Responsible Disclosure melding

De juridische entiteiten behorende tot de Royal Schiphol Group statutair gevestigd in Nederland zijn onderdeel van de vitale infrastructuur van Nederland. We vinden het daarom zeer belangrijk dat onze IT-systemen veilig zijn. Ondanks alle beveiligingsmaatregelen kan het gebeuren dat je een zwakke plek in onze digitale systemen vindt. Je kan ons dan helpen door een Responsible Disclosure melding te doen. In dit document ontdek je de belangrijkste regels voor het opsporen van beveiligingsproblemen en het doen van Responsible Disclosure meldingen.

Wat te doen als je een kwetsbaarheid in ons systeem vindt

Zodra je een zwakke plek in de ICT-systemen hebt gevonden, horen we dit graag direct van je. Dan kunnen we zo snel mogelijk de benodigde maatregelen nemen om dit probleem te verhelpen. Wij nemen meldingen over beveiligingsproblemen in ICT-systemen zeer serieus. Om hier op een verantwoorde manier mee om te kunnen gaan, maken we graag de volgende afspraken met je.

Hoe kan je dit melden?
Heb je iets ontdekt? Dan willen we dat graag direct weten.

- Mail je bevindingen zo snel mogelijk naar:
  responsible [punt] disclosure [apenstaartje] schiphol [punt] nl.
  Versleutel je e-mail indien mogelijk met de PGP-sleutel van Schiphol. Hiermee voorkomen we dat de informatie in verkeerde handen valt.
- Vertel in je mail hoe je op dit probleem bent gestuit, zodat we dit kunnen reproduceren. Omschrijf het probleem en geef het IP-adres of de URL door.
- Vermeld in je mail ook jouw contactgegevens zoals een e-mailadres of telefoonnummer. Dan kunnen we contact met je opnemen om samen te werken aan een veiligere oplossing.
- Je krijgt van ons zo snel mogelijk bericht terug over de verdere gang van zaken.

Fijn als we op je kunnen rekenen
We vertrouwen erop dat je verantwoordelijk omgaat met de informatie over het beveiligingsprobleem. We verwachten dat je deze kennis met niemand anders dan Schiphol deelt. Ook vragen we je vriendelijk om niet meer handelingen te verrichten om het beveiligingsprobleem aan te tonen. En mocht je via het lek vertrouwelijke gegevens hebben verkregen, wil je deze dan direct en onherroepelijk wissen?

Vermijd illegale handelingen
Zodra je een veiligheidsprobleem hebt ontdekt, is het belangrijk dit te melden en het probleem niet verder te onderzoeken. Het kan zijn dat je met goed bedoeld onderzoek illegale handelingen uitvoert, waardoor je de wet overtreedt. Zo is het niet toegestaan om:

- Het probleem met anderen te delen voordat het is opgelost.
- Malware te plaatsen.
- Gegevens in het systeem te kopiëren, te wijzigen of te verwijderen (een alternatief hiervoor is het maken van een directory listing van een systeem).
- Veranderingen aan te brengen in het systeem.
- Herhaaldelijk toegang tot het systeem te verkrijgen of de toegang delen met anderen.
- Gebruik te maken van het zogeheten ‘brute forcen‘ van toegang tot systemen.
- Gebruik te maken van denial-of-service of social engineering.
- Het probleem te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of gegevens van derden in te kijken, te verwijderen of aan te passen.

- Gebruik te maken van aanvallen op fysieke beveiliging, social engineering, distributed denial of service, spam of applicaties van derden.
- Jouw onderzoek te gebruiken om klantgegevens of andere persoonsgegevens openbaar te maken.
- Technieken te gebruiken die de beschikbaarheid van onze onlinediensten kunnen beïnvloeden.

Wat kan je melden?
Het is prettig als je problemen in onze digitale systemen wil melden zoals:

- Remote Code Execution
- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF)
- Injectiekwetsbaarheden
- Gebroken authenticatie en sessie management
- Kwetsbaarheden met betrekking tot encryptie
- Ongeautoriseerde toegang tot gegevens
- API's die onvoldoende beschermd zijn

Waar is de responsible disclosure niet voor bedoeld?

- Het indienen van een vraag, opmerking of klacht over de luchthaven.
- Vragen of klachten over de beschikbaarheid van Schiphol-websites of mobiele applicaties.

Internationaal recht en regelgeving:

Regelgeving met betrekking tot het melden van kwetsbaarheden kan per land verschillen. Wij raden je aan met deze regelgeving rekening te houden. Het is mogelijk dat je met jouw onderzoek de (internationale) wet overtreedt en je strafrechtelijke vervolging riskeert. Heb je kwetsbaarheden gevonden in onze IT-systemen, dan moet je je realiseren dat de regels van de wet boven de regels die Schiphol zelf hanteert staan. Niettemin, als je te goeder trouw en volgens de regels van Schiphol handelt, zullen we jouw acties niet melden bij de autoriteiten, tenzij we dit juridisch verplicht zijn.

Wat mag je van ons verwachten?

- Indien je bij de melding van een door jouw geconstateerde kwetsbaarheid in een ICT-systeem van Schiphol aan bovenstaande voorwaarden voldoet, zal Schiphol geen juridische consequenties verbinden aan deze melding.
- Schiphol behandelt een melding vertrouwelijk en deelt persoonlijke gegevens niet zonder toestemming van de melder met derden, tenzij dit juridisch verplicht is.
- We sturen je binnen vijf werkdagen een ontvangstbevestiging.
- Op korte termijn kan je een reactie op een melding verwachten. Hierin vermelden we de beoordeling van de melding en een verwachte datum voor een oplossing.
- We houden je op de hoogte van de voortgang in het oplossen van het probleem.
- Schiphol lost het door jou geconstateerde beveiligingsprobleem zo snel mogelijk op. We streven ernaar om dit binnen 90 dagen te doen. Na de oplossing kunnen we in overleg bepalen of en op welke wijze we over het probleem extern communiceren.
- In onderling overleg kan Schiphol, indien je dit wenst en hiervoor toestemming geeft, jouw naam vermelden als de ontdekker van de gemelde kwetsbaarheid in de "Schiphol's Responsible Disclosure Hall of Fame".

De Royal Schiphol Group Responsible Disclosure Hall of Fame

Op onze Responsible Disclosure Hall of Fame kunnen wij plaatsen:

- Jouw voornaam, achternaam en/of pseudoniem (naar jouw keuze)
- Omschrijving van de gevonden kwetsbaarheden
- Aantal van gevonden kwetsbaarheden per melder

Als voorwaarden vóór het plaatsen van een naam:

- Je stemt in met algemene privacy voorwaarden van de Schiphol Group, die kun je hier vinden.
- Je bent de eerste die de kwetsbaarheid/bug meldt.
- Wij bepalen of de melding terecht als kwetsbaarheid gezien moet worden en hanteren daarbij industrie normen zoals (Common Vulnerability Scoring System) https://www.first.org/cvss/calculator/3.0 voor plaatsing.
- Je hebt je gehouden aan de regels in de responsible disclosure.
- De disclosure moet opgelost zijn vóór het plaatsen van je naam en details. Dit betekent dat je naam niet geplaatst wordt zolang Schiphol er voor kiest om het (nog) niet op te lossen.
- De melding wordt automatisch van de hall of fame gehaald na twee jaar.
- De melder heeft het recht op het corrigeren, wijzigen of verwijderen van zijn/haar persoonsgegevens.
- Bij onenigheid over (de aard van) de melding behoudt Schiphol Group het recht om de gehele melding van de “Hall of Fame” te verwijderen of niet te plaatsten.