Beleid inzake het op een Verantwoorde Wijze Melden van Kwetsbaarheden

1. Overzicht

1.1 Doel

Batopin NV streeft ernaar om veilige systemen en diensten aan het grote publiek aan te bieden door passende beveiligingsmaatregelen en -processen te implementeren ter bescherming van de informatie die het verwerkt. Hoewel we ernaar streven een hoog beveiligingsniveau te handhaven, kunnen er toch kwetsbaarheden aanwezig zijn.
Het doel van dit beleid is om iedereen met de relevante vaardigheden een duidelijk kader te bieden voor het op verantwoorde wijze identificeren en melden van mogelijke beveiligingskwetsbaarheden. Het beleid beschrijft tevens de procedure voor het indienen van informatie over kwetsbaarheden bij Batopin NV, zodat wij gemelde beveiligingsproblemen kunnen onderzoeken, valideren en verhelpen.

1.2 Toepassingsgebied

Dit Beleid is van toepassing op alle kwetsbaarheden op het gebied van informatiebeveiliging die door derden worden vastgesteld in:
• openbare geldautomaatinterfaces die door Batopin worden beheerd
• cash.be
• batopin.be
Andere systemen die door Batopin worden beheerd of gebruikt, vallen uitdrukkelijk buiten het toepassingsgebied en mogen niet worden getest in het kader van dit beleid.

2. Beleid inzake het Melden van Kwetsbaarheden

2.1 Onderzoek

Op voorwaarde dat u te goeder trouw handelt, zich houdt aan het toepassingsgebied, de voorwaarden en de beperkingen van dit beleid, en alle toepasselijke wet- en regelgeving naleeft, is Batopin niet van plan juridische stappen tegen u te ondernemen in verband met uw onderzoeken naar kwetsbaarheden.

2.1.1 Algemene voorwaarden

Aan de volgende voorwaarden moet worden voldaan bij het uitvoeren van een beveiligingsonderzoek op de toegestane systemen:

- Batopin zo snel mogelijk op de hoogte brengen nadat een beveiligingskwetsbaarheid werd vastgesteld;
- Geen misbruik maken van kwetsbaarheden verder dan strikt noodzakelijk is om de kwetsbaarheid aan te tonen. Er moet evenredigheid worden gehandhaafd: als de kwetsbaarheid op een kleine schaal kan worden aangetoond, mogen er geen verdere acties worden ondernomen;
- De toegang met niemand delen;
- Onmiddellijk stoppen met testen en de kwetsbaarheid melden indien klantinformatie, persoonsgegevens, authenticatiegegevens, transactiegegevens of andere vertrouwelijke informatie toegankelijk worden;
- Het testen moet zodanig worden uitgevoerd dat verstoring, verslechtering of onderbreking van de diensten en systemen van Batopin wordt voorkomen;
- Eventuele achterdeurtjes, toegangsmogelijkheden en persistentie moeten worden verwijderd nadat de kwetsbaarheid werd aangetoond.

2.1.2 Verboden handelingen

De volgende handelingen zijn ten strengste verboden tijdens het onderzoek:

- Het openen, verwerken of kopiëren van gegevens, tenzij dit strikt noodzakelijk is voor het uitvoeren van uw onderzoek. Na afloop van het onderzoek moeten de gegevens definitief worden vernietigd;
- Het wijzigen, verwijderen of anderszins beschadigen van gegevens en systemen;
- Het installeren van malware;
- Alle technieken die uitsluitend tot doel hebben de beschikbaarheid van onze systemen en diensten te beïnvloeden, zoals (Distributed) Denial of Service ((D)DOS)-aanvallen, belastingstests (“loadtests”) en stresstests;
- Elke poging om de fysieke beveiligingsmaatregelen te omzeilen;
- Social engineering en phishing-aanvallen;
- Spammen;
- Het stelen van wachtwoorden of brute-force-technieken;
- Vandalisme;
- Elke poging om contant geld op te nemen, transacties te wijzigen, de

verwerking van transacties te verstoren of de financiële activiteiten op andere wijze te beïnvloeden.

2.1.3 Vertrouwelijkheid

Derden moeten alle informatie die tijdens het onderzoek werd verkregen strikt vertrouwelijk behandelen en mogen deze informatie niet delen, openbaar maken of op enige andere wijze gebruiken voor andere doeleinden dan het melden van de kwetsbaarheid aan Batopin.

Indien de kwetsbaarheid mogelijk ook gevolgen heeft voor andere organisaties in België, mag de verantwoordelijke derde het Centrum voor Cybersecurity België hiervan op de hoogte brengen zonder gedetailleerde informatie over Batopin prijs te geven.

Openbaarmaking, publicatie, bespreking op sociale media, presentaties op conferenties of het delen van details over de kwetsbaarheid met andere partijen is niet toegestaan, tenzij Batopin heeft bevestigd dat de kwetsbaarheid werd verholpen of vooraf schriftelijke toestemming heeft verleend.

Nadat de oplossing door Batopin werd bevestigd of wanneer voorafgaande schriftelijke toestemming werd verkregen, mag de melder het bestaan van de kwetsbaarheid openbaar maken, op voorwaarde dat:

- Batopin vooraf op de hoogte wordt gesteld van de voorgenomen openbaarmaking;
- De openbaarmaking geen exploitcode, proof-of-concept-code, gedetailleerde aanvalinstructies, configuratiegegevens, schermafbeeldingen of enige andere informatie bevat die het misbruik van de kwetsbaarheid redelijkerwijs zou kunnen vergemakkelijken;
- Er geen vertrouwelijke informatie, persoonsgegevens, klantgegevens of andere veiligheidsgevoelige informatie met betrekking tot Batopin wordt bekendgemaakt;
- De openbaarmaking voldoet aan alle toepasselijke wet- en regelgeving.

2.2 Meldingen

Derden, waaronder beveiligingsonderzoekers en ethische hackers, worden aangemoedigd om geïdentificeerde kwetsbaarheden te melden via security@batopin.be. Meldingen kunnen anoniem worden ingediend. Wanneer contactgegevens worden verstrekt, ontvangt u een bevestiging van ontvangst van uw melding.

Op verzoek van de derde zal Batopin een beveiligde link verstrekken waarmee de kwetsbaarheidsmelding kan worden geüpload naar een beveiligde locatie die door Batopin wordt beheerd.

Bij het melden van een kwetsbaarheid raden wij u aan het volgende te verstrekken:

- Een beschrijving van de kwetsbaarheid
- Stappen om het probleem te reproduceren (scripts of schermafbeeldingen zijn nuttig)
- Mogelijke gevolgen
- Locatie van de kwetsbaarheid

Wij verzoeken u vriendelijk om meldingen in het Engels in te dienen.

Voor zover Batopin daartoe in staat is en voor zover wettelijk toegestaan, zal Batopin het bestaan van de kwetsbaarheid bevestigen.

Batopin streeft ernaar om:

- De ontvangst van kwetsbaarheidsmeldingen binnen 5 werkdagen te bevestigen;
- Een eerste beoordeling van de melding uit te voeren;
- Waar nodig updates tijdens het onderzoek te geven;
- Contact op te nemen met de melder wanneer aanvullende informatie nodig is.

Deze streefdoelen zijn indicatief en vormen geen bindende verplichtingen.

2.3 Beloningen

Batopin heeft momenteel geen beloningsprogramma voor kwetsbaarheden of een bug bounty-programma. Batopin kan, naar eigen goeddunken, erkenning geven voor geldige meldingen. Dergelijke erkenning is niet gegarandeerd en wordt per geval beoordeeld.

2.4 Vragen

Vragen over dit beleid kunt u sturen naar security@batopin.be. Wij nodigen u ook uit om contact met ons op te nemen met suggesties ter verbetering van dit beleid.