

Aan de gemeenteraad

22 FEB 2024

Ons kenmerk 481339
Bijlage(n)

Onderwerp Raadsbrief Strategisch Informatiebeveiligingsbeleid 2023 - 2026 en 16 februari 2024
SIEM/SOC

Geachte raadsleden,

Op 12 december 2023 hebben wij het Strategisch Informatiebeveiligingsbeleid 2023–2026 vastgesteld. In deze brief informeren wij u over de inhoud van het beleid en lichten we toe hoe we uitvoering aan het beleid geven. Daarnaast werken we in 2024 samen met de gemeente Westland aan een aanbesteding voor een SIEM/SOC oplossing. Een SIEM (Security Information and Event Management) en SOC (Security Operations Center) zijn beide essentiële componenten in de moderne beveiligingsinfrastructuur en wettelijk verplicht volgens de nieuwe Europese regelgeving op het gebied van informatiebeveiliging. Wij informeren u over de impact hiervan en de middelen die deze oplossing vraagt.

Het strategisch Informatiebeveiligingsbeleid

U leest in de bijlage het Strategisch Informatiebeveiligingsbeleid 2023-2026. Deze vervangt het eerder vastgestelde 'Strategisch Gemeentelijk Informatiebeveiligingsbeleid Gemeente Midden-Delfland 2020-2023.

De kernpunten van het informatiebeveiligingsbeleid zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en andere informatie. Het informatiebeveiligingsbeleid geldt voor alle processen van de gemeente. Het borgt daarmee de informatievoorziening tijdens de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het politieke bestuur, alle medewerkers, inwoners en ondernemers, gasten, bezoekers en externe relaties.

Het document bevat strategische beleidsuitgangspunten op het gebied van onze informatiebeveiliging. Hierin staan de uitgangspunten, het sturings- en verantwoordingsmechanismen en de rollen en verantwoordelijkheden beschreven. Daarnaast is rekening gehouden met de wettelijke kaders die aan informatiebeveiliging worden gesteld. Dit beleid brengt niet de huidige situatie in beeld, maar beschrijft de ontwikkelingen en het ambitieniveau van gemeentebrede informatiebeveiliging. Het beleid heeft een looptijd van drie jaar, waarna wederom een actualisatie plaatsvindt.

NIS2 en de BIO2.0

Momenteel wordt er gewerkt aan de nieuwe wet- en regelgeving voor informatiebeveiliging in Nederland: De Network and Information Systems Directive (NIS2-richtlijn) en de Baseline Informatiebeveiliging Overheid versie 2 (BIO2.0). De NIS2-richtlijn wordt op dit moment nog naar Nederlandse wetgeving vertaald. Duidelijk is wel dat deze richtlijn impact heeft voor gemeenten. Tussen nu en 2026 krijgen gemeenten te maken met 13 nieuwe regelgevende initiatieven op het gebied van digitalisering en cybersecurity. Wat de exacte impact is, is nu echter nog niet te zeggen.

In oktober 2024 treedt ook de Wet beveiliging netwerk- en informatiesystemen (Wbni) in werking, waarnaast ook de BIO2.0 op dat moment wettelijk verankerd zal zijn.

Het is nog onzeker in hoeverre deze wet- en regelgeving van toepassing zal zijn op de gemeente Midden-Delfland. De impact van NIS2 is voor ons afhankelijk van de mate waarin nu al gedocumenteerd voldaan wordt aan de BIO. Daarom is het cruciaal dat we als gemeente door blijven gaan met de cyclus van plannen, uitvoeren, controleren en bijstellen rondom de te nemen maatregelen uit het BIO normenkader.

De personele capaciteit op informatiebeveiliging is al enige jaren stabiel en toereikend voor de wettelijke taken. We verwachten echter dat we meer capaciteit nodig hebben. De nieuwe wetgeving brengt ook een grotere auditlast met zich mee. Daarnaast worden er meer verplichte maatregelen, zoals een Security Information & Event Management (SIEM) proces met de bijbehorende organisatie (SOC), ingevoerd. Deze ontwikkelingen vereisen niet alleen meer capaciteit, maar ook (aanzienlijke) financiële middelen.

Het Security Information & Event Management (SIEM) & SOC (Security Operations Center)

Wij hebben in de afgelopen jaren grote stappen gezet in onze informatiebeveiliging. De volgende logische stap is een sterkere focus op detectie en actieve preventie van incidenten. We hebben op dit vlak al belangrijke afzonderlijke maatregelen genomen zoals onze firewall die ons beschermt tegen bedreigingen van buitenaf. Maar ook onze oplossing voor emailbescherming gericht op bedreigingen zoals phishing en ransomware. De complexiteit van dreigingen en aanvallen neemt toe en de conventionele beveiligingsmaatregelen zijn steeds vaker niet meer toereikend.

Om geavanceerde dreigingen^[1], zowel van binnenuit als van buiten de organisatie, te kunnen adresseren is het essentieel om over de juiste hulpmiddelen en processen te beschikken. Hiermee kunnen we dreigingen en aanvallen in een zeer vroeg stadium detecteren. Het inrichten van een Security Information & Event Management (SIEM) proces met de bijbehorende organisatie (SOC), kan er door vroegtijdige detectie op meerdere bronnen voor zorgen dat de gevolgen van aanvallen worden verminderd of in sommige gevallen worden voorkomen. Wij informeerden u hierover ook tijdens de informatiebijeenkomst op 18 oktober 2022.

Korte toelichting op SIEM/SOC

Een SIEM-systeem verzamelt en analyseert beveiligingsinformatie uit verschillende bronnen, zoals onze firewall, e-mailfilter, IDS/IPS-systemen, antivirussoftware en logboeken van servers en netwerkapparaten. Het identificeert potentiële beveiligingsincidenten en genereert waarschuwingen die kunnen worden onderzocht door een SOC.

Een SOC is een team van beveiligingsprofessionals die verantwoordelijk zijn voor het monitoren van de beveiligingsinfrastructuur van een organisatie en het onderzoeken van beveiligingsincidenten. SOC-medewerkers gebruiken de gegevens die door het SIEM-systeem worden verzameld om beveiligingsincidenten te identificeren en te onderzoeken.

Gezamenlijke aanbesteding

Als gemeente hebben wij deelgenomen aan de door de VNG geleide aanbesteding voor een SIEM/SOC. Het gaat om het perceel van de gemeentebrede aanbesteding GGI-Veilig die in 2019 aan KPN werd gegund. Deze landelijke aanbesteding zou wat de kosten betreft kwantumvoordeel moeten opleveren voor de gemeenten. In 2021 is een bedrag extra in de begroting opgenomen voor een SIEM/SOC oplossing. We gingen daarbij uit van de oorspronkelijke VNG-aanbesteding (€24.000,-).

De VNG heeft het contract met KPN voor het leveren van SIEM/SOC-diensten aan gemeenten opgezegd toen duidelijk werd dat KPN niet aan de verwachtingen kon voldoen. Er kon maar een zeer beperkt SIEM worden opgeleverd met weinig te koppelen bronnen. Ook kon KPN de hoeveelheid gemeenten niet allemaal tegelijk bedienen en er ontstonden wachtlijsten. Dit betekende dat wij werden geconfronteerd met een forse vertraging en op zoek moesten naar een alternatief. Ook het gewenste kostenvoordeel viel daarmee weg.

^[1] https://nl.wikipedia.org/wiki/Advanced_Persistent_Threat

Samen met de gemeente Westland werken we nu aan een Europese aanbesteding voor het SIEM/SOC. Deze aanbesteding voltooien wij in 2024. Hoewel de aanbesteding nog loopt, zien wij wel dat de eerder geraamde kosten niet langer meer toereikend zijn. Wij verwachten een aanzienlijke jaarlijkse stijging. De hoogte is nog niet bekend en hangt onder andere af van welke en hoeveel systeembronnen gebruikt worden om te analyseren en of we 5 of 7 dagen x 24 uur per week actieve monitoring door het SOC vragen.

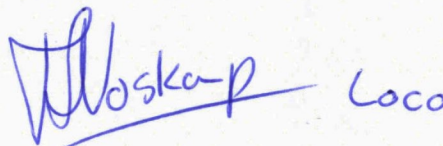
De hogere kosten voor het SIEM/SOC nemen we op in de Kadernota en begroting van 2025 omdat de Europese aanbesteding nog loopt en de oplossing naar verwachting niet eerder dan Q4 2024 in bedrijf zal zijn. De nieuwe Europese eisen verplichten ons om per oktober 2024 een SIEM/SOC te hebben.

In het streven naar optimale informatiebeveiliging beseffen we dat 100% garantie een illusie is, maar met het Strategisch Informatiebeveiligingsbeleid en een SIEM/SOC, zetten we belangrijke stappen richting een robuuste beveiligingsinfrastructuur die ons beschermt tegen cyberdreigingen en datalekken.

Met vriendelijke groet,
het college van burgemeester en wethouders,

b/a 

M.A.I. Born
gemeentesecretaris

 Loco

F.I. Noordermeer – van Slageren
burgemeester