

De fractie van
Senioren Hollands Kroon

Verzenddatum

Ons kenmerk

Uw kenmerk
TV-2426

Uw brief van
8 juli 2024

onderwerp
Jaarverslag informatiebeveiliging 2023
Pagina
1/3

Contact
Tarik Fakir
T 088-321 5000

Beste fractie,

Op 8 juli 2024 heeft u technische vragen (nummer TV-2426) gesteld over Jaarverslag informatiebeveiliging 2023. In deze brief beantwoorden wij de door u gestelde vragen. U vindt de antwoorden direct onder de vragen.

Reactie

1. *Met betrekking tot uw opmerking omtrent het ontbreken van KPI's in het jaarverslag.*

Er is bewust gekozen om geen (detail) informatie en diens afhandeling te openbaren om de beveiliging niet onnodig te compromitteren. Algemene trends en aantallen per soort incident zouden in het vervolg wel met de raad gedeeld kunnen worden mocht deze behoefte er zijn. Dit geldt ook voor de detectietijden, oplostijden en inlogpogingen die correleren met een beveiligingsincident. Casusinformatie en variaties per type blijven vertrouwelijk.

Downtime van informatiesystemen worden benoemd in het jaarverslag als deze een impact hebben gehad op de bedrijfsvoering. Vanuit contract en leveranciersmanagement wordt erop toegezien dat de uptime garantie zoals deze contractueel is afgesteld (doorgaans 99,8% per jaar), gehonoreerd wordt.

Een getal zetten achter de hoeveelheid phishing acties en het detecteren hiervan is natuurlijk mogelijk. In het jaarverslag wordt echter ingegaan op de acties die voor de kwaadwillende actoren succesvol zijn geweest, en hoe de organisatie hiermee is omgegaan. Algemene

aantallen kunnen in het vervolg gedeeld worden. Informatie die betrekking heeft tot de methodiek en doelwitten blijven echter vertrouwelijk.

Mocht er behoefte zijn om deze algemene aantallen in te zien vóór het eerstvolgende verslag? Dan kan dit met de CISO ingepland worden.

2. *1. Is het Jaarverslag informatiebeveiliging 2023 naar de raad verstuurd om bewust een algemeen beeld te schetsen van de informatiebeveiliging?*

Het jaarverslag zoals deze is verstuurd heeft als doel een algemeen beeld te schetsen waarbij detailinformatie die zou kunnen leiden tot een beveiligingsincident of compromittatie van de beveiliging achterwege is gelaten. Verder heeft het jaarverslag als doel om aantoonbaar te maken dat de beveiliging jaarlijks incrementeel verbetert.

3. *Is er naast de informatie beschikbaar gesteld aan de raad, ook uitvoerige informatie beschikbaar bij het college waarop het beleid wordt gebaseerd?*

Het college is nauw betrokken bij de strategische inbedding van de beveiliging van de organisatie. Om adequaat besluiten te kunnen nemen is het van essentieel belang dat er wordt voorzien van informatie op detailniveau. Deze strategische besluiten hebben een effect op het tactisch/ operationele deel voor de uitvoerende organisatie.

4. *Heeft het college voldoende vertrouwen voor nu maar ook in de toekomst om vast te houden aan de ENSIA-methodiek en de baseline informatiebeveiliging overheid (BIO) om informatie veiligheid binnen de gemeente Hollandskroon te waarborgen?*

ENSIA en de BIO in combinatie met de NIS2 is de voedingsbodem van onze informatiebeveiligingsorganisatie. Dit wordt beaamd door de Vereniging van Nederlandse gemeenten, het Nationaal cyber security centrum, het Nationaal coördinator terrorismebestrijding en veiligheid, het forum standaardisatie en de Rijksinspectie digitale infrastructuur. Inclusief de verschillende stelselhouders (Logius, BKWI, RvIG).

Deze standaarden zijn gebaseerd op internationaal erkende normen en kaders. Hollands Kroon blijft inzetten op het inbedden en onderhouden hiervan voor nu en in de toekomst. Ontwikkelingen zoals bijvoorbeeld AI worden aangevuld met kaders die hiertoe specifiek zijn, zoals de Europese AI Act.

Met vriendelijke groet,

A. van Dam
Burgemeester

Deze brief is digitaal gemaakt en daarom niet ondertekend.