Computer Security Incident Response Team of the National bank of Ukraine (CSIRT-NBU) – RFC 2350

1. Document Information

This document contains a description of CSIRT-NBU in accordance with RFC 2350. It provides basic information about CSIRT-NBU, its channels of communication, and its roles and responsibilities.

1.1. Date of Last Update

This document was updated on 24.05.2023. Version 1.2.

1.2. Distribution List for Notifications

Notifications will be sent to the representatives of the Constituency.

1.3. Locations where this Document May Be Found

The current version of this document can be found at:
https://cyber.bank.gov.ua/rfc2350.pdf

1.4. Authenticating this Document

This document has been signed with the PGP key of CSIRT-NBU. See section 2.8 for more details.

1.5. Document Identification

Title: "RFC 2350 CSIRT-NBU"
Version: 1.2
Document Date: May 2023
Expiration: This document is valid until superseded by a later version.

2. Contact Information

2.1. Name of the Team

Computer Security Incident Response Team of the National bank of Ukraine.
Short name: CSIRT-NBU.

2.2. Address

National bank of Ukraine, CSIRT-NBU
01601, Kyiv, Institutska 9
Ukraine

2.3. Time Zone

Time-zone: Europe/Kyiv

2.4. Telephone Number

+380445273818

2.5. Facsimile Number

None

2.6. Electronic Mail Address

E-mail address of team CSIRT-NBU@bank.gov.ua
Days/Hours of Operation: 09:00 to 18:00, Monday to Friday.

2.7. Other Telecommunication

None

2.8. Public Keys and Encryption Information

PGP/GPG is supported for secure communication.
CSIRT-NBU has a public PGP/GPG key for CSIRT-NBU@bank.gov.ua
Fingerprint: 8FBB E0F9 7B77 50C9 0069 DA94 38DA 9545 95B4 BE85
https://csirt.bank.gov.ua/storage/csirt-nbu.asc

2.9. Team Members

The Head of CSIRT-NBU is Oleksandr KLOK. The team includes 10 staff members.

3. Charter

3.1. Mission Statement

Organization and provision of cyber defense of the National Bank of Ukraine, monitoring, detection of cyber incidents and counteraction to cyber threats in the National Bank.
Support and assistance to the subjects of the banking system of Ukraine on issues of cyber defense, response and counteraction to cyber attacks, informing about current cyber threats, indicators of cyber threats and recorded attempts to commit cyber attacks.
Cooperation with international and foreign organizations on cyber incident response, exchange of information on implemented and potential cyber threats, exchange of experience in cyber security, innovative methods and practices in cyber security.

3.2. Constituency

The CSIRT-NBU Constituency includes financial and insurance organizations adherent to CSIRT-NBU.

3.3. Authority

The Computer Security Incident Response Team CSIRT-NBU was established in 2018 and operates within the Cyber Security Center of the National Bank of Ukraine.

CSIRT-NBU support and protect the banking system of Ukraine and the National Bank of Ukraine from cyber threats.

The main activity of CSIRT-NBU is to detect, counteract and eliminate the consequences of cyber incidents in the banking system of Ukraine.

CSIRT-NBU performs its functions in compliance with the national cybersecurity strategy and is a sectoral CSIRT for the banking and financial sectors of Ukraine. In its activity the CSIRT-NBU is guided by the principles of mutually beneficial cooperation in the banking and financial sectors of Ukraine.

4. Policies

4.1. Types of Incidents and Level of Support

CSIRT-NBU is authorized to handle and coordinate cyber security incidents of the Constituency. Depending on the security incident’s nature, CSIRT-NBU will gradually roll out its services which include incident response coordination, alerting, and escalation to the CERT-UA.

4.2. Co-operation, Interaction and Disclosure of Information

CSIRT-NBU highly regards the importance of operational cooperation and information sharing between CERTs and with other organizations, which may contribute towards or make use of their services.

CSIRT-NBU operates within the confines imposed by UA legislation.

4.3. Communication and Authentication

CSIRT-NBU proceed all the information accordingly to the Information Protection Policy during handling and disclosure of information.

CSIRT-NBU observes the Traffic Light Protocol (TLP) and handle all the information accordingly to Information Sharing Policy.

CSIRT-NBU protects sensitive information in accordance with relevant regulations and policies within the Ukraine.

CSIRT-NBU respects the sensitivity markings allocated by originators of information communicated to CSIRT-NBU (originator control).

Communication security (encryption and authentication) is achieved by various means: S/Mime based email encryption, PGP, or other agreed means, depending on the sensitivity level and context.

5. Services

5.1. Incident Response

CSIRT-NBU assists its constituency in handling the technical aspects of cyberincidents. It includes incident report acceptance, technical data analysis and assistance, incident management coordination:

1. Incident Report Acceptance
2. Incident Analysis
3. Incident Response Support
4. Incident Response Coordination

5.2. Proactive Risk Monitoring

CSIRT-NBU offer proactive risk monitoring service, including intelligence on current cyber threats and potential vulnerabilities, collecting information from various sources, researching and analysing data:

1. detection of phishing domains
2. detection of data leakage
3. detection of compromised data of bank users' and customers' accounts
4. monitoring of potential vulnerabilities

5.3. Information services (Communication)

Service of informing banks about current cyber threats and vulnerabilities, measures to counter cyber attacks and security measures necessary to protect customer information systems.

Information exchange and interaction in responding to cyber incidents/cyber attacks is carried out in accordance with the requirements of the Procedure for Information Exchange between Ukrainian Banks and the Cyber Security Centre of the NBU on cyber defence and is carried out through:

1. The portal of the Cyber Security Centre – is a specialised website of the NBU designed to organise interaction and provide services by the Cyber Security Centre. For authorised connection to the portal of the Cyber Defence Centre, you need to register in accordance with the Connection Procedure.

2. MISP-NBU – is a specialised website of the NBU built on the basis of the MISP open source platform for the joint exchange of information on malware and cybersecurity threats. For authorised connection to MISP-NBU, you need to complete the registration procedure in accordance with the Connection Procedure.

3. Corporate messenger – a special system for the exchange of information messages between the participants of the information exchange. For an authorized connection, you need to go through the registration procedure in accordance with the Connection Procedure.

4. E-mail – for the exchange of information messages, the Cyber Security Centre uses the following e-mail accounts: CSIRT-NBU@bank.gov.ua – for the exchange of technical information.

5.4. Training and education

CSIRT-NBU provides service for conducting trainings and educational sessions to raise awareness and understanding in the field of cyber defence, cyber incident response, and countering current cyber threats.

6. Incident Reporting

CSIRT-NBU does not provide any public form for reporting incidents. Any member of the Constituency can send information about security incidents, threats, or related information to CSIRT-NBU either by sending an email, possibly encrypted, to CSIRT-NBU@bank.gov.ua or by filling out the reporting form.

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, CSIRT-NBU assumes no responsibility for errors or omissions, or for damages resulting from the use of information contained within.