AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Hoge Nieuwstraat 8, 2514 EL Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Aangetekend
Cyberveilig Nederland

Gooimeer 4-15
1411 DC NAARDEN

Datum
11 april 2024

Uw brief van
7 maart 2024

Onderwerp
RE: Vorderen van informatie bij incident responsebedrijven

Geachte ,

De Autoriteit Persoonsgegevens (AP) heeft kennis genomen van de brief van Cyberveilig Nederland (CVNL) d.d. 7 maart 2024 met het onderwerp “Vorderen van informatie bij incident responsebedrijven”. In deze brief roept u de AP op bij het onderzoeken van cyberincidenten geen informatie te vorderen van dienstverleners die lid zijn van uw brancheverenigingen, maar alleen van de partijen die getroffen zijn door het incident. Graag voorziet de AP u hierbij van een reactie.

De AP stelt voorop dat zij de uitgangspunten van CVNL onderschrijft voor wat betreft het vergroten van de digitale weerbaarheid van Nederland, en, in dat kader, het belang van transparantie en informatie-uitwisseling met relevante stakeholders. De AP heeft als missie de bescherming van persoonsgegevens te bevorderen en te bewaken. Om dit te bereiken is samenwerking met relevante partijen, waaronder CVNL en haar leden, van groot belang. Het werk van CVNL en haar leden ziet de AP als belangrijk en waardevol en draagt bij aan het bereiken van de missie van de AP.

De AP heeft als onafhankelijk toezichthouder op de bescherming van persoonsgegevens een andere rol dan CVNL en haar leden. De AP heeft een toezichthoudende taak en bijbehorende bevoegdheden. Deze bevoegheden worden door de AP op de minst verstrekkende wijze ingezet. Dat betekent in het concrete geval onder meer dat de AP, wanneer zij een melding ontvangt van een cyberincident, de informatie en stukken die relevant zijn om haar toezichthoudende taken uit te kunnen voeren in beginsel altijd opvraagt of vordert bij de organisatie waar het cyberincident heeft plaatsgevonden. Dat neemt echter niet weg dat de AP, indien zij dit in het belang van het onderzoek nodig acht, zich ook kan richten tot leden van uw brancheverenigingen om informatie op te vragen of te vorderen. Bijvoorbeeld: wanneer de AP wil controleren of de informatie die zij heeft verkregen over een cyberincident juist en volledig is. Daarbij zij opgemerkt dat niemand is ontheven van de verplichting om desgevraagd medewerking te verlenen aan de AP. Indien nodig staat daartegen rechterlijke toetsing open.

Datum
11 april 2024

Reactie AP op uitspraak voorzieningenrechter Midden Nederland 26 maart 2024
Naar aanleiding van een last onder dwangsom die de AP aan één van uw leden heeft opgelegd, heeft het desbetreffende lid van uw brancheverenigingzich tot de bestuursrechter gewend met het verzoek om een voorlopige voorziening. In de uitspraak op het verzoek heeft de voorzieningenrechter bevestigd dat de AP de bevoegdheid heeft inlichtingen te vorderen en dat leden van uw brancheverenigingin beginsel daaraan medewerking moeten verlenen. Deze bevoegdheid wordt begrensd door het evenredigheidsbeginsel, inhoudende dat een toezichthouder van zijn bevoegdheden slechts gebruik maakt voor zover dat redelijkerwijs voor de vervulling van zijn taak nodig is. De voorzieningenrechter heeft aanleiding gezien om de gevraagde voorziening toe te wijzen, omdat de AP naar het oordeel van die rechter in dit concrete geval niet alle minder ingrijpende middelen heeft aangewend. Hoewel de AP van mening blijft dat zij haar bevoegdheden op de juiste gronden en met inachtneming van het evenredigheidsbeginsel heeft ingezet, respecteert zij de uitspraak van de voorzieningenrechter.

Voor de toekomst betekent dit dat de AP de mogelijkheid heeft en houdt om inlichtingen te vorderen bij één van uw leden, indien zij dat in het belang acht van het onderzoek. De AP zal daarbij vanzelfsprekend rekening houden met het evenredigheidsbeginsel.

In aanvulling op het bovenstaande reageert de AP hieronder puntsgewijs op de twee overwegingen die u noemt in uw brief.

Reactie AP op Overweging 1. “De aanpak van de AP werkt marktverstorend”
CVNL stelt in haar brief dat de cybersecurity branche het risico loopt dat organisaties die getroffen zijn door een cyberincident de dienstverlening van cybersecuritybedrijven te laat of helemaal niet meer inschakelen, omdat zij vrezen hiermee de controle over de afhandeling van het incident kwijt te raken. De AP deelt dit standpunt niet.

Bij de beoordeling van de risico’s van een cyberincident moet de getroffen partij de inbreuk (laten) onderzoeken om inzicht te krijgen in de mogelijke gevolgen van de aanval. De getroffen partij moet op verzoek de feitelijke bevindingen van deze onderzoeken overleggen aan de AP, zodat de AP kan controleren of de getroffen partij aan haar verplichtingen uit hoofde van de Algemene Verordening Gegevensbescherming (AVG) heeft voldaan. Indien organisaties die getroffen zijn door een cyberincident besluiten het incident later of helemaal niet te laten onderzoeken door een cybersecuritybedrijf, heeft dat tot gevolg dat deze organisaties de AP niet (tijdig) van volledige informatie over de aard en omvang van de inbreuk kunnen voorzien. Het verzamelen van exacte informatie over de inbreuk is echter essentieel om het risiconiveau vast te stellen en een nieuwe of voortgezette cyberaanval te voorkomen. Bij twijfel over de bijzonderheden van de cyberaanval (bijvoorbeeld: omdat geen onderzoek is gedaan naar de inbreuk) moet het ongunstigste scenario in aanmerking worden genomen en moet het risico dienovereenkomstig worden beoordeeld. Dat betekent onder meer dat getroffen partijen die geen onderzoek (laten) doen naar het cyberincident ervan uit dienen te gaan dat alle gegevens en bestanden op hun systemen zijn getroffen door de aanval, én dat deze gegevens en bestanden zijn geëxfiltreerd door de aanvaller. De AP verwacht in deze gevallen dat de betreffende partij alle betrokkenen informeert waarvan (mogelijk) persoonsgegevens zijn betrokken bij de aanval. Een ander gevolg van het niet onderzoeken van een cyberincident is dat de

getroffen organisatie geen informatie heeft over de beveiligingskwetsbaarheden waarvan de aanvaller (mogelijk) misbruik heeft gemaakt. De getroffen organisatie loopt daardoor het risico om opnieuw het doelwit te worden van een soortgelijke cyberaanval.

Samenvattend kunnen de gevolgen voor getroffen organisaties die geen onderzoek (laten) doen vele malen schadelijker zijn voor de betreffende organisatie dan het wél (laten) uitvoeren van onderzoek. De AP merkt daarbij op dat organisaties die goede medewerking verlenen, en de AP tijdig en volledig informeren over het cyberincident, in principe zelden in aanmerking komen voor handhavende maatregelen van de AP.

Reactie AP op Overweging 2. "De aanpak van de AP heeft een remmend effect op informatie-uitwisseling"
CVNL stelt verder dat zij verwacht dat de branche zich als gevolg van de aanpak van de AP voortaan terughoudender zal opstellen als het gaat om het delen van informatie uit cyberincidenten. De AP deelt dit standpunt niet.

De AP ziet niet hoe haar werkwijze bij het onderzoeken van specifieke cyberincidenten van invloed is op het delen van geanonimiseerde informatie over cyberincidenten door de branche, aangezien deze informatie niet herleidbaar is naar specifieke organisaties. Daarnaast zet de AP zich, net als de cybersecuritybranche, al jaren in om informatie uit ontvangen meldingen over datalekken (waaronder cyberincidenten) te delen met het publiek via voorlichting op de AP website, en via de jaarlijkse datalekkenrapportage. Hiermee levert de AP een bijdrage aan het creëren van bewustzijn, het voorkomen van datalekken en cyberincidenten, en het bevorderen van de weerbaarheid van organisaties in Nederland. Voorts is de AP in 2023 samen met het Centraal Bureau voor de Statistiek (CBS) een project gestart om informatie van geregistreerde datalekken die bij de AP gemeld zijn beschikbaar te stellen voor wetenschappelijk en statistisch onderzoek. De uitkomsten van dit wetenschappelijk onderzoek kunnen verder bijdragen aan het verhogen van de weerbaarheid van organisaties tegen cyberincidenten.

Samenvattend spant de AP zich in om informatie-uitwisseling over cyberincidenten te stimuleren, daarmee is de AP zelf ook onderdeel van de initiatieven waarnaar CVNL refereert in haar brief. De AP verwacht ook dat de branche zich, tesamen met de AP, zal blijven inzetten om relevante informatie uit cyberincidenten te delen met het publiek, gelet op het grotere belang dat daarmee gemoeid is, namelijk: het vergroten van de digitale weerbaarheid van Nederland.

Voor de goede orde merk ik op dat deze brief ook op de website van de Autoriteit Persoonsgegevens (www.autoriteitpersoonsgegevens.nl) is gepubliceerd.

Hoogachtend,
Autoriteit Persoonsgegevens,

mr. A. Wolfsen
voorzitter