Besluit raad

Nummer
C.9
Portefeuillehouder
A. van Dam

Contact en vragen via
Technischevragen@hollandskroon.nl

Datum raadsvergadering	Datum B&W-besluit
14 juli 2022	14 juni 2022

Onderwerp
Jaarverslag informatiebeveiliging 2021

Kern van het voorstel
De gemeenteraad wordt jaarlijks geïnformeerd over de kwaliteit van de informatiebeveiliging. Uit het jaarverslag blijkt dat de organisatie in 2021 adequate beheersmaatregelen heeft getroffen volgens de ENSIA-methodiek en de baseline informatiebeveiliging overheid (BIO).

Voorgesteld besluit
Het college van burgemeester en wethouders stelt de gemeenteraad voor: het Jaarverslag Informatiebeveiliging 2021 vast te stellen.

Wettelijke grondslag
Resolutie Informatieveiligheid, randvoorwaarde voor de professionele gemeente, BALV 29 oktober 2013 van de Vereniging van Nederlandse Gemeenten.

De gemeenteraad besluit: conform
Vastgesteld in de openbare raadsvergadering van 14 juli 2022. Griffier Voorzitter

Sjaak Vriend HK
15-07-2022

A. van Dam
15-07-2022

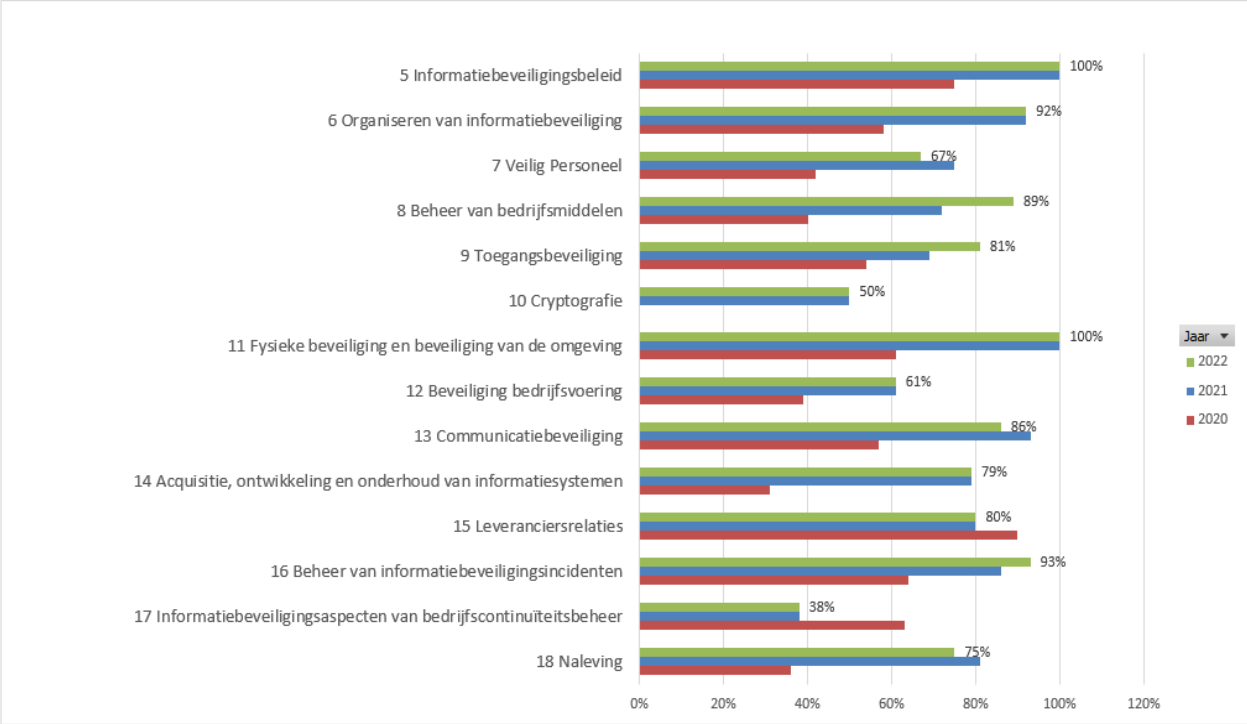
Aanleiding
De jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA) toetst de kwaliteit van de informatiebeveiliging. In deze audit worden afzonderlijke wettelijke audits en zelfevaluaties op het gebied van informatiebeveiliging gebundeld. Een externe IT-auditor controleert en beoordeelt de betrouwbaarheid van de rapportage van ons college aan uw raad. De verklaring die de auditor afgeeft is te vergelijken met de controleverklaring over de jaarrekening. Deze controle is op 14 april van dit jaar positief beoordeeld op alle normen. Informatiebeveiliging moet de gemeentelijke organisatie beschermen tegen onder meer cybercrime (hacken) en datalekken. De gemeente moet kunnen aantonen dat voldoende maatregelen getroffen zijn om de beveiliging adequaat te borgen op basis van een risicoanalyse en een kosten-batenanalyse.

Beoogd bestuurlijk/maatschappelijk doel/effect
Met het jaarverslag informatiebeveiliging legt het college verantwoording af over de kwaliteit van de informatiebeveiliging. Op hoofdlijnen krijgt de gemeenteraad inzicht in de kwaliteit van de informatiebeveiliging en de daarbij behorende beheersmaatregelen.

Motivering per voorgesteld besluit
De organisatie heeft in 2021 mooie stappen gemaakt om de terugval in te halen die is ontstaan na de ingang van de BIO. De BIO heeft onze informatiebeveiligingsorganisatie positief beïnvloed. Er is al geprioriteerd en gepland op de onderdelen waar nog verbetering nodig is. Deze verbeteringen beginnen zoals in de jaren hiervoor is meegedeeld met vastgesteld beleid, vastgelegde procesbeschrijvingen, richtlijnen en werkinstructies en proces- en gegevenseigenaarschap. Verder zijn de onderwerpen bedrijfscontinuïteit en het nemen van aanvullende crypto grafische beheersmaatregelen belangrijk om de digitale weerbaarheid te vergroten. Met dat laatste wordt voorkomen dat ongeoorloofd gebruik kan worden gemaakt van onze koppelingen, verbindingen en applicaties.

Over de werking van onze informatiebeveiligingsorganisatie wordt vanaf 2018 gerapporteerd aan directie en college wanneer dit nodig is. Bijvoorbeeld in het geval van een dreiging of wanneer geconstateerd wordt dat de informatieveiligheid onvoldoende geborgd is.

Hierboven is een samenvatting opgenomen van de uitkomsten van de analyse op basis van de Baseline Informatiebeveiliging overheid (BIO). De BIO is sinds 2020 van kracht en is het basisnormenkader voor informatieveiligheid voor de hele overheid. De samenvatting geeft een meting van de BIO weer, zoals deze is uitgevoerd aan het begin van 2020 en 2021. Daarnaast wordt er in hetzelfde overzicht ook een beeld geschetst van de meting in 2022. Wat op zal vallen is dat onder hoofdstukken 7, 13, en 18 er slechter wordt gescoord ten opzichte van het jaar daarvoor. Dit heeft te maken met de verandering die heeft plaatsgevonden in de kernapplicatie landschap en het ontbreken van een aantal functionaliteiten. Naar verwachting zal deze score consolideren zodra deze functionaliteiten beschikbaar worden gemaakt later dit jaar.



Onze beveiliging is verbeterd. Een 100% beveiliging kan niet worden gegarandeerd. Organisatorische en technische maatregelen zijn niet waterdicht en hebben hun prijs. Op basis van een risicoanalyse is een noodzakelijk pakket maatregelen en middelen gerealiseerd.

Risico's van datalekken en hacken blijven altijd aanwezig. Wij proberen deze risico's tot een minimum te beperken. Gedrag, veiligheidsbewustzijn en risicobewustzijn van medewerkers hebben grote invloed op de informatieveiligheid. In de praktijk blijkt dat veel veiligheidsincidenten worden veroorzaakt door de menselijke factor. Hier zal dan ook meer op geïnvesteerd moeten worden. Om hier stappen in te maken heeft de directie een voorstel goedgekeurd om het bewustzijn van medewerkers verder te vergroten.

De gemeente is niet geconfronteerd met sancties van de Autoriteit Persoonsgegevens (boetes), Logius (afsluiten website) en het BKWI (afsluiten Suwinet).

Kanttekeningen en risico's (incl. argumenten)
n.v.t.

Alternatieven (incl. argumenten)
n.v.t

Financiële gevolgen	
Kosten/opbrengsten	€ 13.750
Dekking binnen begroting	Programma: Dienstverlening Cluster: Bestuur
Geen dekking binnen begroting	Dekkingsvoorstel:
Fiscale gevolgen	
Toelichting: De kosten hebben betrekking op de externe IT-audit t.b.v. de ENSIA	

Communicatie
Na besluitvorming in de raad wordt het jaarverslag toegestuurd naar het Ministerie van BZK.

Bijlagen
Jaarverslag informatiebeveiliging 2021

Digitally signed by Zynyo B.V.
Date: 2022.07.15 11:58:00 CEST
Document ID:
8f7a738e-718e-45f9-8de8-b9466a1dbe8a