Responsible disclosure

De gemeente ’s-Hertogenbosch neemt uitgebreide maatregelen om zijn computersystemen goed te beveiligen. Toch kunnen ook onze systemen (een) zwakke plek(ken) hebben. Wanneer u een zwakke plek in één van onze systemen ontdekt, vernemen wij dit graag van u. Wij kunnen dan snel gepaste maatregelen nemen. Door het maken van de melding van een zwakke plek verklaart de melder zich akkoord met onderstaande afspraken over responsible disclosure. De gemeente ’s-Hertogenbosch handelt uw melding dan volgens onderstaande afspraken af.

Wij vragen het volgende van u:

- Mail uw bevindingen naar informatieveiligheid@s-hertogenbosch.nl. Versleutel de bevindingen als dat mogelijk is met PGP 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 uw 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 a.u.b. 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 social engineering, behalve voor zover dat strikt noodzakelijk is om aan te tonen dat medewerkers met toegang tot gevoelige gegevens in het algemeen (ernstig) tekort schieten in hun plicht om daar zorgvuldig mee om te gaan. Dat wil zeggen dat het, op volkomen legale wijze (dus niet via chantage of iets dergelijks), in het algemeen te eenvoudig is 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 openbaar maken of aan derden verstrekken van gegevens met een vertrouwelijk karakter, zoals privacygevoelige gegevens.
- Het gebruik maken van technieken waarmee de beschikbaarheid en/of bruikbaarheid van het systeem of services wordt verminderd (DoS-aanvallen).
- Het op wat voor (andere) wijze dan ook misbruik maken van de kwetsbaarheid.

Wat u mag verwachten:

- Wanneer u aan alle bovenstaande voorwaarden voldoet, doen wij geen strafrechtelijke aangifte tegen u en spannen we ook geen civielrechtelijke zaak tegen u aan.
- Als blijkt dat u zich niet aan een van de voorwaardes hebt gehouden, kunnen wij alsnog besluiten om gerechtelijke stappen tegen u te ondernemen. 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 reageren binnen 3 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.

In onderling overleg kan worden bepaald of en op welke wijze over het probleem wordt gepubliceerd, nadat het is opgelost.