Voorstel raad

Nummer
C.7
Portefeuillehouder
A. van Dam

Contact en vragen via
Technischevragen@hollandskroon.nl

Datum raadsvergadering	Datum B&W-besluit
11 juli 2024	28 mei 2024

Onderwerp
Jaarverslag informatiebeveiliging 2023

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

Aanleiding
De jaarlijkse eenduidige normatiek single information audit (ENSIA) toetst de kwaliteit van de informatiebeveiliging van de gemeente. 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 beheersmaatregelen.

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 moeten worden. 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] 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.

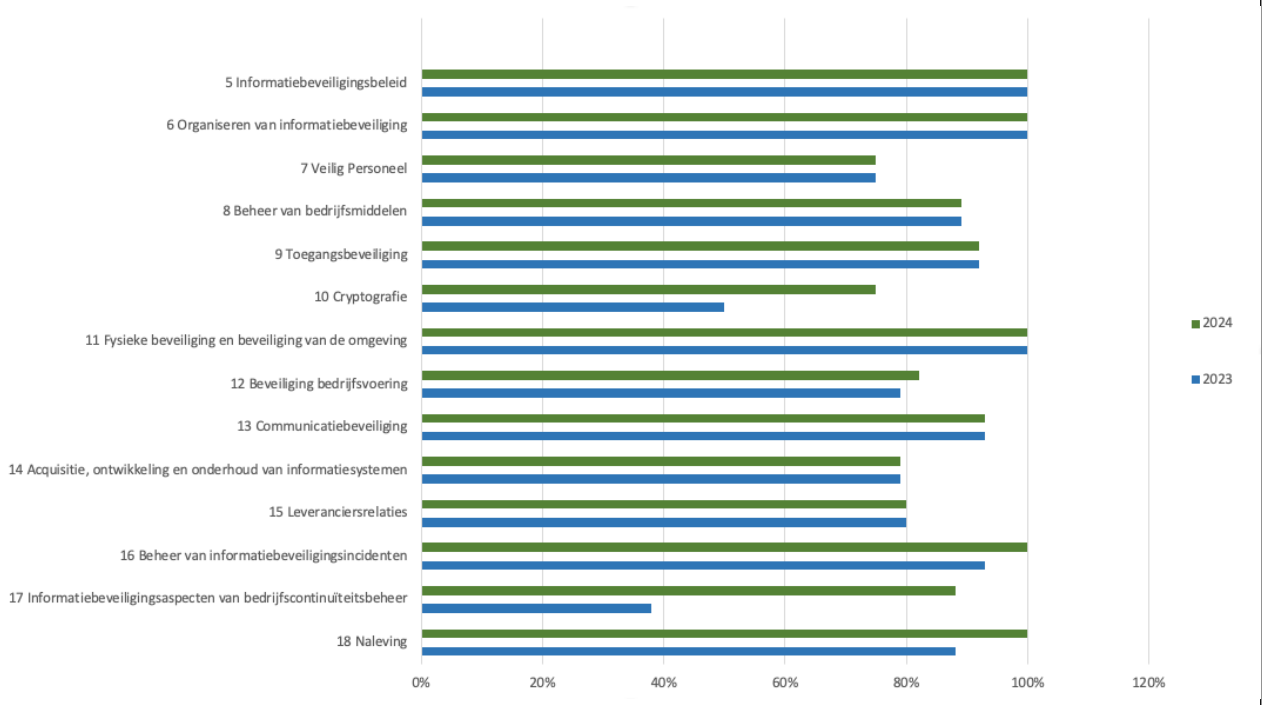
Het onderwerp bedrijfscontinuïteit, en het verder professionaliseren van onze ICT-organisatie is van groot belang om onze digitale weerbaarheid te vergroten. Het blijft daarnaast van groot belang om de lage bezetting van onze ICT-organisatie te compenseren door de dagelijkse beheer activiteiten te documenteren en te standaardiseren. Dat is nodig in geval van uitval, 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.

Voor het onderwerp bedrijfscontinuïteit is in 2023 gestart met het opstellen van een strategisch beleidsdocument dat richting geeft voor het verder vormgeven en borgen van de continuïteit van de gemeentelijke processen. Dit beleid bevat algemene kaders, uitgangspunten en managementafspraken tussen het college van B&W en de directie. Dit beleid wordt in 2024 aan het college aangeboden ter vaststelling.

Als gemeente maken wij gebruik van een diversiteit aan (informatie)systemen die effectief beheerd moeten worden. Dan gaat het zowel om technisch als functioneel beheer. Het doel wat wij willen bereiken met dit beheer is een veilige, integere en beschikbare IT infrastructuur. Om dit doel te bereiken is het maken van afspraken voor de uitvoering van de dagelijkse beheeractiviteiten nodig. In 2023 is hiervoor door de directie intern functioneel applicatiebeheer beleid vastgesteld. Dit beleid biedt helderheid in het verkrijgen van alle noodzakelijke beheertaken op het gebied van technisch en functioneel beheer op onze systemen, ook op het gebied van cyberveiligheid.
Verder is controle en toezicht hierop een speerpunt. Dit is namelijk van belang vanwege het jaarlijks afleggen van de verticale en horizontale verantwoording. Die controle en toezicht draagt bij aan de verdere groei van professionalisering die Hollands Kroon ambieert.

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 2023 en 2024.

[1] Security Information and Event Management (SIEM) is een softwarepakket die technische informatie uit verschillende bronnen opslaat, samenvoegt en daar verbanden in legt.
[2] Een Security Operations Center (SOC) is een gecentraliseerde eenheid die zich bezighoudt met het bewaken beoordelen en verdedigen van systemen a.d.h.v. de informatie die onttrokken wordt uit het SIEM.



Deze meting is een momentopname en geeft weer hoe wij er op het moment voorstaan.
Op de hoofdstukken 10, 12, 16, 17 en 18 is er een stijging waargenomen. Dit heeft te maken met het verder doorontwikkelen van governance, een betere organisatie van processen en procedures en overzicht op onze bedrijfsmiddelen. Wij zijn verder meer in control op onze cryptografische beheerprocessen, en er is een hogere mate van kwaliteit behaald binnen het incidentenbeheer. De grootste focus lag op het organiseren van de bedrijfscontinuïteit van onze IT organisatie. Deze is van 38% naar 88% geklommen. Hierop zijn de meeste punten gescoord.

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 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. We blijven dan ook investeren in veiligheids- en risicobewustzijn van de medewerkers.

De gemeente is verder 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	€ 10.350
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 2023