Meldpunten Kwetsbaarheden (Responsible Disclosure)

FI-ISAC

Help ons de veiligheid van onze (virtuele) dienstverlening continu te verbeteren. <BANK> vindt het belangrijk dat klanten veilig kunnen bankieren. Wij stellen ons daarom open voor deskundigen om ons hierbij te ondersteunen door gevonden mogelijke zwakke plekken aan ons te melden.

Waarom werken aan systeemveiligheid

Elke dag werken specialisten bij <BANK> aan het verbeteren van de systemen en processen, zodat de gegevens van onze klanten beschermd worden tegen misbruik en de beschikbaarheid van de dienstverlening gewaarborgd is. Dat neemt niet weg dat ook in onze systemen zich kwetsbaarheden kunnen voordoen. Daarbij maken we graag gebruik van uw hulp.

Wat kunt u van ons verwachten

U kunt problemen melden die betrekking hebben op de veiligheid van diensten die <BANK> aanbiedt via internet. Mocht u een probleem of zwakke plek gevonden hebben, meld dit ons dan zo snel mogelijk. Voorbeeld van kwetsbaarheden die gemeld kunnen worden:

- Cross site scripting kwetsbaarheden.
- SQL injectie kwetsbaarheden.
- Encryptie zwakheden.

Wat verwachten wij van u

Zorg ervoor dat u tijdens het onderzoeken van de gevonden kwetsbaarheid geen schade aanricht. In geen geval mag uw onderzoek tot onderbreking van de dienstverlening leiden of tot openbaarmaking van bank- of klantgegevens.

Wie kan melding maken

Ieder inzake internetbeveiliging deskundig persoon die een mogelijke zwakte in de systemen van <BANK> heeft ontdekt.

Wat doen we met uw melding

Een team van beveiligingsexperts onderzoekt uw melding en geeft binnen 2 werkdagen een eerste reactie. Maak het probleem niet publiek, maar praat met onze experts en geef hen de tijd het probleem op te lossen. Wij laten u weten wat we van uw melding vinden, of we een oplossing gaan toepassen en wanneer we dat plannen te doen.

Spelregels

Bij het onderzoek zou u mogelijk handelingen kunnen verrichten die strafbaar zijn. Als u te goeder trouw, zorgvuldig en volgens de aangegeven spelregels handelt, is er voor de bank geen aanleiding om aangifte te doen. Volgt u daarom de regels zoals opgenomen in deze responsible disclosure regeling en handel daarnaast niet op onevenredige wijze:

- Maak geen gebruik van social engineering om toegang te verkrijgen tot een systeem.
- Plaats geen backdoor in een informatiesysteem om vervolgens daarmee de kwetsbaarheid aan te tonen, aangezien daarmee aanvullende schade kan worden aangericht en onnodige veiligheidsrisico's worden gelopen.

- Maak minimaal gebruik van een kwetsbaarheid, doe alleen datgene wat noodzakelijk is om de kwetsbaarheid vast te stellen.
- Wijzig of verwijder geen enkel gegeven van het systeem, en wees zo terughoudend mogelijk met het kopiëren van gegevens (als één record genoeg is om het probleem aan te tonen, ga dan niet verder).
- Breng geen systeemveranderingen aan.
- Probeer niet herhaaldelijk toegang tot het systeem te verkrijgen en deel de verkregen toegang niet met anderen.
- Gebruik geen zogeheten “bruteforce” om toegang tot systemen te verkrijgen, daarbij is immers geen sprake van een kwetsbaarheid, maar alleen van het herhaaldelijk proberen van wachtwoorden.

Hoe moet ik de melding doen

Heeft u een kwetsbaarheid gevonden, neem dan contact met ons op via e-mail: <responsibledisclosure@BANK>. Gebruikt u hiervoor de volgende PGP key: <RD PUBLIC PGP KEY BANK>.
Beschrijf het gevonden probleem zo uitgebreid mogelijk. Houd er rekening mee dat uw melding door specialisten wordt ontvangen; een korte specifieke beschrijving of bewijs is voldoende.
U kunt ook een kwetsbaarheid anoniem melden. We kunnen in dat geval geen afspraken met u maken over de opvolging van uw melding, over een eventuele beloning voor de melding en over het doen van aangifte.

Beloning

Voor gemelde kwetsbaarheden die daadwerkelijk door ons zijn verholpen of tot verandering van de dienstverlening hebben geleid, zult u als dank een passende vergoeding ontvangen. <BANK> beslist of de melder hiervoor in aanmerking komt en beslist over de hoogte van de vergoeding.

Wat niet melden

Het meldpunt <responsible-disclosure@BANK> is niet bedoeld voor het:

- Indienen van klachten over de dienstverlening.
- Doen van fraudemeldingen en/of vermoedens van fraude.
- Melden van nepmails of phishing e-mails.
- Melden van virussen.
- Indienen van klachten of vragen over de beschikbaarheid van de website of internetbankieren.
- Melden van problemen met betrekking tot geldautomaten.

Voor deze bevindingen kunt u meer informatie vinden op <LINK NAAR HELP PAGINA’S>.

Uw privacy
Voor het verloop zullen we u vragen om contactgegevens (naam, email, PGP key, en eventueel telefoon) te verstrekken (tenzij u anoniem een melding heeft gedaan). Wij zullen uw identiteit niet zonder uw instemming aan derden vrijgeven of uw gegevens voor andere doeleinden gebruiken dan om passende opvolging te geven aan uw melding, tenzij daartoe een wettelijke plicht bestaat, bijvoorbeeld bij vordering door justitie.

Overige voorwaarden
Wij kunnen alleen meldingen aannemen die in het Nederlands of Engels opgesteld zijn. Voor de uitkering van beloningen hebben wij uw persoonsgegevens nodig. Mochten meerdere melders tegelijk dezelfde bevinding melden, dan is de vergoeding voor de eerste melder.

Nationaal Cyber Security Center
Deze responsible disclosure regeling is tot stand gekomen in overleg met het Nationaal Cyber Security Centrum (www.ncsc.nl) en op basis van de leidraad van het NCSC.