Beleid Responsible Disclosure

Inhoud

1. Beleidsuitgangspunt

De gemeente Someren hanteert de onderstaande beleidsuitgangspunt dat ontleend is aan de Baseline Informatiebeveiliging Overheid (BIO).

- De gemeente Someren hecht veel belang aan de beveiliging van haar systemen. Ondanks alle voorzorgsmaatregelen blijft het mogelijk dat er een zwakke plek in de systemen te vinden is. Wanneer een zwakke plek in een van onze systemen wordt ontdekt, vernemen wij dit graag, zodat wij snel gepaste maatregelen kunnen nemen.

2. Wat wij van u vragen?

Door het maken van een melding verklaart u zich als melder akkoord met onderstaande afspraken over Responsible Disclosure en zal de gemeente Someren uw melding conform onderstaande afspraken afhandelen.

Wij vragen het volgende van u:

- Mail uw bevindingen naar gemeente@someren.nl. Versleutel de bevindingen indien mogelijk om te voorkomen dat de informatie in verkeerde handen valt.
- Geef voldoende informatie om het probleem te reproduceren, zodat we het zo snel mogelijk kunnen oplossen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.
- 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 in feite neerkomt op reclame voor specifieke (beveiligings)producten.
- Laat contactgegevens achter zodat we met u in contact kunnen treden om samen te werken aan een veilig resultaat. Laat minimaal één e-mailadres of telefoonnummer achter.
- Dien de melding zo snel mogelijk in na ontdekking van de kwetsbaarheid.

a. Waaraan moet u voldoen?

De volgende handelingen zijn niet toegestaan:

- Het plaatsen van malware, noch op onze systemen noch op die van anderen.
- Het zogeheten *brute forcen* van toegang tot systemen, behalve voor zover dat strikt noodzakelijk is om aan te tonen dat de beveiliging op dit vlak ernstig tekortschiet. Dat wil zeggen als het buitengewoon eenvoudig is om met openbaar verkrijgbare en goed

betaalbare hardware en software een wachtwoord te kraken waarmee het systeem ernstig kan worden gecompromitteerd.

- Het gebruik maken van social engineering, 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. 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 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 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 gebruik maken van technieken waarmee de beschikbaarheid en/of bruikbaarheid van het systeem of services wordt verminderd (DDoS-aanvallen).
- Het op wat voor (andere) wijze dan ook misbruik maken van de kwetsbaarheid.
- Het bewerkstelligen van enig ander voordeel, financieel of anderszins.

Het niet voldoen aan bovenstaande gedragsregels kan ertoe leiden dat wij aangifte doen bij de politie van computervredebreuk, op basis van artikel 138AB wetboek van Strafrecht, dat luidt:

Lid 1

Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk en wederrechtelijk binnendringt in een geautomatiseerd werk of in een deel daarvan. Van binnendringen is in ieder geval sprake indien de toegang tot het werk wordt verworven:

door het doorbreken van een beveiliging, of door een technische ingreep, of met behulp van valse signalen of een valse sleutel, of door het aannemen van een valse hoedanigheid.

Lid 2

Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk, indien de dader vervolgens gegevens die zijn opgeslagen, worden verwerkt of overgedragen door middel van het geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, voor zichzelf of een ander overneemt, aftapt of opneemt.

Lid 3

Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk gepleegd door tussenkomst van een openbaar telecommunicatienetwerk, indien de dader vervolgens met het oogmerk zichzelf of een ander wederrechtelijk te bevoordelen gebruik maakt van verwerkingscapaciteit van een geautomatiseerd werk; door tussenkomst van het geautomatiseerd werk waarin hij is binnengedrongen de toegang verwerft tot het geautomatiseerd werk van een derde.

b. Wat mag u van ons verwachten?

- Indien u aan alle bovenstaande voorwaarden voldoet, zal de gemeente Someren geen strafrechtelijke aangifte tegen de melder doen en ook geen civielrechtelijke zaak 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 met de Informatiebeveiligingsdienst voor gemeenten (de CERT voor de gemeentelijke overheid). Zo borgen wij dat gemeenten hun ervaringen op dit vlak met elkaar delen.
- In onderling overleg kunnen we, indien de melder dit wenst, uw naam vermelden als de ontdekker van de gemelde kwetsbaarheid. In alle andere gevallen blijft de melder anoniem.
- Wij sturen u binnen een werkdag een (automatische) ontvangstbevestiging.
- Wij reageren binnen drie werkdagen op een melding met een (eerste) beoordeling van de melding en eventueel met een verwachte datum voor een oplossing.
- Wij lossen het gemelde beveiligingsprobleem zo snel mogelijk op. Daarbij streven we ernaar om de melder 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 kan worden bepaald of en op welke wijze over het probleem wordt gepubliceerd, nadat het is opgelost.

3. Vaststelling

Dit beleid treedt in werking na vaststelling door het College van B&W.

Aldus vastgesteld door het College van B&W van de gemeente Someren op 22 februari 2022.

Burgemeester en wethouders van Someren,

de secretaris,	de burgemeester,
J. Koppers-Van der Krabben	D. Blok