Voorstel raad

Nummer
C.6
Portefeuillehouder
A. van Dam

Contact en vragen via
Technischevragen@hollandskroon.nl

Datum raadsvergadering	Datum B&W-besluit
25 mei 2023	4 april 2023

Onderwerp
Jaarverslag informatiebeveiliging 2022

Kern van het voorstel
De gemeenteraad wordt jaarlijks geïnformeerd over de kwaliteit van de informatiebeveiliging. Uit het jaarverslag blijkt dat de organisatie in 2022 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 2022 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:
Vastgesteld in de openbare raadsvergadering van 25 mei 2023 Griffier Voorzitter

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. 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 interne beheersmaatregelen. Deze beheersmaatregelen zijn overigens van essentieel belang voor het beschermen van de gegevens van onze inwoners, bedrijven en instellingen.

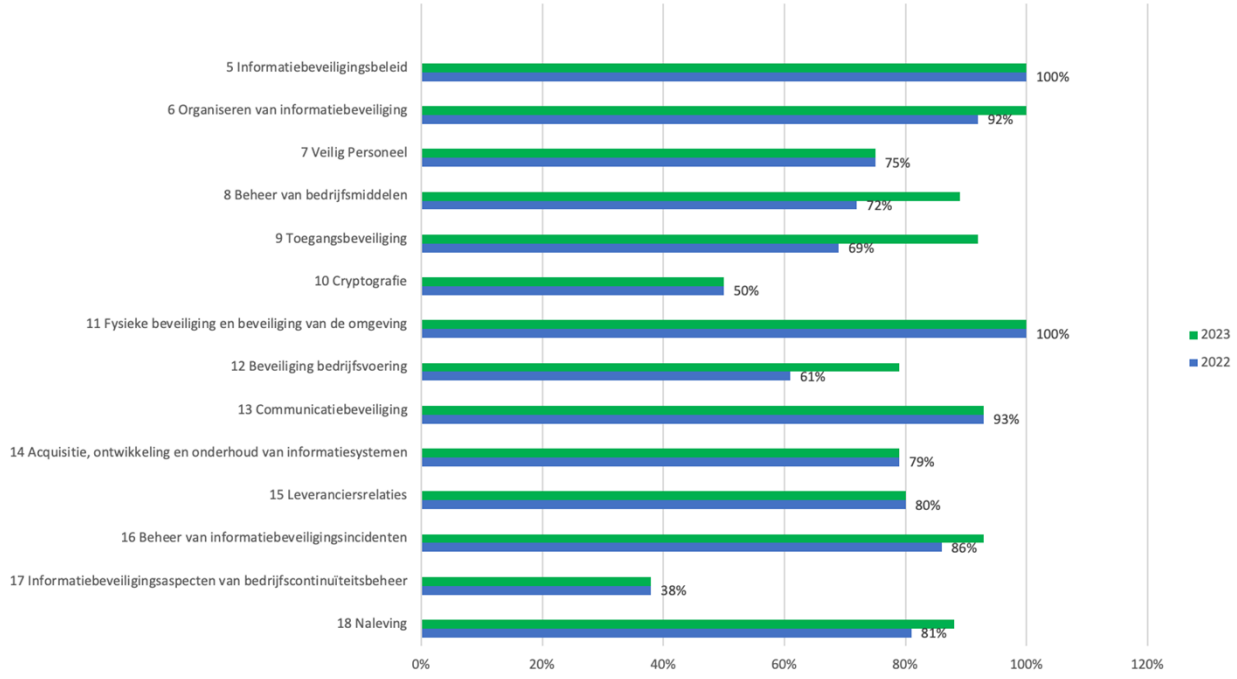
Motivering per voorgesteld besluit
De organisatie heeft qua meting ten opzichte van het jaar daarvoor stappen voorwaarts gezet. Dat heeft te maken met een aantal doorgevoerde maatregelen vanuit het BIO normenkader. Op het moment van schrijven ligt er een set nieuw te prioriteren maatregelen die uitgevoerd moet worden in 2023. Er is aanvullend vooruitgang geboekt in het vormgeven van vastgesteld beleid, processen (procesbeschrijvingen, vastgestelde richtlijnen en werkinstructies) en eigenaarschap. Daarnaast zijn er stappen gezet in het kader van monitoring, detectie en logging van het internet en dataverkeer. Dit in de vorm van het zogeheten SIEM[1]

[1] Security Information and Event Management (SIEM) is een softwarepakket die technische informatie uit verschillende bronnen opslaat, samenvoegt en daar verbanden in legt.

en SOC[2]. Dit is van groot belang om verdachte activiteiten en gedrag op de infrastructuur inzichtelijk te krijgen. Hierop kunnen dan weer de nodige maatregelen toegepast worden ter voorkoming hiervan.

Het onderwerp bedrijfscontinuïteit en het verder professionaliseren van onze ICT-organisatie is zeer belangrijk om de digitale weerbaarheid van de organisatie te vergroten. Het blijft daarnaast van groot belang om de lage bezetting van onze ICT-organisatie te compenseren door de dagelijkse beheer activiteiten te documenteren. Dat is nodig in geval van uitval en/of vervanging. Maar ook om een goed beeld te krijgen bij alle ICT-risico's die wij lopen en de ICT-kwaliteit die moet worden behouden. De bedoeling is om deze zaken op te pakken bij de uitwerking van een roadmap om onze ICT-organisatie verder te professionaliseren de komende jaren.

Hieronder 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 gehele overheid. De samenvatting geeft een meting van de BIO weer, zoals deze is uitgevoerd aan het begin van 2022 en 2023.



Deze metingen zijn een momentopname en geven alleen weer hoe de gemeente er op het moment van

[2] Een Security Operations Center (SOC) is een gecentraliseerde eenheid die zich bezighoudt met het bewaken beoordelen en verdedigen van systemen a.d.v. de informatie die onttrokken wordt uit het SIEM.

meten voor stond. Op de hoofdstukken 6, 8, 9, 12, 16 en 18 is er een stijging waargenomen. Dit heeft te maken met:

1. de doorontwikkeling van de governance
2. een betere organisatie en overzicht op onze bedrijfsmiddelen
3. meer control op onze toegangsbeveiliging binnen het applicatielandschap
4. een hogere mate van kwaliteit van het beveiligen en loggen van onze IT-processen
5. een beter gestroomlijnde keten van beveiligingsmeldingenbeheer

Al met al kan er gesteld worden dat onze beveiliging is verbeterd. Een 100% beveiliging kan niet worden gegarandeerd. Organisatorische en technische maatregelen zijn niet waterdicht. 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. We blijven dan ook investeren in veiligheids- en risicobewustzijn van de medewerkers.

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	€ 8.250
Dekking binnen begroting	Programma: Bedrijfsvoering 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 2022