EUROPEAN CENTRAL BANK

EUROSYSTEM

Andreas Erl
Principal Market Infrastructure Expert
Market Infrastructure Management Division

Arrangements to promote endpoint security in TARGET2

AMI-Pay meeting

Frankfurt am Main, 14 May 2019

Overview

Overview

Endpoint security arrangements in place

- Security and operational reliability of TARGET2 users
  - TARGET2 self-certification
    - in place since 2007
    - scope enlarged in 2017
    - first comprehensive exercise completed in 2018
  - Incident reporting
- SWIFT Customer Security Programme (CSP)
  - implemented by SWIFT following the Bangladesh heist
  - SWIFT users have to self-attest compliance with (mandatory) security controls imposed by SWIFT

Endpoint security arrangements in place

- Noteworthy:
  - different scope
  - scope of the TARGET2 self-certification is broader
- Contacts with operators of bigger RTGS systems suggest that TARGET2 is already quite advanced in terms endpoint security

Overview

The 2018 self-certification exercise

- TARGET2 participants were expected to return their self-certification forms by the end of 2018
- Methodology specifies four compliance levels
  - Fully compliant
  - Non-compliance levels ranging from 1 to 3
- Action plan had to be provided to the responsible central bank in case a Level 2 or Level 3 non-compliance was observed

TARGET self-certification – compliance overview

- 97% of the respondents indicated to be fully compliant

Level2 non-compliance	71
Action plan: compliance by 31 March 2019	7
Action plan: compliance after 31 March 2019	59
Participant not having provided any action plan	5

Level3 non-compliance	13
Action plan: compliance by 31 March 2019	0
Action plan: compliance after 31 March 2019	6
Participant not having provided any action plan	7

- A number of participants did not return their self-certification forms by the indicated deadline.
- 380 participants access TARGET2 via a SWIFT Service Bureau

TARGET2 self-certification - Next steps

- Action plan follow-up
- Annual exercise
- Critical participants: in 2019, for the first time the form needs to be signed by an (internal/external) auditor
- Service bureaus: analysis whether there is a concentration risk is in progress

The 2018 monitoring of the SWIFT CSP

- SWIFT users submit their self-attestation to the Know Your Customer- Self Attestation (KYC-SA) portal
- Central banks requested access to the self-attestations and observed the compliance of TARGET2 participants with the SWIFT CSP mandatory controls
- An action plan had to be provided in case a non-compliance was observed

Monitoring of the SWIFT CSP - compliance overview

- 86% of the TARGET2 users attested to be fully compliant

	"Broadly Compliant" participants		"Severely non-compliant" participants	
Total number of "non-compliant" participants	222		22	
of which % will be fully compliant by 31 March 2019	71	31.98%	5	22.73%
of which % will be fully compliant by 30 June 2019	78	35.14%	6	27.27%
of which % will be fully compliant by 31 Dec 2019	38	17.12%	4	18.18%
of which % will be fully compliant after 31 Dec 2019	3	1.35%	3	13.64%
of which % no information available	32	14.41%	4	18.18%

Monitoring of the SWIFT CSP - Next steps

- Action plan follow-up
- TARGET2 participants submitting action plans with deadlines beyond end 2019 will be contacted by their central bank
- The SWIFT Customer Security Controls Framework version 2019
  - promotes 3 advisory controls from the previous release to mandatory security controls; and
  - introduces 2 new advisory controls
- Compliance needs to be achieved by the end of 2019
- Another review of the self-attestation at the beginning of 2020

Arrangements to promote endpoint security - future challenges

1. Refining the existing arrangements in the current TARGET2 environment
2. Developing measures supporting the compliance process
3. Ensuring that endpoint security is properly managed in the context of the future consolidated T2-T2S environment

Questions?