Bestuur

Controlling

bezoekadres:
Stationsplein 1
2611 BV Delft
IBAN NL21 BNGH 0285 0017 87
t.n.v. gemeente Delft

Behandeld door
mw. H. Koenen
hkoenen@delft.nl
Internet www.delft.nl
Telefoon 14015

Gemeente Delft

Retouradres : Postbus 78, 2600 ME Delft

De gemeenteraad

VERZONDEN 14 FEB. 2019

Datum
12-02-2019
Ons kenmerk
3871098
Uw brief van

Uw kenmerk

Bijlage

Onderwerp
Responsible disclosure

Geachte leden van de raad,

Bij de behandeling van het rapport van de Delftse Rekenkamer over Informatiebeveiliging binnen de gemeente Delft in de raadscommissie EFB (4-10-2018) heeft de fractie van STIP voorgesteld om een procedure voor Responsible Disclosure te introduceren voor het digitale verkeer van de gemeente Delft.
Wethouder Huijsmans heeft in die commissievergadering geantwoord hier positief tegenover te staan en heeft toegezegd met een voorstel te komen (toezegging 2018-09). Bij deze wordt het voorstel aan u voorgelegd.
Wij gaan er van uit dat genoemde toezegging daarmee is afgedaan.

Hoogachtend,
het college van burgemeester en wethouders van Delft,

, burgemeester
J.M. van Bijsterveldt-Vliegenthart

, secretaris
dr. M. Berger, l.s.

3872277

Bestuur

Controlling

Doorkiesnummers:
Telefoon 0653634195

Aan
college van burgemeester en wethouders

Van
mw. H. Koenen CISO
Afschrift aan

Memo

Datum
06-02-2019
Opsteller
Hanneke Koenen / Roel van der Valk
Bijlage

Onderwerp

Responsible Disclosure

Geacht College,

Bij de behandeling van het rapport van de Delftse Rekenkamer over Informatiebeveiliging binnen de gemeente Delft in de raadscommissie EFB (4-10-2018) heeft de fractie van STIP voorgesteld om een procedure voor Responsible Disclosure te introduceren voor het digitale verkeer van de gemeente Delft. Wethouder Huijsmans heeft in die commissievergadering geantwoord hier positief tegenover te staan en heeft toegezegd met een voorstel te komen (toezegging 2018-09). Bij deze wordt het voorstel aan u voorgelegd.

Wat is Responsible Disclosure?
In de normale situatie is het verboden om de gemeentelijke digitale infrastructuur aan te vallen door middel van hacken. Een inbraak op het gemeentelijke netwerk wordt gezien als computervredebreuk en is strafbaar.
Bij de zogenaamde penetratietesten door ethische hackers, zoals bijvoorbeeld door de Delftse Rekenkamer zijn uitgevoerd, wordt aan de hackers vrijwaring verleend voor het inbreken, mits dat geschiedt binnen de afgesproken kaders.
Bij Responsible Disclosure wordt aan iedere goedbedoelende (ethische) hacker vrijwaring verleend voor een inbraak op het gemeentelijk netwerk van buitenaf, mits voldaan wordt aan bepaalde voorwaarden en de gevonden kwetsbaarheden onmiddellijk aan de gemeente worden gemeld. De gemeente kan deze kwetsbaarheden dan snel oplossen. Op die manier kan een goede relatie met ethische hackers leiden tot een veiliger omgeving voor Delft en alle inwoners die gebruik willen maken van de diensten van de Gemeente Delft.

Aanpak
Voor het formuleren van voorwaarden en andere spelregels rondom Responsible Disclosure zal gebruik gemaakt worden van een standaard modelaanpak, beschikbaar op https://responsibledisclosure.nl/ . Deze

aanpak die is uitgewerkt door Ricky Gevers, Fox IT en Deloitte. Deze wordt ook gebruikt op www.ibdgemeente.nl en op gemeente Den Haag https://www.denhaag.nl/nl/algemeen/responsible-disclosure.htm en Gemeente Rotterdam https://www.rotterdam.nl/bestuur-organisatie/responsible-disclosure/ .

Voor de hacker gelden de volgende voorwaarden en spelregels:

- de gevonden kwetsbaarheid aan gemeente Delft te melden via: incident@delft.nl
- niet op onevenredige wijze te handelen en de gevonden kwetsbaarheid niet te misbruiken (zie de bijlage voor meer uitleg)
- niet meer data te downloaden dan nodig is om het lek aan te tonen.
- zorgvuldig om te gaan met gegevens van derden door deze gegevens niet in te kijken, te verwijderen of aan te passen.
- informatie over de kwetsbaarheid niet met anderen te delen en zo snel mogelijk te wissen
- gemeente Delft voldoende informatie te geven om de kwetsbaarheid te reproduceren en de tijd te geven om de kwetsbaarheid te onderzoeken en te verhelpen

De gemeente zal:

- binnen vijf werkdagen reageren op de melding met beoordeling van de melding en de verwachte oplossingsdatum.
- geen strafrechtelijke stappen tegen de hacker ondernemen als deze zich aan bovenstaande voorwaarden houdt.
- de melding vertrouwelijk behandelen en persoonlijke gegevens van de hacker niet zonder zijn of haar toestemming met derden delen, tenzij dat wettelijk gezien of door een gerechtelijke uitspraak nodig is.
- de hacker op de hoogte houden van de voortgang van de oplossing van de kwetsbaarheid
- een beloning verstrekken aan de eerste melder van een kwetsbaarheid.

De gemeente kan een beloning bieden als dank voor de hulp, afhankelijk van de ernst van het lek, of het lek eerder is gemeld, de kwaliteit van de melding, te beoordelen per melding. De beloning kan bestaan uit een T-shirt of een mok, géén geldelijke beloning (zogenaamde bug bounty). Vervolg melders van hetzelfde issue krijgen geen beloning, tenzij hier een bijzondere situatie aan de hand is.

In de bijlage is het volledig overzicht opgenomen van voorwaarden en spelregels.

De aanpak geldt alleen voor de gemeente Delft en wordt gepubliceerd op de website van de gemeente Delft https://www.delft.nl.

Uitvoering
Wanneer het college heeft ingestemd met het voorstel, kan de invoering worden voorbereid. Het Responsible Disclosure beleid van de gemeente wordt op de website geplaatst (zie bijlage voor de te plaatsen tekst).

Het is de bedoeling om in maart 2019 te starten met Responsible Disclosure. Onderzocht wordt nog of het haalbaar is om ter gelegenheid van de start een mini-hackaton te organiseren met studenten en scholieren.

Kosten
De kosten bestaan uit een beloning en uit het afhandelen van meldingen die binnenkomen. Het is vooraf niet exact in te schatten hoeveel meldingen per jaar zullen binnenkomen. Uit onderzoek bij vergelijkbare gemeenten en de "hall of fame" bij de IBD (www.informatiebeveiligingsdienst.nl), lijkt het erop dat er met ongeveer 15 bevindingen (eerste meldingen) per jaar rekening gehouden moet worden.

De kosten voor de beloning (mok of t-shirt) worden bij 15 bevindingen geraamd op € 375, te dekken uit bestaand IT-budget.
De kosten van interne afhandeling bedragen naar schatting € 2400 voor 15 meldingen (gemiddeld). In het lopende pilotjaar zullen de exacte kosten worden bijgehouden. Deze kosten komen ten laste van het bestaande IT-budget.
Deze dienst wordt ook door bedrijven aangeboden. Bij vergelijking blijkt de afhandeling door een bedrijf met € 12.000 per jaar beduidend duurder te zijn.
Bij 15 meldingen per jaar is het bedrijfseconomisch meest voordelig om zelf de Responsible Disclosure uit te voeren. Indien het aantal meldingen een structurele trend laat zien en stijgt naar 75 meldingen per jaar of meer, loont het om een commerciële dienst in te schakelen.

Voorstel voor besluitvorming

1. In te stemmen met de voorgestelde aanpak voor Responsible Disclosure
2. Over de ervaringen te laten rapporteren bij de halfjaarlijkse rapportages over informatiebeveiliging en na een jaar de aanpak te evalueren
3. De raadscommissie voor EFB te informeren over de aanpak door middel van bijgaande brief. De toezegging van de wethouder (2018-09) is daarmee afgedaan.

Over Responsible Disclosure

De gemeente hecht veel belang aan de beveiliging van zijn ICT-systemen. Ondanks alle voorzorgmaatregelen blijft het mogelijk dat er een zwakke plek in de systemen te vinden is. Mocht u een zwakke plek in één van onze systemen vinden, dan horen wij dat graag van U door middel van een melding. Wij nemen dan snel maatregelen om het lek te dichten.

Wij vragen het volgende van U

- Meld de gevonden kwetsbaarheid aan ons via: incident@delft.nl. Indien de gegevens van ernstige of vertrouwelijke aard zijn, kan dit gemeld wordt aan hetzelfde email adres, gebruikmakend van de versleutelde mail service op https://cryptshare.delft.nl
- Dien uw melding zo snel mogelijk na de ontdekking van de kwetsbaarheid in
- Geef ons voldoende informatie om de kwetsbaarheid te reproduceren en de tijd om de kwetsbaarheid te onderzoeken en te verhelpen. 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.
- Laat uw contactgegevens achter, zodat we met u in contact kunnen treden. Minimaal één e-mailadres of telefoonnummer. Melden onder een pseudoniem is mogelijk, mits wij verder met u contact kunnen onderhouden.

De volgende handelingen zijn niet toegestaan

In het algemeen verwachten wij dat U zich passend gedraagt en geen misbruik maakt van de gevonden kwetsbaarheid. De volgende handelingen zijn niet toegestaan:

- Gebruik van social engineering of aanvallen op fysieke beveiliging om zich op die wijze toegang te verschaffen tot het systeem.
- Programmatuur in een informatiesysteem plaatsen om vervolgens daarmee de kwetsbaarheid aan te tonen (malware). Daarmee kan aanvullende schade worden aangericht en worden onnodige veiligheidsrisico's gelopen.
- Gebruik van een gevonden kwetsbaarheid dat verder gaat dan noodzakelijk is om de kwetsbaarheid vast te stellen.
- Gegevens van het systeem te kopiëren, te wijzigen of te verwijderen. Een alternatief hiervoor is het maken van een directory listing of screenshot van een systeem.
- Veranderingen in het systeem aan te brengen.
- Herhaaldelijk toegang tot het systeem te verkrijgen.
- Gebruik te maken van het zogeheten distributed denial of service (dDOS), spam of 'bruteforcen' van toegang tot systemen. Beschikbaarheid en/of bruikbaarheid van systemen moet in stand blijven.
- Meer data downloaden dan nodig is om het lek aan te tonen. Wees zorgvuldig met gegevens van derden door deze gegevens niet in te kijken, te verwijderen of aan te passen.

- Informatie over de kwetsbaarheid met anderen delen. Deel de informatie over de kwetsbaarheid pas nadat wij het lek gedicht hebben en u daarover bericht hebben. Deel geen vertrouwelijke gegevens die u verkregen heeft. Wis de gegevens direct na het dichten van het lek.

Wat wij beloven

- Wij zullen geen strafrechtelijke of civielrechtelijke stappen tegen u ondernemen mits u zich aan bovenstaande voorwaarden houdt. Als blijkt dat u een bovenstaande voorwaarde toch heeft geschonden, kunnen wij alsnog besluiten om gerechtelijke stappen tegen u te ondernemen
- Wij zullen uw melding vertrouwelijk behandelen en uw persoonlijke gegevens niet zonder uw toestemming met derden delen, tenzij dat wettelijk gezien of door een gerechtelijke uitspraak nodig is.
- Wij reageren binnen vijf werkdagen op uw melding met onze beoordeling van uw melding en de verwachte oplossingsdatum.
- We houden u op de hoogte van de voortgang van de oplossing van de kwetsbaarheid. In berichtgeving over de kwetsbaarheid vermelden wij - indien u dat wenst - uw naam als ontdekker.
- Wij kunnen u – als eerste melder van de kwetsbaarheid - een T-shirt of een mok bieden als dank voor uw hulp. Verdere beloning is afhankelijk van de ernst van het lek, of het lek eerder is gemeld, en de kwaliteit van de melding. Dat wordt per melding bepaald.

Publicaties

Gemeente Delft streeft ernaar alle kwetsbaarheden zo snel mogelijk op te lossen. Als U wilt publiceren over de kwetsbaarheid, doe dat dan nadat de kwetsbaarheid is opgelost, Wij zijn graag vooraf betrokken bij deze publicaties.

Dit beleid is geïnspireerd door en deels overgenomen van het voorbeeld op responsibledisclosure.nl.

NB er zal ook een vertaling in het Engels worden gepubliceerd