INFORMATIE
BEVEILIGINGS
DIENST

RESPONSIBLE DISCLOSURE

Een van de producten van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN **IN OPDRACHT VAN**
VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE
BEVEILIGINGS
DIENST

Colofon

Naam document
Responsible Disclosure

Versienummer
1.0

Versiedatum
Februari 2014

Versiebeheer
Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

Met dank aan
De expertgroep en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product.

In samenwerking met
De producten van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) worden vervaardigd in samenwerking met:

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Voorwoord

De IBD is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING) en actief sinds 1 januari 2013. Aanleiding voor de oprichting van de IBD vormen enerzijds de leerpunten uit een aantal grote incidenten op informatiebeveiligingsvlak en anderzijds de visie Digitale Overheid 2017.
De IBD is er voor alle gemeenten en richt zich op bewustwording en concrete ondersteuning om gemeenten te helpen hun informatiebeveiliging naar een hoger plan te tillen.

De IBD heeft drie doelen:

1. het preventief en structureel ondersteunen van gemeenten bij het opbouwen en onderhouden van bewustzijn als het gaat om informatiebeveiliging.
2. het leveren van integrale coördinatie en concrete ondersteuning op gemeente specifieke aspecten in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging.
3. het bieden van gerichte projectmatige ondersteuning op deelgebieden om informatiebeveiliging in de praktijk van alle dag naar een hoger plan te tillen. De ondersteuning die de IBD biedt bij het ICT-Beveiligingsassessment DigiD is een voorbeeld van zo'n project.

Hoe realiseert de IBD haar doelen?
Om invulling te kunnen geven aan haar doelen is door de IBD op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR) een vertaalslag gemaakt naar een baseline voor de gemeentelijke markt. Deze Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) betreft twee varianten, een Strategische- én een Tactische Baseline. Beide varianten van de BIG zijn beschikbaar voor alle gemeenten op de community van de IBD, zodat door iedere gemeente tot implementatie van de BIG kan worden overgegaan. Bestuur en management hebben met deze baseline een instrument in handen waarmee zij in staat zijn om te meten of de organisatie 'in control' is op het gebied van informatiebeveiliging. Om de implementatie van de Strategische en Tactische Baseline te ondersteunen, zijn door de IBD in samenwerking met de Taskforce Bestuur en Informatieveiligheid Dienstverlening producten ontwikkeld op operationeel niveau. Dit heeft een productenportfolio opgeleverd, genaamd de Operationele Baseline Nederlandse Gemeenten. Onderhavig product is onderdeel van het productenportfolio.

Naast een productenportfolio, heeft de IBD voor gemeenten ook een dienstenportfolio ontwikkeld. Voor een volledig overzicht van het producten- en dienstenportfolio, kunt u terecht op de website van de IBD.

De gemeente is zelf verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van de regels. Hierbij geldt:

- Er is wetgeving waar altijd aan voldaan moet worden, zoals niet uitputtend: GBA, SUWI, BAG en PUN, maar ook de archiefwet.
- Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
- De gemeente stelt dit normenkader vast, waarbij er in de naleving van dat kader ruimte is voor afweging en prioritering op basis van het 'pas toe of leg uit' principe.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Leeswijzer

Dit product maakt onderdeel uit van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Doel
In de ICT-wereld bestaan meerdere praktijken om kwetsbaarheden in ICT bekend te maken. Responsible Disclosure binnen de ICT-wereld is het op een verantwoorde wijze, en in gezamenlijkheid tussen melder en organisatie, openbaar maken van ICT-kwetsbaarheden op basis van een, door organisaties hiervoor, vastgesteld beleid voor Responsible Disclosure.
Dit document geeft een template weer voor het beleid op het vlak van Responsible Disclosure, waarin een aantal aspecten standaard is opgenomen, zoals bijvoorbeeld het delen van de meldingen met de IBD. In de bijlage treft u een voorbeeld voor de invullig van de template.

Doelgroep
Dit document is van belang voor het bestuur en het management van de gemeente.

Relatie met overige producten
- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
  - Strategische variant van de Baseline Informatiebeveiliging voor Gemeenten
  - Tactische variant van de Baseline Informatiebeveiliging voor Gemeenten
- Het voorbeeld Incident management en responsebeleid van de operationele baseline.

Maatregelen tactische variant Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
BIG Maatregel 10.8.2.2: Verantwoordelijkheid en aansprakelijkheid in het geval van informatiebeveiligingsincidenten zijn beschreven, alsmede procedures over melding van incidenten.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Inhoud

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN
VERENIGING VAN NEDERLANDSE GEMEENTEN

1 Inleiding

In de ICT-wereld bestaan meerdere praktijken om kwetsbaarheden in ICT bekend te maken. Responsible Disclosure binnen de ICT-wereld is het op een verantwoorde wijze, en in gezamenlijkheid tussen melder en de gemeente, openbaar maken van ICT-kwetsbaarheden op basis van een door de gemeente hiervoor vastgesteld beleid voor Responsible Disclosure.
Dit document is een template voor het beleid op het vlak van Resonsible Disclosure, waarin een aantal aspecten standaard is opgenomen, zoals bijvoorbeeld het delen van de meldingen met de IBD. In de bijlage treft u een voorbeeld voor de invullig van de template. Daar waar dit beleid wordt gepubliceerd op de website van de gemeente dient u ook een invulformulier voor het melden van een kwetsbaarheid ter beschikking te stellen. Een standaard tekst op het invulformulier is dan dat de Melder akkoord gaat met het Responsible Disclosure beleid.

1.1 Doel van Responsible Disclosure

Het doel van Responsible Disclosure is het bijdragen aan de veiligheid van ICT-systemen en het beheersen van de kwetsbaarheid van ICT-systemen door deze kwetsbaarheden op verantwoorde wijze te kunnen melden aan de gemeente en deze meldingen zorgvuldig door de gemeente te laten afhandelen. Op deze manier kan schade zo veel als mogelijk worden voorkomen of beperkt. Hierbij dient dan door de melder voldoende tijd voor herstel beschikbaar gesteld te worden alvorens door de melder of de gemeente tot openbaarmaking wordt overgegaan.

Centraal bij het werken met Responsible Disclosure staat het verhelpen van de kwetsbaarheid en het verhogen van de veiligheid van informatiesystemen. Bij Responsible Disclosure staat voorop dat partijen zich over en weer houden aan afspraken over het melden van de kwetsbaarheid en de omgang hiermee. Een partij die een Responsible Disclosure Policy vaststelt, kan zich bijvoorbeeld binden aan het principe om geen aangifte te doen als aan de, volgens het beleid geldende, spelregels wordt voldaan. In de praktijk van Responsible Disclosure zijn primair de melder en de gemeente, die eigenaar/beheerder van het systeem is, betrokken. Het is van belang om zo min mogelijk schakels te hebben tussen de persoon die de kwetsbaarheid meldt en de gemeente die verantwoordelijk is voor het oplossen van het probleem. De melder en de gemeente kunnen echter gezamenlijk besluiten om de Informatiebeveiligingsdienst voor gemeenten (IBD) of andere partijen binnen de ICT Security Community in te lichten over de kwetsbaarheid. Zeker bij een nog niet bekende kwetsbaarheid, om ook elders (vervolg)schade te voorkomen of te beperken.

2 Uitgangspunt

Het uitgangspunt is om voor gemeenten een template aan te leveren voor het beleid op het vlak van Responsible Disclosure, waarin een aantal aspecten standaard is opgenomen, zoals bijvoorbeeld het delen van de meldingen met de IBD.
In de bijlage staat een voorbeeld Responsible Disclosure Policy van een fictieve gemeente, als aanvulling op de leidraad Responsible Disclosure die het Nationaal Cyber Security Centrum (NCSC) heeft gepubliceerd. Voor het gebruik van deze tekst zal in elk geval, het e-mailadres en de bijbehorende versleutelingsmethode aangepast moeten worden, en een keuze moeten worden gemaakt in de blauwe stukken tekst.
Voor de vindbaarheid is het aan te raden om de tekst op een standaard locatie te plaatsen (www.website.nl/security).

2.1 Wat moet de gemeente doen om Responsible Disclosure in te richten

Om responsible disclosure te laten werken moet de gemeente de volgende stappen zetten:

1. De gemeente moet het eens zijn dat men Responsible Disclosure wil toepassen.
2. De gemeente moet het voorbeeldbeleid uit dit document aanpassen naar de eisen en wensen van de gemeente, en met name aandacht hebben voor:
   a. Waar kan de melding binnenkomen, en wie onderneemt dan actie Benoem een persoon of gebruik een algemene mailbox voor het kunnen ontvangen van meldingen.
   b. Besluiten of men een eventuele beloning wil geven, en indien noodzakelijk, het benodigde financiele proces inregelen.
   c. De afhandeling en bewaking van de melding binnen de gemeente. Bij voorkeur laat men binnen de gemeente ontvangen meldingen oppakken binnen het Incident Management proces van de ICT-afdeling. Dit proces is er al en het is gericht op het oplossen van gemelde incidenten. Zorg er wel voor dat Responsible Disclosure meldingen goed worden opgevolgd en geef deze meldingen apart de vereiste aandacht.
   d. De bewaking van de mogelijk gewenste privacy waarborgen. Indien de melder anoniem wil blijven dient de gemeente ook te waarborgen dat dit zo blijft, er is niets zo schadelijk als er privacy beloofd wordt en deze niet wordt nagekomen.
   e. Test het ontvangen, bewaken en afhandelen van meldingen voordat het beleid gepubliceerd wordt.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Bijlage 1: Tekstvoorstel Responsible Disclosure gemeentelijke website

Responsible Disclosure

Onze gemeente <gemeentenaam> hecht veel belang aan de beveiliging van haar systemen. Ondanks alle voorzorgsmaatregelen blijft het mogelijk dat een zwakke plek in de systemen te vinden is. Wanneer u een zwakke plek in één van onze systemen ontdekt, vernemen wij dit graag van u, zodat wij snel gepaste maatregelen kunnen nemen. Door het maken van een melding verklaart u zich als melder akkoord met onderstaande afspraken over Responsible Disclosure en zal gemeente <gemeentenaam> uw melding conform onderstaande afspraken afhandelen.

Wij vragen het volgende van u:

- Mail uw bevindingen naar <e-mailadres>. Versleutel de bevindingen indien mogelijk met <versleutelingsmethodiek> 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.
- Contactgegevens achter te laten 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 <u>niet</u> toegestaan:

- Het plaatsen van malware, noch op onze systemen noch op die van anderen.
- Het zogeheten “bruteforcen” van toegang tot systemen <, behalve voor zover dat strikt noodzakelijk is om aan te tonen dat de beveiliging op dit vlak ernstig tekort schiet, 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) tekort schieten 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 (DoS-aanvallen).
- Het op wat voor (andere) wijze dan ook misbruik maken van de kwetsbaarheid.

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.
- Als blijkt dat u een bovenstaande voorwaarde toch heeft geschonden, 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 delen de ontvangen melding altijd met de Informatiebeveiligingsdienst voor gemeenten (IBD). Zo borgen wij dat gemeenten hun ervaringen op dit vlak met elkaar delen.
- In onderling overleg kunnen we, indien 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 <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. 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 kan worden bepaald 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 <300> euro. Het moet hierbij wel gaan om een nog onbekend en serieus beveiligingsprobleem.

INFORMATIE BEVEILIGINGS DIENST

INFORMATIEBEVEILIGINGSDIENST
V00R GEMEENTEN (IBD)

NASSAULAAN 12
2514 JS DEN HAAG

POSTBUS 30435
2500 GK DEN HAAG

HELPDESK 070 373 80 11
ALGEMEEN 070 373 80 08
FAX 070 363 56 82

IBD@KINGGEMEENTEN.NL
WWW.KINGGEMEENTEN.NL

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN **IN OPDRACHT VAN**
VERENIGING VAN NEDERLANDSE GEMEENTEN