Voorstel raad

Nummer

Contact en vragen via

Technischevragen@hollandskroon.nl

Portefeuillehouder

A. van Dam

Datum raadsvergadering	Datum B&W-besluit
25 november 2021	19 oktober 2021

Onderwerp
Jaarverslag informatiebeveiliging 2020

Kern van het voorstel
De gemeenteraad wordt jaarlijks geïnformeerd over de kwaliteit van de informatiebeveiliging. Uit het jaarverslag blijkt dat de organisatie in 2020 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 2020 vast te stellen.

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

Voorstel raad

De raad besluit:
Vastgesteld in de openbare raadsvergadering van 25 november 2021, Griffier Voorzitter

Aanleiding
Op grond van de Eenduidige Normatiek Single Information Audit (ENSIA) wordt jaarlijks de kwaliteit van de informatiebeveiliging getoetst. 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 IT-auditor afgeeft is te vergelijken met de controleverklaring van de accountant 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 audit is met instemming van de Auditcommissie uitgevoerd door een externe IT-auditor van het kantoor Avensus. De organisatie is in 2020 een stapje teruggegaan qua meting. Dit heeft te maken met het nieuwe BIO normenkader en de nog uit te voeren maatregelen die hierop van toepassing zijn. Dit betekent niet dat de

Voorstel raad

kwaliteit van onze informatiebeveiligingsorganisatie ten opzichte van het verslagjaar 2019 achteruit is gegaan. Door de gewijzigde norm (van BIG naar BIO) is de meetlat hoger gelegd. Op het moment van schrijven zijn de nog uit te voeren geprioriteerde maatregelen al gerealiseerd en ingepland om uitgevoerd te worden. Net als in de voorgaande jaren onder de BIG ontbreekt op een aantal onderdelen vastgesteld beleid, vastgelegde procesbeschrijvingen, richtlijnen en werkinstructies en proces- en gegevenseigenaarschap. Verder zijn de onderwerpen bedrijfscontinuïteit en logging belangrijk om de digitale weerbaarheid te vergroten. Met logging wordt bedoeld, het nog gerichter bijhouden van ongeoorloofde mutaties en wijzigingen in systemen.

Over de werking van de veiligheidsmaatregelen 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 volgens het normenkader.

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 hele overheid. De samenvatting geeft een meting van de BIO weer, zoals deze is uitgevoerd aan het begin van 2020. Een vergelijking met het voorgaande jaar is niet mogelijk door het gewijzigde normenkader. In de bijlage is het jaarverslag opgenomen. Hierin zijn de verbetermaatregelen vermeld, die geprioriteerd en ingepland zijn voor het resterende deel van 2021 en voor 2022.

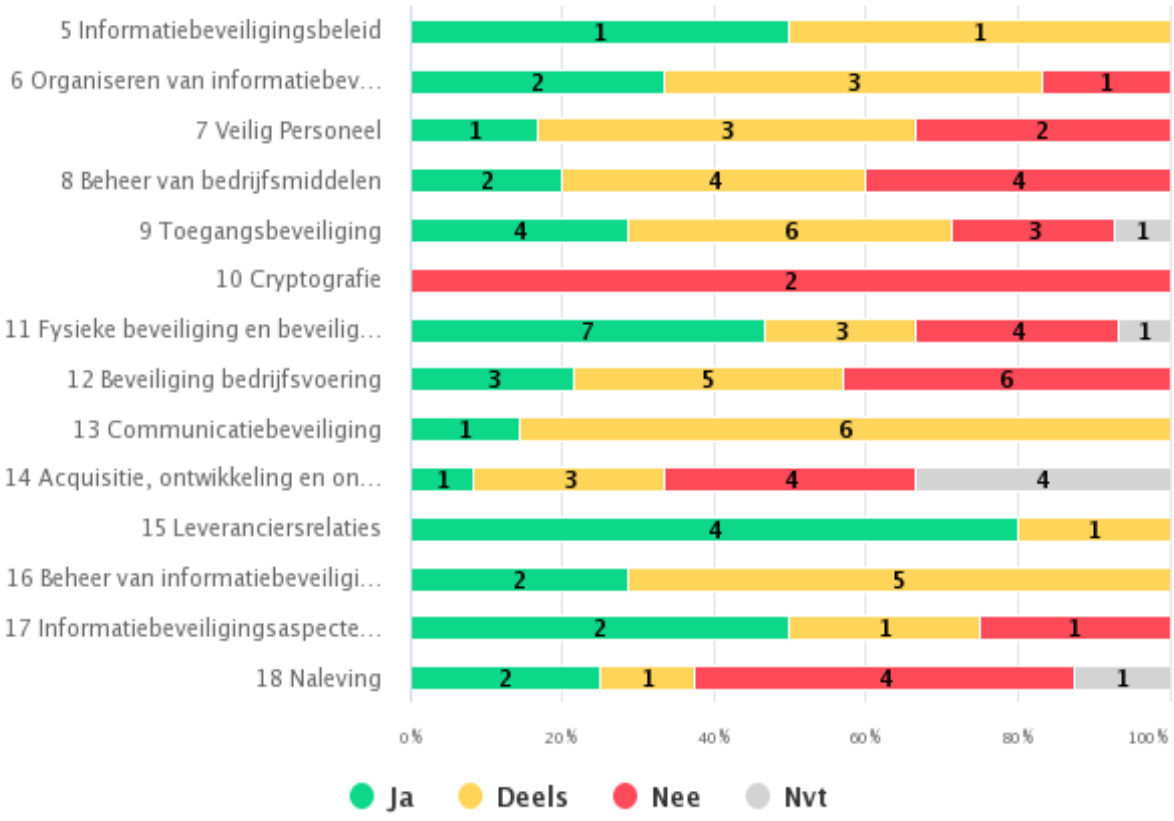
In 2020 zijn een aantal maatregelen genomen om de informatiebeveiliging naar een hoger niveau te tillen. Hierbij wordt opgemerkt dat een 100% beveiliging niet kan worden gegarandeerd. Organisatorische en technische maatregelen (Hard controls) zijn niet waterdicht en hebben hun prijs. Op basis van een risicoanalyse is een noodzakelijk pakket maatregelen en middelen gerealiseerd.
Risico's van datalekken en hacken blijven altijd aanwezig, maar de organisatie probeert deze risico's tot een minimum te beperken. Gedrag, veiligheidsbewustzijn en risicobewustzijn (Soft controls) van medewerkers hebben grote invloed op de informatieveiligheid. In de praktijk blijkt dat veel veiligheidsincidenten worden veroorzaakt door de menselijke factor.

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

Voorstel raad

Er zijn In 2020 maatregelen getroffen van technische en organisatorische aard. Onze technische infrastructuur is en wordt voor een groot gedeelte opnieuw ingericht, zodat deze voldoet aan de BIO normen. Beleid, werkinstructies en processen zijn waar nodig opnieuw ingericht, zodat ook deze aansluiten bij de BIO normen. In het kader van bewustwording worden er trainingen en cursussen aangeboden via het nieuwe educatie systeem (My Learning Factory) dat Hollands Kroon samen met Alkmaar heeft ontwikkeld.

Samenvatting *



***Overzicht van alle BIO hoofdstukken**

5. Informatiebeveiligingsbeleid
6. Organiseren van informatiebeveiliging
7. Veilig personeel
8. Beheer van bedrijfsmiddelen
9. Toegangsbeveiliging
10. Cryptografie

Voorstel raad

11. Fysieke beveiliging en beveiliging van de omgeving
12. Beveiliging bedrijfsvoering
13. Communicatiebeveiliging
14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen
15. Leveranciersrelaties
16. Beheer van informatiebeveiligingsincidenten
17. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
18. Naleving

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

Alternatieven (incl. argumenten)
n.v.t.

Financiële gevolgen	
Kosten	€ 10.000
Dekking binnen begroting*	Programma: Bedrijfsvoering Cluster: Bestuur
Geen dekking binnen begroting*	Dekkingsvoorstel:
Toelichting: de kosten hebben betrekking op de externe IT-audit (ENSIA)	

Bijlagen
Jaarverslag Informatiebeveiliging 2020