centrum informatiebeveiliging en privacybescherming

Implementatie Responsible Disclosure

Een handreiking

Juni 2020 [versie 1.0 definitief]

Titel	Implementatie Responsible Disclosure
Datum	Juni 2020
Status	Versie 1.0 Definitief
Opdrachtgever	Centrum Informatiebeveiliging en Privacybescherming
Regime	Becommentarieerde praktijk
Auteurs	Kernteam CIP: V0.99 20-12-2013 Kernteam CIP: V1.0 juni 2020
Reviewers	

Considerans

CIP-producten steunen op kennis van mensen uit verschillende organisaties actief in het CIP-netwerk, zowel uit de overheid als de markt.

Opmerkingen en aanvullingen kun je melden op cip-overheid.nl/contact

Inhoudsopgave

1 Inleiding

1.1 Aanleiding

De dienstverlening van overheidsorganisaties is in sterke mate afhankelijk van het ongestoord functioneren van informatiesystemen. Het verkrijgen van kennis over de kwetsbaarheden in de eigen systemen en het verbeteren van de beveiliging hiervan is daarmee noodzakelijk voor de dagelijkse bedrijfsvoering.

Bij goedwillende 'hackers' bestaat de angst om gevonden kwetsbaarheden rechtstreeks bij een organisatie te melden vanwege mogelijke juridische consequenties. Hierdoor kan het gebeuren dat een kwetsbaarheid niet, indirect of via de media naar buiten gebracht wordt.

Dit is een onwenselijke situatie aangezien de kwetsbaarheid dan te lang blijft bestaan en hier misbruik van gemaakt kan worden. Het is van belang om de organisatie en de 'ethical hackers' bij elkaar te brengen en samen te werken op basis van afspraken. Met goede afspraken hebben alle partijen meer zekerheid over hun positie en kan een bijdrage worden geleverd aan het gezamenlijke doel: het verhogen van de veiligheid van informatiesystemen.

1.2 Leidraad

De minister van Veiligheid en Justitie heeft het Nationaal Cyber Security Centrum gevraagd om met een leidraad voor bovenstaande problematiek te komen. Dit is de 'Leidraad Responsible Disclosure' geworden. Responsible Disclosure betreft het op een verantwoorde wijze melden van ICT-kwetsbaarheden, op basis van een door organisaties vastgesteld kader.

Dank is verschuldigd aan het IPO (InterProvinciaal Overleg), die de basis voor dit beleid leverde.

1.3 Doelstelling

Ondanks alle zorg die aan het beveiligen van de informatiesystemen wordt besteed, kan geen 100% informatieveiligheid worden gegarandeerd. Dit constateren organisaties enerzijds zelf, door periodieke audits en pentesten uit te voeren, en anderzijds komen kwetsbaarheden aan het licht door de bedrijvigheid van hackers, ethical of door een vijandige hack.

CIP wil overheidsorganisaties helpen bij de invoering van Responsible Disclosure door het aanbieden van een template voor het beleid (hoofdstuk 2) en een checklist met acties die in de organisatie geïmplementeerd moeten zijn om het beleid waar te kunnen maken (hoofdstuk 3).

Deze handleiding bestaat dus uit:

- Een template in de vorm van een communicabele tekst, waarmee ethical hackers duidelijkheid krijgen over het kader waarbinnen zij zonder rechtsvervolging kunnen functioneren en dat daarmee de overheidsorganisatie in de gelegenheid stelt haar voordeel te doen met wat ethical hacking kan opleveren;
- Een checklist van zaken die minimaal moeten ingevuld ter implementatie binnen de organisatie, om de toezeggingen aan de ethical hackers na te kunnen komen.

2 Responsible Disclosure – Template

<naam organisatie>

<datum>

<versie>

<naam organisatie> hecht grote waarde aan de veiligheid van onze informatiesystemen. Ondanks onze zorg voor de beveiliging kan het voorkomen dat er toch een kwetsbaarheid is. Als u een kwetsbaarheid in één van onze systemen heeft gevonden horen wij dit graag zodat we zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met u samenwerken om onze informatiesystemen beter te kunnen beschermen.

Wij vragen u:

- Uw bevindingen te mailen naar <e-mailadres>. [Optioneel:] Versleutel de bevindingen indien mogelijk met de aan u daartoe verstrekte sleutel om te voorkomen dat de informatie in verkeerde handen valt.
- Voldoende informatie te geven om het probleem te reproduceren zodat we het zo snel mogelijk kunnen oplossen. Meestal is het IP-adres of de URL van het getroffen informatiesysteem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.
- Contactgegevens achter te laten zodat we met u in contact kunnen treden om samen te werken aan een veilig resultaat. Laat minimaal een e-mailadres of telefoonnummer achter.
- De melding zo snel mogelijk na ontdekking van de kwetsbaarheid te doen.
- De informatie over het beveiligingsprobleem niet met anderen te delen totdat het is opgelost.
- Verantwoordelijk om te gaan met de kennis over het beveiligingsprobleem, door geen handelingen te verrichten die verder gaan dan noodzakelijk voor het aantonen van het beveiligingsprobleem.

Vermijd dus in elk geval de volgende handelingen:

- Het plaatsen van malware.
- Het kopiëren, wijzigen of verwijderen van gegevens in een informatiesysteem (een alternatief hiervoor is het maken van een directory listing van een informatiesysteem).
- Het aanbrengen van veranderingen in het informatiesysteem.
- Het herhaaldelijk toegang tot het informatiesysteem verkrijgen of de toegang delen met anderen.
- Het gebruik maken van het zogeheten "brute forcing" van toegang tot informatiesystemen.
- Het gebruik maken van denial-of-service of social engineering.

Wat u mag verwachten:

- Indien u bij de melding van een door u geconstateerde kwetsbaarheid in een informatiesysteem van <naam organisatie> aan alle bovenstaande voorwaarden voldoet, zullen we geen juridische consequenties verbinden aan deze melding.
- Wij behandelen een melding vertrouwelijk en delen persoonlijke gegevens niet zonder toestemming van de melder met derden, tenzij dit wettelijk of uit hoofde van een rechterlijke uitspraak verplicht is.
- In onderling overleg kunnen we, indien u dit wenst, nadat maatregelen zijn genomen om de kwetsbaarheid te verhelpen, uw naam vermelden als de ontdekker van de gemelde kwetsbaarheid.
- Wij sturen u binnen <aantal> werkdagen een ontvangstbevestiging.
- Wij reageren binnen <aantal> werkdagen op een melding met de beoordeling van de melding en een verwachte datum voor een oplossing.

- Wij houden u op de hoogte van de voortgang van het oplossen van het probleem.
- In onderling overleg kan worden bepaald of en op welke wijze over het probleem, nadat het is opgelost, wordt gepubliceerd.

Wat doen we met door ons aangetroffen kwetsbaarheden bij anderen:

- <Naam organisatie> voert alleen onderzoek uit naar lekken in door derden beheerde informatiesystemen (onze samenwerkingspartners of leveranciers) na uitdrukkelijke toestemming hiervoor.
- Wij behouden ons het recht voor zonder voorafgaande kennisgeving onderzoek naar kwetsbaarheden uit te voeren op door derden aan de organisatie geleverde informatiesystemen en software als deze door ons zelf worden gehost en beheerd.
- Wij brengen zelf geen beveiligingslekken in software of systemen van derden in de publiciteit.
- Wij zullen door ons geconstateerde zwakke plekken z.s.m. melden aan de partij die verantwoordelijk is voor de hosting en/of het beheer van de informatiesystemen en software.
- Bij kwetsbaarheden in door de organisatie zelf gehoste en beheerde informatiesystemen en software brengen wij de leverancier hiervan op de hoogte.
- Door ons aangetroffen lekken of kwetsbaarheden worden tegelijkertijd ook bij het Nationaal Cyber Security Center van de Nederlandse overheid gemeld.

3 Responsible Disclosure – Te implementeren acties

De volgende acties in de organisatie zijn nodig om te voldoen aan de toezeggingen in de template.

- Creëer een nieuw (of benoem een bestaand) e-mailadres voor het ontvangen van meldingen in het kader van Resposible Disclosure.
- Beleg de beheertaak over dit e-mailadres bij een eenheid of persoon binnen de organisatie.
- Indien daar voor gekozen wordt: encryptiesleutel verstrekken aan de hacker op diens verzoek.
- Taken bij binnenkomst van een melding:
  a. controleer of contactgegevens compleet zijn;
  b. vraag zo nodig aanvullende gegevens op;
  c. mail ontvangstbevestiging aan de melder;
  d. escaleer in de lijn indien uit de gegevens blijkt dat de hacker zich niet heeft gehouden aan de afspraken. *)
- Acties n.a.v. de melding:
  a. uitzetten van de plannen en aansturen van de oplossing;
  b. communiceer verwachtte datum van oplossing aan de melder;
  c. houd de melder periodiek op de hoogte van de voortgang en eventuele verschuivende oplosdatum.
- Acties bij afronding van de melding:
  a. informeer de melder zodra de oplossing een feit is;
  b. maak afspraak over publicatie.

*) In geval de hacker zich buiten het kader begeeft, zal de lijnverantwoordelijk manager moeten bepalen hoe er gehandeld moet worden. In dit geval is het raadzaam juridisch advies in de winnen en in contact te treden met het NCSC. Ook in het kader van de Meldplicht Datalekken zal veelal een afweging noodzakelijk zijn.