Coordinated Vulnerability Disclosure procedure gemeente Hollands Kroon

Als gemeente hechten wij veel belang aan de veiligheid van onze informatiesystemen. Ondanks dat wij ons best doen om deze systemen zo goed mogelijk te beveiligen, realiseren wij ons dat geen enkel systeem 100% veilig is en dat door menselijk handelen en/of onvolkomenheden in software, kwetsbaarheden kunnen ontstaan. Wanneer een kwetsbaarheid in één van onze systemen wordt ontdekt, dan vernemen wij dat graag. We ondernemen dan stappen om de kwetsbaarheid te verhelpen. Door melding te maken van een kwetsbaarheid, verklaart u akkoord te zijn met onderstaande afspraken en zal de gemeente uw melding volgens onderstaande afspraken behandelen.

Als u een kwetsbaarheid in ons systeem ontdekt vragen wij u:

1. Mail uw bevindingen naar security@hollandskroon.nl. Of gebruik het contactformulier dat op onze website staat. https://www.hollandskroon.nl/contact

2. Geef voldoende informatie om de kwetsbaarheid te kunnen reproduceren, zodat we deze zo snel mogelijk kunnen testen. Meestal zal een IP-adres of URL van het kwetsbare systeem voldoende zijn maar bij complexe kwetsbaarheden kan meer informatie benodigd zijn.

3. Als u tips heeft om de kwetsbaarheid op te lossen dan stellen wij die uiteraard op prijs. Beperkt u zich hierbij vooral tot de feitelijkheden die rechtstreeks betrekking hebben op de kwetsbaarheid.

4. Laat uw contactgegevens achter om eventueel nadere informatie op te kunnen vragen en/of samen te kunnen werken om tot een veilige oplossing te komen. Laat minimaal een email adres of telefoonnummer achter.

5. Dien de melding zo snel als redelijkerwijs mogelijk in na ontdekking van de kwetsbaarheid.

Het volgende is uitdrukkelijk niet toegestaan:

1. Het plaatsen van malware op onze systemen of die van derden.

2. Via “brute force” toegang te verkrijgen tot systemen, tenzij dit strikt noodzakelijk is om aan te tonen dat de beveiliging van het systeem hier ernstig tekortschiet. Hiermee bedoelen we dat het buitengewoon eenvoudig is om met openbaar verkrijgbare en/of betaalbare hardware en software een wachtwoord of systeem te kraken is en zodoende het systeem binnen te dringen.

3. Het gebruik maken van social engineering, tenzij om aan te tonen dat medewerkers met toegang tot gevoelige gegevens ernstig tekortschieten in hun plicht om daarmee zorgvuldig om te gaan. Dat wil zeggen als het op overigens volkomen legale wijze (dus niet via chantage of iets dergelijks) in het algemeen te eenvoudig is om hen over te halen tot het verstrekken van dergelijke gegevens aan onbevoegden. U dient daarbij alle zorg te betrachten die redelijkerwijs van u verwacht kan worden om de betreffende medewerkers zelf niet te schaden. Uw bevindingen dienen uitsluitend te zijn gericht op het aantonen van kennelijke gebreken in de procedures en werkwijze binnen gemeente Hollands Kroon en niet op het schaden van individuele personen die bij de gemeente werkzaam zijn.

4. Het openbaar maken of derde partijen inlichten over de kwetsbaarheid voordat deze is verholpen.

5. Het verrichten van handelingen die verder gaan dan strikt noodzakelijk om de kwetsbaarheid aan te tonen en te melden. Dit geldt in het bijzonder als u bij het aantonen van de kwetsbaarheid toegang heeft verkregen tot persoonsgegevens of gegevens waarvan u redelijkerwijs had kunnen begrijpen dat deze vertrouwelijk zijn. Een screenshot van een deel van een database is net zo overtuigend als een kopie van de hele database. Het wijzigen of verwijderen van gegevens is nooit toegestaan.

6. De beschikbaarheid of bruikbaarheid van een systeem verminderen (denial of service aanvallen, bijvoorbeeld).

7. Op enige wijze misbruik maken van de kwetsbaarheid.

Wat mag u van ons verwachten:

1. Als u aan alle gestelde voorwaarden voldoet, zullen wij geen strafrechtelijke aangifte tegen u doen en ook geen civielrechtelijke procedure tegen u starten.

2. Als blijkt dat u toch een van bovenstaande voorwaarden heeft geschonden, kunnen wij alsnog besluiten om juridische stappen tegen u te ondernemen.

3. Wij behandelen iedere melding vertrouwelijk en zullen de persoonlijke gegevens van een melder niet delen met derden zonder toestemming, tenzij wij daar door de wet of een gerechtelijke uitspraak toe verplicht zijn.

4. Wij delen een ontvangen melding altijd met de Informatiebeveiligingsdienst voor gemeenten (IBD). Zo borgen wij dat gemeenten hun informatie op dit vlak met elkaar delen.

5. In onderling overleg kunnen we u vermelden als ontdekker van de kwetsbaarheid. Dit gebeurt uitsluitend met uw toestemming. In alle andere gevallen blijft u anoniem.

6. Wij sturen u binnen één werkdag een (geautomatiseerde) ontvangstbevestiging.

7. Wij reageren binnen 5 werkdagen op een melding met een eerste beoordeling en eventueel een verwachte datum voor een oplossing.

8. Wij lossen de door u gemelde kwetsbaarheid zo spoedig mogelijk op. Daarbij zullen we ernaar streven om u zo goed mogelijk op de hoogte te houden van de voortgang en niet langer dan 90 dagen te doen over het oplossen van de kwetsbaarheid. Wij zijn daarbij echter vaak afhankelijk van leveranciers van de door ons gebruikte producten.

9. In onderling overleg kan bepaald worden of en hoe over de gemelde kwetsbaarheid wordt gepubliceerd, echter altijd nadat het probleem is opgelost.