Richtlinie zur verantwortungsvollen Offenlegung von Sicherheitslücken

1. Überblick

1.1 Zweck

Batopin NV hat sich verpflichtet, der Öffentlichkeit sichere Systeme und Dienste zur Verfügung zu stellen, indem wir geeignete Sicherheitsmaßnahmen und -verfahren zum Schutz der von uns verarbeiteten Informationen anwenden. Obwohl wir bestrebt sind, ein hohes Maß an Sicherheit aufrechtzuerhalten, können dennoch Sicherheitslücken bestehen.
Zweck dieser Richtlinie ist es, den Personen, die über die entsprechenden Kompetenzen verfügen, ein eindeutiges Rahmenwerk für die verantwortungsvolle Erkennung und Meldung potenzieller Sicherheitslücken zur Verfügung zu stellen. Außerdem definiert die Richtlinie das Verfahren zur Weitergabe von Informationen über Sicherheitslücken an Batopin NV, anhand dessen es uns möglich ist, gemeldete Sicherheitsprobleme zu untersuchen, zu beurteilen und zu beheben.

1.2 Geltungsbereich

Diese Richtlinie gilt für alle Sicherheitslücken im Bereich der Informationssicherheit, die Dritte in folgenden Bereichen festgestellt haben:
• von Batopin betriebene, öffentlich zugängliche ATM-Schnittstellen
• cash.be
• batopin.be
Andere von Batopin verwaltete oder verwendete Systeme fallen ausdrücklich nicht in den Geltungsbereich dieser Richtlinie und sind nicht für Testzwecke im Rahmen dieser Richtlinie zugelassen.

2. Richtlinie zur Offenlegung von Sicherheitslücken

2.1 Untersuchung

Unter der Voraussetzung, dass Sie nach Treu und Glauben handeln, den Geltungsbereich, die Voraussetzungen und Einschränkungen dieser Richtlinien einhalten und alle geltenden Gesetze und Vorschriften befolgen, hat Batopin nicht die Absicht, im Zusammenhang mit von Ihnen durchgeführten Untersuchungen von Sicherheitslücken rechtliche Schritte gegen Sie einzuleiten.

2.1.1 Allgemeine Voraussetzungen

Bei der Durchführung einer Sicherheitsuntersuchung der zugelassenen Systeme sind folgende Voraussetzungen einzuhalten:

- Batopin ist so bald wie möglich nach Ihrer Entdeckung einer Sicherheitslücke zu benachrichtigen;
- Nutzen Sie Sicherheitslücken nicht über das zum Nachweis der Sicherheitslücke unbedingt erforderliche Maß hinaus aus. Die Verhältnismäßigkeit muss gewahrt bleiben: Wenn die Sicherheitslücke anhand eines kleines Falls nachgewiesen werden kann, dürfen keine weiteren Maßnahmen ergriffen werden;
- Teilen Sie den Zugang mit niemand anderem;
- Stellen Sie die Prüfung unverzüglich ein und melden Sie die Sicherheitslücke, wenn Kundendaten, personenbezogene Daten, Authentifizierungsdaten, Transaktionsdaten oder andere vertrauliche Informationen zugänglich werden;
- Die Tests müssen so durchgeführt werden, dass Störungen, Beeinträchtigungen oder Unterbrechungen von Batopins Diensten und Systemen vermieden werden;
- Sämtliche Hintertüren, Zugriffsmöglichkeiten und Persistenzen sind zu beseitigen, nachdem die Sicherheitslücke demonstriert wurde.

2.1.2 Verbotene Maßnahmen

Folgende Maßnahmen im Rahmen der Untersuchung sind strengstens verboten:

- Der Zugriff, die Verarbeitung und das Kopieren von Daten, es sei denn, dies ist für die Durchführung Ihrer Untersuchung unbedingt erforderlich. Nach der Untersuchung sind die Daten endgültig zu vernichten;
- Die Veränderung, Löschung oder sonstige Beschädigung von Daten und Systemen;
- Die Installation von Malware;
- Sämtliche Techniken, die allein dem Zweck dienen, die Verfügbarkeit unserer Systeme und Dienste zu beeinflussen, wie z. B. (Distributed-)Denial-of-Service-Angriffe ((D)DOS-Angriffe)), Lasttests und Stresstests;
- Sämtliche Versuche, die physischen Sicherheitskontrollen zu umgehen;
- Social Engineering und Phishing-Angriffe;
- Spamming;

- Der Diebstahl von Passwörtern und Brute-Force-Angriffe;
- Vandalismus;
- Jeder Versuch, Bargeld auszuzahlen, Transaktionen zu verändern, die Verarbeitung von Transaktionen zu stören oder die Finanztransaktionen anderweitig zu beeinflussen.

2.1.3 Geheimhaltung

Dritte müssen alle während der Untersuchung erlangten Informationen streng vertraulich behandeln und dürfen solche Informationen nicht für andere Zwecke als zur Meldung der Sicherheitslücke an Batopin weitergeben, offenlegen oder anderweitig verwenden.

Falls die Sicherheitslücke möglicherweise auch andere Organisationen in Belgien betrifft, kann der verantwortliche Dritte das Zentrum für Cybersicherheit Belgien informieren, ohne dabei detaillierte Batopin-Informationen offenzulegen.

Die Bekanntgabe, Veröffentlichung, Diskussion in den sozialen Medien, Präsentation auf Konferenzen und Weitergabe von Einzelheiten zur Sicherheitslücke an andere Parteien ist nicht zulässig, es sei denn, Batopin hat die Behebung bestätigt oder im Voraus eine schriftliche Genehmigung erteilt.

Nach Bestätigung der Behebung durch Batopin oder wenn eine vorherige schriftliche Genehmigung eingeholt wurde, darf die meldende Person das Vorliegen der Sicherheitslücke offenlegen, sofern

- Batopin im Voraus über die beabsichtigte Offenlegung informiert wird;
- Die Offenlegung keine Exploit-Codes, Proof-of-Concept-Codes, detaillierten Anweisungen für Angriffe, Konfigurationsdetails, Screenshots oder anderen Informationen enthält, welche nach billigem Ermessen die Ausnutzung der Sicherheitslücke erleichtern könnten;
- Keine vertraulichen Informationen, personenbezogenen Daten, Kundendaten oder andere sicherheitsrelevante Informationen im Zusammenhang mit Batopin offengelegt werden;
- Die Offenlegung alle geltenden Gesetze und Vorschriften erfüllt.

2.2 Meldung

Dritte, einschließlich IT-Sicherheitsforscher und Ethical Hacker, werden aufgefordert, die ermittelten Sicherheitslücken per E-Mail an security@batopin.be zu melden. Die Meldungen können anonym eingereicht werden. Sofern Sie uns Ihre Kontaktdaten mitgeteilt haben, bestätigen wir den Eingang Ihrer Meldung.

Auf Anfrage des Dritten stellt Batopin einen sicheren Link bereit, über den die Meldung der Sicherheitslücke auf eine von Batopin verwaltete sichere Internetadresse hochgeladen werden kann.

Wenn Sie uns eine Sicherheitslücke melden, bitten wir Sie freundlich, Folgendes zur Verfügung zu stellen:

- Eine Beschreibung der Sicherheitslücke
- Schritte zur Nachstellung des Problems (Skripte oder Screenshots wären hilfreich)
- Informationen über die potenzielle Auswirkung
- Ort der Sicherheitslücke

Wir bitten Sie, die Meldungen in englischer Sprache einzureichen.

Batopin wird das Vorliegen der Sicherheitslücke nach bestem Wissen und Gewissen bestätigen, sofern dies gesetzlich zulässig ist.

Batopin ist bestrebt,

- Den Eingang von Meldungen über eine Sicherheitslücke innerhalb von 5 Geschäftstagen zu bestätigen;
- Eine Erstanalyse der Meldung vorzunehmen;
- Im Laufe der Untersuchung Aktualisierungen zur Verfügung zu stellen, sofern diese zweckmäßig sind;
- Sich mit der meldenden Person in Verbindung zu setzen, falls weitere Informationen erforderlich sind.

Diese Zielsetzungen sind Orientierungswerte und stellen keine verbindlichen Verpflichtungen dar.

2.3 Prämien

Batopin bietet gegenwärtig weder eine Prämie für das Auffinden einer Sicherheitslücke, noch betreiben wir ein Bug-Bounty-Programm. Batopin kann validierte Meldungen nach eigenem Ermessen anerkennen. Eine solche Anerkennung ist nicht gewährleistet und unterliegt der Einzelfallbeurteilung.

2.4 Fragen

Fragen zu dieser Richtlinie richten Sie bitte an folgende E-Mail-Adresse: security@batopin.be. Wir bitten Sie, auch Kontakt mit uns aufzunehmen, falls Sie Vorschläge zur Verbesserung dieser Richtlinie haben.