Coordinated Vulnerability Disclosure

Bij de gemeente Zoetermeer hechten wij veel belang aan de beveiliging van onze systemen. Ondanks alle voorzorgsmaatregelen blijft het mogelijk dat een zwakke plek in de systemen te vinden is. Als u een zwakke plek in één van onze systemen ontdekt, dan horen wij dit graag. Wij kunnen dan snel gepaste maatregelen treffen. Door het maken van een melding verklaart u zich als melder akkoord met onderstaande afspraken over de Coordinated Vulnerability Disclosure. Wij zullen uw melding conform onderstaande afspraken afhandelen.

Wij vragen het volgende van u:

Ga naar de website www.zoetermeer.nl/datalek en vul het online formulier in.

Houd hierbij rekening met de volgende punten:

- Geef voldoende informatie om het probleem te reproduceren, zodat we het zo snel mogelijk kunnen oplossen. Denk hierbij aan een beschrijving van wat u heeft gedaan, welke tools u heeft gebruikt, het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid.
- Wij houden ons aanbevolen voor tips die ons helpen het probleem op te lossen. Beperkt u zich daarbij wel graag tot verifieerbare feitelijkheden die betrekking hebben op de door u geconstateerde kwetsbaarheid en vermijd dat uw advies neerkomt op reclame voor specifieke (beveiligings-)producten.
- Dien de melding zo snel mogelijk in na ontdekking van de kwetsbaarheid.

De volgende handelingen zijn niet toegestaan:

- Het plaatsen van malware, noch op onze systemen noch op die van anderen.
- Het zogeheten ‘bruteforcen’ van toegang tot systemen.
- Het gebruik maken van technieken waarmee de beschikbaarheid en/of bruikbaarheid van het systeem of services wordt verminderd (DoS-aanvallen).
- Het gebruik maken van social engineering of grootschalige phishing. Behalve voor zover dat strikt noodzakelijk is om aan te tonen dat medewerkers met toegang tot gevoelige gegevens in het algemeen (ernstig) tekortschieten in hun plicht om daar zorgvuldig mee om te gaan. Uw bevindingen dienen uitsluitend te zijn gericht op het aantonen van kennelijke gebreken in de procedures en werkwijze binnen de gemeente en niet op het schaden van individuele personen die bij de gemeente werkzaam zijn.
- Het openbaar maken of aan derden verstrekken van informatie over het beveiligingsprobleem voordat het probleem is opgelost.
- Het verrichten van handelingen die verder gaan dan wat strikt noodzakelijk is om het beveiligingsprobleem aan te tonen en te melden. In het bijzonder waar het gaat om het verwerken (waaronder het inzien of kopiëren) van vertrouwelijke gegevens waar u door de kwetsbaarheid toegang toe heeft gehad. In plaats van een complete database te kopiëren, kunt u normaliter volstaan met bijvoorbeeld een directory listing. Het wijzigen of verwijderen van gegevens in het systeem is nooit toegestaan.
- Het op wat voor (andere) wijze dan ook misbruik maken van de kwetsbaarheid of de verkregen gegevens.

Wat u mag verwachten:

Indien u aan alle bovenstaande voorwaarden voldoet, zullen wij geen strafrechtelijke aangifte tegen u doen en ook geen civielrechtelijke zaak tegen u aanspannen.

- Wij behandelen een melding vertrouwelijk en delen persoonlijke gegevens van een melder niet zonder diens toestemming met derden, tenzij wij daar volgens de wet of een rechterlijke uitspraak toe verplicht zijn.
- Wij delen de ontvangen melding altijd geanonimiseerd met de Informatiebeveiligingsdienst voor gemeenten (IBD). Zo borgen wij dat gemeenten ervaringen op dit vlak met elkaar delen.
- In onderling overleg kunnen we, als u dit wenst, uw naam vermelden als de ontdekker van de gemelde kwetsbaarheid. In alle andere gevallen blijft u anoniem.
- Wij sturen u binnen 1 werkdag een (automatische) ontvangstbevestiging.
- Wij reageren binnen 5 werkdagen op een melding met een (eerste) beoordeling van de melding en eventueel een verwachte datum voor een oplossing.
- Wij lossen het door u gemelde beveiligingsprobleem zo snel mogelijk op. Daarbij streven we ernaar om u goed op de hoogte te houden van de voortgang en nooit langer dan 90 dagen te doen over het oplossen van het probleem. Wij zijn daarbij vaak wel mede afhankelijk van toeleveranciers.
- In onderling overleg bepalen we of en op welke wijze over het probleem wordt gepubliceerd, nadat het is opgelost.
- Wij kunnen u een beloning bieden als dank voor de hulp. Afhankelijk van de ernst van het beveiligingsprobleem en de kwaliteit van de melding, kan die beloning variëren van een eenvoudig ‘dankjewel’ tot een bedrag van maximaal 250 euro, of een vermelding van uw aandeel in het melden en oplossen van het probleem. Het moet hierbij dan wel gaan om een nog onbekend en serieus beveiligingsprobleem.