CJG Rijnmond

Responsible Disclosure Agreement

Binnen CJG Rijnmond vinden wij de veiligheid van onze ICT-systemen zeer belangrijk en streven wij naar een hoge beveiliging. Ondanks onze zorg voor de beveiliging van onze ICT-systemen kan het voorkomen dat er toch een zwakke plek is. Hier lees je hoe CJG Rijnmond daarmee omgaat.

Wanneer je een zwakke plek en/of een beveiligingslek in één van onze systemen vindt, horen wij dit graag van je zodat we zo snel mogelijk maatregelen kunnen treffen. Let wel: ons beleid voor responsible disclosure is geen uitnodiging om ons netwerk uitgebreid actief te scannen om zwakke plekken te ontdekken. Wij willen graag met jou samenwerken om onze systemen beter te kunnen beschermen en deze situatie zo spoedig mogelijk op te lossen. Daarom verzoeken wij deze informatie met ons te delen.

De volgende digitale omgevingen vallen binnen de scope van dit responsible disclosure beleid:

- Openbare website en portalen onder het domein: cjgrijnmond.nl.
- Onze e-mailbeveiliging, denk aan SPF, DKIM, DMARC op cjgrijnmond.nl.
- Publieke API's met administratieve functionaliteit zoals afspraakplanning.

De volgende digitale omgevingen vallen NIET binnen de scope van dit responsible disclosure beleid:

- Productiesystemen met medische gegevens (Digitaal Dossier JGZ).
- Applicaties en infrastructuur van externe leveranciers.
- Social engineering methoden.
- DDoS, of andere handelingen die de beschikbaarheid van onze digitale omgeving in gevaar brengen.

Wij vragen bij een gevonden kwetsbaarheid om het volgende:

- Jouw bevindingen uitsluitend te mailen naar security@cjgrijnmond.nl.
- De zwakke plek die je hebt gevonden niet te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of gegevens van derden in te zien, te verwijderen of aan te passen.
- Jouw bevindingen niet met anderen te delen totdat het is opgelost.
- Alle vertrouwelijke gegevens die je hebt verkregen via het lek direct na het dichten van het lek te wissen.
- Ons voldoende informatie te geven (bijvoorbeeld een uitgebreide beschrijving inclusief IP-adressen, logs, hoe te reproduceren, screenshots, etc.) om het probleem te reproduceren zodat wij het zo snel mogelijk kunnen behandelen.
- Te wachten met eventuele publicaties over de bevindingen totdat CJG Rijnmond je schriftelijke toestemming geeft.

Wij beloven je dat:

- Wij binnen veertien werkdagen reageren op jouw melding met onze beoordeling van de melding en een verwachte datum voor een oplossing.
- Wij jouw melding vertrouwelijk behandelen en je persoonlijke gegevens niet zonder jouw toestemming met derden zullen delen, tenzij dat noodzakelijk is om een wettelijke verplichting na te komen.
- Wij je op de hoogte houden van de voortgang van het oplossen van het probleem
- In de berichtgeving over het gemelde probleem wij, indien je dit wenst, jouw naam zullen vermelden als melder van kwetsbaarheden.
- Wij bieden geen financiële beloning voor meldingen, maar waarderen je inzet voor een veiligere digitale omgeving.

Wij doen geen aangifte zolang je je houdt aan de volgende gedragsregels:

- Je veroorzaakt geen schade. Je constateert de kwetsbaarheid maar exploiteert het niet.
- Je deelt geen data met derden.
- Je meldt de kwetsbaarheid snel en vertrouwelijk. Met snel en vertrouwelijk wordt bedoeld binnen 48 uur en zonder de kwetsbaarheid kenbaar te maken bij andere personen.

Ons doel

Wij ernaar streven om alle ICT-problemen zo snel mogelijk op te lossen en wij worden graag betrokken bij een eventuele publicatie over het probleem nadat het is opgelost.

Wijzigingen

Wij behouden ons het recht voor om dit beleid van tijd tot tijd te herzien. Controleer daarom met enige regelmaat onze website voor de laatste versie van ons Responsible Disclosure.