INTESA SANPAOLO

RFC 2350 Profile for ISP-CERT

Contents

1. Document Information

This document contains a description of Intesa Sanpaolo CERT as implemented by RFC 23501. It provides basic information about ISP-CERT, channels of communication, roles and responsibilities.

1.1 Date of Last Update

This is version 1.00, published on October the 31st.

1.2 Distribution List for Notifications

Changes to this document are not distributed by a mailing list. Please address any specific questions or remarks to the Intesa Sanpaolo CERT e-mail address.

1.3 Locations where this Document May Be Found

The latest version of this document is available on http://www.group.intesasanpaolo.com and can also be requested to the CERT e-mail address.

1.4 Authenticating this Document

This document have been signed with the ISP-CERT's PGP key. The PGP key used is available from the Intesa Sanpaolo CERT's website or requested to the CERT e-mail address.

2. Contact Information

2.1 Name of the Team

Short Name: *ISP-CERT*

Full Name: *Intesa Sanpaolo CERT - Computer Emergency Readiness Team*

2.2 Address

Intesa Sanpaolo CERT

Via Lorenteggio 266, 20152 – Milano (MI) Italy

2.3 Time Zone

Central European Time Zone (GMT+0100 and GMT+0200 from the last Sunday of March to the last Sunday of October).

2.4 Telephone Number

+39 0287966093

2.5 Facsimile Number

None available

2.6 Other Telecommunication

None available.

2.7 Electronic Mail Address

If you need to notify the CERT about an information security incident or a cyber threat targeting or involving the Intesa Sanpaolo Group, please contact us at cert@intesasanpaolo.com

2.8 Public Keys and Other Encryption Information

PGP Key:

- ID: **664E68A8C8112465**
- Fingerprint: **7873 9A62 E5F8 1665 1F58 171B 664E 68A8 C811 2465**

The PGP key is available from the Intesa Sanpaolo CERT's website or requested to the CERT e-mail address.

2.9 Team Members

Corrado Lonati of Intesa Sanpaolo Group is the CERT officer. A full list of the CERT team members is not publicly available. Team members will identify themselves to the reporting parties with their full name in an official communication regarding an incident.

2.10 Other Information

None.

2.11 Points of Customer Contact

The preferred method for contacting the ISP-CERT is via e-mail at cert@intesasanpaolo.com.

The mailbox is monitored during regular office hours: Monday to Friday, 08.30 to 17.00 Central European Time Zone (GMT+0100 and GMT+0200 from the last Sunday of March to the last Sunday of October), except during public holidays in Italy.

Please use PGP if you plan to send sensitive information.

Urgent cases can be reported preferably by phone to +39 0287966093 which is monitored 24x7x365.

3. Charter

3.1 Mission Statement

The mission of the CERT in Intesa Sanpaolo is to:

- Identify threats which might have a potential impact on the Intesa Sanpaolo Group through security intelligence activities;
- Assess the threat landscape and coordinate the response so to prevent potential impacts on the Group's business;

- Keep the Group constituency informed on potential threats and attackers TTPs possibly before they are actively exploited;
- When an incident occurs, working closely with the other internal functions and stakeholders, ensure impacts are evaluated, the response actions are assigned and addressed correctly, the resulting remediation plan is effective;
- Actively develop and promote an information sharing network among the Costituency and with external entities;
- Coordinate the communication for the Group with supervisory authority and regulators;

3.2 Constituency

The Intesa Sanpaolo Group is a Financial institution. The Intesa Sanpaolo CERT constituencies consists of all entities of Intesa Sanpaolo Group, including the holding and all the affiliated entities.

The constituencies are located mainly in the following countries: Italy, Russia, Albania, Czech, Slovenia, Slovakia, Croatia, Romania, Egypt, Serbia, Bosnia Herzegovina, Hungary and in any other country where the Intesa Sanpaolo Group operates.

3.3 Sponsorship and/or Affiliation

Intesa Sanpaolo CERT is hosted by Intesa Sanpaolo Group Services (ISGS). It maintains contacts with other external incident response teams as well as with national and European institutions and government entities.

3.4 Authority

The ISP-CERT operates under the auspices of, and with authority delegated by, the Intesa Sanpaolo Group.

4. Policies

4.1 Types of Incidents and Level of Support

The ISP-CERT is authorized to handle critical incidents that occur, or threaten to occur, to the Intesa Sanpaolo Group.

The level of support given by ISP-CERT will vary depending on e.g. type and severity of the incident, the resulting impacts, the perimeter affected and the target involved.

ISP-CERT is also committed to keeping its constituency informed of potential threats and attackers TTPs possibly before they are actively exploited.

4.2 Co-operation, Interaction and Disclosure of Information

ISP-CERT highly regards the importance of operational cooperation and information sharing between Computer Emergency Response Teams and other organizations.

ISP-CERT operates under Intesa Sanpaolo rules based on the European privacy guidelines (“*95/46/EG*”) and the Italian information handling and disclosure law (“*Decreto Legislativo 30 June 2003 n. 196*” - "*Code for the Protection of Personal Data*").

ISP-CERT will use the information provided to help solving incidents occurred to other Computer Emergency Response Teams and other organizations. Information will only be distributed further to other teams and members by default on a need-to-know base, and preferably in an anonymized way. ISP-CERT supports the Information Sharing Traffic Light Protocol; information that comes in with the tags WHITE, GREEN, AMBER or RED will be handled accordingly.

4.3 Communication and Authentication

The preferred method of communication is via e-mail. Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data.

When the content is sensitive or requires authentication, the ISP-CERT PGP key is used for signing e-mail messages. All sensitive communication to ISP-CERT should be encrypted with the team's PGP key.

Network file transfers will be considered to be similar to e-mail for these purposes: sensitive data should be encrypted before transmission.

5. Services

ISP-CERT service offering is built around three key domains:

- Cyber Threat Surveillance
- Cyber incident Response
- Information Sharing

5.2 Reactive Services

5.2.1 Incident Response

ISP-CERT assists and coordinates the response to cyber security incidents within its constituency to ensure incidents are handled effectively and efficiently. In case of incident, ISP-CERT will support with respect to the following aspects of incident management:

5.2.1.1 Incident Triage

- Collection, correlation and analysis of the information provided by the various sources;
- Classification of the incident to determine the overall severity of the event on the bases of impacts assessment with the support of the company functions/entities involved;

5.2.1.2 Incident Coordination

- Coordination of the stakeholders, internal communication and escalation process;
- Identification of the appropriate actions and coordination of the response of the stakeholders involved;
- Coordination of the external reporting to authorities/regulators with support of the competent internal function;
- Constantly monitoring the progress of the assigned tasks and the severity of the incident;

5.2.1.3 Incident Resolution

- Advise the involved entity for designing and implementing the appropriate countermeasures;
- Support for restoring the affected service to its previous state;
- Constantly monitoring of the remediation plan;

5.2 Proactive Services

- Provide relevant information on threats to its constituency to raise security awareness and competence, mitigate the risks and help preventing security-related incidents;

6. Incident Reporting Forms

ISP-CERT provides a "Group Reporting Form" to its constituency.

In case an incident has to be reported from outside ISP-CERT's constituents, please report at least the following information, preferably using encrypted e-mail:

- Contact details of the reporting organizational (name, e-mail address, telephone);
- Date and Time of the occurrence of the event, if known;
- Type of Incident;
- Description of the incident;
- IP address(es), FQDN(s), and any other relevant technical element with associated observation;
- Any relevant artifact or log related to the event;

7. Disclaimers

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