REKENKAMERCOMMISSIE BUREN

Onderzoek Rekenkamercommissie gemeente Buren

"Quick scan Informatieveiligheid"

Rapport uitgebracht september 2016

INHOUDSOPGAVE

1. Aanbiedingsbrief aan de Raad van de Rekenkamercommissie bij het rapport “Quick scan Informatieveiligheid” d.d. 8 augustus 2016

2. Quick scan Informatieveiligheid Rekenkamercommissie gemeente Buren 2016 van 1 augustus 2016

3. Bestuurlijke reactie op het rekenkameronderzoek “Quick scan Informatieveiligheid” van het college van Burgemeester en Wethouders via de brief van 31 augustus 2016, kenmerk UIT/1654502/Z16-43250

4. Nawoord van de Rekenkamercommissie van 19 september 2016 als reactie op de bestuurlijke reactie van het college van Burgemeester en Wethouders van 31 augustus 2016, kenmerk UIT/1654502/Z16-43250

Aan de Raad van de gemeente Buren

Maurik, 8 augustus 2016
Betreft: Aanbiedingsbrief bij het rapport
"Quick scan Informatieveiligheid"

INLEIDING

Met dit rapport informeren wij u over de resultaten van ons onderzoek "Quick scan Informatieveiligheid".

Digitale veiligheid is een actueel onderwerp voor overheden en dus ook voor de gemeente Buren. De doelstelling van de Rijksoverheid is om voor het jaar 2017 alle overheidsdienstverlening digitaal ontsloten te hebben.

Met grote regelmaat halen cyberaanvallen het nieuws, waarbij dienstverlening is verstoord of misbruik is gemaakt van vertrouwelijke informatie.

Door overheden wordt hard gewerkt aan het optimaliseren van informatieveiligheid, bijvoorbeeld aan de hand van Baselines Informatiebeveiliging (BIG) voor de verschillende overheidslagen. Iedere overheidsorganisatie neemt verantwoordelijkheid voor de eigen informatieveiligheid.

Gemeenten zijn als professionele, meest nabije overheid verantwoordelijk voor het op orde hebben van hun informatieveiligheid. Dit zullen en mogen burgers, bedrijven en ketenpartners van gemeenten verwachten. Deze verantwoordelijkheid strekt uiteraard verder dan de eigen organisatie. Gemeenten hebben er als collectief immers belang bij dat alle gemeenten en alle (keten)partners de informatieveiligheid op orde hebben. In 2013 is in dit kader in de Buitengewone Algemene Ledenvergadering van de VNG met algemene stemmen een aantal besluiten genomen.

In deze aanbiedingsbrief geven wij u inzicht in de stand van zaken rondom informatieveiligheid binnen de gemeente Buren. Wij hebben hiervoor als normenkader 4 onderzoeksvragen opgesteld, namelijk:

1. Hoe staat het met de bekendheid van de Baseline Informatiebeveiliging Gemeenten in de ambtelijke organisatie?
2. Is er een beveiligingsorganisatie en zo ja is de organisatie op beveiligingsgebied ingericht?
3. Is de verantwoordelijkheid bestuurlijk en ambtelijk belegd en zo ja hoe?
4. Is de organisatie qua informatieveiligheid klaar voor de toekomst? En daaraan gekoppeld: is de er voldoende duidelijkheid over rollen etc. van onder meer de security officer(s)?

Wij zijn bij het onderzoek ondersteund door BKBO, Bureau voor Kwaliteitsborging bij de Overheid.
Na de documentenstudie is voor dit onderzoek een aantal interviews gehouden. Een overzicht van de interviews is vermeld op pagina 21 van het onderzoeksrapport.

Wij danken de betrokken bestuurder en de medewerkers voor hun bijdrage aan dit onderzoek.

De rekenkamercommissie heeft op basis van de bevindingen en conclusies in het onderzoeksrapport conclusies getrokken en daarbij aanbevelingen opgesteld.

CONCLUSIE

In Hoofdstuk 4 van het rapport zijn de hiervoor genoemde 4 onderzoeksvragen beantwoord en conclusies getrokken die wij hieronder in verkorte vorm weergeven.

- Positief is dat in de gemeente Buren Informatieveiligheid daadwerkelijk op de agenda staat en goed is opgepakt.
- De gemeente Buren is nog niet gestart met de structurele invoering van de Baseline Informatiebeveiliging (BIG). Hierdoor ontbreekt een integrale aanpak.
- Informatieveiligheid is nog geen onderdeel van de reguliere planning- en controlcyclus.
- Bewustwording van de risico's op het gebied van informatiebeveiliging is een uitdaging voor de gemeente Buren.

Op grond van deze conclusies bevelen wij het volgende bij u aan:

AANBEVELINGEN

Spreek met het college van Burgemeester en Wethouders af:

1. om in 2016 de informatieveiligheid bestuurlijk en organisatorisch te borgen en integraal in te richten overeenkomstig het normenkader zoals vermeld in de Baseline Informatiebeveiliging (BIG).

2. dat in de documenten van de Planning en Controlcyclus in het vervolg de gemeenteraad (smart) wordt geïnformeerd over de informatieveiligheid met de BIG als normenkader.

3. de risico's goed in beeld te brengen en in een gezamenlijke prioriteitenafweging de noodzakelijke verbeteringen door te voeren.

TOT SLOT

Wij hebben in 2013 het rapport E-Buren na 2013 – "Meer grip wenselijk" over de elektronische dienstverlening in de gemeente Buren uitgebracht. De aanbevelingen in dat rapport zijn door de gemeenteraad overgenomen.

Informatieveiligheid is in de bedrijfsvoering een belangrijk item waar het gaat om een doeltreffende en veilige elektronische dienstverlening. Uiteindelijk is het bedoeld om de bedrijfsrisico's in de informatie-uitwisseling te beheersen.
Wij hebben in het rapport over elektronische dienstverlening gewezen op het belang, dat de gemeenteraad in de gelegenheid wordt gesteld om "aan de knoppen" te kunnen draaien. Dat geldt eveneens voor informatieveiligheid.
In dat verband zien wij met belangstelling uit naar de besluitvorming over dit rapport en de verdere afwikkeling van de aanbevelingen.

De Rekenkamercommissie Buren,
H.J.F.L. Meeuwsen MBA AC, voorzitter
Drs. P.J.J. Bremmer
R.F.J. Spelier MSc
W. van Beem, ambtelijk secretaris

Quick scan Informatieveiligheid Rekenkamercommissie gemeente Buren 2016

Kenmerk BKBO/151208-2/QS

Onderzoekers:	Functie BKBO
drs. M.B.H. IJpelaar RE CEH CISA	Lead IT auditor
A.M.J. van Helvoort	Management-assistente

1 augustus 2016
Versie 1.01
Dit rapport heeft 24 pagina's

Inhoudsopgave

1 Managementsamenvatting 4

2 Onderzoeksopzet 7
2.1 Doelstelling van de quick scan 7
2.2 Het normenkader en de beoordelingscriteria 7
2.3 Werkwijze bij de uitvoering van de quick scan 8
2.4 Beperkingen van de quick scan 8

3 Informatiebeveiliging toegelicht 9
3.1 Het belang van informatie 9
3.2 Wat is informatiebeveiliging? 9
3.3 De Baseline Informatiebeveiliging Gemeenten 10
3.4 Verantwoordelijkheden in de informatiebeveiliging 10
3.4.1 College van Burgemeester en Wethouders 10
3.4.2 Directie, ambtelijke top 11
3.4.3 Lijnmanagement 11
3.4.4 ICT afdeling, facilitaire zaken 11
3.4.5 Chief Information Security Officer 11

4 Feitenrelaas 13
4.1 Inleiding 13
4.2 Bekendheid van de Baseline Informatiebeveiliging Gemeenten 13
4.2.1 Feiten m.b.t. de bekendheid van de BIG in de organisatie 13
4.3 Beveiligingsorganisatie 14
4.3.1 Feiten over de beveiligingsorganisatie 14
4.4 Bestuurlijke en ambtelijke verantwoordelijkheden 15
4.4.1 Feiten m.b.t. ambtelijke en bestuurlijke verantwoordelijkheden 15
4.5 Klaar voor de toekomst? 16
4.5.1 Feiten 16
4.6 Conclusies 19
4.6.1 Bekendheid van de Baseline Informatiebeveiliging Gemeenten 19
4.6.2 Beveiligingsorganisatie 19
4.6.3 Bestuurlijke en ambtelijke verantwoordelijkheid 19
4.6.4 Klaar voor de toekomst? 20

Bijlage A Respondenten 21

Bijlage B Geraadpleegde documenten 22

Bijlage C Begrippen 23

1 Managementsamenvatting

De leden van de VNG hebben in de Buitengewone Algemene Leden Vergadering van 29 november 2013 met algemene stemmen besloten dat:

a) Informatieveiligheid onderdeel wordt van collegeambities en opgenomen wordt in de portefeuille van een van de leden van het college van B&W.
b) Gemeenten zorgen voor verankering van informatieveiligheid op de gemeentelijke agenda, waarbij het college de gemeenteraad informeert. Dit gebeurt door middel van een aparte paragraaf informatieveiligheid in het jaarverslag.
c) Gemeenten de Baseline Informatiebeveiliging Gemeenten (= BIG) vaststellen als hét gemeentelijke basisnormenkader voor informatieveiligheid. De BIG is een meetlat waarlangs de inspanningen op het gebied van informatieveiligheid kunnen worden gelegd.
d) Gemeenten informatieveiligheidsbeleid vaststellen aan de hand van de Baseline Informatiebeveiliging Gemeenten.
e) Gemeenten informatieveiligheid bestuurlijk en organisatorisch borgen door aansluiting in de reeds bestaande planning- en controlcyclus.
f) Gemeenten de lokale invulling rondom het thema van informatieveiligheid transparant maken voor burgers, bedrijven en (keten)partners.

Voorliggend onderzoek is een quick scan naar de stand van zaken rondom informatieveiligheid binnen de gemeente Buren. Deze quick scan heeft het karakter van het steken van een thermometer in de gemeentelijke organisatie om zicht te krijgen op de actuele stand van zaken. Dit onderzoek is uitgevoerd ten behoeve van de gemeenteraad van Buren in opdracht van de rekenkamercommissie (= RKC).

Naast het bestuderen van de beschikbare documenten is ook een aantal interviews met sleutelfunctionarissen afgenomen. Deze interviews hebben als doelstelling om het eventuele verschil bloot te leggen tussen de administratieve werkelijkheid zoals in de beleidsplannen en procedures gedefinieerd en de werkelijke situatie.

Op de volgende vier vragen wil de RKC met de quick scan een helder antwoord:

1) Hoe staat het met de bekendheid van de Baseline Informatiebeveiliging Gemeenten in de ambtelijke organisatie?
2) Is er een beveiligingsorganisatie en zo ja hoe is de organisatie op beveiligingsgebied ingericht?
3) Is de verantwoordelijkheid bestuurlijk en ambtelijk belegd en zo ja hoe?

4) Is de organisatie qua informatieveiligheid klaar voor de toekomst? En daaraan gekoppeld: is er voldoende duidelijkheid over rollen etc. van onder meer de security officer(s)?

Wij komen na bestudering van het verkregen bewijsmateriaal, de volledigheid, juistheid en actualiteit van de vergaarde informatie en de mate van medewerking van de medewerkers van de gemeente Buren tot de volgende conclusies.

1) De Baseline Informatiebeveiliging Gemeenten is -behalve bij ICT en de security functionarissen- als zodanig nauwelijks bekend in de organisatie. De gemeente Buren is nog niet gestart met de structurele invoering van de Baseline Informatiebeveiliging Gemeenten, maar heeft eerst een aantal speerpunten aangepakt zoals geformuleerd in het gemeentebrede informatiebeveiligingsplan. Het nadeel van de huidige aanpak is dat niet zichtbaar is welke beveiligings-maatregelen uit de Baseline *niet* worden genomen. Informatieveiligheid staat op de agenda en vastgesteld is dat er aan bewustwording voor beveiligingsrisico's van het ambtelijk apparaat voortvarend wordt gewerkt. Het informatiebeveiligingsbeleid gemeente Buren 2014-2017 is door de organisatie *zelf* opgesteld, en niet van een standaard overgenomen. Dat is zeer positief, want er is binnen de organisatie *zelf* over nagedacht.
2) De governance rondom informatieveiligheid is ingericht, maar is wel afhankelijk van de inzet van enkele personen. Informatieveiligheid is nog geen onderdeel van de reguliere planning- en controlcyclus. Zo wordt niet gerapporteerd over de voortgang van de invoering van de beveiligingsmaatregelen uit het gemeentebrede informatiebeveiligings-plan. Positief is dat er op ambtelijk niveau een periodiek overkoepelend beveiligingsoverleg actief is.
3) De verantwoordelijkheid voor informatieveiligheid is zowel bestuurlijk als ambtelijk belegd. De rolverdeling is helder. Dat laat onverlet dat sommige zaken verder moeten worden geformaliseerd. Bewustwording van de risico's op het gebied van informatiebeveiliging is een uitdaging voor de gemeente Buren. Het thema informatieveiligheid komt (nog) niet regelmatig binnen het college van Burgemeester en Wethouders en de gemeenteraad aan de orde.
4) De gemeente Buren heeft de ICT goed op orde, zeker op het technische vlak. Dat blijkt bijvoorbeeld uit het feit dat andere organisaties de ICT hebben inbesteed bij de gemeente Buren zonder dat dit ten koste is gegaan van de eigen dienstverlening van Buren.

5) De organisatie is echter niet helemaal klaar voor de bedreigingen van de toekomst; vooral omdat een integrale aanpak ontbreekt. De gemeente Buren is gebaat bij harmonisatie van beveiligingsregels. Het implementeren van beveiligingsmaatregelen op basis van de genoemde gemeentebrede Baseline Informatiebeveiliging Gemeenten vormt zo'n integrale aanpak en dit verdient de voorkeur. De huidige aanpak is niet integraal maar domein-gebonden. Elk domein heeft een apart beveiligingsbeleid en/of -plan[1]. Dit wordt veroorzaakt door verkokering op het niveau van de Rijksoverheid, waarbij elk departement zijn eigen (beveiligings)-regels stelt en deze oplegt aan het organisatieonderdeel van de gemeente dat taken in medebewind uitvoert. Deze domein-gebonden beveiligingsaanpak is noch efficiënt noch effectief. Elke keer wordt het "wiel als het ware opnieuw uitgevonden" door anderen. Ondersteunende afdelingen zoals ICT, en in mindere mate facilitaire zaken en personeelszaken hebben hier nadeel van.

[1] *Zoals voor de Basisadministratie Adressen en Gebouwen (= BAG), Basis Registratie Personen (= BRP) voor de Reisdocumenten en Rijbewijzen, en het Suwinet.*

2 Onderzoeksopzet

2.1 Doelstelling van de quick scan

De RKC wil met de -door een onafhankelijk bureau uit te voeren "quick scan"- een peilstok in de gemeentelijke organisatie (laten) steken, om zicht te krijgen op de actuele stand van zaken rondom informatiebeveiliging. Dit alles met als doel de informatieveiligheid op een (nog) hoger niveau te tillen.

Op de volgende vier vragen wil de RKC met de quick scan een helder antwoord:

1) Hoe staat het met de bekendheid van de Baseline Informatiebeveiliging Gemeenten in de ambtelijke organisatie?
2) Is er een beveiligingsorganisatie en zo ja hoe is de organisatie op beveiligingsgebied ingericht?
3) Is de verantwoordelijkheid bestuurlijk en ambtelijk belegd en zo ja hoe?
4) Is de organisatie qua informatieveiligheid klaar voor de toekomst? En daaraan gekoppeld: is er voldoende duidelijkheid over rollen etc. van onder meer de security officer(s)?

2.2 Het normenkader en de beoordelingscriteria

Voorliggend onderzoek is in de periode van 9 maart 2016 tot en met 22 april 2016 door BKBO uitgevoerd conform het vooraf met de RKC afgesproken normenkader.[2] Dit normenkader bestaat uit:

- De richtlijnen zoals opgenomen in de wet Bescherming Persoonsgegevens zoals geldend vanaf 1 januari 2016 (inclusief meldplicht datalekken);
- De beveiligingsmaatregelen zoals omschreven in de Baseline Informatie-beveiliging Gemeenten;
- Specifieke normensets die door de Rijksoverheid zijn opgelegd aan gemeenten, zoals gespecificeerd in de vragenlijst rondom Suwinet van de Inspectie Sociale Zaken en Werkgelegenheid en de zelfevaluaties voor zowel de Basis Registratie Personen als voor de Reisdocumenten van de Rijksdienst voor Identiteits Gegevens (= RvIG).

[2] *De ambtelijke reactie op dit rapport is, voorzover relevant, verwerkt.*

2.3 Werkwijze bij de uitvoering van de quick scan

Naast het bestuderen van een aantal gericht opgevraagde documenten zijn ook interviews met 9 sleutelfunctionarissen afgenomen. Deze interviews zijn bedoeld om het eventuele verschil bloot te leggen tussen de administratieve werkelijkheid zoals in de beleidsplannen en procedures gedefinieerd (= opzet in auditorstaal) en de werkelijke situatie in het gemeentelijk apparaat (= het bestaan). Zeker bij het thema informatieveiligheid, zien wij vaak een kloof tussen de papieren werkelijkheid en de situatie van alledag waarin van prioriteit naar prioriteit wordt gestruikeld [3].

2.4 Beperkingen van de quick scan

Het betreft hier een quick scan met een select aantal interviews op basis van een beperkte doorsnede door de gemeentelijke organisatie. Een quick scan is geen uitgebreid onderzoek waarin tot oordeelsvorming kan worden overgegaan. Wij geven slechts antwoord op de gestelde vragen en matigen ons geen oordeel aan over de kwaliteit en diepgang van alle interne beheersingsmaatregelen rondom informatie-veiligheid die de gemeente Buren al dan niet heeft getroffen.

Wij wijzen u erop dat, indien deze beperkingen niet van toepassing waren, wellicht andere aandachtspunten zouden zijn geconstateerd die voor rapportering in aanmerking zouden zijn gekomen.

[3] *Voor een overzicht van de interviews wordt verwezen naar Bijlage A. - Respondenten*

3 Informatiebeveiliging toegelicht

3.1 Het belang van informatie

Informatie is één van de belangrijkste bedrijfsmiddelen van de gemeente. Toegankelijke en betrouwbare overheidsinformatie is essentieel voor elke gemeente, die zich verantwoordelijk gedraagt, aanspreekbaar en servicegericht is, die transparant en proactief verantwoording aflegt aan burgers en raadsleden en die met minimale middelen maximale resultaten behaalt.
De bescherming van waardevolle informatie is hetgeen waar het uiteindelijk om gaat. Hoe waardevoller de informatie is, hoe meer en zwaardere beveiligingsmaatregelen er getroffen moeten worden.

3.2 Wat is informatiebeveiliging?

Informatiebeveiliging is de verzamelnaam voor de processen, die ingericht worden om de betrouwbaarheid van gemeentelijke processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens te beschermen tegen al dan niet opzettelijk onheil. Het begrip 'informatiebeveiliging' heeft betrekking op:

- *beschikbaarheid:* het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers. Een voorbeeld van het belang hiervan is het niet beschikbaar zijn van systemen door stroomuitval of een virusaanval waardoor het netwerk "plat ligt" en medewerkers niet kunnen werken (recent gebeurd bij de gemeenten Arnhem, Kaag en Braassem).
- *integriteit:* het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking. Een voorbeeld is het onbevoegd kijken in Suwinet. Een ander voorbeeld hoe het verkeerd kan gaan is te vinden bij de opvang van asielzoekers. Uit recent onderzoek blijkt dat gegevens over asielzoekers in ongeveer 300 verschillende bestanden zijn verzameld door het rijk, gemeenten, COA en andere diensten. De kans op een verkeerde overname van gegevens wordt dan levensgroot.
- *vertrouwelijkheid*: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn. Een voorbeeld van het belang is het laten slingeren van een USB stick waarop alle informatie van de cliënten en gezinnen voor de jeugdzorg staat vermeld (recent gebeurd bij de gemeente Amersfoort).

3.3 De Baseline Informatiebeveiliging Gemeenten

De laatste jaren worden alle overheden geplaagd door beveiligingsincidenten. Zo is er een behoefte ontstaan aan een fundamentele oplossing van het informatieveiligheids-probleem. De rijksoverheid gaat eveneens nadere eisen stellen aan de beveiliging van de gemeentelijke informatiehuishouding. Ook in het onderzoek van de Onderzoeksraad voor de Veiligheid naar het DigiNotar-incident is een dergelijk aanbeveling opgenomen. Daarom is de Baseline Informatiebeveiliging Nederlandse Gemeenten ontwikkeld.

Wanneer alle overheden hun informatievoorziening en ICT inrichten volgens een vergelijkbare Baseline, dan is een garantie dat gemeenten hun eigen informatie en die van andere overheidsinstellingen zowel centraal als decentraal veilig behandelen. Onder veilig wordt verstaan: betrouwbaar, beschikbaar en correct. Overheden moeten elkaar hierop kunnen aanspreken. Bij de implementatie geldt voor de normen en eisen een 'Pas toe of leg uit beleid'.

In de Baseline wordt het 'Schengen'-principe gehanteerd. Dit houdt in, dat organisatieonderdelen van de overheid elkaar beschouwen als vertrouwd partner en niet als onvertrouwde buitenwereld. Het gevolg hiervan is dat iedere overheids-organisatie afzonderlijk zijn omgeving beveiligt en 'schoon' houdt en dat de andere omgevingen hierop kunnen vertrouwen. Hierbij moet controle de basis van het vertrouwen zijn (governance). Zo kent het rijk de Baseline Informatiebeveiliging Rijksdienst (= BIR) en de waterschappen de Baseline Informatiebeveiliging Waterschappen (= BIWA).

3.4 Verantwoordelijkheden in de informatiebeveiliging

De Baseline Informatiebeveiliging Nederlandse Gemeenten kent de volgende verantwoordelijkheidsverdeling:

3.4.1 College van Burgemeester en Wethouders

Het college van Burgemeester en Wethouders is integraal verantwoordelijk voor de beveiliging (in de beslissende rol) van informatie binnen de werkprocessen van de gemeente en stelt kaders voor informatiebeveiliging op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders.

3.4.2 Directie, ambtelijke top

De directie (in de sturende rol) is verantwoordelijk voor kaderstelling en sturing. De directie:

- stuurt op concern risico's;
- controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden;
- evalueert periodiek beleidskaders en stelt deze waar nodig bij.

3.4.3 Lijnmanagement

De lijnmanagers van de afdelingen binnen de gemeente zijn (in de vragende rol) verantwoordelijk voor de integrale beveiliging van hun organisatieonderdeel. Het lijnmanagement:

- stelt op basis van een expliciete risicoafweging betrouwbaarheidseisen (beschikbaarheid, integriteit en vertrouwelijkheid) voor zijn informatiesystemen vast (classificatie);
- is verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
- stuurt op beveiligingsbewustzijn, betrouwbaarheidseisen en naleving van regels en richtlijnen (gedrag en risicobewustzijn);
- rapporteert over compliance aan wet- en regelgeving en specifiek beleid van de gemeente in de managementrapportages.

3.4.4 ICT afdeling, facilitaire zaken

De organisatieonderdelen ICT, P&O, Bedrijfsvoering, Facilitaire zaken (gebouwenbeheer) zijn (in de uitvoerende rol) verantwoordelijk voor de uitvoering van beveiligingsmaatregelen.

3.4.5 Chief Information Security Officer

De chief information security officer (beveiligingscoördinator) bevordert en adviseert gevraagd en ongevraagd over informatiebeveiliging en rapporteert periodiek gemeentebreed aan de directie over de stand van zaken. In de gemeente Buren is deze rol belegd bij de concerncontroller (beveiligingscoördinator) welke de volgende taken uitvoert:

- Het (laten) uitvoeren van audits informatiebeveiliging;
- Contactpersoon voor VNG en KING op dit gebied;
- Beoordelen rapportages over beveiligingsincidenten.

Daarnaast is er een security officer Suwinet aangewezen. Deze is verantwoordelijk voor het actueel en volledig zijn en blijven van het Beveiligingsplan Suwinet. Jaarlijks rapporteert hij aan het college van Burgemeester en Wethouders over het beveiligingsplan en de bevindingen op dit gebied. Omwille van de functiescheiding is deze rol onder de afdeling Bedrijfsvoering gebracht in de functie 1.1.23, proces- en informatiemanager (HR21 adviseur).

4 Feitenrelaas

4.1 Inleiding

Op de volgende vier vragen wil de RKC met de quick scan een helder antwoord:

1) Hoe staat het met de bekendheid van de Baseline Informatiebeveiliging Gemeenten in de ambtelijke organisatie?
2) Is er een beveiligingsorganisatie en zo ja hoe is de organisatie op beveiligingsgebied ingericht?
3) Is de verantwoordelijkheid bestuurlijk en ambtelijk belegd en zo ja hoe?
4) Is de organisatie qua informatieveiligheid klaar voor de toekomst? En daaraan gekoppeld: is er voldoende duidelijkheid over rollen etc. van onder meer de security officer(s)?

4.2 Bekendheid van de Baseline Informatiebeveiliging Gemeenten

Op basis van de door ons verzamelde bewijsstukken (documenten en interviews) kunnen we de onderstaande feiten vaststellen met de beperkingen zoals eerder aangegeven.

4.2.1 Feiten m.b.t. de bekendheid van de BIG in de organisatie

- De Baseline Informatiebeveiliging Gemeenten is -behalve bij ICT en de security functionarissen- als zodanig nauwelijks bekend in de organisatie, uiteraard voor zover wij dit hebben kunnen vaststellen in deze uitgevoerde quickscan.
- Het gemeentebrede informatiebeveiligingsbeleid 2014-2017, dat op de min of meer met de BIG vergelijkbare ISO27002 norm is gebaseerd, is wel bekend in de organisatie. Naar dit plan wordt echter niet integraal gehandeld aangezien de organisatieonderdelen eigen beveiligingsplannen hebben zoals voor de BRP en Suwinet.
  Het informatiebeveiligingsbeleid is een goede aanzet temeer daar het geen standaardplan is. Dit plan vormt geen integraal beleid waarin alle gemeentelijke domeinen, interne beheersmaatregelen en beveiligingsmaatregelen met elkaar in verband worden gebracht en geprioriteerd. Het plan focust namelijk op een aantal

aspecten die bij de totstandkoming van het beleid als het meest prangend werden ervaren bij het management. Daarnaast wordt het plan niet aantoonbaar geactualiseerd noch wordt over de voortgang gerapporteerd.

- Hoewel de Baseline Informatiebeveiliging Gemeenten minder bekend is, is informatiebeveiliging zeker een thema binnen de ambtelijke organisatie. Hierin spelen o.a. de bewustwordingssessies en intranetmeldingen van met name de beveiligingscoördinator en de security officer Suwinet een activerende en stimulerende rol in. Zij laten zich horen en weten ook verbeteringen in de uitvoeringsprocessen te bereiken, zoals een afdoende functiescheiding ook al gaat dat ten koste van de efficiency van de bedrijfsvoering.

4.3 Beveiligingsorganisatie

4.3.1 Feiten over de beveiligingsorganisatie

- Het informatiebeveiligingsbeleid gemeente Buren 2014-2017 is door de organisatie *zelf* opgesteld, en niet van een standaard overgenomen. Dat is zeer positief, want er is binnen de organisatie *zelf* over nagedacht.
- Het informatiebeveiligingsbeleid is opgesteld aan de hand van de grootste risico's in 2013, althans die door de groep die er mee bezig was zo werden gezien. Er is geen gestructureerde analyse hiervoor uitgevoerd.
- Er wordt sindsdien niet gerapporteerd over de beheersing van de risico's. Er is geen statusoverzicht hierover. Uit de interviews komt naar voren dat er nieuwe beveiligingsrisico's zijn bijgekomen als gevolg van de decentralisatie van de WMO2015, Participatiewet en de Jeugdzorg. Het informatiebeveiligingsbeleid is vanaf eind 2014 echter niet meer geactualiseerd. De actualisering is voor 2017 gepland.
- Met de materiegebieden BRP en Reisdocumenten gaat het aantoonbaar goed qua beveiliging, data-integriteit (volledigheid, tijdigheid en juistheid) en beschikbaarheid.
- Hetzelfde geldt voor het team Werk en Inkomen. Waar veel andere gemeenten in grote problemen kwamen door de Suwinet zelfevaluatie, verordonneerd door de Inspectie SZW, voldoet Buren gewoon aan de eisen.
- De ambtelijke organisatie gaat in de praktijk niet uit van een gemeentebreed integraal beveiligingsbeleid of -plan maar gaat in de praktijk uit van materie gebonden beveiligingsrichtlijnen zoals bij de BRP, de waardedocumenten en het Suwinet. Een voorbeeld van de verkokerde beveiligingsaanpak is dat bij het team Werk en Inkomen geen beeld is hoe de toegang is geregeld voor Suwinet bij een ander organisatie onderdeel, het Publiekscentrum. Dat was namelijk ook geen eis

in de zelfevaluatie Suwinet. Niettemin is duidelijk een ontwikkeling gaande naar een meer integraal beveiligingsbeleid.
- Positief is dat er periodiek, in principe elke maand, een informatiebeveiligingsoverleg wordt gehouden. De kerngroep informatiebeveiliging bestaat uit de sleutelfunctionarissen op ambtelijk niveau.
- Een sterk punt dat spreekt voor de volwassenheid van de ICT organisatie is dat het wijzigingsbeheer in de ICT organisatie geïmplementeerd is waarbij de informatiebeveiliging een vast onderdeel is.

4.4 Bestuurlijke en ambtelijke verantwoordelijkheden

4.4.1 Feiten m.b.t. ambtelijke en bestuurlijke verantwoordelijkheden

- Bij het samenstellen van het gemeentebrede informatiebeveiligingsbeleid 2014 – 2017 heeft de Baseline Informatiebeveiliging Gemeenten niet als uitgangspunt gediend. Veel beveiligingsmaatregelen vanuit de BIG zijn niet in het plan opgenomen. Het plan bevat slechts een select aantal te realiseren beveiligingsmaatregelen. Dat is niet transparant want op deze wijze wordt de raad onvoldoende in staat gesteld zijn kaderstellende en controlerende rol inhoud te geven. Het is voor de raad dan niet goed mogelijk om duidelijke afspraken te maken met het college van Burgemeester en Wethouders over het informatieveiligheidsbeleid.
- Teamleiders en afdelingshoofden hebben de opdracht gekregen integriteit en informatiebeveiliging als vaste punten aan de orde te stellen in gesprekken met hun medewerkers.
- Meldingen over beveiligingsincidenten worden gerapporteerd. Voorbeelden van zaken die kunnen leiden tot beveiligingsincidenten worden op Intranet geplaatst om de bewustwording van de medewerkers positief te stimuleren.
- Clean desk policy (= het schoonhouden van bureaus en vertrouwelijke documenten opbergen), clear screen policy (computersessies niet open laten staan tijdens afwezigheid) zijn gecommuniceerd maar niet iedereen houdt zich daaraan; handhaving door het management is een aandachtspunt.
- Informatieveiligheid was binnen het college van Burgemeester en Wethouders specifiek als portefeuille bestempeld. Informatieveiligheid was echter geen thema binnen het college van Burgemeester en Wethouders; het wordt incidenteel benoemd.

- Het Informatiebeveiligingsbeleid 2014-2017 is niet expliciet besproken in het college van Burgemeester en Wethouders maar zonder bespreking vastgesteld.
- De security officer Suwinet en de beveiligingscoördinator houden het MT en het college van Burgemeester en Wethouders op de hoogte van de stand van zaken.

4.5 Klaar voor de toekomst?

4.5.1 Feiten

Robuustheid ICT organisatie

- De gemeente Buren lijkt als kleine gemeente over een relatief professionele ICT organisatie te beschikken. Dat uit zich volgens de respondenten in weinig beveiligingsincidenten maar ook doordat niet alleen het ICT incidentenbeheer is geïmplementeerd als ook het beheer van ICT wijzigingen. Dat uit zich ook door derden zoals de gemeente Neder-Betuwe en de Omgevingsdienst Rivierenland te bedienen zonder dat dit blijkbaar ten koste gaat van de eigen kwaliteit.
- Een ontwikkeling die eraan komt is de vraag of de gemeente Buren in staat is alles zelf te blijven doen of dat de gemeente gelet op de beperkte omvang van het ambtelijk apparaat samenwerking moet gaan zoeken. De gemeenteraad heeft besloten n.a.v. deze vraag een aantal uitgangspunten te formuleren en een SWOT analyse te laten uitvoeren op de uitvoering van de gemeentelijke taken. Op basis van de interviews komt naar voren dat de gemeente Buren op dit moment nog geen strategie heeft ontwikkeld op het gebied van ICT. Zelf doen, samenwerking met andere overheden of ICT uit besteden aan de markt zijn daarbij opties. De gemeente heeft de ambitie regiegemeente te zijn maar het is geen doel op zich. Inzet van ICT is steeds een afweging op basis van kosten, kwetsbaarheid en kwaliteit. Tot nu toe is het de keus om op ICT gebied alles in eigen beheer te blijven doen of de ICT voor andere organisaties op te pakken, maar hier ligt geen strategische visie aan ten grondslag. Binnen de organisatie is men bezig om integraal plannen op te stellen en om te kijken hoe omgegaan moet worden met de ontwikkelingen rondom de informatievoorziening (onder andere wordt hiervoor een swot analyse opgesteld.). Met name de ontwikkelingen rond leverancier PinkRoccade worden hierbij betrokken.
  Het voornemen van de ambtelijke organisatie is om deze plannen nog in 2016 in strategische keuzes uit te werken en het nieuwe visiedocument ter vaststelling voor te leggen aan de gemeenteraad.

- De visie achter de ICT inbesteding bij de gemeente Buren door de gemeente Lingewaal is kostenbesparend. De ICT dienstverlening vanuit de gemeente Buren aan de Omgevingdienst Rivierenland (= ODR) is ter compensatie van de achterblijvende kosten na het vertrek van het V&H personeel.

<u>Informatieveiligheid</u>

- Het informatiebeveiligingsbeleid gemeente Buren 2014-2017 geeft aan dat de Baseline Informatiebeveiliging Gemeenten invoeren een kostbaar en langdurig traject is en daarom maar niet ter hand moet worden genomen. Dit wijkt af van het beeld dat wij hebben bij andere gemeenten en is niet juist. Niet alleen hebben *alle* gemeenten de resolutie Informatieveiligheid eind 2013 in de ledenraad van de VNG bekrachtigd en zich daarmee aan de implementatie van de Baseline Informatiebeveiliging Gemeenten gecommitteerd. Maar daarnaast gaat de Baseline Informatiebeveiliging Gemeenten uit van het "pas toe of leg uit principe". De aanpak is normaliter dat gestructureerd wordt nagegaan welke beveiligings-maatregelen uit de BIG al zijn gerealiseerd (dit is de "gap" of verschillenanalyse) en vervolgens welke maatregelen alsnog moeten worden geprioriteerd en gerealiseerd (= de "impactanalyse"). Afwegingen van risico's en kosten spelen dan een rol.
- Verschillende nieuwe uitdagingen waarmee alle gemeenten worden geconfronteerd zijn in beeld. Daarvoor is o.a. de richtlijn Locatie Onafhankelijk Werken opgesteld door het ambtelijke apparaat in Buren. De organisatie is bezig om een richtlijn "veilig werken in de cloud" op te stellen om regels te stellen aan het werkgerelateerde gebruik door medewerkers van cloud voorzieningen als Dropbox etcetera. Ook moeten er nog regels worden opgesteld voor Bring Your Own Device (BYOD) waarbij medewerkers de eigen tablet en smartphone (willen) koppelen aan de gemeentelijke e-mail en ICT infrastructuur. Deze thema's worden ook uitgedragen en gecommuniceerd in de organisatie.
- Bewustheid en bewust houden van de veiligheidsrisico's in het gedrag van de eigen medewerkers en externen is en blijft een aandachtspunt met name voor het management, waarvan het belang niet kan worden onderschat. Hiervoor is ook een informatiebeveiligingsoverleg in het leven geroepen.
- Het opslaan van het systeemgebruik gebeurt wel, maar de analyse om bijvoorbeeld verkeerd gebruik of fraude te kunnen opsporen, verdient verbetering (dit is ook vastgesteld in de zelfevaluatie BRP).
- De externe accountant beveelt aan, ten aanzien van de wachtwoordpolicy m.b.t. Civision Middelen, om deze in overeenstemming te brengen met het eigen informatiebeveiligingsbeleid.

- Er is half december 2015 door het College een meldingenprocedure voor datalekken vastgesteld. De wettelijke plicht is ingegaan per 1-1-2016. De procedure is inmiddels geïmplementeerd.

4.6 Conclusies

4.6.1 Bekendheid van de Baseline Informatiebeveiliging Gemeenten

De Baseline Informatiebeveiliging Gemeenten is -behalve bij ICT en de security functionarissen- als zodanig nauwelijks bekend in de organisatie, voor zover wij hebben kunnen vaststellen tijdens het uitvoeren van deze quickscan. De gemeente Buren is nog niet gestart met de structurele invoering van de Baseline Informatiebeveiliging Gemeenten, maar heeft in plaats daarvan een aantal speerpunten aangepakt zoals geformuleerd in het gemeentebrede informatiebeveiligingsplan. Het nadeel van de door Buren gekozen aanpak is dat niet zichtbaar is welke beveiligingsmaatregelen uit de Baseline *niet* worden genomen. Informatieveiligheid staat evenwel op de agenda en vastgesteld is dat er aan bewustwording voor beveiligingsrisico's van het ambtelijk apparaat voortvarend wordt gewerkt.

4.6.2 Beveiligingsorganisatie

De governance rondom informatieveiligheid is ingericht maar is afhankelijk van de inzet van enkele personen. Informatieveiligheid is nog geen onderdeel van de reguliere planning- en controlcyclus. Zo wordt nog niet gerapporteerd over de voortgang van de invoering van de beveiligingsmaatregelen uit het gemeentebrede informatiebeveiligingsplan. Positief is dat er op ambtelijk niveau een periodiek overkoepelend beveiligingsoverleg actief is onder leiding van de beveiligingscoördinator.

4.6.3 Bestuurlijke en ambtelijke verantwoordelijkheid

De verantwoordelijkheid voor informatieveiligheid is zowel bestuurlijk als ambtelijk belegd. De rolverdeling is helder. Dat laat onverlet dat sommige zaken nog verder moeten worden geformaliseerd. Bewustwording van de risico's op het gebied van informatiebeveiliging is een uitdaging voor de gemeente Buren. Het thema informatieveiligheid komt (nog) niet regelmatig binnen het college van Burgemeester en Wethouders en de gemeenteraad aan de orde.

4.6.4 Klaar voor de toekomst?

De organisatie is niet helemaal klaar voor de bedreigingen van de toekomst; vooral omdat een integrale aanpak ontbreekt. De gemeente Buren is gebaat bij harmonisatie van beveiligingsregels. Het implementeren van beveiligingsmaatregelen op basis van de gemeentebrede Baseline Informatiebeveiliging Gemeenten vormt zo'n integrale aanpak en dit verdient de voorkeur.

De huidige aanpak is niet integraal maar domein-gebonden. Elk domein heeft een apart beveiligingsbeleid en/of -plan[4]. Dit wordt veroorzaakt door verkokering op het niveau van de Rijksoverheid, waarbij elk departement zijn eigen (beveiligings)regels stelt en deze oplegt aan het organisatie onderdeel van de gemeente dat taken in medebewind uitvoert. Deze domein-gebonden beveiligingsaanpak is noch efficiënt noch effectief. Elke keer wordt het "wiel als het ware opnieuw uitgevonden" door anderen. Ondersteunende afdelingen zoals ICT en in mindere mate Facilitaire zaken en Personeelszaken hebben hier nadeel van.

[4] *Zoals voor de Basisadministratie Adressen en Gebouwen (= BAG), Basis Registratie Personen (= BRP,) voor de Reisdocumenten en Rijbewijzen, en het Suwinet.*

Bijlage A Respondenten

Respondenten voor dit onderzoek:	Functie gemeente Buren
Tom ten Hoedt	(Functioneel) applicatiebeheerder BRP/Publiekszaken in de rol van sleutelfunctionaris in het realiseren van beveiligingsmaatregelen in een domein
Hendrik Schulte	Teamleider ICT in de rol van sleutelfunctionaris in het realiseren van beveiligingsmaatregelen en vertegenwoordiger van het lijnmanagement
Holger Peters	Informatie adviseur//architect in de rol van sleutelfunctionaris in het realiseren van beveiligingsmaatregelen
Jeffrey Pfeijffer	Netwerkbeheerder in de rol van sleutelfunctionaris in het realiseren van beveiligingsmaatregelen
Roland van der Starre	Gemeentesecretaris in de rol als voorzitter van het MT en vertegenwoordiger van het lijnmanagement
Ko van den Beemt	Concerncontroller in de rol van beveiligingscoördinator
Yvonne Gasau	Informatiebeveiligingsfunctionaris en security officer Suwinet als controlefunctionaris en in de rol van projectleider van het realiseren van beveiligingsmaatregelen
Hans van Dalem	(Functioneel) applicatiebeheerder Suwinet/Sociale Zaken in de rol van sleutelfunctionaris in het realiseren van beveiligingsmaatregelen in een domein
Henk de Ronde	Wethouder, demissionair in de rol van portefeuillehouder Informatieveiligheid

Bijlage B Geraadpleegde documenten

Nr	Omschrijving document	Aangeleverd
1	de netwerktopologie	Ja
2	architectuurdocument/visie document	Ja (Samen online)
3	informatie en/of automatiseringsplan	Nee. Wel aanzet: a. Toelichting op SOL/toekomstige richting informatiseringsplan b. Samen On Line, presentatie college c. Projectinitiatiedocument SOL d. Raadsbesluit 30-06-2015 dienstverlening gemeente Buren e. Presentatie raad 28-04-2015 bij raadsvoorstel 30 juni 2015
4	informatiebeveiligingsbeleid	Ja. Voortgangsbewaking op acties nav beleid ?
5	informatiebeveiligingsplan	Nee alleen een werkconcept.
6	taken bevoegdheidsverdeling, governance rondom informatiebeveiliging	Ja in opzet
7	Eventueel uitgevoerde Gap en impactanalyse BIG	Nee, niet uitgevoerd
8	Eventueel uitgevoerde baselinetoetsen inzake de 3 D's	Nee, niet uitgevoerd
9	statusrapportage implementatie BIG of beveiligingsplan	Nee is er nog niet
10	rapportage beveiligingsincidenten	Ja
11	Wijzigingsbeheer (procedure, notulen overleg, eventueel enkele Request for Change)	Ja in opzet
12	ICT CMDB (configuration management database)	Ja
13	Benoemingsbesluit beveiligingscoördinator 12a: betreffende teksten benoemingsbesluit beveiligingscoördinator 12b: collegebesluit informatiebeveiligingsbeleid 2014-2017 12c: collegebesluit Beveiligingsplan Suwinet 12d: Beveiligingsplan Suwinet	Geen formele benoeming met een functie omschrijving maar het toewijzen van de rol aan een bestaande functie/functionaris (controller, suwinet security office, twee functies)
14	Opmerkingen register accountant bij jaarrekeningcontrole over informatiebeveiliging	Ja
15	Eventuele opmerkingen in begroting en jaarrekening over informatiebeveiliging	Ja
16	Briefwisseling Inspectie SZW over recente Suwinet zelfevaluatie	Ja
17	Rapportage zelfevaluatie BRP oktober 2015 (Publiekszaken)	Ja
18	Rapportage zelfevaluatie PUN oktober 2015 (Publiekszaken)	Ja
19	Procedure meldplicht datalekken (persoonsgegevens)	Ja

Bijlage C Begrippen

Audit trail	Vastlegging van de complete keten van opeenvolgende wijzigingen op een object in een bepaalde periode.
Basis beveiligingsniveau	Het geheel van maatregelen van beveiliging dat wordt bereikt door het implementeren en toepassen van de normen zoals geformuleerd in de Baseline Informatiebeveiliging Gemeenten
Bedrijfsmiddel	Elk middel waarin of waarmee bedrijfsgegevens kunnen worden opgeslagen en/of verwerkt en waarmee toegang tot gebouwen, ruimten en ICT-voorzieningen kan worden verkregen: een bedrijfsproces, een gedefinieerde groep activiteiten, een gebouw, een apparaat, een ICT-voorziening of een gedefinieerde groep gegevens.
Beschikbaarheid	De waarborg dat vanuit hun functie geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen (informatiesystemen).
Beveiliging	Het brede begrip van informatiebeveiliging, d.w.z. inclusief fysieke beveiliging, Business Continuïty Management (BCM), ofwel beschikbaarheid van bedrijfsprocessen en persoonlijke veiligheid en integriteit.
Beveiligingsincident	Het manifest worden van een beveiligingsrisico (dreiging, oorzaak) als gevolg van een overtreding van beveiligingsregel, bijv. onbevoegde toegang tot ICT-voorzieningen.
Beveiligingsinstellingen	In ICT-voorzieningen kunnen in veel gevallen functionaliteiten die invloed hebben op beveiliging geactiveerd, gewijzigd of uitgeschakeld worden door het opgeven van parameterwaarden.
Clear Desk	Anders dan Clean Desk, waarbij het bureau helemaal leeg is, betekent Clear Desk dat er geen vertrouwelijke informatie op het bureau ligt.
Clean Screen	De medewerkers sluiten beeldschermen af zodat geen vertrouwelijke informatie geraadpleegd kan worden tijdens afwezigheid.
Controleerbaarheid	De mate waarin de werkelijkheid of representaties daarvan toetsbaar zijn, dat wil zeggen te vergelijken met andere 'werkelijkheden of representaties daarvan' zodat objectieve oordeelsvorming mogelijk wordt.
IB-functie	Een geheel van automatische informatiebeveiligingsverwerkingen die logisch met elkaar samenhangen.
ICT-voorzieningen	Applicaties en technische infrastructuur, of wel het geheel van ICT-voorzieningen.
In control statement	Binnen de gebruikelijke Planning en Control cyclus moet door B&W een in control statement worden afgegeven over het BIG. De in control verklaring moet inzicht geven aan welke BIG normen wordt voldaan en voor welke BIG normen een explain is gedefinieerd.
Informatiebeveiliging	Het proces van vaststellen van de vereiste betrouwbaarheid van informatieverwerking in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.
Informatiesysteem	Een samenhangend geheel van gegevensverzamelingen en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.

Integrale beveiliging	Integrale beveiliging is de beveiliging van vastgestelde te beschermen belangen (TBB) door op basis van risicomanagement en een kosten/batenanalyse een samenhangend stelsel van beveiligingsmaatregelen te selecteren en te implementeren. Het besturingsmodel voor integrale beveiliging sluit aan bij de besturingsuitgangspunten binnen de gemeenten: het lijnmanagement is integraal verantwoordelijk en dus ook voor de beveiliging van de TBB.
Integriteit	Het waarborgen van de juistheid en volledigheid en tijdigheid van informatie en de verwerking ervan. Als de tijdigheid van gegevens bepaald wordt door omstandigheden buiten het systeem, kan deze vanzelfsprekend niet als integriteitseis voor het systeem gesteld worden.
Logging	Vastlegging van systeemhandelingen.
Malware	Software met ongewenste functies, zoals virussen en trojans.
Onvertrouwd	Geen zekerheid over het beveiligingsniveau of zekerheid over het lager dan vereiste beveiligingsniveau.
Onweerlegbaarheid	Het niet kunnen ontkennen iets te hebben gedaan (bijvoorbeeld een bericht te hebben ontvangen dan wel te hebben verstuurd).
Technische infrastructuur	Het geheel van ICT-voorzieningen voor generiek gebruik, zoals servers, firewalls, netwerkapparatuur, besturingssystemen voor netwerken en servers, database management systemen en beheer- en beveiligingstools, inclusief bijbehorende systeembestanden.
Two-factor authenticatie	Two-factor authenticatie vereist het gebruik van twee van de drie volgende authenticatiemethoden: • Iets dat de gebruiker weet (b.v. password, PIN); • Iets dat de gebruiker heeft (b.v. toegangspas, sleutel); en • Iets dat de gebruiker is (b.v. biometrische eigenschap zoals een vingerafdruk).
Vertrouwd	In overeenstemming met een door een bevoegde autoriteit vastgesteld beveiligingsniveau. Bijvoorbeeld vertrouwde zones of vertrouwde netwerken zoals in 10.6.1.2 en 10.6.1.3.
Vertrouwelijkheid	Het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd.
Vertrouwelijke informatie	Informatie die niet algemeen bekend mag worden (bron: van Dale). In het kader van de BIG worden maatregelen beschreven die voldoen voor de behandeling van gerubriceerde informatie tot en met vertrouwelijke en persoonsvertrouwelijke informatie, zoals bedoeld in Artikel 16 van de WBP
Zone	De logische verzameling van ICT-voorzieningen met hetzelfde beveiligingsniveau, die via beveiligde koppelvlakken gegevens kunnen uitwisselen

gemeente Buren

GEMEENTE BUREN	
reg.nr.	Z16-44350 IN 1
d.d.	- 1 SEP 2016 1662026
afd.	Griffie
kopie	

Rekenkamercommissie Buren
De Wetering 1
4021 VZ MAURIK

uw brief van:	8 augustus 2016	Maurik, 31 augustus 2016	
uw kenmerk:			
ons kenmerk:	UIT/1654502/Z16-43250	verzonden:	31 AUG. 2016
behandeld door:	Y. Gasau		
bijlage(n):			
onderwerp:	onderzoek Rekenkamercommissie Quick scan Informatieveiligheid: bestuurlijke reactie		

Geachte leden van de Rekenkamercommissie Buren,

In het RKC rapport Quickscan informatieveiligheid doet de commissie 3 aanbevelingen:

AANBEVELINGEN

Spreek met het college van Burgemeester en Wethouders af:

1. om in 2016 de informatieveiligheid bestuurlijk en organisatorisch te borgen en integraal in te richten overeenkomstig het normenkader zoals vermeld in de Baseline Informatiebeveiliging (BIG).
2. dat in de documenten van de Planning en Controlcyclus in het vervolg de gemeenteraad (smart) wordt geïnformeerd over de informatieveiligheid met de BIG als normenkader.
3. de risico's goed in beeld te brengen en in een gezamenlijke prioriteitenafweging de noodzakelijke verbeteringen door te voeren.

Wij hebben het rapport en de bevindingen van de commissie, en de reacties van de ambtelijke medewerkers, met belangstelling tot ons genomen. We zijn erg blij met de conclusie van de Rekenkamercommissie dat de gemeente in grote lijnen haar zaken goed op orde heeft. Hieronder gaan we graag in op de aanbevelingen van de Commissie, die wij ervaren als een positieve impuls voor onze verdere ontwikkeling.

1. Zoals u in de Raadsinformatiebrief (RI/15/02124) heeft gelezen hebben we bewust gekozen voor een andere aanpak voor informatiebeveiliging, die is gebaseerd op de het model van de IBD (Landelijke Informatie Beveiligingsdienst), dat weer is ingericht naar de ISO27001-norm. In de praktijk van de laatste jaren blijkt dat we daarmee goed presteren, met name op de technische beveiliging. Echter we zien ook dat, gelet

op landelijke ontwikkelingen, de aansluiting op de BIG een goede vervolgontwikkeling is.

Het normenkader van de BIG biedt meer structuur en bewustwording als toegevoegde waarde. Dit is ook precies de reden dat het College op termijn aan dit normenkader wil voldoen. Dit sluit ook aan op de aanbevelingen.

De eerste stap hierin is het maken van een analyse van de stand van zaken: waar staan we nu ten opzichte van de BIG, welke zaken willen we met prioriteit gaan oppakken en welke verbeteringen gaan we met voorrang uitvoeren. Dan weten wij ook precies welke termijn er nodig is voor de invoering van de BIG. Het College stelt voor om 2016 en 2017 te gebruiken voor de inventarisatie en verbeterstappen.

2. Het College zal in de bedrijfsvoeringsparagraaf van de Planning en Controlcyclus een korte stand van zaken over de informatieveiligheid opnemen.

3. In aansluiting op uw aanbeveling zullen wij, zoals bij punt 1 beschreven, de stand van zaken analyseren en aan de hand daarvan de noodzakelijke verbeteringen prioriteren.

Met vriendelijke groet,

Burgemeester en wethouders van Buren,

de secretaris, de burgemeester,

Mr. I.P.C. van Wamel-Geene J.A. de Boer MSc

REKENKAMERCOMMISSIE BUREN

Aan de Raad van de gemeente Buren

Maurik, 19 september 2016

Betreft: Nawoord Rekenkamercommissie bij het rapport "Quick scan Informatieveiligheid"

Geachte leden van de Raad,

De Rekenkamercommissie (RKC) heeft met belangstelling kennis genomen van de reactie van het college van Burgemeester en Wethouders van 31 augustus 2016, kenmerk UIT/1654502/Z16-43250.

Wij stellen met tevredenheid vast dat het college van Burgemeester en Wethouders de verbetervoorstellen omarmt. Het college gaat werk maken van de verbetervoorstellen en u wordt in het vervolg in de paragraaf Bedrijfsvoering van de documenten in de P.&C.-cyclus -Smart- geïnformeerd over de vorderingen. Wij vinden dit een goede ontwikkeling. Te meer omdat informatieveiligheid onmiskenbaar een heel belangrijke voorwaarde is voor een goede bedrijfsvoering.

Wij vertrouwen erop dat wij u met dit nawoord voldoende hebben geïnformeerd.

Hoogachtend,

De Rekenkamercommissie Buren,
H.J.F.L. Meeuwsen MBA AC, voorzitter
drs. P.J.J. Bremmer
R.F.J. Spelier MSc
W. van Beem, ambtelijk secretaris