het kader van dit onderzoek. Het streven dat uit de interviews naar voren komt is hierop meer 'in control' te komen op de risico's en raadsleden ertoe te bewegen alleen de mailadressen van De Ronde Venen te gebruiken. Dat maakt het allicht omslachtiger, daar de raadsleden vaak via hun reguliere werkzaamheden al andere apparatuur gebruiken.

Bijlage 1. In informatiebeveiliging en privacy veel voorkomende termen en afkortingen

2FA	Twee factor authenticatie, zo wordt op 2 verschillende manieren gecheckt of degene die inlogt degene is die hij/zij aangeeft te zijn
2-staps-verificatie	zie 2FA
ACIB	Algemeen Contactpersoon Informatiebeveiliging, ontvangt berichten van algemene aard van de Informatiebeveiligingsdienst voor gemeenten (IBD)
Active Directory (AD)	De Active Directory is een database waarin onder andere accounts en inloggegevens zijn opgenomen.
AP	Autoriteit Persoonsgegevens
Applicatie	Softwareprogramma, zoals de BAG, BRP, SUWInet enz.
AVG (GDPR)	Algemene Verordening Gegevensbescherming, Europese regelgeving die de privacyregels in de Europese lidstaten harmoniseert (GDPR = General Data Protection Regulation)
BAG	Basisregistratie Adressen en Gebouwen, applicatie met onder andere gegevens over adressen en gebouwen in de gemeente
BIG	Baseline Informatiebeveiliging Gemeenten, maatregelen voor de informatiebeveiliging bij gemeenten, in 2013 als standaard afgesproken in VNG-verband
BIO	Baseline Informatiebeveiliging Overheid
BIV	Beschikbaarheid – Integriteit – Vertrouwelijkheid. Termen waarop de beveiligingsrisico's van de informatie/applicaties zijn geënt
BRP	Basisregistratie Personen, applicatie met persoonsgegevens van de inwoners
CIO	Chief Information Officer
CISO	Chief Information Security Officer
Cloud	De cloud staat voor een netwerk van computers die een soort 'wolk van computers' vormt, waarbij de eindgebruiker niet weet op hoeveel of welke computer(s) de software draait of waar die computers precies staan
CYOD	Choose your own device, beleid dat inhoudt dat medewerkers en eventueel externen apparaten (laptops, smartphones, usb-sticks enz.) kunnen kiezen uit een beperkt assortiment, waarop de veiligheidsmaatregelen al zijn aangebracht
DPIA (ook PIA)	Data protection impact assessment, analyse op risico's in verband met privacy en gegevensbescherming bij verwerkingsprocessen. Onder de AVG verplicht bij gegevensverwerking met waarschijnlijk een hoog privacy risico.
ENSIA	Eenduidige Normatiek Single Information Audit, eenmalige informatieverstrekking en eenmalige IT-audit voor de horizontale (richting gemeenteraad als toezichthouder) en verticale verantwoording (richting landelijke toezichthouders)
FG	Functionaris gegevensbescherming, verplicht voor overheden.
Firewall	Een firewall is een systeem dat de middelen van een netwerk of computer kan beschermen tegen misbruik van buitenaf.
GAP	Is de Engelse term voor ‘kloof’. Dat betekent hier het verschil tussen de bestaande situatie en de gewenste situatie
GAP-analyse	Controle of en in welke mate de maatregelen uit de BIG geïmplementeerd zijn
GDPR	General Data Protection Regulation (zie AVG)

GBA	Gemeentelijke Basisadministratie, tegenwoordig BRP (zie daar)
GR	Gemeenschappelijke regeling
IBD	Informatiebeveiligingsdienst voor gemeenten
ICT	Informatie- en communicatietechnologie
ISMS	Information securitymanagement system
Metadata	Informatie over data, bijvoorbeeld in het kader van logging wie toegang heeft (gehad) tot gegevens in systemen
NFC	Near Field Communication, contactloze communicatie op korte afstand (vergelijkbaar is de ov-chipkaart)
OWASP	Open Web Application Security Project
PO	Privacy Officer
P&C-cyclus	Planning & Control cyclus
PDCA	Plan-Do-Check-Act beleidsleercyclus
Phishing mail	Vorm van internet oplichting en fraude, door middel van een vals e-mail bericht 'hengelen' naar inlog- of andere persoonsgegevens
PIA (ook DPIA)	Privacy impact assessment, analyse op risico's in verband met privacy en gegevensbescherming bij verwerkingsprocessen. Onder de AVG verplicht bij gegevensverwerking met waarschijnlijk een hoog privacy risico.
PKI-certificaat	Public Key Infrastructure. Een PKI(overheid)-certificaat is een internationale standaard voor de digitale ondertekening bij het versturen van gegevens en berichten.
Privacy by default	Onderdeel van privacy by design, waarbij de standaardinstellingen zo privacy-vriendelijk mogelijk zijn ingesteld
Privacy by design	Betekent dat bij het ontwerp van producten en diensten nagedacht wordt over privacy
RIVG	Rijksdienst voor Identiteitsgegevens
SAAS	Software-as-a-Service is een model waarbij softwaretoepassingen via internet worden aangeleverd.
Smart credentials	Smartphone of smartwatch voorzien van een sleutel app
SSO	Single Sign On, op 1 werkplek via 1 aanmelding toegang krijgen tot alle applicaties waar de gebruiker recht op heeft
Spoofing	Het verzenden van e-mails waarbij het e-mailadres van de afzender vervalst is
Token	Een fysiek apparaat waarmee toegang verkregen kan worden tot een elektronisch beveiligde bron of netwerk
TPM	Third Party Memorandum. Verklaring dat de derde partij, die de gegevens voor de gemeente bewerkt voldoet aan de geldende richtlijnen inzake informatiebeveiliging
Url	Uniform Resource Locator. Verwijst naar een uniek adres waarmee de locatie van een webpagina op internet wordt aangegeven of een e-mailadres
VCIB	Vertrouwd Contactpersoon Informatiebeveiliging, ontvangt berichten van vertrouwelijke aard van de Informatiebeveiligingsdienst voor gemeenten (IBD)
Verwerkingsregister	Register waarin de gemeente bijhoudt welke persoonsgegevens de gemeente en de verwerkers die deze inschakelt verwerkt
VNG Realisatie	Kwaliteitsinstituut van de VNG (voorheen KING)
VPN	Virtueel privé netwerk (versleutelde beveiligde verbinding)

Bijlage 2. Lijst geraadpleegde stukken en lijst respondenten

De geraadpleegde stukken en de geïnterviewde personen zijn hieronder weergegeven.

Geraadpleegde stukken

- 2021 bewustwordingsacties infosec 2021
- Aansluiten Informatieveiligheid en privacy V2
- Beantwoording technische vragen Kadernota 2020, mei 2019
- Beantwoording technische vragen Kadernota 2022, mei 2021
- Beleid en procedures veilig gebruik Suwinet-inkijk 2019-2022
- Beleid Patch- en hardeningsmanagement v1
- Changemanagement – Werkinstructie
- Emailbeveiliging De Ronde Venen sep 2021
- Format Verwerkersovereenkomst 2020 (publieke versie)
- Incident- en datalekmanagement Stappenplan DRV v1.1
- Informatiebeveiligingsbeleid 2018-21 vastgesteld
- Informatienota raad: Reactie op management letter 2020 van accountant BDO, maart 2021
- Integriteits- en geheimhoudingsverklaring externe medewerkers – 2021
- Integraal veiligheidsplan De Ronde Venen 2019-2022 definitief
- Meting en gap analyse Q2 2021
- PO-Ciso-FG Jaarrapport 2020 definitief
- Privacyreglement Gemeente De Ronde Venen 2018
- Procedure afvoer ICT vastgesteld
- Procedure Back-up en Herstel vastgesteld
- Procedure clean desk-screen-ruimte vastgesteld
- Procedure Wachtwoord gebruik en IAM 2019 vastgesteld
- Regeling beheer applicaties
- Responsible Disclosure
- Spelregels ingescande handtekening
- Thuiswerken, hoe zat het ook alweer
- Uitwijkplan DRV vertrouwelijk
- Vastgesteld beleid dataclassificatie
- Vastgesteld beleid logische toegangsbeveiliging
- Vastgesteld beleid mobiele gegevensdragers
- Vastgesteld Beleid uitwisseling van informatie getekend
- Vastgesteld Encryptiebeleid gemeente De Ronde Venen
- Vastgesteld fysieke toegangsbeleid
- Websitebeveiliging De Ronde Venen sep 2021

Functies van geïnterviewde respondenten

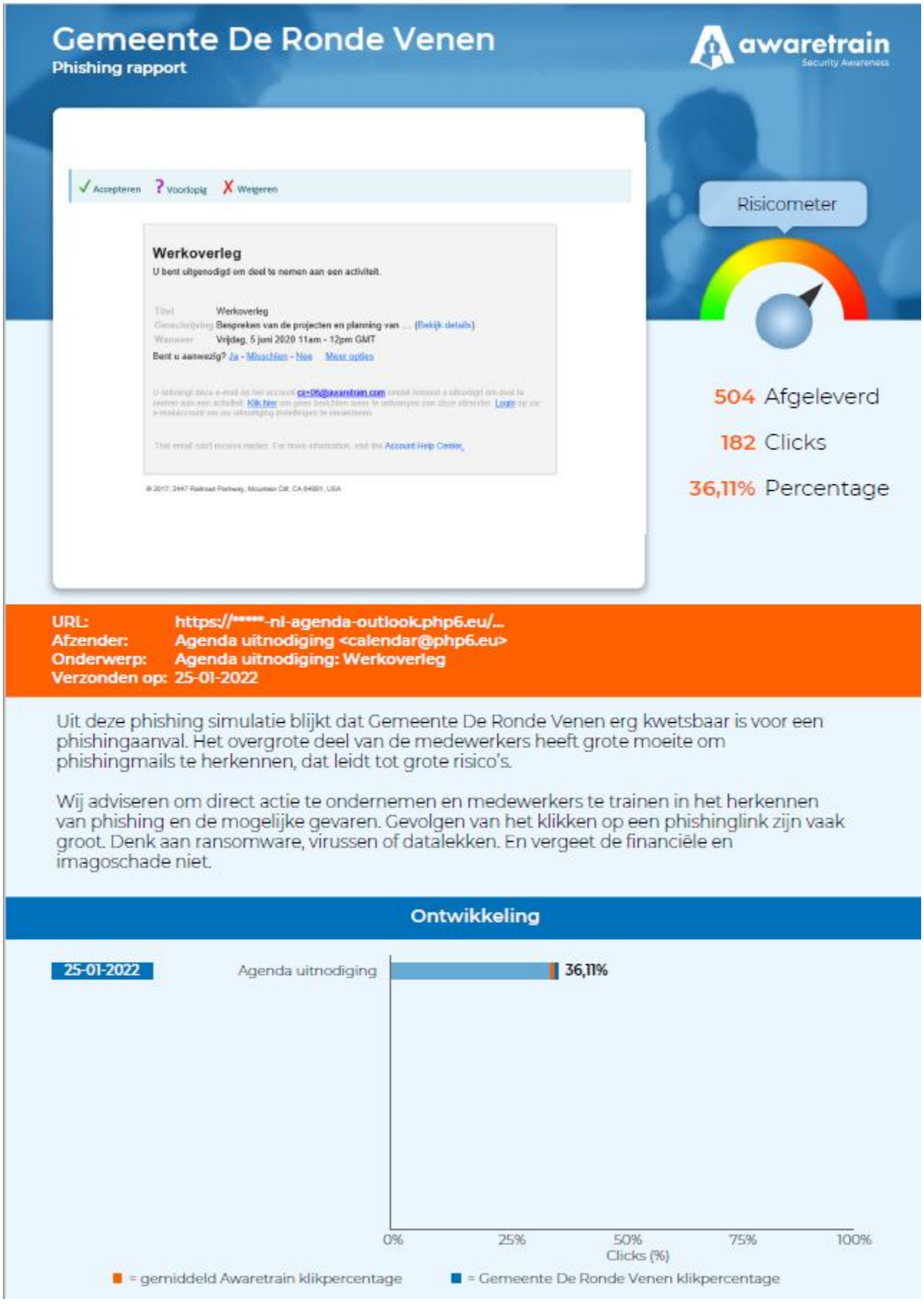
- Beleidsadviseur Team Integrale Veiligheid
- Beleidsmedewerker automatisering
- Chief Information Security Officer (CISO)
- Functionaris Gegevensbescherming (FG)
- Functioneel beheerder, afdeling Burgerzaken
- Gemeentesecretaris
- Netwerkbeheerder
- Teamleider I&A
- Waarnemend teamleider Integrale Veiligheid
- Wethouder

Bijlage 3. Onderzoeksvragen en normen

De onderstaande normen zijn voornamelijk ontleend aan de BIG en de AVG. Mogelijk kunnen de gemeentelijke beleidsplannen aanvullende normen opleveren, waaraan de uitvoering van de informatiebeveiliging getoetst wordt.

Onderzoeksvragen	Normen
1. Beschikt de gemeente De Ronde Venen over een adequaat informatiebeveiligingsbeleid?	- Het college stelt het integrale beleid ten aanzien van informatiebeveiliging en privacy vast. - Er vindt sturing plaats op basis van de BIO. - Het informatiebeveiligingsbeleid is opgesteld aan de hand van een GAP-analyse. Jaarlijks wordt op basis van een risicoanalyse het informatiebeveiligingsplan ingevuld. De gemeente neemt maatregelen om risico's te verlagen. - Op onderdelen van informatiebeveiliging is beleid geformuleerd en zijn richtlijnen opgesteld, zoals gebruik van wachtwoorden, 2 factor authenticatie, mobiele datadragers, autorisaties en monitoring, protocol datalekken, wijzigingsbeleid enz. - De CISO is gepositioneerd en geëquipeerd om diens taak adequaat uit te voeren.
2. Hoe wordt het beleid uitgevoerd en wordt de uitvoering gemonitord?	- Het bestuur en medewerkers dragen het beleid ten aanzien van informatiebeveiliging actief uit. - Medewerkers weten wat ze wel en niet mogen/moeten doen met gegevens, herkennen incidenten en rapporteren deze ook daadwerkelijk. - De gemeente heeft procedures om te leren van beveiligingsmeldingen met als doel beheersmaatregelen te verbeteren. - Over het functioneren van informatiebeveiliging wordt gerapporteerd aan het management, bij voorkeur op basis van een ISMS (Information Security Management System). - Het ISMS, indien aanwezig, is gekoppeld aan de PDCA-cyclus. - Op de systemen is logging geïnstalleerd en er is capaciteit aanwezig om deze te monitoren. - Er is een procedure vastgesteld voor de wijze waarop informatiebeveiligingsgebeurtenissen en zwakke plekken in de beveiliging worden beheerd en gerapporteerd.
3. In hoeverre zijn gegevens bij de gemeente beschermd tegen de toegang door onbevoegden?	- Gegevens die door en/of namens de gemeente worden verwerkt zijn beschermd tegen ongewenste invloeden van buitenaf en van binnenuit. - Er worden jaarlijks beveiligingsaudits uitgevoerd. - De gemeente heeft in beeld met welke partners gegevens worden gedeeld met behulp van het verwerkingsregister. - De gemeente maakt met partners en leveranciers afspraken over het veilig uitwisselen en verwerken van persoonsgegevens en de daarvoor te nemen maatregelen.
4. Hoe wordt de gemeenteraad betrokken bij het informatiebeveiligingsbeleid?	- Over het functioneren van het informatiebeveiligingsbeleid wordt gerapporteerd aan de raad, in ieder geval jaarlijks in het kader van ENSIA.

Bijlage 4. Resultaten Phishing mail



Bijlage 5. Volwassenheidsniveau NOREA

Bron: Handreiking bij Volwassenheidsmodel Informatiebeveiliging, januari 2019, NBA.

Niveau	Naam	Omschrijving	Indicatieve criteria
1	Initieel	Beheersingsmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen.	• Geen of beperkte controls geïmplementeerd. • Niet of ad-hoc uitgevoerd. • Niet /deels gedocumenteerd. • Wijze van uitvoering afhankelijk van individu.
2	Herhaalbaar	Beheersingsmaatregelen zijn aanwezig en worden op consistente en gestructureerde, maar op informele wijze uitgevoerd.	• Control is geïmplementeerd. • Uitvoering is consistent en standaard. • Informeel en grotendeels gedocumenteerd.
3	Gedefinieerd	Beheersingsmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst.	• Control gedefinieerd o.b.v. risico assessment. • Gedocumenteerd en geformaliseerd. • Verantwoordelijkheden en taken eenduidig toegewezen. • Opzet, bestaan en effectieve werking aantoonbaar. • Rapportage van uitvoering van beheersingsmaatregel aan management. • Effectieve werking van controls wordt periodiek getoetst, gebaseerd op het risicoprofiel van de organisatie. • De toetsing toont aan dat de control effectief is.
4	Beheerst en meetbaar	De effectiviteit van de beheersingsmaatregelen wordt periodiek geëvalueerd.	• Periodieke (control) evaluatie en opvolging vindt plaats. • Evaluatie is gedocumenteerd en geformaliseerd. • Frequentie waarop wordt geëvalueerd is gebaseerd op het risicoprofiel van de onderneming en is minimaal jaarlijks. • Rapportage van de evaluatie aan management.
5	Continu verbeteren	De beheersingsmaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering.	• Continu evalueren van de beheersingsmaatregelen om de effectiviteit te verbeteren. Gebruik makend van resultaten uit Self-assessment, gap en root cause analyses. • De getroffen beheersingsmaatregelen worden gebenchmarkt en zijn 'Best Practice' in vergelijking met andere organisaties. • Real time monitoring. • Inzet automated tooling.