REKENKAMER
gemeente Baarn

REKENKAMERBRIEF

AAN	Gemeenteraad Baarn
DATUM	01-05-2024
VAN	Rekenkamer Baarn
Zaaknummer	931532

Geachte leden van de gemeenteraad van Baarn,

De rekenkamer is enige tijd geleden gestart met het onderzoek naar de Informatieveiligheid van de gemeente Baarn.

Eerste onderdeel van het onderzoek Informatieveiligheid (2022)

Als eerste onderdeel van dat onderzoek zijn in de eerste helft van 2022 penetratietests[1] uitgevoerd door een onafhankelijk en daarin gespecialiseerd bureau. Deze penetratietests zijn uitgevoerd in opdracht van de rekenkamer, maar in nauwe samenwerking met de gemeentelijke organisatie en de RID (Regionale ICT-Dienst). Dit aangezien voor dergelijke tests toestemming en vrijwaring is vereist van de eigenaar van de systemen die getest worden en het erg verstandig is om de eigenaar betrokken te laten zijn bij dergelijke tests, zowel inhoudelijk (welke systemen worden aan welke test onderworpen) als procesmatig (wanneer de systemen aan de tests worden onderworpen). Immers, wanneer de eigenaar van de systemen niet op de hoogte is van dergelijke tests, zou de eigenaar onaangenaam verrast kunnen worden wanneer systemen (en mogelijk hun prestaties onbedoeld) geraakt worden en zou een dergelijke -rechtmatige- test als onrechtmatige inbreuk/aanval op de systemen kunnen worden waargenomen.

De conclusies van het externe gespecialiseerde bureau in 2022 luidden als volgt:

1. *"De huidige beveiligingsstatus van de ICT infrastructuur van gemeente Baarn blijkt volgens de testresultaten, beschreven in het rapport van Schippers IT, volgens Schippers IT en hedendaagse standaarden bovengemiddeld goed voor aanvallen door externen op het WiFi netwerk, interne netwerk, werkplekken en servers.* [2]
2. *De beveiligingsstatus van de ICT infrastructuur van Gemeente Baarn is bovengemiddeld te noemen. Dit baseert Schippers IT op eerdere uitgevoerde onderzoeken bij soortgelijke organisaties. Echter zijn er nog wel voldoende (kritische) punten die verbeterd kunnen worden om het netwerk naar een nog hoger niveau te brengen."* [3]

Waarbij de rekenkamer de volgende aanvullende conclusie heeft getrokken n.a.v. het voorgaande en de bevindingen die gedaan zijn in 2022:

[1] Een penetratietest of pentest is een toets van een of meer computersystemen op kwetsbaarheden, waarbij deze kwetsbaarheden ook werkelijk gebruikt worden om in deze systemen in te breken, met als doel de systemen beter te beveiligen. Een penetratietest (pentest) laat zien of de organisatie voldoende weerbaar is tegen digitale aanvallen. Het geeft inzicht in de kwetsbaarheden van de IT-infrastructuur en de mogelijke gevolgen hiervan.

[2] Bron: rapport SchipperIT; penetratietest

[3] Bron: rapport SchipperIT; penetratietest

3. Het deel van het IT-landschap dat in 2022 in beheer was bij de gemeente Baarn was toe aan een grondige praktijktest op het gebied van informatieveiligheid.[4]
   Toelichting:
   a. De 8 onderdelen van het IT-landschap die in beheer waren bij de gemeente Baarn zijn getest. (zie Tabel 1: Overzicht van getoetste onderdelen IT landschap Baarn, op p.15 van de Quickscan Opvolging Penetratietests 2022 in het besloten deel van het raadsinformatiesysteem, voor het detailoverzicht)
   b. In totaal zijn 68 subonderdelen getest, waarbij er bij 58 subonderdelen bevindingen zijn geconstateerd die om actie/verbetering vroegen.
   c. In totaal zijn er 185 bevindingen geconstateerd.[5]

Daarbij werden tegelijkertijd de volgende aanbevelingen gedaan (door SchippersIT aan de ambtelijke organisatie):

1. *"Er zijn door Schippers IT echter veel […][6] aangetroffen. Schippers IT raadt met klem aan de adviezen, beschreven in het rapport, over te nemen en deze door een beveiligingsspecialist uit te laten voeren."*
2. *"Nadat gemeente Baarn de adviezen heeft opgevolgd is het verstandig nogmaals een controle op de externe en interne ICT infrastructuur uit te laten voeren."*
3. *"Tevens raadt Schippers IT aan om monitoring toe te passen op het huidige netwerk van gemeente Baarn."*

Tweede onderdeel van het onderzoek Informatieveiligheid (2023)

Na afronding van de genoemde penetratietests heeft de rekenkamer zich gericht op de afronding van het onderzoek naar 'Inburgering en Integratie' en een nieuw, ander onderzoek naar 'Dienstverlening', met de bedoeling om ca. een jaar na afronding van de penetratietest (ergo: na de zomer 2023) tegelijkertijd:

1. De opvolging van de penetratietests uit 2022 te onderzoeken (met de vraag of de bevindingen / aanbevelingen vanuit de penetratietests adequaat zijn opgepakt).
   a. NB: onderzoek naar de opvolging van dergelijke aanbevelingen vindt bij voorkeur plaats ná een bepaalde periode, zodat: 1. de organisatie de kans heeft gehad om de aanbevelingen op te volgen en 2. de kwetsbaarheden op (kunnen) zijn gelost, zodat niet breder dan functioneel strikt noodzakelijk over bestaande kwetsbaarheden hoeft te worden gerapporteerd;
2. Het tweede deel van het onderzoek naar Informatieveiligheid uit te voeren (een brede assessment op (delen van) de BIO[7]).

---

[4] Conclusie Rekenkamer o.b.v. conclusies SchippersIT en de resultaten uit de penetratietest

[5] NB: voor de servers golden vaak dezelfde aanbevelingen voor meerdere servers; deze aanbevelingen zijn voor elke server apart meegeteld.

[6] Voor meer specifieke informatie wordt – gezien de gevoeligheid ervan – verwezen naar de Quick-scan 'Opvolging Penetratietests 2022' in het besloten gedeelte van het RaadsInformatieSysteem.

[7] De Baseline Informatiebeveiliging Overheid (BIO) beschrijft het basisniveau voor informatiebeveiliging. De BIO wordt gehanteerd binnen de Nederlandse overheid, door het Rijk, Gemeenten, Waterschappen en Provincies. Dit is één basisniveau voor informatiebeveiliging, één gezamenlijke taal voor alle overheidsorganisaties. De BIO heeft controls en benoemd maatregelen die genomen kunnen/moeten worden, op diverse aspecten van informatieveiligheid, zoals:

- Basis-infrastructuur gebouwen, toegang, electriciteitsvoorziening, telecom
- ICT ICT-infrastructuur, ICT-programma's, apps
- Mens & Organisatie werkwijzen, manieren, routiines, gewoonten en gedrag

En kijkt daarnaaast naar de volgende karakteristieken van gegevens:

- Betrouwbaarheid beschikbaarheid van gegevens (bijv. bij uitval systemen)
- Integriteit juiste, up-to-date, volledige informatie
- Vertrouwelijkheid (on)toegankelijkheid van gegevens voor (on)bevoegden

Op 14 november 2023 heeft een college-informatieavond plaatsgevonden voor raadsleden, waarin een presentatie is gehouden over het Informatie(veiligheids)beleid en heeft de gemeenteraad op 16 november 2023 een RIB ontvangen[8] over de voortgang van het informatiebeveiligingsplan (IBB). Naast de inhoudelijke informatie staat in de RIB het volgende vermeld:

> *"De rekenkamercommissie stelt een onderzoek in naar waar we staan op het gebied van Informatiebeveiliging op basis van de BIO. Ook vanuit de regio was al besloten om een BIO gapanalyse uit te voeren. In het eerste kwartaal van 2024 wordt gestart met een onderzoek door een externe auditor waarmee zowel de BIO gap-analyse als het rekenkameronderzoek uitgevoerd worden."*

Gezien de informatieavond die heeft plaatsgevonden, de voortgang van het IBB waarover de gemeenteraad op de hoogte is gesteld én het feit dat in het eerste kwartaal van 2024 wordt gestart met een onderzoek door een externe auditor – ingegeven door de regio en in opdracht van de gemeente Baarn zelf (niet in opdracht van de rekenkamer – heeft de rekenkamer besloten het tweede deel van het onderzoek naar informatieveiligheid zoals was voorgenomen, niet meer in die volle breedte uit te voeren. Dit zou namelijk grotendeels overlappen, of zelfs geheel dubbel werk zijn met dat onderzoek door de externe auditor. De rekenkamer merkt daarnaast graag op dat het genoemde onderzoek dat in het eerste kwartaal van 2024 door een externe auditor wordt uitgevoerd niet moet worden gezien als een onderzoek van/voor/door de rekenkamer. De reikwijdte van het onderzoek door de externe auditor, in opdracht van de gemeente Baarn, lijkt weliswaar redelijk overeen te komen met wat de rekenkamer beoogde te doen, maar bij de uitvoering ervan heeft de rekenkamer geen rol.

Quick-scan 'Opvolging Penetratietests 2022'

Wél heeft de rekenkamer het deel van het voorgenomen onderzoek naar de opvolging van de in 2022 uitgevoerde penetratietests uitgevoerd middels een Quick-scan 'Opvolging Penetratietests 2022'. Daarbij is de rekenkamer nagegaan of en in welke mate er opvolging is gegeven aan de aanbevelingen die door het gespecialiseerde externe bureau in 2022 zijn gedaan.

De conclusies van de Quick-scan – uitgevoerd eind 2023 / begin 2024 – over de opvolging van de aanbevelingen uit 2022 zijn – op hoofdlijnen – de volgende:

1. De aanbevelingen van SchippersIT in juni 2022, naar aanleiding van de penetratietests, zijn in de maanden na het uitkomen van het rapport voortvarend opgepakt door de gemeente Baarn. Daarna is er een periode geweest van verminderde aandacht, o.a. door personele wisselingen zowel bij de gemeente Baarn als bij de RID, maar is (wellicht mede door het doorwerkingsonderzoek van de rekenkamer) eind 2023 hernieuwde aandacht voor de (resterende) acties geweest. Het resultaat is nu dat nagenoeg alle naar aanleiding van de penetratietest in 2022 door SchippersIT geadviseerde acties zijn uitgevoerd, waarbij voor enkele acties geldt dat zij op korte termijn (in 2024) – als onderdeel van nog lopende projecten – worden uitgevoerd.
2. Er zijn acties ondernomen en er is aandacht geweest voor het op informatieveiliger wijze opslaan en delen van documenten (met vertrouwelijke gegevens) binnen de gemeente en bewustwording daarover. Dit heeft zeker de komende periode nog en ook daarna blijvende aandacht nodig.

Hierbij heeft de rekenkamer ook een aantal aanbevelingen gedaan aan de ambtelijke organisatie. Deze aanbevelingen zijn om genoemde reden van vertrouwelijkheid opgenomen in de Quick-scan zelf.

[8] RIB met kenmerk 687485 / 864157.

Het volledige resultaat van de Quick-scan naar de opvolging van de aanbevelingen die uit de penetratietests (2022) zijn gekomen, vindt u in het separate document daarover. Omdat de Quick-scan vertrouwelijke informatie bevat, is deze in het besloten gedeelte van het raadsinformatiesysteem opgenomen.

Met vriendelijke groet,

Rekenkamer Baarn