voorstel

Zwolle

Overdracht College-Raad

Datum 20 april 2017

onderwerp	Beantwoording Art. 45 vragen CDA Veiligheidsrisico's en informatiebeveiliging gemeente Zwolle en jaarverslag Informatiebeveiliging
portefeuillehouder	Jan Brink
informant	Hol, Marrie (2681)
afdeling	Advies

Voorgesteld besluit raad

kennis te nemen van:

1. De beantwoording van de Art. 45 vragen van het CDA inzake de veiligheidsrisico's en informatiebeveiliging gemeente Zwolle.
2. Het jaarverslag Informatiebeveiliging 2016
3. Het verslag van de VNG visitatiecommissie Informatieveiligheid

voorstel

Zwolle

Informatienota voor de raad

Datum 6 april 2017

Onderwerp	Artikel 45-vragen CDA: veiligheidsrisico's en informatiebeveiliging gemeente Zwolle
Versienummer	

Portefeuillehouder J.E. Brink

Informant M. Hol
Afdeling / AF
Telefoon 038 498 2681
Email M.Hol@zwolle.nl

Bijlagen

- Art. 45 vragen CDA veiligheidsrisico's en informatiebeveiliging gemeente Zwolle.
- Jaarverslag Informatiebeveiliging 2016.
- Verslag VNG visitatiecommissie Informatieveiligheid.

Wij stellen u voor kennis te nemen van:

1. De beantwoording van de Art. 45 vragen van het CDA inzake de veiligheidsrisico's en informatiebeveiliging gemeente Zwolle.
2. Het jaarverslag Informatiebeveiliging 2016
3. Het verslag van de VNG visitatiecommissie Informatieveiligheid

Datum 6 april 2017

Toelichting op het voorstel

Inleiding
Artikel 45-vragen CDA: veiligheidsrisico's en informatiebeveiliging gemeente Zwolle. In deze informatienota worden de door het CDA gestelde vragen beantwoord. Ter informatie worden het jaarverslag Informatiebeveiliging 2016 en het verslag van de VNG visitatiecommissie Informatiebeveiliging als bijlagen meegezonden.

Kernboodschap

1. Kent u het onderzoek van de Rekenkamer Rotterdam, de brief van Paul Hofstra (directeur van de Rekenkamer Rotterdam) aan de Rotterdamse gemeenteraad, en/of de rapportages hierover in Nieuwsuur en het NOS-journaal van zondag 2 april 2017?

   Ja, we kennen het onderzoek voor zover hierover is bericht in de media. We kennen het nog niet tot in detail, omdat het betreffende rapport van de Rekenkamer Rotterdam pas recent is vrijgegeven. We hebben kennisgenomen van berichtgeving in het NOS-journaal en Nieuwsuur en van de brief uit het Raadsinformatiesysteem van de gemeente Rotterdam, waarin de Rekenkamer Rotterdam aan de Rotterdamse gemeenteraad uit de doeken doet dat er discussie is over geheimhouding van het onderzoeksrapport.

2. Zijn de veiligheidsrisico's die in het rapport van de Rekenkamer Rotterdam en/of de rapportage van de NOS naar voren komen (en voor zover al openbaar) op Zwolle van toepassing?
   a. Zo ja, welke?
   b. Zo nee, waaruit blijkt dit?

   In de bovengenoemde berichtgeving over de gemeente Rotterdam is summier ingegaan op de inhoud van het document. Uit onze waarneming is gebleken dat het ging om toegang tot gebouwen en toegang tot systemen. Als er toegang was tot gemeentelijke kantoren, dan was daar in principe toegang mogelijk tot gemeentelijke systemen. Wij kunnen uit de berichtgeving niet opmaken tot welke gemeentelijke panden de onderzoekers toegang hadden en welke systemen aldaar werden aangetroffen. Dit maakt het voor ons erg lastig om te bepalen of deze situatie ook voor Zwolle geldt.

   Nu het definitieve rapport recentelijk is vrijgegeven kunnen we beter analyseren welke risico's de gemeente Rotterdam loopt en of dezelfde risico's ook voor de gemeente Zwolle van toepassing zijn. Als we daartoe aanleiding zien, zullen we hierop actie ondernemen.

   Over toegang tot gemeentelijke gebouwen en systemen kunnen wij het volgende meedelen.
   - Het informatiebeveiligingsbeleid van de gemeente Zwolle vereist dat er in gemeentelijke panden en op IT-systemen toegangsbeveiliging wordt uitgevoerd.
   - Toegangsbeveiliging uit zich in toegang tot gebouwen via individuele passen of codesloten op deuren, conform zonering van de panden (openbare zone, kantoorzone, extra beveiligde zone). Medewerkers hebben alleen toegang tot algemene kantoorruimten en in specifieke gevallen tot ruimten die voor de uitoefening van hun taak nodig zijn.

- Insluiping kan alleen voorkomen worden door alle voordeuren te voorzien van zware beveiligingsmiddelen. Dit staat echter haaks op de open houding waarmee de gemeente Zwolle in de samenleving wil staan.
- In de openbare ruimten van het Stadskantoor en het Stadhuis zijn vergaderkamers, waar gebruik gemaakt kan worden van gemeentelijke IT-voorzieningen. Omdat het openbare ruimten betreft, is hier alleen toegang tot het gemeentelijke netwerk mogelijk door gebruik te maken van een extra inlogstap: naast gebruikersnaam en wachtwoord dient hier ook een tokencode ingevoerd te worden. Zijn deze inlogmiddelen niet beschikbaar, dan is alleen toegang te verkrijgen tot stand alone computers, waarvan gebruikers weten dat deze openbaar toegankelijk zijn. Hierom wordt op deze apparaten geen vertrouwelijke informatie opgeslagen.
- Binnen de gemeentelijke panden zijn werkplekken aanwezig met toegang tot zeer veel gegevens, afhankelijk van de aan een medewerker toegekende rechten. Systemen zijn toegankelijk met een inlognaam en bijbehorend wachtwoord. Inloggegevens worden individueel verstrekt aan medewerkers, waarbij duidelijk wordt gemaakt wat het belang is van deze 'digitale sleutel' tot gemeentelijke informatie.

Uiteraard staat of valt beleid bij de uitvoering ervan. Medewerkers worden geïnformeerd over de geldende regels, en gevraagd mensen aan te spreken op gedrag dat hiervan afwijkt. Op verschillende wijzen wordt deze bewustwording gevoed. Op intranet verschijnen regelmatig berichten over diverse aspecten van het toegangs- en informatiebeveiligingsbeleid. Ook worden medewerkers opgeroepen om incidenten zo snel mogelijk te melden, zodat daarop actie ondernomen kan worden. Daarnaast zijn er workshops gestart rond dit thema en is gestart met specifieke bewustwordingscampagnes.

Op het gebruik van een aantal systemen wordt de gemeente Zwolle jaarlijks geaudit, denk aan Suwinet en DigiD. Onderdeel van deze audits is het laten uitvoeren van zogenaamde pentesten (hacktesten of penetratietesten) om aan te tonen dat deze kroonjuwelen niet zomaar door iedereen te benaderen zijn.

3. <u>Wat is het beleid van de gemeente Zwolle omtrent de digitale toegang tot vertrouwelijke informatie?</u>

Het Informatiebeveiligingsbeleid is opgesteld op basis van de Baseline Informatiebeveiliging Gemeenten. Uitgangspunt is dat medewerkers toegang hebben tot informatie die voor de uitoefening van hun werkzaamheden nodig is. Hiermee geven we tevens uitvoering aan de Wet bescherming persoonsgegevens, die vereist dat gegevens alleen beschikbaar zijn als er sprak is van 'doelbinding'.

Inmiddels beschikt de gemeente Zwolle over een systeem waarin wordt bijgehouden (conform PDCA-cyclus) aan welke voorwaarden van de BIG wordt voldaan. Hiermee kunnen we continu monitoren wat de stand van zaken is, welke verbeteracties zijn ingezet en wat daarvan de status is.

4. In hoeverre wordt er binnen de informatiesystemen gebruik gemaakt van automatisch gegenereerde inloggegevens?

   De gemeente Zwolle maakt geen gebruik van automatisch gegenereerde inloggegevens. Bij in dienst treden van een nieuwe werknemer wordt het eerste wachtwoord verstrekt door de Servicedesk. Dit betreft de inloggegevens van een nieuw account, zonder specifieke toegangsrechten.

5. Op welke manier worden deze inloggegevens aan de gebruikers verstrekt?

   Op de eerste werkdag wordt het wachtwoord van het algemene inlogaccount mondeling verstrekt. Vervolgens krijgt de nieuwe medewerker eenmalig toegang tot het netwerk, waarbij het verplicht is direct het wachtwoord aan te passen om permanente toegang te verkrijgen. Met deze gegevens kan de medewerker - op aandragen van het afdelingshoofd - toegangsrechten verkrijgen tot specifieke applicaties.

6. Wat is de houdbaarheid van verstrekte inloggegevens? Na welke tijd komen de inloggegevens te vervallen?

   De algemene toegang tot IT-systemen kent een wachtwoordduur van 60 dagen. Ruim een week voordat deze periode afloopt krijgt een gebruiker bericht het wachtwoord te wijzigen. Doet de gebruiker dit tijdig, dan is er niets aan de hand. Stelt een gebruiker dit wijzigen uit, dan wordt het account geblokkeerd door het systeem. Bij de Servicedesk kan in dat geval gevraagd worden het systeem te 'unlocken'.

   Naast het gemeentelijke IT-systeem wordt er meer en meer gebruik gemaakt van de cloud. Ook voor deze applicaties gelden dezelfde wachtwoordeisen, omdat alle door de gemeente Zwolle gebruikte systemen vallen onder de Baseline Informatiebeveiliging Gemeenten.

7. Wordt er gecontroleerd of de inloggegevens periodiek door de gebruiker gewijzigd worden?
   a. Indien ja, welke stappen worden er genomen als blijkt dat de inloggegevens voor een bepaalde tijd niet door de gebruiker gewijzigd zijn?
   b Indien nee, waarom niet?

   Zoals bij vraag 6 aangegeven, wordt het wijzigen van inloggegevens afgedwongen. Wel wordt periodiek gecontroleerd of medewerkers die toegang hebben tot specifieke systemen (onze kroonjuwelen) daadwerkelijk gebruik maken van hun toegangsrechten. Wanneer blijkt dat dit niet het geval is, wordt voor deze medewerkers de toegang tot het systeem ingetrokken.

8. Hoe frequent en op welke manier onderzoekt de gemeente Zwolle veiligheidsrisico's omtrent haar informatiesystemen?

- Jaarlijks laat het SSC-ONS pentesten (hacktesten of penetratietesten) uitvoeren op onze informatiesystemen.
- Jaarlijks voert een externe IT-auditor controles uit op onze informatiesystemen in opdracht van onze huisaccountant.
- Jaarlijks worden door het Rijk verplichte externe audits uitgevoerd op Suwinet, DigiD.
- Jaarlijks worden controles uitgevoerd door vakspecialisten en medewerkers van Interne Controle op het gebruik van Basisregistraties (zelfassessments).
- Ieder kwartaal controleren medewerkers Interne Controle op het gebruik van toegangsrechten.
- Dagelijkse monitoring op ongeautoriseerde toegang van buitenaf tot onze compliance gerelateerde IT-systemen.
- De gemeente Zwolle (en ook het SSC-ONS) wordt doorlopend geïnformeerd door de Informatiebeveiligingsdienst van de VNG (IBD) over mogelijke veiligheidsrisico's en neemt op basis daarvan passende maatregelen.

In 2017 worden, naast de bovengenoemde testen, ook interne hacktesten (zogenaamde white hacks) en social engineering testen (fysiek pogen binnen te dringen) uitgevoerd. Deze testen leveren veel inzicht in de wijze waarop binnen de gemeente Zwolle omgegaan wordt met informatieveiligheid en privacy. Op basis van deze inzichten kunnen we de implementatie van ons Informatiebeveiligingsbeleid aanscherpen of zonodig bijsturen. Naar verwachting zullen soortgelijke testen in de nabije toekomst verplicht worden vanwege strengere wetgeving rondom privacy en informatiebeveiliging.

Eén van de speerpunten van de onlangs vastgestelde ‘Informatiestrategie gemeente Zwolle 2017-2020’ is het beter benuten van ethical hackers (zogenaamde witte of ethische hackers) door de gemeente Zwolle.

9. Op welke manier monitort de gemeente Zwolle oneigenlijke toegang van vertrouwelijke informatie?

Indien vanuit de in vraag 8 genoemde controles, of op een andere wijze, een incident wordt gemeld, dan wordt dit onderzocht of er sprake is va oneigenlijke toegang. Zo nodig wordt hierop actie ondernomen.

Consequenties
Niet van toepassing.

Communicatie
Niet van toepassing.

Vervolg
Niet van toepassing.

Openbaarheid
Openbaar

Datum 6 april 2017

Burgemeester en Wethouders van Zwolle,

de heer drs. H.J. Meijer, burgemeester

mevrouw mr. I. Geveke, secretaris