INFORMATIE BEVEILIGINGS DIENST

VNG Realisatie

Factsheet

Juridische aspecten bij Monitoring & Response

Een operationeel kennisproduct ter ondersteuning van de implementatie van de Baseline Informatiebeveiliging Overheid (BIO)

INFORMATIE
BEVEILIGINGS
DIENST

Colofon

Naam document

Factsheet Juridische aspecten bij Monitoring & Response

Versienummer

1.0

Versiedatum

April 2019

Versiebeheer

Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

Met dank aan

De expertgroep en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product.

VNG Realisatie

INFORMATIE
BEVEILIGINGS
DIENST

Wijzigingshistorie

Versie	Datum	Wijziging / Actie
1.0	April 2019	Definitieve versie

Over de IBD

De IBD is een gezamenlijk initiatief van alle Nederlandse Gemeenten. De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en richt zich op (incident)ondersteuning op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD ondersteunt gemeenten bij hun inspanningen op het gebied van informatiebeveiliging en privacy / gegevensbescherming en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruikmaken van de producten en de generieke dienstverlening van de IBD.

De IBD is ondergebracht bij VNG Realisatie.

Leeswijzer

Deze factsheet is mede tot stand gekomen door een samenwerking van onder andere VNG, VNG Realisatie, de Informatie Beveiligingsdienst (IBD) en Kenniscentrum Europa Decentraal.

Voor meer informatie en vragen verwijzen we u naar de websites vng.nl en vngrealisatie.nl/privacy. Indien u naar aanleiding van dit document nog vragen heeft, of advies wilt over de AVG of privacy in het algemeen kunt u deze stellen via privacy@vng.nl

INFORMATIE
BEVEILIGINGS
DIENST

Juridische aspecten bij monitorin & response

Inleiding

De digitalisering van de samenleving heeft tot gevolg dat ook gemeenten hun wijze van dienstverlening en informatievoorziening veranderen. Digitalisering biedt vele kansen, maar brengt ook met zich mee dat de informatievoorziening en het gegevensbeheer kwetsbaarder is geworden voor inbreuken op de informatieveiligheid. Juist de informatieveiligheid bij het gegevensbeheer en bij de informatievoorziening is een randvoorwaarde voor het vertrouwen van burgers en bedrijven in de overheid. Digitalisering vormt geen bedreiging als men met de digitalisering ook de digitale weerbaarheid verhoogt. Dit is niet alleen nodig om te kunnen blijven voldoen aan de wet- en regelgeving, maar is ook nodig om zorg te dragen dat burgers en bedrijven vertrouwen blijven houden in de overheid. De IBD adviseert gemeenten om te starten met Security Information & Event Management (SIEM)/ Security Operations Center (SOC). Dit stelt gemeenten in staat om ICT-omgevingen centraal te monitoren en actief en vroegtijdig te handelen.

Deze factsheet beschrijft de juridische aspecten bij het verhogen van de digitale weerbaarheid door de inzet van SIEM/SOC-functionaliteit en biedt de functionaris gegevensbescherming (FG), de privacybeheerder en/of de jurist inzicht in de toepasselijke wet- en regelgeving. Alvorens in wordt gegaan op het juridisch kader zal de SIEM/SOC oplossing eerst kort worden toegelicht.

SIEM/SOC

Gemeenten hebben vanuit de Algemene Verordening Gegevensbescherming (AVG) de verplichting om passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beschermen.[1] Conventionele beveiligingsmaatregelen, zoals antivirussoftware en firewalls, zijn vaak niet meer toereikend en/of kunnen leiden tot een versnippering van beveiligingsoplossingen. Gezien de toenemende mate van complexiteit en impact van dreigingen, zullen aanvullende maatregelen moeten worden genomen om informatie binnen de gemeente te beschermen tegen onrechtmatige toegang en gebruik.

Een SOC kan hiervoor uitkomst bieden. Dit is de plek in de organisatie die alle ICT-security gerelateerde zaken centraal kan begeleiden en uitvoeren. Alhoewel er verschillende definities en doelen zijn waarvoor een SOC wordt ingezet, is de meestvoorkomende functie het monitoren, analyseren en loggen van securityinformatie binnen een ICT-infrastructuur. Relevante informatie van systemen, applicaties en netwerkverkeer worden centraal verzameld, gecorreleerd en geanalyseerd om te zien of afwijkende zaken hebben plaatsgevonden. De informatie binnen een SOC heeft een vertrouwelijk karakter.

Een hulpmiddel dat onlosmakelijk verbonden is met een SOC is een SIEM-systeem. Kort gezegd maakt een SIEM gebruik van bestaande logging en monitoringfaciliteiten. Het betreft software die in staat is om loginformatie vanuit verschillende bronnen te interpreteren en te correleren naar wat zich binnen en rondom het netwerk afspeelt op gebied van cyberaanvallen en andere beveiligingsincidenten. Op basis van deze informatie kunnen kwetsbaarheden ontdekt worden, kunnen aanvallen en verdacht gedrag in een vroeg stadium worden gesignaleerd en kan er direct actie worden ondernomen.

> De kracht van een SIEM zit er met name in dat zij in staat is om loginformatie uit de gehele ICT-infrastructuur te verzamelen en te analyseren. Wanneer er binnen korte tijd bijvoorbeeld 15 foutieve inlogpogingen zich voordoen, dan is zij in staat om 1 melding te weergeven dat er 15 foutieve inlogpogingen door een gebruiker op een bepaald systeem zijn geweest.

Een SOC is ten slotte geen doel op zich, maar een middel om het beveiligingsniveau van de gemeente te verhogen. Het implementeren (intern of middels een leverancier) van een SOC volstaat op zichzelf niet om de gemeente compliant te maken aan privacy en security normenkaders. Bovendien is een SOC een beveiligingsmaatregel op operationeel niveau, namelijk door het monitoren van activiteiten in de ICT-infrastructuur en daarmee ontdekken van ongewenste acties.

Toepasselijke normenkaders en specifieke regelingen

De belangrijkste normenkaders die van toepassing zijn op een SOC zijn de AVG en de Baseline Informatiebeveiliging Overheid (BIO). De “winst” van een SOC op juridisch terrein is dat beter *aantoonbaar* kan worden voldaan aan deze normenkaders. Zo moeten er volgens de AVG aantoonbare beveiligingsmaatregelen worden getroffen.[2] Ook op grond van de BIO moeten gemeenten aantoonbaar ‘in control’ zijn. Verder zijn de Wet op de ondernemingsraden (WOR) en het strafrecht relevant voor een SOC.

[1] Art. 32 AVG.
[2] Art. 5 lid 1 onder f juncto art. 5 lid 2 AVG.

VNG Realisatie

Privacy by Design en Security by Design, vastgelegd in of voortvloeiend uit de AVG, kunnen ook beter worden vormgegeven met behulp van een SOC. Bij bestaande en nieuwe applicaties kan dan immers worden beoordeeld of het nuttig is om de applicatie aan te sluiten op het SOC, waarmee vervolgens alle activiteiten centraal kunnen worden gemonitord en gelogd. Daardoor wordt (direct aan het begin van het traject) de beveiliging van de applicatie, en van de gemeente als geheel, verhoogt.

Speciale aandacht verdient het onderwerp datalekken. Deze incidenten dienen op grond van de AVG binnen uiterlijk 72 uur te worden gemeld aan de toezichthouder.[3] Met een SOC kunnen incidenten sneller worden gesignaleerd en afgehandeld, waardoor ze ook eerder kunnen worden gemeld of nadere informatie kan worden verstrekt. Als een incident heeft plaatsgevonden moet onder omstandigheden, om te kunnen vaststellen dat het geen datalek is geweest, kunnen worden uitgesloten dat de betreffende persoonsgegevens door onbevoegden zijn ingezien. Het bewijs hiervoor kunnen (o.a.) de logs zijn die worden verzameld op een SOC. Deze informatie kan als input fungeren voor het datalekregister, dat een van de verplichte maatregelen is om aan uw verantwoordingsplicht (accountability) te voldoen. Een SIEM/SOC helpt u om invulling te geven aan de verantwoordingsplicht.[4]

Rechtmatigheid

De maatregelen die worden genomen om de digitale weerbaarheid te verhogen, zoals een SOC, dienen er enerzijds voor dat persoonsgegevens die de gemeente in huis heeft op een passende wijze worden beschermd tegen onbevoegden, anderzijds dienen deze maatregelen zelf ook aan de AVG te voldoen wanneer de maatregelen persoonsgegevens verwerken. De eerste vraag is of in een SOC persoonsgevens worden verwerkt.

Persoonsgegevens

Onder een "persoonsgegeven" wordt verstaan "*elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon*"[5]. Eén van de belangrijkste gegevens die in een SOC worden verwerkt zijn IP-adressen. Het Hof van Justitie heeft eerder bepaald dat een IP-adres een persoonsgegeven is, omdat er een mogelijkheid is tot identificatie van de gebruiker.[6] Ook op grond van de AVG is duidelijk dat een IP een persoonsgegeven is.[7] Wanneer de gemeente in het kader van het verhogen van de digitale weerbaarheid loginformatie en andere bronnen analyseert middels een SIEM/SOC waardoor IP-adressen zichtbaar worden, geldt dit dus als het verwerken van persoonsgegevens. De consequentie daarvan is dat de AVG van toepassing is. Daarnaast kunnen er ook andere persoonsgegevens worden verwerkt in een SOC, zoals MAC-adressen[8] en e-mailadressen.

Doel en grondslag

De AVG vereist voor iedere verwerking van persoonsgegevens een geldig doel en rechtmatige grondslag. Er is sprake van een geldig doel voor het verwerken van persoonsgegevens in een SOC, namelijk - kort geformuleerd - het verhogen van de informatiebeveiliging bij gemeenten. Afhankelijk van het doel van het SOC dient dit zo specifiek mogelijk te worden omschreven en gedocumenteerd, zoals in het verwerkingsregister.

Wat betreft de grondslag, vermeldt de AVG dat een verwerking van persoonsgegevens, *voor zover deze strikt noodzakelijk en evenredig*[9] *is* met het oog op netwerk- en informatiebeveiliging, een gerechtvaardigd belang vormt.[10] Ingevolge de AVG dient de gemeente immers passende organisatorische en technische maatregelen te nemen om persoonsgegevens te beveiligen.
Het verwerken van de gegevens in het kader van het verhogen van de digitale weerbaarheid is dus gerechtvaardigd, mits de verwerking van persoonsgegevens strikt noodzakelijk en evenredig is.

Beginselen: noodzakelijkheid, bewaartermijnen, transparantie, geheimhouding

Bij noodzakelijkheid en evenredigheid gaat het om vragen zoals: welke persoonsgegevens zijn noodzakelijk zijn voor het SOC? Staat het doel van de verwerking van persoonsgegevens in verhouding tot de inbreuk op de privacy van betrokkene? En is het doel ook op andere, minder inbreukmakende wijze te realiseren? Het loggen van IP-adressen zal in het kader van beveiliging noodzakelijk zijn om ongeoorloofde toegang of een poging hiertoe in een vroeg stadium te kunnen signaleren.

[3] Art. 33 lid 1 AVG.
[4] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/verantwoordingsplicht#hoe-voldoe-ik-aan-de-verantwoordingsplicht-6099
[5] Art. 1 sub a AVG.
[6] Hof van Justitie 19 oktober 2016, zaak C-582/14.
[7] De AVG heeft het in de overwegingen over 'online identificatoren', waaronder een IP-adres valt.
[8] Dit is een hardware adres gekoppeld aan een systeem, wat ook het herleiden naar een persoon mogelijk maakt.
[9] Ook wel omschreven als het proportionaliteits- (evenredigheid) en het subsidiariteitsbeginsel (noodzakelijkheid).
[10] Art. 6 lid 1 onder f en Overweging 49.

De persoonsgegevens dienen verwijderd te worden wanneer de veiligheidsanalyse is uitgevoerd en geconcludeerd kan worden dat de persoonsgegevens niet leiden tot een (vermoeden van) verdacht gedrag, kwetsbaarheid of aanval. Een bewaartermijn van maximaal drie maanden na verzameling is hiervoor een goede richting. Als wel sprake is van een al dan niet gerichte aanval mogen de persoonsgegevens net zo lang worden bewaard als nodig voor het oplossen van het incident.

Transparantie over de verwerkingen van persoonsgegevens door de gemeente is een belangrijk beginsel uit de AVG. De gemeente kan dit waarborgen door bijvoorbeeld in de privacyverklaring aan te geven dat de gemeente persoonsgegevens verwerkt in een SOC in het kader van het verhogen van de digitale weerbaarheid.[11] Een algemene beschrijving van de maatregelen die worden genomen dienen tevens opgenomen te worden in het register van verwerkingsactiviteiten.[12] Ook in een publieke versie van dit register kunnen burgers worden geïnformeerd over de verwerkingen die plaatsvinden in een SOC.

De security analisten in een SOC werken dagelijks met (zeer) vertrouwelijke informatie. Het is dan ook essentieel dat er periodiek relevante trainingen worden gevolgd door deze medewerkers. Ook kunnen er (extra) geheimhoudingsverklaringen worden getekend en screenings worden uitgevoerd. Het SOC inrichten in een beveiligde ruimte waartoe alleen geautoriseerde medewerkers toegang hebben draagt ook bij aan een betere beveiliging van de gegevens.

Rechten van betrokkenen: Informatieplicht
Wanneer verwerking van persoonsgegevens plaatsvindt, moet voor betrokkenen duidelijk zijn dat dit zo is of zal zijn en wat het doel van de verwerking is. De AVG geeft aan welke informatie in ieder geval verstrekt moet worden[13]. Het doel van het recht op informatie is te laten zien dat verwerking van persoonsgegevens transparant en behoorlijk gebeurt.[14] Het recht op informatie betekent dat een gemeente betrokkenen actief, op een heldere en toegankelijke manier moet informeren. De gemeente kan dit waarborgen door de eerdergenoemde privacyverklaring.

Rechten van betrokkenen: Recht van inzage
Als er persoonsgegevens van iemand worden verwerkt heeft deze het recht te weten welke gegevens dit zijn, waarvoor de gemeente deze gegevens precies gebruikt en met wie deze eventueel worden gedeeld. Dit is het recht op inzage.[15] Betrokkene kan alleen gegevens over zichzelf opvragen, niet over anderen. Er hoeft geen reden te worden gegeven voor een inzageverzoek. De AVG is van toepassing op een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens of wanneer persoonsgegevens opgenomen zijn in een bestand of daartoe bestemd zijn. SIEM/SOC voldoet aan deze criteria en is het recht op inzage van toepassing. Mocht de gemeente nog geen proces hebben ingericht om met inzageverzoeken om te gaan, zorg dan dat dit wordt geïmplementeerd.

SOC uitbesteden: verwerkersovereenkomst
De gemeente dient afspraken te maken over de verwerking van persoonsgegevens wanneer een SOC wordt uitbesteed aan een andere partij. Deze derde partij zal doorgaans aan te merken zijn als verwerker[16] in de zin van de AVG. Er dient dan ook een verwerkersovereenkomst[17] te worden afgesloten met deze partij.

Medezeggenschapswetgeving

De inrichting van een SIEM/SOC zal voorgelegd moeten worden aan de ondernemingsraad (OR) wanneer er logbestanden met IP-adressen verzameld worden. De logbestanden zullen immers niet alleen informatie bevatten van buitenstaanders, maar ook gegevens bevatten van (medewerkers van) de interne organisatie. Op grond van artikel 25 lid 1 sub k van de Wet op de ondernemingsraden (WOR) dient een voorgenomen besluit over de invoering of wijziging van een belangrijke technologische voorziening ter advisering te worden voorgelegd aan de OR. Op grond van artikel 27 lid 1 WOR is bovendien instemming vereist van de OR wanneer het een regeling betreft die invloed heeft op de bescherming van de persoonsgegevens van de in de gemeente werkzame personen. Wanneer er logbestanden van in de gemeente werkzame personen worden verwerkt, en deze gegevens herleidbaar (kunnen) zijn tot individuele medewerkers, dient de OR dan ook om zowel advies als instemming te worden gevraagd bij het inrichten van een SIEM/SOC.

[11] Zie voor meer de ‘Handreiking privacyverklaring’ van de IBD, https://www.informatiebeveiligingsdienst.nl/project/privacy/.
[12] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/verantwoordingsplicht#wat-moet-er-in-het-register-van-verwerkingsactiviteiten-staan-6137
[13] Art. 13 en 14 AVG.
[14] Zie voor meer de ‘Handreiking rechten van betrokkenen AVG deel 1, informatieplicht en recht van inzage’ van de IBD.
[15] Artikel 15 AVG.
[16] Een verwerker verwerkt persoonsgegevens ten behoeve van de verwerkingsverantwoordelijke. De factsheet ‘Verwerkingsverantwoordelijk of verwerker?’ van de IBD biedt u informatie en een beslismodel om te bepalen of een derde partij aangemerkt kan worden als verwerker.
[17] De IBD heeft een standaard verwerkersovereenkomst opgesteld. Deze is beschikbaar via de IBD-website.

Strafrechtelijke gegevens

De gegevens die de gemeente in het kader van beveiliging analyseert, kunnen aanleiding zijn om aangifte te doen van het binnendringen in een computersysteem of netwerk – of een poging hiertoe. Dit is een misdrijf op grond van artikel 138ab van het Wetboek van Strafrecht. De geanalyseerde gegevens zullen in dat geval kwalificeren als strafrechtelijke gegevens nu zij informatie bevatten over (pogingen tot) strafbare feiten, zoals computervredebreuk, het uitvoeren van DDOS aanvallen of het wederrechtelijk wijzigen van digitaal opgeslagen gegevens. Deze gegevens mogen niet met derden worden gedeeld, behoudens opsporingsambtenaren in het kader van het doen van aangifte.

Adviezen

Gezien de toenemende mate van complexiteit en impact van dreigingen is het sterk aan te raden om een start te maken met het verhogen van de digitale weerbaarheid door middel van SIEM/SOC. De IBD adviseert hierbij het volgende:

- Voer een data protection impact assessment (DPIA) uit, voordat een SIEM/SOC wordt ingericht. Op die manier kan gegevensbescherming en de AVG-beginselen al bij de aanschaf en de inrichting van het systeem worden meegenomen. De FG moet om advies worden gevraagd bij de DPIA.
- Stel duidelijk vast wat het doel is van de verwerking, welke (persoons)gegevens nodig zijn om dit doel te bereiken en hoelang de gegevens bewaard mogen worden. Documenteer deze stappen, zoals in het verwerkingsregister, inclusief de motivatie voor de gekozen bewaartermijn.
- Beleg een proceseigenaar voor de maatregelen die worden genomen.
- De FG moet van tevoren worden betrokken. Het verhogen van de digitale weerbaarheid d.m.v. SIEM/SOC zal tot gevolg hebben dat persoonsgegevens worden verwerkt en de AVG van toepassing is. De FG kan advies geven en meedenken over welke systemen kritische informatie bevatten en dus opgenomen moeten worden in de monitoring en logging. Vanuit het SOC kan de FG worden geïnformeerd over toegang tot persoonsgegevens en de verwerking daarvan.
- Wees transparant richting medewerkers en burgers over de wijze van het verwerken van persoonsgegevens.
- Neem de verwerkingen die in het kader van het verhogen van de digitale weerbaarheid d.m.v. SIEM/SOC worden uitgevoerd op in het register van verwerkingsactiviteiten van de gemeente.
- Betrek de OR en vraag hen om advies en instemming.

INFORMATIE
BEVEILIGINGS
DIENST

Kijk voor meer informatie op:
www.informatiebeveiligingsdienst.nl

Nassaulaan 12
2514 JS Den Haag
CERT: 070 204 55 11 (9:00 – 17:00 ma – vr)
CERT 24x7: Piketnummer (instructies via voicemail)
info@IBDGemeenten.nl / incident@IBDGemeenten.nl

VNG Realisatie

VNG Realisatie