Gooimeer 4-15
1411 DC Naarden

info@cyberveilignederland.nl
www.cyberveilignederland.nl

KvK 71802525

Autoriteit Persoonsgegevens
T.a.v. dhr. mr. A. Wolfsen
Hoge Nieuwstraat 8
2514 EL DEN HAAG

Betreft: Vorderen van informatie bij incident responsebedrijven

Geachte heer Wolfsen,

Graag vragen wij uw aandacht voor het volgende. Wij zijn geïnformeerd over een situatie die is ontstaan in relatie tot een klant van één van de leden van onze brancheverenigingen, Cyberveilig Nederland, en uw organisatie, de Autoriteit Persoonsgegevens. Deze klant was getroffen door een cyberincident en heeft daarvan een melding bij uw autoriteit gemaakt. De klant werd bij de afhandeling van dit incident ondersteund door ons lid met incident-response activiteiten.

In de opvolging van deze melding heeft uw organisatie zich weliswaar eerst tot de getroffen organisatie (de klant van ons lid) gewend, maar uiteindelijk het gesprek met hen beëindigd en de informatie van de dienstverlener (ons lid) gevorderd. Naar ons bekend is inmiddels een last onder dwangsom opgelegd om de informatie alsnog aan te leveren.

Wij zijn als brancheorganisatie verbaasd en geschrokken over deze ontwikkeling omdat wij van mening zijn dat deze de gehele cybersecuritybranche schaadt en dat daarmee ook de weerbaarheid van Nederland in het geding komt. Wij verzoeken daarom dringend om te stoppen informatie over cyberincidenten te vorderen bij cybersecuritydienstverleners en verzoeken alle betrokkene deze voortaan op te vragen bij de getroffenen van het desbetreffende cyberincident. Daarbij merken wij op dat wij als brancheverenigingen het belang van transparantie niet ter discussie stellen. Wij vinden dat de Autoriteit Persoonsgegevens te allen tijde volledig geïnformeerd dient te worden. Wij zijn echter van mening dat informatie bij de juiste partij gevorderd dient te worden: de getroffene van het cyberincident. Deze kan waar nodig ingeschakelde dienstverleners hierbij betrekken.

Onze overwegingen zijn als volgt:

1. De basis voor een goede dienstverlening van cybersecuritybedrijven aan hun klanten is vertrouwen. Dit vertrouwen wordt door uw aanpak ondermijnd. Dit betekent dat we als branche het risico lopen dat organisaties met incidenten pas later of helemaal niet meer aankloppen bij deze dienstverleners omdat zij hiermee de controle over de afhandeling van een incident kwijtraken. Uw aanpak werkt hiermee marktverstorend.

   Het is bovendien aan een getroffene van een cyberincident om de verantwoordelijkheid te nemen uw autoriteit tijdig te informeren en van de juiste informatie te voorzien. Zij worden hier doorgaans proactief op gewezen door betrokken dienstverleners en kunnen door hen hierbij worden ondersteund. Als getroffenen van cyberincidenten er niet op kunnen rekenen dat vertrouwelijkheid tussen hen en de dienstverlener is gewaarborgd kan dit betekenen dat zij essentiële informatie over incidenten achterhouden waardoor de dienstverlener zijn diensten onvoldoende goed kan leveren of wellicht helemaal niet meer zal worden ingezet. Ook is Cyberveilig Nederland van mening dat u met deze vordering de verantwoordelijkheid voor de correcte afhandeling van een incident weghaalt bij de getroffene. En juist zij is verantwoordelijk voor deze afhandeling, en niet de ondersteunende cybersecuritydienstverlener.

2. Als branche hebben we de afgelopen jaren hard gewerkt aan meer transparantie en het delen van informatie uit incidenten met elkaar en met de overheid om deze informatie in te zetten om incidenten elders te voorkomen. Ondanks dat dit geanonimiseerde informatie betreft, verwachten wij dat de branche zich als gevolg van uw aanpak in deze initiatieven voortaan terughoudender zal opstellen omdat de gegevens die worden gedeeld onder een vergrootglas komen te liggen. Dit terwijl het delen van deze informatie leidt tot een hogere weerbaarheid van álle organisaties in Nederland en het verminderen van cyberdreigingen. Het doel van informatie-uitwisseling is om Nederland een onaantrekkelijk doelwit te maken voor statelijke actoren en cybercriminelen. Overheidspartijen en private organisaties hebben ieder ‘stukjes van de puzzel’ en zoeken naar manieren om deze, binnen geldende juridische kaders, met elkaar te delen. Het is dus van belang dat deze informatie-uitwisseling richting de toekomst verder wordt gestimuleerd.

Kortom, graag zien wij dat de juiste procesgang wordt gevolgd in voorliggende én toekomstige situaties, waarbij gericht contact wordt gezocht met de getroffenen van cyberincidenten voor het vorderen van informatie en niet met de dienstverleners die hen bij de incidenten ondersteunen.

Wij kijken uit naar uw spoedige reactie en vertrouwen op een juist oordeel in voorliggende voorlopige voorziening en zijn vanzelfsprekend bereid tot het voeren van een gesprek met alle betrokkenen over onze zienswijze in deze kwestie.

Met vriendelijke groet,

Petra Oldengarm
Directeur

Over Cyberveilig Nederland

Cyberveilig Nederland (CVNL) is de belangenvereniging van de cybersecuritysector. In die hoedanigheid maken we ons sterk voor het creëren van meer transparantie en kwaliteit in de markt. Ook behartigen we de belangen van de cybersecuritysector richting stakeholders zoals de overheid, wetenschap en politiek. Onze missie is de digitale weerbaarheid van Nederland te vergroten. Eén van de eisen om dit te bereiken is het actief delen van informatie. Vanuit CVNL stimuleren we dit actief door samen te werken met relevante overheidspartijen en andere belanghebbenden. In die hoedanigheid zijn we ook door het ministerie van Justitie en Veiligheid in 2020 aangewezen als schakelorganisatie onder de wet beveiliging netwerk informatiesystemen (wbni).[1] Daarnaast spelen we een actieve rol in het tot stand komen van een 'landelijk dekkend stelsel van informatieknooppunten'[2] , zijn we vanaf de start betrokken bij het Anti Abuse Netwerk (AAN)[3], zijn we actief deelnemer in het Programma Cyclotron[4] en zijn we mede-initiatiefnemer van Project Melissa.[5]

[1] https://www.ncsc.nl/actueel/nieuws/2020/december/9/intensievere-informatie-uitwisseling-ncsc-en-nederlandse-cybersecuritybedrijven
[2] https://www.nctv.nl/onderwerpen/landelijk-dekkend-stelsel
[3] https://www.abuse.nl/
[4] Programma Cyclotron moet leiden tot een platform waarbinnen publieke en private partijen informatie delen over digitale incidenten en dreigingen. Zie: https://www.nctv.nl/onderwerpen/programma-cyclotron
[5] Project Melissa is een samenwerkingsverband tussen deze publieke en private partijen om ransomwareaanvallen te bestrijden. Het gezamenlijke doel is om Nederland een onaantrekkelijk doelwit te maken voor ransomwarecriminelen. Zie: https://zoek.officielebekendmakingen.nl/stcrt-2023-29185.pdf en https://cyberveilignederland.nl/actueel/cyberveilig-nl-politie-om-en-ncsc-werken-samen-aan-ransomwarebestrijding