BANCO DE PORTUGAL
EUROSISTEMA

CSIRT – BANCO DE PORTUGAL

RFC2350

TLP: WHITE
Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

TLP: WHITE information may be distributed without restriction, subject to copyright controls.

Table of Contents[1]

[1] Table of contents established according to RFC-2350

1. Document Information

This document describes the CSIRT of *Banco de Portugal* according to RFC 2350[2]. Essential information is provided about the CSIRT-BDP, describing its communication channels, roles and responsibilities.

1.1. Date of Last Update

First version was released on 1sh November, 2018.

Second version was released on the 1st July, 2019.

1.2. Distribution List for Notifications

There is no distribution list for notifications.

1.3. Locations where this Document May Be Found

The current and latest version of this document is available from CSIRT-BDP's website. Its URL is:

https://csirt.bportugal.pt/rfc2350.pdf

1.4. Authenticating this Document

This document has been signed with the PGP key of CSIRT-BDP. The signature can be accessed from CSIRT-BDP's website. Its URL is:

https://csirt.bportugal.pt

1.5. Document Identification

Title of Document: "BDP-CSIRT-RFC2350-EN_v1-1"

Version: 1.1

Document Date: 01-07-2019

Expiration: This document remains valid until superseded by a newer version.

[2] http://www.ietf.org/rfc/rfc2350.txt

2. Contact Information

2.1. Name of the Team

Full name: Banco de Portugal CSIRT

Short name: CSIRT-BDP

2.2. Address

CSIRT-BDP
DSI – DSICS – Unidade Centro de CiberSegurança

Rua Francisco Ribeiro, 2 1150-165 LisboaPORTUGAL

2.3. Time Zone

Portugal (Mainland) is in the Western European Time Zone. Western European Standard Time (WET) is Greenwich Mean Time (GMT).

Summer (Daylight-Saving) Time is observed in Portugal, with time shifted forward by 1 hour, 1 hour ahead of Greenwich Mean Time (GMT+1), starting on the last Sunday of March and ending on the last Sunday of October.

After that period, time is shifted back by 1 hour to Western European Time (WET) or (GMT) once again.

2.4. Telephone Number

+351 213 130 404 (regular response hours – 09h00 – 18h00)

2.5. Facsimile Number

Not available.

2.6. Other Telecommunication

Not available.

2.7. Electronic Mail Address

Any information about security incident or cyber threat targeting involving *Banco de Portugal*, please notify us at csirt@bportugal.pt.

For information related with activities and services, please contact us through the same address.

2.8. Public Keys and Encryption Information

The key ID is 0xC1CA6E33 and shall be used whenever information must be sent in a secure encrypted manner to CSIRT-BDP.

PGP Fingerprint: 5EA0 E994 0FF1 05B2 06F5 0322 CAA5 4360 C1CA 6E33

The key is available at https://csirt.bportugal.pt.

2.9. Team Members

The CSIRT-BDP team is composed by Cybersecurity and Intelligence Analysts. The team leader is Luis C. Gonçalves.

2.10. Other Information

General information about CSIRT-BDP can be found in the following URL:

https://csirt.bportugal.pt

2.11. Points of Customer Contact

The preferred method to report incidents is through the following address:

csirt@bportugal.pt

CSIRT-BDP team members are available to answer and support during regular response hours at this email. Regular response hours are usually restricted to regular Portuguese business hours (Monday to Friday, 09:30 to 18:00), excluding local Portuguese holidays.

For Emergency or Urgent cases the incident should be reported with [EMERGENCY] (within brackets) in the subject of the email.

Outside business hours an existing duty-officer will prompt for CSIRT-BDP involvement after communication evaluation.

3. Charter

3.1. Mission Statement

CSIRT-BDP's is the Computer Security Incident Response Team of Banco de Portugal. This unit is in charge of all Digital Forensics and Incident Response (DFIR) activities.

CSIRT-BDP's mission is to support and protect *Banco de Portugal* - the Portuguese national central bank – its business, interests and reputation from any kind of malicious attacks that would hamper or harm it. CSIRT-BDP's activities are constituted by Cyber-vigilance, anticipation, prevention, detection and response and recovery.

The key activities of CSIRT-BDP's operation and mission regarding its constituency are the following:

- Reduce overall corporate Cyber-Risk, through a proactive, preventive and anticipating manner, supporting Business Continuity;
- The promotion of a holistic and integrated corporate security context, according to the highest standards of ethics, integrity and honesty;
- Efficient response and recovery to Cybersecurity incidents, through high quality scenario approaches, as soon as possible;
- Creation, maintenance and development of information and knowledge sharing communities and platforms, as well as promotion of the cooperation between *Banco de Portugal*, its peers and the third-party companies related;
- Provide high quality research, analytical services and potential information security threats;
- Pursuing the objective of becoming recognized as an excellence centre of information security for national and international organizations.

3.2. Constituency

The constituency for CSIRT-BDP is composed by all elements of *Banco de Portugal's* information systems and business functions: its users, systems, applications and networks. CSIRT-BDP, notwithstanding the above cooperative services, can be provided through the Service Level Agreements and specific Cooperation Agreements.

3.3. Affiliation

CSIRT-BDP is affiliated to *Banco de Portugal* and maintains affiliations with various CSIRTs and CERTs in Portugal, Europe and other world regions, accordingly to the needs, the information exchanged and the cooperation principles of its mission and values.

3.4. Authority

CSIRT-BDP operates under the authority of the Deputy secretary General in charge of *Banco de Portugal*'s Information Systems Directorate.

4. Policies

4.1. Types of Incidents and Level of Support

CSIRT-BDP has the authority to coordinate, manage, handle and respond to all type of cyber threats, cyber attacks and computer security incidents which occur or threaten to occur and would be harmful to the business, interests and reputation of *Banco de Portugal*.

CSIRT-BDP services are rolled-out on a phased perspective, according to the type, criticality and potential impact of security incidents.

CSIRT-BDP level of support is also given based on the severity of the security event or incident, its potential or actual impact and the existing resources at the time.

4.2. Co-operation, Interaction and Disclosure of Information

CSIRT-BDP highly considers the paramount importance of operational coordination and information shared between CERTs, CSIRTs, SOCs and similar entities, as well as with other organizations, which may contribute to further deliver the services or which provides benefits to CSIRT-BDP.

CSIRT-BDP will cooperate with other entities on all subjects related to Cyber and Computer Security. Such cooperation includes the exchange of vital information regarding threats, security incidents, attack campaigns and vulnerabilities, as well as mitigation techniques. Nevertheless, CSIRT-BDP will promote information sharing on an anonymized way.

CSIRT-BDP will use provided information to help solve security incidents as all CERTs do. By default and as a principle, information which is distributed further to appropriate parties will be done accordingly to the “need-to-know” principle and preferably in an anonymized fashion.

CSIRT-BDP operates within the Portuguese legal framework and complies with the CSIRT Code of Practice (CCoP) version 2.1[3].

[3] https://www.trusted-introducer.org/CCoPv21.pdf

CSIRT-BDP recognizes, supports and uses the *Information Sharing Traffic Light Protocol – ISTLP*, version 1.1[4], classifying and handling information appropriately to such protocol, with the WHITE, GREEN, AMBER or RED tags.

4.3. Communication and Authentication

For normal communication (not containing sensitive information) CSIRT-BDP will use conventional methods like unencrypted e-mails. CSIRT-BDP protects sensitive information in accordance with relevant Portuguese and European regulations and policies within Portugal and the EU. In particular, CSIRT-BDP respects the sensitivity markings of all information communicated to CSIRT-BDP, allocated by its originators or contributors, commonly known as "originator control".

Sensitive information and communication security (including both encryption and authentication) is achieved by using PGP primarily or on any agreed means, depending on the sensitivity level and context.

5. Services

5.1. Proactive Activities and Announcements

Following a vigilant operation, CSIRT-BDP performs pre-emptive security analysis and controls to detect potential attacks, breaches and related threats, as well as reputational and brand risks, vulnerabilities or misconfigurations that may be leveraged in cyber attacks. Analysis of ongoing incidents with other organizations.

Such service aims to anticipate potential cyber threats by continuous monitoring of external corporate exposure and context (threat monitoring), creating a holistic threat landscape based also on a gathered threat intelligence.

Announcements about existing vulnerabilities and information (threat intelligence) are also provided as part of this service. Proactive service also includes technology watch, evaluation and adoption.

5.2. Incident Response (Triage, Coordination and Resolution)

CSIRT-BDP is responsible for the coordination of security events/incidents involving its constituency. CSIRT-BDP therefore handles both the triage and coordination aspects as well as incident response. The development of mitigation technique is left to the responsible

[4] https://www.trusted-introducer.org/ISTLPv11.pdf

administrators within the constituency. CSIRT-BDP, however will offer support and advice on request.

5.3. Alerting

CSIRT-BDP alerting service aims to disseminate information and “clipping” about cyber attacks, service disruption, vulnerabilities, malware spreading and activity, intrusion attempts that either happened or can possibly happen. The alerting service is complemented with recommendations to tackle its constituency’s security issues. This service can be provided to other similar parties, namely CSIRTs, CERTs, SOCs and similar entities, on a “need-to-know” basis.

5.4. Intrusion and Vulnerability Detection

CSIRT-BDP maintains and evolves a set of technologies, systems and processes with the aim of detecting potential intrusion events, as well as existing vulnerabilities. CSIRT-BDP reports on findings and offers support and advice, upon request, concerning mitigation techniques and incident handling. Within this service CSIRT-BDP has the ability to develop red team / blue team activities to its constituency as well as other parties, namely CSIRTs, CERTs, SOCs and similar entities, upon request.

5.5. Digital Forensics and Incident Response

CSIRT-BDP performs all DFIR activities for its constituency. The incident response service covers 7 steps: anticipation, preparation, identification, containment, eradication, recovery and lessons learned. CSIRT-BDP features an advanced service laboratory, where more in-depth analysis can be performed, such as malicious software analysis, reversal and response as well as physical forensic analysis. Such service can be provided to other parties, CSIRTs, CERTs, SOCs and similar entities, upon request.

5.6. Cyber threat and Cyber security Tool Development

CSIRT-BDP develops its own security tools for internal use, when improvements to existing technology landscape are necessary, in order to enhance defence capabilities and its overall mission and activities. Such security tools may be used by other members of its constituency or third-party entities like CSIRTs, CERTs, SOCs and similar entities, upon request or communications of interest.

5.7. Cooperation and Knowledge Sharing

BDP-CSIRT highly considers the paramount importance of cooperation and information sharing at all levels, between CERTs, CSIRTs, SOCs and similar entities, as well as with other organizations. Such service aims to contribute further on anticipation and proactivity, resulting from shared information and threat intelligence, in order to globally enhance security posture. This service aims the development and promotion of information sharing platforms, frameworks and databases, creating cooperation bonds between BDP-CSIRT and other parties.

6. Incident reporting Forms

No local forms have been developed yet to report incidents to CSIRT-BDP. In case of emergency or crisis, please report using the contacts previously defined, providing, at least, the following information:

- Contact details and organizational information – Person,organization name and address;
- Email address, telephone number;
- Summary description of the observation/event or incident;
- Attached evidences if there are any;
- Indicators of compromise (IOCs), FQDN(s), and any other relevant technical element with associated observation/event or incident;
- Should any email be forwarded to CSIRT-BDP, all email headers, body and any attachments should be included, if possible, as permitted by the regulations, policies and legislation under which operates the reporting party.

7. Disclaimers

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